HikCentral Professional V2.6.1 Web Client

User Manual

Legal Information

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- 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.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT 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

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 About This Document

This user manual is intended for the administrator of the system.

The manual guides you to establish and configure the security system. Follow this manual to perform system activation, access of the system, and configuration of the monitoring task via the provided Web Client, etc. To ensure the proper usage and stability of the system, refer to the contents below and read the manual carefully before installation and operation.

1.1 Introduction

The platform is developed for the management of security system and features flexibility, scalability high reliability, and powerful functions.

The platform provides features including central management, information sharing, convenient connection, and multi-service cooperation. It is capable of adding devices for management, live view, video storage and playback, face picture comparison, access control, time and attendance, alarm linkage, and so on.

Note

The modules on the platform vary with the License you purchased. For detailed information, contact our technical support.

The complete platform contains the following components. You can install the components according to actual needs.

Component	Introduction
System Management Service (SYS)	• Provides the unified authentication service for connecting with the clients and servers. • Provides the management for the users, roles, permissions, devices, and services. • Provides the configuration APIs for monitoring and management modules.
Streaming Service (Optional)	Provides forwarding and distributing the audio and video data of live view.

The following table shows the provided clients for accessing or managing the platform.

Client	Introduction
Control Client	Control Client is a C/S software which provides multiple operating functionalities, including live view, PTZ control, video playback and download, alarm receiving, log search, and so on.
Web Client	Web Client is a B/S client for managing system. It provides multiple functionalities, including device management, area management, recording schedule settings, event configuration, user management, and so on.
Mobile Client	Mobile Client is the software designed for getting access to the platform via Wi-Fi, 4G, and 5 G networks with mobile device. It fulfills the functions of the devices connected to the platform, such as live view, remote playback, PTZ control, and so on.

1.2 Recommended Running Environment

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

CPU

Intel® Core™ i5-8500 and later

Memory

8 GB and later

Web Browser

Internet Explorer® 11 and later, Firefox® 114 and later, Google Chrome® 114 and later, Safari® 16.6 and later, Microsoft® Edge 114 and later.

Note

Upgrading from V1.x to V2.x requires double available disk spaces than usual.

1.3 Application Summary

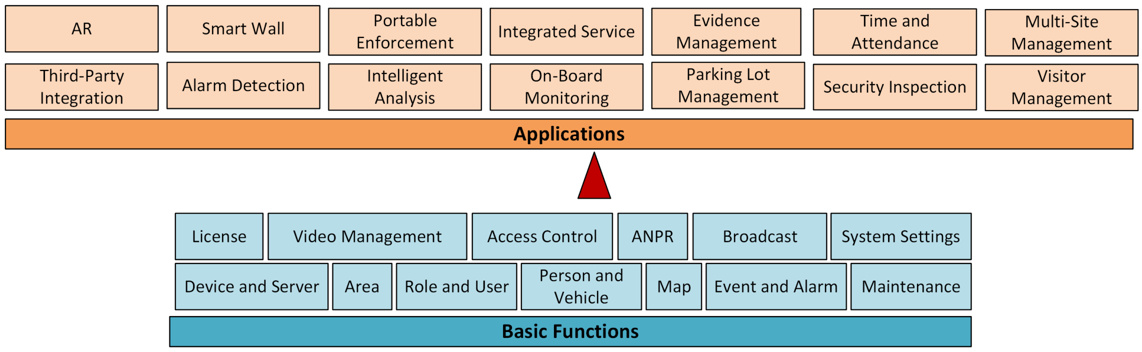


Figure 1-2 Application Summary

Table 1-1 Basic Functions in HikCentral Professional

Basic Function	Description
License	Refer to ***License Management*** for details.
Device and Server	Refer to ***Device and Server Management*** for details.
Area	Refer to ***Area Management*** for details.
Role and User	Refer to ***Management of Platform Accounts and Security*** for details.
Person and Vehicle	Refer to ***Person Management*** and ***Vehicle Management*** for details.
Map	Refer to ***Map Management*** for details.
Event and Alarm	Refer to ***Event and Alarm*** for details.
Maintenance	Refer to ***Maintenance*** for details.
System Settings	Refer to ***Set Basic Security Parameters*** and ***System Configuration*** for details.
Video Security and Management	Refer to ***Flow Chart of Video Security*** and ***Video Management*** for details.
ANPR (Automatic Number Plate Recognition)	Refer to ***ANPR (Automatic Number Plate Recognition)*** for details.
Access Control	Refer to ***Flow Chart of Door Access Control*** and ***Access Control Management*** for details.
Broadcast Management	Refer to ***Broadcast Management*** for details.

1.4 Document Guide

Learn

- ***Data Sheet***
- ***System Requirement and Performance***
- ***Compatibility List of Hikvision Products***
- ***Compatibility List of Third-Party Products***
- ***Product Comparison Between Free and Professional Version***
- ***AE Specification***
- ***Release Notes***
- ***Quick Start Guide of Mobile Client***

Start

- ***Quick Start Guide***
- ***Hardening Guide***

Use

- ***Web Client User Manual***
- ***Control Client User Manual***
- ***Frequently Asked Questions***

Chapter 2 Login

You can access and configure the platform via web browser directly, without installing any client software on the your computer.

Note

- The Web Client transmits data via the HTTPS, using our self-developed HTTPS certificate, which is not issued by the Certificate Authority. So that a risk prompt will show when you opening the Web Client. To avoid the prompt, you can apply for a certificate from the Certificate Authority.
- The login session of the Web Client will expire and a prompt with countdown will appear after the configured time period in which there is no action.

2.1 First Time Login

If this is the first time for you to login, you can choose to login as admin or normal user according to your user role.

2.1.1 Login for First Time for Admin User

By default, the system predefined the administrator user named admin. When you login via the Web Client for the first time, you are required to create a password for the admin user before you can properly configure and operate the system.

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   - You should set the transfer protocol before accessing the SYS. For details, refer to ***Set Transport Protocol*** .
   - You should set the SYS's IP address before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter a password and confirm the password for the admin user in the pop-up Create Password window, and click **Next**.

Note

The password strength can be checked by the system and should meet the system requirements. The default minimum password strength should be **Medium**. For setting minimum password strength, refer to ***Set Basic Security Parameters*** .

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

3. Select a method for password reset verification.
   - **Email**: Click **Verification Code → Next** and set the email address for receiving the password reset verification code.
   - **Security Question**: Click **Security Question → Next** , select three different security questions from the drop-down lists, and enter your answers accordingly.

Note

If you forget the password of your account, you can reset the password by verifying your email address or answering the security questions. Refer to ***Forgot Password*** for details.

4. Click **Finish**.

   The home page of the Web Client will show if the admin password is created successfully.

Result

After you logged in, the Site Name window opens and you can set the site name for the current system as you want.

Note

You can also set it in **System → Normal → User Preference** . See ***Set User Preference*** for details.

2.1.2 First Time Login for Normal User

When you log in to the system as normal user via Web Client for the first time, you should change the initial password and set a new password for login.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press the **Enter** key.

Example

If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

Note

You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and password.

Note

Contact the administrator for the user name and initial password.

3. Click **Log In** and the **Change Password** window opens.
4. Set a new password and confirm the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password.

Caution

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

5. Click **OK** to change the password.

Result

Web Client home page displays after you successfully logging in.

2.2 Login via Web Client (Administrator)

You can access the system via web browser and configure the system.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press **Enter** key.

Example

If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

Note

You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Select the **Management** tab.
3. Enter the user name and password.
4. Click **Log In** to log in to the system.

Note

- If failed password attempt of current user is detected, you are required to input the verification code. The failed password attempts from current client, other client, and other address will all require the verification code.
- The failed password attempt and verification code attempt from current client, other client (e.g., Control Client), and other address will all be accumulated. Your IP address will be locked for a specified period of time after specific number of failed password or verification code attempts detected.
- The account will be frozen for 30 minutes after 5 failed password attempts. The failed password attempts from current client, other clients (e.g., Control Client), and other addresses will all be accumulated.
- When the account is frozen after accumulated failed password attempts, you can still try login on another PC.
- The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password.
- If your password is expired, you will be asked to change your password when login.

Result

Web Client home page displays after you successfully logging in to the system.

2.3 Login via Web Client (Employee)

Employees can access the system via web browser.

Before You Start

The administrator should enable self-service login (enabled by default) and set the login password (employee ID by default) for employees.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press the **Enter** key.

Example

If the IP address of the PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

2. Select the **Self-Service** tab.
3. Enter the employee ID and password.
4. Click **Log In** to log in to the system.

Note

- Employees are required to change the password and set security questions for password retrieval upon the first login.
- If employees forget the password, they can retrieve the password in **Forgot Password** by answering security questions.
- If the password is expired, employees will be asked to change the password upon login.

Result

Web Client home page displays after employees successfully log in to the system.

2.4 Login via an Azure Account

After finishing required configurations on the Azure platform and importing domain users and persons to HikCentral Professional, you can log into HikCentral Professional with Azure account.

Before You Start

- Finish the configurations on the Azure platform including creating tenants, App registrations, and creating new groups and new users.
- Finish the configuration of the active directory on the HikCentral Professional. See ***Set Active Directory*** .
- Import domain users and domain persons to the HikCentral Professional. See ***Import Domain Users*** and ***Import Domain Persons*** .

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96,you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .
2. Select the **Management** tab.

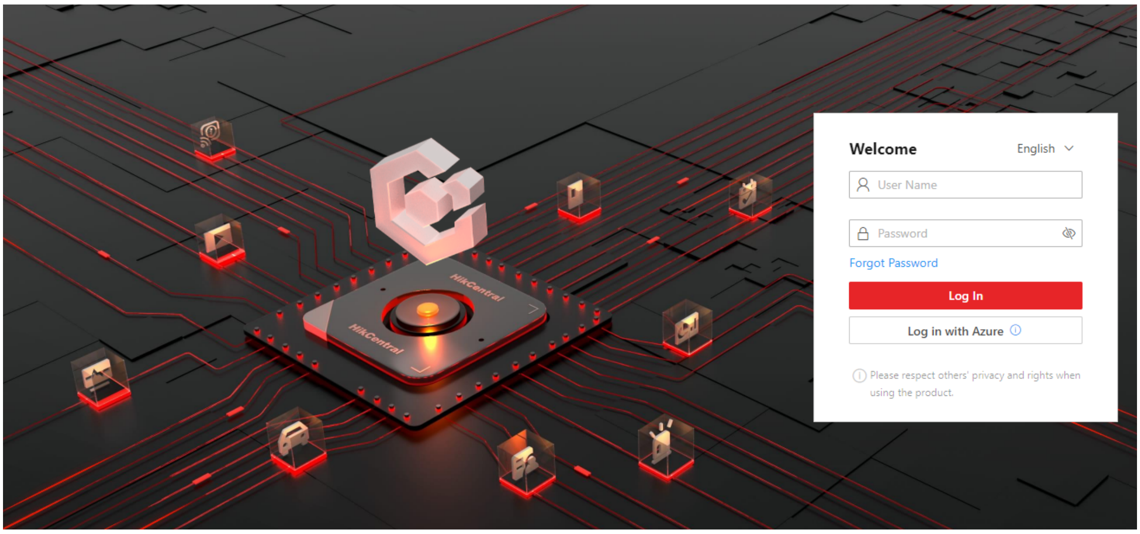


Figure 2-1 Login Page

3. Click **Log in with Azure**.

   For the first time login, the login page of the Microsoft will be displayed.

4. **Optional:** On the login page of the Microsoft, enter your domain account and password, and log in to the account.

   The home page will be displayed after you successfully logging in to the system.

2.5 Change Password for Reset User

When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral Professional via the Web Client.

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and initial password set by the administrator.
3. Click **Log In** and a **Change Password** window opens.
4. Set a new password and confirm the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password.

Caution

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

5. Click **OK**.

Result

Web Client home page displays after you successfully changing the password.

2.6 Forgot Password

If you forget the password of your account, you can reset the password.

Before You Start

- Make sure the normal user has been configured with an available email address.
- Make sure the email server is tested successfully.

Steps

1. On the login page, click **Forgot Password**.
2. Enter your user name and click **Next**.
3. Enter the required information on the Reset Password window.
   - If you are the admin user whose account is configured with security questions, you can select and answer the corresponding questions, click **Next**, and set and confirm your new password.

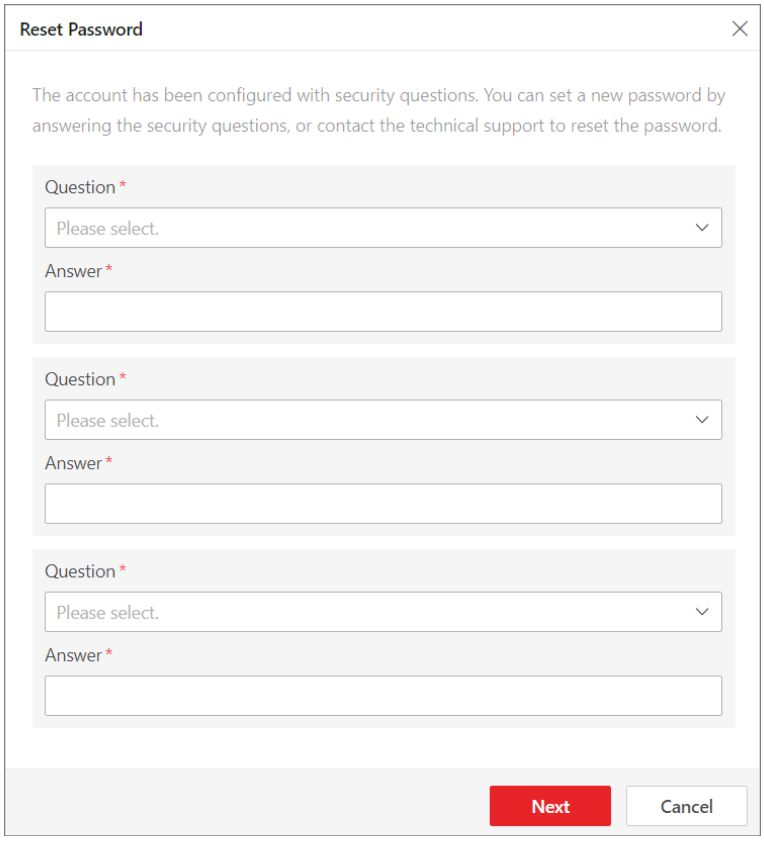


Figure 2-2 Reset Password for admin User via Security Questions

- If you are the admin user or a normal user whose account is configured with an email address, you can click **Get Verification Code** and a verification code will be sent to your email address. Enter the verification code you received, set a new password, and confirm the password within 10 minutes.

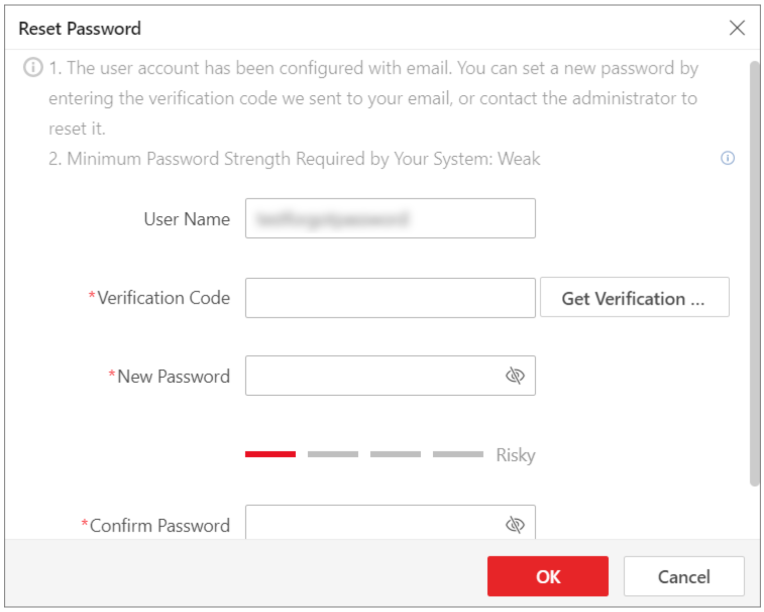


Figure 2-3 Reset Password via Verification Code

Note

If no email address is set for your normal user account, you need to contact the admin user to reset your password.

- If you are an admin whose account is configured with an email address, you can select **Activation Code** and click **Next**, and then reset the password by the code you get.

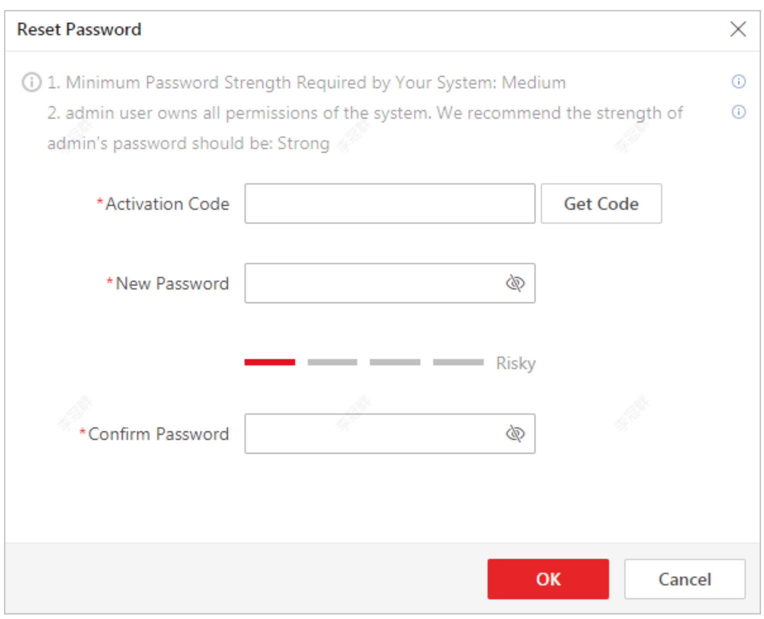


Figure 2-4 Reset Password via Activation Code

- If you are a domain user, you need to contact the admin user to reset your password.

Note

The password strength can be checked by the system and should meet the system requirements. If the password strength is lower than the required minimum strength, you will be asked to change your password. For setting the minimum password strength, refer to ***Set Basic Security Parameters*** .

Caution

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

4. Click **OK**.

2.7 Download Mobile Client

On the login page of Web Client, you can scan the QR code to download the Mobile Client that is used for accessing the system via mobile terminal (e.g., mobile phone).

Perform this task when you need to download the Mobile Client.

Note

You can also search and download the Mobile Client in the App Store.

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS is 172.6.21.96, and you should enter http://172.6.21.96 in the address bar.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Scan the corresponding QR code with your mobile terminal to download the Mobile Client.

2.8 Web Control

For accessing the Web Client via web browser, you must install a web control on the PC on which you access the Web Client when performing some functions. Web Client automatically asks you to install the web control when you want to access the corresponding functions, and you can follow the prompts to install it on the PC.

On the top navigation bar, click **Maintenance and Management → Web Control** to start downloading the web control, or click to view its details and download it.

Chapter 3 Home Page Overview

The default Home page of the Web Client provides a visual overview of function modules on the platform. You can access specific modules quickly and conveniently via the Home page.

Note

After you entered the modules, tabs will appear on the top of the Web Client, you can click tabs to quickly switch modules. You can also click in the tab area to refresh the module.

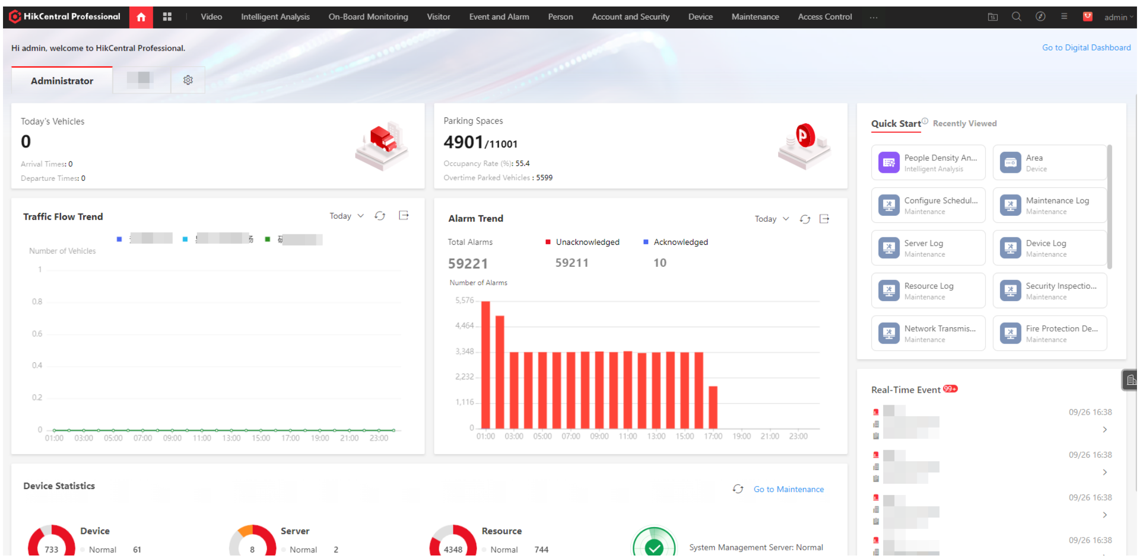


Figure 3-1 Home Page Overview

Note

The supported features and parameters are subject to the applications you installed.

Table 3-1 Home Page Description

Section	Module	Description
Top Navigation Bar	Navigation Icon	The navigation bar shows the available functions determined by the Licenses you purchased. You can add some frequently used or important modules to the navigation bar for convenient access. See details in ***Customize Navigation Bar*** .
	Download Center	You can view and manage all of the downloading and downloaded tasks on the Web Client.

Section	Module	Description
	Search Module	You can search for a specific function module and view the recently viewed pages.
	Wizard	Wizards guides you through the management and applications of different modules.
	Maintenance and Management	**License** You can view the License details, activate, upgrade, and deactivate the License if needed. For more details, refer to ***License Management*** . **Back Up and Restore System Data** You can manually back up the data in the system, or configure a schedule to run the backup task regularly. You can select different storage locations to suit your need. When an exception occurs, you can restore the database if you have backed up the database. For more details, refer to ***Set System Data Backup*** and ***Restore System Data*** . **Export Configuration Data** You can export and save configuration data to your local PC. For more details, refer to ***Export Configuration Data*** . **Download Web Control** Click **Web Control** to start downloading the web control, or click to view its details and download it. **Download Installation Package** Download the installation package of other clients, such as Control Client. **About** Check the version information of the Web Client. View the License Agreement and Open-Source License Agreement.
	Application Market	View the current capacity of the platform. Display or hide applications on the Home page.

Section	Module	Description
		On the application market page, install/uninstall applications, or repair/update installed applications.
Account		**Change Password** Change the password of the current user. For more details, refer to ***Change Password of Current User*** . **Logout** Log out of the system and back to the login page.
Workbench	Workbench	You can configure the available workbenches (including the preset workbench) and customize personal workbench by adding the frequently used components. For more details, refer to ***Customize Preset Workbench*** and ***Customize Personal Workbench*** . You can check the default and the added workbenches to display on the Home page for convenient use.

3.1 Customize Navigation Bar

To conveniently access some frequently used or important modules, you can customize the navigation bar.

Steps

1. On the top left, select ⊞ to display the navigation bar.

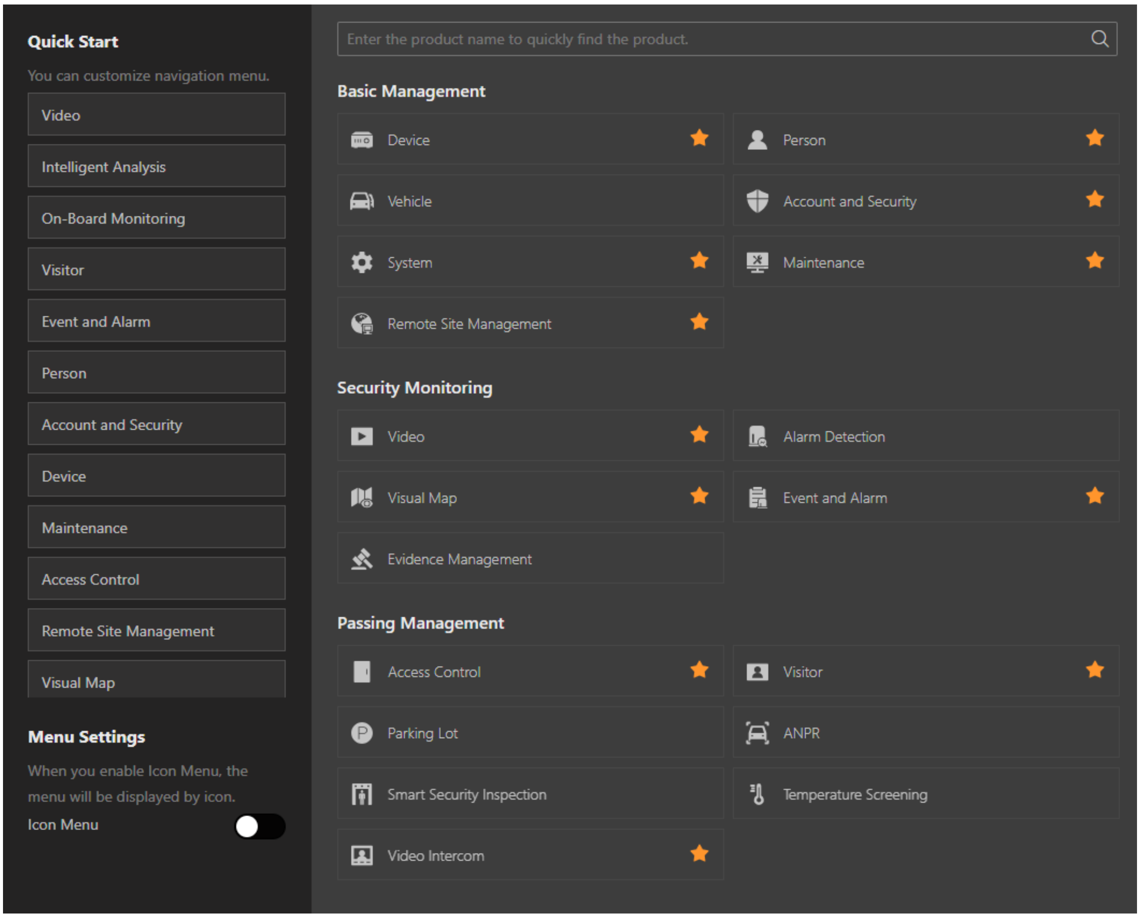


Figure 3-2 Navigation Bar

Note

On the pane, the icon beside the module name indicates that this module has been added to the left navigation bar.

2. **Optional:** Click to remove the module from the navigation bar.
3. **Optional:** In the Quick Start area, drag a module up or down to adjust the module order on the top navigation bar.
4. **Optional:** In Menu Settings area, switch on **Icon Menu**, the module name turns to be an icon displayed on the top navigation bar.

3.2 Application Market

The application market supports installing, repairing, updating, enabling, or disabling applications according to your actual needs.

Click on the top right

The Purchased Page

On this page, if there are purchased applications to install, a prompt will show on the top and you can install these applications.

This page displays the details of your purchased licenses and all installed and free-charged applications. You can disable or enable the applications.

Applications

You can search for applications on the top, install/update/repair/uninstall applications, and download auxiliary tools.

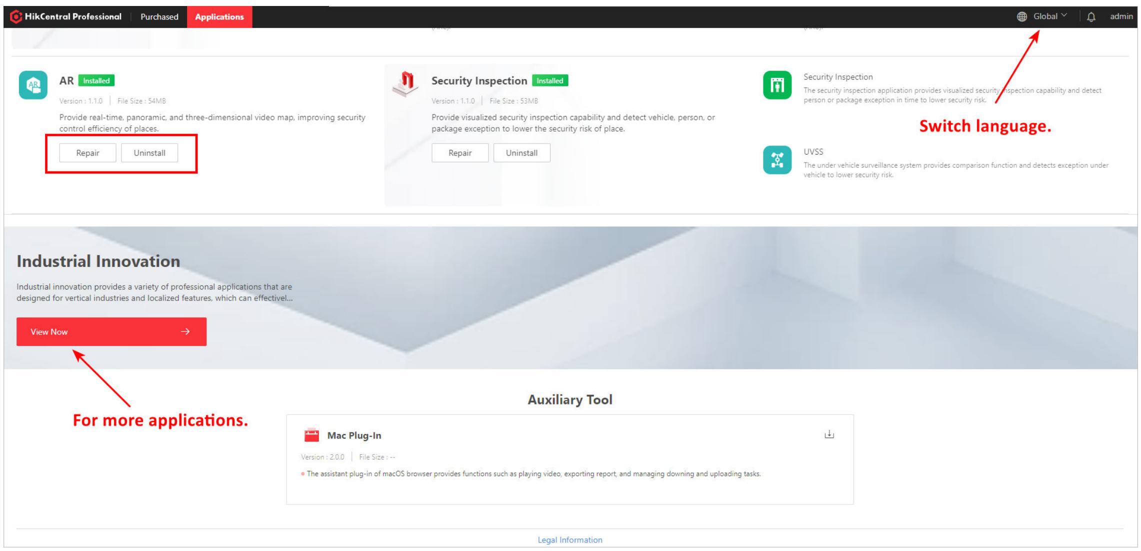


Figure 3-3 Application Market

Note

- The applications may vary by the countries or regions. You can click the globe icon on the top right to select your location. Generally, the platform can get your country or region according to your IP address. When your PC disconnect from the network, you can select the country or region manually.
- For clients running in the LAN, the applications downloading will fail. You can go to the ***official Web Site*** to download the applications you need.

3.3 Customize Preset Workbench

As an administrator, you can link users with the default preset workbench. Also, you can customize preset workbenches.

Note

Make sure you have logged in to the Client by the administrator account. For details, refer to ***Login via Web Client (Administrator)*** .

You can customize a preset workbench by going to one of the two following entries.

- Click to enter the Home page. Then click to expand the workbench configuration pane. In the personal workbench area, click **Preset Workbench Configuration**.
- On the top left, select **→ Basic Management → System** . Select **Workbench Management** on the left.

Note

- You can filter the preset workbenches by conditions, such as workbench name, linked users, and unlinked users.
- You can hover the cursor on the preset workbench, click **Preview** to preview the preset workbench.

Configure Default Preset Workbench

Hover the cursor on the default preset workbench, including Administrator, click , and click on the left to display different components on the workbench.

Note

The default preset workbench name and remark cannot be edited.

Add Preset Workbench

1. Click **Add Workbench** in the upper-right corner.
2. Click to edit the workbench name. Also, you can select an existing workbench as the template from the Copy From drop-down list, link users with the workbench, and add remark.
3. Click **OK**
4. Add displayed components of the workbench on the left.
5. Click **Save**. The added preset workbench will be displayed in the Preset Workbench pane on the Home page.

3.4 Customize Personal Workbench

You can customize personal workbench by adding the frequently used components for overview and quick access to modules, including person and vehicle.

Steps

1. Click to enter the Home page.
2. Click to expand the workbench configuration pane.

3. In the personal workbench area, click **Preset Workbench Configuration** on the top right to enter the Create Personal Workbench page.
4. Click to edit the workbench name.
5. **Optional:** Select an existing workbench as the template from the Copy From drop-down list.
6. Click **OK**.
7. Click + on the right side of the component.

   The component will be displayed on the right.
8. **Optional:** Drag in the lower right corner of a single component or set the display ratio (e.g., 100%, 60%, or 50%) to adjust the display size of the component.
9. Click **Save**.

   The added personal workbench will be displayed in the Personal Workbench pane on the Home page.

3.5 View Digital Dashboard

The platform provides visualized statistics about the digital campus information, including overview, persons, vehicles, and security control and management.

Click to enter the Home page. On the upper-right corner, click **Go to Digital Dashboard** to enter the Digital Campus page.

Note

- Click to select the time period (today, last 7 days, or last 30 days) to display the statistics.
- Click to refresh the real-time statistics.

Overview

- On the left, you can view today's person statistics, access trend, and vehicle parking trend of parking lots.
- On the right, you can view the alarm trend (including the number of total alarms, handled alarms, and unhandled alarms), and device statistics, and you can set cameras auto-switch.

Figure 3-4 Digital Campus Overview

Person

- On the left, you can view the total number of persons (including employees and visitors), today's person employee entry trend, and today's visitor entry trend.
- On the right, you can view the historical employee entry trend and historical visitor entry trend.

Vehicle

- On the left, you can view the vehicle statistics, internal and external vehicle passing trend, and vehicle parking trend of parking lots.
- On the right, you can view the parking space statistics, parking space occupancy trend, and parking duration distribution.

Security

- On the left, you can view the alarm trend (including the number of total alarms, handled alarms, and unhandled alarms), top 5 events, and top 5 areas with alarms.
- In the middle, you can select to view the live view of events.
- On the right, you can view the device statistics and device status.

Chapter 4 Getting Started

The following content describes the tasks typically involved in setting a working system.

Verify Initial Configuration of Devices and Other Servers

Before doing anything on the platform, make sure the devices you are going to use are correctly mounted and connected to the network as specified by the manufacturers. Such initial configurations are required in order to connect the devices to the platform via network.

Log In to Web Client

Refer to ***Login for First Time for Admin User*** .

Activate License

Refer to ***Activate License - Online*** or ***Activate License - Offline*** .

Install Applications

Install applications in the Applications Market. See ***Application Market*** .

Add Devices to Platform and Configure Area

The platform can quickly scan your network for relevant devices, and add them. Or you can add the devices by inputting the required information manually. The devices added should be organized into areas for convenient management. Refer to ***Device and Server Management*** and ***Area Management*** .

Configure Recording Settings

You can record the video files of the cameras on the storage device according to the configured recording schedule. The schedule can be set as continuous, alarm triggered, or command triggered as desired. Refer to ***Set Recording Parameters*** and ***Set Picture Storage*** .

Configure Event and Alarm

The device exception, server exception, alarm input, and so on, can trigger linkage actions in the platform. Refer to ***Event and Alarm*** .

Configure Users

Specify who should be able to access the platform, and how. You can set different permission for the users to limit their operations. Refer to ***Management of Platform Accounts and Security*** .

View How-to Videos

On the lower left of the log-in page, click **Scan QR Code for Help**, and then scan the QR Code by your smart phone to view the how-to videos of the platform.

Chapter 5 License Management

After installing HikCentral Professional, you have a temporary License for a specified number of devices and limited functions. To ensure the proper use of HikCentral Professional, you can activate the SYS to access more functions and manage more devices. If you do not want to activate the SYS now, you can skip this chapter and activate the system later.

Two types of License are available for HikCentral Professional:

- **Base:** You need to purchase at least one basic License to activate the HikCentral Professional.
- **Expansion:** If you want to increase the capability of your system, you can purchase an expanded License to get additional features.

Note

- Only the admin user can perform the activation, update, and deactivation operation.
- If you encounter any problems during activation, update, and deactivation, please send the server logs to our technical support engineers.

5.1 Activate License - Online

If the SYS server to be activated can properly connect to the Internet, you can activate the SYS server in online mode.

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client (Administrator)*** .
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Online Activation** to activate the License in online mode.

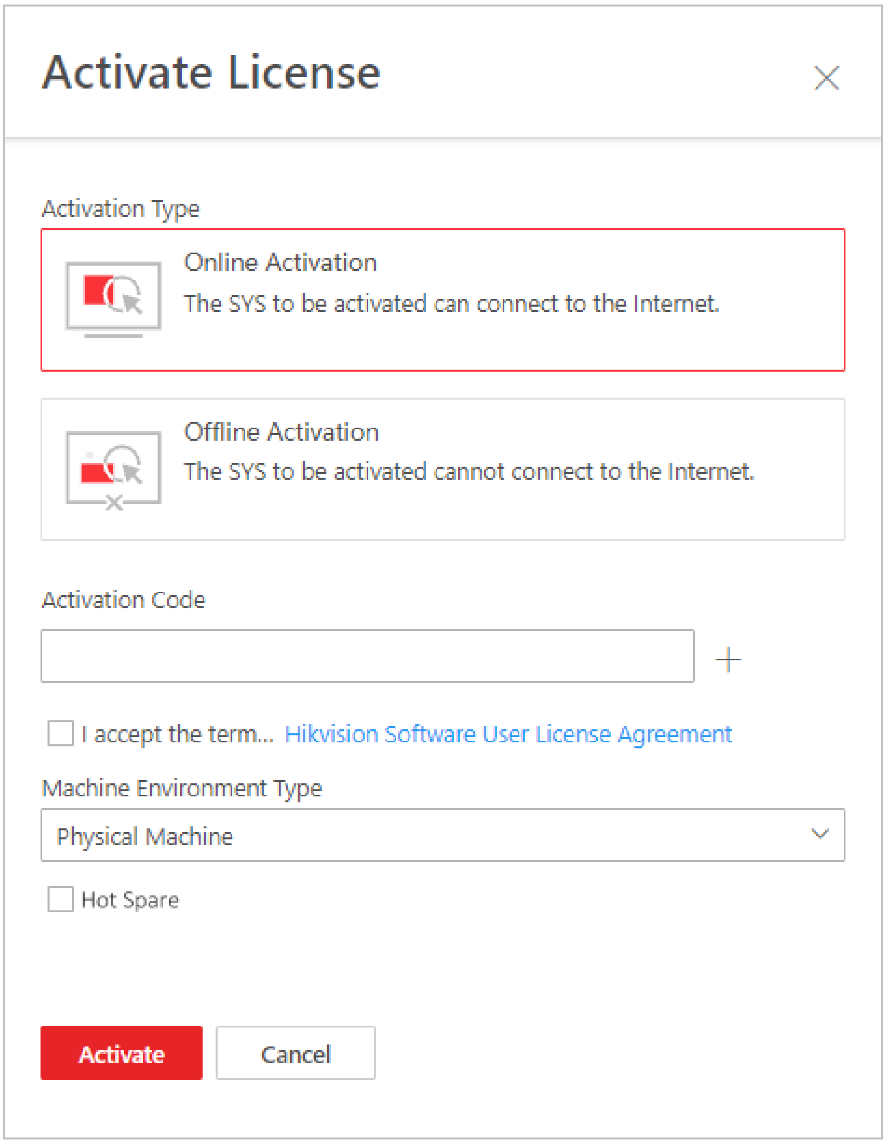


Figure 5-1 Activate License in Online Mode

4. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement pane and click **OK**.
6. **Optional:** Select the machine environment type.

Physical Machine (Default)

A physical computer that contains hardware specifications and is used for running the SYS. If the hardware changed, the License will be invalid, and the SYS may not run normally.

AWS (Amazon® Web Services)

A virtual machine that provides the cloud computing services for running the SYS.

Azure (Microsoft® Azure)

A virtual machine that provides the cloud computing services for running the SYS.

Note

If you select the AWS or Azure as the machine environment type, the pStor server, Streaming Server, and other external servers cannot access the platform. And the Rose hot spare system is also not supported.

7. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

Note

- You must select Hot Spare mode when you install the system.
- For how to build the hot spare system, please contact our technical support engineers.

8. Click **Activate**.

   The details of the activated license will be displayed. The email settings pane will appear after you activated the License.
9. Enter an email address for the admin user.

Note

This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.

10. Set the email server parameters. See details in ***Configure Email Account*** .
11. Click **OK** to save the email settings.

5.2 Activate License - Offline

If the SYS to be activated cannot connect to the Internet, you can activate the License in offline mode.

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Offline Activation** to activate the License in offline mode.

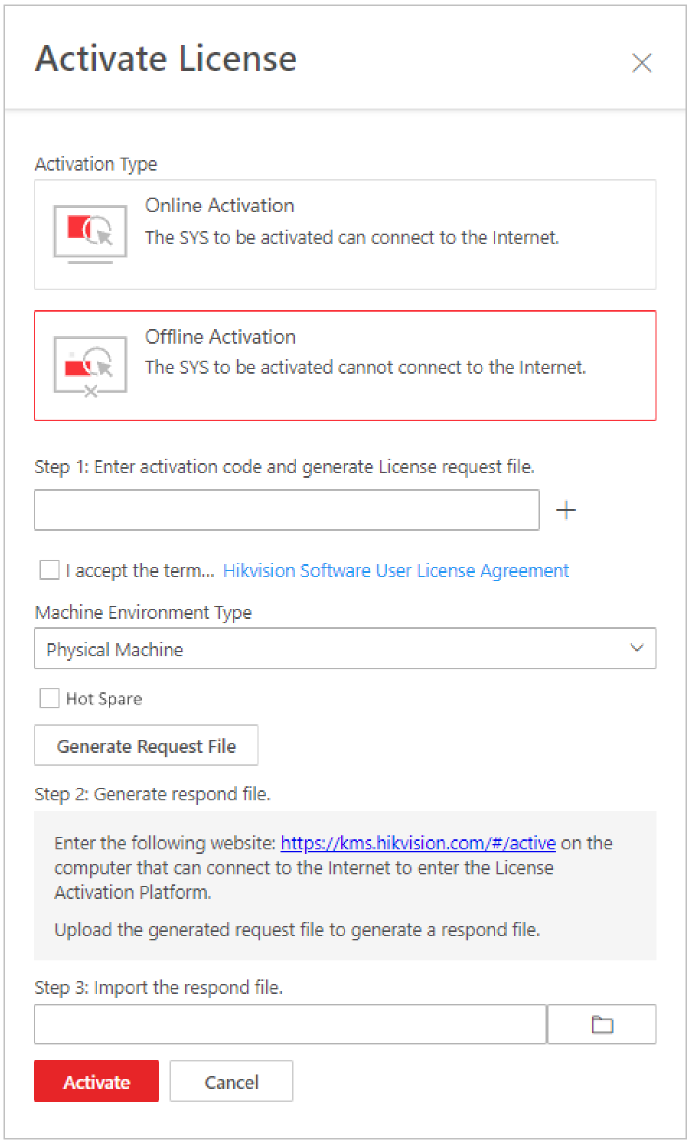


Figure 5-2 Activate License in Offline Mode

4. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click ＋ and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
6. **Optional:** Select the machine environment type.

Physical Machine (Default)

A physical computer that contains hardware specifications and is used for running the SYS. If the hardware changed, the License will be invalid, and the SYS may not run normally.

AWS (Amazon® Web Services)

A virtual machine that provides the cloud computing services for running the SYS.

Azure (Microsoft® Azure)

A virtual machine that provides the cloud computing services for running the SYS.

Note

If you select the AWS or Azure as the machine environment type, the pStor server, Streaming Server, and other external servers cannot access the platform. And the Rose hot spare system is also not supported.

7. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

Note

- You must select Hot Spare mode when you install the system.
- For how to build the hot spare system, please contact our technical support engineers.

8. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
9. Copy the request file to the computer that can connect to the Internet.
10. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
11. Click and then select the downloaded request file.

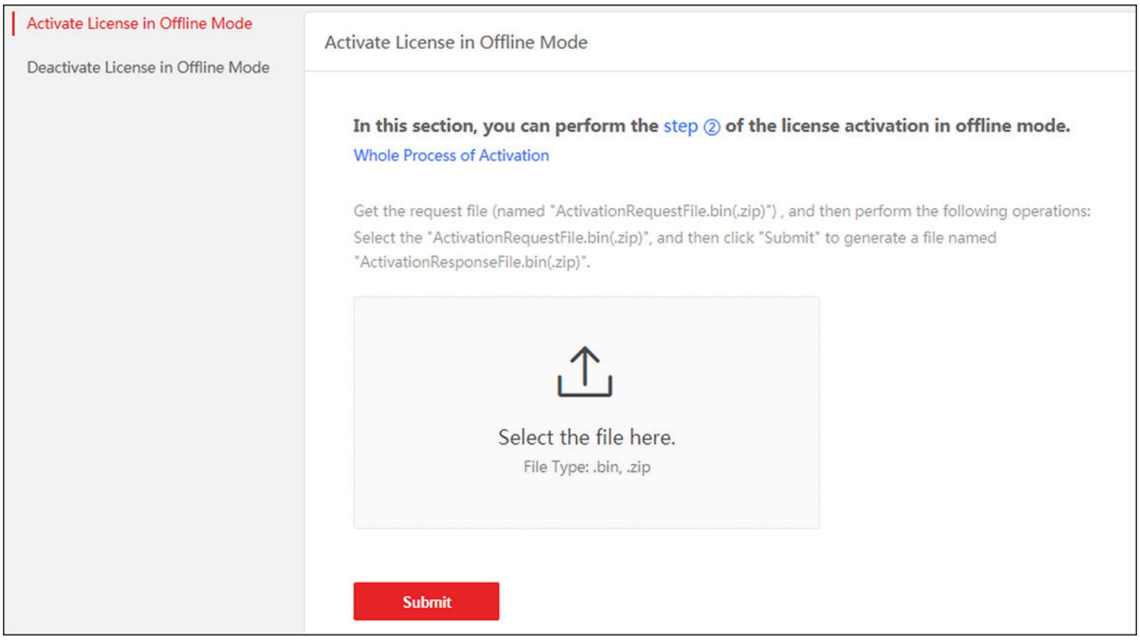


Figure 5-3 Select Request File

12. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
13. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
14. In the Offline Activation panel, click and select the downloaded respond file.
15. Click **Activate**.

    The email settings pane will appear after you activated the License.
16. Enter an email address for the admin user.

Note

This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.

17. Set the email server parameters. See details in ***Configure Email Account*** .
18. Click **OK** to save the email settings.

5.3 Update License - Online

As your project grows, you may need to increase the connectable number of resources (e.g., devices) for your HikCentral Professional. If the SYS to be updated can properly connect to the Internet, you can update the License in online mode.

Before You Start

Contact your dealer or our sales team to purchase a License for additional features.

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the top, move the cursor to ☰ **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Online Update** to update the License in online mode.
5. Enter the activation code received when you purchase your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Update**.

5.4 Update License - Offline

As your project grows, you may need to increase the connectable number of devices for your HikCentral Professional. If the SYS to be updated cannot connect to the Internet, you can update the system in offline mode.

Before You Start

Contact your dealer or our sales team to purchase a License for additional features.

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the top, move the cursor to ☰ **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Offline Update** to update the License in the offline mode.

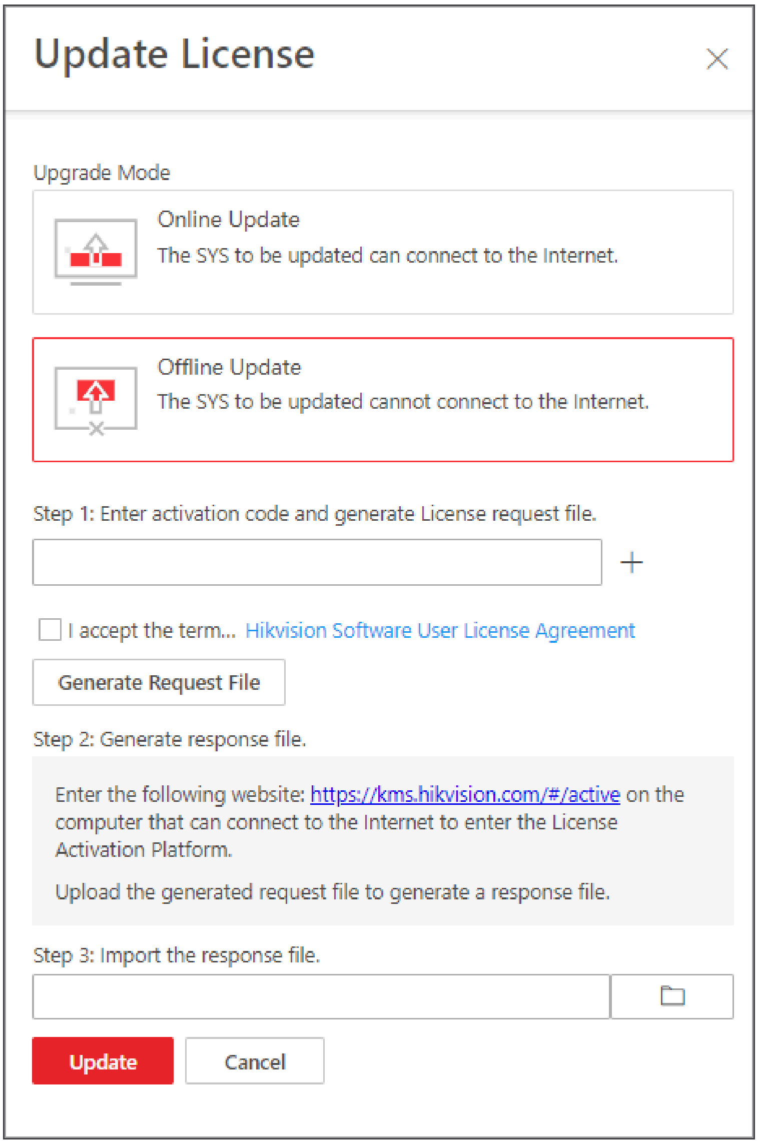


Figure 5-4 Update License in Offline Mode

5. Enter the activation code of your additional License.

Note

- If you have purchased more than one License, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
8. Copy the request file to the computer that can connect to the Internet.

9. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
10. Click and then select the downloaded request file.

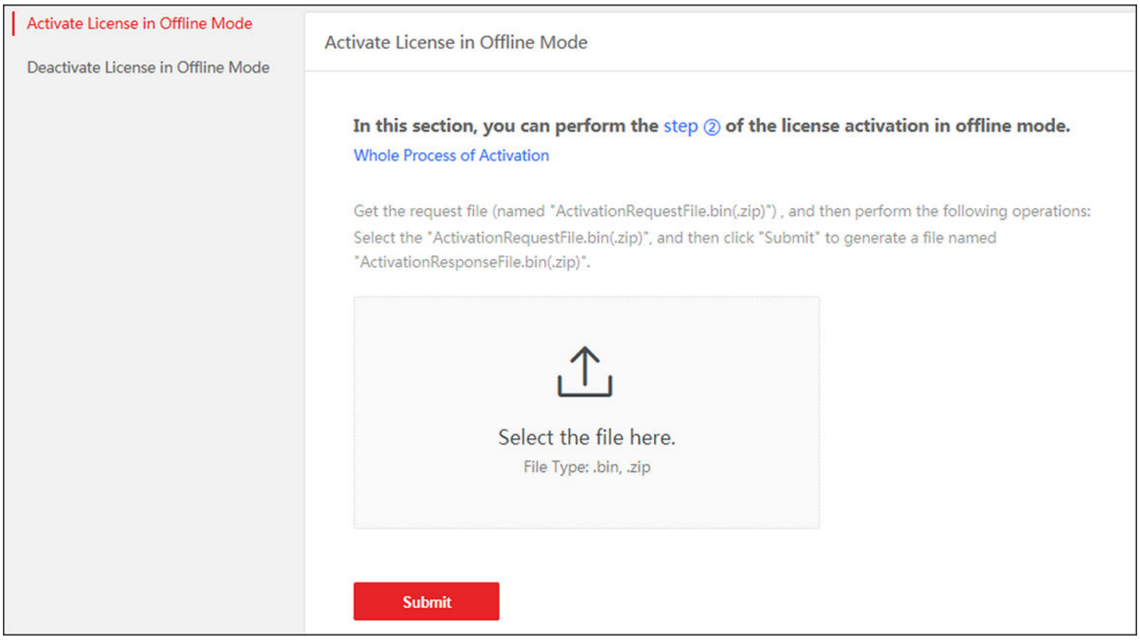


Figure 5-5 Select Request File

11. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
12. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
13. In the offline update panel, click and select the downloaded respond file.
14. Click **Update**.

5.5 Deactivate License - Online

If you want to run the SYS on another PC or server, you should deactivate the SYS first and then activate it again. If the computer or server on which the SYSrunning can properly connect to the Internet, you can deactivate the License in online mode.

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License panel.
4. Click **Online Deactivation** to deactivate the License in online mode.
5. Check the activation code(s) to be deactivated.

6. Click **Deactivate**.

5.6 Deactivate License - Offline

If you want to run the SYS on another computer or server, you should deactivate the SYS first and then activate the SYS again. If the SYS to be deactivated cannot connect to the Internet, you can deactivate the License in offline mode.

Steps

1. Log in to the HikCentral Professional via Web Client.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License pane.
4. Click **Offline Deactivation** to deactivate the License in offline mode.

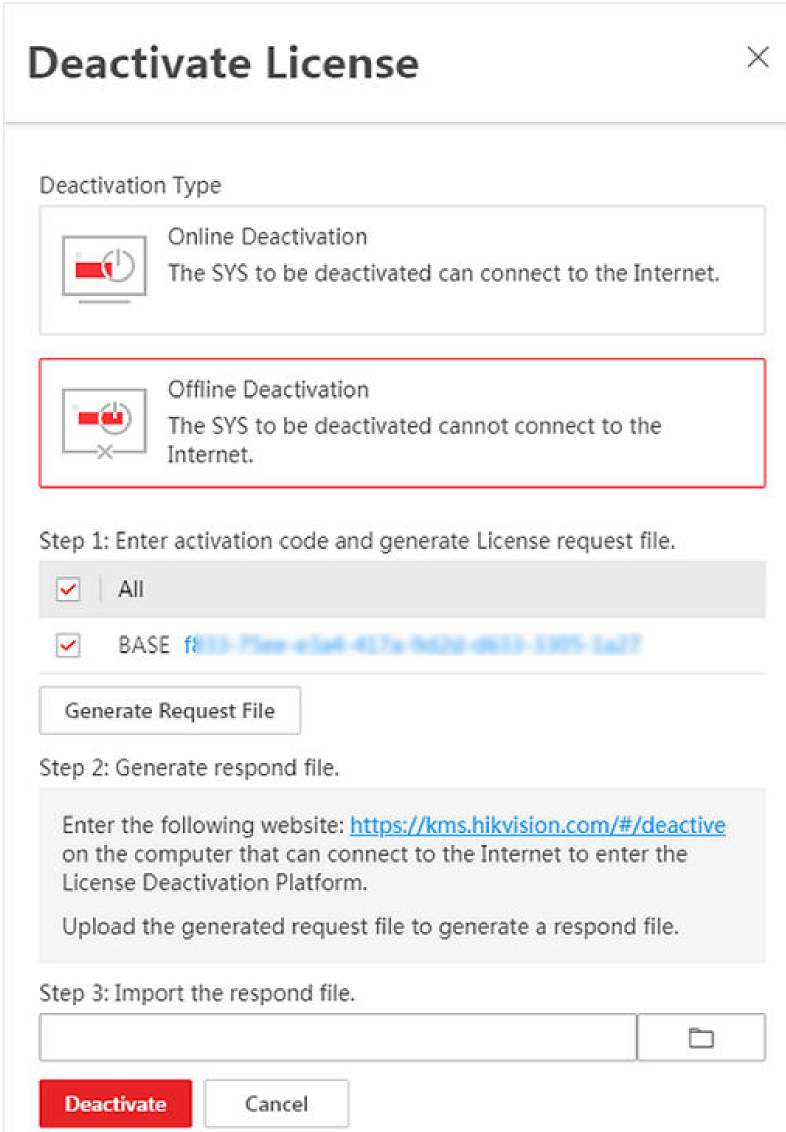


Figure 5-6 Deactivate License in Offline Mode

5. Check the activation code(s) to be deactivated.
6. Click **Generate Request File**.

Note

After the request file is generated, the selected activation code(s) will be unavailable.

A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

7. Copy the request file to the computer that can connect to the Internet.
8. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/deactive*** .

9. Click and then select the downloaded request file.

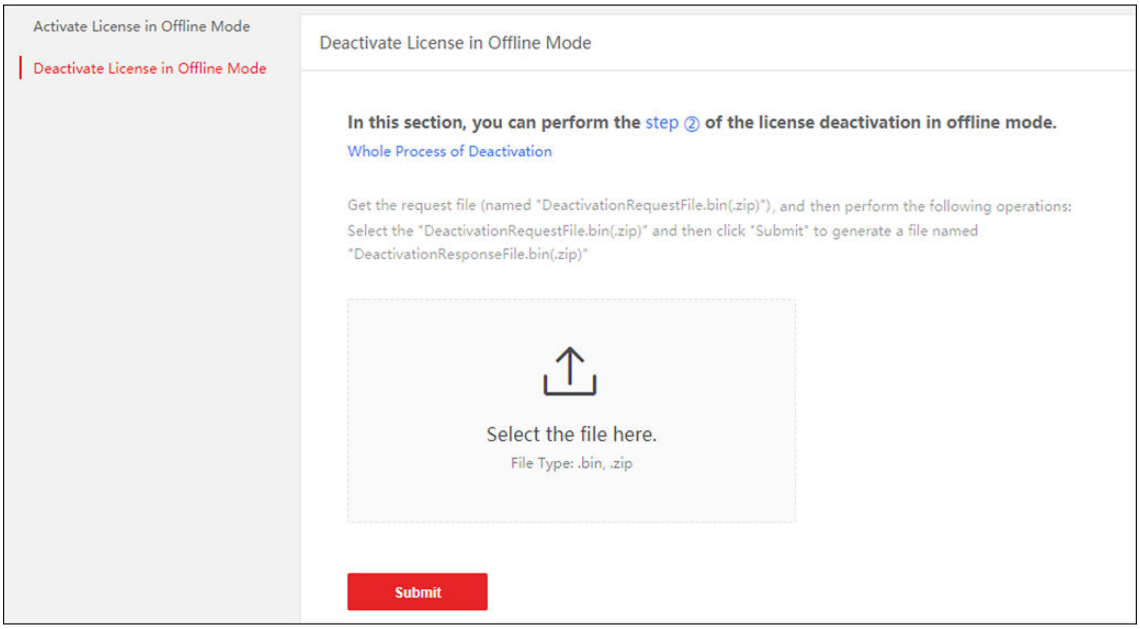


Figure 5-7 Select Request File

10. Click **Submit**.

    A respond file named "DectivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
12. In the Offline Deactivation pane, click and select the downloaded respond file.
13. Click **Deactivate**.

5.7 View License Details

You can check the authorization details of the License you purchased and view the number of manageable devices and functions of your platform. If the License is not activated, you can also view the trial period.

Steps

1. On the top, click **Maintenance and Management → License Details** to open the License Details pane.

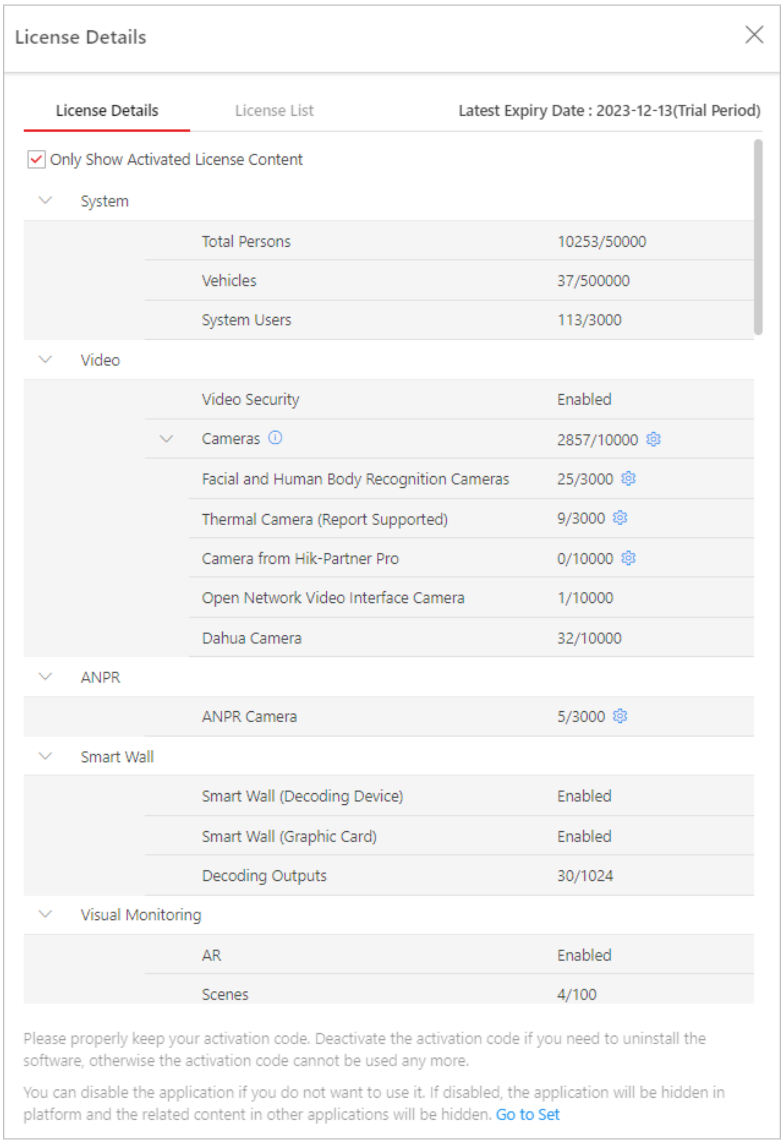


Figure 5-8 License Details Page

2. **Optional:** Click › beside **Cameras** to show the number of facial and human body recognition cameras / thermal cameras (report supported) / ONVIF cameras / cameras from Hik-Partner Pro / Dahua cameras, and click to select the added cameras as these types of cameras respectively.

Note

- Configuration of ONVIF cameras and Dahua cameras is not supported.
- If you do not configure the facial and human body recognition camera / thermal camera, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the platform.

3. **Optional:** Repeat the last step in the ANPR Camera and Software Maintenance Service.

4. **Optional:** Click **License List** to check all the activated License(s) of your platform and click an activation code to view the related authorization details.

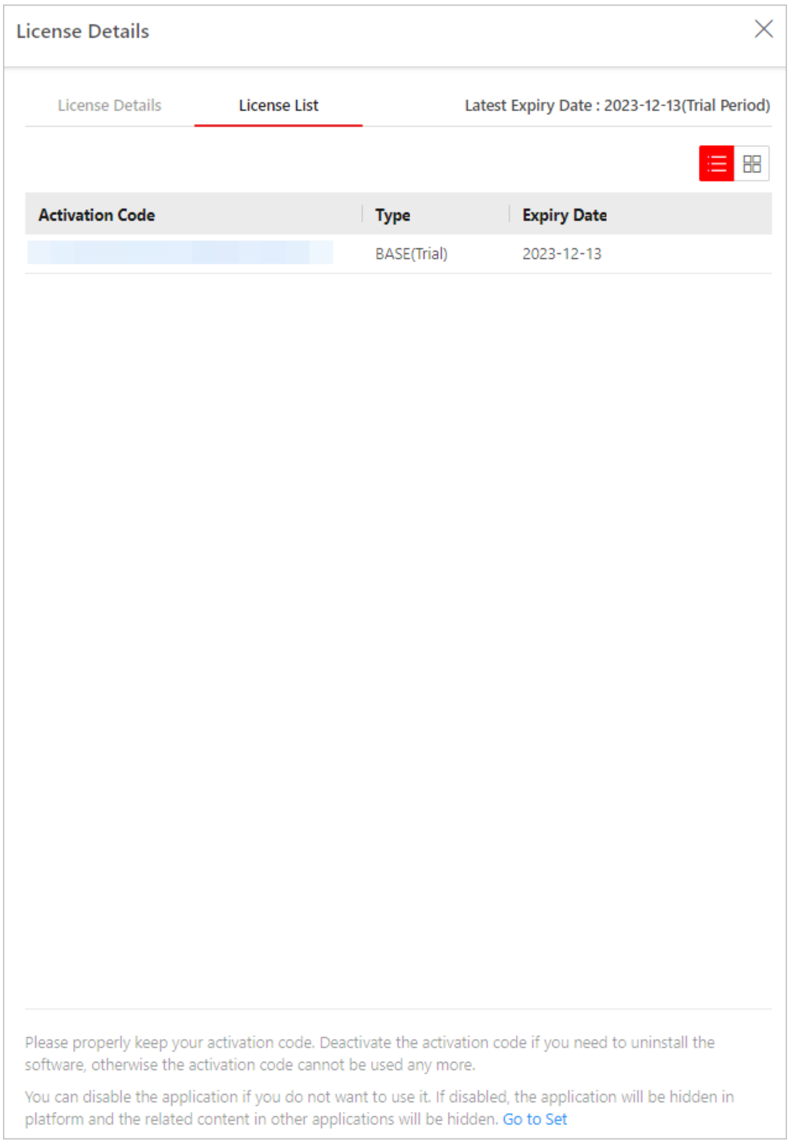


Figure 5-9 License List Page

5.8 Set SSP Expiration Prompt

SSP (Software Service Program) refers to the platform's maintenance service, which has an expire date and needs to be upgraded before expiration. You can set SSP expiration prompt on the platform. After that, when the SSP is going to expire, you can receive an email reminding the expiration every day during the configured period.

Steps

1. On the top, click **Maintenance and Management → License Details** .
2. Click beside **Software Maintenance Service** to enter the SSP Expiration Prompt Settings pane.
3. Set the **Overdue Reminder** switch to ON.
4. Set the days when you will receive the prompt email before expiration.

Note

- You should enter an integer between 1 to 365.
- By default, the platform will send a prompt email 30 days before expiration.

5. Click **Add User** to add user(s) who can receive upgrade prompt.

Note

- You should configure the users' email addresses before adding them as recipients. The added users can receive upgrade prompt via the bound email addresses.
- Up to 64 recipients can be added.
- You can click to delete the added user(s).

6. Click **Add Email** to add email address(es).

Note

You can add email of both the platform user(s) and other user(s). The platform will send expiration prompt to the added email address(es).

7. Click **Save**.

Chapter 6 Device and Server Management

HikCentral Professional supports multiple device or server types. After adding them to the platform, you can manage them, configure required settings and perform further operations.

Go to → **Basic Management → Device** .

You can perform the following operations in the device list.

Note

The functions may vary by device types.

Configure Device	Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Replace Device	When a device is replaced with another one, and the serial No. of the new device is different from that of the old one, you need to confirm the replacement on the platform. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

Batch Set Device Time	Check devices, click **Time Settings** on the top, and set a time for the devices. You can check **Sync with Server Time** to set the same time with the server.
Set Column Width	Click to select **Complete Display of Each Column Title**/**Incomplete Display of Each Column Title** to set the column title width.
Custom Column Item	Click and select the needed column items to display. You can also click **Reset** to reset to the default column items.

6.1 Manage Encoding Device

The encoding devices (e.g., camera, NVR, DVR) can be added to the system for management, including editing and deleting the devices, remote configuration, changing online devices' password, etc. You can also perform further operations based on the added devices, such as live view, video recording, and event settings,

Go to → **Basic Management → Device → Device and Server → Encoding Device** .

6.1.1 Add Encoding Devices

You can add encoding devices by IP address, IP segment, port segment, Hik-Connect DDNS, device ID, device ID segment, and from sites on Hik-Partner Pro. Also, you can add the automatically detected online encoding devices on the same network as the Web Client.

Add Online Detected Encoding Devices

Table 6-1 Add Detected Online Encoding Devices

Adding Mode and Scenario	Description
Method: Add detected online encoding device(s) **Scenario**: The encoding devices are on the same network as the Web Client.	Before you start, make sure: • The web control plug-in is installed. • The devices are correctly installed, connected to the network, and activated. 1. In the Online Device area, select a network type. **Server Network** As the default selection, the detected online devices in the same local subnet with the SYS server will be listed in the Online Device area.

Adding Mode and Scenario	Description
	Local Network The detected online devices in the same local subnet with the Web Client will be listed in the Online Device area. 2. In the Online Device area, select **Hikvision Private Protocol**/ **Hikvision ISUP Protocol**/**ONVIF Protocol** to filter the detected online devices. **Note** - Select **Hikvision Private Protocol** / **Hikvision ISUP Protocol** to add a Hikvision device and select **ONVIF Protocol** to add a third-party device. - To display the devices which are added to the platform via ONVIF/ISUP protocol, you can go to → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and check **Access via ONVIF Protocol**/**Allow ISUP Registration**. 3. In the Online Device area, select the active device(s) to be added, and click **Add to Device List** to open the Add Online Device window.

Add Encoding Devices

Click **Add** to enter the Add Encoding Device page.

Table 6-2 Add Encoding Devices

Adding Mode and Scenario	Description
Method: Add encoding device by IP address / domain. **Scenario:** When you know the IP address or domain name of a device, you can add it to the platform by specifying the IP address	Before you start, make sure the devices (cameras, DVRs, etc.) you are going to use are correctly installed and connected to the network. You should select **Hikvision Private Protocol** / **ONVIF Protocol** / **Dahua Private Protocol** as the Access Protocol, and select **IP Address/Domain**

Adding Mode and Scenario	Description
(or domain name), user name, password, etc.	
Method: Add encoding devices by IP segment. **Scenario:** When multiple encoding devices to be added have the same port number, user name, password, and have different IP addresses within a range, you can add devices by specifying the IP segment and some other related parameters.	Before you start, make sure the devices (cameras, DVRs, etc.) you are going to use are correctly installed and connected to the network. You should select **Hikvision Private Protocol** / **ONVIF Protocol** / **Dahua Private Protocol** as the Access Protocol, and select **IP Segment** as the adding mode.
Method: Add encoding devices by port segment. **Scenario:** When multiple encoding devices to be added have the same IP address, user name, password, and have different port numbers within a range, you can add devices by specifying the port segment and some other related parameters.	Before you start, make sure the devices (cameras, DVRs, etc.) you are going to use are correctly installed and connected to the network. You should select **Hikvision Private Protocol** / **ONVIF Protocol** / **Dahua Private Protocol** as the Access Protocol, and select **IP Segment** as the adding mode.
Method: Add encoding device by Hik-Connect DDNS. **Scenario:** You can add encoding devices with dynamic IP addresses to the system by domain name solutions of Hik-Connect.	Before you start: • Make sure the devices (cameras, DVRs, etc.) you are going to use are correctly installed and connected to the network. • Make sure you have enabled Hik-Connect service for devices to be added on the remote configuration page of the device. You should select **Hikvision Private Protocol** as the Access Protocol, and select **Hik-Connect DDNS** as the adding mode.

Adding Mode and Scenario	Description
	Note The Hik-Connect DDNS Server Address is ***https://open.ezvizlife.com*** by default.
Method: Add encoding device by device ID. **Scenario:** For the encoding devices supporting ISUP, you can add them by specifying a predefined device ID, key, etc.	Before you start: • Make sure the encoding devices you are going to use are correctly installed and connected to the network. • Before adding devices supporting Hikvision ISUP 2.6/4.0 to the system, you need to set related configuration to allow these devices to access the system. You should select **Hikvision ISUP Protocol** as the Access Protocol, and select **Device ID** as the adding mode. **Note** To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** , and enable **Allow ISUP Registration**.
Method: Add encoding devices by device ID segment. **Scenario:** If you need to add multiple encoding devices which have no fixed IP addresses and support ISUP toHikCentral Professional, you can add them to HikCentral Professional at a time after configuring device ID segment for the devices.	Before you start: • Make sure the encoding devices you are going to use are correctly installed and connected to the network. • Before adding devices supporting Hikvision ISUP 2.6/4.0 to the system, you need to set related configuration to allow these devices to access the system. You should select **Hikvision ISUP Protocol** as the Access Protocol, and select **Device ID Segment** as the adding mode.
Method: Add encoding devices in a batch. **Scenario:** When there are multiple devices to be added, you can edit the predefined template containing the required	Before you start, make sure the devices (cameras, DVRs, etc.) you are going to use are correctly installed and connected to the network. You should select **Hikvision Private Protocol** / **Hikvision ISUP Protocol** / / **Dahua Private Protocol** as the access protocol, and select **Batch Import** as the adding mode.

Adding Mode and Scenario	Description
device information, and import the template to HikCentral Professional to add devices in a batch.	
Method: Add encoding devices from sites on Hik-Partner Pro. **Scenario:** If you have configured parameters for the site on Hik-Partner Pro accessing the platform, you can add encoding devices from the site on Hik-Partner Pro to the platform.	Before you start: • Make sure the devices (cameras, DVRs, etc.) you are going to use are correctly installed and connected to the network. • Make sure you have enabled **Access Site on Hik-Partner Pro** in System Configuration and configured the required parameters. You should select **Hik-Partner Pro Protocol** as the access protocol. **Note** You need to first purchase a license to use the Hik-Partner Pro service.

6.1.2 After Adding Encoding Devices: Operations on Device List Page

After you add encoding devices, you can perform further operations on the device list.

Operations	Descriptions
Remote Configurations	Click in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online Hikvision devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Operations	Descriptions
Replace Device	When a device is replaced with another one, and the serial No. of the new device is different from that of the old one, you need to confirm the replacement on the platform. In the **Operation** column, click to replace the old device with the new device on the platform.
Delete Device	Select one or multiple device(s) and click to delete. **Note** If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.
Edit Bandwidth for Video Downloading	Select one or more NVRs (V4.1.5 or later versions), and click **Edit Bandwidth for Video Downloading** to set the bandwidth upper-limit for video downloading of the selected NVR(s).
Set Time Zone	Select one or more device(s), click **Time Zone** to set/edit the time zone of the selected device(s).
Set N+1 Hot Spare for NVR	You can form an N+1 hot spare system with at least two NVRs (Network Video Recorder) or hybrid SANs. The system consists of several host servers and a spare server (cannot be selected for storing videos). When a host server fails, the spare server switches into operation (such as video recording, searching video for playback, etc.), and thus increasing the video storage reliability of HikCentral Professional. 1. Click **N+1 Hot Spare** to set N+1 hot spare for NVRs. 2. Click **Add** to set N+1 hot spare. 3. Select a NVR in the **Spare** drop-down list to set it as the spare server. 4. Select the NVR(s) in the **Host** field to set them as the host server. 5. Click **Add**. **Note** The recording schedules configured on the NVR will be deleted after setting it as the spare Recording Server. 6. Click **Apply Hot Spare Settings to Device** to apply the Hot Spare settings to the devices to take effect.

Operations	Descriptions
Wake Up the Solar Camera	After you add a solar camera, the network status will be displayed as offline, online (Asleep), or online (Waked up). You can click in the **Operation** column to wake up an asleep camera. You can also click the device name to enter the editing device page, and click **Wake Up** to wake the device up. **Note** If a device is in sleep mode, the communication between the solar camera and the platform is not supported.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

6.1.3 Add and Manage Applications

You can give algorithm capabilities to devices by configuring device application packages. After you finish configuring, you can add the applications to specific devices and manage the applications.

Add Applications

You can add device applications to some encoding devices.

Before You Start

- Make sure the devices you are going to use are added to the platform. For details about adding encoding device, see ***Manage Encoding Device*** .
- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

Note

Currently not all encoding devices can be updated via device applications.

1. On the top navigation bar, select → **Basic Management → Device** .
2. Select **Device Application** on the left panel.
3. Click **Add Application**.
4. Select **HEOP** or **AIOP** as the application package source.

- If you select **HEOP**, you need to upload the algorithm package.
- If you select **AIOP**, you need to upload model library, label file, and enter model name.

5. Click **Next**, and then select available device(s) to add the application.
6. Click **Finish** to add the application to the device.

   The device application details are displayed in **All Applications** tab.
7. **Optional:** Perform the following operations after adding applications to device(s).

Enable/Disable Device Application	Click **Enable All** / **Disable All** to enable/disable the corresponding device application.
Refresh Device Application List	Click **Refresh** to refresh the device application list.
Delete Device Application	Click **Delete** to delete the device applications.
Import License	Click **Import License** and upload a license file to specific device(s).
Display Applications Disabled	Check **Display Applications Disabled** to only display the disabled applications.
View Adding Records	Click **Adding Records** to open the adding records page, you can view the records about adding device applications in specific time period. **Note** The icon indicates that adding device application(s) failed.
Search for Applications	On the upper right, enter the keywords of application name, and click to search for added device applications.

Manage Applications on Devices

You can manage device applications after adding the them.

Before You Start

- Make sure the devices you are going to use are added to the platform. For details about adding encoding device, see ***Manage Encoding Device*** .
- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Select **Device Application** on the left panel.
3. Select **All Devices** tab.

The devices that support updating by device applications are displayed on the left.

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

View Device Application Details	Select an encoding device on the list to view device application details on the right, including device application name, device application version, system memory usage, smart RAM usage, and flash usage.
Enable/Disable Device Application	Select an encoding device on the list, click / to enable/disable the corresponding device application. Or select an encoding device on the list, and select multiple applications on the right, and click **Enable/Disable** to batch enable/disable the device applications.
Add Device Application to Specific Device	Select an encoding device on the list, click **Add** to add device application package for this device.
Refresh Device Application List	Select an encoding device on the list, click **Refresh** to refresh the device application list.
Delete Device Application	Select an encoding device on the list, and select the device application(s). Click **Delete** to delete the device application(s).
View Adding Records	Click **Adding Records** to open the adding records page, you can view the records about adding device applications in specific time period. **Note** The icon indicates that adding device application(s) failed.
Search for Devices	On the top of the page, enter the keywords of device name or device address, and click to search devices for adding device applications.

6.2 Manage Access Control Device

You can add the access control devices to the system for access level configuration, etc.

On the left, select **Access Control Device**.

For some access controllers, click on the left of the device list, and click **Add** to enter the Add Access Module page.

1. In the Added Access Module area, click **Add**.
2. Set the access module name and ID.
3. In the Access Module Under Access Controller area, check access modules and click **Expand Access Module List in Access Controller**.
4. Click **Add** at the bottom.

You can go back to the device list to view the added access modules and reboot the access modules.

Note

This function should be supported by the device.

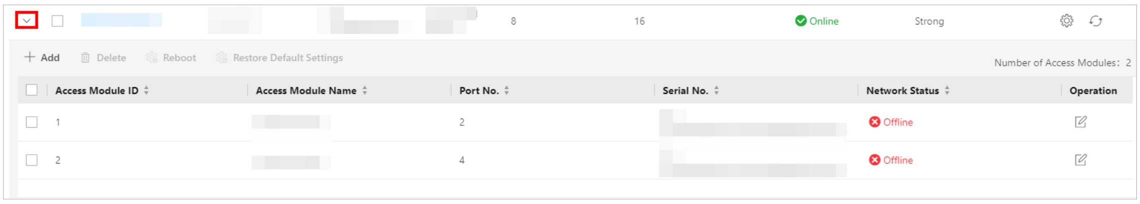


Figure 6-1 Add Access Module

6.2.1 Add Detected Online Access Control Devices

The active online access control devices in the same local subnet with the current Web Client or SYS server will be displayed on a list. You can add one online device one by one, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online Access Control Device

The platform automatically detects online access control devices on the same local subnet with the client or SYS server. You can add the detected access control devices to the platform one by one if they have different user account.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Follow the steps to add a detected online access control device to the platform.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

Local Network

All detected online devices on the same local subnet with the current Web Client.

4. Select **Hikvision Private Protocol** and **Hikvision ISUP Protocol** to filter the detected devices by protocol types.

Note

Make sure you have enabled the ISUP protocol registration to allow the devices to access the system, otherwise the online devices will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.

5. Select an active device that you want to add to the platform.
6. Click **Add to Device List**.

Note

For devices whose device port No. is 8000 and HTTP port No. is 80, the **Hikvision Private Protocol** is selected as the access protocol by default. For devices whose device port No. is 0 but the HTTP port No. is 80, the **ISAPI Protocol** is selected as the access protocol.

7. Configure the basic information for the device, including access protocol, device address, device port, device name, user name, and password.

Caution

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

Note

The access protocol will not show in the following situations:

- You check more than one device in the Online Device area.
- You check only one device in the Online Device area.
  - You can select **Hikvision ISUP Protocol** in the Online Device area.
  - You can select **Hikvision Private Protocol** in the Online Device area, and device port is 0.

8. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone

You can select a time zone of the device. The settings will be applied to the device automatically.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.

10. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

11. Click **Add**.
12. **Optional:** Perform further operations on the added device(s).

Configure Device
Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Parameters for Access Control Devices and Elevator Control Devices*** for detailed instructions.

Change Password
Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Replace Device
When a device is replaced with another one, and the serial No. of the new device is different from that of the old one, you need to confirm the replacement on the platform. In the **Operation** column, click to replace the old device with the new device on the platform.

Restore Default Settings
Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Privacy Settings

To protect the person's private information including the person's name and profile picture, you can configure privacy settings for online access control devices. For details, refer to ***Privacy Settings*** .

Set Device's Time Zone

On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.

Search for Devices

Enter key words in the search box and click to search for a specific device.

Add Access Module

For some access controllers, click on the left of the device list, and click **Add** to enter the Add Access Module page.

a. In the Added Access Module area, click **Add**.
b. Set the access module name and ID.
c. In the Access Module Under Access Controller area, check access modules and click **Expand Access Module List in Access Controller**.
d. Click **Add** at the bottom.

You can go back to the device list to view the added access modules and reboot the access modules.

Note

This function should be supported by the device.

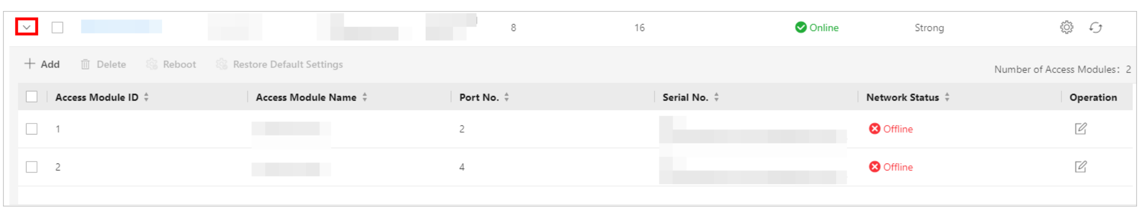


Figure 6-2 Add Access Module

Add Detected Online Access Control Devices in a Batch

If the detected online access control devices share the same user name and password, you can add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Access Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select **Hikvision Private Protocol** and **Hikvision ISUP Protocol** to filter the detected devices by protocol types.

   Note

   Make sure you have enabled the ISUP protocol registration to allow the devices to access the system, otherwise the online devices will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.
5. Select the active devices that you want to add to the platform.
6. Click **Add to Device List**.

   Note

   For devices whose device port No. is 8000 and HTTP port No. is 80, the **Hikvision Private Protocol** is selected as the access protocol by default. For devices whose device port No. is 0 but the HTTP port No. is 80, the **ISAPI Protocol** is selected as the access protocol.
7. Set parameters for the devices.

   Caution

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

8. **Optional:** Set the time zone for the device.
   - **Get Device's Time Zone**

     The time zone of the device will be automatically chosen according to the region of the device.
   - **Manually Set Time Zone (The settings will be applied to the device automatically)**

     You can select a time zone of the device. The settings will be applied to the device automatically.
9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

   Note

   - You can create a new area by device name or select an existing area.
   - You can import all the access points or specific access point(s) to the area.
   - For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
10. Check **Restore Default Settings** to restore configured device parameters to default settings.

    Note

    - Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
    - It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.
11. Click **Add**.
12. **Optional:** Perform further operations on the added device(s).

Configure Device	Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Parameters for Access Control Devices and Elevator Control Devices*** for detailed instructions.
Replace Device	In the **Operation** column, click to replace the device with a new device. If the serial No. of the new device is different from that of the old one, you need to confirm the replacement.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.

Privacy Settings	You can configure privacy settings for online access control devices. For details, refer to ***Privacy Settings*** .
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter key words in the search box and click 🔍 to search for a specific device.
Add Access Module	For some access controllers, click ⌄ on the left of the device list, and click **Add** to enter the Add Access Module page. a. In the Added Access Module area, click **Add**. b. Set the access module name and ID. c. In the Access Module Under Access Controller area, check access modules and click **Expand Access Module List in Access Controller**. d. Click **Add** at the bottom. You can go back to the device list to view the added access modules and reboot the access modules. **Note** This function should be supported by the device.

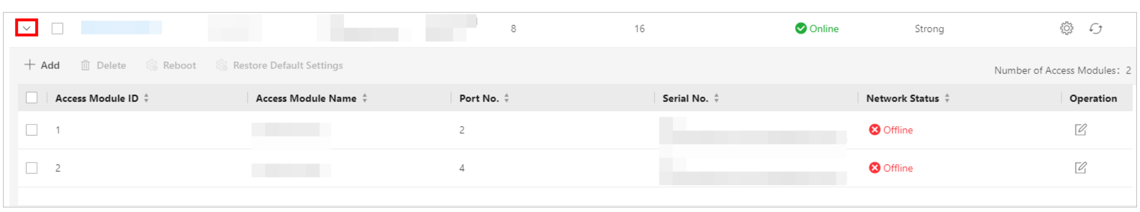


Figure 6-3 Add Access Module

6.2.2 Add an Access Control Device by IP Address / Domain

If you know the IP address/domain of the access control device you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the Access Control Device page, click **Add** to enter the Add Access Control Device page.
2. Select **Hikvision Private Protocol**, **Hikvision ISUP Protocol**, or **Hikvision ISAPI Protocol** as the access protocol.
3. Select **IP Address/Domain** as the adding mode.
4. Enter the required basic information.

Caution

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

5. **Optional:** If you select **Hikvision Private Protocol** or **Hikvision ISAPI Protocol**, check **Encrypted Add**.
6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.
7. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.

8. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

9. Click **Add** to add the device(s) and return to the device management page, or click **Add and Continue** to add the device(s) and continue to add other devices.

6.2.3 Add Access Control Devices by IP Segment

If the access control devices you want to add to the platform share the same user account, and they are in the same IP segment, you can add them to the platform by specifying the start/end IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the Access Control Device page, click **Add** to enter the Add Access Control Device page.
2. Select **Hikvision Private Protocol** or **Hikvision ISAPI Protocol** as the access protocol.
3. Select **IP Segment** as the adding mode.
4. Enter the required information.

Caution

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

5. **Optional:** If you select **Hikvision Private Protocol** or **Hikvision ISAPI Protocol**, check **Encrypted Add**.
6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

8. Click **Add** to add the device(s) and return to the device management page, or click **Add and Continue** to add the device(s) and continue to add other devices.

6.2.4 Add an Access Control Device by Device ID

For access control devices supporting ISUP 4.0 or later protocol, you can add them by specifying a predefined device ID and key. This is a cost-effective choice when you need to manage access control devices that do not have fixed IP addresses.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.

Note

Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.

5. Select **Device ID** as the adding mode.
6. Enter the required the information.
7. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.

- Select **pStor** and select storage locations for the face picture library and captured pictures.

Note

This configuration only affects the facial recognition device which supports face picture comparison. The storage location of captured pictures and face picture libraries cannot be the same.

- Select **Local Storage** as the storage location, click **Configure** to enable **Local Storage** and set the storage locations for pictures and files as needed.

8. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Parameters for Access Control Devices and Elevator Control Devices*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Privacy Settings	To protect the person's private information including the person's name and profile picture, you can configure privacy settings for online access control devices. For details, refer to ***Privacy Settings*** .
Replace Device	When a device is replaced with another one, and the serial No. of the new device is different from that of the old one, you need to confirm the replacement on the platform. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
Add Access Module	For some access controllers, click on the left of the device list, and click **Add** to enter the Add Access Module page. a. In the Added Access Module area, click **Add**. b. Set the access module name and ID. c. In the Access Module Under Access Controller area, check access modules and click **Expand Access Module List in Access Controller**. d. Click **Add** at the bottom. You can go back to the device list to view the added access modules and reboot the access modules. **Note** This function should be supported by the device.

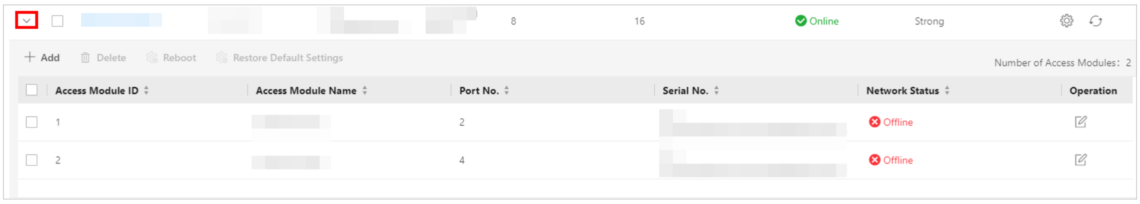


Figure 6-4 Add Access Module

6.2.5 Add Access Control Devices by Device ID Segment

If you need to add multiple access control devices which support ISUP 5.0 protocol and have no fixed IP addresses to the platform, you can add them all at once after configuring a device ID segment for the devices.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select ⊞ → **Basic Management** → **Device** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.

Note

Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network** → **Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.

5. Select **Device ID Segment** as the adding mode.
6. Enter the required parameters.
7. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.
   - Select **pStor** and select storage locations for the face picture library and captured pictures.

   Note

   This configuration only affects the facial recognition device which supports face picture comparison. The storage location of captured pictures and face picture libraries cannot be the same.

   - Select **Local Storage** as the storage location, click **Configure** to enable **Local Storage** and set the storage locations for pictures and files as needed.

8. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. **Optional:** Perform further operations on the added device(s).

Configure Device

Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Parameters for Access Control Devices and Elevator Control Devices*** for detailed instructions.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Replace Device

When a device is replaced with another one, and the serial No. of the new device is different from that of the old one, you need to confirm the replacement on the platform. In the **Operation** column, click to replace the old device with the new device on the platform.

Restore Default Settings

Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Privacy Settings

To protect the person's private information including the person's name and profile picture, you can configure privacy settings for online access control devices. For details, refer to ***Privacy Settings*** .

Set Device's Time Zone

On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.

Search for Devices

Enter one or multiple key words in the search box and click to search for a specific device.

Add Access Module

For some access controllers, click on the left of the device list, and click **Add** to enter the Add Access Module page.

a. In the Added Access Module area, click **Add**.
b. Set the access module name and ID.
c. In the Access Module Under Access Controller area, check access modules and click **Expand Access Module List in Access Controller**.
d. Click **Add** at the bottom.

You can go back to the device list to view the added access modules and reboot the access modules.

Note

This function should be supported by the device.

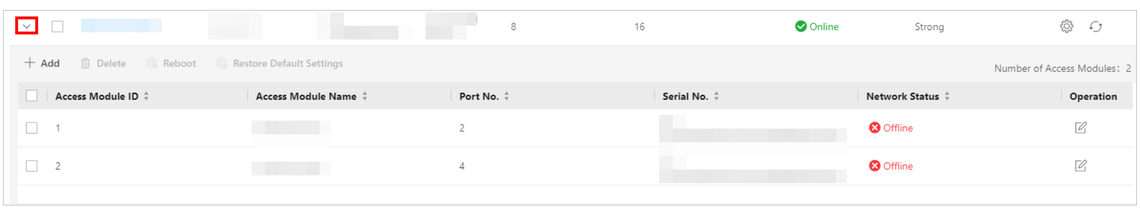


Figure 6-5 Add Access Module

6.2.6 Add Access Control Devices in a Batch

You can download and enter access control device information in the predefined spreadsheet to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol**, **Hikvision ISUP Protocol**, or **Hikvision ISAPI Protocol** as the access protocol.

   Note

   Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined spreadsheet (XLSX format) to local disk.
7. Open the spreadsheet and edit the required device information.
8. Click and select the edited spreadsheet.
9. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.
   - Select **pStor** and select storage locations for the face picture library and captured pictures.

     Note

     This configuration only affects the facial recognition device which supports face picture comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configure** to enable **Local Storage** and set the storage locations for pictures and files as needed.

   Setting picture storage location is not required for devices added via **Hikvision ISAPI Protocol** and **Hikvision Private Protocol**.
10. **Optional:** Set the time zone for the device.

    Get Device's Time Zone

    The time zone of the device will be automatically chosen according to the region of the device.

    Manually Set Time Zone (The settings will be applied to the device automatically)

    You can select a time zone of the device. The settings will be applied to the device automatically.
11. Finish adding the device(s).

- Click **Add** to add the device(s) and return to the device management page.
- Click **Add and Continue** to add the device(s) and continue to add other devices.

12. **Optional:** Perform further operations on the added device(s).

Configure Device	Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Parameters for Access Control Devices and Elevator Control Devices*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
Privacy Settings	To protect the person's private information including the person's name and profile picture, you can configure privacy settings for online access control devices. For details, refer to ***Privacy Settings*** .
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Replace Device	When a device is replaced with another one, and the serial No. of the new device is different from that of the old one, you need to confirm the replacement on the platform. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
Add Access Module	For some access controllers, click on the left of the device list, and click **Add** to enter the Add Access Module page. a. In the Added Access Module area, click **Add**. b. Set the access module name and ID.

c. In the Access Module Under Access Controller area, check access modules and click **Expand Access Module List in Access Controller**.

d. Click **Add** at the bottom.

You can go back to the device list to view the added access modules and reboot the access modules.

Note

This function should be supported by the device.

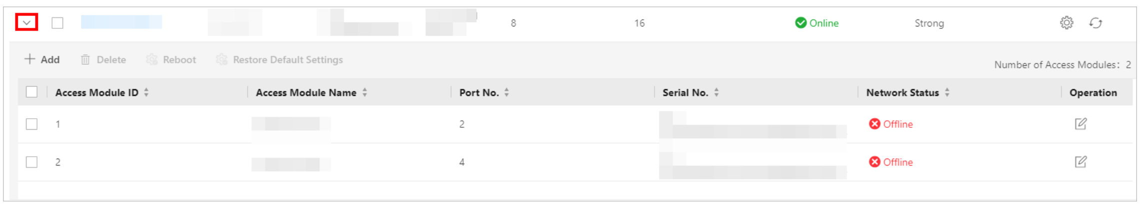


Figure 6-6 Add Access Module

6.2.7 Privacy Settings

You can configure the settings for event storage, authentication, and picture uploading and storage, and clear the pictures on the access control devices to protect the person's private information, including name, profile picture, etc.

On the top, select **Device**. Then select **Device and Server → Access Control Device** on the left.

Select one or more devices and click **Privacy Settings**.

Note

Make sure the selected device is online.

Set the following parameters as needed and click **Save**.

Event Storage

Select the mode of event storage.

Overwrite

The events stored on the device will be overwritten automatically. For example, if a device can store up to 200 events. When this limit is reached, the first event will be overwritten by the newest one, and then the second will be overwritten.

Delete Old Events Regularly

Set a time period. The events stored on the device during the period will be automatically deleted at intervals of the period.

Delete Old Events by Specified Time

Set a specific time. The events stored on the device before the specific time will be automatically deleted.

Authentication

Check the items to be displayed in authentication results.

Picture Uploading and Storage

Check the items as needed.

Upload Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be uploaded to the system.

Save Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be saved to the devices.

Save Profile Pictures

If it is checked, the profile pictures will be saved to the devices.

Upload Event and Alarm Pictures

If it is checked, the event and alarm pictures will be uploaded to the system.

Save Event and Alarm Pictures

If it is checked, the event and alarm pictures will be saved to the devices.

Upload Thermal Pictures

If it is checked, the thermal pictures will be uploaded to the system.

Save Thermal Pictures

If it is checked, the thermal pictures will be saved to the devices.

Clear Pictures Stored on Device

Clear Face Pictures

Click **Clear** to clear all face pictures.

Clear Recognized or Captured Pictures

Click **Clear** to clear all recognized pictures or captured pictures.

6.3 Manage Elevator Control Device

You can add the elevator control device to the system to control the elevator(s), such as assign the access authority of specified floors to person, control the elevator status on the Control Client.

6.3.1 Add Detected Online Elevator Control Devices

The active online elevator control devices on the same local subnet with the current Web Client or SYS server will be displayed on a list. You can add an online device at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function will be available.

Add a Detected Online Elevator Control Device

The Web Client automatically searches for online elevator control devices on the same local subnet with the client or SYS server. You can add the detected elevator control devices to the platform one by one if the devices do not share the same user account.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Elevator Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select an active device that you want to add to the platform.
5. Click **Add** to open the Add Elevator Control Device window.
6. Configure the basic information for the device, including device address, device port, device name, user name, and password.

   Caution

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

   Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

Note

- You can create a new area by device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the resources.
- Enter the range of floor number according to your application scenario.

9. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Click **Add**.
11. **Optional:** Perform further operations on added device(s).

Configure Device

Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default Settings

Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

Add Detected Online Elevator Control Devices in a Batch

If the detected online elevator control devices share the same user account, you can add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Elevator Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select the active devices that you want to add to the platform.
5. Click **Add to Device List** to open the Add Elevator Control Device window.
6. Set parameters for the devices.

   Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

   Note

   - You can create a new area by device name or select an existing area.
   - If you do not import resources to an area, you cannot perform further operations for the resources.
   - Enter the range of floor number according to your application scenario.

9. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

   Note

   - Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
   - It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.

11. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.

Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

6.3.2 Add an Elevator Control Device by IP Address

If you know the IP address of the elevator control device you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **IP Address** as the adding mode.
5. Enter the required parameters.

Note

By default, the device port number is 8000.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

   Note

   - You can create a new area by device name or select an existing area.
   - If you do not import resources to an area, you cannot perform further operations for the resources.
   - Enter the range of floor number according to your application scenario.

8. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

   Note

   Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.

9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.

10. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.

Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

6.3.3 Add Elevator Control Devices by IP Segment

If the elevator control devices you want to add to the platform share the same user account, and they are in the same IP segment, you can add them to the platform by specifying the start/end IP address, user name, and password.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **IP Segment** as the adding mode.
5. Enter the required parameters.

Note

By default, the device port number is 8000.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change

your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

   Note

   - You can create a new area by device name or select an existing area.
   - If you do not import resources to an area, you cannot perform further operations for the resources.
   - Enter the range of floor number according to your application scenario.

8. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.

9. **Optional:** Perform further operations on the added device(s).

Configure Device

Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default Settings

Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click 🔍 to search for a specific device.

6.3.4 Add Elevator Control Devices in a Batch

You can download and enter elevator control device information in the predefined spreadsheet to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined spreadsheet (XSLX file) to the local disk.
6. Open the spreadsheet and edit the required device information.
7. Click and select the edited spreadsheet.
8. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.
9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
10. **Optional:** Perform further operations on the added device(s).

Configure Device	Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

6.4 Configure Parameters for Access Control Devices and Elevator Control Devices

You can configure parameters for access control devices and elevator control devices, including device time, linkage settings (linked device actions), maintenance settings, etc.

In the top left corner of Home page, select → **Basic Management → Device** .

On thel left of the Device module, select **Access Control Device** or **Elevator Control Device**, and click in the Operation column to enter the configuration page of a device.

Configure device parameters according to the following topics.

Note

- Device support required. Parameters vary with different device types and models.
- The supported features and parameters are subject to the applications you installed.

This topic includes the following topics:

- ***Custom Wiegand Parameters***
- ***Set Wiegand Parameters***
- ***Configure Device Actions***
- ***Card Swiping Parameters***

Time

You can view the time zone where the device locates and set the following parameters.

Device Time

Click the **Device Time** field to customize time for the device.

Sync with Server Time

Synchronize the device time with the server of the platform.

Biometrics

You can enable facial recognition and fingerprint recognition of access control devices if the devices support biometrics recognition.

Facial Recognition

Set facial recognition function for the device, and select a facial recognition mode.

Single-Person Recognition

The device can recognize one person at a time.

Multiple-Person Recognition

The device can recognize multiple persons at a time.

Fingerprint Recognition

Set persons' fingerprint recognition for the device. Once enabled, the device can recognize persons by their fingerprints.

Skin-surface Temperature

Set **Temperature Measurement** to on to enable temperature screening function.

Threshold(℃)

Set the range of normal skin-surface temperature. The detected temperature that is not in this range is abnormal temperature. The maximum temperature should be higher than the minimum temperature.

Open Door When Temperature is Abnormal

If it is enabled, the door will open when person's skin-surface temperature is abnormal. By default, the door will not open for abnormal temperature.

Linked Thermal Camera

Enter the device IP address of the linked thermal camera for temperature screening.

Note

It is used for the access control devices that do not support temperature screening.

Registration Device

If you enable this function, the information about added persons and credentials (including face pictures and fingerprints) added on the device will be automatically synchronized to the platform.

Mask Settings

Set **Mask Detection** to on to enable mask detection function. Once enabled, the device can detect persons without face masks.

Do Not Open Barrier when No Mask

If it is checked, the barrier will still open for persons without masks.

RS-485

RS-485 Communication Redundancy

You can check **RS-485 Communication Redundancy** to enable the function if you wire the RS-485 card to the device redundantly.

Working Mode

Select the working mode, including the card reader, door control unit, and access control host.

Turnstile Parameters

You can configure passing mode for the turnstile linked to the device.

Based on Lane Controller's DIP Mode

The device will follow the lane controller's DIP settings to control the turnstile. The settings on the main controller will be invalid.

Based on Main Controller's Settings

The device will follow the settings of main controller to control the turnstile. The DIP settings of the lane controller will be invalid.

Maintenance

You can reboot a device remotely and restore it to its default settings.

Reboot

Reboot the device.

Restore Default Settings

Restore the device to its default settings. The device needs to be activated after being restored.

Facial Recognition Mode

You can check **Deep Mode** to enable the function. Once enabled, all the face credentials applied to the device will be cleared. Go to **Access Control → Access Level** and click to apply the data in the platform to the device.

More

You can click **Configure** to open the remote configuration page of the device and configure more parameters. For details, refer to the user manual of the device.

6.4.1 Configure Relations Between Relays and Floors

You can configure the relations between relays and floors to determine how floor control is managed, including options such as passengers selecting target floors, passengers calling elevators, or automatic floor button pressing and elevator summoning for passengers.

There are three types of relay available.

Button

Control the validity for buttons of each floor. For floors related to **Button**, passengers can press the button of the floors.

Call Elevator

Control to call the elevator to go to the specified floor. For floors related to this feature, people who are waiting for elevators can call elevator to the floor they stay.

Auto Button

Control to press the button when the user swipes card inside or outside of the elevator. The button of the floor will be pressed automatically according to the user's permission.

Configure the relations between the relays and the floors.

- Drag the unconfigured relay from the Unconfigured Relay panel to the target floor.
- Drag the relay from the Floor List panel to the Unconfigured Relay panel.
- Drag the relay from one floor to another floor in the Floor List panel. If the target floor has already configured with a relay of the same type as the dragged one, it will replace the existed one of the same type.

Take the following picture as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents number of the relay, and the color under the number represents the relay type.

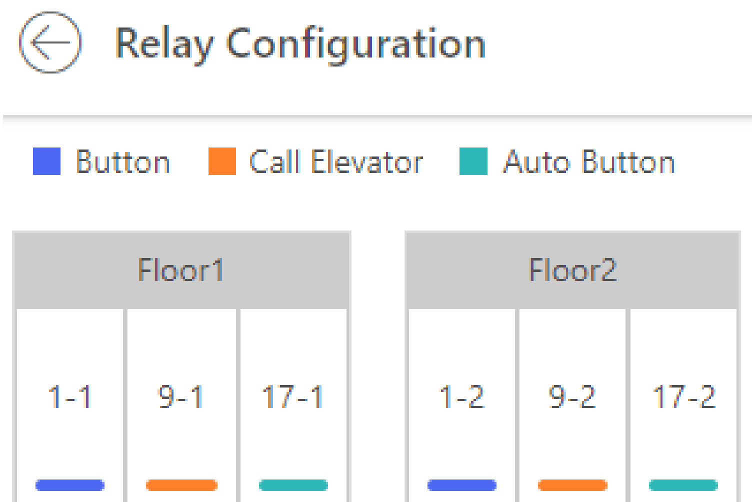


Figure 6-7 Relay Configuration

6.4.2 Custom Wiegand Parameters

Based on the knowledge of uploading rule for the third-party Wiegand, you can configure Wiegand parameters to communicate between the device and the third-party card readers.

Note

- By default, the device disables the custom Wiegand function. If you enable the custom Wiegand function, all Wiegand ports in the device will use the customized Wiegand protocol.
- You can configure up to 5 custom Wiegand devices.

Switch on **Custom Wiegand** and configure the Wiegand parameters. You can select a device from the **Copy From** drop-down list to copy the settings of another device.

Total Length

Wiegand data length.

Parity Type

Set the valid parity for Wiegand data according to property of the third party card reader. You can select **Nothing**, **Odd Even Check**, or **XOR Parity**.

If you select **Odd Even Check**, you can configure the following:

Odd Start, Length

If the odd parity start bit is 1 and the length is 12, then the platform will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0 (Bit 0 is the first bit).

Even Start, Length

If the even parity start bit is 12, and the length is 12, then the platform will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

If you select **XOR Parity**, you can configure the following:

XOR Parity Start Bit, Length per Group, Length for Parity

Depending on the table displayed below, the start bit is 0, the length per group is 4, and the length for parity is 40. It means that the platform will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits (The result length is the same as the length per group).

Output Rule

Set the output rule.

Card ID Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed below, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed below, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

Note

Take Wiegand 44 for example, the setting values in the Custom Wiegand are as follows:

Custom Wiegand Name	Wiegand 44		
Total Length	44		
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]		
Parity Type	XOR Parity		
Odd Parity Start Bit		Length	

Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

6.4.3 Set Wiegand Parameters

You can set Wiegand parameters for access control devices to facilitate communications between card readers and access control devices.

Select a Wiegand protocol in the list, and click in the Operation column to pop up a window of Wiegand information. On the pop-up window, set Wiegand parameters and click **OK**.

Direction

Whether the device is used for inputting (receiving) or outputting (sending) data.

Check **Input** or **Output**.

Wiegand Mode

The signal transmitting mode. Whether the device transmits 26-bit, 34-bit, 27-bit, and 35-bit data.

Note

Wiegand mode can only be selected when the direction is **Output**.

Output Format

Whether to output the signal as employee No. or card No.

Note

Output format can only be selected when the direction is output.

Signal Sending Interval

The interval of sending data.

Linked Card Reader

The card reader No. to be linked.

Note

Linked card reader can only be selected when the device supports linking to a card reader.

6.4.4 Configure Device Actions

You can set the linkage actions of an access control device or elevator control device for different event sources, so that when the device detects a linkage source, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc.

Click **Add** in the Linkage section. Set the event source, and then configure parameters of the linkage target.

Buzzing

Buzzer on Controller

ON

Turn on the buzzer on the access controller when the specified event is triggered.

OFF

Turn off the buzzer on the access controller when the specified event is triggered.

No Linkage

Disable the linkage action.

Buzzer on Reader

ON

Turn on the buzzer on the card reader when the specified event is triggered.

OFF

Turn off the buzzer on the card reader when the specified event is triggered.

No Linkage

Disable the linkage action.

Capture/Recording

Capture

Enable the device's linked camera to capture a picture when the specified event is triggered.

Recording

Enable the device's linked camera to record video footage when the specified event is triggered.

Alarm Output

ON

Trigger the alarm output when the specified event is triggered.

OFF

Stop the alarm output when the specified event is triggered.

No Linkage

Disable the linkage action.

Zone

ON

Arm the zone when the specified event is triggered.

OFF

Disarm the zone when the specified event is triggered.

No Linkage

Disable the linkage action.

Access Point

Unlock

Unlock the door or barrier when the specified event is triggered.

Lock

Lock the door or barrier when the specified event is triggered.

Remain Unlocked

The door or barrier will remain unlocked when the specified event is triggered.

Remain Locked

The door or barrier will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

Floor

Temporary Access

Grant access to the floor for a limited time when the specified event is triggered.

Access with Credential

Grant access to the floor if the user presents valid credentials when the specified event is triggered.

Free Access

Grant access to the floor indefinitely when the specified event is triggered.

Access Forbidden

Deny access to the floor indefinitely when the specified event is triggered.

No Linkage

Disable the linkage action.

6.4.5 Card Swiping Parameters

You can configure card swiping parameters to allow authentication by entering card number on keypad, enable NFC clone card, enable M1 encryption, etc.

In Card Swiping section, configure card swiping parameters.

Reader Communication Protocol

Select the reader communication protocol.

Input Card Number On Keypad

If it is checked, users can enter card number on keypad for authentication.

Enable NFC Card

If it is enabled, users can use cloned cards for authentication.

M1 Encryption

If it is enabled, only the card with the same encrypted sector can be granted access, and you need to choose an encrypted sector.

Voice Prompt

If it is enabled, an audio prompt will be played when swiping cards.

Upload Picture after Linked Capture

Upload the pictures captured by the linked camera(s) to the platform automatically.

Picture Storage

If it is checked, the captured pictures will be automatically saved to the storage location you configured in picture storage settings for the access points.

Note

For details about configuring picture storage settings, see ***Edit Door for Current Site*** .

Picture Size

Select a picture size from the drop-down list for the captured pictures saved to the storage location.

Picture Quality

Select a picture quality from the drop-down list for the captured pictures saved to the storage location.

Capture Times

Select the capture times from the drop-down list for the devices to capture face pictures for the times selected.

6.5 Manage Video Intercom Device

You can add video intercom devices (indoor station, door station, outer door station, and main station) to the system for management, including editing and deleting the devices, remote configuration, changing online devices' password, etc. You can also perform further operations such as video intercom, unlocking door remotely, etc. based on the added devices.

- **Indoor Station:** The indoor station is an intelligent terminal which can provide two-way audio, network transmission, data storage, remote unlocking, etc. It is mainly applied in the community.
- **Door Station:** The door station can send call to indoor station (residents) and main station. It is mainly applied in the community and office buildings.
- **Outer Door Station:** The outer door station can send call to indoor station (residents) and main station. It is mainly applied in the community and office buildings.
- **Main Station:** The main station is an intelligent terminal, which can be used to unlock door remotely, send call to residents and respond to residents' call. It is mainly applied in large community.

6.5.1 Add Detected Online Video Intercom Devices

The active online video intercom devices on the same local subnet with the current HikCentral Professional Web Client or SYS server will be displayed in the list. You can add an online device at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function will be available.

Add a Detected Online Video Intercom Device

The online video intercom devices on the same local subnet with the current Web Client or SYS server can be displayed in the list, and you can add the detected indoor station to the system one by one.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Video Intercom Device** on the left.

3. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the current Web Client will be listed in the Online Device area.
4. In the Online Device area, select the active device to be added.
5. Click in the Online Device area to enter the Add Video Intercom Device page.

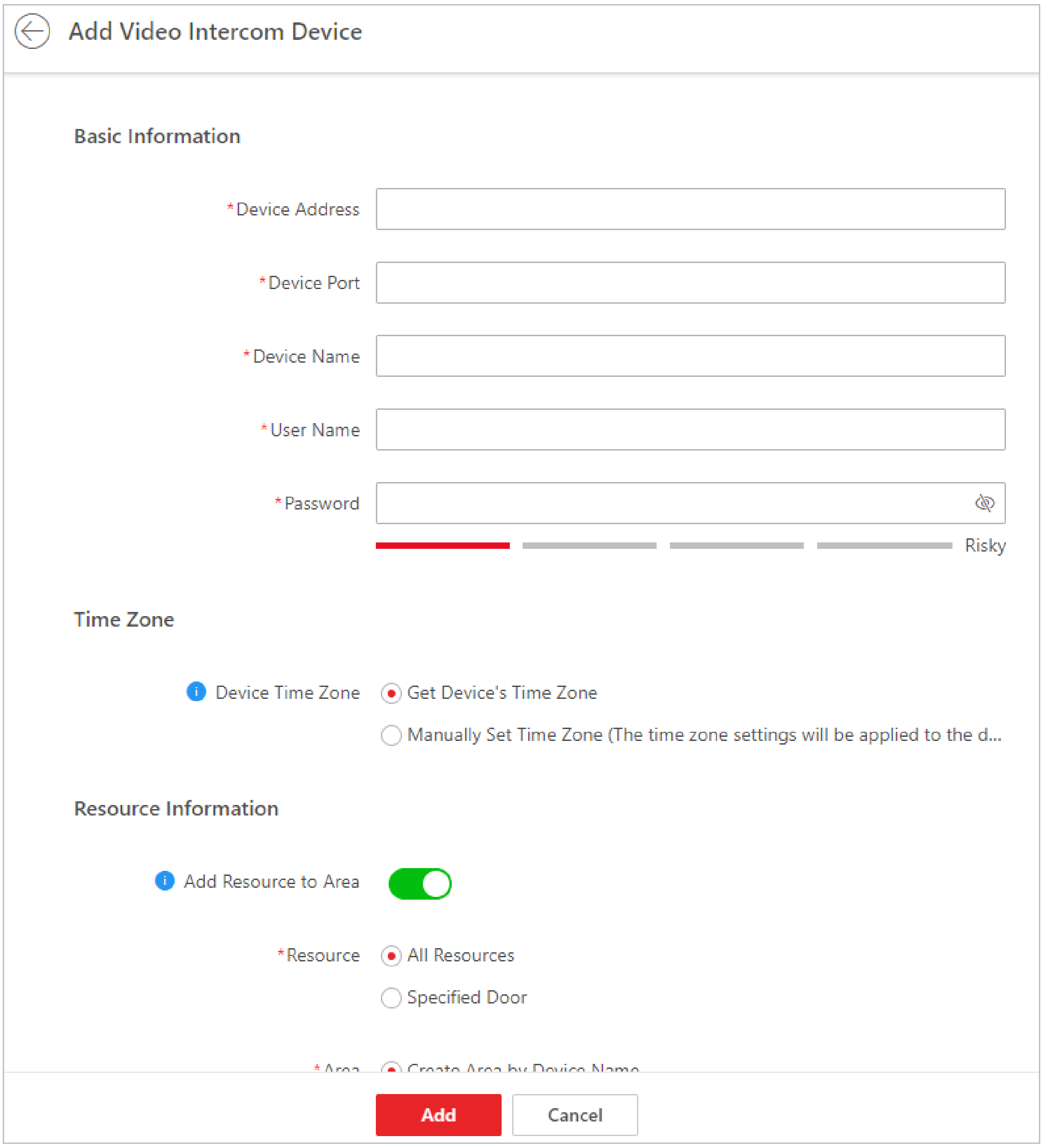


Figure 6-8 Add a Detected Online Video Intercom Device

6. Configure the basic information for the device, including device address, device port, device name, user name, and password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least

three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

7. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
8. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

   Note

   - You can import all the alarm inputs or the specified alarm input to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform further operations for the alarm inputs.
9. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

   Note

   - Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
   - It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.
10. Click **Add**.
11. **Optional:** Perform the following operation(s) after adding the online device.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Restore Default Settings	Select the added device(s), and click to restore the configured device parameters. **Note** If you want to restore all the device parameters, you can check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

Add Detected Online Video Intercom Devices in a Batch

If the detected online video intercom devices share the same user name and password, you can add multiple devices at a time.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Video Intercom Device** on the left.
3. In the Online Device area, select the active devices to be added.
4. Click in the Online Device area to enter the Add Video Intercom Device page.

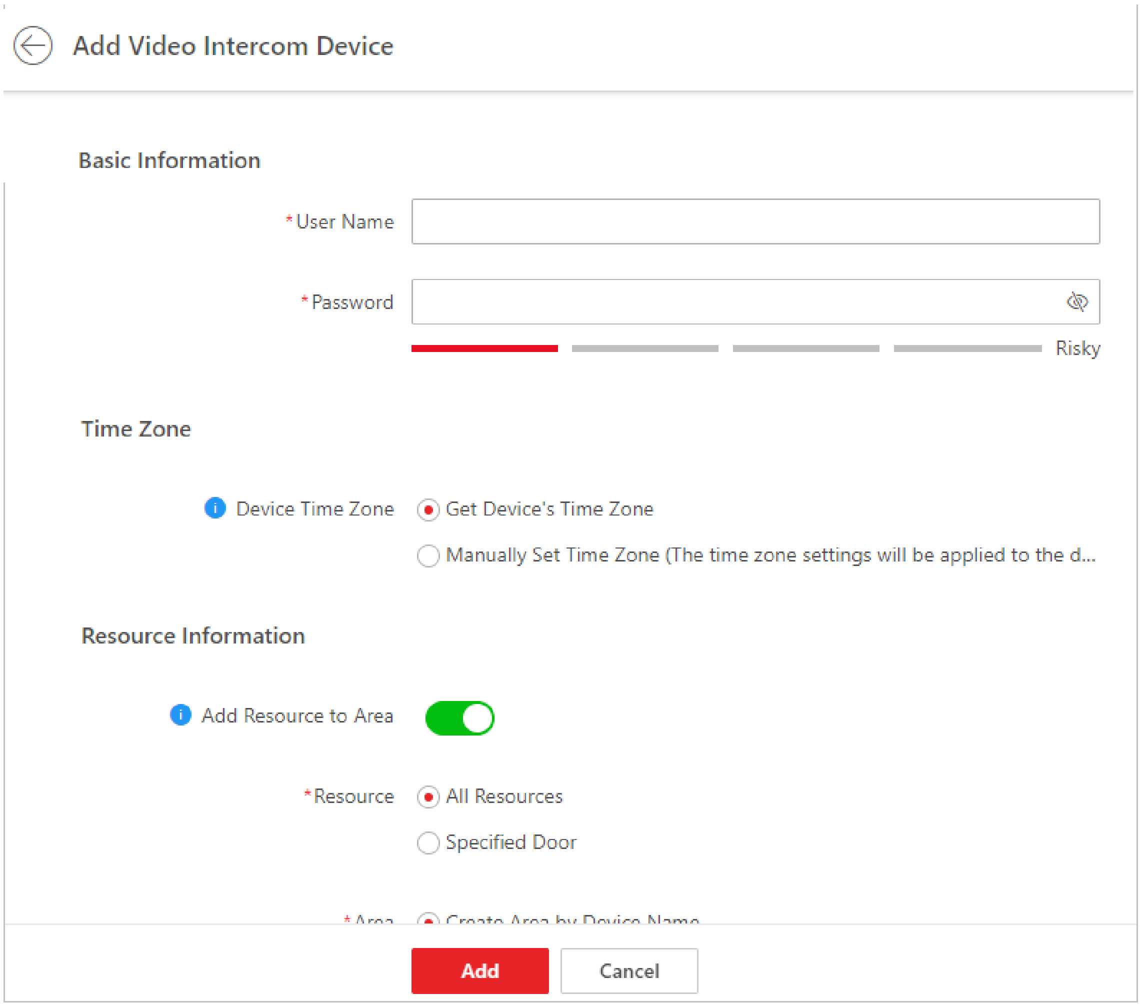


Figure 6-9 Add Detected Online Video Intercom Devices in a Batch

5. Configure the basic information for the device, including user name and password.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the alarm inputs or the specified alarm input to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further operations for the alarm inputs.

8. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

9. Click **Add**.
10. **Optional:** Perform further operations for the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
Privacy Settings	You can configure privacy settings for online video intercom devices.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Search for Devices	Enter the keywords of device name, device address, or serial No., and click to search for devices.

6.5.2 Add a Video Intercom Device by IP Address

When you know the IP address of a video intercom device, you can add it to the system by specifying the IP address, user name, password, etc. for management and further video intercom applications.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Video Intercom Device** on the left.
3. Click **Add** to enter Add Video Intercom Device page.
4. Select **IP Address** as the adding mode.

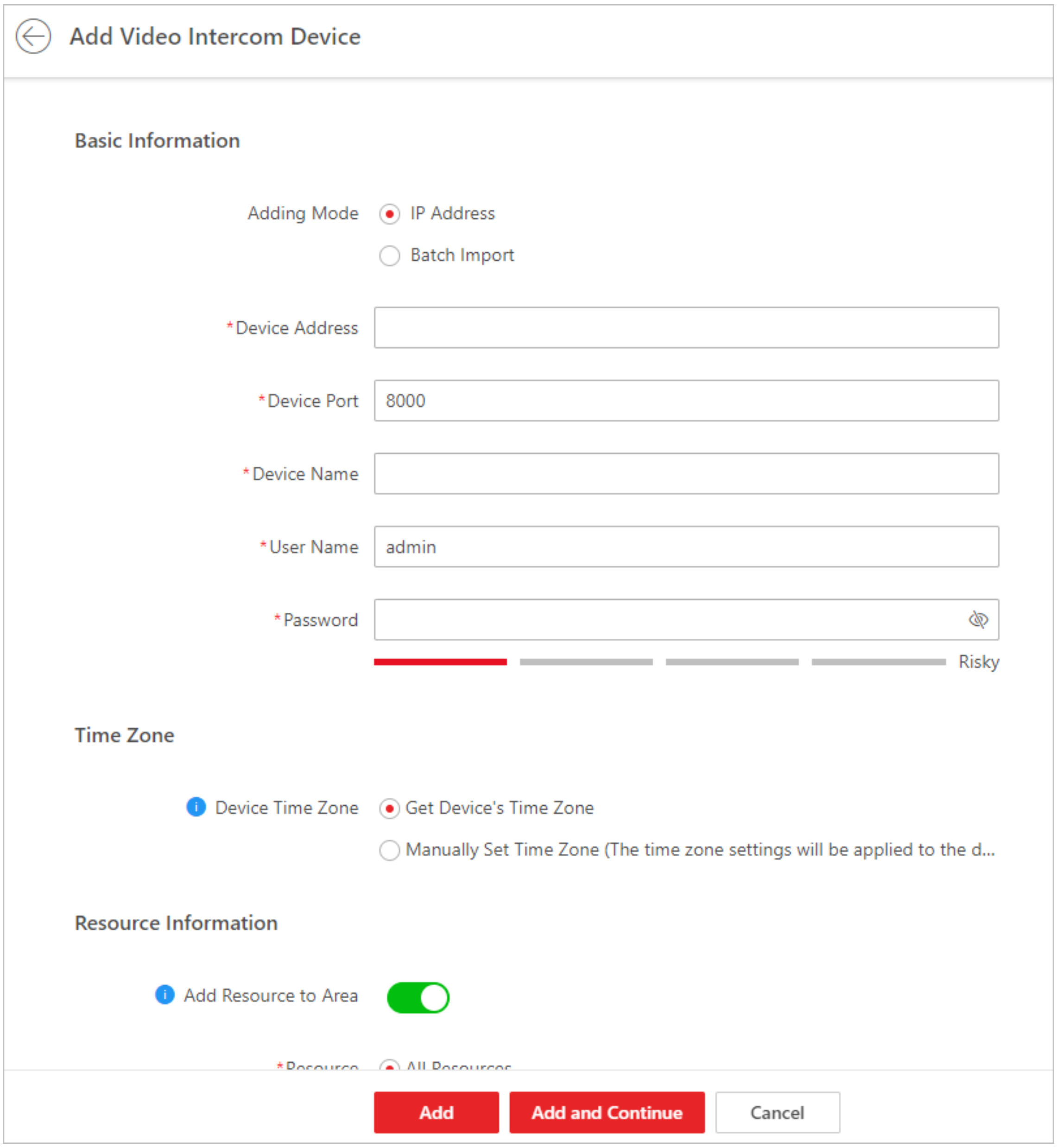


Figure 6-10 Add Video Intercom Device Page

5. Enter the required information.

Device Address

The IP address of the device.

Device Port

By default, the device port No. is 8000.

Device Name

Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

Password

The password required to access the account.

Caution

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

6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the current time zone.
7. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

   Note

   - You can import all the alarm inputs or the specified alarm input to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform further operations for the alarm inputs.
8. **Optional:** Check **Restore Default Settings** to restore all the parameters of the device configured on the system to default settings.
9. Finish adding the device.
   - Click **Add** to add the device and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add the next device.
10. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s).

	Note • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

6.5.3 Add Video Intercom Devices in a Batch

You can add video intercom devices in a batch to the system by entering the device information to the predefined template and importing the template to the system.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Video Intercom Device** on the left.
3. Click **Add** to enter Add Video Intercom Device page.
4. Click **Batch Import** as the adding mode.
5. Click **Download Template** to save the predefined template (Excel file) on your PC.
6. Open the exported template file and enter the required information of the devices to be added.
7. Click and select the template file.
8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

Note

You can click **View** to view the details of the current time zone.

9. Finish adding the devices.
   - Click **Add** to add the video intercom devices in a batch, and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add other video intercom devices.
10. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click 🔍 to search for a specific device.

6.6 Manage Visitor Terminals

The visitor terminals can be added to the system for management, including editing and deleting the devices, remote configuration, etc. The platform supports multiple ways for adding visitor terminals. You can select one of them according to your need.

6.6.1 Add Detected Online Visitor Terminals

The system can perform an automated detection for available visitor terminals in the network where the Web Client or server is located, which makes the devices' information about themselves (e.g., IP address) recognized by the system. Based on the information, you can add the devices quickly.

You can add one online devices at a time, or add multiple online devices in a batch.

Add a Detected Online Visitor Terminal

For the detected online visitor terminals, you can add the devices one by one to HikCentral Professional by specifying the user name, password, and some other parameters.

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. Such initial configuration is required in order for you to connect the devices to the HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
3. In the Online Device area, select the active device to be added.
4. Click **Add to Device List** to open the Add Online Device page.
5. Set the required information.

   Device Address

   The IP address of the device, which is shown automatically.

   Device Port

The port number of the device, which is shown automatically. The default port number is 80.

Device Name

Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

Caution

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

6. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can manually select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

8. Click **Add** to finish adding the device.
9. **Optional:** Perform the following operations after adding the online device.

Remote Configurations	Click ⚙ to remotely configure the corresponding device.

Note

For detailed operation steps about remote configuration, see the user manual of the device.

Change Password
Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Device's Time Zone
In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.

Search for Devices
Enter one or multiple key words in the search box and click to search for a specific device.

Restore Default Settings
Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

Refresh Device Information
Select the added device and click to refresh information of the device.

Add Detected Online Visitor Terminals in a Batch

For the detected online encoding devices, if they have the same user name and password, you can batch add multiple devices to HikCentral Professional.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the SYS server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the Web Client will list in the Online Device area.
3. In the Online Device area, check the active devices to be added.
4. Click **Add to Device List** to open the Add Online Device page.
5. Enter the same user name and password.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

   Caution

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

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can manually select a time zone of the device. The settings will be applied to the device automatically.
7. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

8. Click **Add**.
9. **Optional:** Perform the following operations after adding the online devices in a batch.

Remote Configurations	Click to remotely configure the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.
Refresh Device Information	Select the added device and click to refresh information of the device.

6.6.2 Add Visitor Terminal by IP Address

When you know the IP address or domain name of a device, you can add it to the platform by specifying the IP address (or domain name), user name, password, etc.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. Click **Add**.
3. Select **IP Address** as the adding mode.
4. Enter the required information.

   Device Address

   The IP address of the device.

   Device Port

   By default, the device port No. is 80.

   Device Name

   Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

   Password

   The password required to access the account.

   Caution

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

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

You can manually select a time zone of the device. The settings will be applied to the device automatically.

6. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

7. Finish adding the device.
   - Click **Add** to add the encoding device and back to the encoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other encoding devices.
8. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and**

	account information, such as user name and password. in the pop-up window.
Refresh Device Information	Select the added device and click to refresh information of the device.

6.6.3 Add Visitor Terminals by IP Segment

When multiple visitor terminals to be added have the same port number, user name, password, and have different IP addresses within a range, you can add devices by specifying the IP segment and some other related parameters.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. Click **Add**.
3. Select **IP Segment** as the adding mode.
4. Enter the required information.

   Device Address

   Enter the start IP address and the end IP address where the devices are located.

   Device Port

   By default, the device port No. is 80.

   User Name

   The user name for administrator created when activating the device or the added non-admin users. When adding the device to HikCentral Professional using the non-admin user, your permissions may restrict your access to certain features.

   Password

   The password required to access the device.

   Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

5. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can manually select a time zone of the device. The settings will be applied to the device automatically.

6. Finish adding the device.
   - Click **Add** to add the devices of which the IP addresses are between the start IP address and end IP address and back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add other encoding devices.
7. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

Refresh Device Information	Select the added device and click to refresh information of the device.

6.6.4 Add Visitor Terminals in a Batch

When there are multiple devices to be added, you can edit the predefined template containing the required device information, and import the template to HikCentral Professional to add devices in a batch.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Perform this task when you need to add devices by importing the template which contains information of multiple devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. Click **Add**.
3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template (excel file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.
6. Click and select the edited file.
7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can manually select a time zone of the device. The settings will be applied to the device automatically.
8. Finish adding devices.
   - Click **Add** to add the devices and go back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add next batch of devices.
9. **Optional:** Perform the following operation(s) after adding devices in a batch.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click 🔍 to search for a specific device.
Restore Default Settings	Select the added device(s) and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.
Refresh Device Information	Select the added device and click 🔄 to refresh information of the device.

6.7 Manage Payment Terminal

You can add payment terminals to the platform for management, including editing and deleting the devices, remote configuration, etc. The platform supports multiple ways for adding payment terminals, including adding by IP address, adding by IP segment, batch adding, etc.

6.7.1 Add Detected Online Payment Terminals

The active online payment terminals on the same local subnet with the current Web Client or the server will be displayed in a list. You can add one online device at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function will be available.

Add a Detected Online Payment Terminal

The platform automatically detects online payment terminals on the same local subnet with the client or the SYS server. You can add the detected payment terminals to the platform one by one if they do not share the same user name.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Payment Terminal** on the left panel.
3. In the Online Device area, select a network type.

   Server Network

   The detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
4. In the Online Device area, select an active device to be added.
5. Click **Add to Device List** to open the adding online device window.
6. Set the basic information for the device.

   Device Address

   The IP address of the device, which is shown automatically.

   Device Port

   The port number of the device, which is shown automatically. The default port number is 80.

Device Name

Create a descriptive name for the device.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as the operator. When adding the device to HikCentral Professional using the non-admin account, your permission may restrict your access to certain features.

Password

The password required to access the account.

Caution

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

7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Check **Restore Default Settings** to restore the configured device parameters to default settings.
9. Click **Add** to add the device to the device list.
10. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click in the Operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Refresh Device	Click in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).

Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Search for Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

Add Detected Online Payment Terminals in a Batch

For the detected online payment terminals, if they have the same user name and password, you can batch add multiple devices to the platform.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Payment Terminal** on the left panel.
3. In the Online Device area, select a network type.

   Server Network

   The detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
4. In the Online Device area, select the active devices to be added.
5. Click **Add to Device List** to open the adding online device window.
6. Set the basic information for the device.

   User Name

The user name for administrator account created when activating the device or the added non-admin account such as the operator. When adding the device to HikCentral Professional using the non-admin account, your permission may restrict your access to certain features.

Password

The password required to access the account.

Caution

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

7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. Click **Add** to add the devices to the device list.
9. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Refresh Device	Click ⟳ in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).
Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

	Note If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Search for Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.7.2 Add Payment Terminal by IP Address

When you know the IP address of a device, you can add it to the platform by specifying the IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Payment Terminal** on the left panel.
3. Click **Add**.
4. Select **IP Address** as the adding mode.
5. Set the basic information for the device.

   Device Address

   The IP address of the device, which is shown automatically.

   Device Port

   The port number of the device, which is shown automatically. The default port number is 80.

   Device Name

   Create a descriptive name for the device.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as the operator. When adding the device to HikCentral Professional using the non-admin account, your permission may restrict your access to certain features.

   Password

   The password required to access the account.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
7. **Optional:** Check **Restore Default Settings** to restore the configured device parameters to default settings.
8. Finish adding devices.
   - Click **Add** to add the device and go back to the device list page.
   - Click **Add and Continue** to add the device and continue to add other devices.
9. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click in the Operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Refresh Device	Click in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).
Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Search for Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.7.3 Add Payment Terminal by IP Segment

When multiple payment terminals to be added have the same port number, user name, password, and have different IP addresses within a range, you can add devices by specifying the IP segment and some other related parameters.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Payment Terminal** on the left panel.
3. Click **Add**.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

   Device Address

   Enter the start IP address and the end IP address where the devices are located.

   Device Port

   The port number of the device. The default device port number is 80.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as the operator. When adding the device to HikCentral Professional using the non-admin account, your permission may restrict your access to certain features.

   Password

   The password required to access the device.

Caution

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

6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
7. Finish adding devices.
   - Click **Add** to add the devices and go back to the device list page.
   - Click **Add and Continue** to add the devices and continue to add other devices.
8. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Refresh Device	Click ↻ in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).
Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Search for Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.7.4 Add Payment Terminals in a Batch

When there are multiple devices to be added, you can edit the predefined template containing the required device information, and import the template to the platform to add devices in a batch.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Payment Terminal** on the left panel.
3. Click **Add**.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (excel file) to your PC.
6. Open the template file and enter the required information of the devices to be added.
7. Click and select the edited file.
8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
9. Finish adding devices.
   - Click **Add** to add the devices and go back to the device list page.
   - Click **Add and Continue** to add the devices and continue to add other devices.
10. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click in the Operation column to configure the device remotely.

	Note For details about remote configuration, see the user manual of the device.
Refresh Device	Click in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).
Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Search for Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.8 Manage On-Board Devices

On-board devices are used for driving monitoring. They support live view, playback, remote configuration, alarm notification, GPS data collection, GPS positioning, etc. With on-board devices, you can not only get the GPS information of driving vehicles, but also set fence rules and deviation rules to regulate vehicles' movements (the platform will generate an event if any rule is violated). On the Web Client, you can manage on-board devices, including adding, editing, deleting, and remotely configuring them.

6.8.1 Add Detected Online On-Board Devices

The active online on-board devices on the same local subnet with the Web Client or SYS server will be displayed on the list. You can add online devices one by one or add multiple online devices in a batch.

Note

You should follow the instructions to install the web control properly and then the online device detection function will be available.

Add a Detected Online On-Board Device

The Web Client automatically searches for online on-board devices on the same local subnet or the SYS server. You can add detected online on-board devices to the platform one by one if they do not share the same user account.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting devices to HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **On-Board Device** .
2. Select a detected online on-board device from the Online Device list.
3. Click **Add to Device List**.
4. Set basic information.
   1) Enter the ISUP login password and name of the on-board device.

   Caution

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

   2) **Optional:** Switch on **Device Info on Wi-Fi Network** and enter the address and port No. of the on-board device as well as the user name and password of the Wi-Fi.

   Note

   Once a vehicle reaches its destination and the on-board device successfully connects to the Wi-Fi there, the video recorded during the journey will be copied back to the platform.

   3) **Optional:** Switch on **Verify Stream Encryption Key** and enter the stream encryption key set on the on-board device.

Note

The precondition is that the on-board device supports stream encryption and this feature has been enabled for it.

When starting live view or remote playback of the cameras linked with the on-board device, the Client will verify the key stored in the SYS server for security purpose.

5. Set vehicle information.
   1) Enter the license plate number of the vehicle which the on-board device is linked with.
   2) Add the vehicle to an existing area or click **Add** to add it to a newly-created area.
6. **Optional:** Set picture storage.
   1) Switch on **Picture Storage**.
   2) Select a storage location.

Note

- If you select **Local Storage**, you need to click **Configure** to configure picture storage on the SYS server.
- If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **Network Video Recorder**, you need to select a storage medium from the drop-down list.

7. Set device's time zone.
   - **Get Device's Time Zone**

     The time zone of the device will be automatically chosen according to the region of the device.
   - **Manually Set Time Zone**

     You can select a time zone and the settings will be applied to the device automatically.
8. Set resource information.
   1) Select a Streaming Server.
   2) **Optional:** Check **Wall Display via Streaming Server**.

Note

If the encoding device is not on the same network with cameras, it will get the stream for live view and playback via the Streaming Server; if they are on the same network, the encoding device can get stream directly from cameras.

   3) **Optional:** Check **Get Device's Recording Settings** to get cameras' recording settings configured on the on-board device.
9. Click **Add**.
10. **Optional:** Perform the following operations after adding the on-board device.

Edit On-Board Device	In the device list, click the name of an on-board device to edit it.
Filter Device by Wi-Fi Status	On the top right corner of the device list, select a Wi-Fi status to filter the displayed device(s).

Configure On-Board Device Remotely	In the device list, click in the Operation column to configure an on-board device remotely.
Reset Device's Time Zone	In the device list, select one or multiple on-board devices and click **Time Zone** to edit their time zones.
Delete On-Board Device	Select one or multiple devices and click **Delete** to delete them.
Search for On-Board Device(s)	Enter one or multiple key words in the search box and click to search for the specified on-board device(s).

Add Detected Online On-Board Devices in a Batch

The Web Client automatically searches for online on-board devices on the same local subnet or the SYS server. You can batch add multiple detected online on-board devices to the platform if they share the same user account.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting devices to HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **On-Board Device** .
2. Select some detected online on-board devices from the Online Device list.
3. Click **Add to Device List**.

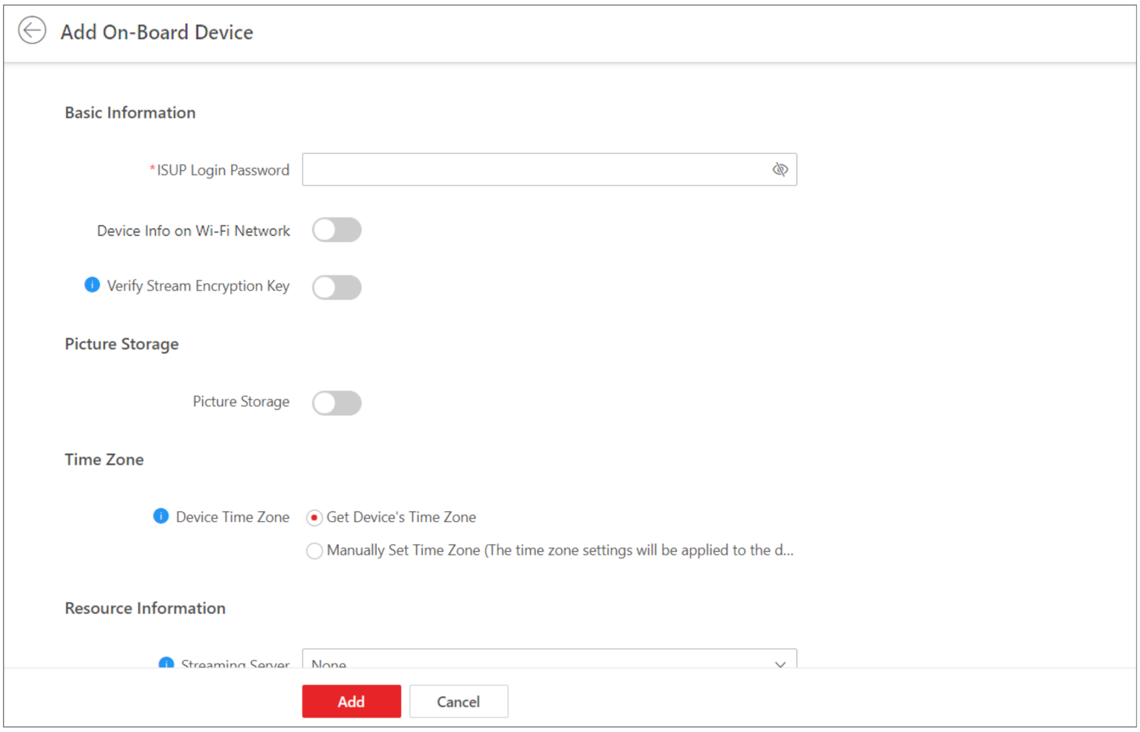


Figure 6-11 Batch Add Detected Online On-Board Devices

4. Set basic information.
   1) Enter the ISUP login password of the on-board devices.

   Caution

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

   Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

   2) **Optional:** Switch on **Device Info on Wi-Fi Network** and enter the address and port No. of the on-board devices as well as the user name and password of the Wi-Fi.

   Note

   Once a vehicle reaches its destination and the on-board device successfully connects to the Wi-Fi there, the video recorded during the journey will be copied back to the platform.

   3) **Optional:** Switch on **Verify Stream Encryption Key** and enter the stream encryption key set on the on-board devices.

Note

The precondition is that the on-board devices supports stream encryption and this feature has been enabled for them.

When starting live view or remote playback of the cameras linked with the on-board devices, the Client will verify the key stored in the SYS server for security purpose.

5. **Optional:** Set picture storage.
   1) Switch on **Picture Storage**.
   2) Select a storage location.

   Note

   - If you select **Local Storage**, you need to click **Configure** to configure picture storage on the SYS server.
   - If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **Network Video Recorder**, you need to select a storage medium from the drop-down list.

6. Set devices' time zone.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone

   You can select a time zone and the settings will be applied to the device automatically.

7. Set resource information.
   1) Select a Streaming Server.
   2) **Optional:** Check **Wall Display via Streaming Server**.

   Note

   If the encoding device is not on the same network with cameras, it will get the stream for live view and playback via the Streaming Server. If they are on the same network, the encoding device can get stream directly from cameras.

   3) **Optional:** Check **Get Device's Recording Settings** to get cameras' recording settings configured on the on-board device.
8. Click **Add**.
9. **Optional:** Perform the following operations after adding these on-board devices.

Edit On-Board Device	In the device list, click the name of an on-board device to edit it.
Filter Device by Wi-Fi Status	On the top right corner of the device list, select a Wi-Fi status to filter the displayed device(s).
Configure On-Board Device Remotely	In the device list, click ⚙ in the Operation column to configure an on-board device remotely.
Reset Device's Time Zone	In the device list, select one or multiple on-board devices and click **Time Zone** to edit their time zones.

Delete On-Board Device	Select one or multiple devices and click **Delete** to delete them.
Search for On-Board Device(s)	Enter key words in the search box and click 🔍 to search for specified on-board device(s).

6.8.2 Add an On-Board Device by Device ID

If an on-board device supports ISUP, you can add it to the platform by its device ID. This way is cost-effective when you need to manage an on-board device on the public network without a fixed IP address.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting devices to HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top left of the Web Client, click ▦ → **Device** → **Device and Server** → **On-Board Device** .
2. Click **Add**.

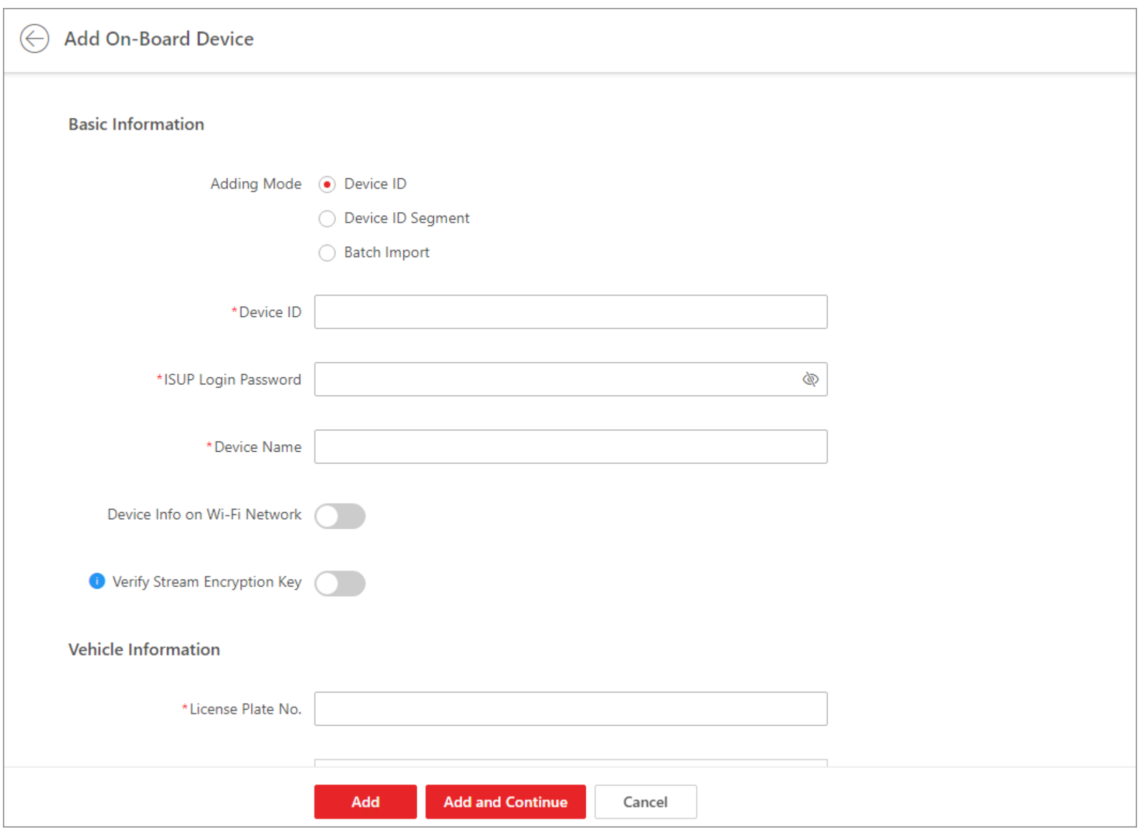


Figure 6-12 Add On-Board Device

3. Set basic information.
   1) Select **Device ID** as the adding mode.
   2) Enter the ID, ISUP login password, and name of the on-board device.
   3) **Optional:** Switch on **Device Info on Wi-Fi Network** and enter the address and port of the on-board device as well as the user name and password of the Wi-Fi.

      Note

      Once a vehicle reaches its destination and the on-board device successfully connects to the Wi-Fi there, the video recorded during the journey will be copied back to the platform.
   4) **Optional:** Switch on **Verify Stream Encryption Key** and enter the stream encryption key set on the on-board device.

      Note

      The precondition is that the on-board device supports stream encryption and this feature has been enabled for it.

      When starting live view or remote playback of the cameras linked with the on-board device, the Client will verify the key stored in the SYS server for security purpose.
4. Set vehicle information.
   1) Enter the license plate number of the vehicle which the on-board device is linked with.
   2) Add the vehicle to an existing area or click **Add** to add it to a newly-created area.
5. **Optional:** Set picture storage.
   1) Switch on **Picture Storage**.
   2) Select a storage location.

      Note

      - If you select **Local Storage**, you need to click **Configure** to configure picture storage on the SYS server.
      - If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **Network Video Recorder**, you need to select a storage medium from the drop-down list.
6. Set device's time zone.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone

   You can select a time zone and the settings will be applied to the device automatically.
7. Set resource information.
   1) Select a Streaming Server.
   2) **Optional:** Check **Wall Display via Streaming Server**.

Note

If the encoding device is not on the same network with cameras, it will get the stream for live view and playback via the Streaming Server, if they are on the same network, the encoding device can get stream directly from cameras.

3) **Optional:** Check **Get Device's Recording Settings** to get cameras' recording settings configured on the on-board device.

8. Click **Add** to finish or click **Add and Continue** to add another on-board device.
9. **Optional:** Perform the following operations after adding the on-board device.

Edit On-Board Device	In the device list, click the name of an on-board device to edit it.
Filter Devices by Wi-Fi Status	On the top right corner of the device list, select a Wi-Fi status to filter the displayed device(s).
Configure On-Board Device Remotely	In the device list, click ⚙ in the Operation column to configure an on-board device remotely.
Reset Device's Time Zone	In the device list, select one or multiple on-board devices and click **Time Zone** to edit their time zones.
Delete On-Board Device	Select one or multiple devices and click **Delete** to delete them.
Search for On-Board Device(s)	Enter key words in the search box and click 🔍 to search for specified on-board device(s).

6.8.3 Add On-Board Devices by Device ID Segment

You can add on-board device(s) to the platform by device ID segment, and perform further operations, such as editing device settings, configuring devices remotely, and deleting devices.

Steps

1. On the top left of the Web Client, click ▦ → **Device** → **Device and Server** → **On-Board Device** .
2. Click **Add**.
3. Select **Device ID Segment** as the adding mode.

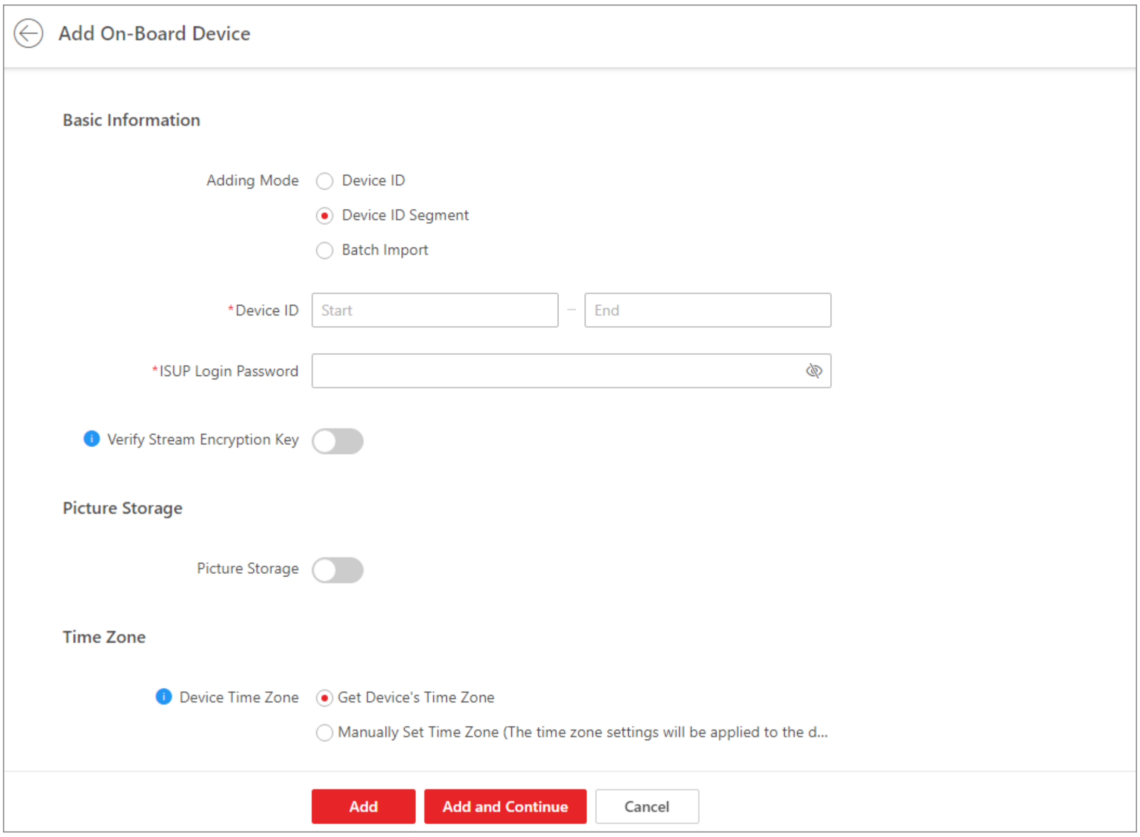


Figure 6-13 Add On-Board Device by Device ID Segment

4. Configure the basic information of the device(s).
   1) Enter the start device ID and end device ID.

   Note

   - If the start ID and end ID are the same, only one device will be added.
   - If the start ID is smaller than the end ID, multiple devices will be added with their IDs arranged in ascending order. For example, if you set the start ID and end ID to 1 and 3 respectively, then devices named 1, 2, and 3 will be added.

   2) **Optional:** Enter the ISUP login password.
   3) **Optional:** Enabled stream encryption, and switch on **Verify Stream Encryption Key** and enter the stream encryption key on the device.

   Note

   This function should be supported by the device.
5. Configure picture storage for the device(s).
   1) Switch on **Picture Storage**.
   2) Select a storage server type and a storage server from the drop-down list as the storage location.
6. **Optional:** Set the time zone for the device.

- **Get Device's Time Zone**

  The time zone of the device will be automatically chosen according to the region of the device.
- **Manually Set Time Zone (The settings will be applied to the device automatically)**

  You can select a time zone of the device. The settings will be applied to the device automatically.

7. Configure the resource information.
   1) Select a streaming server from the drop-down list.
   2) **Optional:** Check **Wall Display via Streaming Server** to use the Streaming Server to play videos on the smart wall.

   Note

   This parameter is configurable only when you select a Streaming Server in the former substep.
   3) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the device.
8. Click **Add** to finish, or click **Add and Continue** to add other device(s).
9. **Optional:** Perform the following operation(s) if needed.

Edit Device Settings	Click the name of a device in the Device Name column to edit its settings.
Filter Devices by Wi-Fi Status	On the top right corner of the device list, select a Wi-Fi status to filter the displayed device(s).
Delete Device	In the device list, check one or multiple devices, and click **Delete** to delete the device(s).
Configure Device Remotely	• Option 1: Click in the Operation column to configure the device remotely. • Option 2: Click the name of a device to enter its settings page, and then click **Configuration on Device** in the upper-right corner to configure the device remotely. **Note** To support remote configuration, the device should be configured with an IP address.
Edit Device's Time Zone	In the device list, check a device, and click **Time Zone** to edit its time zone settings. You can also check multiple devices and configure the same time zone for them.
Search for On-Board Device(s)	Enter one or multiple key words in the search box and click to search for specified on-board device(s).

6.8.4 Add On-Board Devices in a Batch

You can fill in an Excel file with required information of to-be-added on-board devices and upload it onto the platform to batch add them for management.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting the devices to HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top left of the Web Client, click ▦ → **Device** → **Device and Server** → **On-Board Device** .
2. Click **Add**.

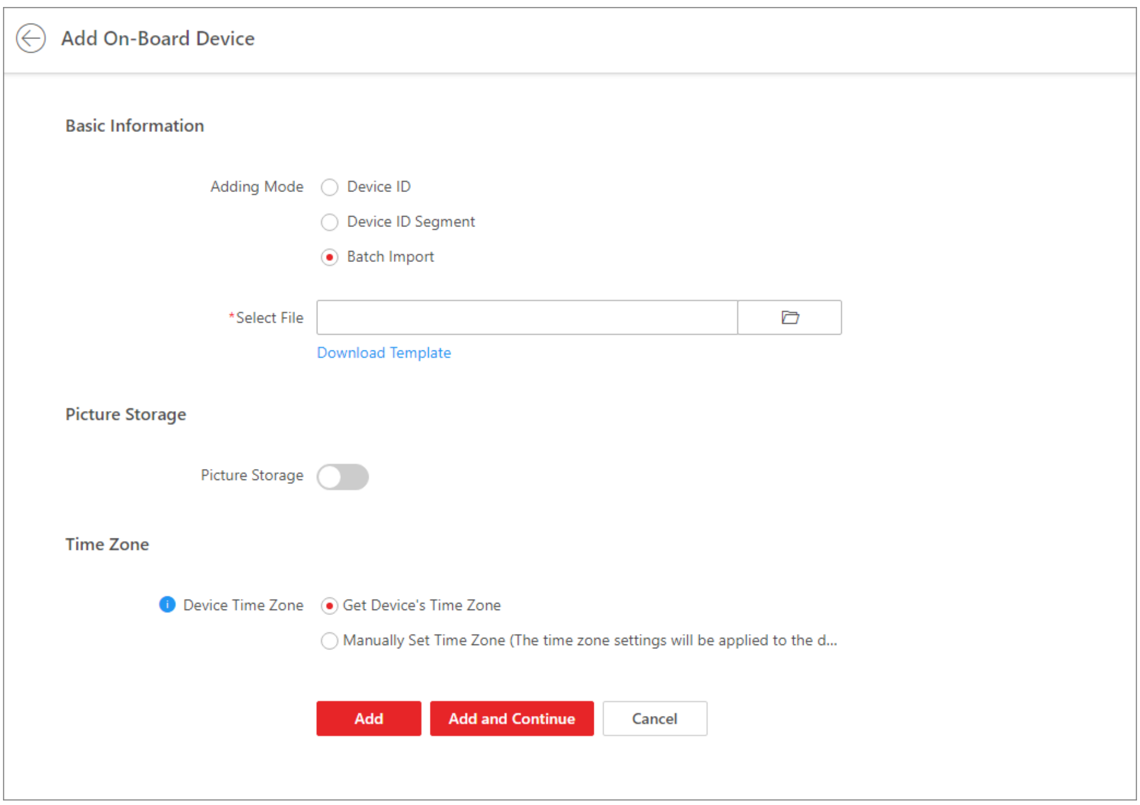


Figure 6-14 Batch Add On-Board Devices

3. Set basic information.
   1) Select **Batch Import** as the adding mode.
   2) Click **Download Template** to save the template file to your PC and fill it in with required information.
   3) Click 🗁 to select the file and upload it to the platform.
4. **Optional:** Set picture storage.

1) Switch on **Picture Storage**.
2) Select a storage location.

Note

- If you select **Local Storage**, you need to click **Configure** to configure picture storage on the SYS server.
- If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **Network Video Recorder**, you need to select a storage medium from the drop-down list.

5. Set devices' time zone.
   - **Get Device's Time Zone**

     The time zone of the device will be automatically chosen according to the region of the device.
   - **Manually Set Time Zone**

     You can select a time zone and the settings will be applied to the device automatically.
6. Click **Add** to finish or click **Add and Continue** to add another batch of on-board devices.
7. **Optional:** Perform the following operations after adding these on-board devices.

Edit On-Board Device	In the device list, click the name of an on-board device to edit it.
Filter Device by Wi-Fi Status	On the top right corner of the device list, select a Wi-Fi status to filter the displayed device(s).
Configure On-Board Device Remotely	In the device list, click in the Operation column to configure an on-board device remotely.
Reset Device's Time Zone	In the device list, select one or multiple on-board devices and click **Time Zone** to edit their time zones.
Delete On-Board Device	Select one or multiple devices and click **Delete** to delete them.
Search for On-Board Device(s)	Enter key words in the search box and click to search for specified on-board device(s).

6.9 Add a Query Terminal

A query terminal is installed with the Self-Service Vehicle Finding Client and is mounted in a parking lot for vehicle owners to locate and find their vehicles. On the Web Client, you can add a query terminal by its device ID and further manage it such as editing its information and removing it from the platform.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Query Terminal** on the left navigation pane.
3. Click **Add** to enter the Add Query Terminal page.

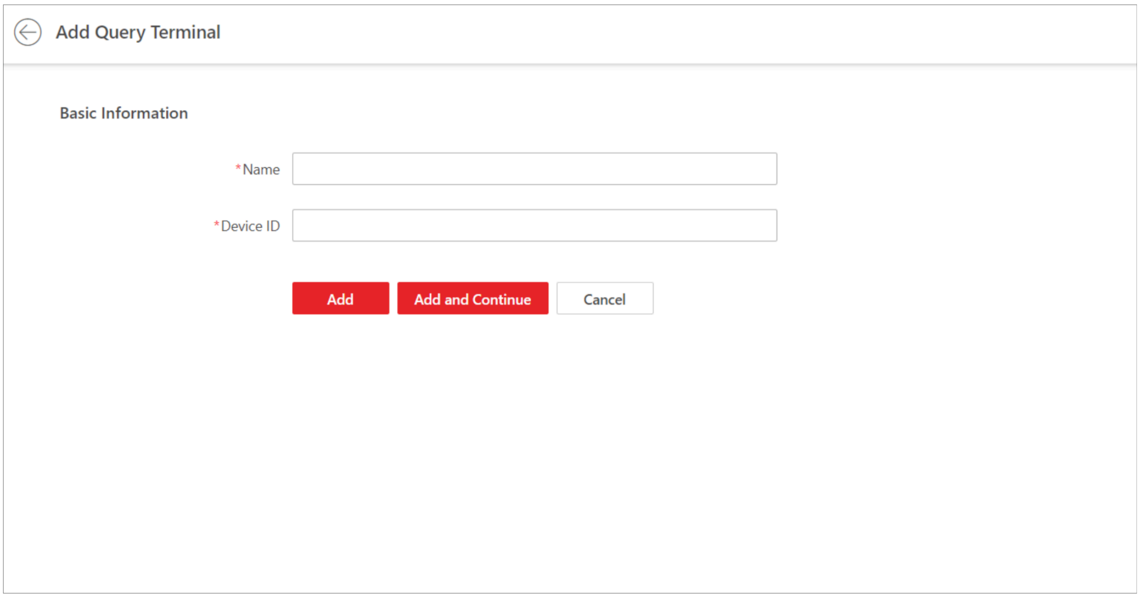


Figure 6-15 Add Query Terminal

4. Create a name for the query terminal.
5. Enter the device ID of the query terminal.
6. Click **Add** to finish, or click **Add and Continue** to add another query terminal.
7. **Optional:** Perform the following operations.

Edit Query Terminal	On the device list, click the name of a query terminal to edit it.
Delete Query Terminal	Select one or multiple query terminals, and click **Delete** to delete them.
Search for Query Terminal	Enter key words in the search box, and click to search for specified query terminal.

6.10 Add an Entrance/Exit Control Device

An entrance/exit control device is used for managing the entrance or exit of a parking lot, especially that of an unattended parking lot. After a vehicle gets a ticket or card from an entrance/exit control device, the device will control the barrier gate to open and let the vehicle enter. After the vehicle returns the ticket or card, the device will allow the vehicle to exit. Besides, if an entrance/exit control device issues cards instead of tickets, its guidance screen is configurable, which means you can configure the information displayed on it.

Steps

1. On the top navigation bar, select ▦ → **Basic Management → Device** to enter the device management module,
2. Select **Device and Sever → Entrance/Exit Control Device** on the left navigation pane.
3. Click **Add** to enter the Add Entrance/Exit Control Device page.

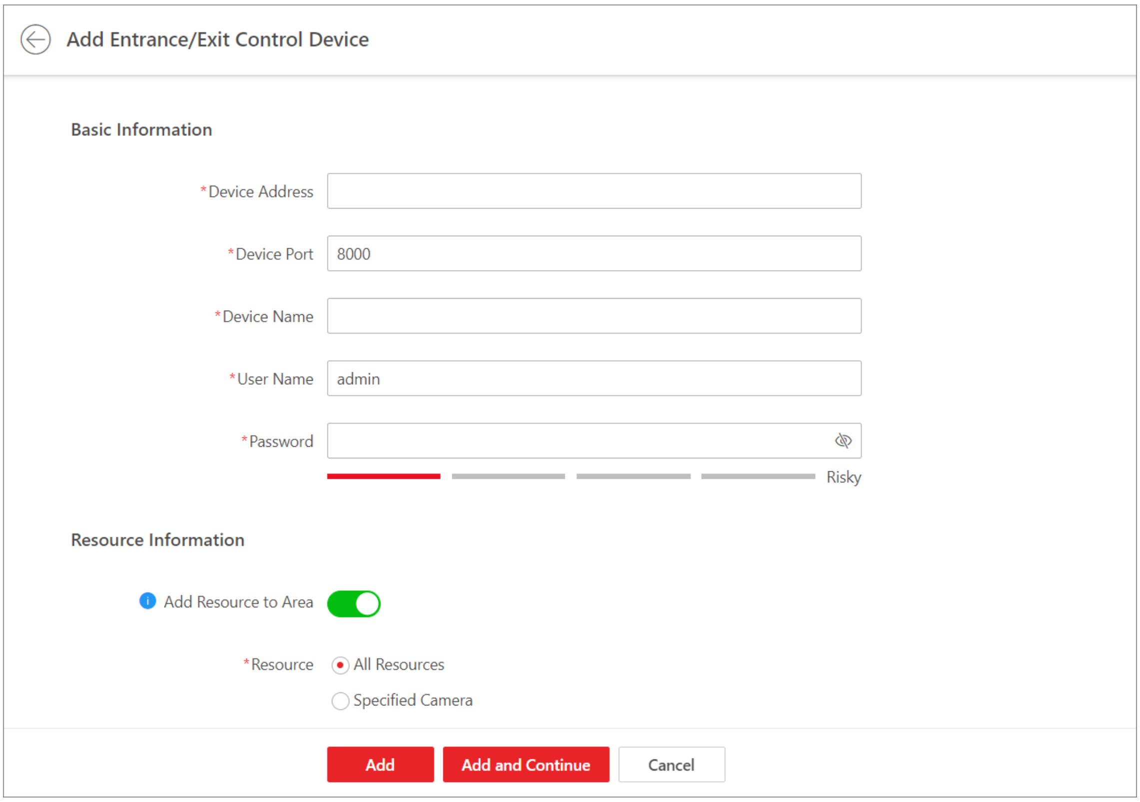


Figure 6-16 Add Entrance/Exit Control Device Page

4. In the Basic Information area, enter the IP address, port No., device name, user name, and password of the entrance/exit control device.
5. **Optional:** Add the entrance/exit control device's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **All Resources** or **Specified Camera**.

   Note

   If you select **All Resources**, all the resources related to the entrance/exit control device will be added to an area; if you select **Specified Camera**, you need to select camera(s) to add.

   3) Select **Create Area by Device Name** or **Existing Area**.

Note

If you select **Create Area by Device Name**, an area named after the entrance/exit control device will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area.

4) Select **None** or a streaming server to get the stream for live view and playback.

Note

After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.

5) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the entrance/exit control device.

6. Click **Add** to finish or click **Add and Continue** to add another entrance/exit control device.
7. **Optional:** Perform the following operations.

Edit Entrance/Exit Control Device	In the Device Name column, click the name of an entrance/exit control device to edit it.
Delete Entrance/Exit Control Device	Select one or multiple entrance/exit control devices and click **Delete** to delete them.
Configure Entrance/Exit Control Device Remotely	In the Operation column, click ⚙ to configure the entrance/exit control device remotely.
Refresh Device Information	In the Operation column, click ⟳ to refresh the entrance/exit control device's information.
Search for Device	Enter a keyword in the search box and click 🔍 to search for a specific device.

6.11 Manage Guidance Terminals

In Resource Management, you can add guidance terminals to the platform, check device details, change device password, and configure device parameters. While you add a guidance terminal, you can add its resources (such as connected parking cameras and alarm inputs/outputs) to areas for further configurations.

Note

After you add and manage guidance terminals int Resource Management, you can set up a parking guidance system for your parking lot. See details in ***Parking Guidance Configuration*** .

6.11.1 Add Detected Online Guidance Terminals

The platform can automatically detect the available guidance terminals on the same network where the Web Client or the SYS server is running. You can add one online terminal at a time, or batch add multiple online terminals if they have the same user name and password.

Add a Detected Online Guidance Terminal

You can add detected online guidance terminals one by one if the terminals do not share the same user name or password.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** to enter the device management module.
2. Select **Device and Server → Guidance Terminal** on the left navigation pane.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select an activated device and click **Add to Device List**.
5. In the Basic Information area, edit the device login information.

   Device Name

   Create a descriptive name for the device. For example, you can use an alias that indicates the location or feature of the device.

   User Name

   User name of administrator account created when the device is activated, or of an added non-admin account such as operator account.

   Note

   Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

   Password

   Password of the account that you are logging in.

Caution

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

6. **Optional:** Add the guidance terminal's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **All Resources** or **Specified Camera**.

   Note

   If you select **All Resources**, all resources related to the guidance terminal will be added to the area; if you select **Specified Camera**, you need to select the camera(s) to add.
   3) Select **Create Area by Device Name** or **Existing Area**.

   Note

   If you select **Create Area by Device Name**, an area named after the guidance terminal will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area.
   4) Select **None** or a streaming server to get the stream for live view and playback.

   Note

   After a streaming server is selected, its linked camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.
   5) Switch on **Video Storage** to select a storage location for recorded videos and set recording schedule for the cameras.

   Note

   - The pStor is the storage access service for managing local HDDs and logical disks.
   - The pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.

- Before you can select **Hybrid Storage Area Network**, **Cluster Storage**, or **pStor** from the storage location list, you should configure them. You can also click **Add New** to add a new one.
- You can check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal and the linked camera(s) will start recording according to the schedule, or uncheck **Get Device's Recording Settings** and set the recording schedule for the cameras, such as recording schedule template and stream type.

7. Click **Add**.
8. **Optional:** Perform further operations after adding the online device.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click ⚙ in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click ⟳ to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device.

Note

- You can change the password for online HIKVISION devices only.
- If multiple devices share the same password, you can select these devices and batch change the password for them.

Batch Add Detected Online Guidance Terminals

You can batch add detected online guidance terminals if the terminals have the same user name and password.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top navigation bar, select ▦ → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Guidance Terminal** on the left navigation pane.
3. In the Online Device area, select a network type.

   Server Network

All detected online devices on the same local subnet with the SYS server.

Local Network

All detected online devices on the same local subnet with the current Web Client.

4. Select multiple activated devices and click **Add to Device List**.
5. In the Basic Information area, edit devices' login information.

User Name

User name of administrator account created when activating the device, or the added non-admin account such as operator account.

Note

Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

Password

Password of the account that you are logging in.

Caution

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

6. **Optional:** Add guidance terminals related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

   Note

   If you select **Create Area by Device Name**, an area named after guidance terminals will be created, and resources will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area.

   3) Select **None** or a streaming server to get the stream for live view and playback.

   Note

   After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.

   4) Switch on **Video Storage** to select a storage location for recorded videos and set recording schedule for the cameras.

Note

- The pStor is the storage access service for managing local HDDs and logical disks.
- The pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.
- Before you can select **Hybrid Storage Area Network**, **Cluster Storage**, or **pStor** from the storage location list, you should configure them. You can also click **Add New** to add a new one.
- You can check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal and the linked camera(s) will start recording according to the schedule, or uncheck **Get Device's Recording Settings** and set the recording schedule for the cameras, such as recording schedule template and stream type.

7. Click **Add**.
8. **Optional:** Perform further operations after batch adding online devices.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click ⚙ in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click ↻ to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device. **Note** • You can change the password for online HIKVISION devices only. • If multiple devices have the same password, you can select these devices to batch change the password for them.

6.11.2 Add a Guidance Terminal by IP Address

If you know the IP address of the guidance terminal you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** to enter the device management module.
2. Select **Device and Server → Guidance Terminal** on the left navigation pane.
3. Click **Add** to open the Add Guidance Terminal page.
4. Set **Adding Mode** to **IP Address**.
5. Edit the device connection and login information.

   Device Name

   Create a descriptive name for the device. For example, you can use an alias that can indicate the location or feature of the device.

   User Name

   User name of the administrator account created when the device is acctivated, or the added non-admin account such as operator account.

   Note

   Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

   Password

   Password of the account that you are logging in.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
6. **Optional:** Add the guidance terminal's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **All Resources** or **Specified Camera**.

   Note

   If you select **All Resources**, all the resources related to the guidance terminal will be added to an area; if you select **Specified Camera**, you need to select the camera(s) to add.

   3) Select **Create Area by Device Name** or **Existing Area**.

Note

If you select **Create Area by Device Name**, an area named after the guidance terminal will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area.

4) Select **None** or a streaming server to get the stream for live view and playback.

Note

After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.

5) Switch on **Video Storage** to select a storage location for recorded videos and set recording schedule for the cameras.

Note

- The pStor is the storage access service for managing local HDDs and logical disks.
- The pStor Cluster Service is a service that manages multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.
- Before you can select **Hybrid Storage Area Network**, **Cluster Storage**, or **pStor** from the storage location list, you should configure them. You can also click **Add New** to add a new one.
- You can check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal and the linked camera(s) will start recording according to the schedule, or uncheck **Get Device's Recording Settings** and set the recording schedule for the cameras, such as recording schedule template and stream type.

7. Click **Add** to finish or click **Add and Continue** to add another guidance terminal.
8. **Optional:** Perform further operations after adding a guidance terminal.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click ⚙ in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click ↻ to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device.

Note

- You can change the password for online HIKVISION devices only.
- If multiple devices share the same password, you can select these devices and batch change the password for them.

6.11.3 Batch Add Guidance Terminals by IP Segment

If the guidance terminals you want to add to the platform are on the same subnet and share the same port, user name, and password, you can add them by specifying the start and end IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** to enter the device management module.
2. Select **Device and Server → Guidance Terminal** on the left navigation pane.
3. Click **Add** to open the Add Guidance Terminal page.
4. Set **Adding Mode** to **IP Segment**.
5. Edit the device connection and login information.

   Device Address

   Start IP address and end IP address.

   User Name

   User name of the administrator account created when activating the device, or the added non-admin account such as operator account.

   Note

   Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

   Password

   Password of the account that you are logging in.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6. **Optional:** Add the guidance terminal's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

   Note

   If you select **Create Area by Device Name**, an area named after the guidance terminal will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area.

   3) Select **None** or a streaming server to get the stream for live view and playback.

   Note

   After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.

   4) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal.
7. Click **Add** to finish or click **Add and Continue** to add guidance terminals with another IP segment.
8. **Optional:** Perform further operations after adding guidance terminals.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click ⚙ in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click ⟳ to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device.

Note

- You can change the password for online HIKVISION devices only.
- If multiple devices have the same password, you can select these devices to batch change the password for them.

6.11.4 Batch Add Guidance Terminals by Port Segment

If the guidance terminals you want to add to the platform share the same IP address, user name, and password, but they are using different ports, you can add them by specifying the IP address, port range, user name, password, etc.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** to enter the device management module.
2. Select **Device and Server → Guidance Terminal** on the left navigation pane.
3. Click **Add** to open the Add Guidance Terminal page.
4. Set **Adding Mode** to **Port Segment**.
5. Edit the device connection and login information.

   Device Port

   Start port number and end port number of the devices.

   User Name

   User name of the administrator account created when activating the device, or the added non-admin account such as operator account.

   Note

   Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

   Password

   Password of the account that you are logging in.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6. **Optional:** Add the guidance terminal's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

   Note

   If you select **Create Area by Device Name**, an area named after the guidance terminal will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area.

   3) Select **None** or a streaming server to get the stream for live view and playback.

   Note

   After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.

   4) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal.
7. Click **Add** to finish or click **Add and Continue** to add guidance terminals with another port segment.
8. **Optional:** Perform further operations after adding guidance terminals.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click ⚙ in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click ⟳ to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device.

Note

- You can change the password for online HIKVISION devices only.
- If multiple devices have the same password, you can select these devices to batch change the password for them.

6.11.5 Batch Add Guidance Terminals by Template

You can download a predefined template and edit the guidance terminals' information in the template to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have activated the devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Guidance Terminal** on the left navigation pane.
3. Click **Add** to open the Add Guidance Terminal page.
4. Set **Adding Mode** to **Batch Import**.
5. Click **Download Template** to download the predefined template file (in XLSX format) to local disk.
6. In your download folder on PC, open the spreadsheet and edit the required device information.
7. On the Web Client, click and open the edited spreadsheet.
8. Click **Add** to finish or click **Add and Continue** to batch add guidance terminals by another spreadsheet.
9. **Optional:** Perform further operations after adding guidance terminals.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device.

Note

- You can change the password for online HIKVISION devices only.
- If multiple devices have the same password, you can select these devices to batch change the password for them.

6.12 Add Display Screen

Display screens can be used in places such as the entrance of a parking lot to show the real-time number of vacant parking spaces. You can add a display screen to the platform by specifying its LAN IP address.

Steps

1. Select **Device and Server → Parking Lot Screen** on the left navigation pane.
2. Click **Add** to open the Add Display Screen page.
3. Select a screen type.
4. Set parameters which vary among different types of display screens.

   LAN IP Address

   IP address assigned to the display screen on LAN.

   Device Port

   For entrance guidance screens and parking guidance screens, the port No. is required.

   Number of Display Rows

   The number of rows of the content can be displayed on the screen, which is determined by the device model.

   For example, if the value is 2, it means the screen supports showing 2 rows of different information.

Figure 6-17 Entrance Guidance Screen - One Row

Number of Directions

The number of directions supported by the parking guidance screen, which is determined by the device model.

For example, if the value is 3, it means the screen supports showing the vacant parking spaces in three directions.

Figure 6-18 Parking Guidance Screen - Three Directions

5. Click **Add** to finish adding the display screen, or click **Add and Continue** to continue adding another display screen.
6. **Optional:** Perform the following operations after adding the screens.

Edit a Display Screen	In the Device Name column, click the name of a display screen to edit it.
Delete Device(s)	Check one or multiple devices in the list, and click **Delete** to delete the selected devices.
Search for Device	Enter the keyword(s) in the search box and click 🔍 to search for a specific device.
Refresh Device Information	In the Operation column, click ⟳ to refresh the display screen's information, or click **Refresh All** to refresh all the added display screens' information.

Test Device Connection	Select a device, click **Test**, enter a text, and click **OK** to apply it to the select screen to test the device connection.

What to do next

- After adding an entrance and exit display screen or an entrance guidance screen, you can link a lane with the screen and configure the related information for the screen in Parking Lot Management.
- After adding a parking guidance screen, you can set up a parking guidance system for your parking lot in Parking Guidance Configuration.

6.13 Add Under Vehicle Surveillance System

You can add Under Vehicle Surveillance System (UVSS) to the system by specifying the device IP address, port number and some other related parameters.

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. Such initial configuration is required in order to be able to connect the devices to the system via network.

Steps

1. On the top navigation bar, select → **Basic Management → Device** to enter the device management module.
2. Select **Device and Server → UVSS** on the left navigation pane.
3. Click **Add** to enter the Add Under Vehicle Surveillance System page.
4. Set the required basic information such as device address, device port number, and device name.
5. **Optional:** Switch on **Add Resource to Area** to import the resources of the added UVSS to an area.
   - Select **Create Area by Device Name** to create an area named after the UVSS for adding the resource(s) to the created area.
   - Select **Existing Area**, and select an existing area to add the resource(s) to.

   Note

   - If you select **Existing Area**, you can also click **Add** to add a new area.
   - If you do not import resources to area, you cannot perform the further configurations for the resources.
6. Click **Add** to finish adding the UVSS, or click **Add and Continue** to continue adding another UVSS.
7. **Optional:** Perform the following operations after adding UVSSs.

Edit a UVSS	In the Device Name column, click the name of a UVSS to edit it.
Delete Device(s)	Check one or multiple devices in the list, and click **Delete** to delete the selected devices.

Search for Device	Enter the keyword(s) in the search box and click to search for a specific device.
Refresh Device Information	In the Operation column, click to refresh a UVSS's information, or click **Refresh All** to refresh all the added UVSS' information.

6.14 Manage Security Control Device

You can add the security control devices to the system for managing partition, zone, arming/disarming, handling alarms,etc.

The security control device includes the security control panel, panic alarm station, Axiom wireless security control panel, security radar etc., which are widely applied to many scenarios. You can also add the channels (including cameras, alarm inputs, alarm outputs and radars) of the security control device to the area.

A security control panel is used for monitoring arming zones, handling alarm signal from the triggers, and uploading alarm reports to the central alarm monitoring station. The security control panel is very important for preventing robbery, theft or other accidents.

A panic alarm station is mainly installed in the areas with the crowd or high incidence of cases, such as school, square, tourist attraction, hospital, supermarket gate, market, station, parking lot, etc. When the emergency happens or someone asks for help, the person can press panic button to send alarm to the monitoring center, and the operator in the center will take the appropriate actions. The panic alarm station helps to realize alarm aid in emergency.

Security radar is an detecting device used to detect the target by electromagnetic wave. Security radar event will be triggered when the security radar detects object(s) entering the radar zone, and the calibration camera(s) will start to work to capture more details about this event.

6.14.1 Add Detected Online Security Control Devices

The active online security control devices in the same local subnet with the current Web Client or SYS server will be displayed on a list. You can add one online device one by one, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online Security Control Device

You can add the detected online security control devices, and here we introduce the process for adding single one device.

Before You Start

- Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the current Web Client will be listed in the Online Device area.
3. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.

   Note

   To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** and switch on **Allow ISUP Registration**.
4. In the Online Device area, select an active device to be added.
5. Click to open the Add Security Control Device window.
6. Enter the required information.

   Note

   The device's IP address and port number can be automatically shown in **Device Address** field and **Device Port** field.

   Caution

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

- Click **Manually Set Time Zone** and select a time zone from the drop-down list.

  Note

  You can click **View** to view the details of the selected time zone.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

   Note

   - You can select **Specified Alarm Input and Radar** and select the specified alarm inputs and radars to import to the area.
   - System will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform the further configurations for the resources.

9. Click **Add**.
10. **Optional:** Perform the following operations after adding the online device.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

Batch Add Detected Online Security Control Devices

For those detected online security control devices, if they have the same password for the same user name, you can add multiple devices at a time.

Before You Start

- Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the SYS server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the Web Client will list in the Online Device area.
3. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.

   Note

   To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** and switch on **Allow ISUP Registration**.
4. In the Online Device area, select the active devices to be added.
5. Click to open the Add Security Control Device window.
6. Enter the required information.

   Caution

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

- Click **Get Device's Time Zone**.
- Click **Manually Set Time Zone** and select a time zone from the drop-down list.

Note

You can click **View** to view the details of the selected time zone.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

Note

- You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars to import to the area.
- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the further configurations for the resources.

9. Click **Add**.
10. **Optional:** Perform the following operations after adding the online devices in batch.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password. **Note** • You can only change the password for online HIKVISION devices currently. • If multiple devices in the device list have the same password, you can change the password for them in a batch.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.14.2 Add Security Control Device by IP Address

When you know the IP address of the security control device to add, you can add the devices to the platform by specifying the IP address, user name, password, and other related parameters.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the system via network.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

Note

- By default, the device port is 8000.
- For wireless security control panels, the default port is 80.
- For alarm boxes, the default port is 502.

Device Address

Enter the IP address of the device.

Device Port

Enter the port number of the device.

Device Name

The name of the device, which can be used to describe the device function, location, etc.

User Name

The admin account (which is created when activating the device) or the non-admin account, such as the operator. If you use a non-admin account to add devices, the permissions might be limited.

Password

The password required to access the account.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers,

and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
7. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs, and radars) of the added security control device to an area.

   Note

   - You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars to import to the area.
   - Platform will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - Up to 64 alarm inputs can be imported in one area. If you don't import resources to area, you cannot perform further operations for the resources.
   - Up to 10 radars can be imported in one area. If you don't import radars to area, you cannot perform further operations for the radars.
8. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
9. **Optional:** Perform the following operations after adding the devices.

   Note

   The supported functions vary according to different device types.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.14.3 Add Security Control Device by Hik-Connect DDNS

You can add security control devices with dynamic IP addresses to the system by domain name solutions of Hik-Connect. Currently, the system only supports domain name solutions function of Hik-Connect.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the system via network.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **Hik-Connect DDNS** as the adding mode.
5. Select a device source.

   New Device

   Add a new device to both Hik-Connect and the system.

   Hik-Connect DDNS Device List

   Add devices managed by Hik-Connect to the system in a batch by getting the device list.
6. Set required parameters.

   Hik-Connect DDNS Server Address

   Enter the address of the Hik-Connect service. By default, it's ***https://open.ezvizlife.com***.

   Note

   If you select Hik-Connect DDNS Device List as the source type, you can click **Get Device List** to get the device list in the account.

Serial No.

For adding a new device, enter the serial No. of the device.

Verification Code

For adding a new device, enter the verification code of the device.

Device Name

The name of the device, which can be used to describe the device function, location, etc.

User Name

The admin account (which is created when activating the device) or the non-admin account, such as the operator. If you use a non-admin account to add devices, the permissions might be limited.

Password

The password required to access the account.

Caution

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

7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

   Note

   - System will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform the further configurations for the resources.
9. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.

10. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.14.4 Add Security Control Devices by IP Segment

If the security control devices having the same port No., user name and password, and their IP addresses are between the IP segment, you can specify the start IP address and the end IP address, port No., user name, password, and other related parameters to add them.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the system via network.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **IP Segment** as the adding mode.
5. Enter the required the information.

Caution

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

6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
7. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

Note

- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the further configurations for the resources.

8. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
9. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.14.5 Add Security Control Devices by Port Segment

If the security control devices having the same user name and password, and their port No. are between the port segment, you can specify the start port No. and the end port No., user name, password, and other related parameters to add them.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **Port Segment** as the adding mode.
5. Enter the required the information.

Caution

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

6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

Note

You can click **View** to view the details of the selected time zone.

7. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

Note

- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the further configurations for the resources.

8. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
9. **Optional:** Perform the following operations after adding the devices.

Remote Configurations

Click to set the remote configurations of the corresponding device.

Note

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

Change Password

Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Time Zone

Select a device and click **Time Zone** to set its time zone.

Search Device(s)

Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).

Refresh Device List

Click **Refresh All** to refresh the device list.

6.14.6 Add Security Control Device by Device ID

For the security control devices supporting ISUP, you can add them by specifying a predefined device ID, ISUP login password, etc. This is an economic choice when you need to manage a security control device in the public network but without fixed IP address by HikCentral Professional.

Before You Start

- Make sure the security control device you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device. For details, refer to the user manual of security control device.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision ISUP Protocol** as the access protocol.

   Note

   To allow device registration via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** and switch on **Allow ISUP Registration**.
4. Select **Device ID** as the adding mode.
5. Enter the required information, including device ID, ISUP login password, and device name.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
6. **Optional:** In the Picture Storage field, switch on **Picture Storage** and select a storage location from the drop-down list.
7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

Note

- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the further configurations for the resources.

9. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
10. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.14.7 Add Security Control Device by Device ID Segment

If you need to add multiple security control devices which have no fixed IP address and support ISUP to HikCentral, you can add them to HikCentral Professional at a time after configuring a device ID segment for the devices.

Before You Start

- Make sure the security control device you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device. For details, refer to the user manual of security control device.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To allow device registration via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** and switch on **Allow ISUP Registration**.
4. Select **Device ID Segment** as the adding mode.
5. Enter the required information, including the start device ID, the end device ID, and the ISUP login password.
6. **Optional:** In the Picture Storage field, switch on **Picture Storage**, and select a storage location from the drop-down list.
7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs and radars) of the added security control device to an area.

   Note

   - System will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform the further configurations for the resources.
9. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
10. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device.

	Note For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.14.8 Batch Add Security Control Devices

You can edit the predefined template with the security control device information to add multiple devices at a time.

Before You Start

- Make sure the security control device you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device when adding devices via Hikvision ISUP. For details, refer to the user manual of security control device.

Steps

1. On the top navigation bar, go to ▦ → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To allow device registration via ISUP, you need to go to ▦ → **Basic Management** → **System** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (excel file) in your PC.

6. Open the exported template file and edit the required information of the devices to be added on the corresponding column.
7. Click and select the template file with device information.
8. **Optional:** In the Picture Storage field, switch on **Picture Storage**, and select a storage location from the drop-down list.

Note

This field displays only when you select **Hikvision ISUP Protocol** as the access protocol.

9. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.

10. Finish adding devices.
    - Click **Add** to add the devices and go back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add other devices.
11. **Optional:** Perform the following operations after adding devices in a batch.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.14.9 Add Security Control Device from the Site on Hik-Partner Pro

If you have configured parameters for the site on Hik-Partner Pro accessing the platform, you can add security control devices from the site on Hik-Partner Pro to the platform. Deleting devices on the platform will not delete devices from the site on Hik-Partner Pro.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- Make sure you have enabled **Access on Hik-Partner Pro**. To complete related configuration, you can 1) go to → **Basic Management** → **System** → **Network** → **Hik-Partner Pro Access** or 2) click **Configure** in the Access Protocol area on the Add Security Control Device page.

Steps

1. On the top navigation bar, go to → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization.
3. Select **Hik-Partner Pro Protocol** as the access protocol.
4. Select the device source.
   - Select **New Device**, and enter the device serial No., verification code, and device name.

     Note

     Make sure the new device to be added has registered to Hik-Connect. After the device is added, the corresponding site where the device is on Hik-Partner Pro will also be added.
   - Select **Hik-Parnter Pro Device List**, and select device(s) from the list.

     Note

     - For devices with the same name on Hik-Partner Pro, suffixes will be added to the names of the devices.
     - If the selected device is deleted from the platform, it will not be deleted from the site on Hik-Partner Pro.
5. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the selected time zone.

6. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, and alarm outputs) of the added security control device to an area.

Note

- Platform will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- Up to 64 alarm inputs can be imported in one area. If you don't import resources to area, you cannot perform further operations for the resources.

7. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
8. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.14.10 Add Security Control Device via Modbus Protocol

You can add security control devices to the platform via Modbus protocol, and the parameters you need to configure include IP address, device name, device port number, etc.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the system via network.

Steps

1. In the top left corner of the Web Client, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. Click **Add** to enter the Add Security Control Device page.
4. Select **Modbus Protocol** as the Access Protocol.

Note

The alarm boxes can only be added to the platform via Modbus Protocol.

5. Enter the required information.

Device Address

Enter the IP address of the device.

Device Port

Enter the port number of the device.

Device Name

The name of the device, which can be used to describe the device function, location, etc.

Manufacture

Select the manufacture from the drop-down list.

Alarm Inputs

The number of alarm inputs of the device. The value range is from 1 to 65535.

Alarm Outputs

The number of alarm outputs of the device. The value range is from 1 to 65535.

Alarm Input

Set the default alarm input signal to low level or high level.

6. **Optional:** Switch on **Add Resource to Area** to import the resources of the added security control device to an area.

Note

- You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars to import to the area.
- The platform will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- Up to 64 alarm inputs can be imported to one area. If you don't import alarm inputs to an area, you cannot perform further operations for them.
- Up to 10 radars can be imported to one area. If you don't import radars to an area, you cannot perform further operations for them.

7. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list.

- Click **Add and Continue** to save the settings and continue to add the next security control device.

8. **Optional:** Perform the following operations after adding the devices.

Remote Configurations
Click to set the remote configurations of the corresponding device.

Note

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

Change Password
Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Time Zone
Select a device and click **Time Zone** to set its time zone.

Search for Device(s)
Enter a keyword in the search box in the upper right corner to quickly search for the target device(s).

Refresh Device List
Click **Refresh All** to refresh the device list.

6.14.11 Add Security Control Device via SIA Protocol

When the device supports the SIA protocol, you can add it to the system via the SIA protocol and then configure zones of the device.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required to connect the devices to the system via the network.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **SIA** as the device type.
4. Enter the required information.

   Device Address

   Enter the IP address of the device.

Device Port

Enter the port number of the device.

Note

- By default, the device port is 8000.
- For wireless security control panels, the default port is 80.
- For alarm boxes, the default port is 502.

Device Name

The name of the device, which can be used to describe the device's function, location, etc.

Account ID

Enter the account ID of the SIA device.

5. **Optional:** Add zones to the device.
   1) Click **Add Zone**.
   2) Enter the zone name and zone ID.
   3) Click **Add**.
6. **Optional:** To set the time zone for the device, select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
7. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs, and radars) of the added security control device to an area.

   Note

   - You can create a new area by the device name or select an existing area.
   - The platform will generate security control partitions in the area, based on the settings on the device.
   - Up to 64 alarm inputs can be imported to one area. If you don't import resources to an area, you cannot perform further operations for the resources.
   - Up to 10 radars can be imported to one area. If you don't import radars to an area, you cannot perform further operations for the radars.
8. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list.
   - Click **Add and Continue** to add the current device and continue to add the next security control device.
9. **Optional:** Perform the following operations after adding the devices.

   Note

   The supported functions vary according to different device types.

Remote Configurations	Click ⚙ to set the configurations of the corresponding device.

	Note For details about the configurations, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search for Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search for the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

6.15 Manage Fire Protection Device

On the left, select **Device and Server → Fire Protection Device** .

6.15.1 Add Fire Protection Device

You can add a fire protection device to the system by IP address and IP segment, and add fire protection devices in a batch.

Click **Add** to enter the Add Fire Protection Device page.

User Intention and Adding Method	Description
Add Fire Protection Device by IP Address: you know the IP address of a fire protection device.	1. Select **Hikvision Private Protocol** as the access protocol. 2. Select **IP Address** as the adding mode. 3. Enter the information as required. 4. (Optional) Select the time zone for device. 5. (Optional) Switch on **Add Resource to Area** to import the resources of the added device to the area.
Add Fire Protection Device by IP Segment: you know	1. Select **Hikvision Private Protocol** as the access protocol. 2. Select **IP Segment** as the adding mode.

User Intention and Adding Method	Description
the IP segment of a fire protection device.	3. Enter the information as required. 4. (Optional) Select the time zone for device. 5. (Optional) Switch on **Add Resource to Area** to import the resources of the added device to the area.
Add Fire Protection Device by Device ID: you know the device ID of a fire protection device.	1. Select **Hikvision ISUP Protocol** as the access protocol. 2. Select **Device ID** as the adding mode. 3. Enter the information as required. 4. (Optional) Select the time zone for device. 5. (Optional) Switch on **Add Resource to Area** to import the resources of the added device to the area.
Add Fire Protection Devices by ID Segment: you know the ID segment of a fire protection device.	1. Select **Hikvision ISUP Protocol** as the access protocol. 2. Select **Device ID Segment** as the adding mode. 3. Enter the information as required. 4. (Optional) Select the time zone for device. 5. (Optional) Switch on **Add Resource to Area** to import the resources of the added device to the area.
Add Fire Protection Devices in a Batch: there are multiple fire protection devices to be added.	1. Select **Batch Import** as the adding mode. 2. Click **Download Template** and save the file in CSV format to the local PC. 3. Open the downloaded template and enter the required information of the devices in the corresponding column. 4. Click and select the edited file. 5. (Optional) Select the time zone for device. 6. (Optional) Switch on **Add Resource to Area** to import the resources of the added device to the area.

Finish adding the device by one of the following methods.

- Click **Add** to save the current device and return to the device list.
- Click **Add and Continue** to save the current device and continue to add another device.

6.15.2 After Adding Fire Protection Device: Operations on Device List Page

You can manage the added devices, including editing and deleting the devices, configuring the devices remotely, changing online devices' password, etc.

Operations	Description
Remote Configurations	Click to configure the device remotely.

Operations	Description
	Note For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Edit Time Zone	Select one or multiple devices and click **Time Zone** to re-edit the time zone of selected device(s).
Search for Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.16 Manage Dock Station

The dock station is a data collector which can automatically detect and back up law-enforcement data and evidence data from body camera(s) connected to it. The dock station can also be used to charge the body cameras.

After adding dock stations to the system, you can search the data (video footage, pictures, and audio files) backed up on the dock stations and download the data via the Control Client for convenient management. You can also monitor the online status of the dock stations, and perform other operations such as playing video footage backed up on the dock stations.

Note

- For more details about the dock station, see the user manual of the device.
- For details about searching video footage of the dock stations, see the *HikCentral Professional Control Client User Manual*.

6.16.1 Add Dock Station by IP Address

When you know the IP address or domain name of the dock station to be added, you can add the device to the platform by specifying the IP address, user name, password, and other related parameters.

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. Such initial configuration is required for connecting the devices to the HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management → Device** .
2. Click **Device and Server → Portable Enforcement Device** on the left panel.
3. Click **Add** to enter the Add Dock Station page.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

   Device Address

   IP address or domain name of the dock station.

   HTTP Port

   Enter the HTTP port of the device. By default, it is 80.

   Device Name

   Create a descriptive name for the device.

   Note

   Up to 64 characters are allowed for the device name.

   User Name

   User name of the dock station.

   Password

   Password of the account that you are logging in.
6. **Optional:** Set time zone for the dock station.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
7. **Optional:** Switch on **File Storage** to set the storage information of files uploaded by the dock station.

   Storage Location

The recording server, in which the videos and pictures will be stored according to the configured backup schedule. The following types of recording servers are supported: Hybrid Storage Area Network, pStor, and Cluster Storage.

Note

You should configure the recording servers in advance, or its storage location cannot be displayed in the drop-down list.

Copyback Time

The backup schedule of files uploaded by the dock station.

Copy-Back File Type

Select **All Files** or **Important Files** as the copy-back file type.

8. Finish adding the dock station.
   - Click **Add** to add the current dock station and go back to the dock station list page.
   - Click **Add and Continue** to add the current dock station and add more other dock stations.
9. **Optional:** Perform the following operations.

Edit Dock Station	• Click the dock station name on the device list to edit the dock station. • Click **Copy To** to select the item (settings of time zone or storage information) to copy, and copy the selected settings of this dock station to other dock station(s).
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.
Set Time Zone	Select a dock station and then click **Time Zone** to set its time zone.
Search for Dock Station(s)	Enter keywords in the search box on the upper right corner of the page to quickly search for the target device(s).

6.16.2 Add Dock Stations by IP Segment

When multiple dock stations to be added have the same port number, user name, password, and have different IP addresses within a range, you can add devices by specifying the IP segment and some other related parameters.

Before You Start

Make sure the dock stations you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting the devices to the HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select ⊞ → **Basic Management** → **Device** .
2. Click **Device and Server** → **Portable Enforcement Device** on the left panel.
3. Click **Add** to enter the Add Dock Station page.
4. Select **IP Segment** as the adding mode.

5. Enter the required information.

   Device Address

   Enter the start IP address and the end IP address. For example, if five dock stations need to be added, and their IP address are "10.41.7.231", "10.41.7.232", "10.41.7.233", "10.41.7.234", and "10.41.7.235" respectively, you should enter ***10.41.7.231*** and ***10.41.7.235***.

   HTTP Port

   Enter the HTTP port number of the device. By default, it is 5651.

   User Name

   User name of the dock station.

   Password

   Password of the account that you are logging in.
6. **Optional:** Set time zone for the dock station.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
7. Finish adding the dock stations.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and continue to add more dock stations.
8. **Optional:** Perform the following operations.

Edit Dock Station	• Click the dock station name on the device list to edit the dock station. • Click **Copy To** to select the item (settings of time zone or storage information) to copy, and copy the selected settings of this dock station to other dock station(s).
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.
Set Time Zone	Select a dock station and then click **Time Zone** to set its time zone.
Search for Dock Station(s)	Enter keywords in the search box on the upper right corner of the page to quickly search for the target device(s).

6.16.3 Add Dock Stations by Port Segment

When multiple dock stations to be added have the same IP address, user name, password, and have different port numbers within a range, you can add devices by specifying the port segment and some other related parameters.

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. Such initial configuration is required for connecting the devices to the HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management → Device** .
2. Click **Device and Server → Portable Enforcement Device** on the left.
3. Click **Add** to enter the Add Dock Station page.
4. Select **Port Segment** as the adding mode.
5. Enter the required information.

   Device Address

   The same IP address where the devices are located.

   HTTP Port

   Enter the start port number and the end port number. For example, if there are five dock stations to be added, and their port number are 80, 81, 82, 83, and 84 respectively, you should enter ***80*** and ***84***.

   User Name

   The same user name of the dock stations.

   Password

   Password of the account that you are logging in.
6. **Optional:** Set time zone for the dock station.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
7. Finish adding the device.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and add more dock stations by port segment.
8. **Optional:** Perform the following operations.

Edit Dock Station	• Click the dock station name on the device list to edit the dock station. • Click **Copy To** to select the item (settings of time zone or storage information) to be copied, and copy the selected settings of this dock station to other dock station(s).
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.
Set Time Zone	Select a dock station and then click **Time Zone** to set its time zone.
Search for Dock Station(s)	Enter keywords in the search box on the upper right corner of the page to quickly search for the target device(s).

6.16.4 Batch Add Dock Stations

When there are multiple dock stations to be added to HikCentral Professional, you can download a predefined template and fill it in with the required information of the dock stations, and then import the template to the platform to add multiple dock stations at a time.

Before You Start

Make sure the dock stations you are going to use are correctly installed and connected to the network as specified by the manufacturer. Such initial configuration is required for connecting the device to the HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management → Device** .
2. Click **Device and Server → Portable Enforcement Device** on the left panel.
3. Click **Add** to open the Add Dock Station page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (CSV file) on your PC.
6. Open the template file and enter the required information of the devices to be added in the corresponding column.
7. Click and select the template file.
8. **Optional:** Set time zone for the dock stations.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the current time zone.

   - Click **Get Device's Time Zone** to get the device's time zone.
9. Finish adding the dock stations.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and continue to add more dock stations.
10. **Optional:** Perform the following operation(s).

Edit Dock Station	• Click the dock station name on the device list to edit the dock station. • Click **Copy To** to select the item (settings of time zone or storage information) to be copied, and copy the selected settings of this dock station to other dock station(s).
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.
Set Time Zone	Select a dock station and then click **Time Zone** to set its time zone.
Search for Dock Station(s)	Enter keywords in the search box on the upper right corner of the page to quickly search for the target device(s).

6.17 Manage Portable Device

You can add portable devices to the platform via four methods: adding by device ID, adding by device ID segment, batch importing devices, and adding auto-detecting devices. After adding portable devices, you can manage them including editing, searching, deleting, etc.

Go to → **Basic Management** → **Device** → **Device** → **Portable Enforcement Device** → **Portable Device** .

6.17.1 Add Portable Devices

The platform can auto detect the portable devices that have been plugged in or are plugged in the dock stations, and you can add these devices to the platform conveniently. You can also add portable devices by device ID and ID segment.

Note

Before you start, make sure the devices you are going to use are correctly installed and connected to the network.

User Intention and Adding Method	Steps
Add auto-detected portable device: Portable devices that have been plugged in or are plugged in the dock stations can be auto detected.	1. Click **Add** to enter the Add Portable Device page. 2. Select **Auto Detect** as the adding mode, and select detected portable device(s) in the list.. 3. Enter the required parameters, and click **Add**.
Add portable device by device ID: You can add portable devices by entering device ID, ISUP login password, device name, etc.	1. Click **Add** to enter the Add Portable Device page. 2. Select **Enter Manually** and **Device ID** as the Adding Mode. 3. Enter the required parameters, and click **Add**.
Add portable devices by ID segment: If you need to add multiple portable devices which have no fixed IP addresses, you can configure ID segment for	1. Click **Add** to enter the Add Portable Device page. 2. Select **Enter Manually** and **Device ID Segment** as the Adding Mode. 3. Enter the required parameters, and click **Add**.

User Intention and Adding Method	Steps
the devices and add them to the platform at a time.	
Add portable devices in a batch: When there are multiple portable devices to be added, you can edit the predefined template containing the required device information, and import the template to the platform to add devices in a batch.	1. Click **Add** to enter the Add Encoding Device page. 2. Select **Batch Import** as the adding mode. 3. Download the predefined template file to your PC, enter the required information, and click to import the file to the platform. 4. Set the required parameters and click **Add**.

6.17.2 After Adding Portable Devices: Operations on Device List Page

After you add portable devices, you can perform further operations on the device list.

Operations	Descriptions
Remote Configurations	Click in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Set Time Zone	Select one or more device(s), click **Time Zone** to set/edit the time zone of the selected device(s).
Batch Apply Parameters / Apply parameters to Platform Devices	Click **Parameter Settings** and select **Batch Apply Parameters / Apply parameters to Platform Devices** to apply set parameters to selected devices or apply current parameter configuration to all portable devices in platform.

6.18 Manage Digital Signage Terminals

Before releasing information, digital signage terminals should be added to the system first. After adding devices, you can edit and delete the devices. Further operations are also supported, including remote configuration, changing devices' password, configuring time zone, etc.

6.18.1 Add Digital Signage Terminal

You can add digital signage terminals to the platform by multiple methods: adding online terminals, adding by IP address, adding by auto registration on device, adding by IP segment, importing devices in a batch, and adding by authentication code. After adding terminals to the platform, you can configure, manage, and control the terminals.

On the left, select **Device and Server → Digital Signage Terminal** .

Adding Operations

Adding Mode and Scenario	Description
Add Terminal by Auto Registration on Device: you have configured the platform's IP address for the device by a web browser.	1. Click **Add → Add by Auto Registration** or click **Auto Registration**. 2. Enter the platform address and authentication code on the device for registration. 3. Select device(s) from the list and click **Batch Add to Device List**. 4. Enter authentication code of the device, select time zone, and select an area. 5. Click **OK**.
Enable General Authentication Code: adding the terminal which supports OTAP/ ISUP.	The authentication code is used for the terminal to register on the platform by OTAP/ISUP. 1. Click **Auto Registration → Add by Configuring General Authentication Code on Platform** . 2. Switch on **General Authentication Code**. 3. Enter the authentication code. 4. (Optional) In the Add Resource to Area list, select an area to add the device to. 5. Click **OK**.
Add Online Terminals: the online terminals	Before you start, make sure: You have downloaded and installed the Web Control.

Adding Mode and Scenario	Description
to be added are on the same LAN as the server.	1. In the online device list, select one or multiple devices to be added, and then click **Add to Device List** to enter the Add Device page. 2. Set the basic information. 3. (Optional) Set the time zone of the device. 4. (Optional) In the Add Resource to Area list, select an area to add the device to. 5. Finish adding the device. - Click **Add** to add the current device and back to the device list page. - Click **Add and Continue** to add the current device and continue to add other devices.
Add Terminal by IP Address: you know the IP address of the terminal to be added.	1. Click **Add → Add Manually** to enter the Add Device page. 2. Select the Access Protocol as **Hikvision Private Protocol** or **Hikvision OTAP Protocol**. 3. If **Hikvision OTAP Protocol** is selected, select **IP Address/Domain** in the Adding Mode list. 4. Set the basic information. 5. (Optional) Set the time zone of the device. 6. In the Add Resource to Area list, select an area to add the device to. 7. Finish adding the device. - Click **Add** to add the current device and back to the device list page. - Click **Add and Continue** to add the current device and continue to add other devices.
Add Terminals by IP Segment: multiple devices to be added have the same port number, user name, password, and have different IP addresses within a range.	1. Click **Add → Add Manually** to enter the Add Device page. 2. Select the Access Protocol as **Hikvision OTAP Protocol**. 3. (Optional) Select **IP Segment** in the Adding Mode list. 4. Enter the required information. 5. (Optional) Set the time zone of the device. 6. (Optional) In the Add Resource to Area list, select an area to add the device to. 7. Finish adding the device. - Click **Add** to add the current device and back to the device list page. - Click **Add and Continue** to add the current device and continue to add other devices.
Batch Import Terminals: multiple devices to be added.	1. Click **Add → Add Manually** to enter the Add Device page. 2. Select the Access Protocol as **Hikvision Private Protocol** or **Hikvision OTAP Protocol**. 3. Select **Batch Import** in the Adding Mode list.

Adding Mode and Scenario	Description
	4. Click **Download Template** and save the predefined template (excel file) on your PC. 5. Open the exported template file and enter the required information of the devices to be added in the corresponding column. 6. Click and select the edited file. 7. (Optional) Set the time zone of the device. 8. (Optional) In the Add Resource to Area list, select an area to add the device to. 9. Finish adding the device. - Click **Add** to add the current device and back to the device list page. - Click **Add and Continue** to add the current device and continue to add other devices.

After Adding Digital Signage Terminals: Operations on Device List Page

After you add digital signage terminals, you can perform further operations on the device list.

Operation	Description
Change Password	Select one or more devices, and click **Change Password** to change the password for the selected devices. **Note** If multiple devices have the same password, you can change the password for them simultaneously.
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zones of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** according to your requirements.
Search Device(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target device(s).

6.18.2 Configure Device Display Settings

After adding terminal (called device in the following pages) to the platform, you can configure the display parameters of the device remotely, including the brightness, boot logo, etc.

Before You Start

Make sure you have added terminal(s) to the platform, and the terminal(s) are online. Refer to ***Add Digital Signage Terminal*** for details.

Steps

1. On the left navigation pane, click **Device and Server → Digital Signage Terminal** .
2. Click ⚙ on the Operation column to enter the device remote configuration page of terminal.
3. In the **Text on Screen** area, set the text related parameters.

   Brightness Settings

   Drag the brightness bar to adjust the brightness of the screen, or manually enter the brightness value. The brightness value is 0 to100. The bigger the value, the lighter the screen.

   Boot Logo

   After enabled, the logo will be displayed when the terminal starts up. The logo is set on the terminal locally.

   Screen Direction

   0

   The screen direction is 0° by default.

   90

   The screen direction will rotate 90° clockwise.

   180

   The screen direction will rotate 180° clockwise.

   270

   The screen direction will rotate 270° clockwise.

   Enter the Password to Unlock Screen

   After the screen is locked, the password is required to unlock the screen. The password is set on the terminal locally.
4. In the **Timed Startup/Shutdown** area, set the timed related parameters.

   Timed Startup / Shutdown

   After enabled, you should select the schedule as **Daily Schedule** or **Weekly Schedule**, and then the terminal will start up or shut down according to the schedule.

   a. Drag the mouse on the time bar to draw the start up time duration (blue bar) of one day. The terminal will be shut down on the other time period.

   Note

   - Supports drawing up to 8 time periods of one day.
   - You can click the time period (blue bar), enter the start time and end time of the time period.

   b. You can click **Clear** to clear the wrong time period you draw on the time bar.

   Volume Schedule

After enabled, you should select the schedule as **Daily Schedule** or **Weekly Schedule**, and then the terminal's volume will turned on/off according to the schedule.

a. Drag the mouse on the time bar to draw the start up time duration (blue bar) of one day. The terminal will be shut down on the other time period.

Note

- Supports drawing up to 8 time periods of one day.
- You can click the time period (blue bar), enter the start time and end time of the time period.

b. You can click **Clear** to clear the wrong time period(s) you draw on the time bar.

5. **Optional:** In the **Maintenance** area, set related parameters such as **Lock USB** and **Lock WLAN**.

SADP

After enabled, the terminal(s) can be detected by the platform via SADP protocol, and be displayed on the online device list.

Note

- You can enable SADP protocol for either single or multiple terminal(s).
- This function should be supported by the device.

Restore to Factory Settings

Click **Restore** and enter the device password to restore the displaying parameters to the default parameters.

6. Click **Save** to save the configuration.

6.18.3 Configure Device Privacy Settings

You can configure the privacy parameters for the device remotely, including event storage mode, authentication result display, picture uploading and storage, and clearing pictures on device, to protect the person's private information.

1. On the top navigation bar, select → **Basic Management → Device** to enter the device management page and then click **Device and Server → Digital Signage Terminal** on the left navigation pane.
2. Select one or multiple device(s), and then click **Privacy Settings** to enter the Privacy Settings page. You can set the following parameters.

Event Storage

Select the mode of event storage.

Overwrite

The events stored on the device will be overwritten automatically. For example, if a device can store up to 200 events. When this limit is reached, the first event will be overwritten by the newest one, and then the second will be overwritten.

Delete Old Events Regularly

Set a time period. The events stored on the device during the period will be automatically deleted at intervals of the period.

Delete Old Events by Specified Time

Set a specific time. The events stored on the device before the specific time will be automatically deleted.

Authentication

Check the items (such as profile photo, name, and employee ID) to be displayed in authentication results.

Picture Uploading and Storage

Check to enable the features as needed.

Upload Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be uploaded to the system.

Save Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be saved to the devices.

Clear Pictures Stored on Device

Clear Face Pictures

Click **Clear** to clear all face pictures.

Clear Recognized or Captured Pictures

Click **Clear** to clear all recognized pictures or captured pictures.

3. Click **Save** to save the configuration.

6.18.4 Configure Device Parameters Remotely

After adding terminal (called device in the following pages) to the system, you can configure the parameters of the device remotely, including configuring built-in camera's parameters, linking external camera, configuring displaying settings and other parameters.

Configure Built-In Camera Parameters

Built-in camera is the camera built in the terminal. After adding a terminal to the platform, you should configure parameters for the built-in camera, such as device name, function, and face similarity.

Before You Start

Make sure at least one terminal is added to the platform, and make sure the terminal is online.

Steps

1. On the left navigation pane, click **Device and Server → Digital Signage Terminal** .

2. Click ⚙ on the Operation column to enter the device remote configuration page of terminal.
3. In the **Linked Device** area, click **Built-In Camera** to enter the camera parameters settings page.
4. Set the parameters.

   Device Name

   The device name of the built-in camera.

   Live View

   The live view of the camera will be displayed in the live view window of the normal programs.

   Similarity

   Set the face similarity. When the captured face picture's similarity reaches the value, it will be regarded as comparison succeeded.

   Recognition Distance

   It is used to control the recognition distance between the person and camera.

   Wearing Mask

   Select **Yes** or **No** from the drop-down list.

   Yes: The camera will recognize persons wearing masks.

   No: The camera will not recognize persons wearing masks.

   Mask Detection

   Check **Mask Detection**, then when the camera detects people without masks, the corresponding prompt will be displayed on the terminal.

   Face Detection Frame

   Check **Face Detection Frame**, then when the camera detects a face, a frame will be displayed on the terminal.

   Quick Capture

   Check **Quick Capture**, then the camera can recognize and capture a face more frequently even if the face is far away.
5. Click **Save** to save the above settings.

Link External Device to Terminal

After adding terminals to the platform, you can link external devices such as cameras to the terminals for attendance, live view, or temperature screening.

Before You Start

- Make sure the external device has been installed properly.
- Make sure at least one online terminal is added to the platform.

Steps

1. On the left navigation pane, click **Device and Server → Digital Signage Terminal** .

2. Click ⚙ in the Operation column of the online device to enter the remote configuration page of the terminal.
3. In the **Linked Device** area, click **Add** to enter the Add Device page.

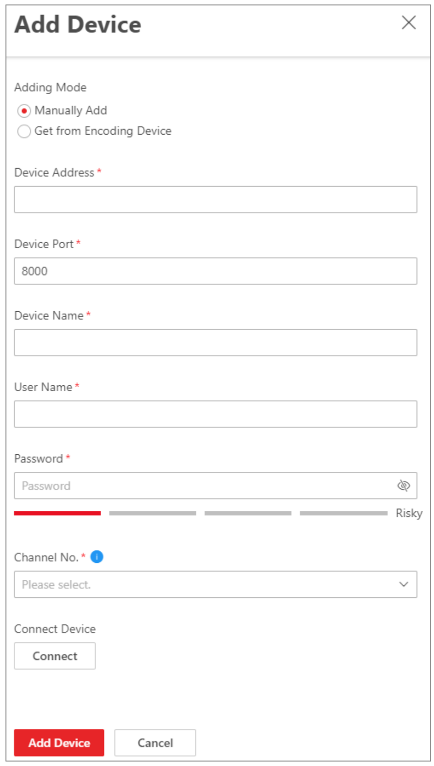


Figure 6-19 Add Device

4. Select the adding mode as **Manually Add** or **Get From Encoding Device**.
5. **Optional:** Set the following parameters when setting the adding mode as **Manually Add**.

   Device Address

   The IP address of the device.

   Device Port

   The port number of the device. By default, it is 8000.

   Device Name

   The name of the device, which can be used to describe the function, location, etc., of the device.

   User Name

   The user name of logging into the device.

   Password

   The password of the device.
6. **Optional:** Select an encoding device from the list when setting the adding mode as **Get From Encoding Device**.

7. Select the channel number of the device to be added to the terminal from the drop-down list.
8. **Optional:** Click **Connect** to connect to the device.

Note

- If you set the adding mode as **Get From Encoding Device**, the device should be online.
- After connecting to the device, you can configure the function for the selected channel. For details, refer to ***Configure Built-In Camera Parameters*** .

9. Click **Add Device**.

Configure More Parameters

On the remote configuration page of terminal, you can configure other parameters except for built-in camera and external camera, such as basic information, time settings, device operations, timed configuration and maintenance.

Note

On the upper-right corner of the configuration page, you can click **Copy To** to copy the configuration of the current device to other devices.

Basic Information

Device Address

Display the IP address of the terminal by default.

Subnet Mask

Display the subnet mask of the terminal by default.

Gateway

Display the gateway of the terminal by default.

Time Settings

Click to customize the time settings.
You can also select **Sync with Server Time** to synchronize time from the server.

Device Operation, Timed Settings and Maintenance

The display settings of the terminal, refer to ***Configure Device Display Settings*** for details.

6.19 Manage Interactive Flat Panel

On the left, select **Device and Server → Interactive Flat Panel** .

6.19.1 Add Interactive Flat Panels

You can add interactive flat panels by auto registration on device and general authentication code.

<table>
<tr><th>Adding Mode and Scenario</th><th>Description</th></tr>
<tr><td>Add Online Interactive Flat Panel: you have registered the interactive flat panel online on the Integrated Control App.</td><td>1. Click Add to enter the Add Interactive Flat Panel page.
2. In the online device list, select one or multiple devices to be added, and then click Add to Device List to enter the Add Interactive Flat Panel page.
3. Set the basic information.
Note
- If you add one device, the device serial number will be displayed automatically. You should configure the authentication code and the device name.
- If you add multiple devices, the device serial number and the device name will be displayed automatically. You should configure the authentication code.
4. (Optional) Set the time zone of the device.
5. (Optional) Switch on Add Resource to Area to import the resources of the added devices to an area.
6. Finish adding the device.
- Click Add to add the current device and back to the device list page.
- Click Add and Continue to add the current device and continue to add other devices.</td></tr>
<tr><td>Add Interactive Flat Panel by Device Serial No.: you know the dice serial No.</td><td>1. Click Add to enter the Add Interactive Flat Panel page.
2. Set the basic information.
3. (Optional) Set the time zone of the device.
4. (Optional) Switch on Add Resource to Area to import the resources of the added devices to an area.
5. Finish adding the device.
- Click Add to add the current device and back to the device list page.
- Click Add and Continue to add the current device and continue to add other devices.</td></tr>
<tr><td>Enable General Authentication Code: the device is configured authentication code.</td><td>1. Click Auto Registration → Add by Configuring General Authentication Code on Platform .
2. Switch on General Authentication Code Settings.
3. Enter the authentication code.</td></tr>
</table>

Adding Mode and Scenario	Description
	4. (Optional) Switch on **Add Resource to Area** to import the resources of the added devices to an area. 5. Click **Save**. 6. Register the interactive flat panel online: Enter the IP address of the platform, device name, registration port No. (7660 by default), and the authentication code on the Integrated Control App on the device. Then the device will be added to the platform automatically.

6.19.2 After Adding Interactive Flat Panels: Operations on Device List Page

After adding interactive flat panels to the platform, you can configure, manage and control them as needed.

Operations	Descriptions
Remote Configurations	Click in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Set Time Zone	Select one or more device(s), click **Time Zone** to set/edit the time zone of the selected device(s).
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.20 Add LED Controller

You can add LED controllers to the platform by multiple methods: adding online LED controllers, adding by IP address, adding by IP segment, and importing devices in a batch. After adding LED controllers to the platform, you can configure, manage, and control them.

On the left, select **Device and Server → LED Controller** , and select one of the following methods to add LED controllers.

User Intention and Adding Method	Steps
Add Online LED Controllers: the online devices to be added are on the same LAN as the server.	Before you start, make sure: You have downloaded and installed the Web Control. 1. In the online device list, select **Local Network** or **Server Network**. 2. Select one or multiple devices to be added, and then click **Add to Device List** to enter the Add Device page. 3. Set the basic information. 4. (Optional) Check **Get Device's Time Zone** or check **Manually Set Time Zone** to select the time zone of the device. 5. In the Add Resource to Area list, select an area to add the device to.
Add by IP Address: you know the IP address of the device to be added.	1. Click **Add** to enter the Add Device page. 2. Select **IP Address** as the adding mode. 3. Set the basic information. 4. (Optional) Check **Get Device's Time Zone** or check **Manually Set Time Zone** to select the time zone of the device. 5. In the Add Resource to Area list, select an area to add the device to.
Add by IP Segment: multiple devices to be added have the same port number, user name, password, and have different IP addresses within a range.	1. Click **Add** to enter the Add Device page. 2. Select **IP Segment** as the adding mode. 3. Set the basic information. 4. (Optional) Check **Get Device's Time Zone** or check **Manually Set Time Zone** to select the time zone of the device. 5. In the Add Resource to Area list, select an area to add the device to.
Batch Import: there are multiple devices to be added.	1. Click **Add** to enter the Add Device page. 2. Select **Batch Import** in the Adding Mode list. 3. Click **Download Template** and save the predefined template (excel file) on your PC. 4. Open the exported template file and enter the required information of the devices to be added in the corresponding column. 5. Click and select the edited file. 6. In the Add Resource to Area list, select an area to add the device to.

Finish adding the device.

- Click **Add** to add the current device and back to the device list page.
- Click **Add and Continue** to add the current device and continue to add other devices.

After adding LED controllers, you can perform the following operations.

Operation	Description
View Device Error	If the device error exist, hover the cursor over to view the error's cause, and click **Configure** to edit the device settings.
Remote Configuration	In the Operation column, click to enter the remote configuration page of device and configure more parameters.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.21 Manage BACnet Device

You can add BACnet devices to the platform via two methods: adding online devices and adding devices by device instance No. After adding BACnet devices, you can manage them including editing, searching, deleting, etc.

6.21.1 Add Online BACnet Device

You can add online BACnet devices to the platform. After adding devices, you can refresh devices, delete devices, etc.

Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting the devices to the HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. On the left navigation pane, click **Device and Server → BACnet Device** .
2. **Optional:** In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
3. Check one or more BACnet devices, and click **Add to Device List** to enter the Add BACnet Device page.
4. **Optional:** Edit the device instance number and device name which are shown automatically.

Note

Skip this step if you have selected more than one device previously.

5. **Optional:** Click ⌄ to select a time zone from the drop-down list.

Note

You can click **View** to view the details of the current time zone.

6. **Optional:** Switch on **Add Resource to Area** to add the resources of the device to an area.

Note

You can click **Create Area by Device Name** to create a new area by the device name, or click **Existing Area** to select an existing area from the list.

7. Click **Add**.

6.21.2 Add BACnet Device by Device Instance No.

You can add BACnet devices to the platform by entering device instance No. and other parameters. After adding devices, you can refresh devices, delete devices, etc.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting the devices to the HikCentral Professional via network.

Steps

1. On the left navigation pane, click **Device and Server → BACnet Device** .
2. Click **Add** to enter the Add BACnet Device page.
3. Enter device instance No., and device name.
4. **Optional:** Click ⌄ to select a time zone from the drop-down list.

Note

You can click **View** to view the details of the current time zone.

5. Switch on **Add Resource to Area** to add the resources of the device to an area.

Note

You can click **Create Area by Device Name** to create a new area by the device name, or click **Existing Area** to select an existing area from the list.

6. Click **Add** to finish adding the device, or click **Add and Continue** to continue adding another device.

6.22 Add Modbus Device

You can add Modbus devices to the platform by the device IP address.

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. Such initial configuration is required for connecting the devices to the HikCentral Professional via network.

Steps

1. On the left navigation pane, click **Device and Server → Modbus Device** .
2. Click **Add** to enter the Add Modbus Device page.
3. Set the required basic information such as device address, device port number, and device name.
4. Set the device time zone.
5. **Optional:** Switch on **Add Resource to Area** to import the resources of the added Modbus device to an area.
   - Select **Create Area by Device Name** to create an area named after the Modbus device for adding the resource(s) to the created area.
   - Select **Existing Area**, and select an existing area to add the resource(s) to.

   Note

   - If you select **Existing Area**, you can also click **Add** to add a new area.
   - If you do not import resources to area, you cannot perform the further configurations for the resources.
6. Click **Add** to finish adding the device, or click **Add and Continue** to continue adding another device.

6.23 Manage Smart Wall

Smart wall can provide security personnel with a rich visual overview of the areas you want to keep an eye on. After you configure a virtual smart wall, you can add smart wall devices like video wall controllers and link device's decoding outputs with windows of the smart wall to show videos on LED or LCD displays.

On the top navigation bar, select → **Basic Management → Device → Device and Server → Smart Wall** .

6.23.1 Add Smart Wall Device

A smart wall device refers to the decoder, video wall controller, or multi-functional video center. A video wall controller is a device that manages the content displayed on a video wall, which is a large display made up of multiple screens tiled together to form a single display area.

1. In the **Smart Wall Device** section, select **Add** to enter the Add Decoding Device page.
2. Set the adding mode.

Adding Mode	Scenario
Online Device	Devices are within the network where the Web Client or SYS server is located. **Note** - For Google Chrome, install the SADP service according to the instructions. For Firefox, install the SADP service and import the certificate according to the instructions. - Server Network: The detected online devices in the same local subnet with the SYS server will be listed. Local Network: The detected online devices in the same local subnet with the Web Client will be listed.
IP Address	Add devices one by one when you know the IP address.
IP Segment	Add multiple decoding devices with the same port number, user name and password, but different IP addresses within a range.
Port Segment	Add multiple decoding devices with the same IP address, user name and password, but different port numbers within a range.

3. Select **Add**.

6.23.2 Add Smart Wall

Steps

1. In the **Smart Wall** section, click **Add**.
2. Set the following parameters: **Smart Wall Name**, **Smart Wall Type**, **Max. Resolution of Single Output**, and **Row × Column**.
3. Click **Add**.

4. **Optional:** Select **Stream Type Settings** to set the default stream type for channels on the smart wall.

Note

To ensure the stream type setting takes effect, go to the video wall controller's web configuration page, select **Sub-Stream Auto-Switch**, and disable automatic switching to the sub-stream when the smart wall window number exceeds the threshold.

6.23.3 Link Decoding Output with Window

After you add the smart wall device and virtual smart wall, link the smart wall device's decoding outputs with the windows of the smart wall to display videos.

Steps

1. Click > in front of a decoding device to show its decoding outputs.
2. Click > in front of a smart wall to show its windows.
3. Drag the decoding output to the window of the smart wall.

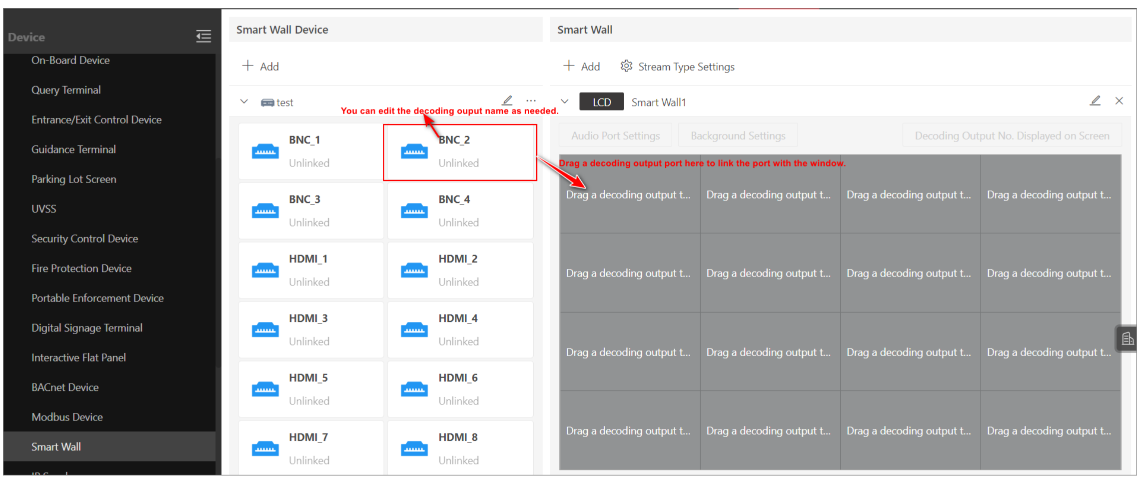


Figure 6-20 Link Decoding Device with Window

4. **Optional:** Set the resolution, audio port and background.

Note

To play the audio of the video wall on the Control Client, set the audio port first.

6.23.4 Configure Cascade

If the widow division number of the smart wall exceeds the decoding capability of a video wall controller, or the cross-decoder functions such as roaming and spanning are required, you can cascade decoders with the video wall controller by linking the decoder's output with the video wall controller's input to expand its decoding capability.

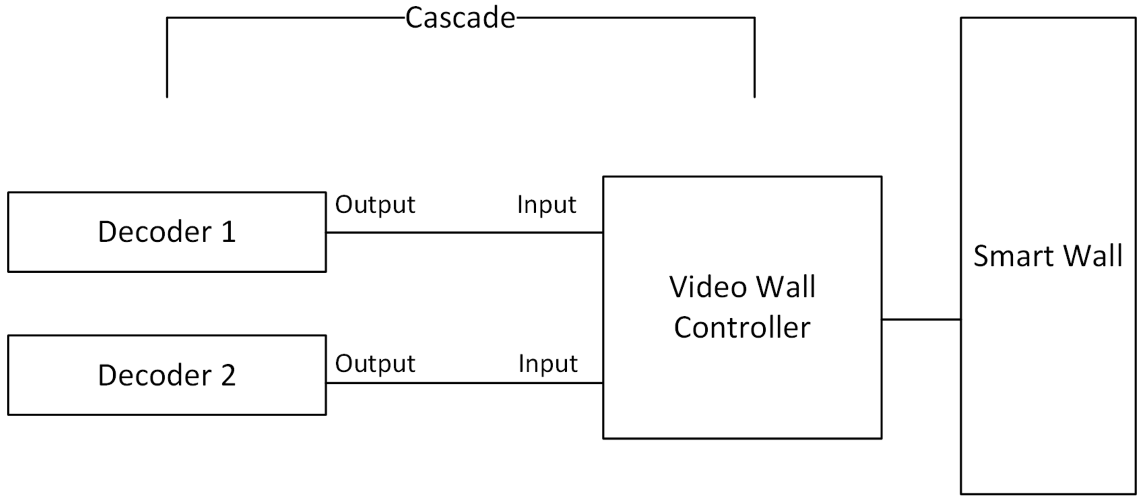


Figure 6-21 Cascade

Steps

1. Click to enter the cascade configuration page.

Note

Only video wall controller DS-C10S, DS-C10S-T, and DS-C30S support this function.

2. Select a decoder's output to set it as the signal input of the video wall controller.

Note

If a decoder is cascaded with a video wall controller, the spare decoding outputs of the decoder cannot be used to display on smart wall.

3. Select **Save**.

6.23.5 Display Alarms on Smart Wall

To view the linked alarms on the Control Client, you should configure the alarm linkage on the platform.

Before You Start

You have added smart wall devices and the virtual smart wall on the platform.

Steps

1. Select → **Event and Alarm** → **Event and Alarm Configuration** → **Normal Event and Alarm** .
2. Select **Add**, set the triggering event and source.
3. In the Alarm Settings section, enable **Trigger Alarm** to set the alarm priority and recipients.

4. Enable **Display on Smart Wall** to set the smart wall type, display resource, stream type, smart wall name, alarm display window, and other parameters as needed.

6.24 Manage IP Speakers

On the left, select **Device and Server → IP Speaker** .

6.24.1 Add IP Speaker

You can add the IP speakers to the platform via multiple methods such as adding by IP address and IP segment.

Adding Mode and Scenario	Description
Add Detected Online IP Speakers: IP speakers are on the same network where the Web Client or the SYS server is located.	1. In the Online Device area, select a network type and protocol type to filter the detected online devices. 2. Select one or more active devices to be added. 3. Click **Add to Device List** to open the Add Online Device window. 4. Set the required information. 5. (Optional) Switch on **Add Resource to Area** to import the resources of the device to the area.
Add IP Speaker by Serial No.: you know the serial No. of an IP speaker.	1. Click **Add** to enter the Add IP Speaker page. 2. Select **Hikvision Private Speaker Protocol** as the access protocol. 3. Select **Serial No.** as the Adding Mode. 4. Enter the required information. 5. (Optional) Switch on **Add Resource to Area** to import the resources of the device to the area.
Batch Add IP Speakers: there are multiple IP speakers to be added.	1. Click **Add** to enter the Add IP Speaker page. 2. Select the access protocol. 3. Select **Batch Import** as the adding mode. 4. Click **Download Template** and save the predefined template to your PC. 5. Open the template file and enter the required information of the devices in the corresponding column. 6. Click and select the edited file.
Add IP Speaker by Device ID: IP speakers supporting ISUP.	1. Click **Add** to enter the Add IP Speaker page. 2. Select **Hikvision ISUP Protocol** as the access protocol. 3. Select **Device ID** as the Adding Mode.

Adding Mode and Scenario	Description
	4. Configure the parameters, including device ID, ISUP login password (optional) and device name. 5. (Optional) Switch on **Add Resource to Area** to import the resources of the device to the area.
Add IP Speakers by ID Segment: add multiple IP speakers which have no fixed IP addresses and support ISUP.	1. Click **Add** to enter the Add IP Speaker page. 2. Select **Hikvision ISUP Protocol** as the access protocol. 3. Select **Device ID Segment** as the Adding Mode. 4. Enter the start and end device ID. 5. Enter the ISUP login password. 6. (Optional) Switch on **Add Resource to Area** to import the resources of the device to the area.

Finish adding the device.

- Click **Add** to add the current device and back to the device list page.
- Click **Add and Continue** to add the current device and continue to add other devices.

6.24.2 After Adding IP Speakers: Operations on Device List Page

You can manage the added IP speakers, including editing and deleting devices, configuring devices remotely, changing devices' passwords, etc.

Operation	Description
Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Operation	Description
Search Device	Enter a key word in the search box in the upper-right corner, and click (or press the Enter key) to search for the target device(s).
View Error Message	If there is an icon appearing beside the device name, hover the mouse cursor to the icon and view the error message. You can click **Edit/Refresh** to edit/refresh the device if needed.
Format SD Card	Click to format the SD card of the IP speaker.

6.25 Manage Security Inspection Devices

You can add security inspection devices to the platform for management, including editing and deleting devices, remote control, etc. The platform supports multiple ways for adding security inspection devices.

6.25.1 Add a Detected Online Security Inspection Device

You can only add a single detected online security inspection device to the platform at a time.

Before You Start

- Make sure the security inspection devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Device and Server → Security Inspection Device** .
3. In the Online Device area, select a network type.

   Server Network

      As the default selection, the detected online devices in the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

      The detected online devices in the same local subnet with the current Web Client will be listed in the Online Device area.
4. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.

Note

To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** and switch on **Allow ISUP Registration**.

5. In the Online Device area, select an active device and click **Add to Device List** to open the Add Security Inspection Device window.
6. Select a device type from the drop-down list.
7. Enter the required information.

Caution

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

8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
9. **Optional:** Switch on **Add Resource to Area** to import the resources of the added security inspection device to an area.

Note

- You can select all resources or the specified camera(s) to be added.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further configurations for the resources.

10. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream.

    Note

    You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying live view on the smart wall.
11. **Optional:** If you choose to add resources to area, switch on **Video Storage** and select a storage location for recording.

Note

Configure the Hybrid Storage Area Network, Cloud Storage Server, or pStor in advance, or the storage location cannot be displayed in the drop-down list.

Encoding Device

The video files will be stored in the encoding device according to the configured recording schedule.

Hybrid Storage Area Network

The video files will be stored in the Hybrid Storage Area Network according to the configured recording schedule.

Cluster Storage

The video files will be stored in the cluster storage server according to the configured recording schedule.

pStor

According to the configured recording schedule, the video files will be stored in the pStor, which is the storage access service for managing local HDDs and logical disks.

pStor Cluster Service

pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.

12. **Optional:** Set the recording schedule for the added resources.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device.
    - Uncheck **Get Device's Recording Settings** and set the required information, including recording schedule template, stream type, etc.
13. Click **Add**.
14. **Optional:** Perform the following operations for the added device(s).

Remote Configurations	Click to set the remote configurations of the device. **Note** For details about the remote configurations, refer to the user manual of the device.
Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.25.2 Add Security Inspection Device by Device ID

For the security inspection devices supporting ISUP, you can add them by specifying the predefined device ID, ISUP login password, etc. This is an economic choice when you need to manage a security inspection device in the public network without a fixed IP address.

Before You Start

- Make sure the security inspection devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Device and Server → Security Inspection Device** .
3. Click **Add** to enter the Add Security Inspection Device page.
4. Select **Security Inspection System**, **Analyzer** or **Walk-Through Metal Detector** as the device type from the drop-down list.
5. Select **Hikvision ISUP Protocol** as the access protocol.

   Note

   To allow device registration via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** and switch on **Allow ISUP Registration**.
6. Enter the required information, including device ID, ISUP login password, and device name.

   Caution

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

   Local Storage

   The pictures will be stored in the local storage space of the platform server.

   Hybrid Storage Area Network

   The pictures will be stored in the Hybrid Storage Area Network.

   Cluster Storage

   The pictures will be stored in the cluster storage server.

pStor

The pictures will be stored in the pStor, which is the storage access service for managing local HDDs and logical disks.

Network Video Recorder

The pictures will be stored in the network video recorder.

8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.

9. **Optional:** Switch on **Add Resource to Area** to import the resources of the added security inspection device to an area.

   Note

   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to the area, you cannot perform further configurations for the resources.

10. **Optional:** If you choose to add resources to an area, select a streaming server to get the video stream.

    Note

    You can check **Wall Display via Streaming Server** to get the stream via the selected Streaming Server when displaying live view on the smart wall.

11. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device.
12. Finish adding the device.
    - Click **Add** to save the settings and go back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add another device.
13. **Optional:** Perform the following operations for the added devices.

Remote Configurations	Click to set the remote configurations of the device. **Note** For details about the remote configurations, refer to the user manual of the device.
Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

6.25.3 Add Security Inspection Device by IP Address

If you know the IP address or domain name of a security inspection device, you can add it to the platform by specifying the IP address (or domain name), user name, password, etc.

Before You Start

- Make sure the security inspection devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to HikCentral Professional via network.
- The devices to be added should be activated.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Device and Server → Security Inspection Device** .
3. Click **Add** to enter the Add Security Inspection Device page.
4. Select **Security Inspection System**, **Analyzer** or **Walk-Through Metal Detector** as the device type from the drop-down list.
5. Select **Hikvision Private Protocol** as the access protocol.
6. Enter the required information, including the device address, device name, user name, and password.

Caution

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

7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources of the added security inspection device to an area.

Note

- You can select all resources or the specified camera(s) to be added.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to the area, you cannot perform further configurations for the resources.

9. **Optional:** If you choose to add resources to an area, select a Streaming Server to get the video stream.

Note

You can check **Wall Display via Streaming Server** to get the stream via the selected Streaming Server when displaying live view on the smart wall.

10. **Optional:** If you choose to add resources to an area, switch on **Video Storage** and select a storage location for recording.

Note

Configure the Hybrid Storage Area Network, Cloud Storage Server, or pStor in advance, or its storage location cannot be displayed in the drop-down list.

Security Inspection Device

The video files will be stored in the security inspection device according to the configured recording schedule.

Hybrid Storage Area Network

The video files will be stored in the Hybrid Storage Area Network according to the configured recording schedule.

Cluster Storage

The video files will be stored in the Cluster Storage Server according to the configured recording schedule.

pStor

According to the configured recording schedule, the video files will be stored in the pStor, which is the storage access service for managing local HDDs and logical disks.

pStor Cluster Service

pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.

11. **Optional:** Set the recording schedule for the added resources.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type, etc.
12. Finish adding the device.
    - Click **Add** to save the settings and go back to the device list page.

- Click **Add and Continue** to save the settings and continue to add another device.

13. **Optional:** Perform the following operations for the added devices.

Remote Configurations	Click ⚙ to set the remote configurations of the device. **Note** For details about the remote configurations, refer to the user manual of the device.
Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click 🔍 (or press the Enter key) to search for the target device(s).

6.26 Manage Network Transmission Devices

Network transmission devices (switch, network bridge, and fiber converter) can be added to the system for management, to help the system monitor the network status of the managed devices.

After the network transmission devices are added to the system, the platform will automatically draw a network topology according to the location of the added devices, and display the information (IP address, port No., port status, and stream rate) and network link status (fluent, busy, congested, disconnected).

On the left, select **Device and Server → Network Transmission Device** .

6.26.1 Add Network Transmission Device

Adding Mode and Scenario	Description
Add Detected Online Network Transmission Devices: IP speakers are on the same network where the Web Client or the SYS server is located.	1. In the Online Device area, select a network type. 2. Select one or more active devices to be added. 3. Click **Add to Device List** to open the Add Online Device window. 4. Set the required information. 5. (Optional) Switch on **Add Resource to Area** to import the resources of the device to the area. 6. Click **Add**.
Add Network Transmission Device by IP Address: you know	1. Click **Add** to enter the Add Network Transmission Device page. 2. Select an access protocol from the drop-down list. 3. Select **IP Address** as the adding mode.

Adding Mode and Scenario	Description
the IP address of a device.	4. Enter the required information. 5. Click **Add** or **Add and Continue** to finish adding.
Import Network Transmission Devices in a Batch: there are a large number of devices to be added.	1. Click **Add** to enter the Add Network Transmission Device window. 2. Select an access protocol from the drop-down list. 3. Select the adding mode as **Batch Import**. 4. Click **Download Template** to download the template to the local PC. 5. Open the downloaded template file, and enter the required device information. 6. Click to select the edited template file. 7. Click **Add** or **Add and Continue** to finish adding.

Note

Country Code: It defines the country/region where device will be used, which is required for wireless bridges.

6.26.2 After Adding Network Transmission Devices: Operations on Device List Page

Operation	Description
Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Search Device	Enter a key word in the search box in the upper-right corner, and click (or press the Enter key) to search for the target device(s).
Set the System Connected Device	Select the device, click **System Connected Switch** to set the switch as the system connected device.

Operation	Description
	Note System connected switch is the switch that is directly connected with the SYS server.

6.27 Manage Recording Server

You can add the Recording Server to the system for storing the videos and pictures. The supported recording servers include Hybrid Storage Area Network, Cloud Storage Server, pStor, and NVR (Network Video Recorder). You can also form an N+1 hot spare system with several Hybrid Storage Area Networks to increase the video storage reliability of system.

Note

NVRs can only be used to store pictures.

On the left, select **Device and Server → Recording Server** .

6.27.1 Add Recording Server

Click **Add** to enter the Add Recording Server page.

Note

Before you start, make sure the servers you are going to use are correctly installed and connected to the network as specified by the manufacturers.

Adding Mode and Scenario	Description
Add pStor	1. Select **pStor**. 2. Enter the network parameters. **ANR Function**: You can check this field to enable the ANR function. This function is enabled default. If the network is disconnected between the pStor and the encoding device, data can be stored on the pStor automatically. 3. (Optional) Switch on **Enable Picture Storage** and specify the port No. for picture downloading.

Adding Mode and Scenario	Description
	4. (Optional) If you need to access the server via WAN, switch on **Enable WAN Access** and set the corresponding parameters which are available when you access the server via WAN. 5. (Optional) In Storage Information field, switch on **Custom Video Copy-Back** and set the start time for copy-back.
Add Hybrid Storage Area Network	1. Select **Hybrid Storage Area Network**. 2. Enter the network parameters. 3. (Optional) Enable picture storage function for storing pictures in this Hybrid SAN, and switch on **Enable Stream Object Storage**. **Note** To obtain the access secret key and secret key, contact our technical support team. 4. (Optional) If you need to access the server via WAN, switch on **Enable WAN Access** and set the corresponding parameters which are available when you access the server via WAN. 5. (Optional) In Storage Information field, switch on **Custom Video Copy-Back** and set the start time for copy-back.
Add Network Video Recorder	1. Select **Network Video Recorder** as the server type. 2. Set the required information. 3. (Optional) If you need to access the server via WAN, set the **Enable WAN Access** switch to ON and set the corresponding parameters which are available when you access the server via WAN.
Add Cluster Storage Server	1. Import the service component certificate to the Cluster Storage Server first before adding it to the system. See ***Import Service Component Certificate to Cloud Storage Server*** for details. 2. Select **Cluster Storage**. 3. Enter the network parameters. 4. (Optional) Switch on **Enable Picture Storage** for storing pictures in this Cluster Storage Server. 5. (Optional) If you need to access the server via WAN, switch on **Enable WAN Access** and set the corresponding parameters which are available when you access the server via WAN.
Add pStor Cluster Service	1. Select **pStor Cluster Service**. 2. Enter the required network parameters.

Adding Mode and Scenario	Description
	3. Enter the user's access key and secret key of the pStor cluster service. 4. (Optional) If you need to access the server via WAN, switch on **Enable WAN Access** and set the corresponding parameters which are available when you access the server via WAN.

Click **Add** to add the server and back to the server list page, or click **Add and Continue** to save the settings and continue to add other servers.

6.27.2 After Adding Recording Servers: Operations on Device List Page

Operation	Description
Remote Configurations	Click to configure the server remotely. **Note** For details about remote configuration, see the user manual of the device.
Search Device	Enter a key word in the search box in the upper-right corner, and click (or press the Enter key) to search for the target device(s).
Edit Hybrid SAN Server	Click the name field of the server to edit the basic information, and storage information including video expiration and storage usage: • You can switch on **Video Expiration**, select a configuration mode (configure by server / storage pool), and set the corresponding video expiration day(s). **Note** ◦ The oldest videos will be deleted automatically after the specified expiration day(s). ◦ If the added storage server supports configuring video expiration by camera, the current video expiration configuration is invalid; after **Video Expiration** is enabled, the previous configuration will be invalid and the expired data will be cleared according to the current one. • You can view the used space and free space for each storage pool.

Operation	Description
One-Touch Configuration	If the Hybrid SAN has not been configured with storage settings, click in the Operation column to perform one-touch configuration before you can store the video files of the camera on the Hybrid SAN.
N+1 Configuration	Click in the top left corner to enter to N+1 configuration page. See details in ***Set N+1 Hot Spare for Hybrid SAN*** .

6.27.3 Import Service Component Certificate to Cluster Storage Server

For data security purpose, the Cluster Storage Server's certificate should be same with the SYS server's. Before adding the Cluster Storage Server to the platform, you should import the certificate stored in the SYS server to the Cluster Storage Server.

Before You Start

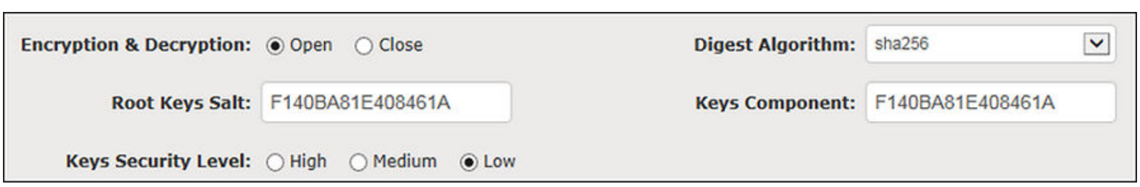
Make sure the Cluster Storage Server you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

Note

If the service component certificate is updated, you should export the new certificate and import it to the Cluster Storage Server again to update.

1. In the top left corner of Home page, select → **Basic Management** → **System** .
2. Click **Security** → **Service Component Certificate** on the left side.
3. Click **Export** to export the certificate stored in the SYS server.
4. Log in the configuration page of the Cluster Storage Server via web browser.
5. Click **System** → **Configuration** → **Cluster Configuration** .
6. Input the root keys salt and keys component according to the parameters in the certificate you export in Step 3.



7. Click **Set**.

What to do next

After importing the certificate to the Cluster Storage Server, you can add the server to the platform for management.

6.27.4 Set N+1 Hot Spare for Hybrid SAN

You can form an N+1 hot spare system with several Recording Servers. The system consists of several host servers and a spare server. When the host server fails, the spare server switches into operation, and thus increasing the video storage reliability of HikCentral Professional.

Before You Start

- Make sure the Hybrid Storage Area Networks you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- At least two online Hybrid Storage Area Networks should be added to form an N+1 hot spare system.

Steps

Note

- The N+1 hot spare function is only supported by Hybrid Storage Area Networks and NVRs.
- The spare server cannot be selected for storing videos until it switches to host server.
- The host server cannot be set as a spare server and the spare server cannot be set as a host server.

1. Select **Device and Server → Recording Server → N + 1 Hot Spare** to enter the N+1 Configuration page.

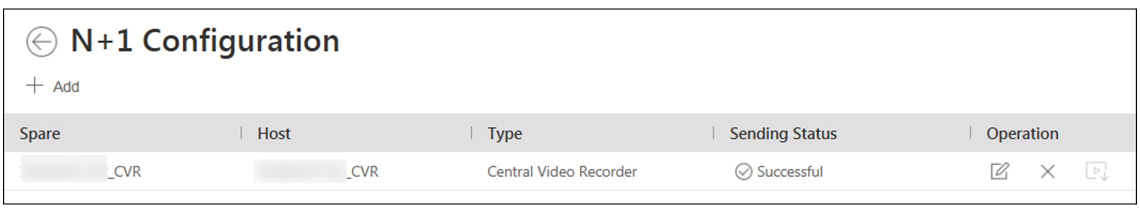


Figure 6-22 N+1 Configuration Page

2. Click **Add** to set the N+1 hot spare.
3. Select a Hybrid Storage Area Network in the Spare drop-down list to set it as the spare server.
4. Select the Hybrid Storage Area Network(s) in the Host field as the host server(s).
5. Click **Add**.

   Note

   The recording schedules configured on the Hybrid Storage Area Network will be deleted after setting it as the spare Recording Server.

6. **Optional:** After setting the hot spare, you can do one or more of the following.

Edit	Click on the Operation column, and you can edit the spare and host settings.
Delete	Click × on the Operation column to cancel the N+1 hot spare settings.

Note

Canceling the N+1 hot spare will cancel all the host-spare associations and clear the recording schedule on the spare server.

Send Recording Schedule	Click on the Operation column to send the recording schedule on the host server to the spare one again if the host server failed to send the recording schedule to spare server.

6.28 Manage Streaming Server

You can add the Streaming Server to the HikCentral Professional to get the video data stream from the Streaming Server, thus to lower the load of the device.

Note

For system which supports Remote Site Management, the cameras imported from Remote Site adopt the Streaming Server configured on the Remote Site by default. You are not required to add the Streaming Server to Central System and configure again.

6.28.1 Input Certificate Information to Streaming Server

For data security purpose, the Streaming Server's certificate should be the same with the SYS server's. Before adding the Streaming Server to the platform, you should enter the certificate information stored in the SYS server to the Streaming Server.

Steps

Note

If the service component certificate is updated, you should enter the new certificate information to the Streaming Server again to update.

1. Log into the Web Client on the SYS server locally.

   You will enter the Home page of the Web Client.
2. In the top left corner of Home page, select → **Basic Management → System** .
3. Click **Security → Service Component Certificate** on the left.
4. Click **Generate Again** to generate the security certificate for Streaming Server verification.

   Note

   You need to enter the account password for verification to generate the security certificate.
5. On the computer which has been installed with Streaming Service, open the Service Manager.
6. Click **Security Certificate**.

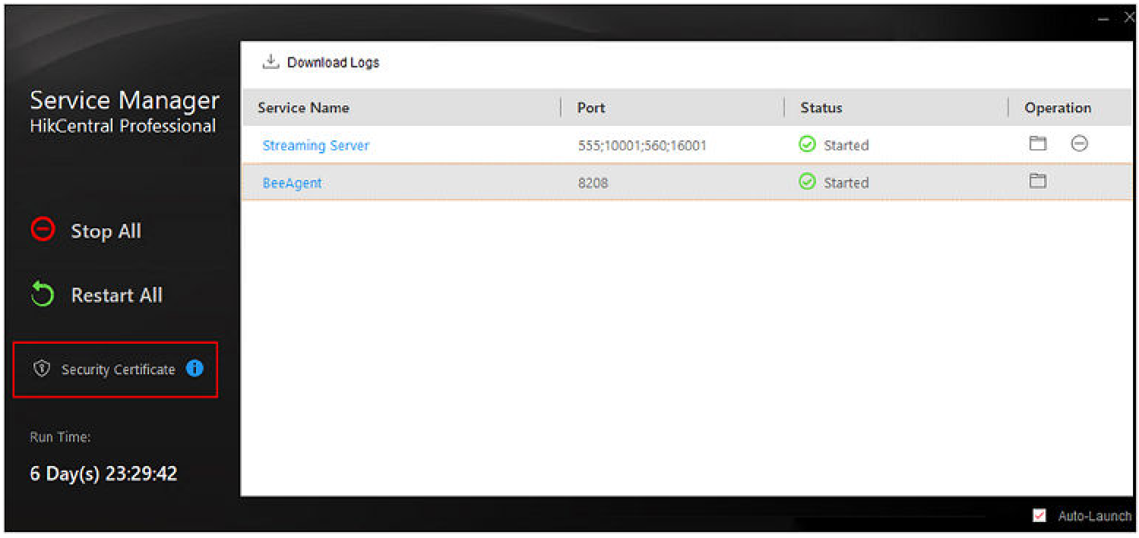


Figure 6-23 Enter Security Certificate

7. Enter the certificate information you generate in step 4.

6.28.2 Add Streaming Server

You can add a Streaming Server to the system to forward the video stream.

Steps

1. On the device module, click **Device and Server → Streaming Server** on the left panel.
2. Click **Add** to enter the Add Streaming Server page.
3. Enter the required information.

Network Location

Select **LAN IP Address** if the Streaming Server and the SYS server are in the same LAN. Otherwise, select **WAN IP Address**.

Address

The IP address of streaming server to be added.

Real Time Streaming Port

It is used for Streaming Service to get stream. If it is not changed, use the default value.

Network Port

It is used for getting the status of Streaming Service. If it is not changed, use the default value.

Web Client Streaming Port

It is used for getting stream for Google Chrome or Firefox. If it is not changed, use the default value.

Management Port (SSL)

It is used for security certificate authentication. If it is not changed, use the default value.

Web Client Streaming Port (SSL)

It is used for Web Client streaming. If it is not changed, use the default value.

RTMP Streaming Port

It is used for OpenAPI streaming. If it is not changed, use the default value.

HLS Streaming Port

It is used for OpenAPI streaming. If it is not changed, use the default value.

4. **Optional:** If you need to access the server via WAN, switch on **Enable WAN Access** and set the corresponding parameters which are available when you access the server via WAN.

Note

- The **Enable WAN Access** switch is available only when you set Network Location as **LAN IP Address**.
- Go to **System → Network → WAN Access** to set the default port No. of streaming media ports.

5. You can switch on **Hot Spare** and set the hot spare type to Host or Spare.
6. Finish adding the Streaming Server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the server and continue to add other servers.

   The servers will be displayed on the server list. You can check the related information of the added servers on the list.
7. **Optional:** Perform the following operations after adding the streaming server.

Edit a Server	Click **Name** field of the server and you can edit the basic information of the server, view its related resources information.
Delete Server(s)	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Search Server(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target server(s).

6.29 Add Intelligent Analysis Server

When you know the related parameters such as IP address and port No. of the intelligent analysis server, you can add it to the platform for intelligent functions, such as abnormal event detection and intrusion detection.

Before You Start

Make sure the intelligent analysis server you are going to use is correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required for connecting the devices to the HikCentral Professional via network.

Steps

1. Click **Device and Server → Intelligent Analysis Server** on the left.

2. Click **Add** to enter the Add Intelligent Analysis Server page.
3. Set the required basic information such as device address, device port number, and WAN access.

   Address

   IP address of the intelligent analysis server.

   Port No.

   Port No. of the intelligent analysis server. If it is not changed, use the default value.

   Enable WAN Access

   Enable the intelligent analysis server to access WAN (Wide Area Network).

   Note

   After enabling the WAN Access, you need to set the WAN IP address and port number of the server for WAN access.
4. Enter the name, user name, and password of the intelligent analysis server.

   Caution

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

   Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
5. Finish adding the intelligent analysis server.
   - Click **Add** to finish adding the server.
   - Click **Add and Continue** to add the current server and continue to add more.
6. **Optional:** Perform the following operations after adding the server.

Edit Server	Click **Name** field of the server, and you can edit the information of the server.
Delete Server	Select the server(s) from the list, and click **Delete** to delete the selected server(s).
Configure Server	Click , and the login interface of the server displays. You can log in and configure the server.
Search for Server(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search for the target server(s).

6.30 General Device Operations

There are some general operations for devices, including creating password for inactive device(s), editing online device's network information, upgrading device firmware, and resetting/restoring device password.

6.30.1 Create Password for Inactive Device(s)

The devices with simple default password may be accessed by the unauthorized user easily. For the security purpose, the default password is not provided for some devices. You are required to create the password to activate them before adding them to the platform. Besides activating the device one by one, you can also batch activate multiple devices which have the same password simultaneously.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- This function should be supported by the device. Make sure the devices you want to activate support this function.

Steps

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, view the device status and select one or multiple inactive devices.
3. Click **Activate** to open the device activation window.
4. Create a password in the password field, and confirm the password.

Caution

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

5. Click **Save** to create the password for the device.

Note

If you have not set security questions, the window of setting security questions will pop up, and you should select the method of resetting password and set the security questions as needed.

An **Operation completed.** message is displayed when the password is set successfully.

6. Click in the Operation column to change the device's IP address, subnet mask, gateway, and so on if needed.

Note

For details, refer to ***Edit Online Device's Network Information*** .

6.30.2 Edit Online Device's Network Information

The online devices, which have IP addresses in the same local subnet with SYS or Web Client, can be detected by HikCentral Professional. For the detected online devices, you can edit their network information as desired via HikCentral Professional remotely and conveniently. For example, you can change the device IP address due to the changes of the network.

Before You Start

For some devices, you should activate it before editing its network information. Refer to ***Create Password for Inactive Device(s)*** for details.

Perform this task when you need to edit the network information for the detected online devices.

Steps

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the SYS will be listed.

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
3. View the device status, and click in the Operation column of an active device.
4. Edit the device parameters, such as IP address, device port, subnet mask, and gateway.

Note

The parameters may vary for different device types.

5. Click .
6. Enter the device's password.
7. Click **Save**.

6.30.3 Upgrade Device Firmware

You can upgrade the devices with the firmware to be upgraded according to device type and upgrade mode.

Select **Firmware Upgrade** on the left navigation pane.

Select Device for Upgrade

You should first select the target device type for upgrade.

The following table shows devices types and their firmware upgrading methods accordingly.

<table>
<tr><th>Via Current Web Client</th><th>Via Hik-Connect</th></tr>
<tr><td>• Camera
• NVR (Network Video Recorder)
• DVR (Digital Video Recorder)
• Decoding Device
• Access Control Device
• Card Reader
• Security Control Panel (including AX Security Control Panel)
• Security Radar
• Indoor Station
• Door Station
Note
Upgrading the card reader linked to the door station is not supported.
• Main Station
• Guidance Terminal
Note
You can also upgrade the cameras access to the NVR in a batch.</td><td>• Camera
• NVR (Network Video Recorder)
• DVR (Digital Video Recorder)
• Indoor Station
• Door Station
Note
Upgrading the card reader linked to the door station is not supported.
• Main Station
• Digital Signage Terminal
Note
You can also upgrade the cameras linked to the NVR in a batch.</td></tr>
</table>

Select Upgrade Mode and Schedule

The upgrade mode is provided by the platform after you select the device, including via the current Web Client, via Hik-Connect (which is a cloud service), and via FTP.

Upgrade Method	Steps
Upgrade Device Firmware via Current Web Client	1. Select **Via Current Web Client**. 2. In the **Upgrade By** field, select the upgrade method. 3. In the **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

Upgrade Method	Steps
	4. Select an upgrade package from the local PC. 5. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.
Upgrade Device Firmware via Oik-ConnectHik-Connect	1. Select **Via Hik-Connect**. 2. In the **Device Access Protocol** field, select the relevant protocol. 3. In the **Upgrade By** field, select the upgrade method. **Note** This field is not required if Hik-Partner Pro Protocol is selected as the device access protocol. 4. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade. 5. Install the required web plug-in. **Note** If you select Local PC as the upgrade method, you should install the required web plug-in if the prompt pops up. 6. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.
Upgrade Device Firmware via FTP	1. Select **Upgrade Firmware via FTP**. 2. Set the basic information. **FTP Server Address** The address of FTP server, where you have uploaded the firmware upgrade package. **Port No.** The port number of FTP server. **User Name** The user name of FTP server. **Password** The password of the FTP server. **Caution** The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters,

Upgrade Method	Steps
	including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user. **Path** If you save FTP firmware upgrade package in a non-root directory, enter the root directory name. If you saved FTP firmware upgrade package in a root directory, keep the field empty. 3. Select an upgrade package from the local PC. 4. Select **Upgrade Now** or **Custom** as the upgrading schedule and click **OK**.

Note

In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.
To view the devices with firmware upgraded, upgrading, to be upgraded, and not upgraded, you can click in the Upgrade Status column. In the upgrade task list, you can click in the Operation column to delete the upgrade task.

6.30.4 Restore/Reset Device Password

If you forgot the password of the detected online devices, you can restore the device's default password or reset the device's password through the system. Then you can access the device or add it to the system using the password.

For detailed operations of restoring device's default password, refer to ***Restore Device's Default Password*** .

For detailed operations of resetting device's password, refer to ***Reset Device Password*** .

Reset Device Password

If you forget the password you use to access the online device, you can request for a key file from your technical support and reset the device's password through the platform.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Perform this task when you need to reset the device's password. Here we take creating password for the encoding device as an example.

Steps

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, view the device status (shown on Security column) and click icon in the Operation column of an active device.

   The Reset Password window pops up.

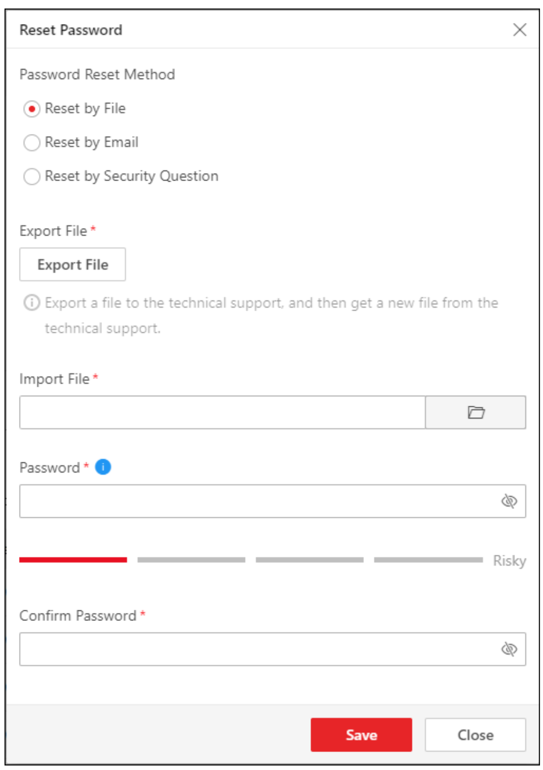


Figure 6-24 Reset Password

3. Select a password reset method:

Reset by File	Click **Export File** to save the device file on your PC. Send the file to the technical support. **Note** For the following operations about resetting the password, contact the technical support.
Reset by Email	Export the QR code and sent it to the email displayed. You will receive the verification code in 5 minutes. Enter the code, new password, and confirm password.
Reset by Security Question	Enter the answer to the security question, new password, and confirm password. **Note** If you have not set security questions, the window of setting security questions will pop up, and you should set the security questions as needed.

Caution

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

4. Click **Save** to save the change.

Restore Device's Default Password

For some devices with old firmware version, if you forgot the password you use to access the online device, you can restore the device's default password through the platform and then you must change the default password to a stronger one for better security.

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. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operations about activating devices.

Perform this task when you need to restore the device's default password. Here we take restoring the default password for an encoding device as an example.

Steps

1. On the top, select **Device**.
2. Click **Device and Server → Encoding Device** on the left.
3. In the Online Device area, view the device status (shown on Security column) and click ↺ in the Operation column of an active device.

   A dialog with security code pops up.
4. Enter the security code and restore the default password of the selected device.

   Note

   Contact our technical support to obtain a security code.

What to do next

You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

Chapter 7 Area Management

HikCentral Professional provides areas to manage the added resources in different groups. You can group the resources into different areas according to the resources' locations. For example, in a house, there mounted 64 cameras, 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one area (named My House) for convenient management. You can do some other operations of the devices after managing the resources by areas.

Note

If the current system is a Central System with a Remote Site Management module, you can also manage the areas on a Remote Site and add cameras on Remote Site into areas.

In the top left corner of Home page, select → **Basic Management** → **Device** , and click **Area** on the left.

7.1 Add Area

You should add an area before managing the elements by areas.

After adding the area, you can perform the following operations on the area list.

Operation	Description
Edit Area	Hover the cursor on a specific area and click ··· → **Edit** to edit the area.
Delete Area	Select an area and click or hover the cursor on an area and click ··· → **Delete** to delete the selected area. You can also press **Ctrl** on your keyboard, select multiple areas, and then click to delete areas in a batch. **Note** After deleting the area, the resources in the area will be removed from the area, as well as the corresponding recording settings, event settings, and map settings.
Search Area	Enter a keyword in the search field of the area list panel to search for the area.
Move Area	Drag the added area to another parent area as the sub area.
Stick on Top	Hover the cursor on a specific area and click ··· → **Stick on Top** → to stick the area to the top.

Operation	Description
	Note The order of the parent area will not be changed.
Cancel Stick Area On Top	Hover the cursor on a specific area and click ⋯ → **Cancel Stick Area On Top** to restore the area order to the default (name order).
Customize Additional Information	In the area list panel on the left, click ⚙ to enter the Customize Additional Information page. Click **Add**, set the name and type, and click **Add** to customize the additional area information.

7.1.1 Add an Area for Current Site

You can add an area for the current site to manage the devices.

Steps

1. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.

2. **Optional:** Select the parent area in the area list panel to add a sub area.

   Note

   - For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
   - The icon indicates that the site is the current site.

3. Click + on the area list panel to open the Add Area panel.

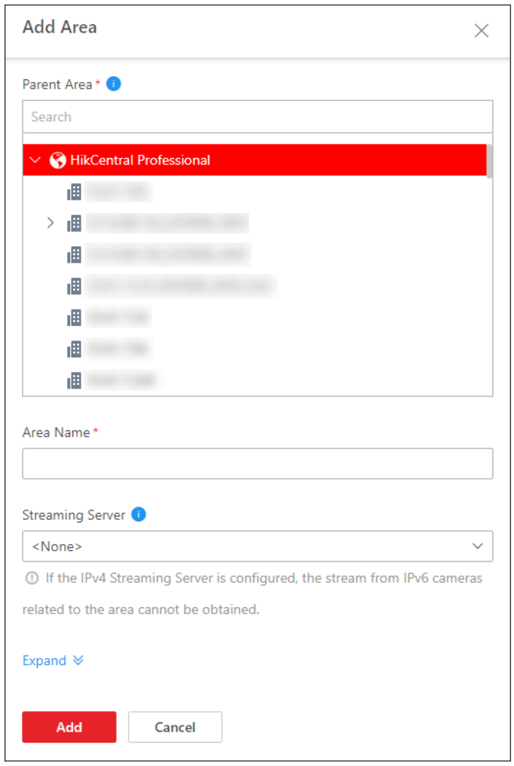


Figure 7-1 Add Area for Current Site

4. Select the parent area to add a sub area.
5. Create a name for the area.
6. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.

   All cameras belonging to this area via the server are listed in the Related Cameras area. If the camera is online, you can click its name to view its basic information, recording settings, and picture storage settings.
7. **Optional:** If you select a Streaming Server for the area, check **Wall Display via Streaming Server** to display the area's resources on the smart wall via this Streaming Server.
8. **Optional:** Click **Expand** to expand and set the additional area information as needed.
9. Click **Add**.

7.1.2 Add Area for Remote Site

You can add an area for the remote site to manage the devices in the Central System.

Steps

1. Click **Area** on the left.
2. In the left panel, select an added remote site from the drop-down site list to show its areas.

Note

The icon indicates that the site is a remote site.

3. Click + on the area list panel to open the Add Area panel.

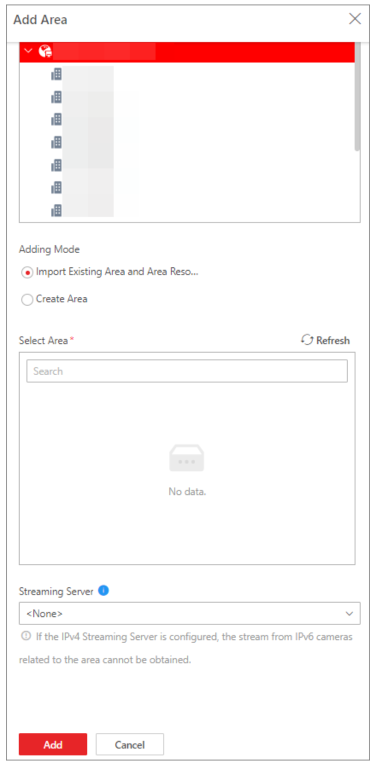


Figure 7-2 Add Area for Remote Site

4. Select a parent area to add a sub-area.
5. Set the adding mode for adding the area.

Import Existing Area and Area Resources

Add the existing area and the available area resources to the parent area.

Add

Add a new area to the parent area.

6. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.
7. **Optional:** After selecting a Streaming Server for the area, check off **Wall Display via Streaming Server** if you want to display the area's resources on the smart wall via this Streaming Server.
8. Click **Add**.

7.2 Add Element to Area

You can add elements to areas for management, including cameras, doors, elevators, vehicles, security radars, alarm inputs, alarm outputs, digital signage terminals, and interactive flat panels, etc.

7.2.1 Add Camera to Area for Current Site

You can add cameras to areas for the current site to get the live view, play the video files, and so on.

Before You Start

The cameras need to be added to HikCentral Professional for area management. Refer to ***Manage Encoding Device*** for details.

Steps

Note

One camera can only belong to one area. You cannot add a camera to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding cameras to.
5. Select the **Camera** tab.
6. Click + on the element page to enter the Add Camera page.
7. Select the device type.
8. Select the camera(s) to be added.
9. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
10. **Optional:** Check **Get Device's Recording Settings** to obtain the recording schedule configured on the local device and the device can start recording according to the schedule.

    Note

    If the recording schedule configured on the device is not continuous recording, it will be changed to event recording on the local device.
11. Click **Add**.

The added camera(s) will be displayed in the list.

12. **Optional:** After adding the camera(s), you can do one or more of the followings:

Configure Camera	Click in the Operation column to configure the camera.
Export Information of All Cameras	Click to export the information of all cameras added to the area to an Excel file.
Synchronize Camera Name	Select the cameras and click to get the cameras' names from the devices in a batch. **Note** You can only synchronize the camera name of the online HIKVISION device.
Apply Camera Name	Select the cameras and click to apply the cameras' names to the devices in a batch.
Get Recording Schedule	Select the cameras and click to get the recording schedules from the devices in a batch.
Set Camera ID	Click to enter the Camera ID page, edit the default identifier number in the **ID** column of each camera, and click **Save**. **Note** The camera ID is unique and is used to display a certain camera's live view on the smart wall via the network keyboard.
Get PTZ Configuration	Select the cameras and click to get the details of PTZ configurations from the devices in a batch.
Move Camera(s) to Another Area	Select the cameras, click , select a target area, and click **Move** to move the selected cameras to the target area.
Set Geographic Location	Click to enter the Map Settings page and drag the camera to the map. For details, refer to ***Add Hot Spot on Map*** .
Display Cameras of Sub Areas	Check **Include Sub-Area** to display the cameras of sub areas.
Filter Cameras by Device Type	Select the device type(s) to be displayed in the list from the drop-down list to the left of the search box.
Mark Camera	Select the cameras, click and check **Two-Way Audio Supported** to mark the cameras which support two-way audio.

7.2.2 Add Camera to Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can also add cameras from the Remote Site to areas in the Central System for management.

Steps

Note

Cameras can only belong to one area. You cannot add a camera to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added Remote Site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is a Remote Site.
4. **Optional:** Select an area for adding cameras to in the area list panel.
5. Select the **Camera** tab.
6. Click + on the element page to enter the Add Camera page.

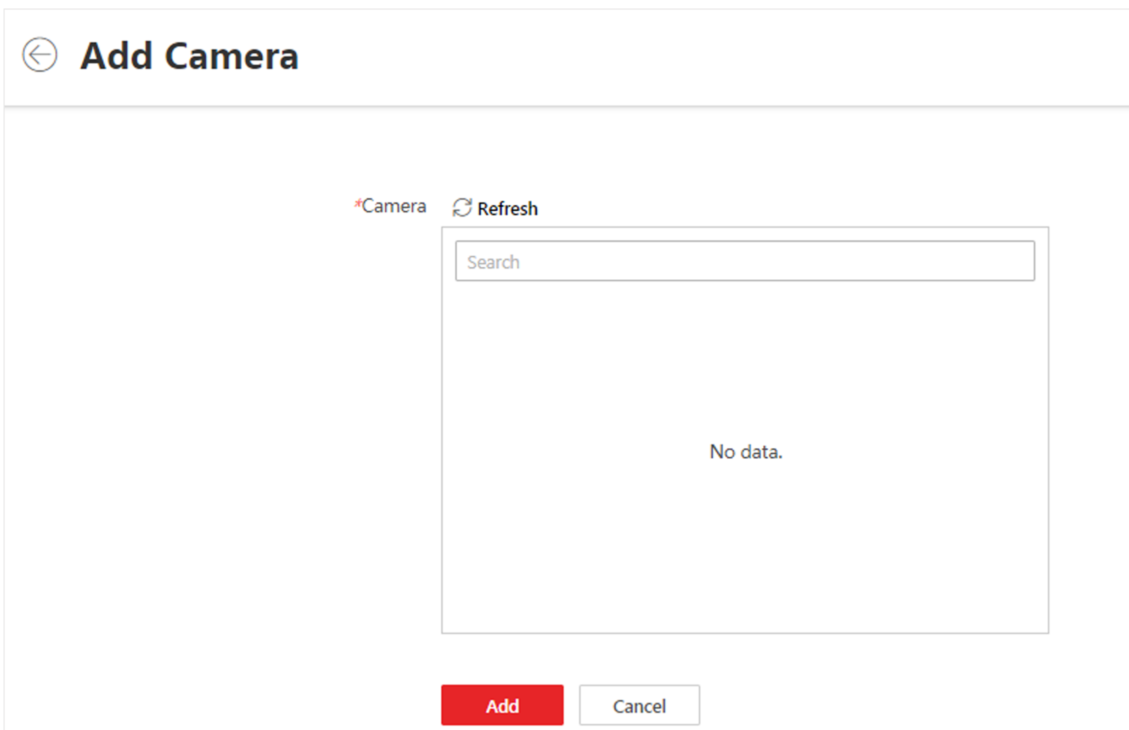


Figure 7-3 Add Camera to Area for Remote Site

7. Select the camera(s) to be added.

Note

Up to 64 cameras can be added to one area.

8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.

   The added camera(s) will be displayed in the list.

10. **Optional:** After adding the camera(s), you can do one or more of the followings:

Export Information of All Cameras	Click to export the information of all cameras added to the area to an Excel file.
Synchronize Camera Name	Select the cameras and click to get the cameras' names from the devices in a batch.
Set Camera ID	Click to enter the Camera ID page, edit the default identifier number in the **ID** column of each camera, and click **Save**. **Note** The camera ID is unique and used to display a certain camera's live view on the smart wall via the network keyboard.
Get PTZ Configuration	Select the cameras and click to get the details of PTZ configurations from the devices in a batch.
Move Camera(s) to Another Area	Select the cameras, click , select a target area, and click **Move** to move the selected cameras to the target area.
Display Cameras of Sub Areas	Check **Include Sub-Area** to display the cameras of sub areas.
Filter Cameras by Device Type	Select the device type(s) to be displayed in the list from the drop-down list to the left of the search box.
Mark Camera	Select the cameras, click and check **Two-Way Audio Supported** to mark the cameras which support two-way audio.

7.2.3 Add Door to Area for Current Site

You can add doors to areas for the current site for management.

Before You Start

The access control devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Access Control Device*** for details.

Steps

Note

One door can only belong to one area. You cannot add one door to multiple areas.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding doors to the area list panel.
5. Select the **Door** tab.
6. Click + on the element page to enter the Add Door page.
7. Select the device type.
8. Select the door(s) to be added.
9. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
10. Click **Add**.

    The added door(s) will be displayed in the list.
11. **Optional:** After adding the doors, you can do one or more of the following.

Synchronize Door Name	Select the doors and click to synchronize the doors' names from the device in a batch. **Note** You can only synchronize the door name of online HIKVISION device.
Apply Door Name	Select the doors and click to apply the doors' names to the device in a batch.
Move to Other Area	Select the doors and click . Then select the target area to move the selected doors to and click **Move**.
Set Geographic Location	Click to enter Map Settings page and drag the door to the map. See ***Add Hot Spot on Map*** for details.
Display Doors of Sub Areas	Check **Include Sub-area** to display the doors in sub areas.
Filter by Device Type	Click and check the device type in the drop-down list to filter the doors.

Search for Doors	Enter the keywords in the Search field to search for doors.

7.2.4 Add Door to Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can add doors from the Remote Site to areas in the Central System for management.

Before You Start

Access control devices need to be added to HikCentral Professional for area management.

Steps

1. In the top-left corner of the Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the left panel, select the added Remote Site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is a Remote Site.
4. **Optional:** Select an area for adding doors to in the area list panel.
5. Select the **Door** tab.
6. Click **Add** on the element page to enter the Add Door page.
7. Select the door(s) to be added.
8. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
9. Click **Add**.

   The added door(s) will be displayed in the list.
10. **Optional:** After adding the door(s), you can do one or more of the followings:

Synchronize Door Name	Select the doors and click **Synchronize Door Name** to get the doors' names from the devices in a batch.
Filter Doors by Device Type	On the top right of the door list page, select **Access Control Device** or **Video Intercom Device** from the drop-down list, or search for a door via the search box.

7.2.5 Add Elevator to Area for Current Site

You should add elevator to areas for further management.

Before You Start

The elevator control devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Elevator Control Device*** for details.

Steps

Note

One elevator can only belong to one area. You cannot add an elevator to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding elevators to in the area list panel.
5. Select the **Elevator** tab.
6. Click + to enter the Add Elevator page.
7. In the **Elevator Control Device** field, all the added elevator control devices are displayed. Select the device to add the elevator to.
8. In the **Range of Floor No.** field, enter the start No. and end No. of the floors that you want to import to the area.

   The floors between the start No. and end No. will be imported to the area. After imported, you can manage the floors in the system, such as adding to access levels, controlling status, etc.
9. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
10. Click **Add**.
11. **Optional:** After adding the elevator, you can do one or more of the followings.

Get Floor Name	Select the elevator and click to get the floors' names of the elevator from the device in a batch.
Apply Floor Name	Select the elevator and click to apply the elevator's floors names to the device in a batch.
Move to Other Area	Select the elevators and click . Then select the target area to move the selected elevators to and click **Move**.
Set Geographic Location	Click to enter the Map Settings page and drag the elevator to the map.
Display Elevators of Sub Areas	Check **Include Sub-Area** to display the elevators of sub areas.
Search for Elevators	Enter the keywords in the Search field to search for elevators.

7.2.6 Add Elevator to Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can add elevators from the Remote Site to areas in the Central System for management.

Before You Start

Elevator control devices need to be added to HikCentral Professional for area management.

Steps

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added Remote Site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is a Remote Site.
4. **Optional:** Select an area for adding elevators to in the area list panel.
5. Select the **Elevator** tab.
6. Click **Add** on the element page to enter the Add Elevator page.
7. Select the elevator(s) to be added.
8. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
9. Click **Add**.

   The added elevator(s) will be displayed in the list.
10. **Optional:** After adding the elevator(s), you can do one or more of the followings:

Synchronize Elevator Name	Select the elevators and click **Get Elevator Name** to get the elevators' names from the devices in a batch.
Filter Elevators by Device Type	Enter key words in the search box to filter elevators.

7.2.7 Add Vehicle to Area for Current Site

You can add vehicles to areas for the current site for management. Only vehicles linked with on-board devices can be added to areas and one vehicle can only be added to one area.

Steps

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area for adding vehicles to in the area list panel.
5. Select the **Vehicle** tab.
6. Click **Add** on the element page to enter the Add Vehicle page.

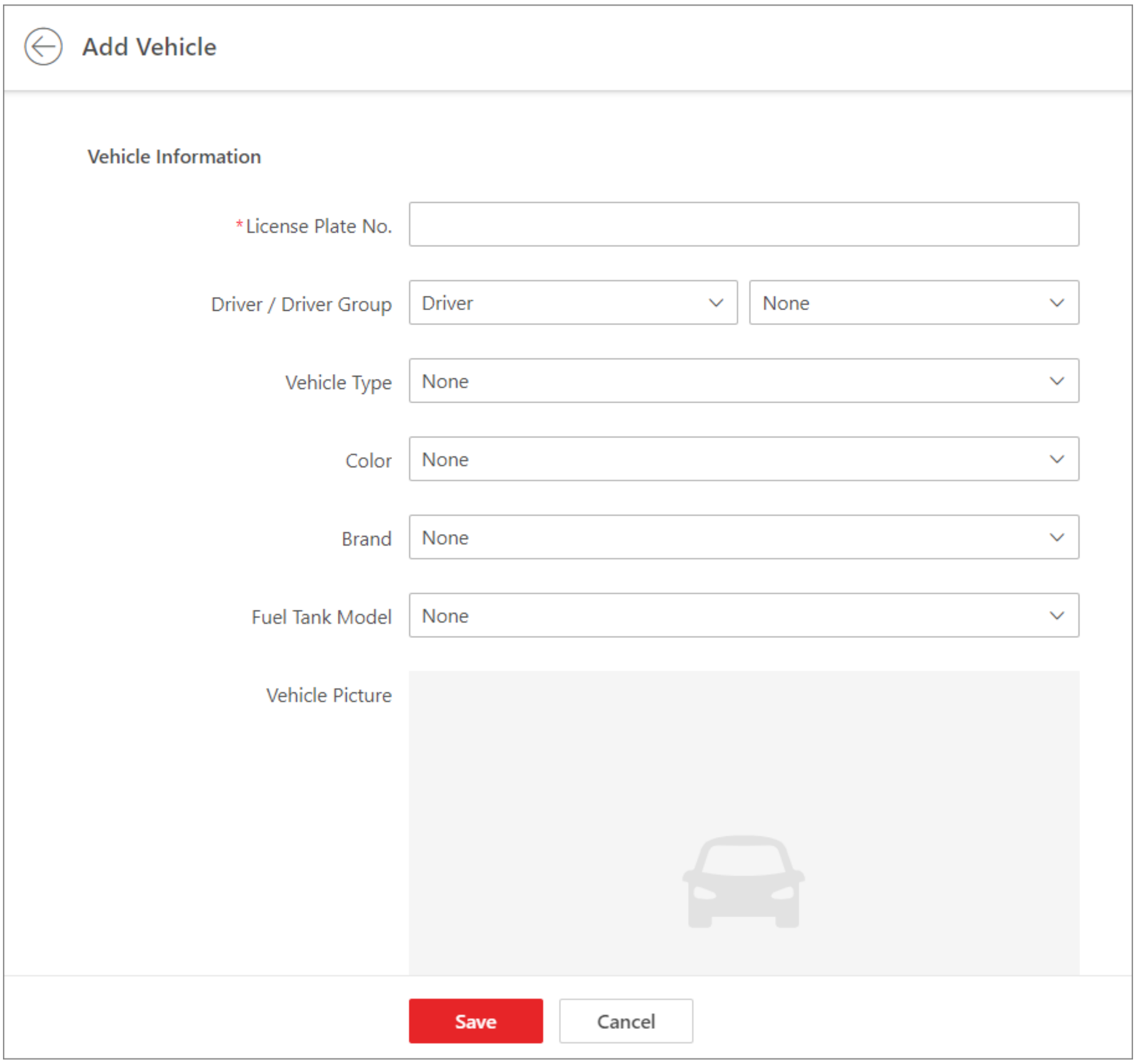


Figure 7-4 Add Vehicle to Area

7. Set the vehicle information, including the license plate No., driver / driver group, vehicle type, color, brand, fuel tank model, and vehicle picture.
8. Select the on-board device linked with the vehicle from the Linkage Device drop-down list.
9. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

10. Click **Save**.

    The added vehicle will be displayed in the list.
11. **Optional:** After adding the vehicle(s), you can do one or more of the followings:

Delete Vehicle	Select the vehicle(s) and click **Delete**.
Set Speed Threshold	Select the vehicle(s), click **Speed Threshold Settings**, and drag the slider or enter an integer in the text field.
Configure Shutdown Delay	Select the vehicle(s), click **Configure Shutdown Delay**, and enable the delay time and enter a time range.
Move to Other Area	Select the vehicle(s) and click **Move to Other Area**. Then select the target area and click **Move**.
Display Vehicles of Sub Areas	Check **Include Sub-Area** to display the vehicles in sub areas.
Remotely Configure Linked Device	Click in the Operation column of a vehicle to go to the remote configuration page of the on-board device. **Note** This function is supported when the transfer protocol between the Web Client and the SYS server is HTTPS.
Search for Vehicles	Enter the keyword(s) in the Search field to search for vehicles.

7.2.8 Add Security Radar to Area for Current Site

You can add security radars to different areas of the current site according to their locations, so that you will be informed when an alarm/event is triggered if you have configured an alarm/event.

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Device and Server Management*** for details.

Steps

Note

You cannot add a security radar to multiple areas.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site in the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area for adding security radars to.
5. Select the **Security Radar** tab.
6. Click + .
7. Select a security radar in the **Security Radar** field.
8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.

   The added security radar will be displayed in the list.
10. **Optional:** After adding the security radars, you can do one or more of the followings:

Arm/Disarm Security Radar	Select the security radar(s) and click / to arm/disarm the selected security radar(s). **Note** An event will be triggered if any person or object enters an armed security radar's detection area.
Move to Other Area	Select the security radars and click . Then select the target area to move the selected security radars to and click **Move**.
Add Security Radar to Map	Click to enter the Map Settings page and drag the security radar to the map. See ***Add Hot Spot on Map*** for details.
Display Security Radars of Sub Areas	Check **Include Sub-Area** to display the security radars of sub areas.
Search for Security Radars	Enter the keywords in the Search field to search for security radars.

7.2.9 Add Alarm Input to Area for Current Site

You can add alarm inputs to areas for the current site for management.

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Device and Server Management*** for details.

Steps

Note

One alarm input can only belong to one area. You cannot add an alarm input to multiple areas.

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding alarm inputs to.
5. Select the **Alarm Input** tab.
6. Click to enter the Add Alarm Input page.
7. Select the device type.
8. Select the alarm inputs to add.

   Note

   For the security control device, you need to select its zones as alarm inputs to add to the area.
9. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
10. Click **Add**.
11. **Optional:** After adding the alarm inputs, you can do one or more of the followings.

    Note

    For partitions (areas) of SIA zones, some operations may be unavailable.

Delete Alarm Input	Select the alarm input(s) and click **Delete**.
Move to Other Area	Select the alarm input(s) and click . Then select the target area to move the selected alarm inputs to and click **Move**.
Add Alarm Input to Map	Click to enter the Map Settings page and drag the alarm input to the map. See ***Add Hot Spot on Map*** for details.
Display Alarm Inputs of Sub Areas	Check **Include Sub-Area** to display the alarm inputs of sub areas.

Filter Alarm Inputs by Device Type	Select the device type(s) to be displayed in the list from the drop-down list to the left of the search box.
View Alarm Input Status	In the **Status** column, the alarm input's online status, arming status, bypass status, alarm status, fault status, and detector connection status are displayed. • **Online Status**: indicates alarm input online; indicates alarm input offline. • **Arming Status**: indicates alarm input armed; indicates alarm input disarmed. • **Bypass Status**: indicates alarm input bypassed; indicates bypass restored. • **Fault Status**: indicates alarm input exception. • **Alarm Status**: indicates that the alarm input is alarming. • **Detector Connection Status**: indicates alarm input not enrolled or offline; indicates detector online. • **Battery Status**: indicates normal alarm input's battery status; indicates abnormal alarm input's battery status.
Bypass/Restore Bypass Alarm Input	When an exception of alarm input occurs, and other alarm inputs can work normally, click to bypass the abnormal alarm input, otherwise, you cannot arm the security control partition which the alarm input belongs to. When a bypassed alarm input works normally, click to restore bypass.
Search for Alarm Inputs	Enter the keywords in the Search field to search for alarm inputs.
Batch Arm/ Disarm	Select multiple alarm inputs and click **Arm/Disarm**.

7.2.10 Add Alarm Output to Area for Current Site

You can add alarm outputs to areas for the current site for management. When the alarm or event linked with the alarm output is detected, alarm devices (e.g., the siren, alarm lamp, etc.) connected with the alarm output will make actions. For example, when receiving the alarm out signal from the system, the alarm lamp will flash.

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Device and Server Management*** for details.

Steps

Note

One alarm output can only belong to one area. You cannot add an alarm output to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding alarm outputs to.
5. Select the **Alarm Output** tab.
6. Click + to enter the Add Alarm Output page.
7. Select the device type.
8. Select the alarm outputs to add.
9. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
10. Click **Add**.
11. **Optional:** After adding the alarm outputs, you can do one or more of the followings.

Delete Alarm Output	Select the alarm output(s) and click **Delete**.
Move to Other Area	Select the alarm outputs and click . Then select the target area to move the selected alarm outputs to and click **Move**.
Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page and drag the alarm output to the map. See ***Add Hot Spot on Map*** for details.
Display Alarm Outputs of Sub Areas	Check **Include Sub-Area** to display the alarm outputs of sub areas.
Search for Alarm Outputs	Enter the keywords in the Search field to search for alarm outputs.
Batch Set Alarm Output Duration	Select multiple alarm outputs, click **Alarm Output Duration**, and set the duration (sec).
Batch Turn On/Off Alarm Outputs	Select multiple alarm outputs and click **Open**/**OFF**.

7.2.11 Add Commercial Display Resource to Area for Current Site

You can add commercial display resources (such as digital signage terminals, interactive flat panels, and LED controllers) to areas for the current site for management.

Before You Start

The commercial display resources need to be added to HikCentral Professional for area management. Refer to ***Manage Digital Signage Terminals*** and ***Manage Interactive Flat Panel*** for details.

Steps

Note

One commercial display resource can only belong to one area. You cannot add one commercial display resource to multiple areas.

1. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
2. **Optional:** Select an area for adding commercial display resources to.
3. Click the **Commercial Display Resource** tab.
4. Click **Add** to enter the add commercial display resource page.
5. Select the device type as **Digital Signage Terminal** / **Interactive Flat Panel** / **LED Controller**.
6. Select the commercial display resources to add them.
7. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
8. Click **Add**.
9. **Optional:** After adding the commercial display resources, you can do one or more of the followings:

Delete Commercial Display Resource	Select the commercial display resources in the list and click **Delete**.
Move to Other Area	Select the commercial display resources and click **Move to Other Area**. Then select the target area to move the selected devices to and click **Move**.
Display Device of Sub Areas	Check **Include Sub-Area** to display the device of sub areas.
Search for Commercial Display Resource	Enter the keywords in the Search field to search for commercial display resources.

7.2.12 Add Speaker Unit to Area for Current Site

You can add speaker units to areas for the current site for management.

Before You Start

The speaker units need to be added to HikCentral Professional for area management. Refer to ***Group Speaker Units*** for details.

Steps

1. Click **Area** on the left.
2. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
3. **Optional:** Select an area for adding speaker units to.
4. Select the **Speaker Unit** tab.
5. Click **Add** on the element page to enter the Add Speaker Unit page.
6. Select the device type.
7. Select the speaker unit(s) to be added.
8. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
9. Click **Add**.

   The added speaker unit(s) will be displayed in the list.
10. **Optional:** After adding speaker unit(s), you can do one or more of the followings:

Move to Other Area	Select the speaker unit(s) and click **Move to Other Area**. Then select the target area to move the selected speaker unit(s) to and click **Move**.
Adjust Volume	Select speaker unit(s) and click **Volume** to adjust the alarm volume and/or volume.
Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page. You can search for the speaker unit(s) to be added to the map and drag the speaker unit to the map. For details, refer to ***Add Hot Spot on Map*** .
Display Speaker Unit of Sub Areas	Check **Include Sub-Area** to display the speaker units in sub areas.
Search Speaker Units	Enter the name of speaker unit(s) and click to search for the speaker unit(s).

Delete Speaker Unit	Select the speaker unit(s) and click **Delete** to delete the speaker unit(s).

7.2.13 Add Fire Detector to Area for Current Site

You can add fire detectors to areas for the current site for management.

Before You Start

The fire protection devices need to be added to HikCentral Professional for area management. Refer to ***Manage Fire Protection Device*** for details.

Steps

1. Click **Area** on the left.
2. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
3. **Optional:** Select an area for adding fire detectors to.
4. Select the **Fire Detector** tab.
5. Click **Add** on the element page to enter the Add Fire Detector page.
6. Select the fire detector(s) to be added.
7. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
8. Click **Add**.

   The added fire detector(s) will be displayed in the list.
9. **Optional:** Perform the following operations.

Remote Configurations	Click in the operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Move to Other Area	Select the fire detector(s) and click **Move to Other Area**. Then select the target area to move the selected fire detector(s) to and click **Move**.
Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page. You can search for the fire detector(s) to be added to the map and drag the fire detectors to the map. For details, refer to ***Add Hot Spot on Map*** .

Display Fire Detector of Sub Areas	Check **Include Sub-Area** to display the fire detectors in sub areas.
Search Fire Detectors	Enter the name of fire detector(s) and click 🔍 to search for the fire detector(s).
Delete Fire Detector	Select the fire detector(s) and click **Delete** to delete the fire detector(s).

7.2.14 Add Modbus Resource to Area for Current Site

You can add Modbus resources to areas for the current site for management.

Before You Start

The Modbus devices need to be added to HikCentral Professional for area management.

Steps

1. In the top-left corner of the Home page, select ▦ → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon 🌐 indicates that the site is the current site.

4. Select an area for adding Modbus resources to.
5. Select the **Modbus Resource** tab.
6. Click **Add** on the element page to enter the Add Modbus Resource page.
7. Select an added Modbus device.
8. Add the resource of selected device.
   - Select the adding mode to **Manually Add** and set the required information to add one resource.
   - Select the adding mode to **Batch Import** to batch add resources.

7.2.15 Add Optimus Resource for Current Site

You can add Optimus resources to areas for the current site for management.

Steps

1. In the top-left corner of the Home page, select ▦ → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon 🌐 indicates that the site is the current site.

4. **Optional:** Select an area for adding Optimus resources to in the area list panel.

5. Select the **Optimus Resource** tab.
6. Click **Add** on the element page to enter the Add Optimus Resource page.

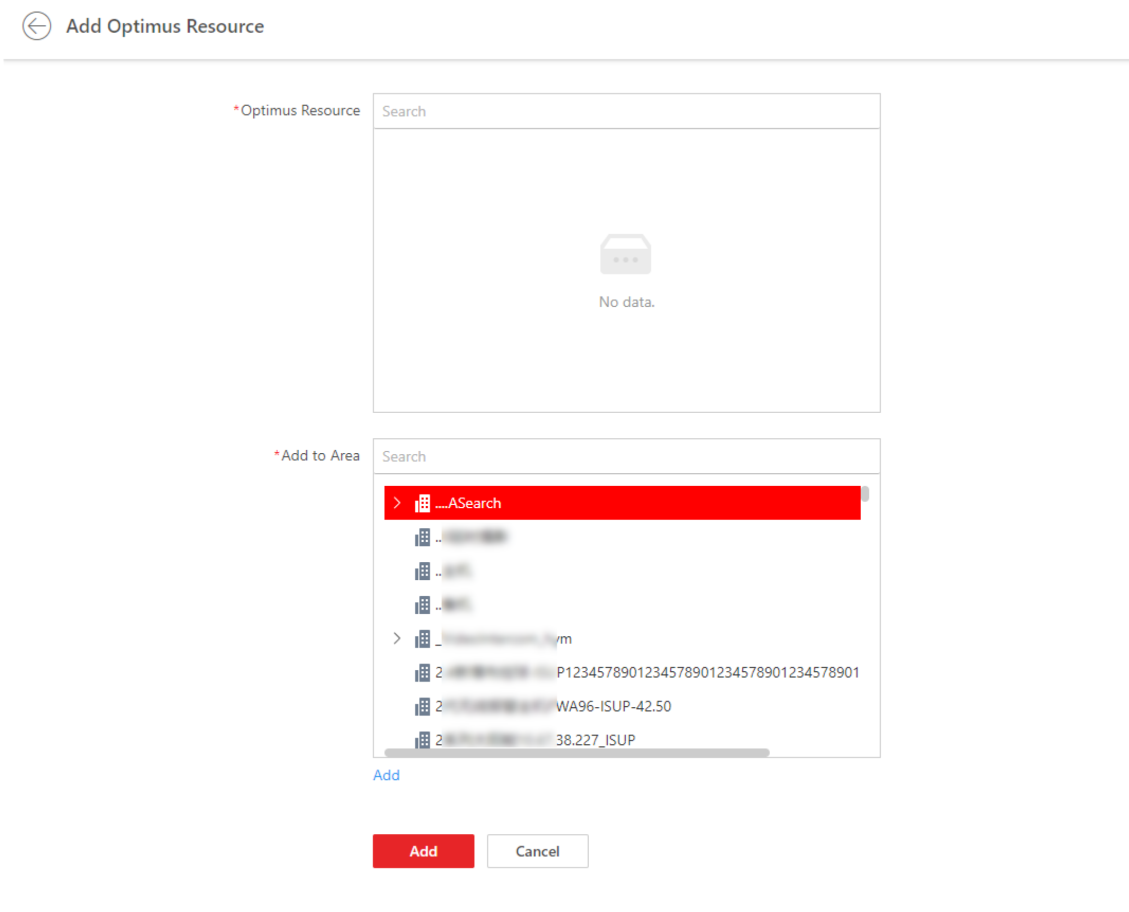


Figure 7-5 Add Optimus Resource to Area

7. Select the resource to be added.
8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.

   The added vehicle will be displayed in the list.
10. **Optional:** After adding the Optimus resource(s), you can do one or more of the followings:

Delete Optimus Resource	Select the Optimus resource(s) and click **Delete**.

Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page. You can search for the Optimus resource(s) to be added to the map and drag them to the map.
Search for Optimus Resource	Enter keyword(s) in the Search field to search for Optimus resource(s).

7.3 Edit Element in Area

You can edit the area's added elements, such as recording settings, event settings, and map settings for cameras, application settings, hardware settings, and so on.

In the top left corner of Home page, select → **Basic Management** → **Device** → **Area** . Then select the current site from the drop-down site list to show its areas, and select an area below.

Note

The icon indicates that the site is the current site.

7.3.1 Edit Camera for Current Site

You can edit the basic information, recording settings, and picture storage settings of a camera for the current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is current site.
4. **Optional:** Select an area.
5. Select the **Camera** tab to show the added cameras.
6. Click a camera's name in the **Name** column to enter the camera editing page.
7. Edit the camera's basic information, including camera name and protocol type.

   Note

   If you change the camera's name, you can click in the added cameras list page to apply the new name to the device.
8. **Optional:** Click **Live View** to view the live view of the camera and click again to switch to playback.

Note

- If the device supports PTRZ, you can long press / to rotate by clockwise/anticlockwise during live view.
- You can click to set rotating speed, and click to refresh the live view.

9. Edit the recording settings of the camera.

Note

- If no recording settings have been configured for the camera, you can click **Configure** to set the parameters.
- You can also select multiple cameras and click **Get Device's Recording Settings** in the added cameras list page to get recording schedules of the devices in a batch.
- When the storage location is set to pStor and the device supports third stream, the **Stream Type** can be selected as third stream.

10. **Optional:** Set the **Picture Storage Settings** switch to ON and select the storage location from the drop-down list for storing the pictures uploaded from the camera to the specified location.

Note

For cameras added by ISUP protocol, this function is not available. You should click **Configure** to edit the picture storage configurations.

11. **Optional:** Click **Configure on Device** in the top right corner of the camera editing panel or click in the **Operation** column of the added camera list page to set the remote configurations of the corresponding device if needed.

Note

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

12. **Optional:** In the top right corner of the camera editing panel, click **Copy To** to select configuration item(s) and copy the settings of this camera to other cameras.
13. Click **Save**.

Set Recording Parameters

For cameras on the current site and Remote Site, the platform provides storage locations such as Hybrid Storage Area Network, Cluster Storage, and pStor for storing the video files of the cameras according to the configured recording schedule. You can get device's recording settings when adding a camera to an area.

Steps

1. Enter the Recording Setting page.
   1) In the top left corner of the Home page, select → **Basic Management** → **Device** → **Area** .
   2) Select an area to show its cameras.

Note

refers to the current site and refers to Remote Site.

3) Select a camera and click its name to enter the camera settings page.
4) Select the **Recording Settings** tab.

2. On the editing camera page, click **Recording Settings** on the top.
3. In the Recording Settings area, switch on **Main Storage** (for the current site) or **Storage in Central System** (for Remote site).
4. Select the storage location for storing the recorded video files.
5. Select the storage type and configure other required parameters.

Note

The parameters vary according to the site (current site or Remote Site) you selected previously.

- Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location in real time.

Note

- If you select **Encoding Device** as the storage location, you needn't select the storage type, but configure the following parameters as real-time storage settings by default.
- If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **pStor Cluster Service**, specify a server and (optional) select a Streaming Server to get video streams from cameras via it.

Recording Schedule Template

Set the template which defines the time periods to record the camera's video.

All-Day Time-Based Template

Record the video for all-day continuously.

All-Day Event-Based Template

Record the video when alarm occurs.

Add New

Set the customized template. For details about setting customized template, refer to ***Configure Recording Schedule Template*** .

View

View the template details.

Note

The event-based recording schedule can not be configured for the **Cluster Storage**, and the command-based recording schedule can not be configured for the **Cluster Storage** and **pStor**.

Stream Type

Select the stream type as main stream, sub-stream or dual-stream.

Note

For storing on Hybrid Storage Area Network, Cluster Storage, pStor or pStor Cluster Service, dual-stream is not supported.

Pre-Record

Record video from periods preceding detected events. For example, when someone opens a door, you can see what happens right before the door opened.

This field displays when the storage location is set as Encoding Device, Cluster Storage, pStor, or pStor Cluster Service. And it is available for the camera that is configured with event-based recording.

Post-Record

Record video from periods following detected events.

This field displays when the storage location is set as Encoding Device or Hybrid Storage Area Network. It is available for the camera that is configured with event-based recording.

Video Expiry Time

If you select **Encoding Device** as the storage location, switch on**Video Expiry Time** and enter expiration day(s).

Automatically delete the oldest videos after the specified retention period. This method allows you to define the longest time period to keep the videos as desired and the actual retention period for the videos depends on the allocated quota.

Enable ANR

If you select the **Encoding Device** or **Hybrid Storage Area Network** as the storage location, check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network fails and transport the video to storage device when network recovers.

- Select **Scheduled Copy-Back** as the storage type to copy the recorded video files from the encoding device or pStor to the specified storage location according to scheduled period.

Note

The recordings can be copied only from the encoding device to Hybrid Storage Area Network, Cluster Storage, pStor or pStor Cluster Service, or from pStor to another pStor.

Upload Time

Specify the time period to copy the recorded video files to the specified storage location.

Recording for Copy-Back

Select the type of recorded video file to backup.

Max. Copy-Back Speed (KBps)

Enter the maximum copy-back speed.

6. **Optional:** Set the **Auxiliary Storage** switch to ON and configure another storage location for the video files.

Note

- If Cluster Storage, Hybrid Storage Area Network, pStor, or pStor Cluster Service is set as the auxiliary storage location, you can select **Real-Time Storage** to store recorded video files or select **Scheduled Copy-Back** to copy recordings from the encoding device or pStor (main storage) to specified auxiliary storage location according to the scheduled period.
- Before setting **Scheduled Copy-Back**, make sure you have configured real-time recording schedule stored in device local storage or pStor for the main storage.
- The recordings can be copied only from the encoding device to Hybrid Storage Area Network, Cluster Storage, pStor or pStor Cluster Service, or from pStor to another pStor.

7. Click **Save**.

Set Picture Storage

The pictures uploaded from the devices, such as alarm triggered pictures, captured face pictures, and captured plate license pictures, can be stored on the HDD of SYS server, Hybrid Storage Area Network, Cluster Storage, pStor, or NVR (Network Video Recorder).

Steps

1. On the editing camera page, click **Picture Storage Settings** on the top.
2. Switch on **Picture Storage**.
3. Select the storage location from the drop-down list.

Note

- If you select System Management Server, the pictures will be stored on the SYS server. Click **Configure** to view the disk on SYS server and storage quota, which can be edited via the Web Client running on the SYS server. Refer to ***Set Storage on System Server*** for details.
- You cannot configure the storage location for the captured undercarriage pictures, which are stored on the UVSS device.

4. Click **Save** to save the uploaded pictures to the specified location.

7.3.2 Edit Door for Current Site

You can edit the basic information, related cameras, picture storage settings, card reader settings, and face recognition terminal settings of a door on the current site.

Steps

1. In the left panel, select the added current site from the drop-down site list to show its areas and select one area.

Note

The icon indicates that the site is current site.

2. Select the **Door** tab to show the added doors in this area.
3. Click a door's name in the **Name** column to enter the door editing page.
4. Edit the door's basic information.

Name

Edit the name for the door.

Note

If you change the name, you can click in the door list page to apply the new name to the device.

Door Contact

The door contact's connection mode.

Exit Button Type

The exit button connection mode.

Lock Door when Door Closed

If it is enabled, the door will be locked once the door magnetic is closed. If there is no door magnetic, the door will be locked after the extended open duration ends.

Note

This function should be supported by the device.

Open Duration

The time interval between the door is unlocked and locked again.

Extended Open Duration

The time interval between the door is unlocked and locked again for the person whose extended access function is enabled.

Door Open Timeout Alarm

After enabled, if the door has been configured with the event or alarm, when the door contact open duration has reached the limit, the event or alarm will be uploaded to the system.

Duress Code

If you enter this code on the card reader keypad, the Control Client will receive a duress event. It should be different from the super password and dismiss code.

Super Password

If you enter this password on the card reader keypad, you are exempted from all the remaining locked (Credential Failed), anti-passback, and first card authorization restrictions. It should be different from the duress code and dismiss code.

Dismiss Code

If you enter this code on the card reader keypad, the buzzer's beeping will be stopped. It should be different from the duress code and supper password.

5. Link cameras to the door, and you can view its live view, recorded videos, and captured pictures via the Control Client.

Note

- Up to 2 cameras can be linked to one door.
- You can click ↑ or ↓ to adjust the priority of cameras.
- You can switch on **Auto Capture** to enable automatic capture of the camera.

6. **Optional:** Switch on **Picture Storage** and select a storage location from the drop-down list.

Note

If an error occurs during picture storage configuration, ⓘ appears on the right of the door name.

7. **Optional:** On the Card Reader panel, switch on **Card Reader 1** or **Card Reader 2** and set the card reader related parameters.

Min. Card Swipe Interval

After it is enabled, you cannot swipe the same card again within the minimum card swiping interval.

Reset Entry on Keypad After(s)

Set the maximum time interval of pressing two keys on the keypad. If timed out, the first entry will be reset.

Failed Card Attempts Alarm

After it is enabled, if the door is configured with event or alarm, when the number of excessive failed card swiping attempts has reached the limit, the event or alarm will be uploaded to the system.

Tampering Detection

After it is enabled, if the door is configured with device tampered event or alarm, when the device body or panel is taken apart, the alarm will be triggered and sent to the system.

OK LED Polarity

Only supported when the device is connected via Wiegand interface. The polarity for OK core wire connection on the card reader mainboard.

Error LED Polarity

Only supported when the device is connected via Wiegand interface. The polarity for ERR core wire connection on the card reader mainboard.

Face 1:N Matching Threshold

Set the threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate. The maximum value is 100.

Face Recognition Interval

The time interval between continuous face recognition twice when authenticating.

Face Anti-spoofing

If it is enabled, the device can recognize the live face. Also, you can check **Protect Sensitivity of Face Anti-Proofing**, and set the face anti-spoofing security level.

Face Recognition Application Mode

Select **Indoor** or **Others** according to actual environment.

Note

The parameters displayed vary according to the different models of the access control devices. For details about the parameters, refer to the user manual of the device.

8. **Optional:** For a turnstile or an access controller of certain types, switch on **Face Recognition Terminal** and add face recognition terminals to link with the selected turnstile.
   1) Click **Add** to enter the Add Face Recognition Terminal page.
   2) Select **IP Address**, **Online Devices**, or **Device ID** as the adding mode, and set the required parameters, which may vary according to different terminals.
   3) Click **Add** to link the terminal to the turnstile or access controller.
   4) **Optional:** Click in the Operation column to configure parameters for the terminal. For details, refer to ***Configure Parameters for Access Control Devices and Elevator Control Devices*** .
9. **Optional:** Click **Copy To** in the upper right corner to apply the current settings of the door to other door(s).
10. Click **Save**.

7.3.3 Edit Elevator for Current Site

You can edit basic information, floor information, related cameras, card reader settings of the elevator on current site.

Steps

1. On the **Elevator** tab, click an elevator's name in the **Name** column to enter the configuration page.
2. Edit the elevator's basic information.

   Name

   Edit the name for the elevator.

   Note

   If you changes the name, you can click in the elevator list page to apply the new name to the device.

   Extended Open Duration

The time interval between the elevator door is open and closed again for the person whose extended access function is enabled.

Elevator Door Open Timeout Alarm

After enabled, if the elevator has configured with event or alarm, when the elevator door open duration has reached the limit, the event or alarm will be uploaded to the system.

Max. Open Duration

The time interval between the elevator door is unlocked and locked again if the person has enabled Extended Access function.

Duress Code

If you enter this code on the card reader keypad, the Control Client will receive a duress event. It should be different with the super password and dismiss code.

Super Password

If you enter this password on the card reader keypad, you are exempted from all the remaining locked (Credential Failed), anti-passback, and first card authorization restrictions. It should be different with the duress code and dismiss code.

Dismiss Code

If you enter this code on the card reader keypad, the buzzer's beeping will be stopped. It should be different with the duress code and super password.

3. In the Floor panel, all the imported floors will be displayed in the list. You can edit the floor's name or reset the imported floor No.

Edit Floor Name

You can edit the floor name if needed.

Note

If you changes the name, you can click **Apply Floor Name** in the elevator list page to apply the new name to the device.

Reset Imported Floor No.

You can click **Reset Imported Floor No.** and enter the range of the floor No. to reset the settings of the floors, such as schedule settings, name, access level settings, etc.

4. Relate cameras (such as the cameras mounted inside the elevator) to the elevator, and you can view its live view, recorded video, captured pictures via the Control Client.

Note

- Up to two cameras can be related to one elevator.
- You can select the door and click ↑ or ↓ to adjust the displaying priority of its auto capture.
- You can switch on **Auto Capture** to realize the function of capturing automatically.

5. In the Card Reader panel, switch on **Card Reader 1** or **Card Reader 2** and set the card reader related parameters.

Min. Card Swipe Interval

After enabled, you cannot swipe the same card again within the minimum card swiping interval.

Reset Entry on Keypad after

Set the maximum time interval of pressing two keys on the keypad. If timed out, the first entry will be reset.

Failed Card Attempts Alarm

After enabled, if the door has configured with event or alarm, when the number of excessive failed card swiping attempts has reached the limit, the event or alarm will be uploaded to the system.

Tampering Detection

After enabled, if the door has configured with device tampered event or alarm, when the device body or panel is taken apart, the alarm will be triggered and sent to the system.

OK LED Polarity

Only supported when the device is connected via Wiegand interface. The polarity for OK core wire connection on the card reader mainboard.

Error LED Polarity

Only supported when the device is connected via Wiegand interface. The polarity for ERR core wire connection on the card reader mainboard.

Buzzer Polarity

Only supported when the device is connected via Wiegand interface. The polarity for buzzer connection on the card reader mainboard.

Fingerprint Security Level

Select the fingerprint security level. The higher is the security level, the lower is the face acceptance rate (FAR). The higher is the security level, the higher is the false rejection rate (FRR).

Note

The parameters displayed vary according to the model of the access control device. For details about the parameters, refer to the user manual of the device.

---

6. **Optional:** Click **Copy to** in the upper right corner to apply the current settings of the elevator to other elevator(s).
7. Click **Save**.
8. **Optional:** In the elevator list, click › on the left of an elevator name to display the floors, check at least one floor, and click **Floor Relay Action Time** or **Elevator Control Delay Time for Visitor** to set time limits for floor access.

7.3.4 Edit Vehicle for Current Site

After adding vehicles to areas of the current site, you can edit the basic vehicle information (e.g., license plate No., driver / driver group, vehicle type, color, brand, fuel tank model, and vehicle picture) for the current site as needed.

Steps

1. In the top left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the area list panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area.
5. Select the **Vehicle** tab to show the added vehicles.
6. Click a vehicle's license plate number in the License Plate No. column.
7. Edit the vehicle information (e.g., license plate No., driver / driver group, vehicle type, color, brand, fuel tank model, vehicle picture).
8. Click **Save**.

7.3.5 Edit Security Radar for Current Site

After adding a security radar to an area of the current site, you can edit the security radar's name, view the drawn zones or trigger lines, and view the related calibrated cameras.

Steps

1. In the top left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the area list panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is current site.
4. **Optional:** Select an area.
5. Select the **Security Radar** tab to show the added security radars.
6. Click a security radar's name in the **Name** column to enter the security radar editing page.
7. Edit the security radar's name.
8. **Optional:** In the **Zone** field, view the drawn zones of the security radar.

Note

If there is no zone drawn for the security radar, you should go to the Map Settings module to draw. Refer to ***Draw Zone or Trigger Line for Radar*** for details.

9. **Optional:** In the **Relate Calibrated Camera** field, view the calibrated cameras related to the security radar.

Note

If there is no calibrated camera related to the security radar, you should go to the Map Settings module to configure. Refer to ***Relate Calibrated Camera to Radar*** for details.

10. Click **Save** to save the settings for the security radar.

7.3.6 Edit Alarm Input for Current Site

You can edit the basic information of alarm input and relate detector to the security control panel's alarm input for current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the area list panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **Alarm Input** tab to show the added alarm inputs.
6. Click an alarm input name in the **Name** column to enter the Edit Alarm Input page.
7. Edit the alarm input name.
8. **Optional:** For the alarm input of security control panel, set the **Related Detector** switch to ON to configure related detector for the alarm input.
   1) Click **Add** to add a detector.
   2) Enter the detector name.
   3) Click to save the detector type.

Note

- Only the alarm input of a security control panel supports this function. Make sure you have added a security control device to the system, and have added its zone to area as an alarm input. See ***Add Alarm Input to Area for Current Site*** for details.
- On Map Settings page, the detectors related to the alarm input of a security control panel will be displayed in the resource list of alarm input on the right panel. When selecting the alarm

input and dragging it to the map, the related detectors will also be added to the map, and the relations among them will be marked with lines. If you only drag the alarm input to the map without selecting it, the related detectors will not be added to the map.
- You cannot edit the detector type here. If you want to edit it, go to the Remote Configuration page of security control panel, and click **Input Settings → Zone** .

9. Click **Save**.

7.3.7 Edit Alarm Output for Current Site

You can edit the alarm output name for current site.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **Alarm Output** tab to show the added alarm outputs.
6. Click an alarm output name in the **Name** column.
7. Edit the alarm output name in the pop-up window.
8. Click **Save**.

7.3.8 Edit UVSS for Current Site

You can edit name of the Under Vehicle Surveillance System (UVSS) and link cameras to the UVSS for current site.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **UVSS** tab to show the added UVSSs.
6. Click a UVSS name in the **Name** column.
7. Edit the name of UVSS.
8. **Optional:** Link cameras to the UVSS.
   1) Set the **Link Camera** switch to ON.

2) Select the camera(s).

9. Click **Save**.

7.3.9 Edit Commercial Display Resource for Current Site

You can edit the name of a commercial display resource for the current site.

Steps

1. Click **Area** on the left.
2. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

3. **Optional:** Select an area.
4. Select the **Commercial Display Resource** tab to show the added commercial display resources.
5. Click a commercial display resource's name in the **Name** column.
6. Edit the name in the pop-up window.
7. Click **Save**.

7.3.10 Edit Speaker Unit for Current Site

You can edit basic information, related cameras settings of the speaker unit on current site.

Steps

1. Click **Area** on the left.
2. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

3. **Optional:** Select an area.
4. Select the **Speaker Unit** tab to show the added speaker unit(s) in this area.
5. Click speaker unit's name in the Name column to enter the speaker unit editing page.
6. Edit the name for the speaker unit.
7. **Optional:** Link camera(s) to the speaker unit.
   - Up to 4 cameras are allowed to be linked.
   - Click ↑ or ↓ to adjust the displaying sequence of the cameras.
8. Click **Save**.

7.3.11 Edit BACnet Object for Current Site

You can edit the names of BACnet objects for current site.

Steps

1. In the top left corner of the Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the area list panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area.
5. Select the **BACnet Object** tab.
6. Click the name of a BACnet object in the **Name** column to enter the editing page.
7. Edit the name of the BACnet object.
8. Click **Save**.

7.3.12 Edit Optimus Resource for Current Site

After integrating the resources on Optimus to the HikCentral Professional via Optimus, the Optimus resources are added to the areas.

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. Optional: Select an area.
5. Select the **Optimus Resource** tab to show the added Optimus resources.
6. Click the name of Optimus resource to enter the details page.
7. You can view the basic information of the resource, such as name, device type, and manufacturer.
8. You can also add the resource on the map so that when an event/alarm is triggered on the resource, you can view the notification and details on the map.

Note

7.3.13 Edit Fire Detector for Current Site

You can edit the basic information of the fire detector on current site.

Steps

1. Click **Area** on the left.
2. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

3. **Optional:** Select an area.
4. Select the **Fire Detector** tab to show the added fire detector(s) in this area.
5. Click fire detector's name in the **Name** column to enter the fire detector editing page.
6. Edit the name for the fire detector.
7. Click **Save**.

7.3.14 Edit Element for Remote Site

If you are using a Central System with a Remote Site Management module, you can edit the cameras, doors, and elevators that have been added to the Remote Site. In this case, you will learn how to edit the added cameras for the Remote Site.

Steps

1. Click **Area** on the left.
2. In the left panel, select the added Remote Site from the drop-down site list to show its areas.

Note

The icon indicates that the site is a Remote Site.

3. **Optional:** Select an area to show its cameras.
4. Click a camera's name in the Name column to enter the camera editing page.
5. Edit the camera's basic information, including camera name and protocol type.

Note

If you change the camera's name, you can click on the added camera list page to apply the new name to the device.

6. **Optional:** Click **Live View** to view the live view of the camera and hover over the window and click in the lower-right corner to switch to playback.
7. Edit the recording settings of the camera.

Note

For recording settings, if no recording settings have been configured for the camera, click **Configuration on Site** to set the parameters.

8. **Optional:** Click **Configuration on Device** in the top-right corner of the camera editing panel or click in the **Operation** column of the added camera list page to set the remote configurations of the corresponding device if needed.

Note

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

9. **Optional:** Click **Copy to** to copy the current camera's specified configuration parameters to other cameras of the Remote Site.

10. Click **Save**.

7.4 Remove Element from Area

You can remove the added cameras, doors, elevators, vehicles, security radars, alarm inputs, alarm outputs, digital signage screens, interactive flat panels, speaker units, and fire detectors from the area.

7.4.1 Remove Element from Area for Current Site

You can remove the added cameras, doors, security radars, alarm inputs, alarm outputs, display screens, interactive flat panels, speaker units, BACnet objects, or fire detectors. from the area for current site.

Steps

1. Click **Area** on the left.
2. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

3. **Optional:** Select an area in the area list panel to show its added elements.
4. Select the **Camera**, **Door**, **Elevator**, **Vehicle**, **Security Radar**, **Alarm Input**, **Alarm Output**, **Display Screen, Speaker Unit**, **BACnet Object**, or **Fire Detector** tab to show the added elements.
5. Select the elements.
6. Click to remove the elements from the area for current site.

7.4.2 Remove Element from Area for Remote Site

If you are using a Central System with a Remote Site Management module, you can remove the cameras, doors, and elevators that have been added from the Remote Site. In this case, you will learn how to remove the added cameras from the Remote Site.

Steps

1. Click **Area** on the left.
2. In the left panel, select the added Remote Site from the drop-down site list to show its areas.

Note

The icon indicates that the site is a Remote Site.

3. **Optional:** Select an area to show its added cameras.
4. Select the cameras.
5. Click to remove the cameras from the area for remote site.

6. **Optional:** If ⊗ appears near the camera name, it means the camera has been deleted from the Remote Site. Hover the cursor over the ⊗ and click **Delete** to delete the camera from the area.

Chapter 8 Person Management

You can add person information to the platform for further operations such as access control (linking a person to an access level), face picture comparison (adding a person to a face picture library), etc. After adding the persons, you can edit and delete the person information if needed.

8.1 Add Departments

When there are a large number of persons managed in the platform, you can put the persons into different departments. For example, you can group employees of a company to different departments.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. Click + at the top of the department list to enter the Add Department page.
4. Set the department information, including the parent department, department name, and description.

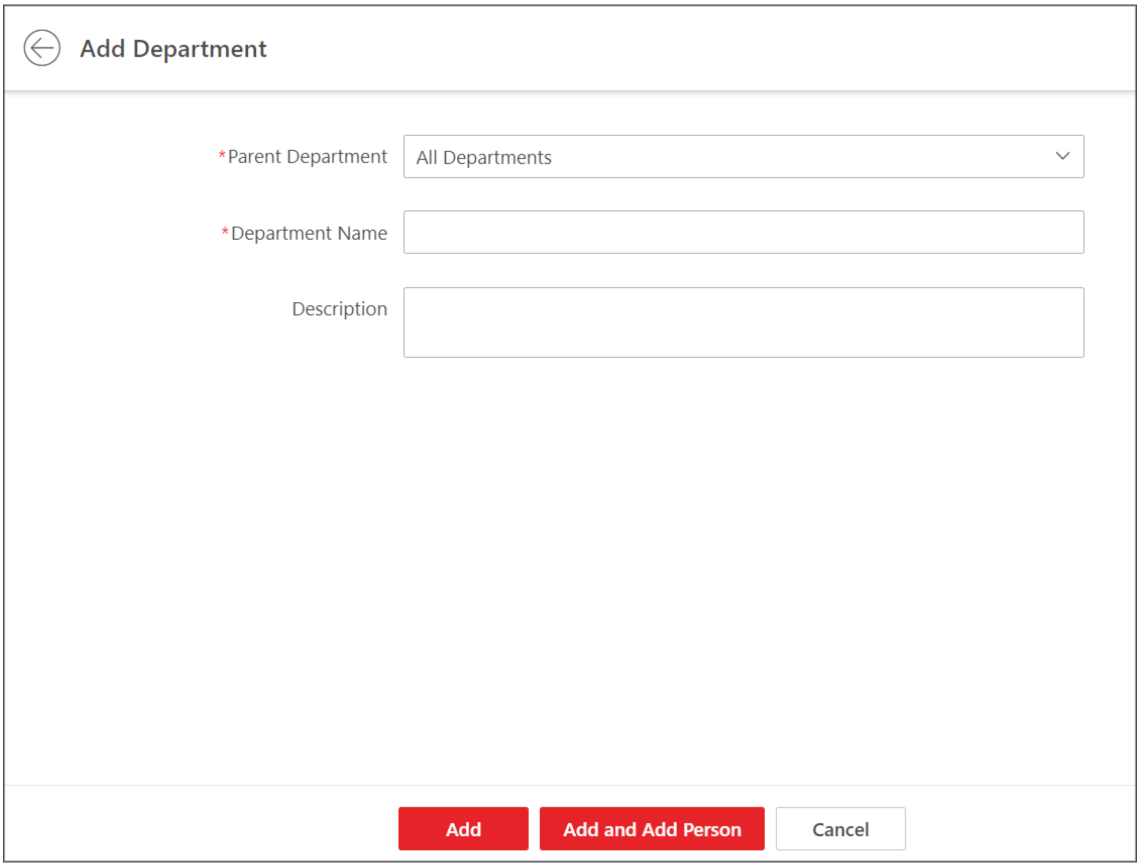


Figure 8-1 Add Department

5. Add department.
   - Click **Add** to add the department and go back to the person management page.
   - Click **Add and Add Person** to add the department and enter the Add Person page.
6. **Optional:** If your HikCentral Professional License contains the permission to access the Access Control module, set parameters of authentication via PIN code.
   1) Click to open the Set Authentication via PIN Code window.
   2) Switch on **Authenticate via PIN Code**.

   Note

   - When enabled, if the authentication mode of the card readers at the access points is also set to **Authenticate via PIN Code**, all the added persons are allowed to use their PIN codes alone as the credential for access authentication.
   - When enabled, no duplicated PIN code is allowed.
   - You can set a PIN code for a person when setting basic information for the person. For details, see ***Add a Single Person*** .

   3) Set the PIN code update mode.

   Auto

The platform will automatically reset all persons' PIN codes and apply the reset PIN codes to the access control devices. The system administrator needs to notify all users of the updated PIN codes.

Manual

The system administrator needs to manually filter out persons who have no PIN code or have duplicated PIN codes, change their PIN codes and then notify them of the updated PIN codes.

Note

The system administrator needs to notify relevant persons of the updated PIN codes in time. Otherwise these persons' access authentication will be affected.

7. **Optional:** Perform the following operations after adding departments.

Edit Department
Select a department, and click at the top of the department list to edit the parent department, department name, or remarks.

Delete a Department
Select a department and click at the top of the department list to delete the selected one.

Note

The root department cannot be deleted.

Delete All Departments
Click beside at the top of the department list to delete all added departments.

8.2 Basic Configuration Before Managing Persons

Perform the following configurations if needed.

8.2.1 Set Person ID Rule

Before adding persons, you should configure a rule to define the prefix No., total length, and whether using random digits for the person ID.

Steps

Note

Once a person is added to the platform, the ID rule will be not configurable, so we recommended that you should ensure the ID rule at the very beginning.

1. In the Person module, select **Basic Configuration → Person ID Rule** on the left.
2. Set the total length.
3. Select the ID generation mode.
4. Click **Save**.

8.2.2 Set QR Code Mode

You can select static QR code or dynamic QR code for employees. If you select dynamic QR code, the platform will generate a dynamic QR code for persons on the platform. Every time the employee uses the QR code to authenticate, the platform will refresh and generate a QR code automatically.

In the left navigation bar of the Person module, click **Basic Configuration → Credential Settings → QR Code Mode** . Select a QR code mode, and set the QR code validity period if you select **Dynamic QR Code**.

8.2.3 Customize Additional Information

Customize a person's basic information by adding additional items as either custom private or custom public information. The former refers to private information such as the person's salary. The latter refers to public information such as the person's department and occupation. When an additional information item is added, it will be displayed as an configuration option on the Basic Information tab of the Add Person page.

Steps

1. Select **Additional Information** on the left.
2. Click **Add**.
3. In the pop-up window, enter the following parameters.

   Type

   Select the type to restrict the format of the contents of the item.

   Sharing Property

   Click **Private** or **Public** to set the sharing property of the contents of the item.

   Example

   For example, if you select **General Text**, enter the text when adding a person. If you select **Date**, setting date as the content of the item is required when adding a person (see the figure below).
4. Click **Add**.

8.2.4 Automatically Generate PIN for Persons

You can enable the function of automatically generating PIN for persons, so that you do not have to set PIN for newly-added persons.

On the top navigation bar, select ⊞ **→ Basic Management → Person → Basic Configuration → PIN Configuration** .

Check **Auto Generate PIN for Person** and save.

8.2.5 Manage Cause of Unauthorizing Persons or Disabling Person Cards

In the left navigation bar of the Person module, click **Basic Configuration → Person Settings → Cause of Disabling** .

8.2.6 Position Management

The platform allows you to add positions to define the hierarchical levels of your company. By assigning the positions to employees, you can quickly understand the number of active employees in each position and the number of employees who have resigned. You can manually add positions one by one or import multiple positions at once via a predefined template.

Add a Position

You can manually add a position to the platform by entering the position name and specifying its upper-level position.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Position Management** on the left.
3. Click + above the left position tree to open the Add Position pane.
4. Enter the name of the position.
5. From the drop-down list, select the upper-level position to which the position to be added is subordinate.

   Note

   If you select **<None>**, the position has no upper-level position.
6. **Optional:** Click to select the persons that have been assigned to this position.
7. Click **Add**.
8. **Optional:** Perform the following operations.

Edit Position	• Select the position from the tree on the left and click at the top to edit its information. • Click in the Operation column of a position to edit its information.
Delete Position(s)	• Select a position from the tree on the left and click at the top to delete the selected position. • Click in the Operation column of a position to delete it. • Select one or multiple positions on the right pane and click **Delete** at the top to delete the selected position(s). • To delete all positions, click ∨ → **Delete All** either above the left tree or on the top of the right pane.

Search for Position	Enter the position name in the search box above the left tree to search in all added positions, and in the search box on the top right to search under the selected upper-level position. Supports fuzzy search.

Import Positions

You can import multiple positions at once by entering the names of the positions and their corresponding upper-level positions in a predefined template.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Position Management** on the left.
3. Click above the left position tree to open the Batch Import Positions pane.
4. Click **Download Template** to download the template to the local PC.
5. Open the downloaded template file and fill in the required information, including the names of the positions and their upper-level positions.
6. Click to select the edited template file from the local PC.
7. **Optional:** Check **Auto Replace Duplicated Position** to allow the platform to automatically replace existing positions if the file to be imported contains positions that are already added to the platform.

   Note

   If it is not checked and the file contains positions that are already added to the platform, the import may fail.
8. Click **Import**.
9. **Optional:** Perform the following operations.

Edit Position	• Select the position from the tree on the left and click at the top to edit its information. • Click in the Operation column of a position to edit its information.
Delete Position(s)	• Select a position from the tree on the left and click at the top to delete the selected position. • Click in the Operation column of a position to delete it. • Select one or multiple positions on the right pane and click **Delete** at the top to delete the selected position(s). • To delete all positions, click → **Delete All** either above the left tree or on the top of the right pane.
Search for Position	Enter the position name in the search box above the left tree to search in all added positions, and in the search box on the top right to search under the selected upper-level position. Supports fuzzy search.

8.3 Add Person

Multiple methods are provided for you to add persons to the platform. You can add a person manually. If you want to add multiple persons at a time, you can import persons by downloading and filling in a template or import persons from access control devices / video intercom devices / enrollment stations. In addition, you can batch add profile pictures for persons, and import domain persons.

On the top navigation bar, select → **Basic Management → Person → Person Management → Person** .

You can perform the following operations for adding persons.

1. Click **Add** to add a single person. For details, refer to ***Add a Single Person*** .
2. Click **Import** and select a mode to import persons in a batch.
   - Batch import persons by template. For details, refer to ***Batch Add Persons by Template***
   - Import users in the AD (Active Directory) domain to the platform as persons. For details, refer to ***Import Domain Persons*** .
   - Import person pictures. For details, refer to ***Import Profile Pictures*** .
   - Import persons information to the platform from devices, including access control devices, video intercom devices, or enrollment station. For details, refer to ***Import Persons from Access Control Devices or Video Intercom Devices*** or ***Import Persons from Enrollment Station*** .
3. If you have enabled the **Use This Device as Registration Device** function on the device's configuration page, the information about added persons and credentials, edited credentials on the device will be automatically synchronized to the platform.

For added persons, you can perform the following operation(s).

Edit Person	Click the person name to edit the person details. **Note** When editing the person's effective period, if you have issued temporary card(s) to the person, make sure the expiry date(s) of the person's temporary card(s) are within the effective period.
Delete Persons	Check the person(s) and click **Delete** to delete the selected person(s). Hover the cursor onto beside **Delete**, and then click **Delete All** to delete all persons.

Clear All Profile Pictures	Hover the cursor onto beside **Delete**, and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.
Export Person Information	Click **Export → Export Person Information** , select the **Exporting Range**, and check information types you need to export person information to your PC. For information security, you need to enter your login password to authenticate.
Export Profile Pictures	Click **Export → Export Profile Picture** , select the **Exporting Range**, enter your login password and a password for decompressing the ZIP file, and click **Export**. **Note** Before using this function, you should activate this function first by going to **General → System Configuration → Security → Export Profile Pictures** page and checking the **Export Profile Pictures**.
Adjust Person	• Move the persons to another department. Once moved, the access levels and schedules of the selected persons will be changed. 1. Select one or more persons, click **Adjust → Adjust Department** . 2. Select the target department to which the persons are about to be moved. 3. Click **Move**. • Adjust the effective period for the person in applications. 1. Select one or more persons, click → **Adjust Effective Period** . 2. Select the effective period from the drop-down list. 3. Click **OK**. • Adjust the person's status as resigned. 1. Select one or more persons, click → **Adjust Effective Period** . 2. Set the departure date, type, and reason.. 3. Click **OK**.

Manage Persons' Cards	See ***Card Management*** .
Synchronize Domain Persons	Select person(s) whose information has changed in the AD domain and click **More → Synchronize Domain Persons** at the top of person list to get the latest person information.
Unauthorize/Restore Persons	Check one or more persons, click **More → Unauthorize Person** , and select a cause. Check one or more persons, click **More → Restore Person** .
Clear Access Levels	Select one or more persons, click **More → Clear Access Levels of Person** to clear the access levels of the selected persons. **Note** The access levels of these persons cannot be restored once they are cleared.
Check Person Authorization	Select one or more persons, click **More → Check Access Levels of Person** to enter Check Person Authorization page. On the page, you can test whether the person's access levels and credentials are applied to the access control devices, elevator control devices, and video intercom devices. If failed to be applied, you can apply them again.
Enable/Disable Check-In/Out via Mobile Client	Select one or more persons, click **More → Enable/Disable Check-In/Out via Mobile Client** .

8.3.1 Add a Single Person

You can manually add a person to the platform by setting the person's basic information, credential information, and other information such as the person's access level. The above-mentioned person information constitutes the data basis for the applications related to identity authentication of the person, such as the access control application .

Steps

Note

Before adding persons to the platform, you should confirm and set the person ID rule. As once a person is added, the ID rule cannot be edited any more. For more about the ID rule settings, refer to ***Set Person ID Rule*** .

1. On the Person page, select a department from the department list on the left.

   All persons in the selected department will be displayed on the right. You can check **Show Sub Department** to display the persons in sub departments (if any).
2. Click **Add** above the person list to enter the Add Person page.
3. Set the person's basic information, such as ID, department, first name, and last name.

   ID (Required)

   The default ID is generated by the platform. You can edit it if needed.

   Profile Picture

   Hover the cursor onto , and you can select from three modes to add a picture.

   From Device

   This mode is suitable for non-face-to-face scenario when the person and the system administrator are on different locations.

   Note

   - For access control devices, only specific models of face recognition terminals are supported.
   - For video intercom devices, door stations and outer door stations are supported.
   - For enrollment stations, you need to set related parameters, including access mode, access protocol, device address, port, user name, password, face anti-spoofing, and security level.

   Upload Picture

   Click **Upload Picture** to select a picture from your PC. On top of the Upload Picture window, click **Detect Now** and select a device type and device to detect the face picture quality.

   Note

   - It is recommended that the face in the picture be in the full-face view directly facing the camera, without a hat or head covering.
   - You can drag the picture to change its position or zoom in/out before cutting it.

Note

If you add a smart terminal to the platform, the smart terminal will automatically create models for the profile picture.

Effective Period (Required)

Set the effective period for the person in applications such as access control application, to determine the period when the person can access the specified access points with credentials.

Click **Extend Effective Period** to show a drop-down list and select **1 Month / 3 Months / 6 Months / 1 Year** to quickly extend the effective period based on the configured end time. For example, if the period is from ***2021/10/23 13:30:00*** to ***2022/01/20 14:10:00*** and the extended time is selected as **1 Month**, the end time of effective period will change to ***2022/02/20 14:10:00***.

Date of Employment

You can set the start date of employment for the person.

Allow Login to Self-Service

Switch on **Allow Login to Self-Service** ans set a password to allow employees to log in to self-service on the platform.

Configure Platform User

Click **Configure Now** to configure a platform user for the person to link the person to a platform user.

Note

No more than one person can be linked to a platform user.

Add New User

Create a new user to link the user with the person by setting the user name, password, user status, and role.

Select Existing User

Select an existing user from the drop-down list to link the user with the person, or click **Add User** to add a user first.

Credential Management

Add credential information for the person. See ***Manage Credentials*** for details.

4. **Optional:** Click **Private Information** tab, and set the person's private information, such as email, and phone No.
5. **Optional:** Click **Access Level** tab, and assign access levels to the person to define the access points where the person can access during the authorized period.

Super Access Permission

Persons with this permission will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first person authorization.

Extended Access

When the person accesses the door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

Note

The extended access and super user functions cannot be enabled concurrently.

Device Administrator

Determine if the person has the administrator permission of access control devices.

If the check-box is checked, when you synchronize person information from access control devices, the administrator permission for the person will be retained.

Open Door via Bluetooth on Mobile Client

Check the box to open enable opening door via bluetooth on the Mobile Client.

PIN Code

If you have enabled the function of automatically generating PIN for persons (See ***Automatically Generate PIN for Persons***), the platform will generate a PIN automatically. You can click **Auto Generate PIN** to generate a new PIN. In most cases, the PIN code cannot be used as a credential alone: it must be used after card or fingerprint when accessing; It can be used alone only when **Authenticate via PIN Code** is enabled on the platform and the authentication mode of the card readers is also set to **Authenticate via PIN Code**.

Note

- The PIN code should contain 4 to 8 characters.
- For details about enabling **Authenticate via PIN Code** on the platform, see ***Add Departments*** .

Assign Access Level

a. Click **Assign**.
b. Select one or more access levels for the person.
c. Click **Assign** to add the person to the selected access level(s).

Note

You can click to view information on access points and access schedules.

6. **Optional:** Click **Schedule** tab, view and edit the schedule of the person in the table.

Allow Check-In/Out via Mobile Client

Note

Make sure you have purchased the license for this function.

Switch on it to allow the person to check in/out via the Mobile Client.

Leave Rule

Select a leave rule for the person.

Schedule Overview

View the schedule of the person. You can click **Set Schedule** to set a schedule for the person.

7. **Optional:** On the **Face Picture Library** page, select a face picture library for the person.
8. On the **Alarm Detection** page, enable **Configure Operation Permission of Security Control Device**. Click **Add** to select device and configure operation permissions including **Arm**, **Disarm**, and **Auto Control** for selected device(s).

User Property

Lifetime

All permissions can be configured for the user.

One-Off

Expires after either a single arming or disarming action, or expires automatically after a 24-hour period. No duress code permission. No Keyfobs and tags permission.

Keypad Password

Only 4 to 6 digits are allowed.

Duress Password

Only 4 to 6 digits are allowed. One-Off users do not need to configure the duress password.

9. On the **Portable Enforcement** page, enable **Link to Unique Portable Device**, change the body camera password, click **Add** to link the body camera to a dock station.
10. **Optional:** On the **Resident Information** page, set resident information to link the person with the indoor station and floor and room number.

Note

- Make sure you have added indoor stations to the platform.
- When you select an indoor station, the room number of the indoor station will be filled in automatically in **Room**. You can edit the room number.
- Up to 10 persons can be linked with one indoor station. And a person cannot be linked to multiple indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

11. **Optional:** In Vehicle Information area, add the vehicle information for the person. Click **Parking Lot Entry and Exit Settings** and select parking lot(s) to assign entry and exit permission(s) to the person's vehicle(s).
12. **Optional:** In Emergency Counting Group area, select an emergency counting group to add the person to it, or click **Add Emergency Counting Group** and enter a group name to create an emergency counting group and add the person to it.

Note

When the platform is in emergency status, it is not allowed to add a person to an emergency counting group.

13. **Optional:** Enter the person's skin-surface temperature and select the corresponding temperature status.

    For example, if a person's skin-surface temperature is 37 °C, then you can select her/his temperature status as normal.

14. **Optional:** In Additional Information area, enter additional information to be applied, or select a public digital signage additional information.

    Note

    Make sure you have set the additional information. See ***Customize Additional Information*** for details.

15. Click **Add**, or click **Add and Continue** to finish adding the person and continue to add other persons.

    The person will be displayed in the person list and you can view the details.

Manage Credentials

When adding a person, you can add the required credential information for the person. The supported credentials include normal cards, faces, fingerprints, and irises. These credentials can be used for the access authentication in applications such as access control and elevator control.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. On the adding or editing person page, click **Credential Management** under the profile picture to open the Add Credential pane.
4. In the Card area, click , and then manually enter the card No. or swipe the card on devices (enrollment station, card enrollment station, or card reader) to add normal cards.

    Note

    - For manually entering, digits, letters, and the combination of digits and letters can be entered.
    - For swiping cards, you can read card information via the enrollment station, card enrollment station, or card reader. For details, see ***Batch Issue Cards to Persons*** .

    A QR code will be generated automatically after adding a card and the icon will appear in the top right corner of the card area when you enter the Add Credential page from the editing person page. You can click to view and scan the QR code or click **Download** to download the QR code picture to the local storage for further operations.

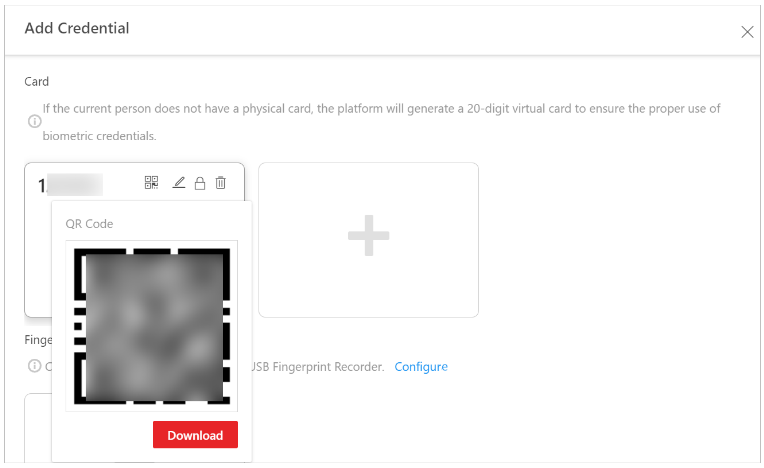


Figure 8-2 View QR Code of Card

5. In the Fingerprint area, click **Configure** to set the method for collecting the person's fingerprint, and then collect the fingerprint.

   USB Fingerprint Recorder

   Plug the USB interface of the fingerprint recorder to the PC on which the Web Client runs and then collect the person's fingerprint via the device.

   Fingerprint and Card Reader

   Select a device type and then select a fingerprint and card reader to collect the person's fingerprint.

   Enrollment Station

   If you set network as the access mode, set other parameters of the enrollment station (e.g., access protocol, device IP address, and device port No.,) to allow the platform to access the device via network. And then collect the person's fingerprint via the device.

   If you set USB as the access mode, plug the USB interface of the enrollment station to the PC on which the Web Client runs, and then collect the person's fingerprint via the device.

6. **Optional:** In the Iris area, collect irises of the person.
   1) Click **Configure** to select a device used for collecting the person's irises.
   2) Click and then start collecting irises.
7. **Optional:** Switch on **Special Credential** and then add special cards and corresponding fingerprint information.
8. **Optional:** Perform the following operation(s).

Edit Card / Fingerprint / Iris Information	Hover the cursor onto an added card, fingerprint, or iris, and then click .
View and Download QR Code of Card	Hover the cursor onto an added card, and then click .

Delete Card / Fingerprint / Iris	Hover the cursor onto an added card, fingerprint, or iris, and then click .

9. Click **Save**.

8.3.2 Batch Add Persons by Template

You can batch add persons to the platform with the minimum effort by importing a template (an Excel file) which contains the person information such as the names of the department and the access levels.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. Click → **Import Person Information via Excel** .

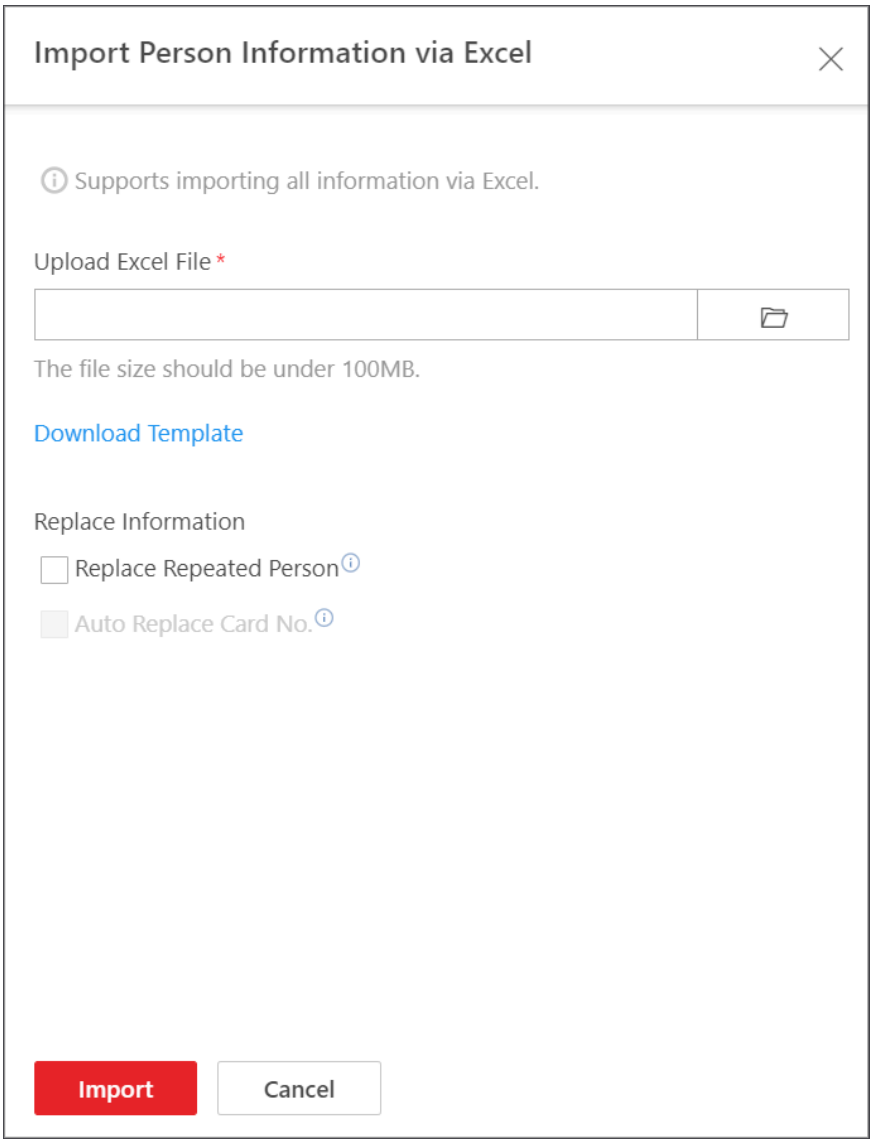


Figure 8-3 Batch Add Persons by Template

4. In the pop-up window, click **Download Template**.
5. Check the basic information items you want to include in the template, such as person type, card No., and email. You can also check custom additional information items. See ***Customize Additional Information*** for how to add custom additional information for persons.
6. Click **Download** to save the template to your PC.
7. In the downloaded template, enter the person information following the rules shown in the template.

Note

If you need to link a person to the indoor station, you should enter Community-Building No.-Unit No.-Room No. in the **Room No.** column.

8. Click , and then select the template (with person information) from your PC.
9. **Optional:** Check **Replace Repeated Person** to replace the person information if the imported ID information is the same with that of the existing persons in the list.
10. **Optional:** Check **Auto Replace Card No.** to replace the card No. automatically if it already exists in the platform.
11. Click **Import** to start importing.

    Note

    - The importing process cannot be stopped once started.
    - You can batch issue cards to the persons by importing the template with card No. information.

    The importing progress shows and you can check the results.

    Note

    You can export the person information that failed to be imported, and try again after editing.

8.3.3 Import Domain Persons

You can import the users in the AD (Active Directory) domain to the platform as persons. After importing the person information (including person name and account name) in the AD domain, you can set other information for the persons, such as credentials.

Before You Start

Make sure you have configured the active directory settings.

Steps

1. On the Person page, click → **Import Person Information via Domain Group** .
2. Select the importing mode.

   Import Domain Persons

   Import specified persons. Select the organization unit and select the persons under the organization unit which are displayed in the Domain Person list on the right. The person information will be synchronized based on each person.

   Import Domain Organization Unit and Person

   Import all the persons in the organization unit. The person information will be synchronized based on each group.

Note

The platform does not support this function if the Azure domain is configured.

Person in Security Group

Import the selected security groups in the AD domain.

3. When selecting **Import Domain Persons** or **Person in Security Group** as the importing mode, select a department to which the selected items (persons or security groups) need to be imported.
4. Set the effective period for the persons as needed.
5. **Optional:** Enable **Add Imported Persons as Users** and select a role for the users from the Linked Role drop-down list.
6. **Optional:** Check **Use Domain Password as Body Camera Login Password**.
7. Click **Import**.

Note

- If the profile picture/email in the domain is linked to the profile picture/email in the platform, the persons' profile picture/email will be imported to the platform from the domain as well. You can view the profile picture/email on the person details page but you cannot edit it.
- If the profile picture/email in the domain is NOT linked to the profile picture/email in the platform, you can take a picture or upload a picture as the person's profile picture and enter the email address.

8.3.4 Import Profile Pictures

You can add multiple persons' profile pictures to the persons in a department. If you access the platform via the Web Client running on the SYS, you need to specify a path where the profile pictures are stored. If you access the platform via the Web Client running on other computers, you can import a ZIP file containing the profile pictures.

Steps

Note

If the ID in the name of the profile picture is duplicate with the person's ID that already exists in the platform, the former will replace the latter. If the ID in the name of the profile picture doesn't exist in the platform, or the name of the profile picture only contains the person name, the platform will create a new person.

1. Name the profile pictures according to the person name or person ID.

Note

- The naming rule of picture is: Person Name, Person ID, or Person Name ID. The person name should contain the first name and the last name, separated by a plus sign.

The naming rule for profile pictures: First Name+Last Name_ID. At least one of first name and last name is required, and the ID is optional. For example, Kate+Smith_123.jpg; Kate_123.jpg; Smith_123.jpg.

- Dimension recommendation for each picture: 295×412.
  Size recommendation for each picture: 60 KB to 100 KB.
- The pictures should be in JPG, JPEG, or PNG format.

2. **Optional:** If you access the platform via the Web Client running on the SYS, move these pictures into one folder and then compress the folder in ZIP format.

Note

The ZIP file should be smaller than 4 GB, or the uploading will fail.

3. On the top navigation bar, select → **Basic Management → Person** .
4. Select **Person Management → Person** on the left.
5. Click → **Import Profile Picture** .
6. Select the person pictures.
   - If you access the platform via the Web Client running on the SYS, select a path where the profile pictures are stored.
   - If you access the platform via the Web Client running on other computers, select ZIP files containing the profile pictures.

   Note

   You can hold CTRL key and select multiple ZIP files. Each ZIP file should be no larger than 4 GB.
7. Select a department from **Department**.
8. **Optional:** Switch on **Check Face Quality by Device** and then select a device type and a device for verifying the face quality.
9. Click **Import** to start importing.

   The importing progress shows and you can check the results.
10. **Optional:** After importing profile pictures, click **Export Failure Details** to export an Excel file to the local PC and view the failure details.

8.3.5 Import Persons from Access Control Devices or Video Intercom Devices

If the added access control devices and video intercom devices have been configured with person information, you can get the person information from these devices and import it to the platform. The person information that can be imported includes person names, profile pictures, credentials (PIN codes, cards, and fingerprints), effective periods, person roles, etc.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. Click → **Import Person Information from Device** .
4. Select **Access Control Device** or **Video Intercom Device** as the device type.

5. Select one or more devices from the device list.

Note

You can enter a key word (fuzzy search supported) in the search box to search the target device(s) quickly.

6. Select the importing mode.

All

Import all the persons stored in the selected devices.

Specified Employee No.

Specify the employee No. of up to five persons and import the persons to the platform.

7. Select a department to which the persons will be imported.
8. **Optional:** Check **Replace Profile Picture** to replace the existed person profile pictures with the new ones from the devices.
9. Click **Import** to start importing.

Note

When importing, the platform will compare person information on the device with person information in the platform based on the person name. If the person name exists on the device but does not exist in the platform, the platform will create a new person. If a person name exists on both sides, the corresponding person information in the platform will be replaced by the one on the device.

10. If the following window pops up, select a method to import the person information.

Note

If not, skip this step.

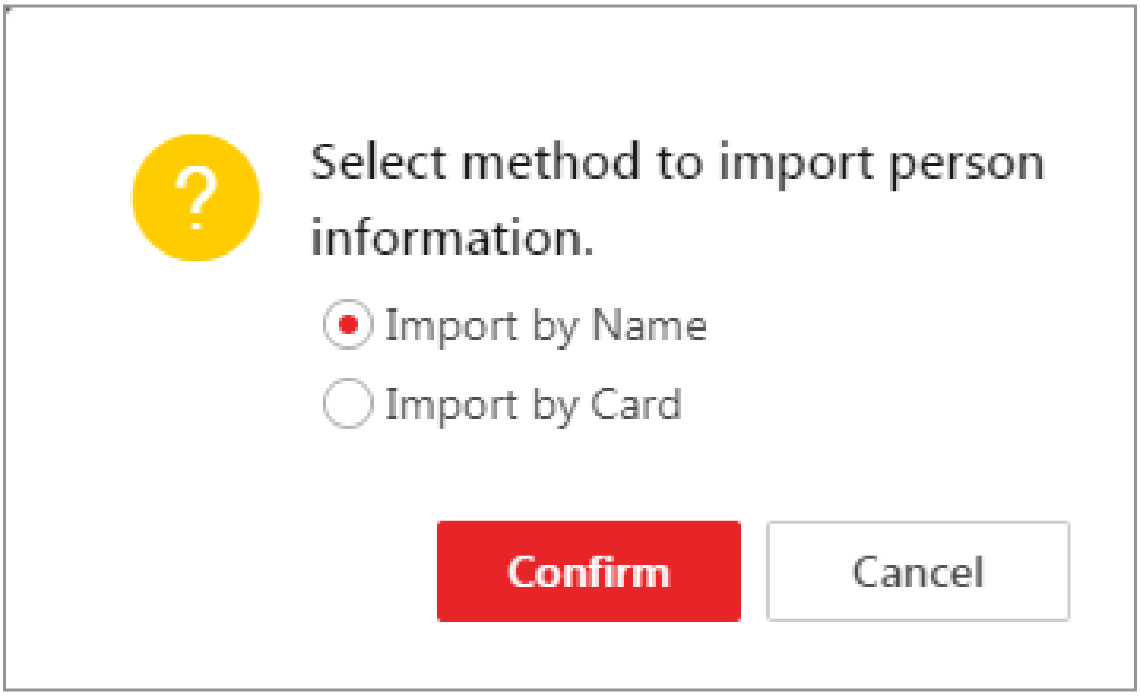


Figure 8-4 Select an Import Method

Import by Name

The person information directly linked to the access control devices will be imported.

Note

This method is usually used for the access control devices with facial recognition capability.

Import by Card

The person information linked to the cards of the access control devices will be imported

Note

This method is usually used for the access control devices which link person information via cards.

8.3.6 Import Persons from Enrollment Station

HikCentral Professional allows you to apply the required person information to an enrollment station via a template or the person list on the platform, and then enroll the persons' credentials via the enrollment station. Once you complete the enrollment, you can import the person and credential information from the enrollment station to the platform by specifying the IP address, port number, user name and password of the device to allow the platform to access it.

Before You Start

Make sure you have enroll the persons' credentials via the enrollment station. For details, see ***Manage Credentials*** .

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Click → **Import Person Information from Device** .
3. Select **Enrollment Station** as the device type.
4. Set other parameters, such as access mode, device address, device port, and stage.

   Device Address

   Enter the IP address of the enrollment station from which the person information needs to be imported.

   Device Port

   Enter the port No. of the enrollment station from which the person information needs to be imported.

   User Name

   Enter the user name of the enrollment station from which the person information needs to be imported.

   Password

   Enter the password of the enrollment station from the person information needs to be imported.
5. Set importing stage and method.

   Apply Person Information

   The persons whose credentials need to be enrolled will be applied to the enrollment station.

   Import from Template

   If the persons are not added to the platform, download the template from the enrollment station and then edit the template and apply it to the enrollment station for enrolling the persons' credentials.

   Import from Person List

   If the persons have been added to the platform, select the department to apply the persons to the enrollment station for enrolling the persons' credentials.

   Copy Back Person and Credential Information

   When the persons' credentials are enrolled, select the department to which the person and credential information will be imported to.
6. Click **Import** to start importing.

8.4 Person Self-Registration

If there are persons to be added to the system, you can generate a QR code for them to scan. After scanning the generated QR code by smart phone, the persons can enter their personal information (including profile) on Self-Registration page. If you have enabled Review Self-Registered Persons function, you need to review and approve their person information, otherwise they cannot be added to the system.

This function is applicable to circumstances like a company where there are a large amount of new employees to be added to the system. For example, you print the generated QR code for the new employees to scan. After scanning the QR code by smart phone, new employees will enter Self-Registration page to import their personal information.

Note

You should set self-registration parameters beforehand. See ***Set Self-Registration Parameters*** for details.

8.4.1 Set Self-Registration Parameters

Before starting self-registration, you need to set self-registration parameters. A QR code is necessary for the persons to register their information by themselves. Besides, you can configure face quality verification and person information review.

On the top navigation bar, select → **Basic Management → Person** . Then select **Basic Configuration → Self-Registration Settings** on the left panel to enter the Self-Registration Settings page.

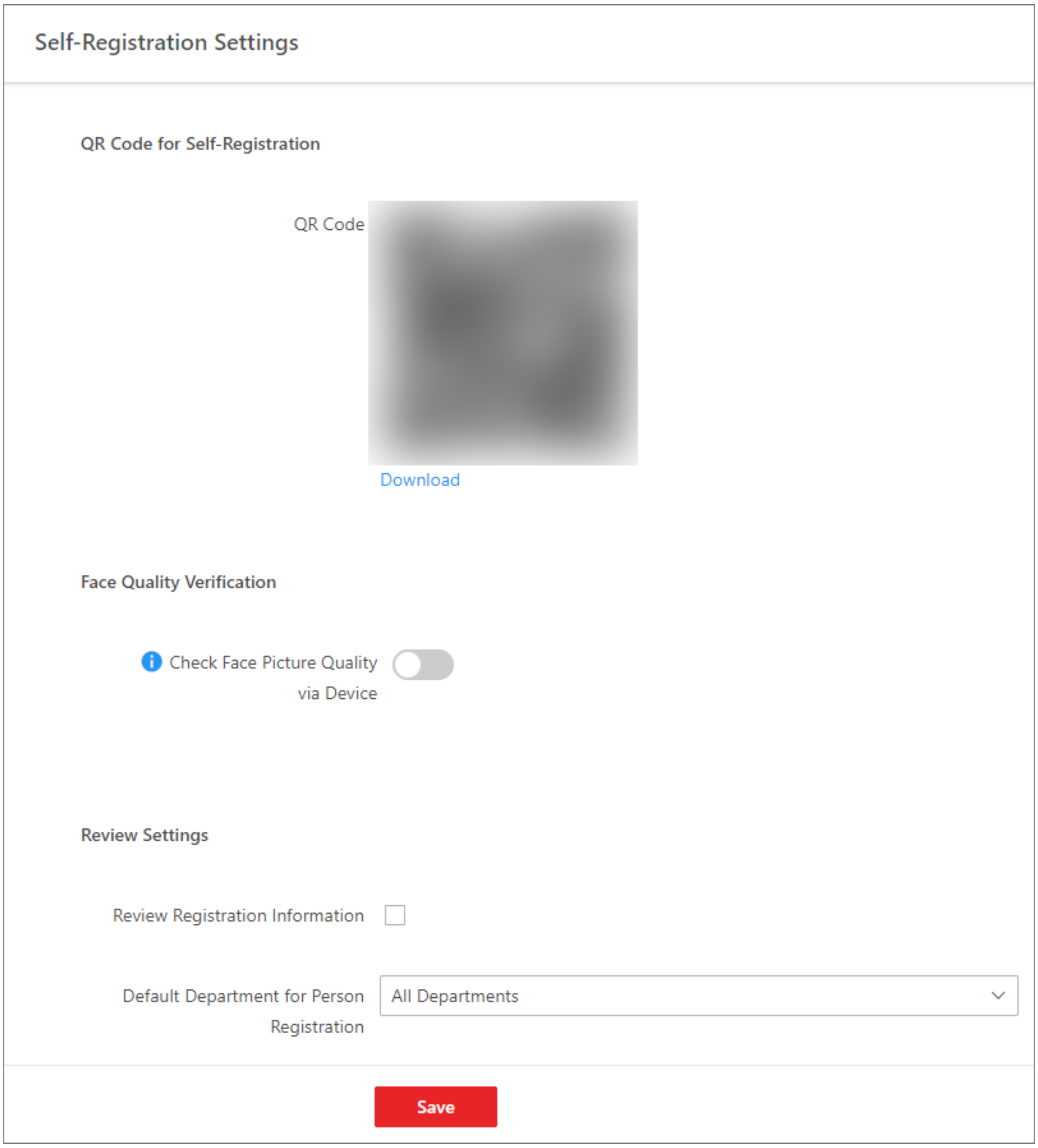


Figure 8-5 Self-Registration Settings

QR Code for Self-Registration

The platform will generate a QR code for you to download. After downloading the QR code, you can print it or send it to persons who are going to register.

Face Quality Verification

After the person uploads profile by a cellphone, the selected device will automatically start checking the profile's quality. If the profile picture is not qualified, the person will be notified. Only when the uploaded profile is qualified can the person register successfully. Otherwise, the person's information cannot be uploaded to the platform.

Note

To use this function properly, make sure you have added an access control device or video intercom device to the platform beforehand.

Review Self-Registered Persons

Set a default department. Once the person information is registered, the person will be added to this group.
If you enable **Review Self-Registered Persons**, after registration, you need to review the person information on the Persons to be Reviewed page. After verification, the person will be added to the selected department. See ***Review Self-Registered Person Information*** for details about how to review.

8.4.2 Scan QR Code for Self-Registration

If a person needs to register by self-service, the person should use a smart phone to scan the self-registration QR code to enter the Self-Registration page and enter person information. After registration, the person details will be uploaded to the platform for review.

Before You Start

The administrator can print the QR code or send the QR code to persons to scan. See ***Set Self-Registration Parameters*** about how to generate a self-registration QR code.

Steps

1. Use your smart phone to scan the self-registration QR code to enter the Self-Registration page.
2. Tap the profile frame to upload a face picture.

   Note

   - You can select a picture from your phone album, or take a photo by phone.
   - After uploading a profile, profile quality checking will automatically start. If the profile is not qualified, you will be notified. Only when the uploaded profile is qualified can you register successfully. Otherwise, your personal information cannot be uploaded to the platform. See ***Set Self-Registration Parameters*** for details about setting Face Quality Verification function.
3. Set your personal information, including name, ID, email, phone number, etc.
4. Enter the verification code.
5. Tap **Save**.
   - If **Review Self-Registered Persons** function is enabled, wait for the review. If you are approved, you will be added to the platform. See ***Review Self-Registered Person Information*** about how to review.
   - If **Review Self-Registered Persons** function is disabled, the person information will be uploaded to the platform.

8.4.3 Review Self-Registered Person Information

If you have enabled **Verify Registration Information** function when you set self-registration parameters, after the persons registered, their person information will be displayed on the Persons to be Reviewed page, and their status will be displayed as **To be Reviewed**. You should review their personal information to approve. After approving, they will be added to the target department.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Then select **Person Management** → **To Be Reviewed** on the left panel to enter the Persons to Be Reviewed page.
3. **Optional:** Click to filter registered persons by name, ID, or status to quickly find your wanted persons.
4. Review the displayed person information and verify them.

Operations	Description
Approve Self-Registered Person Information	If the self-registered person information is correct, approve the information to add the registered persons into the platform. • Select a registered person, and click to approve the person. • Check multiple registered persons, and click **Approve** to approve them all.
Reject Self-Registered Person Information	If there is something wrong or missing with the self-registered person information, reject the person and tell the person to register again with right information. • Select a registered person, and click to reject the person. • Check multiple registered persons, and click **Reject** to reject them in a batch.
Delete Self-Registered Person Information	• Select a registered person, and click to delete the person from the Persons to be Reviewed list. • Check multiple registered persons, and click **Delete** to delete them all from the Persons to be Reviewed list.
Self-Registration Settings	Click **Self-Registration Settings**, jumping to enter the Self-Registration Settings page to set self-registration parameters. **Note** For details, refer to ***Set Self-Registration Parameters*** .

Note

Approved persons will be added to the target department; rejected persons will not be added to the target department, but they will stay in the Persons to be Reviewed list.

8.5 Card Management

8.5.1 Batch Issue Cards to Persons

The platform provides a convenient way to batch issue cards to multiple persons.

Steps

Note

- Up to 5 cards can be issued to one person.
- You cannot issue cards to persons who have temporary cards.

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. Select persons to whom the cards will be issued.
4. Move the cursor onto **Card**, and then click **Batch Issue Cards to Persons**.
5. In the pop-up window, set the related parameters.

   Note

   For details about setting the card issuing mode and parameters, refer to ***Set Card Issuing Parameters*** .
6. Issue one card to one person according to the issuing mode you select.
   - If you set the issuing mode to **Card Enrollment Station**, place the card on the card enrollment station. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you set the issuing mode to **Card Reader**, swipe the card on the card reader. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you set the issuing mode to **Enrollment Station**, place the card on the enrollment station. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you set the issuing mode to **Enter Manually**, enter the card number manually in the Card Number field. Press **Enter** key on the keyboard to issue the card to the person.

     Note

     You can check **Auto Increment Card Number** and enter a start card number to issue cards with incremental numbers to the selected persons in the list.
7. Click **Start** to start issuing cards.
8. Repeat step 5 to issue the cards to the persons in the list in sequence.

   Note

   You cannot change the card issuing mode once you issue one card to one person.
9. Click **Save**.

Set Card Issuing Parameters

HikCentral Professional provides multiple modes for issuing cards, including reading card numbers via devices (card enrollment stations, enrollment stations, or card readers)(card enrollment stations or enrollment stations) and manually entering card numbers.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. Open the card issuing settings window when managing credentials or batch issuing cards to persons.
   - Open the window when managing credentials.
   - Open the window when batch issuing cards to persons.
   - Open the window when filtering persons in the person list.
4. Select an issuing mode and set the related parameters.

   Card Enrollment Station

   Connect a card enrollment station to the PC on which the Web Client runs. You can place the card on the card enrollment station to get the card No.

   If you select this mode, you should set the card format and card encryption function.

   Card No. Type

   If the card type is Wiegand card, select **Wiegand**. If not, select **Normal**.

   Reading Frequency

   If your card supports dual frequency (both IC and ID), select **Dual**. If not, select **Single**.

   Note

   If you select **Dual**, you cannot set card encryption for the card.

   Card Encryption

   If you set **Normal** as the card No. type, you can enable the card encryption function and select section(s) to be encrypted for security purpose. After enabled, you should enable the card encryption in the access control device's configuration page to make card encryption effective.

   Audio

   Turn on or turn off the audio.

   Enrollment Station

   You can enroll the card number remotely via the enrollment station and copy back to the platform.

   If you select this mode, you should set the required parameters below.

   Access Mode

The access mode of the enrollment station. Click **Network** or **USB** from the dropdown list.

Access Protocol

The access protocol of the enrollment station. By default, the access protocol is SDK.

Device Address

The IP address of the enrollment station.

Device Port

The port number of the enrollment station.

User Name

The user name used to log in to the enrollment station.

Password

The password used to log in to the enrollment station.

Card Format

If the card is Wiegand card, select **Wiegand**. If not, select **Normal**.

RF Card Type

Select the needed card type(s), including EM card, M1 card, etc.

Note

When selecting **M1 Card**, you can switch on **Card Encryption** and select section(s) if needed.

Card Reader

Select one card reader of one access control device added to the platform. You can swipe the card on the card reader to get the card number.

Note

- One card reader can be selected for issuing cards by only one user at the same time.
- If you set a third-party card reader to read the card number, you should set the custom Wiegand protocol for the device to configure the communication rule first.

Enter Manually

Note

This parameter is not available on the card issuing settings window opened when managing credentials and filtering persons in the person list.

If you select this mode, you need to manually enter the card number. You can check **Auto Increment Card Number** to enter a start card number to issue cards with incremental numbers to the selected persons in the list

5. Click **Save** (for Credential Management) or **Start** (for Batch Issue Cards to Persons).

8.5.2 Print Cards

After adding persons to the platform, you can print their information onto blank physical cards. If you have set credential information (e.g., virtual card information) for the persons, the credential information will be linked to the physical cards once the physical cards are printed. For example, in the scenario of employee management, you can print physical cards as the employee ID badges, which can be used by your employees as the credentials for access authentication at the access points of your company.

Before You Start

- Make sure you have added the supported printers to the platform.
- Make sure you have added card templates to the platform.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. **Optional:** Set conditions to search for the target persons.
4. Select the persons for whom you need to print cards.
5. Click to open the Print Card window.

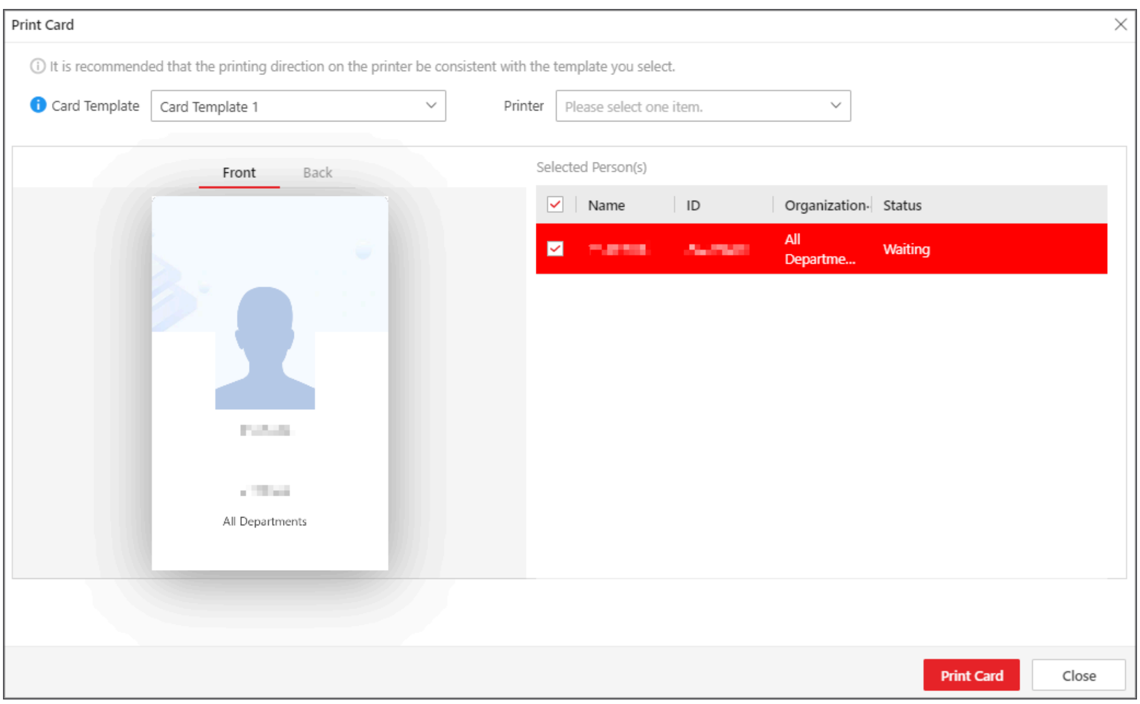


Figure 8-7 Print Card Window

6. Select a card template from **Card Template**.
7. Select a printer from **Printer**.
8. Select person(s) from the Selected Person list.

9. Click **Front** and **Back** to preview the information to be printed on the front and back of the physical cards.
10. Click **Print Card**.

What to do next

If you have not manually added card information for the persons, batch issue card information to them. Otherwise the persons cannot use the physical cards for access authentication. See ***Batch Issue Cards to Persons*** for details.

Related Information Add a Single Person

8.5.3 Report Card Loss

If a person cannot find her/his card, he/she should contact the card issuer as quickly as possible and the card issuer should report card loss via Web Client immediately to freeze the access level of the lost card. The card issuer can issue a temporary card with effective period and access level to the person. When the card is found, the card issuer need to take back the temporary card and cancel the card loss report, and then the found card will be active again.

Report Card Loss

If a person cannot find her/his card, you can report card loss via the platform to freeze the access levels related to the card.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. **Optional:** On the Filter pane, click and set more conditions to search for persons for whom you want to report card loss.
4. Click the name of the person in the person list to enter the basic information page, and then click **Credential Management** to expand the Add Credential panel.

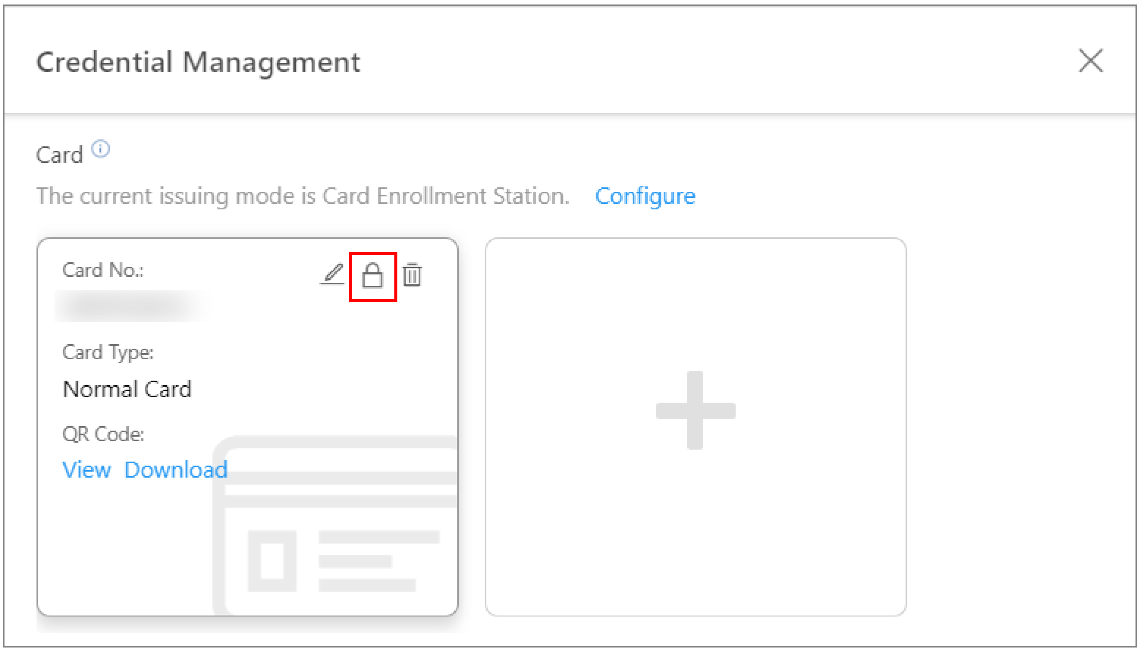


Figure 8-8 Add Credential Panel

5. In the Card area, move the cursor onto the lost card and then click .
6. Click **OK** to confirm the operation.
7. Click **Save**.

   After you report card loss, the access levels of the lost card will be inactive.
8. **Optional:** Move the cursor onto the lost card and then click to cancel the card loss report.

   Note

   You need to delete all the temporary cards before you can cancel the card loss report.

   The card's access level will be active and the original biometric credentials (such as fingerprints and face information) will be linked to this card again.
9. **Optional:** Select the persons in the person list, move the cursor onto on the top, and then click **Report Loss** on the top to batch report loss of multiple cards.

Issue a Temporary Card to a Person

If a card is reported as loss, you can issue a temporary card to the person who loses the card. Once the temporary card is issued, other cards linked to this person will be inactive, and the biometric credentials(such as fingerprints and profile) linked to these inactive cards will be transferred to this temporary card.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.

3. **Optional:** On the Filter pane, click and set more conditions to search for the person to whom you want to issue the temporary card.
4. Click the name of the person in the person list to enter the basic information page.
5. Click **Credential Management** to open the Credential Management pane.
6. In the Card area, click .
7. Click **OK** to confirm the operation.
8. Enter the card number.
9. Set the expiry date to define the time when the temporary card becomes invalid.

Note

The expiry date of the temporary card should be within the effective period of the person (card owner). In other words, the expiry date cannot be later than the effective period. For details about setting or editing the person's effective period, see ***Add a Single Person*** .

10. Click **Save**.

Note

You can delete the temporary card for the person. Once the temporary card is deleted, the inactive cards of the person will restore to the active status, and their previously linked person information such as fingerprints will also restore.

11. Perform the following operation(s) if needed.

Edit the Temporary Card	Move the cursor onto the temporary card, and then click to edit the temporary card.
Delete the Temporary Card	Move the cursor onto the temporary card, and then click .

Batch Cancel Card Loss

If the lost cards are found, you can batch cancel the card loss reports for multiple persons. After that, the cards' access levels will return to be active and the original biometric credentials (such as fingerprints and face information) will be linked to these cards again.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. **Optional:** On the Filter pane, click and set more conditions to search for the persons for whom you want to cancel card loss reports.
4. Select the persons in the person list.
5. Move the cursor onto , and then click **Cancel Card Loss**.

   The persons' temporary cards will be deleted.

8.6 Resigned Persons Management

You can manage resigned persons by adding, deleting, and editing resigned persons. You can also reinstate resigned persons and export resigned person information.

8.6.1 Add Resigned Persons

You can add one or multiple resigned persons, delete and export the resigned person information.

Steps

1. Select **Person Management → Resigned** on the left.
2. Click **Add** to open the Add Resigned Person pane.
3. Click to select one or multiple persons from the departments.

Note

- You can enter specific person name, department, or person ID click **Search** to filter the person information.
- You can check **Include Sub Department** for displaying the person in sub departments.
- You can check **Select All Persons** to select all matched persons.

4. Specify the following parameters.

Departure Date

Last day of the current employment.

Departure Type

Cause of the departure.

Note

You can click **Add Departure Type**, enter the departure type and click **Add** to customize the type. For details, see ***Manage Resignation Types*** .

5. **Optional:** Specify the departure reason.
6. Click **OK**.

Note

You can also adjust the person's status as resigned in Person Management module. See details in ***Add a Single Person*** and ***Batch Add Persons by Template*** .

For persons to be resigned, their permissions of access and vehicles, and credentials such as the card, fingerprint, face picture, iris data will be deleted at the day of resignation.

7. Perform the following operations.

Operation	Description
Edit Resigned Person	Select a person and click in the Operation column to edit the resignation information.

Filter Resigned Person	Click to expand the conditions, set the filter conditions and click **Filter** for filtering the resigned persons.
Export Resigned Person	Click **Export** to export the resigned person information in the current page according to the filter conditions.
Delete Resigned Person	Select one or multiple persons and click **Delete** to delete them.
Set Column Width	Click to select **Complete Display of Each Column Title**/**Incomplete Display of Each Column Title** to set the column title width.
Custom Column Item	Click and select the needed column items to display. You can also click **Reset** to reset to the default column items.

8.6.2 Reinstate Persons

You can reinstate persons who are resigned and to be resigned.

Steps

1. Select **Person Management → Resigned** on the left.
2. Select one or multiple persons and click **Reinstate**.
3. On the pop-up, select the department to which the person(s) will be reinstated, and click **Reinstate**.
   - After the person reinstatement, you can view the related persons in the person list.
   - After the reinstatement, the resigned persons need to upload their credentials, such as face picture, fingerprint, and iris data. Their access levels will be accordance to that of their departments.

8.6.3 Manage Resignation Types

If the default resignation types do not meet your needs, you can add other resignation types.

On the top navigation bar, select → **Basic Management → Person** .

Select **Basic Configuration → Resignation Type** on the left.

- Click **Add**, enter the departure type name, and click **Add** in the pop-up window to customize the type.
- Click in the Operation column to edit the added departure type.
- Click or **Delete** to delete the selected departure type(s).

Note

- The default types (dismiss, departure, redeployment, and suspension with pay) cannot be deleted or edited.
- Up to 100 departure types can be added.

8.7 Approval Management

The platform supports configuring approval flows for departments, attendance groups, persons, positions, and visitors. The approval flow defines the approval process of department / attendance group / personal / position / visitor applications. When configuring approval flows, you can specify application departments, applicants, reviewers, and persons to be notified of the review results via configuring approval roles. Applications from specified departments / attendance groups / persons / position / visitor need to be reviewed according to the configured approval flow.

The priority of different approval flow: personal approval flow > position approval flow > attendance group approval flow > department approval flow.

8.7.1 Add an Approval Role

Approval roles are for specifying reviewers and persons to be notified of review results. You can add approval roles and assign them to persons. Persons assigned with the approval role that is defined as the reviewer have the permission to approve/reject applications of specified departments / attendance groups / persons / positions / visitors, and persons assigned with the approval role that is defined to be notified have the permission to receive and view review results.

Before You Start
Make sure the current admin user has the permissions for configuring approval roles.

Steps

1. On the top left, select → **Basic Management → Person** .
2. Select **Review Management → Approval Role** on the left.
3. Click **Add** to open the Add Role pane.
4. Create a name for the approval role.
5. Click to open the person selection pane.

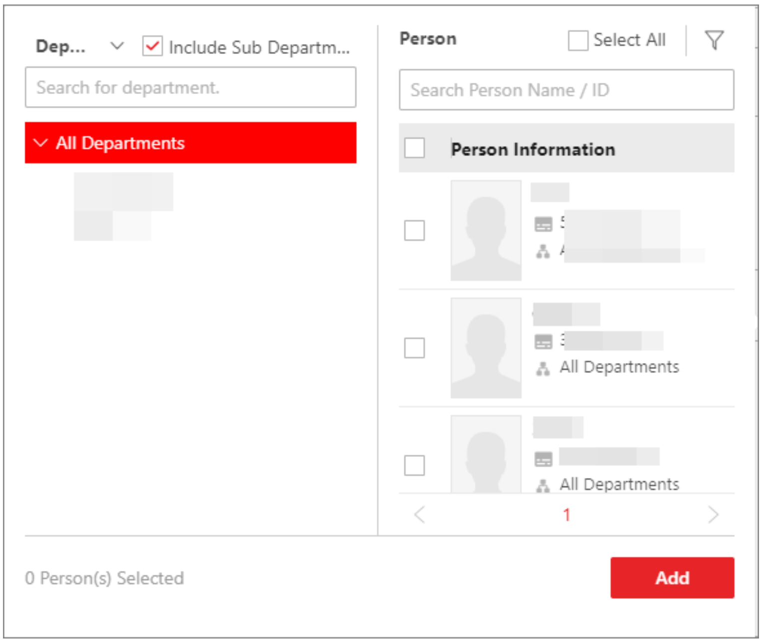


Figure 8-9 Select Person Pane

1) At the top of the left tree, click ⌄ to select **Department** or **Attendance Group** to show all the selectable departments or attendance groups.

Note

If **Department** is selected, you can check **Include Sub Department** to display persons of sub-departments.

2) Select a department or an attendance group to display the linked person(s) on the right.
3) Check the person(s) select the person(s) to assign the approval role to.

Note

You can check **Select All** at the top of the right, or enter keywords to search for persons, or click to filter persons by the position or additional information.

6. Click **Add** to finish adding the approval role.
7. **Optional:** Perform the following operations as needed.

Edit Approval Role	Select an approval role in the list and click to edit it.
Delete Approval Role	• Select one or multiple approval roles in the list and click **Delete** to delete the approval roles. Also, you can click **Delete All** to delete all approval roles. • Select an approval role from the list, and click to delete it.
Assign Approval Role to More Persons	Select an approval role in the list, and click **Assign To** on the right pane to select persons to assign the approval role to.

Unassign Approval Role	Select an approval role in the list, and select the person(s) on the right pane, and click **Unassign** to unassign the approval role for the selected person(s). Also, you can click **Unassign All** to unassign the approval role for all persons.

8.7.2 Add a Department Approval Flow

Department approval flow defines the approval process of reviewing applications from a department. Applications of the persons in the specified application department should be reviewed according to the department approval flow.

Before You Start

- Make sure the current admin user has the permissions for configuring the approval flow.
- Make sure you have added roles of the approval flow. For details about adding roles, refer to ***Add an Approval Role*** .

Steps

1. On the Approval Flow page, move the cursor on **Add**, and click **Department Approval Flow**.
2. On the left, set the basic information of the approval flow.
   1) Enter the name of the approval flow.
   2) Set the start time and end time of the validity time period.
   3) Select the application type (leave, check in&out correction, overtime, and check in&out via Mobile Client).
   4) **Optional:** Switch off **Enable Approval Flow** to disable the approval flow.

Note

The approval flow is enabled by default.

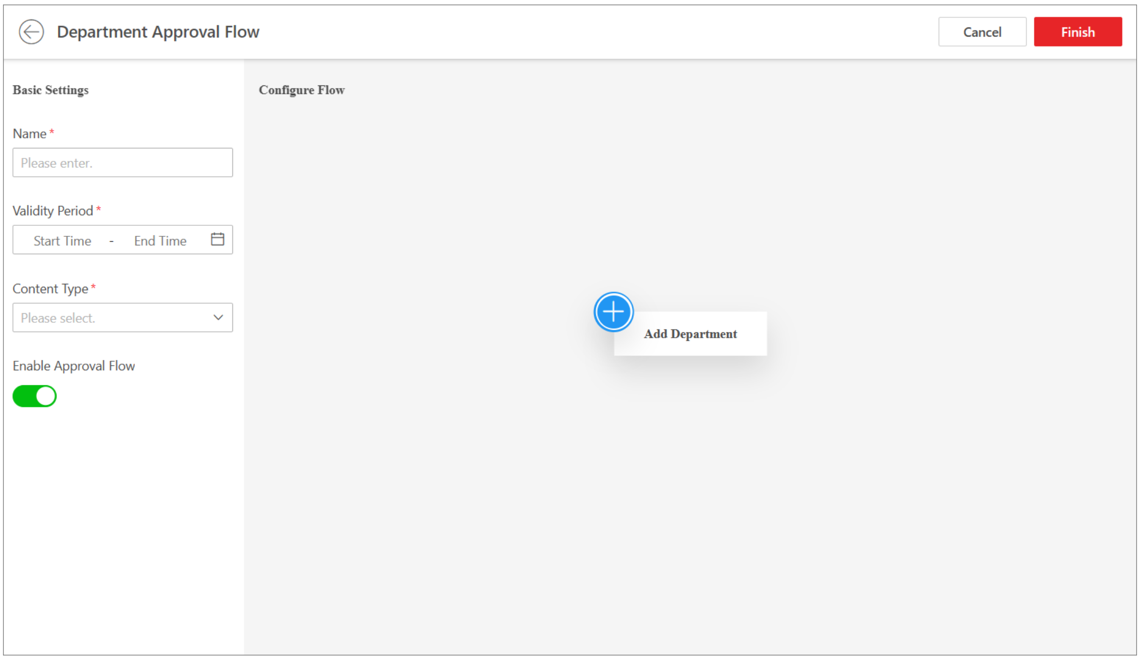


Figure 8-10 Add Department Approval Flow

3. Click **Add Department** to select the application department(s).
4. Click to add the reviewer(s) for the approval flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department(s) of the selected role(s) allowed to review applications.

      Note

      If the reviewers are from the different department, you need to select **All Departments**.

   3) **Optional:** Select the approval role(s) to be notified of the review results in the current node.
   4) **Optional:** Select the department(s) of the approval role(s) to be notified.

      Note

      If the person(s) to be notified are from the different department, you need to select **All Departments**.

   5) Click **Add**.

   Note

   You can repeat this step to add more reviewers and persons to be notified for the approval flow.
5. Click **Finish**.

   The approval flow will be added to the approval flow list.
6. **Optional:** Perform the following operations as needed.

Edit Approval Flow	In the approval flow list, click the name of the approval flow to edit it.

	• Click **Reviewer** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete the node of the approval flow.
Disable Approval Flow	When adding an approval flow, it is enabled by default. You can disable it in the approval flow list.
Delete Approval Flow	In the approval flow list, you can click **Delete** to delete an approval flow, or click **Delete All** to delete all approval flows.
Filter Approval Flow	On the upper-right corner, click , specify conditions such as person name, approval flow type, or content type, and click **Filter** to filter the approval flows.

8.7.3 Add an Attendance Group Application Flow

Attendance group application flow defines the approval process of reviewing applications of an attendance group. Applications of the persons in the specified attendance group should be reviewed according to the group application flow.

Before You Start

- Make sure the current admin user has the permission for configuring the application flow.
- Make sure you have added roles of the application flow. See ***Add an Approval Role*** .

Steps

1. On the Approval Flow page, move the cursor on **Add**, and click **Attendance Group Approval Flow**.
2. On the left, set the basic information of the approval flow.

   Content Type

   Select what employees can apply for.

   Note

   The flow is enabled by default.

3. Click **Add Attendance Group** to select the attendance group(s).
4. Click to add the reviewer(s) for the application flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department range from which the applications can be reviewed by the selected approval role(s).

   Note

   If the reviewers are from different departments, you need to select **All Departments**.

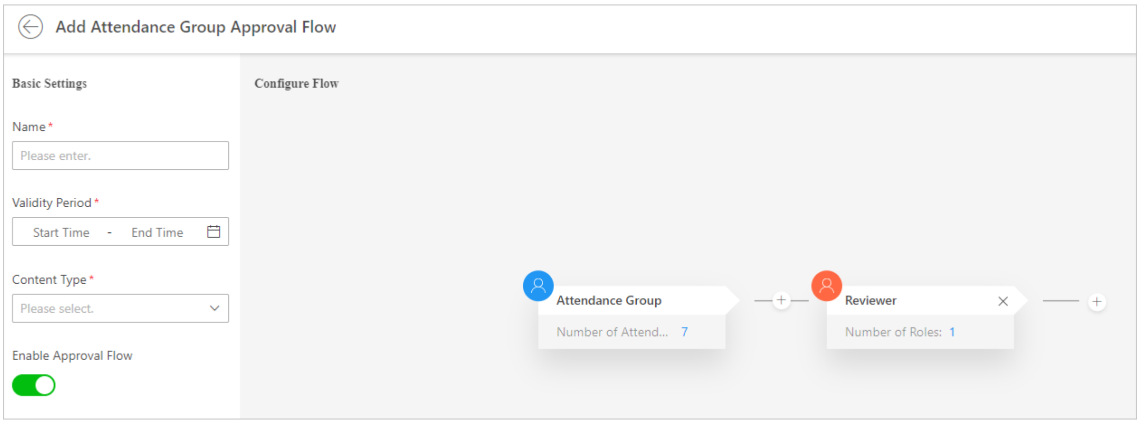


Figure 8-11 Add Attendance Group Application Flow

3) **Optional:** Select the approval role(s) to be notified of the review results.
4) **Optional:** Select the department range from which the approval role(s) will be notified.

Note

If the person(s) to be notified are from different departments, you need to select **All Departments**.

5) Click **Add**.

Note

You can repeat this step to add more reviewers and roles to be notified for the application flow.

5. Click **Finish** on the top right.
6. **Optional:** Perform the following operations as needed.

Edit Application Flow	In the application flow list, click the name of the application flow to edit it. • Click **Reviewer** or **Attendance Group** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete a node of the application flow.
Disable Application Flow	When adding an application flow, it is enabled by default. You can disable it in the application flow list.
Delete Application Flow	In the application flow list, you can click **Delete** to delete an application flow, or click **Delete All** to delete all application flows.

8.7.4 Add a Position Approval Flow

Before You Start

- Make sure the current admin user has the permission for configuring the approval flow.
- Make sure you have added roles of the approval flow. See ***Add an Approval Role*** .

Steps

1. On the Approval Flow page, move the cursor on **Add**, and click **Position Approval Flow**.
2. On the left, set the basic information of the approval flow.

   Content Type

   Select what employees can apply for the approval flow.

   Note

   The flow is enabled by default.
3. Click **Add Position** to select the position(s).
4. Click + to add the reviewer(s) for the approval flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department range from which the applications can be reviewed by the selected approval role(s).

   Note

   If the reviewers are from different departments, you need to select **All Departments**.

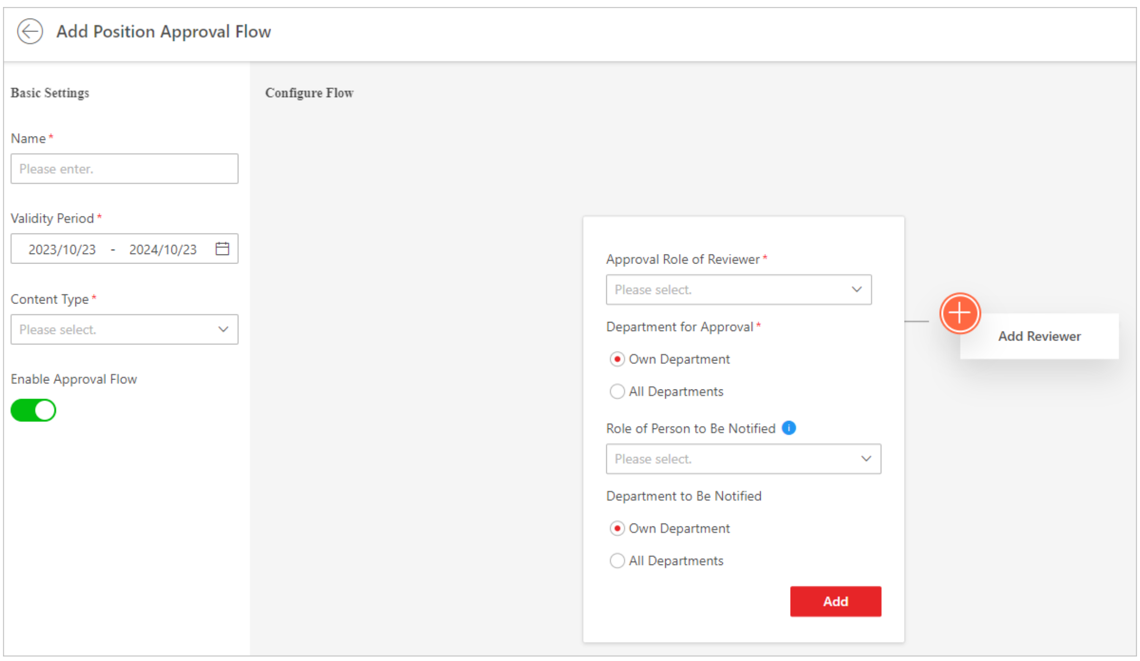


Figure 8-12 Add Position Approval Flow

   3) **Optional:** Select the approval role(s) to be notified of the review results.
   4) **Optional:** Select the department range from which the approval role(s) will be notified.

   Note

   If the person(s) to be notified are from different departments, you need to select **All Departments**.

5) Click **Add**.

Note

You can repeat this step to add more reviewers and roles to be notified for the approval flow.

5. Click **Finish** on the top right.
6. **Optional:** Perform the following operations as needed.

Edit approval flow	In the approval flow list, click the name of the approval flow to edit it. • Click **Reviewer** or **Attendance Group** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete a node of the approval flow.
Disable approval flow	When adding an approval flow, it is enabled by default. You can disable it in the approval flow list.
Delete approval flow	In the approval flow list, you can click **Delete** to delete an approval flow, or click **Delete All** to delete all approval flows.

8.7.5 Add a Personal Approval Flow

Personal approval flow defines the approval process of reviewing applications of a person. Applications of the specified persons should be reviewed according to the personal approval flow.

Before You Start

- Make sure the current admin user has the permissions for configuring the approval flow.
- Make sure you have added roles of the approval flow. For details about adding roles, refer to ***Add an Approval Role*** .

Steps

1. On the Approval Flow page, move the cursor on **Add**, and click **Personal Approval Flow**.
2. On the left, set the basic information of the approval flow.
   1) Enter the name of the approval flow.
   2) Set the start time and end time of the validity time period.
   3) Select the application type (leave, check in&out correction, overtime, and check in&out via Mobile Client).
   4) **Optional:** Switch off **Enable Approval Flow** to disable the approval flow.

Note

The approval flow is enabled by default.

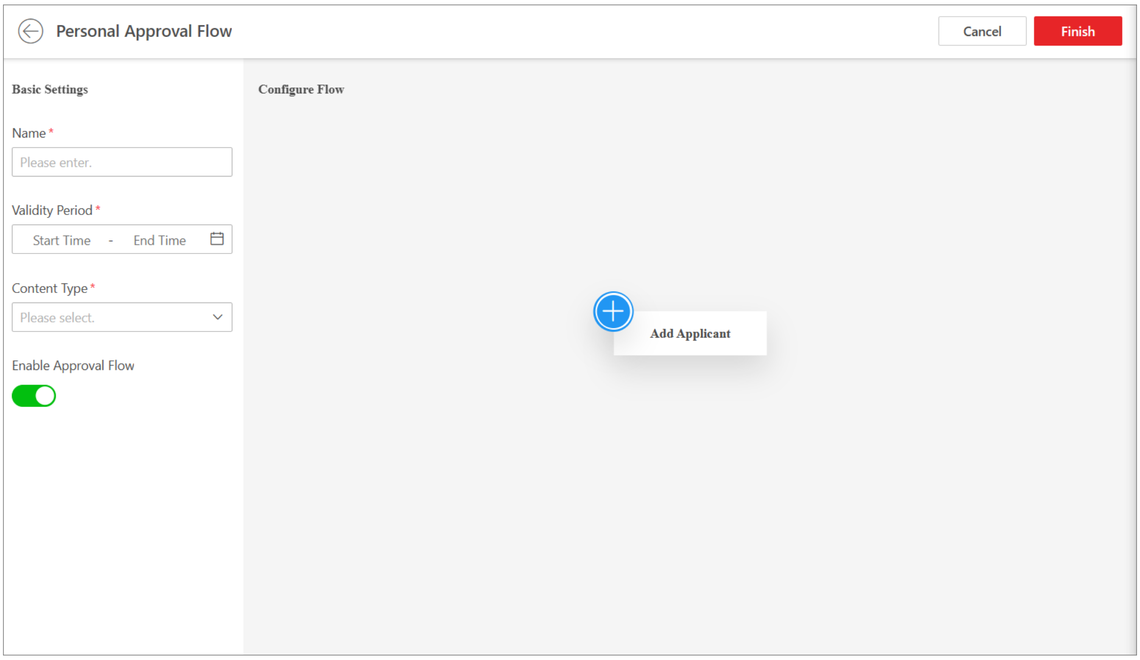


Figure 8-13 Add Personal Approval Flow

3. Click **Add Applicant** and to select the applicant(s).

Note

If you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

4. Click to add the reviewer(s) for the approval flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department(s) of the selected role(s) allowed to review applications.

   Note

   If the reviewers are from the different department, you need to select **All Departments**.

   3) **Optional:** Select the approval role(s) to be notified of the review results in the current node.
   4) **Optional:** Select the department(s) of the approval role(s) to be notified.

   Note

   If the person(s) to be notified are from the different department, you need to select **All Departments**.

   5) Click **Add**.

Note

You can repeat this step to add more reviewers and persons to be notified for the approval flow.

5. Click **Finish**.

The approval flow will be added to the approval flow list.

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

Edit Approval Flow	In the approval flow list, click the name of the approval flow to edit it. • Click **Reviewer** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete the node of the approval flow.
Disable Approval Flow	When adding an approval flow, it is enabled by default. You can disable the flow in the approval flow list.
Delete Approval Flow	In the approval flow list, you can click **Delete** to delete an approval flow, or click **Delete All** to delete all approval flows.
Filter Approval Flow	On the upper-right corner, click , specify conditions such as person name, approval flow type, or content type, and click **Filter** to filter the approval flows.

8.7.6 Add a Visitor Approval Flow

The visitor approval flow defines the approval process of applications from a visitor.

Before You Start

- Make sure the current admin user has the permission for configuring the approval flow.
- Make sure you have added roles of the approval flow. For details about adding roles, refer to ***Add an Approval Role*** .

Steps

1. On the top left, select → **Basic Management → Person** .
2. Select **Review Management → Approval Flow** on the left.
3. Move the cursor on **Add**, and click **Visitor Approval Flow**.
4. On the left, set the basic information of the approval flow.
   1) Enter the name of the approval flow.
   2) Set the start time and end time of the validity time period.
   3) **Optional:** Switch off **Enable Approval Flow** to disable the approval flow.

Note

The approval flow is enabled by default.

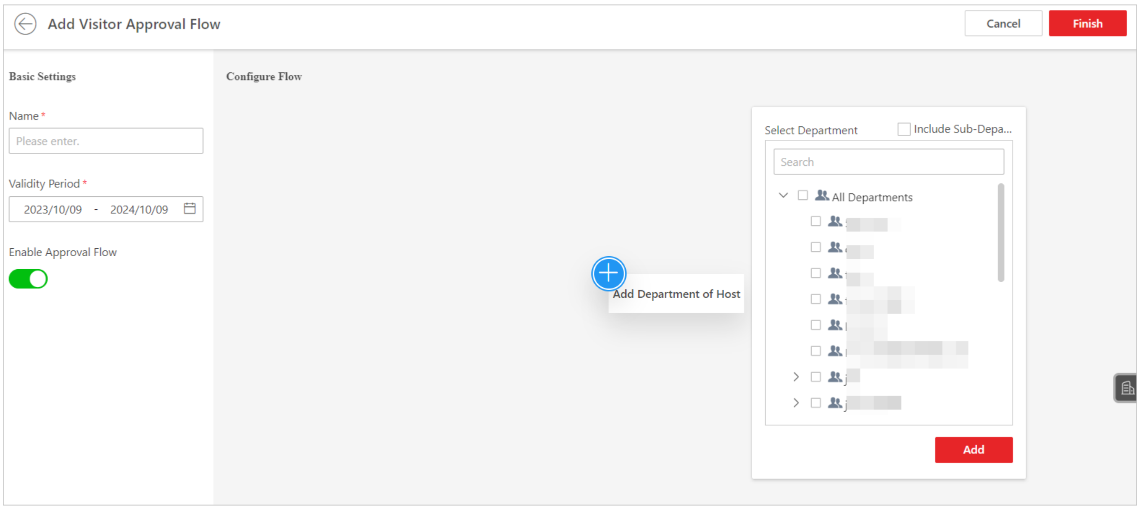


Figure 8-14 Add Visitor Approval Flow

5. Click **Add Department of Host** and select the department(s).
6. Click + to add the reviewer(s) for the approval flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department(s) of the selected role(s) allowed to review applications.

   Note

   If the reviewers are from different departments, you need to select **All Departments**.

   3) **Optional:** Select the approval role(s) to be notified of the review results in the current node.
   4) **Optional:** Select the department(s) of the approval role(s) to be notified.

   Note

   If the person(s) to be notified are from different departments, you need to select **All Departments**.

   5) Click **Add**.

   Note

   You can repeat this step to add more reviewers and persons to be notified for the approval flow.
7. Click **Finish**.

   The approval flow will be added to the approval flow list.
8. **Optional:** Perform the following operations as needed.

Edit Approval Flow	In the approval flow list, click the name of the approval flow to edit it. • Click **Reviewer** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete the node of the approval flow.
Disable Approval Flow	When adding an approval flow, it is enabled by default. You can disable the flow in the approval flow list.

Delete Approval Flow	In the approval flow list, you can click **Delete** to delete an approval flow, or click **Delete All** to delete all approval flows.
Filter Approval Flow	On the upper-right corner, click , specify conditions such as person name, approval flow type, or content type, and click **Filter** to filter the approval flows.

Chapter 9 Vehicle Management

On the Web Client, you can add the vehicle information to the platform, categorize vehicles into different types ((including registered vehicles, temporary vehicles, and vehicles in list), and set rules to define the accuracy when searching for vehicles by license plate number. The managed vehicles can be used in the applications such as ANPR (Automatic Number Plate Recognition) and entrance & exit control.

On the top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.

9.1 Manage Registered Vehicles

A registered vehicle can park in a specific parking lot without paying any fee. To make a vehicle become a registered vehicle, you need to add its information (including the license plate number, vehicle type, etc.) to the platform first, and then you need to link a parking pass to it, so that the vehicle can enter and exit the parking lot as a registered vehicle.

You can perform the following operation(s) after adding registered vehicles.

Operation	Function
Edit a Vehicle	Click a number in the License Plate Number column to edit the vehicle information.
Delete Vehicles	• Check the vehicle(s) and click **Delete** to delete the selected vehicle(s). • Click → **Delete All** beside **Delete** to delete all the added vehicles in different vehicle lists.
Delete Expired Vehicles	Click **Delete Expired Vehicle** to delete all expired vehicles from different vehicle lists.
Filter Vehicles	Click and set conditions to filter specific vehicles. **Note** For the Middle East and North Africa, you can filter vehicles by country/region and plate category.
Export Vehicles	Click **Export All** to save the filtered vehicles or vehicles from all vehicle lists to your PC as an XLSX file, which can be imported to the platform again.

Operation	Function
	Note For the Middle East and North Africa, the exported vehicle information will contain the country/region and plate category.
Edit Effective Period	Select a registered vehicle and click **Edit Effective Period** to edit the effective period for the vehicle.
Custom Column Items	On the top right, click to select column items to be displayed. You can click **Reset** to select again.

9.1.1 Add a Registered Vehicle

You can add the information of one vehicle to the platform as a registered vehicle at one time.

Steps

1. On the left navigation pane, click **Vehicle Management → Registered Vehicle → Vehicle** .
2. In the top left corner of the Vehicle page, click **Add** to enter the Add Vehicle page.

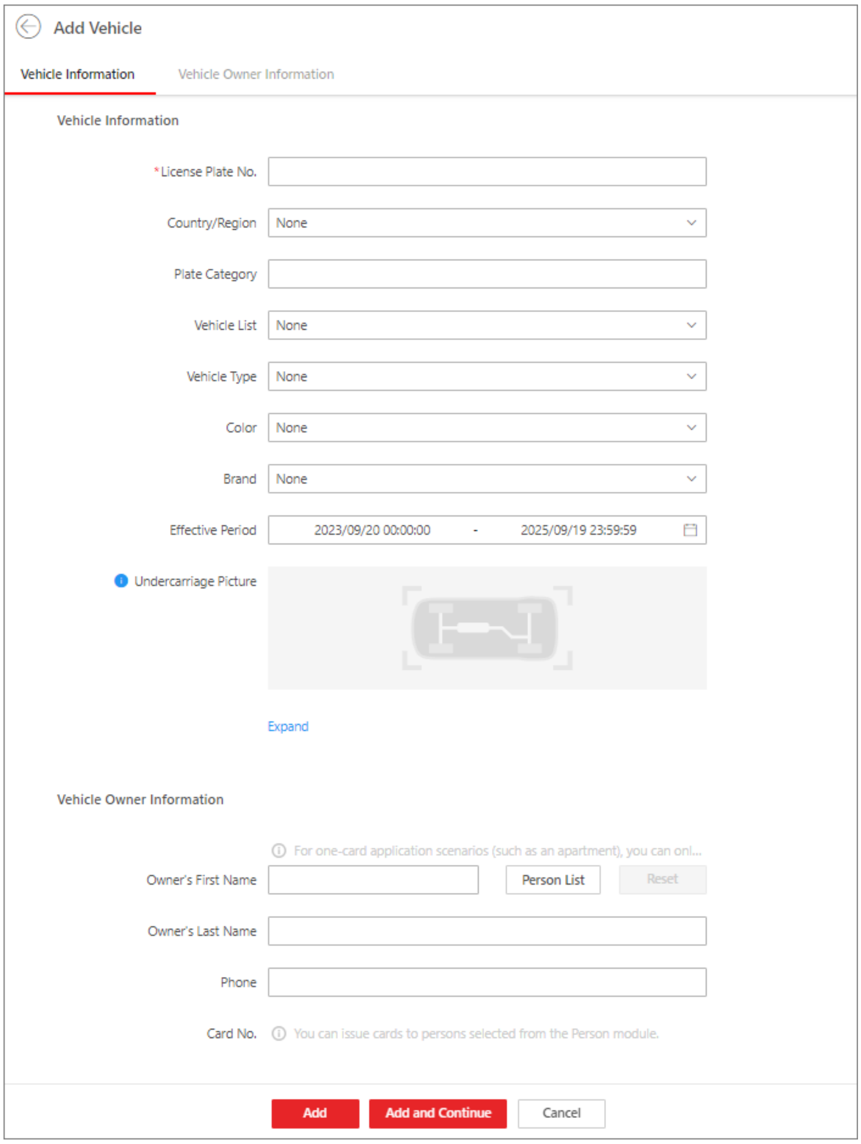


Figure 9-1 Add a Registered Vehicle

3. Set the vehicle information, such as the license plate number, vehicle list, type, color, and brand.

Country/Region, Plate Category

For the Middle East and North Africa, you should select a country or region and enter a plate category for the vehicle.

Note

These parameters will be displayed and configurable only when the area is set to **Middle East and North Africa**. For details about the area settings, refer to ***Customize Vehicle Information*** .

Vehicle List

Select a list that you predefined on the platform from the drop-down list to add the vehicle to. If you have not added any vehicle list to the platform before, you can click **Add** to create a new one. For details, refer to ***Manage Vehicle Lists*** .

Effective Period

Set the effective period for the registered vehicle in applications such as entrance & exit control, to determine the period when the vehicle can enter or exit a parking lot as a registered vehicle.

Undercarriage Picture

Upload an undercarriage picture of the registered vehicle for comparing the captured one to the uploaded one on the Control Client.

Custom Vehicle Information

If you have customized some fields for vehicles, click **Expand** to show the custom fields and fill in the corresponding information.

4. Set the information for the vehicle owner.
   - Enter the owner's first name, last name, and phone number.
   - Click **Person List** to select an existing person as the vehicle owner from a person list and select a card No. (if cards are issued to the person) for the owner to swipe card when entering and exiting the parking lot.

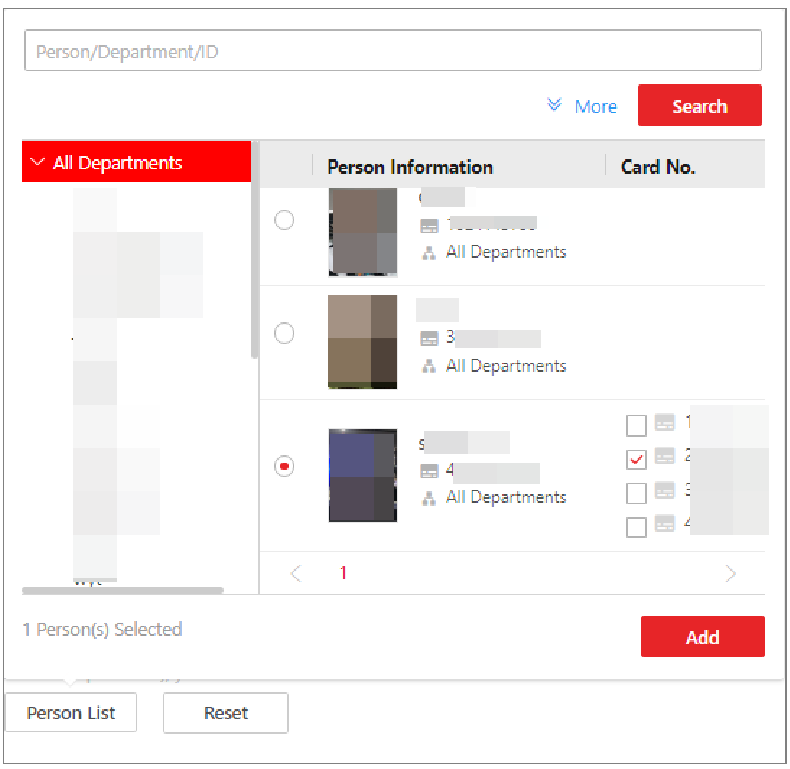


Figure 9-2 Select an Existing Person as Vehicle Owner

Note

- You can also select a person who has been linked to another vehicle.
- On the person list pane, you can enter the person's name, department, or ID to search for a specific person. Or you can click **More** to display persons' additional information fields, enable the field(s), and enter the corresponding keywords to make the search result more accurate.
- For how to add persons and how to issue cards to persons, refer to ***Add a Single Person*** and ***Batch Issue Cards to Persons*** .

5. Set the parking lot entry/exit rule for the vehicle.

Add Parking Lot Entry/Exit Permissions	Click **Parking Lot Entry and Exit Settings** and select parking lots to issue their parking permits to the vehicle. **Note** Under the charge mode, the parking pass top-up is required when you select the pay parking lots.
Edit Effective Time Period of a Entry/Exit Permission	Click **Edit** next to the time period of a parking lot to edit the effective time period of the parking permit.
Cancel Parking Lot Entry/ Exit Permission(s)	Click **Delete** to cancel the parking permit of the parking lot.

6. Click **Add** to add the registered vehicle or click **Add and Continue** to continue adding anther registered vehicle.

Note

If the license plate number already exists (in the current vehicle list or other vehicle lists), a prompt box will be displayed and you can select whether to replace the existing vehicle with the new one.

As only the vehicle with a parking pass can enter and exit the parking lot as a registered vehicle, after adding a registered vehicle, a window will pop up to remind you of topping up a parking pass for the vehicle by clicking **Parking Pass Top-Up**. Or you can click **Return to Vehicle List** and top up a parking pass for the vehicle in the Top-Up Management module later.

9.1.2 Batch Import Registered Vehicles

You can import the information of multiple vehicles to the platform as registered vehicles at one time.

Steps

1. On the left navigation pane, click **Vehicle Management → Registered Vehicle → Vehicle** .
2. In the top left corner of the Vehicle page, click **Import**.

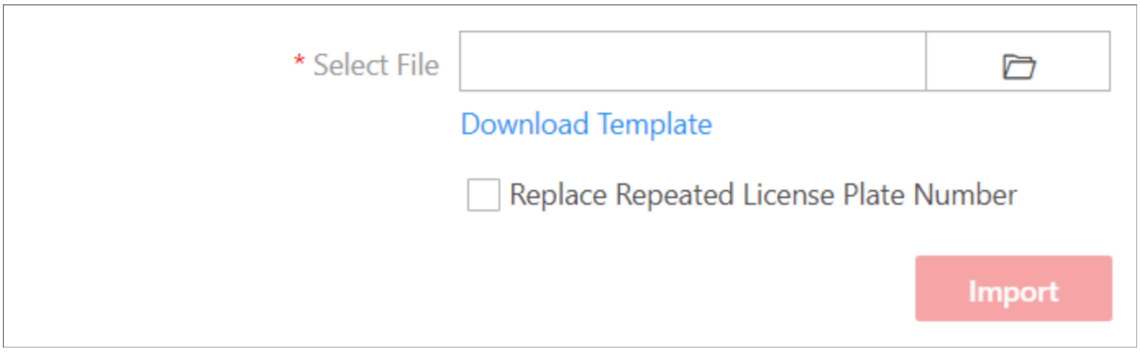


Figure 9-3 Import File

3. Click **Download Template** to download and save the template file to your PC.
4. Open the downloaded template file and enter the required information.
5. Click and select the file.
6. **Optional:** Check **Replace Repeated License Plate Number** to replace the existing vehicle information with the new vehicle information if the file contains the license plate number which has already been added to the platform. Otherwise, the original vehicle information will be reserved.
7. Click **Import**.

What to do next

Only the vehicle with a parking pass can enter and exit the parking lot as a registered vehicle. Therefore, after batch importing vehicles to the platform, you need to link a parking pass to each of them in the Top-Up Management module later.

9.2 Manage Vehicle Lists

A vehicle list can group multiple vehicles so that you can manage them more easily.

Before You Start

Make sure you have selected the vehicle list(s) allowing for further management by the role linked with your account. See ***Add Role*** for details on permission settings.

Steps

Note

Up to 100 vehicle lists can be added.

1. On the top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Vehicle Management** → **Registered Vehicle** → **List Management** .
3. At the top of the left pane, click to open the Add Vehicle List pane.

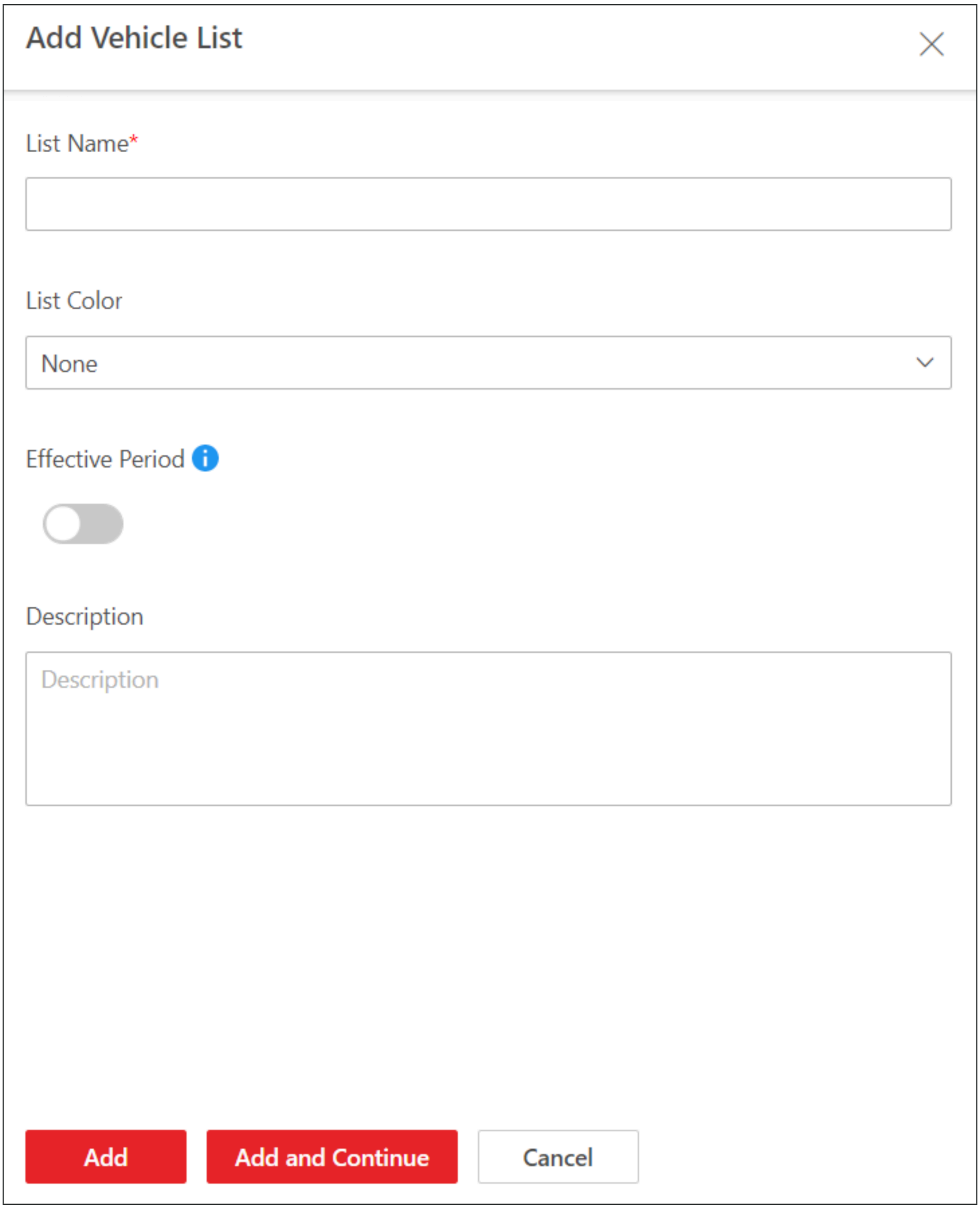


Figure 9-4 Add Vehicle List Page

4. Set the vehicle list's information, including list name, list color, effective period, and description.

Note

- The list color is used to mark different types of vehicle lists.
- If you enable and set the effective period, alarms related to vehicles in the list cannot be triggered and vehicles in the list will not be applied to the allowlist or blocklist after the vehicle list expires.
- When you adds a vehicle to this list later, you do not need to set an effective period for the vehicle, because the vehicle shares the same effective period as that of the vehicle list.

5. Click **Add** to add the vehicle list or click **Add and Continue** to continue adding another vehicle list.
6. **Optional:** Select the added list and click **Add** to search for vehicles to be added to the list.

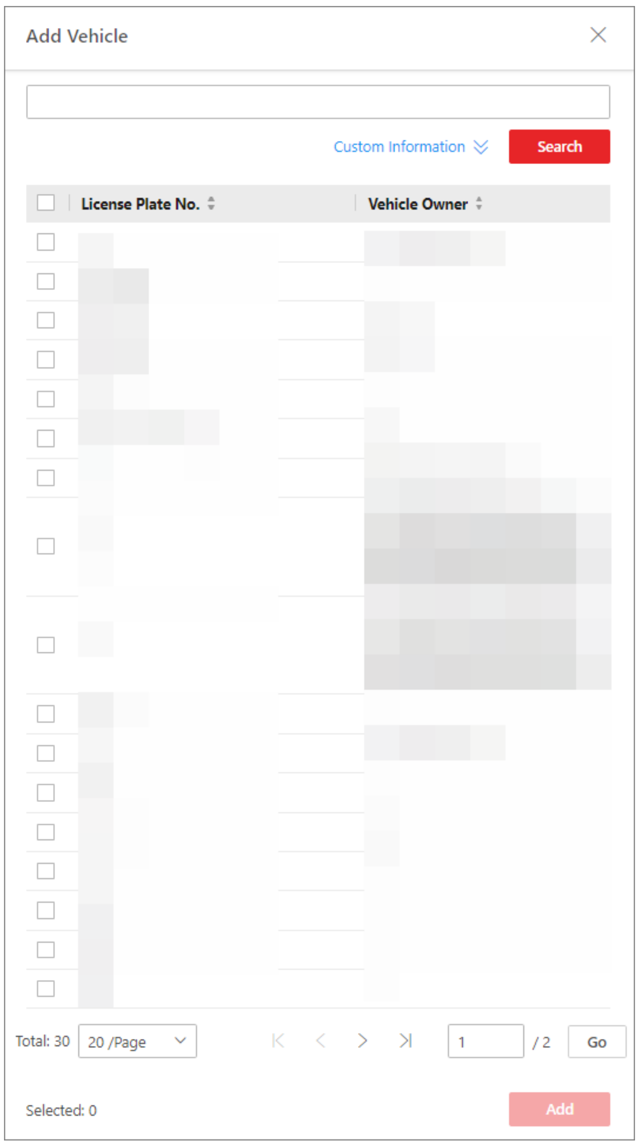


Figure 9-5 Add Vehicles to List

Note

You can enter a keyword to search for vehicles on the Add Vehicle pane. Or you can click **Custom Information** to display vehicles' custom information fields, enable the field(s), and enter the corresponding keywords to make the search result more accurate. For more about the custom vehicle information, refer to ***Customize Vehicle Information*** .

7. **Optional:** Perform the following operation(s) after adding vehicle lists or adding vehicles to lists.

Search for Vehicle Lists	At the top of the left pane, enter a keyword in the search box to search for specific vehicle lists.
Edit a Vehicle List	Select a vehicle list on the left pane and click at the top to edit it.
Apply a Vehicle List	a. Select a vehicle list on the left pane and click at the top to open a pane. b. Enable **Apply List** and select **Allowlist** or **Blocklist** as the list type. c. Select a list to be applied to. d. Click **Save** to apply the select vehicle list as an allowlist or a blocklist.
Delete a Vehicle List	Select a vehicle list on the left pane and click at the top to delete it.
Remove Vehicle(s) from List	• Select a vehicle list on the left pane to show its vehicles, check the vehicle(s), and click **Delete** to remove them from the current list. • Select a vehicle list on the left pane to show its vehicles, click → **Delete All** beside **Delete** to remove all vehicles from the current list.
Move Vehicle(s) to Another List	Select a vehicle list on the left pane to show its vehicles, check the vehicle(s), and click **Move** to move them from the current list to another list.
Export Vehicles in List	Select a vehicle list on the left pane to show its vehicles, and click **Export All** to export vehicles in the current list to the local PC.
Filter Vehicles in List	Select a vehicle on the left pane to show its vehicles, click in the top right corner of the right pane and set conditions to filter specific vehicles in the current list.
Custom Column Items	On the top right, click to select column items to be displayed. You can click **Reset** to select again.

9.3 Filter and Export Visitor Vehicles

If a visitor comes by driving a vehicle, the license plate number will be recorded to the platform so that the platform can control the barrier to open when the capture unit detects this license plate. The recorded vehicles will be displayed in the visitor vehicle list, so you can filter them by multiple conditions and export the vehicle information to the local PC. Once the visitor checked out, the vehicle will be removed from the list.

Steps

1. On the left navigation pane, click **Vehicle Management → Visitor Vehicle** .
2. Click in the top right corner to display the filter pane.

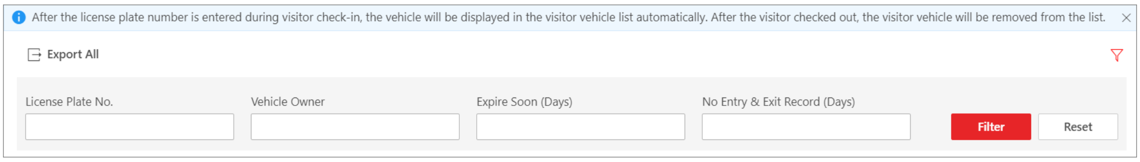


Figure 9-6 Search Visitor Vehicle Page

3. Set the filter condition(s), including license plate number, vehicle owner, expire soon (days), and no entry & exit record (days).

   Expire Soon (Days)

   The days left before the status of the vehicle becomes **Expired**.

   No Entry & Exit Record (Days)

   The number of days during which the vehicle did not enter or exit.
4. Click **Filter**.

   The matched result(s) will be displayed.
5. Click **Export All** to export the filtered vehicles to the local PC.

Note

If you do not filter vehicles before clicking **Export All**, all visitor vehicles will be exported.

9.4 Manage Vehicles in Blocklist

A vehicle added to the blocklist cannot enter the specified region as its license plate number will be recognized at the entrance. When adding a vehicle to the blocklist, the administrator can set a certain period during which the vehicle is not allowed to enter.

You can perform the following operation(s) to manage the blocklist.

Operation	Function
Remove Vehicle(s) from Blocklist	• Select vehicle(s) and click **Delete** to remove the vehicle(s) from the blocklist one by one or in a batch. • Click ⌄ next to **Delete** and click **Delete All** to remove all vehicles from the blocklist.
Export Vehicle Information	Click **Export All** to save the information of all vehicles in the blocklist to the local PC.
Search for Vehicles	Enter a keyword in the search box and click 🔍 to search for vehicles by license plate No., owner's first/last name, phone number, or description.

9.4.1 Add a Vehicle to Blocklist

You can add vehicles to the blocklist one by one. Once added, the vehicle cannot enter the specified region during the period you set.

Steps

1. On the left navigation pane, click **Vehicle Management → Blocklist** .
2. Click **Add** to enter the Add Vehicle to Blocklist page.

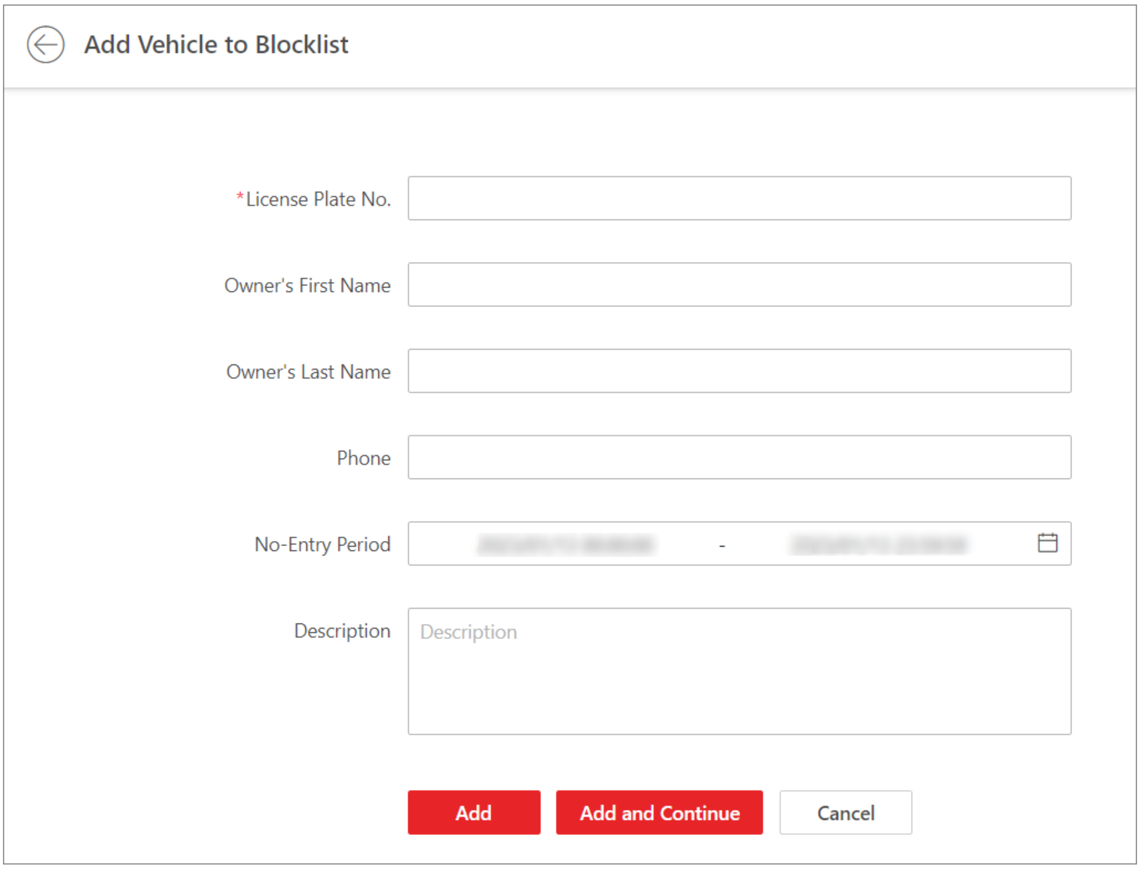


Figure 9-7 Add Vehicle to Blocklist

3. Enter the vehicle's license plate number.
4. **Optional:** Enter the first name, last name, and phone number of the vehicle's owner.
5. Set the period in which the vehicle is not allowed to enter.
6. **Optional:** Enter remarks in the Description field if needed.
7. Click **Add** to finish, or click **Add and Continue** to add another vehicle.

9.4.2 Batch Import Vehicles to Blocklist

You can batch add multiple vehicles to the blocklist. Once added, the vehicles cannot enter the parking lot during the period you set.

Steps

1. On the left navigation pane, click **Vehicle Management → Blocklist** .
2. Click **Import**.

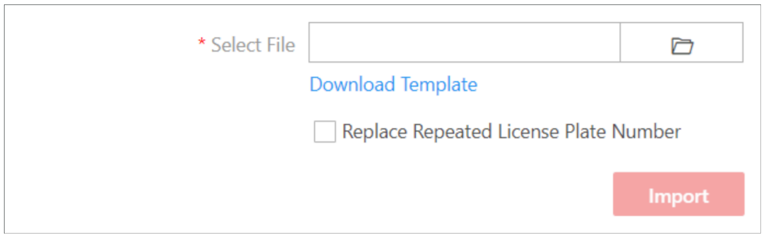


Figure 9-8 Import File

3. Click **Download Template** to download and save the template file to your PC.
4. Open the downloaded template file and enter the required information.
5. **Optional:** Check **Replace Repeated License Plate Number** to replace the existing vehicle information with the new vehicle information if the file contains the license plate number which has already been added to the blocklist. Otherwise, the original vehicle information will be reserved.
6. Click **Import**.

9.5 Customize Vehicle Information

You can customize different items of vehicle information (such as vehicle model) which are not predefined. The customized vehicle information can help to recognize vehicles or search for vehicles more accurately.

Steps

1. On the left navigation pane, click **Vehicle Information**.
2. Add vehicle types.
   1) Click **Add** in the Vehicle Type area to open the Add Vehicle Type pane.

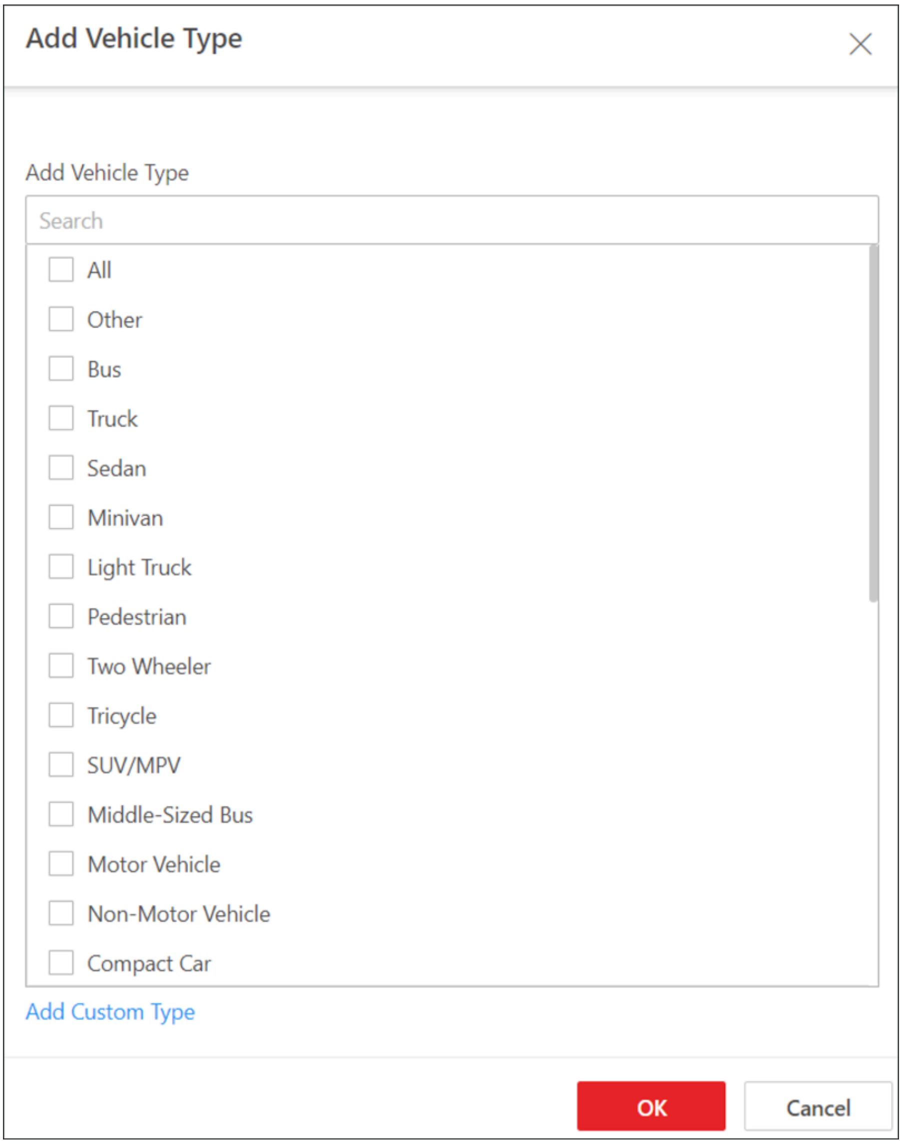


Figure 9-9 Add Vehicle Type

2) Check the vehicle type(s) in the list.

Note

If you cannot find the vehicle type you want in the list, click **Add Custom Type** to customize a vehicle type.

3) Click **OK**.

3. Add the additional information item(s), which can be used as the conditions during the vehicle search.

1) Click **Add** in the Additional Information area to open the following pane.

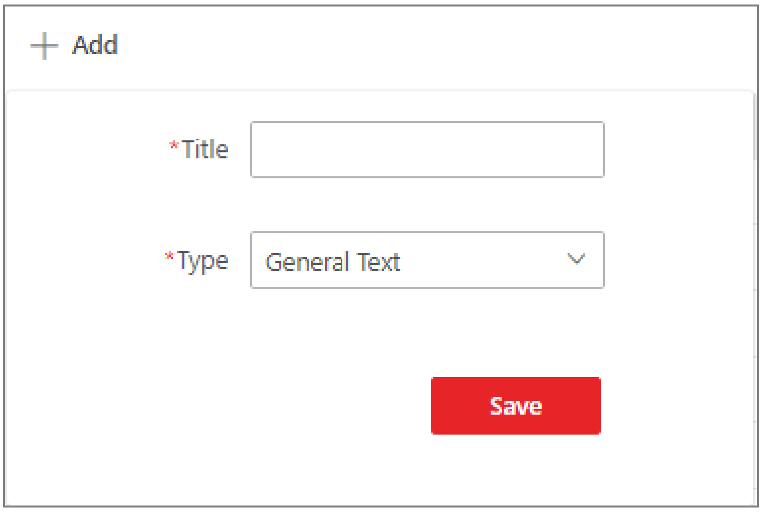


Figure 9-10 Customize Additional Information

2) Create a title for the information.

3) Select an information type.

General Text

The information must be a character string, which contains 1 to 32 characters and excepts certain special characters.

Number

The information must be an integer, which is between 1 to 32.

Date

The information must be in the date format. You should select a start date and an end date from the calendar.

Single Selection

The information must be selected from a drop-down list, whose options are predefined when setting the information type.

4) Click **Save**.

4. Set the area to **General** or **Middle East and North Africa**.

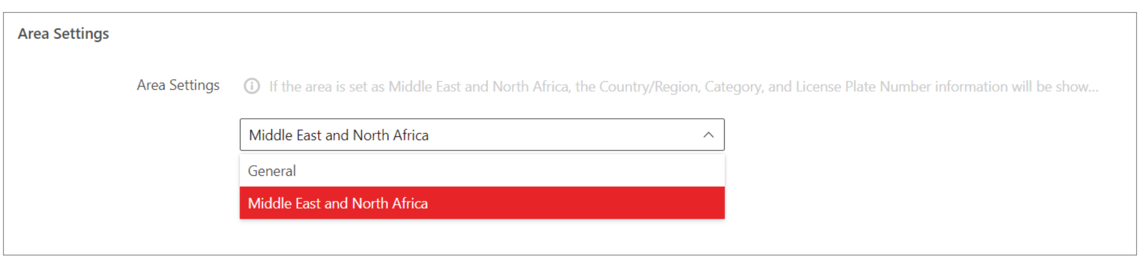


Figure 9-11 Set Area

Note

If the area is set to **Middle East and North Africa**, the country/region and plate category should be configured for vehicles and will be displayed in the vehicle information.

5. **Optional:** Perform the following operation(s) after adding vehicle types or custom items.

Delete a Vehicle Type	Click in the Operation column of a vehicle type to delete it.
Edit a Custom Item	Click in the Operation column of a custom item to edit it.
Delete a Custom Item	Click in the Operation column of a custom item to delete it.

9.6 Configure Fuzzy Matching Rules for License Plate Search

When searching for vehicles by license plate number on the Control Client, the system supports fuzzy matching. You can first set the fuzzy matching rules according to actual needs.

Steps

1. On the left navigation pane, click **Plate Fuzzy Search**.
2. Click **Add**.

Figure 9-12 Add Fuzzy Matching Rule

3. Set the rule.

<=>

Enter an uppercase letter or a digit before and after this symbol respectively.

For example, 0<=>Q means: If you enter 0 or Q for search, the recognized license plate numbers with 0 and the ones with Q will be filtered.

=>

Enter an uppercase letter or a digit before and after this symbol respectively.

For example, G=>6 means: If you enter G for search, the recognized license plate numbers with G and the ones with 6 will be filtered. But if you enter 6 for search, the ones with G will not be filtered.

Note

Up to 16 rules can be added.

4. Click **Save**.
5. **Optional:** Perform the following operations if needed.

Edit Rule	Click in the Operation column of a rule to edit it.
Enable/Disable Rule	Click / in the Operation column of a rule to enable/disable it.
Delete Rule	Click in the Operation column of a rule to delete it.

Chapter 10 Management of Platform Accounts and Security

Assign roles with varying permissions to different users on the platform and configure security parameters and questions to enhance system security.

On the top left corner of Home page, select ■ → **Basic Management** → **Account and Security** .

10.1 Add Role

Role is a group of platform permissions. You can add roles and assign permissions to roles, so that users can be assigned with different roles to get different permissions.

Steps

Note

The platform has predefined two default roles: Administrator and Operator. You can click the role name to view details. The two default roles cannot be edited or deleted.

Administrator

Role that has all permissions of the platform.

Operator

Role that has all permissions for accessing resources and operating the Applications.

1. On the left, select **Roles**.
2. Click **Add** to enter Add Role page.
3. Set the basic information of the role, including role name, effective period, role status, permission schedule template, description, etc.

   Copy From

   Copy all settings from an existing role.

   Permission Schedule Template

   Set the authorized time period when the role's permission is valid. Select **All-day Template**/ **Weekday Template**/**Weekend Template** as the permission schedule of the role, or click **Add** to customize a new permission schedule template.

   Note

   - When role expires or the role's permission is invalid after editing the permission schedule, users assigned with the role will be forced to log out and not able to log in.
   - The permission schedule's time zone is consistent with that of the platform.

- By default, the role will be linked with All-day Template after updating the platform.
- The permission schedule also goes for RSM client and OpenSdk client.

4. Configure permission settings for the role.

   Area Display Rule

   Show or hide specific area(s) for the role. If an area is hidden, the user assigned with the role cannot see and access the area and its resources.

   Resource Access

   Select the functions from the left panel and select resources from right panel to assign the selected resources' permission to the role.

   Note

   If you do not check the resources, the resource permission cannot be applied to the role.

   User Permission

   The role's permission for different operations on the platform.

5. Click **Add** to add the role and return to the role management page, or click **Add and Continue** to save the settings and continue to add another role.

10.2 User Management

10.2.1 Add Normal User

You can add normal users and assign roles to them for accessing the system and assign role to the normal user. Normal users refer to all users except the admin user.

Steps

1. Select **Users** on the left.
2. Click **Add** on the top.
3. Set basic information for the user.

   User Name

   Only letters (a-z, A-Z), digits (0-9), and "-" are allowed.

   Password

   Create an initial password for the user. The user will be asked to change the password when logging in for first time. See ***First Time Login for Normal User*** for details.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers,

and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

Expiry Date

The date when the user account becomes invalid.

Email

The system can notify user by sending an email to the email address. The user can also reset the password via email.

Note

The email address of the admin user can be edited by the user assigned with the role of administrator.

User Status

Active is selected by default. If you select **Inactive**, the user account will be inactivated until you activate it.

4. Configure parameters related to login protection.

Restrict Concurrent Logins

To restrict the number of simultaneous logins for user accounts, switch on **Restrict Concurrent Logins** and set the maximum number of concurrent logins.

Custom Locking of Control Client

Enable this function to disable the user's auto locking of Control Client, or customize the time for auto locking of Control Client.

5. Configure permission settings for the user.

PTZ Control Permission

Set the permission level (1-100) for PTZ control. The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ of a camera.

Assign Role

Select the roles that you want to assign to the user.

Note

If you want to add new roles, click **Add**. See ***Add Role*** for details. Click a role on the list and then **View Role Details** to view the Basic Information and Permission Settings of the role.

6. Do one of the following to complete adding the user.
   - Click **Add** to add the user and return to the user management page.
   - Click **Add and Continue** to save the settings and continue to add another user.
7. **Optional:** Perform further operations on the added normal users.

Edit User	Click user name to view and edit user settings.
Reset Password	Click user name and click **Reset** to set a new password for the user. Enter a new password and click **Reset**. **Note** The admin user can reset the passwords of all the other users (except domain user). Other users with Security permission (in Configuration and Control Permission) can reset the passwords of the users without Security permission. When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral Professional via the Web Client.
Delete User	Select a users and click **Delete** to delete the selected user.
Force Logout	Select an online user and click **Force Logout** to log out the online user.
Inactivate/ Activate User	• The admin user or user with administrator permission can inactivate or activate a user. • Select an active users and click **Inactivate/Activate** to inactivate/activate the user.
Refresh User	Click **Refresh All** to get the latest status of all users.
Filter User	Click to set conditions and filter the users.
Unlock Users	For users whose account is locked due to too many failed attempts for login, Administrators can unlock their accounts for login. On the top of user list, click **Unlock for Login**, check users, and click **Unlock**.

10.2.2 Import Domain Users

You can batch import the users (including the user name, real name, and email) in the AD domain to the platform and assign roles to the domain users.

Before You Start

Make sure you have configured active directory settings. See ***Set Active Directory*** for details.

Steps

1. On the top left corner of Home page, select **→ General → Account and Security → Users** .
2. Click **Import Domain Users**.

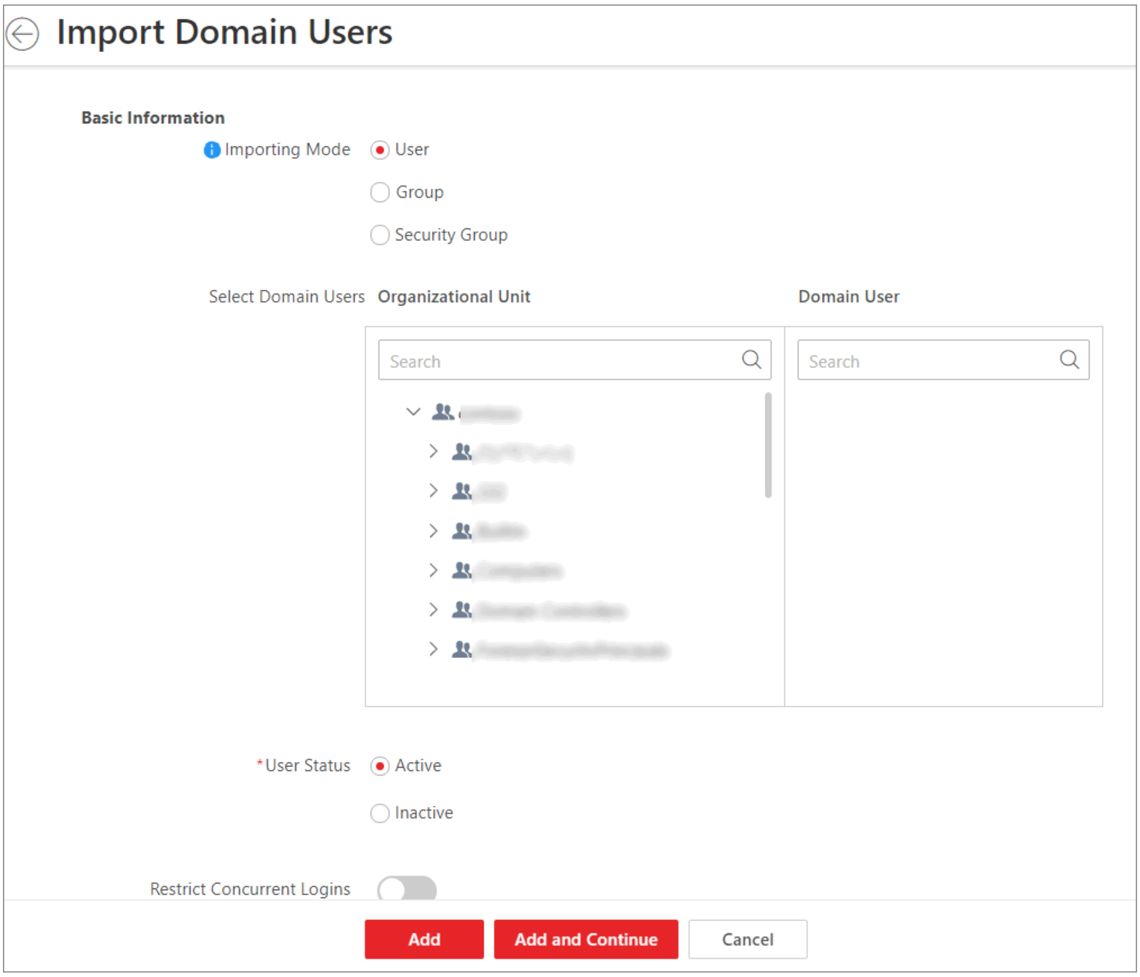


Figure 10-1 Import Domain Users

3. Select an importing mode.

   User

   Import individual users. Select an organization unit and select one or more domain users in this organization unit.

   Group

   Select an organization unit to import all the domain users in this organization unit.

   Note

   The platform does not support this function if the Azure domain is configured.

   Security Group

   Import all the domain users in the security group(s). Select an organization unit and select one or more security groups in this organization unit.
4. Select domain users from active directory.
5. Select the user status as **Active** or **Inactive**.

6. **Optional:** To limit the maximum IP addresses logged in to the platform using the user account, switch on **Restrict Concurrent Logins** and enter the maximum number of concurrent logins.
7. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

Note

The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit.

Example

When two users control the PTZ unit at the same time, the user who has the higher PTZ control permission level takes control of the PTZ.

8. Select the roles that you want to assign to the domain users.

Note

- If no role has been added, two default roles are selectable: administrator and operator.

  Administrator

  The role that has all permissions of the HikCentral Professional.

  Operator

  The role that has all permissions of the HikCentral Professional Control Client.
- If you want to add new roles, you can click **Add New Role**. See ***Add Role*** for details. Click a role on the list and then **View Role Details** to view the Basic Information and Permission Settings of the role.

9. Complete importing the domain users.
   - Click **Add** to import the domain users and return to the user management page.
   - Click **Add and Continue** to save the settings and continue to import other domain users.
10. **Optional:** After importing the domain user information to the platform, if the user information in domain is changed, click **Synchronize Domain Users** to get the latest information of the users imported to the platform. If the users are imported by group, it will synchronize the latest user information from the domain group (including added users, deleted users, edited users, etc., in the group).

Result

After successfully adding the domain users, the users can log in to the HikCentral Professional via the Web Client and Mobile Client with their domain accounts and passwords.

10.2.3 Change Password of Current User

You can change the password of your currently logged-in user account via Web Client.

Steps

1. Move the cursor to the user name at the top-right corner of the Web Client.
2. In the drop-down list, click **Change Password** to open the Change Password panel.

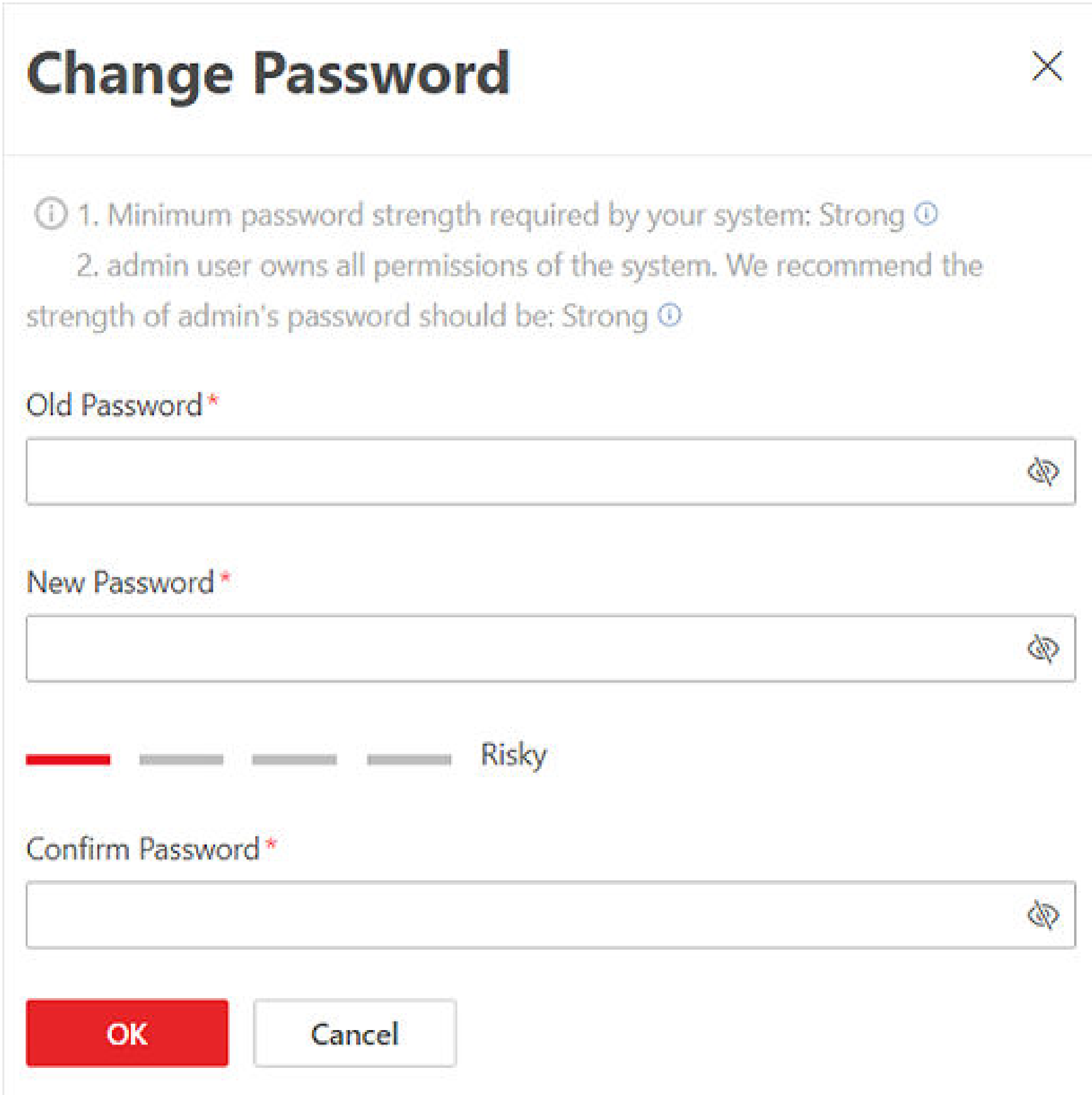


Figure 10-2 Change Password Panel

3. Enter the old password and new password, and confirm the new password.

Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Click **OK** to save the change.

10.2.4 Force Logout a User

In the user list, select an online user and click **Force Logout** to log out the online user.

10.2.5 Unlock a User for Login

For users whose account is locked due to too many failed login attempts, Administrators can unlock their accounts for login.

On the top of user list, click **Unlock for Login**, check users, and click **Unlock**.

10.3 System Security Settings

10.3.1 Set Basic Security Parameters

System security is crucial for your system and property. You can lock IP address to prevent malicious attacks, enable auto lock the Control Client, and set other security settings to increase the system security.

Steps

1. Select **Security Settings → Basic Parameter** on the left.
2. Limit the number of failed login attempts.
   1) Select the maximum allowable login attempts for accessing HikCentral Professional.

      Note

      Failed login attempts include failed password attempt and failed verification code attempt.
   2) Set the lock duration for this IP address. During the lock duration, the login attempt via this IP address is not allowed.

   The number of login attempts is limited.
3. Select the **Minimum Password Strength** to define the minimum complexity requirements that the password should meet.
4. Set the maximum password validity period.
   1) Switch on **Enable Maximum Password Validity Period** to force user to change the password when the password expires.
   2) Set the maximum number of days that the password is valid.

Note

After the maximum number of days, you should change the password. You can select the predefined time length or customize the time length.

3) Set days to remind you at each time you login or in the small hours of each day by sending an email notification before password expiration.

5. Set minutes after which the Web login will expire if there is no actions during the set minutes.
6. Configure the settings to automatically lock the Control Client after a time period of inactivity on the Control Client.
   1) Switch on **Auto Lock Control Client**.
   2) Select time period for user inactivity.

   Note

   You can select the predefined time period or customize the time period.
7. Configure double authentications by selecting the authenticator and the users who need authentication.

   Note

   Double authentications means the users who need authentication should let the authenticator enter the user name and password so that they can use the functions of manual recording, video playback, and video exporting. Resources on the site support double authentication. Only one resource can be configured for a user who needs authentication.

   1) Switch on **Double Authentications**.
   2) Click **Add** to enter the Add Authenticator panel.
   3) Select a user from the drop-down list, configure the authenticatable resource(s) and permission(s), and click **Add** to add the authenticator.
   4) Select the user(s) who need authentication.
8. Click **Save** to save the above settings.

10.3.2 Configure Security Questions

Security questions can be used to verify user identity when users want to reset the password. After setting the security questions, users needs to first answer the security questions correctly before they can reset the password, so as to ensure account security.

Select **Security Question** on the left.

Set three security questions. Select a question from the drop-down list and set an answer to it.

Note

The answer should contain 1 to 128 characters, and cannot contain these special characters: / \ : * ? " < > |

Click **Save** to save the settings.

10.4 Configure Permission Schedule

Permission schedule defines the time when a role's permissions are valid. During unauthorized time periods, the user assigned with the role will be forced to log out and cannot log in. The platform provides 3 default permission schedule templates: All-day Template, Workday Template, and Weekend Template. You can add new templates according to actual needs.

Steps

1. In the top left corner of Home page, select → **Basic Management → Account and Security → Permission Schedule Template** .
2. Click .
3. Set basic information.

   Name

   Create a name for the template.

   Copy From

   Select the template from the drop-down list to copy the settings from another existing template.
4. In the **Weekly Schedule** area, set the weekly schedule as needed.
   1) Click **Authorize**, and select or draw in the box to define the authorized time periods.
   2) **Optional:** Click **Erase**, and select or draw on the authorized time periods to clear the selection.

   Note

   You can set up to 6 separate time periods for each day.
5. **Optional:** Set a holiday schedule if you want different schedules for specific days.
   1) Click **Add Holiday**.
   2) Select existing holiday templates, or click **Add New** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Set the schedule for holidays.

   Note

   The holiday schedule has a higher priority than the weekly schedule.
6. Click **Add** to add the permission schedule template.
7. **Optional:** Perform further operations for the added templates.

View and Edit Template Details	Click the template to view and edit its configuration. **Note** Default templates cannot be edited.
Delete Template	Click a template, and click to delete it.

Note

Default templates cannot be deleted.

What to do next

Set permission schedules for roles to define in which period the permissions for the roles are valid. For details, refer to ***Add Role*** .

Chapter 11 System Configuration

This module allows you to set different types (e.g., normal settings, network settings, storage settings, and so on) of parameters for the platform, such as defining a customized name for the site, setting NTP (Network Time Protocol) for synchronizing the time between the platform and the NTP server, and setting an IP address to allow the platform to access the WAN (Wide Area Network).

In the top right corner of the Web Client, select → **Basic Management** → **System** or click **System** on the top navigation bar (if the menu is added to the navigation bar) to enter this module.

11.1 Normal Settings

The normal settings menu provides entries of setting the user preference, holidays, printers, and card templates.

On the left navigation bar of the System page, select **Normal** to display the normal settings menu.

11.1.1 Set User Preference

For different countries, regions, cultures, and enterprise backgrounds, the user preference might be different. You can set the user preference according to the actual scene, such as the site name, the first day of a week, and the calendar type.

Select **User Preference** on the left navigation bar to enter the following page.

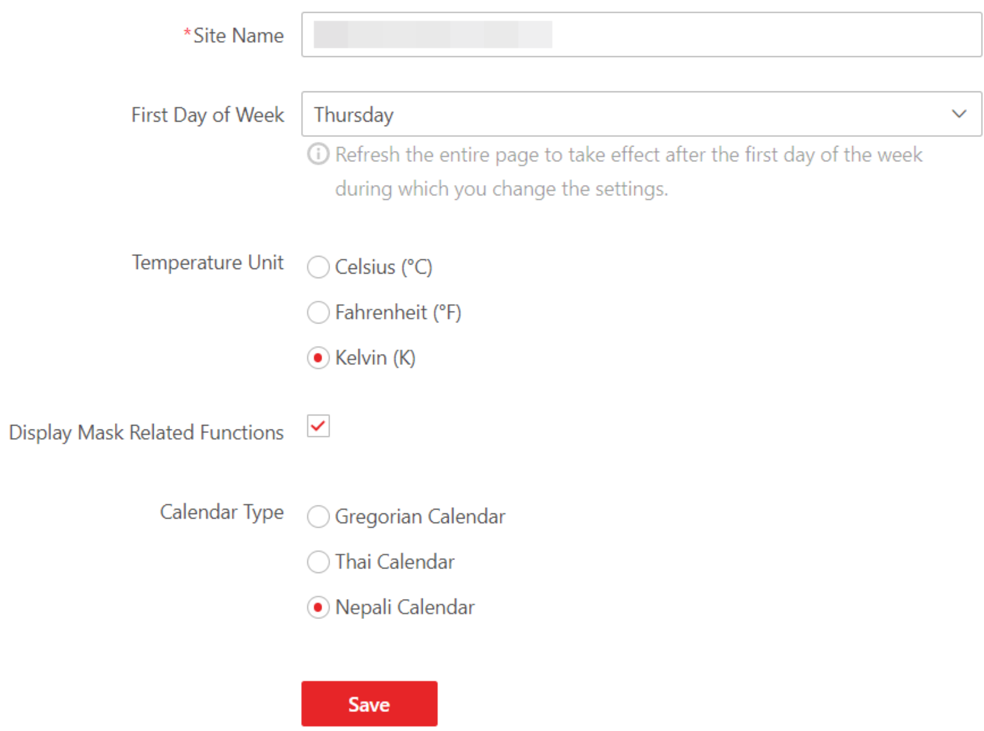


Figure 11-1 User Preference

Set the following parameters:

Site Name

Set the name of current site.

First Day of Week

Set the first day of a week as Sunday, Monday, Tuesday, etc., according to the custom of the actual scene.

Note

This parameter is used in the intelligent analysis report generation, live view and playback, etc.

Temperature Unit

Set the temperature unit according to the custom of the actual scene.

Note

This parameter is used in the temperature analysis report generation, etc.

Display Mask Related Functions

Set whether to display mask related functions. Check the box to display the functions about masks on Control Client, Web Client and Mobile Client. Otherwise these functions will be hidden.

Note

This parameter is mainly used in temperature screening module.

Calendar Type

Set the calendar type as Gregorian Calendar, Thai Calendar and Nepali Calendar according to the custom of the actual scene.

11.1.2 Set Holiday

You can add the holiday to define the special days that can adopt a different schedule or access schedule. You can set a regular holiday and an irregular holiday according to the actual scene.

Select **Holiday Settings** on the left navigation bar to enter the Holiday Settings page.

Add Regular Holiday

The regular holiday is suitable for the holiday that has a fixed date. For example, Christmas is on December 25th of each year.

1. Click **Add** to open the adding holiday dialog.
2. Enter the holiday name and select **Regular Holiday** as the holiday type.
3. Set the parameters according to the following instructions:

   Start Time

   The start date of the holiday.

   Number of Days

   The lasting days of the holiday.

   Repeat Annually

   If checked, the platform will generate the date of the holiday according to the date of SYS (System Server).
4. Click **Add**.

Add Irregular Holiday

The irregular holiday is suitable for the holiday that is calculated by the weekdays, and the specified date might be different in a different year. For example, Mother's Day is on the second Sunday of each May.

1. Click **Add** to open the adding holiday dialog.
2. Enter the holiday name and select **Irregular Holiday** as the holiday type.
3. Set the parameters according to the following instructions:

   Start Time

The start date of the holiday.

For example, select **May**, **Second**, and **Sunday** for Mother's Day.

Number of Days

The lasting days of the holiday.

Repeat Annually

If checked, the system will generate the date of the holiday according to the date of SYS.

Note

If you check **Repeat Annually**, the specified date of this holiday will be generated automatically according to the current year of SYS.
For example, Mother's Day in 2019 and 2020 is on May 12th, 2019, and on May 10th, 2020. The system will automatically set these two days as holidays for Mother's Day if you have checked **Repeat Annually**.

4. Click **Add**.

11.1.3 Set Printer

You can set printers for the platform, which can be used to print the stranded person list in some urgent evacuation scenario, such as fire hazard.

Note

Make sure that the printers are installed on the same network with SYS.

Select **Printer Settings** on the left navigation bar to enter the Printer Settings page.

Click **Add** to select the printer(s) detected by the platform.

Note

After setting a printer for the platform, you can link the printer when configuring alarm/event whose source type is alarm input.

You can click in the Operation column to delete a printer or click **Delete All** to delete all added printers.

11.1.4 Set Card Template

The platform has provided two predefined card template for you. If they do not meet your requirements, you can set styles for card templates by yourself. After settings, the card will be applied in the format of the template.

Steps

1. Select **Card Template** to enter the Card Template page.
2. Click **Add**.

3. Create a name for the template.
4. **Optional:** Select the shape of the template.
5. Set the front style of the template.

Insert Picture	Click **Insert Picture** to select a picture for the template.
Insert Background Picture	Click **Insert Background Picture** to select a background picture for the template.
Insert Text	Click **Insert Text** to set the text for the template.
Customize Contents	Check the attribute(s) for the content of the template. You can also click **Additional Information** to customize the attributes for the template.
Configure Text Settings	• Select a text box and set the font type, font size, font color, and bold front for the text in the box. • Select one or multiple text boxes and click , , or in the Text Alignment field to adjust the alignment of the text in the box. • Select multiple pictures or text boxes and click , , or in the Content Alignment to adjust these elements. • Right-click a picture (except the background picture) or text box to show a drop-down menu and click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down** to adjust the layer of the picture or text box displayed on the template. • Right-click a picture (except the background picture) or text box to show a drop-down menu and click **Delete** to remove the picture or text box.

6. **Optional:** Refer to the previous step to set the back style of the template.
7. Click **Add** to add the template and go back to the card template list page.

   The added card template will be listed on the Card Template page.
8. **Optional:** Perform the following operation(s).

View Template	Click in the Operation column to view the template details.
Edit Template	Click in the Operation column to edit template details. **Note** The predefined card templates cannot be edited.
Delete Templates	Click in the Operation column of a template or click **Delete All** at the top to delete the template or delete all added templates. **Note** The predefined card templates cannot be deleted.

11.2 Network Settings

The network settings menu provides entries of setting NTP for time synchronization, selecting device access protocol, setting an IP address to allow the platform to access the WAN, and so on.

On the left navigation bar of the System page, select **Network** to display the network settings menu.

11.2.1 Set NTP for Time Synchronization

You can set NTP parameters for synchronizing the time between resources managed on the platform and the NTP server.

Steps

1. Select **NTP** on the left navigation bar.
2. Select the **Time Sync Mode**.

   Note

   For time synchronization via network and the local server, just set the synchronization interval and click **Save**. For time synchronization via the NTP server, follow steps below.
3. Set the NTP server address and port No.

   Note

   If the local NTP server has been configured, click **Detect Local NTP** to fill in the NTP server address and port No. automatically.
4. Enter the interval of the automatic time synchronization.
5. **Optional:** Click **Test** to test the communication between resources and the NTP server.
6. **Optional:** Switch on **Configure WAN Mapping** and enter the IP address and port No. for WAN mapping.

   Note

   If the NTP service is locally deployed, you can configure WAN mapping to synchronize the time for devices on the WAN. Otherwise, enabling mapping is not required.
7. Click **Save**.

11.2.2 Set Active Directory

If you have a AD (Active Directory) domain controller which contains the information (e.g., user data, computer information), you can configure the settings to get the related information. In this way, you can add the users that belong to an organization unit (OU) (e.g., a department of your company) to the platform conveniently.

Steps

1. Select **Active Directory** on the left navigation bar.
2. Select **Local Active Directory** or **Azure Active Directory** as the domain type
3. Configure the corresponding parameters for connecting the platform to the AD domain controller.

   Local Active Directory

   Domain Name

   The domain name of the AD domain controller. You can get it from the CMD window.

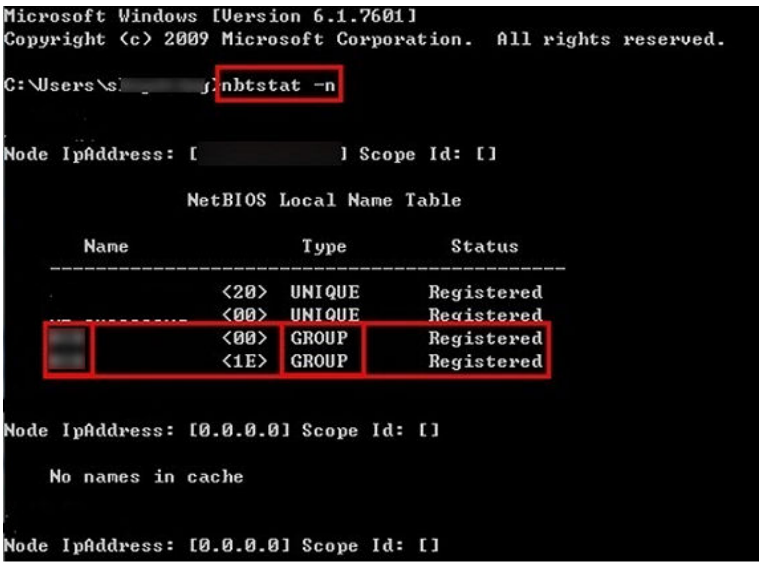


Figure 11-2 How to Get NetBIOS Domain Name

   Host Name

   The IP address of DNS server. You can get it in Network Connection Details.

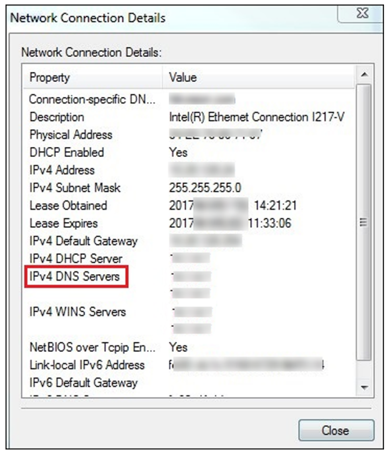


Figure 11-3 How to Get Host Name

Port No.

The port No. of the AD domain controller. By default, it is 389.

Enable SSL (Optional)

Enable SSL if it is required by the AD domain controller.

User Name / Password

The user name and password of the AD domain controller. The user should be the domain administrator.

Base DN (Distinguished Name)

Enter the filter condition in the text field if you are familiar with the format. Or you can click **Fetch DN** to get the filter condition entered automatically.

Note

- Only users found within an OU in the domain can be imported.
- If you enter the Base DN manually, you need to define the root node as desired. If you click **Fetch DN**, then the entire structure stored in the AD domain controller will be obtained.

Azure Active Directory

Note

Before using this domain type, make sure that you have registered an Azure account.

Tenant ID

It is a GUID (Global Unique Identifier) and used to identity your tenant. You can log in to the Azure Portal by using your account, browse to **Identity → Overview → Properties** , and find your tenant ID in the Tenant ID section.

Application (Client) ID

It is a unique identifier of an application created in AD. You can get the ID after you create an application in Azure AD.

Client Secret Name (Optional)

Customize a name for the client secret to help you distinguish the applications and quickly find their secrets.

Client Secret

It is the password created for an application in Azure AD.

4. Set the time to automatically synchronize the users in the AD domain to the platform.
5. **Optional:** Link the person information you are concerned about in the domain to the person information on the platform.

Note

Once enabled, the corresponding person information on the platform will match the linked person information in the domain and cannot be edited.

1) Switch on **Linked Person Information**.

The basic and custom additional information items (see ***Customize Additional Information***) are displayed by default. You can set the relationship for those or add new person information items as needed.

2) **Optional:** Click **Add** to add a person information item you are concerned about.

Note

- You do not need to add the basic person information items (including ID, first name, last name, phone, and remark) manually, which have the default relationship with the information in the domain.
- The person information item is case-sensitive.

3) Click + to show the person information items stored in the domain and check checkboxes in the domain to link them to the custom person information item when importing the domain's persons.
4) Click and drag one item to another to change the relationship between each other.
5) **Optional:** Hover over the linked person information in the domain and click × to remove the relationship.

6. Click **Save**.

After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on the **Account and Security → Users** page.

11.2.3 Set Device Access Protocol

Before adding devices supporting ISUP and ONVIF protocol to the platform, you need to set the related configuration to allow these devices to access the platform.

Select **Device Access Protocol** on the left navigation bar.

Switch on **Allow ISUP Registration** or check **Access via ONVIF Protocol** to allow devices to access the platform via the ONVIF protocol or ISUP.

Note

After **Allow ISUP Registration** is switched on, you can check **Allow ISUP of Earlier Version** to allow devices to access the platform via ISUP of version 2.6 or 4.0.

11.2.4 Set Hik-Partner Pro Access

After setting the Hik-Partner Pro access, you can add devices to Hik-Partner Pro via HikCentral Professional.

Steps

1. Select **Hik-Partner Pro Access** on the left navigation bar.
2. Switch on **Access Hik-Partner Pro**.
3. Enter the installer name of Hik-Partner Pro.
4. Click **Access Now** to open the Site Access pane.
   1) Enter the access key and secret key of Hik-Partner Pro.
   2) Select a domain name where the account locates.
   3) Click **Get Site** to get sites to be accessed.

      The number of accessed sites will be displayed. You can click to view the site name.
5. **Optional:** Switch on **Synchronize Device with DDNS Configured** and select a site to synchronize devices with DDNS configured of the Hik-Partner Pro account to the selected site in Hik-Partner Pro.
6. **Optional:** Switch on **Receive Event From Hik-Partner Pro** as needed.
7. Click **Save**.

   Note

   After saving the settings, you cannot disable this function.

11.2.5 Set WAN Access

In some complicated network environments, you need to set a static IP address or a domain name and ports for HikCentral Professional to access WAN (Wide Area Network).

Steps

1. Select **WAN Access** on the left navigation bar.
2. Click **Export**, and select ports to download a template.

	A	B	C
1	Do not edit the content in the first two columns.		
2	Port Name	LAN Port	WAN Port
3	Client Communication Port (HTTP)	80	
4	Client Communication Port (HTTPS)	443	
5	Client Communication Port (Cluster Port Segment)	18001-18021	
6	Generic Event Receiving Port (TCP)	15300	
7	Generic Event Receiving Port (UDP)	15300	
8	Generic Event Receiving Port (HTTP)	15310	
9	Generic Event Receiving Port (HTTPS)	15443	
10	ISUP Alarm Receiving Port (TCP)	7332	
11	ISUP Alarm Receiving Port (UDP)	7334	
12	ISUP Registration Port (TCP)	7660	
13	Port for Downloading Files from ISUP Devices (TCP)	8555	
14	OTAP Device Registered Port	7666	
15	IP Speaker Registration Port	8877	
16	IP Speaker Communication Port	10015	
17	SDK Alarm Listening Port	8686	
18	Sever Local Picture Storage Port (HTTP)	6011	
19	Server Local Picture Storage Port (HTTPS)	6111	
20	Sever Local File Storage Port (HTTP)	6203	
21	Server Local File Storage Port (HTTPS)	6204	
22	Remote Site Registration Port	14200	
23	Broadcast Signaling Port	7662	
24	Cluster Intercom Command Port	7668	
25	ISUP Streaming Port (TCP)	16000	
26	ISUP Port for Two-Way Audio (TCP)	16001	
27	ISUP Port for Broadcasting (TCP)	16003	
28	Cluster Intercom Streaming Port of ISUP Device	16005	
29	RTSP Streaming Port (TCP)	554	
30	Web Client Streaming Port (TCP)	559	
31	Streaming Media Signaling Port (TCP)	7661	
32	RTMP Streaming Port	1935	
33	HLS Streaming Port	83	

Figure 11-4 Exported Template

3. Send the template to your maintenance staff to enter the WAN port numbers, and get the completed file.
4. Click **Import** to import the completed file.
5. Enable **Access WAN** to enable the WAN access function.
6. Check the imported ports, and click **Save**.

11.2.6 Set IP Address for Receiving Device Information

You can select the NIC of the current SYS (System Server) so that the platform can receive the alarm information of the device connected via ONVIF protocol, and to perform live view and playback for the devices connected via ISUP.

Before You Start

Make sure the server's ports ranging from 8087 to 8097 are available.

Steps

1. Select **Address for Receiving Device Info** on the left navigation bar.
2. Select **Get from NIC** or **Enter Manually**.

   Get from NIC

   Select the currently used NIC name of SYS in the drop-down list. The NIC information including description, MAC address, and IP address will be displayed.

   Enter Manually

   If you have configured hot spare for the SYS, you should manually enter the IP address.
3. Click **Save**.

11.2.7 Register Remote Site to Central System

This page allows the platform without the Remote Site Management module (as we called Remote Site) to register to the Central System. The Central System is the platform that has the Remote Site Management module and can join multiple Remote Sites together to form a larger-scale union. The purpose of joining the Central System and Remote Sites is to allow the Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same platform.

Before You Start

For the Central System, it should enable the receiving site registration function so that it can receive the Remote Site registration. See ***Allow for Remote Site Registration*** for details.

Steps

Note

Registering to the Central System is only available for the platform without the Remote Site Management module.

1. Select **Site Registration** on the left navigation bar.
2. Switch on **Register to Central System**.
3. Enter the IP address and port No. of the Central System.

   Note

   You can get the IP address and port of Central System from the Service Manager, which is installed on the PC running SYS of the Central System.
4. Click **Save**.

11.2.8 Allow for Remote Site Registration

This page allows the platform with the Remote Site Management module (as we called Central System) to receive the registration from Remote Sites. The Remote Site is the platform that does not have the Remote Site Management module and can register to the Central System to form a larger-scale union. The purpose of joining Central System and Remote Sites is to allow the Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same system.

Steps

Note

Allowing for Remote Site registration is only available for the platform with the Remote Site Management module. For details about registering Remote Sites to the Central System, refer to ***Register Remote Site to Central System*** .

1. Select **Site Registration** on the left navigation bar.
2. Check **Receive Site Registration**.
3. Click **Save**.

11.3 Storage Settings

The storage settings menu provides entries of setting storage for pictures and files on SYS and specifying retention periods for different types of records.

On the left navigation bar of the System page, select **Storage** to display the storage settings menu.

11.3.1 Set Storage on System Server

The imported pictures (such as the static e-map pictures and the face pictures in the person list) and files (such as the broadcast recordings and video recordings) can be stored on SYS. You can configure the storage locations and the corresponding quotas for them.

Steps

Note

This configuration is available only when the Web Client is running on SYS.

1. Select **Storage on SYS Server** on the left navigation bar.

   The disks of SYS are displayed with current free space and total capacity.
2. Switch on **Enable Local Storage**.
3. Configure the related parameters for storing pictures.
   1) Select the disk to store the imported pictures.

      Note

      The disk should have at least 1.25 GB of free space for picture storage.
   2) **Optional:** Switch on **Set Quota for Pictures** and set the storage quota for the pictures.
4. Click **Add** to add a resource pool for storing files.

1) Enter the name of the resource pool.
2) Select a disk to store the files.

Note

The disk should have at least 9 GB of free space for file storage.

3) **Optional:** Switch on **Restrict Quota for Pictures** and set the storage quota for the files.
4) Check **Overwrite When Storage Space is Insufficient**, and the newly imported files will overwrite the existing files when the disk space is insufficient.
5) Click **Add**.
6) **Optional:** Click **Delete** or in the Operation column to delete a resource pool.
7) **Optional:** Click a resource pool name to edit related settings.

5. Click **Save**.

11.3.2 Set Storage for Records

The data retention period specifies how long you can keep the events, logs, and some records on SYS.

Steps

1. Select **Records Storage** on the left navigation bar.
2. Select one language from the drop-down list to set the language of the sorting rule.
3. Set the data retention period from the drop-down list for the required data types.
4. Click **Save**.

11.4 Email Settings

The email settings menu provides entries of setting different email templates for scheduled reports, events and alarms, and pending tasks, and configuring the basic email parameters. The email template specifies the recipient, email subject, and content.

On the left navigation bar of the System page, select **Email** to display the email settings menu.

11.4.1 Add Email Template for Sending Report Regularly

You can set email templates (including specifying the recipient, email subject, and content) for sending the report regularly, so that the platform can send the report as an email attachment to the designated recipient regularly according to the predefined email template.

Before You Start

Make sure you have set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. Select **Scheduled Report Email Template** on the left navigation bar.

2. Click **Add** to enter the Add Email Template page.

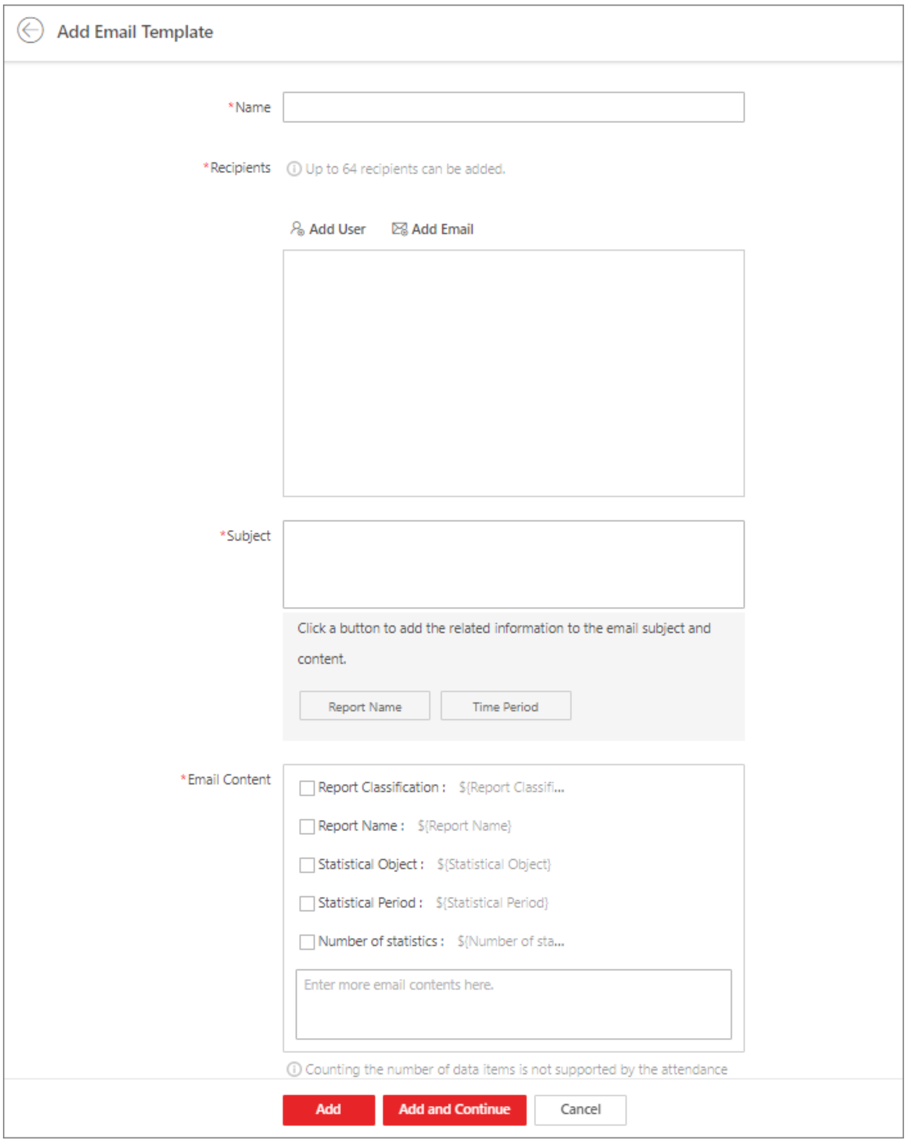


Figure 11-5 Add Email Template for Sending Reports Regularly

3. Enter the required parameters.

Recipients

- Click **Add User** and select the person's email, which is configured when adding the person.
- Click **Add Email** and enter the recipient email address to send the email to.

Note

You can enter multiple recipients and separate them by ";".

Subject

Enter the email subject as desired. You can also click buttons below to add the related information to the subject.

Email Content

Define report contents to be sent. In the Email Content field, check the content type(s) (i.e., Report Classification, Report Name, Statistical Object, Statistical Period, and Number of Statistics) to add the related information to the content and enter more detailed contents in the text box to complete the design of report contents.

Note

If you add the time period to the email subject or add the statistical period to the email content, and the email application (such as Outlook) and the platform are in different time zones, the displayed period may have some deviations.

4. Finish adding the email template.
   - Click **Add** to add the template and go back to the email template list page.
   - Click **Add and Continue** to add the template and continue to add other templates.

   The email template will be displayed in the email template list.
5. **Optional:** After adding email templates, perform the operations such as editing, deleting, and searching for templates.

11.4.2 Add Email Template for Event and Alarm Linkage

You can set email templates (including specifying the recipient, email subject, and content) for event and alarm linkage. When the event or alarm is triggered, the platform can send email as the linkage action to the designate recipient regularly according to the predefined email template.

Before You Start

Make sure you have set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. Select **Event and Alarm Email Template** on the left navigation bar.
2. Click **Add** to enter the Add Email Template page.
3. Enter the required parameters.

Recipients

Click **Add User** and select the person's email as the recipient, which is configured when adding the person.

Click **Add Email** and enter the recipient(s) email address to send the email to.

Note

You can enter multiple recipients and separate them by ";".

Subject

Enter the email subject as desired. You can also click the button in the lower part of the window to add the related information to the subject.

Email Content

Define the event or alarm information to be sent. You can also click buttons below the **Email Content** parameter to add the related information to the content.

Note

If you add the event time to the email subject or content, and the email application (such as Outlook) and the platform are in different time zones, the displayed event time may have some deviations.

4. **Optional:** Check **Attach Captured Picture** and/or **Attach Linked Video**.
5. Select a content language to define the language of the sent content.
6. Click **Add** to add the template and go back to the email template list page. or click **Add and Continue** to add the template and continue to add other templates.

   The email template will be displayed on the email template list.

11.4.3 Add Email Template for Pending Task Notification

You can set email templates (including specifying the recipient, email subject, and content) for pending task notifications. When you add a custom pending task, you can enable the email notification and specify regular time to send email with the pending task information to the designated recipient regularly.

Before You Start

- Make sure you have set the sender's email account first. See ***Configure Email Account*** for details.
- Make sure you have added custom pending tasks and enabled the email notification. See ***Add Custom Pending Tasks*** for details.

Steps

1. Select **Email Template of Pending Task Notification** on the left navigation bar.
2. Click **Add** to enter the Add Email Template page.

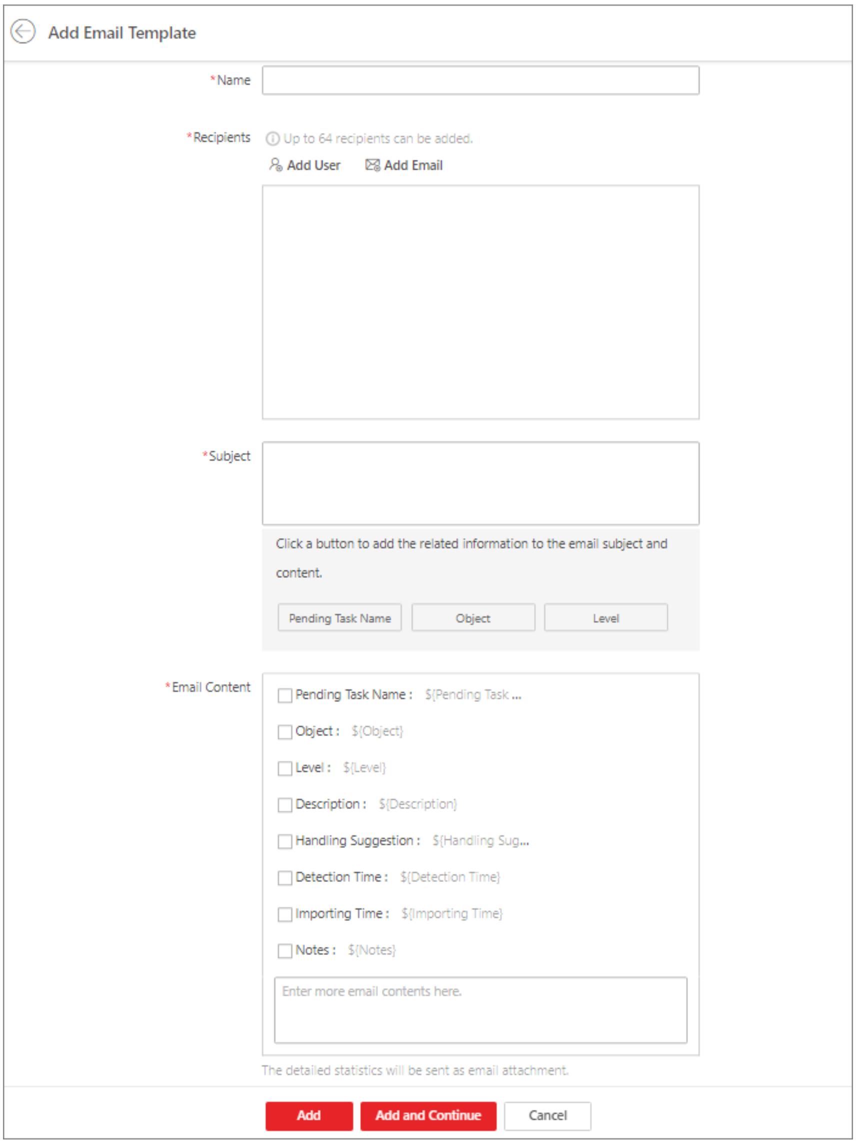


Figure 11-6 Add Email Template for Pending Task Notification

3. Enter the required parameters.

Recipients

- Click **Add User** and select the person's email, which is configured when adding the person.
- Click **Add Email** and enter the recipient email address to send the email to.

Note

You can enter multiple recipients and separate them by ";".

Subject

Enter the email subject as desired. You can also click buttons below to add the related information to the subject.

Email Content

Define report contents to be sent. In the Email Content field, check the content type(s) (i.e., Pending Task Name, Object, Level, Description, Handling Suggestion, Detection Time, Importing Time, and Notes) to add the related information to the content and enter more detailed contents in the text box to complete the design of report contents.

4. Finish adding the email template.
   - Click **Add** to add the template and go back to the email template list page.
   - Click **Add and Continue** to add the template and continue to add other templates.

   The email template will be displayed in the email template list.
5. **Optional:** After adding email templates, perform the operations such as editing, deleting, and searching for templates.

11.4.4 Configure Email Account

You should configure the parameters of the sender's email account before the system can send the message to the designated email account(s) as the email linkage.

Steps

1. Select **Email Settings** on the left navigation bar.
2. Configure the parameters according to actual needs.

Server Authentication (Optional)

If your mail server requires authentication, check this checkbox to use authentication to log in to this server.

Cryptographic Protocol

Select the cryptographic protocol of the email to protect the email content if required by the SMTP server.

Sender Email Address

Enter the email address of the sender to send the message.

Sender Name

Enter the sender name to send the message.

SMTP Server Address

The SMTP server's IP address or host name (e.g., smtp.263xmail.com).

SMTP Server Port

The default TCP/IP port used for SMTP is 25.

User Name (Optional)

User name for authentication to log in to the server. This parameter is valid and optional when server authentication is enabled.

Password (Optional)

Password for authentication to log in to the server. This parameter is valid and optional when server authentication is enabled.

Note

For users of Google email, you should log in to your Google account, enable the 2-step verification function, generate the APP password, and enter here.

3. Click **Email Test** to test whether the email settings work or not.

   The corresponding attention message box will pop up.
4. Click **Save**.

11.5 Security Settings

The security settings menu provides entries of setting the transfer protocol for SYS, exporting service component certificate, enabling export of profile pictures, enabling client auto update, and setting the database password.

On the left navigation bar of the System page, select **Security** to display the security settings menu.

11.5.1 Set Transport Protocol

You can set SYS's transport protocol to define the access mode for SYS via clients as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Steps

1. Select **Transport Protocol** on the left navigation bar.
2. In the **Transport Protocol Between Platform and Browser** field, select **HTTP** or **HTTPS** as the transport protocol between clients and SYS.

   Note

   For HTTPS, only the TLS 1.2 and later versions are supported. The browser must support and has enabled the TLS 1.2 or later version. You are recommended to use the browser supporting TLS 1.3.
3. **Optional:** If **HTTPS** is selected, perform the following steps to set the certificate.
   1) Select **Platform Provided Certificate**, or select **New Certificate** and click to select a new certificate file from your local PC.
   2) **Optional:** Click **Add →** **→ Confirm** to add a upper-level certificate as needed.

   Note

   You can select the added certificate(s) and click **Delete** to delete them, or click in the Operation column of a certificate to download the certificate.
4. Click **Save**.

- The SYS will restart automatically after the transport protocol is changed.
- All logged-in users will be forced to log out during the restarting, which takes about one minute and after that, the users can log in again.

11.5.2 Export Service Component Certificate

For data security, before adding the Streaming Server or Cloud Storage Server to the platform, you should generate the service component certificate stored in SYS and input the certificate information to the Streaming Server you want to add, or export the service component certificate stored in SYS and import the certificate to the Cloud Storage Server, so that the certificates of the Streaming Server, Cloud Storage Server and SYS are the same.

Steps

1. Select **Service Component Certificate** on the left navigation bar.
2. Click **Generate Again** beside **Certificate between Services in System** to generate the security certificate for Streaming Server verification.

   Note

   On the Service Manager of the Streaming Server you want to add, input the certificate information you generate. For the following operations, see ***Add Streaming Server*** for details.
3. Click **Export** to export the service component certificate in XML format and save it to the local PC.

   Note

   On the Cloud Storage Server you want to add, import the service component certificate you export.

11.5.3 Enable Export of Profile Pictures

You can export the profile pictures of the added persons as a ZIP file to your PC in the Person module. For information security, you can choose to convert these profile pictures into unreadable modeling data for saving.

Select **Profile Picture** on the left navigation bar and check **Export Profile Pictures**.

Note

Here it only controls the permission of exporting profile pictures. For the entry of exporting, you can go to the Person module.

11.5.4 Enable Auto Update

You can enable auto update to allow the clients to be updated automatically if there is a new version available.

Select **Auto Update** on the left navigation bar, check **Client Auto Update**, and click **Save**.

11.5.5 Set Database Password

You can set the database password of the platform on the Web Client running on SYS.

Note

Setting database password is only available when you access the Web Client on SYS locally.

Select **Database Password** on the left navigation bar.

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

11.5.6 Watermark Settings

On the left navigation bar, click **Watermark Settings**. and then enable **Watermark**.

1. Configure the display content, text style, transparency, rotation angle, and size.
2. click **Background Settings** to set the watermark's background
3. click **Save**.

11.6 Third-Party Integration Settings

The third-party integration settings menu provides entries of integrating via Optimus, OpenAPI Gateway, SIA Gateway, BACnet Gateway, and Sur-gard Gateway, setting SIA event access, interchanging data, and setting a WhatsApp merchant account.

On the left navigation bar of the System page, select **Third-Party Integration** to display the third-party integration settings menu.

11.6.1 Integrate via Optimus

The platform supports integrating third-party resources via Optimus.

Select **Optimus Integration** on the left navigation bar and switch on **Integrate via Optimus**.

Note

- Only admin/administrator users have the permission to perform this function.
- For details about configuring the related parameters in Optimus, refer to the corresponding user manual.

The default icons of resources integrated from the third-party will be displayed. Hover the cursor over the default icon and click to change the resource icons according to your need.

Click **Save**.

11.6.2 Integrate via OpenAPI Gateway

The platform provides the OpenAPI Gateway to integrate the third-party system. By the provided open APIs (Application Programming Interfaces), the third-party system can obtain some functions of HikCentral Professional to develop more customized features.

Note

The gateway should be deployed on the same network with SYS.

Select **OpenAPI Gateway** on the left navigation bar, switch on **Open API**, and set the IP address and management port of the gateway, or select partner users to define resource and operation permissions in the integration.

(Optional) Click **Test** to test the service availability of the gateway.

Click **Save**.

11.6.3 Set SIA Event Access

For zones configured with SIA event rules, the linked security control devices will report multiple IDs of event types. You can add relationships between event type IDs and names here to allow the platform to receive and display SIA events from the third-party devices.

Select **SIA Access Configuration** on the left navigation bar, click **Add**, and enter the name and the corresponding ID of an event type to set the relationship.

The following operations are available after adding event type names and IDs.

- Click in the Operation column of an item to edit the name or ID.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click in the upper right corner to unfold the filter pane and enter the event type name or ID to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.

11.6.4 Integrate via SIA Gateway

The platform provides the SIA Gateway to integrate the third-party system. By the provided SIA protocol, the third-party system can obtain some functions of HikCentral Professional to develop more customized features.

Select **SIA Gateway** on the left navigation bar and switch on **SIA Gateway** to configure the basic parameters, zones, and event template.

Basic Configuration

Select the access mode (listening mode or arming mode), select a partner user to define resource and operation permissions in the integration, select the version for the integration protocol, enter the IP address and port No. of the third-party system if the listening mode is selected, enter the linecard number and the receiver number, set the heartbeat interval, and then click **Save**.

Note

The default transport protocol is TCP/IP, which is not configurable, and you can also check the connection status of the gateway.

Zone Configuration

1. Click **Add** to enter the Add Zone page.
2. Enter a name for the configuration and set the account ID of SIA protocol.
3. Click **Add** to open the Add Resource pane.
4. Select a resource type for the zone.
5. Click **Add** in the Select Resources field to select the resource(s) from the platform.

   Note

   - If you check **Auto Generate Zone ID**, the platform will generate zone IDs for all the selected resources. Otherwise, you should set a zone ID for each resource manually.
   - You can click in the Operation column of a resource to remove it or click **Delete All** to remove all the selected resources.

6. Select an existing event template or click **Add Event Template** to add a new one (see ***Event Template Configuration***).
7. Click **Add** or **Add and Continue** to finish adding a zone and go back to the Zone Configuration page or continue to add another one.

After adding zones, you can perform the following operations on the Zone Configuration page.

- Click in front of the configuration name to display the linked resource name and zone ID.
- Click a configuration name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click in the upper right corner to unfold the filter pane and set conditions to filter items.

- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.
- Click in the upper right corner and check or uncheck the column name(s) to customize the displayed columns. You can also click **Reset** to restore to the default settings.

Event Template Configuration

1. Click **Add** to enter the Add Event Template page.
2. Enter a name for the template and select a event source type.
3. Click **Add** in the Template Content section to add events for the template by selecting event types and SIA codes.

Note

You can click in the Operation column of an event type to remove it or click **Delete All** to remove all the selected event types.

4. Click **Add** or **Add and Continue** to finish adding a event template and go back to the Event Template page or continue to add another one.

After adding event templates, you can perform the following operations on the Event Template Configuration page.

- Click in front of the template name to display the linked event type and SIA code, which can be edited by clicking in the Operation column.
- Click a template name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click **Import** to batch add event templates by the Excel file. During import, the duplicated templates can be overwritten by checking **Auto Replace Duplicated Template**.
- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** to adjust the column width.

11.6.5 Integrate via BACnet Gateway

The platform provides the BACnet Gateway to integrate the third-party system. By the provided BACnet protocol, the third-party system can obtain some functions of HikCentral Professional to develop more customized features.

Select **BACnet Gateway** on the left navigation bar and switch on **BACnet Gateway** to configure the basic parameters, objects, and event template.

Basic Configuration

Select a partner user to define resource and operation permissions in the integration, select the version for the integration protocol, enter the BACnet instance No. and BACnet device name, set the timeout duration and resending times for APDU, and then click **Save**.

Note

The default transport protocol is UDP/IP, which is not configurable.

Object Configuration

1. Click **Add** to enter the Add Object page.
2. Enter a name for the object.
3. Select an object template (see ***Object Template***).
4. Select a source type and the corresponding resource type for the object.
5. Click **Add** in the Select Resources field to select the resource(s) from the platform.

   Note

   - If you check **Auto Generate Target Instance No.**, the platform will generate target instance No.s for all the selected resources. Otherwise, you should set a No. for each resource manually.
   - You can click in the Operation column of a resource to remove it or click **Delete All** to remove all the selected resources.
6. Click **Add** to finish adding a object and go back to the Object Configuration page.

After adding objects, you can perform the following operations on the Object Configuration page.

- Click in front of the object name to display the linked resource name and target instance No.
- Click an object name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.
- Click in the upper right corner and check or uncheck the column name(s) to customize the displayed columns. You can also click **Reset** to restore to the default settings.

Object Template

On the Object Template page, you can perform the following operations.

- View the information about four predefined object templates, including the object type, attribute, value definition, and the status of active event notification.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.
- Click in the upper right corner and check or uncheck the column name(s) to customize the displayed columns. You can also click **Reset** to restore to the default settings.

11.6.6 Integrate via Sur-Gard Gateway

The platform provides the Sur-gard gateway to integrate the third-party system. By the provided Sur-gard protocol, the third-party system can obtain some functions of HikCentral Professional to develop more customized features.

Select **Sur-Gard Gateway** on the left navigation bar and switch on **Sur-Gard Gateway** to configure the basic parameters, zones, and event template.

Basic Configuration

Select the access mode (listening mode and arming mode), select a partner user to define resource and operation permissions in the integration, select the version for the integration protocol, select the MRL mode, enter the IP address and port No. of the third-party system if the listening mode is selected, enter the linecard number and the receiver number, set the heartbeat interval, and then click **Save**.

Note

- The default transport protocol is TCP/IP, which is not configurable, and you can also check the connection status of the gateway.
- For MRL2, the linecard No. is 1-bit, and for MRL2000, it is 3-bit.

Zone Configuration

1. Click **Add** to enter the Add Zone page.
2. Enter a name for the configuration and set the account ID of Sur-gard protocol.
3. Click **Add** to open the Add Resource pane.
4. Select a resource type for the zone.
5. Click **Add** in the Select Resources field to select the resource(s) from the platform.

   Note

   - If you check **Auto Generate Zone ID**, the platform will generate zone IDs for all the selected resources. Otherwise, you should set a zone ID for each resource manually.
   - You can click in the Operation column of a resource to remove it or click **Delete All** to remove all the selected resources.

6. Select an existing event template or click **Add Event Template** to add a new one (see ***Event Template Configuration***).
7. Click **Add** or **Add and Continue** to finish adding a zone and go back to the Zone Configuration page or continue to add another one.

After adding zones, you can perform the following operations on the Zone Configuration page.

- Click > in front of the configuration name to display the linked resource name and zone ID.
- Click a configuration name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.

- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** on the appeared pane to adjust the displayed column widths.
- Click in the upper right corner and check or uncheck the column name(s) to customize the displayed columns. You can also click **Reset** to restore to the default settings.

Event Template Configuration

1. Click **Add** to enter the Add Event Template page.
2. Enter a name for the template and select a event source type.
3. Click **Add** in the Template Content section to add events for the template by selecting event types and CID codes.

   Note

   You can click in the Operation column of an event type to remove it or click **Delete All** to remove all the selected event types.
4. Click **Add** or **Add and Continue** to finish adding a event template and go back to the Event Template page or continue to add another one.

After adding event templates, you can perform the following operations on the Event Template Configuration page.

- Click in front of the template name to display the linked event type and CID code, which can be edited by clicking in the Operation column.
- Click a template name to edit its settings.
- Check the item(s) and click **Delete** at the top to delete the selected item(s).
- Click **Delete → Delete All** at the top to delete all the added items.
- Click **Import** to batch add event templates by the Excel file. During import, the duplicated templates can be overwritten by checking **Auto Replace Duplicated Template**.
- Click in the upper right corner to unfold the filter pane and set conditions to filter items.
- Click in the upper right corner and select **Complete Display of Each Column Title** or **Incomplete Display of Each Column Title** to adjust the column width.

11.6.7 Data Interchange

The access records in HikCentral Professional can be used by third-party systems for pay calculation or other applications. You can synchronize the access records to a third-party database by entering the information of the database table in the required space. You can also dump the access records in CSV or TXT format, and then let the third-party database read the access records to get them.

Synchronize Access Records to Third-Party Database

You can enable synchronization function to apply the access records of specified resources from HikCentral Professional to the third-party database automatically.

Steps

1. Select **Data Interchange** on the left navigation bar.
2. Switch on **Data Interchange**.
3. Click **Add** and select the resource(s) for access records synchronization.

   Note

   - For card readers, you should also select a direction when adding them. Or you can select the added card readers and click **Set Direction (In/Out) of Attendance Check Point** to batch select directions for them.
   - Click in the Operation column to delete the resource or click **Delete All** to delete all added resources.
   - Select the added resource(s) and click **Synchronize Event** and set the time range for events to be synchronized from devices.
4. Select the encoding format of data interchange.
5. **Optional:** Check **Do Not Push Failed Records**.

   The failed records will not be pushed to the third-party system.
6. Select **Database Synchronization**.
7. **Optional:** Switch on **Auto Push Failed Record** to select the push mode.

   Push at Fixed Time

   The failed record will be pushed at the time you set.

   Push at Fixed Interval

   The failed record will be pushed according to the interval you set.
8. **Optional:** Select a database type.
9. Set the required parameters of the third-party database, including server IP address or domain name, server port, database name, user name, and password.
10. Click **Test Connection** to test whether database can be connected.
11. Set table parameters of database table and table fields according to the actual configurations.
    1) Enter the table name of the third-party database.
    2) Enter the mode of the third-party database.
    3) Set the mapped table fields between the HikCentral Professional and the third-party database.
    4) **Optional:** Click **Customize Items to Display** to select the items to be displayed in the table.
12. Click **Save**.

    A window will pop up and you can choose to push the test data now or later.
13. **Optional:** Click **Quick Diagnosis** in the top right corner to quickly diagnose the settings and the function.

    Note

    If there are errors found, you can export the failed data for checking.

Dump Access Records to Third-Party Database

The access records of specified resources can be dumped as a CSV file or TXT file and the third-party system will read the dumped file (instead of accessing the database and mapping the table fields) for further applications, such as attendance calculation and pay calculation. You can also configure dump rules for dumping access records. After that, the access records will be dumped to the third-party database according to the added rules.

Steps

1. Select **Data Interchange** on the left navigation bar.
2. Switch on **Data Interchange**.
3. Click **Add** and select the resource(s) for access records synchronization.

Note

- For card readers, you should also select a direction when adding them. Or you can select the added card readers and click **Set Direction (In/Out) of Attendance Check Point** to batch select directions for them.
- Click in the Operation column to delete the resource or click **Delete All** to delete all added resources.
- Select the added resource(s) and click **Synchronize Event** and set the time range for events to be synchronized from devices.

4. Select the encoding format of data interchange.
5. **Optional:** Check **Do Not Push Failed Records**.

   The failure records will not be pushed to the third-party system.
6. Select **Access Record Dump**.
7. In the Dump Rule area, click **Add** and set the required parameters.

   Overwrite File

   If it not checked, you re recommended to regularly view the disk capacity in case the new files cannot be generated if the disk if full.

   File Name

   The name of the CSV file or TXT file which the access records are dumped as.

   Storage Location

   Local Storage

   The access records can be dumped as a file saved in the local disk of the SYS. Then you need to copy this file from the server to your PC with the third-party system installed to read the dumped file.

Note

- You need to log in to the Web Client running on the SYS to configure related settings of local storage.
- You need to set **Saving Path**, which is the path where the CSV file or TXT file is saved.

SFTP Storage

You can access the SFTP server as the storage location for saving the dumped file by setting the SFTP address, port, user name, and password. And you can enter the path to save the dumped file in the folder on the SFTP server or leave it empty to save the file in the root directory.

Note

The third-party system should be installed in the SFTP server to read the dumped file.

Content

The display items and data in the dumped file.

Department

The group of persons. You can select and search for departments in the list.

Min. Length of Person ID

For some scenarios, the person IDs need to be dumped as a certain fixed length.

You can switch it on and set the value of **Length**. If the length of the person ID is shorter than the value, zero(s) will be added before the ID to make it equal to the value. If the length is longer than the value, the person IDs will be dumped according to the actual length.

Designated Length of Card No.

For some scenarios, the card numbers need to be dumped as a certain fixed length.

You can switch it on and set the value of **Length**. If the length of the card number is shorter than the value, zero(s) will be added before the card number to make it equal to the value. If the length is longer than the value, the card number will be dumped according to the actual length.

Generate Table Header

When the card swiping records are dumped from the system to the local PC, the column names will be included in the dumped file and used as the table header.

File Format

Two formats are supported, including CSV and TXT.

Dump Frequency

The frequency for dumping access records.

Dump Time

The time when dumping card swiping records is started.

8. Click **Add** on the Add Dump Rule page.

The added rules will be listed in the Dump Rule area.

Note

You can click × in the Operation column to delete the rule or click **Delete All** to delete all added rules.

9. Click **Save**.
10. **Optional:** Click **Quick Diagnosis** in the top right corner to quickly diagnose the settings and the function.

    Note

    If there are errors found, you can export the failed data for checking.

11.6.8 WhatsApp

The platform supports integrating with WhatsApp. After the WhatsApp merchant account is configured and authenticated, the platform can send events messages via WhatsApp.

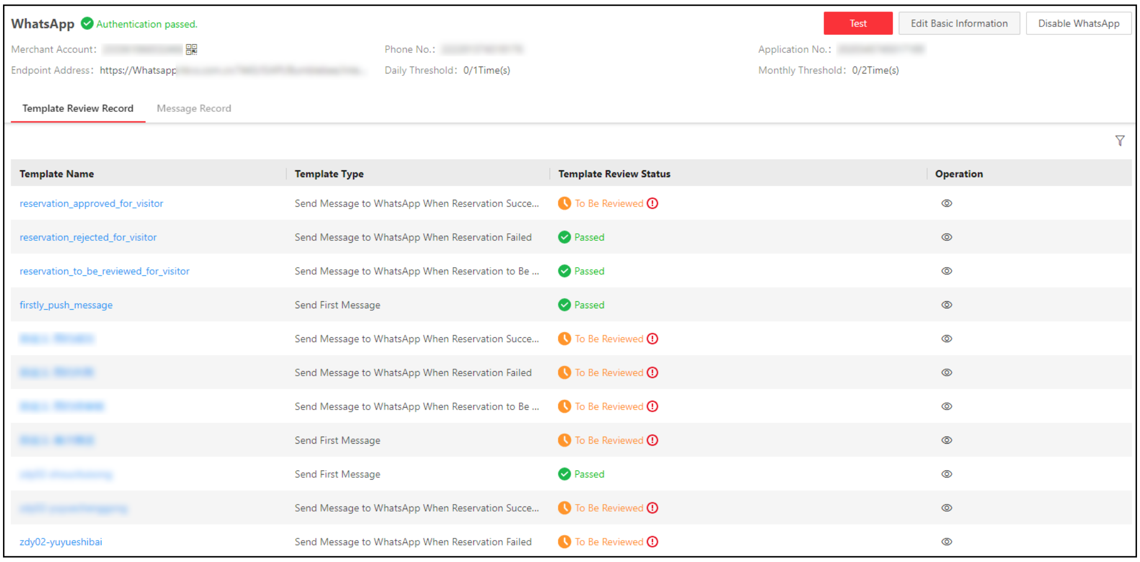
Select **WhatsApp** on the left navigation bar and click **Enable**.

Submit WhatsApp Merchant Account for Authentication

Note

You need to apply for a WhatsApp merchant account first for sending messages of the platform.

1. Enter the account basic information, including merchant account, phone No., application No., access token, and verification token.
2. (Optional) Switch on **Enable Limit** to configure the upper limit of daily and monthly conversation times.
3. Click **Submit for Authentication** to send a request of WhatsApp merchant account authentication.



> **Note**
>
> If the authentication is not passed, you can check the failure reason, edit the basic information, and submit for authentication again.

Manage Authenticated WhatsApp Account

When the merchant account is authenticated, you can view WhatsApp message templates related to the messages receiving/sending records.

Operation	Description
Test Account	Click **Test** and enter a recipient account to test the message sending of merchant account. **Note** The testing might cost fees.
View Account QR Code	Click the QR code thumbnail next to the account ID. You can refresh and download your account QR code for sharing.
View Template Review Status	Click **Template Review Record** tab to view the WhatsApp message templates.
View Message Records	Click **Message Record** tab to view the message sending/receiving records.

11.7 Advanced Settings

The advanced settings menu provides entries of setting system hot spare, generating or debugging logs, downloading the event tracking information, and resetting the network information for devices.

On the left navigation bar of the System page, select **Advanced** to display the advanced settings menu.

11.7.1 Configure System Hot Spare

A hot spare is used as a failover mechanism to provide reliability for your system. If you build the hot spare system when installing SYS, you can enable the hot spare function and configure the hot spare property of the current SYS as host server or spare server. When the host server fails, the spare server switches into operation, thus ensuring the stability of the system.

Steps

1. Select **Hot Spare** on the left navigation bar.
2. Switch on **Hot Spare Configuration** to display the server name and available IP address of the current SYS.
3. Set the server as a host server or a spare server.
4. Click **Save**.

11.7.2 Diagnosis and Maintenance

For the operation and maintenance personnel, they can generate and download logs of a specified time period for locating issues, debug logs, and view or download the event tracking information.

Select **Diagnosis & Maintenance** on the left navigation bar.

Generate Logs

1. Check the service log type(s).
2. Specify the start and end time of the time period in which the logs are to be generated.
3. Click **Generate** to start generating a log file.
   When completes, a zip file name will appear at the bottom of the Maintenance Data section and you can click to download the log file to the local PC.

Debug Logs

1. Click **Download Template** to download the template of log configuration file to the local PC.
2. Fill in the template with required information locally.
3. Click to upload the configured template to the platform and click **Start Debugging**.
   A 24-hour countdown will automatically start.

Note

When the countdown finishes, the on-going debugging will be canceled automatically. You can click **Extend Debugging** to extend the debugging duration.

4. (Optional) Click **Close Debugging** to stop the debugging.

View and Download Event Tracking Information

Click **Event Tracking Information** in the top right corner of the Diagnosis and Maintenance page to open the Event Tracking Information page.
On the Event Tracking Information page, you can view the exception and general information and click **Download Event Tracking Information** in the top right corner to download the event tracking information to the local PC. You can also click **Refresh** to refresh the event tracking information.

11.7.3 Reset Device Network Information

When the system network domain changes (such as server migration), you must reset the network information for the added device to adapt to the new network environment. Otherwise, some functions of the device will be affected.

Steps

1. Select **Reset Network Information** on the left navigation bar.
2. Click **Reset** to one-touch reset the device network information.

11.8 Manage Workbenches

The platform provides three default preset workbenches for administrator, which can only be edited. You can also add new workbenches and manage all of them.

Select **Workbench Management** on the left navigation bar.

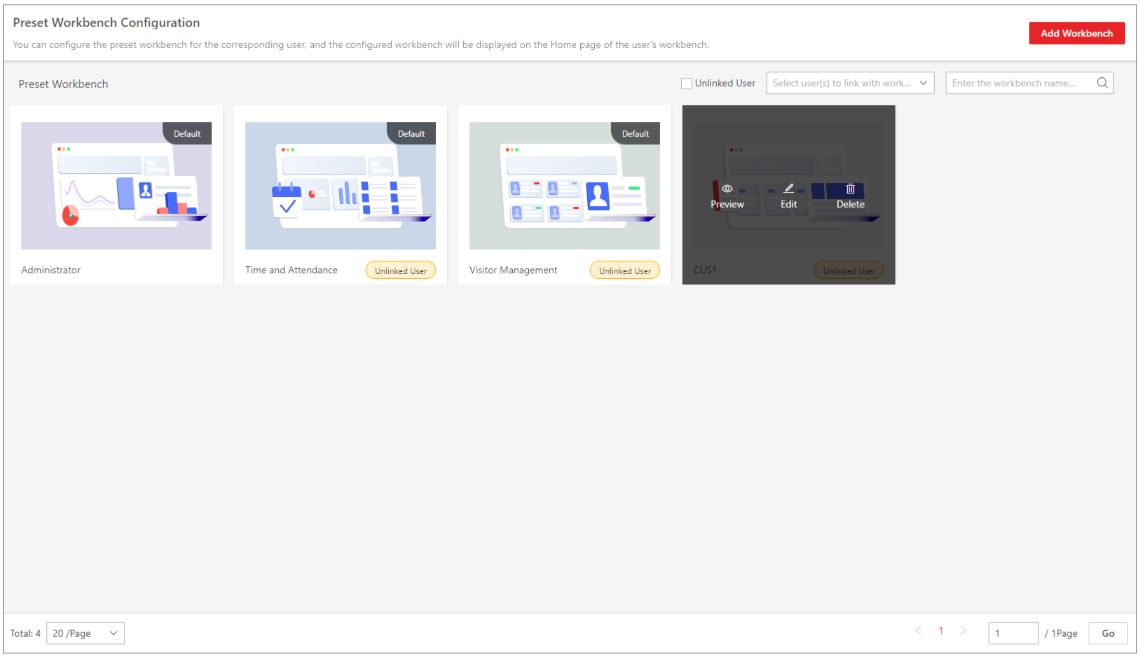


Figure 11-7 Preset Workbench Configuration Page

On the Preset Workbench Configuration page, you can perform the following operations.

- Click **Add Workbench** in the top right corner to create a workbench. See ***Customize Preset Workbench*** for details.
- Move the cursor on a workbench card and click **Preview** to view the workbench. On the Preview page, you can click **Copy and Add** in the top right corner to copy the settings to a new workbench.
- Move the cursor on a workbench card and click **Edit** to edit the configuration.
- Move the cursor on a workbench card and click **Delete** to delete the workbench.
- Check **Unlinked User** to display workbenches that are not linked with users.
- Select the linked user(s) to filter workbenches by user or enter a keyword to search for workbenches by name.

11.9 Set Company Information

You can configure and show the company information on the Web Client for customization requirements.

Select **Company Information** on the left navigation bar.

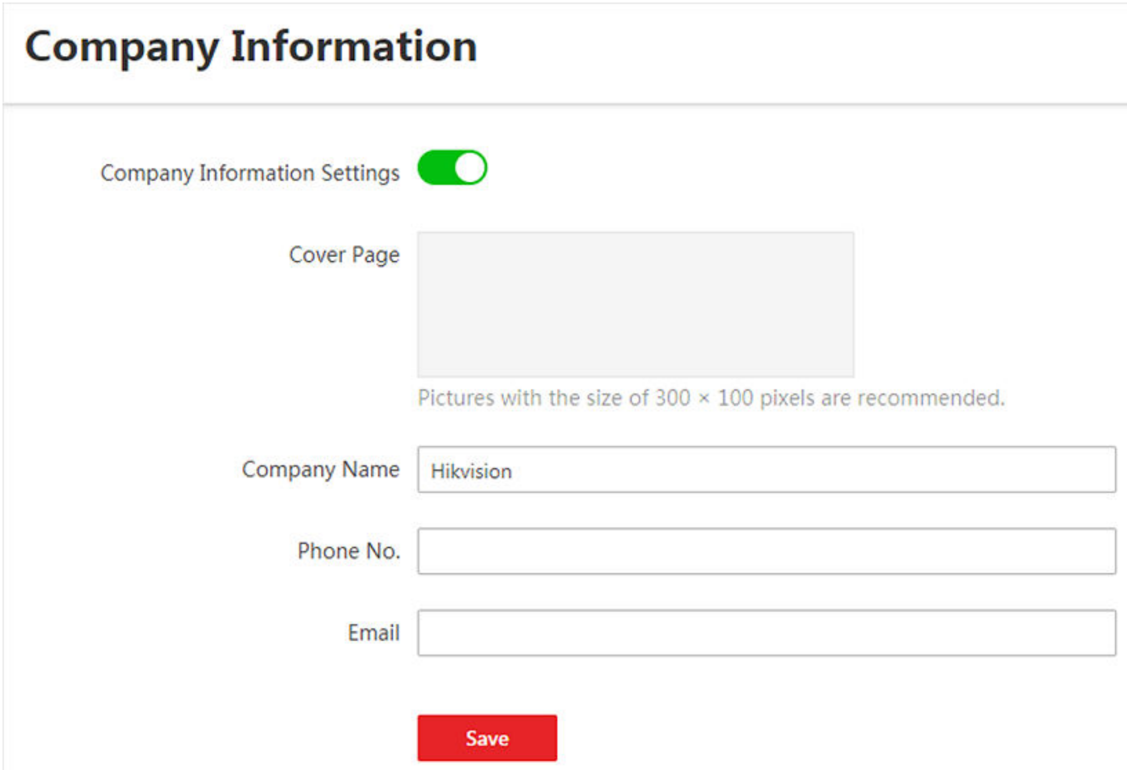


Figure 11-8 Company Information Settings

Switch on **Company Information Settings** to enable displaying company information on the Web Client. Then set the information (cover page, company name, etc.) as needed and click **Save**.

An icon appears at right of the Web Client and keeps displaying. You can click the icon to view the company information.

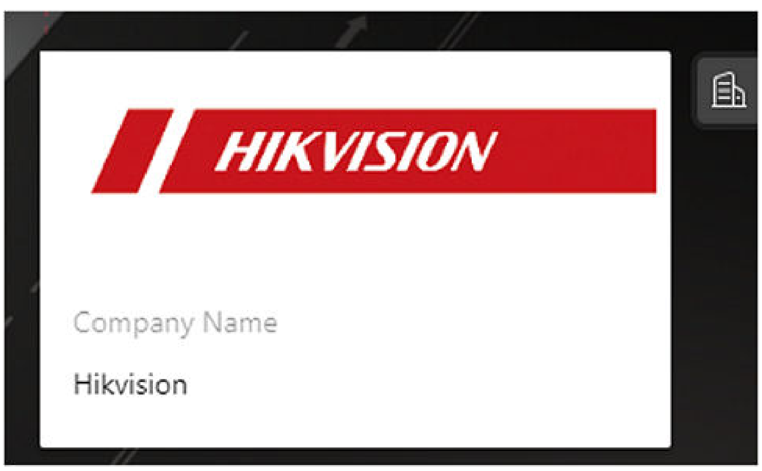


Figure 11-9 Company Information Displayed on Web Client

Chapter 12 Maintenance

The system provides Service Manager to manage the installed services on the SYS server. You can check the service's running status, edit the service port, start/stop service via the Service Manager.

The system also provides backup of the database, so that your data can be well protected and recovered when an exception occurs.

You can also export the system's configuration data and save it to the local PC.

In the top left corner of Home page, select → **All Modules** → **Maintenance** .

12.1 Health Overview

Health Overview provides both near-real-time and history information about the status of the SYS and added resources. It is critical to multiple aspects of operating the servers or devices and is especially important for maintenance. When a resource exception occurs, you can enter this module to check the resource status and find out the abnormal device(s) and view the exception details.

12.1.1 Real-Time Health Status Overview

In the Health Overview module, you can view the real-time health status of the devices, servers, and resources managed on the platform. If there is no network transmission devices added, the Real-Time Overview page provides an at-a-glance view of the health status with charts and basic data of resource status.

Select **Real-Time Overview** on the left.

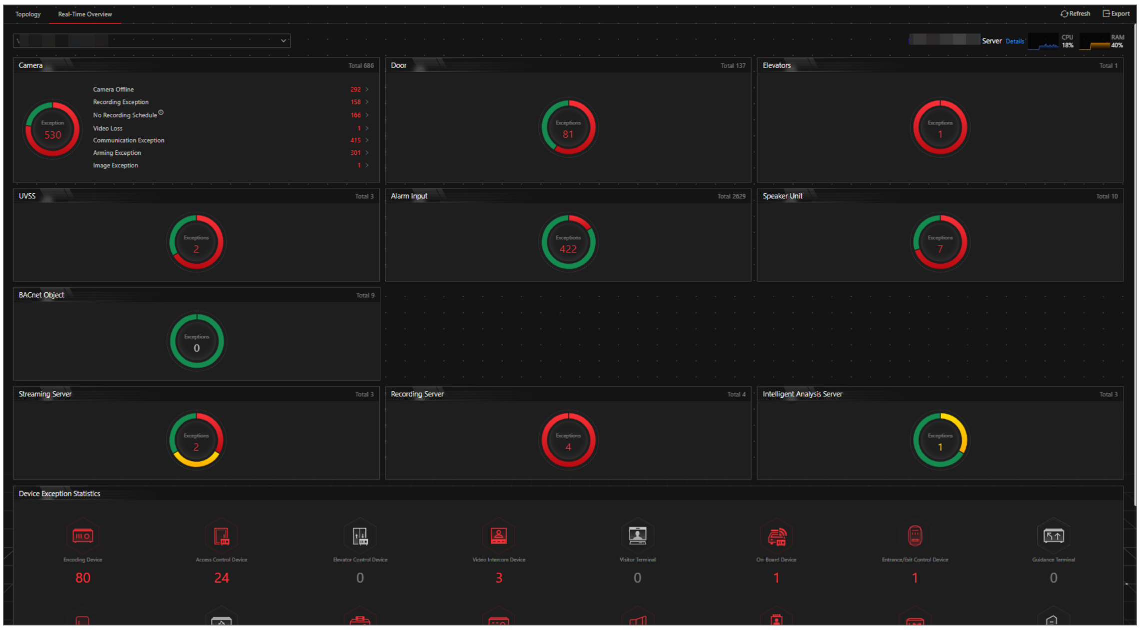
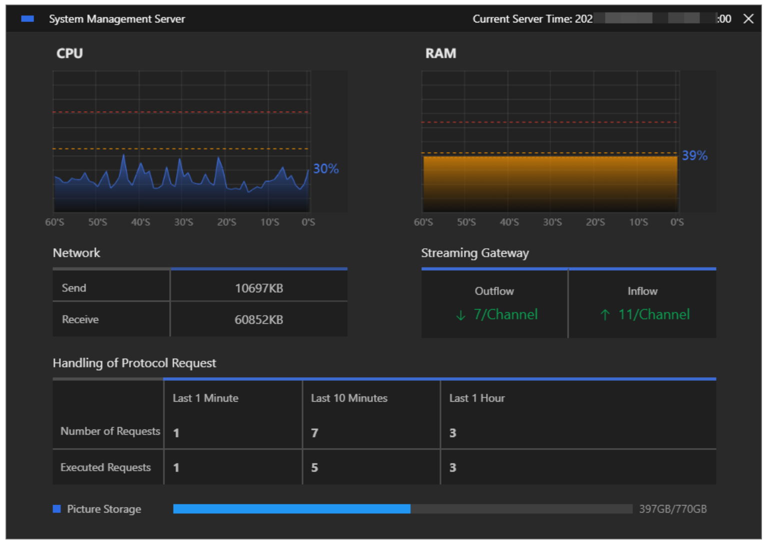
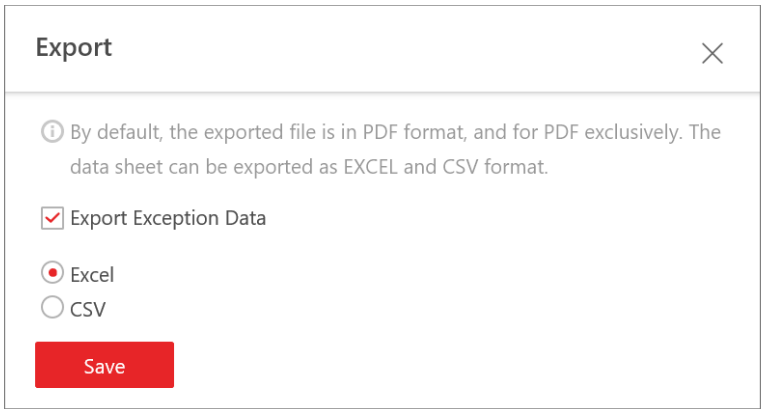


Figure 12-1 Real-Time Health Status Overview

Table 12-1 Real-Time Health Status Page

Section	Description
Display Resource Status by Site	Select a site from the drop-down list in the upper left corner to display the status of resources on the selected site. If an exception occurs on a site, the icon will appear beside the site name and you can move the cursor over it to view the exception details.
System Management Server Status	View the CPU and RAM usages of the site server in the top right corner of the overview page. Click **Details** to open the System Management Server window to view the detailed status, including the current server time, CPU usage, RAM usage, network status, streaming gateway status, handling status of protocol request, and picture storage.

Section	Description
	 **Figure 12-2 Status Details of System Management Server**
Resource Status	View the abnormal data of different resources added to the platform in the graphical way. You can move the cursor over the chart to display the exception types and the corresponding numbers of abnormal devices, and then click a type or the number on the chart to view the real-time status details of resources.
Device Exception Statistics	View the number of abnormal devices with different types added on the platform. You can click a number under the device picture to view the real-time status details of the device. If the icon  appears at the top of device picture, it indicates that the device firmware should be upgraded. For upgrading the firmware, refer to ***Upgrade Device Firmware*** .
Refresh Overview Page	• Manually Refresh: Click **Refresh** in the upper right corner of Real-Time Overview page to manually refresh the resource status on the page. • Auto Refresh: Go to **Maintenance → Basic Configuration → Auto-Check Frequency** to set the interval for automatically refreshing the resource status on the page. See details in ***Set Auto-Check Frequency*** .
Export Overview Page or Exception Data	Click **Export** in the upper right corner of Real-Time Overview page to export the page in PDF format. Or you can check **Export**

Section	Description
	Exception Data to export the exception data in Excel/CSV format.  **Figure 12-3 Export Overview Page or Exception Data**

12.1.2 Real-Time Health Status Overview (Topology)

In the Health Overview module, you can view the real-time health status of the devices, servers, and resources managed on the platform. If there are network transmission devices managed on the platform, the Real-Time Overview page provides a topology of the managed devices. Topology is a figure that displays the connection relations among network transmission devices, security devices, etc. It is mainly used for network maintenance.

Note

- Make sure the network transmission devices have been added to the platform.
- If a network transmission device can not be recognized by the platform, it will be displayed as an unknown device.
- The topology does not support body cameras, but supports ticket dispensers.

On the Health Overview area, select **Real-Time Overview** on the left.

Click **Topology** tab at the top to enter the Topology page.

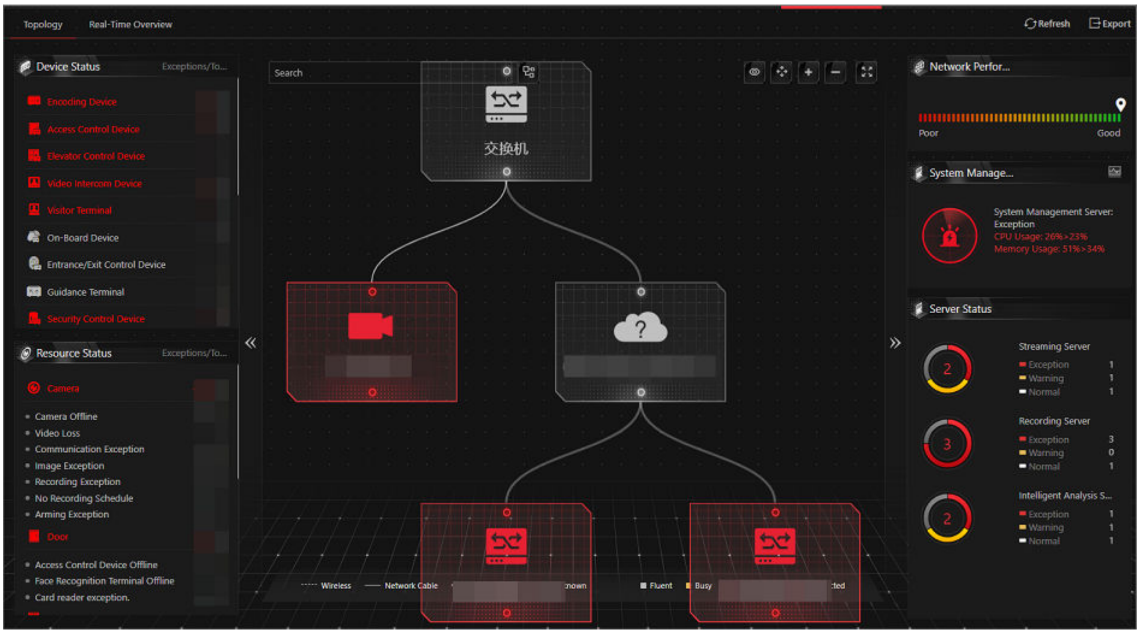
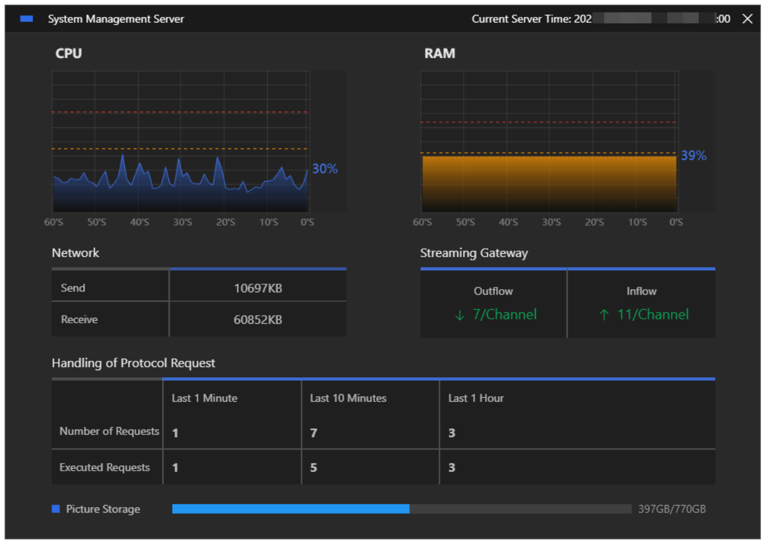
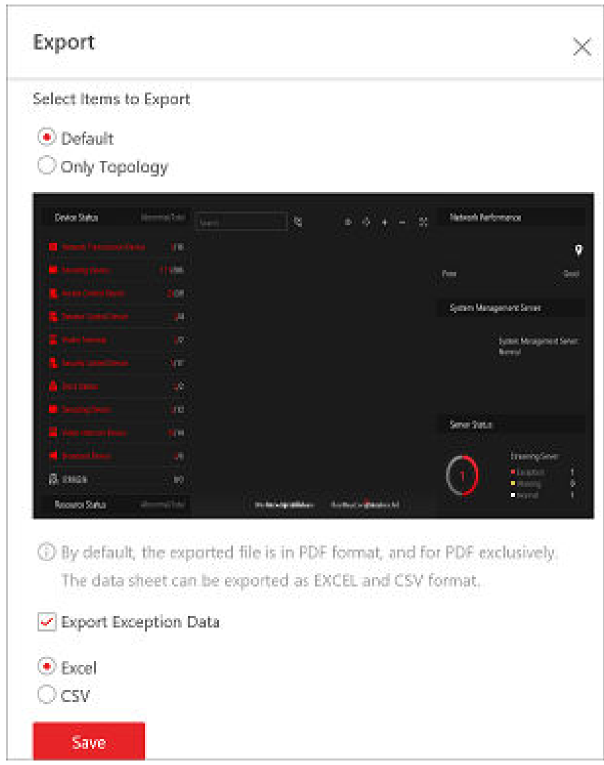


Figure 12-4 Topology Overview

Table 12-2 Topology Page

Section	Description
Device Status	View the abnormal data of different devices added to the platform. You can click the number to locate the abnormal device in the topology or view the devices' real-time status. If the icon appears beside the device type name, it indicates that the device firmware should be upgraded. For upgrading the firmware, refer to ***Upgrade Device Firmware*** .
Resource Status	View the abnormal data of different resources added to the platform. You can click a number to view the real-time status details of resources.
Topology Details	View the relationships among devices, device information, link status, alarm information, etc. See details in ***Topology Details*** .
Network Performance	View the current network performance (poor or good) of the System Management Server.
System Management Server Status	Click in the upper right corner of the System Management Server section to view the detailed status, including the current server time, CPU usage, RAM usage, network status, streaming gateway status, handling status of protocol request, and picture storage.

Section	Description
	 **Figure 12-5 Status Details of System Management Server**
Server Status	View the status (i.e., exception, warning, normal) of servers added on the platform.
Generate Topology Again	Click **Refresh → Generate Topology Again** to draw the network topology again.
Refresh	• Manual Refresh: Click **Refresh** in the upper right corner of the Real-Time Overview page to manually refresh the resource status on the page. • Auto Refresh: Go to **Maintenance → Basic Settings → Health Check Frequency** to set the interval for automatically refreshing the resource status on the page. See details in ***Set Auto-Check Frequency*** .
Export Topology or Exception Data	Click **Export** in the upper right corner of Topology page and select the export type as **Default** or **Only Topology** to export the topology in PDF format or the exception data in Excel/CSV format. **Note** • If the export type is selected as **Default**, the whole displayed information (topology and exception data) on the Health Monitoring page will be exported. • If the export type is selected as **Only Topology**, only the topology will be exported in PDF format.

Section	Description
	 **Figure 12-6 Export Topology**

Topology Details

The topology of devices will display the hierarchical relationships among the devices, device information, link status, alarm information, etc.

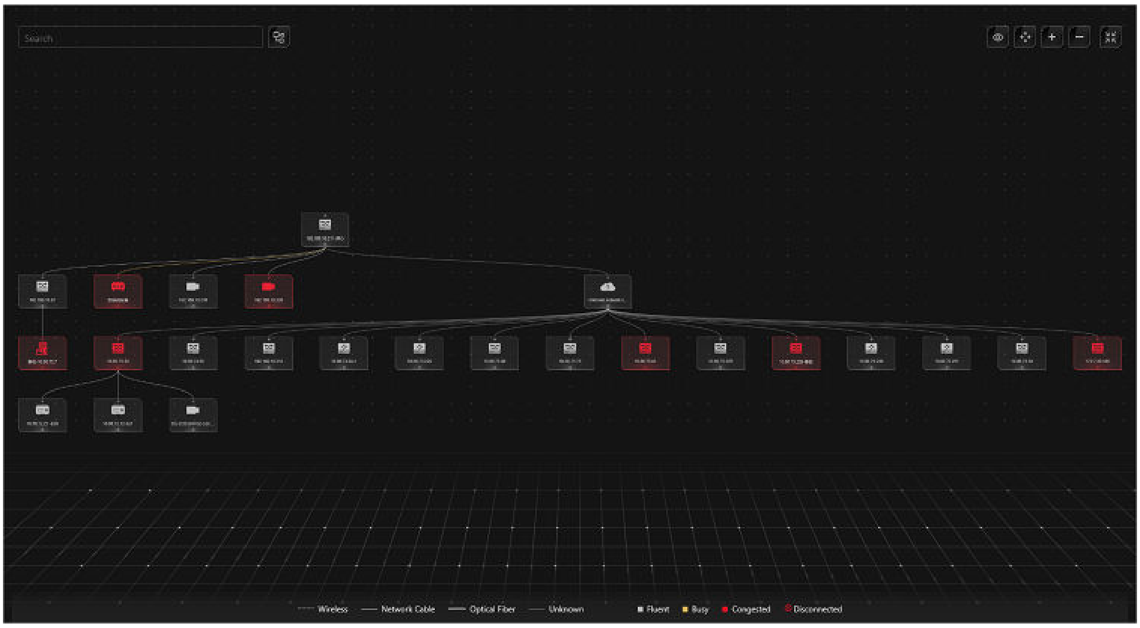


Figure 12-7 Topology Details

Device Node

The device nodes are displayed by icons, including the System Management Server, Recording Server, network transmission device, encoding device, access control device, video intercom device, network bridge, fiber converter, etc. Each device node displays the device name and IP address.

Note

- When the device information (device name, IP address, online/offline status) changes, you should manually refresh to generate the topology again or set auto-refresh.
- When the device hierarchy or physical connection changes, you should manually refresh to generate the topology again.
- If the node icon is displayed in red, it indicates that the device is abnormal or alarms are triggered. You can view the reason for device exception or alarm details.
- For the added online devices, the displayed device alias is the same as the device IP address.

View Device Details

Click the device node in the topology and click **Details** in the drop-down list. You can view the device details, including the basic information (i.e., device name, IP address and device model), device usage (e.g., RAM usage, CPU usage, PoE power), arming status and disk array (for encoding device), live video (if the device is linked with a camera), linked lane name / entrance direction / entrance & exit name / barrier control status (if the entrance and exit is linked with a camera), device panel status (i.e., ports and ports usage), and port information (i.e., port name, and peer device type, peer device IP address, and peer device name).

Note

The device details vary with different device models.

Link

The color of link indicates the utilization rate of network bandwidth (red: congested, yellow: busy, gray: fluent). And the shape of link indicates the link type (wireless, network link, optical fiber).

View Link Details

Move the cursor to the link between nodes to display the link details. You can view the upstream rate and downstream rate to determine whether the network status is normal or not. You can also view the connected device type, IP address, port name, and port status.

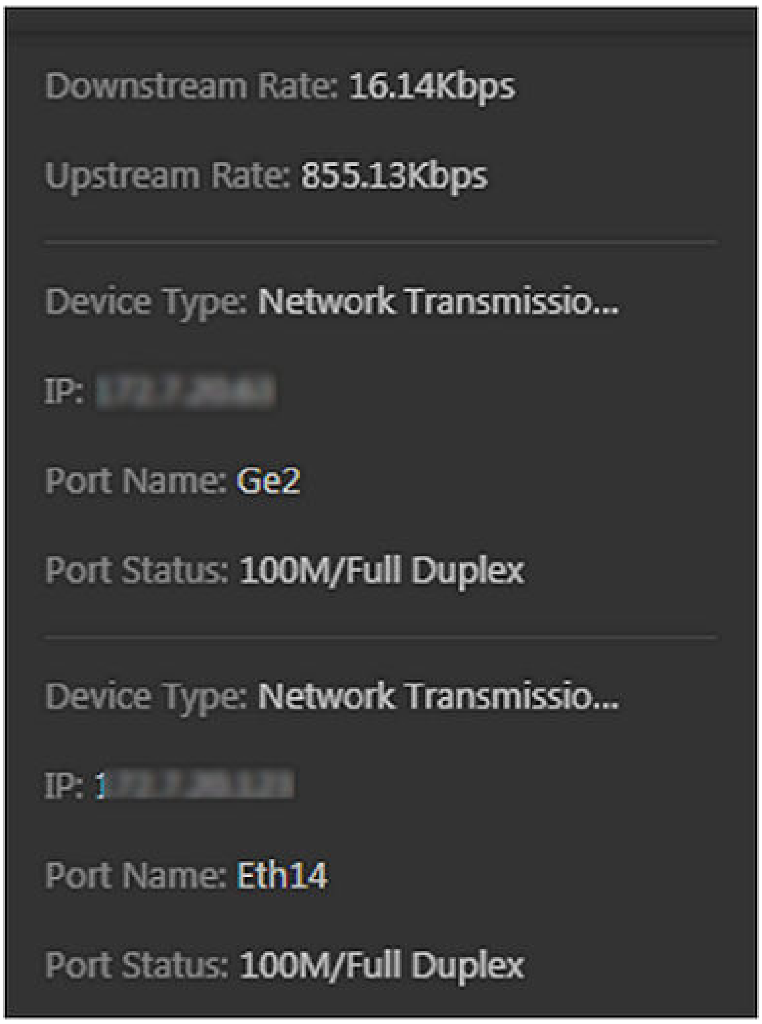


Figure 12-8 View Link Details

View Connection Path

If there is a data transmission failure between the devices, you can view the connection path to judge which link is disconnected, so as to restore the link as quickly as possible. Click the device node and in the topology and click **Show Connection Path** in the drop-down list. According to the information presented in the prompt window, click **Common Unknown Node** or **Select Node** to select the peer node, and then click **OK**. After that, the connection path between the two nodes will be displayed.

Remote Configuration

Click the device node in the topology and click **Remote Configuration** in the drop-down list to configure the device parameters, including system settings, network and port configuration. You can configure the network parameters and device port according to the network usage. For details, refer to the user manual of the device.

Note

This function should be supported by the device.

View Device Logs

When a device failure happens or trouble shooting is required, you can view the device's logs to know the alarms, notifications, operations and events of the device. Click the device node in the topology and click **View Device Logs** in the drop-down list to enter the Device Logs page, and you can set the conditions to search the device logs.

Note

This function should be supported by the device.

Set as Root Node

When you need to adjust the topology structure, you can click the device node in the topology and click **Set as Root Node** in the drop-down list to set the node as the root node.

Note

Only the switch, wireless network bridge, and fiber converter can be set as root node.

Zoom In/Zoom Out

Click or to zoom in or zoom out the device node(s) and the subsidiary device node(s). You can scroll the mouse wheel to zoom in or zoom out the topology.

Adjust Topology

Click the background of the topology to move the topology in up, down, right, or left direction.

Full Screen

Click on the upper-right corner of the topology to display the topology in full-screen mode.

Adaptive View

Click on the upper-right corner of the topology to adapt the topology to the current window, to help you know the whole topology hierarchy quickly.

Search

By entering the device name or IP address in the search box, you can quickly locate the device on the topology.

12.1.3 Historical Health Data Overview

You can view the historical online rate of resources and devices, or the recording integrity rate.

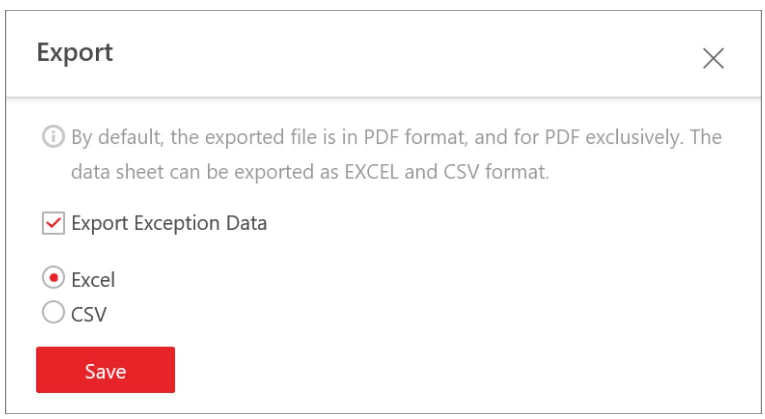
On the Health Overview area, select **History Overview** on the left.

Figure 12-9 Historical Health Data Overview

Table 12-3 Historical Health Data Page

Section	Description
Select Site	In the upper left corner of History Overview page, select a Current or Remote Site from the drop-down list to display the historical data of resources on the Site.
Filter Data	Select a time period from the drop-down list in the upper right corner of each section for filtering data by day, week, or month.
Resource Online Rate	• On the line chart, you can perform the following operations:

Section	Description
	◦ Move the cursor on the line chart to view the camera online rate and the number of offline cameras at specific time points. ◦ Click the a dot on the line to go to Resource Log page to view the detailed network status of cameras at that time point. • On the doughnut chart, you can perform the following operations: ◦ Move the cursor to red part of the doughnut chart to view the number of the cameras which once were offline and the offline rate during the time period you select. ◦ Move the cursor to the green part of the doughnut chart to view the number of the cameras which stay online and the online rate during the time period you select. • On the table, you can do one of the followings: ◦ Click **Total Offline Duration** to rank the cameras in terms of total offline duration within the time period you select. ◦ Click **Offline Times** to rank the cameras in terms of offline times within the time period you select.
Device Online Rate	• On the line chart, you can do one of the followings. ◦ Move the cursor on the line chart to view the device online rate and the number of offline devices at specific time points. ◦ Click the a dot on the line to go to Device Log page to view the detailed network status of devices at that time point. • On the doughnut chart, you can perform the following operations. ◦ Move the cursor to red part of the doughnut chart to view the number of the devices which once were offline and the offline rate during the time period you select. ◦ Move the cursor to the green part of the doughnut chart to view the number of the devices which stay online and the online rate during the time period you select. • On the table, you can do one of the followings. ◦ Click **Total Offline Duration** to rank the devices in terms of total offline duration within the time period you select. ◦ Click **Offline Times** to rank the devices in terms of offline times within the time period you select.

Section	Description
Recording Integrity Rate	To get the recording integrity rate, divide the total video length by the scheduled recording length, and then multiply the result by 100%. On the line chart, you can move the cursor to view the recording integrity rate at specific time points. Click the a dot on the line to go to Resource Log page to view the detailed resource status of devices at that time point.
Recording Copy-Back Rate	On the line chart, you can move the cursor to view the recording callback rate at specific time points. Click a dot on the line to go to Resource Log page to view the detailed resource status of devices at that time point.
Refresh	• Manually Refresh: Click **Refresh** in the upper right corner of History Overview page to manually refresh the data on the page. • Auto Refresh: Go to **Maintenance → Basic Configuration → Health Check Frequency** to set the interval for automatically refreshing the data on the page. See details in ***Set Auto-Check Frequency*** .
Export Overview Page or Exception Data	Click **Export** in the upper right corner of History Overview page to export the page in PDF format. Or you can check **Export Exception Data** to export the exception data in Excel/CSV format.  **Figure 12-10 Export Overview Page or Exception Data**

12.2 Set Basic Maintenance Parameters

You can set parameters to regularly send device and resource log reports to specified users via email, set the warning threshold for SYS usage, configure the default response timeout of the interactions among the Web Client, SYS, and devices, specify the health check frequency, and set the hierarchy and bandwidth threshold for the topology.

12.2.1 Configure Scheduled Health Check

You can configure scheduled health check to proactively detect and address potential problems and maintain the stability and reliability of your devices, services, and systems.

Before You Start

- You have set an email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- You have configured email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

1. Select **Basic Configuration → Scheduled Health Check** on the left.
2. Switch on **Scheduled Health Check**.
3. Select **Health Check Item**.

   Device Health Check

   The device check items include the password, recording exception, HDD temperature, and resolution mismatch.

   System Health Check

   The system check items include the disk space, device inspection frequency, and storage server CPU temperature.

   Service Health Check

   The service check items include the operation timeout and video loss.
4. Set the health check period.

   Note

   You can schedule health checks on a daily, weekly or monthly basis. For an automatic health check on the last day of each month, set the health check period to By Month and the health check time to Last Day. Avoid setting the health check time to 31 for months with fewer than 31 days.
5. Configure the advanced settings. This part will introduce key parameters.

   Auto Import Results to Pending Task

If you switch on **Auto Import Results to Pending Task** and check off **Replace Duplicated Pending**, the new pending task will automatically replace the old one when both the checked items and the objects of the pending tasks are the same.

Auto Export Results as Report

Switch on to send or save the health check reports.

Send Report via Email

If you have switched on **Send Report via Email**, select an email template to define the recipient information and content. You can click **Add** to add a new email template. For setting email templates, refer to ***Email Settings*** .

Upload to SFTP

To ensures secure, reliable, and efficient file transfer, upload the report to SFTP.

Note

You can click **Configure** to set the SFTP.

6. Click **Save**.

12.2.2 Send Log Report Regularly

You can send server, device, resource, and maintenance log reports to specific users regularly via email. Server log reports contain error logs, warning logs, or information logs of the user, system management server, and person. Device log reports contain information on the online/offline status of devices. Resource log reports contain the online/offline status of resources as well as the recording status. Maintenance log reports contain information on maintenance activities and tasks.

Send Resource Log Report Regularly

You can set report sending rules for camera resources, and the platform can send emails with resource log reports to specified users daily, weekly, or monthly.

Before You Start

- You have set an email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- You have configured email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

1. Select **Basic Configuration → Scheduled Report** on the left.
2. Click + to create a new report rule.

Note

If there is no report rule added before, you should click **Add** to add a new one.

3. Enter the report name, select the report type as Resource Log, and select the report language.

4. Edit the report rule. This part will introduce key settings.

Report Content

Specify the resources that you want to add into the report.

Statistical Cycle

Select the generation frequency of the report.

By Day

The report shows data on a daily basis. The platform will send a report at the sending time every day, which contains logs recorded during the day (24 hours) prior to the sending date.

For example, if you set the sending time as 20:00 and select all the dates (from Sunday to Saturday) in **Sending Date**, the platform will send a report at 20:00 every day. The report contains the logs recorded between 00:00 and 24:00 of the previous day.

By Week/Month

The platform will send a report at the sending time every week or every month, which contains logs recorded during the **Report Time** you have set.

For example, for weekly report, if you set the sending time as 6:00 on Monday in **Sending Date**, the platform will send a report at 6:00 in the morning on every Monday. The report contains logs recorded between last Monday and Sunday if you set the **Report Time** as **Last 7 Days**.

Report Time

Set the time period during which the logs will be recorded.

Send via Email

Switch on to send the report via email.

Email Template

If you have switched on **Send via Email**, Select an email template to define the recipient information and content. You can click **Add** to add a new email template. For setting email templates, refer to ***Email Settings*** .

Upload to SFTP

Switch on to upload the report to SFTP.

Note

You can click **Configure** to set the SFTP.

5. Click **Save**.

Send Device Log Report Regularly

You can set report sending rules for encoding devices or specific devices, and the platform can send emails with device log reports to specific users daily, weekly, or monthly.

Before You Start

- You have set an email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- You have configured email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

1. Select **Basic Configuration → Scheduled Report** on the left.
2. Click + to create a new report rule.

Note

If there is no report rule added before, you should click **Add** to add a new one.

3. Enter the report name, select the report type as Device Log, and select the report language.
4. Edit the report rule. This part will introduce key parameters.

Report Content

Specify the devices that you want to add into the report.

Statistical Cycle

Select the generation frequency of the report.

By Day

The report shows data on a daily basis. The platform will send a report at the sending time every day, which contains logs recorded during the day (24 hours) prior to the sending date.

For example, if you set the sending time as 20:00 and select all the dates (from Sunday to Saturday) in **Sending Date**, the platform will send a report at 20:00 every day. The report contains the logs recorded between 00:00 and 24:00 of the previous day.

By Week/Month

The platform will send a report at the sending time every week or every month, which contains logs recorded during the **Report Time** you have set.

For example, for weekly report, if you set the sending time as 6:00 on Monday in **Sending Date**, the platform will send a report at 6:00 in the morning on every Monday. The report contains logs recorded between last Monday and Sunday if you set the **Report Time** as **Last 7 Days**.

Report Time

Set the time period during which the logs will be recorded.

Send via Email

Switch on to send the report via email.

Email Template

If you have switched on **Send via Email**, Select an email template to define the recipient information and content. You can click **Add** to add a new email template. For setting email templates, refer to ***Email Settings*** .

Upload to SFTP

Switch on to upload the report to SFTP.

Note

You can click **Configure** to set the SFTP.

5. Click **Save**.

Send Server Log Report Regularly

To receive the emails of server log reports daily, weekly, or monthly, you can set report sending rules for the server.

Before You Start

- You have set an email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- You have configured email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

1. Select **Basic Configuration → Scheduled Report** on the left.
2. Click + to create a new report rule.

Note

If there is no report rule added before, you should click **Add** to add a new one.

3. Enter the report name, select the report type as Server Log, and select the report language.
4. Edit the report rule. This part will introduce key settings.

Report Content

Specify the resources that you want to add into the report.

Statistical Cycle

Select the generation frequency of the report.

By Day

The report shows data on a daily basis. The platform will send a report at the sending time every day, which contains logs recorded during the day (24 hours) prior to the sending date.

For example, if you set the sending time as 20:00 and select all the dates (from Sunday to Saturday) in **Sending Date**, the platform will send a report at 20:00 every day. The report contains the logs recorded between 00:00 and 24:00 of the previous day.

By Week/Month

The platform will send a report at the sending time every week or every month, which contains logs recorded during the **Report Time** you have set.

For example, for weekly report, if you set the sending time as 6:00 on Monday in **Sending Date**, the platform will send a report at 6:00 in the morning on every Monday. The report contains logs recorded between last Monday and Sunday if you set the **Report Time** as **Last 7 Days**.

Report Time

Set the time period during which the logs will be recorded.

Send via Email

Switch on to send the report via email.

Email Template

If you have switched on **Send via Email**, Select an email template to define the recipient information and content. You can click **Add** to add a new email template. For setting email templates, refer to ***Email Settings*** .

Upload to SFTP

To ensures secure, reliable, and efficient file transfer, upload the report to SFTP.

Note

You can click **Configure** to set the SFTP.

5. Click **Save**.

Send Maintenance Log Report Regularly

To receive the emails of maintenance log reports daily, weekly, or monthly, you can set report sending rules for your maintenance activities.

Before You Start

- You have set an email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- You have configured email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

1. Select **Basic Configuration → Scheduled Report** on the left.
2. Click + to create a new report rule.

Note

If there is no report rule added before, you should click **Add** to add a new one.

3. Enter the report name, select the report type as Maintenance Log, and select the report language.

4. Edit the report rule. This part will introduce key parameters.

Report Content

Specify the resources that you want to add into the report.

Statistical Cycle

Select the generation frequency of the report.

By Day

The report shows data on a daily basis. The platform will send a report at the sending time every day, which contains logs recorded during the day (24 hours) prior to the sending date.

For example, if you set the sending time as 20:00 and select all the dates (from Sunday to Saturday) in **Sending Date**, the platform will send a report at 20:00 every day. The report contains the logs recorded between 00:00 and 24:00 of the previous day.

By Week/Month

The platform will send a report at the sending time every week or every month, which contains logs recorded during the **Report Time** you have set.

For example, for weekly report, if you set the sending time as 6:00 on Monday in **Sending Date**, the platform will send a report at 6:00 in the morning on every Monday. The report contains logs recorded between last Monday and Sunday if you set the **Report Time** as **Last 7 Days**.

Report Time

Set the time period during which the logs will be recorded.

Send via Email

Switch on to send the report via email.

Email Template

If you switch on **Send via Email**, select an email template to define the recipient information and content. You can click **Add** to add a new email template. For setting email templates, refer to ***Email Settings*** .

Upload to SFTP

To ensures secure, reliable, and efficient file transfer, upload the report to SFTP.

Note

You can click **Configure** to set the SFTP.

5. Click **Save**.

12.2.3 Set Warning Threshold for Streaming Media Usage

An alarm can be triggered if the Streaming Media's CPU usage and RAM usage reaches a predefined warning threshold and lasts for a predefined duration, or if the channel usage of

Streaming Media reaches a predefined warning threshold. The related threshold value can be checked via the Control Client.

On the left, select **Basic Settings → Server Usage Thresholds** .

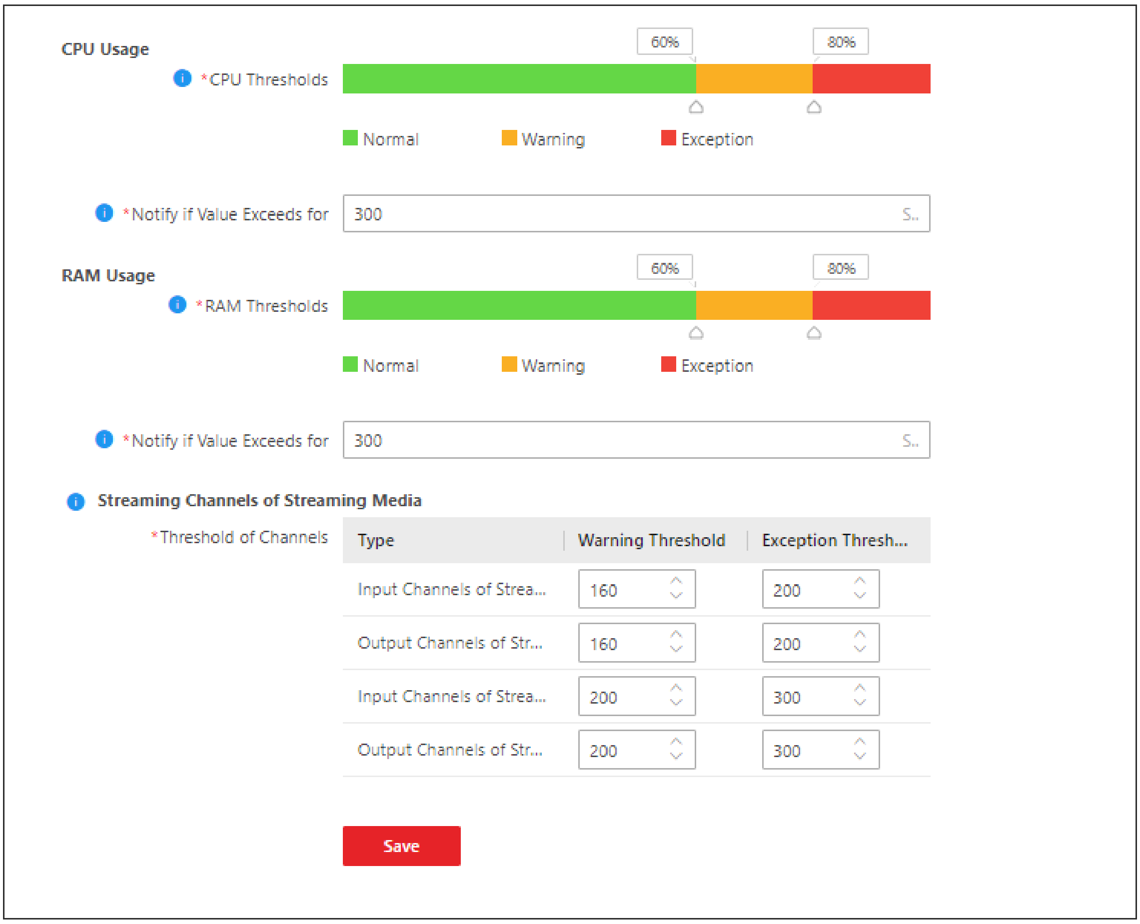


Figure 12-11 Set Server Usage Threshold

CPU/RAM Usage

Drag the ⌂ to adjust the threshold value of CPU or RAM usage, and then define the duration in the **Notify if Value Exceeds for (s)** field.

Example

- If you set the Warning threshold value to 60%, and set 20 in the **Notify if Value Exceeds for (s)** field for the CPU usage, you can view the CPU usage reaching to the Waring threshold line in the status window of SYS on the Health Status Overview page when the CPU usage reaches 60% and lasts for 20 seconds.
- If you set the Warning threshold value to 60%, set 20 in the **Notify if Value Exceeds for (s)** field for the CPU Usage, and set an alarm for CPU Warning, the alarm will be triggered when the CPU usage reaches 60% and lasts for 20 seconds.

Streaming Channels of Streaming Media

Enter a specific value in the text field or click ^ / ˅ to adjust the threshold value for the number of input or output channels of Streaming Media.

Example

If you set the Warning threshold value to 160 for the number of input channels of Streaming Media, you can view the number of used input channels reaching to the Waring threshold line in the status window of SYS on the Health Status Overview page when the number of used input channels reaches 160.

12.2.4 Set Network Timeout

Network timeout is a certain amount of time which is used to define whether the interaction among the Web Client, SYS, and devices is successful or not. To be specific, if one party fails to response after the configured timeout passes, the interaction between them is regarded as a failure.

On the left, select **Basic Settings → Network Timeout** .

Select the network timeout and click **Save**.

Table 12-4 Minimum Response Timeout in Different Interactions

Interaction Relation	Minimum Response Timeout
Between Web Client and SYS	60 s
Between SYS and Device	5 s
Between Web Client and Device	60 s

Note

This parameter affects all Web Clients accessing the current SYS.

12.2.5 Set Auto-Check Frequency

The SYS will check the health of devices, resources, and servers managed on the platform. The platform will display the health check results in the Real-Time Overview module. You can set the frequency which controls how often the platform gets the latest status of the devices, servers, and resources.

On the left, select **Basic Settings → Auto-Check Frequency** .

Device Health Status

You can set the health check frequency for different devices managed on the platform. It controls how often the platform pings these devices to determine whether they are online.

After disabled, the platform will not update the status of the managed devices. You need to refresh manually to get the latest status.

Note

You should adjust the check frequency according to the number of devices. The greater the number of devices, the lower the frequency of health checks. When the frequency set is too high, you will be prompted and recommended to set a lower frequency.

Server Health Status

You can set the health check frequency for the managed recording servers and DeepinMind servers. It controls how often the platform pings these servers to determine whether they are online.
After disabled, the platform will not update the status of the managed servers. You need to refresh manually to get the latest status.

Others

- **Device Capabilities:** Set how often the platform gets the managed devices' capabilities. After disabled, the platform will not update the capability changes of all the managed devices. You need to refresh manually to get the latest capabilities.
- **Recording Status:** Set how often the platform checks the camera's recording status. After disabled, the platform will not update the cameras' recording status.
- **Alarm/Event Enabled or Not:** Set how often the platform checks whether the event and alarm rules are enabled or not. After disabled, the platform will not update the configured event and alarm rule status.
- **Remote Alarm Enabled or Not:** Set how often the platform checks whether the event and alarm rules configured on the Remote Sites are enabled or not. After disabled, the platform will not update the configured alarm rule status configured on the Remote Sites.

12.2.6 Set Topology Show Parameters

You can set parameters in the topology of Health Monitoring module, including topology hierarchy and bandwidth threshold.

Note

For details about health monitoring, see ***Health Overview*** .

On the left, select **Basic Settings → Topology Show**

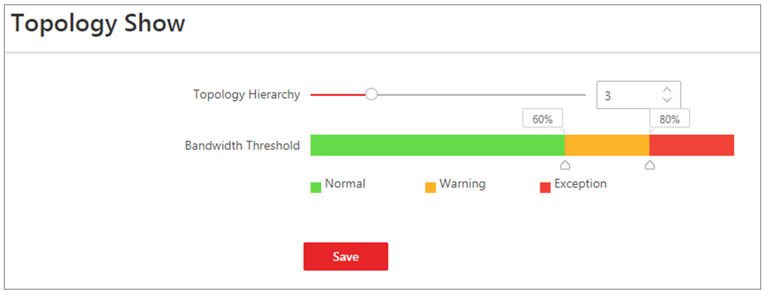


Figure 12-12 Topology Show Settings

Topology Hierarchy

If the devices connection hierarchy is complicated, you can set the topology hierarchy to display the primary devices.

Note

After setting the topology hierarchy, the topology will be generated again.

Bandwidth Threshold

When the bandwidth usage exceeds the threshold, the link on the topology will turns to the corresponding color.

12.3 Health Check

To control the health status of resources on the platform, you can perform manual health check to quickly scan the platform for potential risks by different check types, whose check items can be configured. For issues found during the health check, you can add them as pending tasks for further handling. You can also customize pending tasks according to the actual need.

On the Maintenance module, select **Health Check** on the left.

12.3.1 Perform Manual Check

You can manually start health check to quickly scan the platform for potential risks and configure check items for different check types.

Select **Manual Check** on the left.

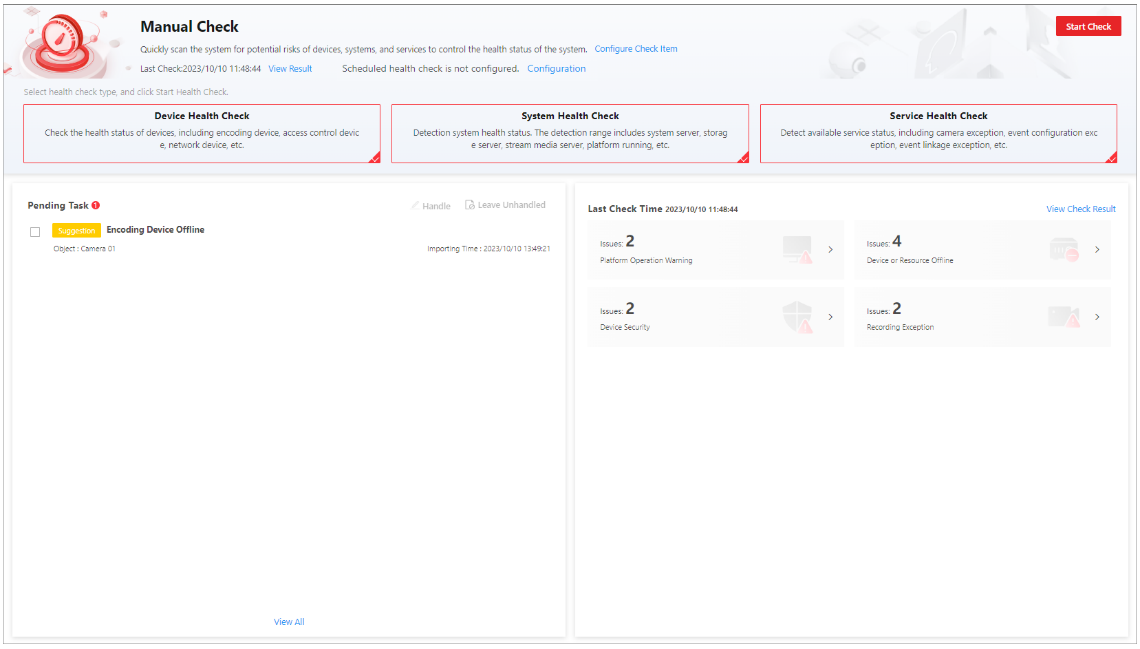


Figure 12-13 Manual Check Page

On this page, you can perform the following operations.

- ***Start Health Check Manually***
- ***Configure Check Items***
- ***Manage Pending Tasks***
- ***View Last Check Results***

Start Health Check Manually

Click **Device Health Check**, **System Health Check**, or **Service Health Check** at the top of the Health Check page to select the type(s) to be checked, and then click **Start Health Check** in the top right corner to enter the Checking page.

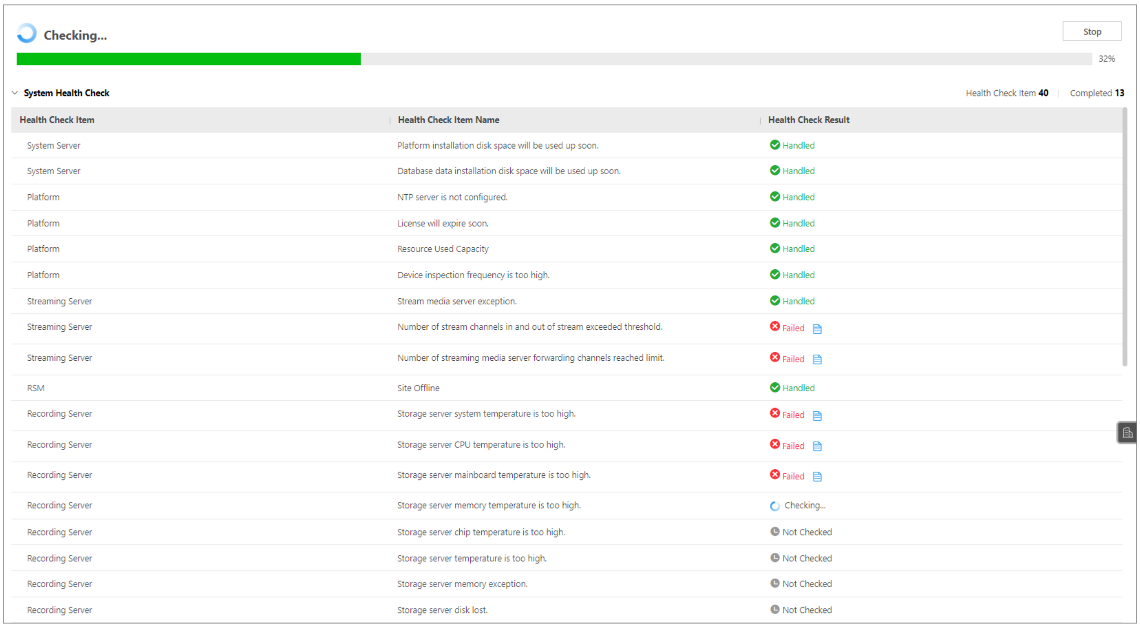


Figure 12-14 Checking Page

During the health check, you can view the progress percentage, real-time check items, and result. For failed items, you can click in the Health Check Result column to view the failure details. You can also click **Stop** in the top right corner to cancel the health check.

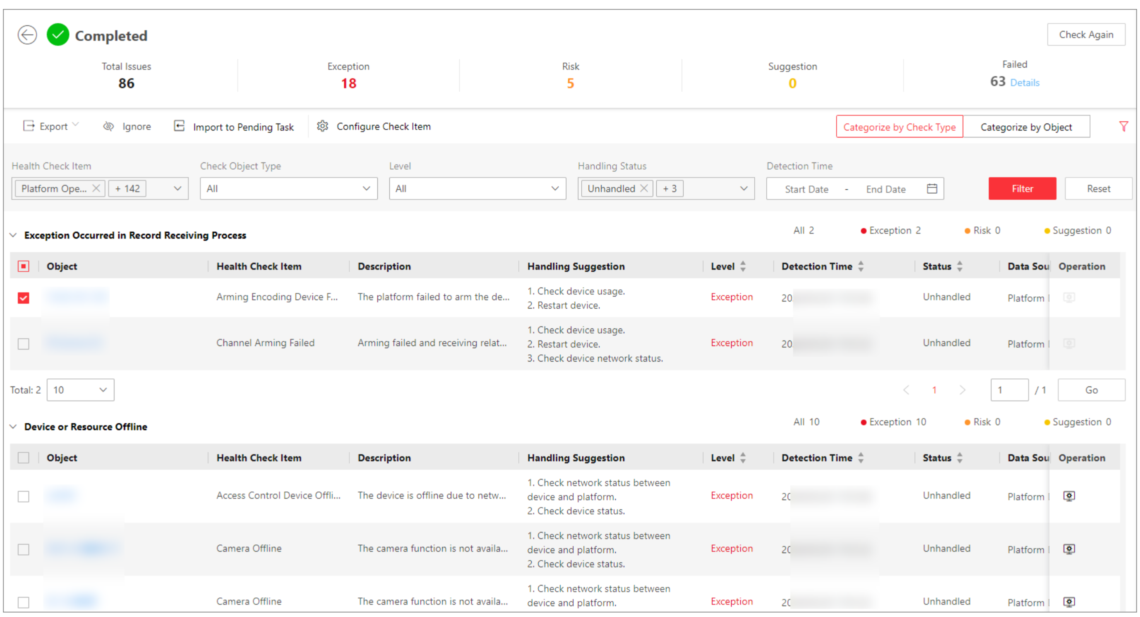


Figure 12-15 Completed Page

When the health check completes, you can perform the following operations.

- View the total numbers of issues, exceptions, risks, suggestions, and failed items, or click **Details** besides the number of failed items to view the failed item details.
- Click **Configure Check Item** to view the health check item list and ignored check items. For more operations on the Health Check Item List page, refer to ***Configure Check Items*** .
- Click **Categorize by Check Type** or **Categorize by Object** at the top of the issue list to display and calculate issues by health check type or object. You can click in front of a category name to unfold the category to view more details.
- Click in the top right of the issue list to open the filter pane and set conditions to filter the issues.
- Move the cursor over the **Export** button and click **Export All** to export all issues to the local PC.
- Check the issue(s) in the list and click **Export** at the top of the issue list to export the selected issue(s) to the local PC.
- Check the issue(s) in the list and click **Import to Pending Task** to move the selected issue(s) to the pending task for further management. Refer to ***Manage Pending Tasks*** for details.
- Click the object name to view the device details and information, and click to go to the device configuration page.
- Check the issue(s) in the list and click **Ignore** to ignore the selected issues.
- Click **Check Again** to start the health check again.

Note

If you want to start health check regularly, you can click **Configure** on the top of the Manual Check page to enable the scheduled health check. For detailed operations, refer to ***Configure Scheduled Health Check*** .

Configure Check Items

On the top of the Manual Check page, click **Configure Check Item** to enter the Health Check Item List page.

- Under the **Configure Check Item** Tab
  - Click in front of the category name to display the available check items.
  - Click in the Operation column of an item which is not ignored and select the object to take effect. Once the check item is ignored, the issues of the selected object checked by this item will not be reported.
- Under the **Ignored Check Item** Tab
  - Click **Categorize by Check Type** or **Categorize by Object** to display the ignored check items by check type or object.
  - Check the ignored item(s) and click **Restore** to cancel ignoring them.

Manage Pending Tasks

On the Pending Task section, the issues imported to the pending task will be listed.

Click a pending task name to edit its name, level, notes, and email notification settings on the right pane.

Move the cursor over a pending task and click **Handle** or **Leave Unhandled** to handle a single task.

Check the pending task(s) and click **Handle** or **Leave Unhandled** in the top right corner of the section to batch handle the selected task(s).
The handled pending tasks will disappear from the Pending Task section and display on the Maintenance Log page. For details, refer to ***Search for Maintenance Logs*** .
Click **View All** at the bottom of this section to enter the Pending Task page. For details, refer to ***Add Custom Pending Tasks*** .

View Last Check Results

On the Last Check Time section, the last check time and the corresponding issue overview will be displayed.
Click > of an issue category to enter the Health Check Result page and locate to the corresponding details list.
Click **View Check Result** in the top right corner of the Last Check Time section or click **View Result** on the top of the Manual Check page to enter the Health Check Result page.

12.3.2 Add Custom Pending Tasks

The Pending Task page lists the custom pending tasks besides pending tasks imported from the Manual Check page. You can add custom pending tasks to accommodate your needs, handle, ignore, delete, and export pending tasks, and batch set notifications. This section will guide you through adding custom pending tasks.

Steps

1. Select **Pending Task** on the left.
2. Select **Add Custom Pending Task**. This part will introduce key parameters.

   Level

   Select one of the following three levels:

   - **Exception**: It refers to an error or an exceptional situation. For example, if a device goes offline due to network issues, it would be considered an exception.
   - **Risk**: It refers to potential compromise of a function or system due to certain factors. For example, if you set a weak password, the device information risks being leaked.
   - **Suggestion**: It refers to a recommendation or advice that improve the performance or functionality of a system. For example, configuring the NTP server or adjusting the device inspection frequency are suggestions to enhance the system's performance.

   Email Notification

   To receive emails of pending task notifications at a scheduled time, switch on **Email Notification**. You can add a new email template or select an email template to define the recipient information and content. For setting email templates, refer to ***Email Settings*** .
3. Click **OK** to save the settings.
4. **Optional:** After adding pending tasks, you can edit them, handle them, leave them unhandled, delete them, batch set notifications, batch disable notifications, export these tasks, filter these

tasks according to various conditions, set the adaptive column width, and customize column items.

12.4 Resource Status

You can monitor the status of the added resources, such as access control devices and Recording Servers, which helps you find out and maintain the abnormal resources in time, ensuring the smooth running of the platform to the greatest extent.

On the top, select → **Basic Management → Maintenance → Resource Status** .

Select a resource type to perform the following operations.

Common Operations

Operation	Description
Filter Resource Status	Check the checkbox in the top right of status display page to select exception types from the drop-down list to filter the resource status.
View Device Status	Click the device name to view the status details and basic information of the device.
Configure Device	Click in the Operation column to go to the Area page to configure the parameters of the specified device.
Filter Device	Select the device type(s) from the first drop-down list on the top to filter the device status by device type.
Export Status Data	Click **Export** to export the status data as CSV or Excel to the local PC.
Refresh Resource Status	Click in the Operation column to refresh the status of the specified resource, or click **Refresh** to refresh the status of all resources displayed on the page. **Note** The resource status will be automatically refreshed in a specified interval.
Edit Current Value	Click in the Current Value column to edit current value of the device.

Camera Status

Operation	Description
View Related Camera Status	Click the IP address to view the status of the device to which the camera is related.
View Online/Offline Records	Click in the Operation column to view the online/offline records of the specified camera. **Note** This operation is not available for the cameras added on Remote Sites.
View the Recording Status	Click in the Operation column to view the recording status of the camera. **Note** This operation is not available for the cameras added on Remote Sites.
View Camera with Abnormal Image	Click **View Camera with Abnormal Image** to view the videos of cameras with abnormal images. And you can also export the image diagnosis results of selected camera(s) or all cameras in PDF format.

Door Status

Operation	Description
Control Door Status	Click in the Operation column and select a control type from the drop-down list to control the door status. • **Unlock**: When the door is locked, unlock the door and it will be open. After the open duration (configured via the Web Client), the door will be closed and locked again automatically. • **Lock**: When the door is unlocked, lock the door and it will be closed. The person who has the access permission can access the door with credentials. • **Remain Unlocked**: The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required (free access).

Operation	Description
	Note For the door linked to video intercom device, setting its status to remain unlocked is not available. • **Remain Locked**: The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the user with super access permission.
Ignore Device Status	Click on the top to ignore the RS-485 card reader status.

Encoding Device Status

Operation	Description
View Error Details	In the **Disk Status** column, view the error details if a disk is abnormal.
View Recording Status of Channels	Click the status in the **Recording Status** column to view the recording status of channels configured to store the video files on this encoding device. If the recording settings are abnormal, you can click **Exception** in the **Recording Status** column to view the exception details in the pop-up pane.
Wake Up Solar-Powered Camera	Click to wake up a solar-powered camera if it is in the sleep mode.
View Online/Offline Records	Click in the Operation column to view the online/offline records of the encoding device.

On-Board Device Status

Operation	Description
Print Debugging Log Command	Click in the Operation column to print debugging log command.
Export Device Logs	Click in the Operation column to export logs of an device.

12.5 Log Search

Three types of log files are provided: server logs, device logs, and resource logs. The server logs refer to the logs files stored in the SYS server on the current site and remote sites; The device logs refer to the log files stored on the connected devices, such as encoding device and security control device; The resource logs refers the logs about camera recording status, online status, and call-back status. You can search the log files, view the log details and backup the log files.

12.5.1 Search for Server Logs

You can search for server logs of the current site or Remote Sites, which contain error logs, warning logs and information logs. Server logs contain historical user and server activities. You can search for the logs and then check the details.

Steps

1. On the left, select **System Log → Server Logs** .
2. In the **Site** area, select the current site or a Remote Site.
3. In the **Event** area, select one or multiple log types and sub types.

   Note

   Error logs record failures or errors. Warning logs record license expiration events. Information logs refer to other general logs which record successful or unknown operation results.
4. In the **Source** area, set the source of the logs that you want to search for.
5. **Optional:** In the **Resource Name** area, enter the name of a resource to search the logs of the resource.
6. Set the time range for search.

   Note

   You can select **Custom** to set a precise start time and end time.
7. Click **Search**.

   All matched logs are listed with details on the right.
8. **Optional:** Check all or specific logs, click **Export**, and then select a file format (i.e., Excel or CSV) to download the searched logs as a single file to your local PC.

12.5.2 Search for Online/Offline Logs of Device

You can search for the online/offline logs of all devices. The online/offline logs provide information on the current device status (online or offline), latest offline time, total offline duration, etc.

Steps

1. On the left, select **System Log → Device Log** .
2. In **Type**, select **Online/Offline Log** as the log type.
3. Select a device type and check the devices you want to search.
4. In **Time**, specify the time range of this search.

   Note

   You can select **Custom Time Interval** to set a precise start time and end time.

5. **Optional:** If there are a large number of devices, switch on **Filtering Time** to set a range of total offline times during the specified time range to filter the devices, or set a total offline duration to filter the devices.
6. Click **Search**.

   The offline/online log of each device are listed on the right. You can check the name, IP address, current status (online/offline), latest offline time, total offline times, and total offline duration of each device.
7. **Optional:** Perform further operations after searching for device logs.

View Offline History	Click on device name to view history online duration (displayed as a line chart) and status (displayed as a list) of the device. You can perform the following operations. • Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter the data. • View Details: Move the cursor to the line chart to view the detailed offline and online duration at each time point.
View Device Logs	Click in the Operation column to view the logs stored on the device.
Export Logs	Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC.

12.5.3 Search for Logs Stored on Device

You can search for the logs stored on encoding devices, security control devices, decoding device, network transmission devicesaccess control devices, elevator control devices, on-board device, and fire protection device.

Steps

1. On the left, select **System Log → Device Log** .
2. Select **Log on Device** as the log type.
3. Select a device type and select the device you want to search.
4. Select the main event as **Normal** or **Battery Information** and check the sub event(s) to be searched for.
5. Specify the time range of this search.

   Note

   You can select **Custom Time Interval** to set a precise start time and end time.
6. Click **Search**.

   All matched logs are listed with details on the right.
7. **Optional:** Perform further operations after searching for device logs.

View Offline History	Click on device name to view history online duration (displayed as a line chart) and status (displayed as a list) of the device. You can perform the following operations. • Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter the data. • View Details: Move the cursor to the line chart to view the detailed offline and online duration at each time point.
View Device Logs	Click in the Operation column to view the logs stored on the device.
Export Logs	Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC.

12.5.4 Search for Online/Offline Logs of Resource

You can search for the online/offline logs of cameras on the current site. The online/offline logs provide information on the current device's status (online or offline), latest offline time, total offline duration, etc.

Steps

1. On the left, select **System Log → Resource Logs** .
2. In **Type**, select **Online/Offline Log**.
3. Click to show the area list on the current site and then select the cameras whose logs are to be searched for.
4. **Optional:** Modify your selection in the selected camera list.

Remove a Camera	Click to remove the camera from the list.
Remove All Cameras	Click to remove all cameras in the list.

5. In **Time**, specify the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

6. **Optional:** If there are a large number of devices, switch on **Filtering Time** to set a range of total offline times during the specified time range to filter the devices, or set a total offline duration to filter the devices.
7. Click **Search**.

The offline/online log of each resource are listed on the right. You can view the name, IP address, current status (online/offline), latest offline time, total offline times, and total offline duration of each resource.

8. **Optional:** Perform further operations after searching fro resource logs.

View Offline History	Click resource name to view history online duration (displayed as a line chart) and status (displayed as a list) of the resource.

	You can perform the following operations. • Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter data. • View Details: Move the cursor to the line chart to view the detailed offline and online duration at each time point.
View Device Online/ Offline Logs	Click the IP address to view the online/offline logs of the device where the resource is linked.
Export Logs	Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC.

12.5.5 Search for Recording Status of Resource

You can search for the recording status of cameras on the current site. The recording status includes the recording integrity rate, total time length abnormal recording, times of recording interruptions, etc.

Steps

1. On the left, select **System Log → Resource Logs** .
2. In **Type**, select **Recording Status**.
3. Click to show the area list of the current site and then select the cameras whose logs are to be searched for.
4. **Optional:** Modify your selection in the selected camera list.

Remove a Camera	Click and then click to remove a camera from the list.
Remove All Cameras	Click and then click to remove all cameras in the list.

5. In **Time**, specify the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

6. **Optional:** If there are a large number of resources, check **Filter Condition** and set the filter conditions.

Retention Duration (Days)

Set a range of the retention duration of the recorded video footage to filter the cameras.

Recording Integrity Rate

Set a range of the recording integrity rate to filter cameras. The recording integrity rate refers to the percentage obtained from dividing the actual recording duration by the scheduled recording time.

Note

For details about recording schedule, refer to ***Configure Recording Schedule Template*** .

7. Click **Search**.

   Recording status of each camera are listed on the right, including camera name, camera IP address, area where the camera belong, video storage type, etc.

   Start Time

   The time when the camera started recording.

   End Time

   The latest time when the camera was recording.

   Retention Duration (Days)

   The retention duration (unit: day) of the recorded video footage refers to the duration between **Start Time** and **End Time**.

   Total Length

   The total time length of video storage.

   Abnormal Total Length

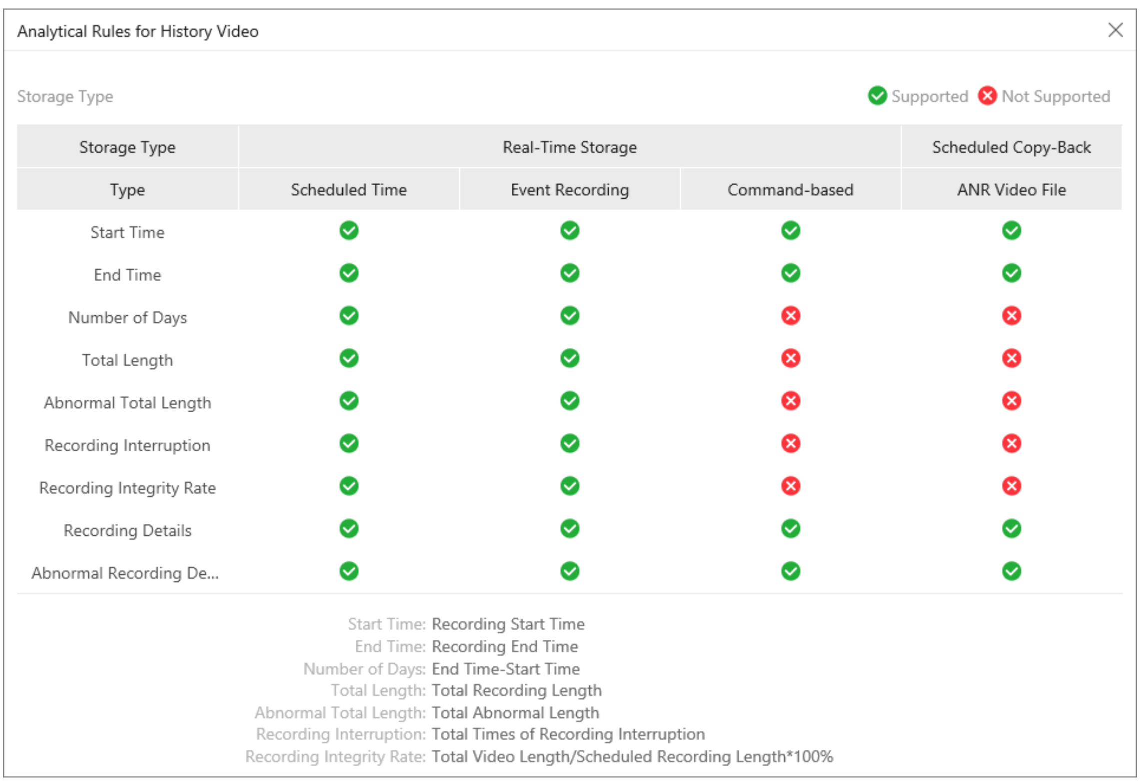
   The total time length of the video loss within the scheduled time.

   Recording Interruption

   The total times of recording interruption within the scheduled time.

8. **Optional:** Check historical recording status.

   1) **Optional:** Click **Rule** in the top right corner to view the analytical rules for history videos.



Analytical Rules for History Video

Storage Type

Supported / Not Supported

Storage Type	Real-Time Storage			Scheduled Copy-Back
Type	Scheduled Time	Event Recording	Command-based	ANR Video File
Start Time	Supported	Supported	Supported	Supported
End Time	Supported	Supported	Supported	Supported
Number of Days	Supported	Supported	Not Supported	Not Supported
Total Length	Supported	Supported	Not Supported	Not Supported
Abnormal Total Length	Supported	Supported	Not Supported	Not Supported
Recording Interruption	Supported	Supported	Not Supported	Not Supported
Recording Integrity Rate	Supported	Supported	Not Supported	Not Supported
Recording Details	Supported	Supported	Supported	Supported
Abnormal Recording De...	Supported	Supported	Supported	Supported

Start Time: Recording Start Time
End Time: Recording End Time
Number of Days: End Time-Start Time
Total Length: Total Recording Length
Abnormal Total Length: Total Abnormal Length
Recording Interruption: Total Times of Recording Interruption
Recording Integrity Rate: Total Video Length/Scheduled Recording Length*100%

Figure 12-16 Analytical Rules for History Video

2) Click a camera name to open the History Recording Status panel.

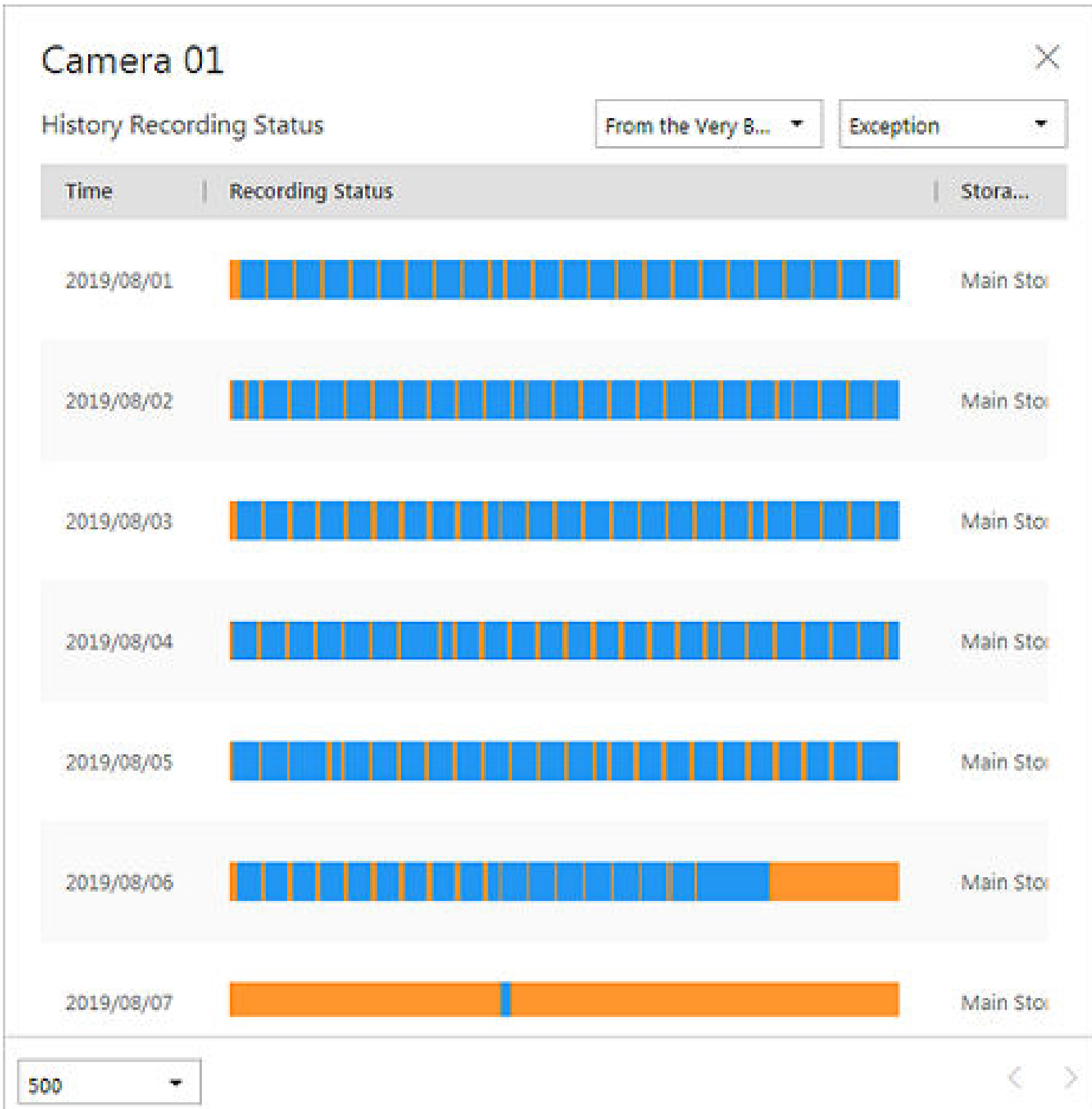


Figure 12-17 History Recording Status

Note

The blue parts on the time bars represent the time periods during which video footage were recorded. The orange parts on the time bars represent the time periods during which video loss occurred or the time periods during which no recording schedule existed.

3) Select a time period and a status (abnormal or all) from the drop-down lists respectively to filter data.

4) **Optional:** Select the number of records displayed on each page of the History Recording Status panel from the drop-down list at the lower-left corner of the panel.

5) **Optional:** Move the cursor to the time bar to show the 24 hours on it, and click one hour to view recording status details within the hour.

9. **Optional:** Click **Export**, and then select a file format and a report type to download the searched logs as a single file to your local PC.

12.5.6 Search for Call-Back Status of Resource

You can search for the call-back status of cameras on the current site. In search results, you can view the camera name, storage type, recording copy-back rate, etc.

Steps

1. On the left, select **System Log → Resource Logs** .
2. In **Type**, select **Call-Back Status**.
3. Click to show the area list of the current site and then select the cameras whose logs are to be searched for.
4. **Optional:** Modify your selection in the selected camera list.

Remove a Camera	Click and then click to remove a camera from the list.
Remove All Cameras	Click and then click to remove all cameras in the list.

5. In **Time**, specify the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

6. Click **Search**.

   Call-back status of each camera are listed on the right.
7. **Optional:** Click **Export** and then select a file format (i.e., Excel or CSV) to download the call-back status to your local PC.

12.5.7 Search for Maintenance Logs

Maintenance logs serve as a reference for troubleshooting and analyzing the history of maintenance events to improve efficiency and reliability. You can search for maintenance logs based on the handler, handling time, handling status and other conditions.

Steps

1. On the navigation bar, select → **Basic Management → Maintenance → System Log** .
2. Select **Maintenance Log** on the left.
3. Edit the search parameters, namely the pending task name, object, level, handler, handling time, and handling status. This part will introduce key parameters.

   Object

   The objects undergoing the health check.

   Level

Select one of the following three levels:

- Exception: It refers to an error or an exceptional situation. For example, if a device goes offline due to network issues, it would be considered an exception.
- Risk: It refers to potential compromise of a function or system due to certain factors. For example, if you set a weak password, the device information risks being leaked.
- Suggestion: It refers to a recommendation or advice that improve the performance or functionality of a system. For example, configuring the NTP server or adjusting the device inspection frequency are suggestions to enhance the system's performance.

4. Click **Search**.

   All matched logs are listed with details on the right.

5. **Optional:** Select specific logs, click **Export** or click **Export → Export All** in the pull-down menu in the upper-right corner of the page, and then select a file format (Excel or CSV) to download the searched logs as a single file to your local PC.

12.6 Service Manager

After successfully installing the service module(s), you can run the Service Manager and perform related operations of service, such as starting, stopping, or restarting the service.

Steps

1. Right-click  and select **Run as Administrator** to run the Service Manager.

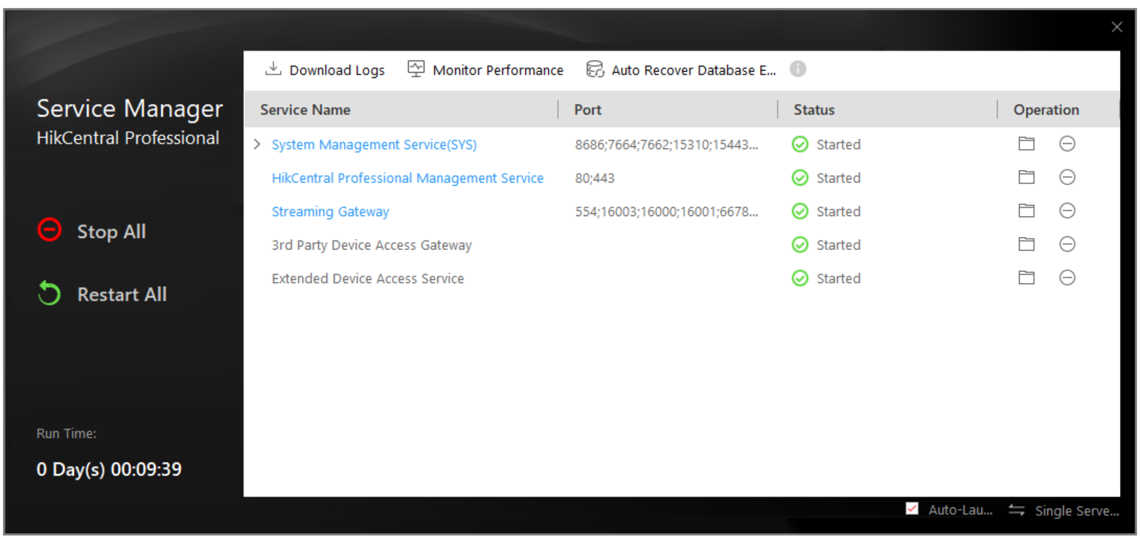


Figure 12-18 Service Manager Main Page

Note

The displayed items vary with the service modules you selected for installation.

2. **Optional:** Perform the following operation(s) after starting the Service Manager.

Stop All	Click **Stop All** to stop all the services.

Restart All	Click **Restart All** to run all the services again.
Stop Specific Service	Select one service and click ⊖ to stop the service.
Edit Service	Click the service name to edit the port of the service. **Note** If the port number of the service is occupied by other service, the port No. will be shown in red. You should change the port number to other value before the service can work properly.
Open Service Location	Select one service and click to go to the installation directory of the service.

3. **Optional:** Click **Auto Recover Database Exception** to recover database exception caused by accidents such as power-off and unexpected reboot.
   1) Enable **Auto Recover Database Exception**.

   Note

   The database service will restart after you enable this function.

   2) Click to set the archive path for recovering the database.

   Note

   - The remaining disk space of the archive path should be twice as the size of database data.
   - The archive path should be under a path in English.

   3) Click **OK** to finish setting.
4. **Optional:** Check **Auto-Launch** to enable launching the Service Manager automatically after the PC started up.
5. Click **Dual-Server Deployment** to deploy the database on another server.

12.7 Set System Data Backup

To restore the original system data after a data loss event or recovering data from an earlier time, you can manually back up system data, or configure a schedule to back up regularly. System data includes data configured in the system, pictures, received events and alarms, card swiping data, and maintenance data.

Steps

Note

The backups are stored in the SYS server. You can edit the saving path only on the Web Client running on the SYS server.

1. In the top right of the client, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Back Up** tab.
3. In **Type**, select the data that you want to back up.
4. Set a backup schedule to run backup regularly.
   1) In **How Often**, select the frequency to back up the system data.
   2) In **Which Day** and **When**, specify which time to back up.
   3) In **Max. Number of Backups**, set the maximum number of backup files. Old backup files will be automatically deleted.

   Note

   The value ranges from 1 to 5.
5. Save the settings.
   - Click **Save** to save the backup schedule.
   - Click **Save and Back Up Now** to back up the system data immediately, and you can monitor the backup progress in the progress bar window.

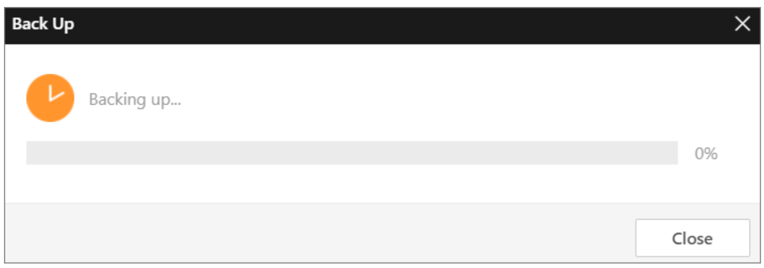


Figure 12-19 Backup Progress

12.8 Restore System Data

When an exception occurs, you can restore the system data if you have backed up system data before.

Before You Start

Make sure you have backed up system data. Refer to ***Set System Data Backup*** for details.

Steps

Note

System data recovery will restore the system to an earlier state, and thus the data added after backup date will be lost.

1. In the top right of the Home Page, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Restore** tab.

3. Select a backup file to be restored.

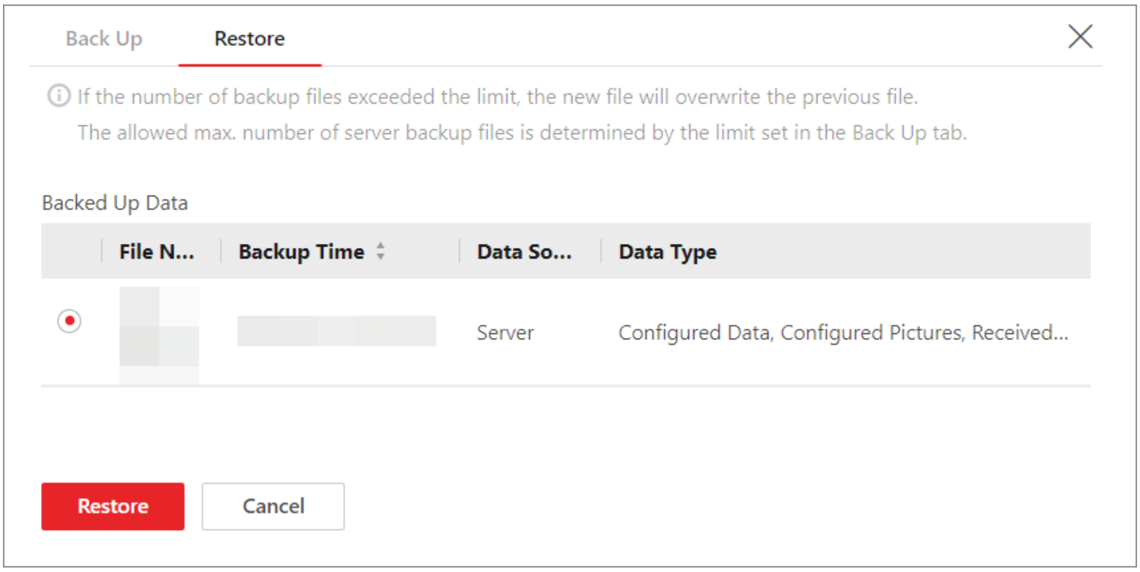


Figure 12-20 Restore System Data

4. Click **Restore** to confirm the system data recovery.

What to do next

After restoring the system data, you must reboot the SYS service via Service Manager and log in to Web Client again.

12.9 Export Configuration Data

You can export and save configuration data to local disk, including recording settings and resource configurations.

Steps

1. In the top right of the client, click **Maintenance and Management → Export Configuration Data** .
2. Select the configuration data types that you want to export.

Note

If you enable Password Protection, you can export only the configuration data of encoding devices, and you need to set a password.

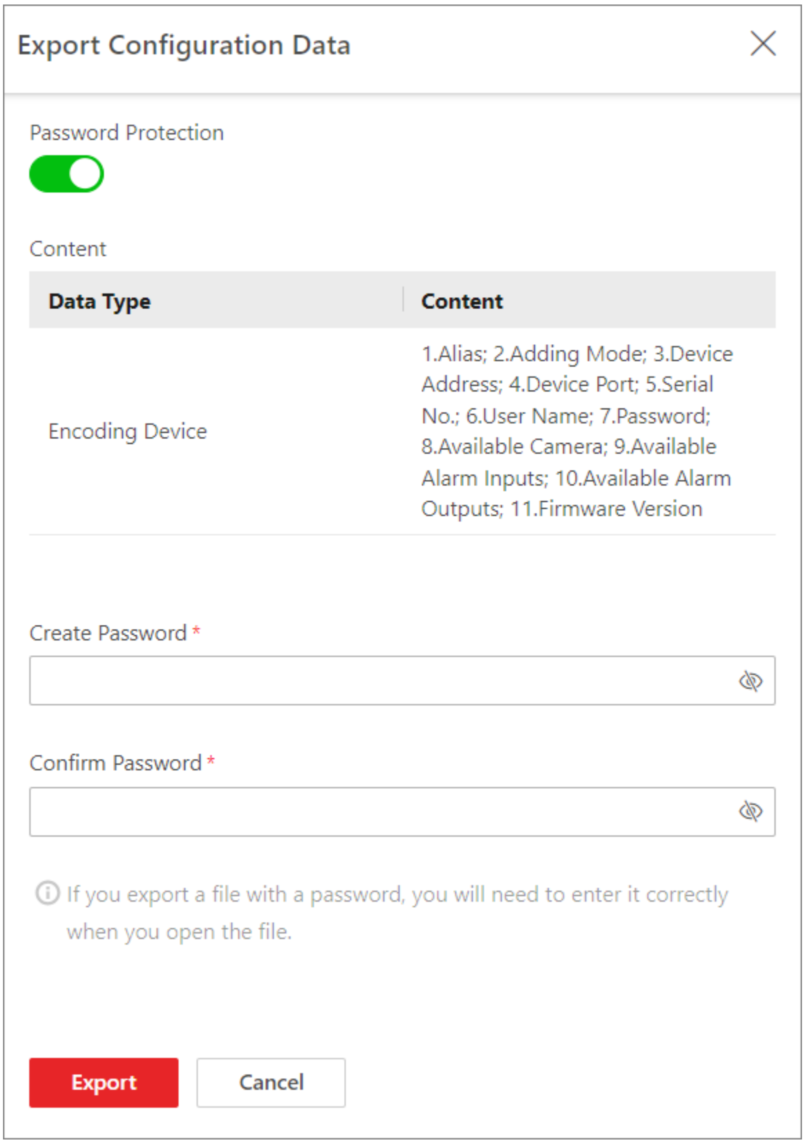


Figure 12-21 Password Protection

3. Click **Export** to download the data to the local PC.

Note

The configuration data file is in CSV format.

Chapter 13 Remote Site Management

You can add other HikCentral Professional without RSM (Remote Site Management) module to the HikCentral Professional with RSM module as the Remote Site for central management.

On the top navigation bar, select → **Basic Management → Remote Site Management** .

After adding the Remote Site to the Central System, you can manage the Remote Site's cameras (such as live view and playback), add the Remote Site's configured alarms so that you can manage the alarms via the Central System, and set the recording schedule for the Remote Site's cameras and store the recorded video files in the Recording Server added to the Central System.

Remote Site

If the HikCentral Professional doesn't have RSM module (based on the License you purchased), you can add it to the Central System as Remote Site.

Central System

If the HikCentral Professional has RSM module (based on the License you purchased), you can add other Remote Sites to this system. This system and the added Remote Sites are called Central System.

Note

- The system with RSM module cannot be added to other Central System as Remote Site.
- If one Remote Site has been added to one Central System, it cannot be added to other Central System.

13.1 Basic Configuration

Select **Basic Configuration** on the left panel.

Check **Receive Site Registration** if you need to access the system via WAN, and click **Save**.

13.2 Add Remote Site

You can add a remote site to the platform by IP address or domain name, add a remote site registered to the Central System, and batch adding remote sites.

Enter the Add Remote Site page by one of the following methods.

- If no Remote Site is added, click **Add Site** to enter the Add Remote Site page.
- If you have already added Remote Site, click + on the left to enter the Add Remote Site page.

Note

If you did not set the NTP server which is used for synchronizing the time between the SYS and the NTP server, a message will be displayed on the top of this page. If you need, click the button to go to the System Configuration page.

Adding Mode and Scenario	Description
Add Remote Site by IP Address or Domain Name: you know the IP address or domain name of the Remote Site to be added.	1. Select **IP Address/Domain** as the adding mode. 2. Enter the required information. 3. (Optional) Enable receiving the alarms configured on the Remote Site. a. Switch on **Select Configured Alarms to Be Received by Central System** to display all the configured alarms on a Remote Site. b. Select **All Alarms** or **Specified Alarm**. If the latter is selected, click to filter the configured alarms by the alarm source, area, triggering event, etc. c. Select the configured alarm(s). **Note** - After receiving the alarm from Remote Site, the alarm will be configured as alarm in Central System automatically. You can click **Default Configuration Rule** to view the imported alarms' default settings including alarm name, alarm priority, actions, etc. - 4. (Optional) Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System. 5. Click **Add** to add the remote site.
Add Remote Site Registered to Central System: the Remote Sites have been registered to the Central System and the Central System also enabled the receiving site registration function.	1. Select **Site Registered to Central System** as the adding mode. 2. Select the Remote Site(s) and enter the user name and password of the Remote Site(s). 3. (Optional) Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System. 4. Click **Add** to add the remote site.
Add Remote Sites in a Batch: add multiple Remotes Sites at a time for convenience.	1. Select **Batch Import** as the adding mode. 2. Click **Download Template** and save the predefined template on your PC.

Adding Mode and Scenario	Description
	3. Open the exported template file and input the required information of the Remote Sites to be added on the corresponding column. 4. Click and select the template file. 5. (Optional) Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System. 6. Click **Add** to add the remote site.

When adding Remote Site, the site's cameras and area information are imported to the Central System by default.

After adding the remote site, you can delete and refresh the newly added site, and search for it using its name.

13.3 Back Up Remote Site's Database to Central System

After adding the Remote Site, you can back up the database of the Remote Site to the Central System. The database backup can be performed according to the configured schedule or immediately. In case of the data deletion or corruption following a natural or human-induced disaster, you can recover the data to ensure the business continuity.

Steps

1. In the site list on the left, click the Remote Site name to view its details.

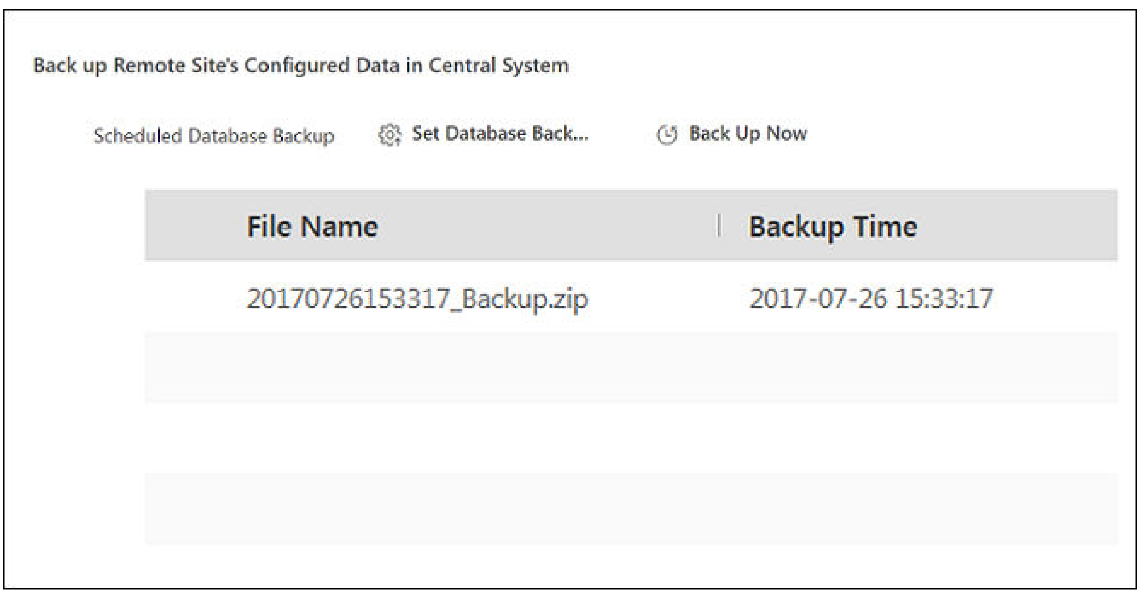


Figure 13-1 Back Up Remote Site Database in Central System

2. Click **Back Up Now** to back up the Remote Site's database manually.
3. **Optional:** Set the backup parameters and enable scheduled database backup if needed to back up the Remote Site's database regularly.
   1) Click **Set Database Backup** to open the Set Database Backup dialog.

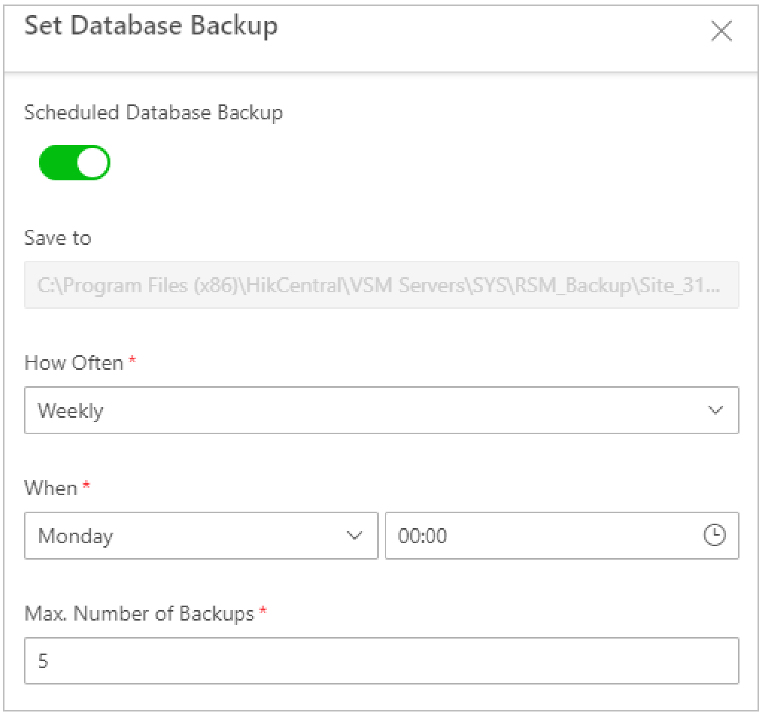


Figure 13-2 Set Database Backup

   2) Switch on the **Scheduled Database Backup** to enable the scheduled backup.
   3) Select how often to back up the database.

Note

If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

   4) Select what time of the day to start backup.
   5) Set the **Max. Number of Backups** to define the maximum number of backup files available on the system.

Note

The maximum number of the backups should be between 1 to 5.

   6) Click **Save**.

Result

The backup file (including manual backup and scheduled backup) will display in the list, showing the file name and backup time.

13.4 Edit Remote Site

After adding the Remote Site, you can view and edit the added Remote Site's information and set its GPS location.

Steps

1. In the site list on the left, click the Remote Site name to view its details.
2. View and edit the basic information of the Remote Site, including IP address, port, and name.

   Note

   You cannot edit the address and port of the site registered to the Central System.
3. In the original information section, view the Remote Site's site name, system ID, system version, and GPS location.

   Note
4. **Optional:** In the upper-left corner, Click **Configuration on Site** to open the Web Client of the Remote Site and log in for further configuration.

   Note

   The site should be online if you need to enter its Web Client.
5. Click **Save**.

13.5 View Remote Site's Changes

When there are changed resources on the Remote Site, such as newly added, deleted, renamed cameras, doors, or elevators, you can view the updated resources and synchronize the resources in Central System with the Remote Site.

Steps

Note

The site should be online if you need to view the changed resources.

1. Click in the site list on the left to get the latest status of the Remote Sites.
2. Click the site name whose resources are changed to enter its details page.
3. On the upper-right corner, click **Changes of Remote Site** to view the changes.

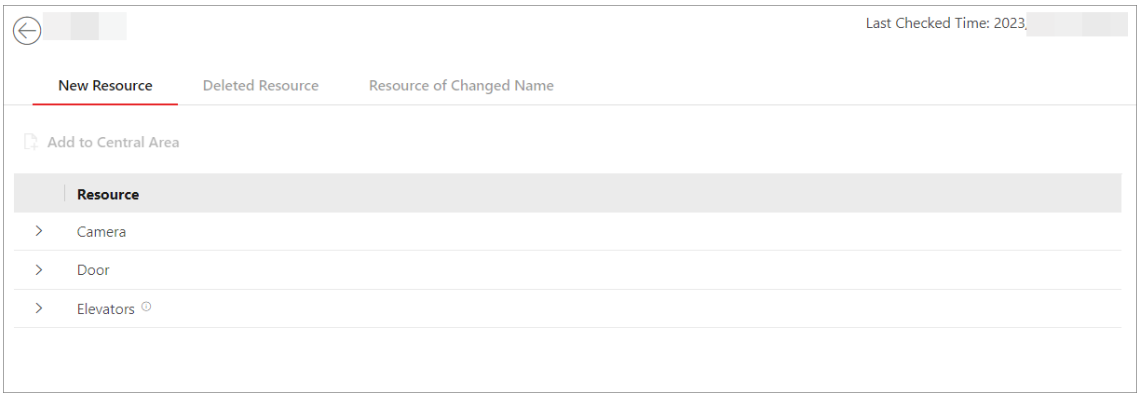


Figure 13-3 Changes of Remote Site

4. **Optional:** When there are newly added cameras, doors, or elevators on the site, you can view the resources and add them to the area in Central System. To add the cameras to the area in Central System, take the following steps:
   1) Click **New Resource → Camera** to expand the newly added camera list.

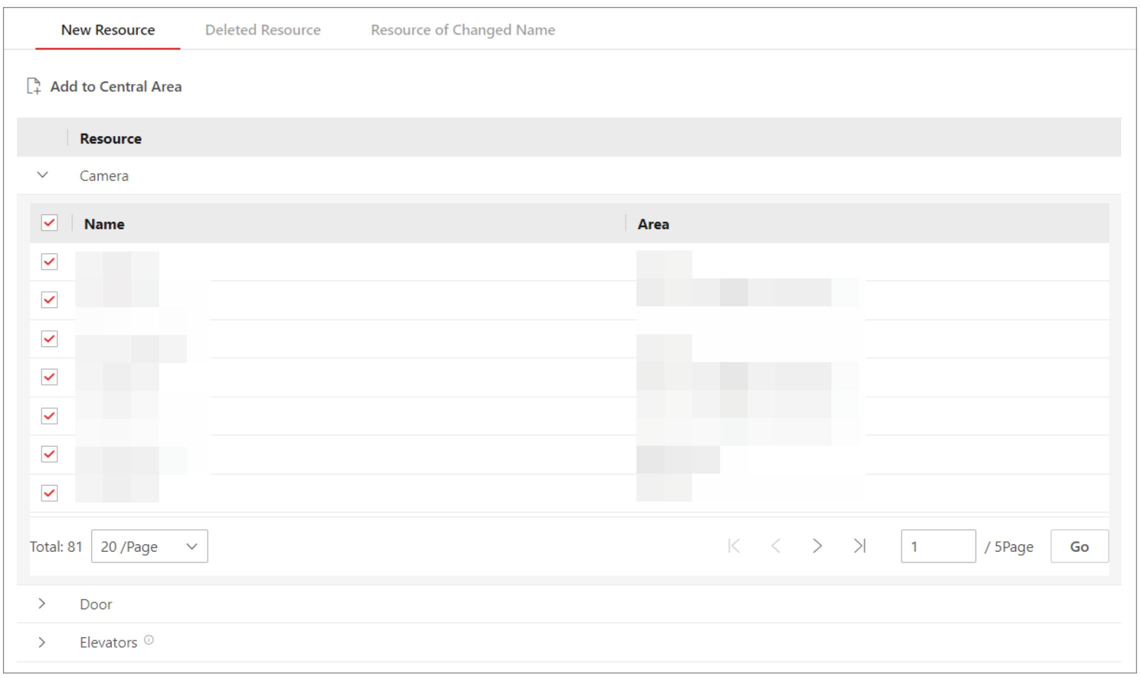


Figure 13-4 New Resource

   2) Select the camera(s) and click **Add to Central Area** to synchronize the newly added cameras to the Central System.
   3) Select the area in the Central System.
   4) Click **Save**.
5. **Optional:** When cameras, doors, or elevators are deleted from the site, you can view the deleted resources and remove them from Central System. To delete the camera(s) in Central System, take the following steps:

1) Click **Deleted Resource Camera** to expand the deleted camera list.

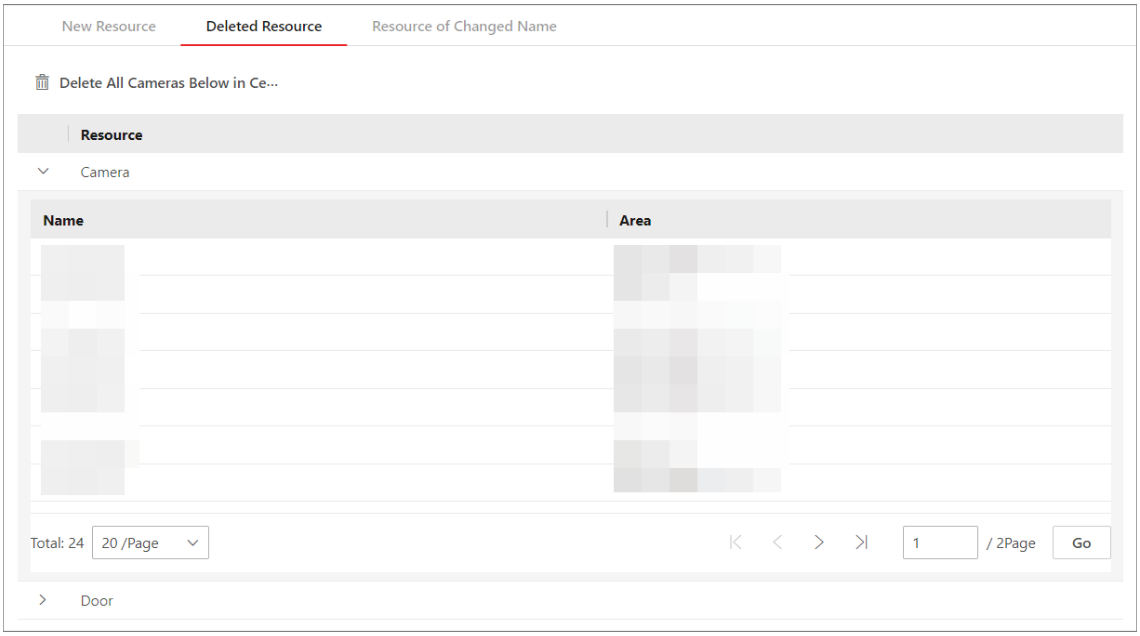


Figure 13-5 Deleted Resource

2) Click **Delete All Cameras Below in Central** to delete the cameras in Central System.

6. **Optional:** When cameras, doors, or elevators are renamed on the site, you can view the renamed resources and synchronize resource name to Central System. To synchronize the renamed cameras to Central System, take the following steps:

1) Click **Resource of Changed Name Camera** to expand the renamed camera list.

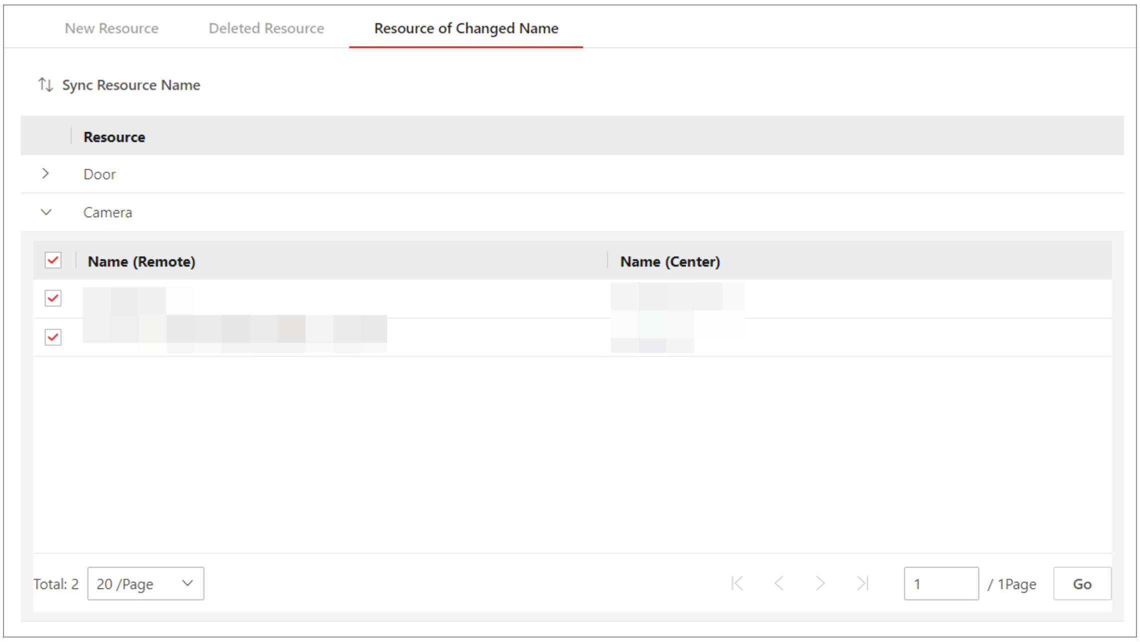


Figure 13-6 Renamed Resource

2) Select the camera(s) and click **Sync Resource Name** to synchronize the resource name in Central System.

Chapter 14 Video Management

In the Video module, you can set video basic parameters such as volume, video storage path, and recording, perform live view, playback, and PTZ control, as well as configure parameters for other important functions such as intelligent recognition, self-learning library, panorama tracking, and visual tracking.

Note

The platform supports video features with and without plugin. However, some functions are only available when there is a plugin. For example, view management, remote sites display on the resources tree, audio recording, dragging cameras to adjust the order of multiple windows, window division other than 1, 4, 9, 16 during live view and playback, and displaying alarm status and viewing alarm details in the camera window reporting the alarm.

14.1 Video Overview

The Video Overview page displays the brief information such as health status of different resources, face picture applying status, and face capture event. You can jump to other pages such as device management, maintenance, event and alarm configuration, and applying center.

In the top left corner of the platform, select ⊞ → **Security Monitoring → Video → Video Overview** .

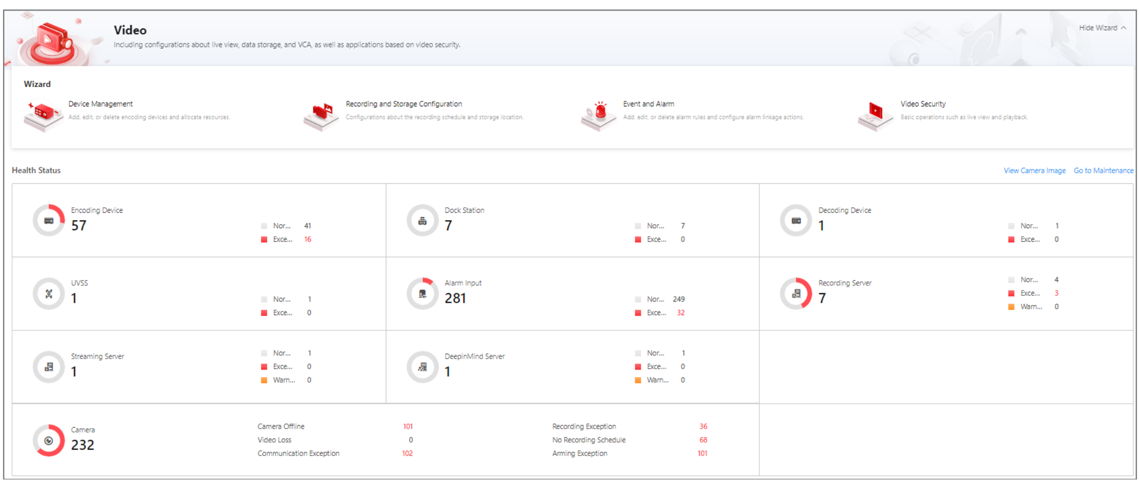


Figure 14-1 Video Overview

The following operations are supported.

Operation	Description
Go to Other Pages	Hover the cursor on the module name (such as **Device Management**, **Recording and Storage Configuration**, **Event and Alarm**, and **Video Security**) in Wizard panel and click ↗ to go to the corresponding page.
Go to Resource Status Page of a Resource Type	• Click the total number of one type of resources to go to the status page of that type of resources. • Click the number of one type of resources in a certain exception status to go to the status page of that type of resources in the corresponding exception status.
View Camera Images	Click **View Camera Image** to view images of all cameras.
Go to Maintenance Module	Click **Go to Maintenance** to go to the Maintenance module. For further operations, refer to ***Maintenance*** .
Go to Applying Center	Click the face picture applying status in Face Picture Applying Status panel to go to ***Applying Center*** .
View Face Capture Event Details	View the information (such as profile picture, capture time, and event source) about captured face pictures in Face Capture Event panel.

14.2 Flow Chart of Video Security

The following flow chart shows the process of configurations and operations required for basic video security functions, such as live view and playback.

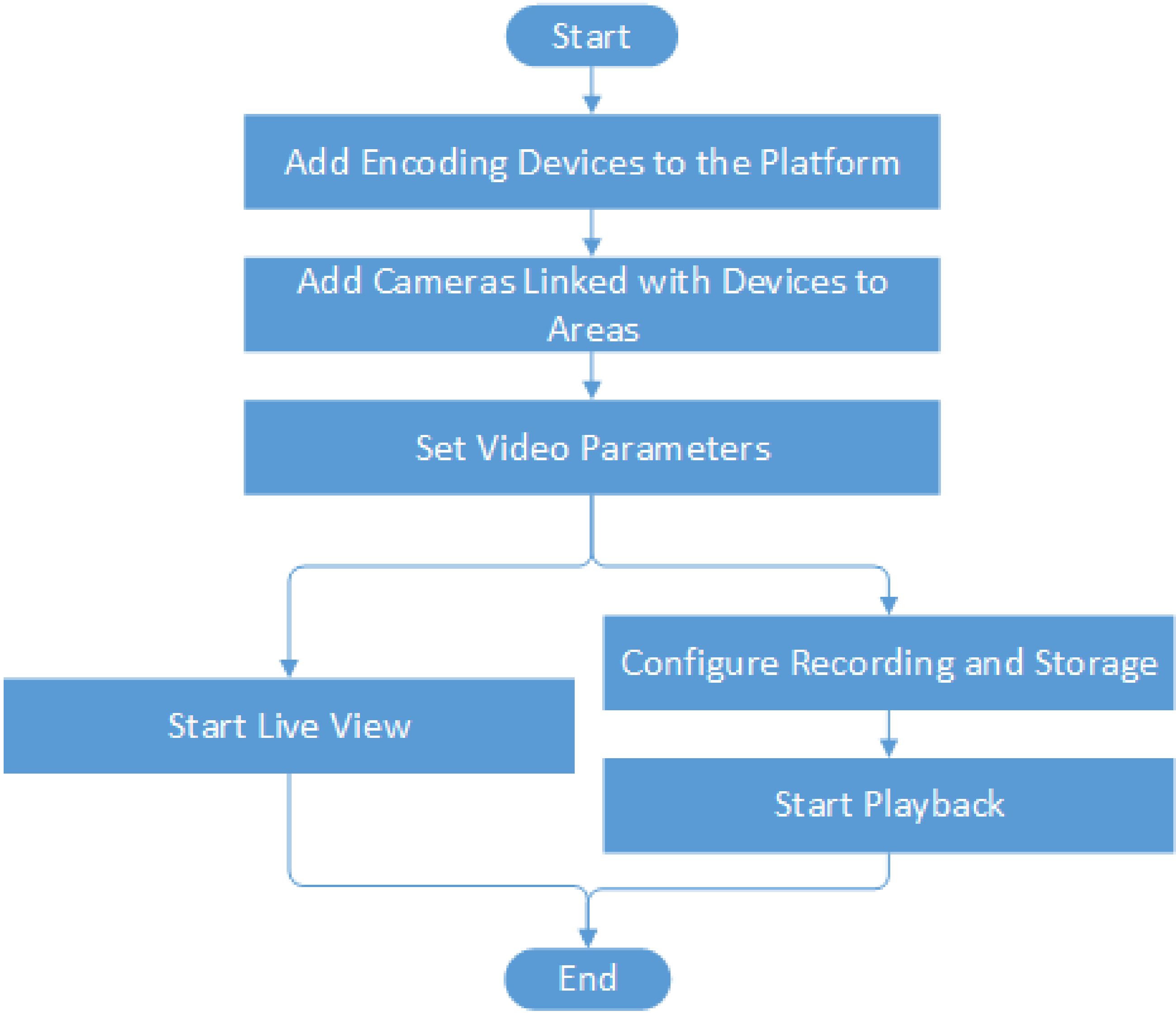


Figure 14-2 Flow Chart of Video Security

Table 14-1 Flow Chart Description

Procedure	Description
Add Encoding Devices to the Platform	Add encoding devices to the platform by online detection, IP address, port segment, **Hik-Connect DDNS**, device ID, device ID segment, etc. For details, see ***Manage Encoding Device*** .
Add Cameras Linked with Devices to Areas	Group cameras linked with encoding devices to different areas according to the locations of the devices for convenient management.

Procedure	Description
	For details, see ***Add Camera to Area for Current Site*** .
Set Video Parameters	Set network parameters, picture file format, display parameters, audio parameter, and so on for video security. For details, see ***Set Video Parameters*** .
Configure Recording and Storage	Define the periods during which video recording is activated. And set the storage location for the recorded video footage and the uploaded pictures (e.g., alarm related pictures).
Start Live View or Playback	Start playing live videos or video footage of cameras. For details, see ***Live View*** or ***Playback*** .

14.3 Video Security

The HikCentral Professional provides functionality of live view, playback, and local configuration through web browser.

Note

- If the SYS's transfer protocol is HTTPS, the Video Security module (including Live View, Playback, and Local Configuration) is available only when accessing the Web Client via Internet Explorer.
- If the SYS's transfer protocol is HTTP, the Live View and Playback modules are available for Internet Explorer, Google Chrome, Firefox, and Safari 11 and above. But Local Configuration module is available for Internet Explorer only.

14.3.1 Live View

In the Live View module of Web Client, you can view the live video of the added cameras and do some basic operations, including picture capturing, recording, PTZ control.

In the top left corner of the Client, select → **Video** → **Video Security**

Choice 1: Start Live View in Area Mode

Note

The areas which the current user has permission to access are listed and the resources which the user has permission to access are shown in the corresponding areas.

1. Click in the upper-right corner to change live view window division.
2. Start live view.

- Drag a camera to the display window to start the live view of the camera, or double-click the camera to start the live view in a free display window.
- Drag an area to a display window, and click **Batch Play**, or double-click the area to start the live view of all cameras in the area.

Choice 2: Start Live View in View Mode

A view is a window division with resource channels (e.g., cameras and access points) linked to each window. View mode enables you to save the window division and the correspondence between cameras and windows (or correspondence between map and window) as the default so that you can quickly access these channels and/or map later. For example, you can link camera 1, camera 2, and camera 3 located in your office to the certain display windows and save them as a view called ***office***. Then, you can access the view ***office*** and these cameras will display in the linked window quickly.

Note

- For live view, the view mode can save resource type, resource ID, stream type, position, and scale after digital zoom, preset No., and fisheye dewarping status.
- For playback, the view mode can save resource type, resource ID, position, and scale after digital zoom, and fisheye dewarping status.

1. Click on the left navigation bar.
2. Add a custom view group.
   a. Select **Public View** or **Private View** to add the view group.

      Note

      The view groups and views that belong to the private view group are hidden from the other users.

   b. Click , set a name for the view group, and click **OK**.
3. Add a view.
   a. Select a view group, click , and set a name for the view.
   b. Click **Add** to select cameras.
   c. Set the required parameters, and click **Add** to add a view.
4. (Optional) Select a view, and click → **Share** on the right side of the view's name to share it with others.
5. Double click a view or move the cursor over a view, and click → **Play** beside the view name.

Choice 3: Start Live View of Favorited Cameras

1. Click on the left navigation bar.
2. Select a parent Favorites, click to add a Favorites under the parent Favorites, and select the camera(s) to be added to Favorites.

Note

Up to 5 levels of Favorites can be added.

3. (Optional) Select a Favorites, and click → **Share** on the right side of Favorites' name to share it with others.
4. When in Live View window, select a Favorites, and click → **Play All** to start viewing the live view of all the camera(s) added in Favorites.

Choice 4: Auto-Switch Cameras in an Area

1. Start auto-switch in the area.
   - Drag an area to the live view window and select **Single-Screen Auto-Switch** to start the auto-switch the cameras of the area in the selected display window.
   - Click on the right side of the area name and click **Area Auto-Switch** to switch the cameras of the area in the live view window.
2. Move the cursor over the live view window and perform further operations after auto-switch starts.

Operations	Descriptions
Adjust Switching Interval	Click or in the lower-left corner of the live view window to adjust the interval of the auto-switch.
View Previous or Next Camera	Click or in the lower-left corner of the live view window to go to the previous or next camera.
Pause	Click in the lower-left corner of the live view window to pause the auto-switch.

14.3.2 Live View Toolbar Applications

You can customize the icons on the toolbar, start the fisheye dewarping mode, perform manual panorama tracking, and so on.

View Dewarped Live View of Fisheye Camera

You can set center calibration and view dewarped live view of a fisheye camera in the client. Dewarping refers to the process of perspective correction of an image, to reverse the effects of geometric distortion caused by the fisheye camera lens. It allows the user to cover a wide area with a single device and have a "normal" view of an otherwise distorted or reversed image. Also, during live view, you can perform more operations such as adjusting view angle and zooming in/out view.

Steps

1. ***Start live view*** of a fisheye camera.
2. On the toolbar of display window, click [icon] to enter the fisheye dewarping mode and view live view.

Figure 14-3 Fisheye Dewarping

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

Adjust View Angle	Put the cursor on the live video, and drag the video to adjust the view angle.
Zoom in/out View	Put the cursor on the live video, and scroll the mouse wheel to zoom in or out the view.
Perform PTZ control	Use the PTZ panel on the left side to perform PTZ control of the camera. **Note** Setting pattern is not supported by fisheye cameras.

Perform Manual Panorama Tracking

During live view, you can enable the panorama tracking manually to locate or track the target appeared in the view of bullet or box camera with a linked speed dome. You can also check and test the calibration results about panorama tracking settings for auto-tracking.

Before You Start

Make sure you have configured the panorama tracking rules for the box or bullet camera on Web Client. For more details, refer to *User Manual of HikCentral Professional Web Client*.

Steps

1. In the top left corner of the Client, select → **Video** → **Video Security** .
2. Start the live view of box/bullet camera, and linked speed dome.
3. Click on toolbar of box/bullet camera to enable manual panorama tracking.

Note

If you choose to enable manual panorama tracking, the auto panorama tracking will not take effect; if you choose not to enable manual panorama tracking and enable **Auto-Tracking** when configuring panorama tracking on the Web Client, when the configured VCA event is triggered by target, the linked speed dome will perform the automatic panorama tracking.

4. Click or draw a rectangle on the live view image of the box/bullet camera, and the speed dome will switch to the close-up view.

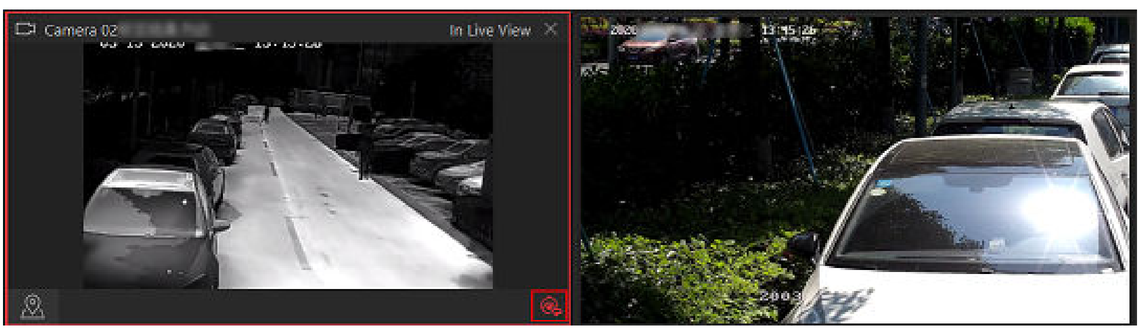


Figure 14-4 Manual Panorama Tracking

Manual Recording and Capture

You can record video files and capture pictures manually during live view.

Manual Recording

Record the live video during live view if needed and store the video files in the local PC.

Capture

Capture pictures during live view if needed and store the pictures in the local PC.

Manual Recording

1. In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Security** .
2. Move the cursor to the live view display window to show the toolbar.
3. Click in the toolbar of the display window to start the manual recording. The icon turns to .

Note

During the manual recording, **Recording...** will display in the upper-right corner of the display window.

4. Click to stop recording.
   A dialog directing to the saving location of the file pops up.

Note

- The video cannot be saved if the free space on your disk is less than 2 GB.

5. (Optional) Click **Open Folder** to access the video file folder in the pop-up dialog box after manually recording.

Capture Pictures

1. In the top left corner of the Client, select → **Security Monitoring** → **Video** → **Video Security** .
2. Move the cursor to the live view display window to show the toolbar.
3. Click in the toolbar to capture a picture.
   A dialog box directing to the saving location pops up.

Note

-
- The picture cannot be saved if the free space on your disk is less than 512 MB.

4. (Optional) After the dialog box popped up, perform the following operation(s).

Operation	Description
Check Picture	Click **Open Folder** in the dialog box to open the folder where the captured pictures stored to and view pictures.
Edit Picture	a. Click **Edit** in the dialog box to open the Capture window. b. Press and move the cursor on the picture to draw. For example, you can mark the suspicious persons in the picture. c. Click **Save As** and specify the path to save the edited picture.

Operation	Description
	Note The picture cannot be saved if the free space on your disk is less than 512 MB.

Customize Icons on Live View Window

You can customize the icons on the toolbar of the live view window, adjust the icon order, and control whether to always show toolbar on the live view window or not.

Steps

1. In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Security** .
2. In the top right corner of the page, click → **Toolbar** .
3. In **Customize Live View Tool Bar** section, add or remove the icons to show or hide the icons on the live view toolbar.
4. Drag the icons in the icon list to adjust the order.

Table 14-2 Icons on Live View Toolbar

	Audio Control	Turn off/on the sound and adjust the volume.
	Capture	Take a snapshot of the current video and save it to the current PC. **Note** After capturing a picture, a thumbnail will pop up on the upper-right corner. You can click **Picture Search** to search the captured picture, archive, and identity verification related with the captured picture.
	Record	Start manual recording. The video file will be stored in local PC.
	Instant Playback	Switch to instant playback mode to view the recorded video files.
	Two-Way Audio	Start two-way audio with the camera to get the real-time audio from the device to realize voice talk with the person at the device.

	Digital Zoom	Zoom in or out the video for cameras that do not have their own optical zoom capabilities. Click again to disable the function.
	PTZ Control	Activate the PTZ icons on the image to pan, tilt, or zoom the image.
	Fisheye Expansion	Available for fisheye camera. In the fisheye dewarping mode, the Control Client will correct the video image and reverse the effects of geometric distortions caused by the fisheye camera lens. See ***View Dewarped Live View of Fisheye Camera*** for details.
	Camera Status	Show the camera's recording status, signal status, connection number, etc.
	Switch Stream	Switch the live view stream to main stream, sub-stream (if supported), or smooth stream (if supported). **Note** The smooth stream will show if device supports. You can switch to smooth stream when in low bandwidth situation to make live view more fluent.
	Alarm Output	Display the Alarm Output Control page and turn on/off the alarm outputs of the connected camera.
	Manual Linkage	Locate or track the target appeared in the view of bullet or box camera with a linked speed dome.
	Enhancement	Adjust the video image including brightness, saturation, etc.
	Rotate Image	Rotate an image.
	Park Action	Click the icon and the speed dome will save the current view to the preset No.32. The device starts to park at preset No. 32 automatically after a period of inactivity (park time).
	Locate Target	Click the icon to measure the distance between camera and target.
	Panorama	Using the AR camera and the speed dome added to a scene, you can perform panoramic tracking of a moving target by clicking on the panoramic image.

	Clean Manually	Click the icon to clean the camera.
	Object Search	Select a person in the image and search for the person.

Note

The icons on the toolbar in the live view window vary with the device's capabilities.

5. Click **Save**.

14.3.3 PTZ Control

The PTZ control for cameras with pan/tilt/zoom functionality is provided. You can set the preset, patrol and pattern for the cameras on the PTZ control pane.

In the top left corner of the Client, select → **Video** → **Video Security**

Start live view of a camera, and click **PTZ Control** to open the PTZ pane.

Note

The PTZ control function should be supported by the camera.

Introduce the Main Pane

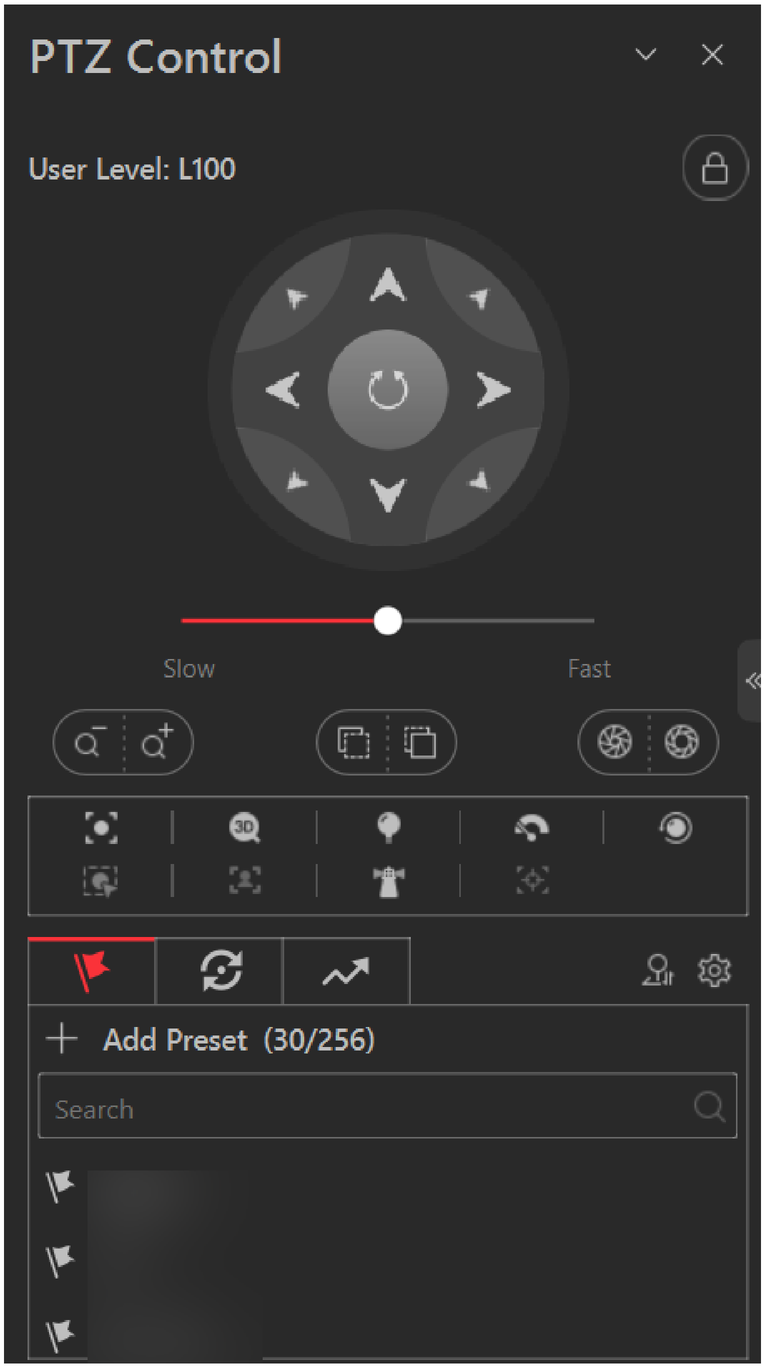


Figure 14-5 PTZ Control Panel

The following buttons are available on the PTZ control pane:

	Lock the PTZ for a designated time period. When the PTZ is locked, users with lower PTZ control permission levels cannot change the PTZ controls. **Note** For details about setting the PTZ control permission level, refer to the *User Manual of HikCentral Professional Web Client*.
	Direction Button, Auto-scan and PTZ speed.
/	Zoom in or out the video for cameras that do not have their own optical zoom capabilities. Click again to disable the function.
/	Used for adjusting the luminance of the image. The larger the iris is, the more the light enters, and the brighter the image will be.
/	Click to move the focal point backward, and click to move the focal point forward.
	Auxiliary Focus: Click to focus automatically.
	3D Positioning: Click on the desired position in the video image and drag a rectangle area in the lower right direction, then the dome system will move the position to the center and allow the rectangle area to zoom in. Click to drag a rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out.
	Light: Click to fill light.
	Wiper: Use the wiper to clear the dust on the camera lens.
	Lens Initialization: Initialize the lens and focus again for a clear image.
	Manual Tracking: For speed dome with auto-tracking function, enable the auto-tracking (via right-click menu) for it and click the icon to manually track the target by clicking on the video.
	Manual Face Capture: Click this button, and hold the left mouse button to select a face in the image to capture it. The picture will be uploaded to the server for viewing.
	Park Action: For the speed dome with one-touch park function, click the icon and the speed dome saves the current view to the preset No.32. The device starts to park at preset No. 32 automatically after a period of inactivity (park time). For setting the park time, refer to user manual of the speed dome.
	Auto Track: For cameras support and tracking, click the icon and select the target (person or vehicle) in the live view to arm and track this target.

- In the live video display window, click the icon to start PTZ control. Click and drag the cursor with a white arrows to control the direction.
- Click to get device PTZ configuration.

Configure Preset

A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. You can also set a virtual preset after enabling digital zoom.

1. Click to enter the PTZ preset configuration pane.
2. Use the direction buttons to control the PTZ movement.
3. Select a PTZ preset number from the preset list and click to name and save the settings.

Configure Patrol

A patrol is a scanning track specified by a group of user-defined presets (including virtual presets), with the scanning speed between two presets and the dwell time of the preset separately programmable.

Before you start, make sure you ***have added two or more presets*** .

1. Click to enter the patrol configuration pane.
2. Select a PTZ patrol number and click to set the patrol.
   a. Select or as the preset type.

   Note

   A device preset ( ) is a predefined image position, while a virtual preset ( ) is a predefined and zoomed image position. You can add a virtual preset by starting live view, zooming in, and adding the image position as a virtual preset.

   b. Click to add a configured preset, hover your cursor over the values in the **Preset**, **Speed**, and **Time** columns, and slide the mouse to change the value.
   c. Click or to adjust the presets sequence.
3. Set other parameters, and click **OK**.

Configure Pattern

By recording pattern, the movement path and the dwell time in a certain position can be recorded precisely. By calling pattern, mobile PTZ starts move totally according to the recorded path.

1. Click to enter the PTZ pattern configuration pane.
2. Click to start recording the movement path of the pattern, use the direction buttons and other buttons to control the PTZ movement, and click to stop and save the pattern recording.
3. Click to call the pattern.

14.3.4 Playback

The video files stored on the local storage devices such as HDDs, Net HDDs, and SD/SDHC cards or the Recording Server, can be searched and played back remotely through the web browser.

In the top left corner of the platform, select → **Security Monitoring → Video → Video Security** .

Start Playback

You can search video files by area or camera and start playback and download found video files to local PC.

Note

- You can search video files by the time of the time zone where the device locates in, or by the time of the time zone where the PC running the Control Client locates in.
- Automatically converting daylight saving time to standard time is supported, or vice versa.
- Synchronous playback or asynchronous playback of devices in different time zones are supported.

Start Playback in View Mode

Click on the left navigation bar.

Click the **Playback** tab to enter the playback page.

Click a view to quickly start the playback of all the cameras related to the view.Click a view to quickly start the playback of all the cameras related to the view.

Start Synchronous Playback

Start normal playback of at least two cameras.

After starting normal playback, click **Synchronous Playback** on the playback toolbar to enable the synchronous playback.

Start Fisheye Playback

Select a fisheye camera from the camera list to start playback.

Move the cursor to the display window, and click on the appearing toolbar to enter the fisheye dewarping mode.

Drag on the video to adjust the view angle, and scroll the mouse wheel to zoom in or zoom out the view.

Start Playback of Favorited Cameras

1. Click on the left navigation bar.
2. Select a parent Favorites, click to add a Favorites under the parent Favorites, and select the camera(s) to be added to Favorites.

Note

Up to 5 levels of Favorites can be added.

3. (Optional) Select a Favorites, and click → **Share** on the right side of Favorites' name to share it with others.
4. When in Playback window, select a Favorites, and click → **Play All** to start viewing the live view of all the camera(s) added in Favorites.

14.3.5 Set Video Parameters

You can set network parameters, picture file format, display parameters, etc.

In the left navigation bar of Video Module, select **Video Security** → .

Table 14-3 Set Video Parameters

Area	Parameters	Description
Set Network Parameters	Network Timeout	The default waiting time for the Client.
	Global Stream	Select the default stream type for global usage.
	Main Stream Live View / Playback: Window Divisions	When the number of divided windows is smaller than the number you set, the live videos or recorded videos will be displayed by main stream.
	Streaming Mode	Set the device access mode as Automatically Judge, Proxy, Directly Access, or Restore Default mode to define how the system accesses all the added encoding devices and decoding devices. If you select Proxy, the system will access the device via Streaming Gateway and Management Service, and it is less effective and less efficient than accessing directly.
Set File Parameters	Picture Format	Select the file format for pictures captured during live view or playback.

Area	Parameters	Description
	File Saving Path	Set the saving path for the files you will download to your computer (manually recorded video files, captured pictures, etc.).
Set Display Parameters	Font Size	Set the font size for resources, views, and favorites.
	View Scale	The image display mode in each display window in live view or playback.
	Window Scale	The scale of the video in live view or playback. You can set it to 4:3 or 16:9 (default).
	Window Division	The number of window divisions.
	Display Window No.	Display the window No. in Monitoring module.
	Display VCA Rule	When switched on, the VCA rule in the live view and playback will be displayed.
	Video Caching	Larger frame caching will result in better video performance. It is determined based on network performance, computer performance, and bit rate.
	Enable Highlight	Enable this function to mark the detected objects with green rectangles in live view and playback.
	Overlay Transaction Information	When On, displays the transaction information on the live view and playback image.
	Wait Prompt for Synchronous Playback	Enable this function to show a prompt of waiting for the synchronous playback.
	Overlay Temperature Information	When On, displays the temperature information on the live view and playback image.
	GPU Hardware Decoding	When On, enables the GPU decoding for live view and playback to save CPU resources.
	Low Frame Compensation	Set the low frame threshold, and when the value is reached, low frame compensation is enabled.
	Time Zone	Set the time zone of the client.

Area	Parameters	Description
Set Audio Parameters	Auto Turn On Audio	if enabled, when you play video, the audio will be automatically turned on.
Set Toolbar	Customize the icons shown during the live view or playback as needed. If you check **Always Display Toolbar**, the toolbar will always be displayed at the bottom of live view or playback window.	

14.4 Picture Center

In the Picture Center, you can search for captured picture(s) according to the capture schedule, cameras, and capture time, and use time-lapse photography to combine captured pictures to generate a video that shows the movement of a long period time.

14.4.1 Search for Scheduled Captures

You can search for captures by specify a capture schedule, camera(s), and time.

Before You Start
Make sure you add a capture schedule. For details, see ***Configure Capture Schedule*** .

Steps

1. In the top left corner of Control Client, select → **Video** → **Picture Center** → **Scheduled Capture Search** .
2. Select a capture schedule, resources for capturing, and time.
3. Click **Search**.

   The results will be displayed on the right pane.
4. **Optional:** You can perform the following operations.

Operation	Description
Real-Time Capture	Click **Real-Time Capture** to capture pictures of the selected resources in real time.
Send Email	Select pictures, click **Send Email**, select an email template, enter remark, and click **OK** to send the selected pictures via email.
Export	Choose file contents and file format, and click **OK**.

14.4.2 Time-Lapse Photography

In the time-lapse photography module, you can combine multiple captured images into a video, which shows the obvious change and movement that happened for an extended period of time. You can also download the combined videos to your local PC.

Steps

1. In the top left corner of the platform, select → **Security Monitoring → Video → Picture Center → Time-Lapse Photography** .
2. Set the material source as **Capture Schedule** or **Local Device**.

   Capture Schedule

   The first choice is to select a capture schedule configured on the platform, and select the captured pictures according to the schedule as the material resource. For example, if a project is from March to May, then you can configure a capture schedule of this period first, and then the captured pictures from the capture schedule will be used as the material source.

   Local Device

   The second choice is to select pictures captured by encoding device(s) that support time-lapse photography as the material resource.
3. Select a capture schedule and encoding device(s) according to the material source you set in the previous step.

   Note

   For encoding devices, you can select cameras whose videos are stored on CVR or pStor.
4. Set **Material Search Total Time** and **Material Search Time for One-Day** to set the time range of searching captured pictures.

   Note

   - You can further narrow down the time range by setting the date and time within one day.
   - Every second of a time-lapse video requires at least 25 pictures. It's recommended to set the time period as long as possible.
5. Set the search time period of a day.
6. Select the video length to be generated.

   The time-lapse videos based on searched pictures are generated and displayed.
7. **Optional:** Move your cursor to a video and click **Download** to download the video.

   The download task is in the task center.

14.5 Manage Face Picture Library

The platform supports face recognition and comparison functions. After adding devices which support face recognition, the devices can recognize faces and compare with the persons in the system.

Steps

1. In the top left corner of the Home page, select → **Video → Face Picture Library** .

14.5.1 Add Face Picture Library

Steps

1. Click + to to add a single face picture library.
2. Click to import face picture libraries from encoding devices or facial recognition servers.

14.5.2 Add Persons to a Face Picture Library

Steps

1. Select a group from the group list.
2. Click **Add → Add New Person** or **Add Existing Person** to add persons to the group.
3. Click on a person's name to add a face picture if the profile picture field is empty.
   - Add from Device: Hover the cursor onto the empty profile picture field, click **Add from Device**, and then select a device.
   - Add by Taking a Picture: Hover the cursor onto the empty profile picture field, and then click **Take a Photo** to take a photo.
   - Add by Uploading Picture: Hover the cursor onto the empty profile picture field, and then click **Upload Picture** to upload a face picture from the local PC.

14.5.3 Import Persons or Profile Pictures

You can import person information by template, and import profile pictures by zipped profile pictures and from an enrollment station.

Before You Start

Make sure you have added the enrollment station to the platform if you want to import pictures from an enrollment station.

Steps

1. Select a face picture library.
2. Click **Import**, and click one among **Import by Template**, **Import Zipped Profile Pictures**, and **Import from Enrollment Station**.

Table 14-4 Import Profile Pictures

Method	Description
Import by Template	a. Click **Download Template** on the pane to download the template. b. Fill required information into the template, and then click to select the filled-in template from the local PC. c. Check **Replace Repeated Person** to allow the system to overwrite the person information already exists in the face picture library when you import the information. d. Click **Import**.
Import Zipped Profile Pictures	Click to select a ZIP file from the local PC, and click **Import**.
Import from Enrollment Station	Set the required information, such as device IP address, device port, and password. **Apply Face Information** Import specific face information from the enrollment station to the face picture library. **Copy Back Face Information** Copy back all the face information acquired by the enrollment station to the selected face picture library. **Select File** Click **Download Template** to download a template and fill in it according to its prompts, and then click and select the filled-in template to import specific face information from the enrollment station to the selected face picture library.

14.5.4 Apply Face Picture Library to Device

After setting the face picture library and adding person(s) to the group, you need to apply the group settings to the device which supports face picture comparison so that the camera can compare the detected faces with the face pictures in the face picture library and trigger alarms (if configured). After applying the face picture library to the device, if the data in the group are changed (such as adding a person to the group, removing person from the group, etc.), the platform will automatically apply the data in the group to the device to take effect.

Before You Start

- Make sure you have added devices which supports face picture comparison to the system.
- Make sure your license supports facial recognition functionality. Or turn to Home page, select **Maintenance and Management → License Details →** , and then click **Configuration** next to

Facial Recognition Camera to added cameras as facial recognition cameras. Otherwise, facial recognition will be unavailable in the system.

Steps

Note

- You can only apply face picture libraries to cameras which support face picture comparison.
- The maximum number of groups that can be applied to the camera depends on the camera capability.

1. In the top left of the Home page, select → **Video** → **Face Picture Library** → **Applying Center** .
2. Select a facial comparison group from the group list on the left side.
3. Click **Face to Be Applied** to display the to-be-applied face information of the selected group.
4. Apply face information to device(s).
   - Apply Specific Face Information: Select face information, and then click **Apply**.
   - Apply All Face Information in the Group: Click **Apply All**.
5. Select the cameras to apply the selected picture libraries to.
6. Click **Apply** to start applying.

14.6 Intelligent Recognition

Intelligent recognition refers to the recognition and analysis of human face, body features, behaviors, vehicles in video images based on intelligent algorithms. The platform will record each recognition and the records can be searched via the Control Client and Mobile Client. The functionality is useful in various scenarios across industries for purposes such as searching for fugitive and finding out security threat.

14.6.1 Step 1. Add Task Schedule Template

A task schedule template is used for defining the weekly time arrangement for an intelligent recognition task. An all-day template is available by default. If you apply the all-day template to an intelligent recognition task, the task will be activated 24*7 hours. If the all-day template cannot meet your demands, you can add a custom template as required.

Go to → **Video** → **Intelligent Recognition** → **Task Schedule Template** .

Click + to add a schedule template.

Set required parameters.

Draw Task Time	Click **Draw Task Time** and then click a grid or drag the cursor on the time line to draw a time period during which the task is activated.
Set Precise Time	Click **Draw Task Time**, move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as 04 : 00 – 04 : 30 .
Erase Task Time	Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period.

14.6.2 Step 2. Add Intelligent Recognition Tasks

In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** .

Task	Parameters
Add Face Picture Comparison Task Once a face picture comparison task is added, the security personnel can view real-time matched face information during live view and search face picture comparison records via the Control Client and Mobile Client.	**Device for Analysis** Select a type of face picture comparison device. **Camera** Select camera(s) from the Available list, and then click > to add selected one(s) to the Selected list. **Face Picture Library** Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s). **Similarity** Drag the slider to adjust the similarity threshold based on your face picture comparison requirements. The higher the threshold, the preciser the comparison will be. The lower the threshold, the higher comparison rate will be. Once the similarity between a detected face and a face picture in the selected face picture libraries reaches the threshold, the detected face will be recognized and a face picturecomparison record will be generated.
Person Feature Analysis Task The feature helps you to recognize and	**Device for Analysis**

Task	Parameters
record body features of the persons appeared in the fields of view of the cameras linked to the person feature analysis device. Once a person feature analysis task is added, the security personnel can search and view person feature analysis records via the Control Client and Mobile Client.	Select a type of person feature analysis device for the execution of person feature analysis. **Camera** Select cameras for detecting persons. **Detection Area** Click **Draw Area** and the drag the cursor on the image to draw an area for detecting persons.
Frequently Appeared Person Analysis Task The feature helps you search out the frequently appeared person in a specific area within a specific period. The function is useful for finding out persons who should not have appeared frequently in a specific area. For example, it can be used in a jewelry store for detecting persons who may commit robbery.	**Device for Analysis** Select the device type for frequently appeared person analysis. **Camera** Select camera(s) for detecting persons. **Face Picture Library** Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s). **Time Period** Set a time period for counting the appearance times of a detected person. **Appeared Times** Set threshold times for regarding a detected person as a frequently appeared person. If the times that a person is detected by the specified camera(s) reaches or exceeds the threshold within the time period you set, he/she will be regarded as a frequently appeared person. **Counting Interval** Set a time interval for filtering out invalid counting. If a person is detected for multiple times within the time interval, the system will regard he/she only appeared for one time. **Similarity**

Task	Parameters
	Drag the slider to adjust the similarity threshold based on your facial recognition requirements. The higher the threshold, the preciser the recognition will be. The lower the threshold, the higher recognition rate will be. Once the similarity between a detected face and a face picture in the selected face picture libraries reaches the threshold, the detected face will be recognized and a face picture comparison record will be generated.
Rarely Appeared Person Analysis Task The feature helps you to search out the rarely appeared person in a specific area within a specific period. Rarely appeared person analysis is useful for finding out specific persons who shall appear regularly in a specific area. For example, in a community where many senile people live alone, when a senile person rarely leaves home (i.e., rarely been detected by the cameras in the community), he/she may need living assistance due to health problems.	**Device for Analysis** Select the device type for rarely appeared person analysis. **Camera** Select camera(s) for detecting persons. **Face Picture Library** Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s). **Time Period** Set a time period for counting the appearance times of a detected person. **Reporting Time** The time when the results of rarely appeared person analysis is reported to system each day. **Appeared Times** Set threshold times for regarding a detected person as a frequently appeared person. If the times that a person is detected by the specified camera(s) is not larger than the threshold within the time period you set, he/she will be regarded as a rarely appeared person. **Counting Interval** Set a time interval for filtering out invalid counting. If a person is detected for multiple times within the time interval, the system will regard he/she only appeared for one time.

Task	Parameters
	Similarity Drag the slider to adjust the similarity threshold based on your facial recognition requirements. The higher the threshold, the preciser the recognition will be. Once the similarity between a detected face and a face picture in the selected face picture libraries reaches the threshold, the detected face will be recognized and a face picture comparison record will be generated.
Archive Analysis Task Once an archive analysis task is added, the platform will save the features and information (including captured picture and video) of the captured person as archive. And the security personnel can search the related archives of a face picture to check the captured pictures or videos of similar persons in the library via the Control Client and the Mobile Client. They can also check whether a person is a stranger.	**Device for Analysis** Select the device type for archive analysis. **Camera** Select camera(s) for detecting persons. **Face Picture Library** Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s). **Similarity** Drag the slider to adjust the similarity threshold based on your face picture comparison requirements. The higher the threshold, the preciser the comparison will be. Once the similarity between a detected face and a face picture in the selected face picture libraries reaches the threshold, the detected face will be compared and a face picture comparison record will be generated.
Abnormal Event Detection Task Abnormal event detection analysis refers to the analysis of abnormal events of people, vehicle, and other objects for purposes such as finding out security threat. The available abnormal event analysis types include perimeter protection (intrusion detection), street abnormal event analysis, prisoner abnormal event analysis, and people density analysis. You can add an	**Behavior Type** The behavior types are categorized into different groups based on their usage scenarios, including behavior indoor, behavior on street, people density analysis, and perimeter protection. **Task Name** Set the task name. **Task Schedule Template**

Task	Parameters
abnormal event analysis task to define conditions such as time, device, and detection area for abnormal event analysis. Once an abnormal event analysis task is added, the specified device will perform abnormal event analysis in the specified detection area during the specified periods.	Select a task schedule template from the drop-down list to define the time when abnormal event detection is activated. **Device for Analysis** Select a device for abnormal event analysis. **Camera** Select camera(s) for detecting abnormal events. **Detection Area** Draw an area or line for abnormal event detection. Take line crossing detection for an example, you need to click **Draw Detection Line** to draw a line on the image, and then set the following two parameters. **Change Line Crossing Direction** Set the crossing direction to determine whether line crossing detection is triggered. For example, if you select **Bidirectional**, when a person crosses the line, no matter what direction the person crosses, line crossing detection will be triggered. **Filter Detection Size** To set a rough detection area, check **Filter Detection Size** and set a maximum size and/or a minimum size. The areas which are bigger than the set minimum size and smaller than the set maximum size will be set as detection areas.
Vehicle Analysis Task Vehicle analysis refers to the analysis of vehicle features such as vehicle license plate number and color. You can add a vehicle analysis task to define the conditions such as the device and detection area for vehicle analysis. After the task is added, the specified device will perform vehicle analysis in the	**Device for Analysis** Select a device from the drop-down list for vehicle analysis. **Camera** Select camera(s) from the Available list, and then click › to add selected one(s) to the Selected list. **Detection Area** Define the area for vehicle analysis. Click **Draw Area** to manually draw a specific area on the video image; Click

Task	Parameters
specified detection area during the configured time.	**Draw Area in Full Screen** to make the whole video image as a detection area.
People Counting Excluding Staff The task is applied when you want to count people with some of them excluded. For example, if you want to count day customer traffic of a store, but staff are obviously not customers, so only actual customers will be counted instead of all people captured by cameras if you use the task.	**Camera** Select camera(s) from the Available list, and then click > to add selected one(s) to the Selected list. **Face Picture Library** Select face picture libraries. The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).

14.6.3 Step 3. Apply Tasks to Devices

In the top left of the Home page, select → **All Modules** → **Video** → **Intelligent Recognition** → **Applying Center** .

View Applying Status

You can view the status of the applying of face picture libraries from different perspectives, including the cameras failed to receive face picture libraries, the cameras to which certain face picture libraries need to be applied, the person information failed to be applied, and the person information to be applied.

Cameras Failing to Receive Faces

Select a device from the device list on the left side, and then click a camera on the camera list to view the details of applying failure, including face picture library, analysis device, and exception details (e.g., the device reaches its maximum face picture library capacity, the face picture library reaches its maximum face picture capacity, face pictures not qualified, etc.) If face pictures are not qualified, you can click to view failure details.
You can also view network status of the listed camera(s). To ensure the success of the applying of face information to these camera(s), make sure they are online.

Cameras to Be Applied To

Select a device from the device list on the left side, and then click a camera on the camera list to view the details of the applying of face picture libraries: the applying status of each face picture library that need to be applied to the camera will be list.

You can also view network status of the listed camera(s). To ensure the success of the applying of face information to these camera(s), make sure they are online.

Faces Failing to Be Applied

Select a face picture library from the group list on the left side to view the face information that fails to be applied to devices, and then click a piece of face information to view its exception details.

Faces to Be Applied

Select a face picture library from the group list on the left side, and then the faces to be applied will be displayed on the right side.

Apply Abnormal Applying Record Again

Applying of face information may fail due to various reasons. To ensure recognition of the target persons in your scenarios, it is important to check the abnormal applying records and apply the face information again.

Apply abnormal face applying records again.

- Click **Cameras Failing to Receive Faces**, select an area from the area list in the left side, and then click **Apply All** to apply face information to all the listed camera(s) again.
- Click **Cameras to Be Applied To**, select an area from the area list in the left side, and then click **Apply All** to apply face information to all the listed camera(s) again
- Click **Face Failing to Be Applied**, select a face picture library from the group list on the left, and then select face information and then click **Apply** to apply the select face information again, or click **Apply All** to apply all face information again.
  Click **Export All** to export all persons' information as a compressed Excel file to the local PC. You need to set a password for decompressing the compressed file.
- Click **Faces to Be Applied**, select a face picture library from the group list on the left, and then select face information and then click **Apply** to apply the select face information again, or click **Apply All** to apply all face information again.

14.7 Video Application

This section introduces advanced features including self-learning library, visual tracking, and person/vehicle arming and panorama tracking.

14.7.1 Configure Self-Learning Library

The self-leaning library is a library of false alarm pictures. The library can store those pictures which are identified as false alarms and help you avoid accepting the same kind of false alarms in the future.

In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Application** → **Self-Learning Library** .

The devices which support the learn-by-example feature are displayed on the left pane.

Switch the **Learn by Example** feature for a certain device, so that the device can learn false alarms by example.

Note

It is recommended that you enable the **Learn by Example** feature to reduce false alarms, and after it is disabled, the self-learning library can still be configured but no longer takes effect.

You can perform the following operations.

Operation	Description
View Applicable Events	Click a device on the left pane, and you can view applicable events on the top of the page.
Sort Pictures	Click to sort pictures in ascending or descending order.
Filter Pictures	Click to filter pictures by date.
Delete Pictures	Check pictures on their top right corner and click **Delete** to delete them. You can also click **Delete All** to delete all pictures.
Refresh Page	Click **Refresh** to refresh the page.

14.7.2 Configure Visual Tracking

Visual tracking allows you to track an individual (such as a suspect) across different areas without losing sight of her/him. Before you can use this function, you need to associate a camera (hereafter named as "camera A") with other cameras nearby. After that, icons representing the nearby cameras will be overplayed on the view of camera A. You can click these icons to redirect to the associated cameras' views during live view or playback.

Steps

1. In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Application** → **Configure Visual Tracking** .
2. Select an area from the area list.

   The page will display the thumbnails of the latest view of the cameras that support visual tracking settings in the selected area.
3. **Optional:** Check **Include Sub-Area** to display the available cameras in the sub-area(s) of the selected area.

4. Select **Configured** to edit the configured cameras or select **Not Added** to set visual tracking for cameras.

Configured Cameras	The camera with the biggest image is the main camera, and all other cameras are related with the camera. Click in the upper-right corner, and click **Add Camera** to add related cameras.
Cameras Not Configured	Click **Set Visual Tracking** in the center of a camera image to add related cameras. Click **Add Camera** and select a camera to set it as a related camera.

Example

Visual Tracking in Hallway

The following picture shows the monitoring image of camera A in a hallway. There are three directions: B, C, and D, and each direction is monitored by camera B, C, and D respectively.

In this case, you can drag camera B to the B position so as to overlay the icon of camera B on the monitoring image, and then do similar operations for camera C and camera D. After that, when an individual passes by the hallway and turns to direction B, the security personnel can click the icon of camera B on the view of camera A to redirect to the view of camera B.

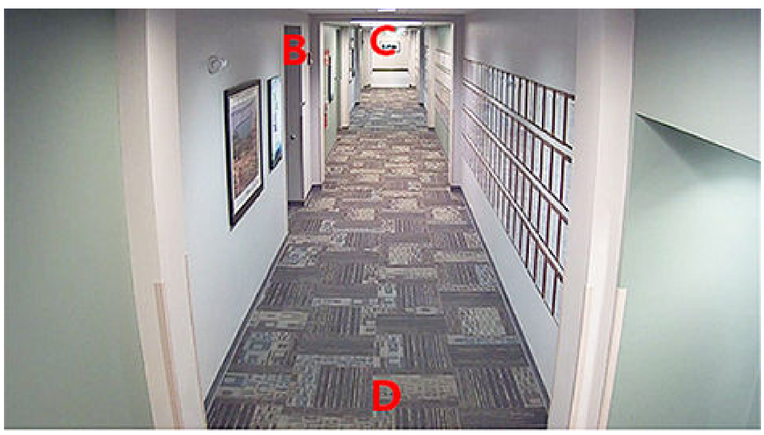


Figure 14-6 Monitoring Image of Camera A

14.7.3 Configure Person/Vehicle Arming

You can add a group with multiple cameras with the person/vehicle arming capability in it, and when a person or vehicle of interest is detected, the cameras will follow the target consecutively.

In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Applications** → **Configure Person/Vehicle Arming** .

Person/Vehicle arming groups are groups containing multiple cameras. The cameras are added to a same group so as to work cooperatively to track a vehicle or person target.

Set Arming Group Information

1. Click **Add Person/Vehicle Arming Group** or **View Service Details → Add Person/Vehicle Arming Group** , and set a name for the arming group.
2. Select the arming type as person arming or vehicle arming. Person arming is to track target persons while vehicle arming is to track vehicles.
3. Select cameras to add them to the group. After a person or vehicle of interest is detected, the cameras will track the target consecutively.
4. (Optional) If you select person arming, drag the slider to adjust the similarity threshold or enter a value to set a similarity threshold. When a person is above the similarity with a target, the cameras in the group will start to track the person.
5. (Optional) If you select vehicle arming, select presets for each camera.
6. Click **Save and Next**.

Set Target Information

1. Click **Add**, and select persons or license plate numbers of vehicles.
2. Click **Add** and the persons / license plate numbers will be applied to the devices. If applying to the device succeeds, you can see the target information show up on the page. If failed, check the items and click **Apply Again** to apply them again.
3. Click **Finish**.

14.7.4 Configure Panorama Tracking

Panorama tracking is a target tracking function based on the linkage between a bullet/box camera and a speed dome. After you configure panorama tracking on the Web Client, the security personnel will be allowed to enable this function during the live view of the bullet/box camera on the Control Client. If this function is enabled, when a Video Content Analysis (VCA) event is detected by the bullet/box camera, or the security personnel manually select a target, the bullet/box camera will work together with the speed dome to locate, zoom in, and track the target.

Before You Start

Make sure you have added the device supporting this function.

Steps

1. In the top left corner of the Home page, select **→ Video → Video Application → Panorama Tracking** .
2. Select one area on the area list.
3. At the thumbnail center, click **Configure Panorama Tracking** to open the Panorama Tracking Settings window.
4. **Optional:** Click **Unlock PTZ** to unlock the PTZ and pan, tilt, and zoom the image to adjust the monitor range.

Note

The feature should be supported by device.

5. **Optional:** Select an elevation range which defines the allowed range of tilting.

Note

The feature should be supported by device.

6. **Optional:** Select **Manual Calibrating** or **Auto Calibrating** as calibration mode and click **Next**.
7. Calibrate the camera and the linked speed dome, and then click **Next**.
   - **Manual Calibrating**: In Manual Calibrating mode, click **Add Calibration Point**, and click the position on the left image of box/bullet camera to add a calibration point. Select the calibration point, and then pan, tilt, and zoom in or out the view of speed dome by digital zoom and PTZ control to make sure the live view of speed dome and the target position of the camera are mostly same.

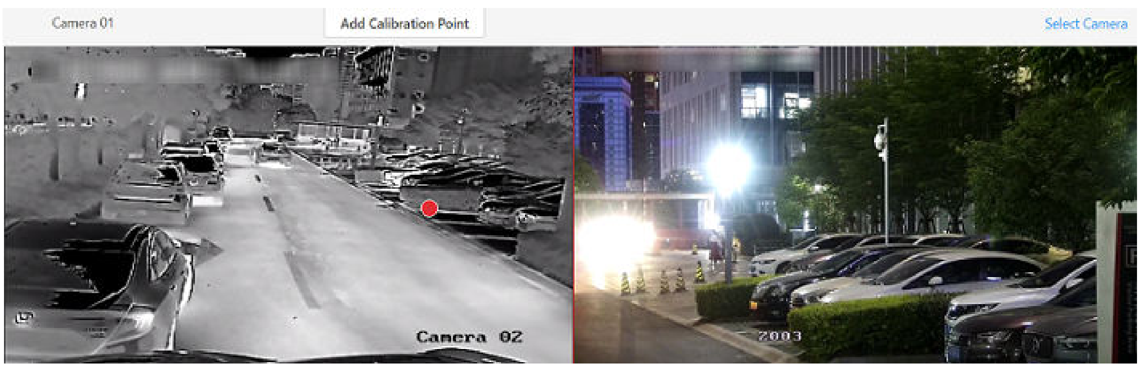


Figure 14-7 Manual Calibrating

Note

- You can repeat the operations to add more calibration points. At least 4 calibration points should be added. It is recommended to add at least 9 calibration points in one scene. For higher tracking precision, up to 12 calibration points are required.
- Click the added calibration point, and you can move it to other position, or delete it.
- It is recommended to place calibration points at distinct positions in live image (for example, corners). If no distinct position is available, you can place the points at something (for example, box, stool, or people) to mark the position.

   - **Auto Calibrating**: In Auto Calibrating mode, click **Start Calibration** to add calibration points automatically.

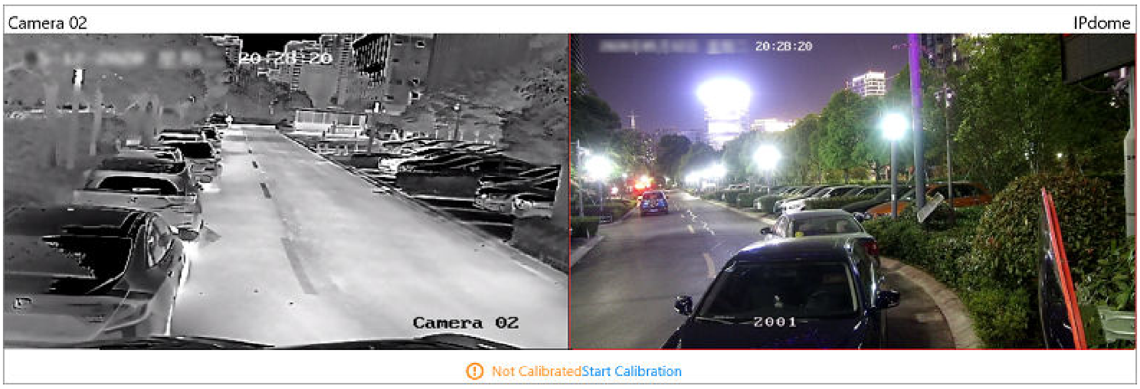


Figure 14-8 Auto Calibrating

Note

You should avoid using auto calibrating for vast similar scenes (for example, lake, lawn, or public square) or dark scenes (for example, night scenes).

8. Set other parameters.

Auto-Tracking

If **Auto-Tracking** is checked, when the VCA event is triggered during live view, the speed dome will track the target automatically.

Note

You need to configure VCA rule for the bullet/box camera on the device. For more details, refer to the user manual of the device.

Target Tracking Mode

Track One Target Continuous

The speed dome tracks the target continuously until the target disappears in the scene.

Track One Target for Certain Duration

Select this mode and set the duration of tracking. The speed dome switches to next target after the set duration time.

Set Tracking Initial Position

Select a preset as tracking initial position, or adjust the view by PTZ control and click **Save** to save the preset as tracking initial position. When tracking finishes or timed out, speed dome returns to the tracking initial position. When tracking initial position is not set, the speed dome stays where tracking finishes or timed out.

9. Click **Save and Test** to finish configuring panorama tracking.

To test the panorama tracking settings, click or draw a rectangle on the video of box/bullet camera, and the speed dome will show the close-up view.

10. **Optional:** After configuring panorama tracking, perform the following operations.

Edit Panorama Tracking Settings	Click **Edit** to reconfigure panorama tracking.
Cancel Panorama Tracking	Click **Cancel Panorama Tracking** to delete all configurations about panorama tracking.

14.8 Video Settings

In Video Settings, you can set recording templates, capture schedule, scheduled report and network parameters.

14.8.1 Configure Recording Schedule Template

Recording schedule is time arrangement for video recording. You can configure the recording schedules to record video in a certain period. Two default recording schedules are available: All-day Time-based Template and All-day Event-based Template. All-day Time-based Template can be used for recording videos for all day continuously, and All-day Event-based Template is for recording videos when alarm is triggered. You can also customize the recording schedule.

Perform this task when you need to customize the schedule to record the video files.

Steps

1. In the top left comer of the Home page, select → **Video** → **Video Settings** → **Recording Schedule Template** .
2. Click + to enter the Adding Recording Schedule page.

Note

Up to 32 templates can be added.

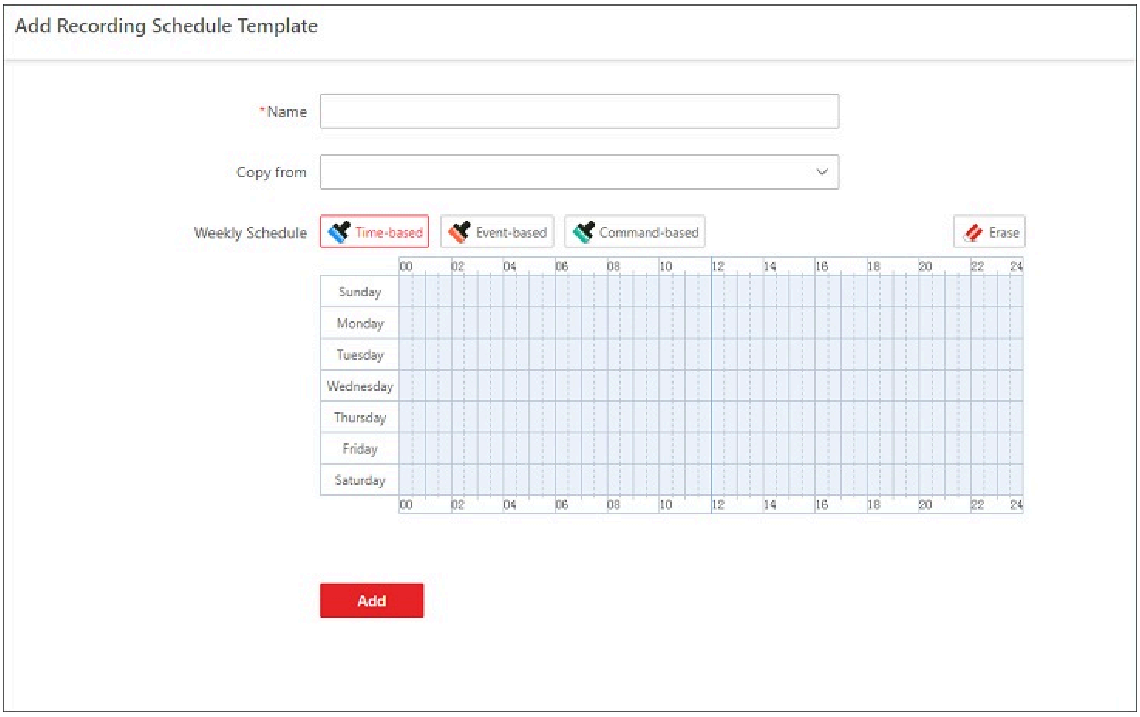


Figure 14-9 Adding Recording Schedule Template Page

3. Set the required information.

Name

Set a name for the template.

Copy from

Optionally, you can select to copy the settings from other defined templates.

4. Select a recording type and drag on the time bar to draw a time period.

Note

By default, the Time-based is selected.

Time-based

Continuous recording according to the time you arranged. The schedule time bar is marked with blue.

Event-based

The recording triggered by the alarm (e.g., alarm input alarm or motion detection alarm). The schedule time bar is marked with orange.

Command-based

The recording triggered by the ATM command. The schedule time bar is marked with green.

Note

Up to 8 time periods can be set for each day in the recording schedule.

5. **Optional:** Click **Erase** and click on the time bar to clear the drawn time period.
6. Click **Add** to add the template and back to the recording schedule template list page.
7. **Optional:** Perform the following operations on the recording schedule template list page.

View Template Details	Click the template to check the detailed settings.
Delete Template	Click to delete a template.

14.8.2 Configure Capture Schedule

You can add a capture schedule to determine when and which camera will capture pictures.

Steps

1. In the top left corner of Control Client, select → **Video** → **Video Settings** → **Capture Schedule** .
2. Click to add a capture schedule.

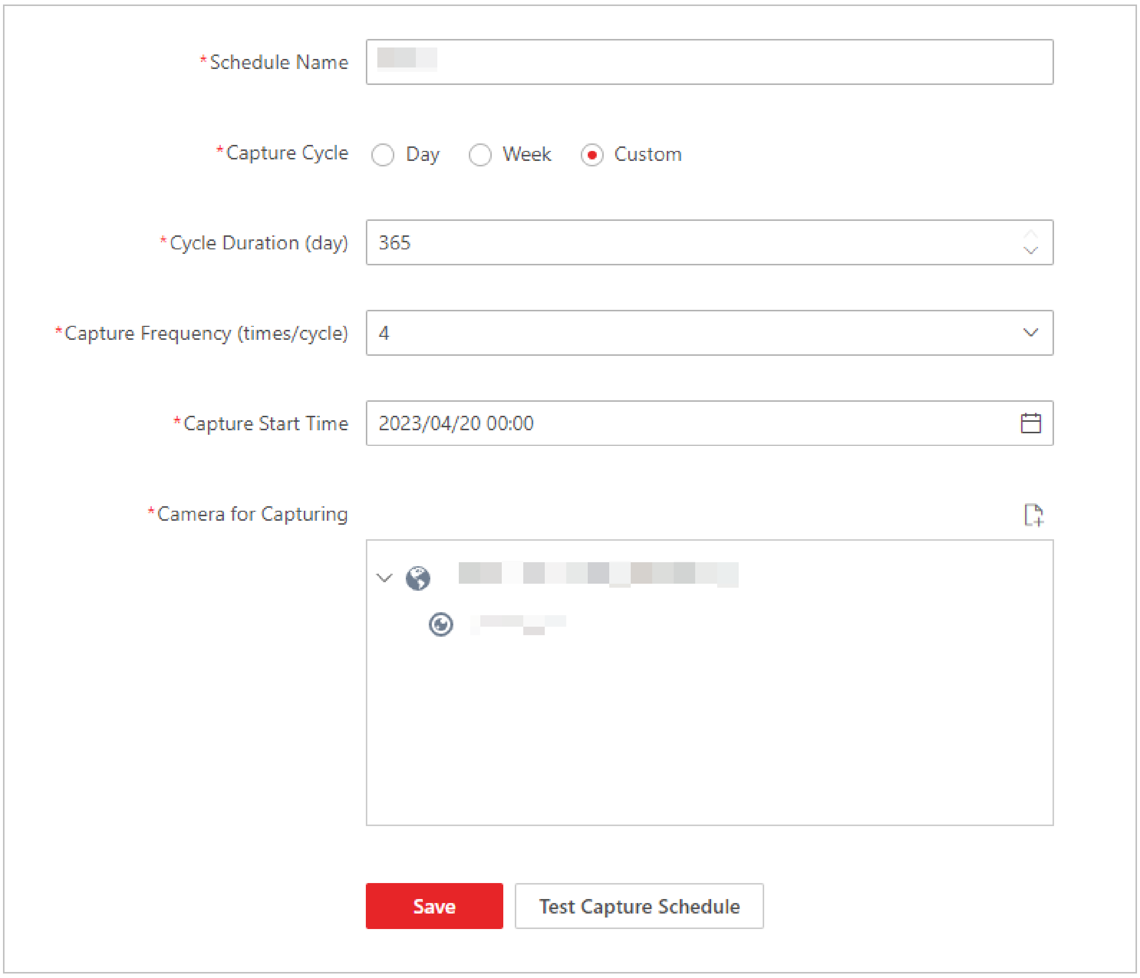


Figure 14-10 Configure Capture Schedule

3. Set a schedule name.
4. Set the capture cycle as **Day**, **Week**, or **Custom**.
5. Set a value for capture frequency.
6. Set a time of starting the task.
7. Select camera(s) and/or preset(s) for capturing.
8. Click **Add**.

   The added schedule will be displayed on the left pane.
9. **Optional:** Click **Test Capture Schedule** to see if the selected resource(s) function properly.

14.8.3 Configure Scheduled Report

You can add a scheduled report so that captured pictures will be sent regularly via email.

Before You Start

Make sure you have added a capture schedule. For details, see ***Configure Capture Schedule*** .

Steps

1. In the top left corner of Control Client, select → **Video** → **Video Settings** → **Scheduled Report** .
2. Click to add a scheduled report.

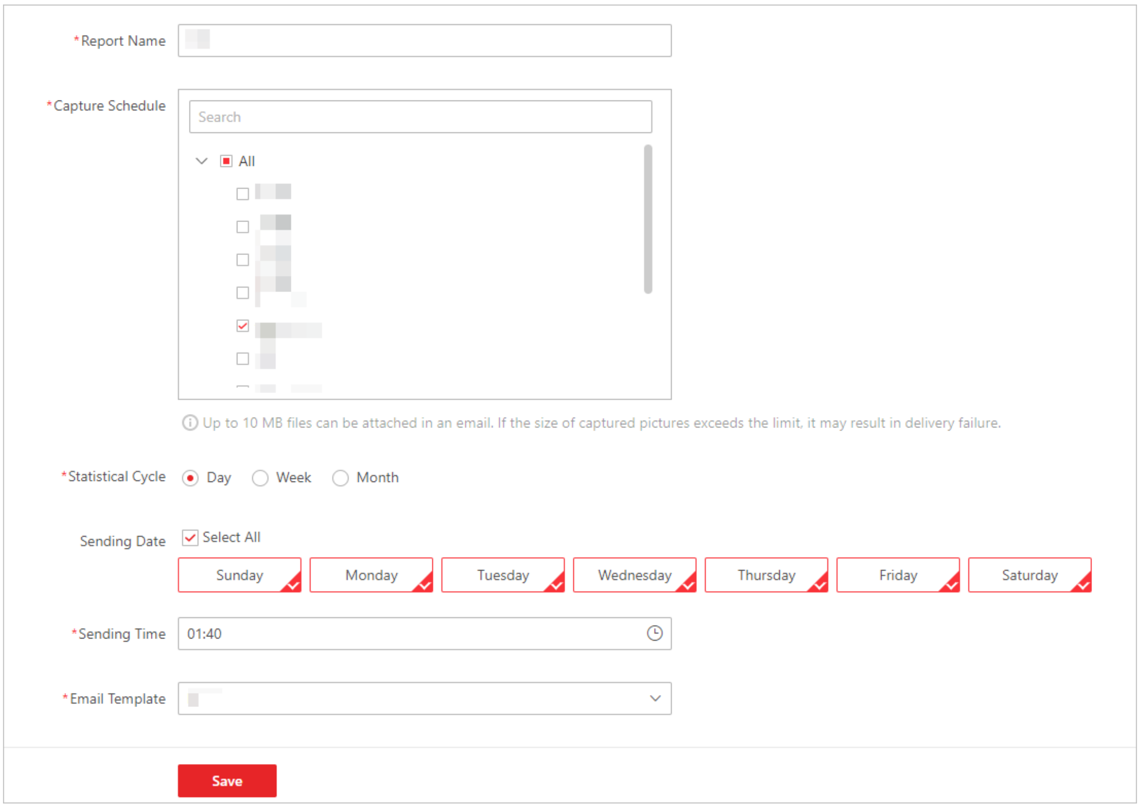


Figure 14-11 Add a Scheduled Report

3. Set the report name, capture schedule, statistical cycle, sending time, email template, and report language.

Note

You can click **Add** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

4. Select the language as **Report Language**.

Note

By default, the language is the same with the selected language when you log in on the Web Client.

5. Click **Save**.

   The added report will be displayed on the left pane.

14.8.4 Set Network Parameters

You can set parameters for registering the platform without Remote Site Management module (or Remote Site) to the Central System, and set access mode for encoding and decoding devices.

Steps

1. In the top left corner of the Home page, select → **Video** → **Video Settings** → **Network** .
2. Set **Device Access Mode**.

   Set the device access mode to **Automatically Judge** or **Proxy** mode to define how the system accesses all the added encoding devices and decoding devices.

   Automatically Judge

   The system will automatically judge the condition of network connection and then set the device access mode accordingly as accessing directly or accessing via Streaming Gateway and Management Service.

   Proxy

   The system will access the device via Streaming Gateway and Management Service. It is less effective and less efficient than accessing directly.

   Note

   The two parameters **Register to Central System** and **Receive Site Registration** are not available at the same time.
3. Click **Save**.

Chapter 15 Alarm Detection

A security control device detects persons, vehicles, or other emergency events in the detection region, and reports event/alarm information (such as location) to the security personnel.

On the Web Client, after adding a security control device to the system, you need to group the device's alarm inputs into areas on the platform. You also need to set one arming schedule for the alarm inputs in a security control partition (area) which defines when and how to arm the alarm inputs in this security control partition (area).

For example, area 1 is created to manage all the resources on the first floor. If there is one security control device mounted on the first floor, you need to add its zones (alarm inputs) into area 1 first, link the zones with security control partitions (areas) and set arming schedules for these security control partitions (areas). After that, the zones in different partitions (areas) can be armed according to the schedules respectively.

15.1 Alarm Detection Overview

On the Alarm Detection Overview page, you can view the health status of security control devices and alarm detection event details.

On the top navigation bar, go to ▦ → **Security Monitoring** → **Alarm Detection** → **Alarm Detection Overview** .

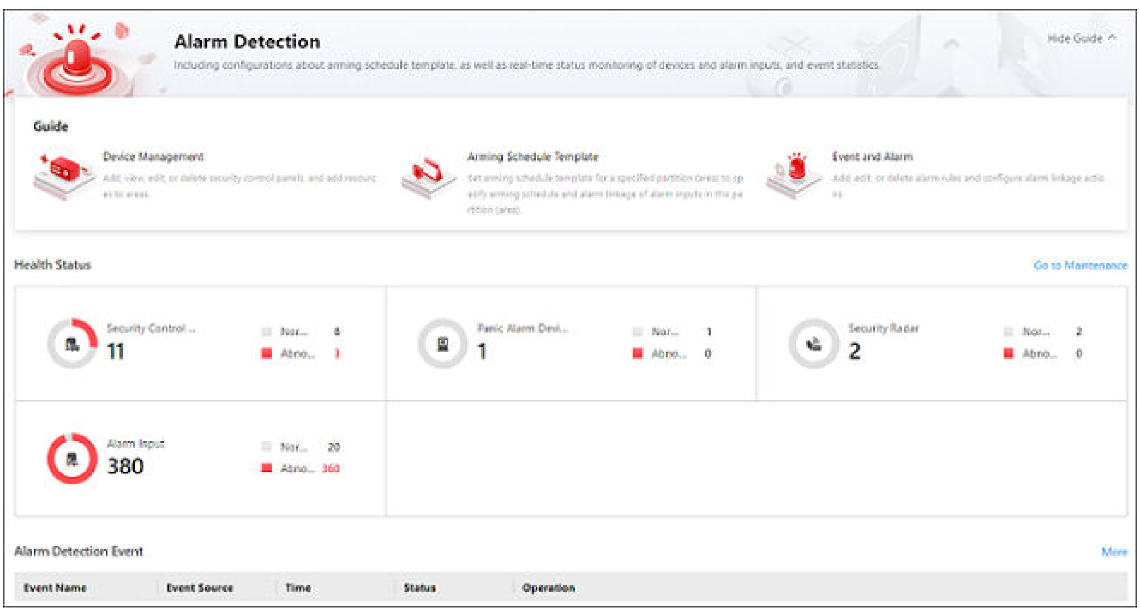


Figure 15-1 Alarm Detection Overview

Content	Description
Guide	You can view the brief introduction of the Alarm Detection function and the major steps of configuration, including device management, arming schedule template setting, and event and alarm configuration. You can hover the mouse cursor over each step and click ↗ to go to the corresponding page.
Health Status	You can view the health status of devices including security control panels, panic alarm devices, security radars, and alarm inputs. Click on the number under the resource type or the number besides **Abnormal** to view their details. Click **Go to Maintenance** to enter the Maintenance module.
Alarm Detection Events	You can view the event details, including the event time, event source, time, status, and available operations.

15.2 Flow Chart of Alarm Detection

The following flow chart shows the process of the configurations and operations of alarm detection.

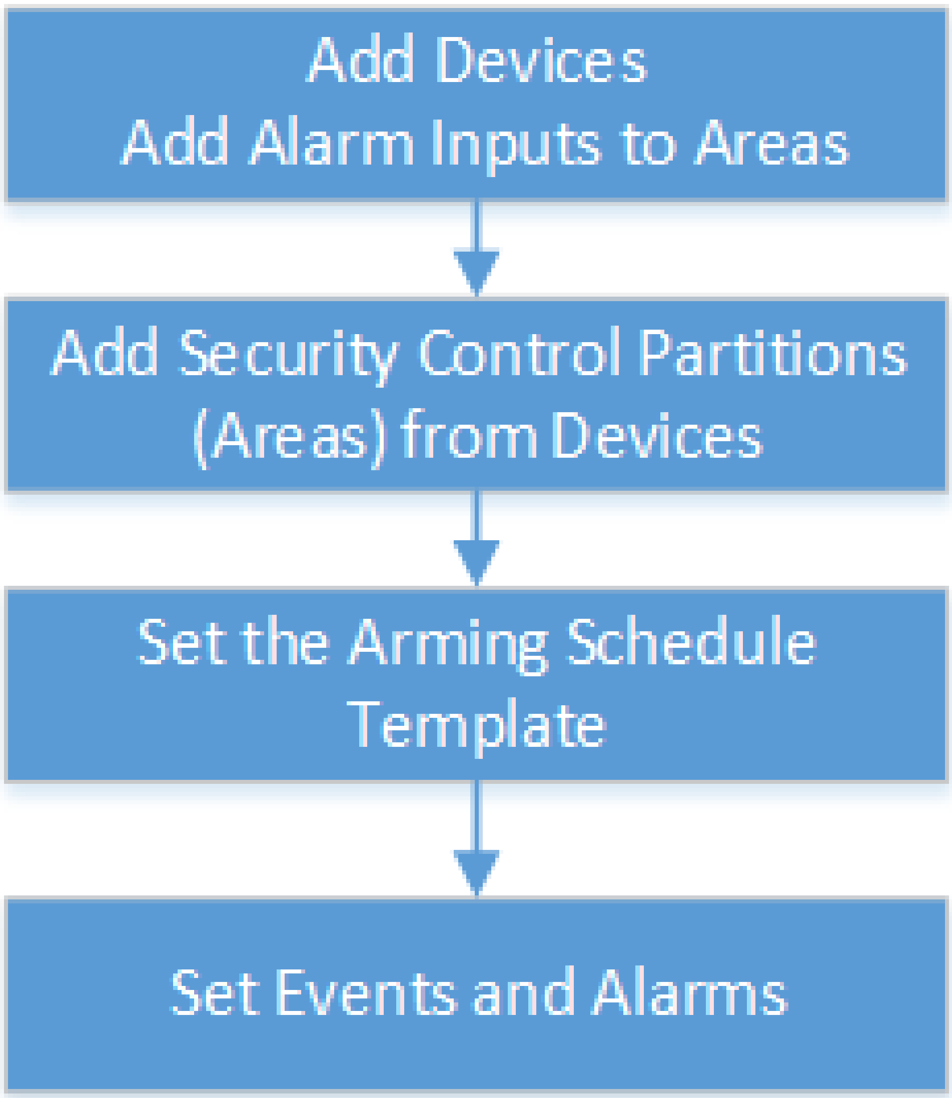


Figure 15-2 Flow Chart of Alarm Detection

- **Add Devices**: Add security control devices to detect persons, vehicles, or other emergency events in the detection region. And then add alarm inputs to areas for management. Refer to ***Manage Security Control Device*** and ***Add Alarm Input to Area for Current Site*** for details.
- **Add Security Control Partitions (Areas) from Devices**: Add alarm inputs and partitions (areas) from devices for arming or disarming zones, bypassing zones, and clearing alarms. Refer to ***Add Security Control Partitions (Areas) from Device*** for details.

- **Set the Arming Schedule Template**: Set an arming schedule template for a specified partition (area) to specify the arming schedule of the alarm inputs in this partition (area). Refer to ***Configure Arming Schedule Template*** for details.
- **Set Events and Alarms**: Set event and alarm parameters and linkage actions to view event and alarm details on the Client, timely remind the security personnel to handle related issues, or search history events and alarms when an emergency occurs.

15.3 Add Security Control Partitions (Areas) from Device

After adding security control devices to the platform, you need to import the partitions (areas) configured on the devices and the alarm inputs in the partitions (areas) to areas on the platform for further operations, including configuring arming schedules for the partitions (areas), arming/ disarming partitions (areas), bypassing zones, clearing alarms, etc.

Before You Start

Make sure you have added security control devices. See details in ***Manage Security Control Device*** .

Steps

1. On the top navigation bar, go to → **Security Monitoring → Alarm Detection → Partition (Area)** .
2. Click + **Add** to show the Add Security Control Partition (Area) pane.

   In the Partition (Area) list, all the security control devices with partitions (areas) which are not added to the platform will be displayed.
3. Select the partitions (areas) that you want to add to the platform.
4. **Optional:** Switch on **Import Alarm Inputs** and select an area that the partitions (areas) and alarm inputs are imported to.

   Note

   After adding the alarm inputs to the area, you can manage them by different areas.
5. Click **Save**.

   The partitions (areas) will be displayed in the partition (area) list.

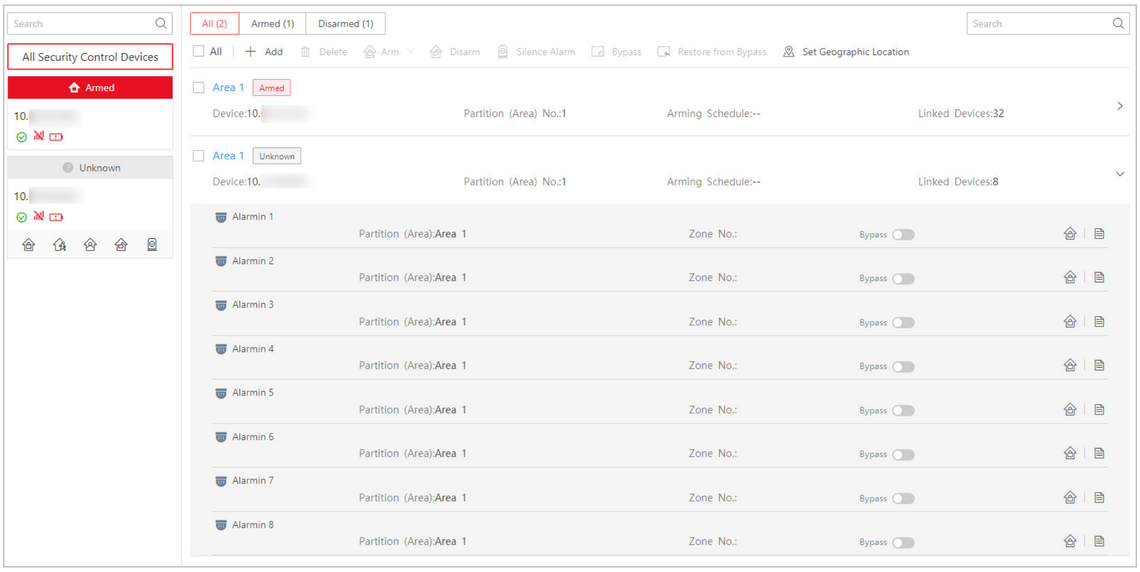


Figure 15-3 Partition (Area) List

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

Edit Security Control Partition (Area)

Click the name of a partition (area) to display the partition (area) details and then edit its name or set the arming schedule for it (see details in ***Configure Arming Schedule Template***).

Note

For the partition (area) of AX security control panel, you configure the arming schedule directly on the partition (area) details page rather than select a template from the platform.

Arm/Disarm Security Control Partition (Area)

After arming the partitions (areas), the platform can receive the triggered alarms in the partitions (areas).

There are three arming modes available.

Note

The supported arming modes are displayed according to the device's capability.

- **Away Arm**: If all people in the detection area are going to leave, turn on this mode to arm the zones in the area after the defined dwell time.
- **Stay Arm**: It is used when people stay inside the detection area. Turn on the Stay mode to turn on all the perimeter burglary detectors (such as perimeter detectors, magnetic contacts, curtain detectors in the balcony). Meanwhile, the detectors inside the detection area are bypassed (such as

PIR detectors). People can move inside the area and alarms will not be triggered.
- **Instant Arm**: When people leave the detection area, the zones will be armed immediately without delay.

In the partition (area) list, select one or multiple partitions (areas) and click these buttons above to arm the partitions (areas), or click **Disarm** to disarm them.

Arm/Disarm Zone

Note

For partitions (areas) that are disarmed, you can arm only a part of their zones.

Expand the partition (area) details and click / to arm/disarm the zone of the alarm input.

Bypass/ Restore Zone

Note

When some exception occurs in one zone, and other zones can work normally, you need to bypass the abnormal zone to turn off the protection of it. Otherwise, you cannot arm the security control partition (area) which the zone belongs to.

Expand the partition (area) details and enable/disable **Bypass** to bypass/ restore the zone of the alarm input.

Clear Alarm

Select one or multiple partitions (areas) and click **Clear Alarms** to clear the generated alarms.

Add Partition (Area) on Map

Select one or multiple partitions (areas) and click **Set Geographic Location** to add them on the map.

15.4 Configure Arming Schedule Template

The arming schedule defines the arming mode (instant arming / away arming / stay arming) in different periods for the partitions (areas) of the added security control devices.

Steps

1. On the top navigation bar, go to → **Security Monitoring → Alarm Detection → Arming Schedule Template** .
2. Click + to enter the Add Arming Schedule Template page.
3. Enter a name for the template.
4. **Optional:** In Copy from field, select an existing template from the drop-down list to copy the settings.
5. Select an arming mode and drag the mouse on the time bar to draw a time period.

Note

Up to 8 time periods can be set for each day.

Instant Arm

When people leave the detection area, the zones will be armed immediately without delay.

Away Arm

If all people in the detection area are going to leave, turn on this mode to arm the zones in the area after the defined dwell time.

Stay Arm

It is used when people stay inside the detection area. Turn on this mode to turn on all the perimeter burglary detectors (such as perimeter detectors, magnetic contacts, curtain detectors in the balcony). Meanwhile, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarms will not be triggered.

6. **Optional:** Click **Erase** and click on the drawn time period to clear it.
7. Click **Add**.

The arming schedule template will be displayed on the arming schedule template list.

Chapter 16 Map Management

Two types of map are available: GIS map and E-map. On the GIS map, you can set and view the current site, Remote Site, and element's geographic location. On the e-map, which is a static map, you can set and view the geographic locations of the installed cameras, alarm inputs, and alarm outputs, etc.

With the GIS map, you can see the geographic locations of your security system. This type of map uses a geographic information system to accurately show all the hot spots' (resources placed on the map are called hot spots) geographic locations in the real world. GIS map lets you view and access devices at multiple locations around the world in a geographically correct way. If the resources locate in multiple locations (e.g., different cities, different countries), GIS map can give you a single view to show them all and help you quickly go to each location to view video from the cameras. With the hot region, you can link to the e-map to view the detailed monitoring scenario, for example, the monitoring scenario of a building.

E-map is a static image (it does not have to be geographical maps, although they often are. Depending on your organization's needs, photos and other kinds of image files can also be used as e-maps) which gives you a visual overview of the locations and distributions of the hot spots (resources placed on the map are called hot spots). You can see the physical locations of the cameras, alarm inputs, and alarm outputs, etc., and in what direction the cameras are pointing. With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

After configuring the e-map via Web Client, you can view the live video and playback of the elements via both Web Client and Control Client, and get a notification message from the map via Control Client when an alarm is triggered.

16.1 Configure Map

You need to configure GIS maps and e-maps before using them. You can add hot spots, hot regions, labels, resource groups, etc. to the maps.

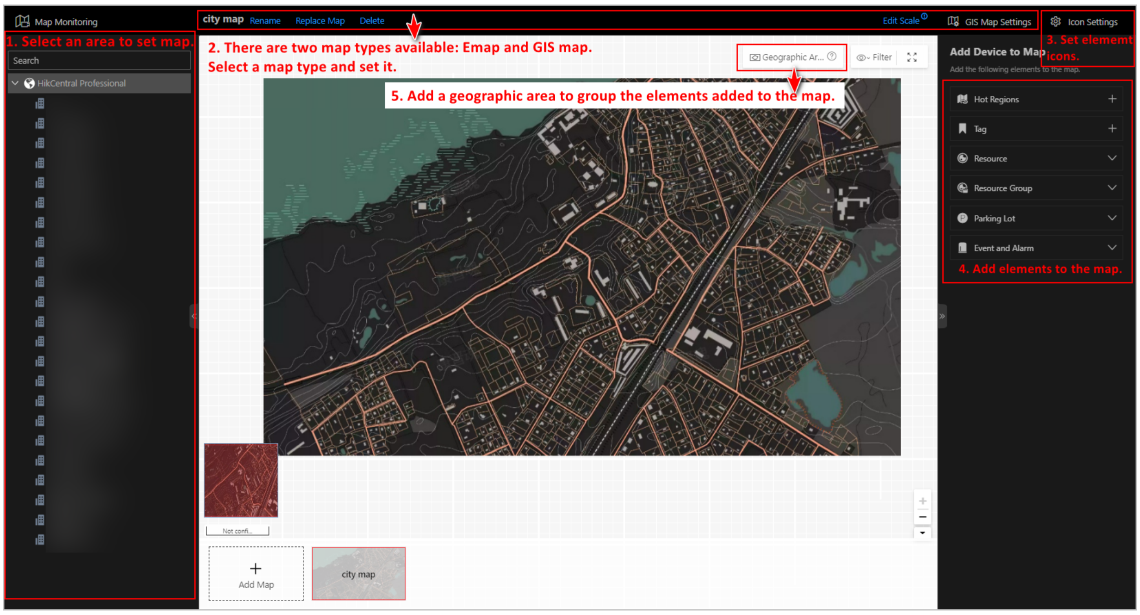


Figure 16-1 Main Interface of Configuring Map

16.1.1 Select and Set GIS or E-map for an Area

You can either set a GIS map for an area or upload an E-map for an area.

Steps

1. On the top navigation bar, select ▦ → **Security Monitoring** → **Visual Map** → **Map** → **Map Settings** .

Add E-Map for Area

You can add and link e-maps to the area so that the elements assigned to the area can be added to e-map.

Steps

1. Select an area on the left.
2. Open the Add Map pane.
   - If you have configured GIS map, click **+** on the lower right of the map.
   - If you did not configure GIS map, click **Add Map** at the center of the page.
3. Select an adding mode.
4. Select a map.
   - If you select **Add E-Map** as the adding mode, select a map picture saved on the PC.
   - If you select **Link to Other Map**, select an area from the following list.
5. Click **Add**.
6. **Optional:** Set a map scale.

Note

The scale of a map is the ratio of a distance on the map to the corresponding distance on the ground. The client can calculate two locations' distance on the map according to the distance on the ground. An accurate map scale is essential for defining a radar's detection area. Perform this step if you plan to add a radar to the map.

1) Click **Edit Scale** on the top right of the map.
2) Click two locations on the map to form a line.
3) Enter the real distance between the two points in the Actual Length field.
4) Click **OK** to finish setting the map scale.

7. **Optional:** Hover the mouse over the added e-map area to perform the following operations.

Edit Picture	Click and change a picture.
Edit Map Name	Click and set a custom name for the map.
Unlink Map	Click to remove the map or cancel the linkage between the map and area.

This page allows you to enable GIS (Geographic Information System) map function to display the online or/and offline GIS map on the Web Client and Control Client, so that the geographic location of the resources (such as current site, Remote Sites, cameras) can be shown on the map.

Steps

1. On the top right, click **GIS Map Settings** and set the GIS Map.
   1) Switch the **GIS Map** on to enable the GIS map function.
   2) According to the actual requirements, select **Online** or **Offline** to set the online GIS map or offline GIS map.
      - For online GIS map, enter the GIS map API URL.

        Note

        - The Google map API is supported currently.
        - Google Maps are provided by Google Inc. (Hereinafter referred to as "Google"). We only provides you the URLs to use Google Maps. You shall apply by yourself for the use of Google Maps from Google. You shall comply with Google terms and provide certain information to Google if required.
        - You shall set the correct GIS map API URL, otherwise the configuration can not be saved.
      - For offline GIS map, you can upload map files in tar.gz or tar format, of which the size is no larger than 1 GB.

        Note

        Click **Download Offline Map Configuration Guide** to refer to the guide and the interface instruction to add and configure the offline map.
   3) Click **Save**.
2. Click **Icon Settings** to set the customized icons.
   1) Select a device type to enter the icon settings page.
   2) Set the icon size, including width (px) and height (px).

3) Click **Add** to select a picture file from the local PC.

Note

The icon picture format can only be PNG, JPG, or JPEG.

4) **Optional:** Click to constrain the aspect ratio.
5) Click **Save**.

Note

You can customize door icons for the five status, namely general, door open, door closed, remain open, remain closed, and unknown.

Result

You can view the GIS map on Map Monitoring page and perform the following operations in the map area.

Operations After Adding Maps

Result

Filter	Click and select the object type you want to show on the map.
Full Screen	Click to show the map in full-screen mode.
Zoom In/Out	Scroll the mouse wheel or click / to zoom in or zoom out the map.
Adjust Map Area	Click-and-drag the map to adjust the map area for view.
View Resource Latitude and Longitude (For GIS Map)	Hover over a resource, and you can view its latitude and longitude on the GIS map.

16.1.2 Add Hot Spot on Map

You can add elements (e.g., doors, alarm inputs, etc.) as the hot spot and place the hot spot on the e-map. Then you can view the elements on the map and perform further operations via Mobile Client.

Before You Start

A map should ***have been added*** .

Steps

1. In the top left corner of Home page, select → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.

3. **Optional:** Select a map.
4. Click **Resource Group** on the right.
5. Select a device type and an area from the drop-down lists.
6. Select a device and drag it to the map.

   The hot spot is displayed on the map.
7. **Optional:** Perform the following operations after adding the hot spot.

Adjust Hot Spot Location	Drag the added hot spot on the map to the desired locations.
Edit Hot Spot	Click the added hot spot icon on the map and click **Edit** to edit the detailed information (such as selecting icon style).
Delete Hot Spot	Click the hot spot icon on the map and click **Delete** to remove the hot spot from the map.

Draw Zone or Trigger Line for Radar

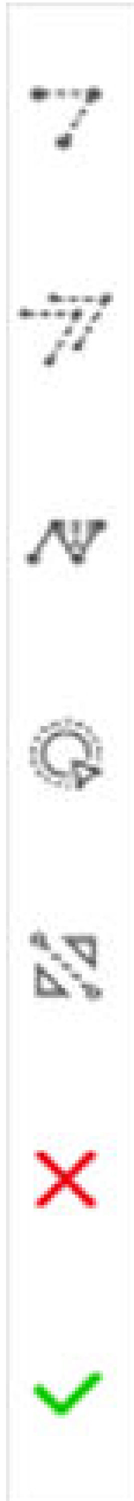
You can draw zones or trigger lines for radar, so if an object is detected to have crossed the trigger line or entered the area shaped by the dual-trigger line or zone, the event and alarm will be triggered.

Before You Start

A radar has been added to the area and map. Refer to ***Add Hot Spot on Map*** for details.

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** .
2. Click the radar's icon on the map and then select **Draw Zone/Trigger Line** from the drop-down list to start drawing zone or trigger line for radar.
3. Select a zone drawing method in the tool bar in the upper-left corner of the map.



Draw Trigger Line

A trigger line is a virtual line drawn in the radar's detection area. An event or alarm will be triggered if an object is detected to have crossed the line. Click to draw a trigger line in the detection area. Select a direction for the trigger line. The three directions indicate three directions to which a detected object crosses the line. You can drag the anchor (the red point on the trigger line) to reshape the trigger line, or drag the trigger line to move it to another place.

Note

No more than 4 trigger lines can be drawn.

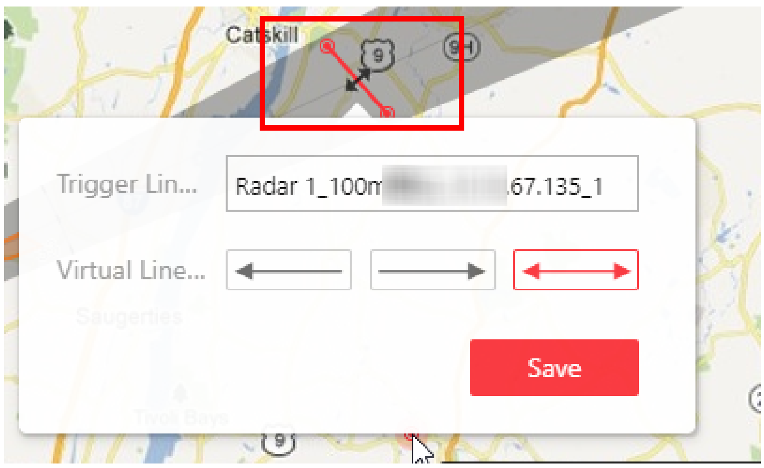


Figure 16-3 Trigger Line in the Detection Area

Draw Dual-Trigger Line

A dual-trigger line consists of 2 virtual lines drawn in the radar's detection area. Generally, it is used to mark an area in the radar's detection area. An event or alarm will be triggered if an object is detected to have entered the area shaped by the dual-trigger line. Click to draw a dual-trigger line in the detection area. Select a direction for the trigger line. The three directions indicate three directions to which a detected object crosses the line. You can drag the anchor (the red point on the trigger line) to reshape the dual-trigger line, or drag the dual-trigger line to move it to another place.

Note

Only 1 dual-trigger line can be drawn in the radar's detection area.

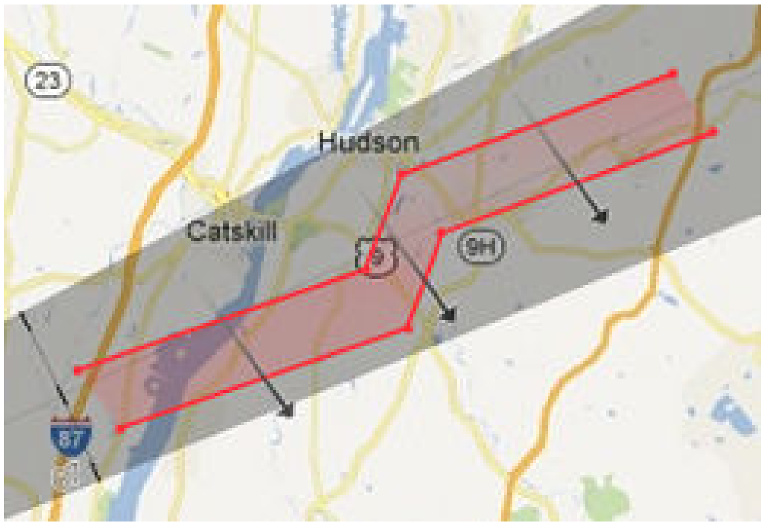


Figure 16-4 Dual-Trigger Line in the Detection Area

Manually Draw

You can draw any shape for the zone using this method.

Zone Segmentation

Split a zone into two smaller zones by a line.

Figure 16-5 Zone Segmentation

Distance Segmentation

Split a zone into two smaller zone by an arc.

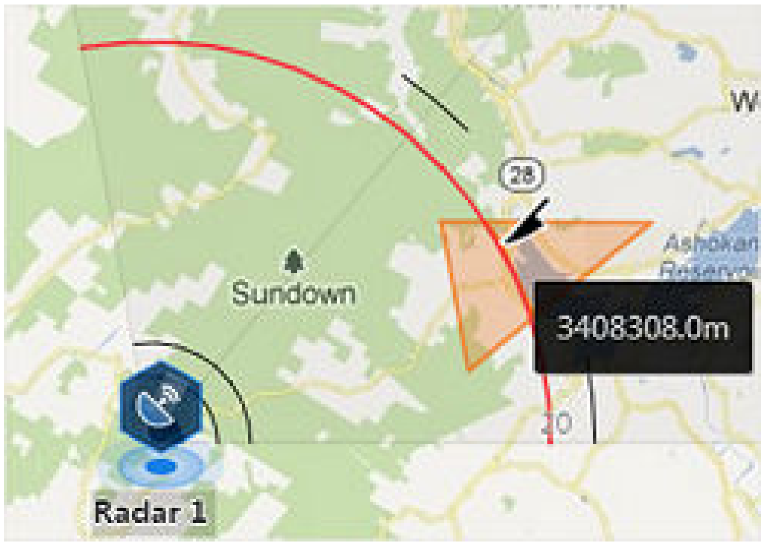


Figure 16-6 Distance Segmentation

4. Right click to finish drawing and open a configuration window.
5. Set parameters for the drawn trigger line or zone.
6. Click **Save**.
7. Right click to exit the zone or trigger line drawing mode.

Relate Calibrated Camera to Radar

This operation requires two persons' teamwork: person A walks into the radar's detection area (the person's position will be displayed on the map as a red point), while person B who operates the computer running the Web Client adds calibration points by PTZ control of the camera(s) according to person A's position.

Before You Start

A radar has been added to the area and map. Refer to ***Add Hot Spot on Map*** for details.

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** .
2. Click the radar's icon on the map and then select **Relate Calibrated Camera** from the drop-down list to relate cameras.
3. Click **Resource** on the Map Settings panel and drag camera(s) to the map.

Note

- This function needs to be supported by the device.
- Up to 4 calibrated cameras can be added.

4. Click the radar's icon first, and then click camera icon(s) to relate the camera(s) with the radar.

Note

You can right click to finish relating cameras or it will automatically finish when no camera can be related.

5. Click the radar's icon on the map and then select **Calibrate PTZ Camera** from the drop-down list to enter the camera calibration settings page.
6. Person A goes to the location which can be detected by one of the cameras.

   Person A's location will appear on the map as a red point .
7. Person B clicks on the map to open the adding calibration point window.

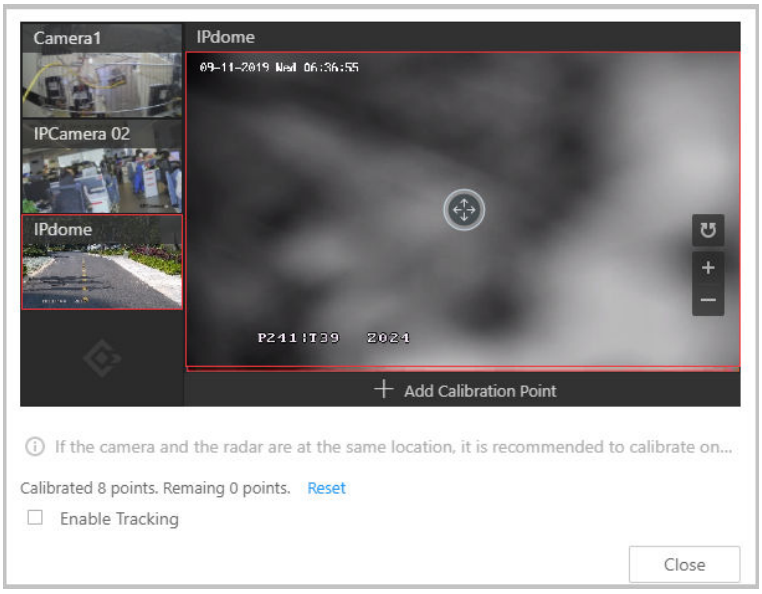


Figure 16-7 Add Calibration Point

   The cameras' thumbnails will be displayed on the left of the window.
8. **Optional:** Undo-check the **Enable Tracking** if you have enabled visual tracking for the calibrated cameras.
9. Click a camera's thumbnail to display its image in the window on the right.
10. Click the image to turn the camera to the position of person A until person A appears in the image.
11. Click **Add Calibration Point** to add the current image as a calibration point.

Note

- If the camera locates above or under the radar vertically, only 1 calibration point is enough; if not, at least 4 calibration points are required.
- Up to 8 calibration points can be added for one cameras.

12. **Optional:** Check **Enable Tracking** if you have enabled visual tracking for the calibrated cameras.
13. Close the Add Calibration Point window and click to save the settings.

16.1.3 Add Hot Region on Map

The hot region function links a map to another map. When you add a map to another map as a hot region, an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

Before You Start

At least 2 maps should ***have been added*** .

Steps

1. In the top left corner of Home page, select → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Hot Region** icon on the right.
5. Click a position on the map to select it as the location of the hot region.
6. Select an area from the area list.
7. Click **Save** on dialog to add the hot region.

   The added hot region icon will be displayed on the parent map.
8. **Optional:** Perform the following operation(s) after adding the hot region.

Adjust Hot Region Location	Drag the added hot region on the parent map to the desired locations.
Edit Hot Region	Click the added hot region icon on the map to view and edit the detailed information, including GPS location (only available when parent map is GIS map), hot region name, icon style, name color, and remarks on the appearing dialog.
Edit Hot Region Area	Drag the white point on the hot region's line to edit the hot region's size or shape as the following picture.
Delete Hot Region	Click the hot region icon on the map and click **Delete** on the appearing dialog to delete the hot region.

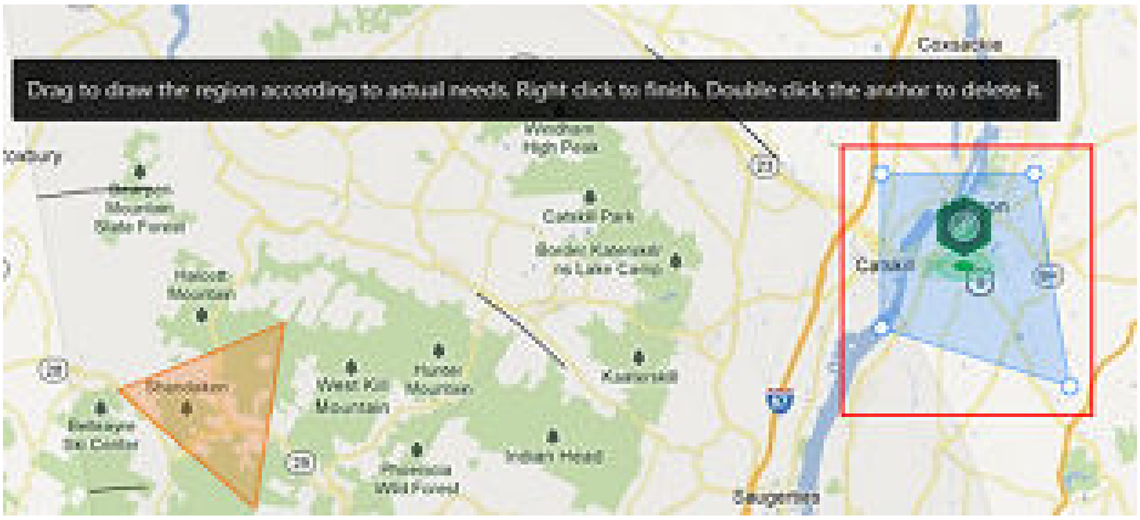


Figure 16-8 Edit Hot Region Area

16.1.4 Add Tag on Map

You can add tags with description on the map.

Before You Start

At least one map should ***have been added*** .

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Tag** icon on the right.
5. Click on the map where you want to place the tag.
6. Customize a name for the tag, and you can input content for the tag as desired.
7. Click **Save**.

   The added tag icon will be displayed on the map.
8. **Optional:** Perform the following operation(s) after adding the tag.

Adjust Tag Location	Drag the added tag on the map to the desired locations.
Edit Tag	Click the added tag icon on the map to view and edit the detailed information, including name and content on the appearing dialog.
Delete Tag	Click the tag icon on the map and click **Delete** on the appearing dialog to delete the tag.

16.1.5 Add Resource Group on Map

You can also add the resource groups on the map by locating the resources in the group on the map and setting the edge of the region for detection.

Note

Before adding resource groups to a map, make sure that at least one map ***has been added*** .

Currently, the following resource groups can be added on the map for further operations:

People Counting Group

After adding the people counting group on the map, you can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Control Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

Heat Analysis Group

After adding the heat analysis group on the map, the resources (such as doors, fisheye cameras, people counting cameras) will be grouped in certain region and displayed on map, and you can know the dwell time of the people stayed in this region, how many persons stayed in this region, and average dwell time of each people.

Pathway Analysis Group

After adding the pathway analysis group on the map, you can view the real-time number of people walking by in the Monitoring module on the Control Client.

Person Feature Analysis Group

After adding the person feature analysis group, the cameras which support facial recognition and feature analysis will be grouped in one region and displayed on the map. You can view the features of the persons appeared in this region, based on the data detected by the cameras in the group.

Anti-Passback Group

After adding the anti-passback group on the map, when an anti-passback alarm is triggered by the doors in the group, the client will notify the user by highlighting the region on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Mobile ClientControl Client.

For details about how to add an anti-passback group on the map, refer to ***Configure Area Anti-Passback*** .

Multi-Door Interlocking Group

After adding the multi-door interlocking group on the map, when multi-door interlocking alarm is triggered by the doors in the group, the client will notify the user by highlighting the region on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Mobile ClientControl Client.

For details about how to add a multi-door interlocking group on the map, refer to ***Configure Multi-Door Interlocking***

Final Authentication Counting Group

After adding the entry &exit counting group on the map, you can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Mobile ClientControl Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

For details about how to add an entry &exit counting group on the map, refer to ***Add a Final Authentication Counting Group*** .

Batch Locking and Unlocking Group

After adding the emergency operation group on the map, you can operate access points (remaining locked/unlocked) in the group in a batch.

This function is mainly applicable for emergent situation. For example, after grouping the doors of the school's main entrances and exits into one emergency operation group, the school's security personnel can lock down the doors in this group by quick operation on the Mobile ClientControl Client, so that the school closes and no one can get into the school except for maintenance and high level admins. This function would block out teachers, custodians, students, etc.

For details about adding an emergency operation group, refer to ***Add a Batch Locking and Unlocking Group*** .

Partition Group

After adding the security control partition (area) on the map, the security control device's alarm inputs will be grouped according to the zones on the device and displayed on map, and you can set an arming schedule to define when and how to arm the alarm inputs in a batch.

16.1.6 Add Parking Lot on Map

You can add parking lots and entrance and exits on the map to locate them for a visualized monitoring.

Before You Start

A map should ***have been added*** .

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Parking Lot** on the right.
5. Drag a parking lot or an entrance and exit to the map.

The parking lot, entrance or exit will be displayed on the map.

6. **Optional:** Perform the following operations after adding the entrance and exit.

Adjust Parking Lot/ Entrance and Exit Location	Drag the added parking lot/entrance and exit on the map to the desired locations.
Edit Parking Lot/ Entrance and Exit	Click the added parking lot/entrance and exit icon on the map and click **Edit** to edit the detailed information (such as setting GPS location (only available when parent map is GIS map), and selecting icon style).
Delete Parking Lot/ Entrance and Exit	Click the parking lot/entrance and exit icon on the map and click **Delete** to remove the parking lot/entrance and exit from the map.

16.1.7 Add Event and Alarm on Map

You can add the combined alarms and generic alarms on map to locate the alarm for a visualized monitoring.

Before You Start

Make sure you ***have added a map*** .

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Event and Alarm** on the right.
5. Drag a combined alarm or generic event to the map.
6. **Optional:** Perform the following operations after adding the combined alarm.

Adjust Event and Alarm Location	Drag the added element on the map to the desired locations.
Edit Event and Alarm	Click the added element icon on the map and click **Edit** to edit the detailed information (such as setting GPS location (only available when parent map is GIS map), and selecting icon style).
Delete Event and Alarm	Click the element icon on the map and click **Delete** to remove the element from the map.

16.1.8 Add Remote Site on GIS Map

After adding remote sites to GIS map, you can get and manage the global view of the central system. The GIS map shows the geographic locations of remote sites, of which the resources can be displayed.

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** to enter the Map Settings page.
2. **Optional:** Select an area on the left to show its GIS map.
3. Click **Remote Site** on the right to display available remote site(s).
4. Drag a remote site to the map.

   The icon will be displayed on the map.
5. **Optional:** Perform the following operations.

View Site's Resources	Click the site on the map, and select **View Site's Resources**. The resource list of the site will be displayed on the left.
Edit Site	Click the site on the map, and select **Edit** to enter the description of the site.
Delete Site	Click the site on the map, and select **Delete** to remove the site from the map.
Move Site	Drag the site to change its location on the map.

Note

Editing remote site resource is not supported.

16.1.9 Add Geographic Area to Map

Geographic areas refer to a customized map area with elements added to the map. Geographic areas are used to manage multiple elements added to the map. After adding a geographic area to the map, you can batch operate the elements within the area.

In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** to enter the map settings page.

Select an area on the left, and select an E-map or GIS map.

Click **Geographic Area**, left-click to draw a point, and right-click to finish.

Note

- When an alarm occurs from a camera in the area, the geographic area will blink in the color configured in the event and alarm module.
- A resource within the area will be highlighted to indicate that it has been successfully associated with the area. Resources can be dragged in and out so that you can add or remove resources to the region.

16.2 Monitor on Map

After configuring the maps via Web Client, you can view hot spots, hot regions, and resource groups etc., on the map. You can also zoom in/out to view the map and search locations on the map.

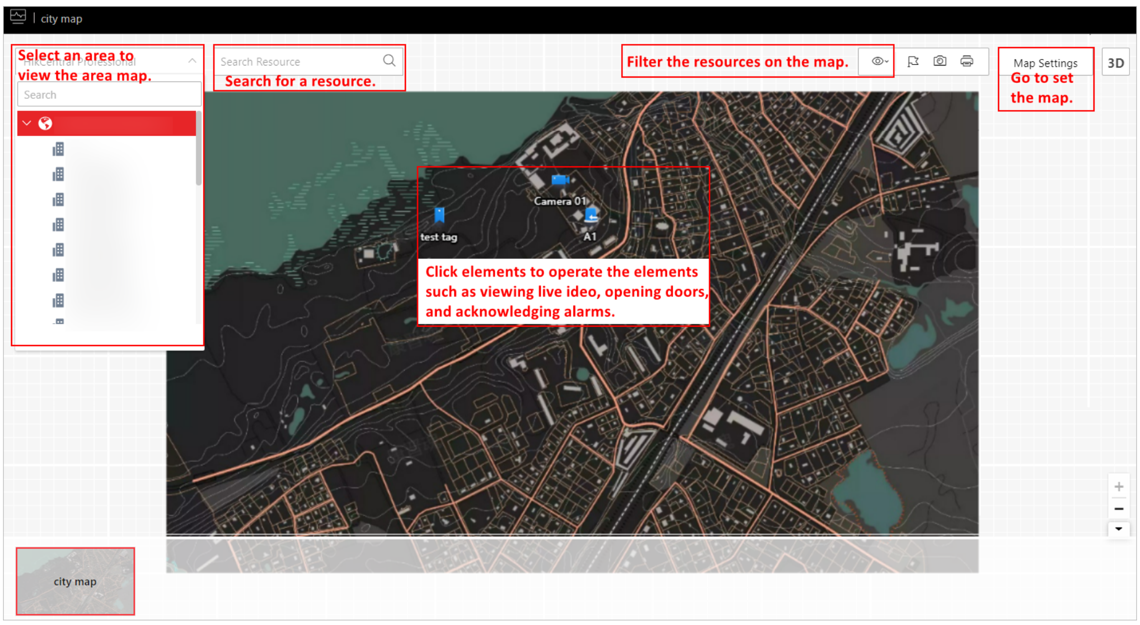


Figure 16-9 Map Monitoring

16.2.1 View and Operate Hot Spot

You can view locations of hot spots including cameras, alarm inputs, alarm outputs, access points, radars, sites, UVSS, etc. on the map. Also, you can set the arming control and view history alarms of monitoring scenarios through the hot spots. You can view latitude and longitude information and available operations of a certain resource by hovering over a resource on GIS map as well.

Before You Start

Configure the map settings via the Web Client. For details, see ***Map Management*** 。

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Monitoring** .
2. On the top left of the map, select an area from the **Select Map** drop-down list.

   All maps of the area will be displayed.
3. Select a map to enter the map.
4. **Optional:** Perform the following operations on the map.

Filter Resource on Map	Click and check resource type(s) as desired.
More Tools	: Add a label on map. **2D/3D**: Switch the displaying dimension of the map. Search : Search hot spot or location on the map.

5. Click the hot spot to open the dialog which displays its related functions.

Note

- If there is an alarm triggered on the hot spot, the hot spot icon will turn into red alarm mode . Click the red icon, and you can view the detailed alarm information.
- Click parking lot data, a panel of parking lot details will pop-up. You can view detailed parking lot information such as parking space occupancy rate and parking floor details.

6. Operate in the dialog.

Arm or Disarm Hot Spot	You can arm or disarm the hot spots via the arming control function. After arming the device, the current Control Client can receive the triggered alarm information from the hot spot. Click a hot spot to open the dialog which displays its related functions. In the dialog, click **Arm/Disarm** to arm/disarm the hot spot.
View History Alarm	When an alarm is triggered, it will be recorded in the system. You can check the history log related to an alarm, including the alarm source details, alarm category, alarm triggered time, etc. Click a hot spot to open the dialog which displays its related functions. In the dialog, click to enter the event and alarm search page. Then you can search history alarms of the hot spot.
Broadcast via Hot Spot	You can broadcast via hot spot through real-time speaking or playing the saved audio files. **Note** Make sure you have added broadcast resources on the map. a. On the map, click the broadcast resource to view details such as Status, Area, and Remark. b. Click **Broadcast** to select the broadcast mode. c. Select **Speak** or **Play Audio File** as the broadcast mode.

Note

Speak: Speak in real-time, and the audio will be recorded and uploaded to the server.

Play Audio File: Play the files saved in the server. You can search or select a desired audio file to play. You can click **Download** to download a selected audio file, and the broadcast will be more fluent.

d. Click **Start**.
   - If you select Speaking, the broadcast will start immediately.
   - If you select Play Audio File, it will start downloading the audio file from the cloud if you choose a cloud file, or to play the audio file immediately if it is a local file.

Figure 16-10 Arm Hot Spot / View History Alarm

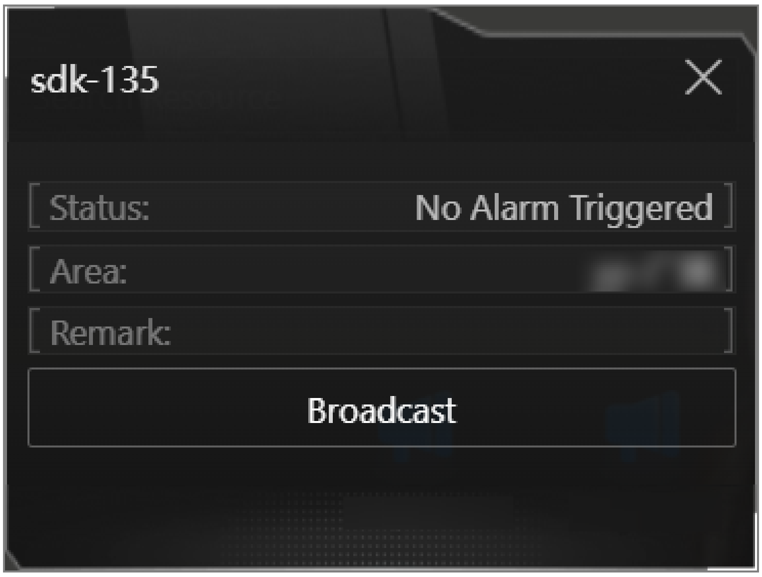


Figure 16-11 Broadcast via Hot Spot

16.2.2 Preview Hot Region

The hot region function links a map to another map. When you add a map to another map as a hot region, an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

Before You Start

Configure the map settings via the Web Client. For details, see ***Map Management*** .

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Monitoring** .
2. Click **Select Map** on the top left to display the map(s) of an area.
3. **Optional:** If an area has multiple maps, click a map to select it.
4. Click a hot region on the map to enter the map of the hot region.

> **Note**
>
> If you enter an area map from a particular map, the full path of the hot region map will be displayed in the upper-left corner. Each time you click **Back**, it only returns to the previous level of the map.

16.2.3 Preview Resource Group

During displaying map, you can view locations and regions of the resource groups, including people counting group, multi-door interlocking group, and anti-passback group. You can also perform further operations on the resources in the group.

Note

Make sure you have configured the required resource group and map settings via the Web Client. For details, see ***Map Management*** .

In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Monitoring** .

- People Counting Group: You can view the real-time number of people entered, exited the region, or stayed in the region. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the region of the group will be highlighted on the map to notify the user on the Control Client.
- Pathway Analysis Group: You can view the real-time number of people walking by in the Monitoring module on the Control Client.
- Anti-Passback Group: When an anti-passback alarm is triggered by the doors in the group, the region of the group will be highlighted on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Control Client.
- Multi-Door Interlocking Group: When multi-door interlocking alarm is triggered by the doors in the group, the region of the group will be highlighted on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Control Client.
- Entry & Exit Counting Group: You can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Control Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

16.2.4 View Remote Site Alarm

If you have added a remote site on a GIS map, you can view the information of alarms triggered on the remote site. Even if there is no alarm triggered at the current time, you can also view history alarms of the site.

Before You Start

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Monitoring** to enter the Map Monitoring page.
2. **Optional:** Select an area on the left to show its GIS map.
3. Click the site icon to open the site details page.

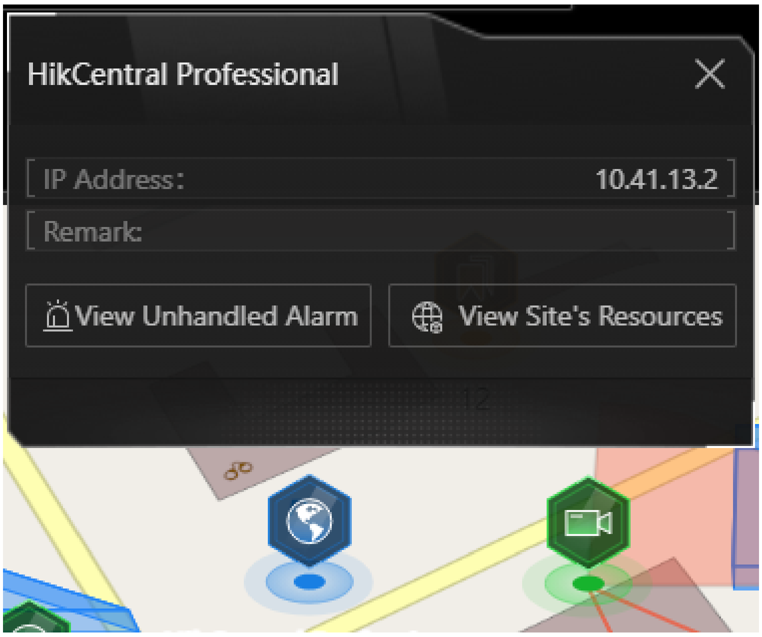


Figure 16-12 Site Details

The color of site icon will turn blue.

4. Click **View Unhandled Alarm** to open the Unhandled Alarm window.

   Alarm information including alarm name, alarm priority, triggering time, alarm source, etc. is displayed.

5. **Optional:** Perform the following operation(s).

Filter Alarm by Priority	Click on the Alarm Priority column to filter alarms by alarm priority.
Filter Alarm by Status	Click on the Alarm Status column to filter alarms by alarm status.

16.2.5 Operate Resources from Geographic Area

After you add a geographic area to a map, you can batch operate the resources within the area.

In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Monitoring** ..

Click **Select Map** on the top left to display the map(s) of an area.

Note

- When multiple geographic regions overlap, you can select the geographic region from the list first and then click the menu.
- Batch operation is not supported when there are more than 100 resources in a geographic area.

Click the geographic area to perform the following operations.

Block All Alarms	Click **Ignore All** to block all alarms in the area.
Broadcast	Click **Broadcast**, and all IP speakers in the area will start to broadcast and the device icon status will change.
Audio Alarm Control	Click **Audio Alarm Control** to start audible alarms.
Strobe Light Alarm Control	Click **Strobe Light Alarm Control** to start sound and light alarm of all devices in the area with the feature.

Chapter 17 Augmented Reality (AR) Monitoring

To start AR monitoring, you need to first add AR cameras, then add scenes, and finally add scenes to maps on the Web Client. After configuration on the Web Client, you can monitor on the Control Client.

Based on the augmented reality (AR) technology and AR real map service (ARRM), by analyzing the person/vehicle event information overlaid in the real-time videos that are streamed from linked AR camera channels and speed dome channels, you are able to grasp the key area's situation and develop strategies for commanding and dispatching in response.

Note

If the AR license is not purchased, the AR menu will not be displayed.

17.1 Add Scene

Scenes refer to panoramic images captured by AR channels. You can add a scene to an area, and link an AR camera channel and a speed dome camera with the scene.

Go to → **Visual Map → AR → Add Scene** .

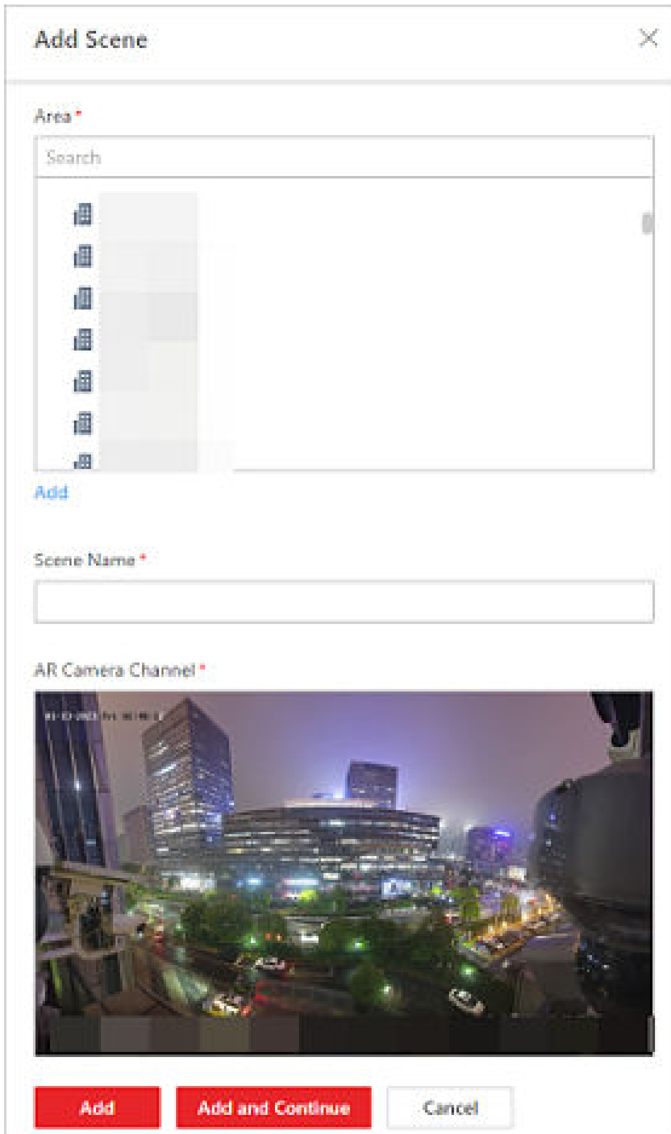


Figure 17-1 Add Scene

Select an area for the scene and set a name for the scene.

You can add an AR camera and a speed dome to a scene or just add an AR camera. AR cameras are for getting panoramic images, and speed domes are for tracking targets or zooming in parts on panoramic images.

Note

Under the condition that speed domes are not configured for the scene, visual tracking will not be available.

Click **Add**, or click **Add and Continue** to add another scene.

After adding scenes, you can set their locations on the map. For details, refer to ***Add Scene to Map*** .

17.2 Add Scene to Map

After scenes are added, you need to configure their locations on maps.

Note

Make sure you add scenes first. For details, refer to ***Add Scene*** .

1. Go to → **Security Monitoring → Visual Map → AR** .
2. In the scene list, click in the Operation column, and you will be redirected to the Geographic Location Configuration page.
3. Hover over a scene, click , and drag its icon to adjust its location on the map.

   Note

   The added scene will be marked with a small map icon in its upper right corner.

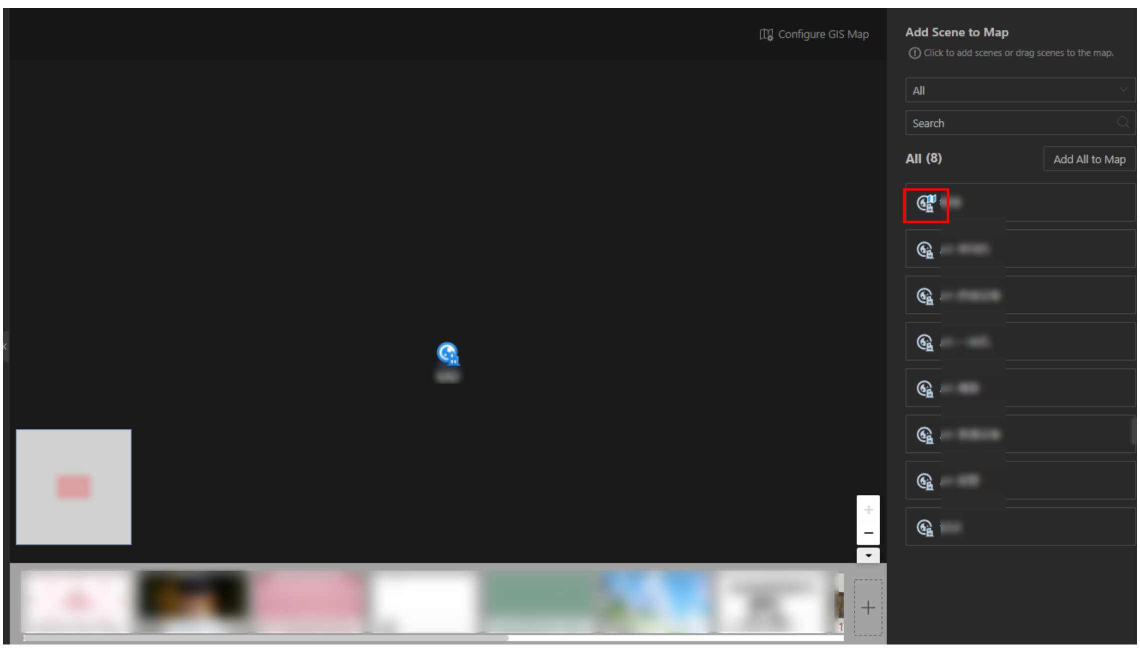


Figure 17-2 Icon of Added Scene

4. Click **Finish**.

Chapter 18 Event and Alarm

On the Web Client, you can set rules to detect events and alarms, and set linkage actions for notification. The detailed information of the events and alarms can be received and checked via the Mobile Client.

Event

Event is the signal that resource (e.g., device, camera, server) sends when something occurs. The platform can receive and record events for checking, and can also trigger a series of linkage actions for notification. The event can also trigger an alarm for further notification and linkage actions (such as alarm recipients and pop-up window). You can check the event related video and captured pictures if you set the recording and capturing as event linkages.

The rule of an event includes four elements, namely, "event source" (i.e., the device which detects the event), "triggering event" (the specified event type), "what to do" (linkage actions after this event is detected), and "when" (during the specified time period, the linkage actions can be triggered).

Alarm

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. Alarm can trigger a series of linkage actions (e.g., popping up window, showing the alarm details) for notification and alarm handling. You can check the received real-time alarm information and search for history alarms.

The rule of an alarm includes six elements, namely, "alarm source" (i.e., the device which detects the triggering event), "triggering event" (the specified event type occurred on the alarm source and triggers the alarm), "when" (during the specified time period, the alarm can be triggered), "recipient" (the user on the platform who can receive this alarm), "priority" (the importance or urgency of this alarm), and "what to do" (linkage actions after this alarm is triggered).

Linkage Action

An event's linkage actions (such as recording and capturing) are used to record the event details and trigger basic actions (such as linking access point to lock or unlock, triggering alarm output, and sending email).

An alarm's linkage actions (such as popping up an alarm window, displaying on the smart wall, and audible warning) are used to record the alarm details and provide recipients multiple ways to view the alarm information for alarm acknowledgment and handling.

Example

What is an Event

The event can be defined as intrusion ("triggering event") which happens in the bank vault and be detected by the camera mounted in the bank vault ("event source") on weekend ("when"), and triggers the camera to start recording ("what to do") once happened.

Example

What is an Alarm

The alarm can be defined as intrusion ("triggering event") which happens in the bank vault and be detected by the camera mounted in the bank vault ("alarm source") on weekend ("when"), and triggers the camera to start recording ("what to do") once happened. This alarm is marked as High priority ("priority"), and users including the admin and operators ("recipient") can receive this alarm notification and check the alarm details.

18.1 Manage Event and Alarm

You can configure parameters for event types provided by the platform to detect normal events or trigger normal alarms, or add combined alarms, generic events, and user-defined events for a wider range of applications.

18.1.1 Supported Events and Alarms

Currently, the platform supports following events and alarms for different types of resources.

Video

Camera

Video exceptions or events occurred in the monitoring area of the camera, such as the motion detection, line crossing, and so on.

Alarm Input

Events occurred on alarm inputs of video devices on the platform.

Face Picture

Events detected by facial recognition camera or temperature screening cameras, such as the face matched events, face mismatched events, rarely appeared person events, and so on.

Person/Vehicle Arming Group

Events occurred when the camera group detect and track a person or vehicle of interest, including auto person arming and tracking and auto vehicle arming and tracking.

Portable Enforcement

Portable Device

Events occurred on portable devices, including Low Battery Alarm, Use Device Before File Copied Back, and Use Device Before Full Charging.

Alarm Input

Events occurred on alarm inputs of portable devices on the platform.

Access Control

Door

Events occurred on doors of access control devices and video intercom devices, such as access event and door status event.

Elevator

Events occurred in elevators, such as card swiping event and elevator status event.

Alarm Input

Events occurred on alarm inputs of access control devices on the platform.

Person

Events occurred during the process of authentication by person, such as card No. matched events and person matched events.

Patrol

Events occurred during the patrol process, such as early patrol, late patrol, and so on.

ANPR (Vehicle Attribute)

Events occurred during the vehicle recognition process, such as vehicle matched events, vehicle type matched events, and vehicle mismatched events.

Parking Lot

Events occurred in different parking lots or during the parking process, such as blocklist events, overstayed events, and so on.

Alarm Detection

Radar

Events detected by radar or during the radar configuration process, such as arming events, line crossing event, and so on.

Alarm Input

Events occurred on alarm inputs of security control devices on the platform, such as alarm input restored events, bypass events, and so on.

Partition (Area)

Events occurred in partitions (areas) of security control panels on the platform, such as away arming events, instant arming events, and so on.

Intelligent Analysis

Events occurred during the regional people counting process and store people counting.

Digital Signage

Events detected by digital signage terminals, such as abnormal temperature events.

Maintenance

Operation exceptions occurred on the resources (e.g., cameras, doors, dock stations, recording servers) added to the platform, such as the device offline, server exception, and so on.

Third Party

Alarms of third-party devices.

User

Events occurred during the user login and logout process.

Custom Event

User-Defined Event

Events defined by users themselves.

Generic Event

Events transferred in the form of TCP/UDP/HTTP/HTTPS data packages from resources (e.g., external systems and devices) if something occurred and matched the configured expression.

Device Application Event

Events uploaded by the added resources which contain HEOP or AIOP application.

Visitor

Events occurred during the visiting process.

Note

You should enable the detection frequency of automatic checkout for visitor after the effective period.

Broadcast

Events occurred on alarm inputs linked with IP speakers.

Security Inspection

Events occurred on walk-through metal detectors.

On-Board Monitoring

Events detected by driving devices and occurring during the vehicle driving process.

18.1.2 Add Normal Event and Alarm

The platform provides multiple triggering event types for you to configure rules for detection or triggering alarms.

In the top left corner of the Home page, select → **Security Monitoring → Event and Alarm** .

Select **Event and Alarm Configuration → Normal Event and Alarm** on the left.

Click **Add** to enter the Add Event and Alarm page

Basic Information

Triggering Event

The specific event type detected on the event source will trigger an event or alarm.

Note

If you select Intrusion (VCA Event) as the triggering event, you can select specific regions under a source.

Source

This field refers to the specific entity (such as devices, servers, etc.) which can trigger this event and alarm.

Note

- When setting a thermal-related event and alarm for thermal cameras, you can select areas, points, or lines as event and alarm sources.
- Triggering event types including **Camera**, **Alarm Input**, and **Face** in **Video** and **Camera**, **Encoding Device**, **Decoding Device**, **Recording Server**, and **Streaming Server** in **Maintenance** support selecting sources in remote sites. For different device types, the labels vary.
- The Triggering Event and Source fields support fuzzy search.

Name

After selecting the source(s), you need to name the event or alarm. You can customize a name, or click the labels below to name the event or alarm by the selected label(s). If you name the event or alarm by the selected labels, the platform will display the event/alarm name by the combination of source name, area name, triggering event name, or site name, so that you can quickly know the location where the event/alarm occurs.

Face Picture Library

If the triggering event you select is **Face**, you need to select the face picture library so that the platform can compare the detected face pictures with face pictures in the library.

Threshold

If the triggering event you select is **Regional People Counting**, you need to set extra conditions to define the triggering event.

Currently, you can set **People Counting Above/Below Threshold** and **People Counting Above/ Below Threshold (Pre-Alarm)** for the people counting group. For these two alarms, you need to set the threshold which determines whether the selected people counting groups will trigger an alarm when the detected number of people stayed less than or more than the threshold.

For example, if you set the threshold as ***"≥ 100 or ≤ 10"***, when the number of people detected in the selected people counting group is more than 100 or less than 10, an alarm will be triggered to notify the security personnel.

Frequency

For some sources and events, you can set the frequency. For example, if the source type you selected is **Parking Lot** and the triggering event is **Frequently Appeared Vehicle in All Selected Lists** or **Frequently Appeared Vehicle in One of the Selected Lists**, you can predefine the frequency.

For example, if you set the frequency to daily 3 times, when the devices in the source parking lot detect the license plate numbers of the vehicles in the selected vehicle list more than 3 times in one day, an alarm will be triggered.

Vehicle List

If you select triggering events related to vehicle recognition, you need to select vehicle lists, so that the platform will compare detected vehicles with vehicles in the selected list.

Vehicle Type

If the source type you selected is **Vehicle Features** and the triggering event is **Vehicle Type Matched Event**, you need to specify the vehicle type(s). When the source camera detects a vehicle the type of which matches the one(s) you selected here, a vehicle type matched alarm will be triggered.

For example, if the oil tank truck is not allowed on one road, you can set a vehicle type matched alarm for the camera mounted on this road and set the vehicle type as **Oil Tank Truck**. When the camera detects an oil tank truck, an alarm will be triggered.

Color

Select the color to indicate this event or alarm. You can set the color according to the emergency of this event or alarm. For example, you can set red color for the urgent alarm and set green color for the prompt event.

Ignore Repetitive Events/Alarms

This function is used to avoid the same event or alarm occurring frequently in a short time. You need to set the **Ignore For (Second)** which is the threshold of the recurring events or alarms.

For example, if you set **Ignore For (Second)** to 30 seconds, the events or alarms of the same type that occurred on the same camera within 30 seconds will be regarded as one event or alarm.

Delay Alarm

If the source type you selected is **Camera** of **Maintenance** and the triggering event is **Camera Offline**, you can enable this function and set a delay duration. During the delay duration, when the source detects the triggering event, the triggering event will not be uploaded to the platform. After this duration, if the source still detects this triggering event, the triggering event will be uploaded to the platform and trigger an alarm.

With this function, when the platform detects that the camera is offline, if the camera gets online again within the delay duration, it will not trigger a camera offline alarm. Thus the maintainers can focus on the cameras which are truly disconnected.

Actions

The field links actions for the alarms, you can click **Add Linkage Action** to select actions.

Trigger Recording

Select the related camera to record the alarm video (make sure the related camera(s) have been configured with the recording schedule) when the alarm is triggered.

- To relate the source camera itself for recording, select **Source Camera** and select the storage location (i.e., **Store in Main Storage**, **Store in Auxiliary Storage**, and **Not Store**) for storing the video files.

Note

If the camera is not configured with the main storage, you can still select the storage location as **Store in Main Storage**, but the rule exception will be prompted.

- To relate other cameras, select **Specified Camera** and click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
- **View Pre-Event Video:** You can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record the video for after the alarm stops. You can also click **Custom** to custom the time period.
- **Lock Video Files For:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the video to be displayed by default on the Control Client when receiving the triggered alarm information. You can select the recorded video or the live video to be displayed.

Capture Picture

Select cameras to capture pictures during the alarm, and you can view the captured pictures when checking the alarm.

- If the alarm source is a camera, you can set it to trigger the source camera itself for capturing pictures by selecting **Source Camera**.
- To trigger other cameras for capturing pictures, select **Specified Camera** and select cameras for capturing pictures.

Capture Picture: Specify the number of seconds to define when the camera will capture pictures for the alarm. After you set the number of seconds for pre/post-event (here the event refers to the triggering event), the camera will capture one picture at 3 time points respectively: at the configured seconds before the alarm starts, at the configured seconds after the alarm ends, and when the event is happening (as shown in the picture below).

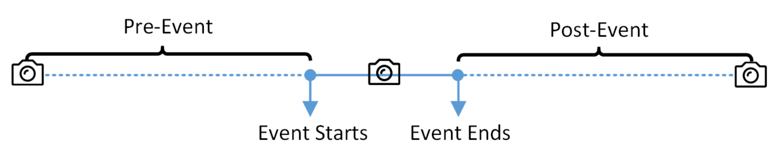


Figure 18-1 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video footage. This pre-event capture function is only supported by the camera which is set to store the video in the recording server.

Create Tag

Select the camera(s) to record video when the event occurs and set the storage location for storing video files. The platform will add a tag to the event-triggered video footage for convenient search.

- If the event source is a camera, to relate the source camera itself for tagged recording, select **Source Camera** and select the storage location (i.e., **Store in Main Storage**, **Store in Auxiliary Storage**, and **Not Store**) for storing the video files.

  Note

  If the camera is not configured with the main storage, you can still select the storage location as **Store in Main Storage**, but the rule exception will be prompted.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged length of the video footage. For example, you can set it to record the tagged video starting from 5 seconds before the event and lasting until 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Link Access Point

You can enable this function to trigger the access points to take certain actions.

For doors, the doors can be locked, unlocked, remained locked, or remained unlocked when the event occurs.

For floors, the elevators can access the floors freely, with credentials, temporarily, or the access is forbidden.

For example, you can set it to trigger all the doors remaining locked and all the floors access forbidden when the intrusion of a suspicious person is detected.

- **All Access Points**: When the alarm is triggered, the platform will trigger all the doors and floors to take certain actions.
- **Specified Access Point:** Click **Add** to select specified access points or emergency operation groups as the linkage targets. When the event occurs, the platform will trigger these doors/ floors in the emergency operation groups to take certain actions.

Link Alarm Input

Select alarm inputs and these alarm inputs will be armed or disarmed when the event occurs.

For example, when adding an intrusion alarm of camera A, which is mounted at the entrance of the building, you can link to arm the alarm input B, C, and D, which are PIR detectors mounted in different rooms in the building and are disarmed usually. When camera A detects the intrusion alarm, these PIR detectors will be armed and trigger other events or alarms (if rules are configured), so that the security personnel will get to know where the suspect goes.

Link Alarm Output

Select alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Alarm Output Closing Method: The added alarm outputs can be closed manually, or you can set the time period after which the alarm outputs will be closed automatically.

Trigger PTZ

Call the preset, patrol, or pattern of the selected cameras when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Link Third-Party Integrated Resource

Click **Add** to select the resources integrated from a third-party platform and set the control about detailed operations that will happen when the event occurs.

Send Email

Select an email template to send the event information according to the defined email settings. If you have purchased the License for emergency mustering, you can select an emergency counting group of an area in the drop-down list of **Send Data of Emergency Counting Groups**. When the event occurs, the platform will send the data of the selected emergency counting group to the email in a PDF file.

Note

For details about setting the email template, refer to ***Set Email Template*** .

Attach with Entry & Exit Counting

If the source type you selected is **Alarm Input**, you can select an entry & exit counting group from the drop-down list to attach a report of entry & exit counting in the sent email.

For example, if the fire alarm input detects fire in the building, the security personnel will receive a file, which contains information such as the number of people still in the building, their names and profile photos, phone numbers, and locations of last access.

Trigger User-Defined Event

Select the user-defined event(s) in the event list as the linkage action when the event occurs.

Note

- Up to 16 user-defined events can be selected as linkage actions.
- For setting the user-defined event, refer to ***Add User-Defined Event*** .

Link Printer

If the source type you selected is **Alarm Input**, you can link to print the entry & exit counting report of a certain entry & exit counting group.

For example, if the fire alarm input detects fire in the building, the platform will automatically send the entry & exit counting report to all the printers configured on the platform so that they can get the information such as how many people are still in the building, their names and profile photos, phone numbers, and locations of last access.

For details about printer settings, refer to ***Set Printer*** .

Apply Notice to Indoor Station

If the source type you selected is **Alarm Input**, you can apply notice to specific indoor stations.

Link Speaker Unit

You can link the speaker unit to an event and set the broadcast content (audio file, custom broadcast content, or none). The linked speaker unit will play the set content when the event occurs. When you select **None** for the broadcast content, you can perform remote speaking via the Control Client.

Send HTTP Request

Set the HTTP command, HTTP link, user name, password, etc., to send the HTTP request when the event occurs.

Trigger Remaining Open for Entrance and Exit

When the event occurs, the selected entrance(s) and exit(s) will turn to the status of remaining open so that the vehicles can enter or exit the parking lot without authentication or the allowance of guards.

Event Receiving Schedule

The field defines a time period when the event or alarm can be triggered.

Receiving Schedule

The source is armed for detecting or triggering events or alarms during the receiving schedule. The platform provides two types of receiving schedules:

- **Schedule Template**: Select a receiving schedule template for the event or alarm to define when the event or alarm can be detected or triggered. For customizing a template, refer to ***Configure Receiving Schedule Template*** .
- **Event Based**: Specify a user-defined event or an alarm input as the start or end of the receiving schedule. You can set the **Stop Receiving** switch to on and set the specified time to automatically stop receiving this event or alarm even if the schedule does not end.

Note

For example, assume that you have set event A as the start event, event B as the end event, and set the value of **Automatically Stop Receiving After** to ***60 s***. Under these conditions, when event A occurs at T1, if event B occurs within 60 s, the receiving schedule ends at the occurrence of event B (see the following figure Receiving Schedule 1); if not, ends at 60 s after the occurrence of event A (see the following figure Receiving Schedule 2).

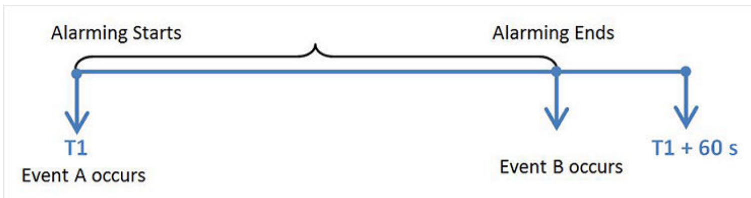


Figure 18-2 Event Receiving Schedule 1

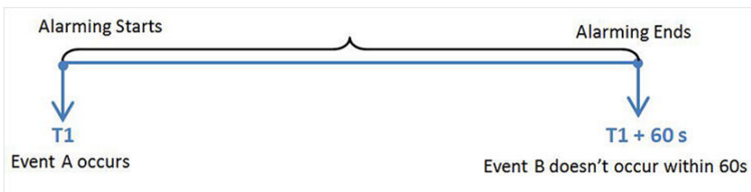


Figure 18-3 Event Receiving Schedule 2

When A occurs at time T1, the event or alarm will be armed from T1, if A occurs again at time T2 but B doesn't occur, the event or alarm will be armed from T2 again.

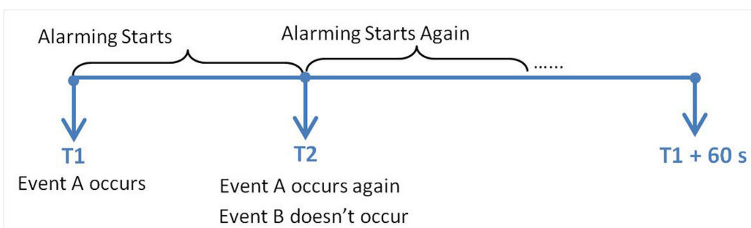


Figure 18-4 Event Receiving Schedule 3

Alarm Settings

Switch on **Trigger Alarm** to trigger the configured event as an alarm.

Alarm Priority

The field defines the importance or urgency of this alarm. Priority can be used for filtering alarms.

Recipients

The field defines users who can receive the alarm notification and check the alarm details when the alarm is triggered.

Select the recipient group(s) or user(s) to send the alarm information to and the recipient(s) can receive the alarm information when he/she logs in to HikCentral Professional via the Mobile Client.

Note

By default, users configured as the default recipients on the Alarm Receiving Configuration page will be automatically selected and cannot be deselected.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm-related cameras' live videos and playback when the alarm occurs.

Trigger Emergency

Select **Trigger Emergency** or **Turn Off Emergency**, and select the **Area for Triggering Emergency**. When the alarm is triggered by an emergency (such as a fire) in the selected area, the platform automatically switches to the **Trigger Emergency** mode or **Turn Off Emergency** mode.

Link Map

Select a map to show the alarm information and you should add the camera to the map as a hot spot (refer to ***Add Hot Spot***).

Display on Smart Wall

Display the alarm video or the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Wall Related to Graphic Card**: Display the alarm video on the wall which adopts the graphic card of the PC that runs the Control Client to decode the video.
- **Wall Related to Decoding Device**: Display the alarm video on the wall which adopts the decoding device (namely the wall that is linked to the decoding device) to decode the video.
- **Alarm's Related Cameras**: Display the video of the alarm-related cameras on the smart wall. You can select to display the video on which smart wall and which window and set the video's stream type.
- **Public View**: A view enables you to save the window division and the correspondence between cameras and windows as the Favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the platform will display the selected public view on the specified smart wall and users can view the video of the cameras predefined in the view.
- **Smart Wall No.**: Select the No. of the smart wall window to display the alarm video.
- **Stop Displaying Alarm**: Define when the platform will stop displaying the alarm on the smart wall. The platform can stop displaying the alarm within specified seconds, or replace the original alarm when another alarm with higher alarm priority is triggered.

Audible Alarm

Set the voice text for playing on the PC when the alarm is triggered.

Note

You should set the voice engine as the alarm sound on the System Settings page of the Control Client.

Restrict Alarm Handling Time

Enable this function to trigger the user-defined event(s) / alarm output(s) or automatically acknowledge the alarm if the alarm is not handled within the configured alarm handling time.

Note

Up to 16 user-defined events and alarm outputs can be triggered when handling alarm timed out.

Custom Alarm Receiving

Enable this function to set and view the customized alarm receiving schedule.

Other Operations

Click **Add** to add the event to the platform, or click **Add and Continue** to save the current settings and add another one. The added event will be listed on the Normal Event and Alarm page, and then you can perform the following operations if needed.

Table 18-1 Other Operations

Operation	Description
Edit Event	Click the event name to enter the details page and edit the settings.
Copy to Other Events	1. Click the event name to enter the details page. 2. Click **Copy To** in the top right corner of the page. 3. Select **Add a New Event/Alarm** to add a new event/alarm with the same settings, or **Copy Settings to Other Alarm** to copy the settings to the existing event/alarm. 4. Specify the settings of the source and select the target(s). 5. Click **OK** to copy the current event's specified parameter(s) to other added events for batch configuration.
Delete Events	Select events and click **Delete** to delete the selected ones.
Delete All Invalid Events	Click **Delete All Invalid Items** to batch delete all the invalid events.
Enable Events	Select an event and click **Enable → Enable** to enable the selected event, or click **Enable → Enable All** to enable all the added events.

Operation	Description
Disable Events	1. Select an event and click **Disable → Disable** , or click **Disable → Disable All** . 2. Set the time when the event(s) start being disabled and the duration of how long the event(s) will be disabled for. 3. (Optional) Enter the reason for disabling the event(s). 4. (Optional) Check **Disable Device Alarm** to change the alarm status of the device(s) displayed in the event list. 5. Click **OK** to disable the selected event(s) or all the events.
Test Events	Select the event(s) and click **Test** to manually trigger the event(s) for testing if the linkage actions work properly.

18.1.3 Add Combined Alarm

For some complicated scenarios, the alarm should be triggered when multiple events or alarms are detected or triggered. For example, the platform detects intrusion in area B, then the arming of area A starts. After that, if the platform detects intrusion in area A, then an alarm will be triggered to notify the security personnel.

Steps

1. In the top left corner of Home page, select ▦ **→ Security Monitoring → Event and Alarm** .
2. Select **Event and Alarm Configuration → Combined Alarm** on the left.
3. Click **Add Combined Alarm** to open the Add Combined Alarm pane.

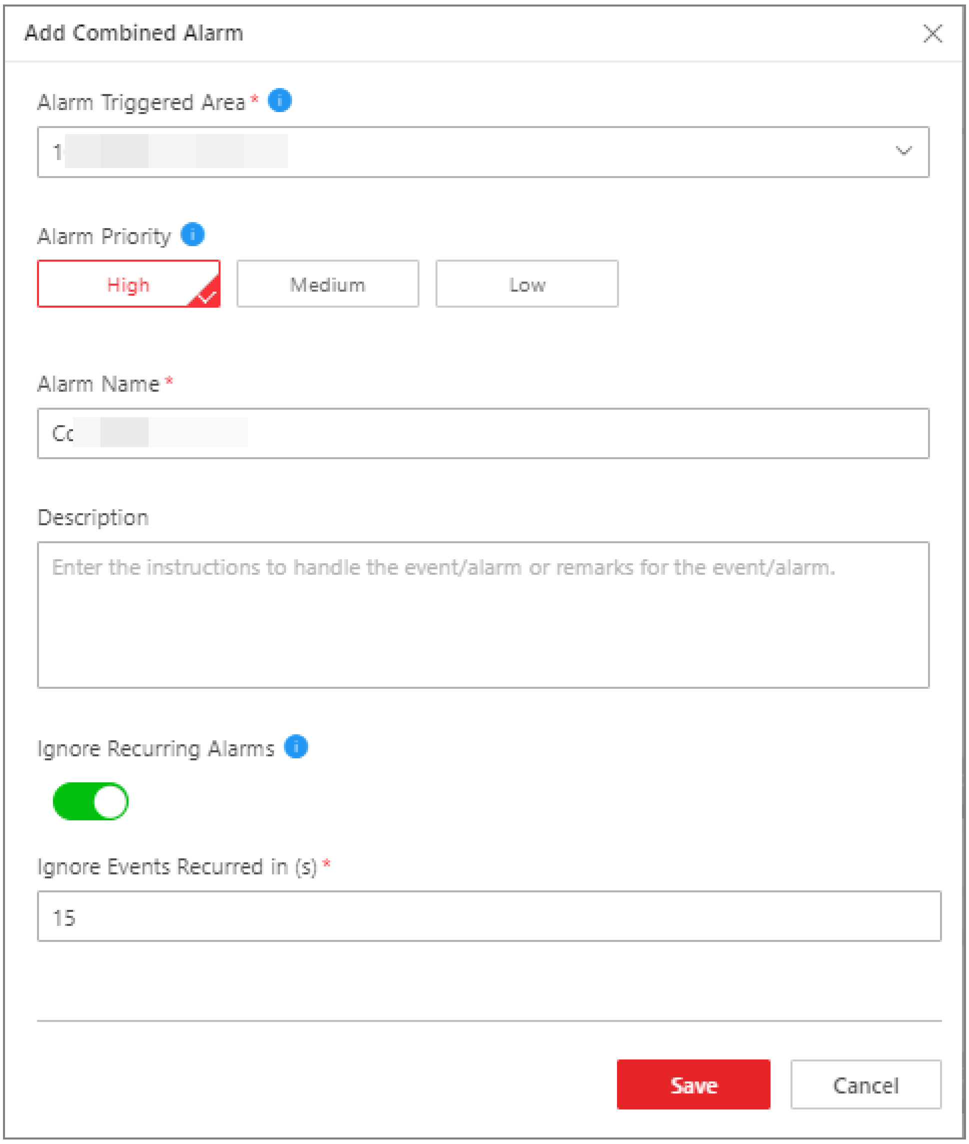


Figure 18-5 Add Combined Alarm

4. Set parameters on the page.

Alarm Triggered Area

Select the area where the combined alarm will be triggered.

Alarm Priority

The priority including low, medium, high, and custom level, which indicates the urgent degree of the combined alarm.

Alarm Name

Create a name for the combined alarm.

Description

Describe the combined alarm according to your requirements.

Ignore Repetitive Events/Alarms

Once it is enabled, the platform will ignore the combined alarm recurred within the configured time period.

5. Click **Save** to enter the configuration page.
6. Configure a receiving schedule for the combined alarm.
   1) Click on the configuration page to open the Select Schedule Template pane.
   2) Select a schedule template as **All-Day Template**, **Weekday Template**, **Weekend Template**, or a custom template.

   Note

   For how to customize a schedule template, refer to ***Configure Receiving Schedule Template*** .

   3) Click **Save**.

   A Receiving Schedule card will appear on the page.

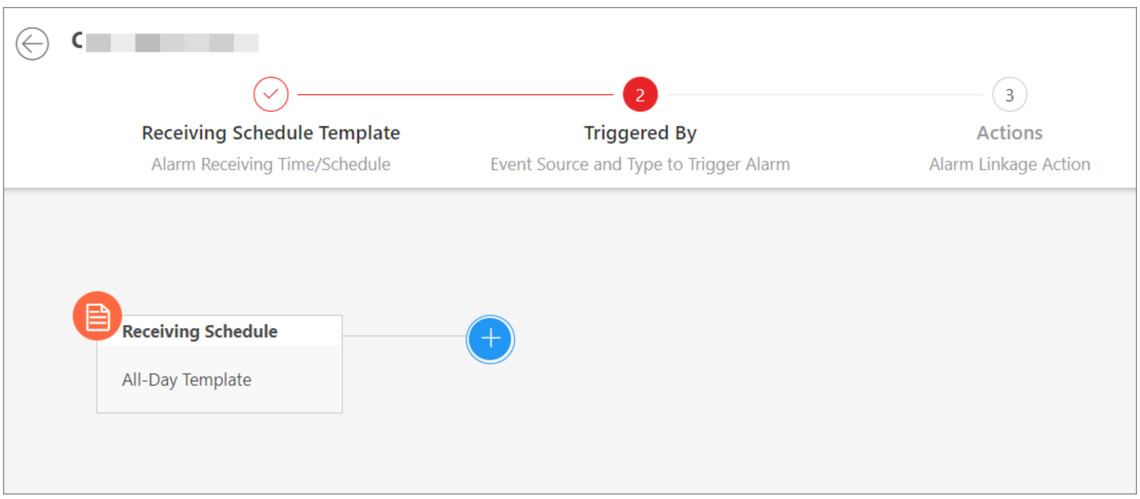


Figure 18-6 Receiving Schedule Card

7. Configure conditions for triggering the combined alarm.
   1) Click at the right of the Receiving Schedule card to open the Select Alarm Triggering Logic pane.
   2) Select a triggering logic and click **Save**.

   The condition card will appear.

   3) Click on the condition card to open the Select Event Source and Event Type pane.
   4) Select a triggering event and a source, and click **Save**.

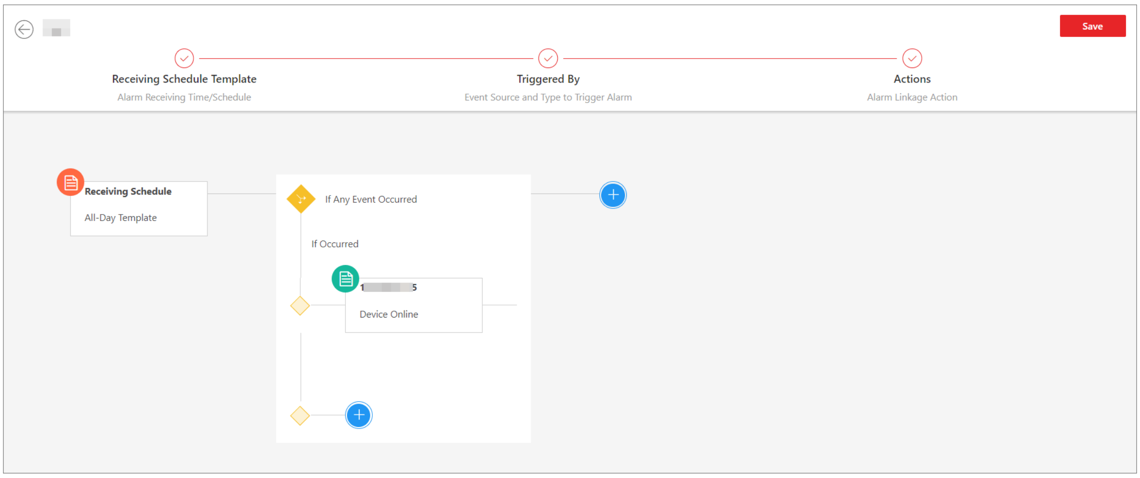


Figure 18-7 Condition Card

5) **Optional:** Click below the newly added event source and type card to select more event sources and types.
6) **Optional:** Click on the event source and type card to enter the remote configuration page of the event source. For details about remote configuration, refer to the user manual of the corresponding device.

8. Configure the alarm recipient(s) and linkage action(s) for the combined alarm.
1) Click at the right of the triggering logic card to open the Select Alarm Linkage Action panel.
2) Click **Alarm Recipients** and select the recipient(s).

Note

If **Automatically Receive Alarm** is enabled for some users (refer to ***Add Normal User*** for details), the Alarm Recipients card will be automatically generated after the event source and type is configured, and these users will be selected as recipients. You can click the generated card to edit the alarm recipients, but the selected users cannot be unselected.

3) Click **Save**.
4) Click below the Alarm Recipients card to select a linkage action and set the corresponding parameters. For details, refer to ***Add Normal Event and Alarm*** .

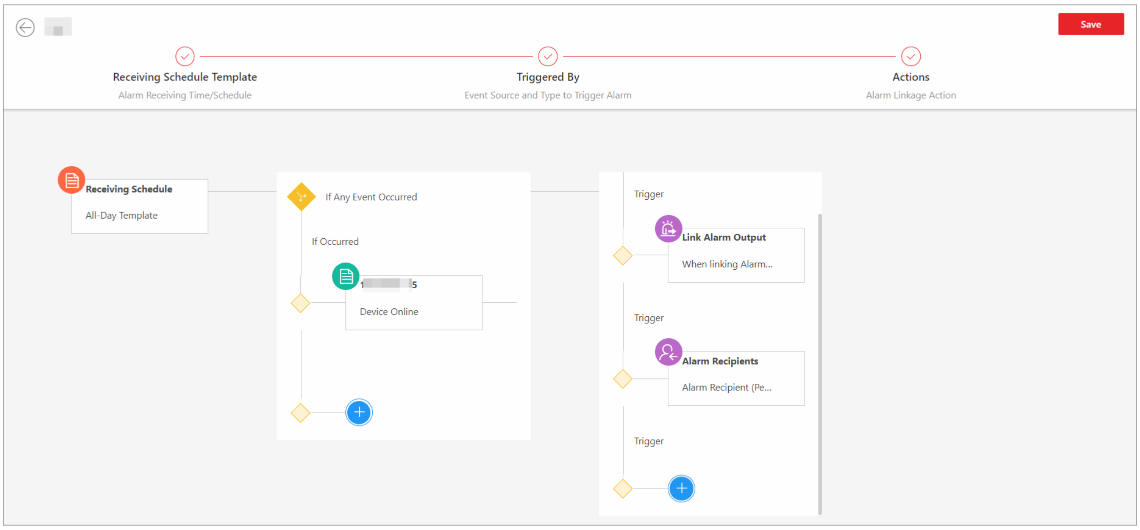


Figure 18-8 Action Card

5) **Optional:** Click ⊕ below the Alarm Recipients card to add more linkage actions.

9. **Optional:** Click the icon on the top left of each card to reselect the content.
10. **Optional:** Move the cursor on each card and click 🗑 appeared on the top right of the card to delete the card.

Note

If the card is deleted, the following cards or sub cards (if any) will also be deleted.

11. Click **Save** in the top right corner of the combined alarm configuration page to add the combined alarm to the platform.

Note

If the alarm recipients are not configured for this combined alarm, you cannot save the combined alarm.

12. **Optional:** Perform the following operations according to your requirements.

Add to Map	Click **Add to Map** to add this alarm to the map. After that, the alarm will be marked on the map when the alarm is triggered.
Copy Parameters to Existing Alarm	Click **Copy**, and then select the items (such as basic information, actions, receiving schedule, receiving mode), and select the target alarm to copy to.
Delete Alarm	Click **Delete** to delete this alarm.
Test	Click **Test** to trigger this alarm manually, and you can check whether the linkage actions take effect and whether the recipients can receive the notification.
Enable/Disable	Switch on the button beside **Status** to enable or disable this alarm. After the alarm is enabled, it can be received by the platform. If you

disable this alarm, you will be required to set the start time and duration of disabling and the platform cannot receive the alarm in the duration.

18.1.4 Add Generic Event

A generic event is a signal transferred in the form of TCP/UDP/HTTP/HTTPS data package from the resource (e.g., external systems and devices) if something occurred and matched the configured expression. In this way, you can easily integrate the platform with a very wide range of external sources, such as access control systems and alarm systems.

Steps

1. In the top left corner of Home page, select → **Security Monitoring → Event and Alarm** .
2. Select **Custom Event → Generic Event** on the left.
3. Click **Add** to enter the Add Generic Event page.

Note

You can also click **Import** to batch import the events by the template.

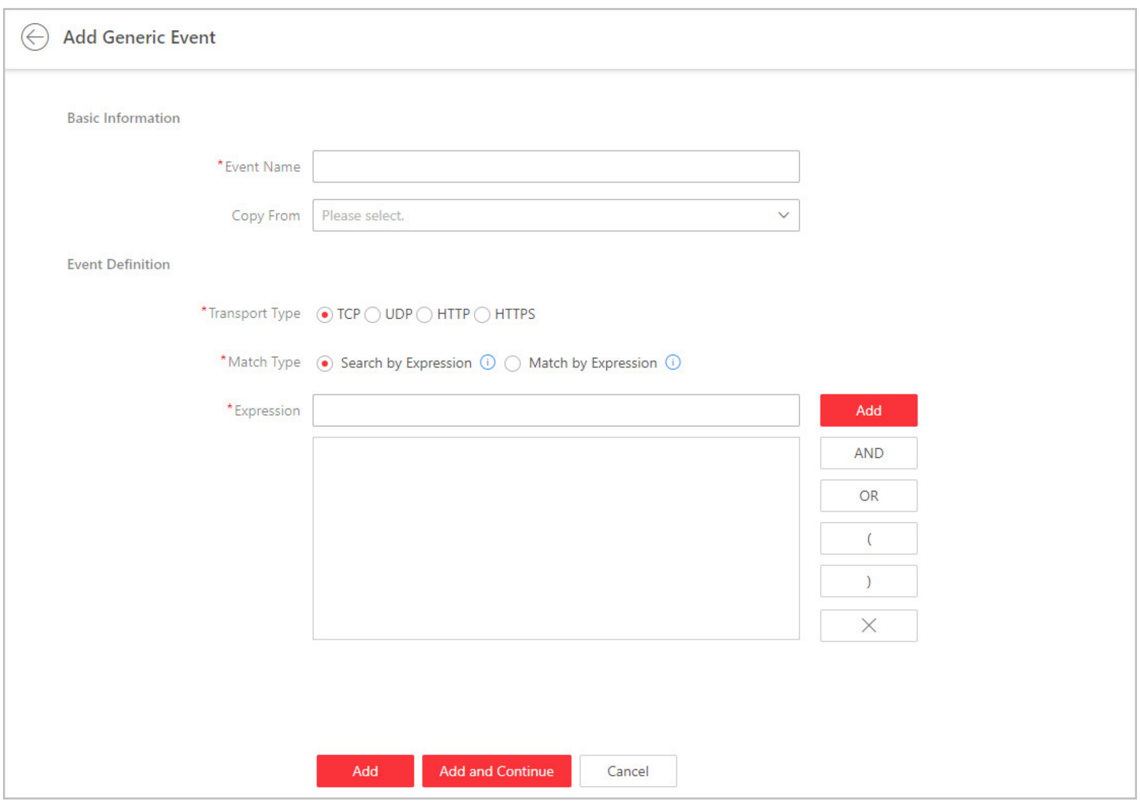


Figure 18-9 Add Generic Event Page

4. Set a name for the event.

5. **Optional:** Copy the settings from other generic events in the **Copy from** field.
6. Select **TCP**, **UDP**, **HTTP**, or **HTTPS** as the transport protocol.
7. Select the match type to define what received data packages can trigger events.

Search by Expression

The received package must contain the text defined by the expression or more. For example, if you have defined the expression as 'Motion' AND 'Line Crossing', the event can be detected when the received package contains "Motion", "Intrusion", and "Line Crossing".

Match by Expression

The text in the received package must be exactly the same as that defined by the expression.

Search by Keyword

The received package must contain the keywords.

8. Define the expression for analyzing the received package.
   1) Enter the term which should be contained in the expression in the text field.
   2) Click **Add** to add the term to the expression.
   3) Click the parenthesis or operator button to add it to the expression.
   4) **Optional:** Click × to remove the item at the left of the cursor from the expression.

Note

You can position the cursor inside the expression in order to determine where a new item should be included or where an item should be removed.

The parenthesis or operator buttons are described in the following:

AND

You specify that the terms on both sides of the AND operator must be included.

For example, if you define the rule as 'Motion' AND 'Line Crossing' AND 'Intrusion', the term Motion, and Line Crossing as well as the term Intrusion must be all contained in the received package for the conditions to be met.

Note

In generally, the more terms you combine with AND, the fewer events will be detected.

OR

You specify that any term should be contained.

For example, if you define the rule as 'Motion' OR 'Line Crossing' OR 'Intrusion', any of the terms (Motion, Line Crossing, or Intrusion) must be contained in the received package for the conditions to be met.

Note

In generally, the more terms you combine with OR, the more events will be detected.

(

Add the left parenthesis to the rule. Parentheses can be used to ensure that related terms are processed together as a unit; in other words, they can be used to force a certain processing order in the analysis.

For example, if you define the rule as ('Motion' OR 'Line Crossing') AND 'Intrusion', the two terms inside the parentheses will be processed first, then the result will be combined with the last part of the rule. In other words, the system will first search any packages containing either of the terms Motion or Line Crossing, then it searches the results to look for the packages that contain the term Intrusion.

)

Add the right parenthesis to the rule.

9. Click **Add** to add the event and back to the event list page, or click **Add and Continue** to add the event and continue to add a new event.
10. **Optional:** Perform the following operations after adding the event.

Edit Event Settings	Click the name in the Event Name column to edit the corresponding event settings.
Receive Generic Event	Select the events, click **Receive Generic Event** to open the settings pane, and check the checkboxes to enable receiving the generic events via different protocols.
Import/Export Events	Select the events, and click **Import**/**Export**.

18.1.5 Add User-Defined Event

When you are viewing videos or checking the alarm information, if there is some information that needs to be paid attention to, you can manually define a new event type which is not in the provided event and alarm list or the defined generic events for triggering an alarm or being configured as a linkage action of alarms. This kind of event is called as the user-defined event.

Steps

1. In the top left corner of Home page, select → **Security Monitoring → Event and Alarm** .
2. Select **Custom Event → User-Defined Event** on the left.
3. Click **Add**.

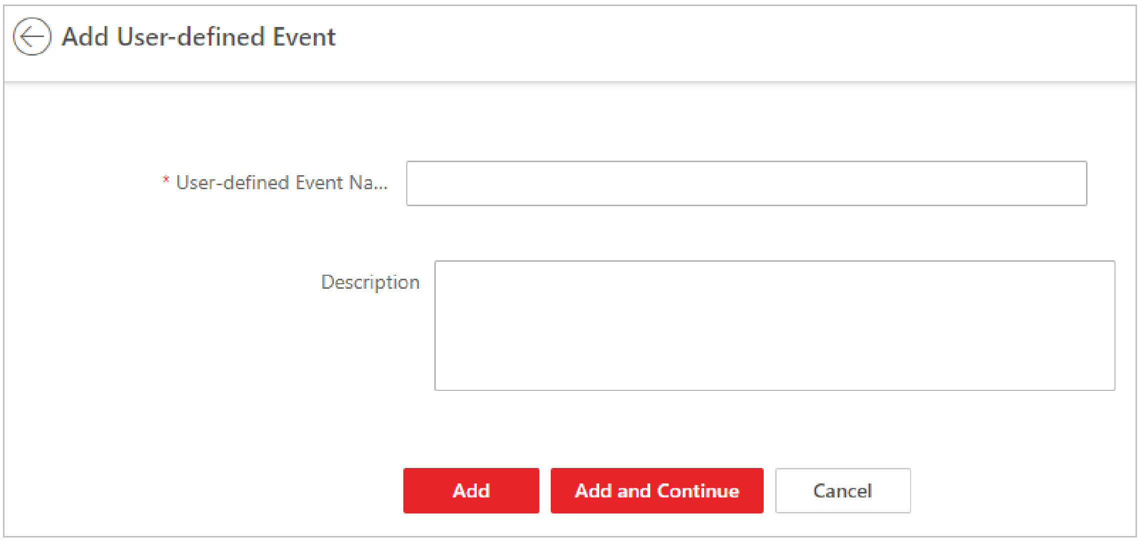


Figure 18-10 Add User-Defined Event

4. Create a name for the event.
5. **Optional:** Enter the information to describe the event.
6. Click **Add** to add the event and go back to the event list page, or click **Add and Continue** to add the event and continue to add a new one.

   With the customized user-defined event, the platform provides the following functions:

   - Integrate other third-party systems with HikCentral Professional by using the data received from the third-party system. The user-defined events can be triggered as an alarm outside the HikCentral Professional. For details, contact our technical support.

18.2 Set Basic Event and Alarm Parameters

After setting basic parameters for events and alarms, you can set receiving schedules, and recipient groups or specific recipients who can receive events and alarms in specific timeout period, and you can send events/alarms reports regularly via email to the recipients / recipient groups. You can also define alarm priorities, alarm categories, and alarm icons to meet the actual requirements.

18.2.1 Configure Receiving Schedule Template

When adding events and alarms, you can select the predefined receiving schedule template to define when the event and alarm can be triggered and notifying the recipients. The platform has predefined three default receiving schedule templates: All-Day Template, Weekday Template, and Weekend Template. You can also customize a template according to actual needs.

Steps

Note

Receiving schedule template defines the time when you can receive events or alarms. If the event schedule differs from the alarm receiving schedule, make sure the time of the event receiving schedule covers that of the alarm receiving schedule.

1. In the top left corner of Home page, select → **Security Monitoring → Event and Alarm** .
2. Select **Basic Configuration → Receiving Schedule Template** on the left.
3. Click + to enter the Add Receiving Schedule Template page.

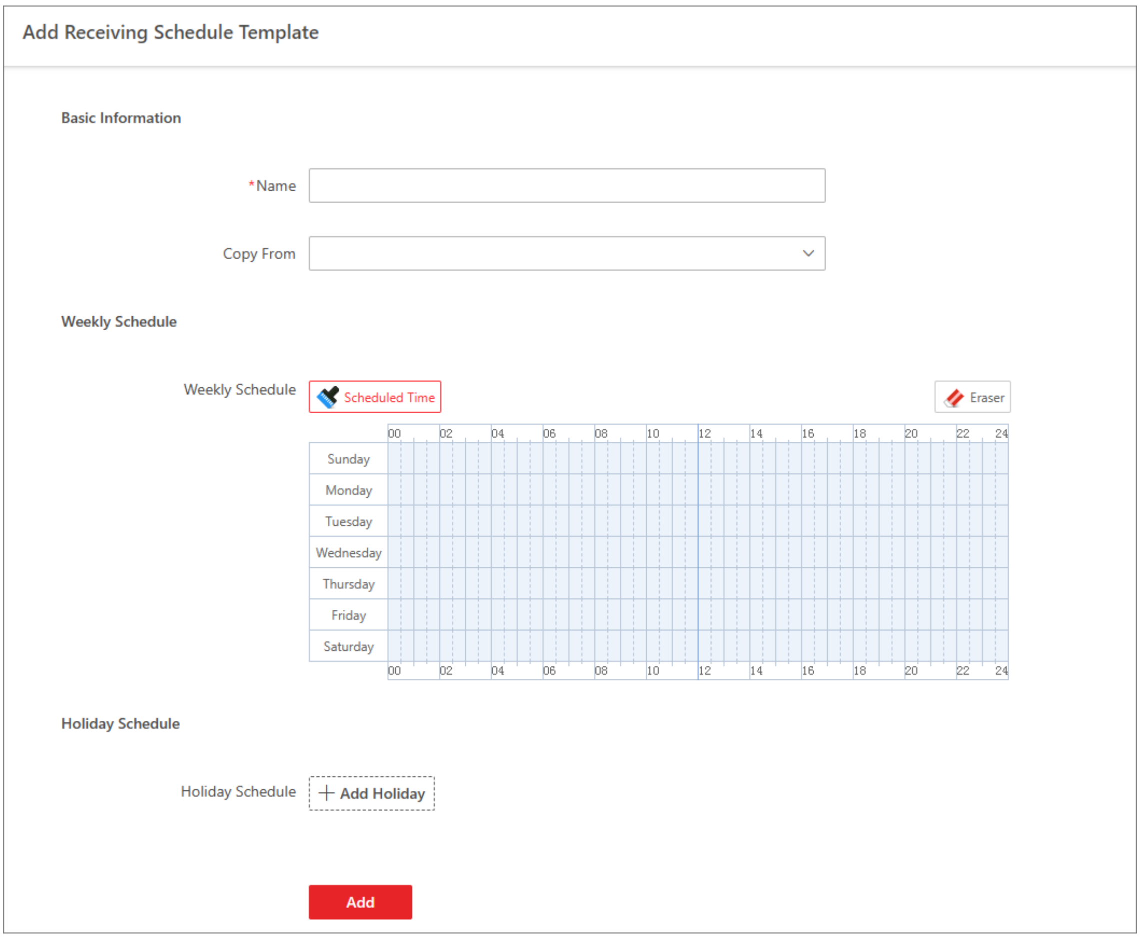


Figure 18-11 Add Receiving Schedule Template

4. Enter a name for the template.
5. **Optional:** Select another defined template to copy the settings to the current template.
6. Click **Scheduled Time** and drag on the time bar to set time periods during which the event can be triggered on the event source and notified the recipients.

Note

- Up to 4 time periods can be set for each day.
- On the schedule time table, you can click to set the specific time period which accurate to minute.

7. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
8. **Optional:** Set a holiday schedule if you want different schedules for specific days.
   1) Click **Add Holiday**.
   2) Select existing holiday templates, or click **Add** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Set the schedule for holidays.
9. Click **Add** to add the template.

   The receiving schedule template will be displayed on the receiving schedule template list.
10. **Optional:** Perform the following operations after adding the receiving schedule template.

View Template Details	Click the template name to view its details.
Edit Template	Click the name of a custom template to edit template details. **Note** The predefined templates cannot be edited.
Delete Template	Select a template and click 🗑 to delete the template. **Note** • The predefined templates cannot be edited. • If there are events/alarms configured with this template, you can replace the template with other receiving schedule. Or you can click **Delete Now** to delete the template, and this operation will cause exceptions of related events/alarms.

18.2.2 Custom Alarm Settings

The platform has predefined several alarm priorities, alarm categories, color template, and alarm icons for basic needs. You can edit the predefined alarm priority and alarm category, and customize alarm priority and alarm category according to actual needs.

Steps

Note

Alarm Priority

Define the importance or urgency of alarms for handling or acknowledgment.

Alarm Category

Used when the user acknowledges the alarm and categories what kind of alarm it is, e,g., false alarm, or alarm to be verified. You can search for alarms by the alarm category.

Alarm Icon When Alarm Occurs

The platform has predefined some icons of resources for several special alarms.

For example, it predefined the icon for the Door Opened Abnormally alarm. When this alarm is triggered, the door icon will turn to the icon displayed here to notify users.

1. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** .
2. Select **Basic Configuration** → **Alarm Custom Settings** on the left.
3. Customize alarm priorities according to actual needs. By default, three kinds of alarm priority exist.

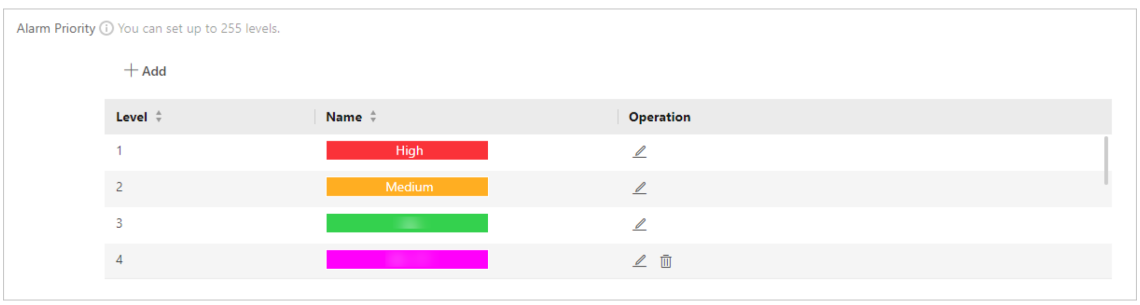


Figure 18-12 Alarm Priority

1) Click **Add** to open the adding alarm priority pane.

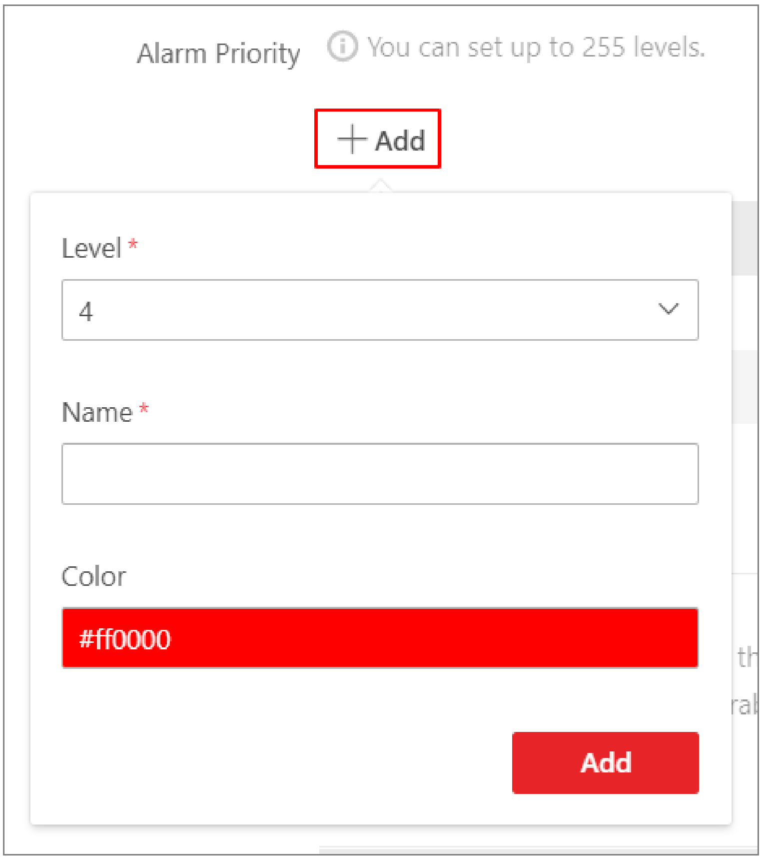


Figure 18-13 Add Alarm Priority

2) Select a level No. for the priority.
3) Enter a descriptive name for the priority.
4) Select the color for the priority.
5) Click **Add**.

The priority will be displayed on the alarm priority list.

4. Customize alarm categories according to actual needs. By default, four alarm categories exist.

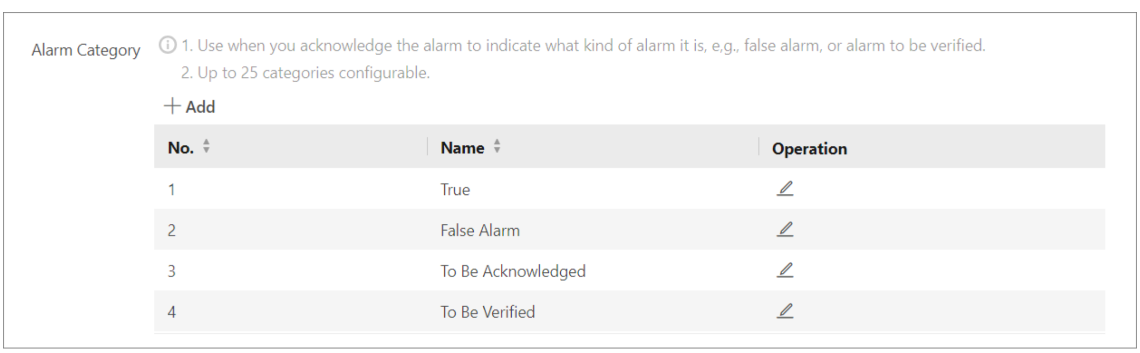


Figure 18-14 Alarm Category

1) Click **Add** to open the adding alarm category pane.

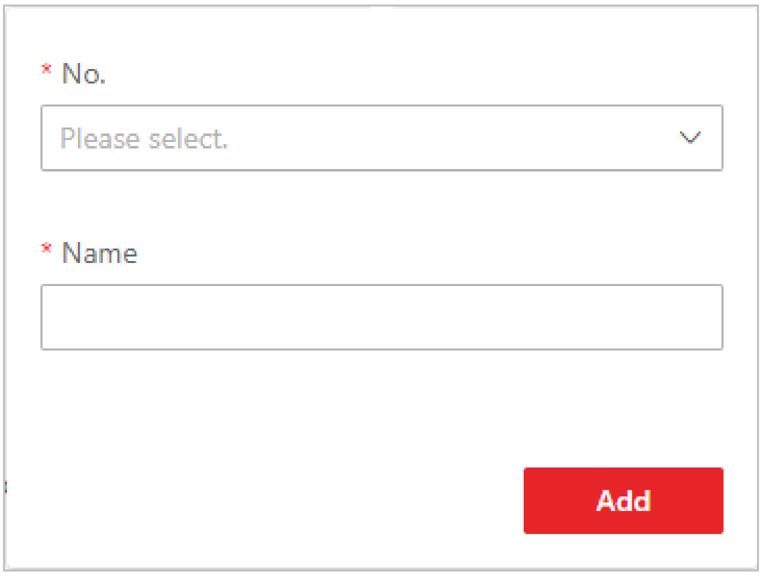


Figure 18-15 Add Alarm Category

2) Select a No. for the alarm category.
3) Enter a descriptive name for the alarm category.
4) Click **Add**.

The alarm category will be displayed on the alarm category list.

5. Customize color template according to actual needs. By default, three alarm categories exist.

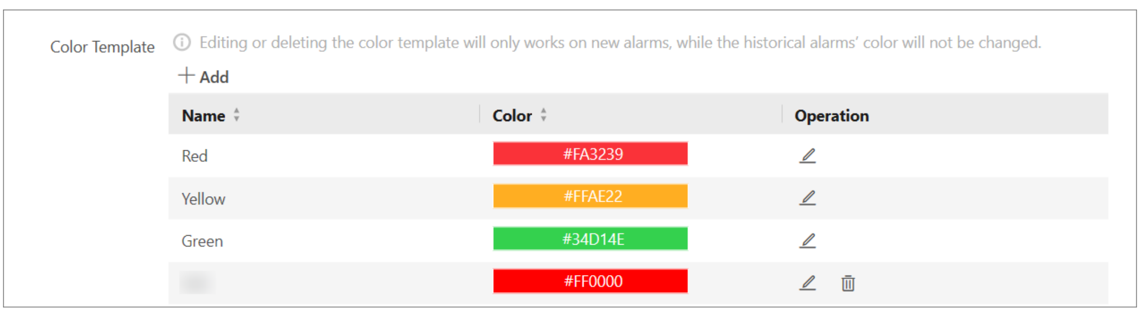


Figure 18-16 Color Template

1) Click **Add** to open the adding color template pane.

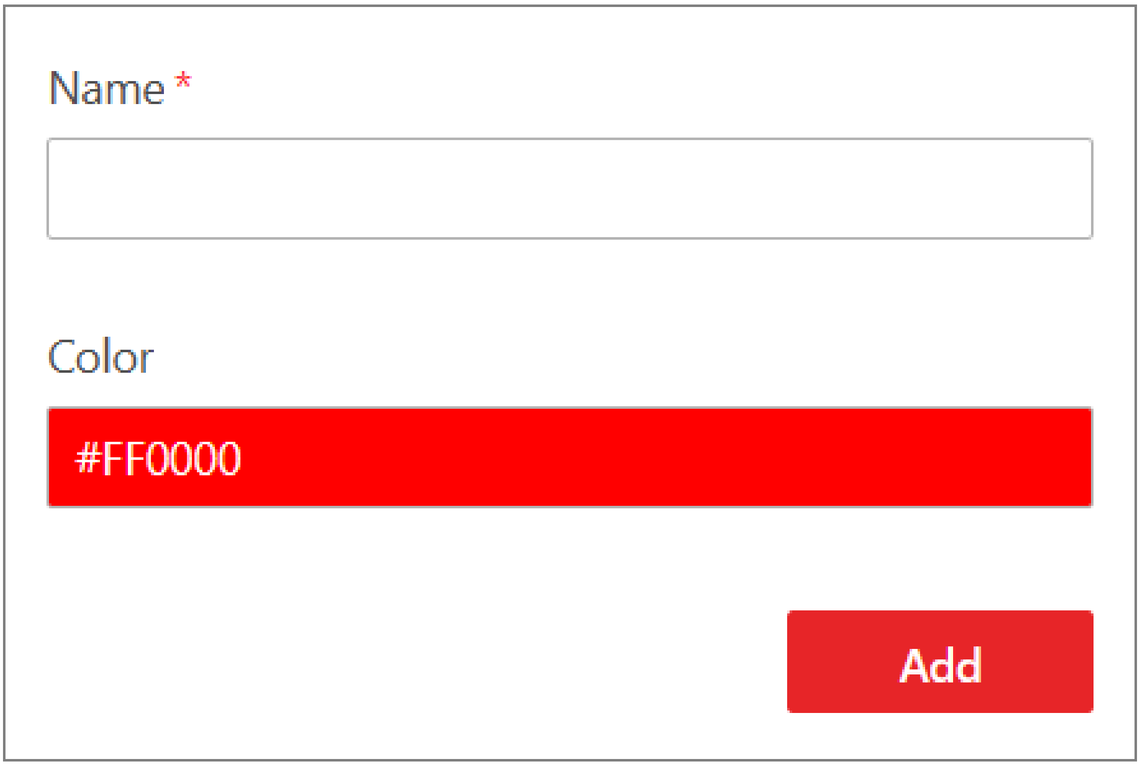


Figure 18-17 Add Color Template

2) Enter the name of the color template.
3) Select a color.
4) Click **Add**

The alarm category will be displayed on the alarm category list.

6. In the Alarm Icon When Alarm Occurs field, view the alarm icons provided by the platform which are used to notify the users that the alarm is triggered.

Note

These predefined alarm icons cannot be edited and deleted.

7. **Optional:** Perform the following operation(s) after adding alarm priority and category.

Edit Click to edit the alarm priority and category.

Note

You cannot edit the No. of predefined alarm priorities and categories.

Delete Click to delete the alarm priority and category.

Note

You cannot delete the predefined alarm priorities and categories.

18.2.3 Configure Alarm Receiving Settings

You can manage alarm recipients in groups to quickly set recipients for different categories of alarms, and set default alarm recipients who can receive all the alarms triggered by resources they have access permissions, so that you do not have to select recipients for each single alarm. You can also set the timeout period of acknowledging alarms for filtering alarms on the Control Client and upload historical alarms to the Control Client.

Steps

1. In the top left corner of the Client, select → **Security Monitoring → Event and Alarm** .
2. Select **Basic Configuration → Alarm Receiving Configuration** on the left.
3. In the Alarm Recipient Group field, click + above the group list to open the adding alarm recipient group pane.
4. Enter a name for the group and click **Add**.

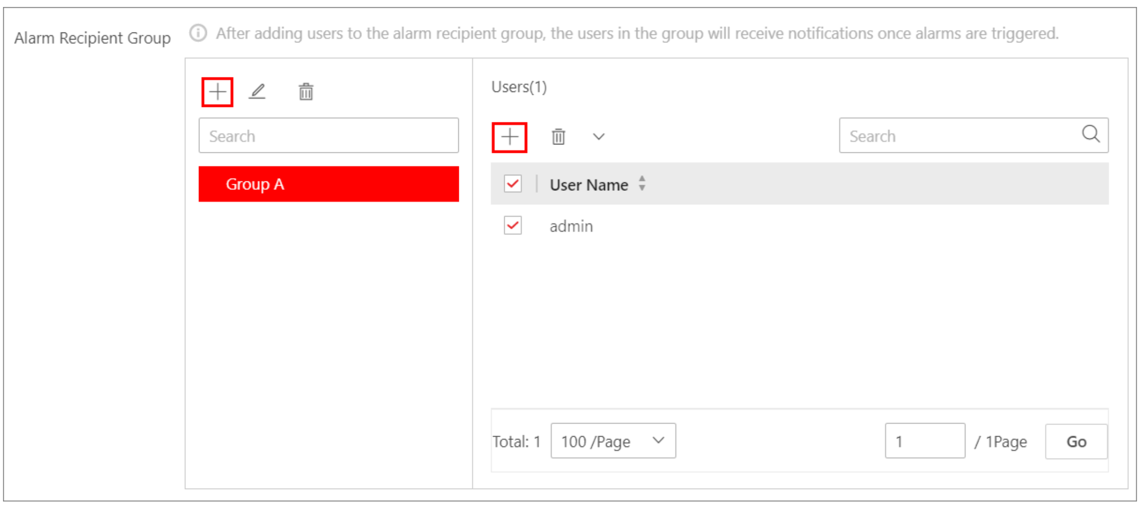


Figure 18-18 Alarm Recipient Group Field

5. Select an alarm recipient group and click + in the Users field to add user(s) to the group.
6. **Optional:** Check user(s) in the group and click to remove the selected user(s) from the group or click → **Delete All** to remove all the users from the group.
7. Check user(s) in the Recipient field as the default alarm recipient(s).

   The default alarm recipients will be automatically selected when setting recipients for alarms, and they cannot be deselected.
8. **Optional:** Switch on **Acknowledging Time Limitation** and set the timeout period for enable filtering timeout alarms on the Control Client.

   Note

   You can click **Custom** on the drop-down list to custom time out period.
9. **Optional:** Check **Upload Historical Alarm** to enable uploading the historical alarms to the Control Client.

10. Click **Save**.

    The configured alarm recipient group(s) will appear on the Add Event and Alarm page and they can be selected when setting recipients for alarms.

18.2.4 Send Event and Alarm Report Regularly

You can set a scheduled report rule for specified events or alarms, and the platform can send an email with a report attached to the target recipients by day or week, showing the details of specified events or alarms triggered on the day or the week.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Email Settings*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

One report can contain up to 10,000 event records in total.

1. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** .
2. Select **Basic Configuration** → **Scheduled Report** on the left.
3. Click **Add** if there is no scheduled report rule or click + above the rule list to enter the Create Report page.
4. Set the basic information.

   Report Name

   Create a name for the report.

   Format

   Select **Excel** or **PDF** as the report format and select a language for report contents.

   Note

   You can skip this step if you want to keep the default settings.

   Report Language

   Select the report language.
5. In the Report Content field, select **Event Alarm Rule** or **Area** as the statistics dimension, and click **Add** to select statistical objects to be contained in the report.

   Note

   Up to 32 events and alarms can be added in one report.
6. Set the report sending rule and time.

Statistical Cycle

By Day

If the statistics cycle is selected as **By Day**, the report shows data on a daily basis. The platform will send a report at the sending time on the selected day(s) of the week, which contains information of the events triggered on the day (24 hours) before the sending date.

For example, if you select **Monday**, **Tuesday**, and **Friday** in the Send On failed, and set the sending time as 18:00, the platform will send a report at 18:00 on every Monday, Tuesday, and Friday, containing details of all the events triggered between 00:00 and 24:00 on every Sunday, Monday, and Thursday.

By Week

If the statistics cycle is selected as **By Week**, the report shows data on a weekly basis, which may be less time-consuming. The platform will send a report at the sending time on the selected day of the week, which contains information of events and alarms triggered on the recent 7 days or recent 14 days before the sending date.

For example, if you set the sending time as 6:00 on Monday, the platform will send a report at 6:00 in the morning on every Monday, containing details of all the events triggered between last Monday and Sunday.

Report Time

Select the specific report time.

Send On

Select the date of a week for sending the report. You can click **Select All** to set all dates of a week.

Send At

Select the time of a day for sending the report.

Effective Period

Set an effective period for the report to improve the data security.

7. Set advanced parameters.

Send via Email

If it is enabled, you can select an email template from the drop-down list to define the recipient information and email format.

Note

You can click **Add New** to add a new email template. For setting the email template, refer to *Email Settings* .

Upload to SETP

If it is enabled, the platform will automatically upload and save reports to the FTP server.

Save to Local Storage

If it is enabled, the platform will automatically upload and save reports to the local storage.

Save to File Management

If it is enabled, the platform will automatically upload and save reports to the Evidence Management Center. You can set the file tag and file description for the scheduled reports. For details, refer to ***Evidence Management*** .

Note

You can click **Configure** or click ⚙ ⌵ → **SFTP Settings / Configure Local Storage** to log in to the SFTP server by entering the IP address, port, user name, and password, and set the saving path on the SFTP server or local storage for reports.

8. Click **Save** to add the report rule.

18.3 Event and Alarm Search

The platform provides the statistics and analysis results of historical events and alarms for you to have an overview and further applications. You can also search for historical events and alarms by setting different conditions to view the details as required.

18.3.1 Event and Alarm Overview

In the event and alarm overview module, it gives you an overview of the event or alarm distribution, top 5 event types or alarm categories, and top 5 event or alarm areas.

In the top left corner of the Home page, select ⊞ → **Security Monitoring → Event and Alarm** .

Select **Search → Overview** on the left.

Figure 18-19 Event and Alarm Analysis

Module	Description
1	• Daily Trend: The numbers of events or alarms in the last 7 days or last 30 days are displayed in the vertical bar chart. • Hourly Trend: The numbers of events or alarms of 24 hours for the last 7 days, the last 30 days, or the custom period are displayed in the line chart.
2	The data of top 5 event types or alarm categories triggered in the current day, last 7 days or last 30 days are displayed in the horizontal bar chart. You can click the red number of an item to jump to the Event and Alarm Search page.
3	The data of the top 5 event or alarm areas in the current day, last 7 days or last 30 days are displayed in the horizontal bar chart.

You can click **Settings** in the upper-right corner to customize event types or alarm categories to be calculated on the overview page.

Note

The information displayed in each area will change according to the report target on the Settings pane. For example, if you select **Alarm** on the Settings pane as the report target, the upper area will only display the number of alarms, the lower-left area will only display the data of top 5 alarm categories, and the lower-right area will only display the data of top 5 alarm areas.

18.3.2 Search for Event and Alarm Logs

You can search for event and alarm log files of the added resource by setting different conditions.

Before You Start

Make sure you have configured events and alarms first. See ***Add Normal Event and Alarm*** for details.

Steps

1. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** → **Search** → **Event and Alarm Search** .
2. Set the time range for search.
   - Select a predefined time period for search.
   - Select **Custom** and specify the start time and end time for search.
3. In the field of **Trigger Alarm**, select the event status (whether the event is triggered as the alarm).

   All

   Both events and alarms.

   Disabled

   The events happened but were not triggered as alarms.

   Enabled

   The events happened and were triggered as alarms. If you select this, you can set conditions for filtering alarms by marking status, acknowledging status, alarm priority, or alarm category.
4. Switch **Area** on and then click to select the area of the event or alarm source.
5. Switch **Triggering Condition** on and then click to select the triggering events and source from the current site or remote sites.

Note

- The remote site is only available for the Central System with Remote Site Management module (based on the License you purchased).
- If you select triggering events in the Access Control category, enter the entered/exited person's name.
- If you select triggering events in the Third-Party Resource Integration category and have entered the additional information about the alarm on the third-party system, enter the additional information.

6. Switch **Event/Alarm Name** on to select the event/alarm name in the drop-down list.
7. Click **Search**.

   The matched event or alarm logs will be listed on the right page.
8. **Optional:** Click **Export** and select the format as **Excel** or **PDF** to save all searched events and alarms to the local PC.

Note

When exporting all events and alarms in Excel format, you can check **Include Picture Information** to export the related pictures.

18.3.3 View Device Application Events

You can view and search for event and alarm log files uploaded by the added resources which contain HEOP or AIOP application.

Note

Make sure you have configured HEOP or AIOP events and alarms first. See ***Add Normal Event and Alarm*** for details.

In the top left corner of the Client, select → **Security Monitoring → Event and Alarm** .

Select **Custom Event → Device Application Event** on the left.

You can view the event list including event name, original event name, event type, and description. You can also enter the keywords to search for specific device application events.

You can click the event name to view the event details and edit the event name.

Note

Only the name of AIOP events are supported to be edited.

Chapter 19 Evidence Management

In the Evidence Management module, you can manage case and the files (including pictures, videos, audios and other files), which contain important information about incidents such as traffic accidents and violent crimes for settling disputes or legal cases.

In the top left corner of the platform, select → **Security Monitoring → Evidence Management** .

19.1 Basic Settings

You can set the storage location for case and set custom items to define the file type, case tag, and additional content for file management and case management.

19.1.1 Set Basic Parameters

Before managing the files and cases, you should add case types, file tags, and additional contents to the platform for further filtering and searching.

Steps

1. On the left pane, select **Basic Configuration → Basic Parameter** .
2. Set the following parameters.

   Case Type

   The type of accident or suspect incident recorded in the case, such as theft, robbery, attack, and missing person, which is used for adding cases.

   Default case types are provided, and you can click **Add** to add more.

   File Tag

   The tag of file describing the file format, related case, etc, which is used for uploading files.

   Click **Add** and enter the file tag name to add a file tag.

   Case Additional Content

   The text such as the result/conclusion of incidents based on the evidence collected from the on-site organization, such as arrested, warned, and injured, which is used for adding cases.

   a. Click **Add**, and enter the additional content name.
   b. Select the type. If you select **Single Selection**, you need enter the options. If you select **General Text**, you can click **Add** to finish adding.
3. Click **Save**.

19.1.2 Set Storage Parameters

You can set the storage location for files and cases.

Steps

1. On the left pane, select **Basic Configuration → Storage Configuration** .
2. Set the storage location and configure related parameters.

   Local Storage

   Set the required fields including address, port, user name, and password.

   SFTP

   Select the local resource pool.
3. Click **Save**.

19.2 Manage Files

The files refer to the videos, pictures, and documents about incidents such as traffic accidents and violent crimes in case of the need for settling disputes or legal cases. You can upload files from the local PC, set schedules for getting files from devices, and share added files. You can also link the added files with the specific cases.

Note

- The permission (such as viewing, editing, exporting, and sharing) of specified files (files linked to cases or files uploaded by portable devices) varies according to the user roles. On the User Permission page of an uploaded file displays the permission details.
- If the file is a portable device file uploaded by a police officer, then the officer is the default file owner.
- The file owner has all permissions. Upper-level users of the file owner have the same file permissions as the file owner. Users with super access permission can view all files. Persons in the same department of the file owner can also view the files.

19.2.1 Upload a Local File

You can upload files from your local PC to the Evidence Management Center. For the uploaded files, you can perform more operations such as viewing the added files by file type and file tag, and filtering and exporting the files.

Steps

1. Select **File Management** on the left.

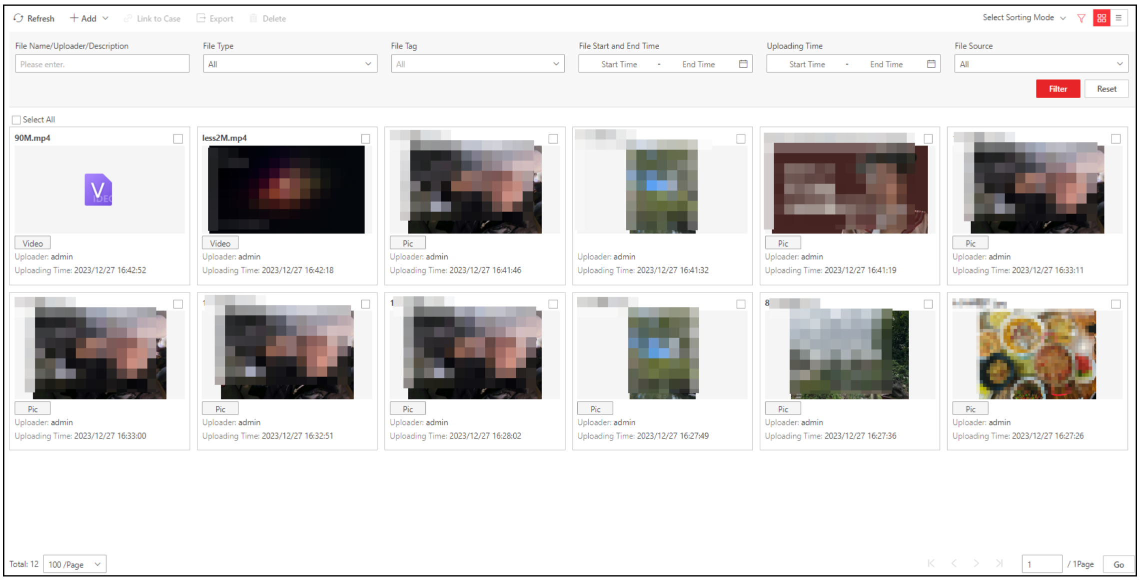


Figure 19-1 File Management Page

2. Click **Add** → **Upload Local File** to open the Upload Local File pane.
3. **Optional:** Select one or multiple file tags.
4. **Optional:** Set the geographic location when file was created according to the instructions on the interface.
5. Click **Upload** and select the pictures, videos, audios, or other files from the local PC to add.
6. Click **Save**.

19.2.2 Upload Files from Device

You can set a schedule to upload files from on-board cameras, portable devices, etc. to the Evidence Management Center. For the added files, you can perform more operations such as viewing the added files by file type and file tag, filtering and exporting the files.

Before You Start

Make sure you have added device(s) to the platform.

Steps

1. Select **File Management** on the left.
2. Click **Add** → **Upload from Device** .
3. **Optional:** Select one or multiple file tags, and enter the file description.
4. Select the uploading mode and set related parameters.

   Upload at Specified Time

   Specify the start time and end time of file uploading and recording.

   Upload When Wi-Fi Connected

The files will be automatically uploaded once the Wi-Fi is detected and connected, so you are only required to specify the start/end recording time of cameras.

Note

Make sure you have added devices such as on-board devices and portable devices which support connecting to Wi-Fi.

5. Select one or multiple cameras in the Linked Camera list.
6. Click **Save**.

19.2.3 Save Files in Other Modules

Files generated from other modules can be saved in the Evidence Management Center, including Portable Enforcement and Event and Alarm module. When saving the videos/audios/pictures/ documents in other modules to the Evidence Management Center, you can specify the adding mode and file tag of the files for further management.

19.2.4 View and Edit Files

After adding files to the Evidence Management Center, you can view the details of files and edit the information. For example, you can play the video files, add masks and texts, clip videos, enable the silent mode for linking video files with corresponding cases afterward.

Select **File Management** on the left.

Manage Added Files

Operation	Description
Filter the Files	Click in the upper right corner to unfold the filter pane, set conditions such as file type and file tag, and then click **Filter** to filter the target file.
Refresh the Files	Click **Refresh** to refresh the file list.
Link the Files to Case	Select files to link to cases.
Export the Files	Select the files and click **Export** to export them. **Note** For viewing the file exporting records, refer to ***Manage Operation Records*** .

Operation	Description
Delete the Files	Select the files and click **Delete** to delete them.
Switch Display Mode	Click or or to display added files in card mode or list mode or map mode.

View and Edit a File

In the card mode or list mode, you can click the file name to open the file details pane and perform the following operations if needed.

Note

Only videos in PS, TS, or MPEG-4 container format can be played and edited after fully loaded.

File Format	Operation	Description
Common	View Details	View who uploaded the file, uploading time, file size, and description. Persons of the file owner's department have the permission to view file details.
	Edit Basic Information	Edit the file name, file tag, and description.
	Edit User Permission	In User Permission, click to edit the file permissions of the shared users.
	Link to Case	Click and enter the case name, ID, or description to search for the cases to be linked.
	Confirm Integrity Verification Value	Click to copy the case's integrity verification value. You can check the file integrity by comparing the integrity verification value of the platform and that of the exported file.
	Search File on Map	Click to search files on the map by entering a geographic location or specifying an area for search.
Picture	Zoom in Picture	Click to zoom in the picture.
Video	Start/Pause/Stop Video Play	Click / / to start/pause/stop playing the video.
	Normal/Reverse Playback	Click to perform reverse playback. Click and to perform speed playback.
	Full Screen	Click to show the video in full-screen mode.
	Edit Video	Click to enter the Edit Video page, and drag the timeline to position the desired video segment.

File Format	Operation	Description
		• Click **Add Text** to enter the text, and drag it to the proper location. • Click **Add Mosaic**, and draw a desired region of mosaic on the video. • Click **Clip**, drag the timeline to a desired position, and click again to finish clipping. • Select one or multiple clips and click **Delete** to delete them. • Select the audio and click **Audio Off** to set the video to the mute mode.

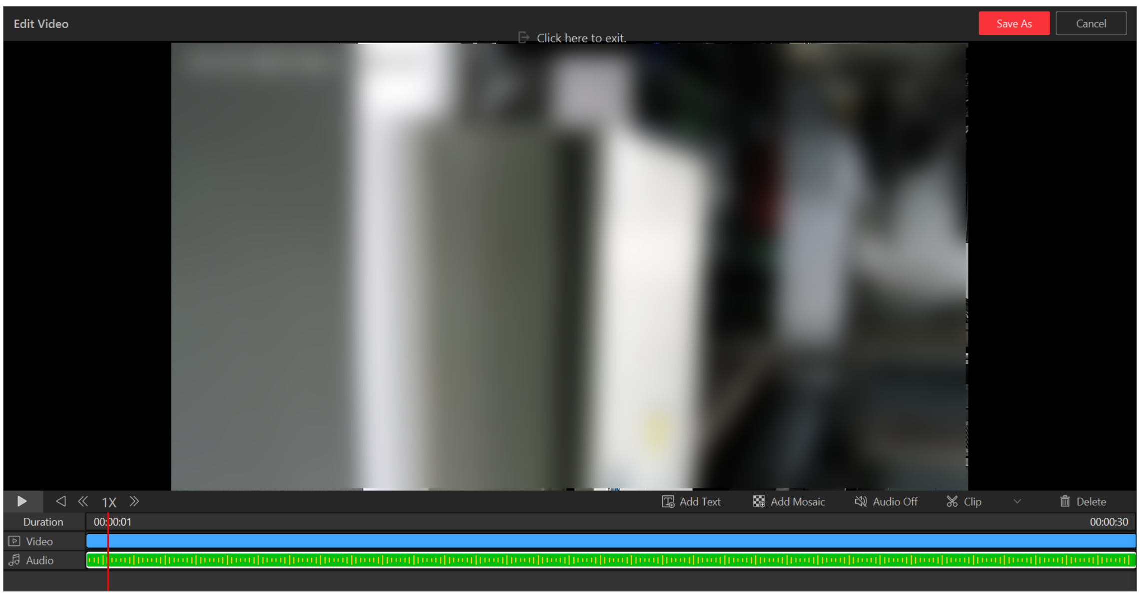


Figure 19-2 Edit a Video File

19.2.5 Share Files

You can share files to users whom you have the permission to share with. The shared users have the permissions for, such as viewing, sharing, and editing the file, as you set. You can also view the files shared by other users.

Selected the added files and click **Share**.

Share to System Internal User

Click **Add** to select users as file receivers. Set the permissions of receivers, and click **Share**.

Share to System External User

Click **Add Email** to add the emails of file receivers. Set the email title and content. Set the permissions of receivers and the expiry date, and click **Share**.

19.3 Manage Cases

A case is about incidents such as traffic accidents and violent crimes. You can add, edit, and share cases. After adding cases, you can link files uploaded from the local/device to cases and the linked files can be used as materials for settling disputes or legal cases.

Note

- The case permission (such as viewing, editing, exporting, and sharing) varies according to the user roles. On the User Permission page of an added case displays the permission details.
- The case owner has all permissions. Upper-level users of the file owner have the same permissions as the file owner. Users with super access permission can view all cases. Persons in the same department of the case owner can also view the case.

19.3.1 Add a Case

You can add case about incidents such as traffic accidents and violent crimes for settling disputes or legal cases. You can set detailed information for the added case, including the case name, ID, type, tag, on-site organization, result/conclusion, status, and time. Also, you can upload the file (including pictures, audios, videos, Excel files, CSV files, PDF files, and others) as the case content from cameras or the File Management page.

Before You Start

Make sure you have configured basic settings. For details, refer to ***Basic Settings*** .

Steps

1. On the left navigation pane, select **Case Management**.
2. Click **Add** to enter the Add Case page.

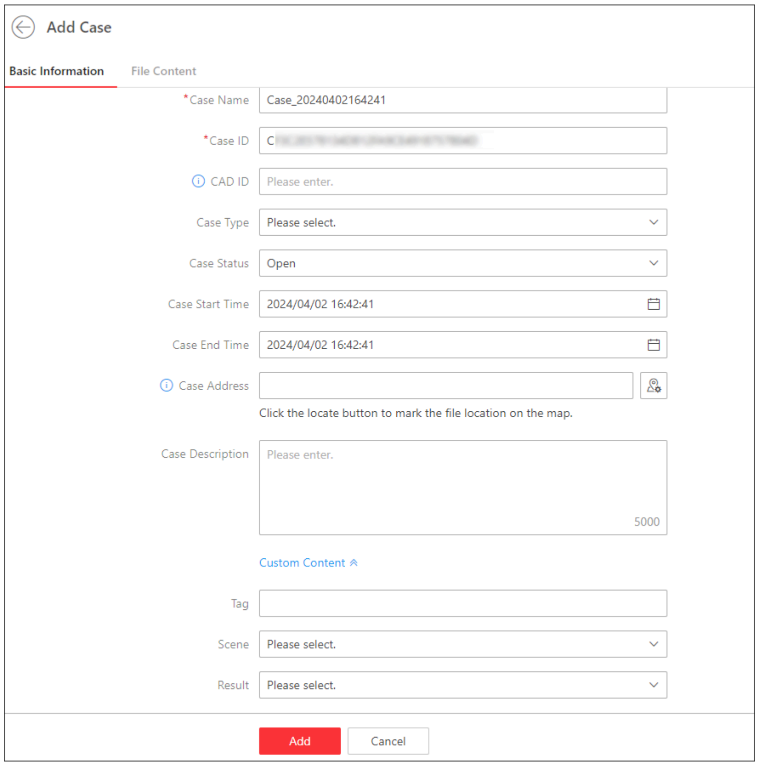


Figure 19-3 Add Case

3. Create a name for the case.

   The case ID will be generated automatically on the Client. You can edit the case ID which should include 1 to 64 letters or digits.
4. **Optional:** Set the CAD ID, type, status, time (start time and end time of the case event), case address, description, etc. for the case.
5. Click **File Content** tab to enter the File Content page.
6. **Optional:** Set the mode of adding files to the case.
   - Select **Add → Upload Local File** to upload files (such as pictures, audios, and videos) from the local PC for the case content.
   - Select **Import From File Management**, check one or multiple files related to the case, and click **Confirm**.
7. Click **Add** to add the case and back to the Evidence Management page.

19.3.2 View and Edit Cases

Select **Case Management** on the left.

You can view the details of cases, edit the case information, and export cases to your local PC.

Operation	Description
Refresh Case	Click **Refresh** to refresh the latest view of case information.
Switch Display Mode	Click or or to display added cases in card mode or list mode or map mode.
Select Sorting Mode	Click **Select Sorting Mode** to select the display order.
Delete Case	Select the case(s) and click **Delete** to delete the case(s).
Filter Case	Click on the upper right corner of the Evidence Management page, enter a keyword in the search box or set filter conditions, and click **Filter** to filter the target case(s). You can also click **Save Filtering Condition** to save the current filtering conditions settings for later use.
Open/Close Case	Select one or multiple cases, and click **Close Case** to close the case if the related case is settled, or click **Open Case** to open the selected case if the related-case is pending.
Export Case Record	Click **Export** to export the selected case record(s) in Excel, CSV, or PDF format. Or click **Export All** to export all cases. **Note** • You can check **Include Case File** to export the attached case file. • You can view the download records in the Download Record page.
View Case Details and Edit Case	• In the card mode or list mode, you can click the case name to view the case's basic information, file content, and operation records. • You can edit the case's basic information, such as the case type, time, and tag. • You can upload more related files from local PC for the case content, delete unneeded files, and search for files. • You can click **Case Report** to download the case report. The report includes case basic information, linked evidence file, and detailed operation record. You can view the download records in the Download Record page.
Search Case on Map	In the map mode, you can search for cases by entering a geographic location or specifying an area.

19.3.3 Share Cases

You can share cases to users whom you have the permission to share with. The shared users have the permissions for, such as viewing, sharing, and editing the case, as you set.

Selected the added files and click **Share**.

Share to System Internal User

Click **Add** to select users as case receivers. Set the permissions of receivers, and click **Share**.

Share to System External User

Click **Add Email** to add the emails of file receivers. Set the email title and content. Set the permissions of receivers and the expiry date, and click **Share**.

19.4 Link Files to Cases

You can link the added file to the existing case or newly added case. The linked files recorded in the case can be used as materials for settling disputes or legal cases.

Note

Make sure you have added the file(s).

On the left pane, select **File Management**.

Link a Single File to One or Multiple Cases

1. Click a file to open the file details pane.
2. In **Basic Information** page, click + to add a case field.

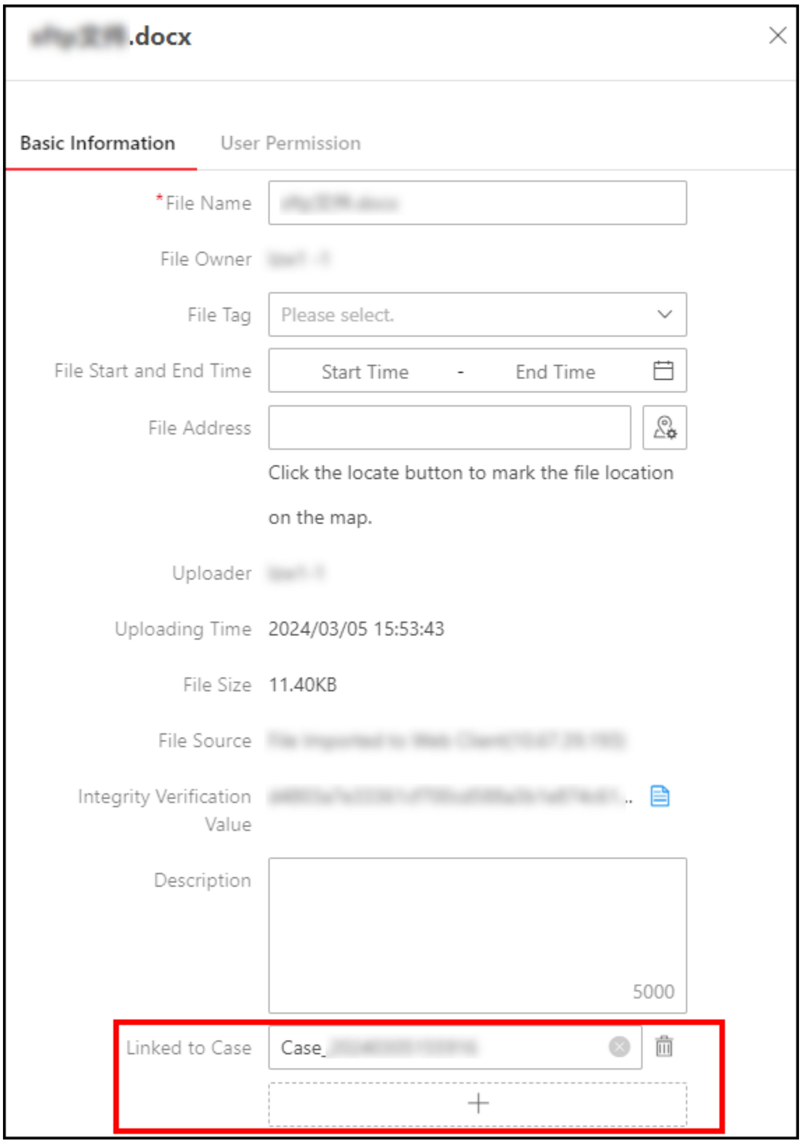


Figure 19-4 Link a Single File to Case

3. Search and select a case by the name or ID.
4. Click **Save**.

Batch Link Files to One Case

1. Select multiple files.
2. Click **Link to Case** to open the Link to Case pane.
3. Search and select a case by the name or ID.
4. Click **Save**.

19.5 Manage Operation Records

You can manage the operation records, including viewing or deleting the upload/download records of case or files.

Select **Operation Record → Upload Record** or **Operation Record → Download Record** on the left.

On the Upload Record page, you can view the records (including case or file size and upload status) of the case or files uploaded from local PC or related cameras. And on the Download Record page, you can view the records (including case or file size and download status) of exporting case or files on the platform.

You can also search for records by name, check a record and click / / in the Operation column to pause/resume/retry the upload/download task. Or you can check record(s) and click **Delete** to delete the selected record(s).

Chapter 20 Access Control Management

Access control is a security technique that can be used to regulate who can get access to the specified door.

On the Web Client, the administrator can add access control devices and video intercom devices to the system, group resources (such as doors) into different areas, and define access permissions by creating an access level to group the doors and an access group to group the persons. After assigning the access level to the access group, the persons in the access group will be authorized to access the doors in the access level with their credentials during the authorized time period.

20.1 Access Control Overview

On the Access Control Overview page, you can view the system data, health status, person credential status, etc.

Select **Access Control Overview** on the left navigation bar.

Perform the following operations as needed.

Name	Description
Wizard	You can view the brief introduction of the Access Control function and the major steps of configuration. You can hover the mouse cursor over each step and click ↗ to go to the corresponding page; click **Quick Configure** to complete the configuration process step by step in the Access Control Wizard.
Health Status	In Health Status, click the number in a circle to view status of each resource type, or click the number on the right of **Exception** to go to the Maintenance page for details about alarm inputs. In the upper-right corner, click **Go to Maintenance** to enter the Maintenance module. For more about the Maintenance module, refer to ***Maintenance*** .
Person Credential Status	Click the number in the circle of each credential to go to the Person page. Click the number under the application items (including person information and credentials) to go to the corresponding pages for details. See ***Figure 20-1*** .
Access Event Statistics	Click ⌄ and select a period to view the statistics of this period.

Name	Description
	Hover over , select a file format, and click **Export** to export the data generated in the selected period.
Person Access Event Statistics	Click to show the details of the recognized person. Click **Auto Update Record** to automatically display the latest record. Click **More** to go to the Person Authentication Record page to search for more data.

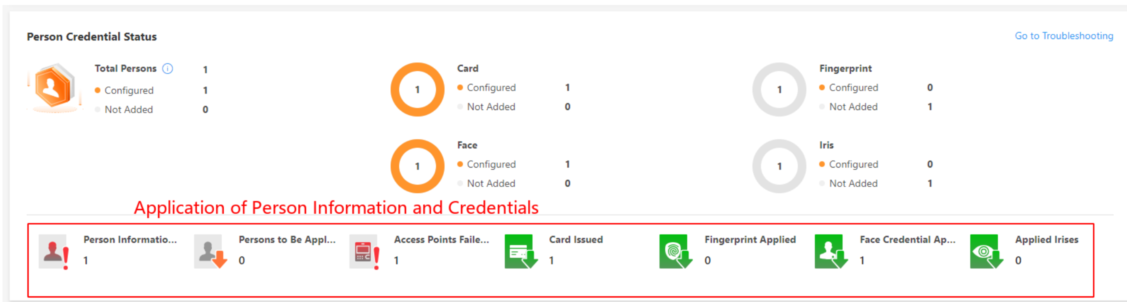


Figure 20-1 Application of Person Information and Credentials

20.2 Flow Chart of Door Access Control

The following flow chart shows the process of the configurations and operations of door access control.

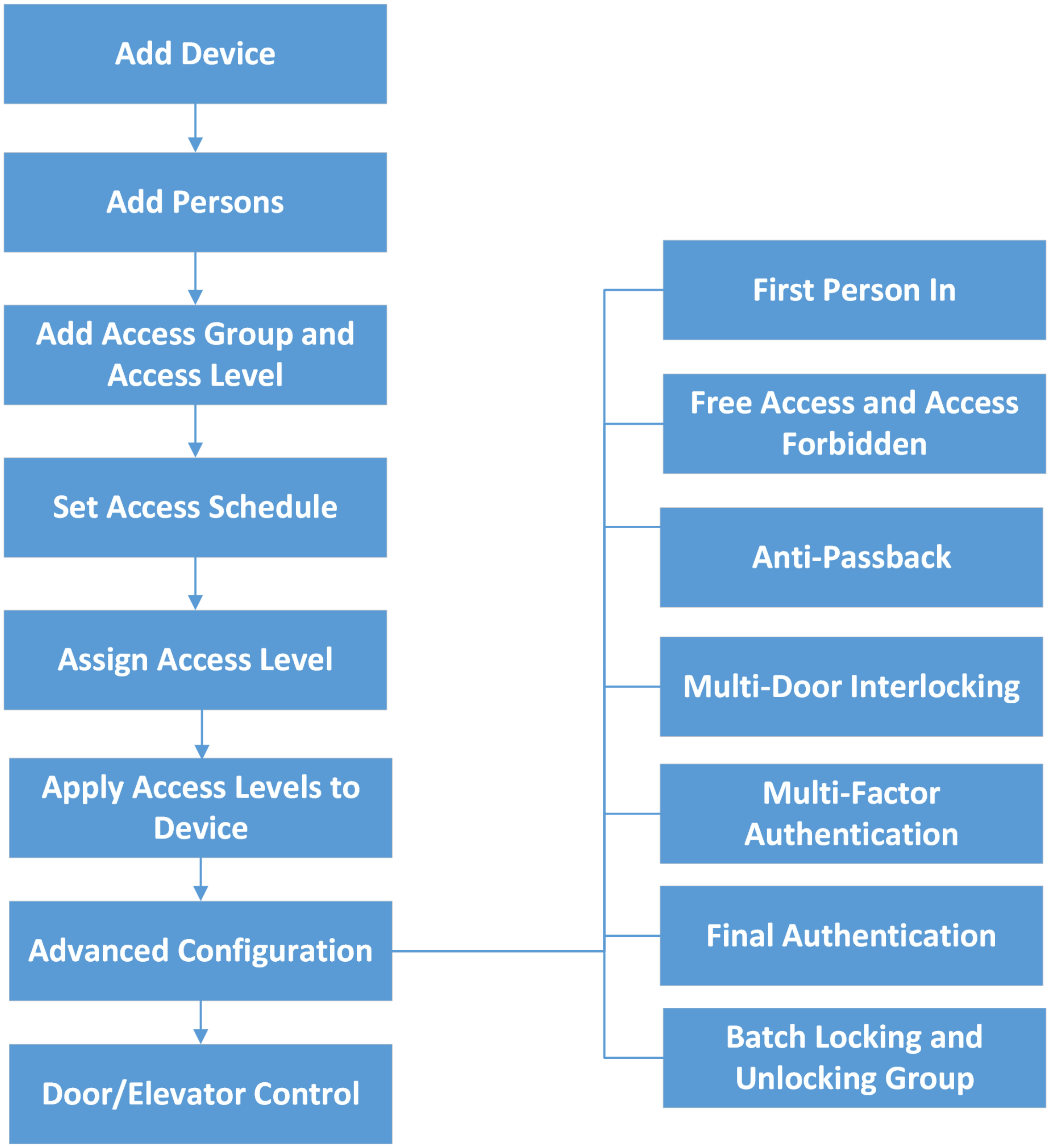


Figure 20-2 Flow Chart of Door Access Control

Table 20-1 Procedures of Door Access Control

Procedure	Description
Add Access Control Devices to the Platform	You need to add access control devices to the system. For details, refer to ***Manage Access Control Device*** .
Add Doors Linked with Devices to Areas	Group doors linked with added devices for management. Refer to ***Add Door to Area for Current Site*** for details.

Procedure	Description
Add Departments and Persons	Add person information and set person's credentials (such as PIN, card, and fingerprint). For details, refer to ***Person Management*** .
Set Access Schedules	The access schedule defines when the person can access the access point with credentials. For details, refer to ***Set Access Schedule Template*** .
Add Access Levels	An access level is a group of doors. After assigning access level, the assigned objects can get access to these doors during the authorized time period. For details, refer to ***Manage Access Level*** .
Assign Access Levels to Persons	You need to assign access levels to persons, so that the assignees can access the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person or a department. For details, refer to ***Manually Assign Access Level*** .
Control Door Status	You can manually change the door status to locked, unlocked, remaining locked, or remaining unlocked. Refer to ***Door Control*** for details.
Advanced Functions	Refer to ***Configure Free Access and Access Forbidden Rules*** , ***Configure First Person In*** , ***Configure Multi-Factor Authentication Rule*** , ***Configure Multi-Door Interlocking*** , ***Configure Area Anti-Passback*** , ***Add a Batch Locking and Unlocking Group*** , ***Add a Final Authentication Counting Group*** , ***Configure Authentication Mode*** , ***Apply Advertisement to Access Control Devices*** , and ***Add Audio Broadcast*** for details.
Data and Record Search	Refer to ***Search for Person Authentication Records*** and ***Search for Device Logs*** for details.

20.3 Flow Chart of Floor Access Control

The following flow chart shows the process of the configurations and operations of floor access control.

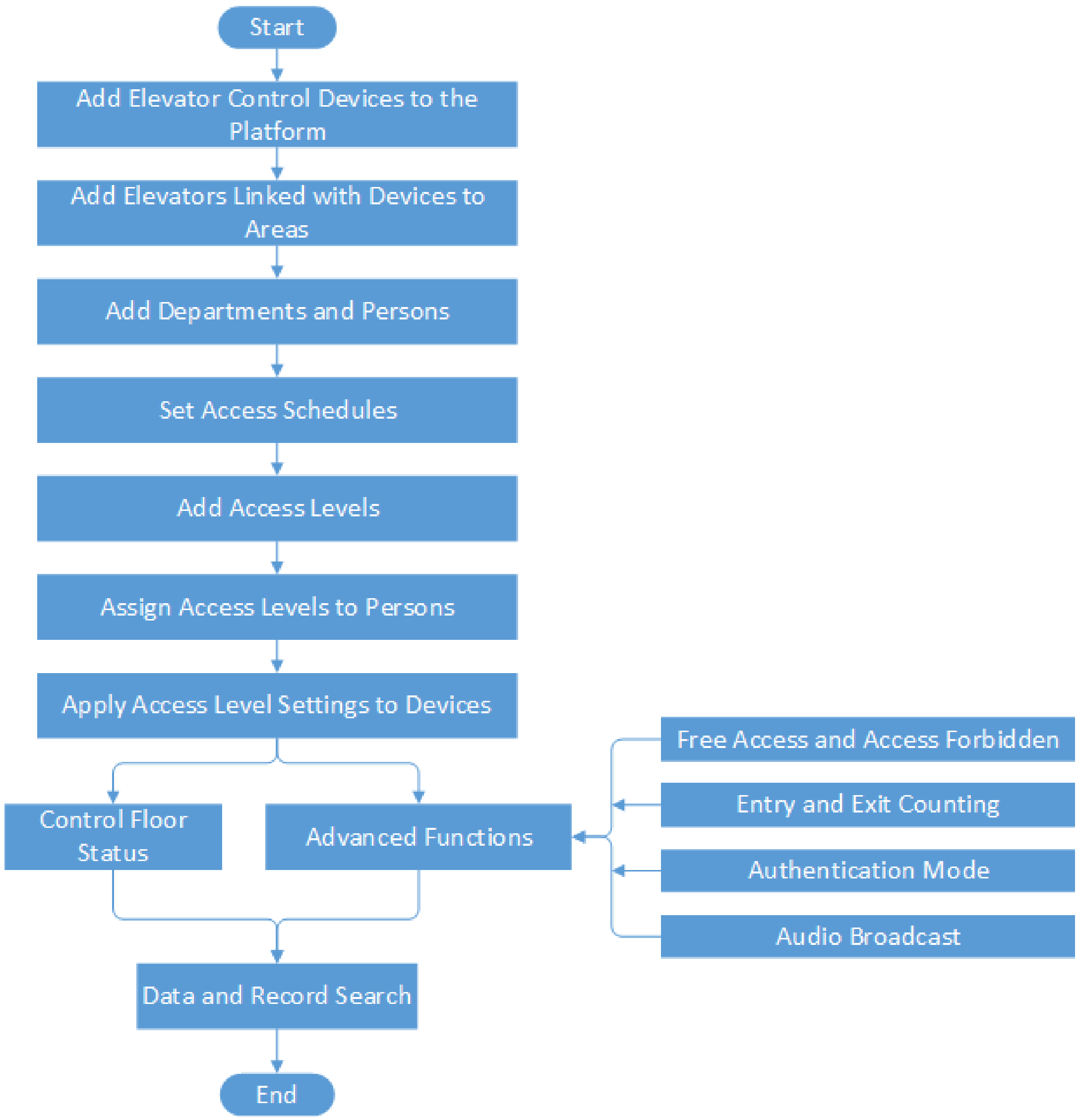


Figure 20-3 Flow Chart of Floor Access Control

Note

Some functions in this flow chart need the License.

Table 20-2 Procedures of Floor Access Control

Procedure	Description
Add Elevator Control Devices to the Platform	You need to add elevator control devices to the system. For details, refer to ***Manage Elevator Control Device*** .
Add Elevators Linked with Devices to Areas	Group elevators linked with added devices for management. Refer to ***Add Elevator to Area for Current Site*** for details.
Add Departments and Persons	Add person information and set person's credentials (such as PIN, card, and fingerprint).
Set Access Schedules	The access schedule defines when the person can access the access point with credentials.
Add Access Levels	An access level is a group of floors. After assigning access level, the assigned objects can get access to these floors during the authorized time period.
Assign Access Levels to Persons	You need to assign access levels to persons, so that the assignees can access the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person or a department.
Apply Access Level Settings to Devices	After setting the linkage between the persons and the access level, the person's access level settings will be automatically applied to the elevator control devices of the elevators linked to the access level to take effect. After that, the persons can access these floors during the authorized time period defined by the related access level. You can also set a schedule to apply the settings regularly.
Control Floor Status	You can manually change the floor status to temporary access, access with credential, free access, or access forbidden.

20.4 Manage Access Level

In access control, access level is a group of access points. Assigning access level to persons, departments, or access groups can define the access permission that which persons can get access to which access points during the authorized time period.

20.4.1 Access Level Overview

The platform provides an overview of all persons' access levels for access points. You can filter persons and perform some operations on their access levels.

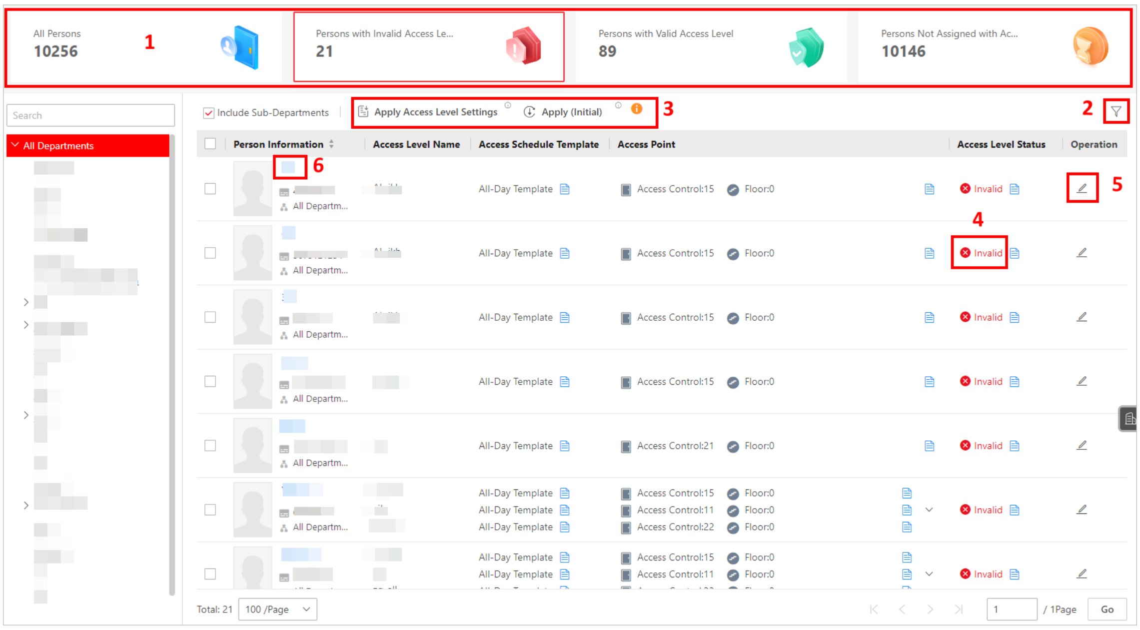


Figure 20-4 Access Level Overview

1	On the top, you can click the cards to display all persons, persons with invalid access levels, persons with valid access levels, or persons not assigned with access levels if needed.
2	Filter persons by different conditions such as person name, ID, access level.
3	For persons whose access levels failed to be applied, persons with invalid access levels, or persons not assigned with access levels, you can apply access levels for them. You can select access points before applying.
4	If a person's access level failed to be applied, "Invalid" will show in the Access Level Status column. You can click to view the details.
5	Click to edit a persons access levels. You can add or delete access levels.
6	Click a person name to view the person information.

20.4.2 Add Access Level

To define access permission, you need to add an access level to group the access points.

Steps

1. In the top left corner of Home page, select → **Passing Management → Access Control → Access Level** .
2. Click **Manage Access Level** on the left.
3. Click **Add** to enter the Add Access Level page.
4. Create a name for the access level.
5. **Optional:** Edit the description for the access level.
6. Select the access point type.
7. Select the access point(s) to add to the access level.
   1) In the **Available** list, select the access point(s) you want to add to the system and click .
   You can view your selection in the **Selected** list.
   2) **Optional:** In the **Selected** list, select the access point(s) that you no longer want to add to the system, and click to undo selection.

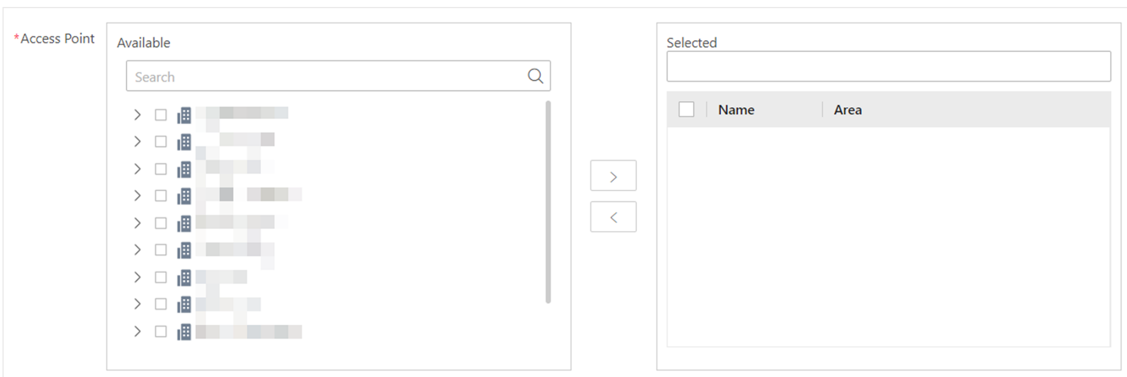


Figure 20-5 Select Access Points

8. Select an access schedule to define in which time period, persons are authorized to access the access points you select in the previous step.

Note

All default and custom access schedules are shown in the **Access Schedule** drop-down list. You can click **New Access Schedule Template** to customize a schedule. Or you can predefine access schedule templates. For details, refer to ***Set Access Schedule Template*** .

9. Click **Add** to add the access level and return to the access level management page.
10. **Optional:** Perform further operations on the added access level(s).

Edit Access Level	Click the name of an access level to view and edit its configurations.
Delete Access Level	Select an access level and click **Delete** to delete it.
Delete All Access Levels	Click → **Delete All** to delete all access levels.

What to do next

You need to assign the access level to persons, so that the assignees can have the access to the access points in the access level according to the access schedule. For details, refer to ***Manually Assign Access Level*** .

20.4.3 Manually Assign Access Level

You need to assign access levels to persons, so that the assignees can have the access to the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person, department, or access group.

Assign by Access Level

You can assign an access level to multiple persons so that the assigned persons can have the access to the access points in the access level.

Before You Start

- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .
- Make sure you have added persons to the system. For details, refer to ***Person Management*** .

Follow the steps to assign an access level to persons.

Steps

1. Select **Assign Access Level** on the left.
2. Click **Assign by Access Level** on the top.

   Note

   For the first time assignment, click **Add** at the center of the page to enter the assignment page.
3. Click on the access level that you want to assign to persons.
4. On the assignee pane, click **Assign To** to show person list.
5. Select the persons whom you want to assign the access level to and click **Add**.

   Note

   If you check **Select All**, all persons who matched the search conditions you set will be selected.

   The access level settings will be applied to devices automatically.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

Assign by Person

You can assign access levels to persons, so that the assignees can have the access to the access points in the access levels.

Before You Start

- Make sure you have added persons to the system. For details, refer to ***Person Management*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to specific persons.

Steps

1. Select **Assign Access Level** on the left.
2. Click **Assign by Person** on the top.
3. Check persons in the list, and click **Assign Access Level** to open the Assign Access Level pane.
4. **Optional:** In the Assign Access Level pane, click to add persons.
5. In the Access Level list, check the access levels that you want to assign to the selected persons.
6. Click **Assign**.

   The access level settings will be applied to devices automatically.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

Assign by Department

You can assign access levels to departments, so that the persons in the department can have the access to the access points in the access levels.

Before You Start

- Make sure you have added persons to the system. For details, refer to ***Person Management*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to specific departments.

Steps

1. Select **Assign Access Level** on the left.
2. Click **Assign by Department** on the top.
3. **Optional:** For the first time assignment, click **Assign Now** in the center of the page to open the Batch Assign Access Level to Departments page, and then see the second choice in ***4*** .
4. Do one of the following to assign access levels to departments.
   - Assign access levels to each department one by one.
     a. In the department list, click a department.
     b. Click **Assign Access Level** on the top.

c. In the Assign Access Level pane, select the access levels you want to assign to the selected department.
d. Click **Assign**.

- Assign access levels to multiple departments at a time.
  a. Click **Batch Assign** on the upper left.
  b. In the department list, select the departments where you want to assign access levels.

  Note

  Sub-departments are excluded from selection by default. To include all sub-departments of each department, check **Select Sub-Departments**.

  c. In access level list, select the access levels you want to assign to the departments.
  d. Click **Save**.

The access level settings will be applied to devices automatically.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

Assign by Access Group

An access group is the group of persons who have the same access permissions (In a specified time period, they have the permission to access the specified access points). You can add the persons who have the same access permission to the same access group. For example, the employees in the same department should access the company gates during the working hours. The employees can be added to the same access group and be related to the access level which contains the access permission of the company gates. You can assign one or multiple access levels to the access group, and the persons in the access group will get the permission to access all the access points in the access level(s).

Before You Start

- Make sure you have added persons to the system. For details, refer to ***Person Management*** .
- Make sure you have added access levels to the platform. For details, refer to ***Add Access Level*** .

Steps

1. Select **Assign Access Level** on the left.
2. Click **Assign by Access Group** on the top.

   Note

   For the first time assignment, click **Assign Access Level** at the center of the page to enter the assignment page.

3. **Optional:** Add access groups.
   1) Click + at the top of the access group list to open the Manage Access Group pane, and then click **Add** to enter the Add Access Group page.

Note

If no access group is added to the access group list, click **Add Access Group** in the access group list to enter the Add Access Group page.

2) In the **Group Name** field, enter the name of the access group.
3) In the **Group Member** area, click **Add** to open the person list, select the person(s) to be added to the access group.

Note

If you check **Select All**, all persons who matched the search conditions you set will be selected.

4) Click **Add** to add the selected person(s) to the access group.
5) Click **Add** at the bottom.

4. Check access group(s) to assign access levels to.
5. Click **Assign Access Level** on the top.
6. In the Assign Access Level page, select the access level(s) to be assigned to.
7. Click **Assign**.

   The access level settings will be applied to devices automatically.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

20.4.4 Regularly Apply Access Level Settings to Devices

You can set a schedule to apply the access level settings in the system to devices automatically.

Before You Start

Make sure you have assigned access levels to persons in the system. For details, refer to ***Manually Assign Access Level*** .

Steps

1. In the top left corner of Home page, click → **Access Control** → **Basic Configuration** → **General** .
2. Switch on **Apply to Device (Scheduled)**.
3. Select an applying mode.
   - **Apply at Fixed Time**: Apply the changed access level settings and the settings that failed to be applied last time to devices at a specific time (System Management Server time) on a daily basis. You can select a time in the **Auto-Apply At** drop-down list.
   - **Apply Every Certain Hours**: Apply the changed access level settings and the settings that failed to be applied last time to devices immediately and every certain hours afterward. You can select an interval in the **Time Interval** drop-down list.
4. Click **Save**.

20.4.5 Clear Persons' Access Levels

You can clear the access levels of persons so that they cannot access the access points in the access levels. For example, if there is no access record of certain persons entering or exiting for a long time, the administrator can clear their access levels to make sure the persons' credentials will not be misused.

On the left, select**Assign Access Level**, then select an access level assigning mode on the top.

The unassigning operations vary by different assigning modes.

- On the **Assign by Access Level / Assign By Person** page, select the target person, hover the cursor on ⌄ , and select **Unassign All Access levels** or **Unassign Specified Access Levels**.

  Note

  For the latter one, if you selected multiple persons, only the common access levels shared by the selected persons can be unassigned.
- On the **Assign by Department / Assign by Access Group** page, check access level(s) and click **Unassign**, or hover the cursor on ⌄ and select **Unassign All**.

Note

- Once cleared, the previous access level settings of the persons cannot be restored. You need to re-assign access levels for them again when needed.
- After the access level settings of the selected persons are cleared , these persons will be removed from the related access groups.
- After the access levels are unassigned, the changes will be automatically applied to devices, and the access level settings of the persons will be deleted from the devices.

20.4.6 Set Access Schedule Template

Access schedule defines when persons can open access points in an access level with credentials, or when access points remain unlocked so that persons can open the access points with free access. The system provides three default access control schedule templates: All-day Template, Weekday Template, and Weekend Template. You can also add customized templates according to your needs.

Steps

1. In the top left corner of Home page, click ▦ → **Passing Management → Access Control → Basic Configuration** .
2. Click **Access Schedule Template** on the left.
3. Click + to create a blank template.
4. Configure the template in the template information panel on the right.

   Name

   Create a name for the template.

Copy from

Optionally, you can select to copy the settings from existing templates.

5. In the **Weekly Schedule Template** box, set a schedule pattern for each day.
   1) Click **Authorize** and select or draw in the box to define the authorized time periods. After drawing, you can enter a time or adjust the time by clicking the arrows in the box popped up.
   2) **Optional:** Click **Erase** and select or draw on the authorized time periods to clear the selection.

Note

You can set up to 8 separate time periods for each day.

6. **Optional:** Set a holiday schedule if you want different schedules for specific days.

Note

Holiday schedule has a higher priority than weekly schedule.

   1) Click **Add Holiday**.
   2) Select existing holiday templates, or click **Add New** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Set a schedule pattern for holidays.
7. Click **Add** to save the template.
8. **Optional:** Perform further operations on added templates.

View and Edit Template Details	Click a template item to view and edit its configurations.
Delete Template	Click a template item and click 🗑 to delete it.

What to do next

Set access schedule for access level to define in which time period persons are authorized to access the access points in the access level. For details, refer to ***Add Access Level*** .

20.4.7 Advanced Functions

Configure Free Access and Access Forbidden Rules

To set access points accessible or inaccessible during certain periods, configure free access and access forbidden rule for certain access points.

Steps

Note

This function should be supported by the device.

1. On the left navigation bar, select **Free Access & Access Forbidden**.
2. Click **Add** to enter the Add Free Access and Access Forbidden Rule page.

3. Enter the rule name.
4. Select an access point from the following area list.
5. Select free access schedules or access forbidden schedules.

   Free Access Schedule

   During free access period, all persons can access the selected access points without credentials required.

   Access Forbidden Schedule

   During access forbidden period, no persons can access the selected access points even if he/she has the authorized credentials, except the users with super access permission.

   Note

   - You can click **Add** to add a custom access schedule or holiday schedule. See ***Set Access Schedule Template*** for details.
6. Click **Add**.

   The system will automatically apply the schedule(s) to devices.

Configure First Person In

First Person In refers to a rule that only after the first person is authorized to enter with his or her card, fingerprint, or face, can other people's permission be activated.

Steps

Note

This function should be supported by the device.

1. Select **Access Control Application → First Person In** on the left.
2. Click **Add** to enter the Add First Person In Rules page.

   Note

   For the first time configuration, click **Configure Now** in the center of the page to enter the Add First Person In Rule page.
3. Enter the rule name.
4. Select a door from the resource list.
5. Set **Rule of Opening Door**.
6. Set the consecutive authentication times and the interval of consecutive authentication.
7. **Optional:** Enable **First Person Authentication Time** to set a time when the rule takes effect and a fixed time period requiring first person authentication.
8. In the First Person area, click **Add** to select first person(s).

Note

If you check **Select All**, all persons who matched the search conditions you set will be selected.

9. Click **Add** to add the rule.

Add a Batch Locking and Unlocking Group

The batch locking and unlocking group is a group for access points which need to be controlled in a batch. This function is mainly applicable for emergent situations. You can add doors of access control devices, doors of video intercom devices, and floors of elevator control devices to the group.

Before You Start

Add the access points into different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. On the left, select **Access Control Application → Batch Locking and Unlocking Group** .
2. Click **Add** on the top.

Note

For the first time configuration, click **Configure Now** in the center of the page to enter the Add First Person In Rule page.

3. Create a name for the group.
4. In the Access Point area, select the access points and click › to add them to the group.
5. Click **Save**.

Anti-Passback Configuration

The anti-passback is designed to minimize the misuse or fraudulent use of access credentials such as passing back the card to an unauthorized person, or tailed access. Only one person can pass the access point after swiping the card. You can configure area anti-passback rules or route anti-passback rules for different scenarios. This function is mainly used for enhanced access security of some important or specific places (e.g., laboratories, offices).

Perform the following operations after adding an anti-passback group to the area.

Edit Anti-Passback Group	Click the group name to edit the anti-passback group settings. You can edit the name of the group, add or delete doors in the group, change the settings of forgiving anti-passback violation regularly,

	and edit the locations of the group and doors on the map.
Set/Cancel Forgiving Anti-Passback Regularly	Select the group(s), click **Set Forgiving Anti-Passback Regularly**, and specify a fixed time so that the platform can automatically forgive the anti-passback violations occurred in the selected anti-passback group(s) at that time everyday. You can also select the group(s) and click **Cancel Forgiving Anti-Passback Regularly** to cancel the settings of the selected group(s).

Configure Area Anti-Passback

The area anti-passback function establishes a specific door group for an area. When a person accesses the area by swiping card, he/she should exit the area via the door in the anti-passback group if the person enters the area via the door in the group, and the person cannot enter the area via the door in the anti-passback group if he/she exited the area not by swiping card at the door in the group before.

Before You Start

Add the access points to different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. On the left, select **Anti-Passback**, and then select **Area Anti-Passback** on the top..
2. Click **Add**.

 Note

 For the first time configuration, click **Configure Now** in the center of the page to enter the Add Area Anti-Passback Rule page.

3. Configure basic information, including rule name and anti-passback effective mode.
4. **Optional:** If you select **Control Anti-Passback by Platform** as the anti-passback effective mode, check **Enable Rule Now**.
5. Click **Next**, and start the rule configuration.
 1) **Optional:** If you select **Control Anti-Passback by Platform** as the anti-passback effective mode, click in the Person area, and check persons on the platform.
 2) Select doors in the Available list and click to add them to the Selected list.
 3) **Optional:** If you select **Control Anti-Passback by Platform** as the anti-passback effective mode, select an access schedule.
6. Click **Next**, and configure the advanced parameters.

 Forgive Anti-Passback Violation Regularly

Set a fixed time so that the platform can forgive the anti-passback violations occurred in this group automatically everyday.

Anti-Passback Violation

When a person attempts to use a card without following the rule, the access will be denied. When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven.

Non Anti-Passback Period

Set a fixed time during which persons can access the area without following the rule. This function should be supported by the device.

7. Click **Save**.

Configure Route Anti-Passback

The route anti-passback depends on the card swiping route. Establish a card reader sequence for access control, setting the initial and subsequent card readers to authenticate anti-passback based on stored entrance and exit data.

Steps

1. On the left, select **Anti-Passback**, and then select **Area Anti-Passback** on the top.
2. Click **Add** to enter the Add Route Anti-Passback page.

Note

For the first time configuration, click **Configure Now** in the center of the page to enter the Add Area Anti-Passback Rule page.

3. Configure basic information, including rule name and anti-passback effective mode.
4. **Optional:** In you select **Control Anti-Passback by Platform** as the anti-passback effective mode, check **Enable Rule Now**.
5. Click **Next**, and start the rule configuration.
   1) **Optional:** If you select **Control Anti-Passback by Platform** as the anti-passback effective mode, click in the Person area, and check persons on the platform.
   2) In the Card Reader area, click **Add Card Reader** and select a card reader to add it.
   3) **Optional:** Click to add more card readers.
   4) **Optional:** If you select **Control Anti-Passback by Platform** as the anti-passback effective mode, select an access schedule.
6. Click **Next**, and configure the advanced parameters.

First Card Reader

Set the first card reader in the route to the first card reader. If you violate the route anti-passback rule, you should swipe the card again from the first card reader.

Forgive Anti-Passback Violation Regularly

Set a fixed time so that the platform can forgive the anti-passback violations occurred in this group automatically everyday.

Anti-Passback Violation

When a person attempts to use a card without following the rule, the access will be denied. When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven.

Non Anti-Passback Period

Set a fixed time during which persons can access the area without following the rule. This function should be supported by the device.

7. Click **Save**.

Configure Multi-Door Interlocking

Multi-door interlocking is used to control the entry of persons to a secure area such as a clean room, where dust or small particles may cause a major issue. One multi-door interlocking group is composed of at least two doors and only one door can be opened simultaneously.

Before You Start

Add the access points to different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the top left corner of the Home page, select → **Passing Management → Access Control → Access Control Application → Multi-Door Interlocking** .
2. Click **Add**.
3. Create a name for the group.
4. Select doors and click .
5. Click **Add**.

Manage Multi-Factor Authentication

Multi-Factor Authentication is an access authentication scheme which requires all the predefined persons to be present and get authentication. Multi-Factor Authentication is generally used in places such as bank vault to ensure the security of important assets and data. To perform this function, you need to configure multi-factor authentication rule and add multi-factor authentication group first. Besides, you can add persons to receive remote door open request.

Configure Multi-Factor Authentication Rule

In access control, multi-factor authentication is an authentication method in which the door will unlock only after multiple persons present authenticating multiple credentials in turn. This method is mainly used for locations with high security requirements, such as bank vault. With the mutual supervision of the persons, multi-factor authentication provides higher security for the assets in these locations.

Steps

Note

This function should be supported by the device.

1. In the top left corner of the Home page, select → **Passing Management → Access Control → Access Control Application → Multi-Factor Authentication** .
2. Click **Add**.
3. Enter the rule name.
4. Select a door from the following area list.
5. Set the access mode of the door.

   Unlock After Access Granted

   The door will be unlocked automatically after the persons swiping their cards (or other type of credentials) on the card readers of the door and the access is granted.

   Remotely Unlock After Granted

   After the persons swiping their cards (or other type of credentials) on the card readers of the door and the access is granted, a window will pop up. The operator should confirm to unlock the door remotely and then the door will be unlocked successfully.

   Enter Super Password After Granted

   After the persons swiping their cards (or other type of credentials) on the card readers of the door and the access is granted, they should enter the super password on the card reader. After that, the door will be unlocked successfully.
6. Set the access schedule to define in which time period, the persons are authorized to access the door.

   Note

   The default and customized access schedules are displayed in the drop-down list. You can click **Add** to customize a new schedule. For details, refer to ***Set Access Schedule Template*** .

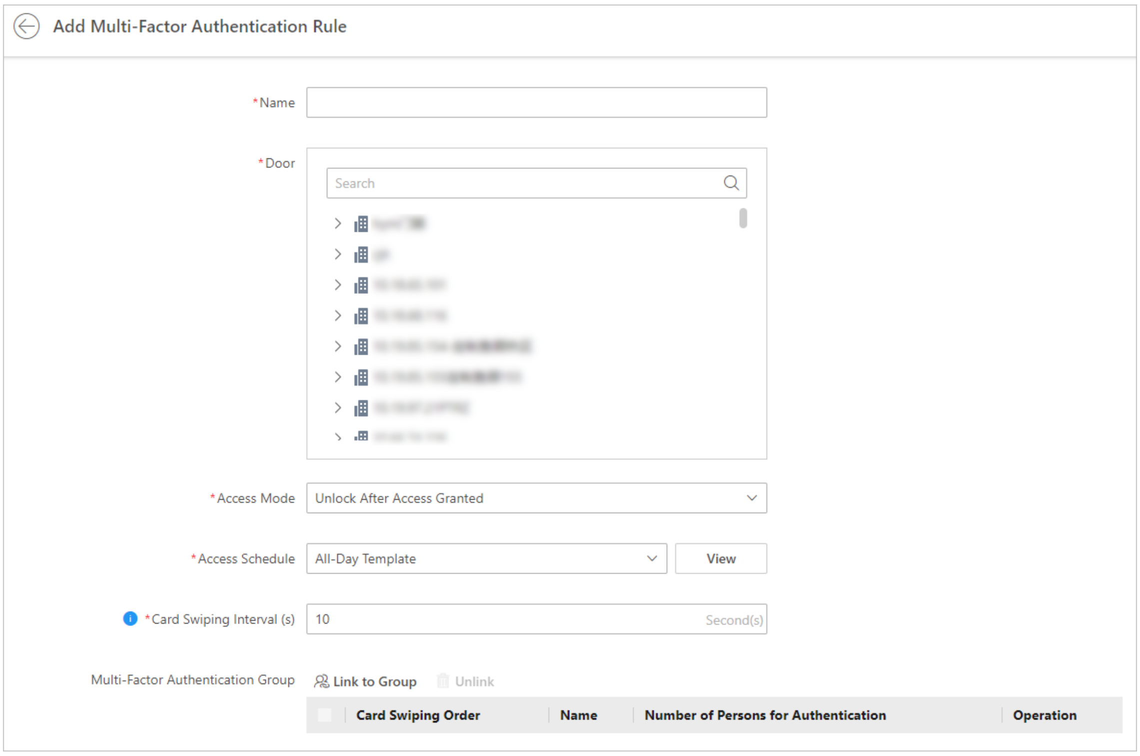


Figure 20-6 Add Multi-Factor Authentication Rule

7. Set the card swiping interval and make sure the interval between two authentications on the card reader is within this value.

Example

When you set the interval as 5s, if the interval between two authentications is longer than 5s, the authentications will be invalid, and you should authenticate again from the beginning.

8. Click **Link to Group** to set the access group(s) to define who have the permission to access the door.

Note

When adding groups, if you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

Card Swiping Order

Click ↑ or ↓ in the **Operation** column to set the authentication order of different access groups.

Number of Persons for Authentications

Define how many persons should authenticate on the card reader.

For example, if you set 3 for access group Security Guard and 1 for access group Bank Manager, it means three security guards should swipe cards on the card reader (or other access mode), and one bank manager should swipe card on the card reader (or other access mode) for this multi-factor authentication.

Note

This value should be no larger than the number of persons in the access group.

9. Click **Add**.

Add Multi-Factor Authentication Group

To perform the multi-factor authentication function, you need to create a multi-factor authentication group and appoint persons as the member of the group first. Persons in the group have the permission for multi-factor authentication of specific doors.

Steps

1. In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** .
2. Click **Multi-Factor Authentication** on the left.
3. Click **Multi-Factor Authentication Group Management** on the top.
4. Click **Add** to open the Add Multi-Factor Authentication Group panel.
5. Enter the multi-factor authentication group name.
6. Click **Add** to select group members from the person list.

   Note

   When adding groups, if you check **Select All Persons**, all persons who matched the search conditions you set will be selected.
7. Click **Add**.

Add User to Receive Remote Door Open Request

To handle remote door open requests on the Control Client, you need to appoint persons to receive these requests beforehand.

Steps

1. In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **Multi-Factor Authentication** .
2. Click **User to Receive Remote Door Open Request** on the top.
3. Click **Add** to open the User to Receive Remote Door Open Request pane.
4. Select users from the list.

   Note

   If you check **All**, all persons will be selected.
5. Click **Add**.

Configure Authentication Mode

The authentication mode is used to determine whether a person has the permission to pass the access point by using single or multiple authentication modes (e.g., employee ID, face, fingerprint, password, PIN code, or a combination of them). You can set the reader authentication mode for access points or set the private authentication mode for persons. If a device has been configured with different authentication modes by two methods, the person's private authentication mode has higher priority than the reader authentication mode.

Set Reader Authentication Mode

You can set the reader authentication mode to employee ID, password, face, fingerprint, PIN code, or a combination of them in normal time periods or custom time periods according to your actual need.

Before You Start

Make sure you have added doors to the area. See ***Add Element to Area*** for details.

Steps

Note

This function should be supported by the device.

1. In the upper-left corner of the Home page, select → **Passing Management → Access Control → Access Control Application → Authentication Mode** .
2. Select the **Card Reader Authentication Mode** tab.
3. Select an area from the area list.
4. Click a door name on the right.
5. Select the Card Reader Authentication Mode Settings.

   Batch

   Set the same reader authentication mode for all the readers of a door.

   Single

   If you want to set different reader authentication modes for different readers, select this mode.
6. Select the Card Reader Authentication Mode.

   Reader Authentication Mode

   Set the reader's authentication mode in normal time periods. For example, if you select **Card**, persons on the platform should open the door by swiping the card for authentication each time.

   Reader Authentication Mode (Custom)

When you want persons on the platform to open the door via another authentication mode in some special time periods, you need to set the reader's authentication mode and select the custom time period. For example, if you select **Fingerprint** and **Weekend Template**, persons on the platform should open the door via fingerprint at weekends.

7. **Optional:** Click **Copy To** in the upper-right corner to apply the settings to other doors.
8. Click **Save**.

Set Person Private Authentication Mode

In some situations, different persons need to use different authentication modes for accessing the same access point, and a person may need to use different authentication modes for accessing different access points. Setting the private authentication modes for different persons can provide an easy way for them to authenticate by less credentials or enhance the security of some important places by forcing them to use more credentials.

Steps

Note

The person's private authentication mode has higher priority than the existing authentication mode of the device.

---

1. In the upper-left corner of the Home page, select → **Passing Management → Access Control → Access Control Application → Authentication Mode** .
2. Select the **Private Authentication Mode** tab.
3. Select a department from the left list.

   All persons in the department will be listed on the right panel.
4. Click in the Operation column to open the Authentication Device pane.
5. Click **Add**, check the device(s) from the list, and select the authentication mode from the drop-down list for the selected device(s).
6. Click **OK** to add the device(s) for authentication for the person.
7. **Optional:** Perform one of the following operations to edit the authentication mode(s) for the device(s).
   - Select an authentication mode from the Authentication Mode drop-down list to configure the authentication mode for each device.
   - Click **Batch Configuration**, select an authentication mode from the drop-down list, and click **Save** to configure the same authentication mode for all added devices.
8. **Optional:** In the Private Authentication Mode page, click in the Operation column, select the person(s), and click **OK** to copy the person's private authentication mode settings to another person or other persons.

Result

The number of devices added for each person is displayed in the Device for Authentication column. You can click beside the number to view names and authentication modes of all devices.

Add a Final Authentication Counting Group

The final authentication counting group is used to group the access points in a certain area. You can set certain access points as the region edge. Only the persons accessing these access points are counted, and other access points inside the region are ignored. By grouping these access points, the platform provides counting functions based on the entry and exit records on these access points. With this function, you can know who enters/exits this region and how many persons still stay in this region. This is applicable for certain emergency scenes. For example, during a fire escape, the number of the remaining/stayed-in persons and name list are required for rescue.

Before You Start

Add the access points into different areas. For details, refer to ***Add Element to Area*** .

Steps

1. On the left, select **Final Authentication Counting Group**.
2. Click **Add**.
3. Create a name for the group.
4. Click **Add** and select doors from the area list.
5. Set the entering or exiting direction of the card readers of the selected access points.
6. Click **Save**.

Add Audio Broadcast

You can add daily audio broadcasts for daily use and add particular broadcasts for holidays or specific days. After adding broadcasts, you can apply them to devices.

Steps

1. In the top left corner of Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **Audio Broadcast** .
2. Click **Add Audio Broadcast**.
3. Select the broadcast device(s).
4. Enable the daily broadcast.

   Note

   For the two types of authentication result, 4 time periods in total can be added.

   1) **Optional:** Enable **Broadcast Address** to select the broadcast address type.
   2) Set the broadcast time and content.
      - Click **Add** to add new broadcast time and content.
      - Click to create a copy and set the time and content based on the existing one.
5. In the Particular Broadcast area, click **Add** to add particular broadcasts.

Note

For the two types of authentication result, 4 time periods in total can be added.

1) Select the particular day type.
2) Select the holidays(s) or select the specified day(s).

Note

- On the days without particular broadcasts, daily broadcasts will be played. If the specified days overlap the holidays, the broadcasts for specified days will be played.
- Click **Add** to add new holidays. For details, refer to ***Set Holiday*** .

3) **Optional:** Enable **Broadcast Address** to select the broadcast address type.
4) Set the broadcast time and content.
   - Click **Add** to add new broadcast time and content.
   - Click to create a copy and set the time and content based on the existing one.
5) Click **Save**.

6. Click **Add**.

   The settings will be applied to the selected device(s).
7. **Optional:** After applying, perform the following operations as needed.

View Device Details	Click the device name to view the broadcast details of the device. You can also edit the broadcast settings to apply for another time.
View Broadcast Details	Click to view broadcast details.
Copy Broadcast Settings to Other Devices	In the operation column, click to select the device(s) to copy to. Click **Copy** and the settings will be applied to the selected device(s).
Apply Failed Broadcast to Device	• At the top of the broadcast list page, click **Details** to view failure details or click **Apply Again**. • In the Operation column, click to apply again.
Delete Broadcast of Device	Check the device(s) and click **Delete** to delete the broadcast(s) of the selected device(s). You can also click → **Delete All** to delete the broadcasts of all devices.

Apply Advertisement to Access Control Devices

You can add picture(s), video(s), and text(s) in the advertisements, then apply the advertisements to access control devices. After applying advertisements, you can filter or delete them.

Steps

1. In the upper-left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **Apply Advertisement** .

2. Select the available door station in the left list and click › to add it to the right list. You can click ‹ to remove it from the selected door station list on the left.
3. Add materials (picture, video, or text) for an advertisement to be applied to access control devices.

Note

- The material type (picture, video, or text) should be supported by devices.
- You can check two types of advertisement materials at the same. For example, you can check both picture and video at the same time, excluding text.
- You can up to 8 videos and pictures, or 3 texts at one time.

- a. Click **Picture →** + to add picture(s) for an advertisement.
  b. Set the duration for pictures switching interval.
  c. Set the time period to play the added picture(s).

  Note

  Up to 2 time periods are allowed. You can click **Add** to add the time period if needed.
- a. Click **Video →** + to add a video for an advertisement.
  b. Set the duration for videos switching interval.
  c. Set the time period to play the added video.

  a. Click **Text →** + to add a text for an advertisement.
  b. Set the advertisement texts, including uploading the background picture, setting the text title/font size/color, and selecting the layout style.
  c. Set the time period to play the added texts.

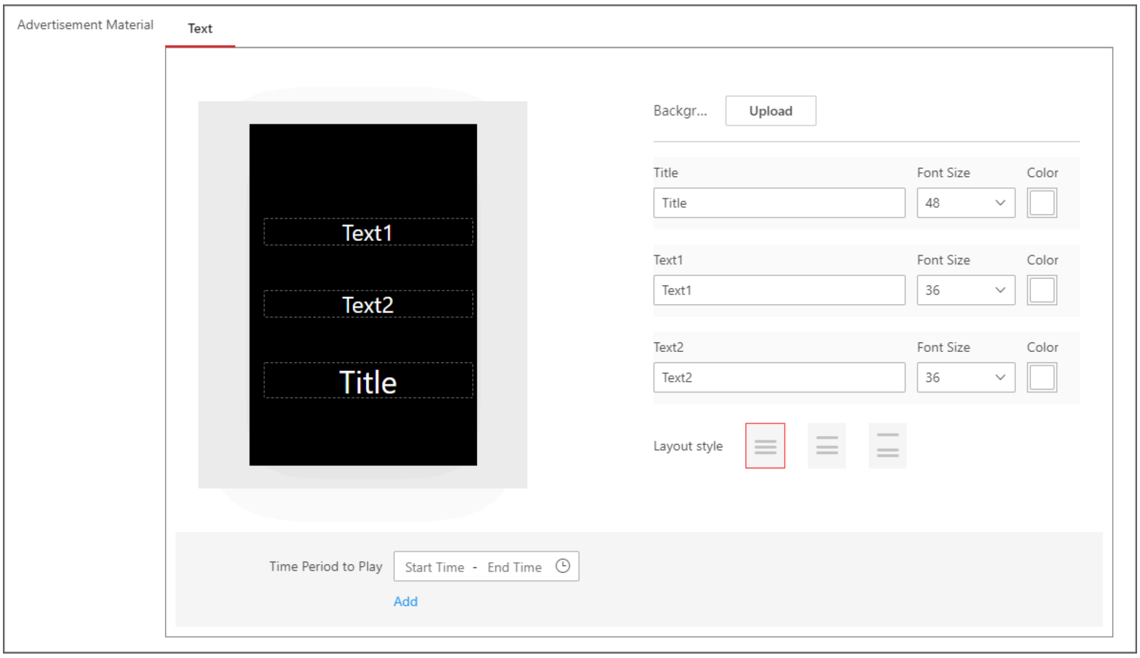


Figure 20-7 Add Text in Advertisement

4. The playing schedules set for the picture(s), video(s), and text(s) in the advertisement will be displayed by different color blocks.
5. Switch on **Sleep**, and set the sleep duration (from 20 to 60 seconds).
6. Click **Apply**.
7. **Optional:** Perform the following operations.

Filter Advertisement	Click and set filter conditions such as device name, and then click **Filter** to filter the target advertisement.
Delete Advertisement	Select one or multiple advertisements in the list and click **Clear Advertisements** to delete the advertisements. Also, you can click **Delete All** to delete all of the advertisements.
Copy Advertisement	Select one advertisement in the list, click in the operation column to copy the current advertisement to other devices.
View Details	Select one advertisement in the list, click to view the details of applying progress.

Add an Authentication Password

You can set an authentication password for a person so that the person with access level can access via entering the authentication password on the devices.

Before You Start

Add the access points to different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the upper-left corner of the Home page, click ▦ → **Passing Management → Access Control → Access Control Application → Authentication Password** .
2. Click **Add**, and select persons.
3. If there are cards without PIN, select **Auto Generate** or **Enter Manually** to automatically generate or enter an authentication password manually.

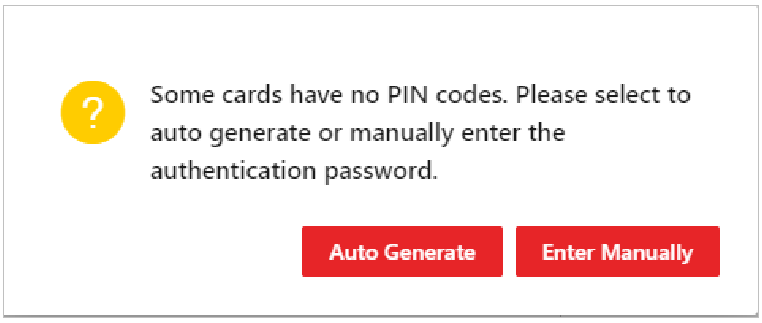


Figure 20-8 The Prompt

4. **Optional:** Enter the authentication password for persons whose authentication password is empty, or check persons and then click **Auto Generate Authentication Password**.
5. Select devices in the following list.

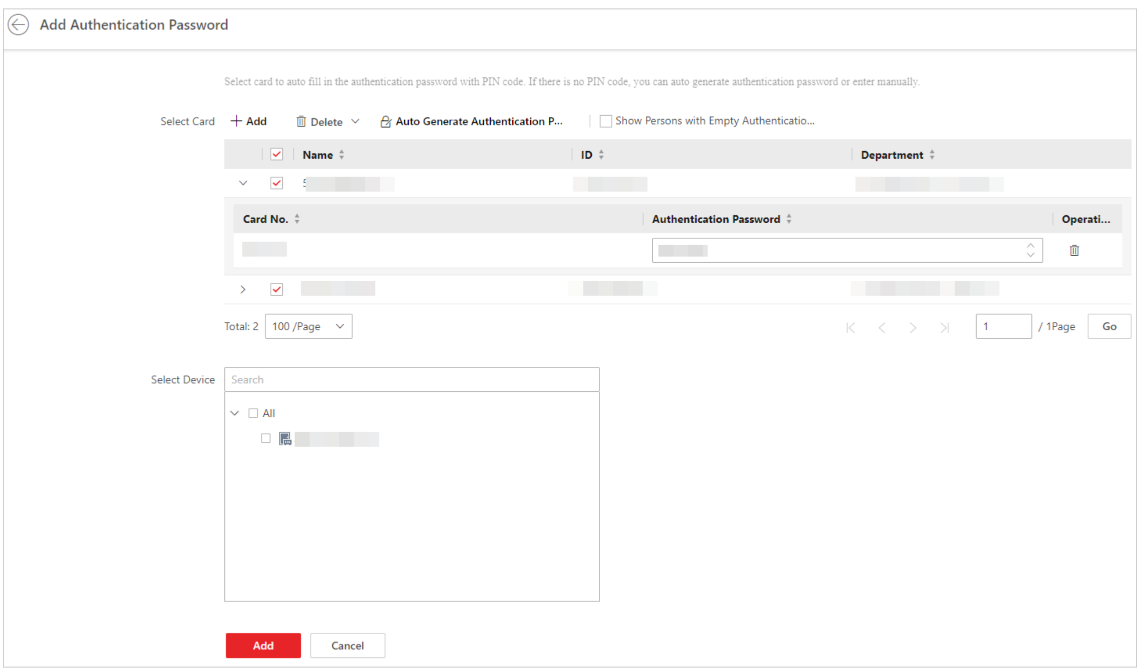


Figure 20-9 Add Authentication Password Page

6. Click **Add**.

   The platform will automatically apply the authentication passwords to the selected devices, and the applying progress will be displayed.

7. **Optional:** Check persons and click **Batch Edit Linked Devices** to batch add or delete devices they can access via authentication password.

20.4.8 Access Control Test

HikCentral Professional provides **Access Control Test**. It is a tool through which you can test whether the configurations about access control (such as persons' credentials and access levels for access control and video intercom) are set correctly and completely and whether the devices are running properly.

In the top left corner of the Home page, click ▦ → **Passing Management** → **Access Control** → **Troubleshooting** .

Check Credential Status

Select the **Credential Status** tab to view the status of the added credentials.

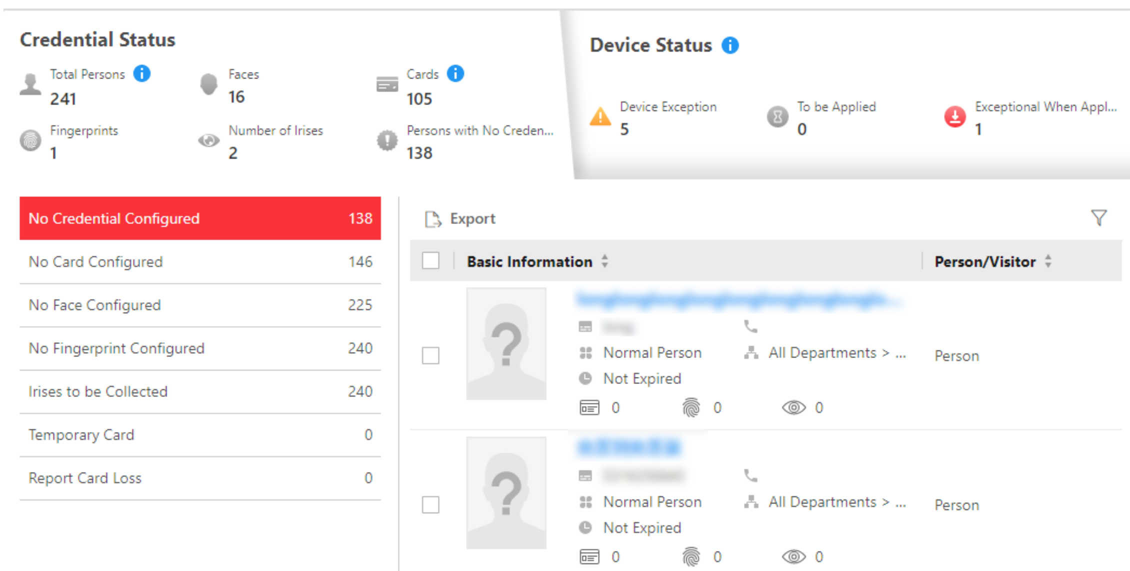


Figure 20-10 Credential Status

There are 6 types of exceptions on credential settings in the system. The number next to each exception type indicates the number of persons whose credential settings are abnormal.
Click each exception type to view the information about the persons with exceptions.
You can click the person's name to edit the credentials if necessary.

Check Device Status

Select the **Device Status** tab to view the status of the devices (including access control devices, elevator control devices, and video intercom devices). You can check person information and credential information that are already applied to the devices, configured in the system, fails to be applied, and check information of persons to be applied to the devices.

Note

Only the status of the devices which have been configured with access levels are shown.

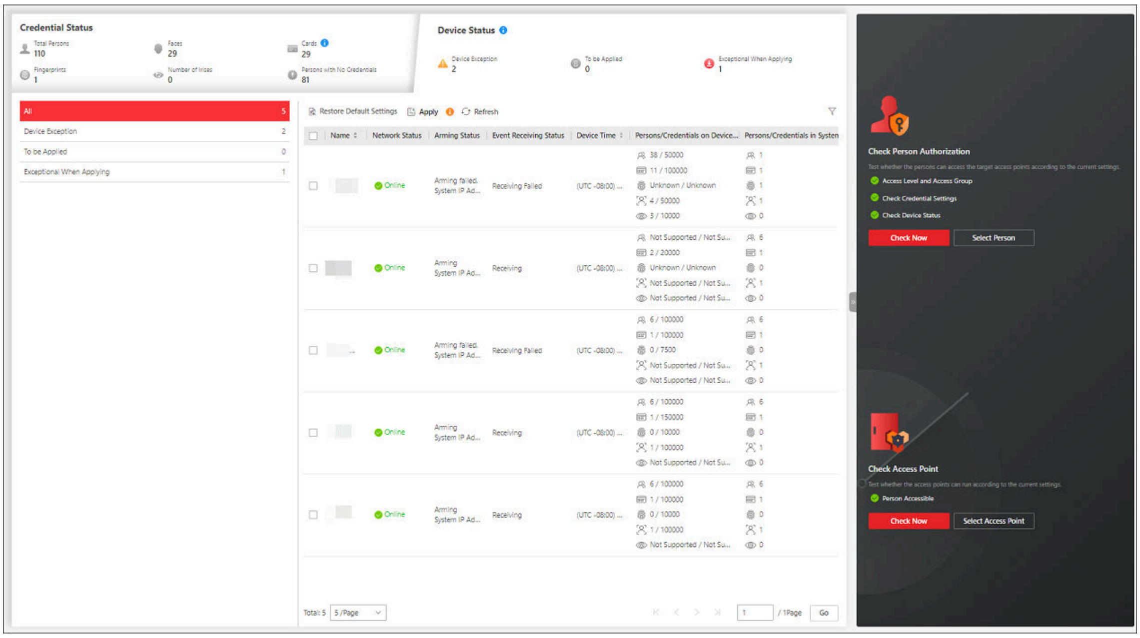


Figure 20-11 Device Status

Click each exception type to view the information about the persons with exceptions.
You can select the devices and click the following buttons to solve device issues.

Restore Default Settings	Restore the settings on the devices to the default value.
Apply	Apply person information and credential settings to these devices again.
Refresh	Refresh the list to get the latest device status.

Check Authorization Settings of Persons

You can check the authorization settings (such as access levels and access group settings, credential settings, and applying status) of specific persons in the system. This function helps you to test whether the persons can access the target access points according to the current settings.

Click  to expand the side panel.

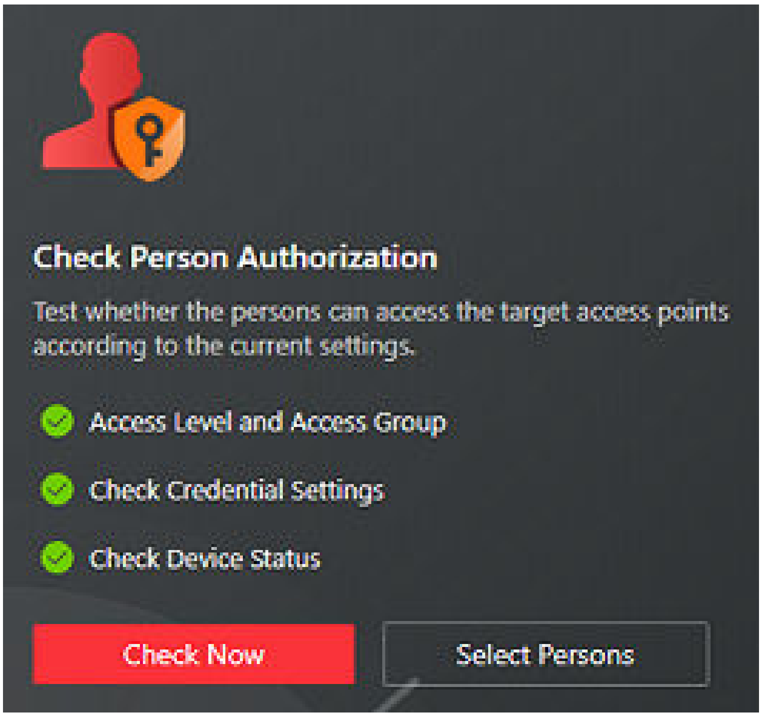


Figure 20-12 Check Authorization Settings

In the **Check Person Authorization** section, select the item(s) you want to check.
Click **Check Now** to test the authorization settings of all existing persons.
Or click **Select Persons** to select the persons you want to test and then click **Check Now** to test the authorization settings of the selected persons.

Check Access Point Settings

You can test whether the persons can access the access points according to the settings in the system.

Click  to expand the side panel.

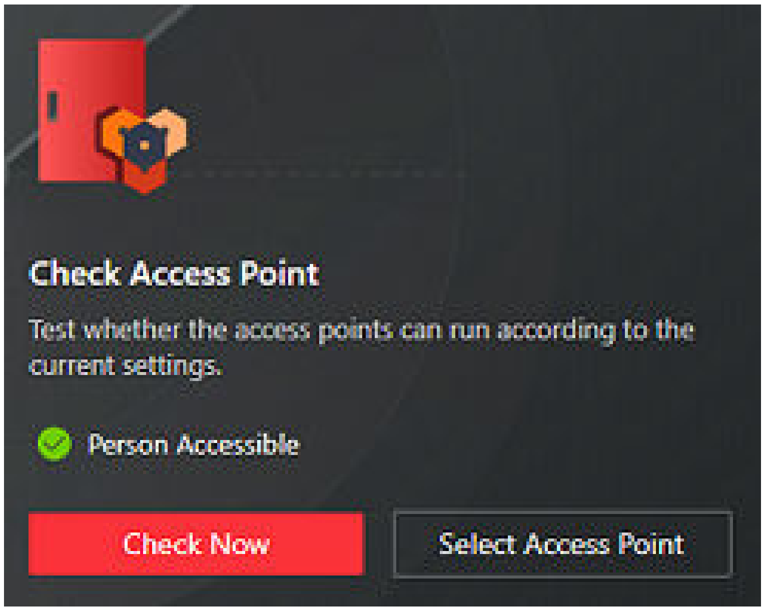


Figure 20-13 Check Access Point Settings

In the **Check Access Point** section, select the item(s) you want to check.
Click **Check Now** to test the settings of all existing access points in the system.
Or click **Select Access Points** to select the access points you want to test and then click **Check Now** to test the settings of the selected access points.

Note

The access points which are not added to any access levels will not be checked.

20.5 Real Time Monitoring

With emergency operation group, you can control access point status in a batch when an emergency happens. For example, after grouping the doors of a school's main entrances and exits into one emergency operation group, school's security personnel can lock down the doors in the group, so that no one can enter or leave the school except for maintenance and high-level admins. This function can also block out teachers, custodians, students, etc.

Note

Only the users with Administrator or Operator role can control all access points in a batch.

- Make sure you have grouped doors into an emergency operation group.
- Only the users with Administrator or Operator role can control all doors in a batch.

On the left, select **Real-Time Monitoring**.

You can control all or part of the access points in the selected site andarea according to your need. When the emergency is over, you can restore the status to Access with Credential.

On the top right, click [icon] to select a site and area.

20.5.1 Start Live View of Access Control / Elevator Control Devices

For access control devices with cameras installed inside or linked outside, and elevator control devices linked with cameras, you can start live view of these devices.

Before You Start

Make sure you have added the devices to the platform.

Steps

1. In the top left corner of the Home page, select [icon] → **Passing Management** → **Access Control** → **Real-Time Monitoring** .
2. Click a device and select **Live View**.

   The live view window of the device will be displayed on the right.

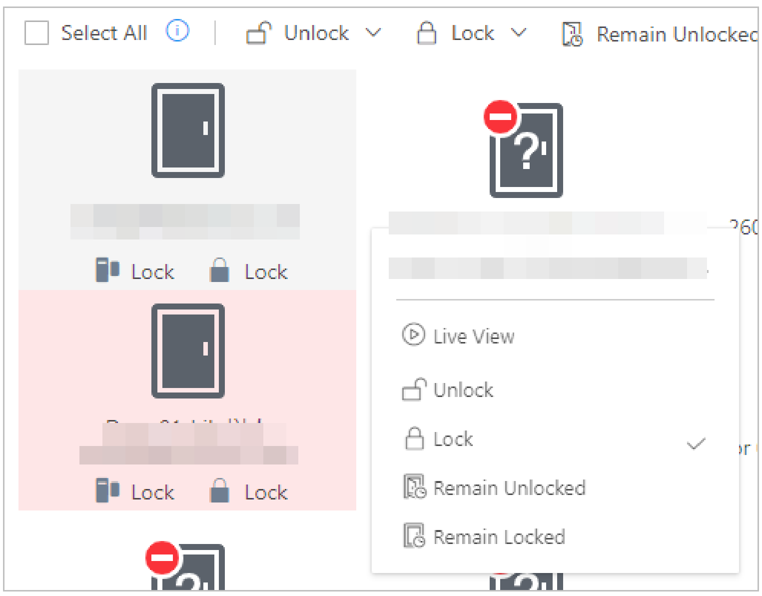


Figure 20-14 Real-Time Monitoring Page

3. Hover the cursor on the live view window to show the tool bar at the bottom. You can click different buttons according to your need.

   Example

   You can click [icon] to start two-way audio with persons by the device.

20.5.2 View Real-Time Access Event

In the Access Control module, you can view events triggered by doors and elevators. You can also control door and elevator status according to the event details, search for more event information, and so on.

On the left, select **Real-Time Monitoring**.

Select the site and area that you want to view the access events. Real-time access events are displayed at the bottom of the page.

Search Device Records	Click in the Operation column to go to the Device Recorded Data Retrieval page to search for records by customizing search conditions.
Filter Events	You can filter the real-time events by setting conditions according to record types and event source. Click to set conditions.
Custom Column	Click to customize the columns to be displayed.
Clear Events	Click to clear all events in the list.
View Details of Latest Access Record	On the lower-right corner of this page, check **Auto Update Record** to display the person information contained in the newest access record. If you uncheck the **Auto Update Record**, the platform will display the person information contained in the historical access records. The platform supports hiding the window.

20.5.3 Door Control

You can change the status of all doors in a site or doors in specific emergency operation groups to locked, unlocked, remaining locked, or remaining unlocked.

Note

Make sure you have grouped doors into an emergency operation group. See details in ***Add a Batch Locking and Unlocking Group*** .

On the left navigation bar, select **Real-Time Monitoring**.

Control all or part of the doors in the current site.

Unlock

When a door is locked, if you unlock the door, it will be unlocked. When open duration is over, the door will be locked again automatically.

Click **Unlock → All** to unlock all doors in the current site.

Click **Unlock → Part** and select the emergency operation groups you want to unlock. Click **OK** to unlock the doors in the selected emergency operation groups.

Note

For details about setting the door's open duration, see ***Edit Door for Current Site*** .

Lock

When the door is unlocked, if you lock the door, it will be closed and locked. The person who has the access permission can access the door with credentials.

Click **Lock → All** to lock all doors in the current site.

Click **Lock → Part** and select the emergency operation groups that you want to lock. Click **OK** to lock the doors in the selected emergency operation groups.

Remain Unlocked

Doors will be unlocked. All persons can access the door with no credentials required. This function is used when an emergency happens and all people are required to leave as quickly as possible, such as in a fire escape.

Click **Remain Unlocked → All** and all doors in the current site will remain unlocked.

Click **Remain Unlocked → Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain unlocked.

Remain Locked

Door will be closed and locked. No person, except for the users with super access permission, can access the door even with authorized credentials. This function is applicable for situations such as preventing unwanted persons in the building from getting away.

Click **Remain Locked → All** to lock down all the doors in the site.

Click **Remain Locked → Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain locked.

20.5.4 Floor Control

You can change the status of all floors in a site or floors in specific emergency operation groups to temporary access, access with credential, free access, or access forbidden.

Note

Make sure you have grouped floors into an emergency operation group.

On the left navigation bar, select **Real-Time Monitoring**.

Control all or part of floors in the current site.

Temporary Access

During the temporary access time, persons can access this floor with no credentials required. After the access time, the floor will recover to Access with Credential status.

Click **Unlock / Temporary Access → All** to set all the floors in the current site to Temporary Access.

Click **Unlock / Temporary Access → Part** and select one or more emergency operation groups to set all floors in the group(s) to Temporary Access.

For details about setting the temporary access duration, see ***Edit Elevator for Current Site*** .

Access with Credential

Person who has the access permission can access this floor with credentials.

Click **Lock / Access with Credential → All** to set all the floors in the current site to Access with Credential.

Click **Lock / Access with Credential → Part** and select one or more emergency operation groups to set all the floors in the group(s) to Access with Credential.

Free Access

All persons can access this floor with no credentials required.

Click **Remain Unlocked / Free Access → All** to set all floors in the current site to Free Access.

Click **Remain Unlocked / Free Access → Part** and select one or more emergency operation groups to set all floors in the group(s) to Free Access.

Access Forbidden

No person, except the users with super access permission, can access this floor even with authorized credentials. This function is applicable for situations such as preventing unauthorized persons in the building from getting away.

Click **Remain Locked / Access Forbidden → All** to set all floors in the current site to Access Forbidden.

Click **Remain Locked / Access Forbidden → Part** and select one or more emergency operation groups to set all floors in the group(s) to Access Forbidden.

20.6 Subscribe to Device and Access Events

You can subscribe to device events and access events, so that when these events occur, you can see the real-time event records via the Web Client and Mobile Client.

Follow the steps to enable the subscription to device and access events.

Steps

1. In the top left corner of the Home page, select → **Passing Management → Access Control → Basic Configuration → Device Event Subscription** .
2. Select an event category from **Device Event**, **Normal Access Event**, and **Abnormal Access Event**.
3. Switch on the event types to subscribe to these events.

4. **Optional:** Switch off the event types whose real-time event records you do not want to receive.

Note

If you switch off an event type, the Web Client and Mobile Client will no longer receive real-time event records of the event. However, you can still search for the device/access records via the Web Client. For details, see ***Search for Person Authentication Records*** and ***Search for Device Logs*** .

5. Click **Save** to save the settings.

What to do next

View the real-time event records of the device and access events that you subscribe to. For details, see ***View Real-Time Access Event*** .

20.7 Set User to Receive Access Control Calls

You can specify users to receive calls from the access control devices on the Control Client, and then the users can remotely perform the access control, such as remotely open door.

In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Basic Configuration** → **Call Recipient Settings** .

Note

If the Video Intercom module is enabled, this page will be displayed in the Video Intercom page.

Click **Add** to select user(s) to receive access control calls on the Control Client.

20.8 Synchronize Access Records to System Regularly

Access records stored in devices can be synchronized to the system for central management. You can specify a fixed time in order to automatically synchronize access records from devices to the system at the specified time every day.

Click → **Passing Management** → **Access Control** → **Basic Configuration** → **General** .

In the Synchronize Records (Scheduled) area, switch on **Synchronize (Scheduled)**, set a fixed time, and click **Save** to synchronize access records from the devices to the system regularly.

20.9 Enable Open Door via Bluetooth

You can enable Open Door via Bluetooth, select a door opening mode, and set the validity of offline locking.

Select **Basic Configuration** → **General** on the left.

In the **Open Door via Bluetooth** area, select the door opening mode as **Open Door by Rotating Smart Phone** and **Open Door Manually**. In the Offline Unlocking area, select the validity of offline unlocking.

20.10 Data Search

On the Search page, you can search for person authentication records, data recorded on devices, and perform final authentication counting.

On the left, select **Search**.

20.10.1 Search for Person Authentication Records

You can search for persons' authentication records triggered on specified access points by setting search conditions. For example, if you select specific access points and set the event type to access denied by card, you can get all access denied events (accessing by swiping a card) triggered on the access points.

Before You Start

Make sure you have configured the access point event. For details, refer to ***Add Normal Event and Alarm*** .

Steps

1. **Optional:** On the Person Authentication Record page, import person authentication records to the system.
   - Import from the device(s).
     a. Click **Import Event → Import from Device** to enter the Import from Device page.
     b. Select the device(s) from the device list.
     c. (Optional) Switch on **Specified Time Range** and set the start time and end time to import records generated in the specified time period.

        Note

        - If the device has uploaded records to the system before, switching on **Specified Time Range** is not required and records during the past 7 days of the selected device(s) will be imported by default if no time range is specified.
        - If the device has never uploaded any record to the system before, you must switch on **Specified Time Range** for importing records from the selected device(s).

     d. Click **OK** to start importing.

     A window will pop up to display the importing progress and the failure details.
   - Import from the file which is exported from the device.
     a. Click **Import Event → Import from File** to enter the Import from File page.
     b. Click to select the file to be imported.

Note

Only the encrypted file can be imported.

c. Enter the password in the **Password** field.
d. Click **OK**.

2. In the **Time** drop-down list, select the time during which the records are generated.
3. Select a site from the Site drop-down list.
4. **Optional:** In the **Access Point** area, click , select the area on the left list, and select door(s) or elevator(s), or select all on the right list.
5. **Optional:** In the **Event Type** area, click to select the event type(s).
6. In the **Authentication Result** drop-down list, select an access result type to quickly filter access granted records or access denied records.
7. Set the searching mode.
   - a. Select as the searching mode.
     b. Select **Select Person** or **Fuzzy Matching** as the searching mode.

     Select Person

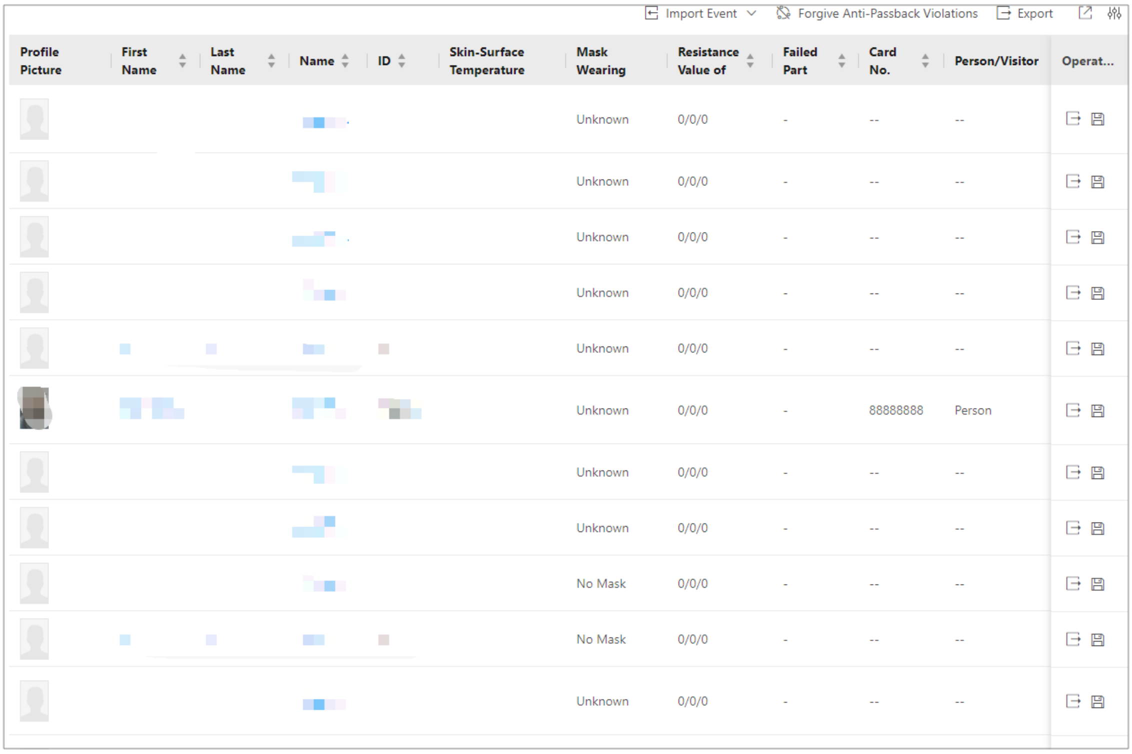
     Click to select the person(s)

     Fuzzy Matching

     Enter a keyword to search for persons whose name contains the keyword.

     c. Click **Add** to select the person(s), or enter the keywords of the person's name for fuzzy matching.
   - a. Select **Card No.** as the search mode.
     b. Enter the card number.
8. **Optional:** Switch on **Temperature Status** and select **Normal** or **Abnormal**.
9. **Optional:** Switch on **Mask Wearing Status** and select **Wearing Mask** or **No Mask**.
10. Click **Search**.

    Matched records are listed on the right.



Profile Picture	First Name	Last Name	Name	ID	Skin-Surface Temperature	Mask Wearing	Resistance Value of	Failed Part	Card No.	Person/Visitor	Operat...
						Unknown	0/0/0	-	--	--	
						Unknown	0/0/0	-	--	--	
						Unknown	0/0/0	-	--	--	
						Unknown	0/0/0	-	--	--	
						Unknown	0/0/0	-	--	--	
						Unknown	0/0/0	-	88888888	Person	
						Unknown	0/0/0	-	--	--	
						Unknown	0/0/0	-	--	--	
						No Mask	0/0/0	-	--	--	
						No Mask	0/0/0	-	--	--	
						Unknown	0/0/0	-	--	--	

Figure 20-15 Person Authentication Records

11. **Optional:** Perform the following operations after searching for records.

View Record Details	Click the person name in the Full Name column to view the record details, such as person information, and access information.
Forgive Anti-Passback Violation	When a person attempts to use a card without following the anti-passback rule, the access will be denied. This is called "Anti-Passback Violation". When the anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven. You can click **Forgive Anti-Passback** on the top to forgive all the anti-passback violation events in the search results.
Export Single Record	Click in the Operation column to save a record as an Excel or CSV file on your PC, including the event details, the person information, person profile, recorded video file (if configured), etc.
Export All Searched Records	Click **Export** in the upper-right corner to save the searched record details in your PC. You can select the file format as an Excel, PDF or a CSV file, and select items to export.
Save a Record As Evidence	Click to save the record to the evidence management center.

Note

- The password is required for security.
- You can view the downloading progress in the Download Center when exporting the data.

20.10.2 Search for Device Logs

The logs can be events/alarms triggered by abnormal events detected by devices and those triggered by devices (such as device faults). You can search for the logs in different dimensions according to your needs.

Steps

1. On the top left of the Device Log page, select a time range for searching.
2. Select a site from the Site drop-down list.
3. Switch on the resource types where you want to search for records.

   Access Point(s)

   Access points include doors of access control devices and video intercom devices, and floors of elevator control devices. The logs can be access records, operation records, and alarms triggered by human behaviors.

   Device

   Devices include access control devices and video intercom devices. The logs recorded in these devices can cover all events triggered by devices (such as device faults).

   Alarm Input

   The alarm inputs included in devices. The logs are arming status changes.
4. Select the event source(s) and event type(s) for each switched-on resource type.
5. Click **Search**.

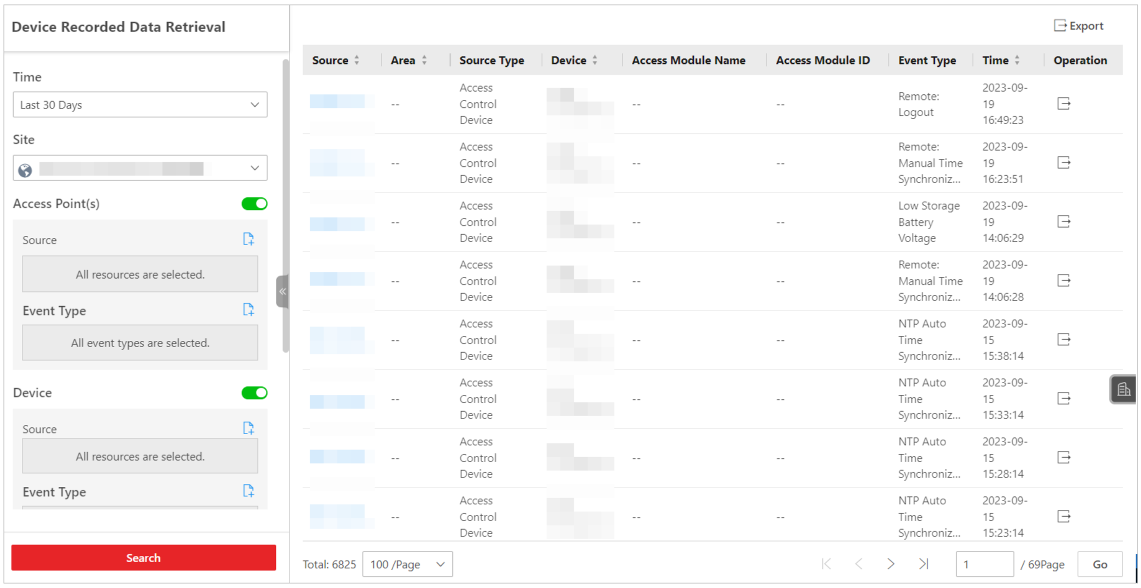


Figure 20-16 Device Recorded Data Retrieval

6. **Optional:** Perform further operations on the searched records.

View Record Details	Click the device name in the Source column to view the record details, such as the device name and record type.
Export Single Record	Click in the Operation column to save the record to the local PC as a CSV file.
Export All Searched Records	Click **Export** to save all the searched records to the local PC as an Excel, PDF, or a CSV file.

Note

- The password is required for security.
- You can view the downloading progress in the Download Center when exporting the data.

20.10.3 View Final Authentication Statistics

The system can count individuals in a region by grouping doors and using final authentication records. This allows you to see who has been granted access and how many people are still in the area. The function is applicable for certain emergency scene. For example, during a fire escape, all people are required to exit the region.

Before You Start

Make sure you have added final authentication counting groups to group the doors. See ***Add a Final Authentication Counting Group*** .

Steps

1. On the page of Final Authentication Counting, select a time range for the counting.

2. In the **Source** list, select a final authentication group.
3. In the **Entry & Exit Counting Type** drop-down list, select the type of persons you want to search.

   All Persons

   All the entering and exiting access records in the last 24 hours will be listed.

   People Stayed

   Persons who are still staying in the region will be listed. The system filters the persons whose entering record is found but exiting record is not found.

   People Exited

   Persons who entered and exited the region afterward will be listed.
4. Click **Search**.

   All matched records will be listed, showing information such as person details, location of last access, etc.
5. **Optional:** Perform further operations after searching.

View Event Details	Click the person name in the Name column to view the record details, including the recorded video of the access point's related camera (if configured), person information, and access information.
Export Single Record	Click in the Operation column to download the record, including the person information, person profile, phone number, location of last access, etc.
Export All Searched Records	Click **Export** in the upper-right corner to export the searched access control events details (including the person information, person profile, phone number, location of last access, etc.).

Note

- The password is required for security.
- Up to 100,000 records can be exported each time.
- You can view the downloading progress in the Download Center when exporting the data.

Chapter 21 Visitor Management

The system provides an entire process for visitor management from reservation to check-out. You can group visitors to different visitor groups for convenient management, determine the areas where the visitors can access, and assign visitors access credentials like visitor passes.

On the Web Client, you can add visitor information to the system and assign access levels to the visitors to define which doors and which floors the visitors can access with credentials.

21.1 Visitor Information Overview

The Visitor Information Overview page shows the wizard for visitor management and the chart of the visit trend today.

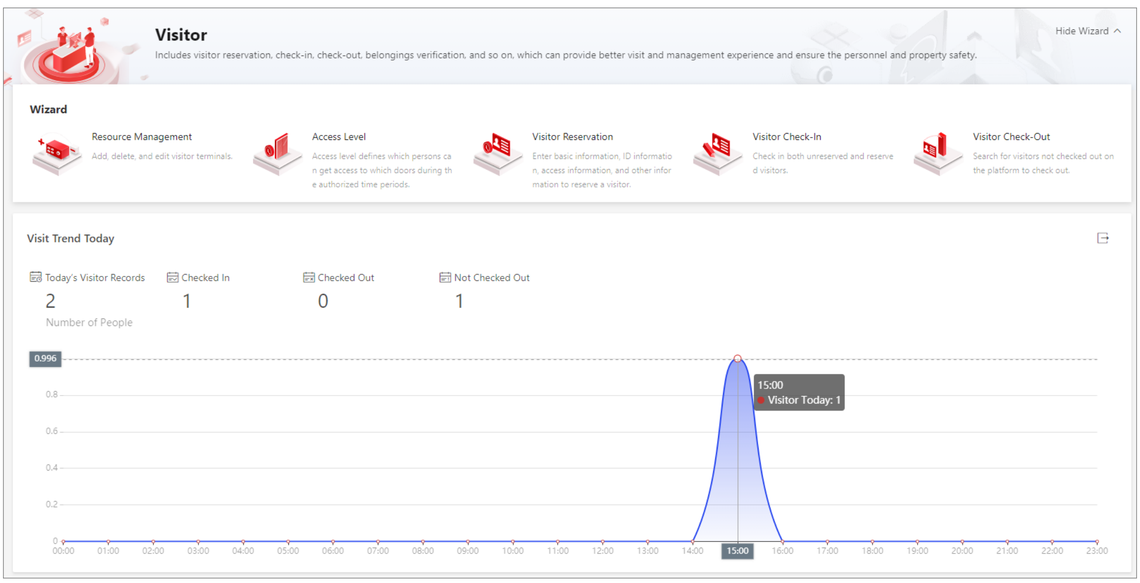


Figure 21-1 Visitor Information Overview

Wizard

The wizard shows you the entire process for visitor management, including the resource management, access level management, visitor reservation, visitor check-in, and visitor check-out. Move your cursor to each section and click to go to the corresponding page for configurations and operations. For example, you can move your cursor to the Resource Management section and click to go to the page for managing visitor terminals.

Visit Trend Today

You can view the variation trend of the number of visitors on the current day through a line chart. Also, you can view the numbers of today's visitor records, checked-in visitors, checked-out visitors, and not-checked-out visitors.

On the line chart, you can perform the following operations:

- Move the cursor to a specific point on the chart to view the number of visitors at the corresponding time.
- Click on the right side to export the chart to the local PC as a file in the format of PDF, PNG, or JPG.

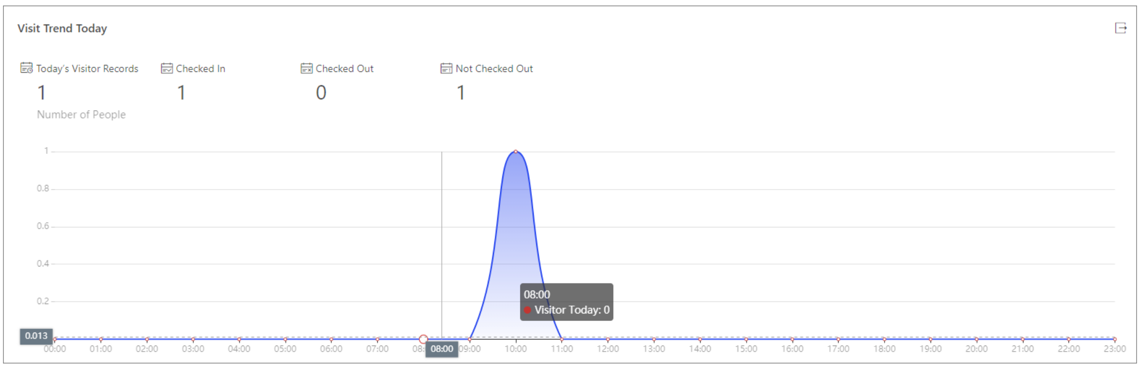


Figure 21-2 Visit Trend Today

21.2 Flow Chart of Visitor Management

The flow chart below shows the process of visitor settings management.

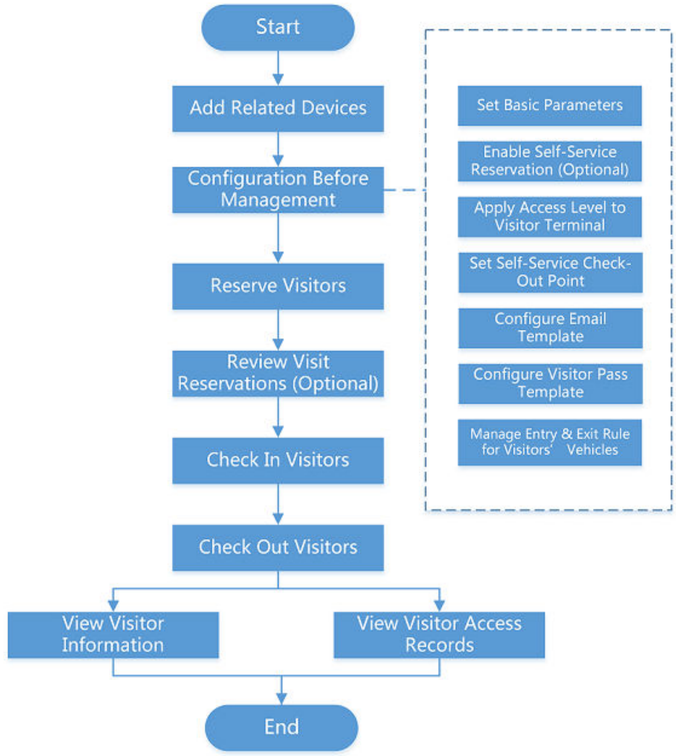


Figure 21-3 Flow Chart of Visitor Management

Table 21-1 Flow Chart Description

Procedure	Description
Add Related Devices	Add devices used for visitor reservation, check-in, check-out, authentication, etc. See ***Manage Visitor Terminals*** and ***Manage Elevator Control Device*** for details.
Configuration Before Visitor Management	Before any operations in the visitor system, you need to set the parameters according to actual situation such as setting basic parameters to define the scenario for the visiting process, managing visitor types, adding access levels for visitors, etc. See ***Configurations Before Visitor Management*** for details.
Manage Entry & Exit Rule for Visitors' Vehicles	Register license plate number of the visitors' vehicles to allow the system to control the barrier to open when capture unit of parking lot detect license plate number. See ***Manage Entry & Exit Rule for Visitors' Vehicles*** .
Reserve the Visitors	Before visiting, visitors can make a reservation. The Administrator can make a reservation for the visitors by entering the visitor and host information on the platform. Visitors can also reserve by

Procedure	Description
	themselves. After self-reservation, the Administrator should review the visitor information to approve or disapprove the reservation. See ***Visitor Reservation*** for details.
Visitor Check-In	The platform supports checking in visitors both with or without a reservation. See ***Check In a Visitor Without Reservation*** and ***Check In a Reserved Visitor*** for details.
Visitor Check-Out	You should check out for the visitor before him/her leaves, or let visitors check out at self-service check-out point. After checking out, the visitor's access information will expire. See ***Visitor Check-Out*** for details.
View and Delete Visitors	View all checked-in visitors (including those who have checked out) in the visitor list and perform other operations such as deleting visitors. See ***View Visitor Information*** for details.
Check Visitor Records	Filter and check visitor records. See ***Check Visitor Access Records*** .

21.3 Configurations Before Visitor Management

Before any operations in the visitor system, you need to set the parameters according to actual situation such as setting basic parameters to define the scenario for the visiting process, managing visitor types, adding access levels for visitors, etc.

21.3.1 Add a Visitor Group

You can add visitor groups to categorize different visitors for convenient management. For example, you can add a business group for visitors coming for business communication and add a tour group for touring visitors. Moreover, you can control other users' access to any visitor group to ensure the security of visitor data if you have corresponding configuration permissions.

Steps

1. On the top left of the Web Client, select ⊞ → **Passing Management → Visitor → Visitor Information** .
2. Click + to open the Group Name window.
3. Create a visitor group name, and then click **Add** to add a visitor group.

Note

System administrators or other roles who have the permission to manage roles can define which HikCentral Professional users have permission to access the visitor group.

4. **Optional:** Perform the following operations after adding the visitor group.

Edit Visitor Group	Click to change the information about the visitor group.
Delete Visitor Group	Select a visitor group and click to delete it.

21.3.2 Add Access Level for Visitors

An access level contains access points that are accessible during a certain time period. If you select an access level for a visitor for check-in and apply the settings to devices, the visitor can access the access points during the specified time period with credentials.

Before You Start

Make sure you have added at least one access level in the Access Control module.

Steps

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Access Level** .
2. Click **Add**.
3. Select existing access levels.
4. Click **Add**.

   The added access levels will be displayed in the access level list. You can view its accessible access points and time periods.
5. **Optional:** Perform the following operations after adding access levels.

View Access Schedule Template Details	Click in the Access Schedule Template column to view when the access point is accessible for the visitor.
View Access Point Details	Click in the Access Point column to view the name of related access points.
Set Default Access Level	Select an added access level and switch on the button in the Default Access Level column. The default access level will be automatically selected when a visitor makes reservation for themselves, under the precondition that you have enabled the Self-Service Reservation feature (see ***Set Review and Self-Service Reservation Parameters***). The default access level will also be automatically selected when you reserve for visitors again and check in visitors again on the Visitor Information page (see ***View Visitor Information***).
Delete Access Levels for Visitors	Select access levels and click **Delete** to delete the selected access level. Or click → **Delete All** to delete all the access levels.

What to do next

Apply visitor's access levels to the visitor terminals connected to the platform. See ***Manually Apply Visitors' Access Level Settings to Visitor Terminals*** for details.

21.3.3 Manually Apply Visitors' Access Level Settings to Visitor Terminals

If you have added visitors to an access group, or deleted/edited visitors of an access group, or changed access levels of an access group, you have changed the access group's settings. In these cases, you should apply the changes to the connected visitor terminals to make the changes take effect.

Before You Start

- Make sure you have added access levels for visitors. See ***Add Access Level for Visitors*** for details.
- Make sure you have added the visitor terminal to the platform. See ***Manage Visitor Terminals*** for details.

Steps

1. On the top left of the Web Client, select → **Passing Management → Visitor → Basic Configuration → Access Level** .
2. Select the access levels that need to be applied to visitor terminals.

   Note

   You can select up to 10 access levels that need to be applied.
3. Click **Apply Access Level to Visitor Terminal** to apply the selected access levels to the visitor terminals.

   If the applying process failed, will be displayed next to **Apply Access Level to Visitor Terminal**. In this case, you can move the cursor to it and then click **View** or **Apply Again** to view the failure details or apply the access levels again respectively.

21.3.4 Set Review and Self-Service Reservation Parameters

Self-service reservations refer to visit reservations made by visitors themselves. You can set whether to auto approve the reservations. You can also enable the Self-Service Reservation feature to get a QR code, which you can send to visitors to allow them to make visit reservations by scanning the QR code. In addition, you can set related parameters to ensure that self-service reservations meet the visitor management standards of your organization/company.

Steps

Note

Self-reserved visitors are only allowed to access the access points contained in the default access level for visitors. For details about setting the default access level, see ***Add Access Level for Visitors*** .

To configure a different access level for a visitor, you need to make a reservation for them. For details, see ***Reserve a Visitor*** .

1. On the top left of the Web Client, select ▦ → **Passing Management → Visitor → Basic Configuration → Review and Self-Service Reservation** .
2. **Optional:** Enable **Auto Approve Reservation**.

   If you enable this, visitor reservations will be approved automatically. If you disable this, visitor reservations need to be approved according to the configured approval flow. The configuration is only valid to the current users.

   If you disable this, see ***Review Visitor Reservations*** for details about how to review.
3. Enable **Self-Service Reservation**.

   The platform will generate a QR code. After downloading the QR code, you can print it or send it to the hosts or visitors who are going to reserve. The host can scan the QR code to reserve for the visitor, while the visitor can also scan the QR code to reserve if the visitor knows the visitor's person ID.

   Note

   QR codes generated by different users are different, and a user can only review the visitors reserved via the QR code the user generated, which allows different users to manage their own visitors independently.
4. **Optional:** Configure the following parameters.

   Face Quality Verification

   After the visitor uploads a profile picture by a cellphone, the selected device will automatically start checking the profile picture's quality. If the profile picture is not qualified, the visitor will be notified. Only when the uploaded profile picture is qualified can the visitor reserve successfully. Otherwise, the visitor information cannot be uploaded to the platform.

   Note

   To use this function properly, make sure you have added an access control device or video intercom device to the platform beforehand.

   Visitor Group

   Select a visitor group. After reserving successfully, the visitors will be added to the group. If you do not select, the visitor will be added to the default visitor group.

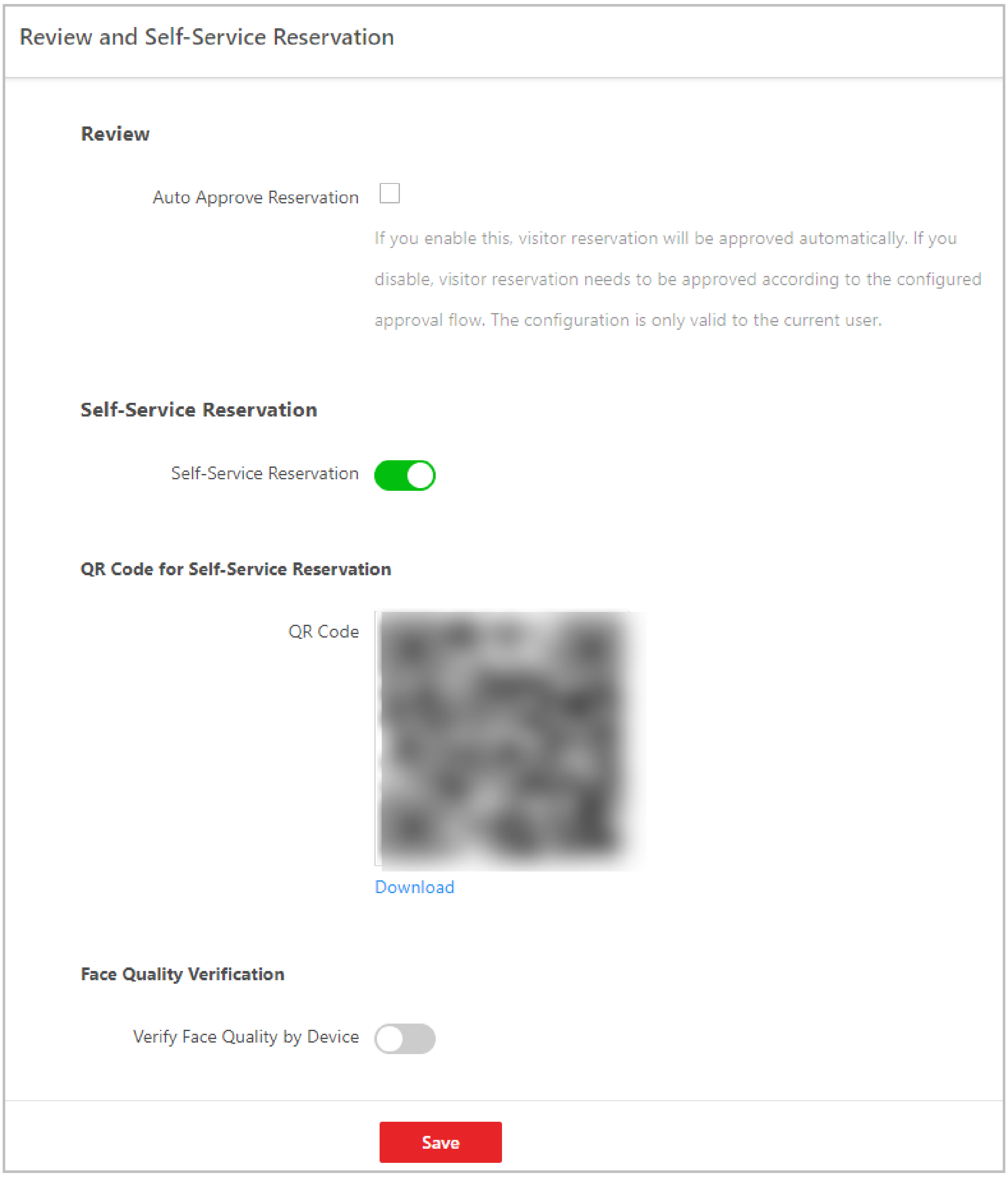


Figure 21-4 Review and Self-Service Reservation

5. Click **Save**.

Note

If the auto approval of visitor reservation has been disabled, you will be prompted to configure the approval flow. Click **Yes** to enter the Approval Flow page to configure a visitor approval flow.

21.3.5 Set Self-Service Check-Out Point

After setting self-service check-out points, visitors can check out by credentials at the self-service check-out points without the help of receptionists. If you have issued a card to a visitor when you check in the visitor, after checking out, the visitor should put the card in the place for card collection. The access permission granted via visitor cards, fingerprints, face pictures, and QR codes will expire automatically.

Before You Start

Make sure you have added at least one device that supports this function.

Steps

Note

This function needs to be supported by devices.

---

1. On the top left of the Web Client, select → **Passing Management → Visitor → Basic Configuration → Self-Service Check-Out Point** .
2. Click **Add** to show the resource list.

   Note

   You can enter a keyword of a door name in the searching bar to search for wanted doors.

   ---
3. Select one or more doors / card readers and click **Add**.

   Note

   - If there are two card readers related to one door, you can specify one for check-out, so the other one can be used for check-in.
   - After setting self-service check-out points, the visitors can check out at the points according to the assigned access levels by swiping cards or fingerprint/face authentication.

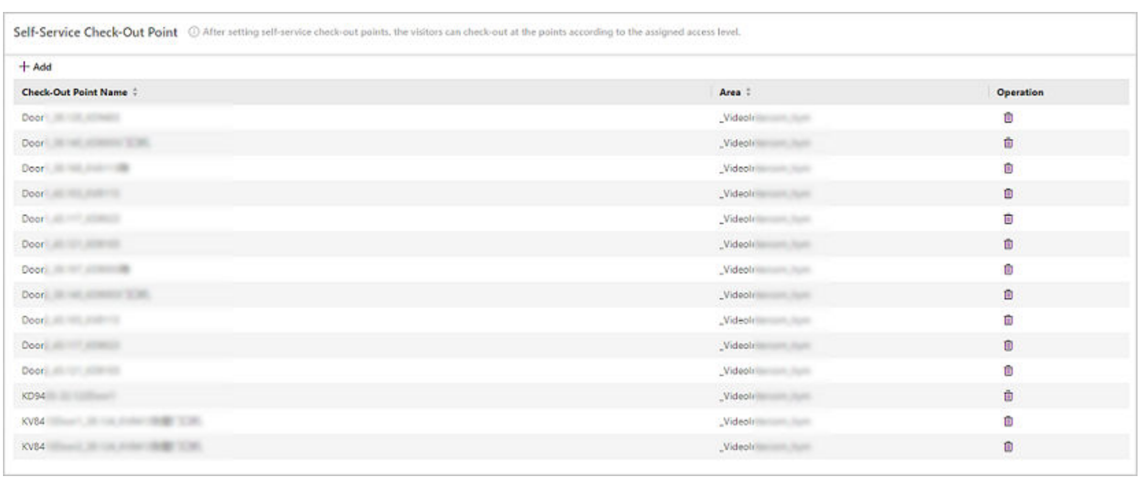


Figure 21-5 Set Self-Service Check-Out Point Page

4. **Optional:** Select a self-service check-out point and click to cancel setting the door as a self-service check-out point.

21.3.6 Add Visitor Receiving Template

You can set the receiving template (including the template type, recipient, and content) so that the platform can send emails or WhatsApp messages automatically to the recipient according to the predefined template.

Before You Start

Before adding the template, you should set the sender's email account first.

Steps

1. On the top left of the Web Client, select → **Passing Management → Visitor → Basic Configuration → Receiving Template** .
2. Click **Add**.
3. Enter the required parameters.

   Receiving Mode

   The platform sends emails or WhatsApp messages.

   Template Type

   The email type defines when the platform automatically sends a predefined email or WhatsApp message to the recipient.

   Recipient

   Set the type of the email recipient (visitor or host).

   Subject

   Enter the subject for the email template if required. You can also click the button in the lower part of the window to add the related information to the subject.

   Template Content

   Define the content to be sent. You can also click the buttons below **Content** to add the related information to the content.

   Note

   If you add the arrival time to the email subject or email content, and the email application (such as Outlook) and the platform are in different time zones, the displayed time period may have some deviations.

   Text on Button

   If required, define the text on the button for WhatsApp messages.
4. Finish adding the template.
   - Click **Add** to add the template and go back to the email template list page.
   - Click **Add and Continue** to add the template and continue to add other templates.

The email template will be displayed in the email template list.

21.3.7 Add Visitor Pass Template

The platform offers default receipt and card templates of visitor passes. If the default templates do not meet your needs, you can add a template to customize the style.

Add Receipt Visitor Pass Template

The platform offers a default receipt template that defines a default style. If the default style does not meet your needs, you can add a receipt template to customize the style.

Steps

1. On the top left of the Web Client, select ⊞ → **Passing Management → Visitor → Basic Configuration → Visitor Pass Template → Receipt Template** .
2. Click ＋ to enter the Create Receipt Template page.

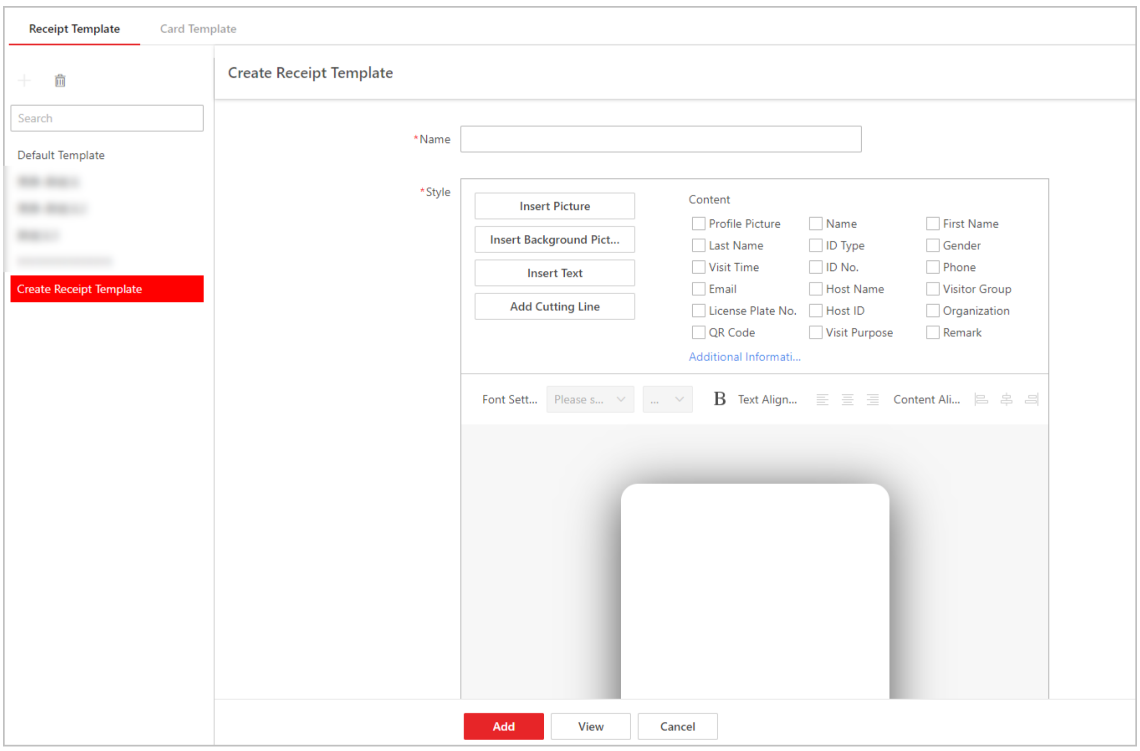


Figure 21-6 Create Receipt Template Page

3. Create a name for the receipt template.
4. Perform one or more of the following operations to add elements to the template.

Insert Background Picture	Click **Insert Background Picture** to select a picture from the local PC and set it as the background of the template.

Set Content	Check the check-box(es) to add the content element(s). Or click **Custom Information** and then select element(s) in the pop-up window to add them. **Note** Make sure you have set custom visitor attributes; otherwise, **Custom Information** will be unavailable. For details about setting custom visitor attributes, see ***Set Basic Parameters*** .
Insert Picture	Click **Insert Picture** to select a picture from the local PC and add it to the template.
Insert Text	Click **Insert Text** to add a text box to the template. You can set the font, font size, and text alignment for the entered text.
Add Cutting Line	Click **Add Cutting Line** to add a cutting line to the template.

5. Adjust positions of the added elements.

Manually Adjust Position	Drag an element to adjust its position.
Align Elements	Drag to select elements and then click , , or .
Adjust Position via Right-Click Menu	Right click an element and then click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down**.

6. **Optional:** Right click an element and then click **Delete** in the right-click menu.
7. **Optional:** Click **View** to preview the template.
8. Click **Add** to add the template.

   The added template will be displayed in the template list on the left.
9. **Optional:** Perform the following operations.

Edit a Template	Select a template from the template list to edit it.
Delete a Template	Select a template from the template list and then click .

Add Card Visitor Pass Template

The platform offers two default card templates (horizontal and vertical). If the default templates do not meet your needs, you can add a card template to customize the style.

Steps

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Basic Configuration** → **Visitor Pass Template** → **Card Template** .
2. Click + to enter the Create Card Template page.

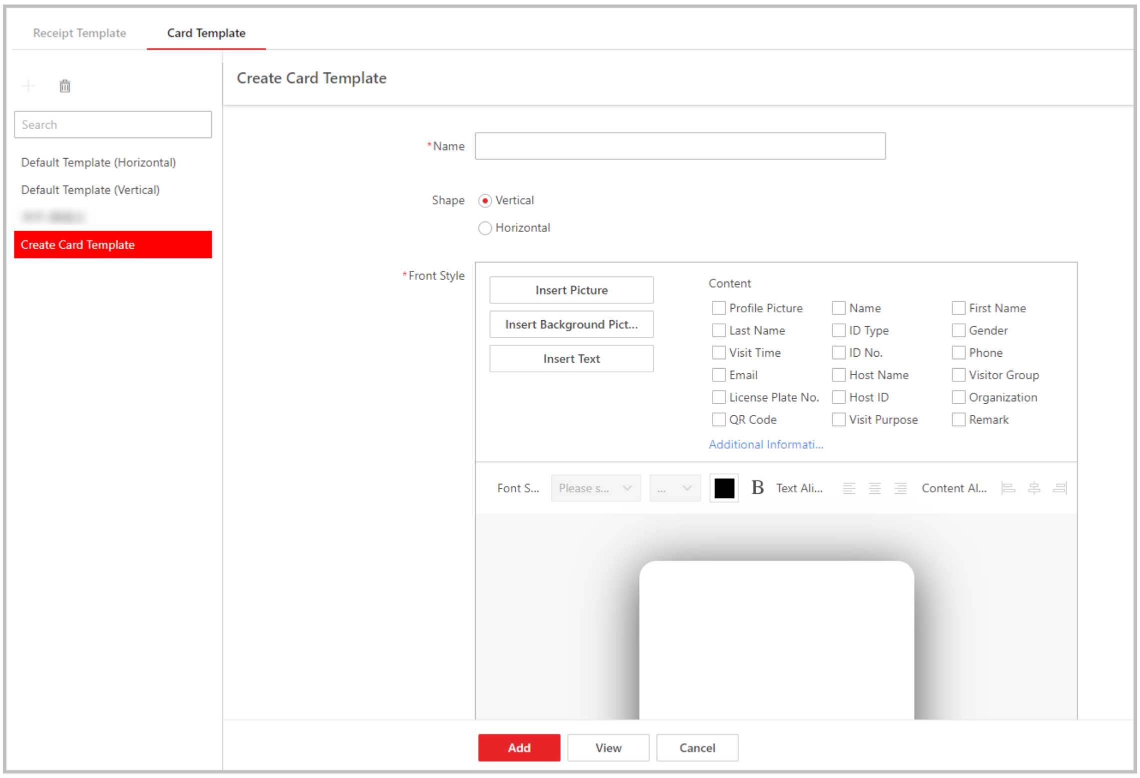


Figure 21-7 Create Card Template Page

3. Create a name for the card template.
4. Set the shape of the card template to **Vertical** or **Horizontal**.
5. Perform one or more of the following operations to add elements to the template in the Front Style section.

Insert Background Picture

Click **Insert Background Picture** to select a picture from the local PC and set it as the background of the template.

Set Content

Check the check-box(es) to add the content element(s). Or click **Custom Information** and then select element(s) in the pop-up window to add them.

Note

Make sure you have set custom visitor attributes; otherwise, **Custom Information** will be unavailable. For details about setting custom visitor attributes, see ***Set Basic Parameters*** .

Insert Picture

Click **Insert Picture** to select a picture from the local PC and add it to the template.

Insert Text

Click **Insert Text** to add a text box to the template.

You can set the font, font size, color, and text alignment for the entered text.

6. Adjust positions of the added elements.

Manually Adjust Position	Drag an element to adjust its position.
Align Elements	Drag to select elements and then click , , or .
Adjust Position via Right-Click Menu	Right click an element and then click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down**.

7. **Optional:** Right click an element and then click **Delete** in the right-click menu.
8. **Optional:** Set the back style.

Note

The operations are the same as that of the front style. You can refer to steps 5 to 7 when you set the back style.

9. **Optional:** Click **View** to preview the template.
10. Click **Add** to add the template.

    The added template will be displayed in the template list on the left.
11. **Optional:** Perform the following operations.

Edit a Template	Select a template from the template list to edit it.
Delete a Template	Select a template from the template list and then click .

21.3.8 Set Basic Parameters

To manage visitors in actual scenarios, you can set basic parameters such as Take Photo of Visitor's Belongings, Default Check-Out Time, Visiting Purpose, and Digits of Reservation Code.

Steps

Note

If you do not configure basic parameters, the platform will manage visitors according to the default settings.

1. On the top left of the Web Client, select → **Passing Management → Visitor → Basic Configuration → Basic Parameters** .
2. Configure the following parameters according to your needs.

   General Settings

   Take ID Photo as Visitor Profile Picture

   If enabled, the ID photo can be read via a connected passport reader and set as the visitor profile picture when you reserve for a visitor or check in a visitor without reservation. See ***Reserve a Visitor*** or ***Check In a Visitor Without Reservation*** for details.

Visit Purpose

You can define visiting purposes as options on the Reserve page. Click **Add** to add a new visiting purpose. You can also edit the name of an added visiting purpose, delete an added visiting purpose, or search for a visiting purpose.

Custom Visitor Attribute

Click **Add** to add custom visitor attributes. The added ones will be displayed as fields on the Reserve page and the Unreserved Visitor Check-In page.

You can set a custom visitor attribute as a **General Text**, **Number**, **Date**, or **Single Selection** field. For example, if you name a custom visitor attribute as ***Covid-19 Vaccination Date*** and set it as a **Date** field, it will be displayed on the Reserve page as shown in the figure below.

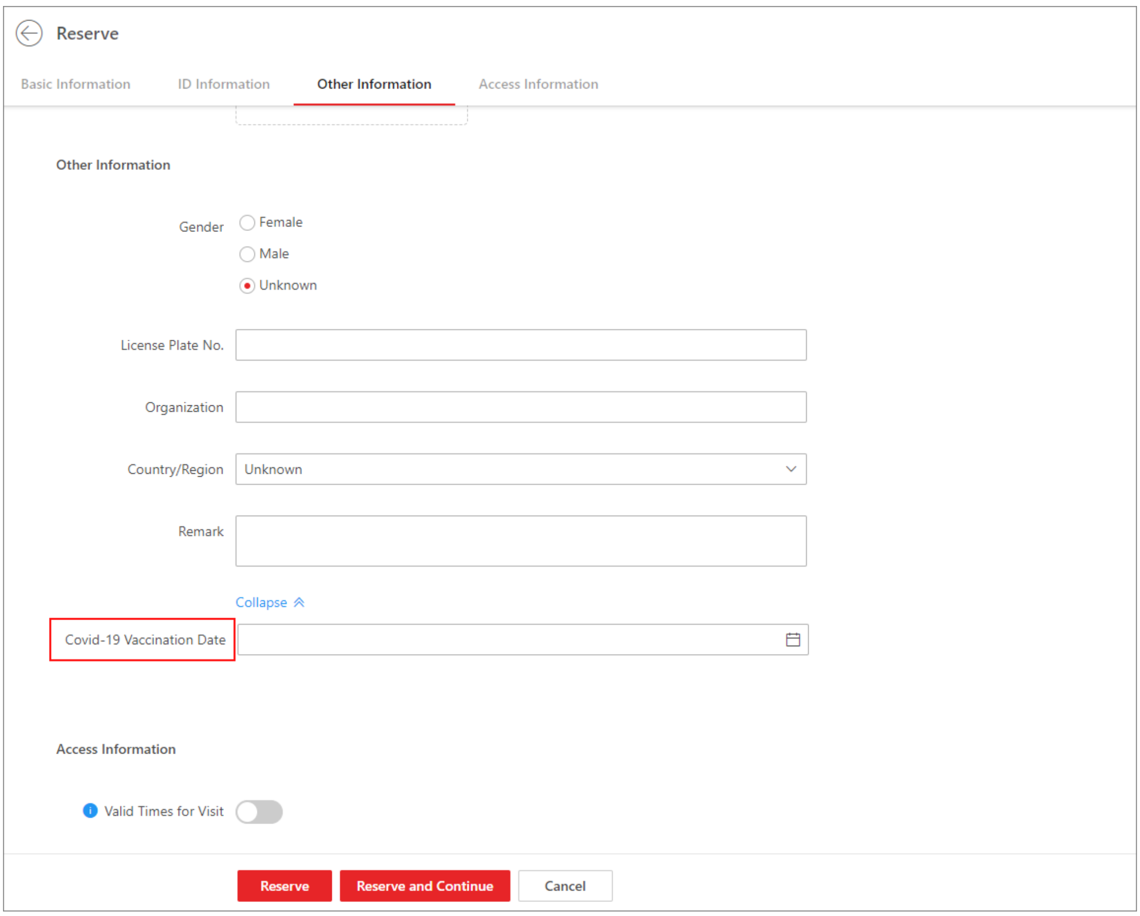


Figure 21-8 Example

Custom Field for Reservation & Check-In

Check fields to display on the visitor reservation page and the visitor check-in page.

Moreover, you can turn on the switches in the Set as Required column to set corresponding fields as required fields.

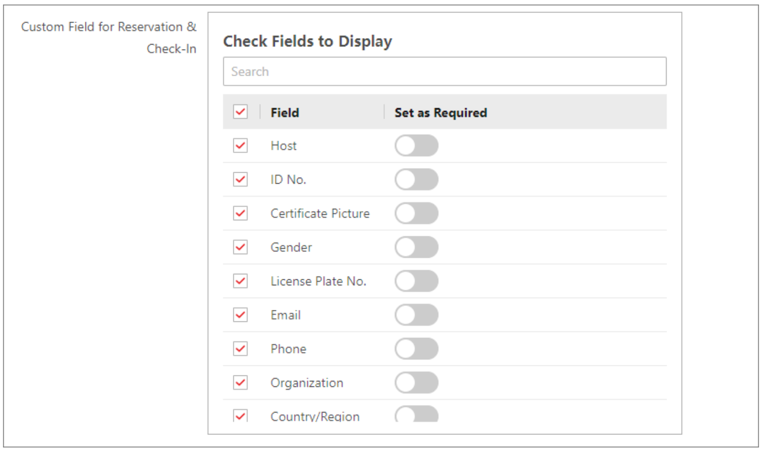


Figure 21-9 Check Fields to Display

Visitor Reservation

Check-In Not Required If Reservation Confirmed

Applicable to reception areas where neither a receptionist nor a visitor terminal is deployed. If this is checked, visitors will be automatically checked in when reservations are made for them.

Digits of Reservation Code

Define the number of digits (4 digits or 6 digits) contained in each reservation code. The visitor reservation code acts as a verification code for visitor check-in. After reservation, the visitor will receive the reservation code by email and text message. When checking in, the visitor should provide the reservation code.

Send Email When Reservation Approved

Send an email based on the selected email template to the recipient (the host or visitor) specified in the template when a visit reservation is approved.

Send Email When Reservation Rejected

Send an email based on the selected email template to the recipient (the host or visitor) specified in the template when a visit reservation is rejected.

Note

- If the recipient is the host, make sure that the host's email address is provided when you add the host to the platform.

If the recipient is the visitor, make sure that the visitor's email address is provided when you make a reservation for or check in the visitor.

- You can customize email templates according to your needs. See ***Add Visitor Receiving Template*** for details.

Visitor Check-In

Print Visitor Pass Once Checked In

When checked, the printer connected to your PC will automatically print a visitor pass once a visitor is checked in.

Format of Visitor Pass

Select **Receipt** or **Card** as the format of the printed visitor passes.

Visitor Pass Template

Select a template as the one that will be automatically printed.

You can click **View Template** to preview the selected template.

Note

Make sure you have set templates as needed. For details about setting visitor pass templates, see ***Add Visitor Pass Template*** .

Take Photo of Visitor's Belongings

If you enable this function, you can take a picture of the visitor's belongings and upload it to the platform when checking in/out the visitor.

Send Email When Checked In

Send an email based on the selected email template to the recipient (the host or visitor) specified in the template when a visitor checks in.

Note

- If the recipient is the host, make sure that the host's email address is provided when you add the host to the platform.
  If the recipient is the visitor, make sure that the visitor's email address is provided when you make a reservation for or check in the visitor.
- You can customize email templates according to your needs. See ***Add Visitor Receiving Template*** for details.

Visitor Check-Out

Default Check-Out Time

The default check-out time will be displayed on the Reserve page. After setting the time, you need not enter the visitor check-out time when reserving for a visitor. By default, the check-out time is 23:59:59. You can specify a time according to your needs.

Visitor Not Checked Out After Exit Time

If a visitor does not check out before the end time of the visit or the exit time, the platform can automatically check out the visitor or trigger an alarm.

Check Out Automatically

When this is selected, if a visitor does not check out before the end time of the visit or the exit time, the platform will automatically check out the visitor. You can set the **Detection Frequency** for detecting whether the visitors have checked out. For example, if you set it to 30 min, the platform will check the visiting status of all visitors every 30 minutes on the platform. The **Detection Frequency** should range from 30 to 60 minutes.

Trigger Alarm

When this is selected, if a visitor does not check out before the end time of the visit or the exit time, an alarm will be triggered for notification. You can set the **Alarm Detection Frequency** for detecting whether the visitors have checked out. For example, if you set it to 3 min, the platform will check the visiting status of all visitors every 3 minutes on the platform. The **Alarm Detection Frequency** should range from 3 to 10 minutes.

Authorization Code for Self-Authentication on Visitor Terminal

Set the authorization code for allowing visitors to perform self-authentication on visitor terminals. The authorization code will be the initial verification code for all visitor terminals connected to the platform. The receptionist (or other similar staff) needs to enter the authorization code to allow visitors to skip authentication.

Note

This parameter is available only when the visitor terminal is added to the platform. See ***Manage Visitor Terminals*** for details.

Visitor Information Reading

Visitor Information Reading Device

- By checking **KR420**, you can read and collect visitor information on their passports via the KR420 passport reading device.
- By checking **United Arab Emirates ID Card Reader**, you can read and collect visitor information (email, phone number, expiration date, and so on) on the United Arab Emirates ID cards via the United Arab Emirates ID card reader.
- By checking **Thai ID Card Reader**, you can read and collect visitor information (ID number, Thai name, English name, birth date, expiration date, and ID photo) on the Thai ID cards via the Thai ID card reader.

Verify Visitor ID Validity Period

If you enable this, the reading device will check the validity of the IDs provided by visitors and a hint will come up if the IDs have expired. If this is disabled, the validity of ID will not be checked.

Unlocking Door by QR Code

Set the QR code mode for unlocking the door: static QR code (remaining unchanged on visitor information and visitor pass) and dynamic QR code (changing regularly after the set time period, in your phone or the invitation link).

3. Click **Save**.

Note

After you click **Save**, the platform will apply the authorization code to all the connected visitor terminals. If the authorization code failed to be applied to specific visitor terminals, will appear next to **Authorization Code for Self-Authentication on Visitor Terminal**. In this case, you can move the cursor to the icon and then click **View** or **Apply Again** to view the failure details or apply the authorization code to visitor terminals again.

21.3.9 Manage Entry & Exit Rule for Visitors' Vehicles

If one visitor comes by driving a vehicle, when checking in, you need to enter the license plate number so that the platform can make the barrier open when the capture unit of the parking lot detects this license plate.

Default Vehicle List for Visitors

There is a default vehicle list which is for the vehicles of visitors and is only in the Vehicle module. After visitor check-in, if you enter the license plate number for the visitor, the license plate number will be displayed in this default vehicle list automatically.
You can click to edit the color of the vehicle list and enter description for the list if needed.

Note

This vehicle list cannot be deleted.

Entry & Exit Rule for Visitors' Vehicles

There is one default entry & exit rule for the vehicles of the checked-in visitors on the **Entry & Exit Rule** page.
By default, the rule is that whenever the vehicles in the list enter/exit the parking lot, the platform will automatically open the barrier. You can edit the rule according to actual needs.

Note

This rule cannot be deleted.

21.4 Watch List Management

You can use the watch list to monitor special visitors for security or other purposes.

What is the Watch List

The watch list contains entities (individual visitors, companies, or countries/regions) that need to be monitored in the visitor reservation or check-in process.
Different from the visitor blocklist, which only contains visitors whose visits are denied in any case, the watch list can contain both the unwanted entities and ones that deserve preferential treatment.

How the Watch List Works

The platform can detect whether a visitor registered in the reservation or check-in process has attributes (e.g., name, ID, company, and country/region) that match entities in the watch list. When entities are matched, the Entities in Watch List Matched window will pop up.
In this case, if the visitor is unwanted, you can reject the reservation or check-in directly on the pop-up window; if the visitor deserves preferential treatment, you can approve the reservation and notify related personnel, so that they can prepare corresponding work beforehand for the visitor.

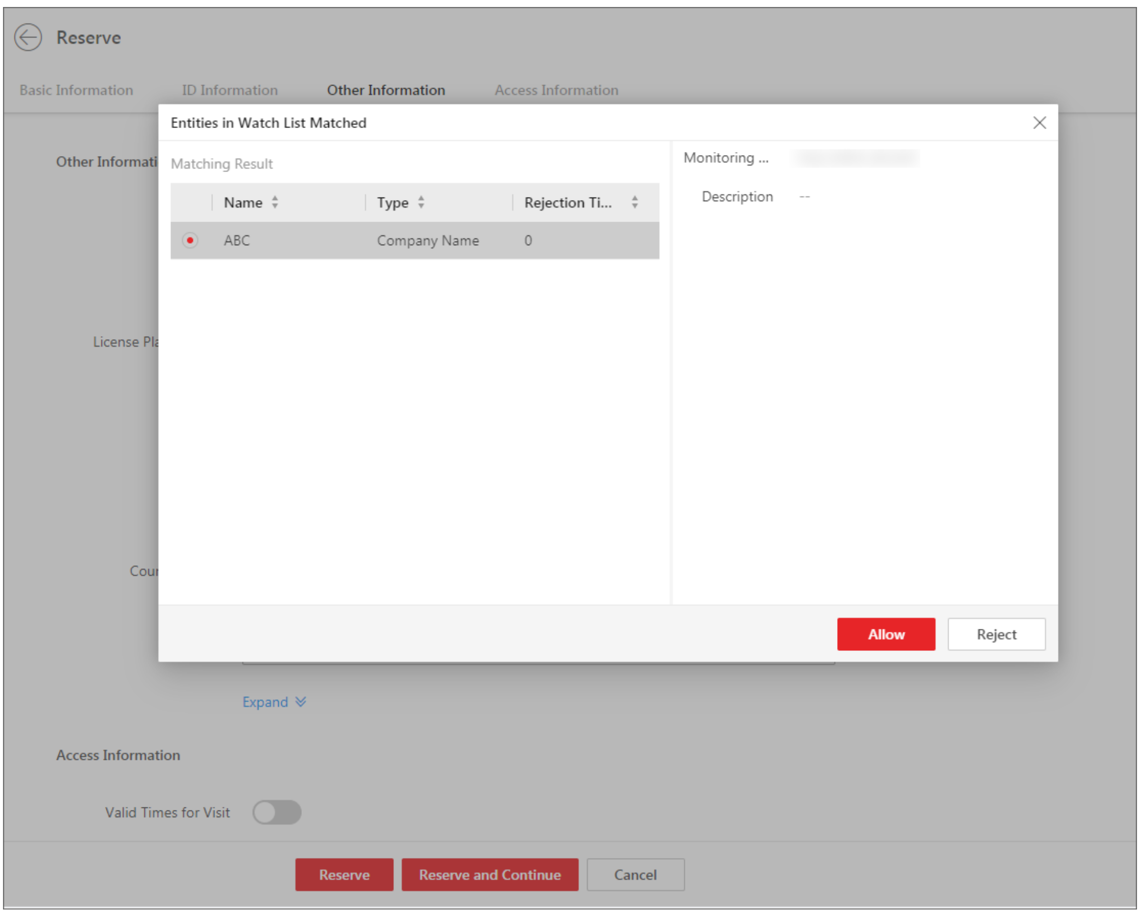


Figure 21-10 The Entities in Watch List Window

21.4.1 Add Entity Type

You can add and define the types of entities to be monitored.

Steps

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Watch List** .
2. Click **Category on Watch List** to open the Category on Watch List pane.
3. Click **Add** on the top left of the pane.
4. Create a type name.
5. **Optional:** Enter a remark for the type.
6. Click **Add** to finish adding the type.
7. **Optional:** Perform one or more of the following operations.

Edit Type	Click a type name to edit it.
Delete Type(s)	Select type(s) and then click **Delete** to delete the selected one(s). Or move the cursor to and then click **Delete All** to delete all types.

21.4.2 Set Match Method

You can set the match methods to determine the match items (e.g., the name and ID) to match the visitors and the entities to be monitored when checking in and reserving for visitors.

Steps

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Watch List** .
2. Click **Match Method** to open the Match Method pane.
3. Set the match items for matching the visitors and the entities during reservations or checked-in.

   Match via Name

   If the name of a visitor matches that of an entity in the watch list, the Entities in Watch List Matched window will pop up when the visitor is reserved or checked in.

   Match via ID

   If the ID number of a visitor matches that of an entity in the watch list, the Entities in Watch List Matched window will pop up when the visitor is reserved or checked in.

   Match via Company

   If a visitor's company matches an entity in the watch list, the Entities in Watch List Matched window will pop up when the visitor is reserved or checked in.

   Match via Country/Region

   If a visitor's country/region matches an entity in the watch list, the Entities in Watch List Matched window will pop up when the visitor is reserved or checked in.
4. Configure name match settings.

Note

To make the name match settings take effect, you need to check **Match via Name** first.

Match First Name Only

If the first name of a visitor matches that of an entity in the watch list, the platform will determine that the visitor name matches the entity. For example, assume that the name of a visitor is Andrew Lee and an entity in the watch list is Andrew Peterson, the platform will determine that the former matches the latter.

Match Full Name

Only when the full name of a visitor matches that of an entity in the watch list will the platform determine that the visitor name matches the entity.

5. Click **OK**.

21.4.3 Add an Entity to the Watch List

You can add a to-be-monitored entity to the watch list and determine how long the entity will be monitored.

Steps

1. On the top left of the Web Client, select → **Passing Management → Visitor → Watch List** .
2. Click **Add** to open the Add Entity page.
3. Set the entity type (**Person**, **Company**, or **Country/Region**).
4. Set other information for the entity.
   - For **Person**, set other information including the first name, last name, category, effective period, ID type, ID number, and ID picture.
   - For **Company**, set other information including the company name, category, and effective period.
   - For **Country/Region**, set other information including the country/region, category, and effective period.

Category

Select a category to which the entity belongs. Or click **Create New Category** to create a new one.

You can manage categories in **Category and Match Method**. For details, see ***Add Entity Type*** .

Effective Period

If enabled, you can determine the time period when the platform monitors the entity. If disabled, the platform monitors the entity indefinitely.

5. Click **Add** or **Add and Continue**.
6. **Optional:** Perform the following operations if needed.

Disable Entities	Select entities and then click **Disable** to disable them. Once disabled, they will not be monitored.

Enable Entities Select disabled entities and then click **Enable** to enable them. Once enabled, they become monitored.

Edit an Entity Click the name of an entity to edit it.

Delete Entities Select entities and then click **Delete** to delete them.
Or hover the cursor over and then click **Delete All** to delete all entities.

21.4.4 Import Existing Visitors to the Watch List

You can import specific existing visitors to the watch list. Existing visitors refer to the visitors once reserved or checked in.

Steps

1. On the top left of the Web Client, select → **Passing Management → Visitor → Watch List** .
2. Click **Import Existing Visitor** to show the Import Existing Visitor pane.
3. Click to select the existing visitors from a specific visitor group and then click **Add**.

   The selected visitors will be displayed on the pane.

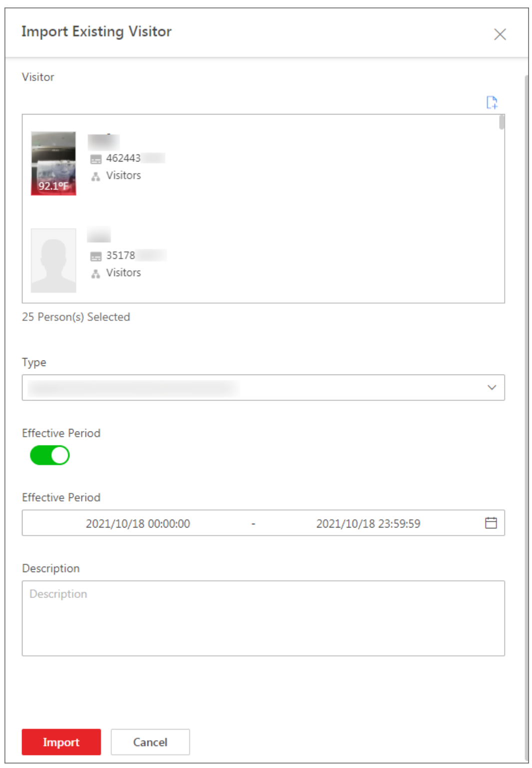


Figure 21-11 Import Existing Visitor

4. Set other information, including the type, effective period, and description.

   Type

Select a type to which the entity belongs.

Make sure you have added types in **Category on Watch List**. For details, see ***Add Entity Type*** .

Effective Period

Determine the time period when the selected visitors will be monitored if their reservations are made or they check in again.

5. Click **Import**.

   The visitors will be displayed in the watch list.
6. **Optional:** Perform the following operations if needed.

Disable Monitoring of Existing Visitors	Select visitors and then click **Disable** to disable them. Once disabled, they will not be monitored.
Enable Monitoring of Existing Visitors	Select disabled visitors and then click **Enable** to enable them. Once enabled, they become monitored.
Edit an Existing Visitors in the Watch List	Click the name of an entity to edit it.
Delete Existing Visitors from Watch List	Select visitors and then click **Delete** to delete them. Or hover the cursor over and then click **Delete All** to delete all visitors.

21.5 Visitor Reservation

Before visiting, visitors can make a reservation. The Administrator can make a reservation for the visitors by entering the visitor and host information on the platform. Visitors can also reserve by themselves. After self-reservation, the Administrator should review the visitor information to approve or disapprove the reservation.

21.5.1 Reserve a Visitor

You can make a reservation for one visitor by entering the visitor and host information on the platform.

Before You Start

Before any operations in the visitor system, you can set the parameters according to actual situations such as setting basic parameters to define the scenario for the visiting process, managing visitor types, adding access levels for visitors, etc. See ***Configurations Before Visitor Management*** for details.

Steps

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Reservation** .
2. Click **Reserve** on the top left to enter the Reserve page.

3. Set basic information for the visitor, such as the name, host, visit purpose, estimated entry time, visitor group, email, and phone. You can also set a profile picture for the visitor.

Note

- You can connect a KR420 passport reader to read the information on the visitor's passport/ID card (including the name, ID No., and ID photo) and set the information for the visitor automatically. You have to enable **KR420** under the Visitor Information Reading tab of the Basic Parameters page. See ***Set Basic Parameters*** .
- You can connect a United Arab Emirates ID card reader to read the information on the visitor's United Arab Emirates ID card (including the name, ID No., ID photo, email, phone number, and expiration date) and set the information for the visitor automatically. You have to enable **United Arab Emirates ID Card Reader** under the Visitor Information Reading tab of the Basic Parameters page. See ***Set Basic Parameters*** .
- You can connect a Thai ID card reader to read the information on the visitor's Thai ID card (including the ID number, Thai name, English name, birth date, expiration date, and ID photo) and set the information for the visitor automatically. You have to enable **Thai ID Card Reader** under the Visitor Information Reading tab of the Basic Parameters page. See ***Set Basic Parameters*** .
- You can customize parameters such as the visit purpose. See ***Set Basic Parameters*** .
- Enter the email address for the visitor to receive an email containing the reservation code or notification that the reservation is approved/rejected.

4. Set ID information for the visitor, including the ID type, ID No., and ID picture.
5. Set other information.
   1) Set the license plate number, organization, country/region, and remark.

   Note

   The license plate number will be shared with the parking lot system so that the visitor's vehicle will be allowed to enter or exit the parking lot.

   2) **Optional:** Click **Expand** to show the additional information fields and then enter additional information of the visitor.

   Note

   Make sure you have set custom visitor attributes, otherwise the additional information fields will be unavailable. For details about how to set custom visitor attributes, see ***Set Basic Parameters*** .

6. Set the access information.

Valid Times for Visit

The maximum times a visitor can access certain doors or floors by QR code authentication. For example, if you set it to 4, the visitor can access the authorized doors and floors up to 4 times by QR code authentication.

Access Level

Click **Configure** to assign access levels to the visitor so that the visitor can access the corresponding access points according to the access schedule of the access levels.

Note

To add a new access level for the visitor, see instructions in ***Add Access Level for Visitors*** .

Extended Access

If you check **Extended Access**, the access points that are configured with extended open duration will stay unlocked or open longer for the visitor.

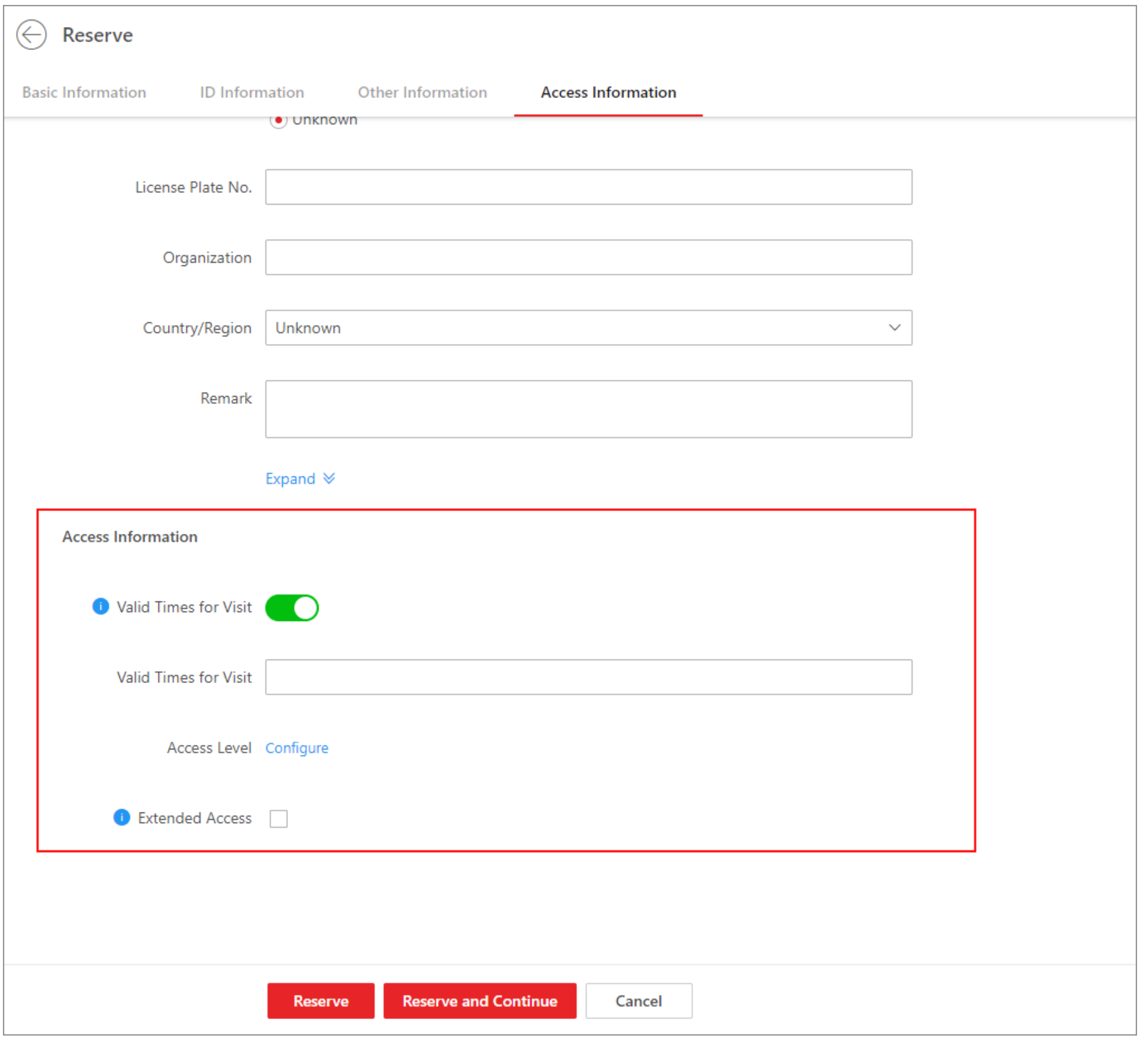


Figure 21-12 Set Access Information

7. Click **Reserve** to finish the reservation, or click **Reserve and Continue** to finish the reservation and continue to reserve for other visitors.

Note

Under the precondition that you have enabled **Check-In Not Required If Reservation Confirmed**, when a visitor is reserved, the platform will perform the following operations automatically:

- Checks in the visitor.
- Applies the access level to the visitor.
- Sends an email with a QR code to notify the specified recipient that the visitor is checked in (if the email address is provided).

8. **Optional:** Perform the following operations on the reservation list page if needed.

Delete Reservation(s)	Select one or more visitors and then click **Delete** to delete the reservations of the selected visitor(s). Or hover the cursor onto ⌄ and then click **Delete All** to delete all reservations.
Edit a Reservation	Click the name of a visitor to edit the reservation for the visitor.
Filter Reservations	Set conditions, such as the phone and visit purpose, and then click **Filter** to filter reservations. For the **Status** condition, you can click ⌄ to select one or more reservation status (reserved, expired, checked in, etc.) to filter reservations. You can also click **Select Additional Information** to filter reservations.

Note

If a reservation has not expired, the reservation will expire after it is deleted.

21.5.2 Batch Import the Visitor Reservation Information

You can add the information of multiple visitors to the platform by importing an excel file with visitor information. Also, by entering the names of visitor groups of multiple persons in the excel file, you can add them to different groups in a batch.

Before You Start

Before any operations in the visitor system, you can set the parameters according to actual situation such as setting basic parameters to define the scenario for the visiting process, managing visitor types, assigning access levels to visitors, etc. See ***Configurations Before Visitor Management*** for details.

Steps

1. On the top left of the Web Client, select ▦ → **Passing Management → Visitor → Visitor Reservation** .
2. Click **Import** to open the Import Visitor Reservation Information panel.
3. Click **Download Template** to save the template file in your PC.
4. In the downloaded template, enter the visitor information following the rules in the template.

5. Click and select the excel file with visitor information from local PC.
6. **Optional:** Check **Replace Repeated Visitor**.

Note

If you check **Replace Repeated Visitor**, the existing visitor information (with repeated certificate type and number) in the list will be replaced. Otherwise, importing visitors with repeated certificate number will fail.

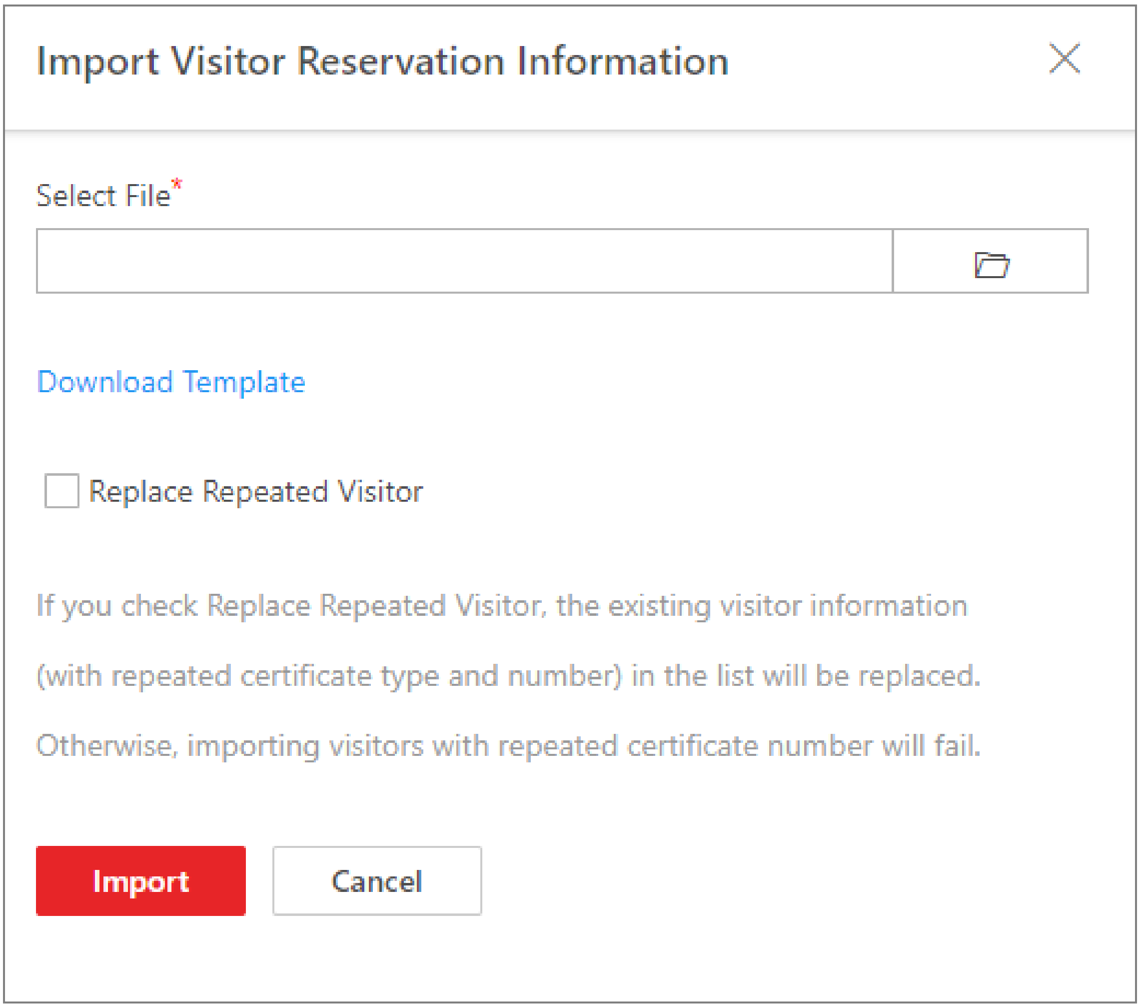


Figure 21-13 Import Visitor Reservation Information

7. Click **Import**.
8. **Optional:** Check one or more visitor(s) and click **Delete** to delete the reservations for the selected visitor(s); or click → **Delete All** to delete all the reservation information.

Note

If a reservation has not expired, the reservation will expire after you delete it.

21.5.3 Review Visitor Reservations

If you have enabled self-service reservation when you set visitor self-service reservation parameters, after the visitors reserve, their information will be displayed on the Visitor to Be Approved page. You should review their information to approve or reject the reservations. After approving, they will be added to the target visitor group.

Before You Start

Make sure you have enabled self-service reservation and configured related parameters. See ***Set Review and Self-Service Reservation Parameters*** for details.

Steps

Note

- You need to have the permission (**User Permission → Configuration Permission → Visitor → Visitor Reservation and Review → Review**) shown in the picture below before you can review reservations.
- If you are set as a reviewer in the visitor approval flow, you can review the visitors. If you are the administrator, all expired flows and all flows with no reviewers will be shown on the page for you to review.

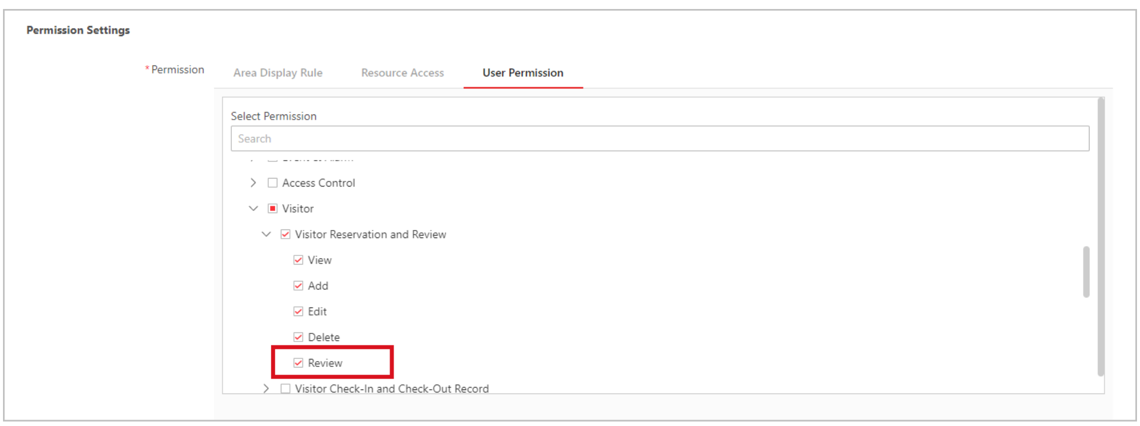


Figure 21-14 The Permission for Reviewing Reservations

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Reservation** .
2. For visitors to be approved, click to approve the reservation, or click to reject the reservation.
3. **Optional:** Click to filter reserved visitors by name, ID, status, etc. to quickly find your wanted visitors.
4. Review the displayed visitor information and verify them.

Approve Self-Service Reserved Visitor Information	If the self-service reserved visitor information conforms to the rules and regulations of your company or organization, approve the information to add the visitors into the platform. Select one or more reserved visitors, and click **Approve** to approve the visitor(s).
Reject Self-Service Reserved Visitor Information	If the self-service reserved visitor information does not conform to the rules and regulations of your company or organization, reject the visitor and tell the visitor to reserve again with right information. Select one or more reserved visitors, and click **Reject** to reject the visitor(s).
Delete Self-Service Reserved Visitor Information	Select one or more reserved visitors, and click **Delete** to delete the visitor(s) from the list. You can also hover the cursor on **Delete** and click **Delete All** to delete all visitors from the list.

Note

Approved visitors will be added to the target visitor group; rejected ones will not be added to the target visitor group, but they will stay in the Visitors to be Reviewed list.

21.6 Visitor Check-In

The platform supports checking in visitors both with or without a reservation.

See ***Check In a Visitor Without Reservation*** for details about checking in visitors without a reservation.

See ***Check In a Reserved Visitor*** for details about checking in visitors with a reservation.

21.6.1 Check In a Visitor Without Reservation

Prior to a visitor's arrival or when the visitor arrives, you need to add the visitor's information to the platform. Once added and checked in, the visitor can authenticate by biometrics (including the fingerprint and face) or QR code, and be able to access the predefined doors and floors.

Steps

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Check-In/Out → Visitor Check-In** .
2. Click **Unreserved Visitor Check-In**.
3. Enter the first name and last name.
4. **Optional:** Set other basic information, including the profile picture, host, visiting purpose, exit time, visitor group, email, and phone.

Note

- For visitors who have visited before, you can click **Select** next to **First Name** to reuse the information.
- You can click **Select** next to **host** to select an existing person as the host.
- You can connect a KR420 passport reader to read the information on the visitor's passport/ID card (including the name, ID No., and ID photo) and set the information for the visitor automatically. You have to enable **KR420** under the Reading Device tab of the Basic Parameters page. See ***Set Basic Parameters*** .
- You can connect a United Arab Emirates ID card reader to read the information on the visitor's United Arab Emirates ID card (including the name, ID No., ID photo, email, phone number, and expiration date) and set the information for the visitor automatically. You have to enable **United Arab Emirates ID Card Reader** under the Reading Device tab of the Basic Parameters page. See ***Set Basic Parameters*** .
- You can connect a Thai ID card reader to read the information on the visitor's Thai ID card (including the ID number, Thai name, English name, birth date, expiration date, and ID photo) and set the information for the visitor automatically. You have to enable **Thai ID Card Reader** under the Visitor Information Reading tab of the Basic Parameters page. See ***Set Basic Parameters*** .
- You can set the visitor profile picture in four ways: collecting a face picture from devices, taking a picture by the camera of your computer, uploading a picture saved in your computer, or reading from the passport / ID card via passport reader (as mentioned in the previous list item).
- Hover the cursor on the uploaded profile picture and click **×** to delete it.
- Enter the email address for the visitor to receive an email containing the QR code or notification that the visitor has checked in.

5. **Optional:** Click **Credential Management** to set the credentials for the visitor, including the card and fingerprint.

Card

Issue a card to the visitor to assign the card number to the visitor. You can enter the card number manually, or swipe a card on the card enrollment station, enrollment station, or card reader to get the card number, and then issue it to the visitor.

Note

Only one card can be issued to a visitor.

a. Click + in the **Card** field.
b. Place the card that you want to issue to this visitor on the USB fingerprint recorder, fingerprint and card reader, or enrollment station, and the card number will be read automatically. Or you can enter the card number manually.

Note

You can click **Card Issuing Settings** to set the issuing parameters.

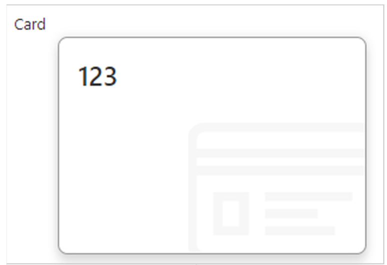


Figure 21-15 Read Card

Fingerprint

The platform provides three ways to collect fingerprints: via a USB fingerprint recorder, via an enrollment station, or via a fingerprint and card reader.

Click **Configure** to set the collection mode as follows.

USB Fingerprint Recorder

Collect fingerprints via a USB fingerprint recorder connected to the computer running the Web Client, which is plug-and-play and does not require any settings. This mode is suitable for face-to-face scenarios where the person and the system administrator are in the same location.

After connecting the fingerprint recorder to your computer, click , place and lift your finger on the recorder following the prompts, and it will collect your fingerprint automatically.

Fingerprint and Card Reader

Collect fingerprints via the fingerprint scanner of an access control device or a video intercom device which is managed in the system. This mode is suitable for non-face-to-face scenarios where the person and the system administrator are in different locations.

Select an access control device or a video intercom device from the managed device list.

Click , place and lift your finger on the selected fingerprint and card reader following the prompts, and it will collect your fingerprint automatically.

Enrollment Station

You need to specify the device IP address, port number, user name, and password to access the enrollment station. Then click , place and lift your finger on the device, and it will enroll your fingerprint automatically.

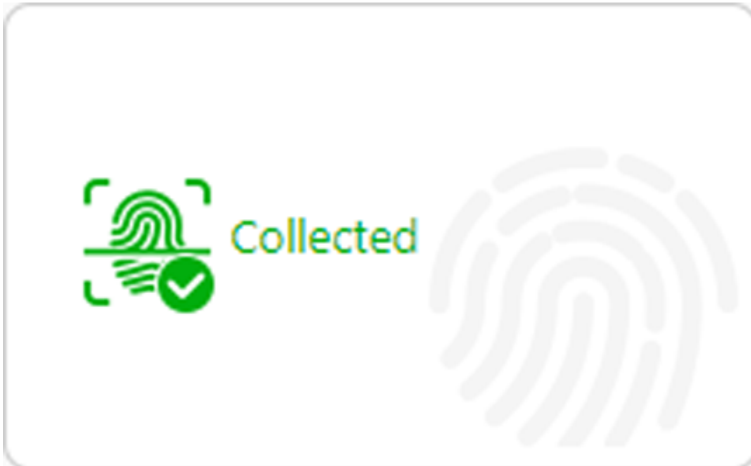


Figure 21-16 Fingerprint Recorded

Note

- No more than one fingerprint can be collected for 1 visitor.
- You can configure either cards or fingerprints.

6. **Optional:** Edit the ID information, including the ID type, ID No., and ID picture.
7. **Optional:** Take a phone of the visitor's belongings.

Note

Make sure you have enabled this function. See ***Set Basic Parameters*** for details.

8. Set other information.

1) Set other information, such as the license plate number, and skin-surface temperature.

Note

The license plate number will be shared with the parking lot system so that the visitor's vehicle will be allowed to enter or exit the parking lot.

2) Click **Expand** to show the additional information fields and then enter additional information about the visitor.

Note

Make sure you have set custom visitor attributes; otherwise, the additional information fields will be unavailable. For details about how to set custom visitor attributes, see ***Set Basic Parameters*** .

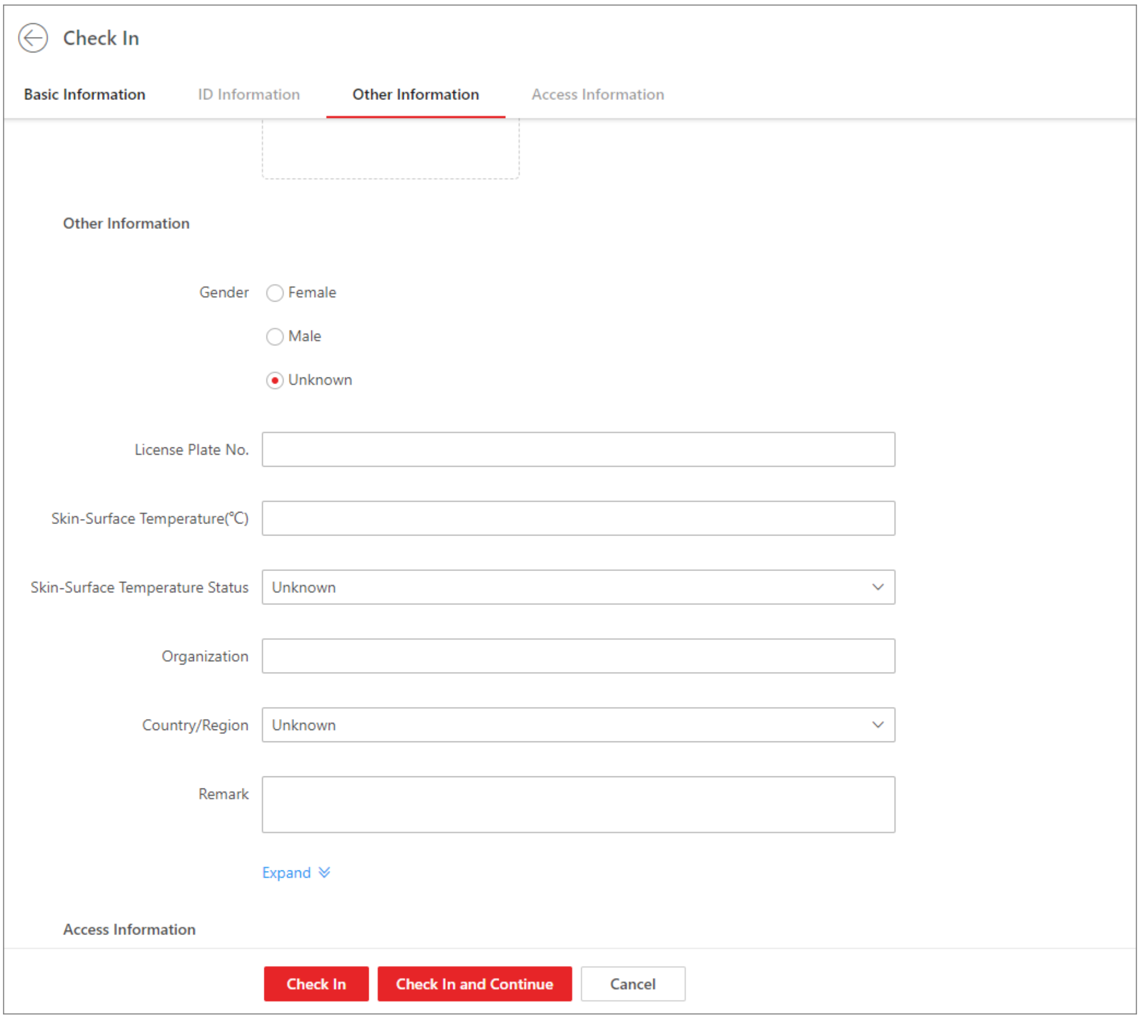


Figure 21-17 Set Other Information

9. Set the access information.

Valid Times for Visit

The maximum times a visitor can access certain doors or floors by QR code authentication. For example, if you set it to 4, the visitor can access the authorized doors and floors up to 4 times by QR code authentication.

Access Level

Click **Configure** to assign access levels to the visitor so that the visitor can access the access points within the access schedule of the access levels.

Note

To add a new access level for the visitor, see the instructions in ***Add Access Level for Visitors*** .

Extended Access

If you check **Extended Access**, the access points that are configured with extended open duration will stay unlocked or open longer for the visitor.

10. Complete checking in the visitor.
    - Click **Check In**.
    - Click **Check In and Continue** to check in the visitor and continue to check in another.

Note

If the operation succeeds and you have enabled **Print Visitor Pass Once Checked In** when you set basic parameters, the Preview window will pop up showing the preview of the visitor pass for the visitor. You can click **Print** on the window to print the visitor pass.

11. Go back to the Visitor Check-In page to check whether the visitor information fails to be applied to the visitor terminal(s). If it fails, check the failure details, troubleshoot, and apply again.

Note

If there is visitor information which fails to be applied to visitor terminal(s), a notification will show above the visitor list on the Visitor Check-In page. In this case, you can click **View** to view the failure details and troubleshoot according to the reasons shown on the window, and then click **Apply Now** or **Apply Again** to apply the visitor information to the visitor terminal(s) again.

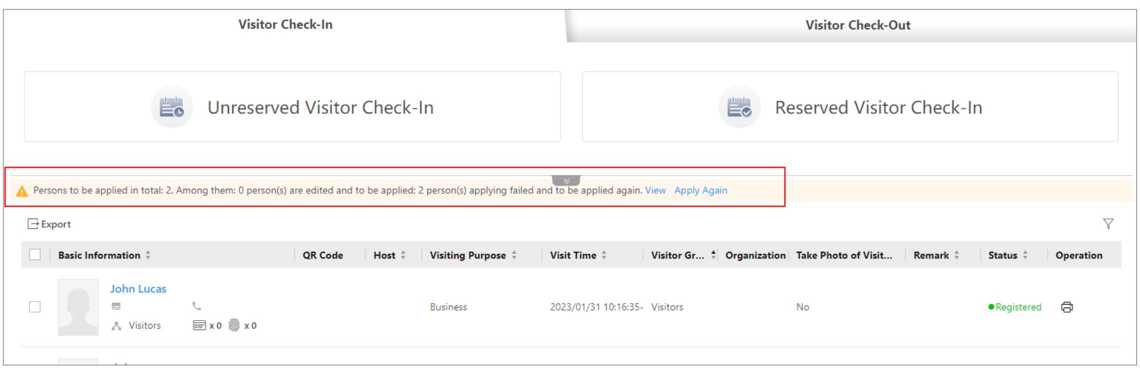


Figure 21-18 Notification of Applying Failures

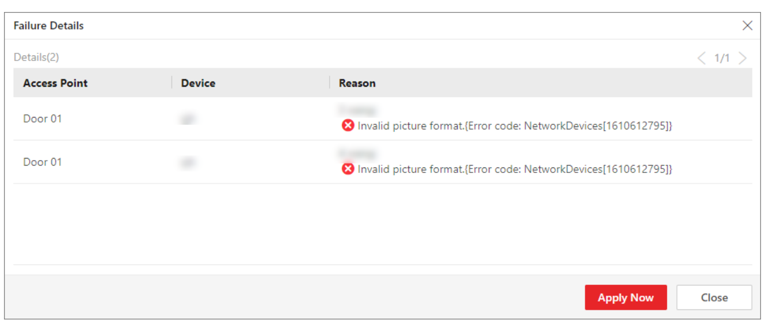


Figure 21-19 Failure Details

12. **Optional:** Perform the following operations on the Visitor Check-In page if needed.

Filter Visitors	Click to filter visitors by conditions such as the ID No., name, phone, and organization. For the **Status** condition, you can click to select one or more reservation status (reserved, expired, checked in, etc.) to filter visitors. You can also click **Select Additional Information** to filter visitors.
Export Visitors	Select visitors and click **Export** to export checked-in visitors to the local PC as a file. **Note** You will be required to set a password for the exported file for security. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.
Edit Visitor Information	Click on a visitor's name to edit the information. **Note** If the visitor is checked out, you cannot edit the information.
Download a Visitor QR Code	Click in the **QR Code** column to download the QR code for the visitor. You can print it or send it to the visitor for identity authentication at access points.
Print a Visitor Pass	Click to print the visitor pass for the visitor.

What to do next

You can view the added visitors in the Visitor List. For details, see ***View Visitor Information*** .

21.6.2 Check In a Reserved Visitor

If a visitor has a reservation, you can check in the visitor by entering reservation information and visitor information.

Steps

1. On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Visitor Check-In/Out** → **Visitor Check-In** .
2. Click **Reserved Visitor Check-In**.
3. Select a reservation credential type.
4. Enter the reservation code, or phone number, or select a ID type and enter the ID No.

   The Reservation Information window will show.

5. **Optional:** Click **Edit Visitor Information** to edit the visitor information. See ***Check In a Visitor Without Reservation*** for details.
6. Click **Check In**.

Note

If the operation succeeds and you have enabled **Print Visitor Pass Once Checked In** when you set basic parameters, the Preview window will pop up showing the preview of the visitor pass for the visitor. You can click **Print** on the window to print the visitor pass.

7. Go back to the Visitor Check-In page to check whether the visitor information fails to be applied to the visitor terminal(s). If it fails, check failure details, troubleshoot, and apply again.

Note

If there is visitor information failing to be applied to visitor terminal(s), a notification will show above the visitor list on the Visitor Check-In page. In this case, you can click **View** to view the failure details and troubleshoot according to the reasons shown on the window, and then click **Apply Now** or **Apply Again** to apply the visitor information to visitor terminal(s) again.

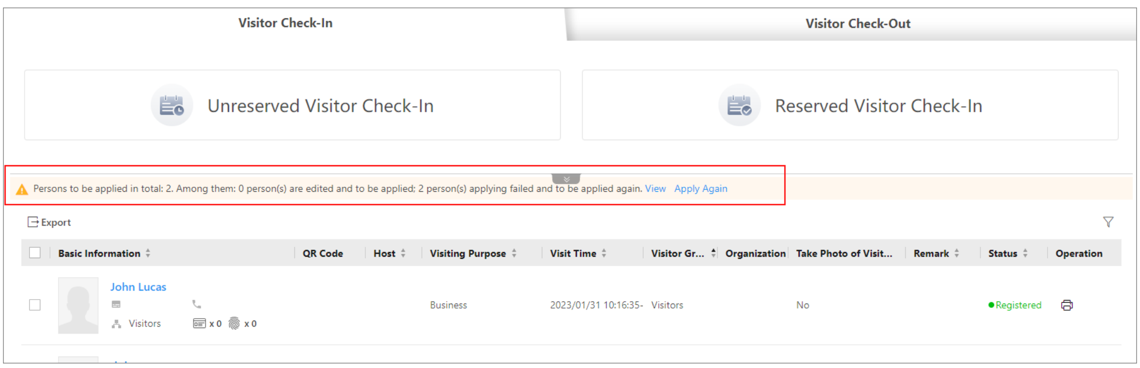


Figure 21-20 Notification of Applying Failures

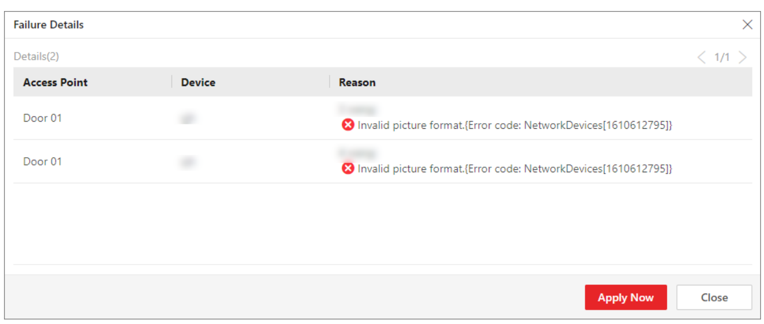


Figure 21-21 Failure Details

8. **Optional:** Perform the following operations on the Visitor Check-In page if needed.

Filter Visitors	Click to filter visitors by conditions such as the ID No., name, phone, and organization.

	For the **Status** condition, you can click ⌄ to select one or more reservation status (reserved, expired, checked in, etc.) to filter visitors. You can also click **Select Additional Information** to filter visitors.
Export Visitors	Select visitors and click **Export** to export checked-in visitors to the local PC as a file. **Note** You will be required to set a password for the exported file for security. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.
Edit Visitor Information	Click on a visitor's name to edit the information. **Note** If the visitor is checked out, you cannot edit the information.
Download a Visitor QR Code	Click in the **QR Code** column to download the QR code for the visitor. You can print it or send it to the visitor for identity authentication at access points.
Print a Visitor Pass	Click to print the visitor pass for the visitor.

21.7 Visitor Check-Out

You should check out a visitor or let the visitor check out at a self-service check-out point before the visitor leaves. This is to ensure that the access level assigned to the visitor expires after they leaves.

On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Check-In/Out → Visitor Check-Out** to enter the Visitor Check-Out page.

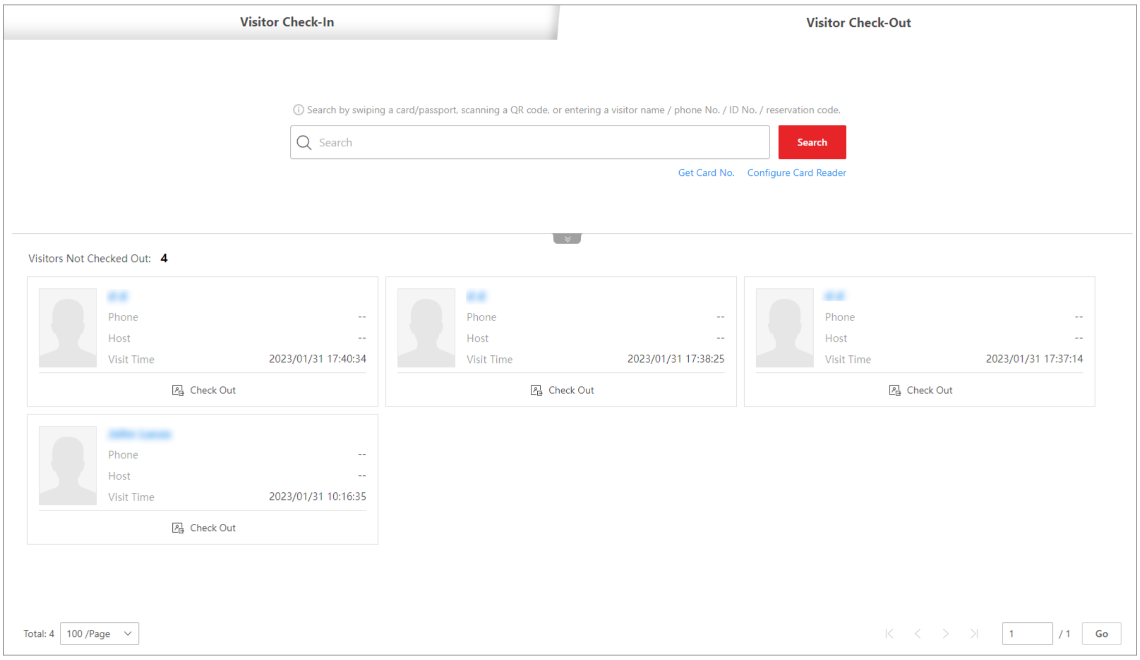


Figure 21-22 Visitor Check-Out Page

A visitor can be checked out in the following ways:

Check Out at Self-Service Check-Out Point

If you have set a self-service check-out point, the visitor can check out by authenticating at the self-service check-out points without the help of the receptionist. If you have issued a card to a visitor when checking in, after checking out, the visitor should put the card in the place for card collection. The access level of their cards, fingerprints, face pictures, and QR codes will expire automatically.

Note

See ***Set Self-Service Check-Out Point*** for details about how to set a self-service check-out point.

Check Out by Swiping Card

If you want to allow visitors to check out by swiping their cards, you need to click **Configure Card Reader** in the upper-right corner of the Visitor Check-Out page to configure the card reader first.

Note

Before configuring the card reader, make sure that you have added the corresponding device (enrollment station or card enrollment station) to the platform, otherwise ⓘ will appear next to **Configure Card Reader**, indicating that the platform fails to detect the device.

By default, **Card Enrollment Station** is selected as the card reader. If you select **Enrollment Station** and complete related settings, you need to click **Get Card No.** on the Visitor Check-Out page to activate the settings.

Search for and Check out a Visitor

You can swipe a card/passport, scan a QR code, or enter a visitor name / phone No. / ID No. / reservation code, and click **Search** to search for the visitor, and then click **Check Out** on the search result page to check out them.

Note

- Only if a bar code reader is plugged into the PC where the platform runs, can you use the bar code reader to scan the QR code on the visitor pass of a visitor to search for the visitor to check them out.
- Only if a KR420 passport reader / United Arab Emirates ID card reader / Thai ID card reader is plugged into the PC where the platform runs, can you use the KR420 passport reader / United Arab Emirates ID card reader / Thai ID card reader to swipe the passport / ID card to search for the visitor to check them out.

Check Out Visitors in the Visitors Not Checked Out Section

Visitors not checked out will be displayed on the Visitor Check-Out page, you can click **Check Out** on the visitor card to check them out, or you can click the name of a visitor to go to the details page and click **Check Out**.

Automatic Check-Out

If you do not manually check out a visitor, the visitor will be checked out by the platform automatically when the configured visiting duration ends.

Note

Automatic check-out is available only when **Check Out Automatically** is selected for visitors not checked out after the exit time on the Basic Parameters page. For details, see ***Set Basic Parameters*** .

21.8 View Visitor Information

You can view all checked-in visitors (including those who have checked out) in the visitor list and perform related operations such as adding visitors to the blocklist.

On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Information** to view the list of all visitors.

You can perform the following operations on the Visitor Information page.

- Click on the top right to filter visitors by ID No., name, phone, company, skin-surface temperature, reservation/check-in time, and whether the visitor is in the blocklist.

If you have set custom visitor attributes, you can click **Select Additional Information** to select additional information for the filtering. See ***Set Basic Parameters*** for details about how to set custom visitor attributes.

- **Delete Visitor**: Check one or more visitors and click **Delete** to delete the selected visitor(s). Or click → **Delete All** to delete all visitors.

Note

After deleting the visitor's personal information, you can still search the visitor's visiting records in the Visitor List.

- **Move Visitors to Blocklist**: Select the visitors and click **Move to Blocklist** to move the selected visitors to the blocklist.
- **Remove Visitors from Blocklist**: Select the visitors and click **Remove from Blocklist** to remove the selected visitors from the blocklist.
- **Move Visitor to Another Group**: Check one or more visitors and click **Move** to move the selected visitor(s) into a different visitor group.
- **Clear Visitor Information**: When enabled, the platform will clear all visitors who did not check in during the time period which you specify by setting **Not Checked In For**.
- **Reserve Again**: For normal visitors who have checked out, you can click to make reservation for them again quickly without the need to set the visitors' existing basic information (e.g. visitor name, ID, fingerprint) again.
- **Check In Again**: For normal visitors who have checked out, you can click to check in them again quickly without the need to set the visitors' existing basic information (e.g., profile picture and fingerprint).

Valid Times for Visit

The times a visitor can enter/exit the area managed by the related access group after authentication. For example, if you enter 5 as the valid times and relate an access group for a door to the visitor, the visitor can enter/exit the door for 5 times. After 5 times of authentication, the visitor cannot enter/exit the door.

21.9 Check Visitor Access Records

When a visitor accesses an access point by credentials, a visitor access record is stored on the platform. After searching for a visitor, you can view all access records of the visitor, no matter the visitor has checked out or not. This allows you to track all the access points where the visitor has visited and view the corresponding visit times.

On the top left of the Web Client, select → **Passing Management** → **Visitor** → **Visitor Access Record** to display the visitor access records. By default, only the current-day records will be displayed. If you need to view other time's records, manually filter the records (see ***Filter Visitors***).

You can perform the following operations.

Filter Visitors

Click on the top right to filter visitors by ID No., name, phone, company, host, visit purpose, visit time, status, and skin-surface temperature status. You can also click **Select Additional Information** to select additional information to filter.
For the **Status** condition, you can click to select one or more reservation status (checked-in, checked-out, checked-out (auto), self checked-out, and not check out in effective period) to filter visitors.
After filtering, you can click the visitor name to view the information of the visitor.

View Information on First & Last Authentication

By default, only the first and last access authentication records are displayed. To view more information, click to open the Visitor Access Authentication Records window to view all access authentication records of the visitor.

Chapter 22 Parking Management

HikCentral Professional provides parking management services covering entry & exit rule management, parking fee rule management, and so on. The platform can perform relevant operations according to the rules you set.

On the Web Client, you need to create a parking lot and set its entrances and exits as well as lanes according to actual needs. For vehicles managed in the platform, you can predefine parking fee rules and entry & exit rules for them. For vehicles not managed in the platform, you can also set an entry & exit rule to define how to open the barrier when these vehicles are detected at the entrances and exits.

On the top navigation bar, select → **Passing Management** → **Parking Lot** .

22.1 Flow Chart of Parking Lot Management

The flow chart below shows the overall process of parking lot management.

Note

Make sure you have added the relevant vehicle information to the platform and managed the vehicles as needed (e.g., categorize them into different types or add them to vehicle lists).

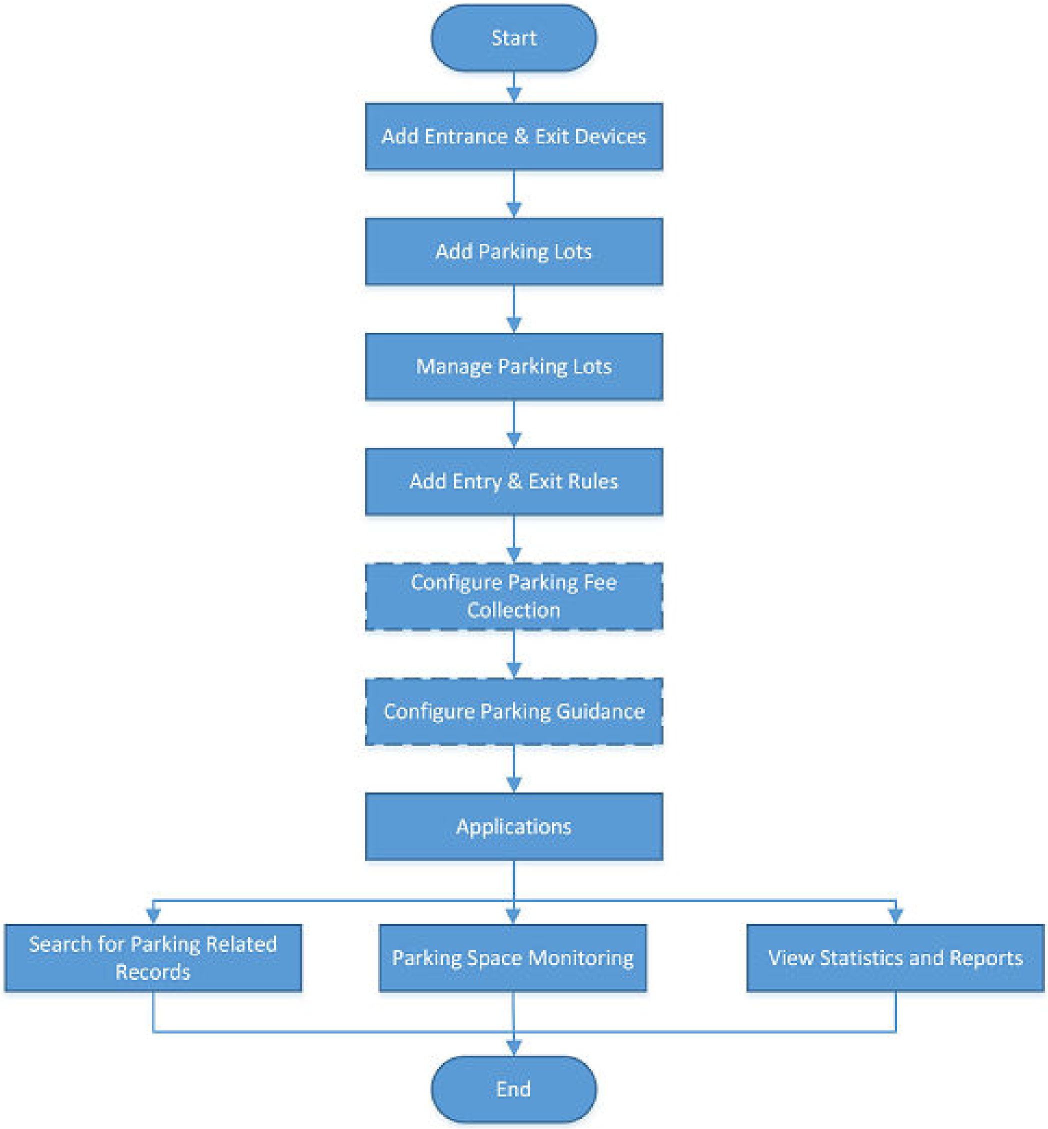


Figure 22-1 Flow Chart of Parking Lot Management

Procedure	Description
Add Entrance & Exit Devices	Add the relevant devices, such as cameras, entrance/exit control devices, display screens, etc., to the platform via the Resource Management module according to your needs.
Add Parking Lots	Refer to ***Add Parking Lot*** for details about how to add parking lots to the platform.
Manage Parking Lots	After adding parking lots, you can add entrances and exits to the platform, add lanes for linking different devices to realize different

Procedure	Description
	functions, and link display screens to parking lots. Refer to ***Add Entrance and Exit***, ***Add Lane***, and ***Link Display Screen and Set Displayed Content*** respectively for more details.
Add Entry & Exit Rules	An entry & exit rule defines how the barrier gate opens when the platform detects a vehicle at the lane. The barrier gate can be set to open automatically when a vehicle is detected or you can also open it manually by clicking the **Allow** button on the Control Client after verifying its identity. Refer to ***Configure Entry & Exit Rules*** for details.
Configure Parking Fee Collection	If the parking lot is a paid parking lot that charges money for parking, you can configure rules for how to calculate and collect the parking fees. Refer to ***Flow Chart of Parking Fee Collection*** for details.
Configure Parking Guidance	For parking lots with guidance terminals and display screens, parking guidance can be configured so that the guidance terminal can link with multiple parking cameras for management, and the display screen displays the number of vacant parking spaces in a parking lot to guide drivers to those parking spaces. Refer to ***Flow Chart of Parking Guidance Configuration*** for details.
Applications	After completing the above-mentioned configurations, you can perform operations such as monitoring parking spaces, searching for parking related records, and viewing the relevant statistics and reports. For details, refer to ***Parking Space Monitoring***, ***Record Search***, and ***Statistic and Report*** respectively.

22.2 Flow Chart of Parking Fee Collection

For paid parking lots that require a certain fee to park, the flow chart below shows the process of configuring parking fee collections.

Note

Make sure you have added the relevant vehicle information to the platform and managed the vehicles as needed (e.g., categorize them into different types or add them to vehicle lists).

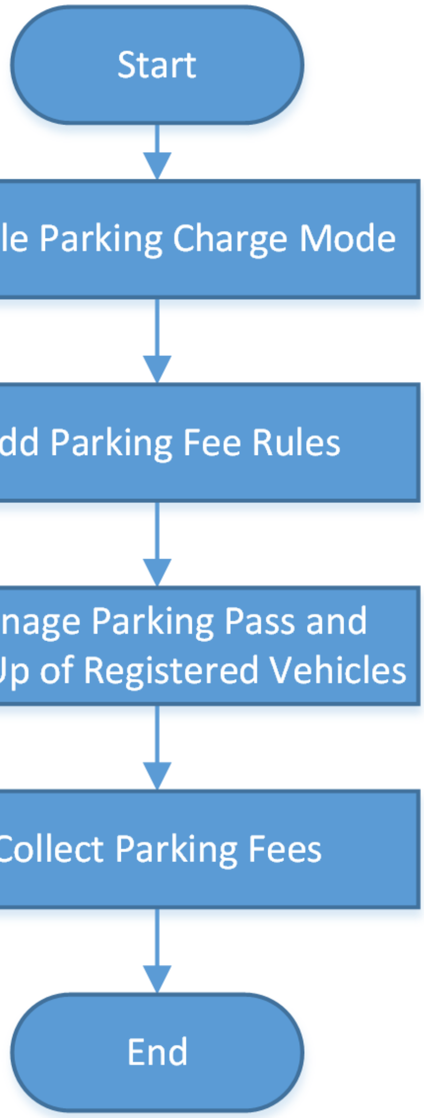


Figure 22-2 Flow Chart of Parking Fee Collection

Procedure	Description
Enable Parking Charge Mode	To enable parking pass top up for registered vehicles or to charge other vehicles for temporary parking, you need to first set the parking fee mode to Charge. Refer to ***Enable Parking Charge Mode*** for details.
Add Parking Fee Rules	You can set parking fee rules for a parking lot, including rules for certain types of vehicles, the parking pass rule, the discount rule, and the parking fee rule for abnormal entry & exit. Once you set a rule,

Procedure	Description
	the platform will automatically calculate the fee for parking based on this rule and present the parking fee related information. Refer to ***Configure Parking Fee Rules*** for details.
Manage Parking Pass and Top-Up	If a vehicle is topped up with a parking pass of a parking lot, it can enter and exit that parking lot as a registered vehicle and park without paying any additional fees. Refer to ***Top Up Parking Pass*** for details.
Collect Parking Fees	Registered vehicles can park in a parking lot without paying additional fees if they have been topped up with a parking pass, whereas other vehicles (e.g., temporary vehicles, vehicles in list, and vehicles with abnormal entries/exits) can pay for parking at the booth or in the toll center by searching for their parking information by license plate No., swiping the temporary card, or scanning the parking receipt. Refer to ***Pay in Toll Center*** for details.

22.3 Flow Chart of Parking Guidance Configuration

The flow chart below shows the process of configuring parking guidance for parking lots with guidance terminals and display screens to guide drivers to vacant parking spaces.

Note

Make sure you have added the relevant vehicle information to the platform and managed the vehicles as needed (e.g., categorize them into different types or add them to vehicle lists).

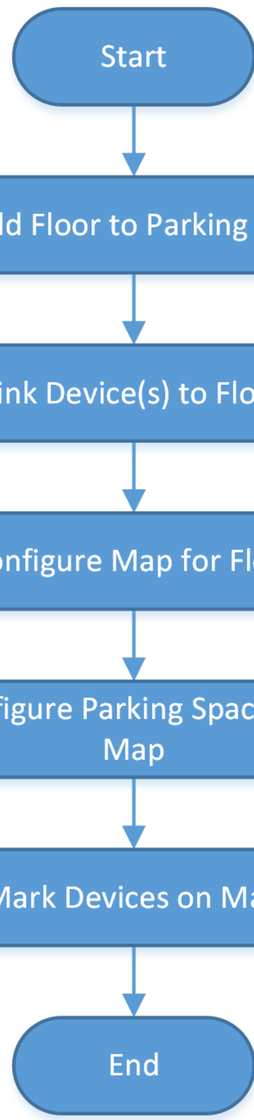


Figure 22-3 Flow Chart of Parking Guidance Configuration

Refer to ***Parking Guidance Configuration*** for details about each step.

22.4 Manage Parking Lot

Parking lot is a parking facility that is intended for parking vehicles. You can add one or multiple parking lots to the platform and set entrances and exits as well as lanes for them according to actual needs.

There are three elements in the parking management platform:

Parking Lot

A parking facility that is intended for parking vehicles. The platform supports adding multiple parking lots and you need to create them at the very beginning.

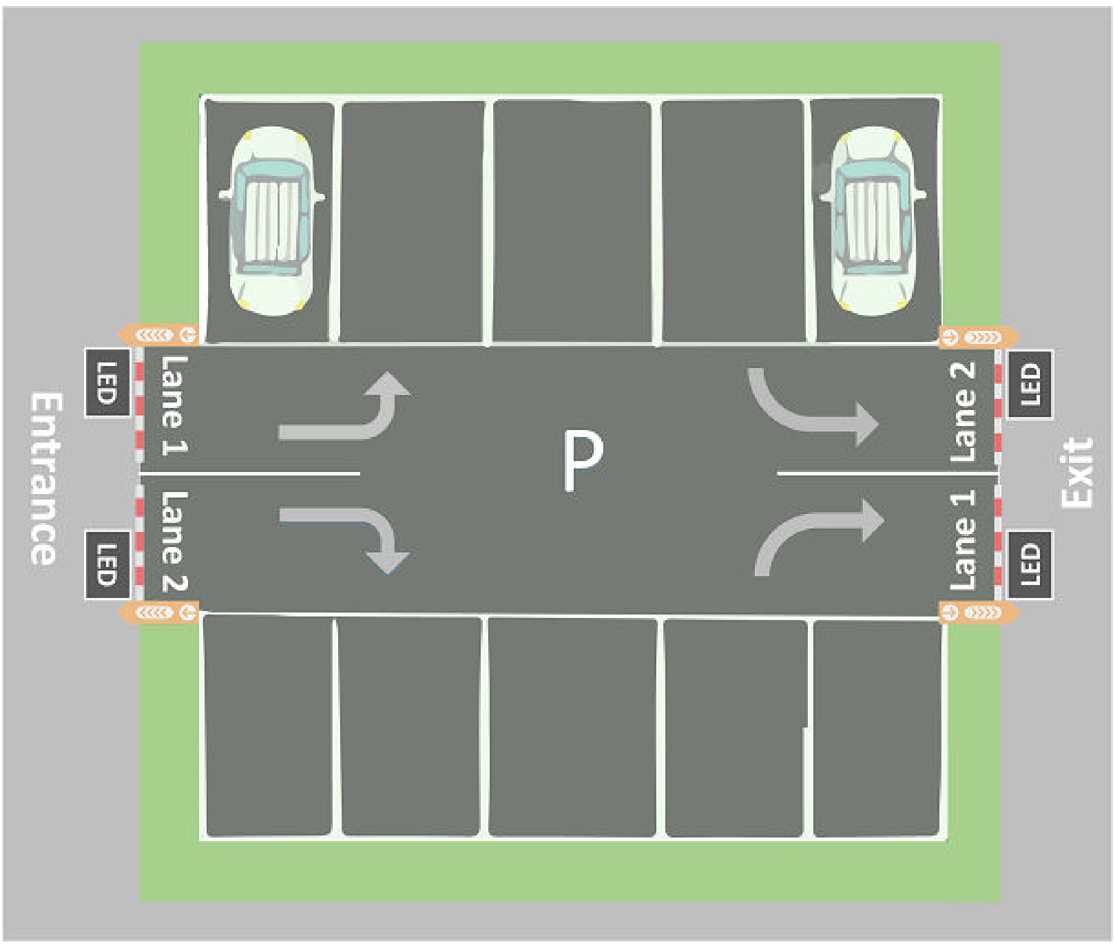
Entrance & Exit

The vehicles can enter or exit the parking lot via entrance & exit.

Lane

Each entrance or exit should contain at least one lane. The lane can be related with devices, including the capture unit, access control device, video intercom device, guidance screen, and entrance/exit station, which can be used for capturing and recognition, identity verification, video intercom, parking guidance, and barrier control. See ***Add Lane*** for details.

The two pictures below shows the typical relation of parking lot, entrances & exits, and lanes.



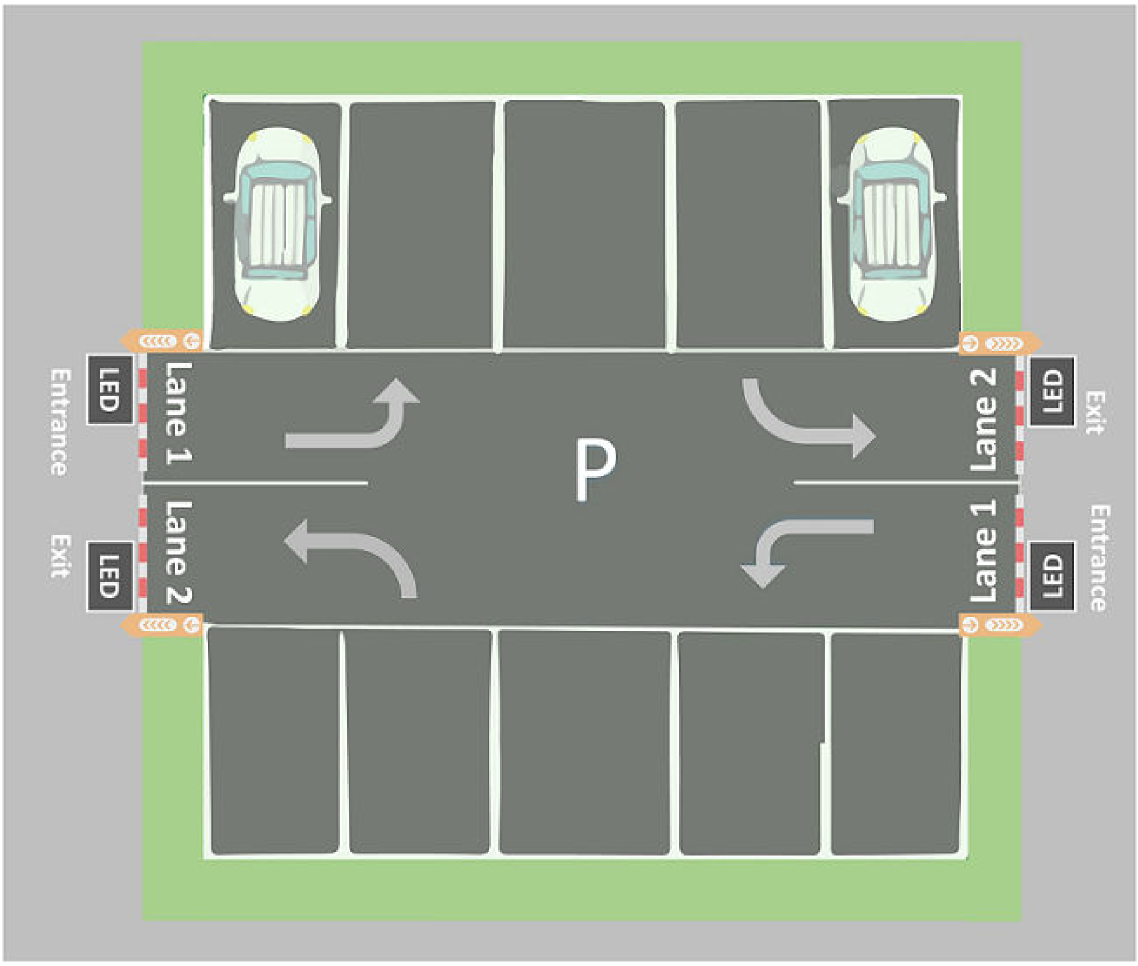


Figure 22-4 Parking Lot

22.4.1 Parking Lot Overview

On the Parking Lot Overview page, you can view different information about the parking lot, including the occupancy statistics of parking spaces, the number of daily entries and exits, the health of devices, etc. You can also go to different pages via hyperlinks to view detailed information.

Occupancy: You can view the total number of parking spaces, the number of vacant parking spaces, and the occupancy statistics of different types of parking spaces. You can click **Parking Space Overview** to go to the Parking Space Overview page and view more detailed statistics of parking spaces. See ***Parking Space Monitoring*** for details.

Today's Entries & Exits: You can view the number of daily entries and exits, the entry/exit trend, and the number of entries and exits at different entrances and exits.

Vehicle Passing Event: You can view the vehicle-passing information of the parking lot. If you are managing more than one parking lot, you can click the name of a parking lot to view its detailed vehicle-passing information.

Device Monitoring: You can view the health of devices related to the parking lot, including guidance terminals, parking cameras, and display screens. You can also click **Maintenance** to go to the Maintenance page and view more detailed statistics of the health of devices. See ***Maintenance*** for details.

Other Parking Lot Entrance & Exit: In the lower-right corner, you can view the list of devices linked to lane(s) for other parking lot(s). You can click **Configure Now** to configure settings of the parking lot.

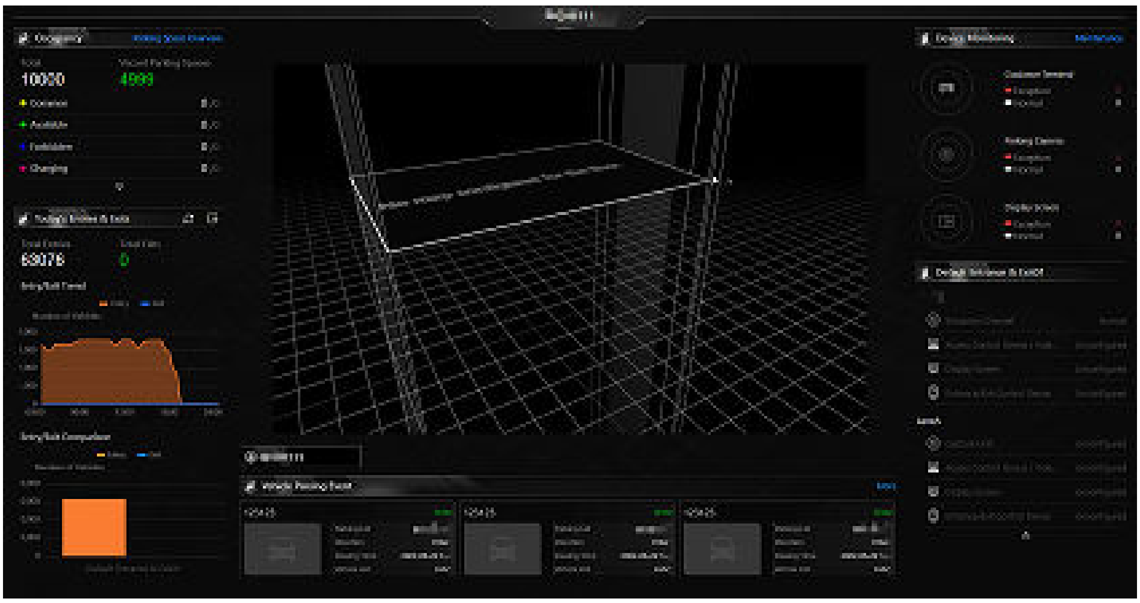


Figure 22-5 Parking Lot Overview Page

22.4.2 Add Parking Lot

You can add one or multiple parking lots for management, including adding entrances and exits, setting the number of parking spaces, editing the parking lot formation, setting entry & exit rules and parking fee rules.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. In the top right corner of the page, click **Add Parking Lot** to open the Add Parking Lot pane.

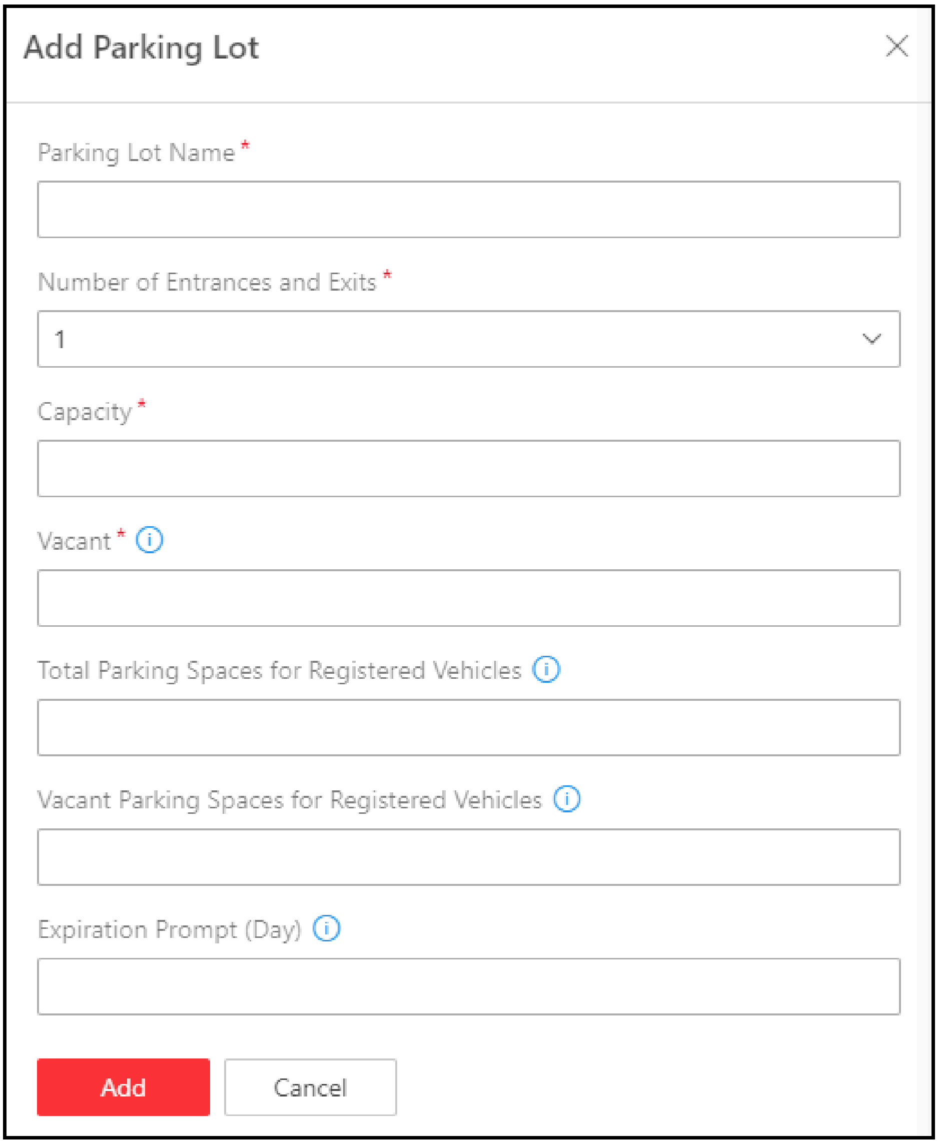


Figure 22-6 Add Parking Lot

3. Set the name, number of entrances and exits, the total parking capacity, and the number of vacant parking spaces for the parking lot, and set other related parameters as needed, such as the number of total/vacant parking spaces for registered vehicles, the number of days for displaying expiration prompts in advance, etc.

   Expiration Prompt (Day)

   Take a vehicle that expires on Jan. 6th, 2023 as an example, if you enter 5 here, the expiration prompt will be displayed on the LED screen linked to the parking lot from Jan. 1st, 2023 to Jan. 5th, 2023.

4. Click **Add** to create the parking lot.
5. **Optional:** Edit the parking lot as needed.

Delete a Parking Lot

In a parking lot area, click **Delete** to delete it.

Edit the Number of Vacant Parking Spaces

In a parking lot area, click above **Vacant** to edit it.

Edit the Number of Vacant Parking Spaces for Registered Vehicles

In a parking lot area, click above **Vacant Parking Spaces for Registered Vehicles** to edit it.

Edit Parking Lot Information

a. In a parking lot area, click **Settings → Basic Information** to enter the page of this parking lot.
b. In the upper-right corner, click **Edit** to open the Edit Parking Lot pane.

Note

You can also click on the top of the parking lot list to edit its information.

c. Edit the information of the parking lot, such as the name, capacity, etc.
d. Click **Save**.

Add Allowed Parking Duration

a. In a parking lot area, click **Settings → Basic Information** to enter the page of this parking lot.
b. On the right side of **Allowed Parking Duration**, click **Add**.
c. In the pop-up window, select a vehicle type from Vehicle List.
d. Enter the maximum parking duration allowed for the selected vehicle parked in the created parking lot.

Note

You can configure an event or alarm which will be triggered when a vehicle's parking is due. For example, if you enter 300 here, an event or alarm (if any) will be triggered if a vehicle of the selected type has parked longer than 5 hours (i.e., 300 minutes).

Add/Edit/Delete a Sub Parking Lot

In a parking lot area, click **Settings → Basic Information** to enter the page of this parking lot.

- On the top of the parking lot list, click to add a sub parking lot.
- Select a sub parking lot, and click on the top of the parking lot list or **Edit** in the upper-right corner to edit it.
- Select a sub parking lot and click on the top of the parking lot list to delete it.

22.4.3 Add Entrance and Exit

An entrance or exit helps control vehicles to enter/exit the parking lot or prevent vehicles from entering/exiting the parking lot. For example, the entrance or exit allows a vehicle in the allowlist to enter/exit the parking lot, and prevent a vehicle in the blocklist from entering the parking lot. You need to configure lanes linked with devices for an entrance and exit to control the barriers.

Before You Start

Make sure you have added a parking lot. See ***Add Parking Lot*** for details.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** of an added parking lot to enter the configuration page of this parking lot.
3. Select a parking lot from the left list and click .

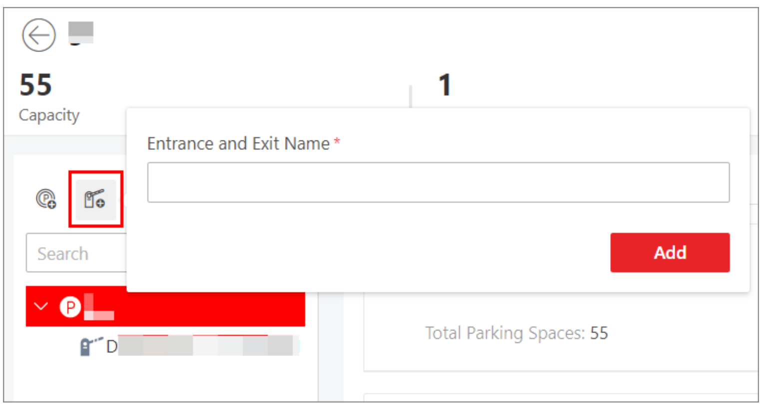


Figure 22-7 Add Entrance and Exit

4. Enter the name of the entrance and exit.
5. Click **Add**.
6. **Optional:** Perform the following operations if needed.

Edit an Entrance & Exit	Select an entrance & exit, and click to edit it.
Delete an Entrance & Exit	Select an entrance & exit, and click to delete it.

What to do next

Add lane for the entrance and exit. See ***Add Lane*** for details.

22.4.4 Add Lane

A lane is used to link different devices to realize different functions. For example, a lane linked with an entrance/exit control device is used for managing the entrance or exit of a parking lot, a lane linked with a capture unit (which can recognize a vehicle at the lane and compare the vehicle information with vehicles in a vehicle list) or card-swiping device (i.e., access control device and video intercom device) is used for controlling the barrier, a lane linked with a camera is used for capturing pictures, and a lane linked with a display screen is used for displaying information such as the number of vacant parking spaces.

Before You Start

Make sure you have added at least an entrance/exit for the parking lot. See ***Add Entrance and Exit*** for details.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** of an added parking lot to enter the configuration page of this parking lot.
3. Select an entrance & exit from the left list.
4. Click to enter the Add Lane page.

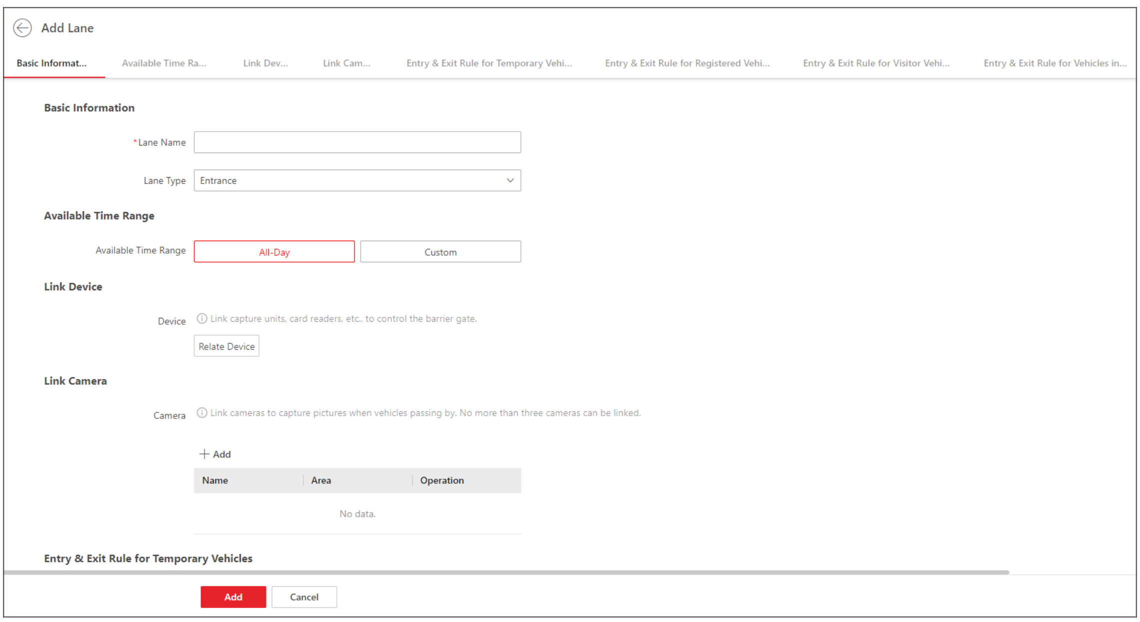


Figure 22-8 Add Lane Page

5. Set the lane.
   1) In the Basic Information area, create a name for the lane, and select **Entrance** or **Exit** as the lane type from the drop-down list.
   2) In the Available Time Range area, set the period during which the lane is available. Select **All-Day**, or select **Custom** to customize a period.
   3) **Optional:** In the Link Device area, click **Link to Device** to select device(s) to be linked to the lane, and set one device as the barrier control unit according to actual needs.

   Entrance/Exit Control Device

   An entrance/exit control device is used for managing the entrance or exit of a parking lot, especially that of an unattended parking lot. After a vehicle gets a ticket or card from an entrance/exit control device, the device will control the barrier gate to open and let the vehicle enter; after the vehicle returns the ticket or card, the device will allow the vehicle to exit. Besides, if an entrance/exit device assigns cards instead of tickets, its guidance screen is configurable. See ***Link Display Screen and Set Displayed Content*** for details.

Capture Unit

A capture unit is used for capturing and recognizing license plate number. For example, the capture unit will open the barrier to allow the vehicle to enter the parking lot when recognizing a license plate number in the vehicle list, and will not open the barrier to prevent the vehicle from entering the parking lot when recognizing a license plate number in the blocklist. See ***Configure Entry & Exit Rules*** for details about setting an entry & exit rule.

Note

You can link up to two capture units to a lane. If so, you need to set the **Matching Time**. Hence, when two capture units capture two pictures within the matching time, the picture captured by the capture unit with the higher confidence value will be kept.

Access Control Device

If the administrator selects a card (already issued to the owner for card authentication) for the owner when adding the owner's vehicle, the administrator actually binds the card with the vehicle's license plate number. So the barrier will open when the owner swipes the card on an access control device at the lane. In this circumstance, a capture unit is not needed.

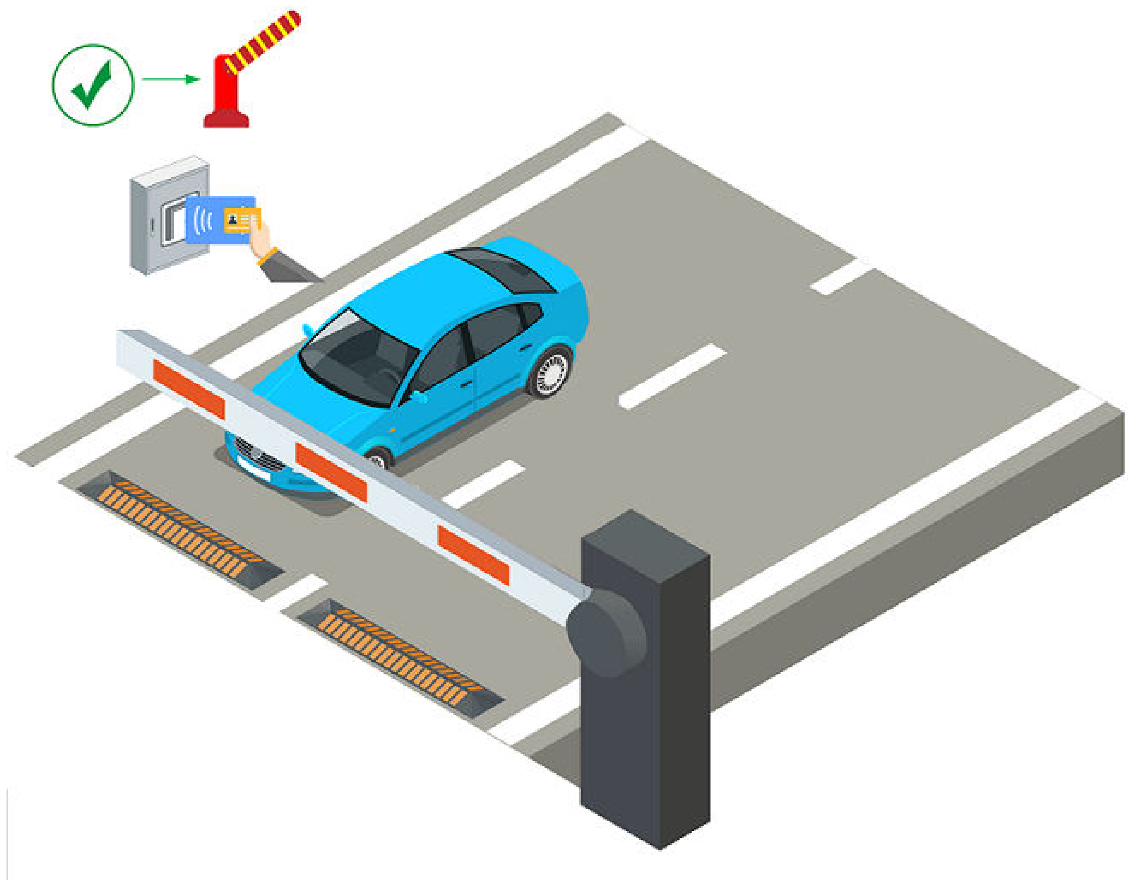


Figure 22-9 Opening Barrier by Card Swiping

Video Intercom Device

a. The vehicle owner calls the security guard by the video intercom device (some access control devices can also be used for video intercom).
b. The security guard verifies the owner's identity by viewing her/him by the video intercom device or the license plate number captured by a capture unit.
c. The security guard opens the barrier manually if the vehicle owner is authenticated.

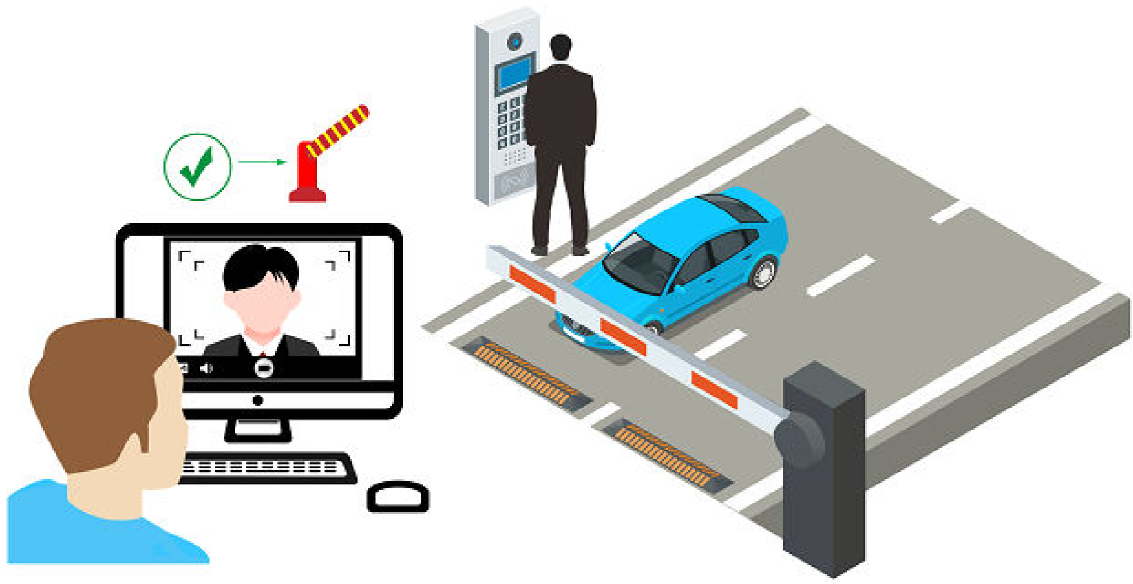


Figure 22-10 Opening Barrier by Video Intercom

Display Screen

A display screen is used for displaying information such as the number of vacant parking spaces, vehicle expiration date. See ***Link Display Screen and Set Displayed Content*** for details.

4) In the Link Camera area, select camera(s) to be linked to the lane.

Note

- Make sure you have enabled picture storage for the camera. Otherwise, you cannot see the captured pictures.
- Up to three different cameras can be linked to the lane.
- One camera can be linked to multiple lanes.
- You can view the pictures captured by the linked camera when viewing the vehicle-passing information.

5) Set the entry & exit rule for temporary vehicles, registered vehicles, and visitor vehicles, and vehicles in list. You can switch on **Same Rule as Parking lot** to use the rule for the parking lot, or switch it off to set a new rule.

Note

For how to configure entry & exit rules, refer to ***Configure Entry & Exit Rules*** .

6. Click **Add**.

22.4.5 Link Display Screen and Set Displayed Content

The display screen linked to the parking lot can be used for displaying information including the date and time, parking duration, license plate number, expiration prompt, etc.

Note

Make sure you have added display screens to the platform. See ***Add Display Screen*** for details about how to add a display screen.

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** of an added parking lot to enter the parking lot configuration page.
3. Click **Display Screen Configuration**.
4. Click **Relate Display Screen** and select a display screen on the Relate Display Screen pane to link a screen to the parking lot.
5. Click **Display Screen Configuration** beside the name of the display screen to open the Screen Configuration pane.

Configure Entrance and Exit Display Screen

Note

The parameters to be configured for the entrance and exit display screen vary according to the linkage between the screen and the lane. If the screen is linked with a lane, both the Vehicle Detected screen and the Idle screen should be configured. If the screen has not been linked with a lane, only the Idle screen is required to be configured.

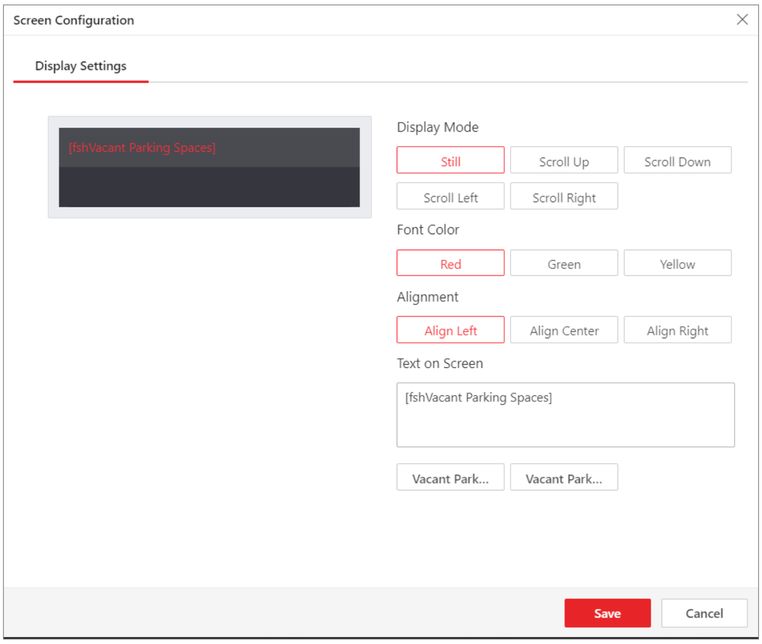


Figure 22-11 Configure the Entrance and Exit Display Screen Not Linked with a Lane

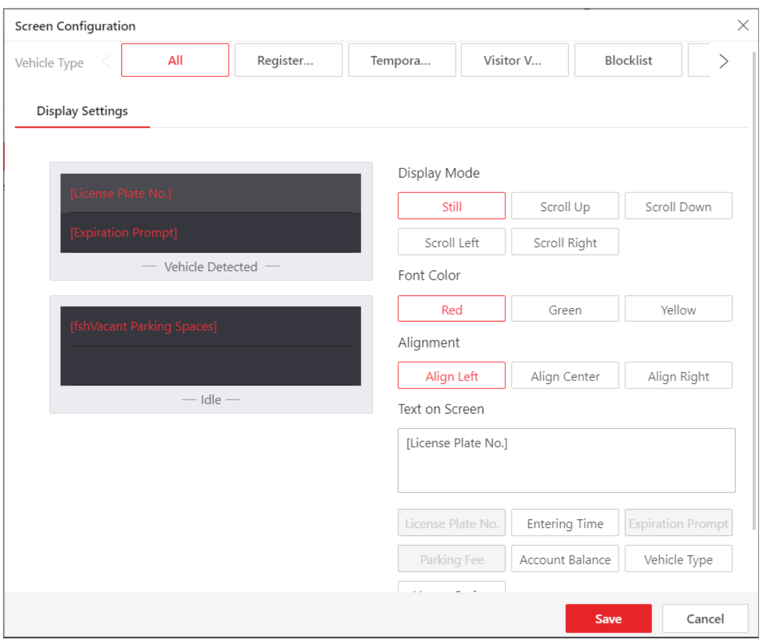


Figure 22-12 Configure the Entrance and Exit Display Screen Linked with a Lane

1. Select a vehicle type.

Note

Vehicle type is not configurable for the entrance and exit display screen not linked with a lane.

2. Configure the Vehicle Detected screen.

a. Click a line on the Vehicle Detected screen to set its **Display Mode**, **Font Color**, and **Alignment**.
b. Select the information to be displayed on the line from **Text on Screen**.

License Plate No.

Display the license plate number recognized by the capture unit. By default, this text is selected to be displayed on the screen linked with a lane.

Entering Time

The time when a recognized vehicle enters the parking lot. This text is selectable only when the display screen is linked with an entrance lane.

Exit Time

The time when a recognized vehicle exits the parking lot. This text is selectable only when the display screen is linked with an exit lane.

Parking Duration

Display the parking duration when the vehicle exits the parking lot.

Expiration Prompt

Inform the vehicle owners that their vehicles are about to expire. You need to enable the expiration prompt for a parking lot and set when to inform vehicle owners the expiration date. See ***Add Parking Lot*** for details. This text is selectable only when the display screen is linked with an exit lane.

Parking Fee

Display the parking fee to be paid when the vehicle exits the parking lot. This text is selectable only when the parking lot is in the Charge mode.

Account Balance

The balance in the vehicle owner's account.

Vehicle Type

Display the vehicle type recognized by the capture unit.

Vacant Parking Spaces

Display the number of vacant parking spaces on the selected floor with which the display screen is linked.

Vacant Parking Spaces in Vehicle List

Display the number of vacant parking spaces for vehicles in a vehicle list. However, in the case that a parking lot is used by more than one company at the same time, a vehicle list can be regarded as a company.

Entry and Exit Not Allowed Prompt

Inform the driver of reasons why the entry/exit is not allowed. For example, to remind the driver to pay the parking fee before exiting.

c. Configure other lines in the same way.

Note

There is only one line for displaying information on the screen not linked with a lane.

3. Configure the Idle screen in the same way you configure the Vehicle Detected screen.
4. Click **Save**.

Configure Indoor Guidance Screen

Note

The number of sub screens on the indoor guidance screen varies with the model. Here only take the model with one sub screen as an example.

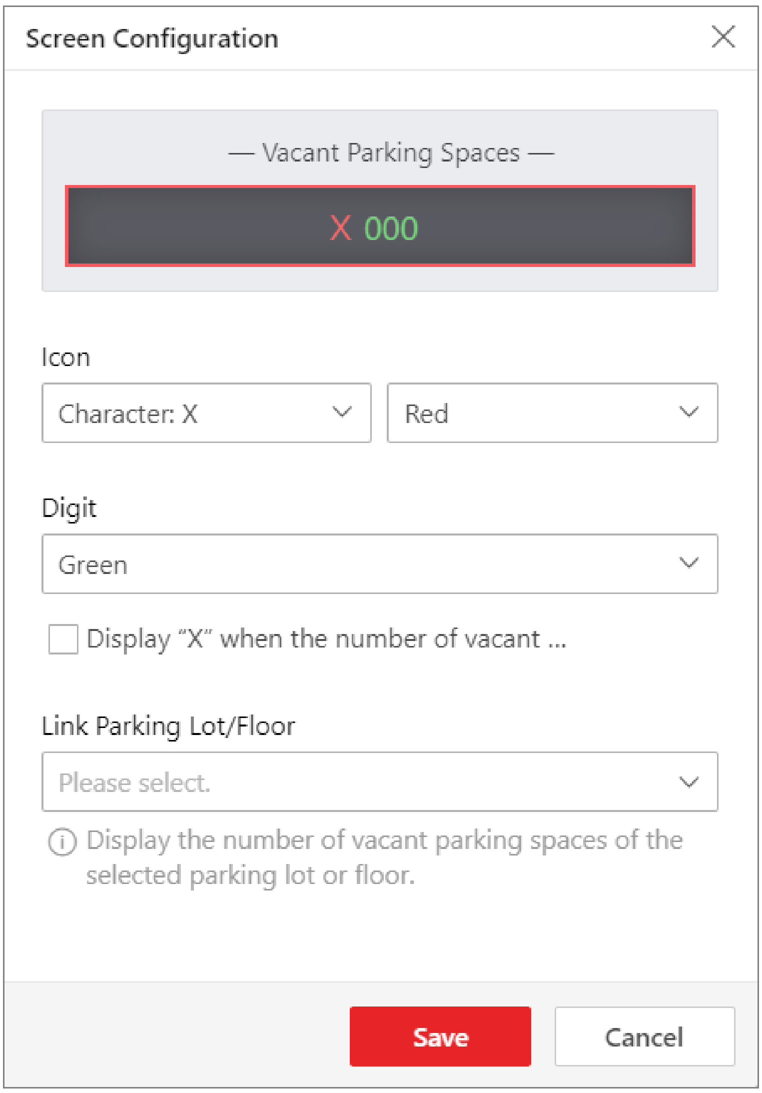


Figure 22-13 Configure Indoor Guidance Screen

1. Click a sub screen and select a icon type and color to be displayed.
2. Select a color for the digits displayed on the screen.

Note

If the current number of vacant parking spaces is 0, you can check the checkbox below the Digit field to display "X".

3. Select the parking lot(s) or floor(s) to be linked with the indoor guidance screen.

Note

If the linked parking lots contain sub parking lots, the parking space information of sub parking lots will be displayed by default. If the sub parking lots are linked, only the parking space information of sub parking lots will be displayed.

4. Click **Save**.

Configure Entrance Guidance Screen

Note

The number of sub screens on the entrance guidance screen varies with the product model. Here only take the product model with three sub screen as an example.

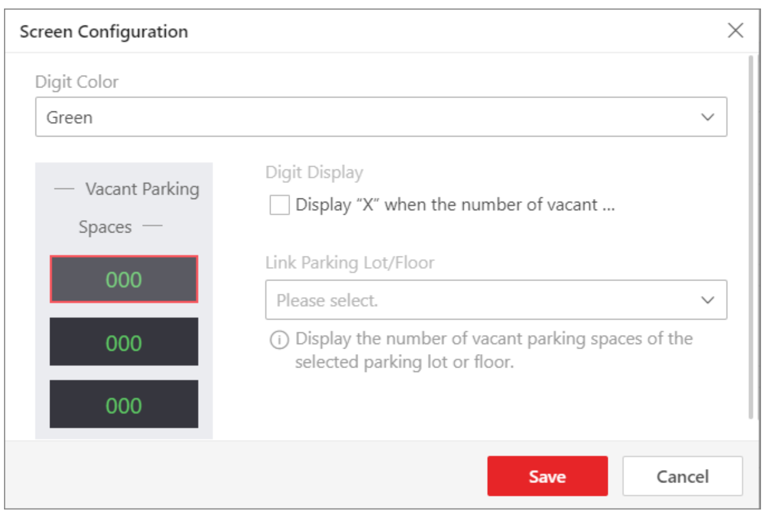


Figure 22-14 Configure Entrance Guidance Screen

1. Click a sub screen and select a color for the digits displayed on the screen.

Note

If the current number of vacant parking spaces is 0, you can check the checkbox below the Digit field to display "X".

2. Select the parking lot(s) or floor(s) to be linked with the indoor guidance screen.

Note

If the linked parking lots contain sub parking lots, the parking space information of sub parking lots will be displayed by default. If the sub parking lots are linked, only the parking space information of sub parking lots will be displayed.

3. Click **Save**.

22.4.6 Configure Entry & Exit Rules

The entry & exit rules define how to open the barrier gate when a vehicle is detected at the lane. You can set the vehicle entering & exiting verification mode for a parking lot, set entry & exit rules for different types of vehicles, including temporary vehicles, registered vehicles, visitor vehicles, and vehicles in list. You can also set an entry & exit rule for a special time period, such as a holiday. With this function, you can manage the entrances and exits in parking lots more easily.

Set Vehicle Verification Mode

You can set the vehicle entering & exiting verification mode and account deduction mode for a parking lot, which can help you manage the entry and exit of vehicles more easily.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Vehicle Verification Mode**.

Note

When the parking fee mode has been set to **Charge** in the basic configuration, the account deduction mode needs to be configured. Refer to ***Set Account Deduction Mode*** for details.

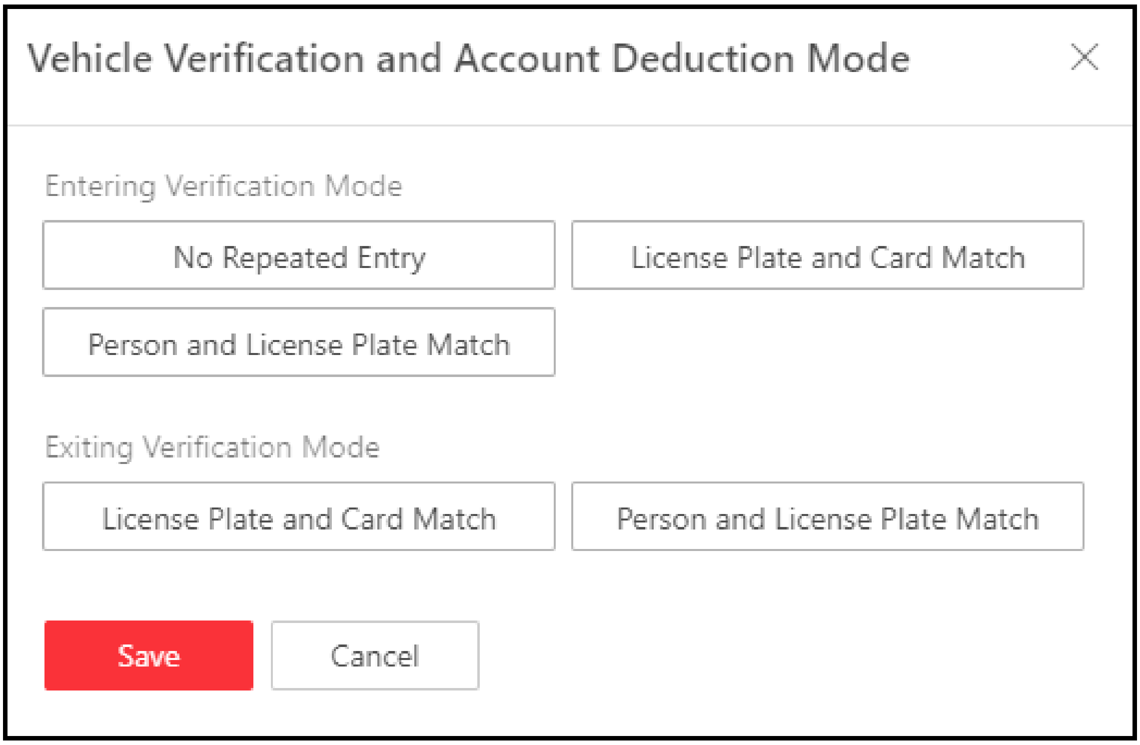


Figure 22-15 Set Vehicle Verification Mode

5. Select the entering verification mode and exiting verification mode accordingly.

Entering Verification Mode

The condition in which a vehicle is allowed to enter.

No Repeated Entry

Repeated entry for an vehicle is not allowed.

License Plate and Card Match

The vehicle is allowed to enter only when the license plate and the card match.

Person and License Plate Match

The vehicle is allowed to enter only when the driver and the license plate match.

Exiting Verification Mode

The condition in which a vehicle is allowed to exit.

6. Click **Save**.

Set Entry & Exit Rule for Temporary Vehicles

Temporary vehicles are the ones that are not added to the platform and just park in the parking lot for a certain period. You can set the entry & exit rule for temporary vehicles, which can help you to manage the entry and exit of them more easily.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Entry & Exit Rule for Temporary Vehicles** to open the following pane.

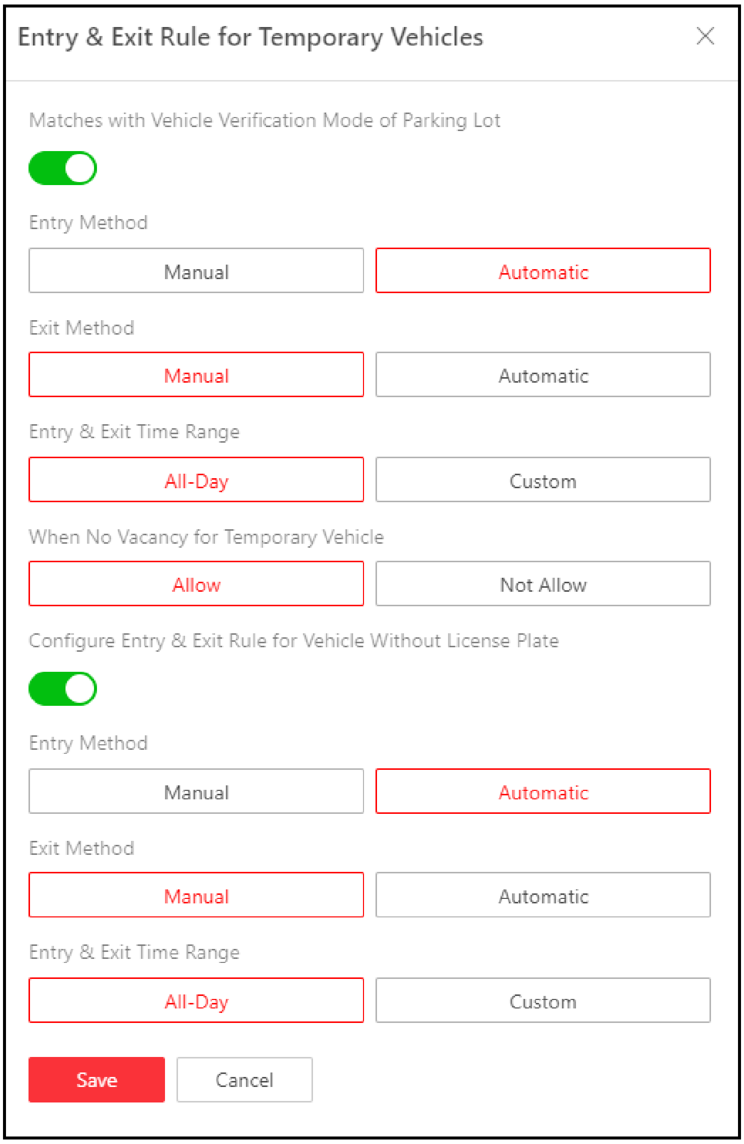


Figure 22-16 Entry & Exit Rule for Temporary Vehicles

5. Set the rule.

Matches with Vehicle Verification Mode of Parking Lot

Whether to use the same vehicle verification mode of the parking lot. It is enabled by default. You can switch it off to set the entering & exiting verification mode according to different types of vehicles. Refer to ***Set Vehicle Verification Mode*** for details.

Entry Method

How the barrier gate is opened when a vehicle enters.

Exit Method

How the barrier gate is opened when a vehicle exits.

Entry & Exit Time Range

The period in which the vehicles are allowed to enter and exit.

Note

This parameter is configurable only when one of the **Entry Method** and **Exit Method** or both of them are set to **Automatic**.

When No Vacancy for Temporary Vehicle

Whether to allow the temporary vehicles to enter when where are no vacant parking spaces.

Configure Entry & Exit Rule for Vehicle Without License Plate

Set a rule for the vehicle's automatic or manual passing at entry or exit without license plate.

6. Click **Save**.

Set Entry & Exit Rule for Registered Vehicles

Registered vehicles are the ones that have been added to the platform. You can set the entry & exit rule for registered vehicles, which can help you to manage the entry and exit of them more easily.

Before You Start

Make sure that at least one vehicle has been added to the platform.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Entry & Exit Rule for Registered Vehicles** to open the following pane.

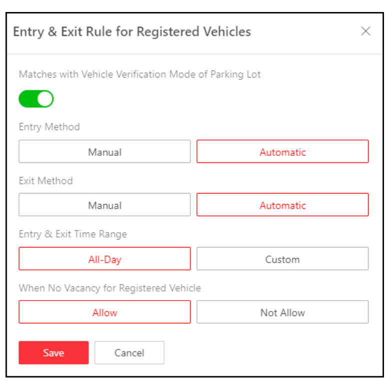


Figure 22-17 Entry & Exit Rule for Registered Vehicles

5. Set the rule.

Matches with Vehicle Verification Mode of Parking Lot

Whether to use the same vehicle verification mode of the parking lot. It is enabled by default. You can switch it off to set the entering & exiting verification mode according to different types of vehicles. Refer to ***Set Vehicle Verification Mode*** for details.

Entry Method

How the barrier gate is opened when a vehicle enters.

Exit Method

How the barrier gate is opened when a vehicle exits.

Entry & Exit Time Range

The period in which vehicles are allowed to enter and exit.

Note

This parameter is configurable only when one of the **Entry Method** and **Exit Method** or both of them are set to **Automatic**.

When No Vacancy for Registered Vehicle

Whether to allow the registered vehicles to enter when there are no vacant parking spaces.

6. Click **Save**.

Set Entry & Exit Rule for Visitor Vehicles

Visitor vehicles are the ones that are not added to the platform and are driven by visitors who come for a visit. You can set the entry & exit rule for visitor vehicles, which can help you to manage the entry and exit of them more easily.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Entry & Exit Rule for Visitor Vehicles** to open the following pane.

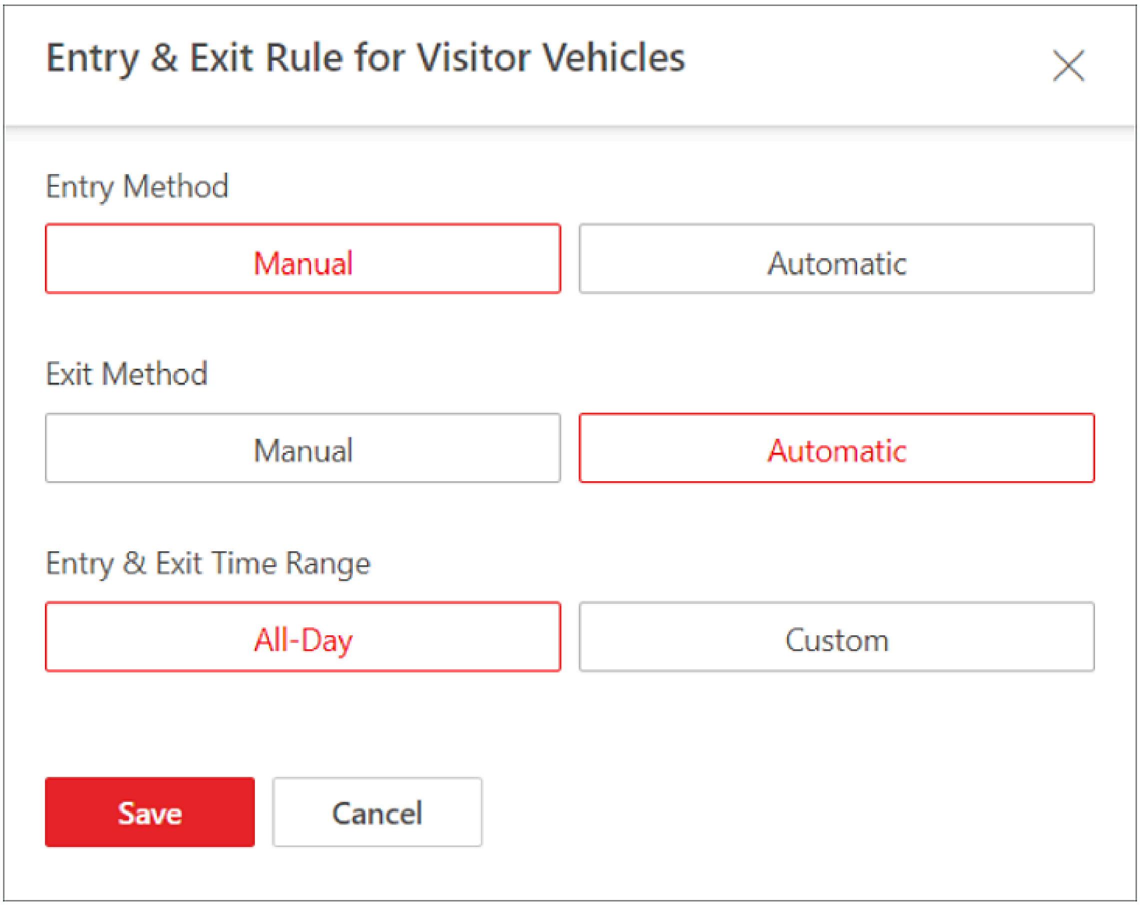


Figure 22-18 Entry & Exit Rule for Visitor Vehicles

5. Set the rule.

   Entry Method

   How the barrier gate is opened when a vehicle enters.

   Exit Method

   How the barrier gate is opened when a vehicle exits.

   Entry & Exit Time Range

   The time period when vehicles are allowed to enter and exit.

   Note

   This parameter is configurable only when one of the **Entry Method** and **Exit Method** or both of them are set to **Automatic**.

6. Click **Save**.

Add Entry & Exit Rule for Vehicles in List

Vehicles in list are the ones that have been added to the platform and managed in the list you created. You can add the entry & exit rule for a vehicle list, so that the entry and exit of all vehicles in this list will be controlled by the rule.

Before You Start
Make sure that at least one vehicle list has been added.

Steps
1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Add** beside **Entry & Exit Rule for Vehicles in List** to open the Add Rule pane.

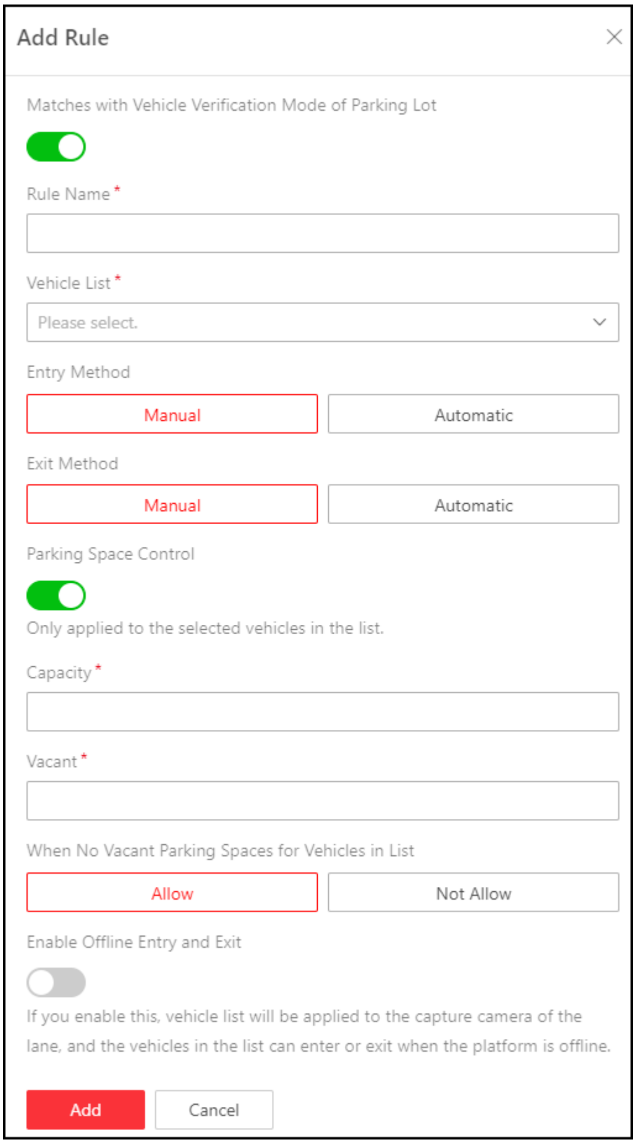


Figure 22-19 Add Rule

5. Set the rule.

Matches with Vehicle Verification Mode of Parking Lot

Whether to use the same vehicle verification mode of the parking lot. It is enabled by default. You can switch it off to set the entering & exiting verification mode according to different types of vehicles. Refer to ***Set Vehicle Verification Mode*** for details.

Vehicle List

The list of vehicles that the rule is applied to.

Entry Method

How the barrier gate is opened when a vehicle enters.

Exit Method

How the barrier gate is opened when a vehicle exits.

Entry & Exit Time Range

The period in which vehicles are allowed to enter and exit.

Note

This parameter is configurable only when one of the **Entry Method** and **Exit Method** or both of them are set to **Automatic**.

Parking Space Control

Note

If you switch on **Parking Space Control**, you need to configure the following parameters.

Capacity

The total number of parking spaces for vehicles in list.

Vacant

The number of vacant parking spaces for vehicles in list.

When No Vacant Parking Spaces for Vehicles in List

Whether to allow vehicles in list to enter when there are no vacant parking spaces.

6. Click **Add**.
7. **Optional:** Manage added rules.

Copy a Rule to Other Parking Lots	Click and select the parking lot(s) to which the rule is to be copied.
Edit a Rule	Click to edit a rule.
Delete a Rule	Click to delete a rule.

Add Entry & Exit Rule for Holidays

You can configure free entry and exit for vehicles during holidays or certain days of a week, which can help you to manage the entry and exit of vehicles in this period more easily.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Add** beside **Auto Entry & Exit on Holidays** to open the Add Holiday pane.

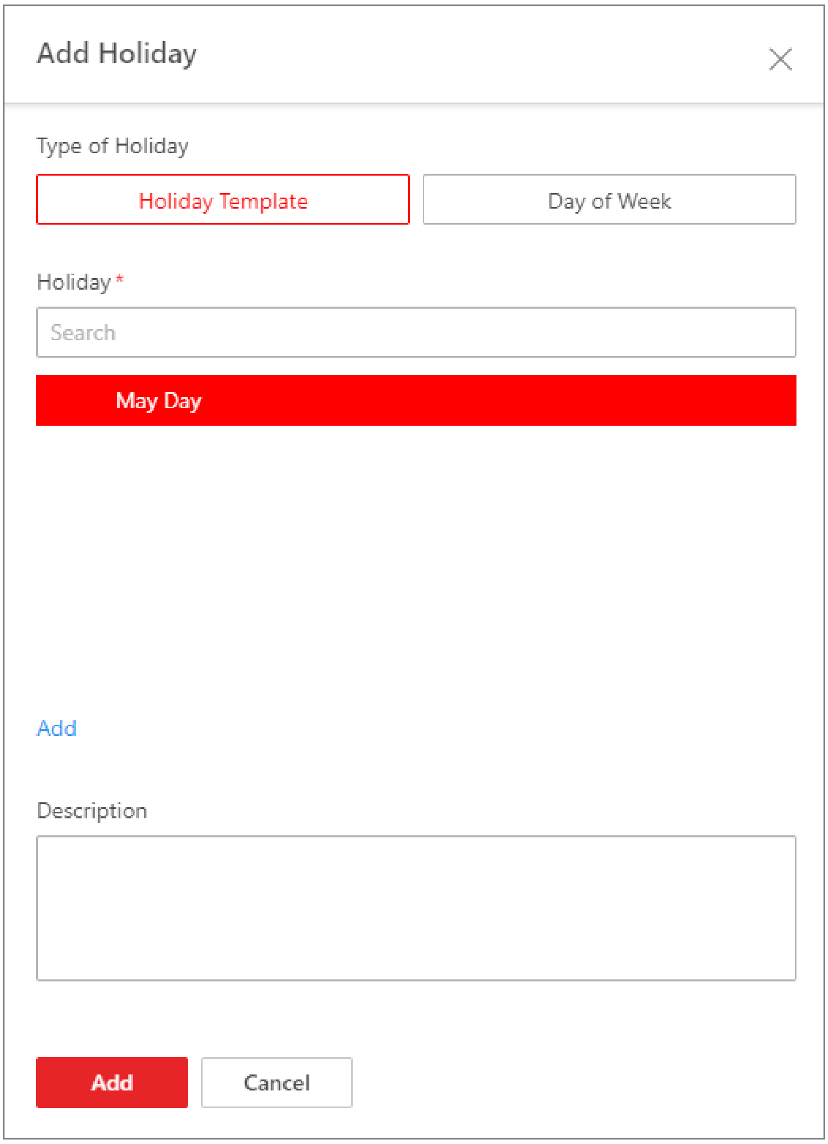


Figure 22-20 Holiday Template

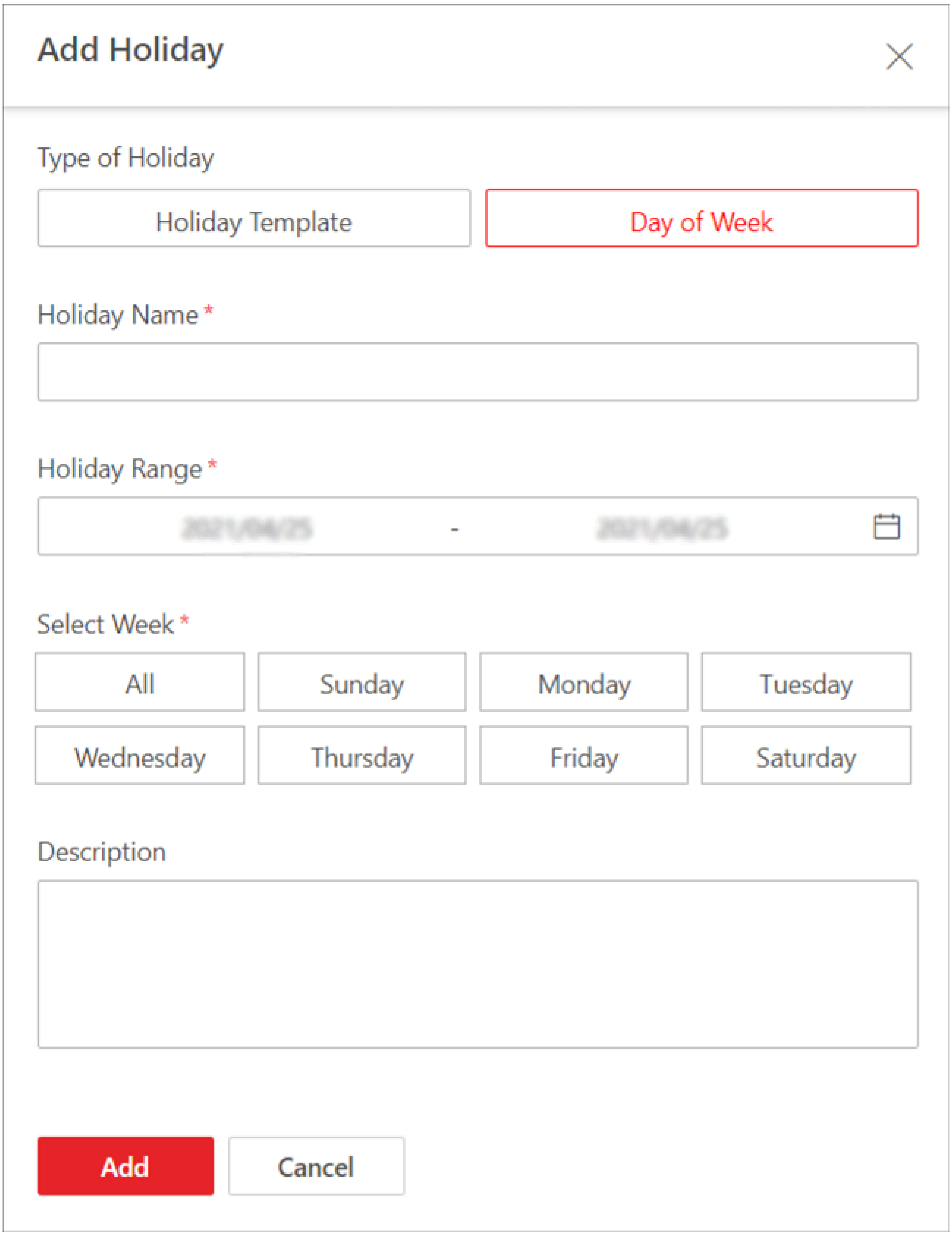


Figure 22-21 Day of Week

5. Select **Holiday Template** or **Day of Week** and complete relevant settings.

Holiday Template	a. Select a holiday from the list if any holiday has been added, or click **Add New** to create a new holiday. b. (Optional) Enter remarks in the Description field if needed. c. Click **Add**.
Day of Week	a. Create a name for the holiday. b. Click to set a time range for the holiday. c. Select the day(s) of a week that the rule is applied to. d. (Optional) Enter remarks in the Description field if needed. e. Click **Add**.

6. **Optional:** Manage added rules.

Copy a Rule to Other Parking Lots	Click and select the parking lot(s) to which the rule is to be copied.
Edit a Rule	Click to edit a rule.
Delete a Rule	Click to delete a rule.

Specify User to Receive Entry & Exit Calls

You can specify users to receive calls from the entry & exit devices on the Control Client, and then the user can remotely perform further operations for the vehicles, such as correcting license plate number and manually allowing passing.

On the left navigation pane, click **Basic Configuration → Call Recipient Settings** .

Click **Add** to select user(s) to receive entrance & exit calls on the Control Client.

Click next to a user name to open the **Receiving Range of Calling Event** pane and select entrances & exits in the list. The user will only receive calls from devices linked to the selected entrances & exits.

22.4.7 Configure Parking Fee Rules

You can set parking fee rules for parking lots, including adding parking fee rule for certain types of vehicles, adding parking pass rule, adding discount rule, adding parking fee rule for abnormal entry & exit. Once you set a rule, the platform will automatically calculate the fee for the parking based on this rule and present the information related to the fee.

Note

Make sure that the parking fee mode has been set to **Charge**. See ***Enable Parking Charge Mode*** for details.

Enable Parking Charge Mode

You can set the parking fee mode for parking lots, and select the type of currency to pay. This configuration will affect the functions related to parking fee.

Steps

1. On the left navigation pane, click **Basic Configuration → Parking Fee Mode** .

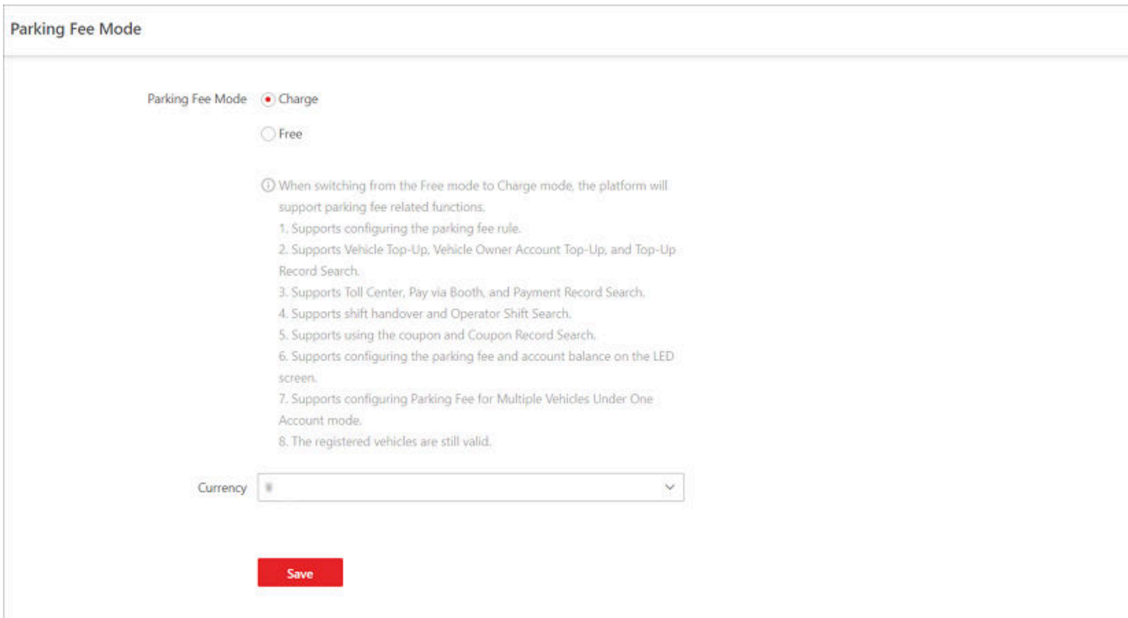


Figure 22-22 Parking Fee Mode Settings Page

2. Select **Charge** or **Free** as the parking fee mode.

Note

If you select **Free**, the settings related to parking fee are disabled.

3. Select a type of currency from the drop-down list.

Note

This step is valid only when you set the parking fee mode to **Charge**.

4. Click **Save**.

Set Account Deduction Mode

You can set the account deduction mode for a parking lot, which can help you manage parking fee payments more easily.

Before You Start

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Edit** beside **Vehicle Verification and Account Deduction Mode**.

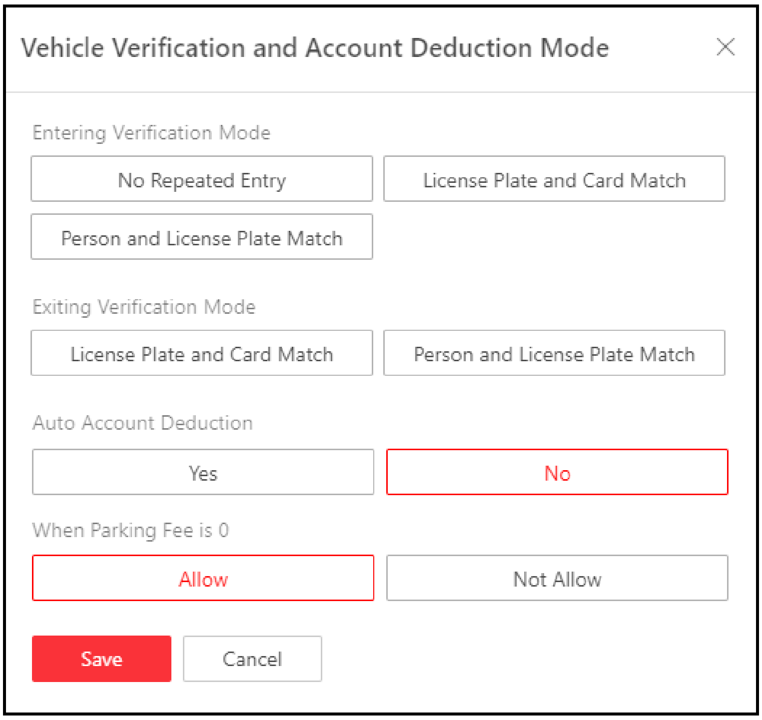


Figure 22-23 Vehicle Verification and Account Deduction Mode

5. Set the modes.

   Entering/Exiting Verification Mode

   The condition in which a vehicle is allowed to enter/exit the parking lot. Refer to ***Set Vehicle Verification Mode*** for details.

   Auto Account Deduction

   Whether to automatically deduct the parking fee from the vehicle owner's account.

   When Parking Fee is 0

   Whether to allow a vehicle to enter and exit when its parking fee is 0.

6. Click **Save**.

Add Parking Fee Rule for Temporary Vehicles

You can add parking fee rule for temporary vehicles, which can help you calculate parking fees more easily.

Before You Start

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Parking Fee Rule for Temporary Vehicles** to enter the Add Parking Fee Rule pane.

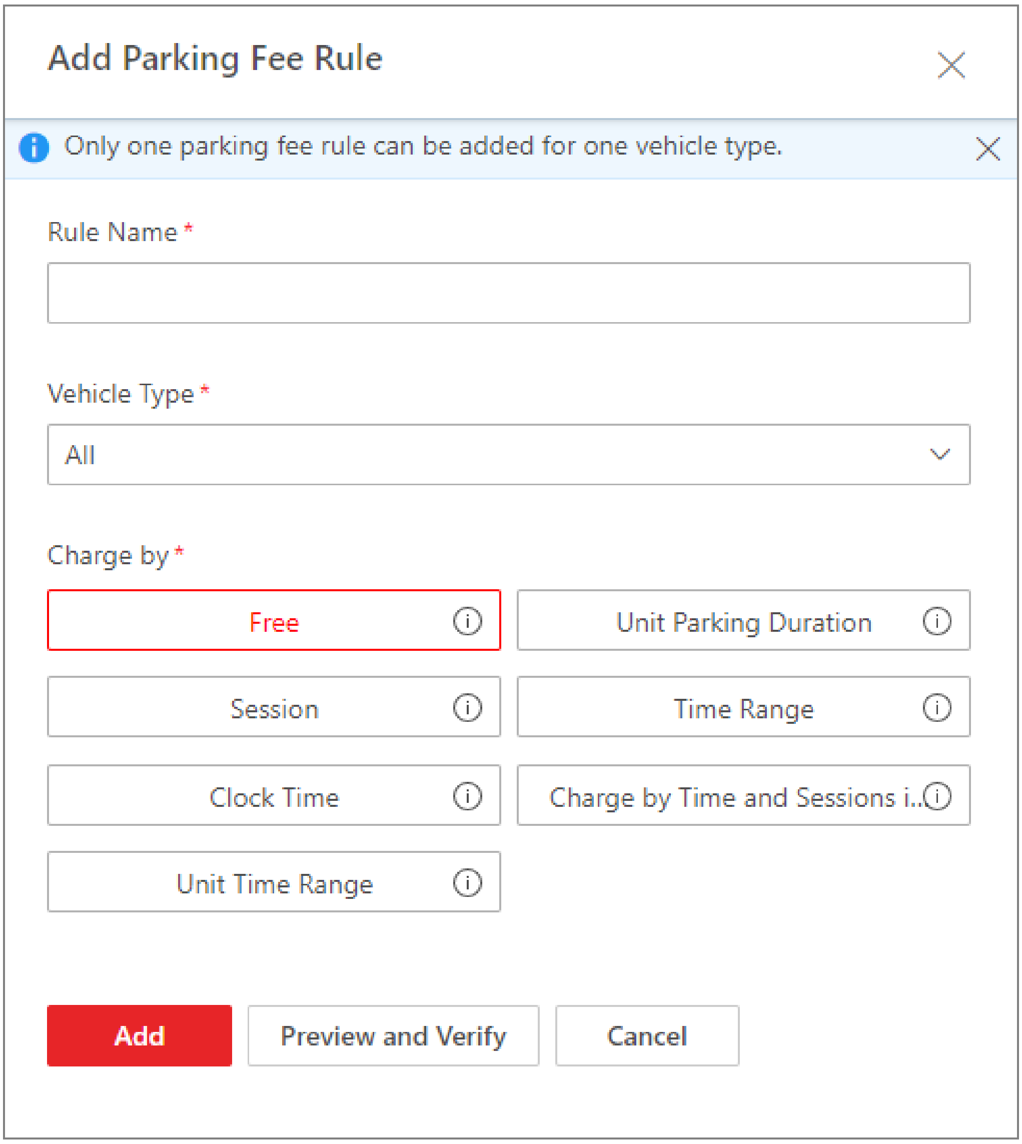


Figure 22-24 Add Parking Fee Rule for Temporary Vehicles

5. Create a name for the rule.
6. Select the type of vehicle to which the rule applies.

Note

No more than one rule can be added for each vehicle type.

7. Select the way by which vehicles of the selected type will be charged and complete the corresponding settings.

Free
No charge for any parking.

Unit Parking Duration
The duration of one parking is separated into different parts and these parts are charged different fees. For example, if a vehicle has parked for 2 hours, the

parking fee for the first hour is a specific amount, and the parking fee for the duration after the first hour is an another amount.

a. Enter the parking duration that is free of charge.
b. Enter the fee for the initial parking duration.
c. Enter the fee for subsequent parking duration.
d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

Session

The parking fee is charged by session. For example, if a vehicle has parked twice in a parking lot, its times of parking are counted as two sessions.

Enter the fee for each session.

Time Range

The parking fee is charged by the duration of a parking.

a. Enter the parking duration that is free of charge.
b. Enter a time range and the fee for a parking within this range.

Note

You can click **Add** to add different time ranges and fees.

c. Enter the fee for the duration beyond the maximum duration allowed.
d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

Clock Time

The parking fee is charged according to the time of a day.

a. Enter the parking duration that is free of charge.
b. Click to select a time range and enter the fee for a parking within this range.

Note

You can click **Add** to add different time ranges and fees.

c. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

Charge by Duration and Session in Daytime and Nighttime

The parking fee is charged according to the time of a day (daytime and nighttime).

a. Enter the parking duration that is free of charge.
b. Select **Free** or **Charge** when a parking exceeds the duration that is free of charge.
c. Click to set the time when daytime starts.

Note

The parking fee is charged by time range in daytime.

d. Enter the fee for the initial parking duration.
e. Enter the fee for subsequent parking duration.
f. Click to set the time when nighttime starts.

Note

The parking fee is charged by session in nighttime. You can select a charging mode from **Count One Entry and Exit as One Session** and **Count Multiple Entries and Exits as One Session** below.

g. Enter the fee for each parking.
h. (Optional) Switch on **Daily Max. Fee**, and enter the fee.
i. (Optional) Switch on **Charge by Daytime If Parking Duration Includes Daytime**.

Unit Time Range

The parking fee is charged by the time range of a day.

a. Enter the parking duration that is free of charge.
b. Select **Free** or **Charge** when a parking exceeds the duration that is free of charge.
c. Click to select a time range, and enter relevant information in **Charged Parking Duration**, **Parking Fee**, **Max. Fee**, and **Min. Threshold Duration**.

Note

You can click **Add** to add different time ranges and fees.

d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

8. **Optional:** Click **Preview and Verify** to preview and verify the rule.
9. Click **Add**.

Note

A temporary card will be issued for a temporary vehicle as it enters the parking lot for calculating its parking duration (see ***Issue Temporary Cards*** for details), and the parking fee can be paid accordingly in the toll center (see ***Pay in Toll Center*** for details).

10. **Optional:** Perform the following operations if needed.

Copy a Rule to Other Parking Lot(s)	Click and select the parking lot(s) to which the rule is to be copied.
Edit a Rule	Click to edit a rule.
Delete a Rule	Click to delete a rule.

Add Parking Fee Rule for Registered Vehicles

A parking pass costs a certain amount of money. Within the validity period of a parking pass, the vehicle can enter and exit a specific parking lot as a registered vehicle, so that it can park in that parking lot without paying any fees. You can add rules for parking passes.

Before You Start

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Parking Fee Rule for Registered Vehicle** to enter the Add Parking Pass Rule pane.

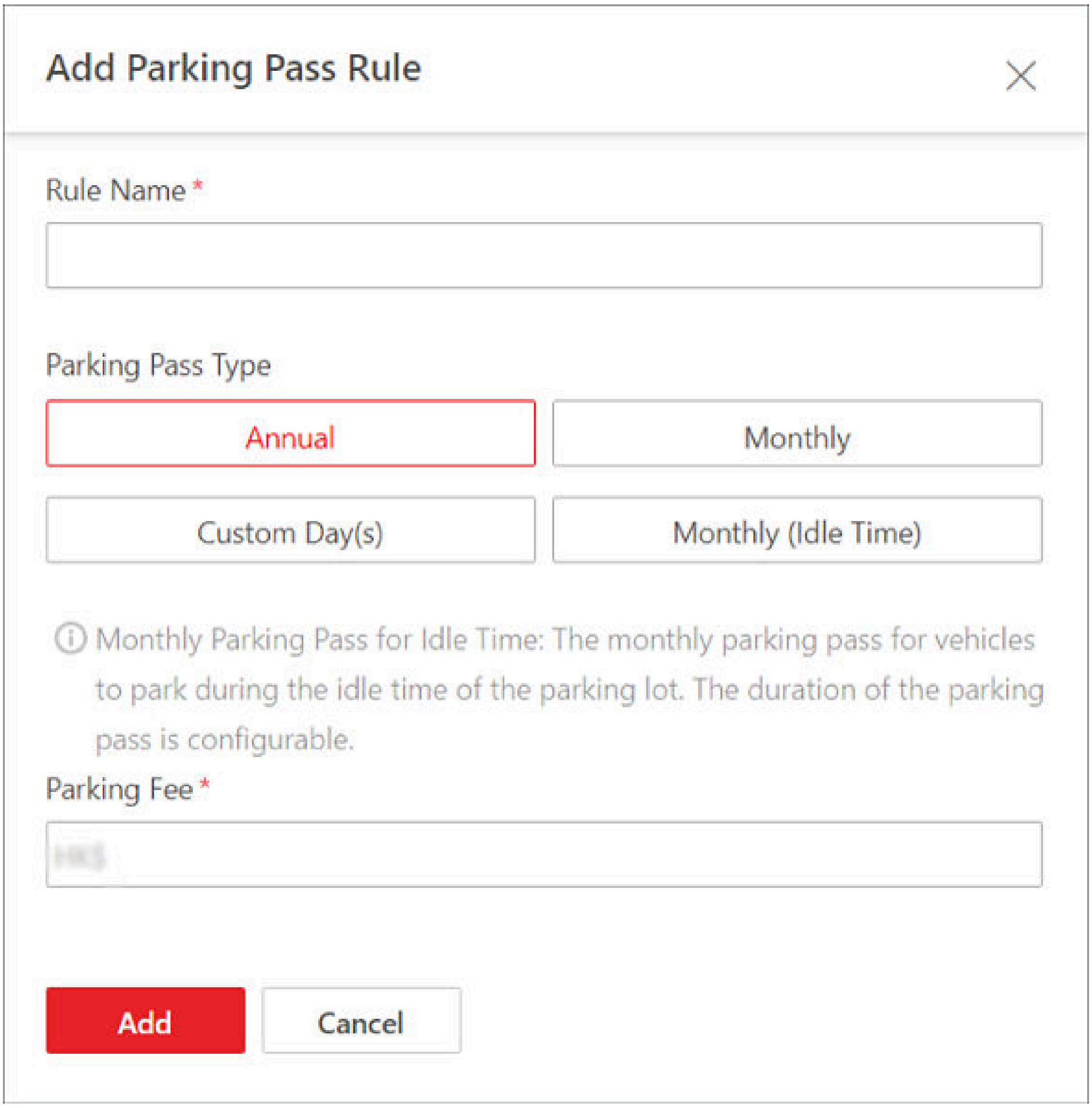


Figure 22-25 Add Parking Pass Rule Pane

5. Create a name for the rule.
6. Select a type for the parking pass and complete the corresponding settings.

Annual/ Monthly	Enter the fee for an annual/monthly parking pass.

Custom Day(s)	Enter the valid days of a parking pass and the fee for it.
Monthly (Idle Time)	Select a template of monthly parking pass for idle time from the drop-down list, and enter the fee for the parking pass.

Note

- This parking pass is used during the period in which the parking lot is not busy (in idle time).
- If you have not added any template, you need to click **Template of Monthly Parking Pass for Idle Time** to create a template first.

7. Click **Add**.

Note

Vehicle owners can top up their parking passes as needed. Refer to ***Top Up Parking Pass*** for details.

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

Copy a Rule to Other Parking Lot(s)	Click and select the parking lot(s) to which the rule is to be copied.
Edit a Rule	Click to edit a rule.
Delete a Rule	Click to delete a rule.

Add Parking Fee Rule for Vehicles in List

You can add parking fee rule for vehicles in list, which can help you calculate parking fees more easily.

Before You Start

- Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.
- Make sure that at least one vehicle list has been added.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Parking Fee Rule for Vehicles in List** to enter the Add Parking Fee Rule pane.
5. Create a name for the rule.
6. Select a vehicle list from the drop-down list.

Note

No more than one rule can be added for each vehicle list.

7. Select the way by which vehicles in the selected list will be charged and complete the corresponding settings.

Free
No charge for any parking.

Unit Parking Duration
The duration of one parking is separated into different parts and these parts are charged different fees. For example, if a vehicle has parked for 2 hours, the parking fee for the first hour is a specific amount, and the parking fee for the duration after the first hour is an another amount.

a. Enter the parking duration that is free of charge.
b. Enter the fee for the initial parking duration.
c. Enter the fee for subsequent parking duration.
d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

Session
The parking fee is charged by session. For example, if a vehicle has parked twice in a parking lot, its times of parking are counted as two sessions.

Enter the fee for each session.

Time Range
The parking fee is charged by the duration of a parking.

a. Enter the parking duration that is free of charge.
b. Enter a time range and the fee for a parking within this range.

Note

You can click **Add** to add different time ranges and fees.

c. Enter the fee for the duration beyond the maximum duration allowed.
d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

Clock Time
The parking fee is charged according to the time of a day.

a. Enter the parking duration that is free of charge.
b. Click to select a time range and enter the fee for a parking within this range.

Note

You can click **Add** to add different time ranges and fees.

c. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

Charge by Duration and Session in Daytime and Nighttime
The parking fee is charged according to the time of a day (daytime and nighttime).

a. Enter the parking duration that is free of charge.
b. Select **Free** or **Charge** when a parking exceeds the duration that is free of charge.
c. Click to set the time when daytime starts.

Note

The parking fee is charged by time range in daytime.

d. Enter the fee for the initial parking duration.
e. Enter the fee for subsequent parking duration.
f. Click to set the time when nighttime starts.

Note

The parking fee is charged by session in nighttime. You can select a charging mode from **Count One Entry and Exit as One Session** and **Count Multiple Entries and Exits as One Session** below.

g. Enter the fee for each parking.
h. (Optional) Switch on **Daily Max. Fee**, and enter the fee.
i. (Optional) Switch on **Charge by Daytime If Parking Duration Includes Daytime**.

Unit Time Range

The parking fee is charged by the time range of a day.

a. Enter the parking duration that is free of charge.
b. Select **Free** or **Charge** when a parking exceeds the duration that is free of charge.
c. Click to select a time range, and enter relevant information in **Charged Parking Duration**, **Parking Fee**, **Max. Fee**, and **Min. Threshold Duration**.

Note

You can click **Add** to add different time ranges and fees.

d. (Optional) Switch on **Daily Max. Fee**, and enter the fee.

8. **Optional:** Click **Preview and Verify** to preview and verify the rule.
9. Click **Add**.

Note

A temporary card will be issued for a temporary vehicle as it enters the parking lot for calculating its parking duration (see ***Issue Temporary Cards*** for details), and the parking fee can be paid accordingly in the toll center (see ***Pay in Toll Center*** for details).

10. **Optional:** Perform the following operations if needed.

Copy a Rule to Other Parking Lot(s)	Click and select the parking lot(s) to which the rule is to be copied.
Edit a Rule	Click to edit a rule.
Delete a Rule	Click to delete a rule.

Add Discount Rule

You can add the discount rule to manage parking fee more flexibly.

Before You Start
Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

Steps
1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Discount Rule** to enter the Add Discount Rule panel.
5. Create a name for the rule.
6. Select a discount method and complete relevant settings.

Discount	Here you can set a discount rate. For example, if you enter 70, the discount rate is 70%. If the parking fee due is 100 RMB, the actual amount tendered is 70 RMB.
Fee Discount	Here you can set a discount amount. For example, if you enter 70 and the parking fee due is 100 RMB, the actual amount tendered is 30 RMB.
Free	Here you can set a period during which the vehicles are allowed to park without being charged.
Parking Duration Reduction	Here you can set a duration which will be deducted from the total parking duration. For example, if you enter 2 and the parking duration of a vehicle is 6 hours, the actual duration counted for parking fee is 4 hours.

7. Click **Save**.
8. **Optional:** Perform the following operations as needed.

Issue & Print a Rule	Click to issue and print the discount rule in the coupon format.
Copy Rule to Other Parking Lots	Click and select the parking lot(s) that the rule is copied to.
Edit a Rule	Click to edit the rule.
Delete a Rule	Click to delete the rule.

Add Parking Fee Rule for Abnormal Pass

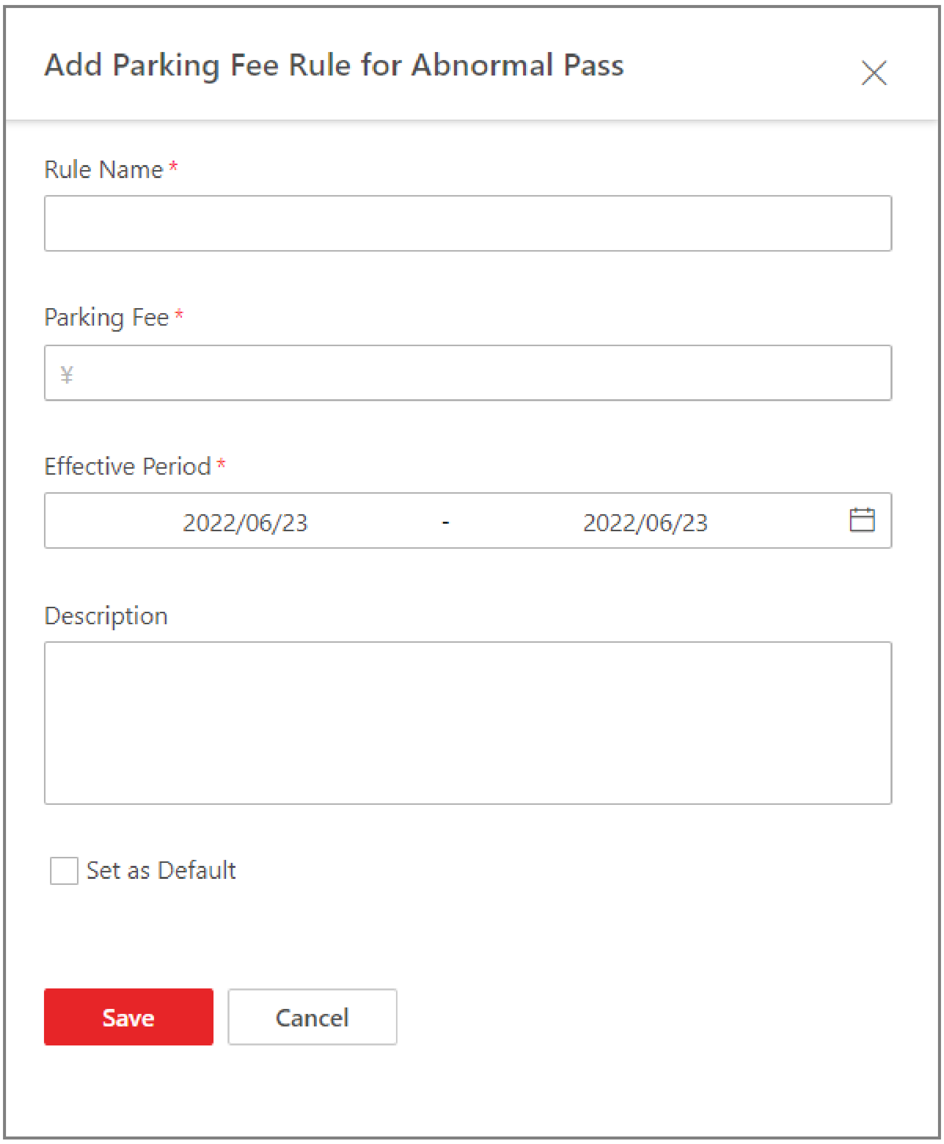
You can add parking fee rule for abnormal pass (e.g., a vehicle with an entry record but without an exit record), which can help you manage abnormal entries and exits more easily.

Before You Start

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add** beside **Parking Fee Rule for Abnormal Pass**.



5. Create a name for the rule.
6. Enter the parking fee for abnormal pass.
7. Set a validity period for the rule.
8. **Optional:** Enter remarks in the Description field as needed.
9. **Optional:** Check **Set as Default** to set the rule as the default rule for abnormal entry & exit.

10. Click **Save**.

Note

The parking fees incurred in this case will have to be paid at the booth or in the toll center. See ***Pay in Toll Center*** for details.

11. **Optional:** Perform the following operations as needed.

Copy a Rule to Other Parking Lot(s)	Click and select the parking lot(s) to which the rule is to be copied.
Edit a Rule	Click to edit a rule.
Delete a Rule	Click to delete a rule.

Set Additional Parking Fee Rule

You can set additional parking fee rules, including free parking duration after payment, and the parking fee rule for multiple vehicles under one account, which can help you to manage parking fee more flexibly.

Before You Start

Make sure that the parking fee mode has been set to **Charge**. Refer to ***Enable Parking Charge Mode*** for how to set the parking fee mode.

Steps

1. On the left navigation pane, click **Parking Lot Management**.
2. Click **Settings** to enter the settings page of a parking lot.
3. Click the **Parking Fee Rule** tab.
4. Click **Edit** beside **Additional Configuration** to open the Additional Configuration pane.

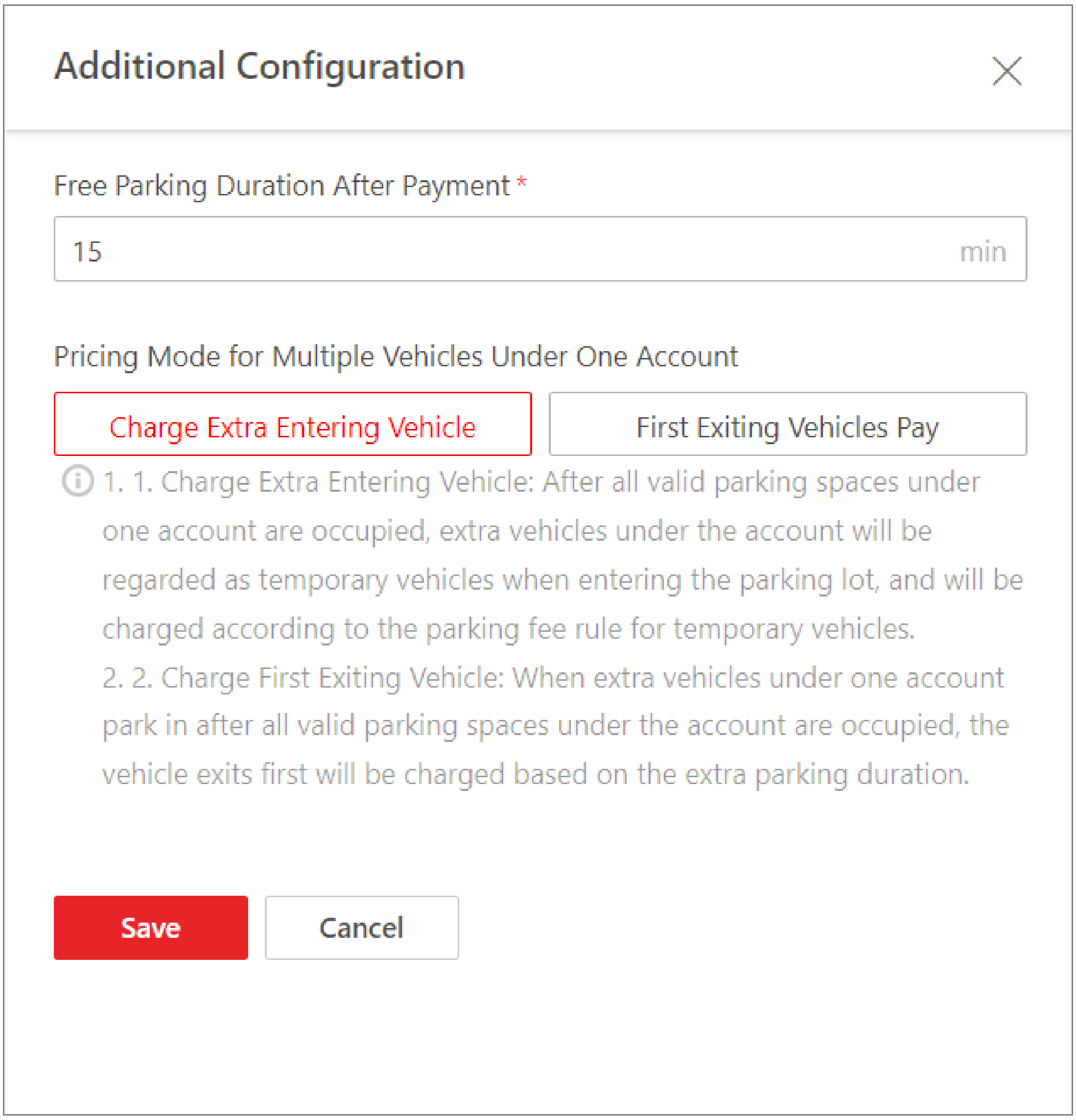


Figure 22-27 Additional Configuration

5. Enter the parking duration that is free of charge after paying the parking fee.
6. **Optional:** Set the parking fee rule for multiple vehicles under one account to **Extra Vehicles Pay** or **First Exiting Vehicles Pay**.

   Extra Vehicles Pay

   After all valid parking spaces under one account are occupied, extra vehicles under the account will be regarded as temporary vehicles when entering the parking lot, and charged according to the parking fee rule for temporary vehicle.

   First Exiting Vehicles Pay

When extra vehicles under one account park in after all valid parking spaces under the account are occupied, the vehicle exiting first will be charged based on the extra parking duration.

7. Click **Save**.

Issue Temporary Cards

You can add temporary cards to parking lots. The temporary cards are mainly designed for temporary vehicles. Before a temporary vehicle enters a parking lot, the driver needs to take a temporary card from the machine. Before exiting the parking lot, the driver needs to return the card and pay the parking fee.

Steps

1. On the left navigation pane, click **Temporary Card**.

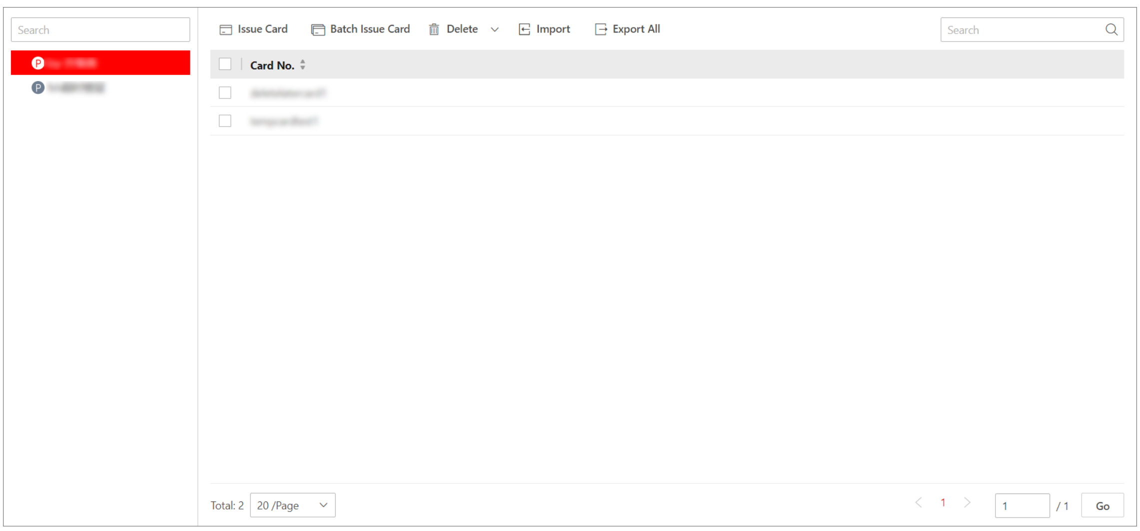


Figure 22-28 Issue Temporary Card Page

2. Select a parking lot from the left list.
3. Click **Issue Card**.

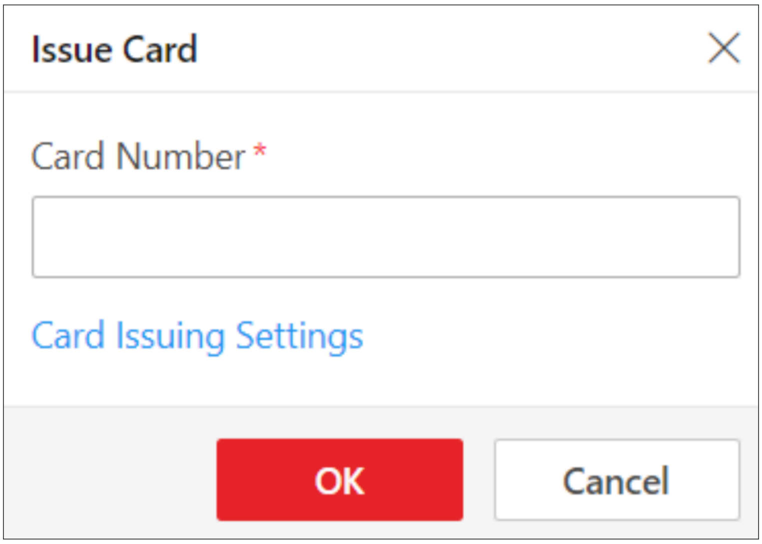


Figure 22-29 Issue Card Window

4. Enter the card number.
5. **Optional:** Click **Card Issuing Settings** to set card issuing parameters.
6. Click **OK**.

   The card will be added to the selected parking lot.
7. **Optional:** Perform the following operations as needed.

Batch Issue Cards	Click **Batch Issue Card** to issue multiple temporary cards at the same time.
Delete Selected Card(s)	Select the temporary card(s) and click **Delete** to delete the selected card(s).
Delete All Cards	Click next to **Delete**, and click **Delete All** to delete all temporary cards of the selected parking lot.
Import Temporary Card Information	Click **Import**, click , select a template file from your PC, and click **Import**. **Note** • You can click **Download Template** and save the predefined template (in XLSX format) to the local PC. • You can check **Auto Replace Duplicate Card No.** to allow the platform to overwrite card numbers that already exist.
Export Temporary Card Information	Click **Export All** to save the information about all temporary cards added for the selected parking lot to the local PC.
Search for Temporary Cards	Enter a keyword in the search box and click to search for temporary cards by card number.

22.5 Methods for Parking Charges

There are several ways to pay for parking in paid parking lots for different types of vehicles. Registered vehicles can park in a parking lot without paying additional fees if they or their owners have been topped up with a parking pass, whereas other vehicles (e.g., temporary vehicles, vehicles in list, and vehicles with abnormal entries/exits) can pay at the booth or in the toll center by searching for their parking information by license plate No., swiping the temporary card, or scanning the parking receipt.

22.5.1 Top Up Parking Pass

A parking pass costs a certain amount of money and is valid for a specific time period. You can top up parking passes by vehicle or by person (vehicle owner) in Top-Up Management.

On the left navigation pane, click **Top-Up Management**.

When vehicles or vehicle owners have been topped up with parking passes, you can perform the following operations.

In Top-Up by Vehicle Mode

- Click a license plate No. in the list to enter the parking pass details page of the vehicle. The parking pass information and the vehicle owner (if configured) information card are displayed.
- On the vehicle owner information card, click **Top-Up** / **Refund** to top up / refund the account. You can also click **Settings** to set the upper limit for auto deduction and low balance notice.
- In the upper-right corner, click **Add Parking Pass** to top up by vehicle.
- Click **Top-Up** of a parking lot to renew the parking pass of the vehilce in this parking lot.

In Top-Up by Person Mode

- Click a vehicle owner name in the list to enter the parking pass details page of the person.
- On the vehicle owner information card, click **Top-Up** / **Refund** to top up / refund the account. You can also click **Settings** to set the upper limit for auto deduction and low balance notice.
- In the upper-right corner, click **Add Parking Pass** to top up by person.

Top Up by Vehicle

If a vehicle is topped up with a parking pass, within the effective period, it can enter, park in, and exit a specific parking lot as a registered vehicle without paying any fees. You can top up parking passes for one or multiple vehicles at the same time.

Before You Start
Make sure you have added parking pass rule(s) to the platform. See ***Add Parking Fee Rule for Registered Vehicles*** for more details.

Steps

1. On the left navigation pane, click **Top-Up Management**.
2. Click **Top-Up by Vehicle** in the upper-right corner.
3. Select one or multiple vehicles in the list, and click **Top-Up** in the upper-left corner.

Note

You can also click **Top Up All** to top up for all vehicles in the list.

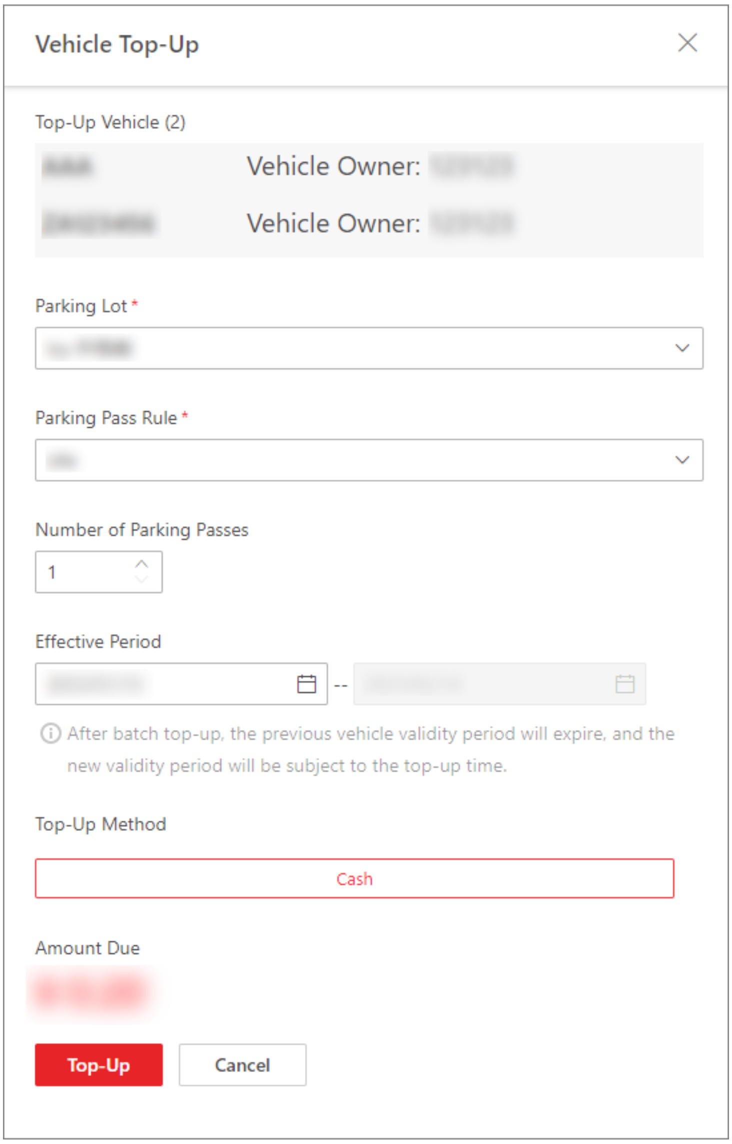


Figure 22-30 Vehicle Top-Up Pane

4. Select a parking lot for the vehicle(s) to park in.
5. Select a parking pass rule from the drop-down list.
6. Set the number of parking passes to be topped up.

Example

If the number here is set to 2 and the type of parking pass you selected in **Parking Pass Rule** is an annual pass, the parking pass will be valid for 2 years.

7. Set the effective period of the parking pass.

Note

- You can only select the start date for the parking pass; the end date will be automatically calculated by the platform according to the parking pass rule and the number of parking passes you set.
- For a monthly parking pass, you can select the effective period as **Natural Month** or **30 Days**. For example, when the start date of the effective period is 2023/7/10, if **Natural Month** is selected, the end date will be 2023/8/10, and the total effective period is 31 days.

8. Select the top-up method.

Note

Currently, the platform only supports cash top-ups when you are topping up for more than one vehicle, whereas you can select from **Cash** and **Account Balance** when topping up for one vehicle only. The amount due will be automatically calculated according to the parking pass rule and the number of parking passes you set.

9. Click **Top-Up**.

A result window will pop up and you can click **Print Receipt** to print the top-up receipt.

Top Up by Person

If a vehicle owner is topped up with a parking pass, within the effective period, one of vehicles linked to this person can enter, park in, and exit the specific parking lot without paying any fees. You can top up parking passes for one or multiple vehicle owners at the same time.

Before You Start

Make sure you have added parking pass rule(s) to the platform. See ***Add Parking Fee Rule for Registered Vehicles*** for more details.

Steps

1. On the left navigation pane, click **Top-Up Management**.
2. Click **Top-Up by Person** in the upper-right corner.
3. Select one or multiple vehicle owners in the list, and click **Top-Up** in the upper-left corner.

Note

You can also click **Top Up All** to top up for all vehicle owners in the list.

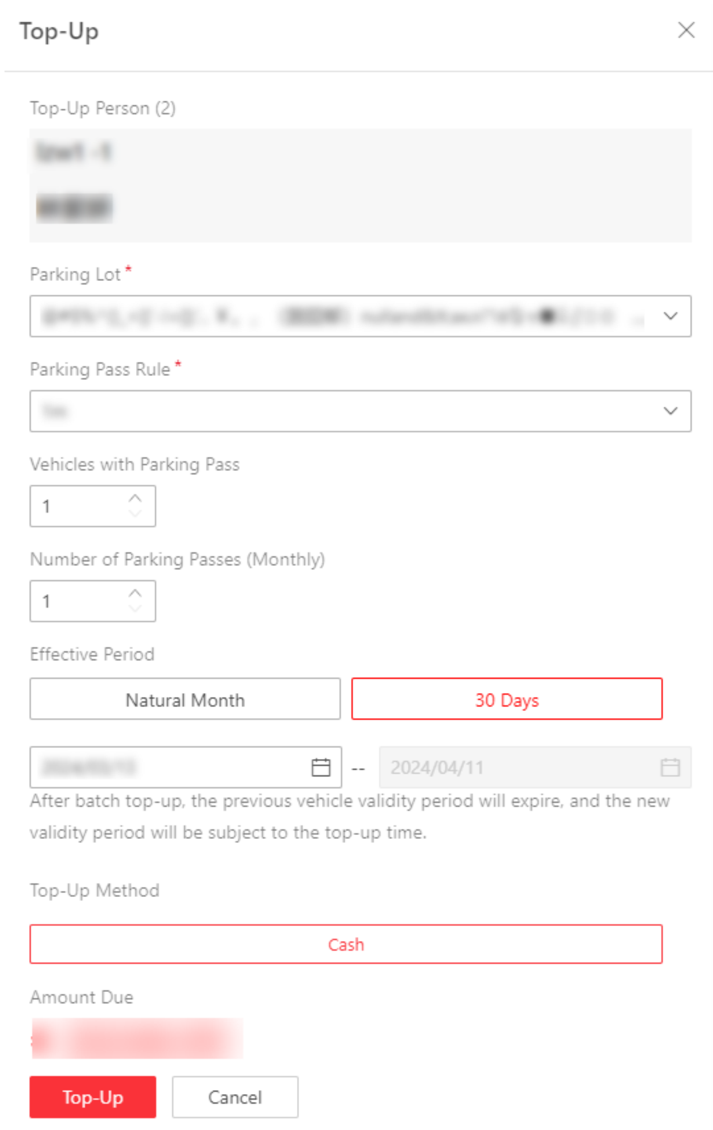


Figure 22-31 Person Top-Up Pane

4. Select a parking lot for the vehicle(s) to park in.
5. Select a parking pass rule from the drop-down list.
6. Set the number of vehicles with parking pass.

   Example

   If the number here is set to 2, parking passes for two vehicles of the owner will be topped up.
7. Set the number of parking passes to be topped up.

   Example

   If the number here is set to 2 and the type of parking pass you selected in **Parking Pass Rule** is an annual pass, the parking pass will be valid for 2 years.
8. Set the effective period of the parking pass.

Note

- You can only select the start date for the parking pass; the end date will be automatically calculated by the platform according to the parking pass rule and the number of parking passes you set.
- For a monthly parking pass, you can select the effective period as **Natural Month** or **30 Days**. For example, when the start date of the effective period is 2023/7/10, if **Natural Month** is selected, the end date will be 2023/8/10, and the total effective period is 31 days.

9. Select the top-up method.

Note

Currently, the platform only supports cash top-ups when you are topping up for more than one person, whereas you can select from **Cash** and **Account Balance** when topping up for one person only. The amount due will be automatically calculated according to the parking pass rule, the number of vehicles with parking pass, and the number of parking passes you set.

10. Click **Top-Up**.

 A result window will pop up and you can click **Print Receipt** to print the top-up receipt.

22.5.2 Pay in Toll Center

In the Toll Center module, you can search for a specific vehicle to view its parking information, such as the parking duration and the total parking fee. Once all the information is confirmed, the vehicle owner can pay the parking fee in the toll center.

Steps

1. On the left navigation pane, click **Toll Center**.

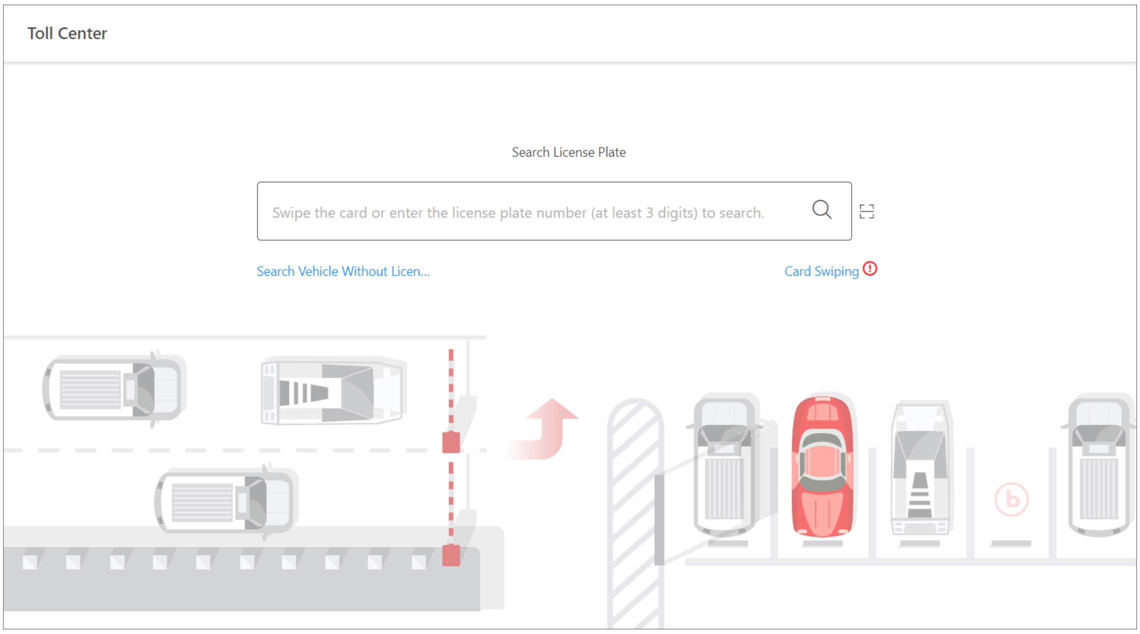


Figure 22-32 Toll Center Page

2. Search for a specific vehicle to get its parking information.
   - Search by license plate number: Enter at least three digits of a license plate number to search for the vehicle.
   - Search by vehicle picture: If a vehicle's license plate is not captured and recorded, you can click **Search Vehicle Without License Plate** and select the target vehicle from the displayed picture(s).
   - Swipe temporary card: Swipe the temporary card that the vehicle owner received when entering the parking lot. After swiping the card at the site, the parking details will be displayed. You can click **Card Swiping** to switch on/off the card encryption and turn on/off the audio.
   - Scan parking receipt: Click next to the search box. After scanning the code on a parking receipt, the parking details will be displayed for the vehicle.

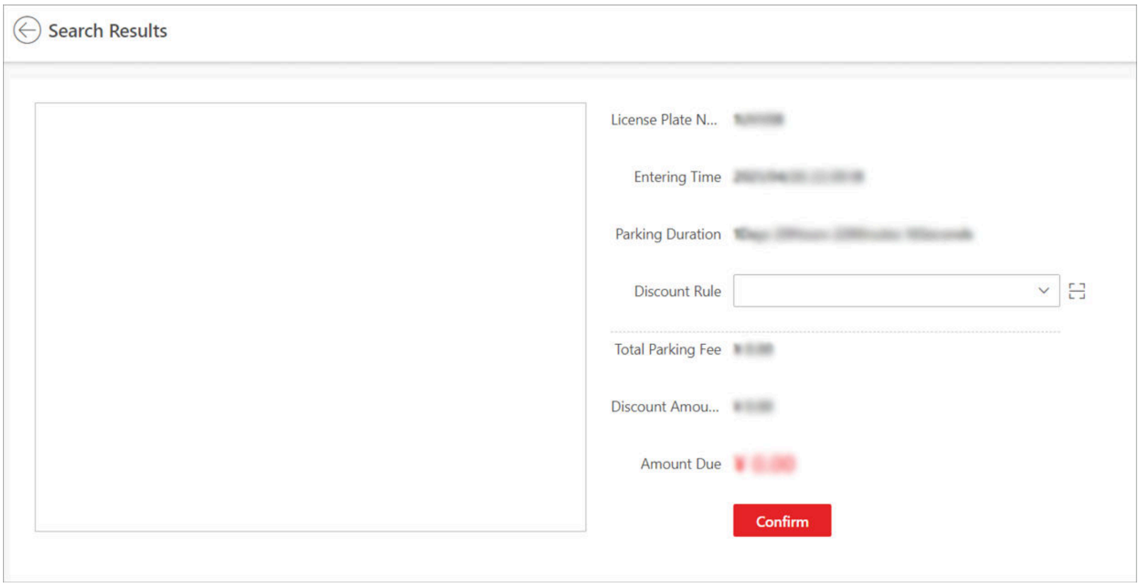


Figure 22-33 Search Result Page

3. **Optional:** Set the discount rule on the Search Results pane.
   - Select a coupon from the drop-down list.
   - Click to add a coupon.
4. Check the information and click **Confirm**.
5. **Optional:** On the pop-up window, click **Print Receipt** to print the receipt or save the receipt to the local PC in PDF format.

22.6 Parking Guidance Configuration

Parking guidance is designed for both the administrator and the vehicle owners, and it is performed by two devices: the guidance terminal and the display screen. The guidance terminal can relate multiple parking cameras for management, and the display screen can guide the vehicle owners to the area where there are vacant parking spaces. With parking guidance, the parking lot can be better operated.

Note

Make sure you have added a parking lot. For details, refer to ***Add Parking Lot*** .

On the left navigation pane, click **Parking Guidance Configuration**, and then select a parking lot to enter the corresponding configuration page.

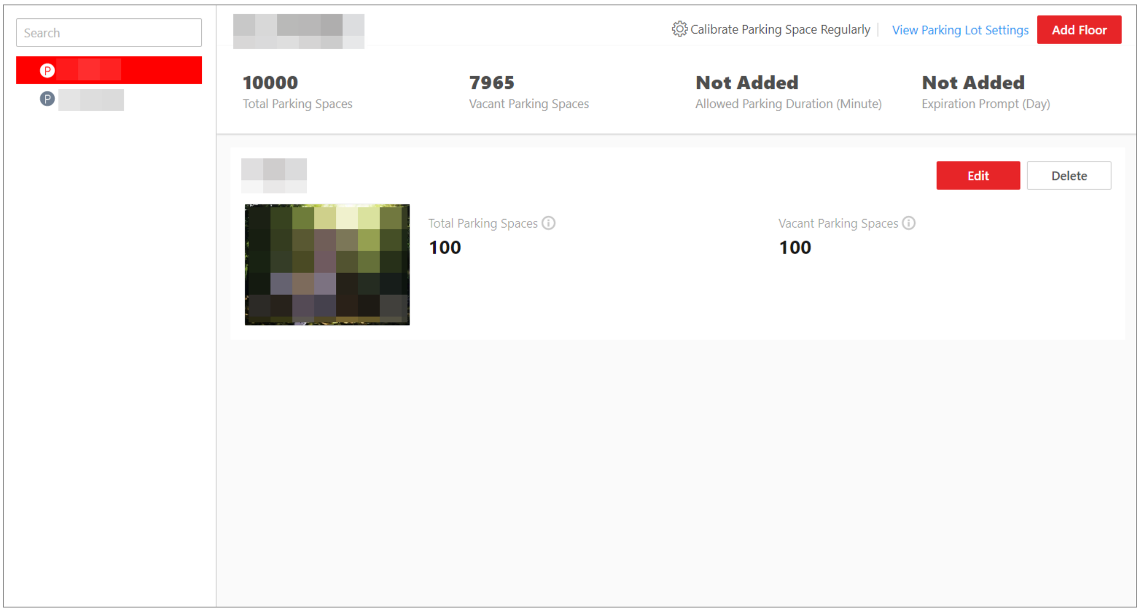


Figure 22-34 Parking Guidance Configuration Page

You can follow the steps below to finish the parking guidance configuration.

1. ***Add a Floor to the Parking Lot***
2. ***(Optional) Link Devices to the Floor***
3. ***(Optional) Configure a Map for the Floor***
4. ***Set Types for Parking Spaces on the Map***
5. ***Mark Devices on the Map***

22.6.1 Add a Floor to the Parking Lot

Before configuring parking guidance, you need to add a floor to a parking lot. After that, you can perform further operations to the floor, including relating devices, configuring a map, marking display screens, and configuring the types of parking spaces.

Steps

1. On the parking guidance configuration page of a selected parking lot, click **Add Floor**.

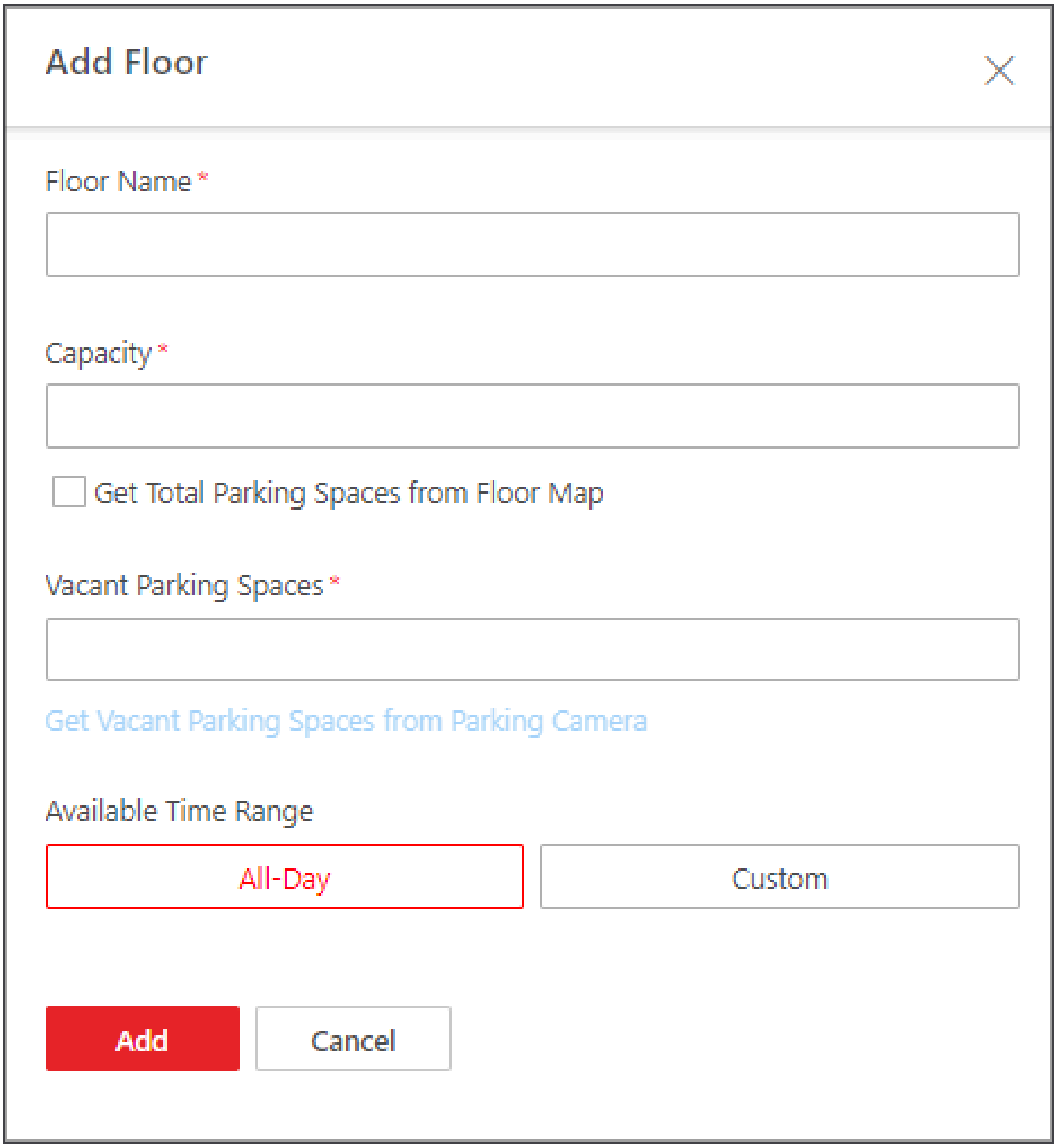


Figure 22-35 Add Floor Pane

2. Create a name for the floor.
3. Set the total number of parking spaces (capacity) of the floor.

Note

If you have added parking spaces on the map of the floor, you can check **Get Total Parking Spaces from Floor Map**, and the number of parking spaces on the map will be synchronized here.

4. Set the number of vacant parking spaces of the floor.

Note

If the floor has been related with parking camera(s), you can check **Get Vacant Parking Spaces from Parking Camera**, and the number of vacant parking spaces counted by the parking camera(s) will be synchronized here.

5. Set the period during which the floor is available for parking. Click **All-Day**, or click **Custom** to customize a period.
6. Click **Add**.

   You will enter the page where you can relate devices, configure a map, mark guidance screen, and configure types for parking spaces.

22.6.2 (Optional) Link Devices to the Floor

After adding a floor to the parking lot, you can link devices (guidance terminal, indoor guidance screen, ANPR camera, query terminal) to the floor. A guidance terminal can be related with multiple parking cameras for management, such as playing the live video and playing back the recorded video from linked cameras. A guidance screen can display the number of vacant parking spaces in the parking lot and guide vehicles to the area where there are vacant parking spaces. An ANPR camera can recognize license plates, capture the pictures of license plates and vehicles, and count the number of vehicles entering and exiting the parking lot which will be used to calculate the number of vacant and occupied parking spaces.

Steps

1. Enter the following page after adding a floor.

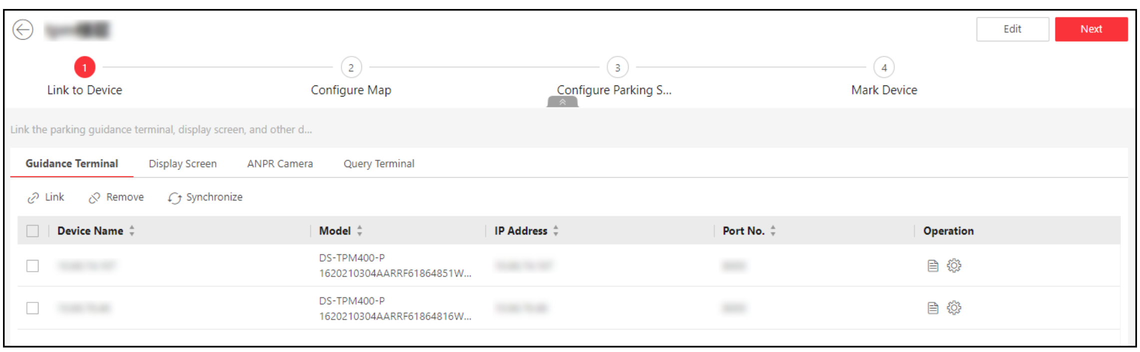


Figure 22-36 Link Device

2. Click **Link to Device**.
3. Link device(s) to the floor.
   1) Click **Guidance Terminal → Link** , and select guidance terminal(s) to link.

Note

After relating a guidance terminal, you can perform the following operation(s) if needed.

- Select one or multiple guidance terminals and click **Synchronize** to synchronize the parking spaces monitored by the parking cameras linked to the terminal(s).
- Click to view the parking camera(s) linked to a guidance terminal, and the parking spaces monitored by the parking camera(s).
- Click to edit settings of a guidance terminal.

2) Click **Display Screen → Link** , and select indoor guidance screen(s) to link.

Note

If both of the ANPR cameras and parking cameras are linked to a parking lot, the indoor guidance screen displays the number of vacant parking spaces counted by ANPR cameras and parking cameras respectively.

3) Click **ANPR Camera → Link** , and select ANPR camera(s) to link. After relating a camera, you need to set its calculation mode in the **Entry and Exit** field.

Standard (Entry Detection) / Standard (Exit Detection)

Count the number of vehicles entered detected by the camera as the number of vehicles entered the floor, and count the vehicles exited as those exited the floor. Select this mode when the direction for entry detection configured on the camera is the same as the actual entry direction.

Reverse (Entry Detection) / Reverse (Exit Detection)

Count the number of vehicles entered detected by the camera as the number of vehicles exited the floor, and count the vehicles exited as those entering the floor. Select this mode when the direction for entry detection configured on the camera is opposite to the actual entry direction.

Note

- An ANPR camera can be linked to different floors.
- The number of vacant parking spaces on the top floor is counted by the ANPR camera.

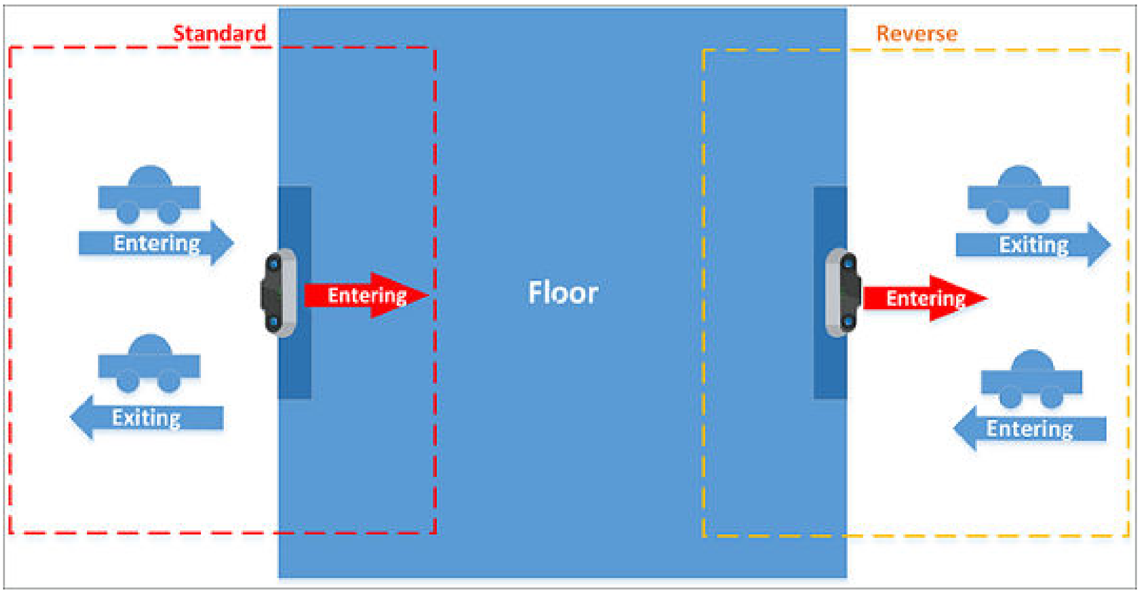


Figure 22-37 Schematic Diagram of Calculation Mode

4) Click **Query Terminal** and select query terminal(s) to link.

Note

A query terminal is mounted inside a parking lot and is installed with the Self-Service Vehicle Finding Client for vehicle owner to locate and find their vehicles in the parking lot. See ***Self-Service Vehicle Finding Client*** for details.

4. **Optional:** Select one or multiple devices, and click **Remove** to remove the device(s) from the floor.

22.6.3 (Optional) Configure a Map for the Floor

You can add a map to the floor, add parking spaces to the map, and configure the layout of parking spaces.

Steps

1. Enter the following page after linking device(s) to the floor.

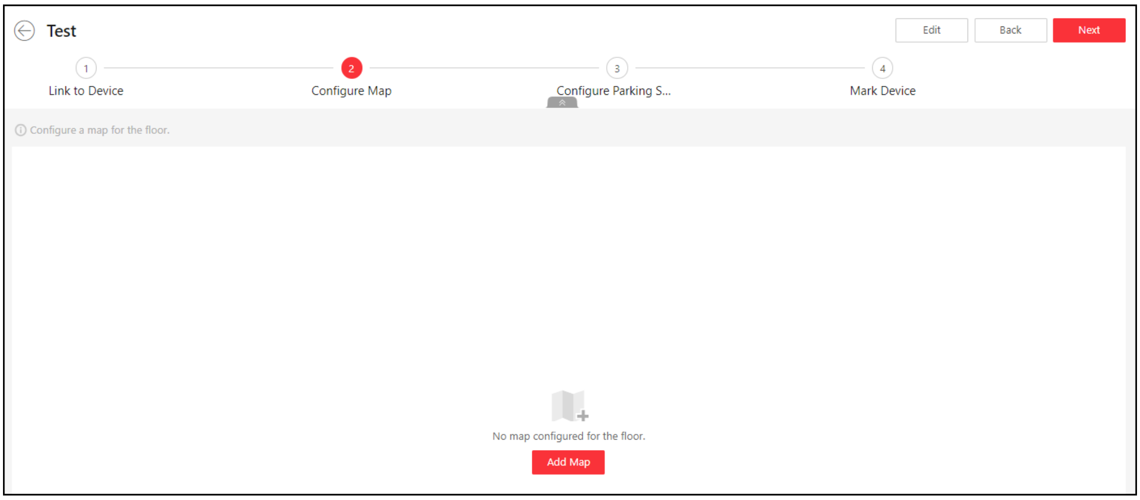


Figure 22-38 Add a Map

2. Click **Add Map**.
3. Select **E-Map** or **Vector Map** as the map type, and click **Confirm**.
4. Select a map from your PC and add it to the floor.

Note

The vector map does not support adding/deleting parking spaces. You can directly go to the next step of configuring parking space type.

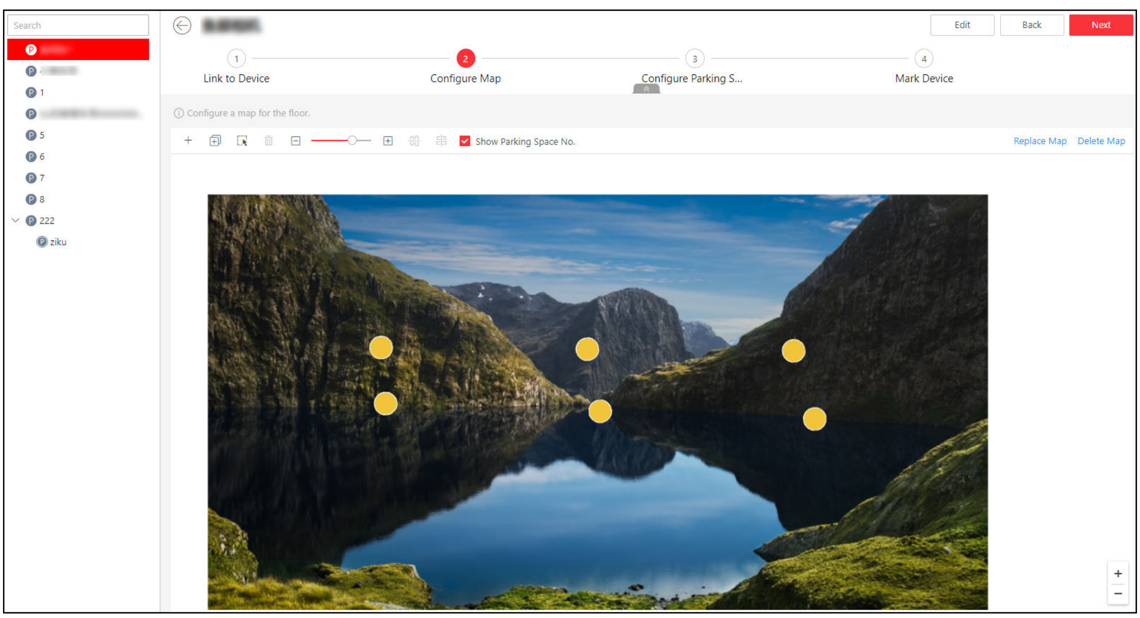


Figure 22-39 Configure the Map

5. Add parking space(s).
   - Add parking spaces one by one.

a. Click + to add one parking space.
b. On the pop-up panel, enter a No. for the parking space.
c. Click **Save**.

- Batch add multiple parking spaces at one time.

a. Click .
b. Click on the map to draw a line.
c. On the pop-up panel, check **Parking Space No.** or **Number of Parking Spaces** as the adding mode.

Note

For the **Parking Space No.** mode, the start No., end No., and No. interval are required; for the **Number of Parking Spaces** mode, the start No., end No., No. interval, and display order (i.e., ascend or descend) are required.

d. Click **Save**.

6. **Optional:** Perform the following operation(s) if needed.

Move Parking Space	Drag a parking space to move it.
Delete Parking Space(s)	• Click one parking space (the green point) and click to delete it. • Click , drag you cursor to select multiple parking spaces, and click to batch delete them.
Adjust the Size of the View of Parking Space(s)	• Click one parking space and click or to make it bigger or smaller. • Click , drag you cursor to select multiple parking spaces, and click or to make them bigger or smaller.
Align Parking Spaces Horizontally	Click , drag you cursor to select multiple parking spaces, and click to align them in a horizontal line.
Align Parking Spaces Vertically	Click , drag you cursor to select multiple parking spaces, and click to align them in a vertical line.
Show Parking Space No. on Map	Check **Show Parking Space No.** to display the parking space No. on the floor map during parking space monitoring.

What to do next

Click **Next** to set types for parking spaces on the map. See ***Set Types for Parking Spaces on the Map*** .

22.6.4 Set Types for Parking Spaces on the Map

You can set types for parking spaces and manage the types according to actual needs.

Steps

1. Enter the following page after configuring the map.

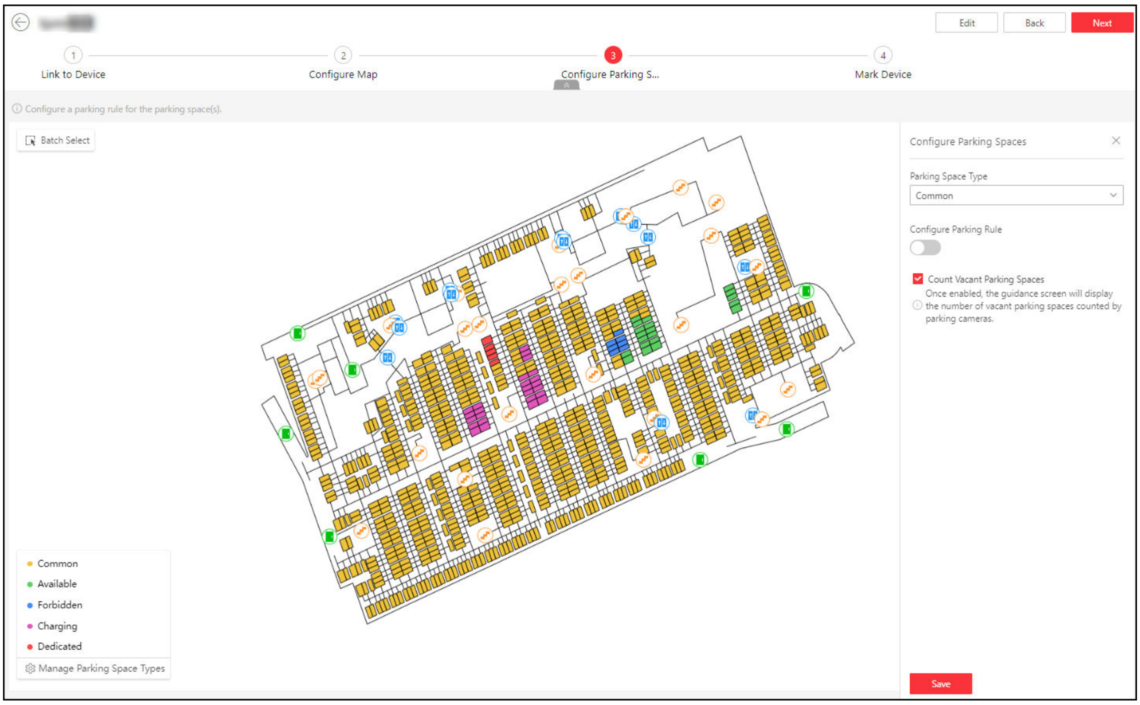


Figure 22-40 Set Types for Parking Spaces

2. Configure parking spaces.
   1) Click a parking space or click **Batch Select** to select multiple parking spaces.

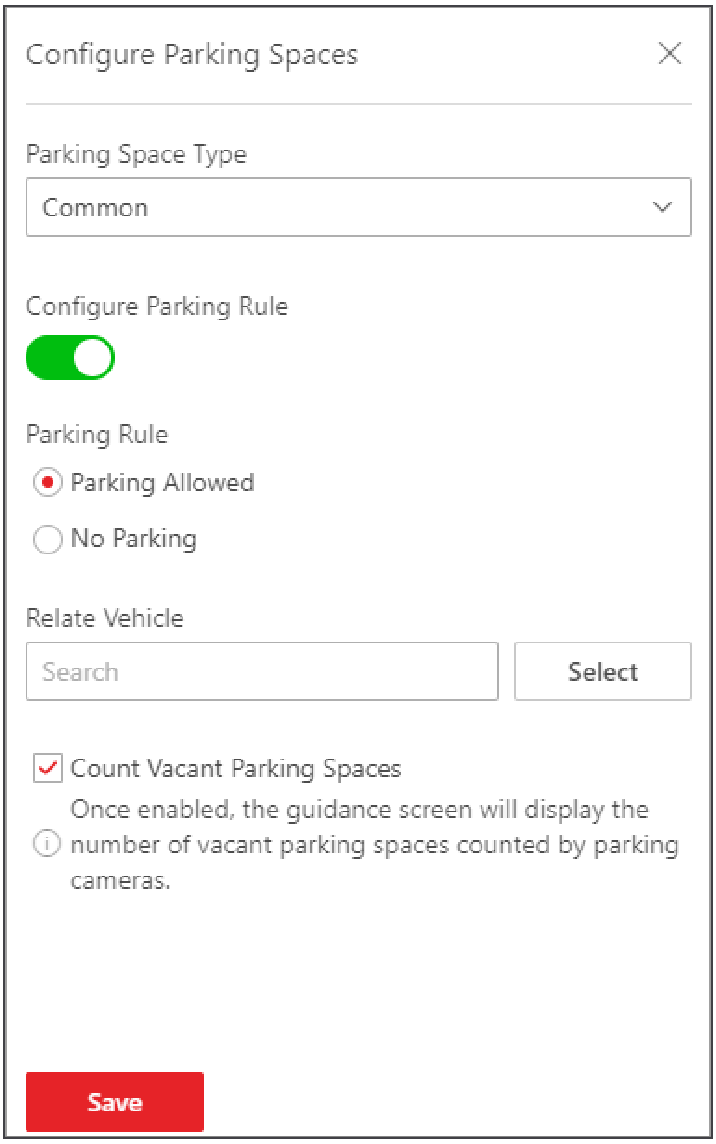


Figure 22-41 Configure a Parking Space

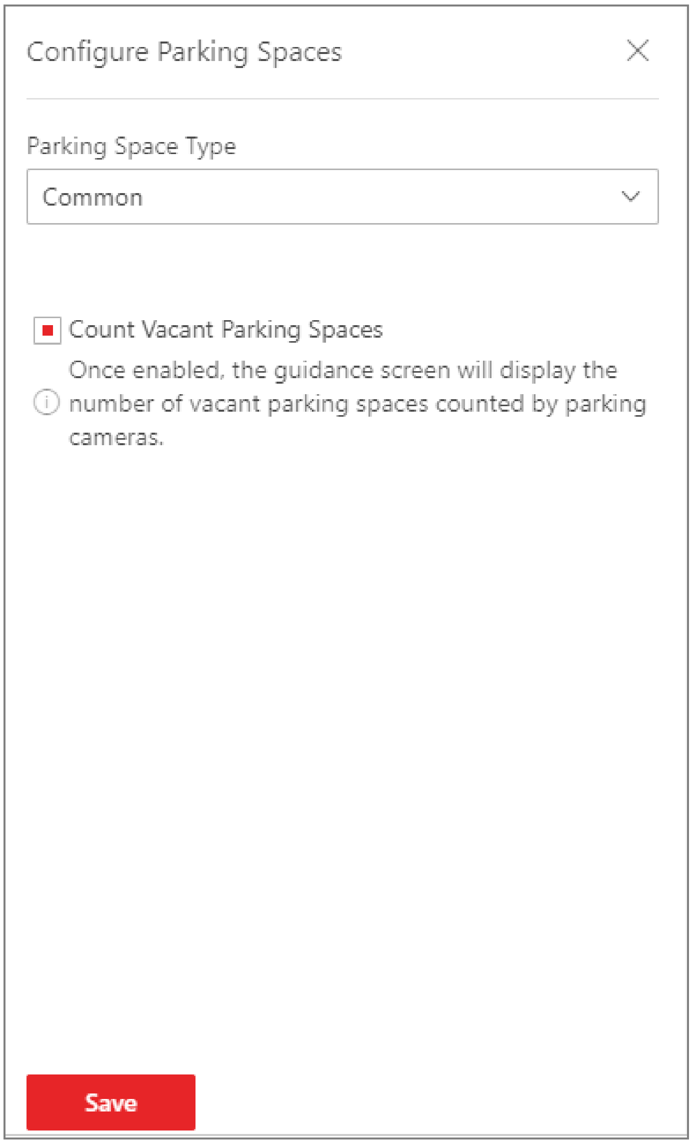


Figure 22-42 Batch Configure Parking Spaces

2) Select a type for the parking space from the drop-down list.
3) Switch on **Configure Parking Rule** to set the parking rule and link vehicle(s) or vehicle list(s) to the parking space.

Note

This step is not supported during batch configuration.

4) **Optional:** Check **Count Vacant Parking Spaces** to display the number of vacant parking spaces on the guidance screen.

Note

During batch configuration, if some of the selected parking spaces are configured with the vacancy counting function, the checkbox will be displayed as ■ , you can still check or uncheck it.

3. **Optional:** Click **Manage Parking Space Types** on the floating pane and perform the following operations if needed.

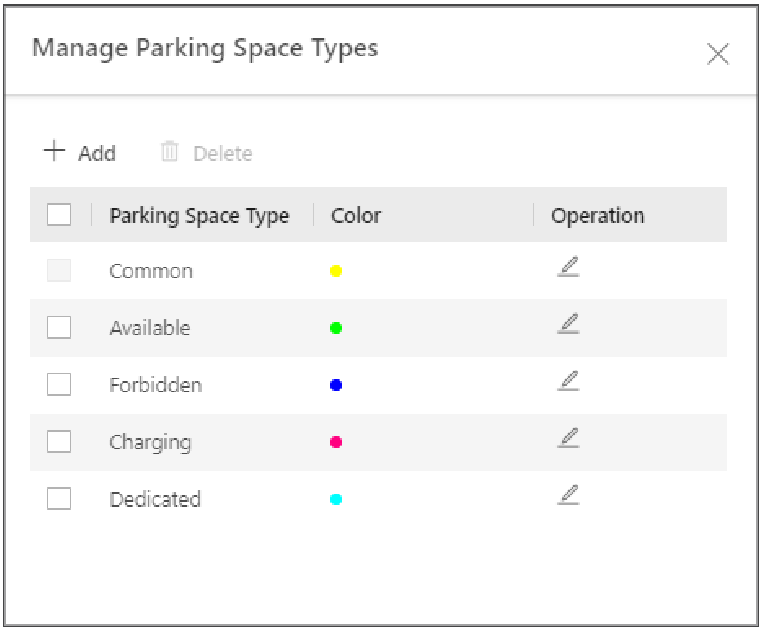


Figure 22-43 Manage Parking Space Types

Add a Parking Space Type

a. Click **Add**.
b. Create a name for the type.
c. Set a color for the type.

Note

The color will be applied to the indicator light of the parking cameras monitoring this type of parking spaces.

d. Click**Save**.

Edit a Parking Space Type

Click ✎ to edit the name and color of a type.

Note

The name of the default type (common) cannot be edited.

Delete Parking Space Type(s)

Select one or multiple types and click **Delete** to delete them.

Note

The default type cannot be deleted.

What to do next

Click **Next** to mark device(s) on the map. See ***Mark Devices on the Map*** .

22.6.5 Mark Devices on the Map

You can link guidance screens to parking spaces at a specific direction in the parking lot. Once linked, the guidance screen can display the number of vacant parking spaces and guide vehicles to them.

Steps

1. Enter the following page after configuring the parking space type.

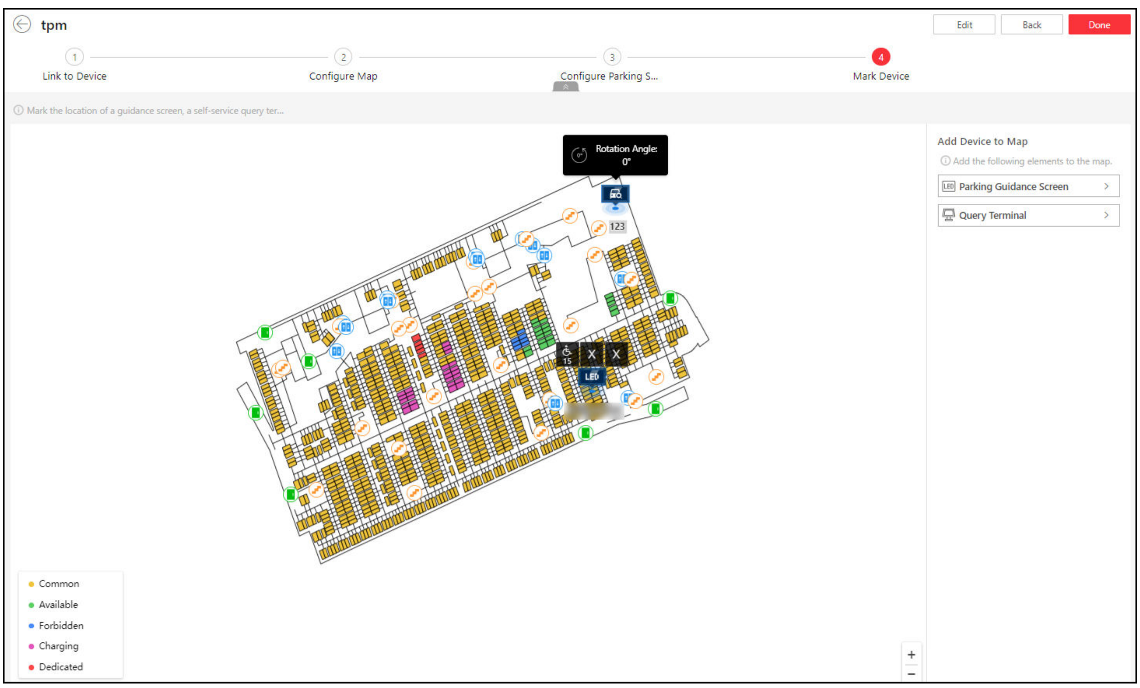


Figure 22-44 Mark Device

2. Add a device (indoor guidance screen or query terminal) to the map by dragging the device from the device list to the map.

Note

Only the indoor guidance screen can be marked. The entrance guidance screens or entrance and exit display screens will not be displayed in the list.

3. Configure devices added to the map.

- Configure a query terminal.

Click the device icon on the map, and click **Configure Rotation Angle** to configure its direction for the self-service vehicle finding client to display a more adaptable map view.

- Configure an indoor guidance screen.

Link Parking Spaces	a. Click the device icon on the map, and click **Link Parking Space** on the pop-up menu to open the parking spaces marking pane. Select the parking space(s) and click **OK** to link the selected parking space(s) with the device. **Note** - When you select the parking space(s), you can click a parking space icon on the map, or click **Batch Select**, or check **Select All Parking Spaces**. - If the current floor has linked with multiple maps, you can click **Switch Map** to switch to another map for marking.
Configure Guidance Screen	Click the device icon on the map and click **Guidance Screen Configuration** on the pop-up menu to enter the Guidance Screen Configuration page. Refer to ***Link Display Screen and Set Displayed Content*** for details.
Check Information Currently Displayed on Guidance Screen	Click the device icon on the map and click **Guidance Screen and Parking Space Status** on the pop-up menu to check information currently displayed on the guidance screen. You can click a screen to view the detailed information about the parking space(s) linked to it, such as parking space No., floor where the parking space is located, whether the parking space is occupied, and the picture of the parking space captured at the moment. **Note** This function is only supported by some guidance screens.

4. Click **Done** to finish the parking guidance configuration.

22.6.6 Calibrate Parking Spaces Regularly

To reduce the manual operation costs of a parking lot and avoid parking disputes caused by the incorrect number of vacant parking spaces displayed on the display screen, you can enable the functions of regularly calibrating vacant parking spaces on each floor or in the parking lot, so the real-time number of vacant parking spaces in the parking lot will be counted regularly and the number of vacant parking spaces to be reserved for vehicles that entered the parking lot but not parked will also be regularly counted and displayed by floor.

Before You Start

Make sure you have deployed ANPR cameras if you want to regularly calibrate parking spaces on floors.

Steps

1. On the parking guidance configuration page of a selected parking lot, click **Calibrate Parking Space Regularly** in the top right corner of the parking lot details page.

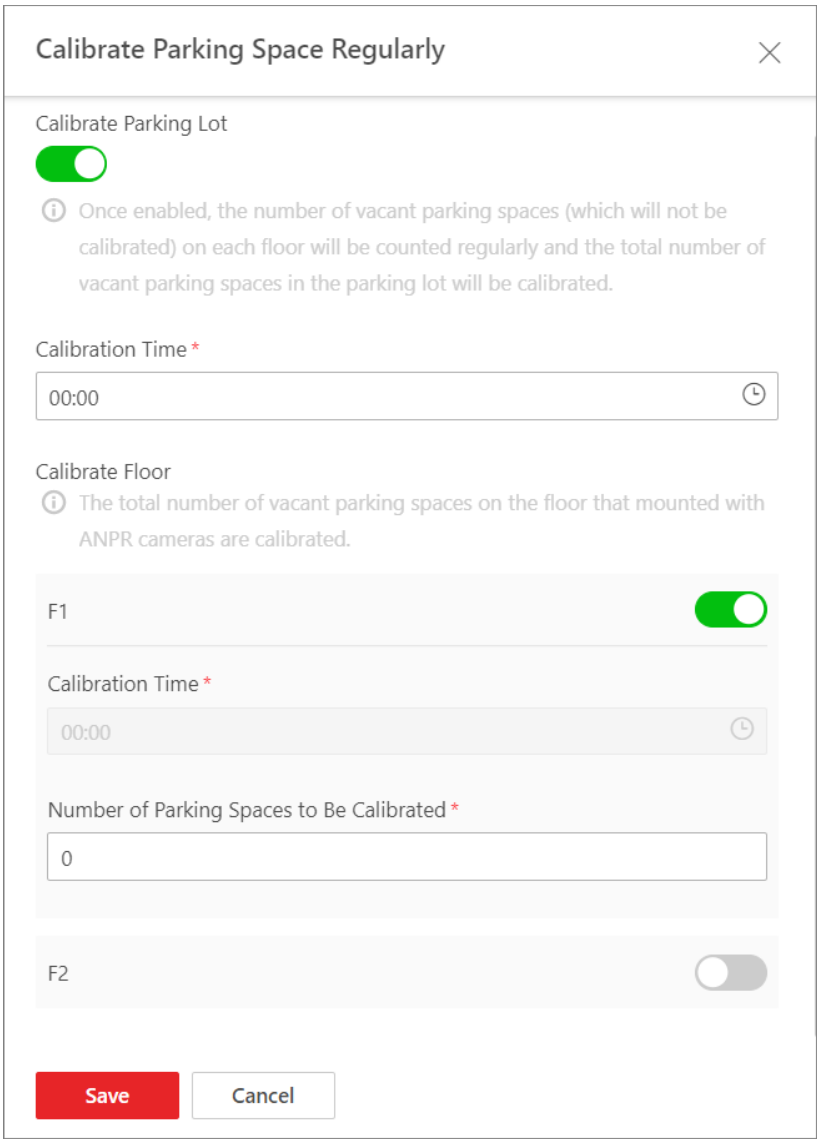


Figure 22-45 Calibrate Parking Spaces Regularly

2. Switch on **Calibrate Parking Lot**.
3. Set the calibration time for the parking lot.

Example

If you set the calibration time to 12:00, the number of vacant parking spaces in the parking lot will be calibrated at 12:00 every day.

4. In the Calibrate Floor field, enable the switch beside a floor name.

Note

Only the floors deployed with ANPR cameras will be displayed in the Calibrate Floor field.

Two configuration fields will be displayed and the calibration time will automatically inherit that from the parking lot.

5. Set a number of parking spaces on the floor to be calibrated.

Note

The entered number must be smaller than the total number of parking spaces on the floor, otherwise, a window with the error information will appear when you save the settings.

6. **Optional:** Repeat the above two steps to enable regular calibration for other floors.
7. Click **Save**.

22.6.7 Parking Space Monitoring

On the Parking Space Overview page, you can view the statistics of parking spaces, and can search for specific statistics by parking space No., license plate No., and parking time.

The Parking Space Overview page displays various kinds of statistics of parking spaces, including the occupancy rate of the parking spaces in a parking lot, the number of vacant parking spaces, occupied parking spaces, parking spaces with unknown status, and the number of overtime parking and parking violations.

Note

- If there is no map added for the parking lot, parking space information will be overlaid directly on the monitoring video.
- An icon will be displayed on a parking space for overtime parking. Click the icon to view the parking space details and check the type of the vehicle that parked overtime.
- By selecting → **Export Unknown Parking Space Information** next to the number of parking spaces with the unknown status under **Violation**, you can export details such as the related parking space numbers and the corresponding parking lot and floor information to the local PC as an XLSX file.

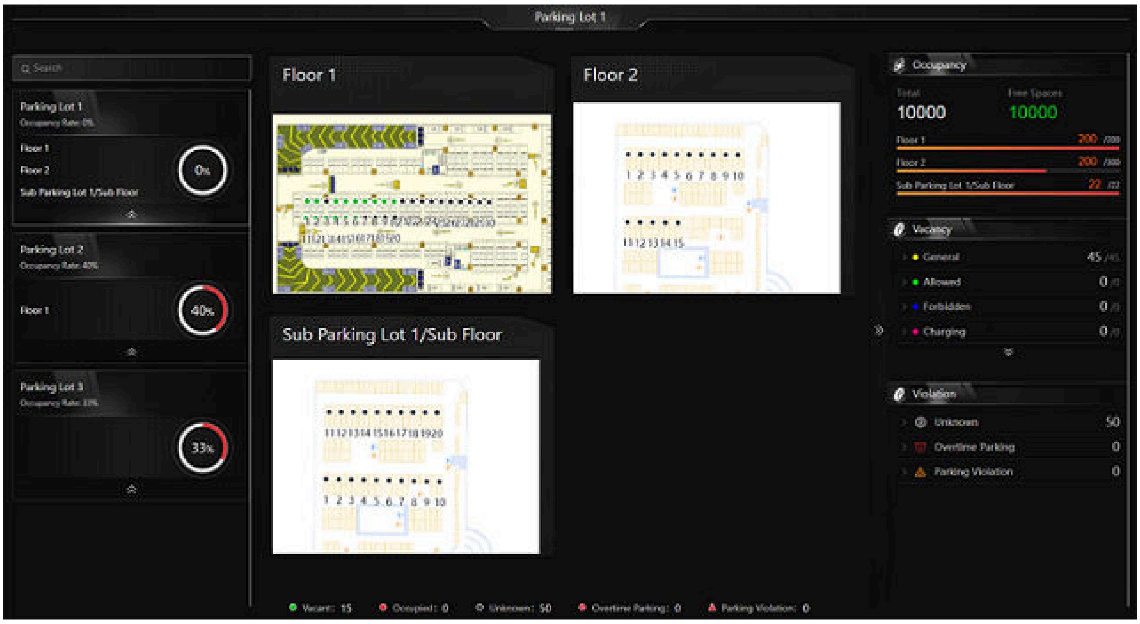


Figure 22-46 Parking Space Overview

You can click a floor name to view the statistics of the parking spaces of this floor. On the following page, you can move to a specific parking space to view its detailed information, and can click a parking space to view its real-time status and search for parking records. Moreover, you can click **Occupancy Status Overview** or **Parking Duration Overview** to view these two types of statistics respectively.

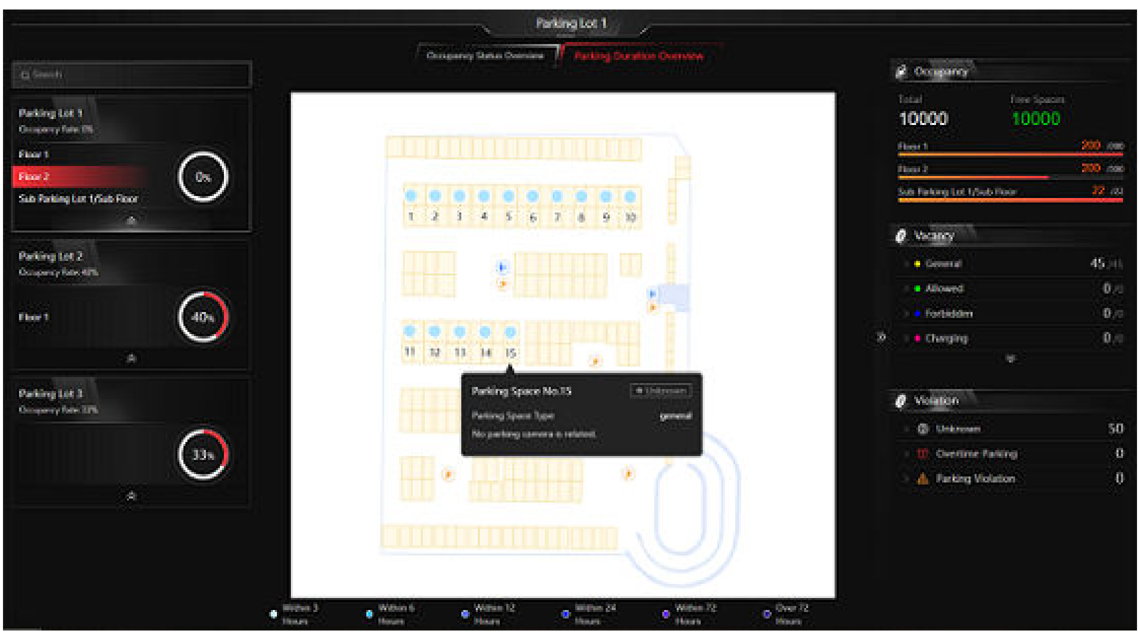


Figure 22-47 Floor Parking Space Overview

22.7 Record Search

You can search for various types of records, including passing vehicles, parking records, payment records, etc. Each record is attached with highly detailed information related to it, which can give the vehicle owner and the administrator a whole picture of the vehicle's activity in a parking lot. Therefore, these records can help you to manage parking much better.

22.7.1 Search for Passing Vehicles Detected by Entrances & Exits

If the license plate number of a vehicle is recognized by cameras or capture units linked to an entrance and exit, you can search for the related vehicle passing information.

Steps

1. On the left navigation pane, select **Search → Passing Vehicle Search** .
2. Select one or multiple entrances and exits where you want to search for the vehicle passing records.
3. Set the time duration for search.
4. Switch on and set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   Country/Region

   Select the country/region where the vehicle's license plate number is registered.

   License Plate No.

   - **No License Plate**: Search for vehicles without license plates.
   - **With License Plate**: Enter a vehicle's license plate number or part of it.

   Enter or Exit

   Select whether the vehicle is entering or exiting.

   How to Open Barrier

   Select how the barrier gate is opened when a vehicle enters/exits the parking lot. **Manual** indicates that a security guard manually controlled the barrier gate to open after identifying the vehicle owner; **Auto Allow for Entry and Exit** indicates that the barrier gate opened automatically after the license plate number was recognized by a capture unit; **Not Opened** indicates that the barrier gate did not open even after the capture unit recognized the license plate number.

   Reason

   Select the reason(s) for allowing or not allowing the vehicle to enter/exit from the drop-down list.

   Vehicle List

   Select from the drop-down list to search for records of temporary vehicles, visitor vehicles, registered vehicles, or vehicles in the blocklist or other custom lists.

Additional Information

The item(s) of additional vehicle information you customized.

5. Click **Search**.

   The matched results will be displayed on the right.

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

View Vehicle Details	Click a license plate number in the License Plate No. column to open the vehicle details pane. You can view the captured picture and information about the vehicle owner, the vehicle, and details related to its entry/exit.
View Owner's Picture	Click a license plate number, and click the name of the vehicle owner to view pictures of the owner, including an uploaded profile photo and a picture captured at the entrance & exit. **Note** This operation can only be performed if the entry & exit modes of the parking lot are set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Vehicle Verification Mode*** .
Export a Passing Vehicle	Click **Export** and select **Excel** or **CSV** as the format of the exported file. **Note** • If you select **Excel** as the file format, you can check **Export Picture** to save pictures contained in the search results to the local PC with the exported file. The exported pictures will be named and sorted by the capture time. • No more than 500 passing vehicles with captured pictures can be exported in the Excel format at one time. If the number exceeds 500, you need to go to the Control Client to export them. • No more than 100,000 passing vehicles without captured pictures can be exported at one time.

22.7.2 Search for Parking Records

On the platform, you can search for parking records generated in a specific parking lot or records of a specific vehicle by setting relevant search conditions according to actual needs, and perform further operations, such as viewing the detailed information of vehicles and exporting the records to your PC.

Steps

1. On the left navigation pane, select **Search → Parking Record Search** .
2. Set the time duration for search.

3. Set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   Parking Space No.

   Enter the parking space No. of a specific parking lot to search for records of vehicles which park or have parked in that parking space.

   Parking Status

   Select a parking status. **Parking** indicates the vehicle still parks in the parking lot, whereas **Exit** indicates the vehicle has already left the parking lot.

4. Click **Search**.

   The matched results will be displayed on the right.

   Note

   You can click ☰ or ⊞ to switch between list mode and thumbnail mode.

5. **Optional:** Perform the following operations as needed.

View Vehicle Details	Click a license plate number in the License Plate No. column to open the vehicle details pane. You can view the captured picture and information about the vehicle owner, the vehicle, and details related to its entry/exit.
View Owner's Picture	Click a license plate number, and click the name of the vehicle owner to view pictures of the owner, including an uploaded profile photo and a picture captured at the entrance & exit. **Note** This operation can only be performed if the entry & exit modes of the parking lot are set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Vehicle Verification Mode*** .
Export Vehicle Parking Records	Click **Export** and select **Excel** or **CSV** as the format of the exported file. **Note** • If you select **Excel** as the file format, you can check **Export Picture** to save pictures contained in the search results to the local PC with the exported file. • No more than 500 parking records with captured pictures can be exported in the Excel format at one time. If the number exceeds 500, you need to go to the Control Client to export them. • No more than 100,000 parking records without captured pictures can be exported at one time.

22.7.3 Search for Parked Vehicles

If the actual number of vacant parking spaces is different from the number displayed on the guidance screens, you can search for the vehicles that already exited but still recorded in the parking lot to edit the vehicle information. For example, for parking lots requiring all on-site vehicles out at the end of a day, you can search for the vehicles that are still in the parking lot and export the vehicles' information. In another situation, if a vehicle is manually allowed to exit the parking lot, the number of vacant parking spaces may not be updated in time. In this situation, you can search for the vehicle and delete it from the vehicle list of the parking lot to update the number of vacant parking spaces.

Steps

1. On the left navigation pane, select **Search → Parked Vehicle Search** .
2. Select a parking lot from the drop-down list.
3. Switch on and set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   Country/Region

   Select the country/region where the vehicle's license plate number is registered.

   License Plate No.

   - **No License Plate**: Search for vehicles without license plates.
   - **With License Plate**: Enter a vehicle's license plate number or part of it.

   How to Open Barrier

   Select how the barrier gate is opened when a vehicle enters/exits the parking lot. **Manual** indicates that a security guard manually controlled the barrier gate to open after identifying the vehicle owner; **Automatic** indicates that the barrier gate opened automatically after the license plate number was recognized by a capture unit; **Barrier Not Open** indicates that the barrier gate did not open after the capture unit recognized the license plate number.

   Vehicle List

   Select from the drop-down list to search for records of temporary vehicles, visitor vehicles, registered vehicles, or vehicles in the blocklist or other custom lists.

   Additional Information

   The item(s) of additional vehicle information you customized.
4. Click **Search**.

   The matched results will be displayed on the right.
5. **Optional:** Perform the following operations as needed.

View Vehicle Details	Click a license plate number in the License Plate No. column to open the vehicle details pane. You can view the captured picture and information about the vehicle owner, the vehicle, and details related to its entry/exit.

View Owner's Picture	Click a license plate number, and click the name of the vehicle owner to view pictures of the owner, including an uploaded profile photo and a picture captured at the entrance & exit. **Note** This operation can only be performed if the entry & exit modes of the parking lot is set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Vehicle Verification Mode*** .
Export All Records	Click **Export** and select **Excel** or **CSV** as the format of the exported file. **Note** • If you select **Excel** as the file format, you can check **Export Picture** to save pictures contained in the search results to the local PC with the exported file. • No more than 500 records with captured pictures can be exported in the Excel format at one time. If the number exceeds 500, you need to go to the Control Client to export them. • No more than 100,000 records without captured pictures can be exported at one time.
Delete Vehicle from Parking Lot	Click **Delete All** to remove all displayed vehicles from the parking lot.

22.7.4 Search for Payment Records

If a vehicle pays the parking fee and exits the parking lot, its payment information, such as the payment source and operation time, will be recorded in the platform. On the platform, you can search for the payment records generated in a specific parking lot or the records of a specific vehicle by setting search conditions according to actual needs. You can also export the records to your PC. With the statistics, you can monitor some of the transactions done in the parking lots, which can help you manage the parking lots better.

Steps

1. On the left navigation pane, select **Search → Payment Record Search** .
2. Set the time duration for search.
3. Set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   Operator

   Select the person responsible for collecting the fee from the drop-down list.

Payment Method

Select how the parking fee is paid. **Cash** indicates the fee is paid in cash; **Vehicle Owner Account** indicates the fee is deducted from the owner's account balance.

Payment Source

Select where the parking fee is paid. **Booth** indicates the parking fee is paid at the booth; **Toll Center** indicates the parking fee is paid in the toll center.

4. Click **Search**.
5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

22.7.5 Search for Vehicle Top-Up and Refund Records

In the Search module, you can search for the top-up and refund records of vehicles or parking lots, and export the records to your PC. With the statistics, you can monitor some of the transactions happened in the parking lots, which can help you manage the parking lots better.

Steps

1. On the left navigation pane, select **Search → Top-Up and Refund Record Search** .
2. Set the search mode to **By Vehicle** or **By Person**.
3. Select **Today**, **Yesterday**, **Current Week**, **Last 7 Days**, or **Last 30 Days** from the drop-down list as the time range for search, or click **Custom Time Interval** to customize a time range.
4. Set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

Transaction Type

Select the transaction type. **Top-Up** indicates adding money to a parking pass to keep it valid or extend its validity period; **Refund** indicates getting paid back (e.g., when you paid too much for one parking).

Transaction Method

Select how the transaction is made. **Cash** indicates the transaction is made in cash; **Vehicle Owner Account** indicates the transaction is made with/to the vehicle owner's account.

Operator

Select the person responsible for handling the top-up/refund transaction from the drop-down list.

5. Click **Search**.
6. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

22.7.6 Search for Transaction Records of Vehicle Owner Account

You can search for the transaction records of a specific vehicle owner account, and export the records to your PC. With the statistics, you can see the details about the transactions between a vehicle owner and the parking lot.

Steps

1. On the left navigation pane, select **Search → Account Transaction Record Search** .
2. Select **Today**, **Yesterday**, **Current Week**, **Last 7 Days**, or **Last 30 Days** from the drop-down list as the time range for search, or click **Custom Time Interval** to customize a time range.
3. Set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   Transaction Type

   Select the transaction type. **Top-Up** indicates adding money to a parking pass to keep it valid or extend its validity period; **Refund** indicates getting paid back (e.g., when you paid too much for one parking); **Deduction** indicates paying parking fees with the account balance.

   Operator

   Select the person responsible for handling the transaction from the drop-down list.
4. Click **Search**.
5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

22.7.7 Search for Work Records of Operators

You can search for the work records of operators (i.e., the person responsible for payment management) to get the information such as the on-duty and off-duty time of an operator as well as the amount of payment the operator managed during working hours.

Steps

1. On the left navigation pane, select **Search → Operator Shift Search** .
2. Select **Today**, **Yesterday**, **Current Week**, **Last 7 Days**, or **Last 30 Days** from the drop-down list as the time range for search, or click **Custom Time Interval** to customize a time range.
3. Select an operator (the person responsible for collecting the fee or handling a transaction) or **All** from the drop-down list.
4. Click **Search**.
5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

22.7.8 Search for Coupon Records

You can search for coupon records and view detailed information about the coupons, such as the discount rule, expiration time, and the coupon status.

Steps

1. On the left navigation pane, select **Search → Coupon Record Search** .
2. **Optional:** Select a specific parking lot, coupon status, and discount rule from the drop-down lists as needed.
3. Click 📅 to specify a time range for the search.

   Note

   Only coupons of which the effective period falls within the specified time range will be displayed as search results.
4. Click **Search**.
5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported file, and click **Save** to export the search results to the local PC.

22.8 Statistic and Report

In the Statistics and Report module, you can view and export the operation report and transaction report of each parking lot for having a general understanding of the usage, revenue, and expenditure of the parking lot.

22.8.1 Export Operation Reports of Parking Lots

You can view the statistics related to the operations of parking lots, such as real-time parking space statistics, parking space occupancy rate and times, parking duration distribution, and traffic flow. The statistics can give you a general picture of the operation situation of parking lots.

Steps

1. On the left navigation pane, select **Statistics and Reports → Operation Report** .
2. In the top right corner of the Operation Report page, click **Configure Report Contents** and select the types of statistics to be displayed for the parking lot(s).

   Note

   - Any user with the permission to view the parking lot operation is able to set which content(s) to display on the page.
   - All users share a common configuration.
3. Select a report type from **Day**, **Month**, and **Year**, or click **Custom** to customize a time period for generating the operation data.

4. View statistics of all parking lots by default or select a parking lot from the drop-down list to view statistics of the specific parking lot.

Note

You can view the last update time and refresh the statistics by clicking **Refresh** on the top right corner.

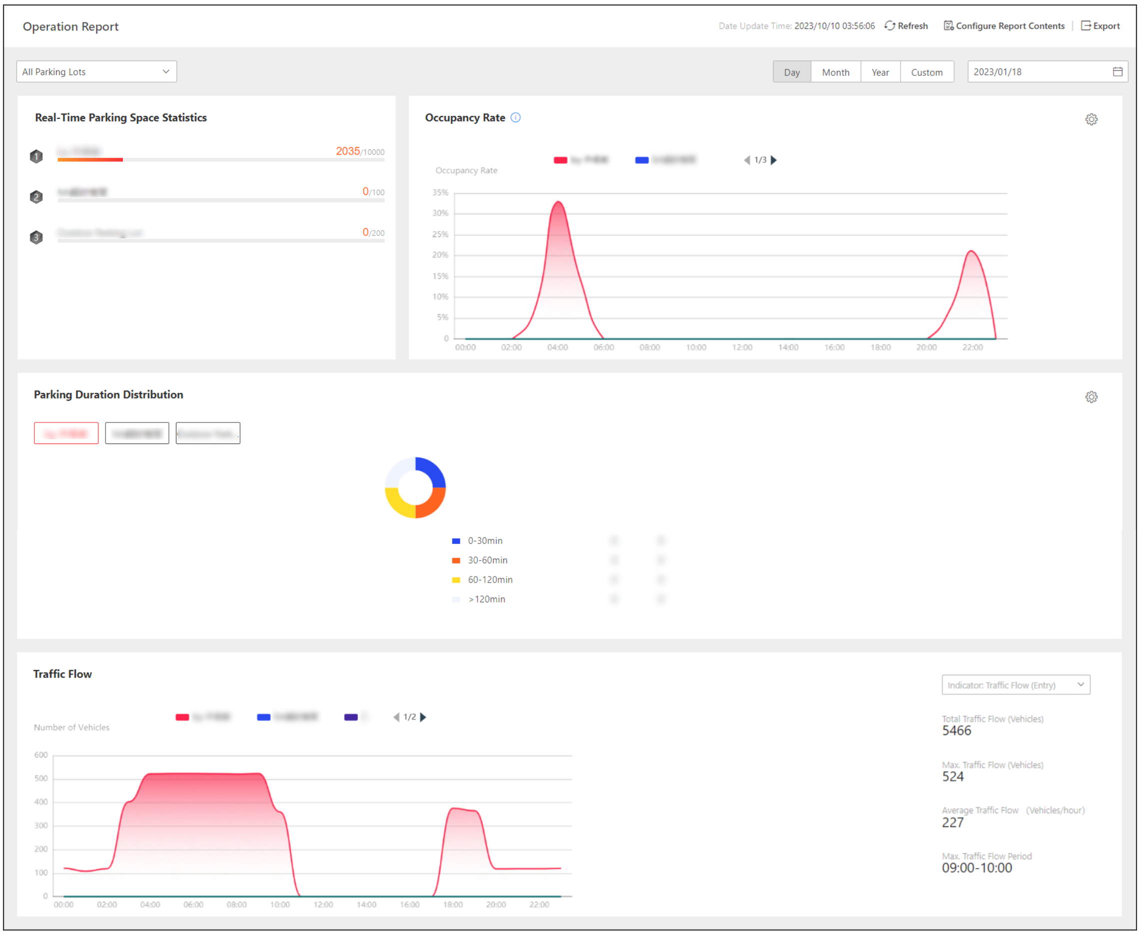


Figure 22-48 Operation Report of All Parking Lots

Table 22-1 Operation Report of All Parking Lots

Statistics Type	Description
Real-Time Parking Space Statistics	Display the real-time numbers of occupied and total parking spaces in each parking lot.
Occupancy Rate	Click ⚙ to set a time period. The statistics generated in the set period will be displayed.
Parking Duration Distribution	Click ⚙ to set the parking duration(s) to be calculated.

Statistics Type	Description
	The distribution of the selected parking duration(s) will be displayed. Click tabs above the pie chart to switch between parking lots for viewing the corresponding distribution.
Traffic Flow	In the top right corner of the area, select one or multiple indicators from the drop-down list. **Traffic Flow (Entry)** Total number of vehicles that entered parking lots. **Traffic Flow (Exit)** Total number of vehicles that exited parking lots. **Note** If the user only has permissions related to parking guidance, there will be no drop-down list in this area used for selecting indicators.

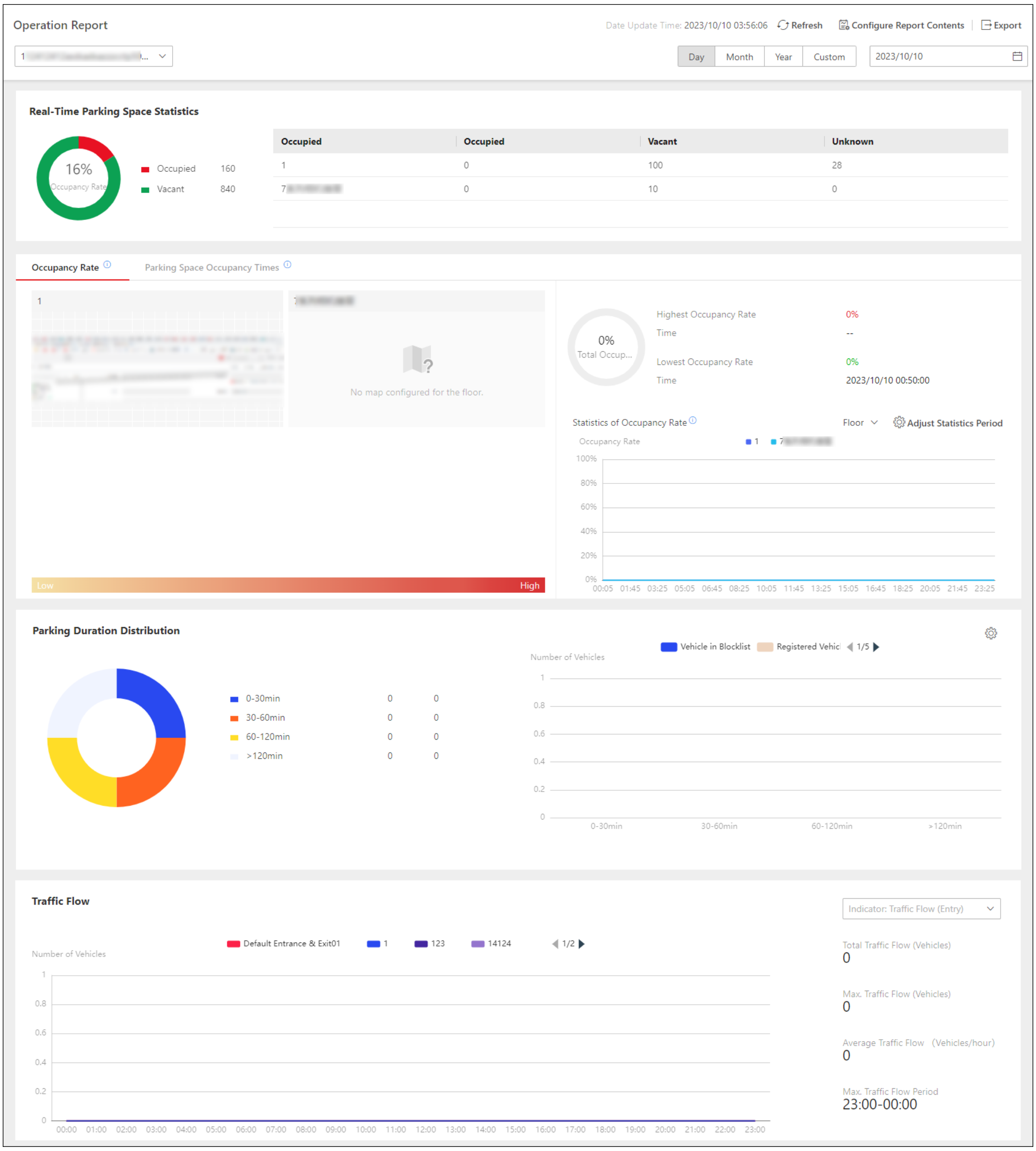


Figure 22-49 Operation Report of a Parking Lot

Table 22-2 Operation Report of a Parking Lot

Statistics Type	Description
Real-Time Parking Space Statistics	Display the real-time numbers of occupied/vacant parking spaces in the parking lot and numbers of occupied/vacant/unknown parking spaces on each floor of the parking lot.
Occupancy Rate	Click ⚙ **Adjust Time Period** at the right to set a time period. The map on each floor of the parking lot will be displayed, and you can click the map to enlarge it for viewing. The parking space icons on the map are marked with different colors that indicate different occupancy rates. The deeper the color, the higher the occupancy rate of the parking space during the selected time. The statistics generated in the set time period, including the total occupancy rate of the parking lot, the maximum/minimum occupancy rate, the corresponding happening time, and the occupancy rate of each floor or parking space type, will be displayed.
Parking Space Occupancy Times	The report of occupancy times indicates the exposure rates of areas in the parking lot, which can help the parking lot manager to determine whether to place advertisements. Click ⚙ **Adjust Time Period** at the right to set a time period. The map on each floor of the parking lot will be displayed, and you can click the map to enlarge it for viewing. The parking space icons on the map are marked with different colors that indicate different occupancy times. The deeper the color, the more times the parking space is taken up during the selected time period. The statistics generated in the set time period, including the total occupancy times of the parking lot, the maximum/minimum occupancy times, the corresponding parking floors, and the occupancy times of each floor, will be displayed.
Parking Duration Distribution	Click ⚙ to set the parking duration(s) to be calculated. The distribution of the selected parking duration(s) will be displayed in a pie chart. The number(s) of vehicles with the selected parking duration(s) will be displayed by vehicle list.
Traffic Flow	In the top right corner of the area, select one or multiple indicators from the drop-down list.

Statistics Type	Description
	Traffic Flow (Entry) Number of vehicles that entered the parking lots. **Traffic Flow (Exit)** Number of vehicles that exited the parking lots. **By: Entrance and Exit** If only one indicator is selected, you can select the entrance(s) and exits(s) for displaying the traffic flow by entrance and exit. **By: Vehicle List** If only one indicator is selected, you can select the vehicle list(s) for displaying the traffic flow by vehicle list. **Note** If the user only has permissions related to parking guidance, there will be no drop-down list in this area used for selecting indicators.

5. **Optional:** In the upper-right corner, click **Export**, select **Excel** or **CSV** as the format of the exported data file(s), and click **Save** to download the report and the detailed statistics to the local PC.

Note

The entire operation report will be saved as a PDF files by default. For the operation report of a parking lot, the floor map(s) containing the parking space occupancy information will also be saved as the PDF file(s) named by the floor name(s) by default. Other than the report, each type of statistics will be individually exported in the format you selected.

22.8.2 Export Transaction Reports of Parking Lots

You can view the statistics related to the revenue and expenditure of parking lots, such as the trend and type of revenue and expenditure, the revenue and expenditure generated in a specific period. The statistics can give you a general picture of the transactions done in the parking lots.

Steps

1. On the left navigation pane, select **Statistics and Reports → Transaction Report** .

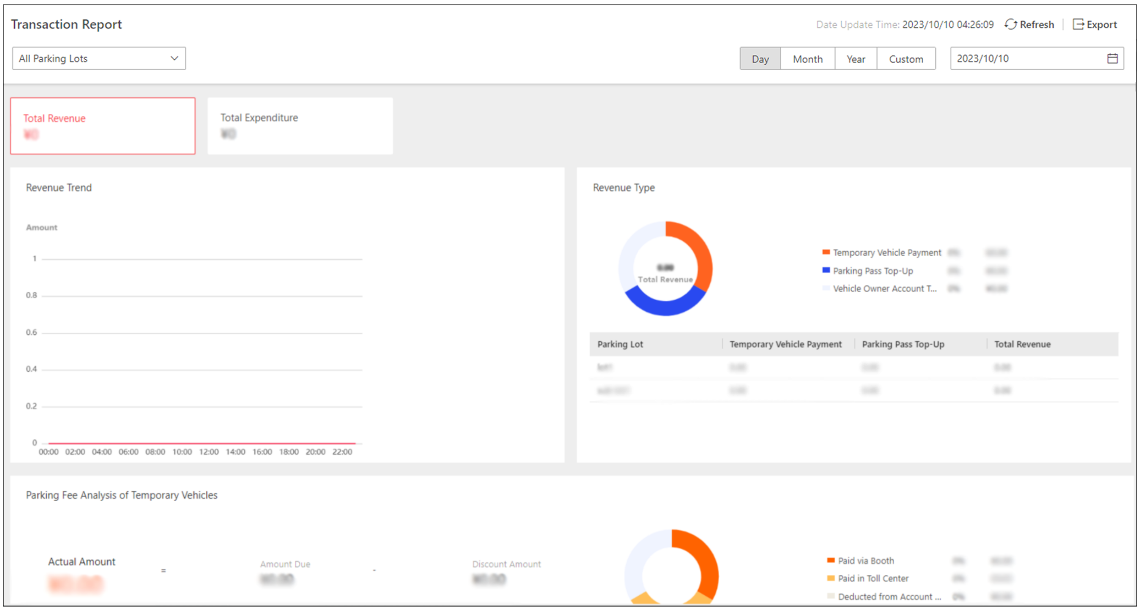


Figure 22-50 Transaction Report Page

2. Select a parking lot from the drop-down list.
3. Select a report type from **Day**, **Month**, and **Year**, or select **Custom** to display the operation data generated within the custom period.
4. Click **Total Revenue** to view the statistics of revenue, and the parking fee analysis of temporary vehicles.
5. Click **Total Expenditure** to view the statistics of expenditure.
6. **Optional:** Click **Refresh** on the top right corner to refresh the statistics.
7. **Optional:** In the upper-right corner, click **Export** to save the analysis report to your PC.

22.8.3 Configure Scheduled Overtime Parking Reports

You can configure scheduled overtime parking reports by specifying parking lot(s) and the statistical cycle. Once set, the platform will send an email to the specified recipient(s) regularly with the report attached, which shows the records of overtime parking vehicles detected during the set time period.

Before You Start

- Set the email template with recipient information, subject, and content.
- Set email settings such as the sender's email address, name, and SMTP server address and port No.
- Make sure you have added the parking lot(s). For details, refer to ***Add Parking Lot*** .

Steps

1. On the left navigation pane, select **Basic Configuration → Overtime Parking Report** .
2. Enter the Create Report page.

- For configuring scheduled reports for the first time, click **Add** in the middle of the page.
- If you have configured scheduled reports before, click + at the top of the left pane.

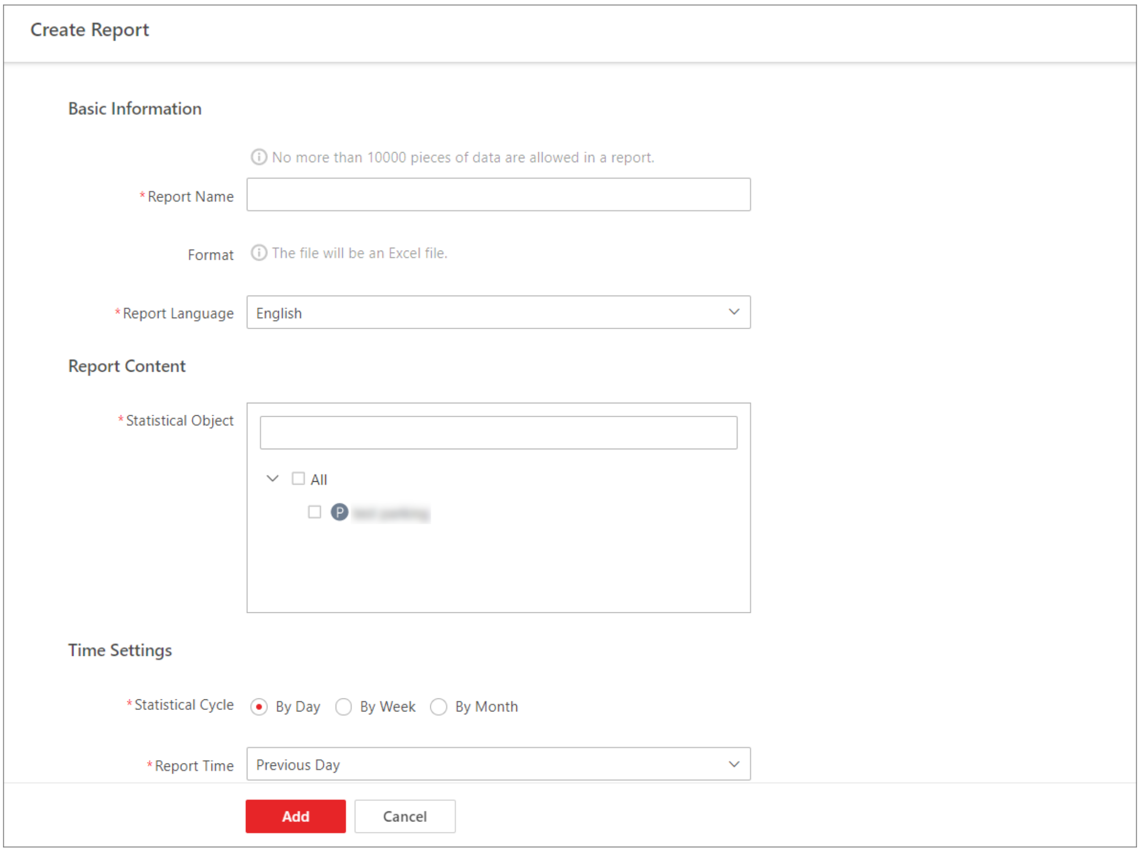


Figure 22-51 Configure Scheduled Report

3. Create a name for the report and select a report language from the drop-down list.
4. Select the parking lot(s) as the statistical object(s).
5. Set time parameters for the report.

Statistical Cycle

By Day

The report contains analysis results of a day.

By Week

The report contains analysis results of a week or two weeks.

By Month

The report contains analysis results of a month.

Report Time

The available report time varies with the statistical cycle you selected.

- If the statistical cycle is set to **By Day**, you can select **Previous Day** as the report time, which means the report will contain analysis results of the day (24 hours) before the sending time.
- If the statistical cycle is set to **By Week**, you can select **Recent 7 Days** or **Recent 14 Days** as the report time, which means the report will contain analysis results of the last 7/14 days before the sending time.
- If the statistical cycle is set to **By Month**, you can select **Current Month** or **Last Month** as the report time, which means the report will contain analysis results of the current/last month.

Sending Date / Sending Time

- When the statistical cycle is set to **By Day**, the Sending Date field is required, as you need to select the day(s) of the week to determine the day(s) of which analysis results will be contained in the report and on which the report will be sent.
  For example, if you select **Friday** and **Monday**, and set the Sending Time field to ***08:00***, a report containing analysis results of Thursday will be sent at 08:00 on Friday and another report containing analysis results of Sunday will be sent at 08:00 on Monday.
- When the statistical cycle is set to **By Week**, you should set the time and a day of the week to determine the period during which analysis results will be contained in the report and at what time the report will be sent.
  For example, if you select **Recent 7 Days** in the Report Time field and set the Sending Time field to ***Sunday*** and ***12:00***, a report containing analysis results between the last Sunday and the current Saturday (7 days in total) will be sent at 12:00 on the current Sunday.
- When the statistical cycle is set to **By Month**, you should set the time and a specific date to determine the period during which analysis results will be contained in the report and at what time the report will be sent.
  For example, if you select **Current Month** in the Report Time field and set the Sending Time field to ***30*** and ***12:00***, a report containing analysis results of the current month will be sent at 12:00 on the 30th.

Effective Period (Optional)

Set a period in which the above time settings will take effect. Outside the effective period, no report will be sent according to the configured sending time.

6. **Optional:** Set the advanced parameters.

Send Report via Email

Select an email template from the drop-down list to define the recipient information and email format (subject and content), so that the report can be sent to the recipient(s) regularly via email.

Note

You can select an existing email template or click **Add** to add a new one.

Upload to SFTP

Configure SFTP settings including the SFTP address, port No., user name, password, and the saving path for the report to be uploaded to the SFTP server regularly.

Note

You can also click → **SFTP Settings** at the top of the left pane to configure the corresponding parameters.

Save to Local Storage

Configure a saving path for the report to be saved to the local storage regularly.

Note

You can also click → **Configure Local Storage** at the top of the left pane to configure the saving path.

7. Click **Add** to finish setting the scheduled report rule.

22.9 Set Basic Parameters of Parking Management

On the Web Client, you can select the statistical source of parking and enable fuzzy search for the Self-Service Vehicle Finding Client in the parking lot to help vehicle owners find their vehicles more quickly and conveniently. The date format displayed on the Self-Service Vehicle Finding Client or display screens of the parking lot can also be predefined.

On the left navigation pane, select **Basic Configuration → Basic Parameter** .

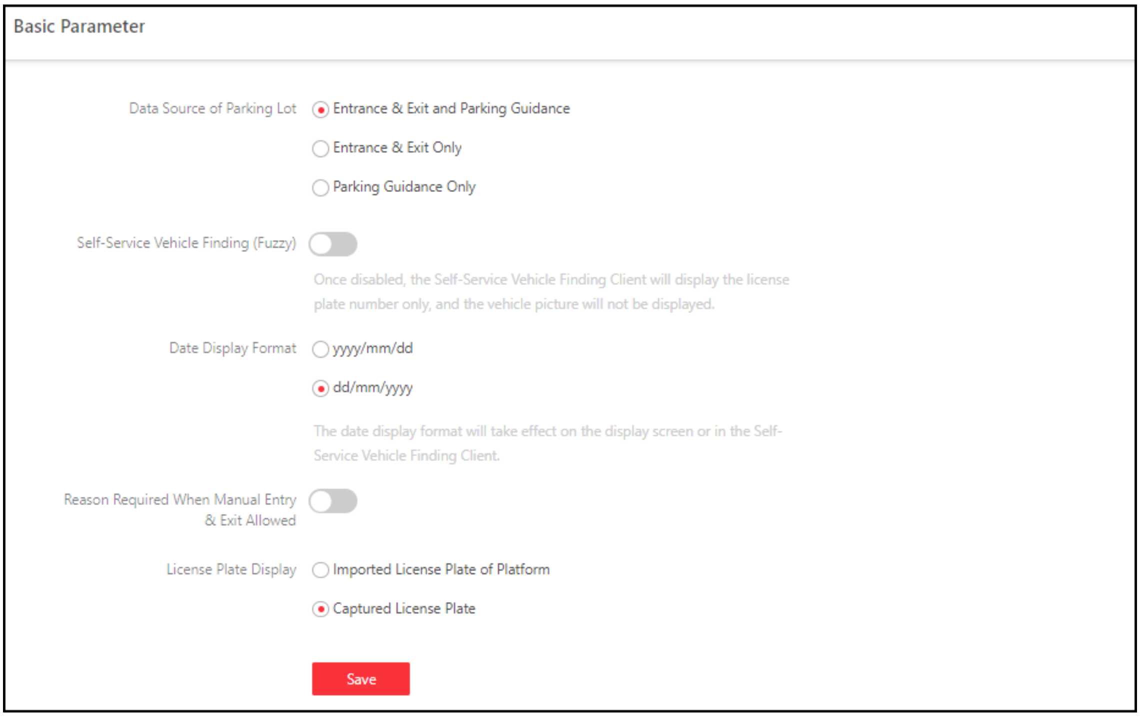


Figure 22-52 Set Basic Parameters

Statistical Source of Parking

Select a source for parking statistics. The following table shows the relations between statistics types and sources.

Table 22-3 Relations Between Statistics Types and Sources in Different Modes

Mode	Statistics Type	Source
Entrance & Exit and Parking Guidance Mode	(Web Client) Real-Time Parking Space Statistics in Operation Report	Entrance & Exit
	(Web Client) Parking Space Occupancy Statistics in Operation Report	Parking Guidance
	(Web Client) Parking Duration Distribution in Operation Report	Entrance & Exit
	(Web Client) Traffic Flow Statistics in Operation Report	Entrance & Exit
	(Web Client & Control Client) Parking Space Overview	Entrance & Exit
	(Control Client) Occupancy Rate of Parking Lot in Parking Space Monitoring	Entrance & Exit

Mode	Statistics Type	Source
	(Control Client) Occupancy Rate of Floor in Parking Space Monitoring	Parking Guidance
Entrance & Exit Mode	(Web Client) Real-Time Parking Space Statistics in Operation Report	Entrance & Exit
	(Web Client) Parking Space Occupancy Statistics in Operation Report	By default, the statistics is not displayed. You can configure the source by yourself.
	(Web Client) Parking Duration Distribution in Operation Report	Entrance & Exit
	(Web Client) Traffic Flow Statistics in Operation Report	Entrance & Exit
	(Web Client & Control Client) Parking Space Overview	Entrance & Exit
	(Control Client) Occupancy Rate of Parking Lot in Parking Space Monitoring	Entrance & Exit
	(Control Client) Occupancy Rate of Floor in Parking Space Monitoring	Entrance & Exit
Parking Guidance Mode	(Web Client) Real-Time Parking Space Statistics in Operation Report	Parking Guidance
	(Web Client) Parking Space Occupancy Statistics in Operation Report	Parking Guidance
	(Web Client) Parking Duration Distribution in Operation Report	Parking Guidance
	(Web Client) Traffic Flow Statistics in Operation Report	By default, the statistics is not displayed. You can configure the source by yourself.
	(Web Client & Control Client) Parking Space Overview	Parking Guidance
	(Control Client) Occupancy Rate of Parking Lot in Parking Space Monitoring	Parking Guidance
	(Control Client) Occupancy Rate of Floor in Parking Space Monitoring	Parking Guidance

Self-Service Vehicle Finding (Fuzzy)

Switch on **Self-Service Vehicle Finding (Fuzzy)** to enable fuzzy search for the Self-Service Vehicle Finding Client. Once enabled, the Self-Service Vehicle Finding Client will display license plate numbers without displaying vehicle pictures when finding vehicles, so that the time consumption in vehicle finding will be reduced.
For details, refer to ***Self-Service Vehicle Finding Client*** .

Date Display Format

Select **yyyy/mm/dd** or **dd/mm/yyyy** in the Date Display Format field to determine the date format displayed on the Self-Service Vehicle Finding Client or display screens of the parking lot.

Reason Required When Manual Entry & Exit Allowed

Switch on **Reason Required When Manual Entry & Exit Allowed** to require entering a reason when the entry & exit is allowed manually.

License Plate Display

Select the license plate display mode for display screens, real-time events, and passing records of parking lots. **Imported License Plate of Platform** is to display the registered license plate number, and **Captured License Plate** is to display the actual license plate number recognized by ANPR cameras.

22.10 Self-Service Vehicle Finding Client

The self-service vehicle finding client is for users to find their vehicles in the parking lot easily and accurately.

- You can search for your vehicle by license plate No., parking space No., and the time the vehicle is parked in.
- If your vehicle does not have a license plate, you can click **No License Plate**, and set specific conditions to search for it.
- When you are searching for your vehicle, both your and your vehicle's position will be displayed on the map, which makes it more helpful for you to find your vehicle.
- When entered a parking lot, you can quickly find vacant parking spaces. When leaving a parking lot, you can get the route to find the vehicle on the map by entering the license plate numer.

Note

On the Web Client, you can choose whether to enable fuzzy search for the self-service vehicle finding client and set the date display format of the client. For details, see ***Set Basic Parameters of Parking Management*** .

Chapter 23 ANPR (Automatic Number Plate Recognition)

You can search for passing vehicles detected by ANPR cameras, generate a report for showing the number of passing vehicles detected by the specified ANPR camera(s) during the specific period, and set parameters to regularly send the generated report to target recipients.

On the top navigation bar, select → **Passing Management → ANPR** .

23.1 Search for Passing Vehicles Detected by Cameras

If the added ANPR (Automatic Number Plate Recognition) cameras are properly configured, and the vehicles' license plates are successfully detected and recognized, you can search for the related passing vehicle information.

Before You Start

Make sure the License you purchased supports ANPR function.

Steps

1. On the left navigation pane, click **Passing Vehicle Search** .
2. Select **Camera** or **UVSS** as the type of sources that detected the passing vehicles.
3. Select the source(s).
   - If **Camera** is selected as the source type, click , select the current site or a remote site, and specify the ANPR camera(s).
   - If **UVSS** is selected as the source type, check the UVSS(s).
4. Set the time duration for search.
5. Switch on and set the search condition(s) according to your needs. Here we only introduce some conditions that may confuse you.

Note

For the Middle East and North Africa regions, Country/Region and Plate Category must be enabled. Once enabled, the country/region and plate category information will be included in the search results.

Country/Region

The country/region where the vehicle's license plate number is registered.

License Plate Number

- **No License Plate**: Search for vehicles without license plates.
- **With License Plate**: Enter a keyword to search for vehicles by license plate number.

Driving Speed

Range of vehicle driving speed. This condition is available only when the source type is selected as **Camera**.

Driving Direction

- **Forward**: The vehicle moved toward the camera with its headstock facing the camera.
- **Reverse**: The vehicle moved away from the camera with its rear facing the camera.
- **Other**: The vehicle moved toward or away from the camera in other directions.

Vehicle List

Search for passing vehicles in the specific vehicle list(s). This condition is available only when the source type is selected as **Camera**.

Additional Information

The item(s) of additional vehicle information you customized. For how to customize vehicle information, refer to ***Customize Vehicle Information*** .

6. Click **Search**.

   The matched passing vehicles will be displayed on the right.
7. **Optional:** Perform the following operation(s) after searching for passing vehicles.

View Vehicle Details	Click a license plate number in the License Plate No. column to open the vehicle details pane. You can view the captured vehicle / undercarriage / license plate picture, the recognized license plate number, the vehicle owner information, the vehicle information, and the detection source information.
Export Passing Vehicles	Click **Export** and select **Excel** or **CSV** as the exported file format. • If you select **Excel** as the file format, you can check **Export Picture** to save pictures contained in the search results to the local PC with the exported file. • No more than 500 passing vehicles with captured pictures can be exported in the Excel format at one time. Otherwise, you need to go to the Control Client to export them. • No more than 100,000 passing vehicles without captured pictures can be exported at one time. • Check the export task status and progress in **Download Center**.
Sort Search Results	**Sort by Time** Sort search results by the time when vehicles are passing through the camera. **Sort by Vehicle Passing Times** Sort search results by times that vehicles passed through the camera.

23.2 Generate Vehicle Analysis Report

For ANPR cameras, you can generate a report to show the number of passing vehicles detected by specified cameras during specified time periods.

Steps

1. On the left navigation pane, click **Vehicle Analysis** .
2. Select the camera(s) for this report.
   1) Click in the Camera field to open the Select Camera pane.
   2) On the pane, select a site from the drop-down list to show its areas.
   3) Click an area to show its cameras which support the ANPR function.

   Note

   Only the online ANPN cameras will be displayed here.

   4) Check the camera(s) for analysis.

   Note

   No more than 20 ANPR cameras can be selected for one time analysis.

   5) Click anywhere outside the Select Camera pane to finish selecting the camera(s).
3. Select the report type as daily report, weekly report, monthly report, or annual report, or customize the time interval for a report.

   Daily Report

   The daily report shows data on a daily basis. The platform will calculate the number of vehicles in each hour of one day.

   Weekly Report / Monthly Report / Annual Report

   As compared with the daily report, the weekly report, monthly report, and annual report can be less time-consuming, since they are not to be submitted every day. The platform calculates the number of vehicles on each day of a week, on each day of one month, and in each month of one year.

   Custom Time Interval

   Customize the days in the report to analyze the number of vehicles on each day or in each month of the custom time interval.
4. Set the time or a time period for analysis.
5. Click **Generate Report**.

   The statistics of passing vehicles detected by all the selected camera(s) are displayed on the right pane.

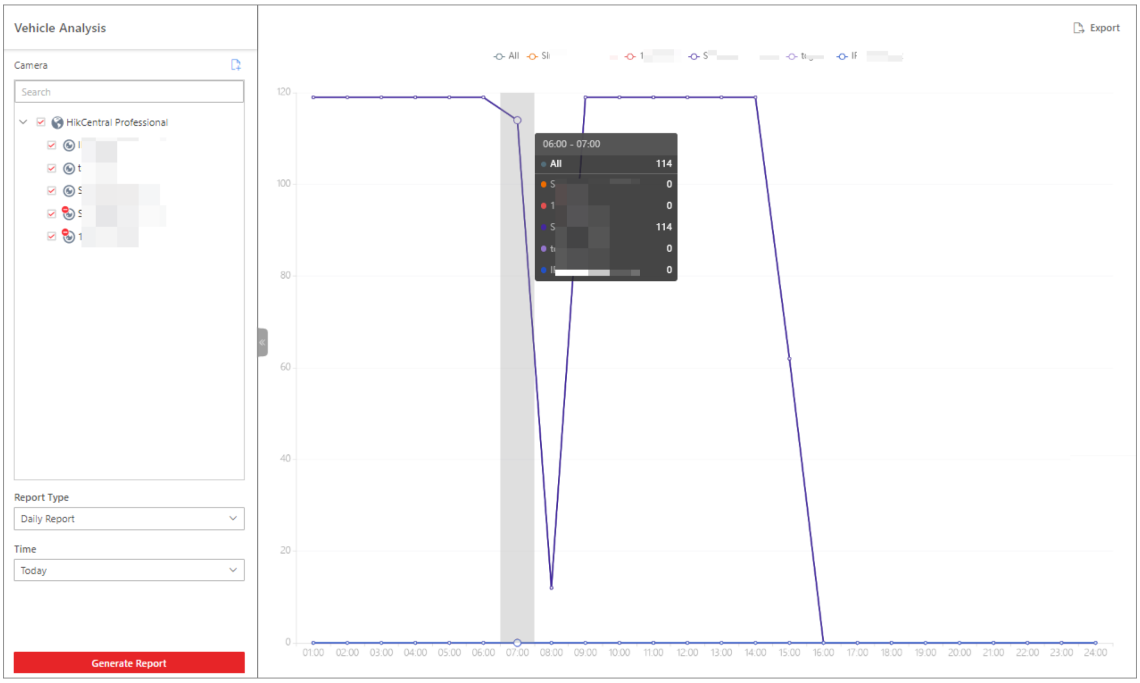


Figure 23-1 Vehicle Analysis Report

6. **Optional:** Export the generated report to the local PC.
   1) Click **Export** in the top right corner of the report pane.

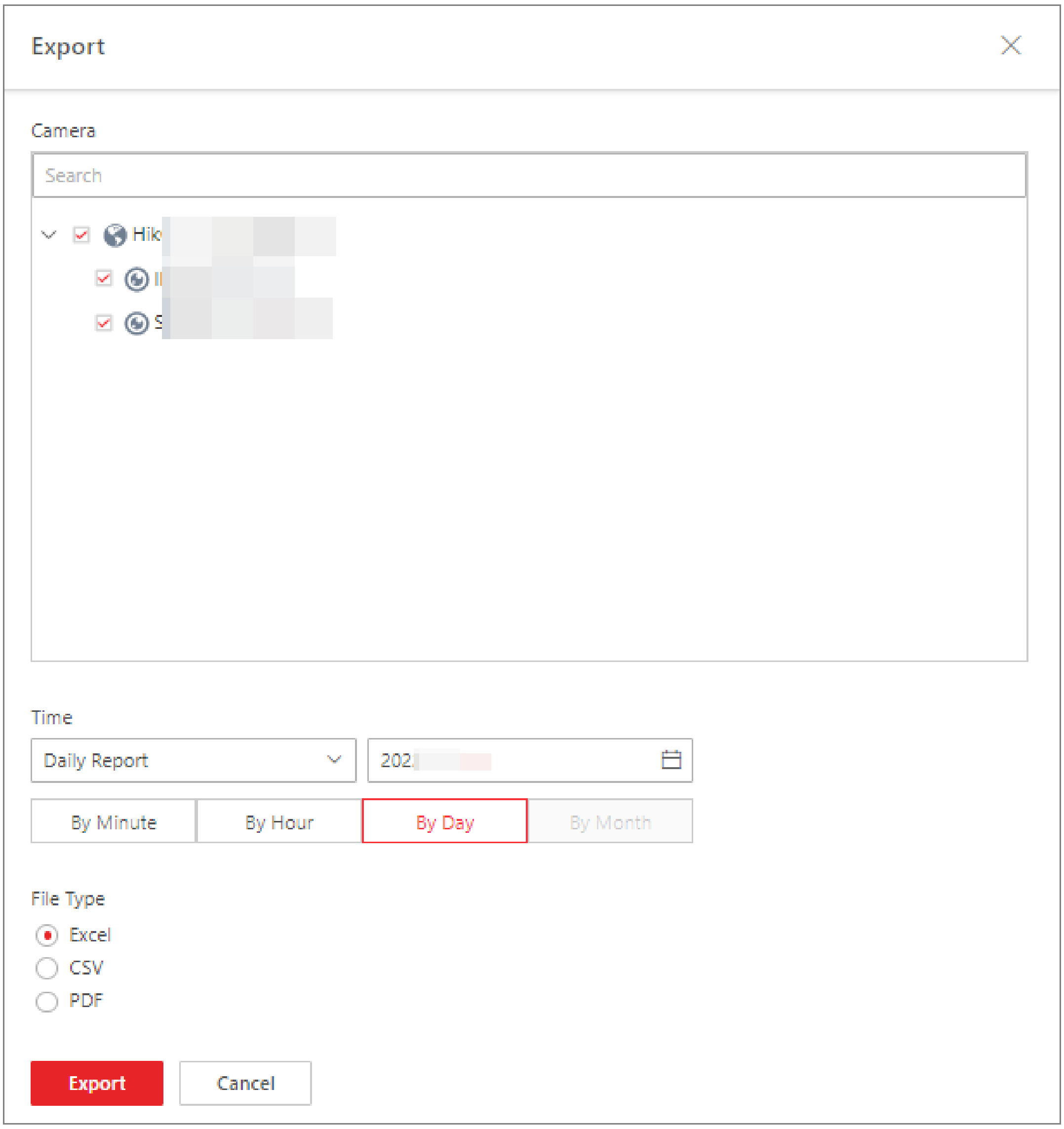


Figure 23-2 Export Vehicle Analysis Report

2) **Optional:** Select the camera(s) contained in the report and change the report type or time.

3) Select a shorter time period to view more detailed data of each camera.

By Minute

The exported report shows the detailed data of each minute for each camera (if the camera has been configured to report vehicle analysis data to the platform every minute). This option is only available for the daily report.

By Hour

The exported report shows the detailed data of each hour for each camera. This option is available for the daily/weekly/monthly/customized-interval report.

By Day

The exported report shows the detailed data of each day for each camera. This option is available for all types of reports.

By Month

The exported report shows the detailed data of each month for each camera. This option is available for the monthly/annual report.

4) Set the exported file format to **Excel**, **CSV**, or **PDF**.
5) Click **Export** to start exporting the report.

Note

You can check the export task status and progress in Download Center.

23.3 Send Vehicle Analysis Reports Regularly

You can set a regular report rule for specified ANPR cameras. Once set, the platform will send an email with a report attached to the target recipients daily, weekly, or monthly, showing the number of passing vehicles detected by these ANPR cameras during the set time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as sender address, SMTP server address, and port No. For details, refer to ***Configure Email Account*** .

Steps

1. On the left navigation pane, click **Scheduled Report Configuration** .
2. Enter the Create Report page.
   - For the first time, click **Add** in the middle of the Scheduled Report Configuration page.
   - For non first time, click + at the top of the left pane.

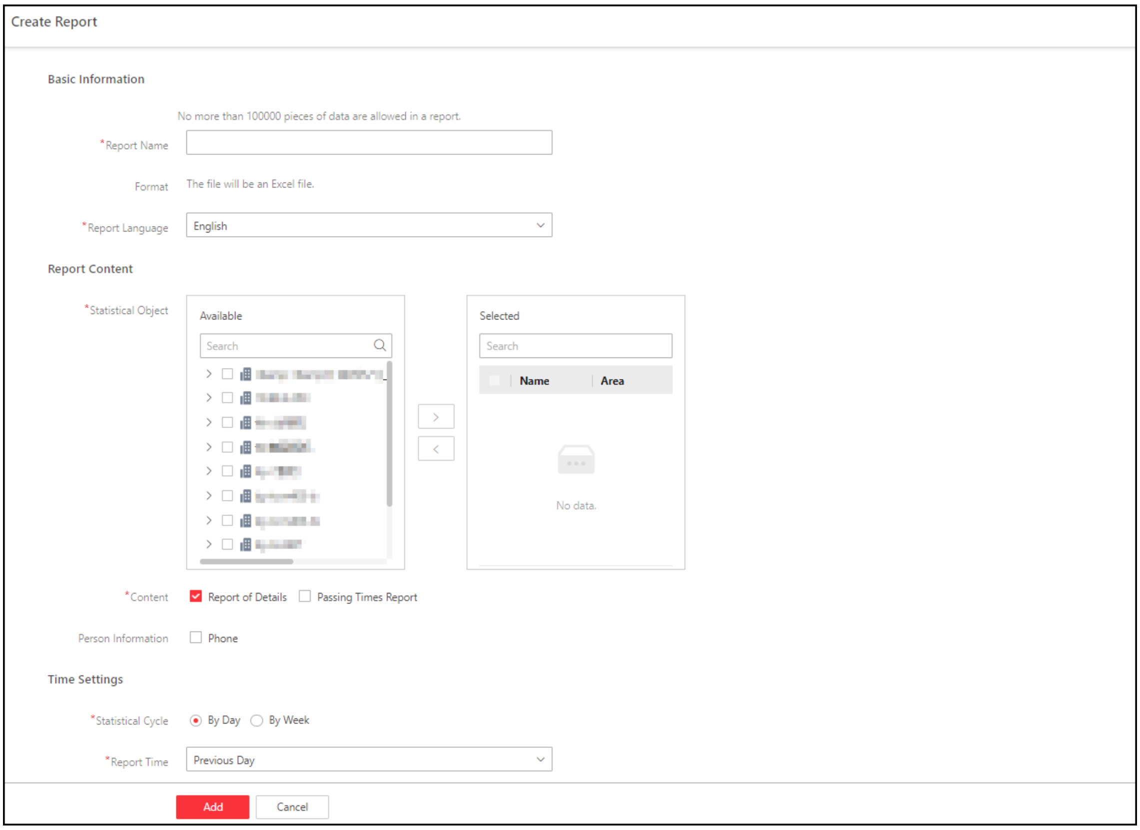


Figure 23-3 Create Report Page

3. Create a name for the report and select a report language from the drop-down list.
4. Set the report content.

Statistical Object

Select the ANPR camera(s) whose analysis results should be contained in the report.

Content

Check **Report of Details** or **Passing Times Report**or both of them to determine the content contained in the report. If you checked **Passing Times Report**, you can get the statistics of vehicle passing times in the report.

Person Information

Check the sensitive information about the vehicle owner to be exported in the report.

5. Set time parameters for the report.

Statistical Cycle

By Day

The report contains analysis results of a day.

By Week

The report contains analysis results of a week or two weeks.

Report Time

The available report time varies with the statistical cycle you selected.

- If the statistical cycle is set to **By Day**, you can select **Previous Day** as the report time, which means that the report will contain analysis results of the day (24 hours) before the sending time.
- If the statistical cycle is set to **By Week**, you can select **Recent 7 Days / Recent 14 Days** as the report time, which means that the report will contain analysis results of the recent 7/14 days before the sending time.

Send Date / Send Time

- When the statistical cycle is set to **By Day**, the Send Date field is required, as you need to select the day(s) of the week to determine the day(s) of which analysis results will be contained in the report and on which the report will be sent.
  For example, if you select **Friday** and **Monday** in the Send Date field, and set the Send Time field to ***08:00***, a report containing analysis results of Thursday will be sent at 08:00 on Friday and another report containing analysis results of Sunday will be sent at 08:00 on Monday.
- When the statistical cycle is set to **By Week**, you should set the time and a day of the week to determine the period during which analysis results will be contained in the report and at/on which the report will be sent.
  For example, if you select **Recent 7 Days** in the Report Time field and set the Send Time field to ***Sunday*** and ***12:00***, a report containing analysis results between the last Sunday and the current Saturday (total 7 days) will be sent at 12:00 on the current Sunday.

Effective Period (Optional)

Set a period in which the above time settings will take effect. Outside the effective period, the report will not be sent according to the configured sending time.

6. **Optional:** Set advanced parameters.

Send Report via Email

Select an email template from the drop-down list to define the recipient information and email format, so that the report can be regularly sent to the recipient via email.

Note

You can click **Add** to add a new email template. For setting an email template, refer to ***Add Email Template for Sending Report Regularly*** .

Upload to SFTP

Configure SFTP settings including address, port No., user name, password, and saving path for the report to be uploaded to the SFTP regularly.

Note

You can also click → **SFTP Settings** at the top of the left pane to open the SFTP Settings pane to configure the corresponding parameters.

Save to Local Storage

Configure a saving path for the report to be saved to the local storage regularly.

Note

You can also click → **Configure Local Storage** at the top of the left pane to configure the corresponding parameter.

7. Click **Add** to finish setting the scheduled report rule.

Chapter 24 Security Inspection Management

You can manage the added security inspection devices in the platform and perform the related operations, such as adding security inspection channels to the area, viewing videos of security inspection, searching for historical data, etc.

24.1 Flow Chart of Security Inspection

The following flow chart shows the process of the configurations and operations of security inspection.

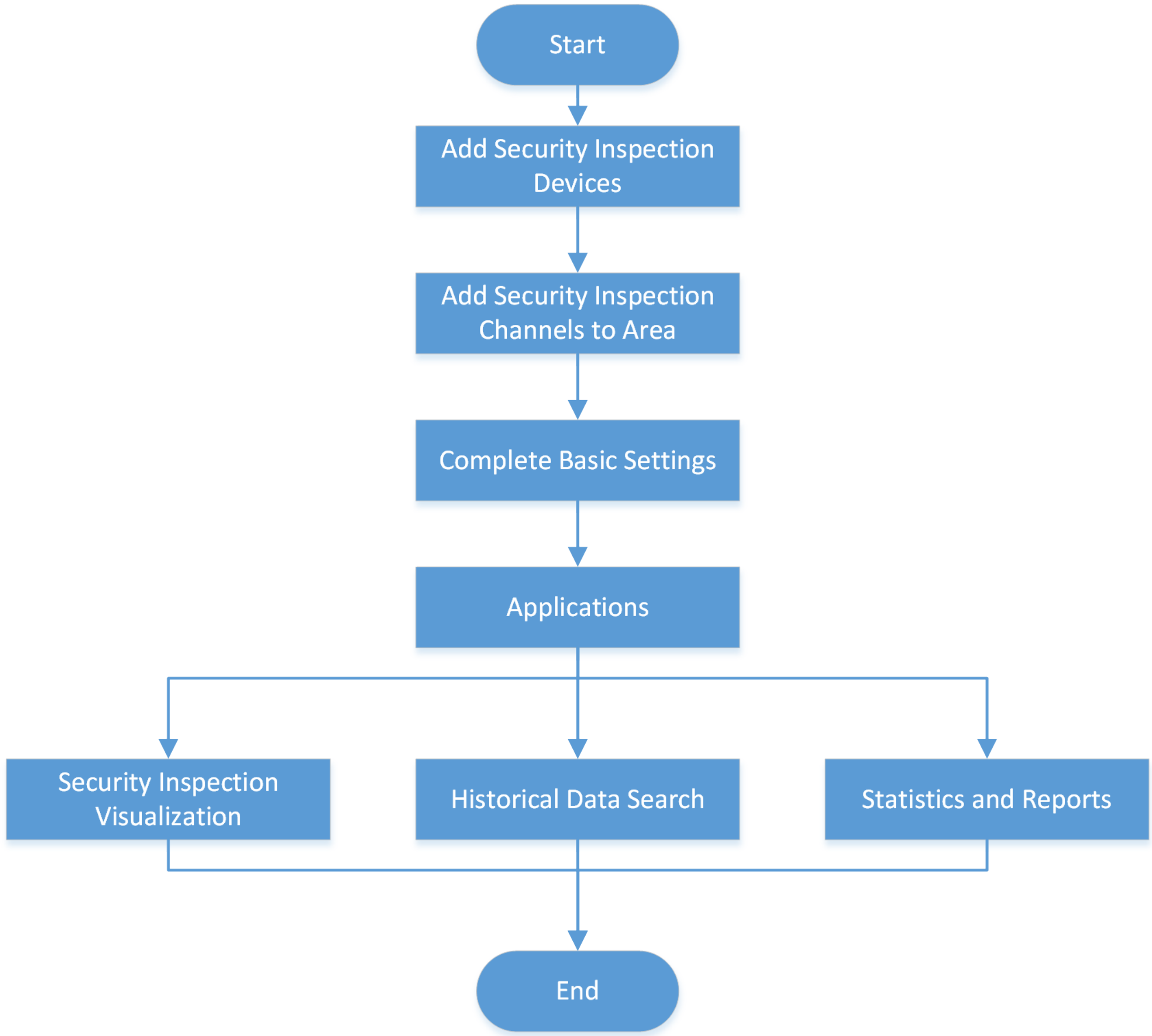


Figure 24-1 Flow Chart of Security Inspection

Table 24-1 Flow Chart of Security Inspection

Step	Description
Add Security Inspection Devices	Add devices that support security inspection to the platform by different methods (e.g., online detection, IP address, port segment, device ID). For details, refer to ***Manage Security Inspection Devices*** .
Add Security Inspection Channels to Area	Add security inspection channels and link security inspection devices to them for live view and playback.

Step	Description
	For details, refer to ***Add Security Inspection Channels to Area*** .
Complete Basic Settings	Configure the basic parameters for security inspection, such as absence alarm interval and event retention duration. For details, refer to ***Configure Security Inspection*** .
Security Inspection Visualization	During live view and playback of the videos streamed from analyzers, you can view the marked out articles of the checked package, package information, and package owner. For those of walkthrough metal detectors, you can view the information of the checked people. For details, refer to ***View Videos of Security Inspection*** .
Historical Data Search	Search for the historical data of security inspection, including package detection records, metal detection records, and inspector absence records. For details, refer to ***Historical Data Search*** .
Statistics and Reports	Generate a package detection report and a people inspection report based on the specified features. You can also export reports to the local PC. For details, refer to ***Generate Package Detection Report*** and ***Generate People Inspection Report*** .

24.2 Configure Security Inspection

You can configure the basic parameters for security inspection.

Steps

1. In the top left corner of the Home page, select ▦ → **All Modules** → **Smart Security Inspection** → **Basic Settings** → **Parameter Configuration** .
2. Configure the following parameters and click **Save**.

   Time of Matching Person with Package (sec)

   This parameter is for analyzers. When the package is detected, the owner is more likely to be captured within the configured time range.

   Absence Alarm Interval (sec)

   Set the interval to upload the absence alarm information.

   Abnormal Skin-Surface Temperature Threshold (℃)

   Set the abnormal skin-surface temperature threshold. An alarm will be triggered if a person's skin-surface temperature above the threshold is detected.

Event Retention Duration

Select the duration that the event information can be saved for.

Real-Time Alarm Configuration

Select the prohibited article(s) for package detection, the abnormal event type(s) for abnormal event detection, and the alarm type(s) for metal detection.

Manual Handling Action

Click **Add** to customize manual handling actions which will be displayed in the alarm pop-up window.

24.3 Add Security Inspection Channels to Area

You can add security inspection channels and link security inspection devices to them for live view and playback.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Basic Settings** → **Security Inspection Channel Management** .
2. Click **Add** to enter the Add Security Inspection Channel page.
3. Enter the channel name.
4. Select an area from the area list.
5. **Optional:** In the Link Device field, select one security inspection device in the available list and click .

   Note

   If you do not link a device to the channel, live view and playback are not available via this channel.

   The device will be displayed in the added list.
6. **Optional:** In the Link Camera field, select one security inspection device in the available list and click .

   The camera will be displayed in the selected list.
7. Click **Add**.

24.4 View Videos of Security Inspection

During live view and playback of the videos streamed from analyzers, you can view the marked out articles of the checked package, package information, and package owner. For those of walk-through metal detectors, you can view the information of the checked people.

Note

Make sure you have added security inspection channels and linked devices with them. See details in ***Add Security Inspection Channels to Area*** .

In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Security Inspection Visualization** .

Select a security inspection device and click **Live View** or **Playback**.

Note

In the top right corner of the Live View or Playback page, you can click to set video parameters.

Live View

Move the mouse cursor to the lower edge of the live view window and perform more operations.

Icon	Function	Description
	Capture	Take a snapshot of the current video.
	Start Recording	Start recording the video.
	Enable Audio	Turn off/on the sound and adjust the volume.
	Enable Video Enhancement	Adjust the video image including brightness, saturation, contrast, and hue.
	Stream Switch	Switch the video stream to main stream, sub-stream (if supported), or smooth stream (if supported).
	Instant Playback	Switch to instant playback mode to view the recorded videos.
	Turn on Alarm Output	Turn on/off the alarm outputs linked with the camera.
	Start Two-Way Audio	Start two-way audio to realize voice talk with the person at the device.

Playback

Move the cursor to the lower edge of the playback window and perform more operations.

Icon	Function	Description
	Capture	Take a snapshot of the current video.
	Clip	Clip the video files for current playback.
	Enable Audio	Turn off/on the sound and adjust the volume.
	Open Digital Zoom	Zoom in/out the video.
	Show Stream Information	Display the stream information in the video image.
	Enable Video Enhancement	Adjust the video image including brightness, saturation, contrast, and hue.
	Stream Switch	Switch the video stream to main stream, sub-stream (if supported), or smooth stream (if supported).
	Fisheye Expansion	Correct the video image and reverse the effects of geometric distortions caused by fisheye camera lens. **Note** This function is available only for fisheye cameras.
	Add a Tag	Add a tag to the video file to mark a time point.
	Add a Lock	Lock a video segment to protect it from being deleted or being overwritten when the HDD is full.
	Counterclockwise Rotate	Counterclockwise rotate the video image.
	Start Two-Way Audio	Start two-way audio to realize voice talk with the person at the device.

24.5 Historical Data Search

You can search for the historical data of security inspection, including package detection records, metal detection records, and inspector absence records.

24.5.1 Search for Package Detection Records

You can set search conditions, including time, article type, and location, to search for the package detection records.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Historical Data Search** → **Package Detection Record Search** .
2. Select a period of time from the drop-down list.
3. In the Article Type field, select one or multiple prohibited or normal articles.
4. In the Location field, select one or multiple channels from the list.
5. Click **Search**.

   The matched records will be displayed.

   Note

   You can view the event details by clicking the event time.

No.	Time	Location	Type	Number of Prohibited Articles
1	2021-05-08 16:57:18	[illegible]	Normal Article	-
2	2021-05-08 16:56:41	[illegible]	Normal Article	-
3	2021-05-08 16:55:01	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
4	2021-05-08 16:55:01	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
5	2021-05-08 16:54:56	[illegible]	Normal Article	-
6	2021-05-08 16:54:39	[illegible]	Normal Article	-
7	2021-05-08 16:54:37	[illegible]	Firework and Firecracker/Taser/Umbrella	10
8	2021-05-08 16:54:37	[illegible]	Firework and Firecracker/Taser/Umbrella	10
9	2021-05-08 16:54:12	[illegible]	Battery/Firework and Firecracker/Taser/U...	12
10	2021-05-08 16:54:12	[illegible]	Battery/Firework and Firecracker/Taser/U...	12
11	2021-05-08 16:53:51	[illegible]	Battery/Firework and Firecracker/Taser/U...	8
12	2021-05-08 16:53:51	[illegible]	Battery/Firework and Firecracker/Taser/U...	8
13	2021-05-08 16:53:32	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
14	2021-05-08 16:53:32	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
15	2021-05-08 16:53:18	[illegible]	Normal Article	-
16	2021-05-08 16:53:10	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
17	2021-05-08 16:53:10	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
18	2021-05-08 16:52:49	[illegible]	Battery/Firework and Firecracker/Taser/U...	8
19	2021-05-08 16:52:49	[illegible]	Battery/Firework and Firecracker/Taser/U...	8
20	2021-05-08 16:52:43	[illegible]	Normal Article	-

Total: 398 50 /Page < 1 2 3 4 5 6 ··· 8 > 1 / 8 Go

Figure 24-2 Search for Package Detection Records

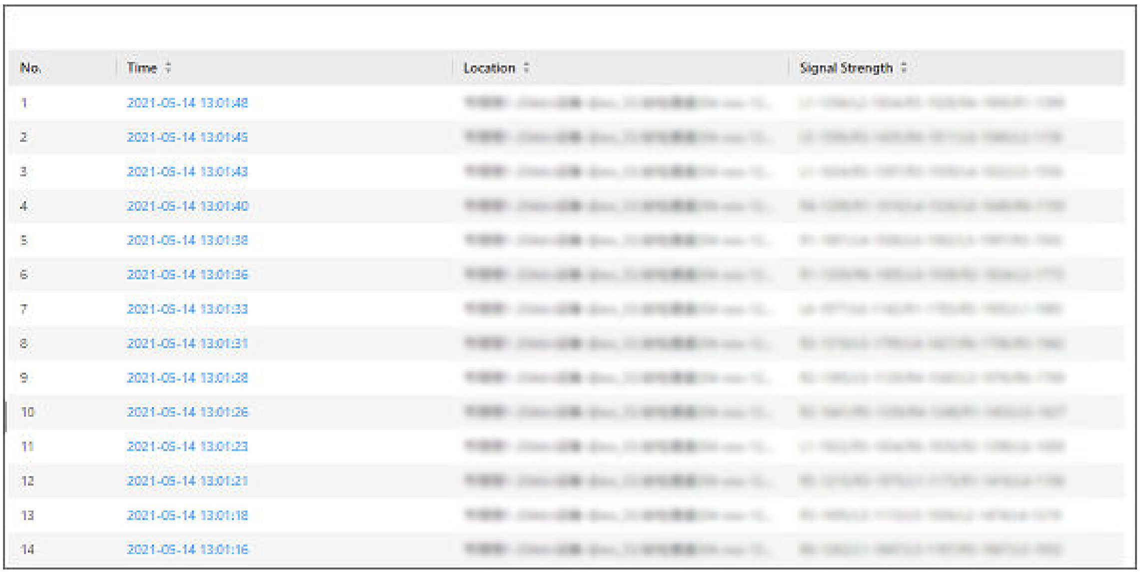
24.5.2 Search for Metal Detection Records

You can set the search conditions, including time and location, to search for the metal detection records.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Historical Data Search** → **Metal Detection Record Search** .
2. Select a period of time from the drop-down list.
3. In the Location field, select one or multiple channels from the list.
4. Click **Search**.

   The matched records will be displayed.



No.	Time	Location	Signal Strength
1	2021-05-14 13:01:48	[illegible]	[illegible]
2	2021-05-14 13:01:45	[illegible]	[illegible]
3	2021-05-14 13:01:43	[illegible]	[illegible]
4	2021-05-14 13:01:40	[illegible]	[illegible]
5	2021-05-14 13:01:38	[illegible]	[illegible]
6	2021-05-14 13:01:36	[illegible]	[illegible]
7	2021-05-14 13:01:33	[illegible]	[illegible]
8	2021-05-14 13:01:31	[illegible]	[illegible]
9	2021-05-14 13:01:28	[illegible]	[illegible]
10	2021-05-14 13:01:26	[illegible]	[illegible]
11	2021-05-14 13:01:23	[illegible]	[illegible]
12	2021-05-14 13:01:21	[illegible]	[illegible]
13	2021-05-14 13:01:18	[illegible]	[illegible]
14	2021-05-14 13:01:16	[illegible]	[illegible]

Figure 24-3 Search for Metal Detection Records

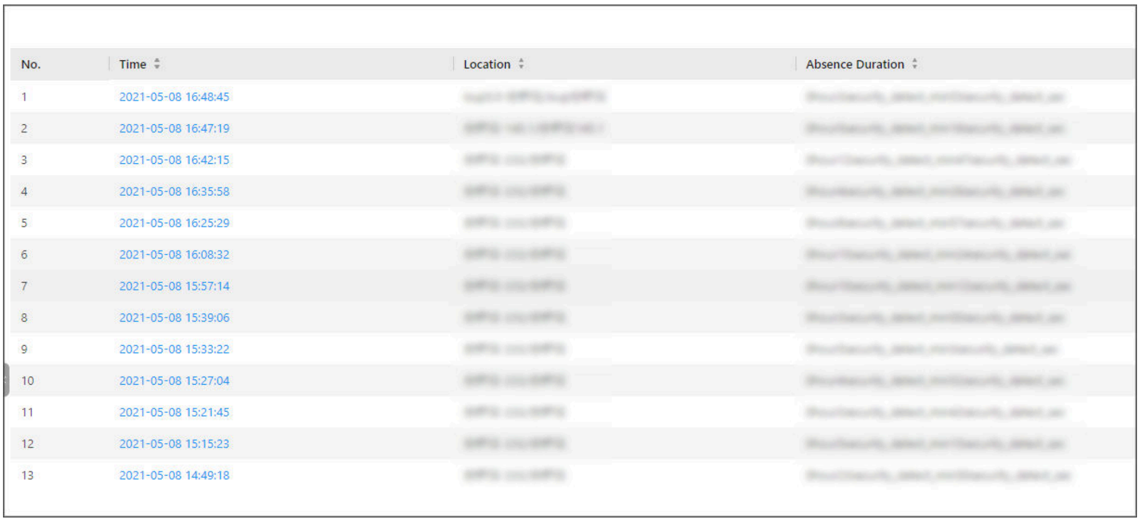
24.5.3 Search for Absence Records

You can set the search conditions, including time and location, to search for the absence records.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Historical Data Search** → **Absence Record Search** .
2. Select a period of time from the drop-down list.
3. In the Location field, select one or multiple channels from the list.
4. Click **Search**.

   The matched records will be displayed.



No.	Time	Location	Absence Duration
1	2021-05-08 16:48:45	[illegible]	[illegible]
2	2021-05-08 16:47:19	[illegible]	[illegible]
3	2021-05-08 16:42:15	[illegible]	[illegible]
4	2021-05-08 16:35:58	[illegible]	[illegible]
5	2021-05-08 16:25:29	[illegible]	[illegible]
6	2021-05-08 16:08:32	[illegible]	[illegible]
7	2021-05-08 15:57:14	[illegible]	[illegible]
8	2021-05-08 15:39:06	[illegible]	[illegible]
9	2021-05-08 15:33:22	[illegible]	[illegible]
10	2021-05-08 15:27:04	[illegible]	[illegible]
11	2021-05-08 15:21:45	[illegible]	[illegible]
12	2021-05-08 15:15:23	[illegible]	[illegible]
13	2021-05-08 14:49:18	[illegible]	[illegible]

Figure 24-4 Search for Absence Records

24.6 Generate Package Detection Report

You can generate a package detection report based on the package detection records, percentage of packages with prohibited articles, or prohibited article types. You can also export the report to the local PC.

Steps

1. In the top left corner of the Home page, select ⊞ → **All Modules** → **Smart Security Inspection** → **Statistics and Reports** → **Package Detection Report** .
2. In the Type field, select **Package Detection Records**, **Percentage of Packages with Prohibited Articles**, or **Prohibited Article Types**.
3. In the Location field, select one or multiple channels from the list.
4. Select a report type and a specific time period.
5. Click **Generate Report**.
6. **Optional:** Click **Export** to export the report to the local PC.

24.7 Generate People Inspection Report

You can generate a people inspection report based on the number of checked persons or percentage of metal detection alarms. You can also export the report to the local PC.

Steps

1. In the top left corner of the Home page, select ⊞ → **All Modules** → **Smart Security Inspection** → **Statistics and Reports** → **People Inspection Report** .
2. In the Type field, select **Number of Checked Persons** or **Percentage of Metal Detection Alarms**.
3. In the Location field, select one or multiple channels from the list.

4. Select a report type and a specific time period.
5. Click **Generate Report**.
6. **Optional:** Click **Export** to export the report to the local PC.

Chapter 25 Skin-Surface Temperature Screening

After adding the temperature screening cameras and access control devices with temperature screening function to the system, you can view the temperature of the detected persons in the Skin-Surface Temperature module. The system also shows whether the detected person is wearing a mask or not. With skin-surface temperature screening and mask detection functions, the system provides an alert if an individual is running a fever or not wearing a mask.

In the Skin-Surface Temperature module, you can view the real-time and history temperature screening records and face mask detection records. You can also generate a report about these records to view the overall information.

Note

The mask detection function will show when the mask related function is turned on in the **System → Normal → User Preference** page.

25.1 Temperature Screening Configuration

Before temperature screening, you should set temperature screening point groups and add related temperature screening points to the added groups. Also, for the temperature screening points, you can configure their parameters including temperature screening threshold and alarm threshold.

25.1.1 Group Temperature Screening Points

You can group multiple temperature screening points for convenient management. For example, you can group all the temperature screening points on the same floor into a group.

Steps

1. On the top navigation bar, select → **Passing Management → Temperature Screening** .
2. On the left pane, click **Basic Configuration → Temperature Screening Configuration** .
3. Create temperature screening point group(s).
   1) Click + on the upper left corner of the page.
   2) Enter the name for the temperature screening point group as desired.
   3) Click **Add**.
4. Add temperature screening point(s) for the added temperature screening point group.

   Note

   Temperature screening points can be cameras and access control points that support temperature screening.

   1) Click **Add**.
   2) In the pop-up device list, check temperature screening point(s) as desired.

Note

You can enter a key word (supports fuzzy search) in the search box to quickly search for the target device(s).

3) Click **Add**.

5. **Optional:** After adding temperature screening point(s), perform following operations.

Delete	• Click to delete single temperature screening point. • Check multiple temperature screening points, and click **Delete** to batch delete the selected devices.
Configure Parameters	Check one or multiple temperature screening points, and click **Configuration** to configure related parameters for the selected device(s). **Note** For details, refer to ***Configure Temperature Screening Parameters*** .
Export	Click **Export** to export detailed information of temperature screening point(s) such as device type, serial No., and temperature screening threshold to the local PC.

25.1.2 Configure Temperature Screening Parameters

For the added temperature screening point(s), you can configure the related parameters including temperature screening threshold and alarm threshold.

Check one or more added temperature screening point(s), and click **Configuration** to configure temperature screening parameters.

Temperature Screening Threshold

Set the threshold for temperature screening. When the detected skin-surface temperature is higher than the threshold, a temperature screening event will be triggered.

Alarm Threshold

Set the threshold for alarm. When the detected skin-surface temperature is higher than the threshold, an alarm will be triggered.

Note

- The temperature screening threshold should be smaller than alarm threshold.
- For temperature screening points which are access control points, you should configure their temperature screening parameters on the device parameters configuration page.

25.2 Real-Time Skin-Surface Temperature Monitoring

You can view the latest skin-surface temperature information detected by screening points. If there are persons whose skin-surface temperatures are abnormal, you will know at the first time. Besides, you will be able to quickly locate the persons according to the displayed screening point name and screening group. For unregistered persons, you can quickly register for them.

On the top navigation bar, select ▦ → **Passing Management** → **Temperature Screening** . Then on the left pane, click **Skin-Surface Temperature**. Select a temperature screening point group on the left. Red number indicates the number of skin-surface temperature screening points. Black number indicates the total number of devices in a temperature screening point group.

In the Picture area, the latest captured picture is displayed on the left. When new pictures are captured and displayed here, old captured pictures will be displayed on the right as thumbnails with faces, screening point name, person name, similarity, temperature, wearing mask or not, and detecting time.

Persons with different features will be marked by different colors. Orange means the captured person is not wearing a mask, but skin-surface temperature is normal; red means the captured person's skin-surface temperature is abnormal; green means the captured person's skin-surface temperature is normal and the person is wearing a mask. Click **More** to jump to the History page to view more captured pictures.

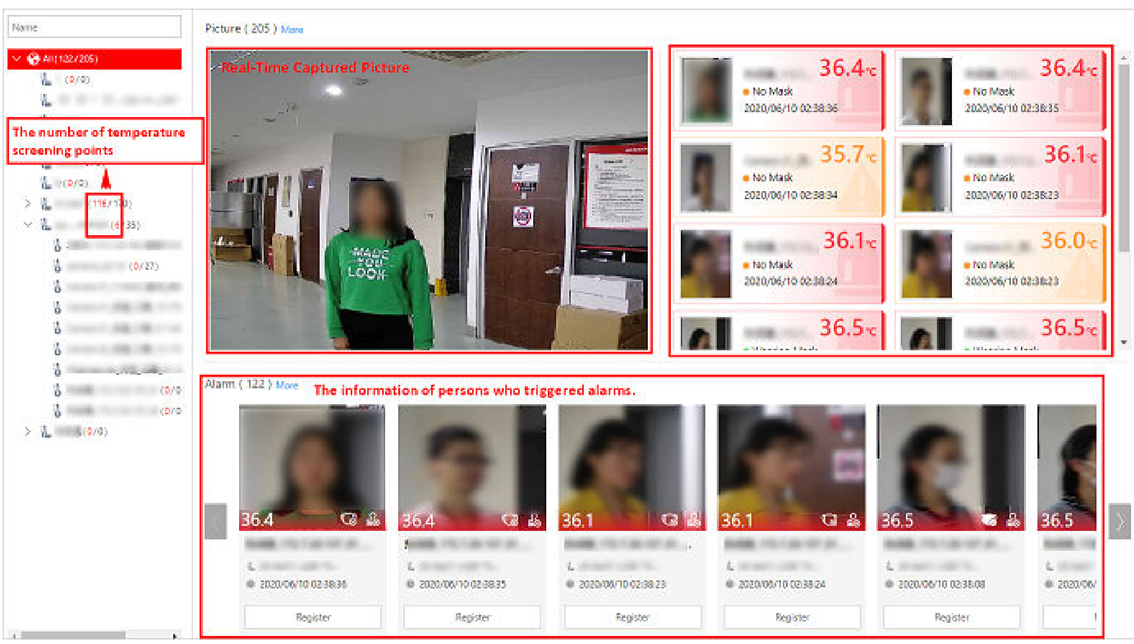


Figure 25-1 Real-Time Skin-Surface Temperature

When a person's skin-surface temperature exceeds the threshold you set, or the person is not wearing a mask, an alarm will be triggered. In the Alarm area, the pictures and information of persons who have triggered alarms are displayed. Following the title Alarm, the alarm amount is displayed. See *The User Manual of HikCentral Professional Web Client* for details about how to set a temperature threshold.

The person information includes skin-surface temperature, wearing mask or not, registered or unregistered, temperature screening point name, temperature screening point group name, and detecting time. You can click **Register** to register for the person, or click **More** to go to the History page to view more alarm information.

25.3 Search History Temperature Screening Data

You can set search conditions such as start time, end time, and skin-surface temperature to search for history temperature screening data.

Before You Start

Make sure temperature screening data has been generated in real-time skin-surface temperature monitoring.

Steps

1. On the top navigation bar, select → **Passing Management → Temperature Screening** .
2. On the left pane, click **History**.
3. Select a temperature screening point group or a temperature screening point from the list.
4. Click to unfold the Filter panel.
5. Set the search condition(s) including start time, end time, skin-surface temperature, etc.
6. Click **Filter**.

   History temperature screening data that meets the search condition(s) will be displayed below.
7. **Optional:** For the searched results, perform the following operations as desired.

View Result Details	You can view the detailed information of the searched results, including temperature screening group, temperature screening point, captured time, person's skin-surface temperature, whether wearing masks, etc. **Note** represents that the person wears a mask, and represents that the person doesn't wear a mask.
Edit/Register Person Information	You can edit or register person information based on the different icons. • : The person is registered. For the registered person, click **Edit** to edit the person information. • : The person is unregistered. For the unregistered person, click **Register** to enter person's registration information. For details, refer to ***Register Person Information*** .
Export	Click **Export** to export temperature screening data including temperature screening point, temperature screening point group, temperature status, etc., in excel file.

25.4 Registration

To manage the people who have been screened skin-surface temperature conveniently, you can register for them by entering their personal information. After registration, you can view and filter the registered persons' information.

25.4.1 Register Person Information

For unregistered persons displayed on real-time skin-surface temperature page or history page of skin-surface temperature, you can register for them.

Steps

1. On the top navigation bar, select ▦ → **Passing Management** → **Temperature Screening** .
2. On the left pane, select **Skin-Surface Temperature** or **History**.

   The skin-surface temperature screening information will be displayed.
3. If a screened person is not registered, you can click **Register** to enter the Register page to register for the person.

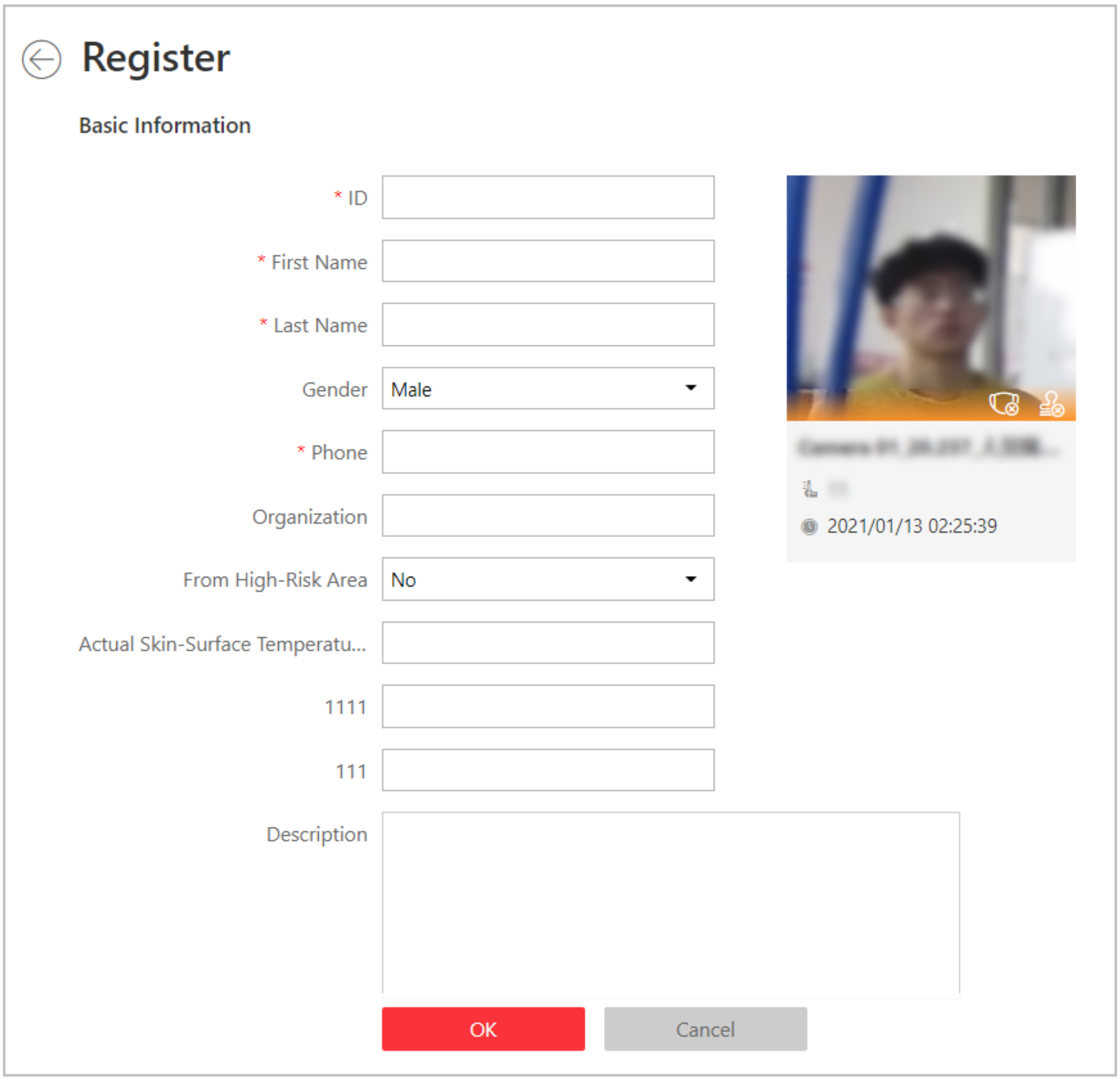


Figure 25-2 Register Page

4. Set personal information, including ID, name, phone number, whether from high-risk areas etc.

Note

You can custom the information displayed on this page according to your needs. See ***Customize Registration Template*** for details.

5. Click **OK** to finish the registration.

   Registered persons' information will be displayed on Registration page for a centralized management. See ***View Registered Person Information*** for details.

25.4.2 Customize Registration Template

You can set customized person information for registration which are not predefined in the system according to your actual needs.

Steps

Note

Up to 5 additional items can be added.

1. On the top navigation bar, select → **Passing Management → Temperature Screening** .
2. On the left pane, click **Registration**.
3. Click **Registration Template** to enter the Registration Template page.
4. Click **Add**.
5. Create a name for the additional item.

   Note

   Up to 32 characters are allowed for the name.
6. Select the format type as general text, number, date or single selection for the additional item.

   Example

   For example, if you select general text, you need to enter words for this item when registering person information.
7. Click **Add**.
8. **Optional:** Perform one or more of the following operations.

Edit Name	Click to edit the name.
Delete	Click to delete the additional item.

25.4.3 View Registered Person Information

For the registered persons, you can view their detailed information including person name, ID, phone, skin-surface temperature, wearing mask or not, etc.

On the top navigation bar, select → **Passing Management → Temperature Screening** . Then on the left pane, click **Registration**.

You can view person name, ID, phone, skin-surface temperature, wearing mask or not, registering time and other information in the list.

Click in the Operation column to edit person information as desired.

Click **Export** on the upper left corner of the page to export and view detailed registered person information in excel file.

25.5 Search for Temperature Screening Records

Skin-surface temperature screening records give you an overview of skin-surface temperature, mask-wearing detection results, and registered person information. Based on the temperature status and mask-wearing detection results, you will quickly learn how many person's skin-surface temperatures are abnormal and how many persons are not wearing masks. With registered person information, you can quickly filter persons with abnormal skin-surface temperature or with no mask on to learn their detailed information such as name, location, face picture, from high-risk area or not, etc.

On the top navigation bar, select → **Passing Management → Temperature Screening** . Then on the left pane, click **Search**.

Select a temperature screening point group or temperature screening point, set the time range at the bottom and click **Generate Report**.

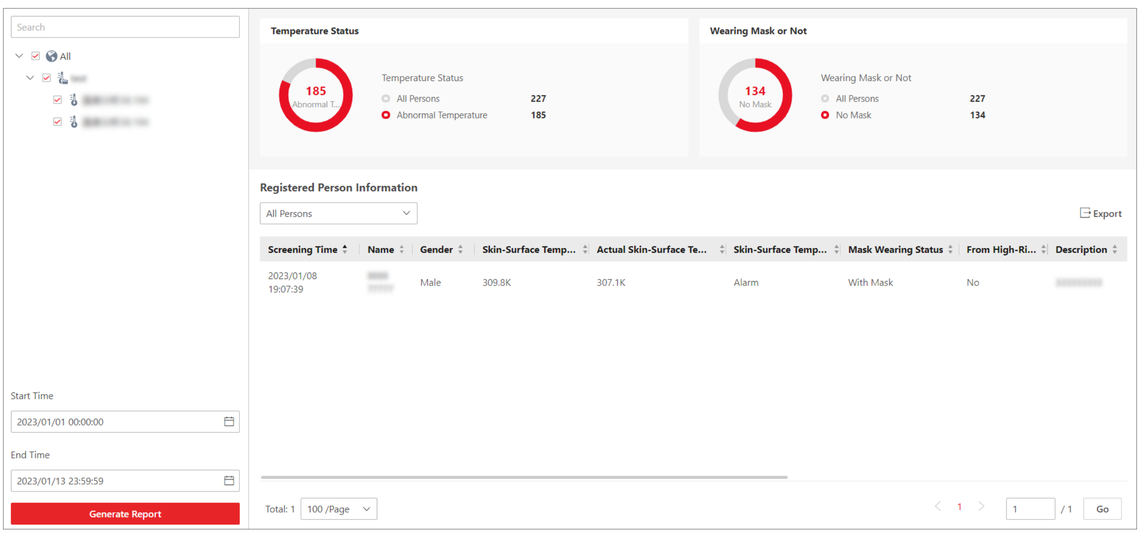


Figure 25-3 Skin-Surface Temperature Screening Records

Temperature Status

Temperature Status gives you the total number of persons whose skin-surface temperatures are screened and the number of persons with abnormal temperature.

Wearing Mask or Not

It gives you the total number of persons whose mask wearing status had been detected, and the number of persons with no mask on.

Registered Person Information

You can filter persons with abnormal skin-surface temperature or those not wearing any mask quickly to view their detailed information. For example, if a person with abnormal skin-surface temperature is not wearing a mask, you need to pay attention to him or her. Based on the temperature screening point name or temperature screening point group name, you can quickly locate the person.

Click to view a person's detailed information including an enlarged face picture, event details, and registered information.

Click **Export** to save the registered person information in your PC as an Excel file.

25.6 Generate Skin-Surface Temperature Analysis Report

You can generate skin-surface temperature analysis reports to view the variation trend of the number of people with abnormal skin-surface temperature over a specified time period.

Before You Start

Make sure you have added device that supports temperature screening and have enabled temperature screening on the device. For details, see the user manual of the device.

Steps

1. On the left navigation bar of the Temperature Screening page, select **Statistics Analysis**.
2. Select a statistics type for the analysis report from **Temperature Screening Point** and **Department**.
3. Select temperature screening point(s) or department(s) for analysis.
   - For selecting temperature screening points:
     a. Click to open the resource list pane.
     b. Select an area in the area list to show the corresponding temperature screening points.
     c. Check the temperature screening point(s) of which the screening results are to be analyzed.
   - For selecting departments:

     Check the department(s) of which the persons' skin-surface temperature screening results are to be analyzed.

   Note

   You can check **Select Sub-Groups** to simultaneously select/deselect the sub department(s) of the department that you have selected/deselected.
4. Select a report type from **Daily Report**, **Weekly Report**, **Monthly Report**, and **Annual Report**, or a report with custom time interval.
5. In the Time field, select a predefined time period or customize a time period accordingly.
6. Click **Generate Report**.

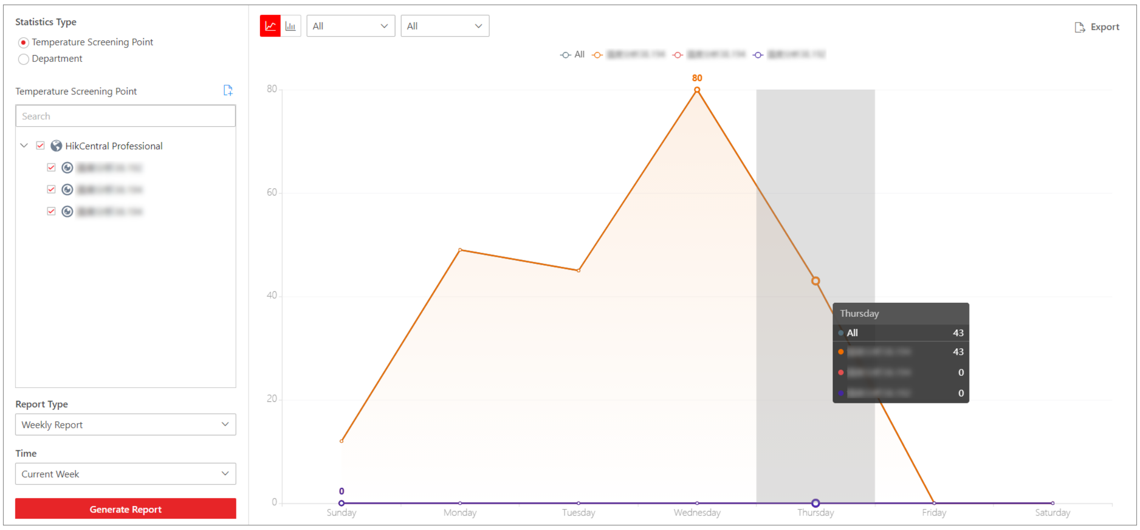


Figure 25-4 Skin-Surface Temperature Analysis Report

The statistics of the selected item(s) will be displayed.

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

Show/Hide Certain Data	Click the legend to show or hide the screening results of the corresponding statistical object, such as certain temperature screening point or certain department.
View Abnormal Temperature or No Mask Statistics	In the top left corner of the chart, select Abnormal Temperature or No Mask from the first drop-down list to display the statistics of people with abnormal temperature or those not wearing any face masks respectively.
Switch Between Line Chart and Histogram	Click / to switch between line chart and histogram.

8. **Optional:** Export the report to the local PC.
   1) On the top right of the page, click **Export**.
   2) Select the dimension (time-related) of the report to be exported.

   Example

   For example, if you are exporting a daily report, you can select from **By Day** and **By Hour**, and you will be able to export 1 or 24 records respectively for each statistical object (i.e., temperature screening point or department).

   Note

   For reports of department(s), you may also choose the export content from **By Department** and **By Person**.

   3) Select the format of the exported file from **Excel**, **CSV**, and **PDF**.
   4) Click **Export**.

25.7 Configure the Scheduled Report of Screening

You can configure scheduled temperature screening analysis reports by specifying a statistical cycle, the analysis type, and the relevant statistical objects (i.e., temperature screening points or departments). Once set, the platform will send an email to the specified recipient(s) regularly with the report attached, which shows the variation trend of the number of people whose skin-surface temperatures are abnormal during the set time period.

Steps

Note

- A report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. On the top navigation bar, select → **Passing Management → Temperature Screening → Basic Configuration → Scheduled Report** .
2. Enter the Create Report page.
   - For configuring scheduled reports for the first time, click **Add** in the middle of the page.
   - If you have configured scheduled reports before, click + at the top of the left pane.

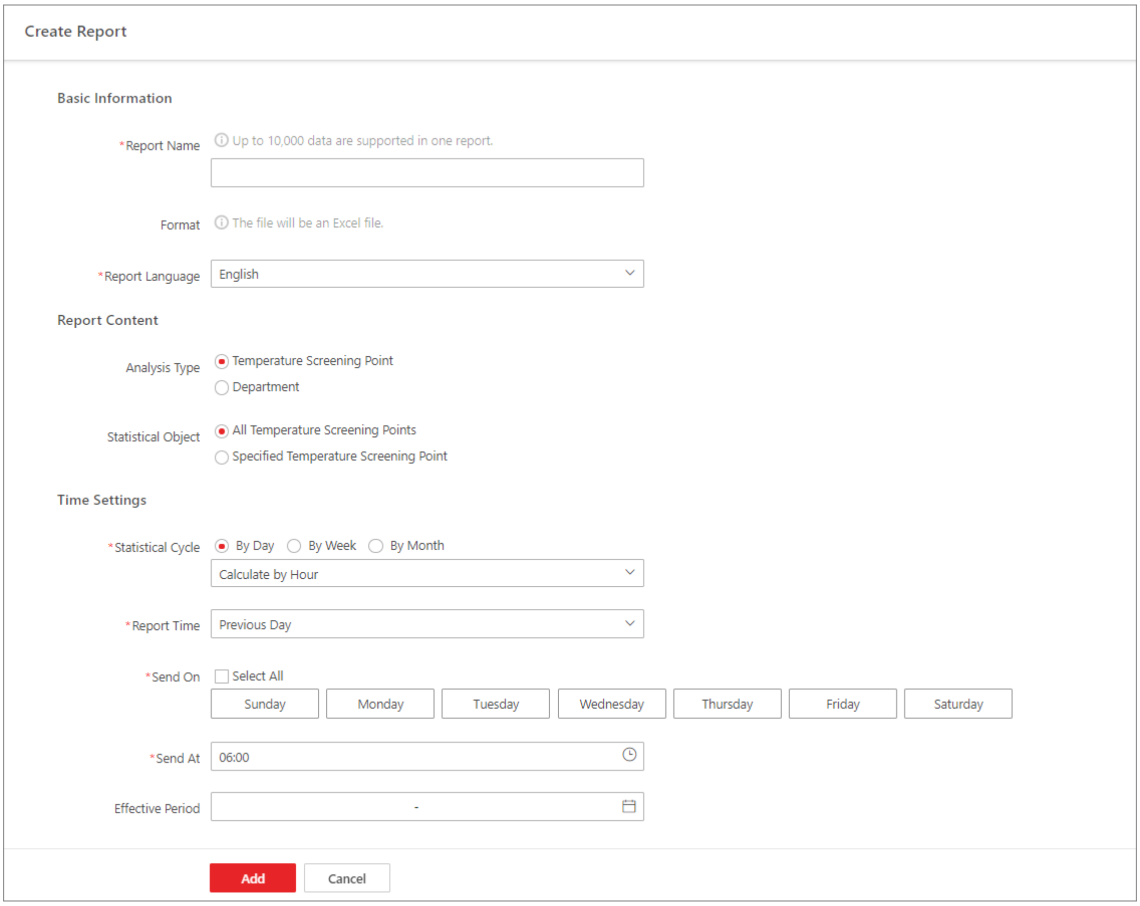


Figure 25-5 Configure Scheduled Report

3. Create a name for the report and select a report language from the drop-down list.
4. Set the report content.
   1) Select an analysis type from **Temperature Screening Point** and **Department**.
   2) Select the statistical objects accordingly. You can select all or specify specific temperature screening points / departments.

Note

If the analysis type is set to **Department**, you may also select the way you would like to export the report content from **By Department** and **By Person**.

5. Select a statistical cycle from **By Day**, **By Week**, and **By Month**, and set the statistical period and report sending time accordingly.

By Day

The daily report shows data on a daily basis. The platform will send one report at the set sending time on the specified day(s) with analysis results of the previous day.

For example, if you set the sending time as 20:00 and select all days of a week, the platform will send a report at 20:00 every day, containing the analysis results of the day before the current day between 00:00 and 24:00.

By Week or By Month

Compared with the daily report, the weekly/monthly report can be less time consuming, since they are not to be generated every day. The platform will send one report on the set day/date at the specified sending time every week/month with analysis results of the last 7/14 days or the current/last month respectively.

For example, for the weekly report, if you set the sending time as 6:00 on Monday and the statistical period as the last 7 days, the platform will send a report at 6:00 every Monday morning, containing the analysis results between last Monday and Sunday.

Note

If the analysis type is set to **Temperature Screening Point**, you may also set how the report will present the analysis results generated in the specified time period below the statistical cycle options. You can choose from **Calculate by Hour** and **Calculate by Day** accordingly.

6. **Optional:** Set an effective period (start time and end time) for the scheduled report.
7. **Optional:** Set the advanced parameters.

Send Report via Email

Select an email template from the drop-down list to define the recipient information and email format (subject and content), so that the report can be sent to the recipient(s) regularly via email.

Note

- You can select an existing email template or click **Add** to add a new one.

Upload to SFTP

Configure SFTP settings including the SFTP address, port No., user name, password, and the saving path for the report to be uploaded to the SFTP server regularly.

Note

You can also click → **SFTP Settings** at the top of the left pane to configure the corresponding parameters.

Save to Local Storage

Configure a saving path for the report to be saved to the local storage regularly.

Note

You can also click → **Configure Local Storage** at the top of the left pane to configure the saving path.

8. Click **Add** to finish setting the scheduled report rule.

Chapter 26 Video Intercom Management

Video intercom is an audiovisual communication and security technique used in a building or a small collection of buildings. With microphones and cameras at both sides, it enables the intercommunication via video and audio signals and provides a safe and easy monitoring solution for apartment buildings and private houses.

On the Web Client, you can add video intercom devices to the system, group resources (e.g., doors and cameras) into different areas, configure call schedules, link resources (cameras, persons, and doorbells) with indoor station, manage notices, call indoor stations, and view recents. After settings related parameters, the person can view the live video of the camera, call indoor station, answer call via Control Client, etc.

In the top left corner of Home page, select → **Passing Management → Video Intercom** .

26.1 Flow Chart of Video Intercom

For the first time, you can follow the flow chart to perform configurations and operations.

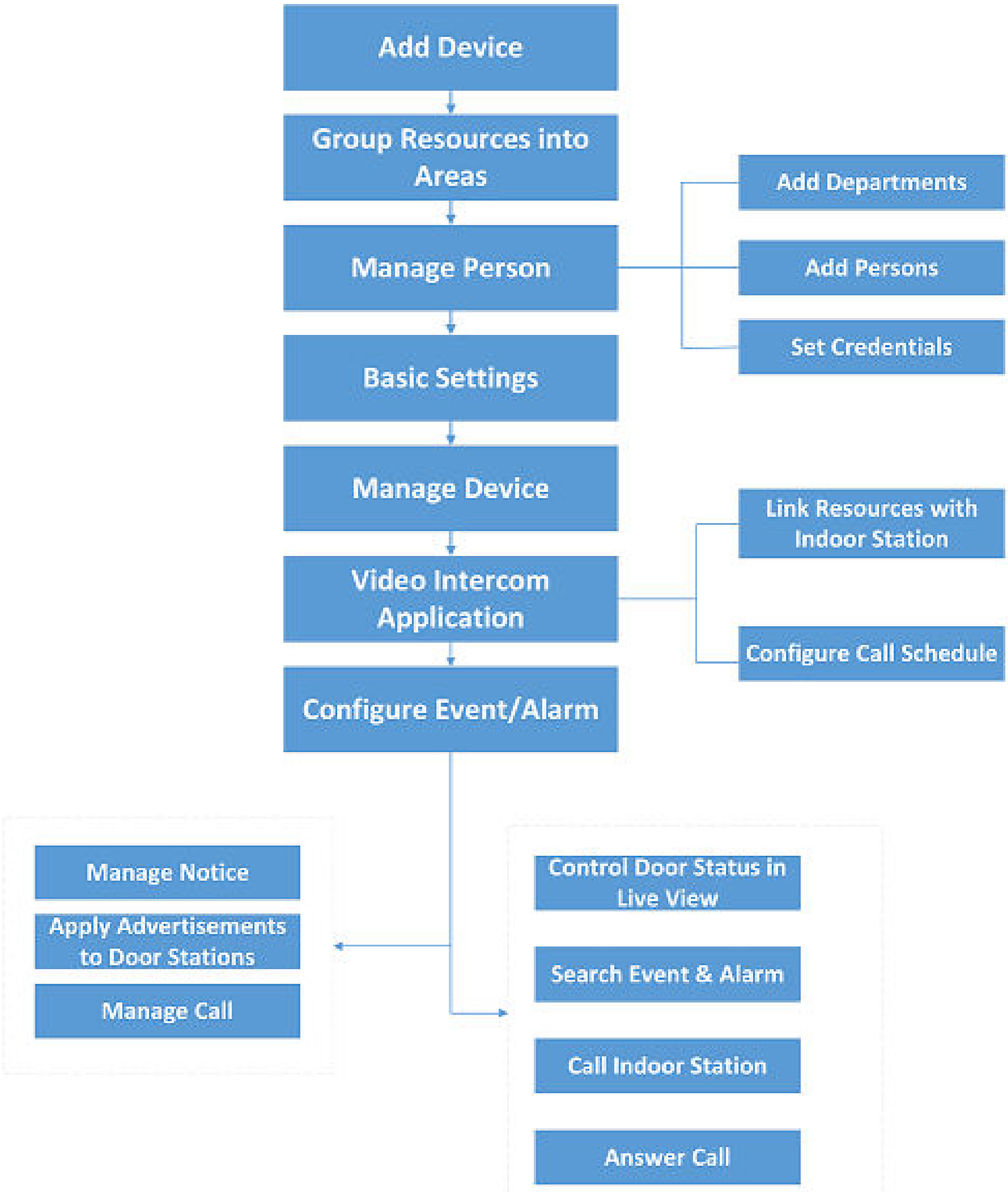


Figure 26-1 Flow Chart of Video Intercom

- **Add Device**: Add video intercom devices (such as main station, outer door station, indoor station, and door station) to HikCentral Professional and configure device parameters remotely. For more details, refer to ***Manage Video Intercom Device*** and ***Configure Device Parameters*** .
- **Group Resources into Areas**: After adding the devices to the system, you need to group the devices' resources (such as doors) into different areas according to the resources' locations. For details, refer to ***Area Management*** .

- **Manage Person**: Add departments and persons to the system, and set credential information.
- **Basic Settings**: Add call recipients, add call schedule templates, add receiving schedule template, and configure call parameters.
- **Manage Device**: Set location information for video intercom devices and apply the settings to devices.
- **Video Intercom Application**: Add call schedules and apply them to devices, link resources (camera, person, and doorbell) to indoor stations.
- **Configure Event / Alarm**: Configure event and alarm for video intercom resources.
- **Manage Notice**: Add notices and apply them to indoor stations.
- **Apply Advertisements to Door Stations**: Apply pictures or video to door stations as advertisements.
- **Manage Call**: Call indoor stations and view recents.
- **Operations on Control Client**: After the above configurations on the Web Client, you can control door status during live view, search event and alarm, call indoor station and answer call. For more details, refer to *User Manual of HikCentral Professional Control Client*.

Note

The doors of video intercom device can be used similarly as the doors of access control device.

26.2 Add Video Intercom Device

Device Management

1. Select **Device Management** on the left.
2. Select **Add** to set the basic information and location information.
3. Select **Apply Settings**, select devices and the applying mode, and select **Apply** to apply the location information to devices.

26.3 Configure Device Parameters

After adding the video intercom devices, you can configure parameters for them remotely, including device time, maintenance settings, etc.

After adding a video intercom device, click in the **Operation** column to configure the device.

Note

The parameters may vary with different models of devices.

Time

You can view the time zone where the device locates and set the following parameters.

Device Time

Click **Device Time** field to customize time for the device.

Sync with Server Time

Synchronize the device time with that of the SYS server of the system.

Call Management Center

For door station, you can set this function switch to on and select a shortcut button. When the configured button on the device is pressed, it will call management center. The default button is 1.

Note

This should be supported by the device.

Card Swiping

For outer door station and door station which supports M1 encryption, you can enable **M1 Encryption** and select the sector. Only the card with the same encrypted sector can be granted by swiping the card on the card reader.

Related Cameras

For indoor station, you can relate the camera(s) with it to view the video of the related camera(s) on the indoor station. You can also delete the related camera(s). Up to 16 related cameras are supported.

Maintenance

You can reboot a device remotely, and restore it to its default settings.

Reboot

Reboot the device.

Restore Default

Restore the device to its default settings. The device should be activated after restoring.

More

For more configurations, you can click **Configure** to go to Remote Configuration page of the device.

26.4 Add a Call Schedule for a Door Station

You can add a call schedule for a door station to configure when door stations can call indoor stations or management centers.

Steps

1. On the top navigation bar, select **Video Intercom Application → Door Station Call Schedule Settings** .
2. Select **Add** to add a door station call schedule.
3. Select a door station in the list.

4. Add a call schedule template. Click **Add Call Schedule Template** to set the template name, weekly schedule template, and holiday schedule, and select a room number for each button.
   1) Select **Add Call Schedule Template**.
   2) Set the template name.
   3) Select an existing template from the **Copy from** the drop-down list.
   4) Select **Indoor Station** if there is someone indoor who can answer the call from the door station and select **Management Center** if there is no one who can answer the call.
   5) Configure the weekly schedule.

Operations	How To
Draw Task Time	Click a grid or drag the cursor on the time line to draw a time period during which the task is activated.
Set Precise Time	Move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as  .

   6) **Optional:** Select **Add Holiday** to select an existing holiday template, or select **Add** to add a new template.

Note

If you configure a template for a management center, the Room cannot be selected.

5. Click **Add** to save the schedule.
6. Select **Apply Settings** to apply call schedules to devices.
7. **Optional:** To add call templates to devices in a batch, select **Batch Import Call Schedule → Download Template** , fill in the template, upload the template, and select **Import**.

26.5 Apply Advertisements to Door Stations

You can add pictures or videos in the advertisements, then apply the advertisements to door stations. After applying advertisements, you can filter or delete them. This function is only supported by this model: DS-KD9403-E6.

Steps

1. Select **Video Intercom → Apply Advertisements to Door Stations** .
2. Click **Apply Advertisements to Door Stations** on the top.
3. Select the available door station in the left list and click › to add it to the right list.
4. Add picture(s) or a video for an advertisement to be applied to door stations.

Note

For the picture advertisement, you can add up to six pictures. For the video advertisement, you can add up to three videos.

- a. Click **Picture** → + to add picture(s) for an advertisement.
  b. Set the **Picture Switching Interval**.
  c. Set the time period to play the added picture(s).

  Note

  Click **Add** to add the time period if needed.
- a. Click **Video** → + to add a video for an advertisement.
  b. Set the time period to play the added video.

  Note

  Click **Add** to add the time period if needed.

5. The playing schedules set for the picture(s) and the video in the advertisement will be displayed by different color blocks.
6. Click **Apply**.

26.6 Link Resources with Indoor Stations

After adding an indoor station to the plaform, you can relate cameras with the added indoor station to view video of the related camera(s) by the indoor station. You can also link persons with an indoor station. You can also relate a doorbell with an indoor station. When the Call Management Center function of this doorbell is disabled, you can call the related indoor station by the doorbell.

26.6.1 Link Doorbell to Indoor Station

Steps

1. On the left pane, select **Video Intercom Application → Link Doorbell to Indoor Station** .
2. Select **Link** to enter the Link Doorbell with Indoor Station page.
3. From the drop-down list of **Device Name**, select a location. And then select the doorbell to be linked to the indoor station.
4. In the indoor station list, select the corresponding indoor station that the doorbell is to be linked to and click **Add**.

Note

The location information of the indoor station is the same as that of the doorbell.

26.6.2 Link Cameras to an Indoor Station

After adding indoor stations to the system, you can link cameras to indoor stations to view videos of the linked cameras on the indoor station. You can link up to 16 cameras to an indoor station.

Before You Start

Make sure the cameras to be linked are correctly installed and are added to the system by Hikvision Private Protocol/ONVIF.

Steps

1. In the top left corner of the Home page, select **Video Intercom Application → Link Camera to Indoor Station** .
2. Select **Link**.

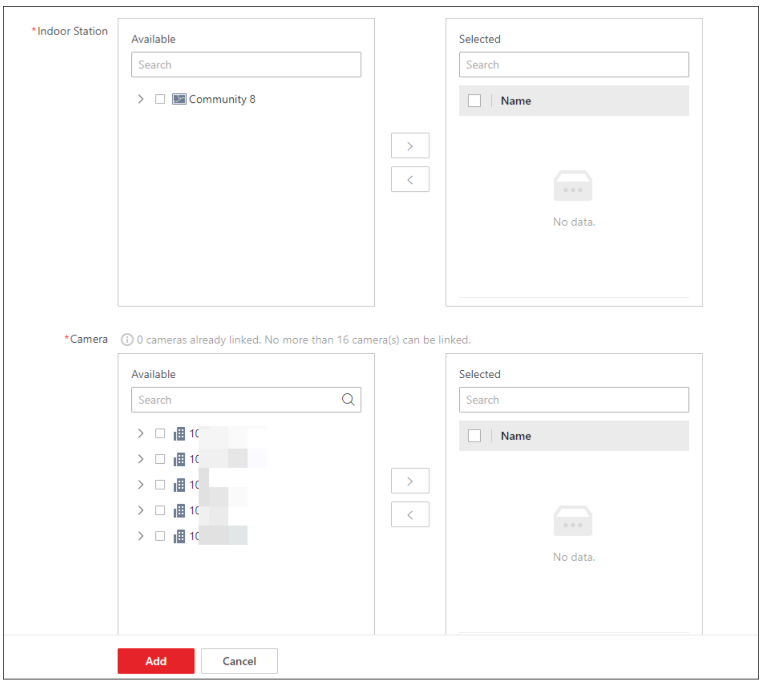


Figure 26-2 Add Linked Camera

Note

You can also link camera to indoor station in the configuration page of the indoor station. For details, refer to ***Configure Device Parameters*** .

3. In the Indoor Station list, select an indoor station.
4. In the Camera list, check one or more cameras.
5. Select **Add**.
6. Select **Apply Settings** to apply the settings to devices.

26.6.3 Link Persons to Indoor Station

Steps

1. Select **Video Intercom Application → Link Person to Indoor Station** on the left.
2. Click **Link**.

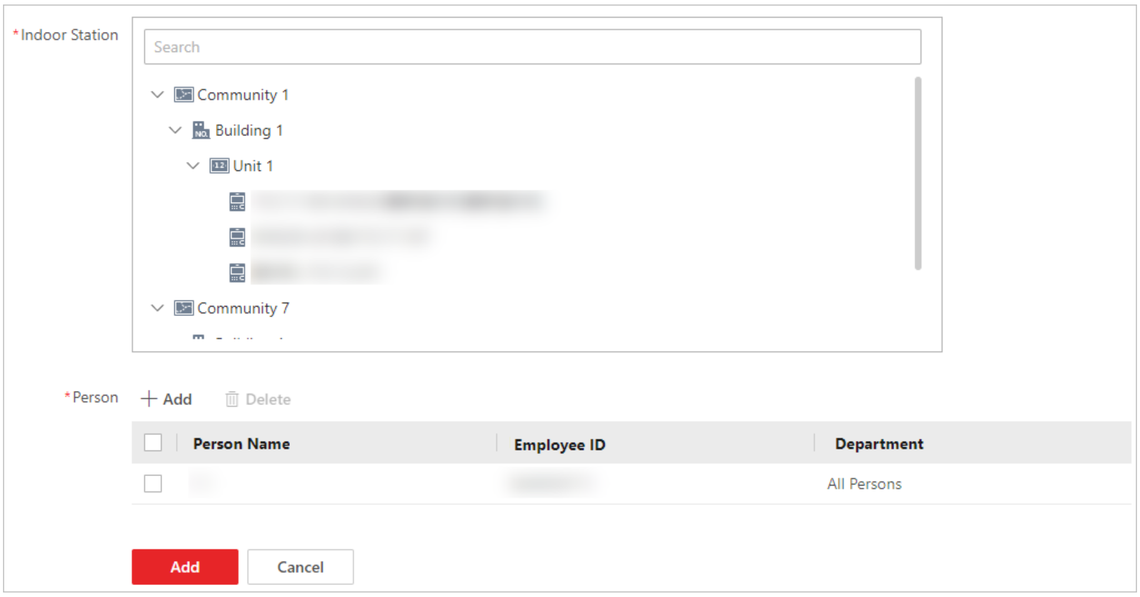


Figure 26-3 Add Linked Person

3. Select an indoor station.

Note

Up to 10 persons can be linked to an indoor station and the person cannot be linked to multiple indoor stations.

4. Click **Add** to select persons to be linked to the indoor station.
5. Click **Add**.

26.7 Apply Data to Indoor Station

You can apply notices to an indoor station to alert people in emergencies or install a software on indoor stations to expand their functions. After applying a software package to the indoor stations, the software will be installed automatically.

26.7.1 Add and Apply a Notice

There are four types of notice, including advertisement, property information, alarm, and notification. They are used for sending information to residents. You can add and apply notices to indoor stations. For example, when an emergency occur, you can add and apply a notice to indoor stations to inform residents for timely actions. After adding and applying notices, you can delete, filter, and export them. You can also copy a notice and apply it to indoor stations conveniently.

1. On the left pane, select **Apply Data to Indoor Station → Manage Notice** .
2. Select the **Apply Notice** tab, and select **Add** to add a notice.
3. Configure the notice.
   a. Create a title of the notice and set the notice type.
   b. Select + to add pictures.

   Note

   Up to 6 JPG pictures can be added, and each picture should be no larger than 512 KB.

   c. Enter the content of the notice.
   d. Select indoor stations to receive the notice.
4. Select **Preview** to preview the notice.
5. Select **Apply** to apply the notice to indoor stations.
6. (Optional) Select the **Apply Notice** tab.
   - Select one or more notices, and select **Copy and Apply** to apply notices to indoor stations.
   - If you want to edit the notice content, select to copy the current notice and edit the notice as needed. Select **Apply** to apply the notice to indoor stations.

26.7.2 Apply Software Package to Indoor Station

This function is only supported by certain models.

Steps

1. In the left pane of the Home page, select **Apply Data to Indoor Station → Apply Software Package** .
2. Click **Apply Software Package**.
3. Select **All Indoor Stations** or **Specified Indoor Station(s)**.

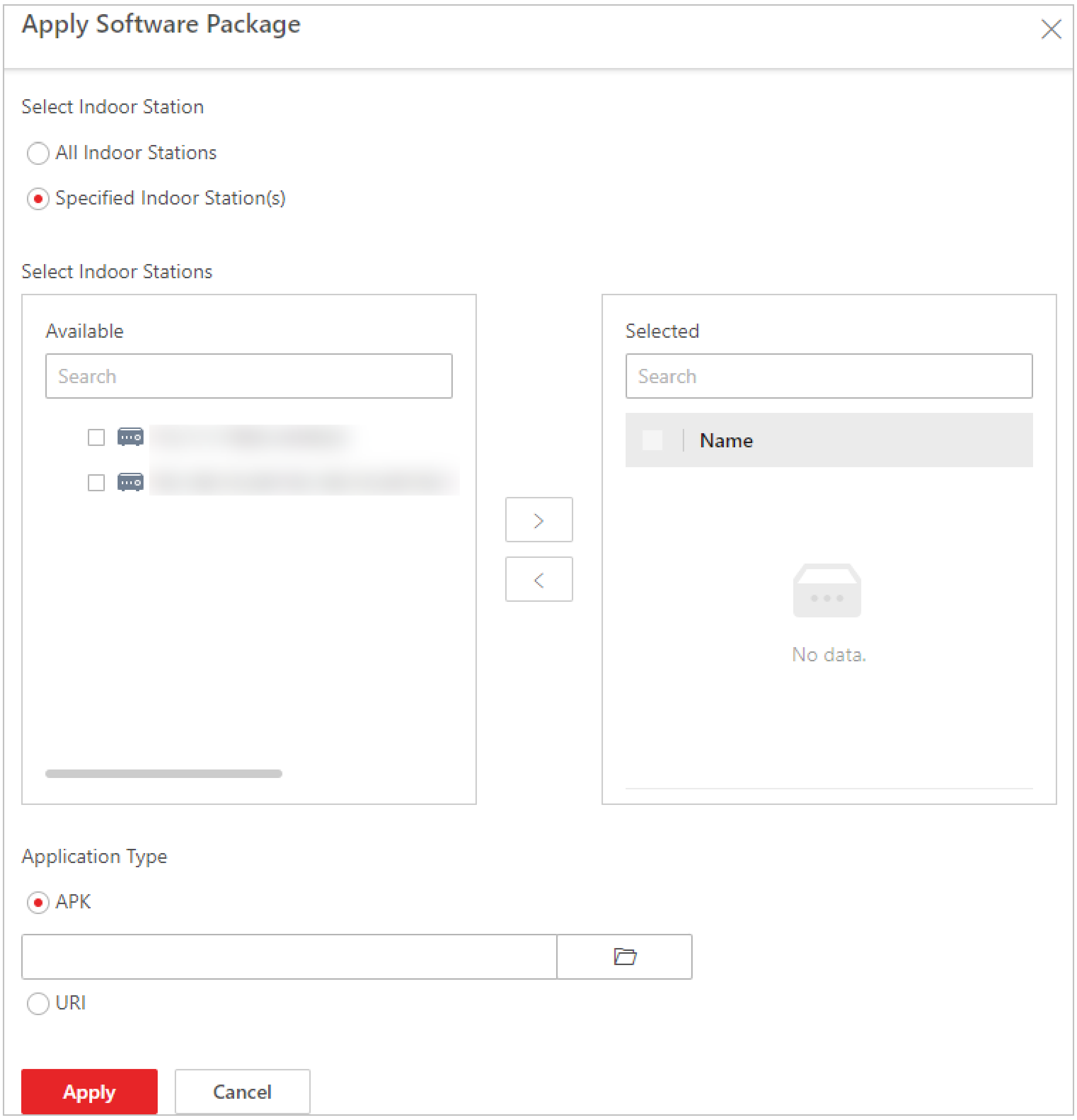


Figure 26-4 Apply Software Package

4. Select an application type.
5. Select **Apply**.

26.8 Make and Receive Calls on Platform

You can configure a receiving schedule template to define when the platform user can receive calls. After configuring receiving schedule templates, you can adding platform users as call recipients. When someone calls the platform, the added recipients can receive and answer the call. In case of door station call failure or emergencies, you can also directly call indoor stations from the platform.

26.8.1 Add Receiving Schedule Template

Steps

1. On the top navigation bar, select **Basic Configuration → Schedule Template → Receiving Schedule Template** .
2. Select + to add a schedule template.

   You cannot edit or delete The two default templates, namely All-Day Call Schedule Template for Indoor Station and All-Day Call Schedule Template for Call Center.
3. Configure the template.
   1) Create a name for the template.
   2) **Optional:** Select an existing template from the **Copy from** drop-down list.
   3) Select **Indoor Station** if there is someone indoor who can answer the call from the door station and select **Management Center** if there is no one who can answer the call.
   4) Set the weekly schedule.

Operations	Description
Set Task Time	Click a grid or drag the cursor on the time line to draw a time period during which the task is activated.
Set Precise Time	Move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as  .

   5) **Optional:** Select **Add Holiday** to select an existing holiday template, or click **Add** to add a new template.
4. Select **Add** to save the template.

26.8.2 Add Call Recipients

Steps

1. In the top left corner of Home page, select **Basic Configuration → Call Recipient** .
2. Select **Add**, select users to receive calls, set device for receiving calls from, and select a receiving schedule template.
3. Select **Add**.

Answer Call

If someone calls the platform, the added recipients can receive and answer the call.

Steps

1. Select **Basic Configuration → General** to set the following parameters: **Ringtone**, **Max. Speaking Duration with Door Stations**, and **Max. Speaking Duration with Access Control Devices**.
2. Answer the incoming call. For details, see the following picture.

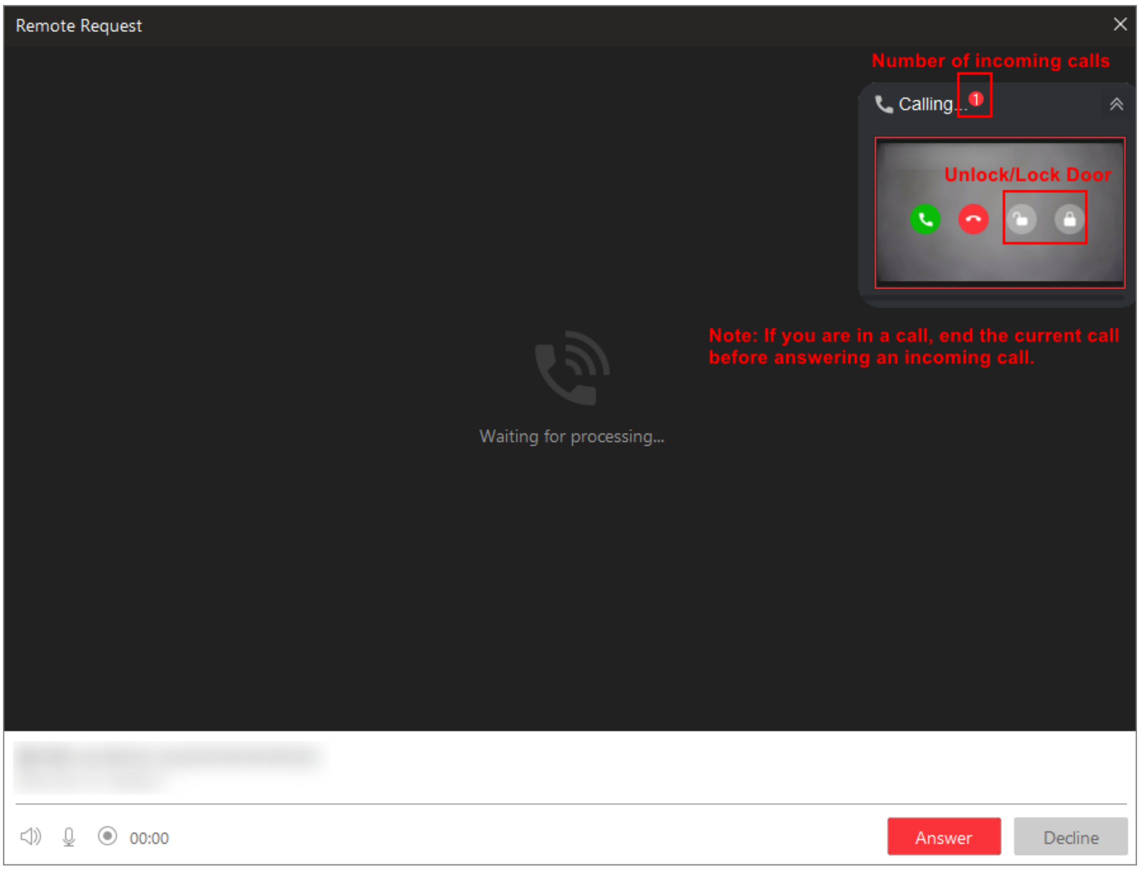


Figure 26-5 Answer Call

26.8.3 Call Indoor Stations

Steps

1. Select **Video Intercom → Contacts** .
2. Configure the following call parameters.

   Go to **Basic Configuration → General → Call Parameter** to set the following parameters.

Parameter	Description
Auto Hang Up After	The call will be hung up automatically after the duration.
Max. Speaking Duration with Indoor Stations	Enter the maximum duration during which you can speak with the device.

3. Select an indoor station and select to make a call.
4. **Optional:** Select **Recents** to view call logs, select **Export** to export call logs to Excel/CSV file format, and select to download the recorded audio in MP4 format to the local PC.

26.9 Configure General Parameters

You can configure general parameters, including the storage location of configuration data and records.

On the top navigation bar, select **Basic Configuration → General** .

Configure the following parameters as needed, then click **Save** to save settings.

Storage of Configuration Data

You can store the configuration data of video intercom.

Select **Local Storage** or **pStor** from the drop-down list to store the records on the local PC or on the pStor server. After that, you can view and select the corresponding resource pool.

Storage of Records

You can store the records generated in the operation of video intercom, such as the records of linking the video or audio files to call logs.

Select **Local Storage** or **pStor** from the drop-down list to store the records on the local PC or on the pStor server. After that, you can view and select the corresponding resource pool.

Note

- For **Local Storage**, make sure you have enabled local storage and added the local resource pool.
- For **pStor**, make sure you have added pStor as the recording server.

Chapter 27 On-Board Monitoring

The On-Board Monitoring module is for users to monitor driving vehicles, including locating vehicles to get their real-time GPS information and driving speed, talking to drivers via two-way audio, playing videos streamed from vehicle-mounted cameras, playing back the tracks vehicles have traveled along, and record search. You can configure driving rules to assist you to monitor vehicles by regulating the areas where vehicles are allowed or not allowed to drive and the routes that vehicles are required to drive along.

27.1 On-Board Monitoring Overview

The Overview page displays the major steps of On-Board Monitoring configuration and presents statistics reports by different contents and device health check reports.

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **On-Board Monitoring Overview** .

Wizard

On the top of the overview page, you can view the brief introduction of the On-Board Monitoring function and the major steps of configuration, including device management, vehicle monitoring configuration, event and alarm configuration, and driving monitoring. Hover the cursor over each step and click to go to the corresponding page.

Report

Click the **Report** tab.
You can have an overview of on-board monitoring data in the last 7 days on one page, including the GPS information, driving distance, driving duration, overspeed times, and driving events. See ***Statistics and Reports*** for how to view more details and reports.

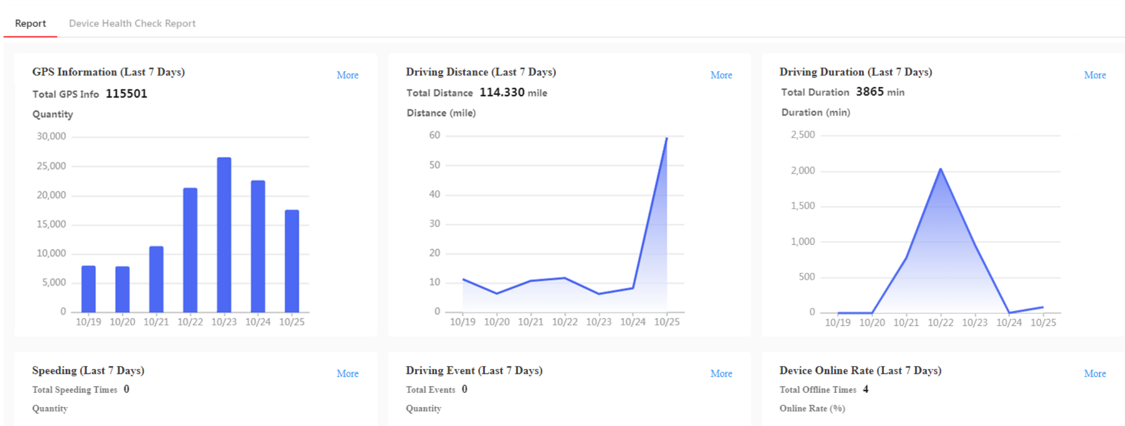


Figure 27-1 Statistics Overview

You can perform the following operations on the page.

- **View One Day's Data**
  Hover the cursor onto a chart to view the data of a specific day.

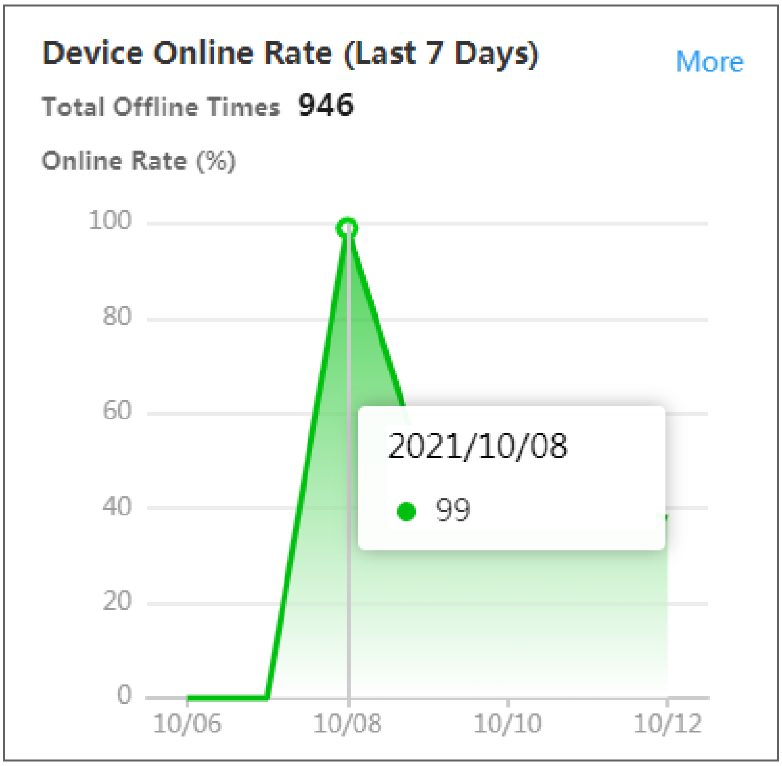


Figure 27-2 Example

- **Jump to the Report Generation Page**
  If you need to view the data in other periods, click **More** in the upper-right corner of a chart. For example, you can click **More** in the Driving Distance chart area to jump to the page as shown in the figure below and be ready for generating driving distance reports according to the conditions you set.

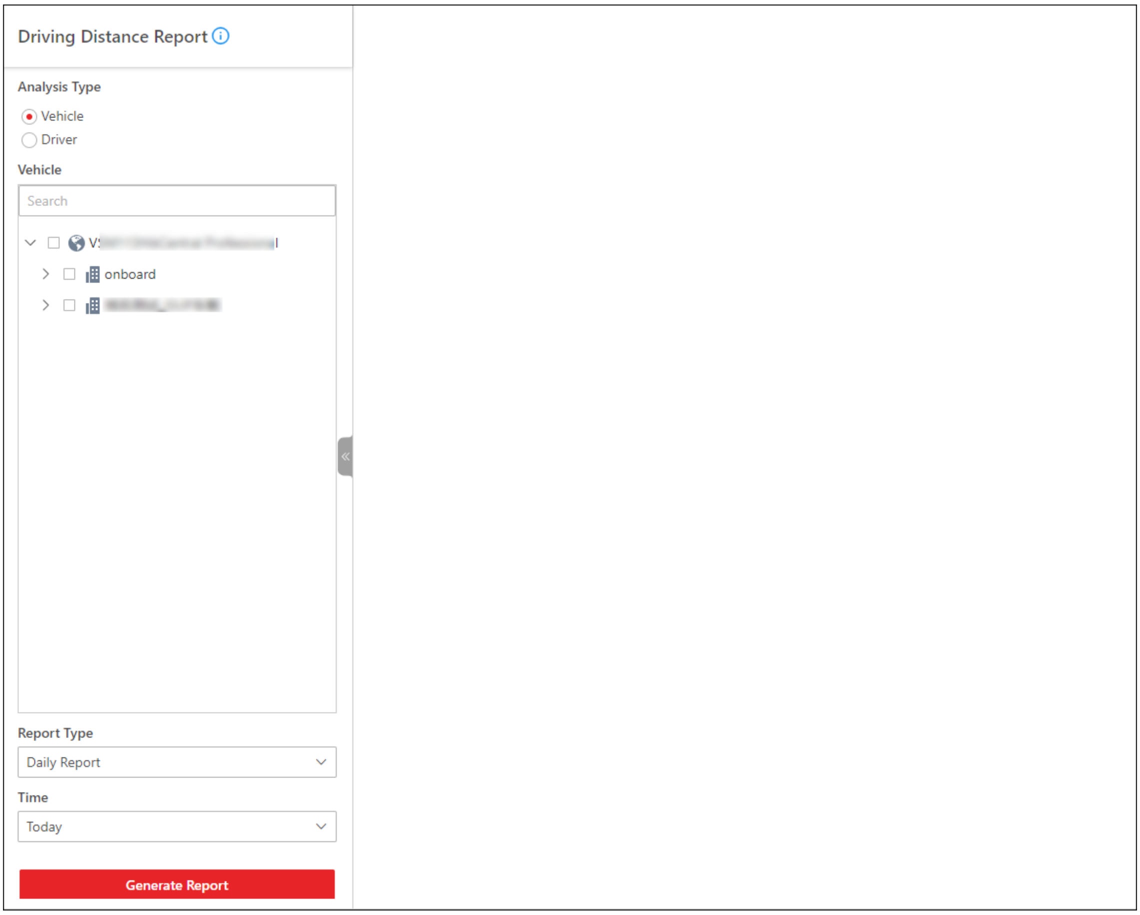


Figure 27-3 Generate Report

Device Health Check Report

Click the **Device Health Check Report** tab.

You can view the device health check by different vehicles.

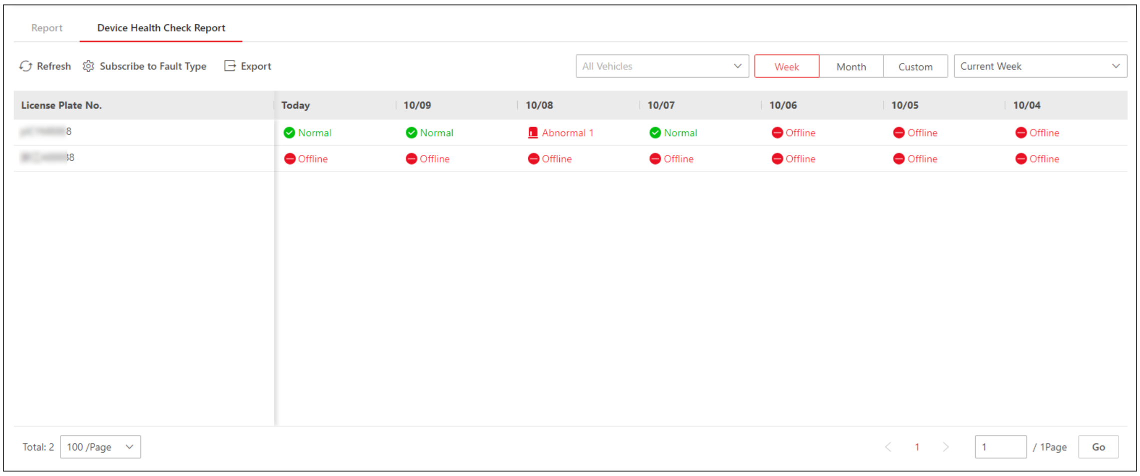


Figure 27-4 Device Health Check Report

Perform the following operations as needed.

Specify Vehicle	Click **All Vehicles** and select vehicles from the drop-down list to be displayed.
View Health Check of A Specific Device	Click the status of a device on a specific date to view the health check details on the right. In the panel of health check details, you can click **All Fault Types** and select a fault type from the drop-down list to filter the fault(s) displayed.
Select Time Range	Click **Week** or **Month**, and select a specific week or month; click **Custom**, and customize the time range as needed.
Refresh Health Check	Click **Refresh** to refresh the health check for devices.
Subscribe to Fault Type	Click **Subscribe to Fault Type**, and check fault type(s) as needed.
Export	Click **Export** to open the Export Report panel, check contents to be exported as needed, and click **Save** to export the report.

27.2 Flow Chart of On-Board Monitoring

The flow chart introduces the process of on-board monitoring configuration.

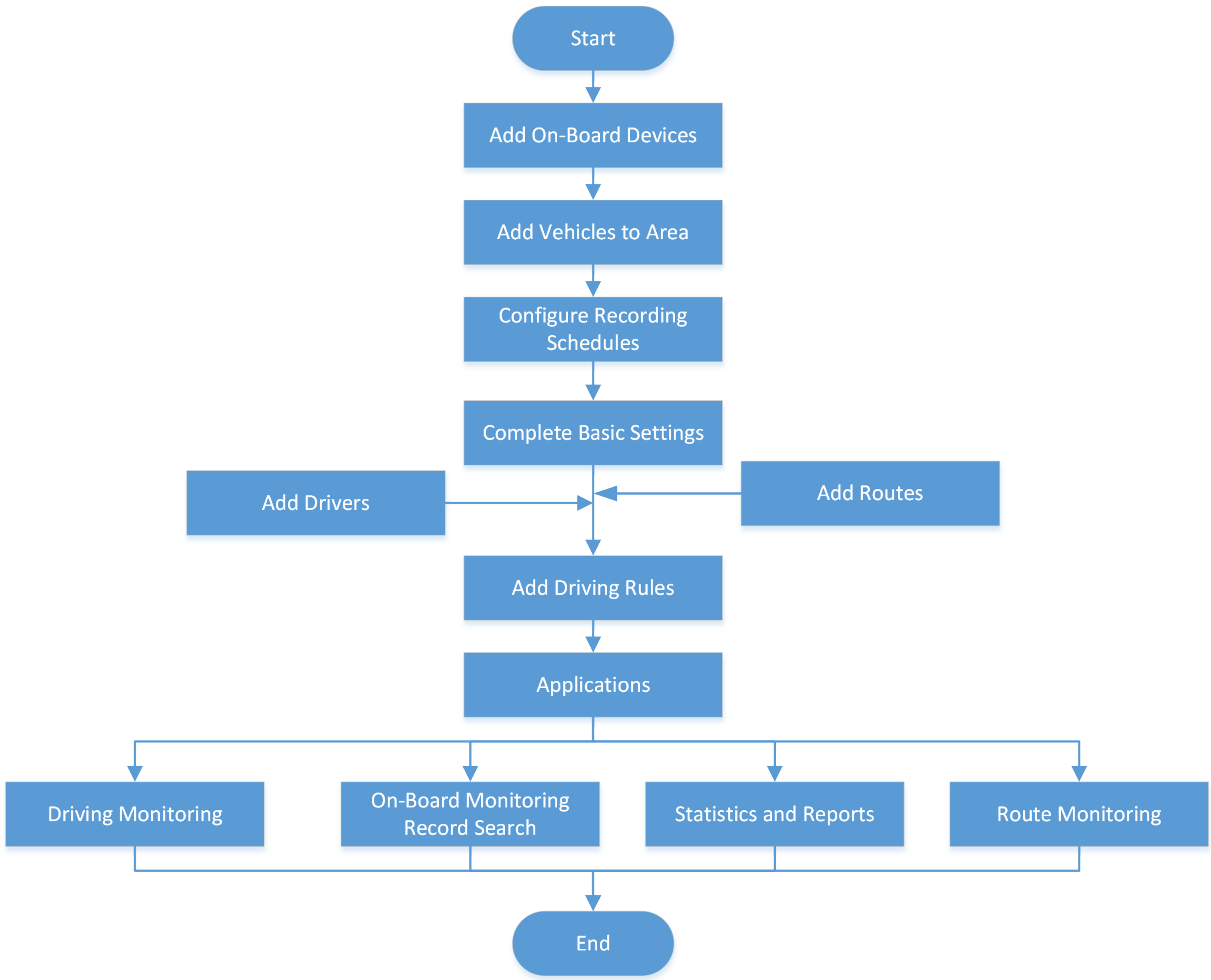


Figure 27-5 Flow Chart of On-Board Monitoring Configuration

27.3 Basic Settings

To ensure the smooth operations of on-board monitoring, you need to configure the basic parameters, route parameters, fuel level monitoring parameters, and scheduled reports in advance.

27.3.1 Configure Basic Parameters

You can configure the basic parameters including the distance unit, GIS map, and retention period of GPS data.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Basic Configuration → Basic Parameters** .

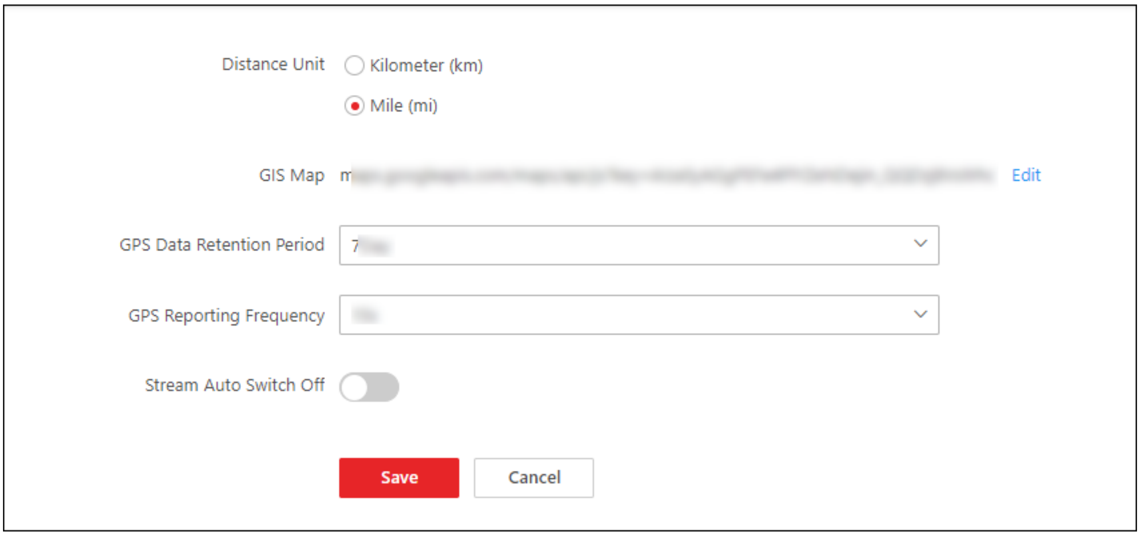


Figure 27-6 Basic Parameter Configuration

2. Select a distance unit.
3. Click **Edit** to edit the GIS map.

   Note

   If you have not configured a GIS map, you should click **Configure GIS Map** to configure an online or offline GIS map first.
4. Select the retention period of GPS data.

   Note

   GPS data can be retained for one year at most.
5. Set the frequency at which the GPS information is reported to the platform.
6. **Optional:** Switch on **Stream Auto Switch Off** and set a duration.

   Note

   If a user has enabled live view or playback but does not perform any operation during the set duration, the platform will automatically stop streaming cameras to save network traffic.

27.3.2 Configure Route Parameters

By configuring route parameters, you can change the rules for deciding a late departure or arrival, and you can customize the causes of unpunctual departure/arrival to select on the Route Monitoring page.

On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Basic Configuration → Route Parameters** , configure the parameters as needed, and click **Save**.

Flexible Duration for Departure

If the time difference between the actual departure time and scheduled departure time is less than this flexible duration you set, the departure will not be determined as an unpunctual departure.

Flexible Duration for Arrival

If the time difference between the actual arrival time and scheduled arrival time is less than this flexible duration you set, the arrival will not be determined as an unpunctual arrival.

Cause of Unpunctual Departure/Arrival

You can customize the causes of unpunctual departures or arrivals for vehicles according to your needs. When an unpunctual departure or arrival happens, you can select a cause on the Route Monitoring page.

27.3.3 Configure Fuel Level Monitoring Parameters

You can configure parameters for fuel level monitoring, including fuel quantity unit, fuel tank model, and fuel tolerance in tank.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Basic Configuration → Fuel Level Monitoring Parameters** .
2. Enable **Fuel Level Monitoring Parameters**.

   Note

   When it is disabled, the functions of searching for fuel level monitoring records and generating fuel consumption statistics reports are unavailable.
3. Enable **Fuel Consumption Monitoring**.

   Note

   It is disabled by default; when it is enabled, the fuel consumption per 100 km will be displayed and reported in **Driver Analytics**.
4. Select the **Fuel Quantity Unit** for fuel consumption calculation.
5. Add a fuel tank model.
   1) Click **Add**.
   2) Enter the fuel tank name, capacity, fuel height, and threshold of fuel consumption.

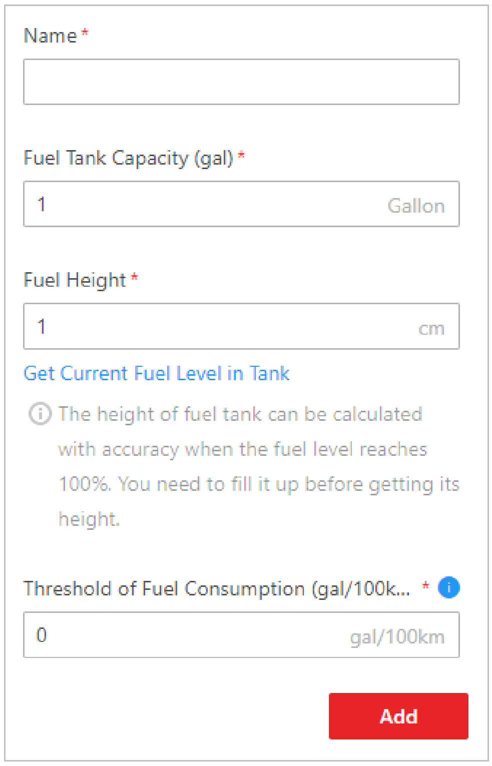


Figure 27-7 Window of Adding Fuel Tank Model

Threshold of Fuel Consumption

When the actual fuel consumption each 100 km exceeds the configured value, the Abnormal Fuel Consumption per 100 Kilometers event will be triggered.

3) **Optional:** Click **Get Current Fuel Level In Tank**, and then select a vehicle to get the current fuel level of the vehicle's tank.

4) Click **Add**.

6. Enter the **Fuel Tolerance in Tank**.
7. Click **Save**.

27.3.4 Configure Scheduled Reports

You can set parameters for sending scheduled reports including driver analysis reports, fuel level analysis reports, and stop traffic analysis reports.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Basic Configuration** → **Scheduled Report** .

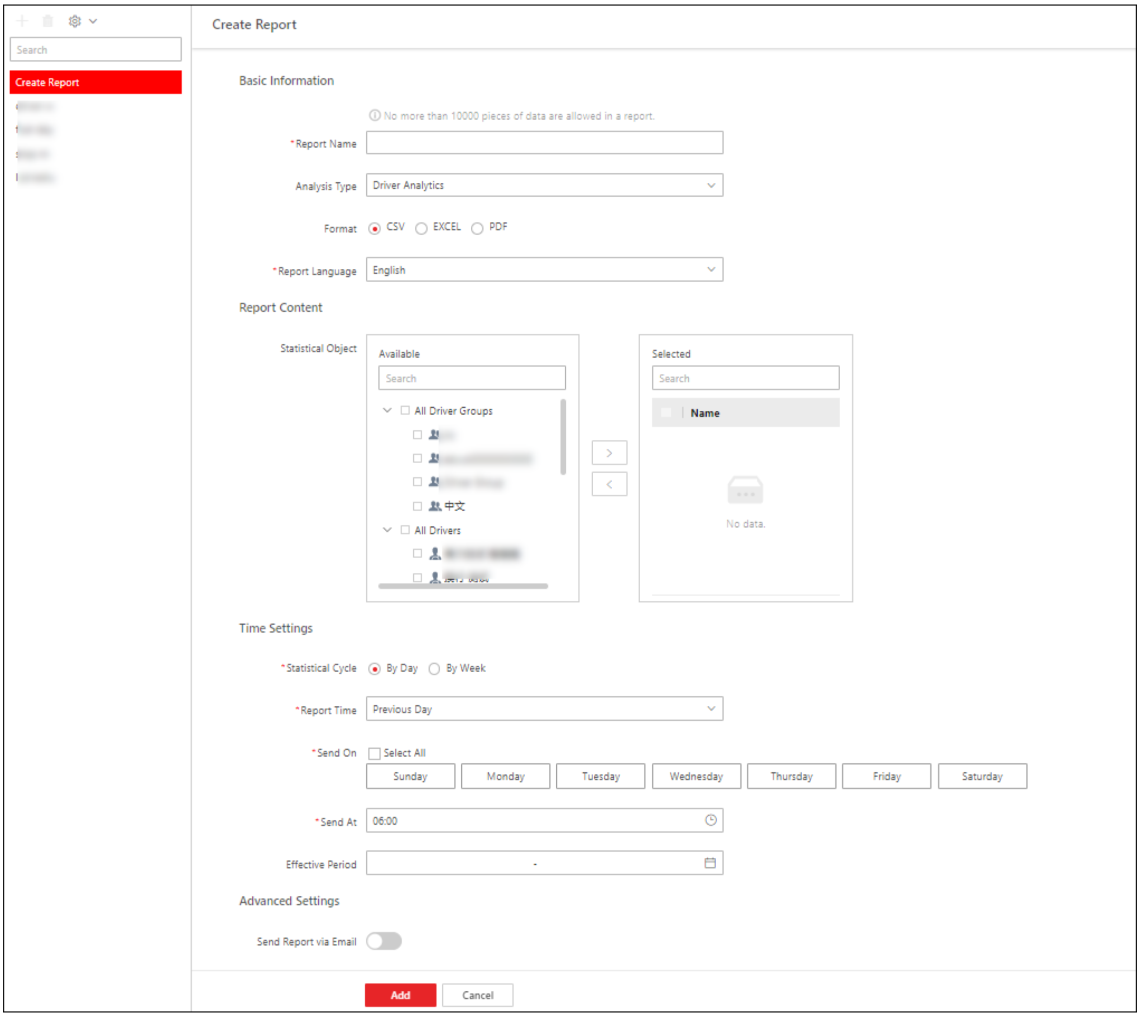


Figure 27-8 Create Report Page

2. Click + to enter the Create Report page, or click a report to enter the report's page.
3. Set the basic information, including the report name, analysis type, report format, and report language.
4. Select the contents to be included in the report.

Note

The report contents change according to the analysis type.

5. Complete the time settings.
   1) Select a statistical cycle.

   By Day

   The report shows data on a daily basis. The platform will send one report every day. The report contains data recorded on the day prior to the current day.

For example, if you set the sending time to 20:00, the system will send a report at 20:00, containing data between 00:00 and 24:00 prior to the current day.

By Week

The platform will send one report every week. The report contains data of the recent one/two weeks.

For example, for weekly report, if you set the sending time to 6:00 on Monday, the platform will send a report at 6:00 a.m. every Monday, containing data of the last week or recent two weeks based on your selection.

2) Select the report time, which means the statistical range of the report.

Note

The options change according to the statistical cycle you select.

3) Select a day and/or time of sending the report at the **Send At** / **Send On** field.
4) (Optional) Select an effective period for the settings.

6. **Optional:** Complete the advanced settings.

1) Enable **Send Report via Email**, and then select an email template.

Note

You can click **Add** to add a new email template.

2) Enable **Upload to SFTP** and/or **Save to Local Storage**.

Note

To set the SFTP or local storage, click → **SFTP Settings / Configure Local Storage** on the top left of the page.

7. Click **Add**/**Save**.

27.4 Driver Management

You can add driver information to the platform in multiple ways and add driver groups for further management. In addition, you can export information and profile photos of drivers from the platform.

27.4.1 Add Drivers

Multiple methods are provided for adding drivers to the platform. You can add a single driver by entering his/her information or add drivers from existing persons. In addition, you can batch add driver information by importing a template with driver information or importing ZIP files containing driver's profile photos.

Add a Single Driver

Steps

1. On the top navigation bar, go to ▦ → **On-Board Service → On-Board Monitoring → Driver Management → Driver** .
2. Hover the mouse cursor over **Add** and click **Add Driver** to enter the Add Driver page.

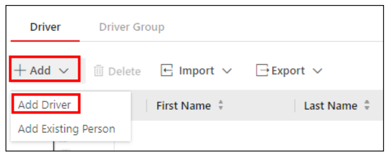


Figure 27-9 Add Driver

3. Set the driver's basic information, such as the ID, driver group, first name, last name.

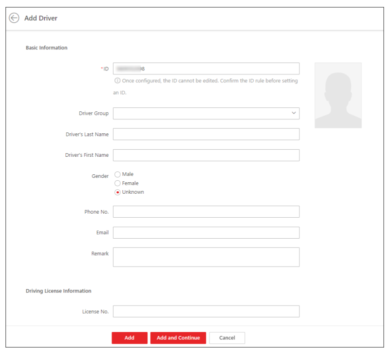


Figure 27-10 Add Driver Page

ID (Required)

The default ID is generated by the platform. You can edit it if needed. Once the driver is added successfully, the ID cannot be edited any more.

Driver Group

See details about how to add a driver group in ***Add a Driver Group*** .

Driver's Last/First Name (Required)

Either the last name or the first name is required.

Profile Photo

Hover over , and then take or upload a profile photo of the driver.

4. **Optional:** Set the driver's driving license information, including the driving license No. and picture.
5. Finish adding the driver.
   - Click **Add**.
   - Click **Add and Continue** to finish adding the driver and continue to add other drivers.
6. **Optional:** Perform the following operations.

Edit a Driver	Click the driver name to edit the driver details.
Delete Drivers	Select one or multiple drivers and click **Delete** to delete the drivers.
Filter Drivers	Click to filter drivers by name, ID, phone No., driver group or/and driving license No.

Add from Existing Persons

If you have added persons to the platform, you can add them as drivers.

Before You Start

Make sure you have added persons to the platform.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driver Management** → **Driver** .
2. Hover the mouse cursor over **Add** and click **Add Existing Driver**.

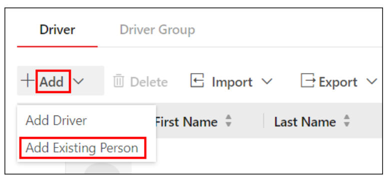


Figure 27-11 Add Existing Driver

3. Select one or multiple persons from the list and click **Add**.

Note

You can search for target persons by keywords.

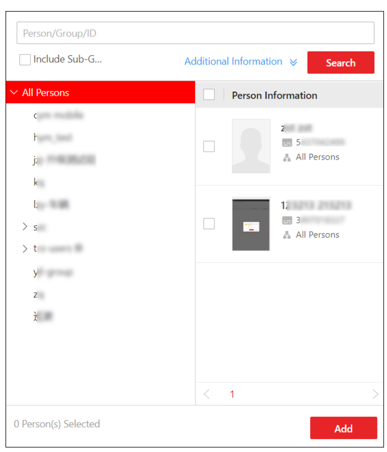


Figure 27-12 Add Existing Person Page

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

Edit a Driver	Click the driver name to edit the driver details.
Delete Drivers	Select one or multiple drivers and click **Delete** to delete the drivers.
Filter Drivers	Click to filter drivers by name, ID, phone No., driver group or/and driving license No.

Import Drivers via the Template

You can batch add drivers to the platform by importing a template which contains driver information including name, driver group.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driver Management → Driver** .
2. Hover the mouse cursor over **Import** and click **Import Driver via Template**.

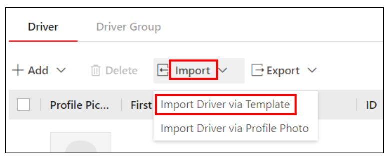


Figure 27-13 Import Drivers via the Template

3. In the pop-up window, click **Download Template** to save the template to the local PC.

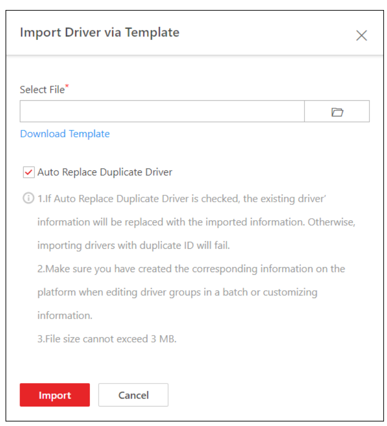


Figure 27-14 Import Drivers via the Template Page

4. In the downloaded template, enter the driver information by following the rules shown in the template.
5. Click and select the template with driver information from the local PC.
6. **Optional:** Check **Auto Replace Duplicate Driver** to replace the existing driver information if the imported ID is the same as that of the existing driver.
7. Click **Import** to start importing driver information.
8. **Optional:** Perform the following operations.

Edit a Driver	Click the driver name to edit the driver details.
Delete Drivers	Select one or multiple drivers and click **Delete** to delete the drivers.
Filter Drivers	Click to filter drivers by name, ID, phone No., driver group or/and driving license No.

Import Drivers via Profile Photos

You can batch add driver information to the platform by importing ZIP files containing JPG, JPEG, or PNG profile photos.

Steps

1. Name the profile photos as required, move these photos into one folder, and then compress the folder in ZIP format.

Note

- Naming rule of profile photos: First Name+Last Name_ID. Either first name or last name is required, and the ID is optional. For example, Kate+Smith_123.jpg; Kate_123.jpg; Smith_123.jpg; Kate+Smith.jpg; Smith.jpg
- If the ID in the profile photo name is the same as that of an existing driver on the platform, the existing driver's information will be modified.
- If the ID in the profile photo name does not exist on the platform or the existing driver with the same name does not have an ID, a new driver with the profile photo, name, and ID will be created.
- If the profile photo name contains ID only, the existing driver with the same ID will be modified.

2. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driver Management → Driver** .
3. Hover the mouse cursor over **Import** and click **Import Driver via Profile Photo**.

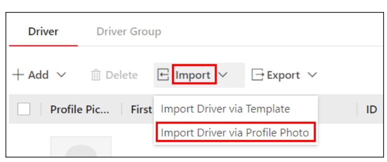


Figure 27-15 Import Drivers via Profile Photos

4. Click and select the ZIP files from the local PC.

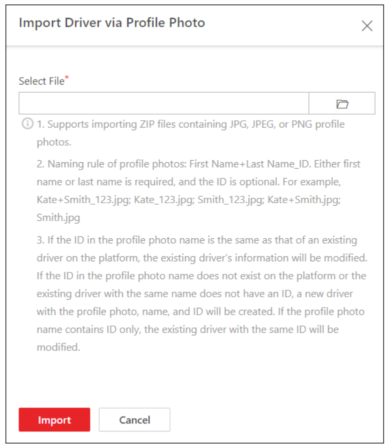


Figure 27-16 Import Drivers via Profile Photos Page

5. Click **Import**.
6. **Optional:** Perform the following operations.

Edit a Driver	Click the driver name to edit the driver details.
Delete Drivers	Select one or multiple drivers and click **Delete** to delete the drivers.
Filter Drivers	Click to filter drivers by name, ID, phone No., driver group or/and driving license No.

27.4.2 Export Drivers

You can batch export driver detailed information and driver's profile photos.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driver Management → Driver** .
2. Hover the mouse cursor over **Export** and click **Export Driver Information** or **Export Driver Profile Photo** as required.
3. Set a password and confirm the password for decompressing the exported ZIP file.

Note

For exporting driver profile photos, the user name and password are also required.

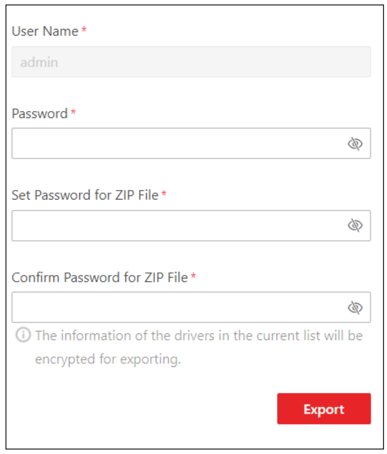


Figure 27-17 Export Driver Profile Photos

4. Click **Export**.

Note

You can use the password you set previously to decompress the exported ZIP file.

27.4.3 Add a Driver Group

You can add driver group(s) to categorize different drivers for convenient management.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driver Management → Driver Group** .
2. Click + and enter the driver group name.
3. Click **OK**.

   In the driver group list, the added driver group will be displayed with the number of people.
4. **Optional:** Perform the following operations.

Edit Driver Group	Select a driver group, click to edit the driver group name and then click **OK**.
Delete Driver Group	Select a driver group, click to delete the driver group.
Search for Driver Group	Enter a key word in the search box, and click to search for the target driver group.

27.4.4 Add Drivers to a Driver Group

After adding a driver group, you can add drivers to the driver group for management.

Before You Start

Make sure you have added drivers and driver group(s) on the Client. For details, refer to ***Add Drivers*** and ***Add a Driver Group*** .

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driver Management → Driver Group** .
2. Select the added driver group in the left list.
3. Click **Add**.

   The Add Driver pane will pop up.
4. Select driver(s) and click **Add**.

   Note

   You can search the target driver by name or ID.
5. **Optional:** Perform the following operations.

Filter Drivers	Select a driver group, click and set filter conditions such as name, and then click **Filter**.
Delete Drivers	Select a driver group in the driver list on the left, then select one or multiple drivers on the right and click **Delete** to delete the drivers.

27.5 Driving Rule

There are two types of driving rule: fence rule and deviation rule. A fence rule specifies the area where vehicles are allowed or not allowed to drive and a deviation rule specifies the route that vehicles should drive along. Besides, you can configure rule schedule templates to define when the rules should take effect. As a result, if a vehicle breaks an effective rule, an alarm will be triggered and uploaded to the platform.

27.5.1 Configure a Fence Rule

You can add a fence rule to specify the area where vehicles are allowed or not allowed to drive.

Before You Start

Make sure you have set the GIS map. For details, refer to ***Configure Basic Parameters*** .

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driving Rule Configuration → Fence Rule** .
2. Click **Add** to enter the Add Rule page.

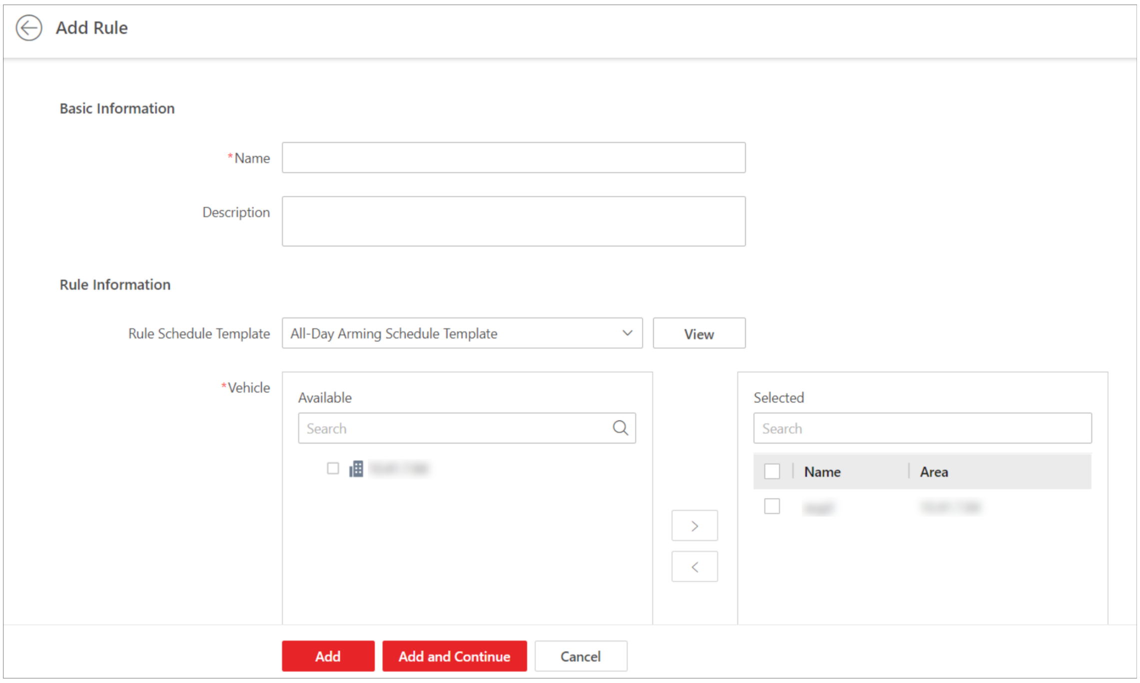


Figure 27-18 Add a Fence Rule

3. Set the basic information for the fence rule, including the name and description.

4. Set rule information.

1) Select a rule schedule template.

Note

You can click **View** to view the scheduled time of the selected template. If you have not configured any rule schedule template, you can see ***Configure a Rule Schedule Template*** for how to configure one.

2) Select vehicle(s) that the fence rule will be applied to.

3) Set the fence type.

Fence for Entry Detection

An alarm and event will be triggered when a selected vehicle enters the fence area.

Fence for Exit Detection

An alarm and event will be triggered when a selected vehicle exits the fence area.

4) Set **Threshold for Triggering Rule** (0 to 60 minutes allowed).

5) In the Fence Area area, click to draw a fence area on the map.

5. Click **Add** to finish or click **Add and Continue** to add another fence rule.

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

Edit Fence Rule	On the rule list, click the name of a fence rule to edit it.
Filter Fence Rule	On the fence rule page, click in the upper-right corner, set filtering conditions, and click **Filter** to filter fence rules.

Delete Fence Rule	On the rule list, select one or multiple fence rules and click **Delete** to delete them.

27.5.2 Configure a Deviation Rule

You can add a deviation rule to specify the route that vehicles should drive along.

Before You Start

Make sure you have set the GIS map. For details, refer to ***Configure Basic Parameters*** .

Steps

1. On the top navigation bar, go to ▦ → **On-Board Service → On-Board Monitoring → Driving Rule Configuration → Deviation Rule** .
2. Click **Add** to enter the Ad Rule page.

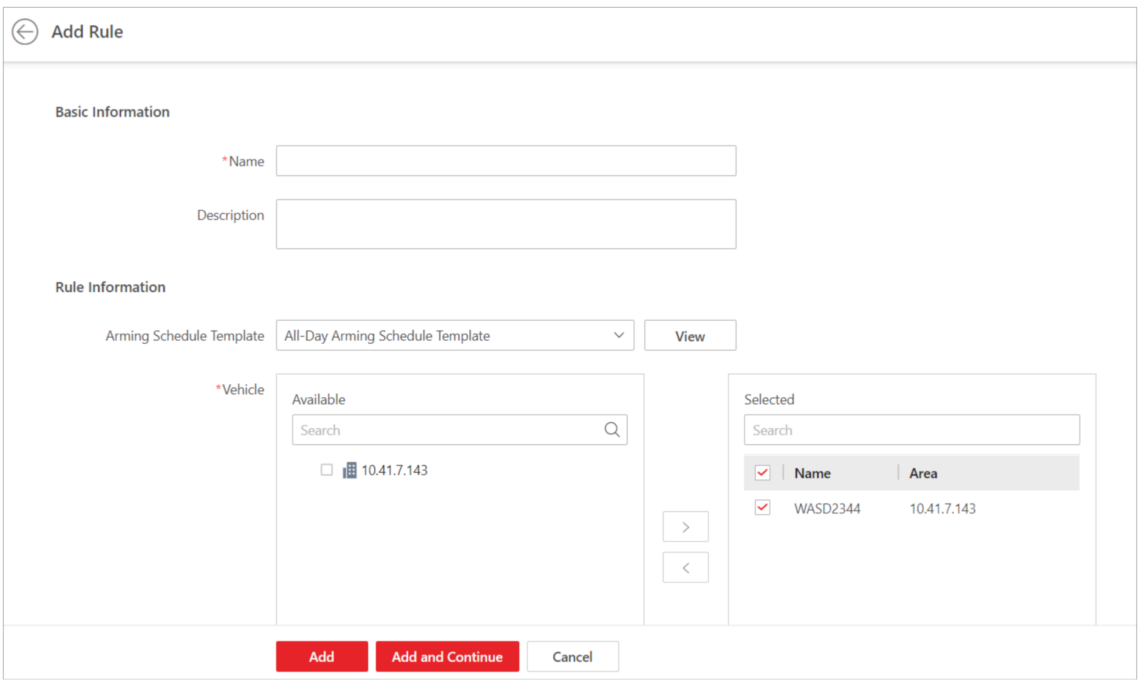


Figure 27-19 Add a Deviation Rule

3. Set the basic information for the fence rule, including the name and description.
4. Set rule information.
   1) Select a rule schedule template.

   Note

   You can click **View** to view the scheduled time of the selected template. If you have not configured any rule schedule template, you can see ***Configure a Rule Schedule Template*** for how to configure one.

   2) Select vehicle(s) that the deviation rule will be applied to.

3) Set the deviation threshold.

Note

An event will be triggered if a selected vehicle deviates from the route beyond the threshold.

4) In the Driving Route area, click to draw a route on the map.

5. Click **Add** to finish or click **Add and Continue** to add another deviation rule.
6. **Optional:** Perform further operations.

Edit Deviation Rule	On the rule list, click the name of a deviation rule to edit it.
Filter Deviation Rule	On the deviation rule page, click in the upper-right corner, set filtering conditions, and click **Filter** to filter deviation rules.
Delete Deviation Rule	On the rule list, select one or multiple deviation rules and click **Delete** to delete them.

27.5.3 Configure a Rule Schedule Template

You can add a rule schedule template to define the time when the related driving rules are effective in a week.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driving Rule Configuration → Rule Schedule Template** .
2. Click + to enter the Add Rule Schedule Template page.

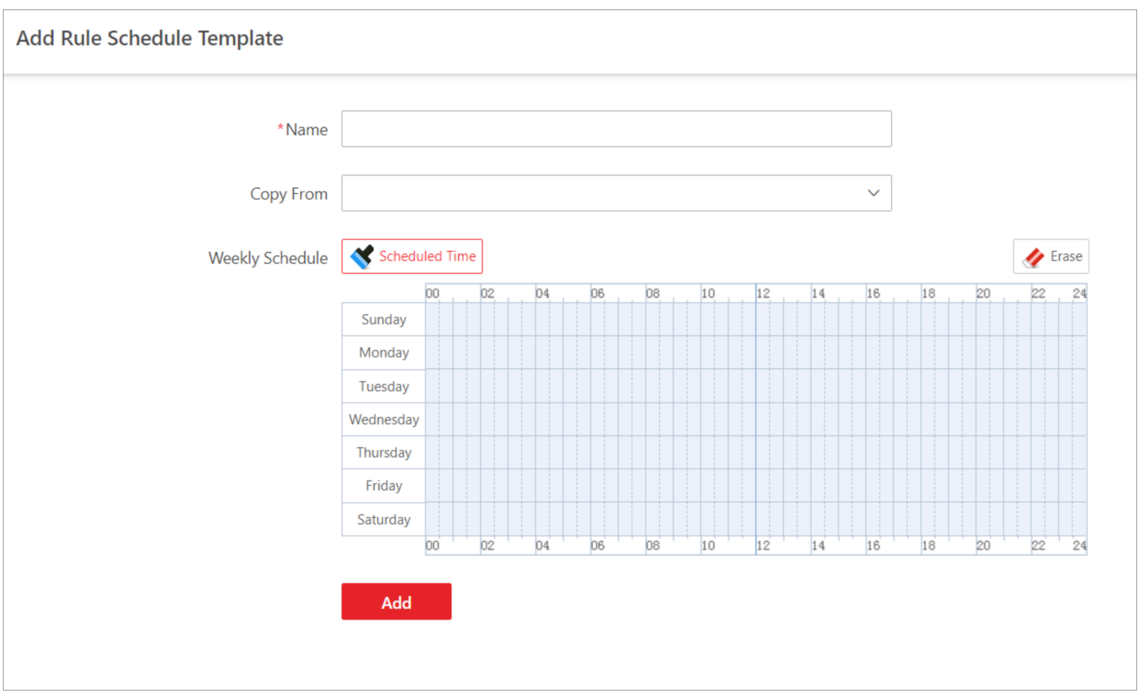


Figure 27-20 Add Rule Schedule Template

3. Create a name for the rule schedule template.
4. **Optional:** In the **Copy from** field, select an existing template to copy its weekly schedule to the current one.
5. Click **Scheduled Time** and click or drag on the timetable to define the period.

Note

- A rectangle represents half an hour.
- You can click a selected rectangle to set a more accurate time.
- You can click **Erase** and drag on the formerly selected rectangle(s) to remove them from the scheduled time.

6. Click **Add**.
7. **Optional:** Perform further operations.

Edit Rule Schedule Template	On the template list, click a rule schedule template to edit it.
Delete Rule Schedule Template	On the template list, select a rule schedule template and click **Delete** to delete it.

27.6 Route Management

HikCentral Professional supports managing driving stops, routes, and stop event rules. You can add stop groups to the platform and add stops to the groups in multiple ways for further management. Then you can select stops for a driving route and configure shift schedules. Also, you can configure event rules for specified stops.

27.6.1 Manage Stops

You can add driving stop groups to the platform. After that, you can add a single stop to the groups for further management. Also, you can import multiple stops in a batch to the added groups via a predefined template.

Add a Stop Group

You can add a stop group to categorize different stops for convenient management.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Route Management → Stop** .
2. Click in the top left coner, enter the stop group name, and click **Add**.

   The added stop group will be displayed in the stop group list.

What to do next

Add a single stop or import stops via the template to the stop group. See details in ***Add a Stop*** and ***Import Stops via the Template*** .

Add a Stop

After adding a stop group, you can add a single stop to the group.

Before You Start

Make sure you have set the GIS map. For details, refer to ***Configure Basic Parameters*** .

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** → **Stop** .
2. Select a stop group in the stop group list.
3. Click .
4. Move your mouse cursor to the target location on the map and click .

Note

You can search for the target geographic location by entering keywords in the search box in the top left corner of the map.

5. Select **Circle** or **Polygon** as the stop shape, move your mouse cursor to adjust the size, and click to confirm.
6. Enter a name and description for the stop and switch on/off **People Counting for Stops**.
7. Click **Save**.
8. **Optional:** Perform the following operations.

Edit a Stop	Select a stop, click to edit the information of the stop.
Delete a Stop	Select a stop, click to delete the stop.
Filter Stops	Check **Stops with People Counting Enabled Only** to filter stops.

Import Stops via the Template

You can fill the predefined template with the stop information to add multiple stops to the group at a time.

Before You Start

Make sure you have set the GIS map. For details, refer to ***Configure Basic Parameters*** .

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** → **Stop** .
2. Click .
3. Click **Download Template** and save the predefined template (EXCEL file) in your PC.

4. Open the downloaded template file and edit the required information of the stops to be added in the corresponding column.
5. Click and select the template file.
6. Click **Import**.
7. **Optional:** Perform the following operations.

Edit a Stop	Select a stop, click to edit the information of the stop.
Delete a Stop	Select a stop, click to delete the stop.
Filter Stops	Check **Stops with People Counting Enabled Only** to filter stops.

27.6.2 Configure Driving Routes and Shift Schedules

You can configure the driving route manually or generate it automatically, and manage stops of the route. After configuring routes, you can configure shift schedules which can repeat by week, and can also configure schedules which are effective only at a fixed date or during a specific time period for temporary use.

Before You Start

Make sure you have added stops on the platform. For details, refer to ***Manage Stops*** .

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** → **Route** .
2. Click **Add Route** (if no route exists) or + (if routes exist), enter a name for the route, and click **Add**.

   Note

   If there are routes added before, hover the cursor over a route on the route list page and click to create a copy and edit it as needed.

3. Select at least two stops on the map.
   - Click **Switch to List Mode** and select stops in the list.
   - Click the stop icon on the map to select the stop.

     Note

     Click the stop icon again on the map to deselect it.

   Note

   - In the top left corner of the map, you can search for a specific location on the map.
   - You can click **Reverse** to reverse the order of the selected stops.
   - You can hover the cursor over the stop name on the left and click to delete the stop.

   The selected stops are displayed on the left.
4. In the top right corner of the page, click **Next** and configure the driving route.

- Adjust the driving route manually: Hover the cursor over the line between two stops and drag to adjust the driving route manually.
- Generate the driving route automatically: Click **Auto Generate Route** to generate the route automatically.

Note

To generate the driving route automatically, you need to enable the Google map charging service.

5. Click **Next** to configure shift schedules.

Note

You can also click **Finish** to finish adding the route without configuring shift schedules.

6. Configure a single schedule or batch configure schedules for the route.
   1) Click **Add Schedule** or **Batch Add Schedules**.
   2) Set the schedule information.

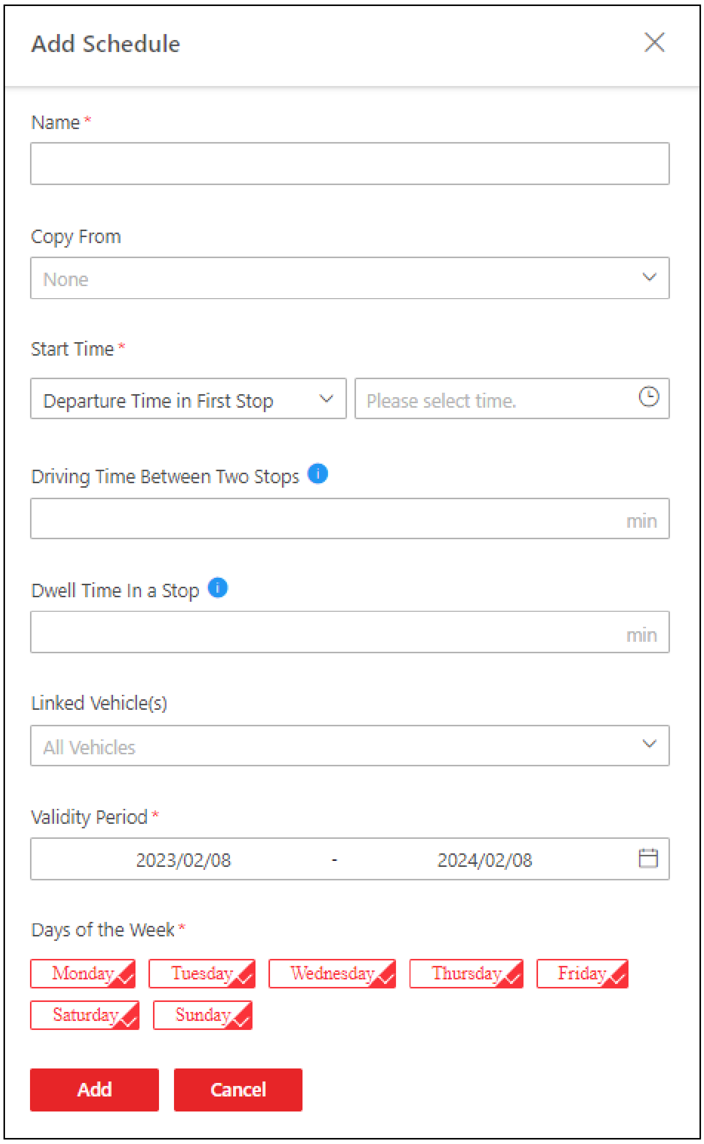


Figure 27-21 Add a Single Schedule

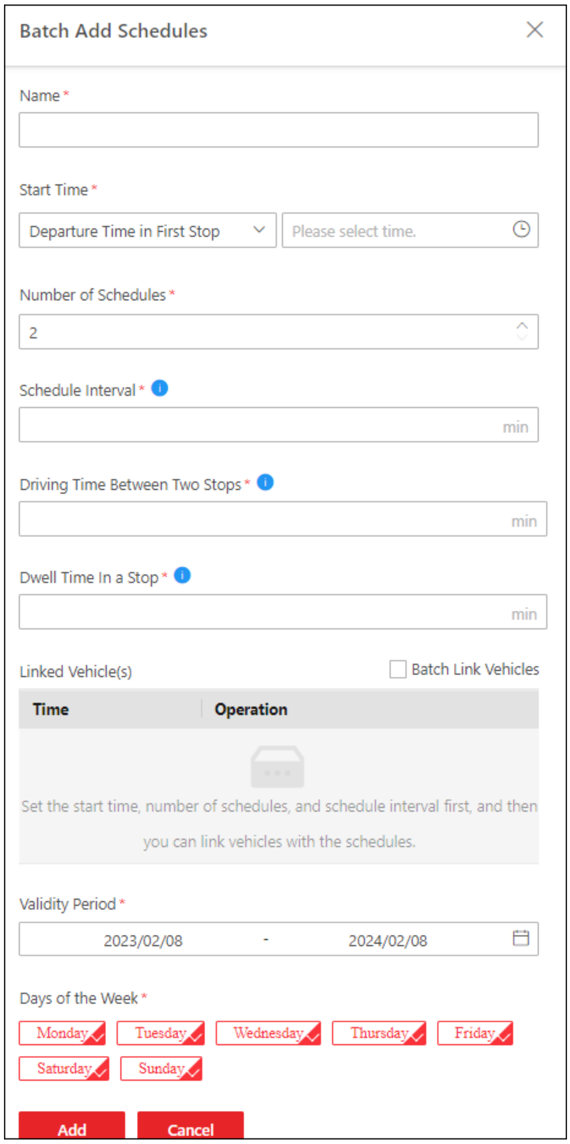


Figure 27-22 Batch Add Schedules

3) Click **Add**.

Note

You can set route parameters to define late arrivals/departures for the schedules. For details, refer to ***Configure Route Parameters*** .

7. Click **Finish** in the top right corner.
8. **Optional:** Perform the following operations.

Delete Route	Select the route and click to delete.
Filter Routes	Click to set filtering conditions to search for matched routes.

View Route Details	Click the route name to view details of the route. On the details page, you can click **Edit Route** to edit the route and click **Edit Schedule** to edit the shift schedule(s) of the route.
Enable/ Disable Route	Click ⊘ / ⊖ to enable/disable the route.
Switch Display Mode	• At the top of the route list, click **Week** or **Day** to display the timetable of routes on a weekly or daily basis. You can click ‹ / › to adjust the time period. • Click the route name displayed on the timetable, you can view the route's shift schedule details, including the departure time, arrival time and vehicle. You can also click ⊘ / ⊖ to enable/disable the route.

27.6.3 Add a Stop Event Rule

You can configure event rules for specified stops. After configurations, alarm inputs triggered outside/within the selected stops will be recorded as unintended alarm inputs.

Before You Start

- Make sure you have added devices on the platform and alarm inputs to areas. For details, refer to ***Device and Server Management*** .
- Make sure you have added stops on the platform. For details, refer to ***Manage Stops*** .

Steps

1. On the top navigation bar, go to ⊞ → **On-Board Service → On-Board Monitoring → Route Management → Stop Event Rule** .
2. Click **Add** to add a stop event rule.
3. Set rule basic information.
   1) Create a rule name.
   2) **Optional:** Enter the rule description.
4. Select the rule type.

   Stops Allowing Triggering Alarm Inputs

   Alarm inputs triggered outside the selected stops will be recorded as unintended alarm inputs.

   Stops Forbidding Triggering Alarm Inputs

   Alarm inputs triggered within the selected stops will be recorded as unintended alarm inputs.
5. Select the alarm input(s).
6. Select the stop(s) by stop or route.
7. Click **Add** to finish or click **Add and Continue** to add another rule.
8. **Optional:** On the rule list page, perform the following operations.

Delete Rule	Select the rule(s) and click **Delete**.

Edit Rule	On the rule list, click the name of a rule to edit the rule.
Filter Rules	Click in the upper-right corner, set filtering conditions, and click **Filter**.

27.7 Driving Monitoring

On the Driving Monitoring page, you can monitor driving vehicles to get their real-time information such as locations, speeds, and events. You can also play the live videos streamed from vehicle-mounted cameras, talk to drivers via two-way audio, track vehicles in real time, play back the tracks vehicles have traveled along, and add vehicles to the Favorites list for quick and easy management.

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driving Monitoring** .

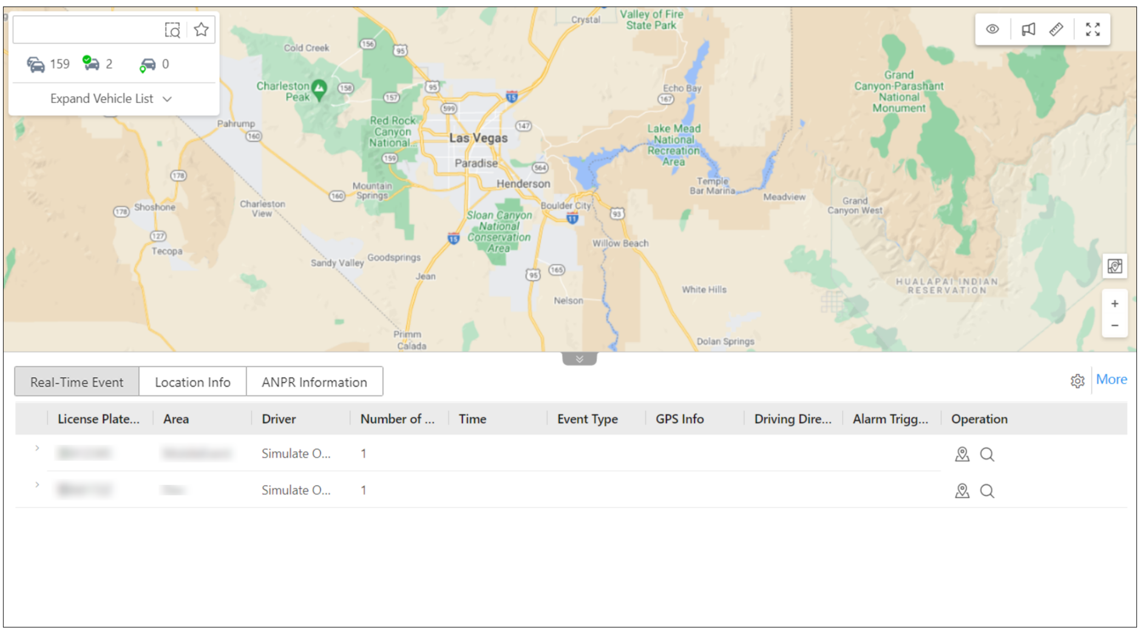


Figure 27-23 Driving Monitoring Page

Vehicle List Pane

Perform the following operations as needed:

Operation	Step
Search for / Filter Vehicles	• Enter keywords in the search box to search for target vehicles. • Click to specify an area for vehicle search.

Operation	Step
	• Click / / to view all/online/located vehicles. • Click to view vehicles in the Favorites list.
Locate / Broadcast to Vehicles	Click , click on the map to select a center and move the mouse to draw a circle based on the selected center, and then click on the map again to finish drawing. Hover over the drawn circle and click **Locate** or **Broadcast** to locate or broadcast to all vehicles in the circle.
View Vehicle Details	On the vehicle list, hover over a vehicle to view its real-time information, including its location, speed, etc.
Locate Vehicle	On the vehicle list, hover over a vehicle and click to locate the vehicle on the map and click again to cancel locating it.
Play Back Track	On the vehicle list, hover over a vehicle and click to play back the track the vehicle has traveled along.
Start Live View	Expand the camera list of a specific vehicle, and double-click to view the live videos streamed from the vehicle-mounted cameras.
Other	On the vehicle list, hover over a vehicle and click ··· to display the operation menu. You can choose to play video, talk to a driver via two-way audio, track a vehicle in real time, play back the track the vehicle has traveled along, control alarm outputs, and add/ remove a vehicle to/from the Favorites list.

Driving Monitoring on the Map

On the GIS map, you can view the number of unacknowledged alarms on the vehicles. You can click the icon of a located vehicle on the map to open the driving monitoring pane. On the pane, you can view the vehicle's real-time information including its location, speed, etc, and can perform the following operations:

Note

For an event that has been subscribed and configured with alarm trigger, only one record will be displayed and will be marked as an alarm.

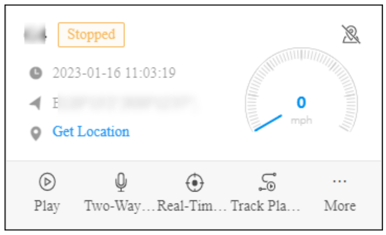


Figure 27-24 Driving Monitoring Pane

Operation	Step
Cancel Locating Vehicle	Click to cancel locating the vehicle.
Get Vehicle's Location	Click **Get Location** to get the vehicle's real-time location.
Play / Play Back Video	Click **Play** to play live or recorded videos streamed from vehicle-mounted cameras.
Talk to Driver	Click **Two-Way Audio** to talk to the driver.
Track Vehicle	Click **Real-Time Tracking** to track the vehicle in real time. You can click **Stop** in the upper-left corner of the vehicle-tracking page to stop tracking.
Play Back Track	Click **Track Playback** and select a period and camera to play back the track recorded by the camera in the specified period.
Control Alarm Output	Click **More → Alarm Output** and then click / in the Operation column to enable/disable the alarm output related to the vehicle.
Send Text	Click **More → Send Text** to send a text to the vehicle, and the text will be converted to audio in the vehicle.
View History Alarms	Click **More → View History Alarms** to view the vehicle's history alarms.
View Alarm Details	The number of triggered alarms is marked on the icon of the vehicle on the map. You can click the number to view alarm details. You can also view the videos streamed from the vehicle-mounted cameras.

Real-Time Event

The Real-Time Event table presents real-time events triggered by monitored online vehicles. Each record is attached with detailed information such as the license plate number, driver, event type, and GPS information. You can perform the following operations:

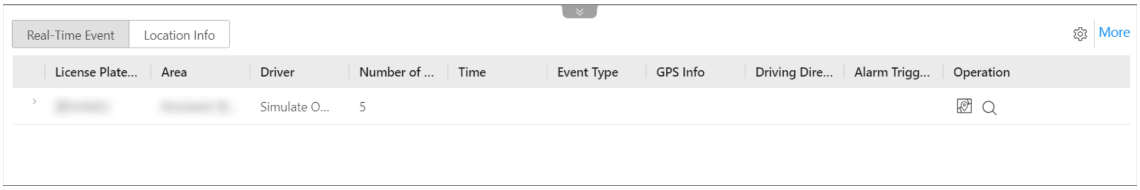


Figure 27-25 Real-Time Event Table

Operation	Step
Locate Vehicle	Click in the Operation column to locate a vehicle.
Center Vehicle	Click in the Operation column to place a located vehicle in the center of the map.
Search for Track	Click in the Operation column to go to search for the track a vehicle has traveled along.
Save As Evidence	Click in the Operation column to save the event as the evidence.
Select Event Type	Click to open the Settings pane and select the types of event to be reported to the platform.
Search for Driving Event	Click **More** to go the Driving Event Search page to search for driving events triggered in the past.

Location Info

The Location Info table presents the real-time locations of located vehicles. Each record is attached with detailed information such as the license plate number, GPS info, and driving direction. Besides, you can perform the following operations:

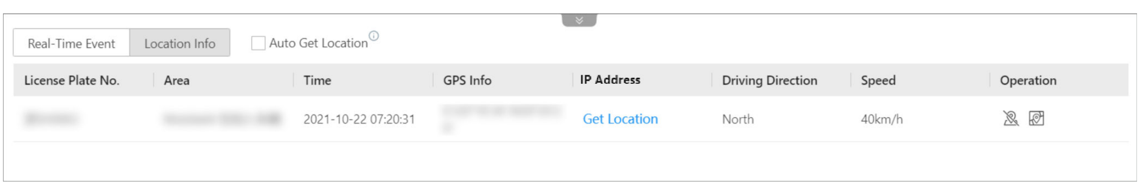


Figure 27-26 Location Info Table

Operation	Step
Get Vehicle's Location	Click **Get Location** in the IP Address column to get the real-time location of a vehicle.
Auto Refresh Location	Check **Auto Get Location** to automatically refresh locations frequently.
Cancel Locating Vehicle	Click in the Operation column to cancel locating a vehicle.
Center Vehicle	Click in the Operation column to place a vehicle in the center of the map.

ANPR Information

The ANPR Information table presents the vehicle passing records. Each record is attached with detailed information such as the license plate number, GPS info, and driving direction.
Click **More** to jump to **Passing Vehicle Search** in the ANPR module; you can also click the different buttons in the operation column of each record to jump to **Passing Vehicle Search** with different conditions.

Map Management

You can perform the following operations on the map:

Operation	Step
Display Driving Rule	Click and select **Fence Rule** or/and **Deviation Rule** to display the areas where vehicles are allowed or not allowed to drive and the routes that vehicles should drive along.
Broadcast to Vehicle	Click and select vehicle(s) to broadcast to them.
Measure Distance	Click and specify the start point and end point on the map to measure the actual distance between them.
Full-Screen Display	Click to display the map in full-screen mode.

27.8 Route Monitoring

On the route monitoring page, you can monitor the vehicles' driving routes to get stop information, route status, unpunctual causes, and vehicles' driving status. You can also view the detailed information of vehicles in the routes, such as locations, speeds, and events.

On the top navigation bar, go to ▦ → **On-Board Service → On-Board Monitoring → Route Monitoring** .

Route List

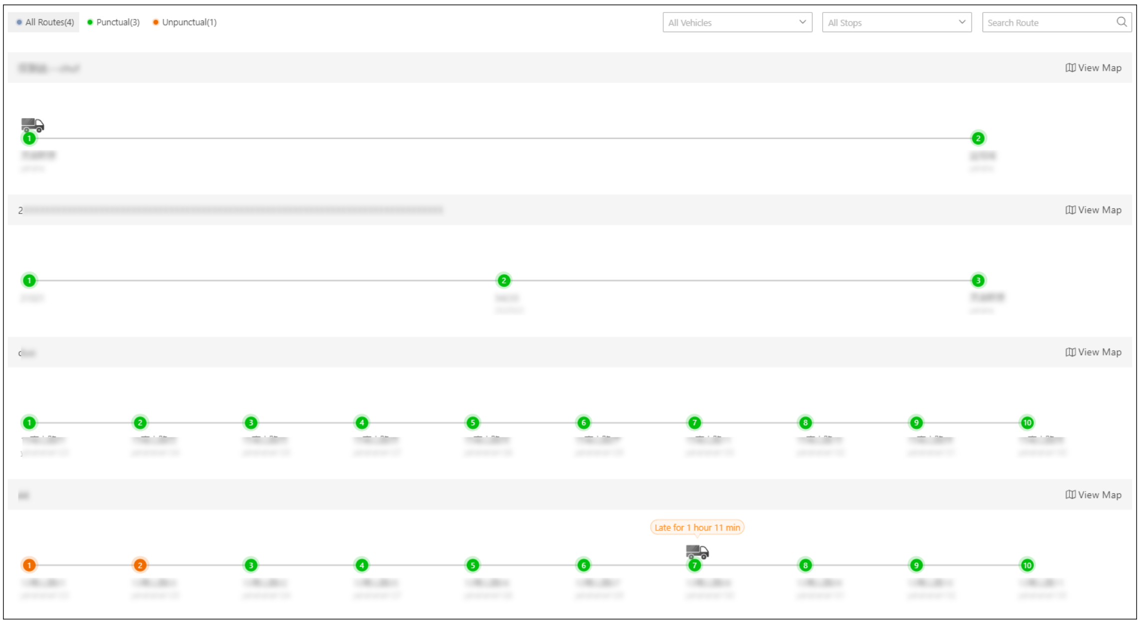


Figure 27-27 Route List

Perform the following operations as needed:

Operation	Description
Filter / Search for Routes	• In the top left corner of the page, click **All Routes** / **Punctual** / **Unpunctual** to view corresponding routes. • In the top right corner, select vehicles and/or stops from the drop-down list and/or enter keywords in the search box to quickly find target routes.
View Route Details	• You can view the total number of stops, the stop names, the status (punctual/early/late) and the current location of vehicles in each route. • Hover the mouse cursor over a stop to view its details, including punctual rate, vehicle, scheduled arrival time, actual arrival time, scheduled departure time, and actual departure time.
Add Cause of Unpunctual Departure/Arrival	Hover the mouse cursor over a stop, click 🗎 in the Operation column to add notes for unpunctual departures/arrivals.

Single Route Monitoring

Click **View Map** to view the details of a single route.

Note

The two panes on the left and at the bottom of the page can be displayed or hidden by clicking the arrows.

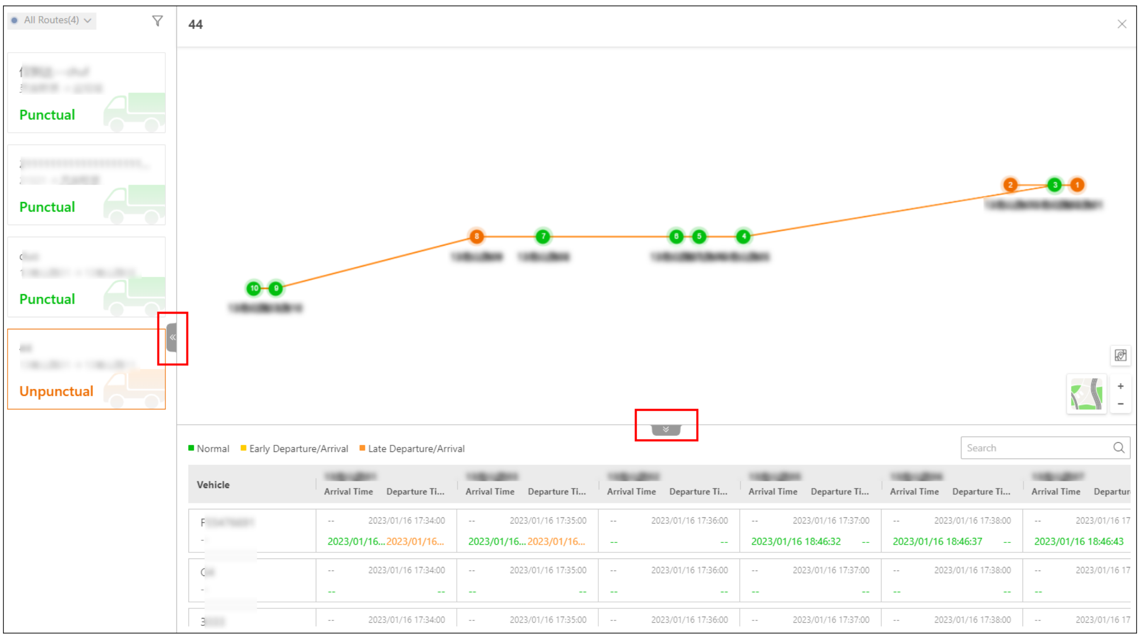


Figure 27-28 Single Route Monitoring

Perform the following operations as needed:

Operation	Description
View Route Details	• You can view the stops and vehicles in the selected route on the GIS map. • You can view the scheduled departure/arrival time and actual departure/arrival time in the table at the bottom, with different colors for different status (normal, early departure/arrival, and late departure/arrival).
Add Cause of Unpunctual Departure/Arrival	Hover the mouse cursor over the actual departure/arrival time in the timetable and click **Add Remarks** to add notes for unpunctual departures/arrivals.
Monitor Vehicles in the Route	Click the icon of a vehicle on the map to open its driving monitoring pane. For details about driving monitoring, see ***Driving Monitoring*** .

Operation	Description
View Alarm Details	The number of triggered alarms is marked on the icon of the vehicle on the map. You can click the number to view alarm details.
Filter / Search for Routes	• In the top left corner, you can filter routes by route status (all/punctual/unpunctual). • Click to select vehicles and/or stops from the drop-down list and/or enter keywords in the search box to quickly find target routes.
Switch to Another Route	You can select another route on the left pane to view its details.

27.9 On-Board Monitoring Record Search

On-board monitoring records include the tracks vehicles have traveled along, the events triggered by them in a specified period, the routes related to specific vehicles / vehicle groups, and fuel level monitoring records. You can search for records, view the details of each record, and export records to your PC for further use.

27.9.1 Search for Vehicle Tracks

You can search for the tracks that vehicles have traveled along in the specified period, view detailed information of each record, play back tracks, and export records to the PC.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Search → Vehicle Track Search** .
2. Set search conditions.
   1) Specify the period you want to search for vehicle tracks in.
   2) Select vehicle(s).
   3) **Optional:** Switch on **Speed Range** and set a speed range.
   4) **Optional:** Switch on **Triggered By** and click to select event type(s).

   Note

   All event types have been selected by default.
3. Click **Search**.

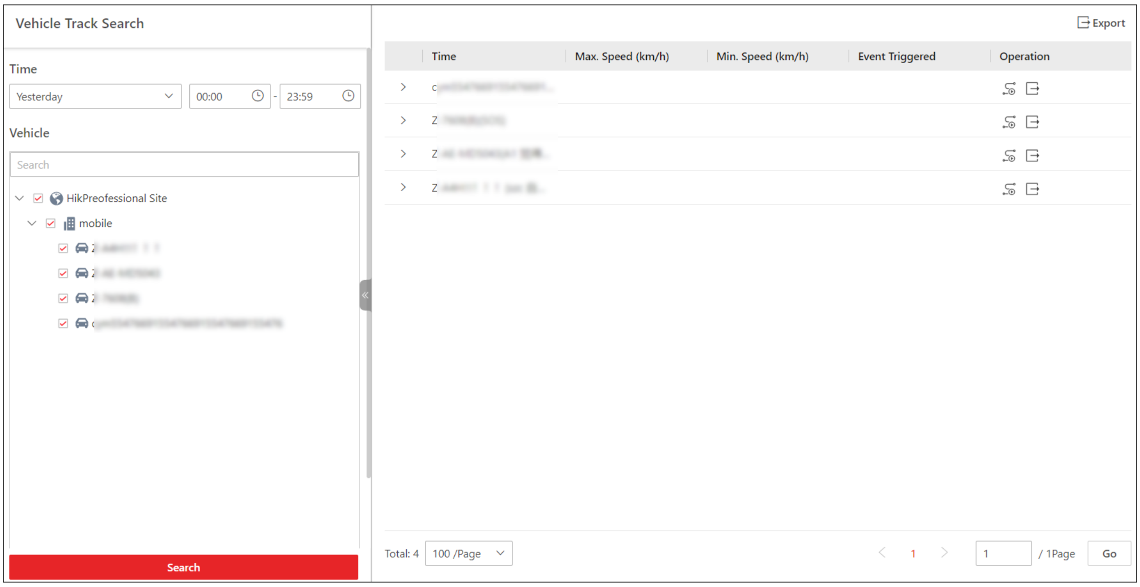


Figure 27-29 Vehicle Track Search

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

Play Back Track	Click to play back a track.
Export Record	Click to export a single record to the PC. Click **Export** in the upper-right corner to export all records to the PC.
Other	Click and more records generated in the specified period will be displayed. You can also click to play back a track and click to export a record to the PC.

27.9.2 Search for Driving Events

You can search for the events triggered by vehicles, drivers, or driver groups, view detailed information of each record, and export records to the PC.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Search → Driving Event Search** .
2. Set search conditions.

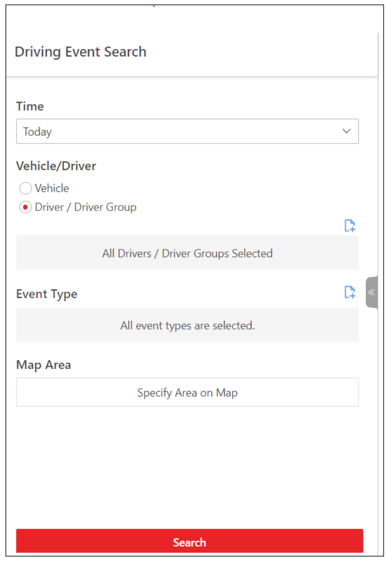


Figure 27-30 Search for Driving Events

1) Specify the period you want to search for driving events in.
2) Select **Vehicle** or **Driver / Driver Group** as the type.
3) Click to select vehicle(s), driver(s), or driver group(s).

Note

All vehicles / drivers / driver groups have been selected by default.

4) In the Event Type area, click to select event type(s).

Note

All event types have been selected by default.

5) In the Map Area area, click **Specify Area on Map** and draw an area on the map.

The platform will search for events triggered in the specified area.

3. Click **Search**.
4. **Optional:** Perform the following operations.

Play Back Track	Click to play back a track.
Export Record	Click to export a single record to the PC. Check record(s) and click **Export** in the upper-right corner to export them to the PC.

27.9.3 Search for Routes

You can search for routes, view detailed information of each route, and export route information to the local PC.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Search** → **Route Search** .
2. Set search conditions.

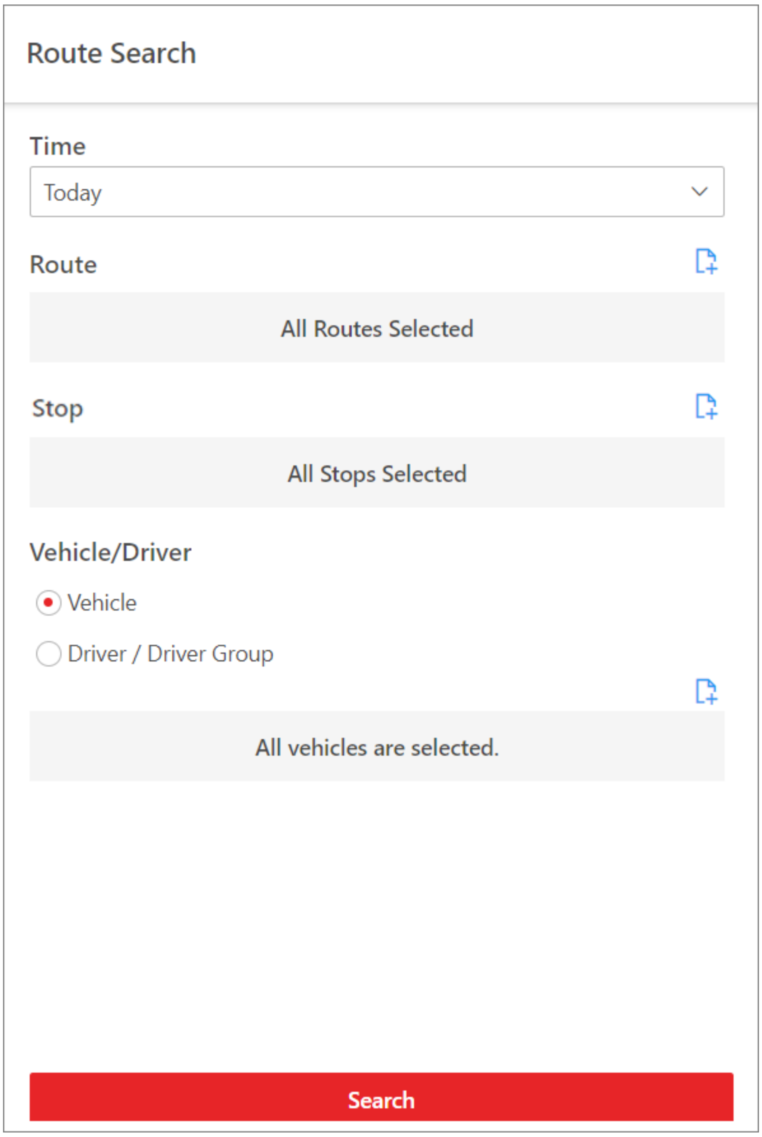


Figure 27-31 Search Conditions

1) Specify the period you want to search for routes in.
2) Click to select route(s).

Note

All routes have been selected by default.

3) Click to select stop(s).

Note

All stops have been selected by default.

4) Select **Vehicle** or **Driver / Driver Group** as the type.

5) Click to select vehicle(s), driver(s), or driver group(s).

Note

All vehicles / drivers /driver groups have been selected by default.

3. Click **Search**.

The needed routes will be displayed in the list.

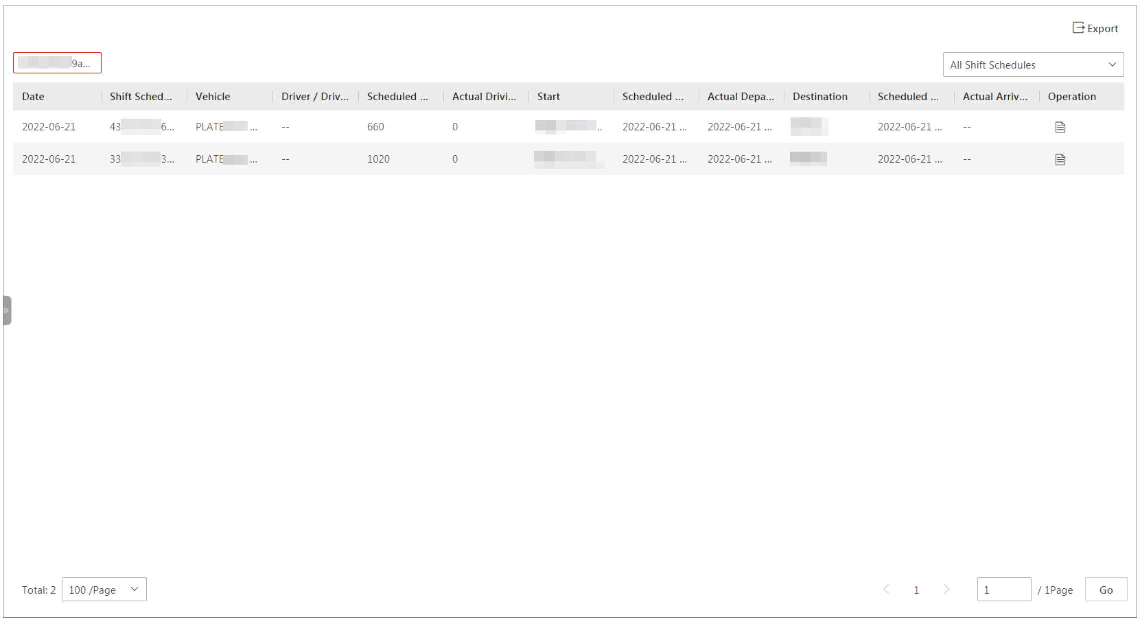


Figure 27-32 Search for Routes

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

Play Back Track In the Operation column, click to play back a track.

Export Record Click to export a single record to the PC.

Check records and click **Export** in the upper-right corner to export them to the PC.

27.9.4 Search for Fuel Level Monitoring Records

You can search for records of fuel level in the specified period and view details of the license plate No., area, driver's name, fuel tank model, fuel quantity, fuel level in tank (%), GPS info, and fuel filling or not.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Search → Fuel Level Record Search** .
2. Set search conditions.
   1) Specify the period you want to search for fuel level records in.
   2) Select **Vehicle** or **Driver / Driver Group**, and all vehicles or all drivers / driver groups are selected by default.

   Note

   Click to specify certain vehicles or driver / driver groups.
3. Click **Search** to get the list of fuel level monitoring records.

   Note

   You can click **Export** in the upper-right corner to export the records to your local PC.

27.10 Statistics and Reports

HikCentral Professional provides multiple types of reports for you to get insight into the variation trend of the driving data, driving behaviors, number of passengers, and device online rate related to the vehicles in your company/organization. These reports, which can be exported to your local PC, demonstrate data in a visualized way through charts and (or) tables, helping you make better business decisions, operation strategies, device maintenance plans, etc.

Note

The report export tasks can be managed in **Download Center**.

27.10.1 Generate a Driver Analytics Report

You can generate a driver analytics report showing the driver analytics information of specific drivers in a certain period, including the basic information of driver, driving distance, driving duration, events per 100 km, number of events, total fuel consumption, etc.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Driver Analytics** .

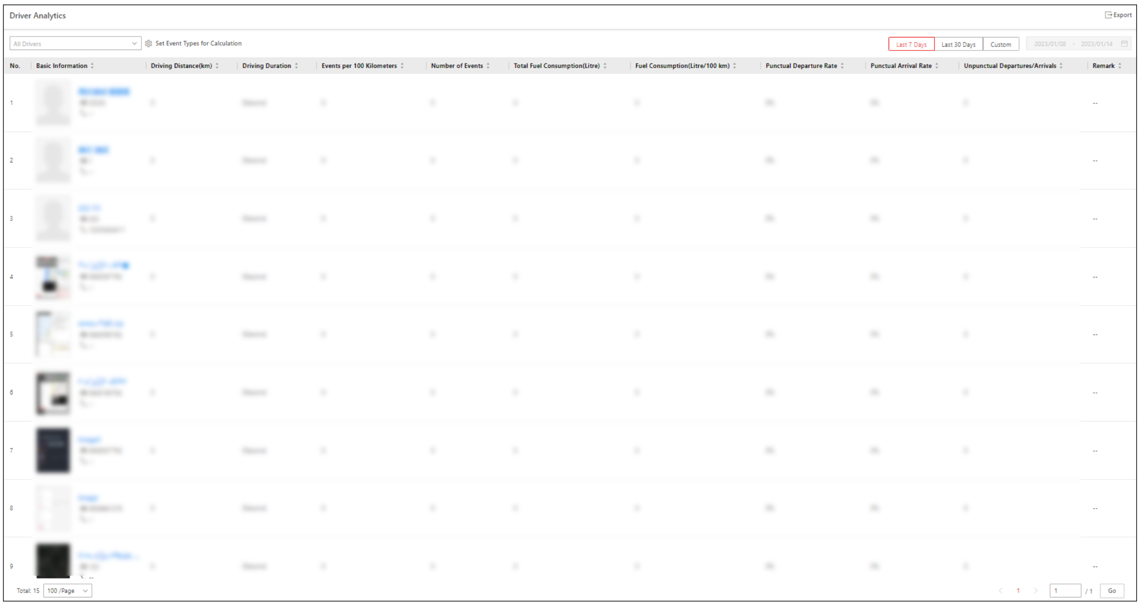


Figure 27-33 Generate a Driver Analytics Report

2. Select drivers from the drop-down list.
3. Click **Set Event Types for Calculation** to select event(s).
4. Set the time period within which driver's statistics will be shown in the report.

   The filtered records will be displayed automatically.
5. Click **Export** in the top right corner. Select **All Drivers** or **Filtered Drivers** and click **Export** to export the corresponding statistics report to the local PC.

27.10.2 Generate a GPS Information Report

You can generate a GPS information report showing the GPS information of specific vehicles in a certain period, including the number of locations detected by GPS, license plate number, area, time, GPS, driving direction, and driving speed.

Steps

1. On the top navigation bar, go to ▦ → **On-Board Service → On-Board Monitoring → Statistics and Reports → GPS Information Report** .
2. Set search conditions.

   Vehicle

   Select vehicles from the areas listed below.

   Note

   Up to 20 vehicles can be selected.

   Report Type

Select a report type.

Daily Report

The report to be generated will show the data of the selected vehicles in one calendar day.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

By default, the data will be shown in a line chart, on which the Y-axis represents the number of locations and the X-axis the time.

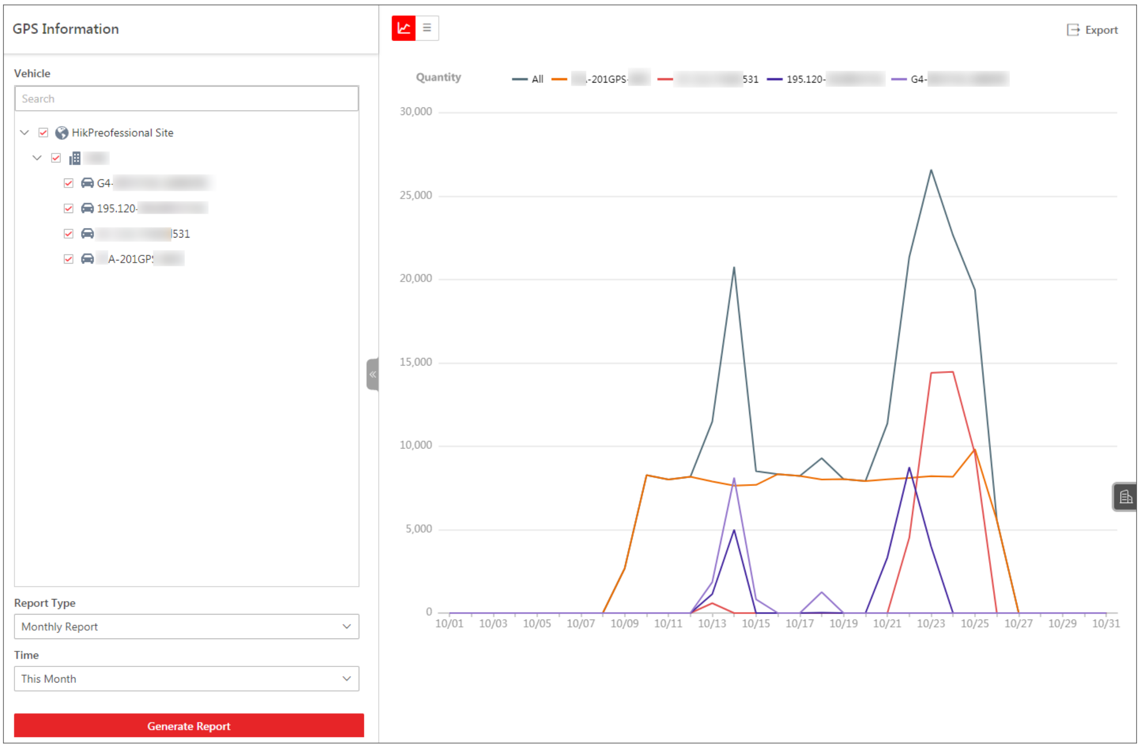


Figure 27-34 View Data in Line Chart

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.
View Data in Table	Click ≡ to view the data in a table that shows the license plate number, area, time, GPS information, direction, and speed. You can select a vehicle from the drop-down list and set a period to further filter the data.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles, time, content, and file format to export the report.

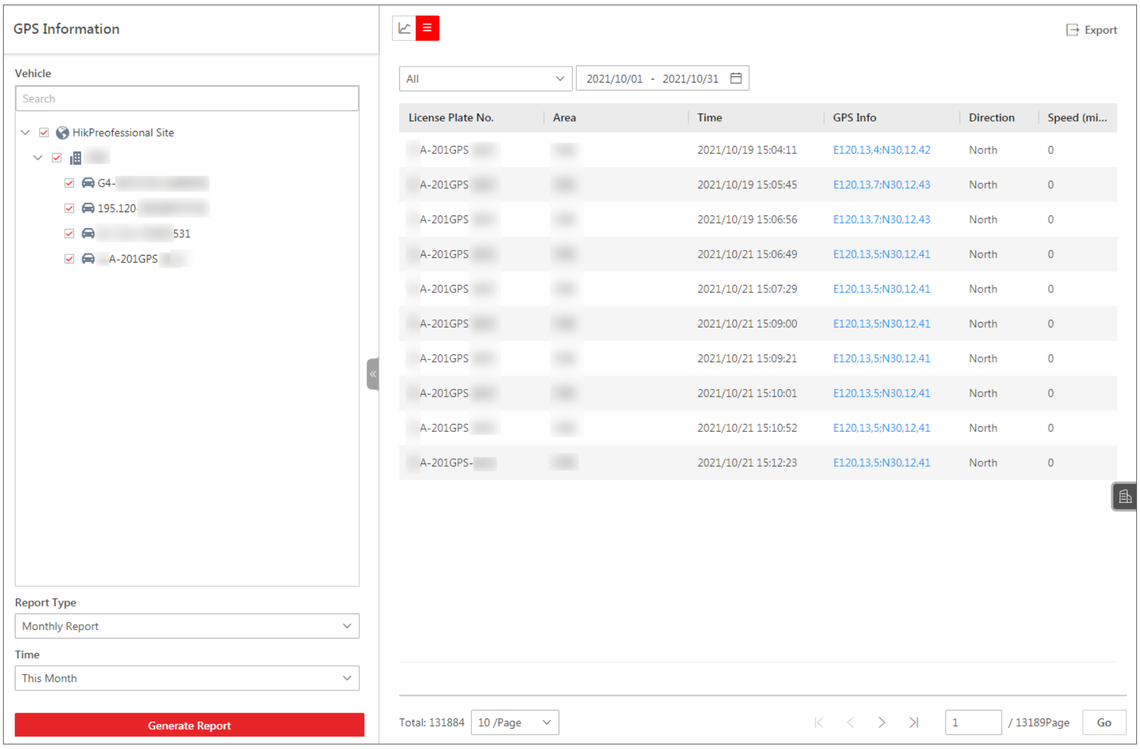


Figure 27-35 View Data in Table

27.10.3 Generate a Driving Distance Report

You can generate a driving distance report to view the driving distance of specific vehicles or drivers in a certain period.

Steps

1. On the top navigation bar, go to ▦ → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Driving Distance Report** .
2. Set search conditions.

   Analysis Type

   Select vehicle or driver as the analysis type and select vehicles/drivers from the list accordingly.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the driving distance of the selected vehicles in one calendar day.

   Weekly Report

The report to be generated will show the driving distance of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the driving distance of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the driving distance of the selected vehicles in a custom period of no more than 31 days.

Time

The driving distance in the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

By default, the data will be shown in a line chart, on which the Y-axis represents the driving distance and the X-axis the time.

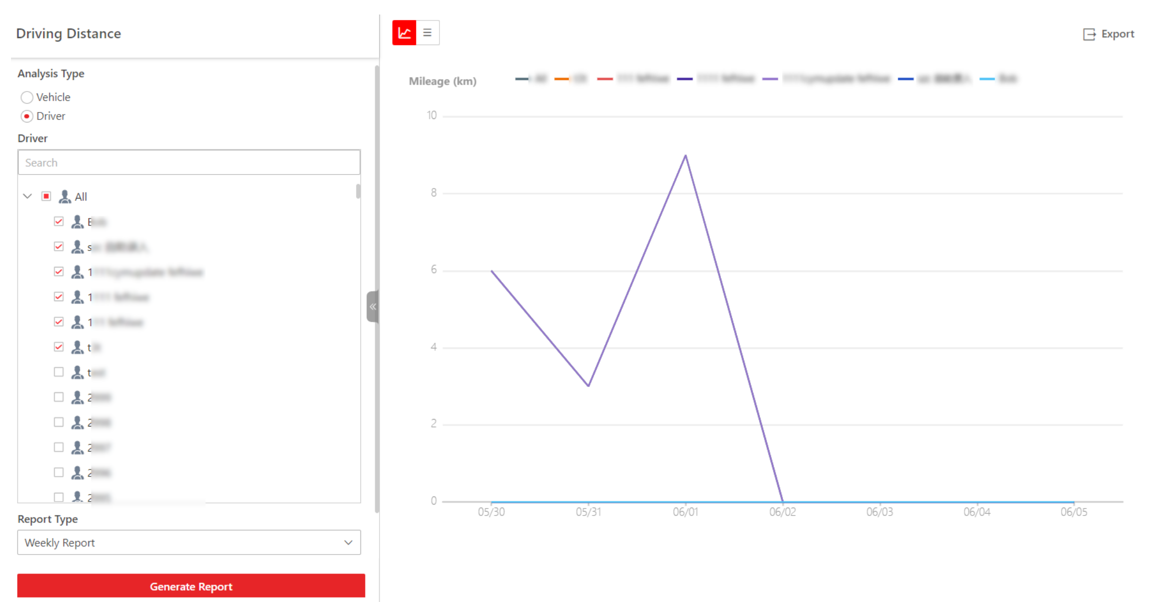


Figure 27-36 Generate Report

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles/drivers at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide the corresponding data.
View Data in Table	Click ≡ to view the data in table.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles/drivers, time, and file format to export the report.

27.10.4 Generate a Driving Duration Report

You can generate a driving duration report to view the driving duration of specific vehicles or drivers at a certain speed in a certain period.

Steps

1. On the top navigation bar, go to ▦ → **On-Board Service → On-Board Monitoring → Statistics and Reports → Driving Duration Report** .
2. Set search conditions.

   Analysis Type

   Select vehicle or driver as the analysis type and select vehicles/drivers from the list accordingly.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the data of the selected vehicles in one calendar day.

   Weekly Report

   The report to be generated will show the data of the selected vehicles in one calendar week.

   Monthly Report

   The report to be generated will show the data of the selected vehicles in one calendar month.

   Custom Time Interval

   The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

   Time

   The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

Driving Speed Exceeds

Determine the threshold for calculating the driving duration. For example, if you select **40 mile/h**, the duration when the selected vehicles drove faster than 40 mile/h will be calculated.

3. Click **Generate Report**.

By default, data will be shown in a line chart, on which the Y-axis shows the driving duration (unit: second) and the X-axis the time.

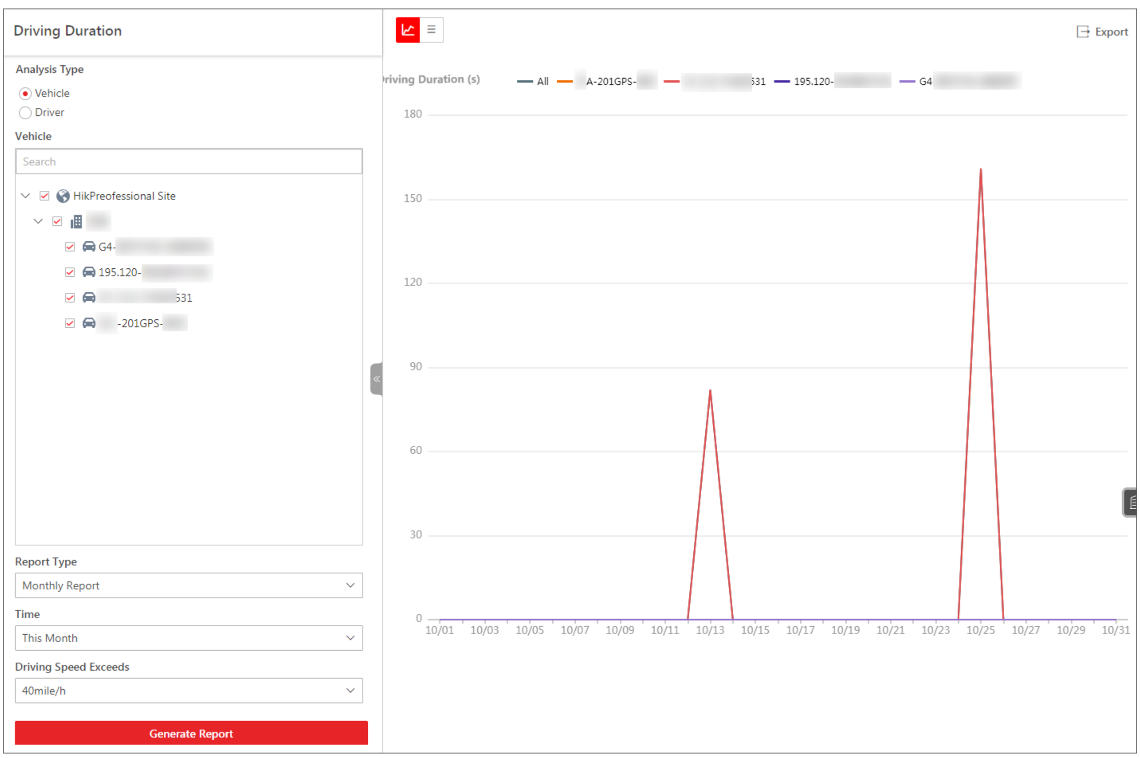


Figure 27-37 Monthly Report Example

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

View Detailed Data
Hover the cursor onto the line chart to view detailed data of the selected vehicles/drivers at the corresponding time point.

Show/Hide Legend
Click a legend on the top of the line chart to show/hide it.

View Data in Table	Click ≡ to view the data in a table.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles/drivers, time, and file format.

27.10.5 Generate a Speeding Report

You can generate a speeding report to view the vehicles' speeding records in a specific period.

Steps

Note

You can set the speed threshold for vehicles in a specific area.

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Speeding Report** .
2. Set search conditions.

   Vehicle

   Select vehicles from the areas listed below.

   Note

   Up to 20 vehicles can be selected.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the data of the selected vehicles in one calendar day.

   Weekly Report

   The report to be generated will show the data of the selected vehicles in one calendar week.

   Monthly Report

   The report to be generated will show the data of the selected vehicles in one calendar month.

   Custom Time Interval

   The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

   Time

   The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

By default, the data will be shown in a line chart, on which the Y-axis represents the speeding times and the X-axis the time.

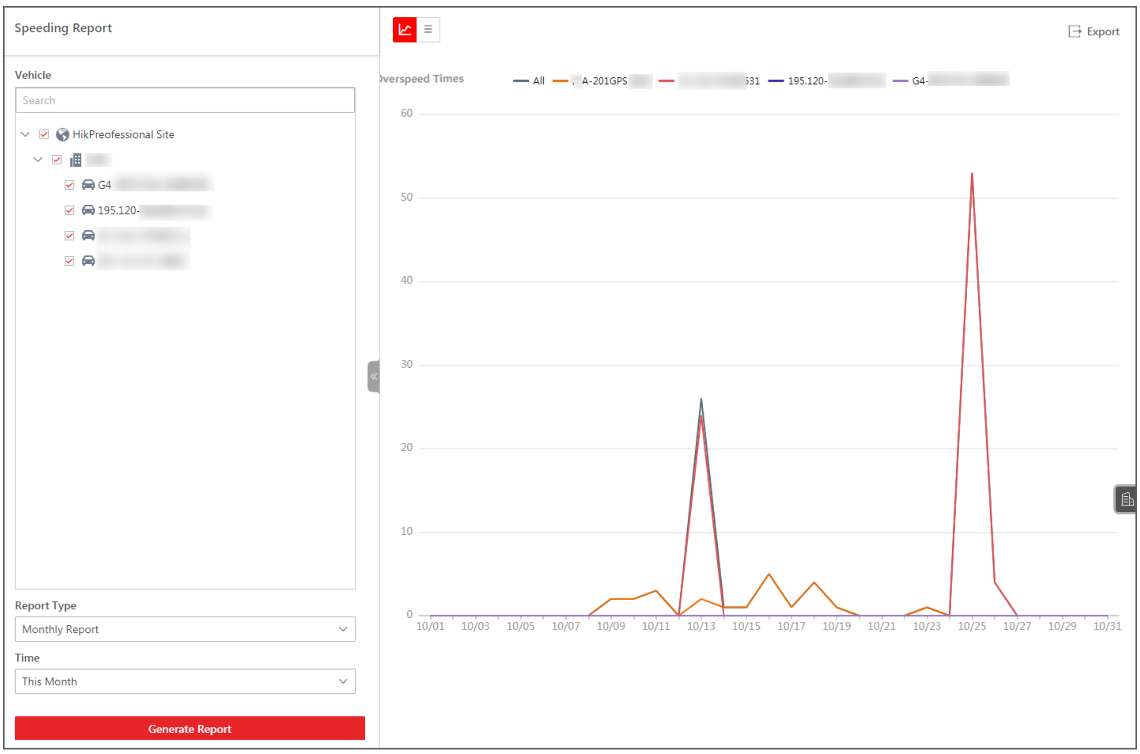


Figure 27-38 View Data in Line Chart

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.
View Data in Table	Click ≡ to view the data in a table that shows the license plate number, area, time, data, direction, and speed.

You can select a vehicle from the drop-down list and set a period to further filter the data.

Export Report Click **Export** to open the Export pane, and then set parameters including vehicles, time, content, and file format to export the report.

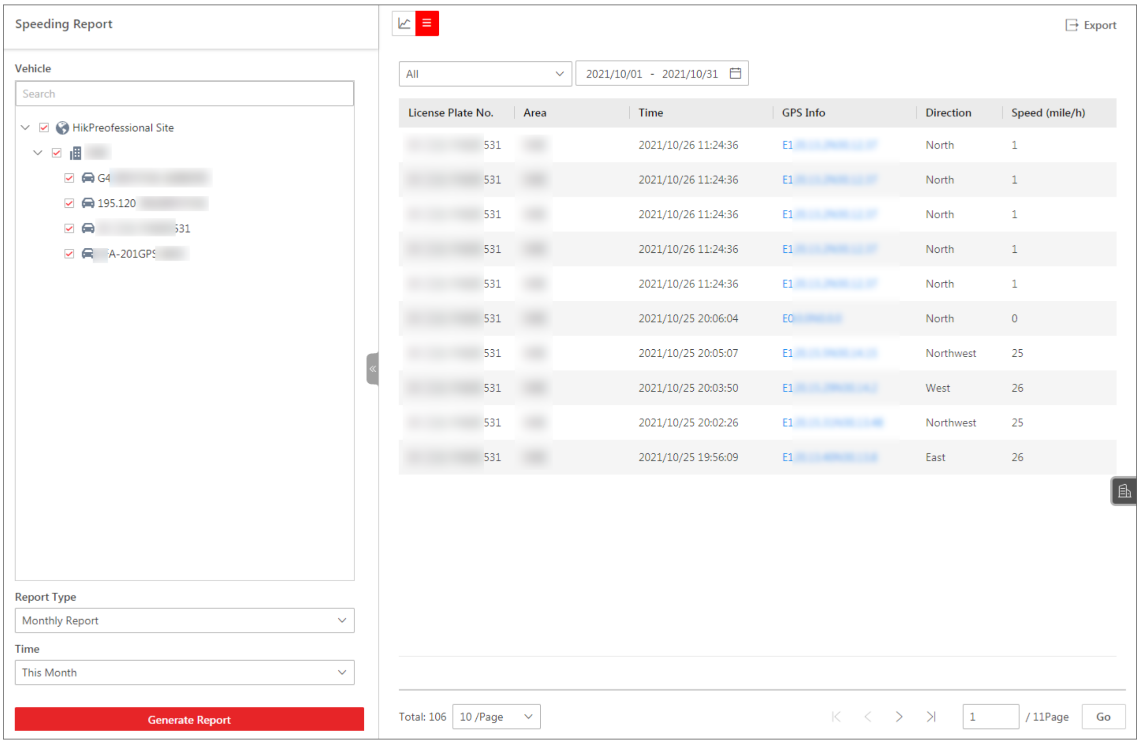


Figure 27-39 View Data in Table

27.10.6 Generate a Stop Analytics Report

You can generate a stop analytics report showing the overall statistics of the selected stops in a certain period, including the average punctual departure rate, average punctual arrival rate, average dwell time (in minutes), total unpunctual arrivals, and total unpunctual departures. When enough results are generated, the report also shows the top 10 / bottom 10 stop rankings for punctual departure rate, punctual arrival rate, and dwell time.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Stop Analytics** .
2. Select route(s) and stop(s) accordingly from the drop-down lists.
3. Select a time period for the report from **Today**, **Last 7 Days**, and **Custom**.

Note

The custom time period should be within 7 days.

The stop analytics report of the selected time period will be displayed on the page.

27.10.7 Generate a Driving Event Report

You can generate a driving event report to view the times of event detection related to specific vehicles in a specific period.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Driving Event Report** .
2. Set search conditions.

   Analysis Type

   Select **Vehicle** or **Driver** as the analysis type and select vehicles/drivers from the list.

   Statistics Type

   Select **Total Events** or **Events per 100 Kilometers** as the statistics type.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the data of the selected vehicles in one calendar day.

   Weekly Report

   The report to be generated will show the data of the selected vehicles in one calendar week.

   Monthly Report

   The report to be generated will show the data of the selected vehicles in one calendar month.

   Custom Time Interval

   The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

   Time

   The data of the selected period will be shown in the report.

   - For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
   - For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).

- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

Event Type

By default, all event types are selected.

You can click to select the events whose detection times will be calculated.

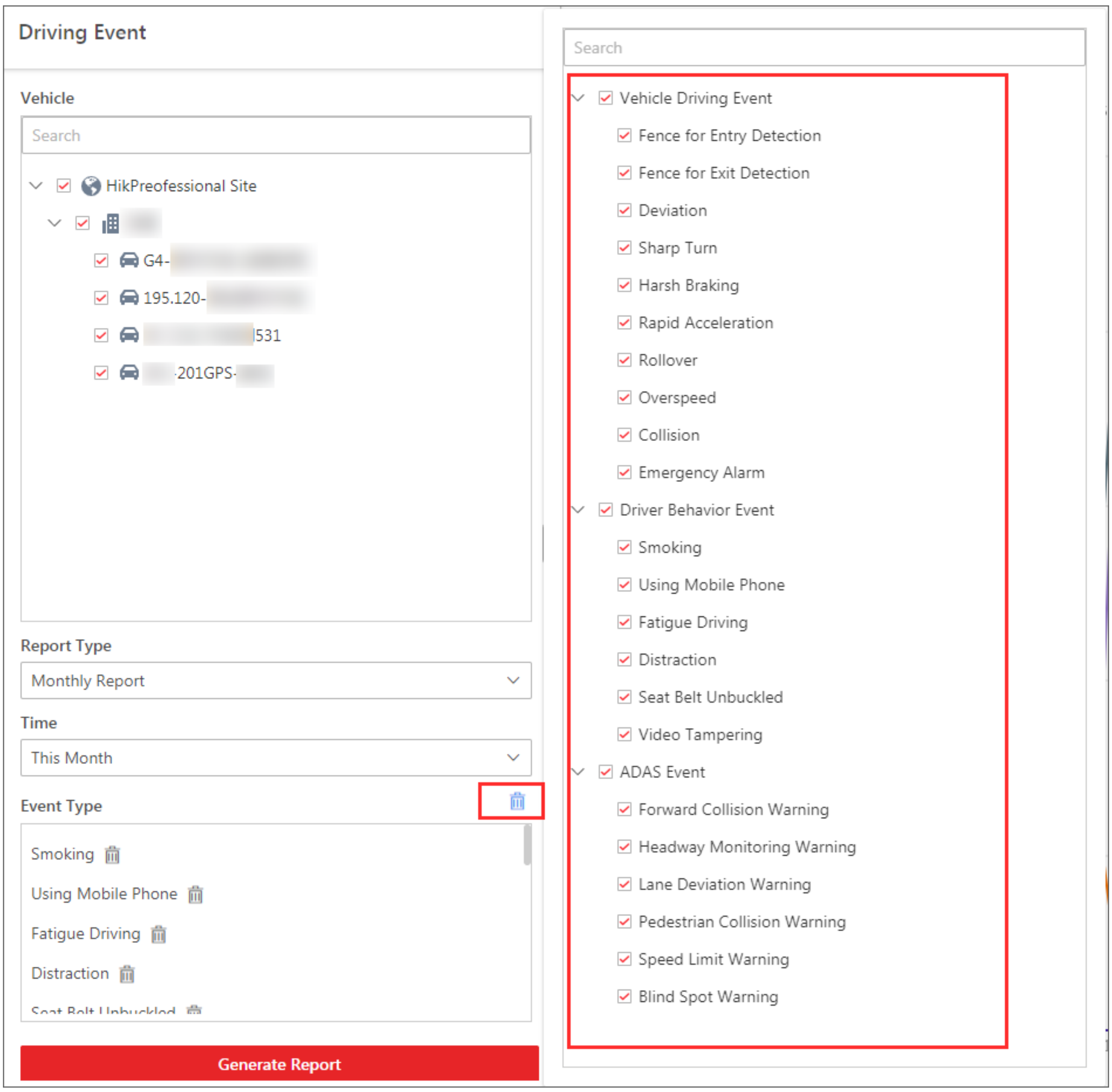


Figure 27-40 Select Events

3. Click **Generate Report**.

   The data will be shown in a line chart on which the Y-axis represents the number of events and the X-axis the time.

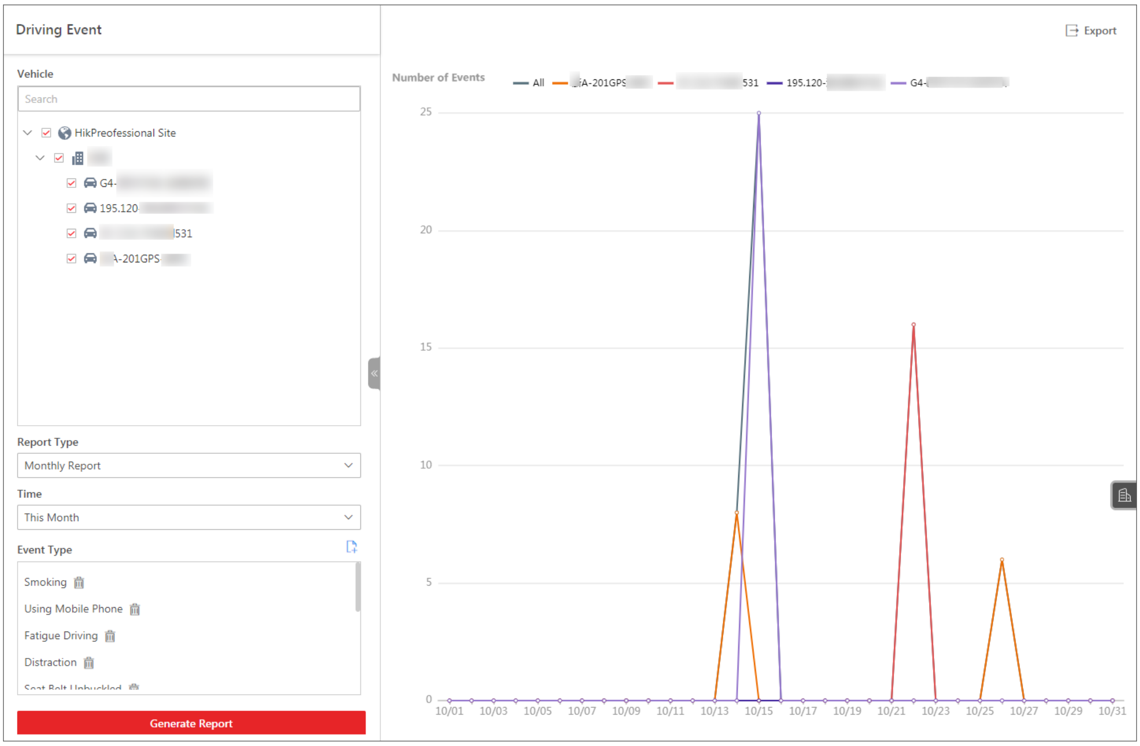


Figure 27-41 View Data in Line Chart

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.
Export Report	Click **Export** to open the Export pane, and then set parameters to export the report to your local PC.

27.10.8 Generate a Fuel Consumption Analytics Report

You can generate a fuel consumption analytics report to view the fuel consumption of specific vehicles or drivers in a certain period.

Steps

Note

Fuel consumption analytics reports can only be generated with fuel level monitoring enabled and the related parameters configured. For details, see ***Configure Fuel Level Monitoring Parameters*** .

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Fuel Consumption Report** .

2. Set search conditions.

Analysis Type

Select vehicle or driver as the analysis type and select vehicles/drivers from the list accordingly.

Report Type

Select a report type.

Daily Report

The report to be generated will show the fuel consumption of the selected vehicles/drivers in one calendar day.

Weekly Report

The report to be generated will show the fuel consumption of the selected vehicles/drivers in one calendar week.

Monthly Report

The report to be generated will show the fuel consumption of the selected vehicles/drivers in one calendar month.

Custom Time Interval

The report to be generated will show the fuel consumption of the selected vehicles/drivers in a custom period of no more than 31 days.

Time

Fuel consumption in the selected time period will be shown in the report.

- For **Daily Report**, you can select from **Today**, **Yesterday**, and **Custom Time Interval** (any calendar day).
- For **Weekly Report**, you can select from **Current Week**, **Last Week**, and **Custom Time Interval** (any calendar week).
- For **Monthly Report**, you can select from **Current Month**, **Last Month**, and **Custom Time Interval** (any calendar month).
- For reports of a custom time interval, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

The report will be shown on the right side of the page.

Note

By default, data will be shown in a line chart, of which the y-axis is the overall fuel consumption value of all selected vehicles/drivers and the x-axis is the time. A table listing the statistics for each vehicle/driver is shown below the line chart.

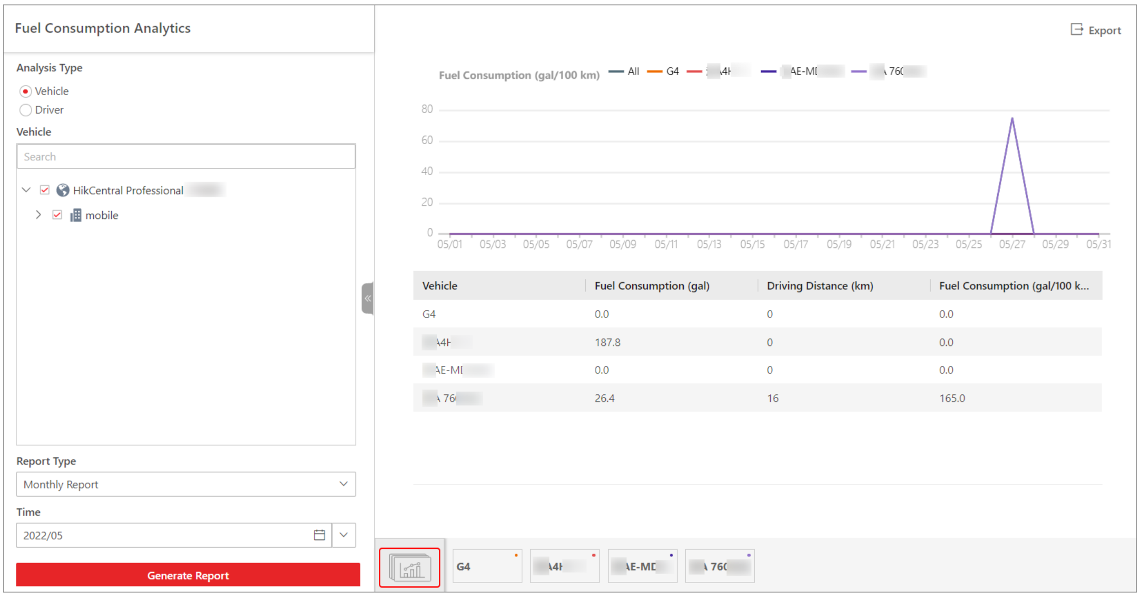


Figure 27-42 Monthly Report Example

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

View Fuel Consumption of a Specific Vehicle/ Driver	Click the name of a specific vehicle/driver at the bottom and select the **Fuel Consumption** tab on top. Hover the cursor over the line chart to view the fuel consumption value of specific time points and the average consumption value of the selected time period. Data such as total fuel consumption, total driving distance, and fuel consumption per 100 kilometers are shown above the chart.
View Fuel Level Change of a Specific Vehicle	Click the name of a specific vehicle at the bottom and select the **Fuel Level Change** tab on top. Hover the cursor over the line chart to view detailed information of specific time points, including the specific report time, license plate number, driver, fuel level, fuel quantity, and GPS information. Click a point on the chart to pinpoint the vehicle's report location on the map above.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles/drivers, time, report content, and file format.

27.10.9 Generate a Passenger Counting Report

You can generate a passenger counting report to view the number of passengers who got on/off in a specific period.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Passenger Counting Report** .
2. Set search conditions.

   Analysis Type

   Select vehicle or stop as the analysis type and select vehicles/stops from the list accordingly.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the data of the selected vehicles in one calendar day.

   Weekly Report

   The report to be generated will show the data of the selected vehicles in one calendar week.

   Monthly Report

   The report to be generated will show the data of the selected vehicles in one calendar month.

   Custom Time Interval

   The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

   Time

   The data of the selected period will be shown in the report.

   - For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
   - For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
   - For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
   - For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.
3. Click **Generate Report**.

   By default, the data will be shown in a line chart on which the Y-axis represents the number of passengers and the X-axis the time.

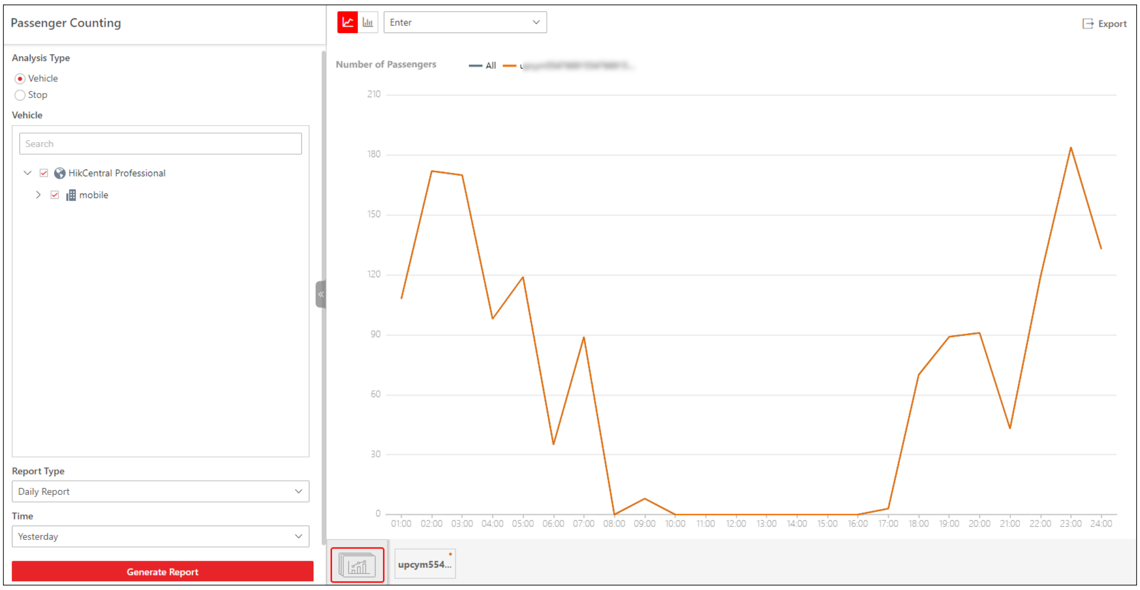


Figure 27-43 Generate a Passenger Counting Report

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

Switch Chart Mode	Click to switch the chart mode to histogram.
View Detailed Data	Hover the cursor onto the chart to view detailed data of the selected vehicles/stops at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the chart to show/hide it.
Filter by Passenger Movement Direction	Click the drop-down list on the top of the chart to select a passenger movement direction (Enter, Exit, Enter and Exit) to filter the data.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles/stops, time, and file format.

27.10.10 Generate a Device Online Rate Report

You can generate a report to view the online rate of the on-board devices mounted on the selected vehicles in a specific period.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Device Online Rate Report** .
2. Set search conditions.

   Vehicle

   Select vehicles from the areas listed below.

Note

Up to 20 vehicles can be selected.

Report Type

Select a report type.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

The data will be shown in a line chart on which the Y-axis represents the devices' online rate and the X-axis the time.

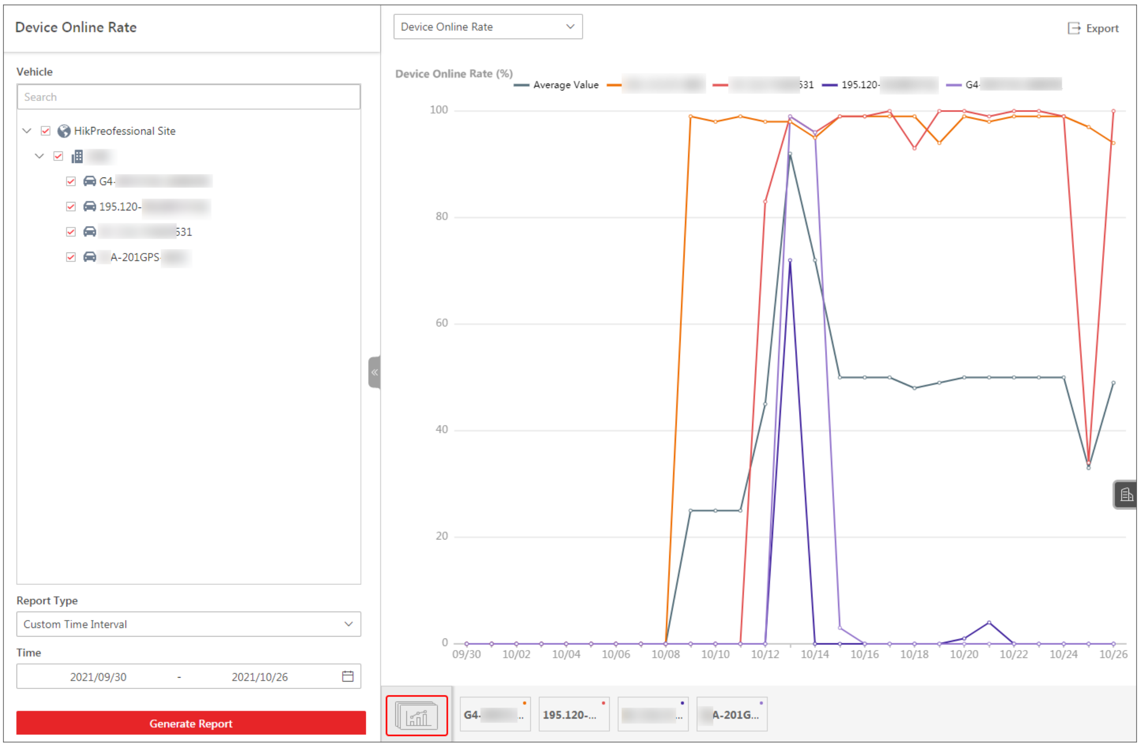


Figure 27-44 View Data in Line Chart

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

Switch Data Type	Select a data type (device online rate, online duration, or offline times) from the drop-down list on the top of the chart to display the selected type of data.
View Detailed Data	Hover the cursor onto the chart to view detailed data of the selected vehicles at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the chart to show/hide it.
Filter by Vehicle	Click a vehicle at the bottom of the chart to view the data of the vehicle in the selected period.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles, time, and file format.

Chapter 28 Portable Enforcement Management

In the Portable Enforcement module, you can apply person information to dock stations and search for device receiving records after the persons receive portable devices. Also, you can monitor in real time the locations of persons who have received portable devices, search for person's historical moving path on the map in a specific time duration, and search for files on the portable devices.

In the top left corner of the Web Client, Go to → **Portable Enforcement** → **Portable Enforcement** to enter the this module.

28.1 Flow Chart of Portable Enforcement

Refer to the following flow chart for using the Portable Enforcement module for the first time.

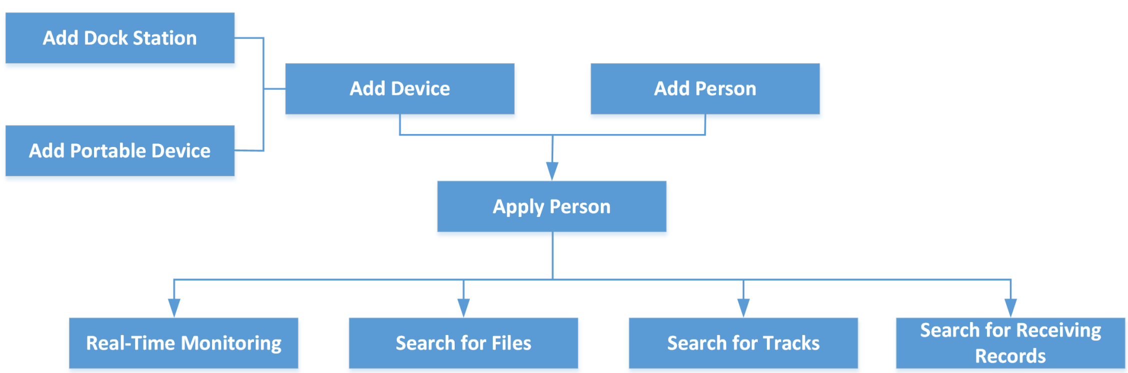


Figure 28-1 Flow Chart of Portable Enforcement

- **Add Device**: Add dock stations and portable devices to the platform. For details, refer to ***Manage Dock Station*** and ***Manage Portable Device*** .
- **Apply Person**: Apply the person information to the dock stations. For details, refer to ***Apply by Person*** and ***Apply by Department*** .
- **Real-Time Monitoring**: Monitor the person with the portable device on the map in real-time. For details, refer to ***Real-Time Monitoring*** .
- **Search for File**: Set conditions to search for files on portable devices. For details, refer to ***Search for Files on Portable Devices*** .
- **Search for Track**: Set conditions to search for person's historical tracks. For details, refer to ***Search for Historic Track*** .
- **Search for Receiving Records**: Set conditions to search for the records of receiving portable devices. For details, refer to ***Search for Receiving Records*** .

28.2 Basic Configuration

In the Basic Configuration module, you can configure basic parameters and cluster intercom.

Go to → **Portable Enforcement → Portable Enforcement → Basic Configuration** .

28.2.1 Basic Parameter Configuration

You can configure basic parameters such as distant unit and GPS data retention period for the portable enforcement module.

Steps

1. Select **Basic Parameter Configuration** on the left panel.
2. Configure the parameters.

    Distance Unit

    Select **Kilometer (km)** or **Mile (mi)** as the distance unit according to actual needs.

    GIS Map

    Click **Edit Configuration**, enable **GIS Map** and configure online or offline GIS map. For online GIS map, enter the API URL of the GIS map; for offline GIS map, configure the map beforehand and upload the file to the platform.

    Show GIS Map

    Enable/disable GIS map display as needed for the portable enforcement real-time monitoring page.

    GPS Data Retention Period

    The retention period of the GPS data. Select from the drop-down list to set the retention period.
3. Click **Save** to save the above settings.

28.2.2 Group Intercom Configuration

You can configure person groups for group intercom. In the same group intercom, persons can listen and speak to each other. Up to 128 groups can be added and up to 100 persons can be added to each group.

Steps

1. Select **Group Intercom Configuration** on the left panel.
2. Click + on the left of the page to add a group intercom group.
3. On the pop-up pane, configure the following parameters.

    Group Name

    Enter a group name of the group intercom as required.

Streaming Server

If this parameter is enabled, select a server from the drop-down list.

Group Person

Click and check persons from different apartments. Click **Add**.

4. Click **Add** to add the group intercom group.

   The list of added group intercom group(s) will be displayed on the left.

5. **Optional:** For added group intercom groups, you can delete them or edit the name, group members, etc. as needed.

28.3 Real-Time Monitoring

On the Real-Time Monitoring page, you can monitor the person with portable device on the map in real-time. The supported operations include getting the person's real-time location, viewing the person's real-time moving path, receiving the real-time alarm from the person, etc.

Go to → **Portable Enforcement** → **Portable Enforcement** → **Real-Time Monitoring** . Select a person in the list, and refer to the following for the supported operations on this page.

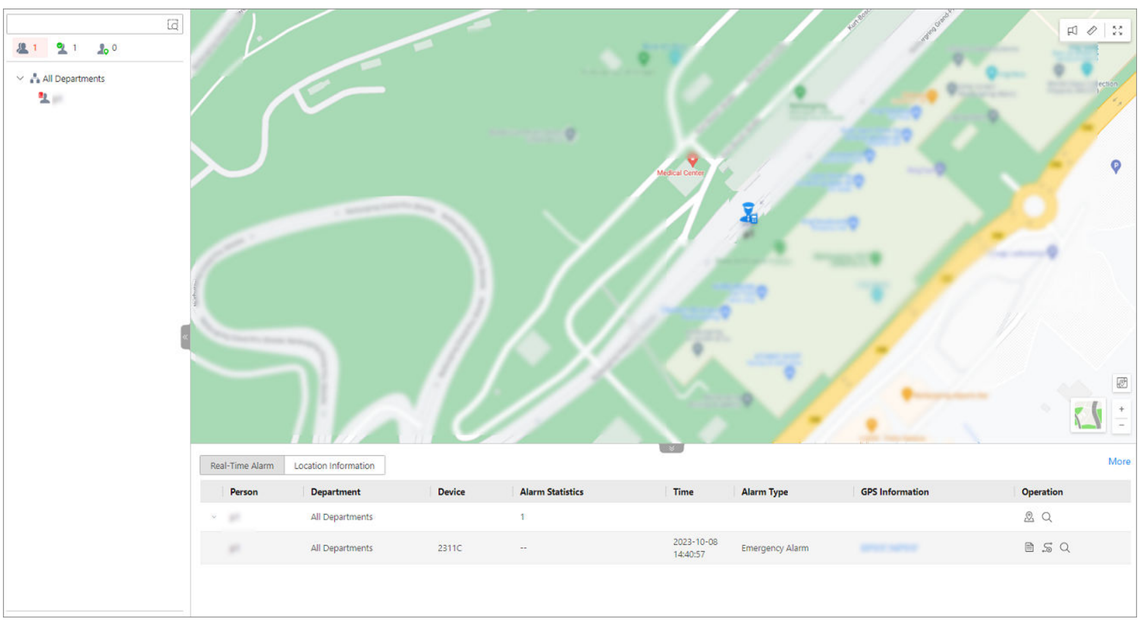


Figure 28-2 Real-Time Monitoring

Note

For many retail scenarios without GPS information indoors, the Web Client also supports real-time monitoring in GPS free mode. Click **Configure Now** on the top and turn off the GIS map display. After it is disabled, the section of GIS map on this page will be hidden. The configuration will be remembered next time you log in.

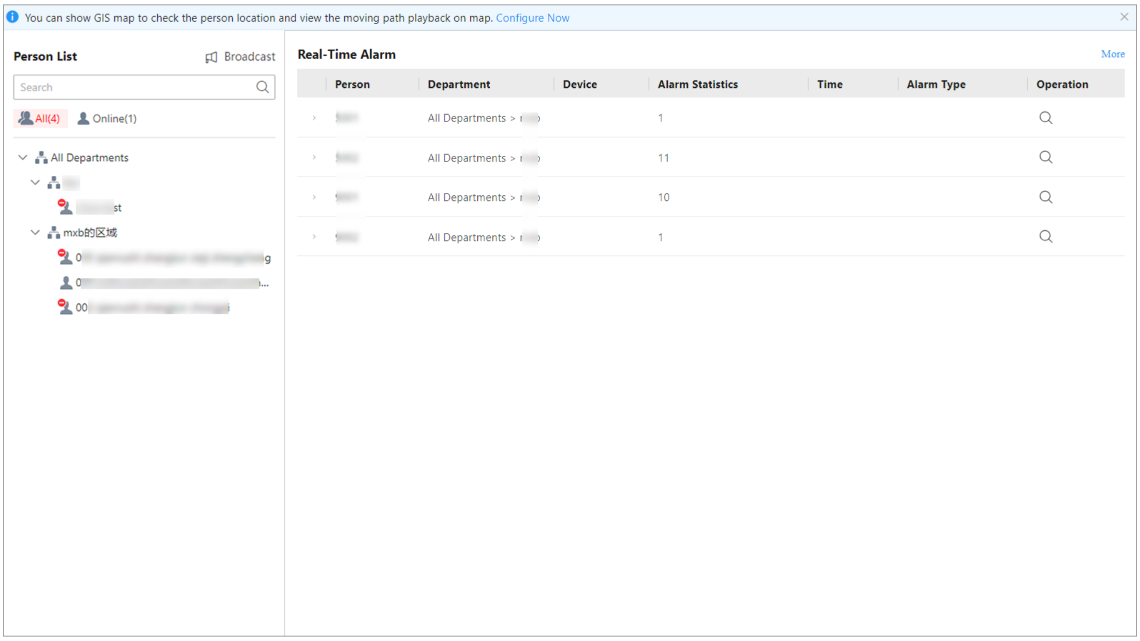


Figure 28-3 Real-Time Monitoring Without GIS Map

- **Search for Person**: Search for the target person(s) by entering keywords in the search box.
- : Search for the target person(s) by drawing an area. During search, you can locate person(s) and broadcast to person(s).
- **View Person Details**: View person's profile picture, department, battery capacity of the portable device, phone number, location information, etc.
- / : Locate or cancel locating the person on the map.
- : Make the person in the center of the view.
- **Play Video**: View the live view of the person.
- **Two-Way Audio**: Start two-way audio with the person.
- **Track in Real Time**: View the real-time moving path of the person.
- **Play Back Track**: View the history moving path of the person during the selected time period. You can view the video on the right side if it is recorded.
- : Start broadcasting to the person.
- : Measure the distance on the map.
- : View real-time monitoring in full screen.
- **Real-Time Alarm**: View the real-time alarm uploaded by the person. You can view the alarm type, alarm time, GPS information, etc.
- **Location Information**: View person's detailed longitude and latitude information, which will be refreshed every 10 seconds by default (the refresh frequency can be edited on the device). You can check **Auto Get Location** to get person's location information automatically.

28.4 Search for Historic Track

You can set conditions to search for persons' history tracks. After searching, you can play back track and export track information.

Before You Start

- Make sure the person information has been applied to the dock station. For details, refer to ***Apply by Person*** and ***Apply by Department*** .

Steps

1. Go to → **Portable Enforcement** → **Portable Enforcement** .
2. Select **Track Search** on the left panel.
3. Set the time range for search.
4. Click to select person(s).
5. Click **Search**.

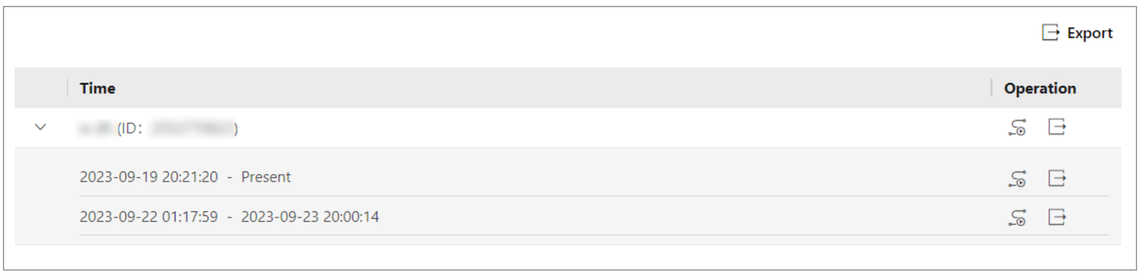


Figure 28-4 Search Result

The search results are displayed on the right side.

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

Play Back Person's Track	Click in the Operation column to play back all tracks of a person, or the track in a specific time duration of a person on the map. If there is any video recorded, You can view the video on the right side of the page and person's moving direction on the map. During track playback, you can perform the followings on the map: click **Stop** to stop playing back person's track; click to start broadcasting; click to measure the distance of track; click to view the track in full screen. During track playback, you can perform the followings on the bottom toolbar: click **Skip No-Recording Time** to skip the no-recording time of the video; click **Switch Time** to switch to another time period for viewing playback; click **Center Person** or **Cancel Centering Person** to center or cancel centering the person on the map.

Export Track Information	Click in the Operation column to export all tracks of a person, or the track in a specific time duration of a person to local PC. Click **Export** in the upper-right corner to export all tracks of all persons to local PC.

28.5 Apply Person

You should apply person information to the dock stations, so that the corresponding person can receive and use the portable device on the dock station. You can apply by person or by department. After application, you can have an overview of application. For persons who failed to be applied, you can reapply them.

28.5.1 Application Overview

You can have an overview of person application records of all departments or a certain department, including the number of persons who are applied, the number of persons failed to be applied, etc. For the persons failed to be applied, you can reapply them to the dock stations. Also, you can edit the linked dock station of the person, link the person with the unique portable device, etc.

Select **Application Overview** on the left navigation bar.

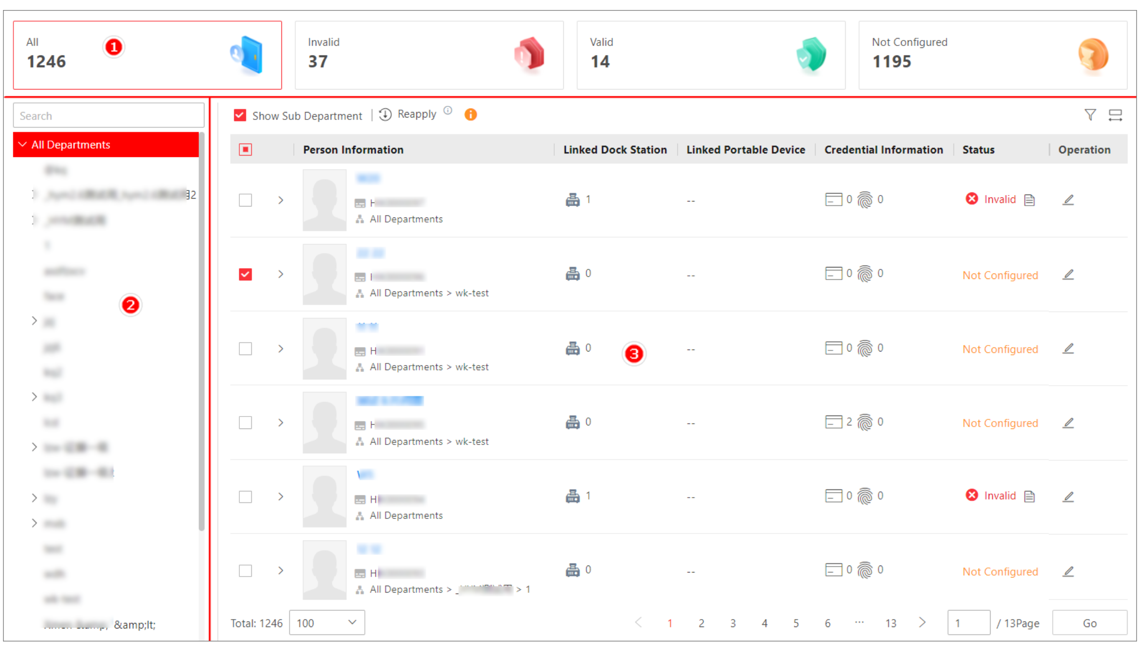


Figure 28-5 Application Overview

Table 28-1 Introduction of Application Overview Page

No.	Introduction
1	View the number of persons in different status. • **All**: The number of all persons added to the platform. • **Invalid**: The number of persons that failed to be applied to the dock stations. • **Valid**: The number of persons that are applied to the dock stations. • **Not Configured**: The number of persons that have not been applied to the dock stations.
2	Select a department in the list to view the application records of persons in this department.
3	View person application details and perform the following operations if needed. • Check **Show Sub Department** to display person application details in sub departments. • Check persons whose status is **Invalid**, and click **Reapply** to reapply these persons to the dock stations. • Click in the upper-right corner and set conditions to search for the related application records. • Click in the upper-right corner to select the type of self-adaptive column width (complete or incomplete display of each column title). • Click a person name in the Person Information column to enter the person information page. • Click in the Operation column to edit the linked dock station of the person. You can switch on **Link to Unique Portable Device** and select a portable device in the list to link the person with the portable device. The linked portable device will be displayed in the list of person applying information, as well as on the application overview page. **Note** represents that the dock station is offline. • Click beside the person profile to view the details of linked dock stations including device name and IP address.

28.5.2 Apply by Department

You can select a department and apply the information of persons in the selected department to dock stations. After applying, you can view the application details, unlink the dock station with the department, etc.

Before You Start

- Make sure you have added dock stations to the platform. For details, refer to ***Manage Dock Station*** .

Steps

1. Select **Apply by Department** on the left navigation bar.
2. **Optional:** Select a department on the left.
3. Link department(s) to dock station(s).
   - Click **Link to Dock Station**, select dock station(s), and click **OK**.

   Note

   represents that the dock station is offline.
   - Click **Batch Link**, select departments and dock station(s), and click **OK**.

   The persons in the selected department(s) are applied to the selected device(s). You can view the applying results. If applying failed, you can view the failure details.
4. **Optional:** Perform the following operations.

Unlink Dock Station With Department	Select one or more dock stations, and click **Unlink** to unlink the dock stations with department(s). Move the mouse cursor to , and click **Unlink All** to unlink all dock stations with departments.
Search for Dock Station	Enter keywords in the search box in the upper-right corner to search for dock stations.
View Failed Applying Details	If there are failed applying records, will be displayed beside **Link to Dock Station**. You can hover over and click **View Details** to view the failure details.
Set Self-Adaptive Column Width	Click to select the type of self-adaptive column width (complete or incomplete display of each column title).

28.5.3 Apply by Person

You can select persons and apply the information of selected persons to the dock stations. After applying, you can edit the linked dock station of the person, view application details, etc.

Before You Start

- Make sure you have added dock stations to the platform. For details, refer to ***Manage Dock Station*** .

Steps

1. Select **Apply by Person** on the left navigation bar.
2. Click **Add Linked Person** to pop up the Add Linked Person panel on the right side.
3. Click to select person(s).
4. Select dock station(s).

Note

represents that the dock station is offline.

The selected person(s) are applied to the selected device(s). You can view the applying results. If applying failed, you can view the failure details.

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

Edit Linked Device(s)	Click in the Operation column to enter the Device Configuration pane. • Edit the linked dock station. • Enable/disable **Link to Unique Portable Device**. After it is enabled, select a portable device for a unique linkage between the specific device and person. The linked portable device will be displayed in the list of person applying information, as well as on the application overview page.
View Application Details	View person information such as person name, department, and the number of linked dock stations. Click beside the person profile to view the details of linked dock stations including device name and IP address.
Delete Person	Check one or more persons, and click **Delete Person** to delete the selected persons. Move the mouse cursor to , and click **Delete All Persons** to delete all persons.
View Applying Failed Details	If there are applying failed records, will be displayed beside **Add Linked Person**. You can move the mouse course to and click **View Details** to view the failure details.
Set Self-Adaptive Column Width	Click in the upper-right corner to select the type of self-adaptive column width (complete or incomplete display of each column title).
Search for Application Records	Click in the upper-right corner and set conditions to search for the related application records.

28.6 Search for Receiving Records

After the persons receive portable devices, you can set conditions to search for receiving records. You can either search by person or by device. For the search result(s), you can export them as needed.

On the left pane of the Portable Enforcement module, select **Receiving Record**.

For search results, you can perform the following operations as needed:

- Click and select a self-adaptive column width mode.
- Click and select display items like the name of portable device, person ID, dock station of receiving/returning, battery when receiving/returning, department, receiving time, return time, etc. as needed. By default, all supported column items are selected. You can click **Reset** to reset the selected items.

28.6.1 Search for Receiving Records by Person

You can select persons and set other conditions to search for receiving records.

Before You Start

- Make sure you have added portable devices to the platform. For details, refer to ***Manage Portable Device*** .

Steps

1. On the left pane of the Receiving Record page, select **Receiving Record by Person**.
2. **Optional:** Set the search conditions including receiving time, return status, and person range.
3. Click **Search**.

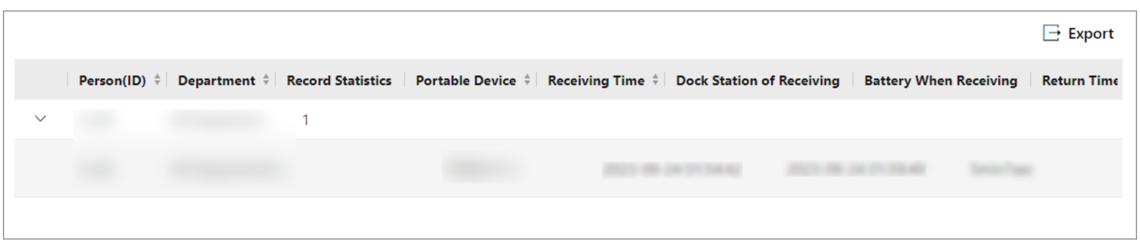


Figure 28-6 Search for Receiving Records by Person

The search results are displayed on the right side.

4. **Optional:** Click **Export** in the upper-right corner to export the receiving records to local PC.

28.6.2 Search for Receiving Records by Device

You can select devices and set other conditions to search for receiving records.

Before You Start

- Make sure you have added portable devices to the platform. For details, refer to ***Manage Portable Device*** .

Steps

1. On the left pane of the Receiving Record page, select **Receiving Record by Device**.
2. **Optional:** Set the search conditions including receiving time, return status, and device.
3. Click **Search**.

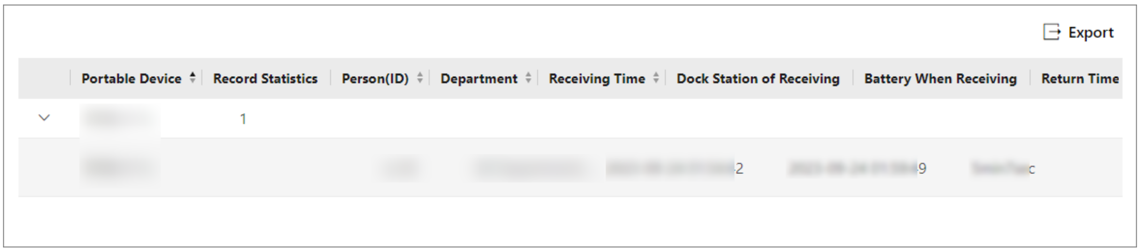


Figure 28-7 Search for Receiving Records by Device

The search results are displayed on the right side.

4. **Optional:** Click **Export** in the upper-right corner to export the receiving records to local PC.

28.7 Search for Files on Portable Devices

You can set conditions such as file type, searching dimension, and time to search for files on portable devices. For the searched files, you can mark files as important, save files to the evidence management center, export files, etc.

Steps

1. On the left pane of the Portable Enforcement module, select **File Search**.
2. Set the search conditions including file type, searching dimension, time, and the corresponding device(s)/person(s).

Note

For searching by persons, up to 200 persons are allowed.

3. Click **Search**.

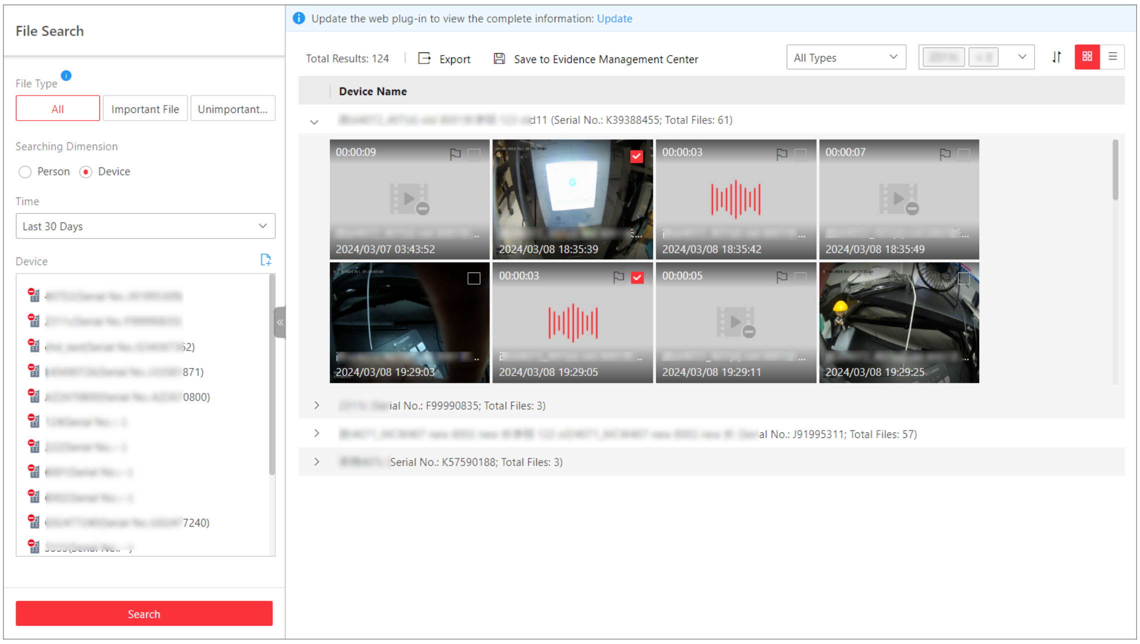


Figure 28-8 Search Results by Device

The search results are displayed and sorted by person/device on the right side. Click › to expand the list of files under certain person/device. You can view the file name, file time/ duration, and total files of each person/device.

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

Filter Search Results	Click **All Types** to filter the search results by type (Video, Audio, or Picture). Next to **All Types**, click ⌄ to check person(s)/device(s) to be displayed.
Switch View Mode	Click or in the upper right corner to view the search results in thumbnail or list mode.
Mark as Important File	On the top right corner of a file, click to mark the file as the important file. You can also click a file to enter the file details pane, and click on the top to mark the file as the important file.
View File Details	Click a file to view its related video, picture, or audio; its basic information including person/device name, time range, and file backup location, etc.; and its location information.

Note

Click to unlock the file; and click to view the details in a pop-up window.

Play Video in Order	Click a video file and check **Play in Order** to play the video files continuously in order. The pictures and audios will be skipped.
Save File to Evidence Management Center	Select one or more files, click **Save to Evidence Management Center**, configure the parameters such as adding mode and file tag, and click **OK** to save the selected files to the evidence management center.
Export File	Select one or more files, click **Export**, and select the file type (MP4 or AVI) to export the selected files to the local PC.

Chapter 29 Intelligent Analysis Report

Reports, created for a specified period, are essential documents, which are used to check whether a business runs smoothly and effectively. In HikCentral Professional, reports can be generated daily, weekly, monthly, annually, and by custom time period. The reports can also be added to the dashboard for browsing at a glance. You can use reports as basis in creating decisions, addressing problems, checking tendency and comparison, etc.

In the top left corner of the Web Client, select → **Operation Analytics** → **Intelligent Analysis** to enter the this module.

29.1 Flow Chart of Intelligent Analysis Report in Retail/Supermarket Scenario

The following flow chart shows the process of configurations and operations required for intelligent analysis reports in retail or supermarket scenario.

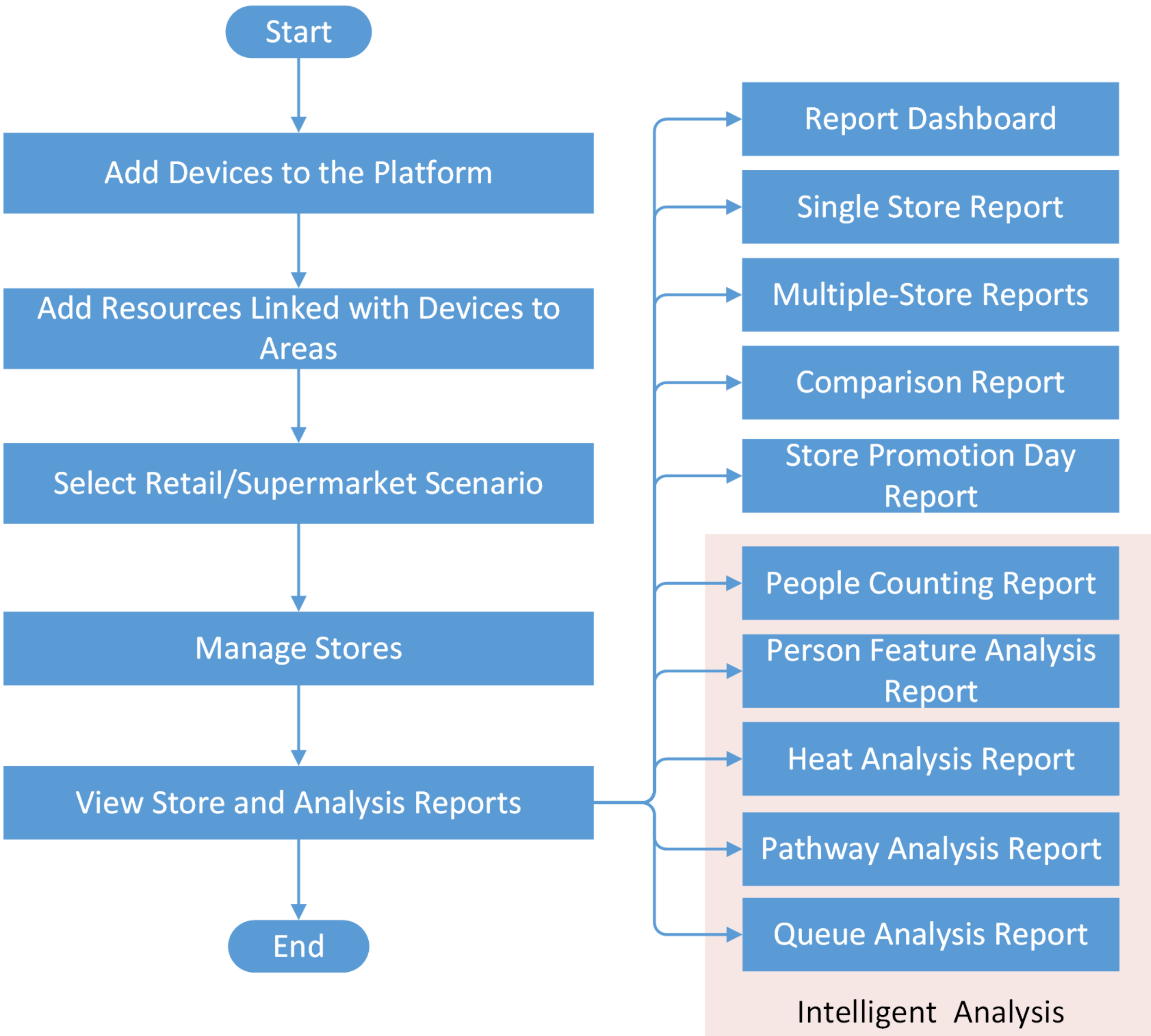


Figure 29-1 Flow Chart of Intelligent Analysis Report in Retail/Supermarket Scenario

Table 29-1 Flow Chart Description

Procedure	Description
Add Devices to the Platform	Add devices that support specific detection functions to the platform by different methods (e.g., online detection, IP address, port segment, device ID) for generating statistics reports.
Add Resources Linked with Devices to Areas	Group resources linked with devices to different areas according to the locations of the devices for convenient management.

Procedure	Description
Select Retail/Supermarket Scenario	The scenario is specially designed for stores. In this scenario, you can view reports of a store or multiple stores. For details, see ***Configure Scenario*** .
Manage Stores	Add stores to the platform and link resources to stores for generating reports of stores. For details, see ***Manage Store*** .
View Store Reports	View store reports of a single store / two stores / multiple stores and store intelligent analysis reports (including people counting reports, person feature analysis reports, heat analysis reports, pathway analysis reports, and queue analysis reports). For details, refer to ***View Store Report*** and ***View Store Intelligent Analysis Report*** .

29.2 Flow Chart of Intelligent Analysis Report in Public Scenario

The following flow chart shows the process of configurations and operations required for intelligent analysis reports in public scenario.

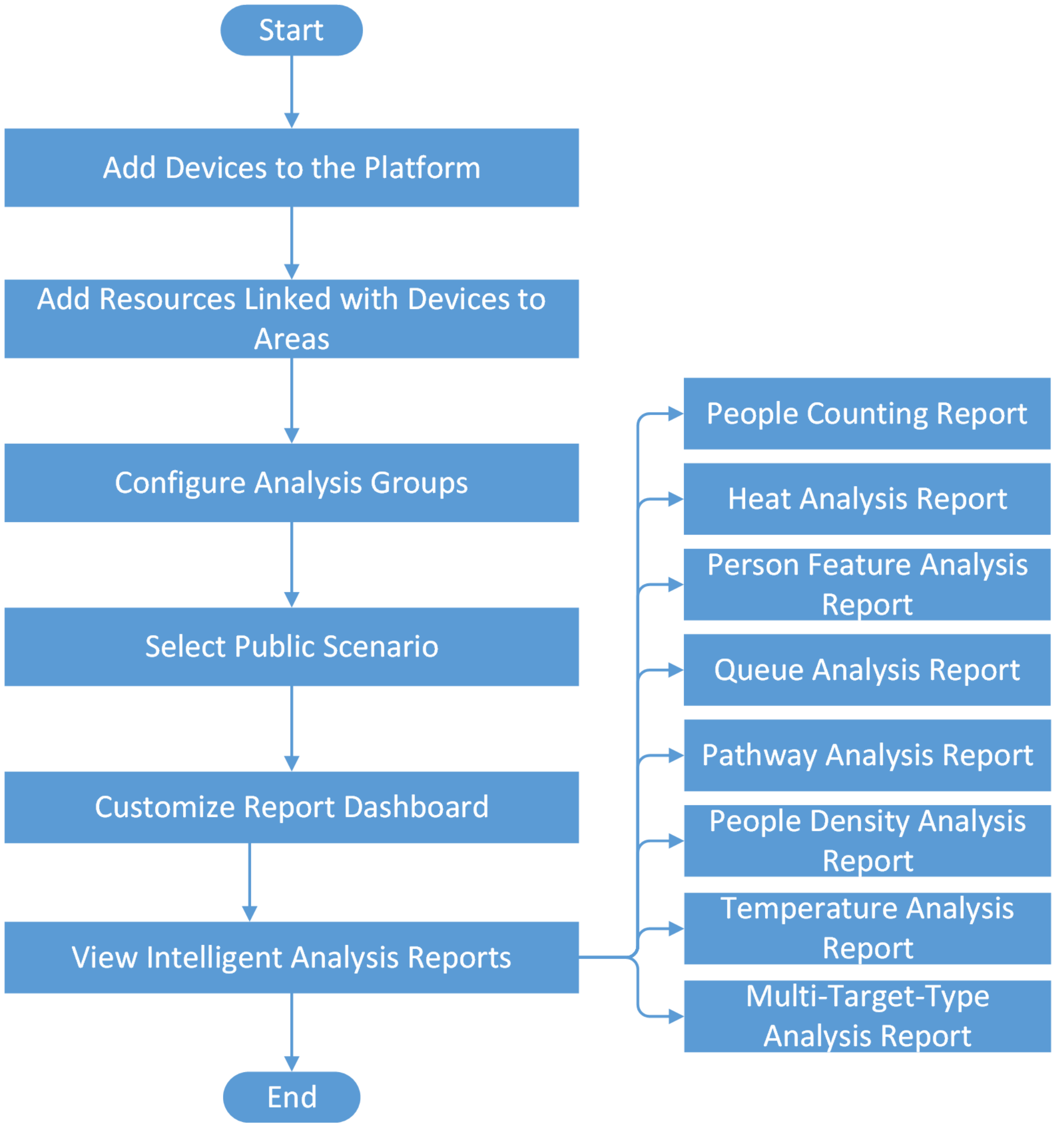


Figure 29-2 Flow Chart of Intelligent Analysis Report in Public Scenario

Table 29-2 Flow Chart Description

Procedure	Description
Add Devices to the Platform	Add devices that support specific detection functions to the platform by different methods (e.g., online detection, IP address, port segment, device ID) for generating statistics reports.
Add Resources Linked with Devices to Areas	Group resources linked with devices to different areas according to the locations of the devices for convenient management.
Configure Analysis Groups	Group analysis resources of certain regions for calculation.

Procedure	Description
	For details, see ***Add Analysis Group*** .
Select Public Scenario	In the non-store scenario (e.g., subway, square), you can view reports collected from an analysis group or camera about people counting, person features, heat data, etc. For details, see ***Configure Scenario*** .
Customize Report Dashboard	Customize a report dashboard for an at-a-glance view for the public scenario reports. For details, see ***Customize Report Dashboard*** .
View Intelligent Analysis Reports	View people counting reports, person feature analysis reports, heat analysis reports, pathway analysis reports, queue analysis reports, people density analysis reports, temperature analysis reports, and multi-target-type analysis reports. For details, see ***View Intelligent Analysis Report*** .

29.3 Configure Scenario

There are two scenarios available: public scenario and retail/supermarket scenario. After you switch to the other scenario, a navigation in accord with the scenario will be generated, and the platform will be refreshed and loaded to a scenario-fit status.

Public Scenario

Non-Store Scenario (e.g., Subway, Square). You can view reports collected from an analysis group or camera about people counting, person features, heat data, etc.

Retail/Supermarket Scenario

The scenario is specially designed for stores. In this scenario, you can view reports of a store or multiple stores.

Note

After you switch scenarios, the data of the previous scenario will be preserved for 30 days and then cleared.

29.4 Retail/Supermarket Scenario

The Retail/Supermarket Scenario is designed for stores in the retail industry. In the section, you can view single/two/multiple store reports. You can also view intelligent reports such as store people counting and store heat analysis reports.

On the left pane of the Intelligent Analysis module, select **Configure Scenario**.

Switch to the retail scenario.

29.4.1 View Store Report Dashboard

The report dashboard provides an at-a-glance view for stores. You can select a store or multiple stores to view reports.

Steps

1. Under the Intelligent Analysis module, select **Dashboard**.

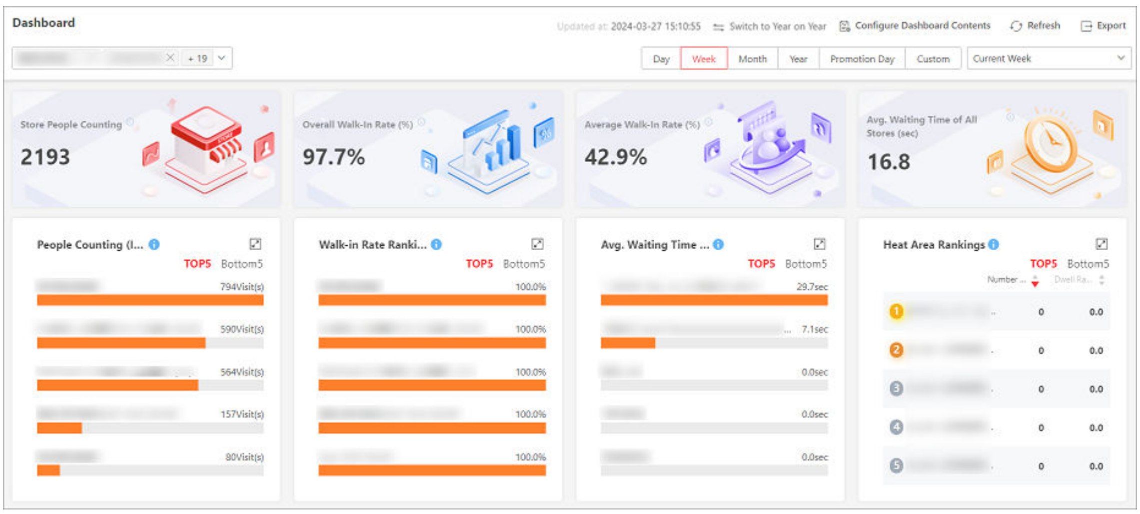


Figure 29-3 Dashboard

2. **Optional:** Select a store or multiple stores, and you can perform the following operations.

Operation	Description
Set Report Time	Click **Day**, **Week**, **Month**, **Year**, **Promotion Day** or **Custom** to select the report time.
View Dashboard/Report Meaning	Hover your cursor over or on the top right corner of a certain parameter, and you will see the explanations of the dashboard/report.
Export Dashboard	Click **Export** to export the dashboard in PDF format to the local PC. **Note** You can get the exported report in the Download Center.
Configure Dashboard Contents	Click **Configure Dashboard Contents** to select dashboard/ report contents to be displayed.

Operation	Description
Switch Between Year on Year and Cycle on Cycle	Click **Switch to Cycle on Cycle** or **Switch to Year on Year** for switching the report statistics mode.
Refresh Dashboard	Click **Refresh** to refresh the dashboard.
Zoom in Dashboard/Report	Click ⤢ to zoom in the dashboard or report.

29.4.2 Manage Store

HikCentral Professional supports people counting report and heat analysis report of stores. With the reliable data, store manager can have insight into the customer traffic, dwell rate, tendency of people amount change around promotion days, and consumers movements of stores. Before generating reports of stores, you need to add stores to the platform first, and add the resource group to stores.

Add a Single Store

You should add a store before generating reports of stores.

Steps

1. On the left pane of the Intelligent Analysis module, select **Store Management → Configure Store** .
2. Open the Add Store panel.
   - If you have not added any store yet, you can click **Add Store** on the page to open the Add Store panel.
   - If you have added stores, you can click + in the top left corner to open the Add Store panel.
3. Set store parameters.
   1) Set store name.
   2) Select an area for the store.
   3) Set business hours for the store.

   Note

   At least one and up to 5 time periods are allowed. The added business hours cannot overlap and will be sorted by start time. The list of business hours will be sorted again every time you edit a start time.

   4) Set the store location on the map, and its coordinates will be automatically generated.
   5) Select **Single Floor** or **Multiple Floors** for the store.
   6) **Optional:** Set names for each floor if you select **Multiple Floors**.
   7) Click **Save**.
4. Add resources to the store.
   1) Click an added store.
   2) Click **Configure** to open the Configure Resources page.

3) In the **Configure Resource Capability** section, click **Add** to add a device, and you can switch on/off a certain capability of the resource.

Note

- Enabling different capabilities will result in different parameters below.
- You can click **Configure** to draw the dwell area of heat analysis.

4) In the **Configure People Counting** section, click **Add** to add entries & exits.
5) **Optional:** Select entries and exits of the store for collecting store statistics.
6) **Optional:** Switch on **Regularly Clear All**, and set a time when all data will be cleared.
7) **Optional:** Switch on **Store Capacity Limit**, and when the number of people in the store exceeds the limit, you will be notified. For details, click **Configure Event and Alarm** to configure it.
8) **Optional:** Click **Configure People Counting Excluding Staff Task** to configure who will be excluded when counting people.
9) For **Deduplication Interval in Device**, click **Sync from Device** to sync the deduplication interval information from the selected resource, or click **Batch Configured and Apply** to enter a specific interval and click **Apply** to apply the interval to all.

Note

For DeepinMind device, click **Configure People Counting Excluding Staff Task** to set deduplication interval.

The device name, deduplication interval, and applying status will be displayed below.

10) Click **Save and Continue**.

5. Add resources to floor.
1) **Optional:** Select a map for the floor.
2) Select a floor under the Resource tab on the right pane.
3) Drag the resources to the left map.
4) Click **Finish**.

You will see a dashboard displaying resource status.

6. **Optional:** Perform the following operations for managing added stores.

Edit the Store Information	Select a store and click **Edit** on the right top corner to edit the store information.
Delete Store(s)	• Delete a single store: Select a store from the store list panel and click to delete it. • Batch delete multiple stores: Check multiple stores of a site and click **Delete** to delete selected stores.
Edit Opening Hours of Store(s)	• Edit opening hours of a single store:

	Select a store from the store list panel and click **Configure Opening Hours** on the store details page. Adjust the opening hour and click **Save**. • Batch edit opening hours of multiple stores: Check multiple stores of a site and click **Configure Opening Hours**. Adjust the opening hour and click **Save**. **Note** The opening hours of store(s) should be within one day.
Search Store	Enter a keyword in the search field on the upper-right corner of the page to search for the store.
View Resource Capability Status	After you add a store, click the store, and click **Resource Capability** to view resource status, including the online status and data uploading status.

Batch Add Stores

You can batch add stores by template before generating reports of stores.

Steps

Note

Make sure you have switched the scenario to Retail/Supermarket scenario. For details, refer to *Configure Scenario* .

1. In the top left corner of Home page, select → **Operation Analytics → Intelligent Analysis → Store Management → Configure Store** .
2. Open the Batch Import panel.
   - If you have not added any store yet, you can click **Batch Import** on the page to open the Batch Import panel.
   - If you have added stores, you can click in the top left corner to open the Batch Import panel.
3. Click **Download Template** to download the store template and save it to your PC.
4. In the downloaded template, enter the store information (such as store name, site, and area) following the rules shown in the template.
5. Click , and then select the template from your PC.
6. Click **OK**.

   The importing progress shows and you can check the results.
7. **Optional:** Perform the following operations for managing added stores.

Edit the Store Information	Select a store and click **Edit** on the right top corner to edit the store information.

Delete Store(s)	• Delete a single store: Select a store from the store list panel and click to delete it. • Batch delete multiple stores: Check multiple stores of a site and click **Delete** to delete selected stores.
Edit Opening Hours of Store(s)	• Edit opening hours of a single store: Select a store from the store list panel and click **Configure Opening Hours** on the store details page. Adjust the opening hour and click **Save**. • Batch edit opening hours of multiple stores: Check multiple stores of a site and click **Configure Opening Hours**. Adjust the opening hour and click **Save**. **Note** The opening hours of store(s) should be within one day.
Search Store	Enter a keyword in the search field on the upper-right corner of the page to search for the store.
Edit Configuration of Resource Capability and People Counting	After you add a store, click the store, and select **Resource Capability**/ **Floor Configuration** to edit the resource status, people counting parameters, resources of floors, etc.

Configure Promotion Day

After setting promotion days, you can get the customer traffic on promotion day so as to analyze how many customers the promotions bring more than the days without a promotion.

Steps

1. In the top left corner of Home page, select → **Operation Analytics → Intelligent Analysis → Store Management → Configure Promotion Day** .
2. Click **Add** to open the promotion day configuration page.

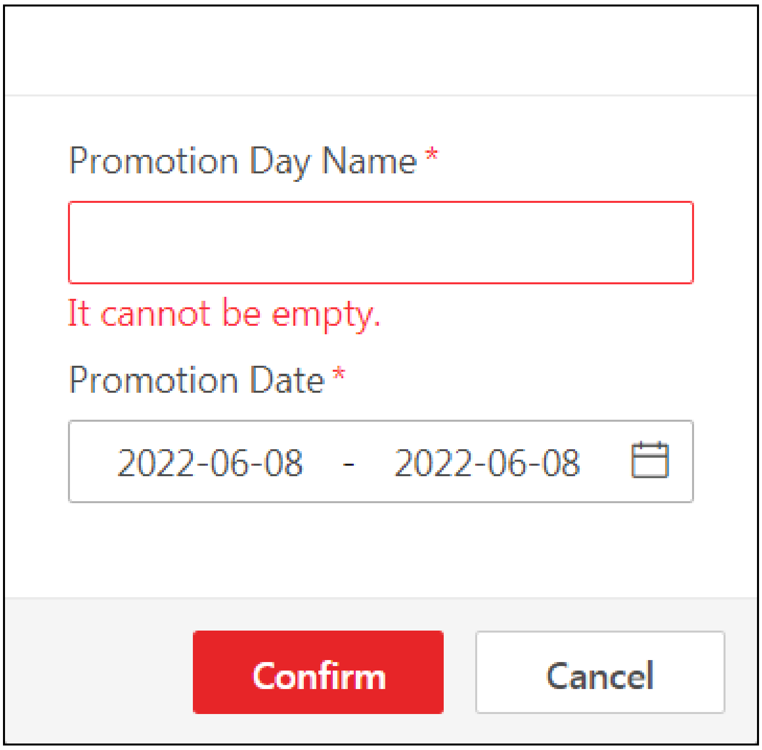


Figure 29-4 Promotion Day Configuration

3. Enter the promotion day name.
4. Set the promotion duration.

Note

The promotion time period should be within 30 days.

5. Click **Confirm** to finish adding a promotion day.
6. **Optional:** Perform the following operations after adding promotion days.

Edit a Promotion Day	Click the promotion day name to open the promotion day configuration pane, and edit the promotion day information.
Delete Promotion Days	Check one or multiple promotion days, and click **Delete** to delete the selected promotion days.
Search Promotion Days	Enter a keyword in the search field to search for promotion days.

Send Store Analysis Report Regularly

You can set scheduled reports to designated recipients.

Steps

1. In the top left corner of Home page, select → **Operation Analytics → Intelligent Analysis → Store Management → Scheduled Report** .
2. Open the Create Report panel.
   - If you have not added any scheduled report yet, you can click **Add** on the page to open the Create Report panel.
   - If you have added stores, you can click + in the top left corner to open the Create Report panel.
3. Set basic information such as report name, report type, report language.
4. Set the report contents.

   Statistical Object

   Select the available stores as the report statistics targets.

   Note

   Up to 32 targets are supported in one report.

   Dwell Duration

   For example, if you set the dwell duration as > 15s, then when a person stays in an area for over 15 seconds, they will be considered as dwelling within the area.

   Queuing Duration

   For example, if you set it as Range 1 < 300 < Range 2 <600 < Range 3, then you can view reports about the number of queuing people who waited for less than 300 sec / from 300 to 600 sec / more than 600 sec.

   Number of Queuing People

   For example, if you set it as Range 1 < 5 < Range 2 <10 < Range 3, then you can view reports about the distribution of queues whose number of people are less than 5 / from 5 to 10 / more than 10.
5. Set time settings which define how often and when the report will be sent to the recipient. For example, if you select By Week, Recent 7 Days, and Send at Sunday 06:00, then the recent 7 days store report will be sent to you weekly at every Sunday 6:00.
6. In the Advanced Settings section, perform the following operations as you need.
   1) Switch on **Send via Email**, and select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add** to add a new email template.

   2) Switch on **Upload to SFTP**, and click **Configure** beside **Saving Path** to configure the SFTP settings, including SFTP address, port number, user name, password, and saving path.

Note

If you have configured the SFTP settings, you can click → **Configure SFTP** in the top left corner to edit SFTP settings. For details, refer to the table below.

3) Switch on **Save to Local Storage**, and click **Configure** beside **Saving Path** to configure the saving path of local storage.

Note

If you have configured the local storage, you can click → **Configure Local Storage** in the top left corner to edit the saving path of local storage. For details, refer to the table below.

7. Click **Add**.
8. On the left pane, you can see all scheduled reports you added. You can perform the following operations.

Operation	Description
Edit Report	Click the name of a certain report, and you can edit the report.
Delete Report	Select a store, and click in the top left corner to delete the store.
Configure SFTP / Local Storage	Click in the top left corner to configure SFTP or Local Storage. • Click **SFTP Settings** to configure the SFTP settings, including SFTP address, port number, user name, password, and saving path. • Click **Configure Local Storage** to set the local saving path.

29.4.3 View Store Report

If you choose the Retail/Supermarket scenario, you can view store reports of a single store, two stores, and multiple stores.

Under the Intelligent Analysis module, select **Store Report**.

View Single Store Report

You can view reports of a single store.

Select **Single Store Report** on the left.

On the top of the page, the set contents are displayed. Hover your cursor on the top right corner of a certain parameter, and you will view the explanations of the parameters.

In the People Counting Trend section, you can view the daily and hourly trend of people counting (in), people counting (in + passby), and walk-in rate, etc.

In the People Counting Details section, you can view data collected from each floor and their rankings.

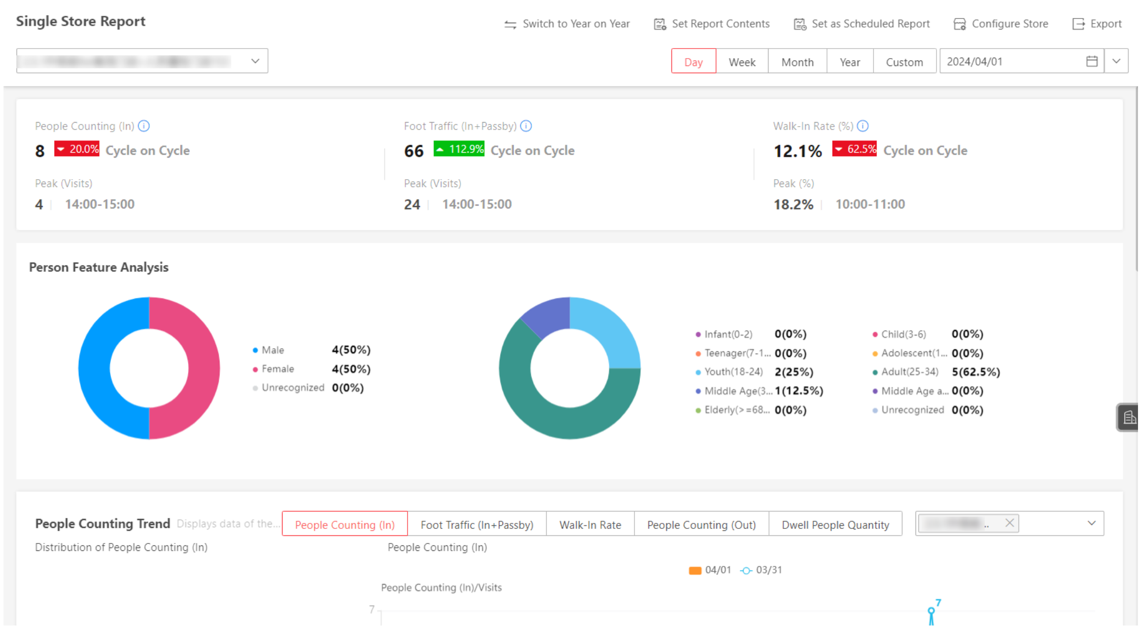


Figure 29-5 Single Store Report

You can perform the following operations.

Operation	Description
Select Store	Click to select a store.
Set Report Time	Click **Day/Week/Month/Year/Custom** to select the report time.
View Parameter Meaning	Hover your cursor over on the top right corner of a certain parameter, and you will view the explanations of the parameter.
Switch Between Year on Year and Cycle on Cycle	Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways. **Note** For exporting reports, year on year statistics and cycle on cycle statistics will be both exported.

Operation	Description
Set Report Contents	Click **Set Report Contents** to open the Set Report Contents pane. • Switch on **Stick Statistics on Top**, and check the items so that they will be displayed on the top of the report. • Switch on the other items such as person feature analysis so that you can view the selected reports of the store.
Configure Store	Click **Configure Store** to configure the store. For details, refer to ***Add a Single Store*** .
Set as Scheduled Report	Click **Set as Scheduled Report** to set the current report as a scheduled report. For details, refer to ***Send Store Analysis Report Regularly*** .
Export Report	• Check/uncheck **All** for **Statistics Target**. When it is checked, the report contents will be displayed. Check the items as needed. • Click **Export** to display the Export panel. • Select Excel, CSV, or PDF as the format of the exported report(s). • Select By Day, By Hour, or By Month as the report dimension. • Click **Export**.

View Multiple-Store Reports

You can view reports of multiple stores.

Select **Multiple-Store Reports** on the left.

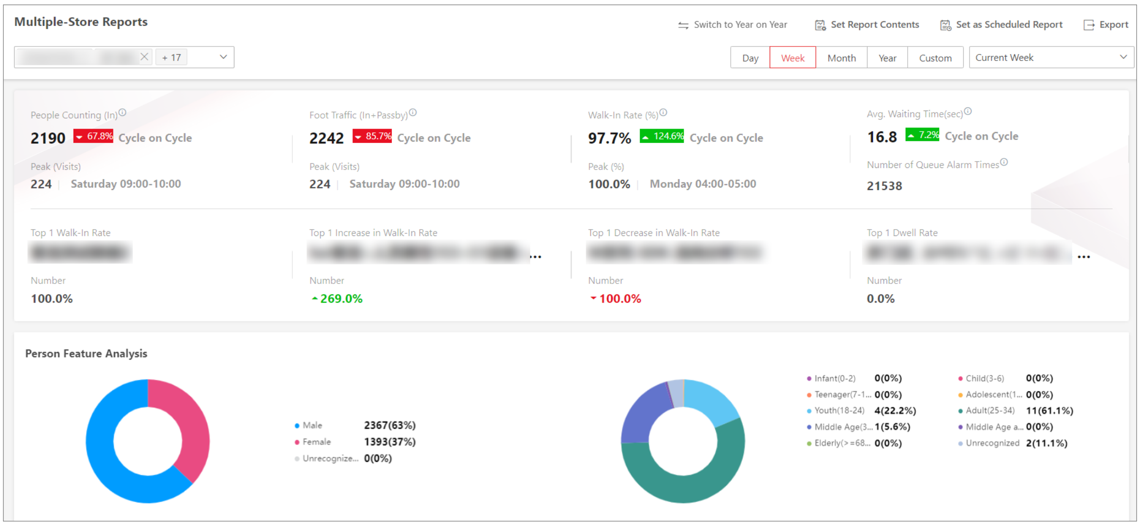


Figure 29-6 Multiple-Store Reports

You can perform the following operations.

Operation	Description
Select Stores	Click ⌄ to select multiple stores.
Set Report Time	Click **Day/Week/Month/Year/Custom** to select the report time.
View Parameter Meaning	Hover your cursor over ⓘ on the top right corner of a certain parameter, and you will view the explanations of the parameter.
Switch Between Year on Year and Cycle on Cycle	Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways. **Note** For exporting reports, year on year statistics and cycle on cycle statistics will be both exported.
Set Report Contents	Click **Set Report Contents** to open the Set Report Contents pane. • Switch on **Stick Statistics on Top**, and check the items so that they will be displayed on the top of the report. • Switch on the other items such as person feature analysis so that you can view the selected reports of the store.
Set as Scheduled Report	Click **Set as Scheduled Report** to set the current report as a scheduled report.

Operation	Description
	For details, refer to ***Send Store Analysis Report Regularly*** .
Export Report	• Click **Export** to display the Export panel. • Check/uncheck **All** for **Statistics Target**. When it is checked, the report contents will be displayed. Check the items as needed. • Select Excel, CSV, or PDF as the format of the exported report(s). • Select By Day, By Hour, or By Month as the report dimension. • Click **Export**.

View Comparison Report

You can view comparison reports of two stores.

In the top left corner of the Client, select ▦ → **Operation Analytics** → **Intelligent Analysis** → **Store Report** → **Comparison Report** .

Click ⌄ to select two stores.

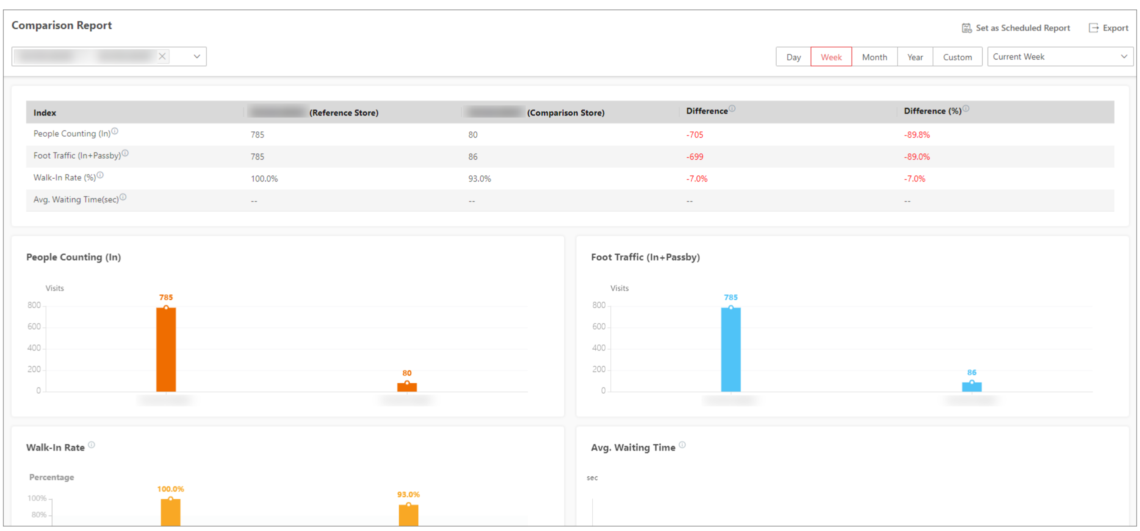


Figure 29-7 Comparison Report

You can perform the following operations.

Operation	Description
Set Report Time	Click **Day/Week/Month/Year/Custom** to select the report time.
View Parameter Meaning	Hover your cursor over on the top right corner of a certain parameter, and you will see the explanations of the parameter.
Set as Scheduled Report	Click **Set as Scheduled Report** to set the current report as a scheduled report. For details, refer to ***Send Store Analysis Report Regularly*** .
Export Report	• Click **Export** to display the Export panel. • Select Excel, CSV, or PDF as the format of the exported report(s). • Select By Day, By Hour, or By Month as the report dimension. • Click **Export**.

View Store Promotion Day Report

You can view the report containing people counting, foot traffic, and walk-in rate on a promotion day, and get a direct view of people counting trend and rankings of different store(s).

Select **Store Promotion Day Report** on the left.

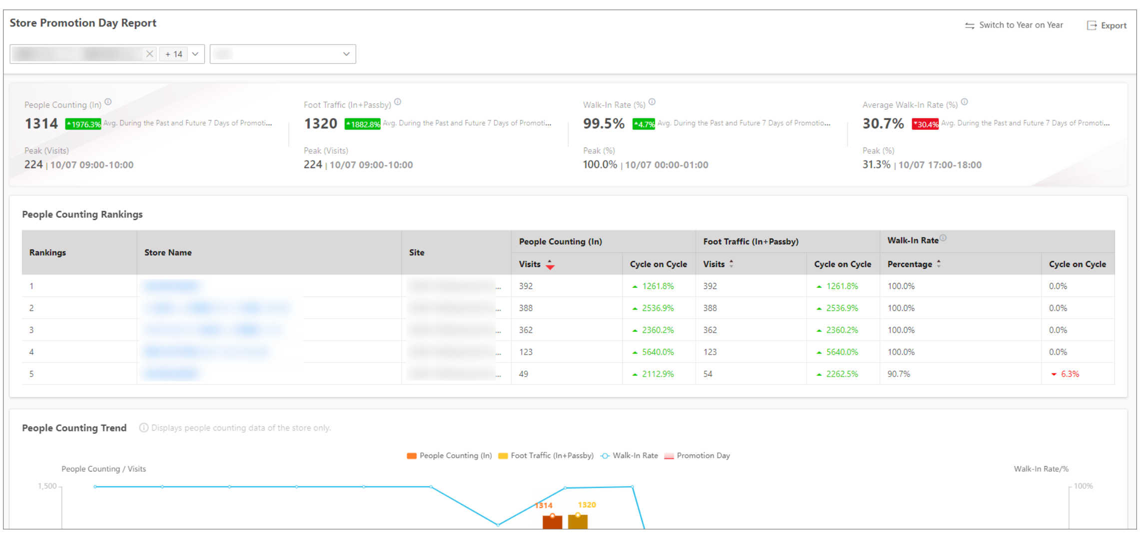


Figure 29-8 Store Promotion Day Report

You can perform the following operations.

Operation	Description
Select Store and Promotion Day	Check stores in the drop-down list. You can also enter the store name in the search field to search for the store. Select a promotion day for generating a report of store(s) on that day. The corresponding report of selected store(s) on the promotion day is displayed.
View Parameter Meaning	Hover your cursor over on the top right corner of a certain parameter, and you will view the explanations of the parameter.
Switch Between Year on Year and Cycle on Cycle	Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways. **Note** For exporting reports, year on year statistics and cycle on cycle statistics will be both exported.
Export Report	• Click **Export** to display the Export panel. • Check/uncheck **All** for **Statistics Target**. When it is checked, the report contents will be displayed. Check the items as needed. • Select Excel, CSV, or PDF as the format of the exported report(s). • Select By Day, By Hour, or By Month as the report dimension. • Click **Export**.

29.4.4 View Store Intelligent Analysis Report

In the retail/supermarket scenario, to view intelligent analysis reports including people counting analysis, person feature, heat analysis, pathway analysis, and queue analysis, you should configure store(s) and add them to the platform in advance.

- **Store People Counting Report**: You can generate a people counting report which displays the period over period data and trend of people counting statistics to have a direct view of people entering, exiting, passing by, and walk-in rate. You can also export the report to the local PC.

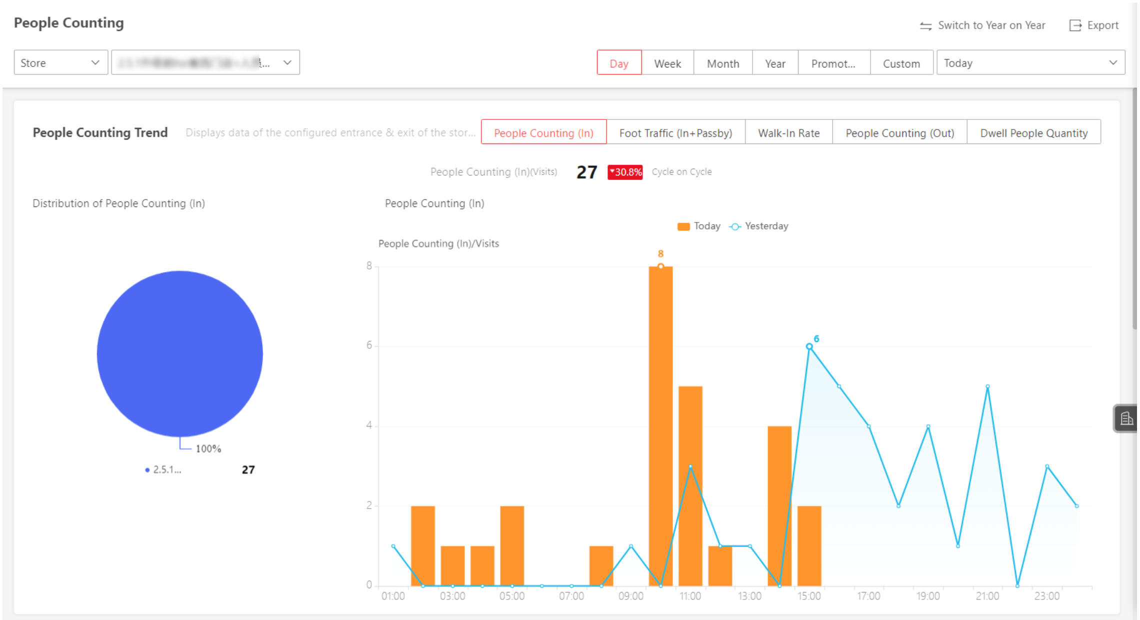


Figure 29-9 Store People Counting Report

- **Store Person Feature Analysis Report**: The platform supports saving features of recognized human faces and generating reports in various time periods. The reports tells the percentage and number of people of different features in different time period. It can be used in places such as shopping mall to analyze interests of people in different features.

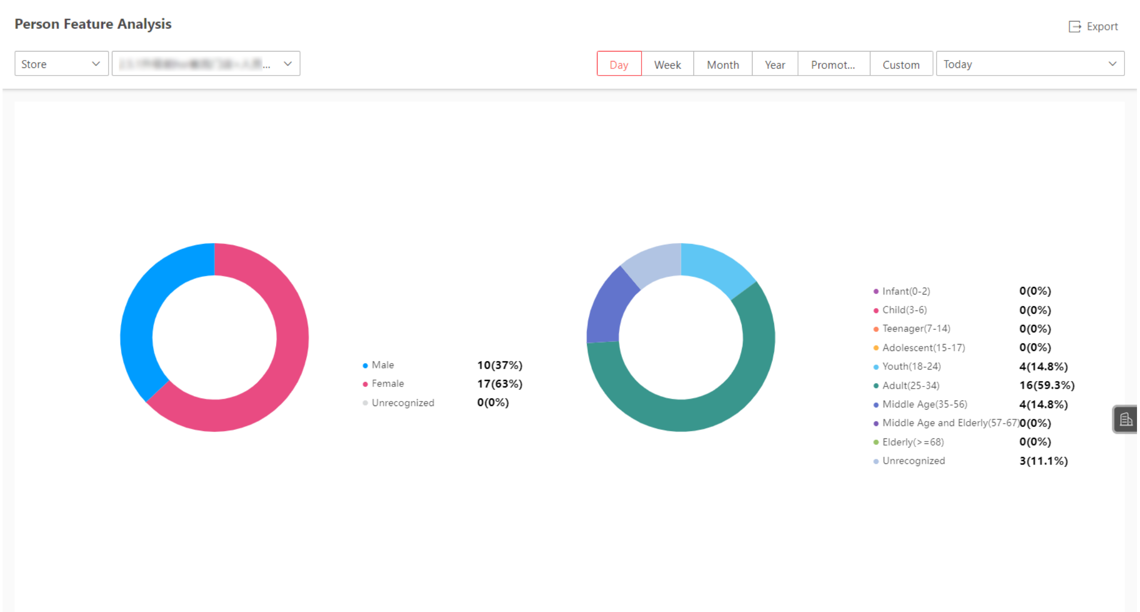


Figure 29-10 Store Person Feature Analysis Report

- **Store Heat Analysis Report**: You can generate a heat analysis report to show consumer movements, the visit times, and dwell time in a configured area.

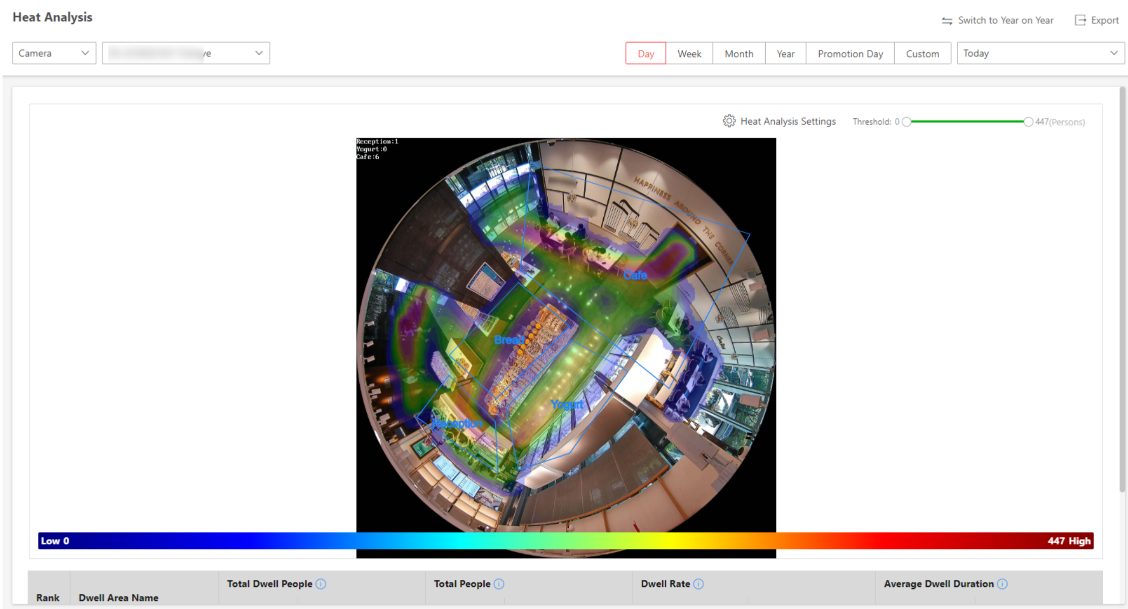


Figure 29-11 Store Heat Analysis Report

Note

- Make sure you have added a heat map network camera to the platform and properly configure the camera with heat map rule for the required area. To add a heat map network camera, please refer to the *User Manual of HikCentral Professional Web Client*. To configure the heat map rule, please refer to the user manual of heat map network camera.
- Make sure you have added the camera to a static map. For details about how to add a camera to the static map, refer to *User Manual of HikCentral Professional Web Client*.

- **Store Pathway Analysis Report**: Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the platform can collect the consumers data (for example, where the customers walk mostly). This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked. After setting the fisheye camera's pathways and their directions, the platform calculates the people dwell time at each pathway and number of people walking by, thus helps them make decisions.

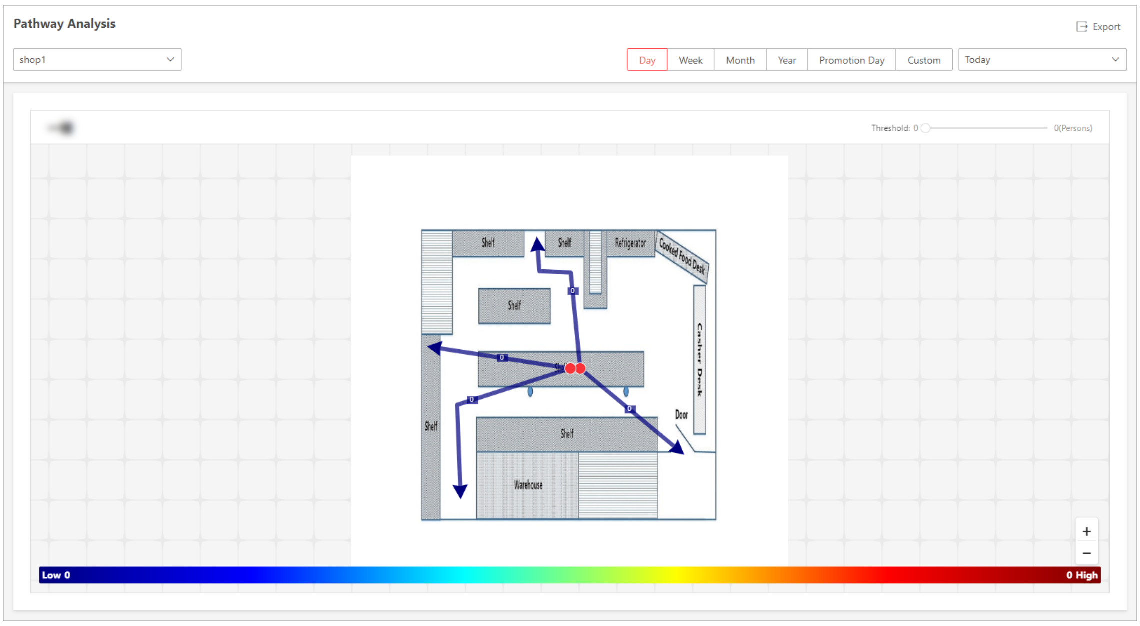


Figure 29-12 Store Pathway Analysis Report

Note

- Make sure you have properly added the camera to a static map and set its pathways on the map via the Web Client first. For details about adding camera to map and set pathways, refer to the *User Manual of HikCentral Professional Web Client*.

- **Store Queue Analysis Report**: For cameras which support queue management, you can generate a report to show the number of queue exceptions and number of persons in each queue, and show the queue status including waiting duration and queue length.

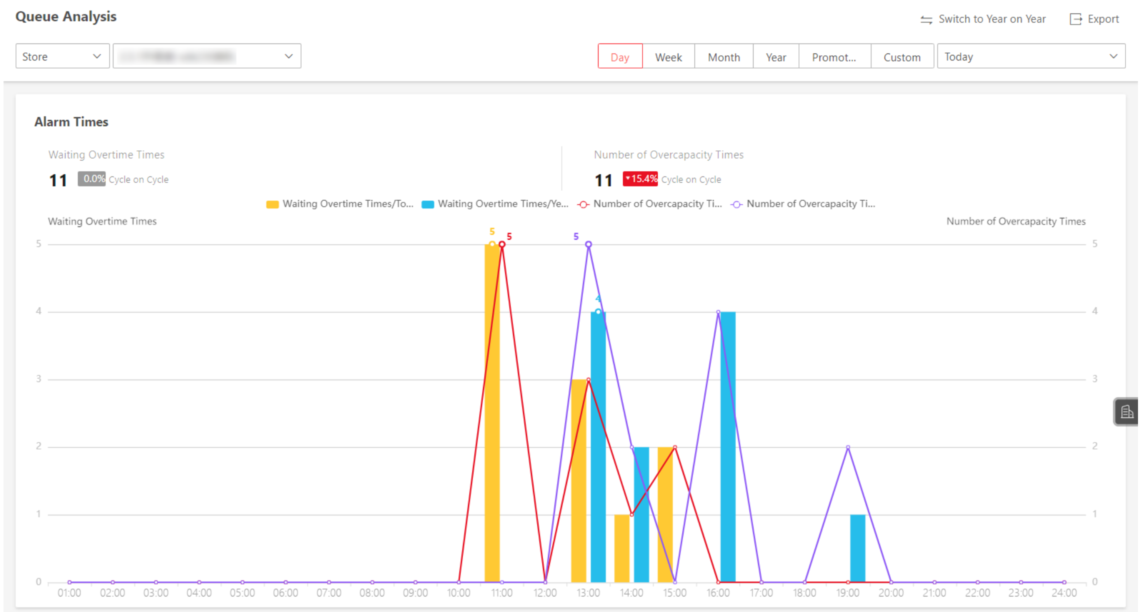


Figure 29-13 Store Queue Analysis Report

Note

Make sure you have added a camera which supports queue management to the system and configure queue regions. To configure the queue region, refer to user manual of the camera.

See the example process of viewing a heat analysis report. Some specific parameter configurations may vary by reports.

1. Under the Intelligent Analysis module, select **Analysis Center → Heat Analysis** .
2. Select a store/camera to search for queue data. A queue analysis report of the selected camera/ store will be displayed.
3. (Optional) Set the statistical cycle as **Day**, **Week**, **Month**, **Year**, **Promotion Day**, or **Custom**.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the queue data detected in each hour of one day.

   Weekly Report, Monthly Report, and Annual Report

   As compared to daily report, weekly report, monthly report, and annual report can be less time-consuming, since they are not to be submitted every day. The platform will calculate the number of people or people dwell time in each day of way week, in each day of one month, and in each month of one year.

   Promotion Day

   Promotion day report shows data on a promotion day basis. The platform will send one report at the sending time on a promotion day, which contains analysis results on the day.

Note

For details of configuring a promotion day, refer to ***Configure Promotion Day*** .

Custom Time Interval

Users can customize the days in the report to analyze the number of people or people dwell time in each day or month of the custom time interval.

4. (Optional) Set the time or time period for statistics.

Note

For custom time interval report, you need to set the start time and end time to specify the time period.

5. (Optional) Perform the following operation(s).

Operation	Description
Set Heat Analysis Parameters	a. Click **Heat Analysis Settings**. b. Set the **Dwell Duration** to get statistics within the configured range. **Note** For example, if you set the dwell duration as > 15s, then when a person stays in an area for over 15 seconds, they will be considered as dwelling within the area. c. Select the **Meaning of Heat Color**, including total people and dwell time. d. Check **Show** or **Hide** the divided heat areas. e. Click **Save**. f. Drag the threshold slider in the upper-right corner to adjust the range of the statistical dimension. The heat data out of the range will not be displayed.
Switch Between Year on Year and Cycle on Cycle	Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways.

Operation	Description
	Note For exporting reports, year on year statistics and cycle on cycle statistics will be both exported.
Export Report	a. Click **Export**. b. Set the format of the exported file as Excel, CSV, or PDF. c. Select the time dimension as **By Hour**, **By Day**, or **By Month**. d. Click **Export**. **Note** You can get the exported report in the Download Center.

29.5 Public Scenario

The Public Scenario is designed for public situations such as stations and hospitals. You can view reports such as people counting and heat analysis reports.

On the left pane of the Intelligent Analysis module, select **Configure Scenario**.

Switch to the public scenario.

29.5.1 Customize Report Dashboard

The report dashboard provides an at-a-glance view for the public scenario reports. There are people counting reports, heat analysis reports, vehicle analysis reports, queue analysis reports, etc. You can customize the report dashboard as required.

Steps

1. Under the Intelligent Analysis module, select **Dashboard**.
2. **Optional:** On the top left corner, click → **Add Dashboard** on the report dashboard page and create a name to add a new dashboard.

Note

- You can add up to 100 dashboards.
- The new dashboard appears and it is by default named as "Dashboard + The Time When It was Added" by default. For example, in "Dashboard20190916102436", "2019" represents year, "09" month, "16" date, "10" hour, "24" minute, and "26" second.

You can view the added dashboard by clicking to expand the list of added dashboard(s).

3. **Optional:** You can perform the following operations.

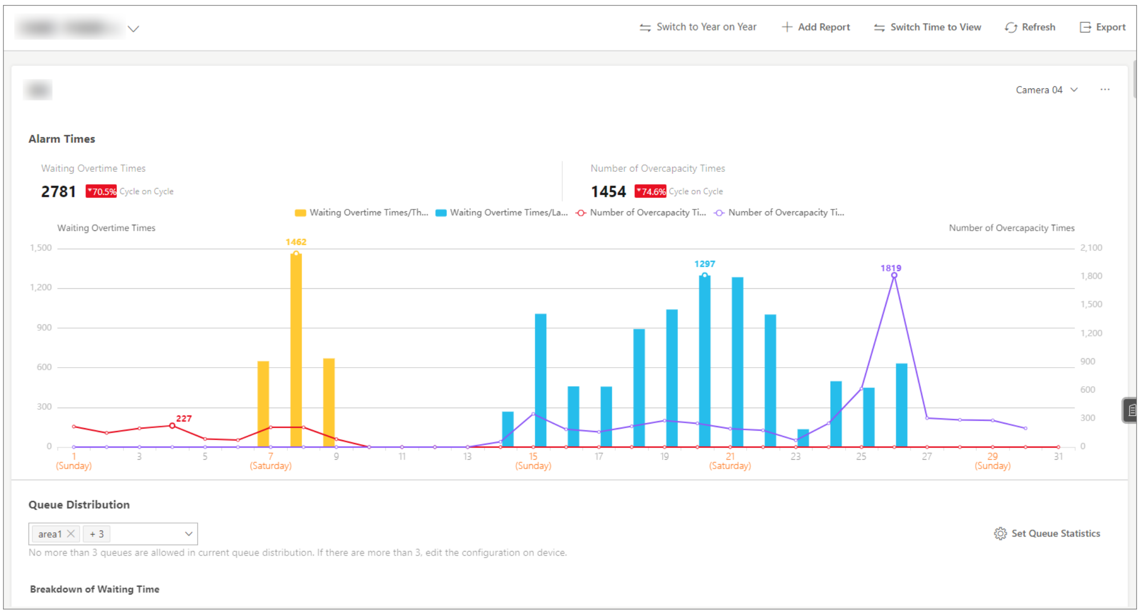


Figure 29-14 Dashboard

Operation	Description
Edit Dashboard Name	On the top left corner, click . Click to edit the dashboard name.
Delete Dashboard	On the top left corner, click . Click to delete the dashboard.
Add Report to Dashboard	a. After you select a dashboard, click **Add Report**, select a report type, and click **Next**. b. Set the report name, analysis type, report type, and time.

Note

- If you select analysis for one camera, you need to select the camera already added to the platform.
- If you select analysis in one region, you need to select the analysis group already added to the platform.

	c. Click **Add** to add the report to dashboard. The report will appear on the selected dashboard. d. Click **Add Report** to add more reports to the dashboard as needed.
Edit Report Name	On the top right corner of a report, click ··· and then click **Edit**.
Delete Report from Dashboard	On the top right corner of a report, click ··· and then click **Delete**.
Switch Between Year on Year and Cycle on Cycle	Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways.
Switch Time to View Report Data	Select a dashboard and then click **Switch Time to View** to set the report type and time. **Report Type** Select the time basis for the reports. For example, daily report shows data on a daily basis. **Time** Set the specific time for generating the reports. For example, if you select **Custom Time Interval** as the report type, you can click to specify a time interval for generating report data. Click **Save** to change the default time basis of all the reports in the dashboard to the time you set in the previous sub step.
Export report	Export report(s) on the dashboard to the local PC. a. Click **Export** to display the Export panel. b. Select report(s) from the report list. c. Select **Excel**, **CSV**, or **PDF** as the format of the exported report(s). d. Click **Export**.

29.5.2 View Intelligent Analysis Report

In the public scenario, to view intelligent analysis reports including people counting analysis, person feature, heat analysis, pathway analysis, queue analysis, people density analysis, temperature analysis, and multi-target-type analysis, you should configure corresponding analysis groups / camera(s) in advance.

People Counting Report

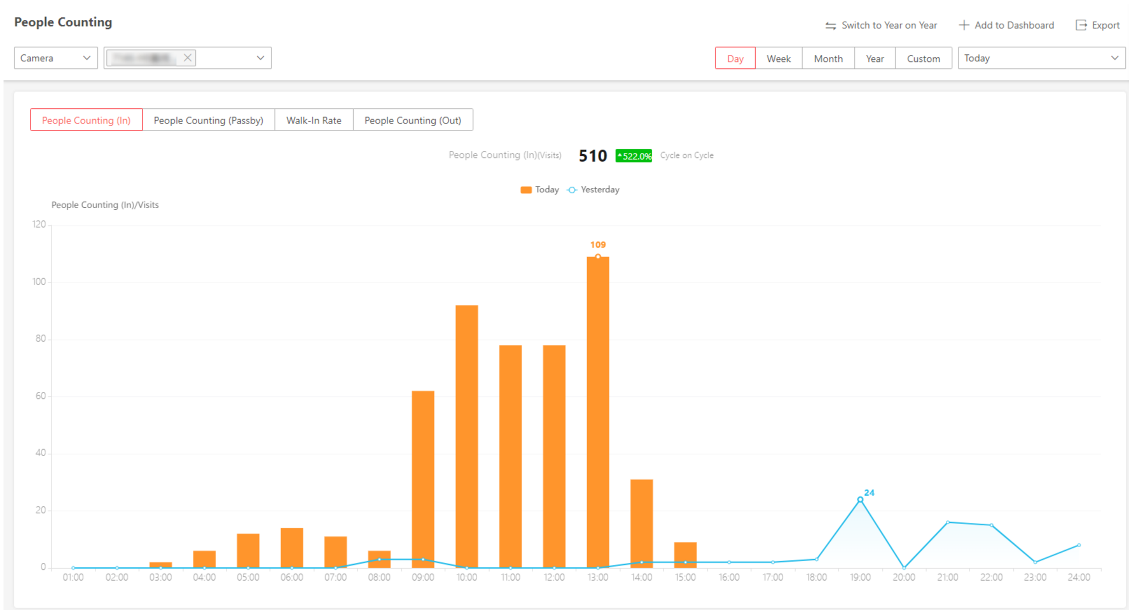


Figure 29-15 People Counting Report

People counting report shows the number of line crossing people counted by people counting cameras or obtained from access records of access control devices in a specific region and within a certain time period. The report lets you know the number of persons who stay in a specific region, which can be used for certain commercial or emergency scenarios. For example, for emergency scenario, during a fire escape, the number of stayed persons will be displayed on the map which is required for rescue. For commercial scenario, the shopping mall manager can get the people counting report to know whether the store is attractive and get the number of people entering each stores to determine whether to limit the number of customers staying in the mall for security reasons during the peak time. You can also generate a people counting report for a single store or multiple stores.

Before generating a people counting report, you can add people counting group(s) to group the doors and people counting cameras of a certain region so as to define region edge. After that, you can set a regular report rule for the specified cameras which support people counting or people counting groups, and the platform will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a people counting report at any time to view the data if required.

Heat Analysis Report

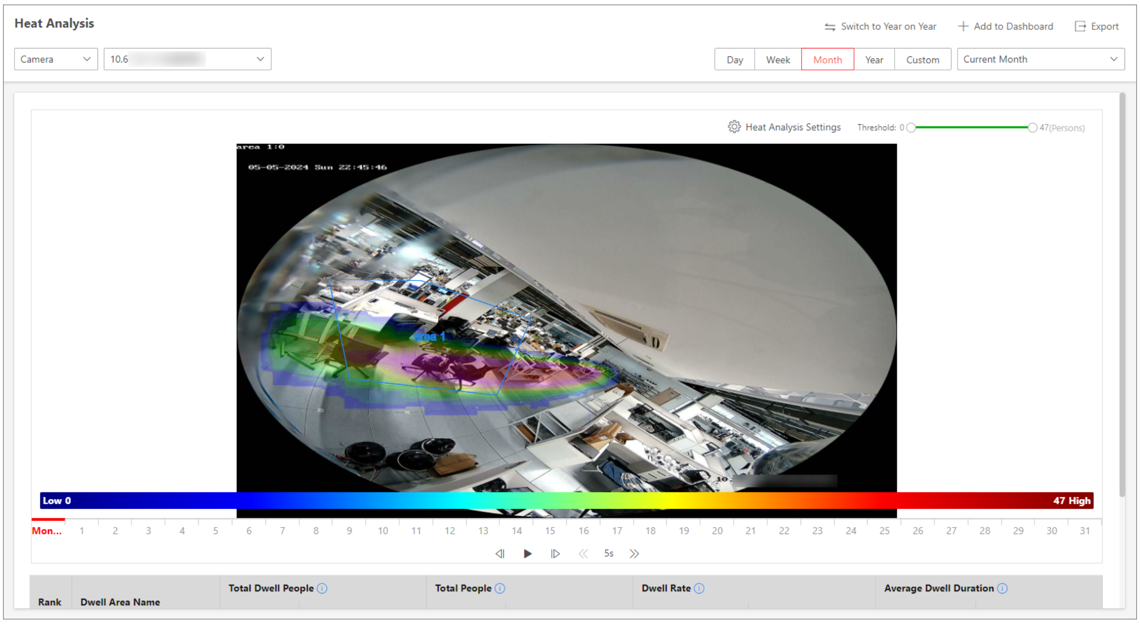


Figure 29-16 Heat Analysis Report

Heat analysis report shows data with a heat map, which is a graphical representation of data represented by colors. The heat map function of the camera is usually used to track the consumers movements (where the customers walk, and what items they stop to touch and pick up) and analyze the visit times and dwell time in a configured area. This report is mainly used for store managers or retailers to see which part of the store got the most attention from consumers and which got least. Knowing where customers move is useful for retailers. They can optimize store layouts, for example, where to place popular and unpopular goods.

Before using heat analysis report, you can add a heat analysis group to define the region for heat analysis. After that, you can set a regular report rule for the specified cameras or the specified heat analysis groups, and the system will send emails with heat analysis reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a heat analysis report at any time to view the data if required.

Person Feature Analysis Report

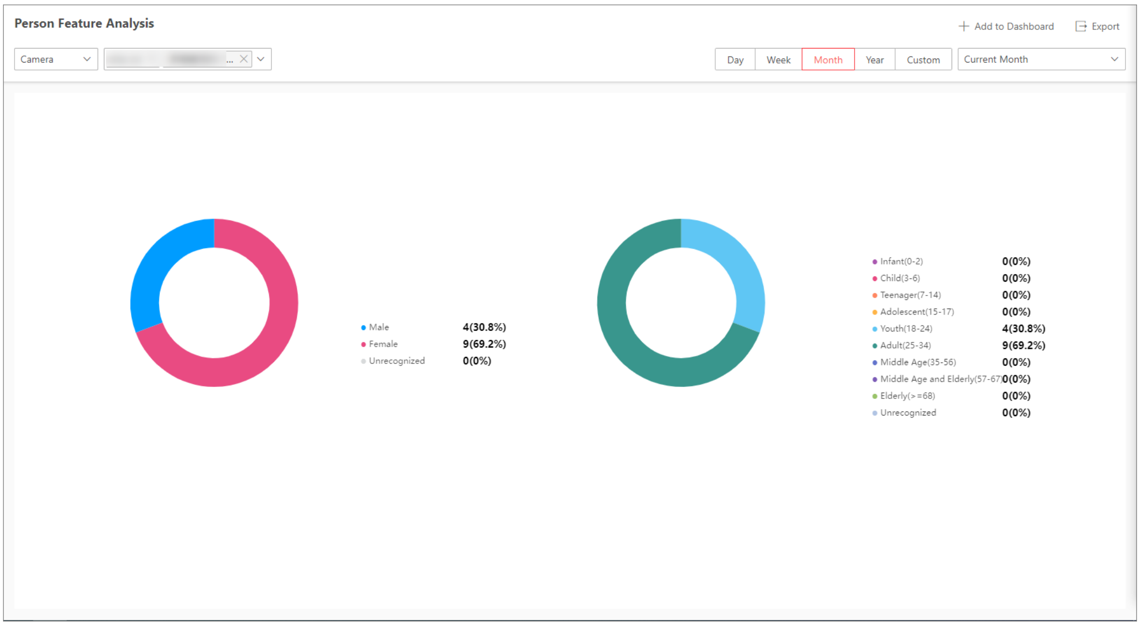


Figure 29-17 Person Feature Analysis Report

Person feature analysis report shows the proportion of persons with different features detected by cameras which support facial recognition.

You can add a person feature analysis group before generating a report to define the region for person feature analysis by grouping the cameras which support facial recognition and feature analysis. After that, you can set a regular report rule for the specified cameras or specified person feature analysis groups, and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a person feature analysis report at any time to view the data if required.

Queue Analysis Report

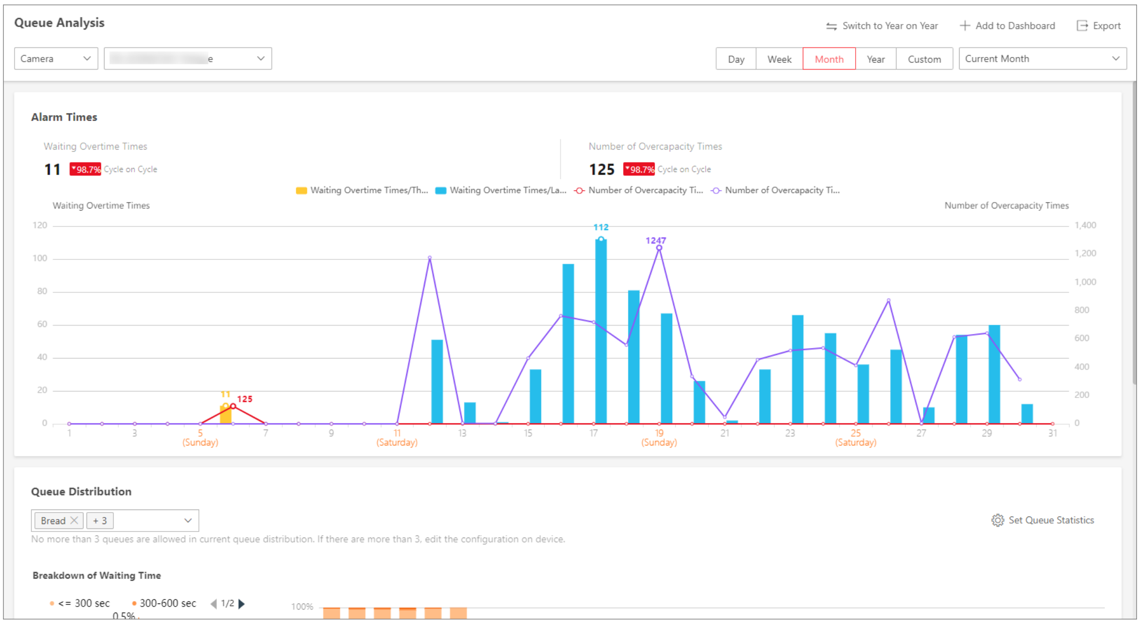


Figure 29-18 Queue Analysis Report

Queue analysis report shows the number of queue exceptions and number of persons in each queue, and show the queue status including waiting duration and queue length. It is helpful for allocating resources for retailers.

You can set a regular report rule for the specified cameras, and the system will send emails with queue analysis reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a queue analysis report at any time to view the data if required.

Pathway Analysis Report

Figure 29-19 Pathway Analysis Report

Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the system can collect the consumers data (for example,where the customers walk mostly) and translate that data onto a dashboard for mall managers. This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked.

Before using pathway analysis, you should add pathway analysis groups first, which define the region for pathway analysis. After that, you can set a regular report rule for the specified pathway analysis group, and the system will send emails with pathway analysis reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a pathway analysis report at any time to view the data if required.

People Density Analysis Report

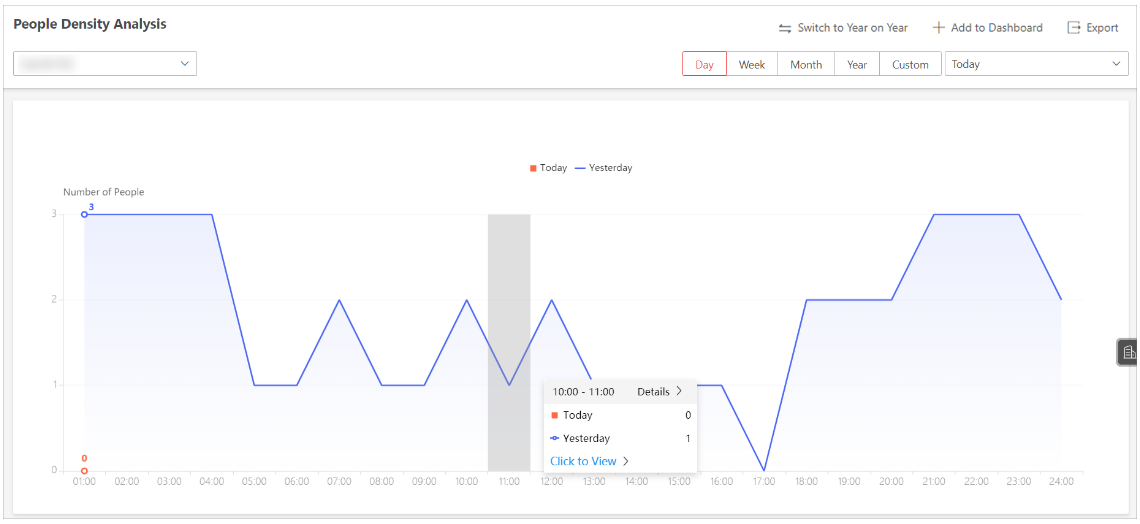


Figure 29-20 People Density Analysis Report

People density analysis report shows the variation trend of the people density data in line chart. The people density data refers to the peak amount of people appeared in the images of a specific camera during a certain time period. The data is useful for the management and control of the amount of people in specific areas or space during special time periods. For example, assume that you were a manager of a shopping mall during epidemic outbreak, you could generate a people density analysis report to find out the time period(s) during which excessive people density usually occurs in the shopping mall, and then arrange in advance the personnel and related works accordingly to limit people gathering at those time periods to prevent the spread of the infectious disease.

Temperature Analysis Report

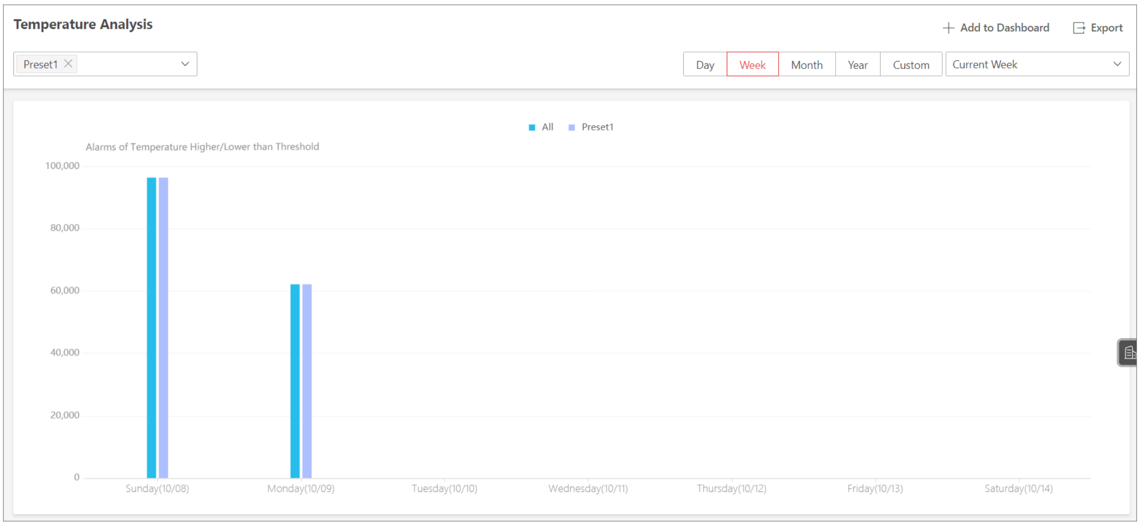


Figure 29-21 Temperature Analysis Report

The temperature analysis report shows the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different thermometry points on different presets. You can set a regular report rule for the specified thermal cameras and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a temperature analysis report at any time to view the data if required.

Multi-Target-Type Analysis Report

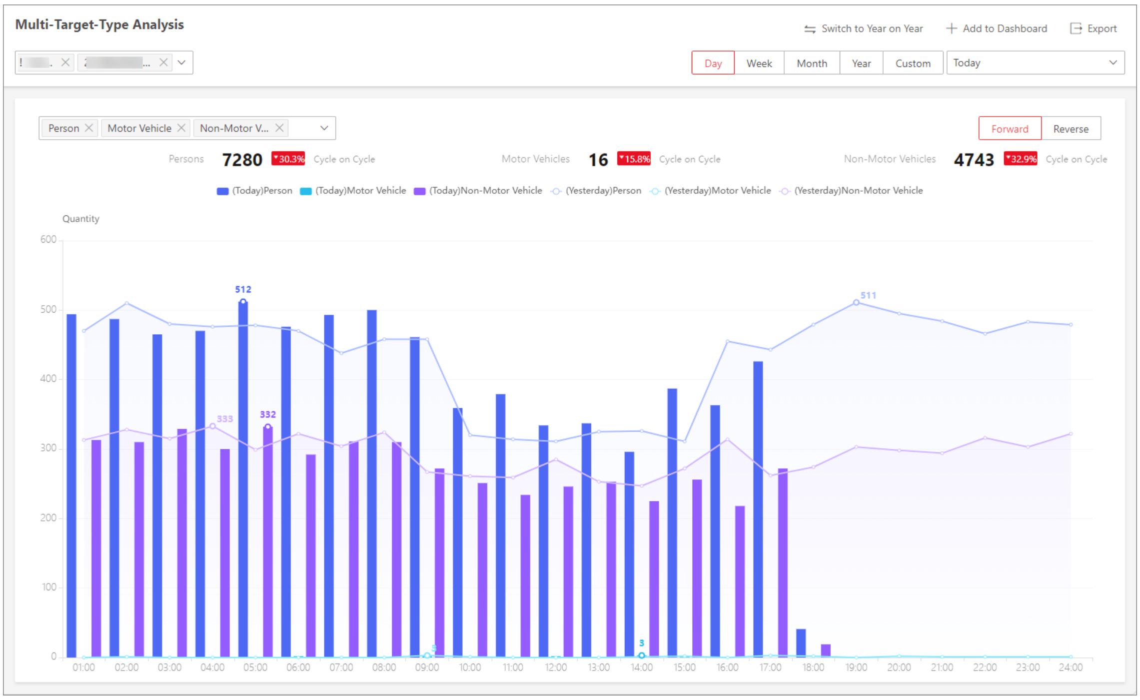


Figure 29-22 Multi-Target-Type Analysis Report

The multi-target-type analysis report shows the number of persons, motor vehicles, and non-motor vehicles within a specified period. You can set a regular report rule for the specified cameras and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a analysis report at any time to view the data if required.

Add Analysis Group

Before generating people counting report, you can add people counting group before the report; before generating heat analysis report, person feature analysis report, and pathway analysis report, you can add the corresponding analysis groups.

People Counting Group: The people counting group is used to group the doors, people counting cameras, queue management cameras, and fisheye cameras of certain region. You can set some doors and cameras as the region edge. Only the persons accessing these doors or detected by the cameras are calculated, and other doors and cameras outside the region are ignored. By grouping these doors and cameras, the platform provides counting functions based on the detected records on these doors and cameras.

Heat Analysis Group: The heat analysis group is used to group the resources (such as doors, fisheye cameras, people counting cameras) in certain region. By grouping these resources, you can know the dwell time of the people stayed in this region, how many persons stayed in this region, and average dwell time of each people. This function is mainly used to calculate and show the popularity of each stores in one shopping mall.

Person Feature Analysis Group: Person feature analysis is a group of cameras which support face recognition and feature analysis. You can group the cameras in one region into one group. After that, when generating a report, you can view the features of the persons appeared in this region, based on the data detected by the cameras in the group. For example, if there are five cameras which support facial recognition mounted in the store, the store manager can add these five cameras into one group. Then you can view features of the customers who entering the store in the Intelligent Analysis module.

Pathway Analysis Group: Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the system can collect the consumers data (for example,where the customers walk mostly) and translate that data onto a dashboard for mall managers. This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked. After setting the fisheye camera's pathways and their directions, the system calculates the people dwell time at each pathway and number of people walking by, thus helps them make decisions.

Note

Adding analysis groups is not supported by queue analysis report, people density analysis report, temperature analysis report, and multi-target-type analysis report.

The process of adding analysis groups for these reports can be generally divided into 3 sections: basic configuration, adding analysis resource, adding analysis group to map. Some specific parameter configurations may vary by reports.

See the example process of adding person feature analysis group.

1. Under the Intelligent Analysis module, select **Analysis Group → Person Feature Analysis Group** .
2. Click **Add**.

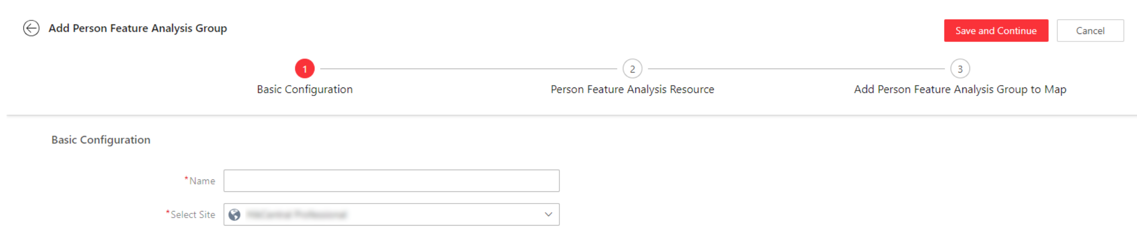


Figure 29-23 Add Analysis Group (Person Feature Analysis Group)

3. Set basic configurations such as name and site, and click **Save and Continue**. Click **Save and Continue**.
4. Configure resources for analyzing the detected persons' features.
   a. In the **Person Feature Analysis Resource** part, click **Add** to select the resources.
   b. Click **Save**.

c. (Optional) Click **Remote Configuration** to go to Remote Configuration page of the device.
d. Click **Save and Continue**.

5. (Optional) Locate the person feature analysis group on the map by setting the locations of the cameras in the group and setting the edge of the region for detection.
   a. Drag the person feature analysis group from the Resource Group list on the right to the map. The region as well as the cameras in the group will be added on the map.
   b. Drag to draw the region according to the actual needs.
   c. Drag the icons of the cameras to set the their locations on the map.
   d. Right click to finish.
   e. (Optional) Check **Only Display the Current Group** to only display the added analysis group on the map.
6. Click **Finish**. After adding the person feature analysis group on the map, you can view the features of the persons appeared on the Control Client.

Generate Analysis Report

You can generate people counting reports, heat analysis reports, person feature analysis reports, queue analysis reports, pathway analysis reports, people density reports, temperature analysis reports, and multi-target-type analysis reports. For people counting report, heat analysis report, pathway analysis report, and person feature analysis report, make sure you have added the corresponding analysis groups.

- **People Counting Report**: You can generate a people counting report which displays the period over period data and trend of people counting statistics to have a direct view of people entering, exiting, passing by, and walk-in rate. You can also export the report to the local PC.

  Note

  Before you begin, make sure you have properly configured the camera with a people counting rule for the required area. To configure the people counting rule, refer to the user manual of people counting camera.
- **Heat Analysis Report**: You can generate a heat analysis report to view consumer movements and analyze the visit times and dwell time in a configured area.

  Note

  - Before you begin, make sure you have added a heat map network camera to the platform and properly configure the camera with heat map rule for the required area. To configure the heat map rule, please refer to the user manual of heat map network camera.
  - Before you begin, make sure you have added the camera to a static map.
- **Person Feature Analysis Report**: The platform supports saving features of recognized human faces and generating reports in various time periods. The reports tells the percentage and number of people of different features in different time period. It can be used in places such as shopping mall to analyze interests of people in different features.

Note

Before you begin, make sure you have added a person feature analysis group if you want to perform feature analysis in one region. See for details about adding a person feature analysis group.

- **Queue Analysis Report**: For cameras which support queue management, you can generate a report to show the number of queue exceptions and number of persons in each queue, and show the queue status including waiting duration and queue length.

Note

Before you begin, make sure you have added a camera which supports queue management to the system and configure queue regions. To configure the queue region, refer to user manual of the camera.

- **Pathway Analysis Report**: Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the platform can collect the consumers data (for example, where the customers walk mostly) and translate that data onto a dashboard for mall managers. This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked. After setting the fisheye camera's pathways and their directions, the platform calculates the people dwell time at each pathway and number of people walking by, thus helps them make decisions.

Note

- Before you begin, make sure you have properly added the camera to a static map and set its pathways on the map via the Web Client first. For details about adding camera to map and set pathways, refer to the *User Manual of HikCentral Professional Web Client*.

- **People Density Analysis Report**: You can manually generate a people density report to view the people density data of two adjacent time period. You can also export the report to the local PC.

Note

- Before you begin, make sure you have purchased the License that supports people density analysis, or the function will be unavailable.
- Before you begin, make sure you have added the abnormal event detection server to the HikCentral Professional and linked cameras to the server.
- Before you begin, make sure you have configured people density analysis on the abnormal event detection server. For details, see the user manual of the server.

- **Temperature Analysis Report**: For thermal cameras, you can generate a report to show the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different temperature screening points on different presets, and generate a report to show corresponding figures of a specified preset of the temperature screening point.
- **Multi-Target-Type Analysis Report**: You can generate a report to show the number of persons, motor vehicles, and non-motor vehicles within a specified period.

The process of generating these reports can be generally divided into 4 sections: selecting report data resource, setting statistical cycle, setting the time or time period for statistics, and perform subsequent operations on the report as needed. Some specific parameter configurations may vary by reports.

See the example process of generating a people counting report.

1. Under the Intelligent Analysis module, select **Analysis Center → People Counting** .
2. Select the report data resource type.

   Camera

   A people counting report based on the data from the cameras you select will be generated. You can compare the data of different cameras.

   Analysis Group

   A people counting report based on the data from the people counting groups you select will be generated. You can compare the data of different groups.

   Note

3. Select people counting camera(s) or people counting group(s) based on the data resource type you set in the previous step.

   Note

   Up to 20 cameras/groups can be selected.

   The corresponding report of selected camera(s)/group(s) will be displayed.

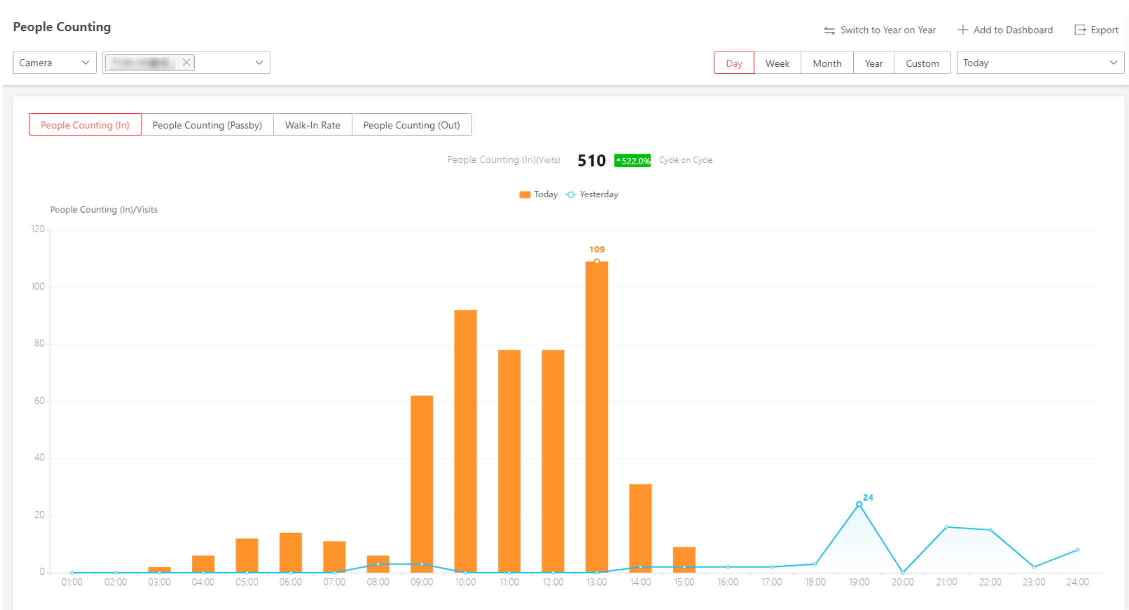


Figure 29-24 People Counting Report

4. Set the statistical cycle as **Day**, **Week**, **Month**, **Year**, or **Custom**.

   Daily Report

Daily report shows data on a daily basis. The platform will display the people counting data detected in each hour of two adjacent days.

Weekly Report, Monthly Report, and Annual Report

As compared to daily report, weekly report, monthly report, and annual report can be less time-consuming, since they are not to be submitted every day. The platform will display the people counting data detected in each day of two adjacent weeks, in each day of two adjacent months, and in each month of two adjacent years.

5. Select a pre-defined time period or customize a time period for statistics.

Note

For custom time interval report, you need to set the start time and end time to specify the time period.

6. Perform the following operation(s) after generating the people counting report.

Operation	Description
Switch Between Year on Year and Cycle on Cycle	Click **Switch to Year on Year** / **Switch to Cycle on Cycle** to compare the report statistics in different ways. **Note** For exporting reports, year on year statistics and cycle on cycle statistics will be both exported.
Add to Dashboard	a. Click **Add to Dashboard** in the upper-right corner of the page. b. Create a report name. c. Select a dashboard. Or click **New** to create a new board and then select it. d. Click **OK** or **Add and Go to Dashboard**.
Export Report	a. Click **Export**. b. Check/uncheck **All** for **Statistics Target**. When it is checked, only Excel will be available for file type in the next step. **Note** This option is only available for people counting analysis report. c. Set the format of the exported file as Excel, CSV, or PDF.

Operation	Description
	d. Select the time dimension as **By Hour**, **By Day**, or **By Month**. e. Click **Export**.

Send Analysis Report Regularly

You can set a regular report rule for specified analysis resources or targets, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the corresponding analysis data during the specified time periods. You can regularly send people counting reports, heat analysis reports, person feature analysis reports, queue analysis reports, pathway analysis reports, people density reports, temperature analysis reports, and multi-target-type analysis reports.

Note

- Set the email template with recipient information, subject, and content.
- Set the email settings such as sender address, SMTP server address and port.
- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

The process of setting the report sending schedule be generally divided into 4 sections: setting basic information of the report, setting report content, setting the time-related information for statistics, and advanced parameters. Some specific parameter configurations may vary by reports. See the example process of generating a heat analysis report.

1. Under the Intelligent Analysis module, select **Analysis Group → Scheduled Report** .
2. Click **Add** or + in the upper-left corner to open the Create Report page.

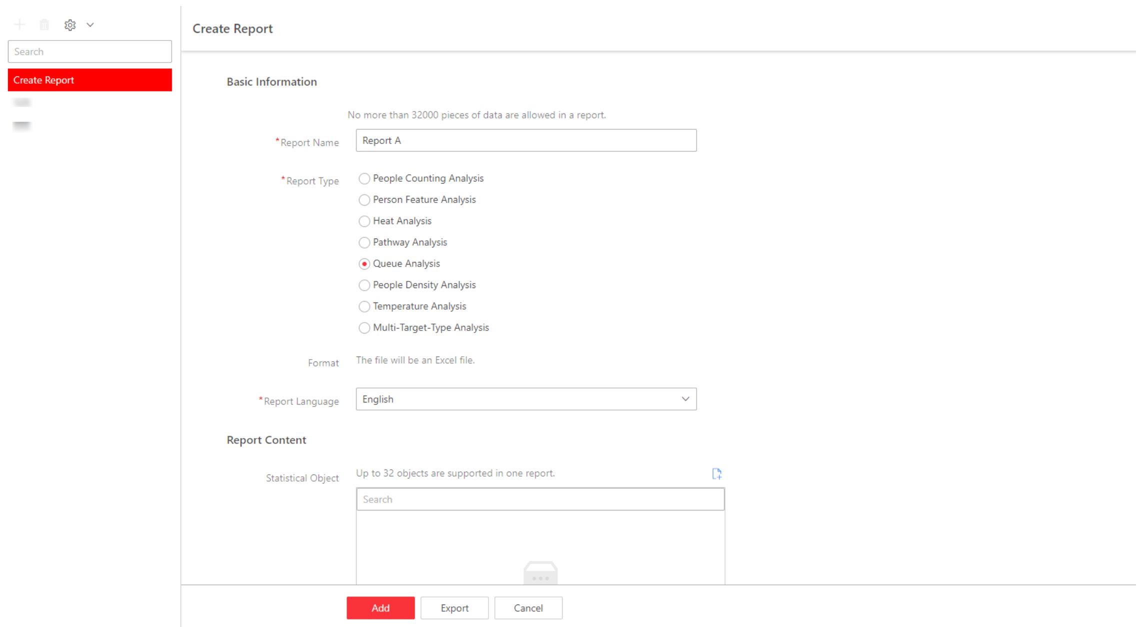


Figure 29-25 Send Analysis Report Regularly (Heat Analysis)

3. Create a name for the report.
4. Select the report category as **Heat Analysis**.
5. Select a language as **Report Language**.

Note

By default, the language is the same with the selected language when you log in on the Web Client.

6. Select heat analysis type.

Heat Analysis for One Camera

Analyze people dwell time and number of people detected by the specified camera(s).

Heat Analysis in One Region

Analyze people dwell time and number of people detected by the cameras in the specified heat analysis group(s).

Note

For details about adding heat analysis group, see ***Add Analysis Group*** .

7. Select the stores, heat analysis camera(s) or groups contained in the report.

Note

If you select **Heat Analysis for One Camera** as the analysis type, you should select camera(s). If you select **Heat Analysis in One Region**, you should select heat analysis group(s).

8. (Optional) Set the dwell duration.

9. Set the **Statistical Cycle** as **By Day**, **By Week**, or **By Month** and set the sending time, and set how the report will present results analyzed in the specified time period.

   Daily Report

   Daily report shows data on a daily basis. The platform will send one report at the sending time every day, which contains analysis results on the day (24 hours) before the current day. For example, if you set the sending time as 20:00, the platform will send a report at 20:00 every day, containing analysis results between 00:00 and 24:00 before the current day.
   For example, if you select the report type as Daily, you can select Calculate by Hour or Calculate by Minute. There will be 24 or 24×60 records for each camera respectively in the report, showing the number of passing vehicles detected in each hour or each minute for one camera.

   Weekly Report and Monthly Report

   As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The platform will send one report at the sending time every week or every month, which contains analysis results on the last 7 days or last month before the sending date.
   For example, for weekly report, if you set the sending time as 6:00 on Monday, the platform will send a report at 6:00 in the morning on every Monday, containing analysis results between last Monday and Sunday.
10. Set the report time and sending time according to the report type.
11. (Optional) Set the effective period (start time and end time) of sending the report regularly.
12. (Optional) Switch on **Send via Email**, and select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add** to add a new email template.
13. (Optional) Switch on **Upload to SFTP**, and click **Configure** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

   Note

   You can also hover the cursor on , then click **Configure SFTP** from the drop-down list to enter the panel to configure the corresponding information.
14. (Optional) Switch on **Save to Local Storage**, and click **Configure** beside **Saving Path** to configure the saving path of local storage.

   Note

   You can also hover the cursor on and click **Configure Local Storage** to enter the panel to configure the corresponding information.
15. Click **Add**.
16. (Optional) Click **Export** to export the report of this schedule for verifying the report sending schedule settings.

Chapter 30 Time & Attendance

In the Attendance module, you can easily manage the time & attendance system of your department and check your employees' attendance.

On the Home page, you can view the attendance report, attendance status statistics, and overall work hours / overtime.

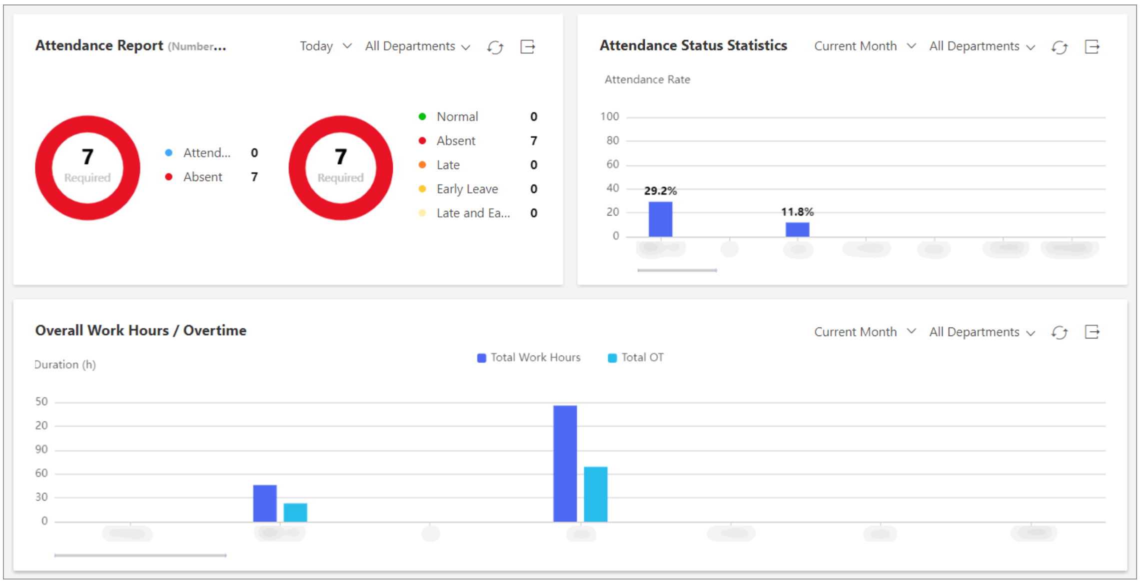


Figure 30-1 Attendance Charts

30.1 Time and Attendance Overview

The Attendance module provides time and attendance overview, including the attendance report, attendance status statistics, overall work hours / overtime, and personal credential status. In Time & Attendance Overview page, you can also set up a time & attendance system from the start.

On the top left, select → **Integrated Service** → **Attendance** . Select **Time & Attendance Overview** on the left.

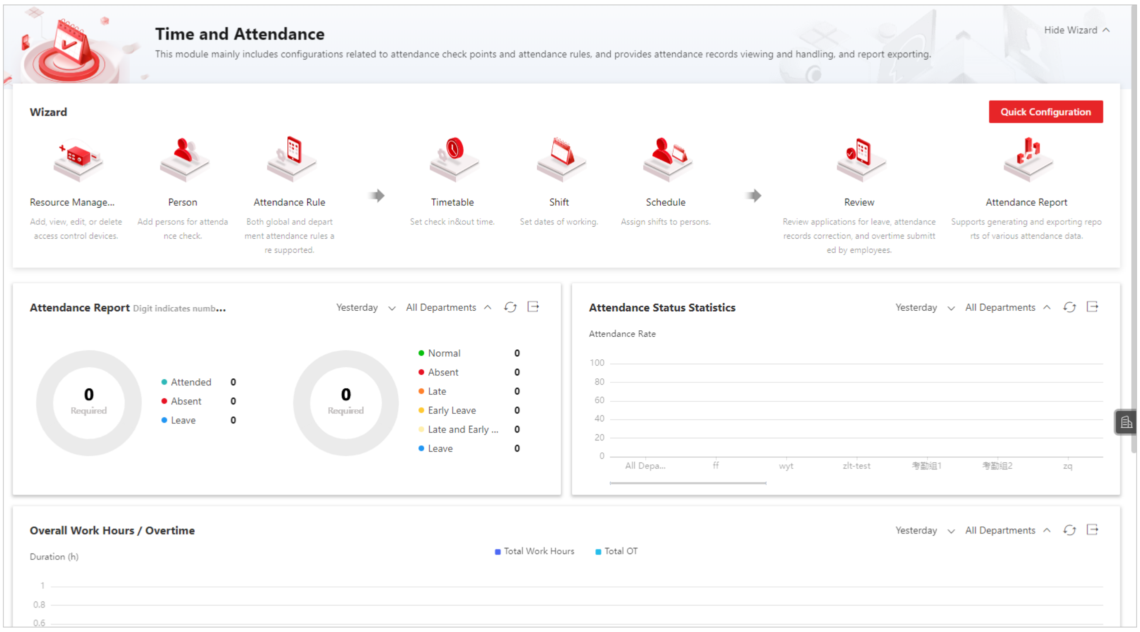


Figure 30-2 Attendance Overview

In the upper-right corner, click **Display Wizard** ⌄ to view the flow chart of time and attendance configuration.

To set up a time & attendance system from the start, click **Quick Configuration** and follow the instructions on screen.

1. **Person**: Add persons for attendance.
2. **Timetable Configuration**: Set a working time period. For more details, refer to ***Add Timetable*** .
3. **Shift**: Set the working time of a day and set the repeat schedule by day, week, or month. For more details, refer to ***Add Shift*** .
4. **Schedule**: Assign a shift to persons and set schedules. For more details, refer to ***Manage Schedule*** .

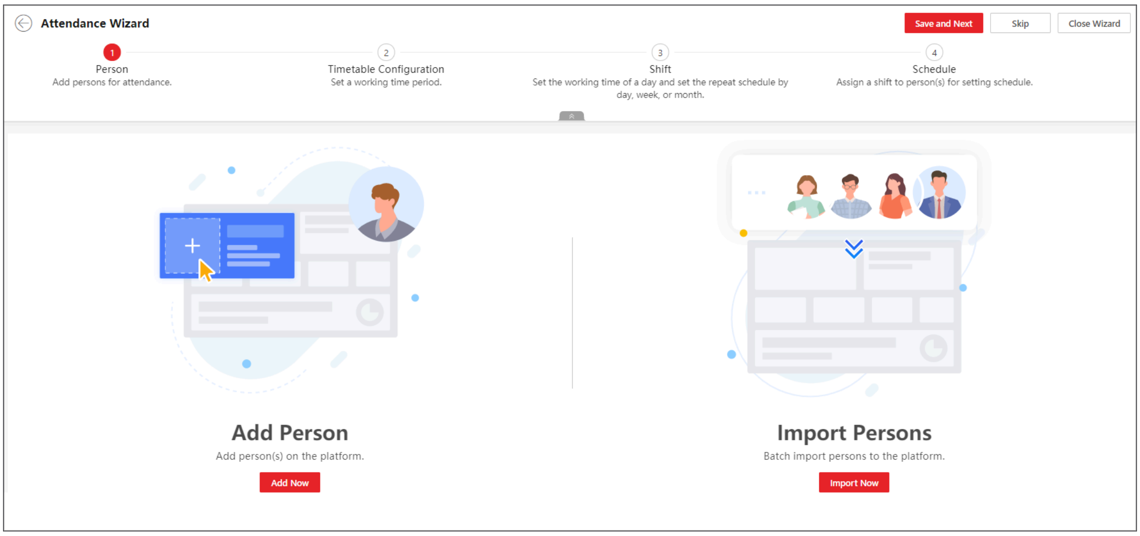


Figure 30-3 Attendance Wizard

You can view the attendance report, attendance status statistics, overall work hours / overtime, and personal credential status.

Note

- You can select the departments to view the attendance statistics. Also, you can select the time range for the statistics.
- You can click to export the current chart to local PC in the file format of PDF, PNG, or JPG.
- You can click to refresh the statistics data.

30.2 Flow Chart of Time and Attendance

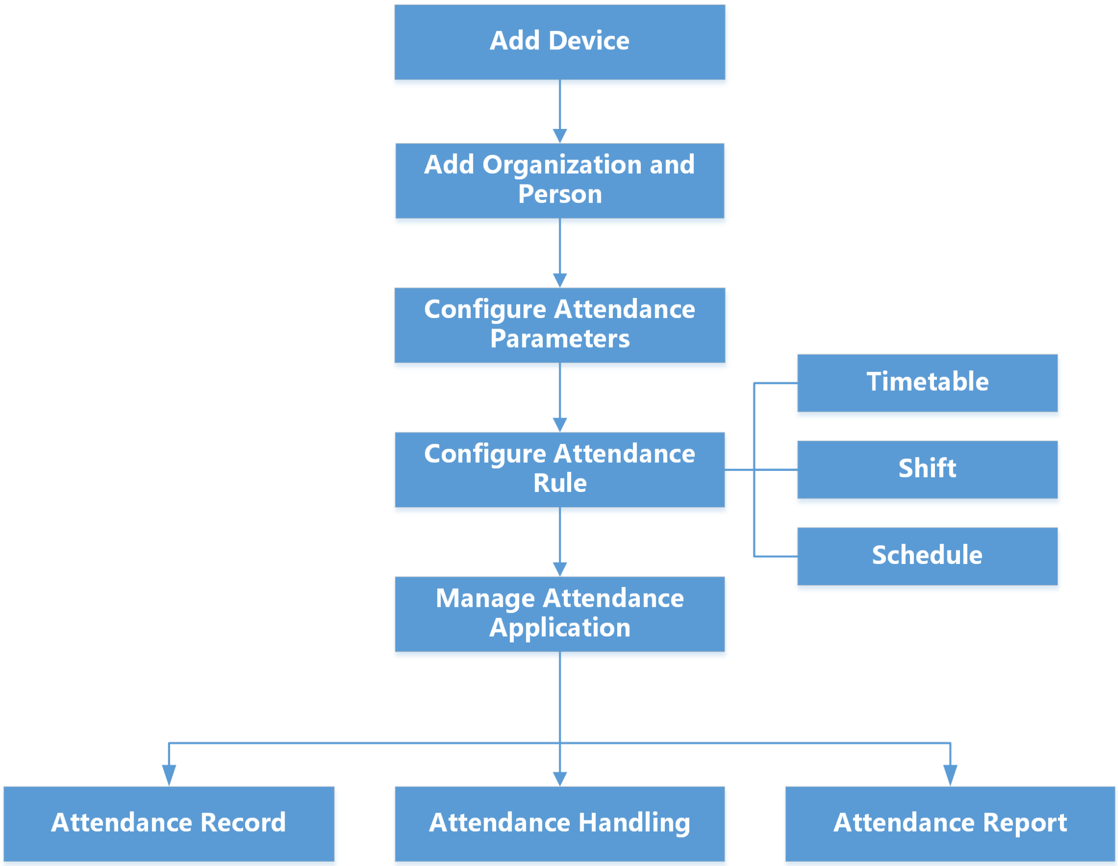


Figure 30-4 Flow Chart of Time & Attendance

- **Add Device**: Add devices (e.g., access control devices) to the platform.
- **Add Organization and Person**: Add departments, attendance group, and persons. For more details, refer to ***Add an Attendance Group*** .
- **Configure Attendance Parameters**: Configure attendance check points, general rule, overtime rule, leave types, check-in/check-out via Mobile Client, display rule for report, third-party database, etc. For more details, refer to ***Configure Attendance Rules for Global / Department / Attendance Group*** , ***Set Display Rules for Attendance Report*** .
- **Configure Attendance Rule**: Add timetable (including break timetable and work timetable), shift, and schedule. For more details, refer to ***Add Timetable*** , ***Add Shift*** and ***Manage Schedule*** .
- **Manage Attendance Application**: Manage applications for employees and admins. For more details, refer to ***Application Management for Employee*** and ***Application Management for Admin*** .
- **Attendance Record, Attendance Handling**: Search and correct attendance records, apply for leave, get devices' attendance records, manually calculate attendance results, etc. For more details, refer to ***View Attendance Records*** .
- **Attendance Report**: Export attendance report to local PC or send it via email regularly. For more details, refer to ***Manage Attendance Reports*** .

30.3 Add an Attendance Group

For situations where users need to set exclusive attendance rules for specified employees, users can add the employees to an attendance group configured with attendance rules different from and prior to that of a department.

Before You Start

Make sure you have added the employees to the platform.

Steps

1. On the top left, select → **Integrated Service → Attendance → Attendance Group** .
2. Click **Add**.
3. On the Add Attendance Group pane, enter a name of the group.

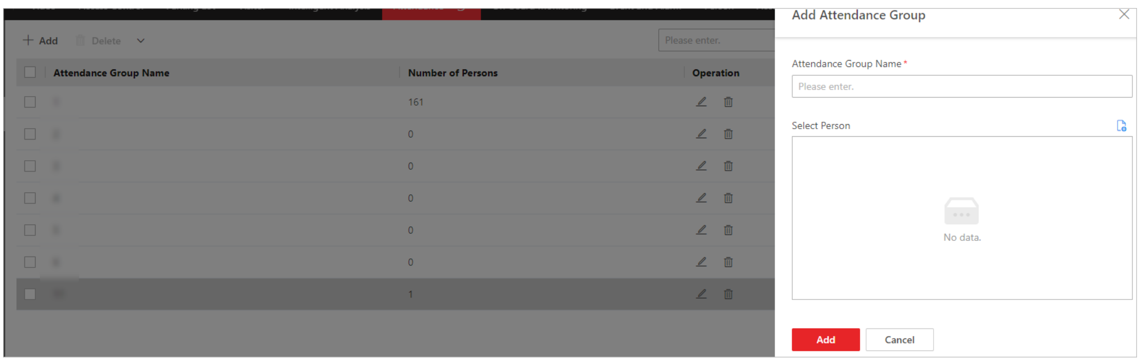


Figure 30-5 Add Attendance Group

4. Click and check persons in different departments, and click **Add** to save the selections.

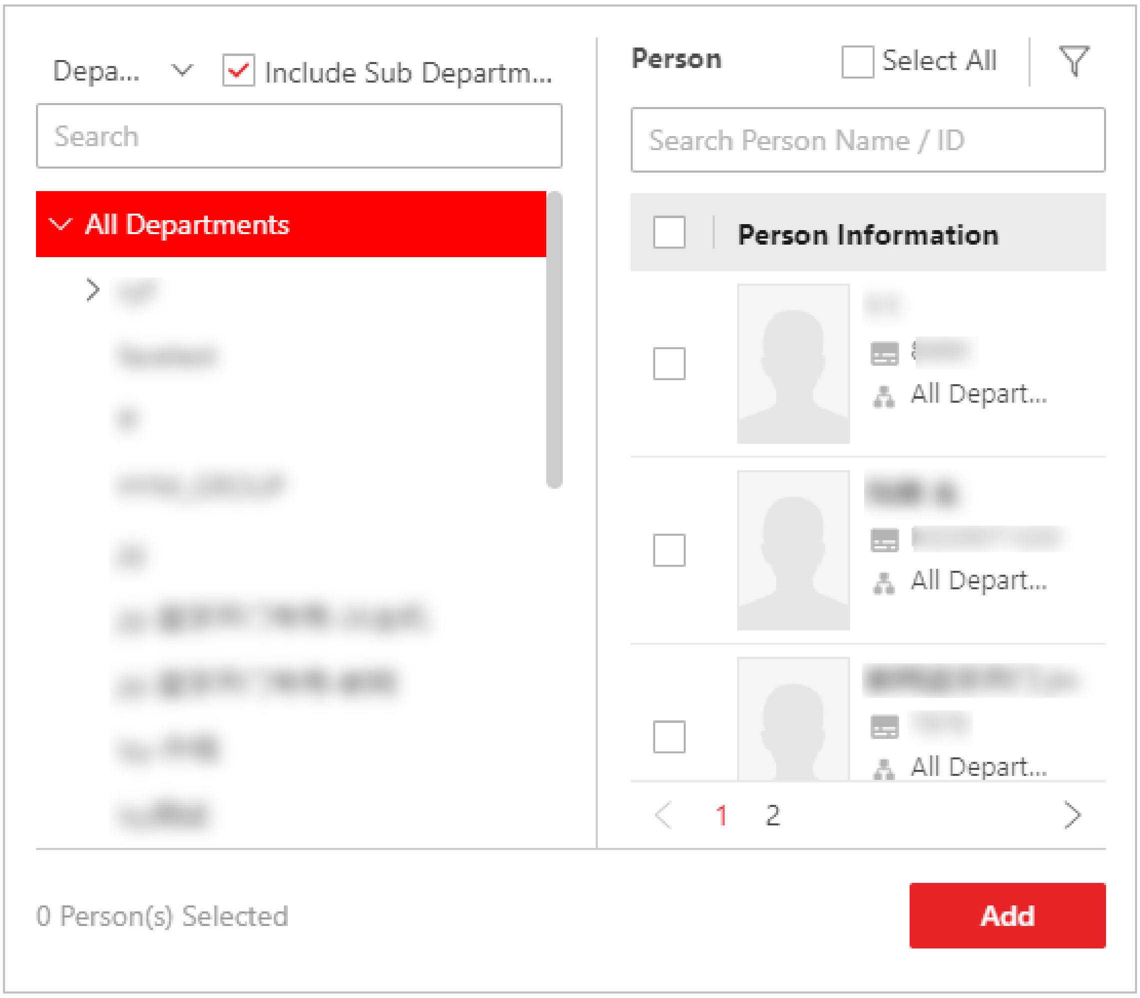


Figure 30-6 Add Persons to Attendance Group

Note

You can click on the top left to filter persons by additional information.

5. Perform the following operations.

Edit an Attendance Group	Click and then edit the group name or click to add persons to the group.
Add Persons to an Attendance Group	Click an added group to show persons on the right. Then click **Assign To** to add persons to the group.
Remove Persons from an Attendance Group	Click an added group to show persons on the right. Then check persons and click **Unassign** to remove the selected persons from the group. Or click → **Unassign All** to remove all persons from the group.

Set Display Mode of Each Column	Click to display each column title completely/incompletely.

What to do next

Configure attendance rules for the group. See ***Configure Attendance Rules for Global / Department / Attendance Group*** .

30.4 Basic Configuration

You can set basic parameters for the attendance module, such as adding pay codes, editing the fixed codes, setting the storage location, and customizing attendance status.

30.4.1 Specify Attendance Check Points

By default, all devices are attendance check points. You can specify some access points for attendance check, so that the check-in/out by credentials (such as swiping card on the access point's card reader, or face detected by the (linked) camera) will be valid and will be recorded.

Steps

1. On the top left, select → **Integrated Service → Attendance** .
2. Select **Basic Configuration → Attendance Check Point** on the left.
3. **Optional:** Click **Customize Attendance Status** to select attendance mode and custom attendance parameters. For details, see ***Customize Attendance Status on Device*** .
4. **Optional:** Check **Get Historical Data Stored in Devices** to synchronize the historical data generated by attendance check points to existing data. This will cause a recalculation of attendance results.
5. Click **Specify** to start customizing attendance check points.
6. Click **Add**.
7. Select the type of the attendance check point.

   Check-In & Out

   The attendance records of check-in or check-out on the attendance check point are both valid.

   Check-In Only

   The attendance records of swiping card or face recognition on the attendance check point will be only calculated as check-in. Persons cannot check out on this check point.

   Check-Out Only

   The attendance records of swiping card or face recognition on the attendance check point will be only calculated as check-out. Persons cannot check in on this check point.
8. Select the resource type (e.g., door) from the drop-down list.

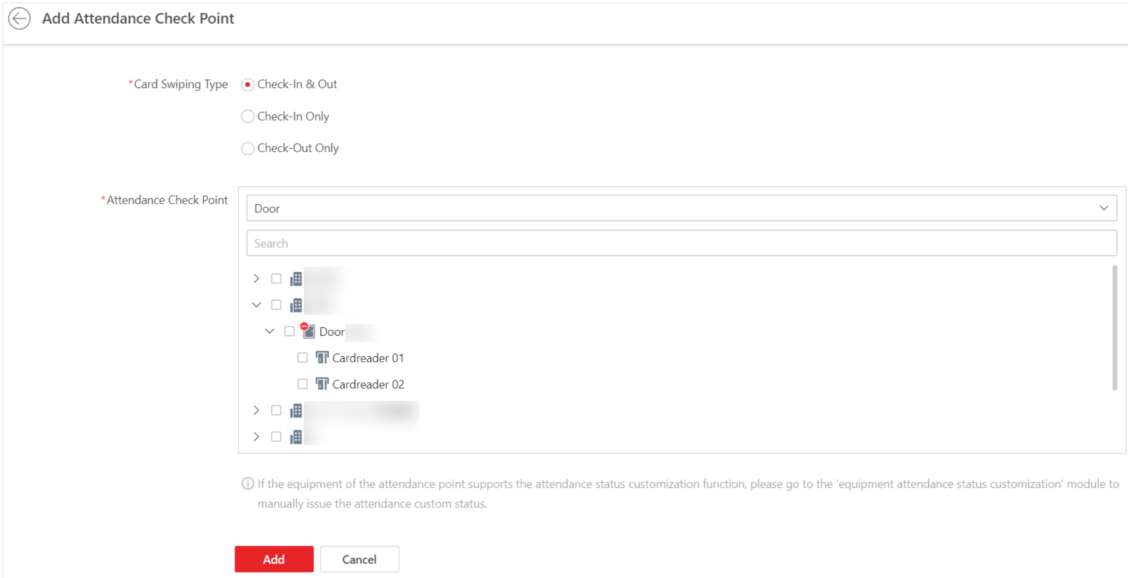


Figure 30-8 Add Attendance Check Point

All the resources which have not been set as attendance check point will be displayed.

9. Select the resources.

> **Note**
>
> If you select Door as the resource type, you can set the attendance check point type for different card readers separately. For example, there is a card reader installed at both side of the door. You can set the card reader of the entry direction as check-in only and the exit one check-out only.

10. Click **Add**.

    The selected resources will be displayed in the attendance check point list.

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

Change Check Point's Type
For the added attendance check points, you can select one or more items and click **Set as Check-In Only**, **Set as Check-Out Only**, or **Set as Check-In/Out** from drop-down list to change the current type to another.

Delete Check Point
To delete the added attendance check point, select the added attendance check point(s) and click **Delete**.

> **Note**
>
> If the attendance check point is deleted, the attendance records on this attendance check point will be deleted as well, and it will affect the persons' attendance results for the days on which the attendance data haven't been calculated.

Customize Attendance Status on Device

You can customize the rules of attendance status on device. After setting up Attendance Status on Device and applying the settings to the devices, you can choose to use the attendance status on the devices to calculate the attendance results.

Before You Start

Make sure the devices support this feature.

Steps

1. In the upper-left corner of Home page, select → **Attendance** → **Basic Configuration** .
2. Select **Custom Attendance Status on Device** on the left.
3. Switch on **Enable Attendance Status on Device**.
4. Set the parameters.

Attendance Mode

Manual: No attendance schedule. Manual selection of attendance status is required when a person checks in or checks out on a device.

Automatic: Specify an attendance schedule and the attendance status of a person is judged according to the schedule.

Manual And Auto: Specify an attendance schedule and the attendance status of a person is judged according to the schedule. The person can also change the attendance status manually on device.

Attendance Status Required

On: Manual selection of attendance status is required for a valid check-in/out.

Off: Manual selection of attendance status is optional.

Note

Not available when in Manual mode, because manual selection of attendance status is always required.

Custom Name of Working

Customize the status name for check-in and check-out.

Custom Break Name

Customize the status name for the start and end of a break.

Custom Overtime Name

Customize the status name for the start and end of an overtime.

Schedule Template

Select a status and drag on the template to define the attendance status of a period of time.

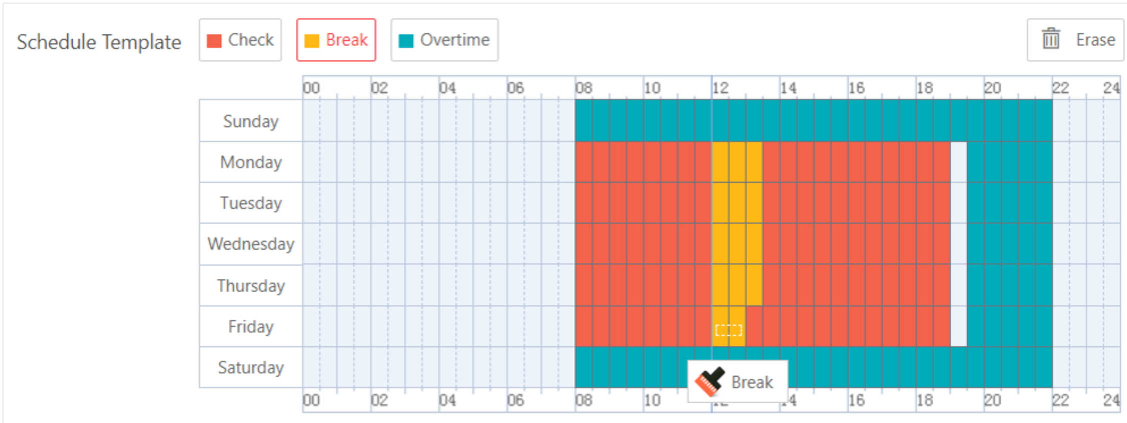


Figure 30-9 Schedule Template

Note

- Not available when in Manual mode. Because manual selection of attendance status is always required and no attendance schedule is needed.
- Work time and break time must be continuous.
- Overtime cannot be continuous with work and break time.
- Overtime must be before or after work or break time.

5. Click **Save** to save the settings and apply the settings to the attendance check points you added.

Note

- You can view the applying result on the Apply Custom Status window.
- See details about adding attendance check points in ***Specify Attendance Check Points*** .
- You can switch on **Enable T&A Status on Device** when configuring break timetables, timetables, or shifts to record the T&A status on devices, which will be used in attendance results calculation.

30.4.2 Add a Pay Code

Pay code defines the attendance status and calculation codes for calculating the attendance statistics on the third-party system. You can add, edit, and delete pay codes, filter the pay codes by conditions, set the column title, and custom column items.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Basic Configuration** → **Pay Code** on the left.
3. Click **Add** to open the Add Pay Code pane.
4. Create the pay code name.
5. Set the pay code type and related parameters.

Leave

leave type which displays in reports and leave applications.

Unit: Unit of pay code. Select from minute, hour, day, and HH:MM (time accurate to minute).

Overtime

Overtime type which displays in configuration of overtime rules, reports and overtime applications.

Work Hour Rate

Used for calculating the overtime period, e.g., the actual working time of overtime is 2 hours and the work hour rate is 1.5, then the overtime period is 3 hours.

Color

Used for making differences among pay codes.

6. Set the rounding rule.

Round Up

Round the number of pay code up, e.g., if you make 0.5 go up, then 6.5 rounds up to 7.

Round to Nearest

Round decimal numbers to nearest integers either by rounding up or rounding down based on the tenths places, e.g., 6.5 rounds to 7 and 6.4 rounds to 6.

Round Down

Round the number of pay code down, e.g., if you make 0.5 go down, then 6.5 rounds down to 6.

7. Set the Min. Value for the rounding rule.
8. Set whether to display the pay code in report.
9. Click **Add**.
10. **Optional:** Perform the following operations.

Operation	Description
Edit Pay Code	Click in the Operation column to edit the pay code information.
Delete Single Pay Code	Click in the Operation column to edit the pay code information.
Batch Delete Pay Codes	Select one or multiple pay codes and click **Delete** to delete them. Or Select **Delete All** to delete all the pay codes.
Filter Pay Code	Click to expand the conditions, set the filter conditions and click **Filter** for filtering the pay codes.
Set Column Width	Click to select **Complete Display of Each Column Title**/ **Incomplete Display of Each Column Title** to set the column title width.
Custom Column Item	Click and select the needed column items to display. You can also click **Reset** to reset to the default column items.

30.4.3 Edit a Fixed Code

Fixed code refers to the calculation rules of attendance types. You can set parameters of fixed codes such as the unit, symbol, and rounding rule.

On the top left, select → **Integrated Service → Attendance** .

Select **Basic Configuration → Fixed Code** on the left.

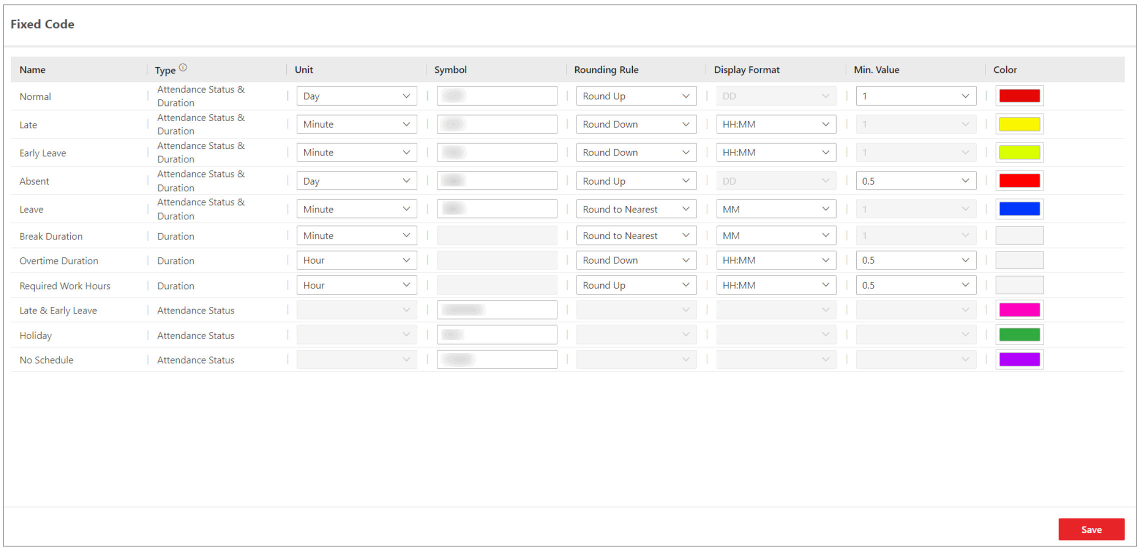


Figure 30-10 Edit Fixed Code

You can set the following parameters and click **Save** to finish editing.

Unit

Unit of pay code. Select from minute, hour, and day.

Symbol

Different symbols indicate different status respectively, including late, absent, no schedule, holiday, etc. You can customize these marks according to actual needs.

Rounding Rule

Rule for calculating the attendance.

Round Up

Round the number of pay code up, e.g., to make 0.5 go up, so 6.5 rounds up to 7.

Round to Nearest

Round decimal numbers to nearest integers either by rounding up or rounding down based on the tenths places, e.g., 6.5 rounds to 7 and 6.4 rounds to 6.

Round Down

Round the number of pay code down, e.g., to make 0.5 go down, so 6.5 rounds down to 6.

Display Format

Time format of the fixed code, including HH:MM, DD, HH, and MM.

Min. Value

The minimum value of the fixed code. Select from 1 and 0.5.

Note

When the Unit is "hour", the min. value is 0.25.

Color

Used for making differences among fixed codes.

30.4.4 Add a Leave Rule

A leave rule refers to a group of leave types and persons, where the persons in the group enjoys certain leaves.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** → **Basic Configuration** → **Leave Rule** .
2. Click **Add Leave Rule**.

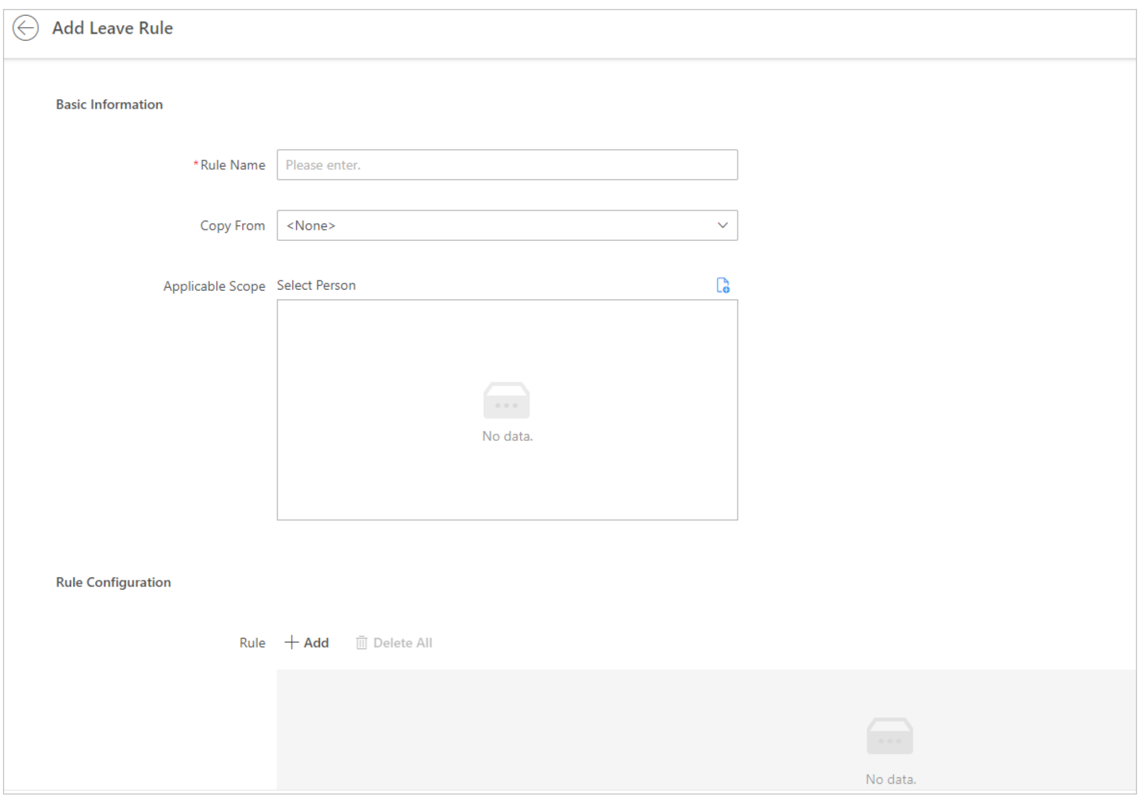


Figure 30-11 Add Leave Rule

3. Enter a rule name.

4. **Optional:** Select an existing leave rule from the drop-down list of **Copy From** to copy the persons using the selected leave rule here.
5. Click to select persons who are going to use the leave rule.
6. Add a rule.
   1) In the Rule Configuration area, click **Add** to open the Add Rule pane.
   2) Select a pay code from the drop-down list.
   3) Set the related parameters.

   Min. Days of Employment Allowed for Leave Application

   Only when the days of employment reaches this value, can the employee apply for a leave.

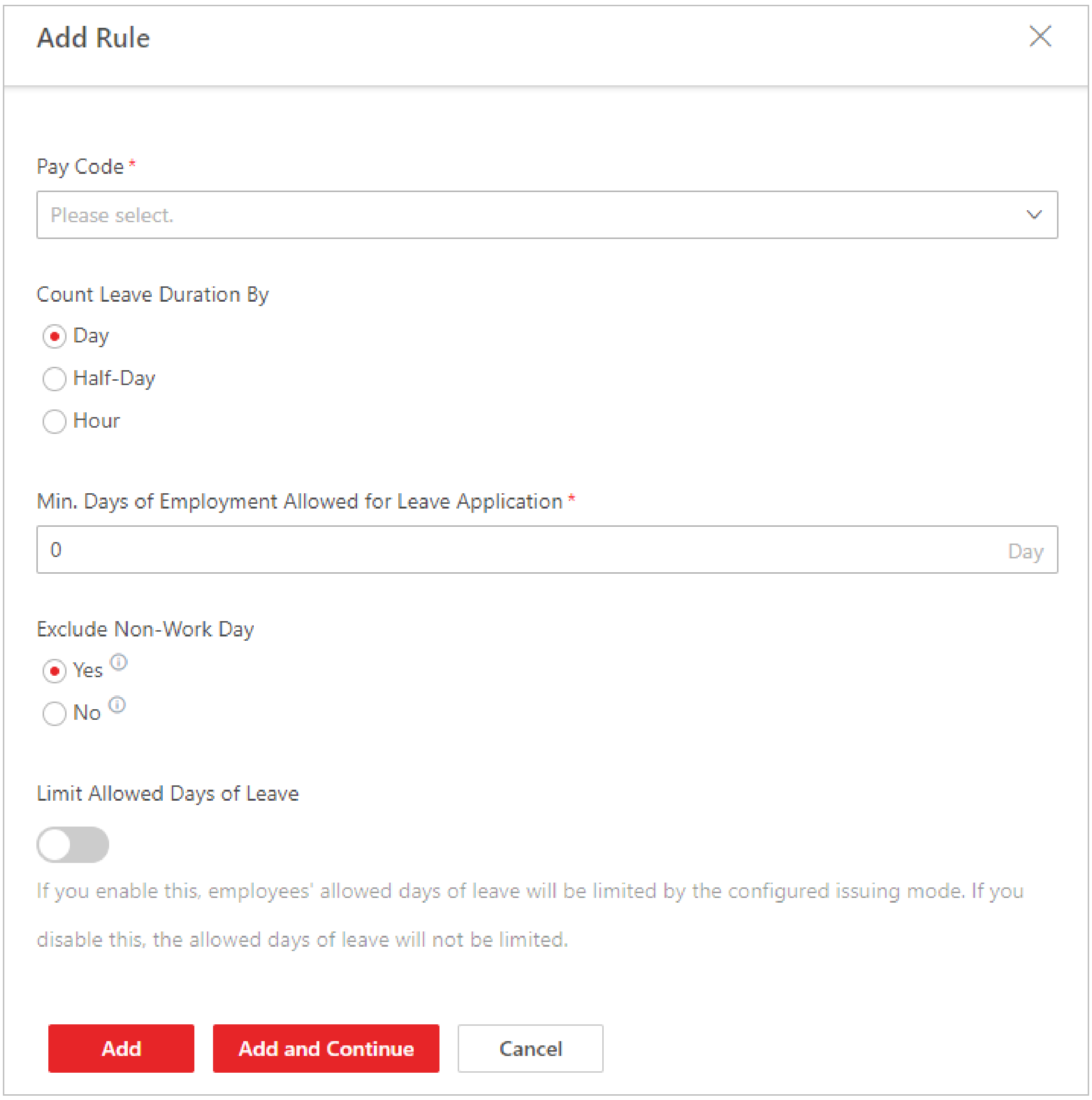


Figure 30-12 Add Rule

   4) **Optional:** Enable **Limit Allowed Days of Leave** and set the related parameters.

Issuing Mode

Auto Issue Annually

The platform issues allowed days of leave to employees on a specified day each year. You need to select an issuing date and select an issuing rule.

Issuing Rule

Fixed Amount

The platform issues the same days of leave to employees each year.

Depends On Employment Years

The issued days of leave depend on the employment years.

Issue All Days of Leave Once

Issue all days of leave to employees once. You need to set the number of days and you can configure expiry date of the days if needed.

7. Save the settings.

30.4.5 Configure Check-In/Check-Out via Mobile Client

After configuring the function of check-in/check-out via mobile client, employees in the platform will be able to check in/out inside the valid geographic scope via the Mobile Client. And the platform will perform attendance calculation of check-in records collected by the Mobile Client.

Click **Check-In/Out Area via Mobile Client** on the left navigation bar.

For Configuration of the First Time

For configuration of the first time, you will enter the following page.

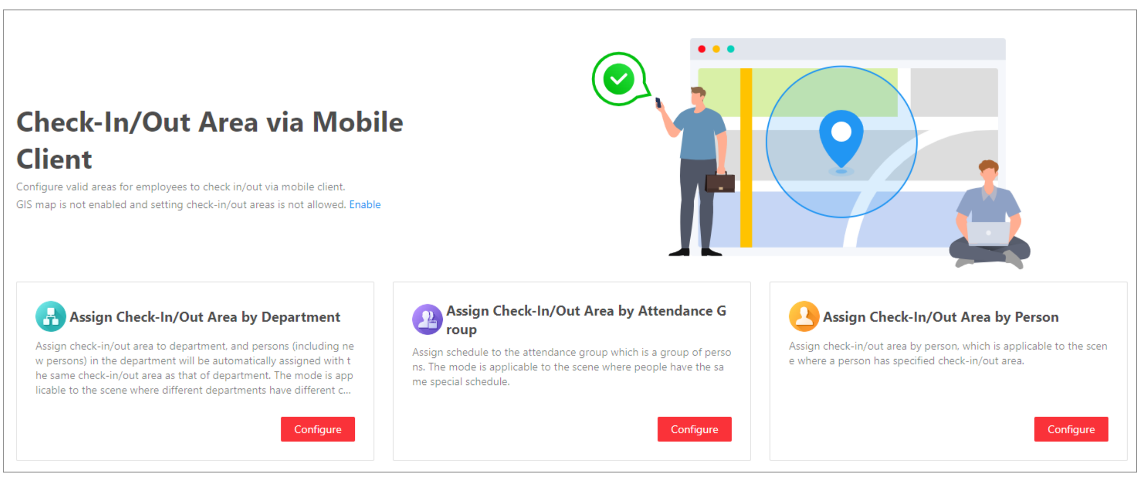


Figure 30-13 Page for Configuration of the First Time

Click **Enable** to enable GIS map, and then click **Configure** to start assigning check-in/out area by department / attendance group / person.

The following shows how to assign check-in/out area by department.
Click **Configure** to show the page of Assign Check-In/Out Area by Department. Select department(s) and click **Next** on the top left. Enter an area name, an draw the area in the radius mode or custom mode. Hover the cursor on the edge of the area and drag to change the scope.

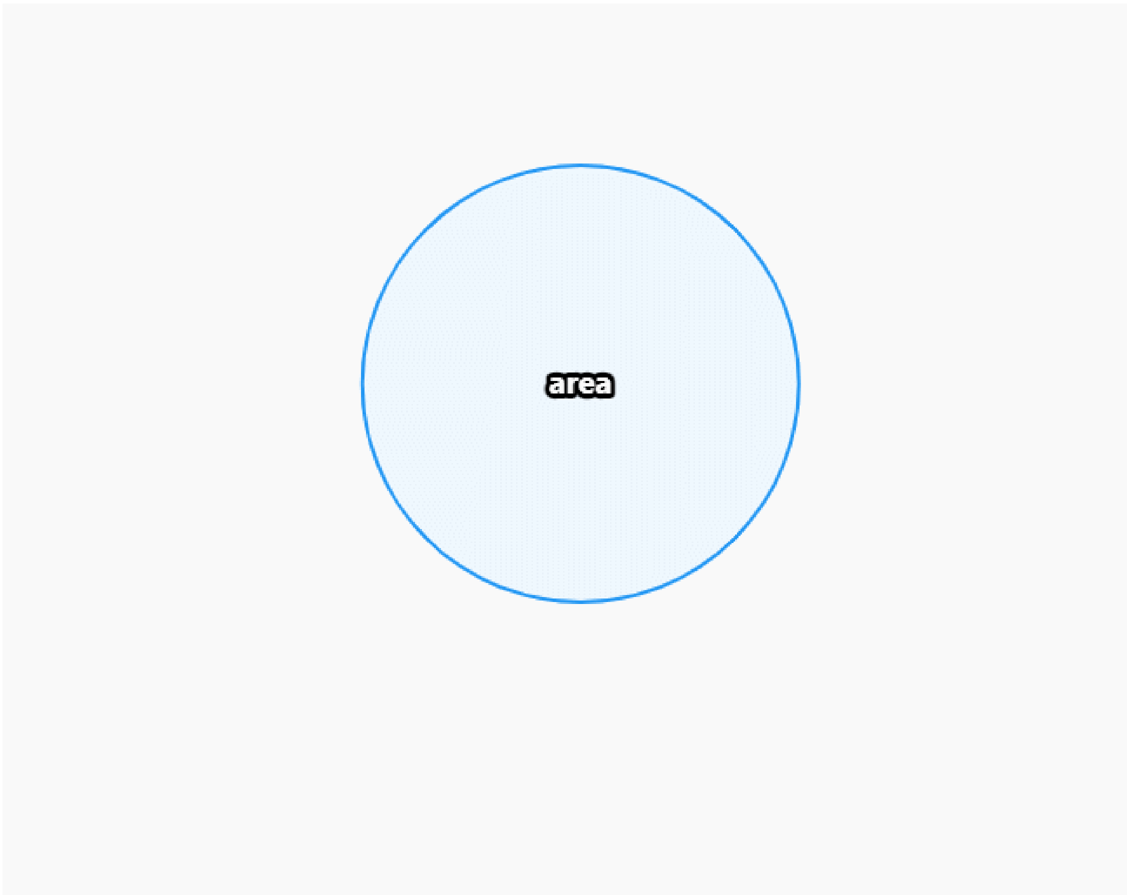


Figure 30-14 Draw Check-In/Out Area

For Configuration of Not the First Time

For configuration of the first time, you will enter the following page.

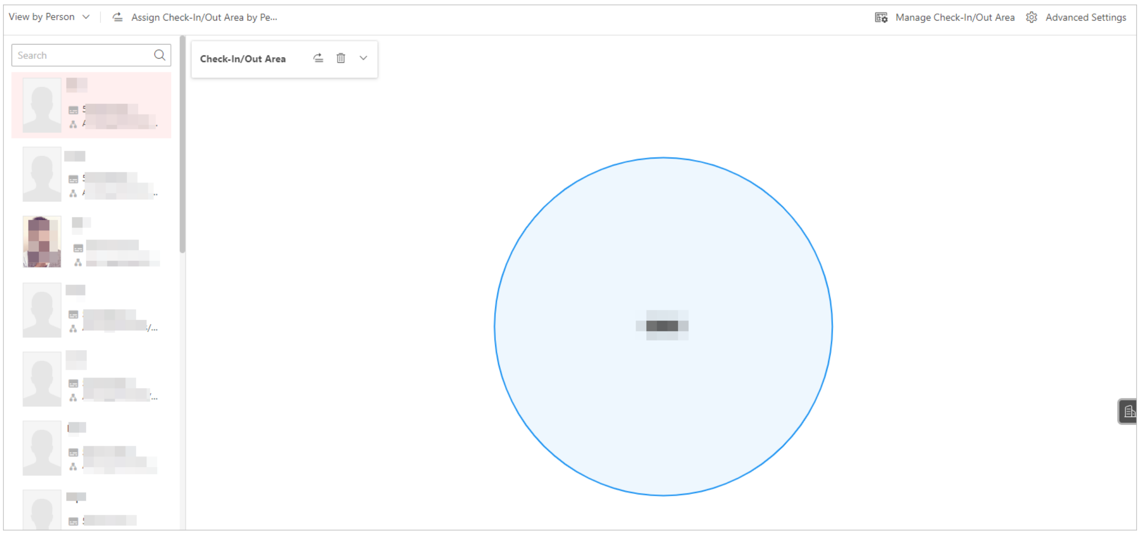


Figure 30-15 Page for Configuration of Not the First Time

Manage Check-In/Out Area

Add/edit/delete check-in/out area(s).

Advanced Settings

Set requirements for employees when checking in/out, approval method of check-in/out, and configure GIS map.

View by Department / Attendance Group / Person

Select the view mode of check-in/out.

You can also select a person /attendance group / department, and click to select check-in/out area(s).

30.4.6 Configure Storage Settings

You can set the storage location of the attachment in exception application.

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Basic Configuration** → **Storage Settings** on the left.
3. Select a backup file to be restored.
4. Click **Save**.

30.5 Configure Attendance Rules for Global / Department / Attendance Group

The attendance rule indicates a set of parameters about time and attendance, including the weekend settings, absence rule, overtime parameters, attendance calculation mode, holiday settings, the calculation of leaves, the authentication mode selection of attendance check, etc. It can be defined as a global rule, department rule, or group attendance rule. You can configure an attendance group with a group attendance rule which has higher priority than the department rule. You can also configure a department with a department rule which has higher priority than the global rule used for the whole company or institution.

30.5.1 Define Weekends

Different countries or regions adopt different weekend convention. HikCentral Professional provides weekends definition function. You can select one or more days of week as the weekends according to actual situation.

On the top left, select → **Integrated Service → Attendance → Attendance Rule → Global Rule / Department Rule / Group Rule** . For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups.

In the Weekend Settings area, select the day(s) of week from Monday to Sunday. The attendance data of the selected date(s) will be calculated with the weekend rule.

30.5.2 Configure Attendance Calculation Mode

You can set the mode of attendance calculation.

Choose a calculation mode of work duration.

Calculated by

First In & Last Out: Only count and calculate the duration of the first and last check-in/out records within the valid check-in/out period.

Each Check-In/Out: Count each check-in/out record within the valid check-in/out period and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/out records.

Enable T&A Status on Device

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

Note

- If a break timetable in the timetable is not enabled with T&A Status on Device, it will be enabled if you enable this function for the timetable.

If a break timetable in the timetable is already enabled with T&A Status on Device, this setting will not change even if you disable the function for the timetable.
- To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

Day Change Time

Set a time to mark the change of a day. For example, if the day change time is set as 08:00:00, check-in before 08:00:00 will be calculated into the attendance of the previous day, and check-in after 08:00:00 will be calculated into the attendance of the current day.

30.5.3 Define Absence

You can define the absence rule in the global dimension or define an absence rule for a certain department or attendance group. When the employee's attendance conforms to the absence rule, the attendance record will be marked as absent or other status you define.

On the top left, select → **Integrated Service → Attendance** . Select **Attendance Rule → Global Rule / Department Rule / Group Rule** on the left. For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups. Click **Attendance Calculation** on the right.

In the Absence Settings area, you can define the absence rules.

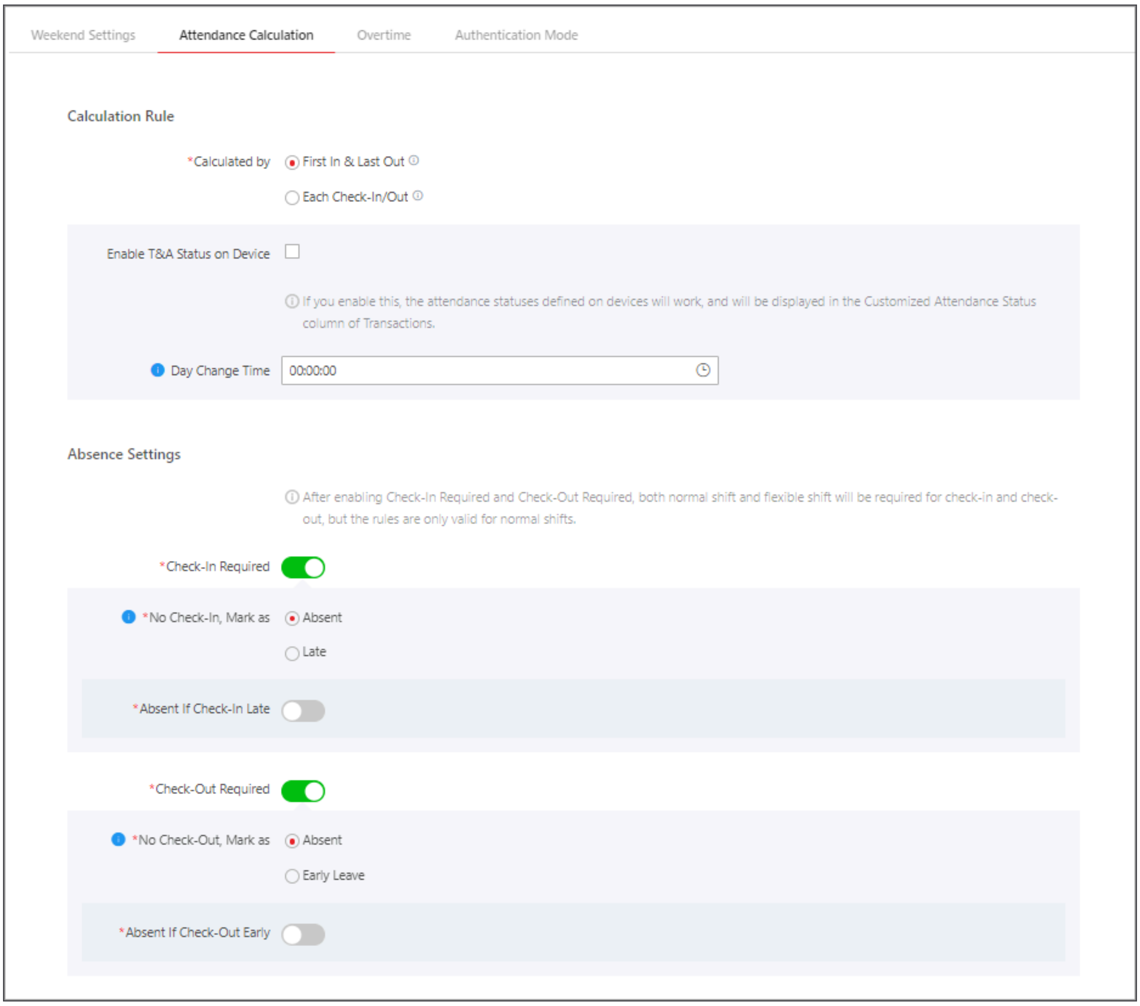


Figure 30-16 Absence Settings

Set Absence Rule for Check-In

Switch on **Check-In Required**. Once this function is disabled, employees will not be required to check in.

In **No Check-In, Mark as**, specify an attendance status when a person does not check in or fails to check in within the valid check-in period. If you select **Late**, you need to set a fixed late duration. For example, if the scheduled start work time is 9:00, valid check-in period is 6:00-12:00 (defined in Timetable - Attendance), **Late Duration** is set to 60 minutes, and **No Check-In, Mark as** is set to **Absent**, the attendance status of an employee will be:

- Normal, if the employee checks in between 6:00 and 9:00.

Note

You can set overtime rules to count the extra hours before scheduled start work time as overtime. See details in ***Configure Overtime Parameters*** .

- Late, if the employee checks in between 9:01 and 9:59.
- Absent, if the employee checks in after 10:00 or does not check in.

Switch on **Absent If Check-In Late** and set a tolerant threshold in **Late for**. When the employee's check-in time minus scheduled start work time is longer than the **Late for** value, the employee's attendance status on that day will be marked as Absent.

Set Absence Rule for Check-Out

Switch on **Check-Out Required**. Once this function is disabled, employees will not be required to check out.

In **No Check-Out, Mark as**, specify an attendance status when a person does not check out or fails to check out within the valid check-out period. If you select **Early Leave**, you need to set a fixed late duration.

For example, if the scheduled end work time is 18:00 and valid check-out period is 17:00-21:00 (defined in Timetable - Attendance), and **Early for** is set to 60 minutes, the attendance status of an employee will be:

- Absent, if the employee checks out before 17:00 or does not check out.
- Early Leave, if the employee checks out between 17:01 and 17:59.
- Normal, if the employee checks out between 18:00 and 21:00.

Note

You can set overtime rules to count the extra hours after scheduled end work time as overtime. See details in ***Configure Overtime Parameters*** .

Switch on **Absent If Check-Out Early** and set a tolerant threshold in **Early for**. When the scheduled end work time minus employee's check-out time is longer than the **Early for** value, the employee's attendance status on that day will be marked as Absent.

30.5.4 Add Holidays Requiring Attendance

You can set a holiday that requires normal attendance as in weekdays.

Steps

1. On the top left, select → **Integrated Service → Attendance** .
2. Select **Attendance Rule → Global Rule / Department Rule / Group Rule** on the left.
3. **Optional:** For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups.
4. Select the **Attendance Calculation** tab.

Note

For details of adding a holiday, see ***Add a Holiday*** .

5. In **Holidays Requiring Attendance** area, select a holiday that requires attendance. You can click **Add** to add a holiday.

Add a Holiday

You can add the holiday to define the special days that can adopt a different schedule or access schedule. You can set a regular holiday or an irregular holiday according to the actual scene.

Steps

1. On the top left, select **→ Integrated Service → Attendance** .
2. Select **Basic Configuration → Holiday Settings** on the left. You can also access the Holiday Settings page in **System** on the top.
3. Click **Add** to add a holiday.

Regular Holiday

The regular holiday is suitable for the holiday that has a fixed date. For example, Christmas is on December 25th of every year.

You can set the **Start Time** and the number of daysfor the holiday, and choose whether to **Repeat Annually** in the system.

Irregular Holiday

The irregular holiday is suitable for the holiday that is calculated by the day in a specific week, and the specified date might be different every year. For example, Mother's Day is on the second Sunday of each May.

For the **Start Time**, you can set the start day of the holiday. For example, select May, Second, and Sunday for Mother's Day. Then, you can set the number of days for the holiday, and choose whether to **Repeat Annually** in the system.

30.5.5 Calculation of Leaves

You can set the status of leaves as normal attendance, leave, or absent.

On the top left, select **→ Attendance** . Select **Attendance Rule → Global Rule / Department Rule / Group Rule** on the left.

Note

For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups.

Select the **Attendance Calculation** tab. In the **Leave Settings** area, you can choose to mark leave as **Normal**, **Leave**, or **Absent**. The leave status will be displayed in the attendance results.

30.5.6 Configure Overtime Parameters

Overtime is the amount of time a person works beyond scheduled work hours. You can configure parameters, including work hour rate, overtime level, and attendance status for overtime, for workdays, weekends, and holidays.

Steps

1. On the top left, select → **Integrated Service → Attendance** .
2. Select **Attendance Rule → Global Rule / Department Rule / Group Rule** on the left.
3. **Optional:** For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups on the left.
4. Select **Overtime** on the right to enter the overtime settings page.
5. In the Overtime on Workday/Weekend area, switch on **Calculate Overtime** to set the calculation mode of overtime duration on workdays and weekends.

Calculation Mode

Select a calculation mode.

By Total Work Hours

Overtime is calculated according to the extra work hours that exceed the required work hours.

OT Duration Calculation Mode

Select a method for overtime duration calculation.

Fixed

Overtime duration is fixed regardless of the actual overtime. You need to set a fixed duration in the **Overtime Duration** field.

Actual

Count the actual duration of the overtime. You need to set a minimum threshold for a valid overtime.

For example, if you set the threshold to 60 minutes:

- Overtime duration is 0 if a person works for 59 minutes longer than the required work hours;
- Overtime duration is 61 if a person works for 61 minutes longer than the required work hours.

By Time Points

Overtime duration is calculated according to the extra work hours earlier than the start-work time or later than end-work time in one day.

You can enable **Count Early Check-In as OT** and **Count Late Check-Out as OT** to set the overtime duration calculation mode respectively.

OT Duration Calculation Mode

Select a method for overtime duration calculation.

Fixed

Overtime duration is fixed regardless of the actual overtime. You need to set a fixed duration in the **Overtime Duration** field.

Actual

Count the actual duration of the overtime. You need to set a minimum threshold for a valid overtime.

For example, if you set **Earlier than Check-In Time for Mark as Valid Overtime** to 30 minutes, and the start-work time is 9:00:

- Overtime duration is 0 if a person checks in at 8:31.
- Overtime duration is 31 if a person checks in at 8:29.

Overtime Level Settings

Click **Configure Rule** to open the Configure Overtime Rule window. Select an attendance data, and click **Add Rule** to set a total overtime duration and select an overtime mode. You can click **Copy** to copy another day's overtime rule. The total work hours will be calculated according to the work hour rate of each overtime level.

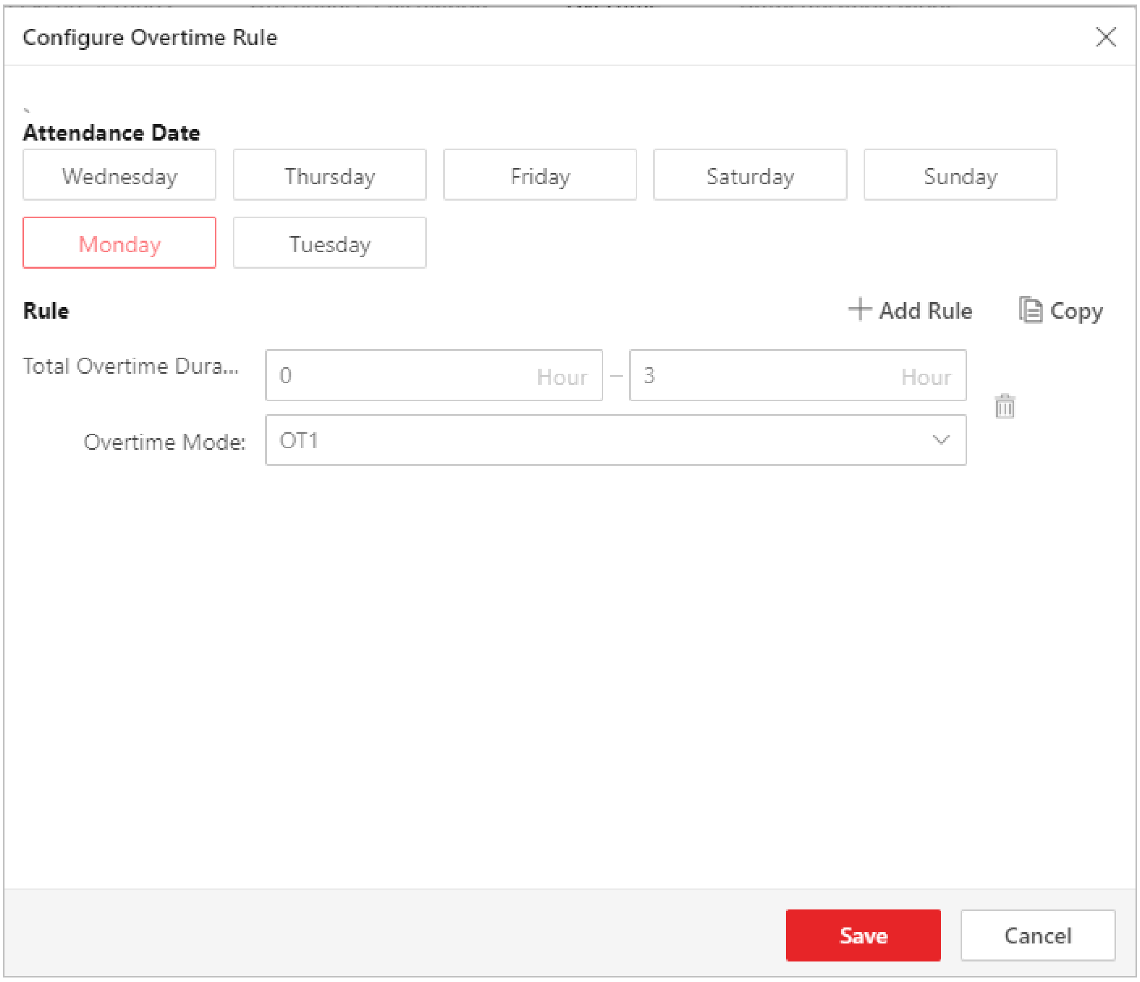


Figure 30-17 Configure Overtime Rule

Overtime on Weekends

You can switch on **Overtime on Weekends** and set the valid overtime threshold. Then when a person's work hours on weekends are less than the threshold, the overtime will be 0.

6. In the Overtime on Holidays area, switch on **Calculate Overtime**, and then set the overtime rule for holidays.

If Works Longer than Mark as Valid Overtime

Set a minimum threshold for a valid overtime.

Set Max. Overtime

Switch on to set an upper limit for the overtime duration in the **If Works Longer than Mark as Invalid Overtime** field. Exceeded work hours will not be counted as valid overtime.

Overtime Level on Holiday

Set the overtime level for each holiday.

You can select multiple holidays and click **Batch Set Overtime Level** to batch set the overtime level, or set the overtime level for each holiday separately.

Note

- To add a new holiday, click **Add Holiday**.
- To edit holidays, click **Holiday Settings**.

7. **Optional:** Switch on **Calculate Overtime** in the Overtime Not in Valid Attendance Check Period area to count the extra work time outside the valid check-in/out period as valid overtime. And then select an overtime level from the drop-down list.
8. For global rules, click **Save**; for department rules, click **Add** on the top right.

30.5.7 Configure Authentication Mode

You can configure authentication modes, including card, fingerprint,, face, and iris. After setting authentication mode, you can get attendance records of the configured authentication mode and calculate attendance data of the configured authentication mode.

On the top left, select → **Attendance** . Select **Attendance Rule → Global Rule / Department Rule / Group Rule** on the left. Select **Authentication Mode** on the right.

Note

For department rules and attendance group rules, you need to click **Add** on the Department Rule or Group Rule page, and then check departments or attendance groups.

Switch on **Customize Authentication Mode**, and select card, fingerprint, iris, or/and face as the authentication mode.

Note

This function requires device capability.

30.6 Add Timetable

The timetable defines the detailed time rules for attendance, such as work time, break time, etc. According to the actual requirements, you can select normal shift or flexible shift as timetable type for further configuration and application, and then the employees need to follow the time rules to check in, check out, etc.

30.6.1 Add Break Timetables

Break timetables define the start/end time of breaks and the calculation method of break duration. You can create break timetables in advance and use them as templates when configuring break time in a timetable.

Steps

1. On the top left, select ▦ → **Integrated Service → Attendance** .
2. Select **Shift Settings → Break Timetable** on the left.
3. Click **Add**.
4. Set parameters for the break timetable.

Name

Create a descriptive name for the break timetable, such as "Launch Break".

Start Time

Start time of the break.

Earliest Allowable Start Time

Flexible start time of the break. If a person checks out earlier than **Earliest Allowable Start Time**, the check-out will not be counted as the break start time and no break will be recorded.

End Time

End time of the break.

Latest Allowable End Time

Flexible end time of the break. If a person checks in later than **Latest Allowable End Time**, the check-in will not be counted as the break end time.

Break Duration Calculation Mode

Method for counting the duration of a break.

Period

Fixed duration. The actual break start/end time of persons will only be recorded but not be used to calculate the duration of breaks.

Break Duration

Set the duration of the break.

Must Check

Actual duration calculated by the check-out time and check-in time.

In **Count Early/Late Return**, you need to choose to count early or late return time **By Duration** or **By Time Point**.

By Duration

When the actual break duration (end time minus start time) is shorter than or longer than the specified duration, it will be counted as early or late return.

By Time Point

When the actual return time is earlier than or later than the specified end time, it will be counted as early or late return.

You also need to set the threshold and the attendance status for the early/late return time.

If early/late for

Threshold for counting the early/late return time.

Mark as

Choose to count the remaining time of a early return as overtime or the exceeded time of a late return as late, early leave, or absent.

If you do not want to count the early/late return time, set it to **Normal**.

Set Calculation Mode

Switch on to set the calculation method of break duration.

Calculated by

First In & Last Out: Only count and calculate the duration of the first and last check-in/out records during the start/end time of the break.

Each Check-In/Out: Count each check-in/out record during the start/end time of the break and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/outs.

Enable T&A Status on Device

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

Note

To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

5. Click **Add** to finish adding the timetable, or click **Add and Continue** to finish adding the timetable and add a new break timetable.
6. **Optional:** Perform further operations after adding the break timetable.

Edit Break Timetable	Click on the name of a break timetable to edit it.
Delete Break Timetable	Select the break timetables you want to delete and click **Delete** to delete them.

What to do next

Use the break timetable to set the break time in a timetable. See ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .

30.6.2 Add Timetable for Normal Shift

Normal shift is usually used for the attendance with fixed schedule. The employees should check in before the start-work time and check out after the end-work time. Otherwise, their attendance status will be late, early leave, or absent. You can add the timetable for normal shift to define the detailed rules (e.g., start-work time, end-work time, late rule, valid check-in/out time, break time, etc.), in order to monitor employees' working hours and attendance.

Steps

1. On the top left, select ▦ → **Integrated Service → Attendance → Shift Settings → Timetable** .
2. Click **Add**.
3. Configure the **Basic Settings**.
   1) On the top, create a timetable name.
   2) Click on the **Color** field and set the color for the timetable. Different colors represent the corresponding timetables when drawing for Schedule in time bar.
   3) Select **Normal Shift** as the time period type, and set the following parameters.

Scheduled Work Time

Range of the scheduled work time, including start-work time and end-work time.

Valid Check-In Period

If the employee does not check in during the valid check-in period, the check-in will not be recorded and the attendance status will be absent or late depending on the absence settings.

Note

It is allowed to set the valid check-in period crossing days, therefore the time period can be more than 24 hours. For example, you can set the start time to 08:00:00 on the previous day, set the end time to 10:00:00 on the current day.

Valid Check-Out Period

If the employee does not check out during the valid check-out period, the check-out will not be recorded and the attendance status will be absent or early leave depending on the absence settings.

Note

It is allowed to set the valid check-out period crossing days, therefore the time period can be more than 24 hours. For example, you can set the start time to 18:00:00 on the previous day, set the end time to 19:00:00 on the current day.

Min. Work Hours

Employees' work duration in one day must be longer than minimum work hours. Otherwise, the attendance status will be absent.

Flexible Mode

Allow Late/Early Leave

The employees are allowed to arrive late or leave early for a specific period of time. For this mode, you need to set the allowable time for late and early leave. If an employee checks in/out within the period after the start-work time or before the end-work time, the attendance status will be **Normal**. For example, if the start-work time is set to 09:00:00, and the late allowable duration is 30 minutes, and the employee checks in at 09:15:00, the attendance status will be **Normal**.

Flexible Period

Flexible period allows employees to extend their start-work time and end-work time. For this mode, you need to set the flexible duration, which defines the extended duration for both start-work time and end-work time. If the total late and early leave time is within the flexible duration, the attendance status will be **Normal**. For example, if the scheduled work time is set to 09:00:00 to 18:00:00, and the flexible duration is 30 minutes, and the employee checks in at 09:15:00, and checks out at 18:15:00, the attendance status will be **Normal**.

4. In **Break Period**, set the following parameters.

Break Time

Click **Add** to select one or multiple break timetables. For adding timetables, see ***Add Break Timetables*** .

Exclude Break Duration from Work Hours

Enable the function and set the break duration which will not be counted into work hours.

5. In **Attendance Calculation**, set the following parameters.

Note

The attendance calculation rule has higher priority than the department and global rules.

Set Calculation Rule

Switch on to set the calculation method of work duration.

Calculated by

First In & Last Out: Only count and calculate the duration of the first and last check-in/out records within the valid check-in/out period.

Each Check-In/Out: Count each check-in/out record within the valid check-in/out period and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/out records.

Enable T&A Status on Device

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

Note

- If a break timetable in the timetable is not enabled with T&A Status on Device, it will be enabled if you enable this function for the timetable.

If a break timetable in the timetable is already enabled with T&A Status on Device, this setting will not change even if you disable the function for the timetable.

- To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

Day Change Settings

Switch on to set the day change time.

Absence Settings

Set a different absence rule instead of using the general absence rule.

Note

See details about setting a general absence rule in ***Define Absence*** . You can also refer to this topic for explanations for the parameters in the absence rule.

6. In **Overtime**, switch on **Count Timetable as Overtime**, and set the following parameters.

Note

- The overtime timetable has higher priority than the department and global rules.
- See details about setting an overtime timetable in ***Configure Overtime Parameters*** . You can also refer to this chapter for explanations of the parameters.

7. **Optional:** In **Timetable Overview**, view the timetable in a time line.

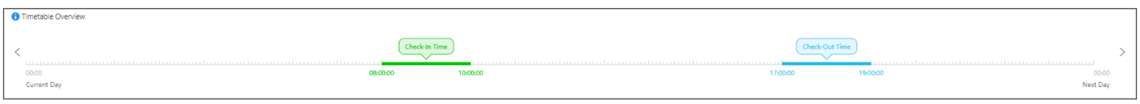


Figure 30-18 Timetable Overview

Note

You can drag the time line to the left or right.

8. Click **Add** to save the timetable, or click **Add and Continue** to continue adding another timetable.

What to do next

Use the timetables to define the work schedule on each day in a shift. For more details, refer to ***Add Shift*** .

30.6.3 Add Timetable for Flexible Shift

Flexible shift is usually used for the attendance with flexible schedule. It does not require a strict check-in time and check-out time and only requires that the employees' work hours are longer than the minimum work hours.

Steps

1. On the top left, select ▦ → **Attendance** → **Shift Settings** → **Timetable** .

2. Click **Add**.
3. Configure the **Basic Settings**.
   1) On the top, create a timetable name.
   2) Click on the **Color** field and set the color for the timetable. Different colors represent the corresponding timetables when drawing for Schedule in time bar.
   3) Select **Flexible Shift** as the time period type, and set the following parameters.

   Valid Check-In/Out Period

   If the employee does not check in/out within the valid check-in/out period, the check-in/out will not be recorded and the attendance status will be late or absent.

   Min. Work Hours

   Employees' work duration in one day must be longer than minimum work hours. Otherwise, the attendance status will be absent.

   Latest Check-In Time

   If the actual check-in time is later than this time, the attendance status will be marked as Late.
4. In **Break Period**, click **Add** to select the break timetables to define the break time in the timetable.

Note

- You can click **Add** to create a new break timetable. See details in ***Add Break Timetables*** .
- Enable **Exclude Break Duration from Work Hours** and set the break duration which will not be counted into work hours.

5. In **Attendance Calculation**, switch on **Set Calculation Mode**, and set the following parameters.

Note

The attendance calculation rule has higher priority than the department and global rules.

Calculation Rule

Calculated by

First In & Last Out: Only count and calculate the duration of the first and last check-in/out records within the valid check-in/out period.

Each Check-In/Out: Count each check-in/out record within the valid check-in/out period and calculate the total duration. You need to set a minimum interval in **Min. Interval** to filter out repeated check-in/out records.

Enable T&A Status on Device

Check to record the T&A status on the attendance check devices.

Uncheck to discard the T&A status on the devices and only record the person information and check-in/out time.

Note

- If a break timetable in the timetable is not enabled with T&A Status on Device, it will be enabled if you enable this function for the timetable.
  If a break timetable in the timetable is already enabled with T&A Status on Device, this setting will not change even if you disable the function for the timetable.
- To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

Day Change Settings

Switch on to set the day change time.

Absence Settings

Set a different absence rule instead of using the general absence rule.

Note

See details about setting a general absence rule in ***Define Absence*** . You can also refer to this topic for explanations for the parameters in the absence rule.

6. In **Overtime**, switch on **Count Timetable as Overtime**, and set the following parameters.

Note

- The overtime timetable has higher priority than the department and global rules.
- See details about setting a overtime timetables in ***Configure Overtime Parameters*** . You can also refer to this topic for explanations for the parameters.

7. **Optional:** In **Timetable Overview**, view the timetable in a timeline.

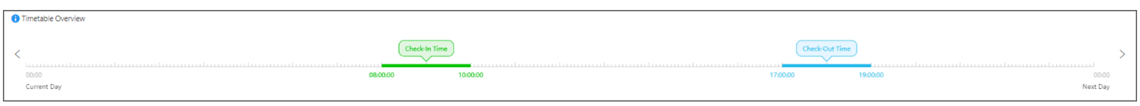


Figure 30-19 Timetable Overview

Note

You can drag the timeline to the left or right.

8. Click **Add** to save the timetable, or click **Add and Continue** to continue adding another timetable.

What to do next

Use the timetables to define the work schedule on each day in a shift. For more details, refer to ***Add Shift*** .

30.7 Add Shift

Shift is the time arrangement for employees. Shifts can be assigned to employees to regulate their duties. You can adopt one or multiple timetables in one shift.

Before You Start

Make sure you have added timetables. See details in ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .

Steps

1. On the top left, select → **Attendance → Shift Settings → Shift** .
2. Click **Add**.
3. Set the shift's basic information, including creating a descriptive name and editing its description.
4. **Optional:** Select another shift from the drop-down list of **Copy from** field to copy the shift information to the current shift.
5. Set the shift's repeating pattern.

   Week

   The shift will repeat every 1 to 52 weeks based on your selection.

   Day

   The shift will repeat every 1 to 31 days based on your selection.

   Month

   The shift will repeat every 1 to 12 months based on your selection.
6. Select a timetable and click on the table below to apply the timetable on each day.

   Note

   You can use up to 8 different timetables in one shift.
7. Switch on **Configure Attendance During Holidays**, and select the holidays. On holidays, the shift will not be effective.
8. Click **Add** to finish adding the shift.

What to do next

Assign shift to persons or departments. See details in ***Assign Schedule to Person*** or ***Assign Schedule to Department*** .

30.8 Manage Schedule

Schedule is used to specify the persons and effective periods during which the persons perform their duties following the attendance rule defined in the shift. After setting the shift, you need to assign it to the department or persons, or add a temporary schedule, so that it will calculate the attendance records for persons according to this schedule.

30.8.1 Schedule Overview

The schedule overview shows the schedule information of each person in the department / attendance group. You can also view the detailed schedule of one person for each day in one month/week.

On the top left, select ▦ → **Attendance** → **Schedule** → **Schedule Overview** .

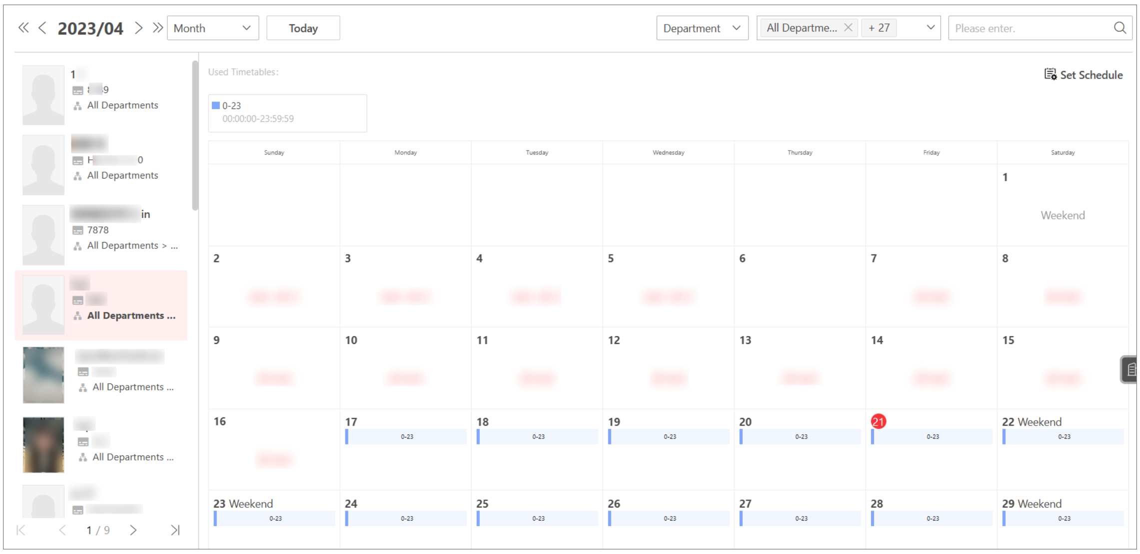


Figure 30-20 Schedule Overview

On the top, select **Department** / **Attendance Group** to view the schedule information by department or attendance group.

Select specific department / attendance group.

Note

- You can check **Include Sub-Department** to display the persons of sub-departments.
- You can enter keywords to search for specific departments / attendance groups.

On the left, you can view the schedule information about every person in the department / attendance group.

Click the person name to enter the detailed schedule of this person for each day in one month, such as effective period, schedule name, and so on.

You can perform the following operations.

- Select **Month**/**Week** to view the schedule by month or week.
- Click **Today** to locate today in the schedule.

- Click **Set Schedule** to edit the schedule. For details, see ***Assign Schedule to Department*** and ***Assign Schedule to Attendance Groups*** .
- On the upper-right corner, enter the keyword to search for specific persons to view schedules related to them.

30.8.2 Assign Schedule to Department

After setting the shift, you need to assign it to the department so that it will calculate the attendance records for persons in the department according to this schedule.

Before You Start

Make sure you have added departments and persons.

Steps

1. On the top left, select **Schedule → Department Schedule** .
2. Open the add schedule page.
3. Set schedule parameters.

   Effective Period

   The shift is effective within the period you set.

   Shift

   Select a shift to be assigned, and you can click **View** to preview the schedule.

   Note

   You can click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .
4. **Optional:** Click to select attendance check points linked with the schedule.

   Note

   Only authentications at the linked attendance check points will be counted.
5. **Optional:** Switch on **Configure Check In/Out Not Required**, check one of the following parameters if needed.

   Check-In Not Required

   Persons in the person group(s) in this schedule do not need to check in when they arrive.

   Check-Out Not Required

   Persons in the person group(s) in this schedule do not need to check out when they leave.

   Effective for Overtime

   The overtime of the persons in the person group(s) in this schedule will be recorded.
6. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.

30.8.3 Assign Schedule to Attendance Groups

After setting the shift, you need to assign it to an attendance group so that the platform will calculate the attendance records for persons in the group according to this schedule.

Before You Start

Make sure you have added an attendance group and persons. For details, refer to ***Add an Attendance Group*** .

Steps

1. On the top left, select **Schedule → Group Schedule** .
2. Click **Add Schedule** to open the Add Schedule pane on the right.
3. In the Attendance Group area, check group(s) you want to assign a schedule to.

   Note

   You can click **Add Attendance Group** to add a new one.
4. Set schedule parameters.

   Effective Period

   The shift is effective within the period you set.

   Shift

   Select a shift to be assigned.

   Note

   - click **View** to preview the schedule.
   - Click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .

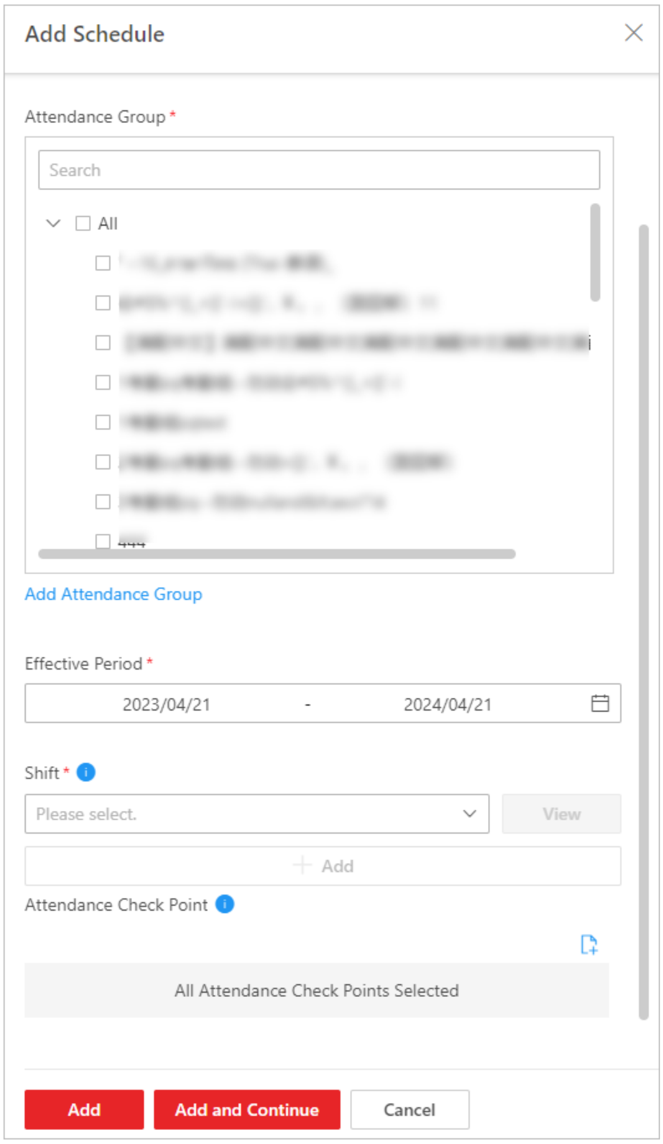


Figure 30-21 Add Schedule

5. **Optional:** Click to select attendance check point(s) linked with the schedule.

Note

Only authentications at the linked attendance check points will be counted.

6. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.

30.8.4 Assign Schedule to Person

You can add a person schedule and assign a shift to one or more persons, so that it will calculate the attendance records for the persons according to this schedule.

Before You Start

Make sure you have added the person(s).

Steps

Note

The person schedule has the higher priority than department schedule.

1. On the top left, select **Schedule → Person Schedule** .
2. Click **Add Schedule** to enter the Add Schedule page.
3. On the Add Schedule pane, click to select person(s) you want to assign schedule to,
4. Set required parameters.

   Effective Period

   Within the period you set, the shift is effective.

   Shift

   Select a shift to be assigned, and you can click **View** to preview the schedule.

   Note

   You can click **Add** to add another shift if needed. For operation details, refer to ***Add Shift*** .
5. **Optional:** Click to select attendance check points linked with the schedule.

   Note

   Only authentications at the linked attendance check points will be counted.
6. **Optional:** Switch on **Configure Check In/Out Not Required**, check one of the following parameters if needed.

   Check-In Not Required

   Persons in the person group(s) in this schedule do not need to check in when they arrive.

   Check-Out Not Required

   Persons in the person group(s) in this schedule do not need to check out when they leave.

   Effective for Overtime

   The overtime of the persons in the person group(s) in this schedule will be recorded.
7. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.
8. **Optional:** Perform the following operations.

Edit Schedule	Select a person in the list and click to edit the person's schedule.
Filter Schedule	Click and set filter conditions such as person name, and then click **Filter** to filter the target schedule.
Delete Schedule	Select one or multiple schedules in the list and click **Delete Schedule** to delete the schedules. Also, you can click **Delete All** to delete all of the schedules.

30.8.5 Add Temporary Schedule

You can add a temporary schedule for a person and the person will be assigned with the schedule temporarily. You can also view and edit the temporary schedule details.

Before You Start

You should have added the person(s) and the shift. For details, refer to ***Add Shift*** .

Steps

Note

The temporary schedule has the higher priority than other schedules.

---

1. On the top left, select **Schedule → Temporary Schedule** .
2. Click **Add** to enter Add Temporary Schedule page.
3. In **Select Person** area, click and select the needed persons.
4. In **Select Timetable(s)** area, select the needed timetable.

   Note

   You can also click to add timetable if needed. For details, refer to ***Add Timetable for Normal Shift*** or ***Add Timetable for Flexible Shift*** .

   ---
5. Above the calendar, select the year and month.
6. In the calendar area, click one or multiple dates, then the selected timetable will be added to the selected date(s).
7. **Optional:** In the specific date of the calendar, click and select whether to perform the following operations.

   Clear Shifts

   Click to clear all schedules of the selected date.

   Restore to Initial Schedule

   Click to cancel the adding and restore to the initial schedule.

   Specify Attendance Check Points

   Click to select specific devices as the attendance check points. By default, all devices are attendance check points.
8. Click **Finish** on the top right.

30.9 Configure Calculation Mode of Attendance Results

You can set the attendance calculation mode as manual calculation or auto calculation.

30.9.1 Manually Calculate Attendance Results

If department or schedule changes or abnormal attendance records are handled, you can recalculate the attendance results according to the latest data. After re-calculation, the original results will be replaced by new attendance results.

Steps

Note

HikCentral Professional can calculate the attendance data automatically at a fixed time point (4 o'clock by default) every day. You can edit the time point in **Attendance → Attendance Calculation → Auto Calculation** .

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Attendance Calculation** on the left, and then select **Manual Calculation** on the right.
3. Set the start time and end time for attendance calculation.
4. Select target person(s) for attendance calculation.
   - **All Persons**: Calculate all persons' attendance records.
   - **Specified Attendance Group(s)**: Select one or multiple attendance groups for calculation.
   - **Specific Person(s)**: Click to select one or multiple persons for calculation.
5. Click **Calculate**.

   Note

   It can only calculate the attendance data recorded within three months.

30.9.2 Set Auto-Calculation Time of Attendance Results

Attendance results calculation refers to calculating the attendance status and duration according to persons' check-in/out records. You can set an auto-calculation time so that the platform will calculate the attendance results for all persons at a specific time every day.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Attendance Calculation** on the left, and then select **Auto Calculation** on the right.
3. Select a time in **Calculate at**.
4. **Optional:** Enable **Recalculate Historical Data**.
5. Click **Save**.

30.10 Application Management for Employee

If you are an employee, you can log in to the Self-Service module where you can have an overview of your attendance records, review applications (if you are an administrator and assigned with the approval role as reviewer), and view your schedule. Besides, in this module, you can submit applications for leave, overtime, or attendance correction, and view the details and the handling status of applications. You can also view and export attendance records.

30.10.1 Overview of Personal Attendance Data

You can have an overview of your attendance records in a specific time period, review applications, and view personal schedule.

When you log in to the Self-Service module, the overview page will be displayed, which shows the recent and history attendance statistics.

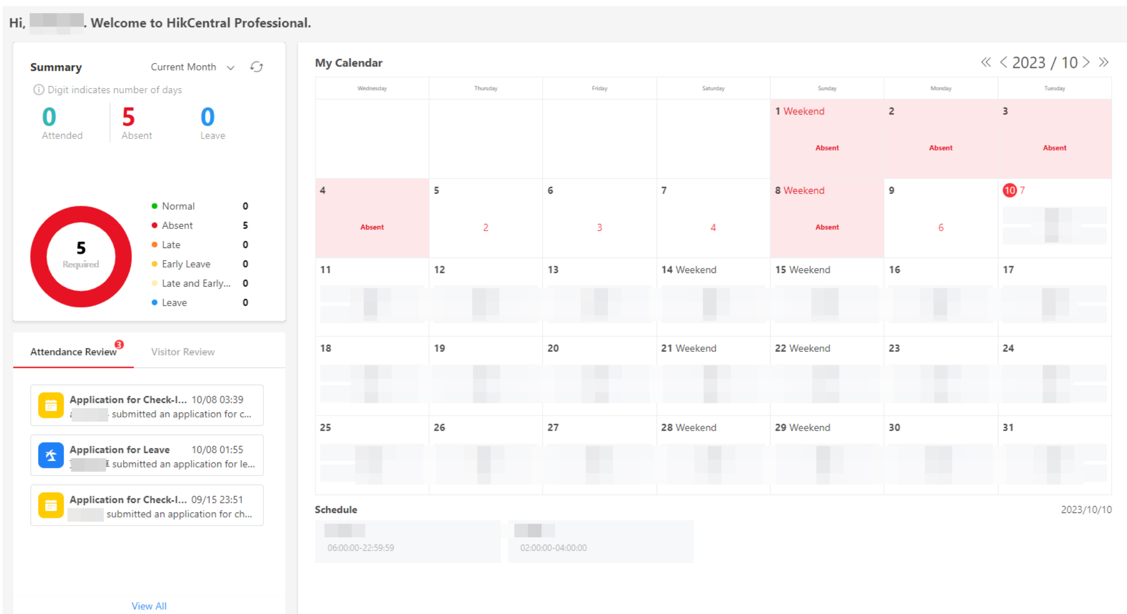


Figure 30-22 Overview of Personal Attendance Data

Summary	Click ⌄ to select a time period to view the attendance records in the time period.
My Calendar	You can have an overview of your attendance data and schedule in a month. Move the cursor to a day on the calendar and click ⚙, you can submit an application for the current day. For details about submitting applications, refer to ***Submit and View Applications*** .
Attendance/Visitor Review	You can select an application and click **Handle** to handle the application.
Schedule	View personal schedule.

30.10.2 Submit and View Applications

As an employee, you can submit attendance applications for leave, overtime, or attendance correction. Also, you can view the application details and the application flow to know the status of each handling.

Note

For details about reserving a visitor, see the chapter of Visitor Management.

Apply for a Leave

As an employee, you can apply for a leave by yourself. And the application will be reviewed by the administrator.

Steps

1. Select **Apply → Leave** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

   Leave Type

   The leave type such as sick leave, maternity leave, annual leave, etc.

   Start Time

   The start time of leave.

   End Time

   The end time of leave.

   Application Reason (Optional)

   The application reason for the leave.

   Attachment (Optional)

   The attachment for the leave application, such as the medical records for sick leave.
5. Click **Add**.

What to do next

View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

Apply for a Check-In/Out Correction

As an employee, you can apply for correcting the check-in or check-out records according to actual need (e.g., you forgot to check in or check out). And the application will be reviewed by the administrator.

Steps

1. Select **Apply → Attendance Correction** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

   Correction Item

   The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.

   Actual Time

   The right time of the attendance item.

   Application Reason (Optional)

   The application reason for the correction.

   Attachment (Optional)

   The attachment for the correction application, such as the certificate of the right attendance time.
5. Click **Add**.

What to do next

View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

Apply for Overtime

As an employee, you can apply for working overtime. And the application will be reviewed by the administrator.

Steps

1. Select **Apply → Overtime** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

   Overtime Type

   The type of working overtime.

   Start Time

   The start time of working overtime.

   End Time

   The end time of working overtime.

   Application Reason (Optional)

   The application reason for the leave.

Attachment (Optional)

The attachment for the overtime application.

5. Click **Add**.

What to do next

View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

Review or Undo Submitted Applications

The employee can review or undo the submitted application(s) for attendance after logging into the self-service account.

Note

Log in to the platform via self-service.

1. Select **Review → Leave / Check In&Out Correction / Overtime / Check-In/Out via Mobile Client / Visitor Reservation** on the left.
2. Select the **Pending** or **Handled** tab.
3. You can perform the following operations in the Operation column after checking applications.
   - Click to approve the employee's attendance application.
   - Click to reject the employee's attendance application.

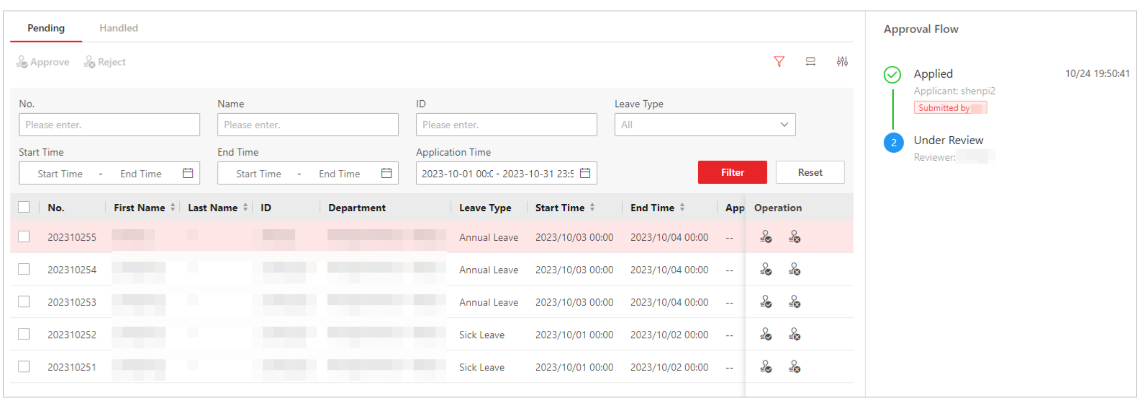


Figure 30-23 Review Employees' Applications

30.10.3 View and Export Attendance Records and Reports

As an employee, you can view the attendance records and reports. Also, you can export the records or reports in the file format of Excel, PDF, or CSV.

Note

Log in to the platform via self-service.

1. Select **Report** on the left.
2. Select the menu item as needed to view the records or report details.
3. You can perform the following operations in the Operation column for application review.
   - Click **Export** to export the records or reports in the file format of Excel, PDF, or CSV..
   - On the top-right corner, click to select the type of self-adaptive column width (complete or incomplete display of each column title).
   - On the top-right corner, click to select the items for custom display in the column.

30.11 Application Management for Admin

The persons' attendance records will be recorded and stored in the system. As the administrator, you can search for the target persons and perform attendance applications for a single person or multiple persons according to the actual need, including applying for leave, overtime, and attendance correction. After submitting applications, you can view the application details and status of each handling. You can also review (approve or reject) and undo applications.

30.11.1 Apply for a Leave

As the administrator, you can perform leave application for the employee one by one.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Application and Approval** → **Leave** .
3. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

   Leave Type

   The leave type such as sick leave, maternity leave, annual leave, etc.

   Start Time

   The start time of leave.

   End Time

   The end time of leave.

   Application Reason (Optional)

   The application reason for the leave.

   Attachment (Optional)

The attachment for the leave application, such as the medical records for sick leave.

Auto Approve (Optional)

If the box is checked, the added application for the person will be approved automatically.

6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

30.11.2 Apply for a Check-In/Out Correction

As the administrator, you can apply for correcting the check-in or check-out records for the employee one by one.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Application and Approval** → **Attendance Correction** .
3. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

   Correction Item

   The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.

   Actual Time

   The right time of the attendance item.

   Application Reason (Optional)

   The application reason for the correction.

   Attachment (Optional)

   The attachment for the correction application, such as the certificate of the right attendance time.

   Auto Approve (Optional)

   If the box is checked, the added application for the person will be approved automatically.
6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

30.11.3 Apply for Overtime

As the administrator, you can apply for working overtime for the employee one by one.

Steps

1. On the top left, select ▦ → **Integrated Service → Attendance** .
2. Select **Application and Approval → Attendance Correction** .
3. **Optional:** Click ▽ , enter a person's full name, card No., ID, etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

   Overtime Type

   The type of working overtime.

   Start Time

   The start time of working overtime.

   End Time

   The end time of working overtime.

   Application Reason (Optional)

   The application reason for the leave.

   Attachment (Optional)

   The attachment for the overtime application.

   Auto Approve (Optional)

   If the box is checked, the added application for the person will be approved automatically.
6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

30.11.4 Import Applications

As the administrator, you can batch apply for leave, overtime, or attendance correction for multiple employees.

Steps

1. On the top left, select ▦ → **Integrated Service → Attendance** .
2. Select **Application and Approval → Leave / Attendance Correction / Overtime** on the left.
3. **Optional:** Click ▽ , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. Click **Import**.
5. In the pop-up window, click **Download Template** and edit the related information in the downloaded template.
6. Click 🗁 and import the template with the corrected attendance records.
7. Click **Import**.

What to do next

You can review or undo the imported applications. For details, refer to ***Review or Undo Applications*** .

30.11.5 Review or Undo Applications

As an administrator, after applying for employees' leave, overtime, attendance correction, or check in&out via Mobile Client, you can review (including approving or rejecting) or undoing the application.

1. On the left, select **Leave / Check In&Out Correction / Overtime / Check-In/Out via Mobile Client**.
2. (Optional) Click to filter the target employee by setting conditions (such as name, ID, department).
3. Select the target employee, the employee's application flow will be displayed on the right.
4. You can perform the following operations.
   - (Optional) Click to view the check in/out areas of the employee.
   - Check employee(s) and click **Approve** to approve the employee's attendance application.
   - Check employee(s) and click **Reject** to reject the employee's attendance application.
   - Check employee(s) and click **Undo** to undo the employee's attendance application.

30.12 View Attendance Records

Persons' attendance records will be recorded and stored in the system. You can view different types of attendance records.

On the top left, select → **Integrated Service** → **Attendance** . Then select **Attendance Record** on the left.

Click **Transaction**, **Time Card**, **Check In&Out Record**, **First & Last Access Report**, **Leave Record**, **Check In&Out Correction Record**, and **Overtime Record** according to your need.

You can perform the following operations on the pages of attendance records.

- Click **Export** to export the report in Excel, PDF, or CSV format. You can also select the calculating dimension of the report.
- For transactions, click **Import** to import transactions recorded in files or devices to the system.
- Click to customize column items.
- After customizing column items, click **Save Layout** to save the current layout for later use.

  Exporting Allowed

  After enabled, the layout can be exported in the report.

  Sharing Allowed

  After enabled, the layout will be shared among accounts.

  Fixed Date

After enabled, you can set a specific time period for attendance data displayed the layout. Only attendance data generated during this time period will be displayed in the layout.

- Click **Load Layout** to display the report in a layout shared by other users. You can search for a layout before loading it. For layout saved by yourself, you can edit or delete them.
- Click to display each column title completely/incompletely.

30.12.1 Import Transactions

Transactions on the attendance check devices could fail to be transmitted to HikCentral Professional due to many causes, such as device offline and network connection failure. Or some of your attendance check devices are not added to the platform, but you still need to manage their transactions on the platform. You can use this function to get the latest transactions from the devices.

On the top left, select → **Integrated Service** → **Attendance** . Then select **Attendance Record** → **Transaction** on the left.

Click **Import** → **Import from Device / Import from File** .

Import from Device

Applicable to getting the latest transactions on the attendance check devices that are added to the platform.
Select the devices that store the transactions, and then select the time range to be imported. Click **OK** to import the transactions within the range on the selected devices.

Import from File

Applicable to attendance check devices added or not added to the platform.

Note

For devices that are not added to the platform, you need to make sure that the devices are supported by the platform. See *HikCentral Professional Compatibility List* for reference.

Many attendance check devices have the ability to export a file that contains persons' transactions. You can import the file to the platform so that the transactions can be managed on the platform.

Note

- To export the data file on an attendance check device, please refer to the user manual of the device.
- Usually, you need to enter the back-stage management page of the device to export the event file to a connected external storage device via USB port, and then transfer the event file to the PC where the platform runs.

30.13 Manage Attendance Reports

Attendance report is the statistics of the attendance results of the specific department(s) or person(s) in a certain time period. For example, the employer or related persons can view the employees' attendance via attendance report and make it as the standard of performance evaluation or pay calculation. You can define the display rules on the report, set the rule of sending reports regularly, add a custom report, and manually export reports.

30.13.1 Set Display Rules for Attendance Report

You can configure the contents displayed in the attendance report, such as the company name, logo, date format, time format.

On the top left, select → **Integrated Service** → **Attendance** → **Basic Configuration** → **Report Settings** → **Report Display** to set the following display rules.

Company Information

The company information (including company name and logo) will be displayed on the cover page of the attendance report. You can customize the company name. You can also upload a picture for the logo.

Note

Hover over your cursor on the uploaded logo picture, and you can click **Delete Logo** to delete the picture.

Format of Date and Time

The formats of date and time may vary for the persons in different countries or regions. You can set the date format and time format according to the actual needs.

30.13.2 View Daily/Weekly/Monthly/Summary Attendance Reports

You can view and export daily/weekly/monthly/summary attendance reports.

In the Attendance module, select **Daily Report**, **Weekly Report**, **Monthly Report**, or **Summary Report** on the left as needed.

Report Type	Description
Daily Report	Daily report shows data on a daily basis. The report contains data recorded on the day prior to the current day.
Weekly Report	The report contains the persons' attendance results of the recent one week.

Report Type	Description
Monthly Report	The report contains the persons' attendance results of the current month.
Summary Report	The summary report provides an overview of the person's/ department's attendance results.

Under these four types of reports, you can select a report as needed.

For some kinds of reports, you can perform the following operations as needed.

- Click **Export** to export the report in Excel, PDF, or CSV format. You can also select the calculating dimension of the report.
- Click **Select Person(s)** and select the desired persons to filter the attendance report by person.
- Click and select the desired time range to filter the attendance report by time range.
- Click and select the order to sort the attendance report.
- Click to customize column items.
- After customizing column items, click **Save Layout** to save the current layout for later use.

  Exporting Allowed

  After enabled, the layout can be exported in the report.

  Sharing Allowed

  After enabled, the layout will be shared among accounts.

  Fixed Date

  After enabled, you can set a specific time period for attendance data displayed in the layout. Only attendance data generated during this time period will be displayed in the layout.
- Click **Load Layout** to display the layouts saved by you and the layouts shared by other users. After loading layouts, you can search for a specific layout, and edit or delete the layouts you saved.
- Click to display each column title completely/incompletely.

30.13.3 Send Attendance Report Regularly

You can set a regular report rule for specific departments, and the platform will send an emails attached with a report to the recipients daily, weekly, or monthly, showing the attendance records of the persons in these departments during specific periods.

Before You Start

- Set the email template with recipient information, subject, and content.
- Set the email parameters such as sender address, SMTP server address and port, etc.

Steps

Note

The report is an Excel file.

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Basic Configuration** → **Report Settings** → **Scheduled Report** on the left.
3. Click **Add** (for first time) or click + .
4. Create a descriptive name for the report.
5. Select a type, format, and language for the scheduled report.

   Note

   You can select **TXT** as the format if the report type is **Time Card**.
6. In **Statistics Department**, check the department(s) / attendance group(s) of which the persons' attendance data will be delivered in this report.

   Note

   - For Department Attendance / Overtime Summary, you can only select departments. For Group Attendance / Overtime Summary, you can only select attendance groups.
   - You can check **Include Sub-Department** to display the persons of sub-departments.
   - You can click and filter persons by status (all, employed, or resigned).
7. **Optional:** For reports excluding Attendance/Overtime Summary and Attendance/Overtime Summary, click **Select Extra Person**, and click to include individual persons whose attendance data will be delivered in this report.

   Note

   - You can check **Include Sub-Department** to display the persons of sub-departments.
   - You can click and select person status (all, employed, resigned), or enable **Additional Information** and enter the keyword in the text field to search for matched persons.
   - You can check **Select All** to select all persons.
8. Set the statistical cycle to **By Day**, **By Week**, or **By Month** and set the report time range and sending time.

   Daily Report

   Daily report shows data on a daily basis. The platform will send one report at the sending time every day. The report contains data recorded on the day prior to the current day.

   For example, if you set the sending time to 20:00, the system will send a report at 20:00 every day, containing the persons' attendance results between 00:00 and 24:00 prior to the current day.

   Weekly/Monthly Report

The platform will send one report at the sending time every week or every month. The report contains the persons' attendance results of the recent one/two weeks or current/last month of the sending date.

For example, for weekly report, if you set the sending time to 6:00 on Monday, the platform will send a report at 6:00 in the morning on every Monday, containing persons' attendance results of the last week or recent two weeks based on your selection.

Note

- Daily or weekly report is not available when you set report type to monthly or weekly report.
- To ensure the accuracy of the report, you are recommended to set the sending time at least one hour later than the auto-calculation time of the attendance results. By default, the platform will calculate the attendance results of the previous day at 4 A.M. every day. You can change the auto calculation time in General Rule. See details in ***Set Auto-Calculation Time of Attendance Results*** .

9. In the Export Settings, select a format for the report.

Note

If you select PDF, you can customize the paper size and direction of printing.

10. **Optional:** Click to set the effective period for the report.
11. **Optional:** Select and enable the way of sending the report from **Send Report via Email**, **Upload to SFTP**, and **Save to Local Storage**.

Note

To set up the SFTP or local storage, click > **SFTP Settings** or **Configure Local Storage**.

12. **Optional:** Select the email template from the drop-down list to define the recipient information and email format.

Note

You can click **Add** to add a new email template.

13. Click **Add** to save the report schedule.

The report will be generated and sent to the recipient at the specified sending time.

30.13.4 Add a Custom Report

You can create a fully-customized attendance report. After creating a custom report, you can export the report manually or set a schedule to send the report to your email regularly.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Custom Report** on the left.
3. Click + .
4. Create a descriptive name for the report in the **Report Name** field.

5. Choose whether to merge the data of the same person/department/date.
6. Select a sorting rule for records from the **Table Display Rule** drop-down list.
7. Select the data items you want to include in the report from **Optional Fields**.

Note

- Selected data items will show in **Selected Fields**.
- You can drag the items in **Selected Fields** to set the order of the items.

8. **Optional:** Click **Preview** to view the report to make sure the format and content are correct.
9. Click **Add** to save the custom report, or click **Add and Continue** to add another one.
10. **Optional:** Perform further operations.

Edit Report	Select a report and click to edit it.
Delete Report	Select a report and click to delete it, or click → **Delete All** to delete all reports.
Export Report	Click **Export** and specify the departments, target persons, time range, and report format to export the report to the PC.
Send Report Regularly	You can set a schedule to send the report regularly. See details in ***Send Attendance Report Regularly*** .

Export a Custom Report

You can specify the department / attendance group, time period, and format to export a custom report to your local PC.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Custom Report** on the left.
3. Select a custom report on the left pane, and click **Export** to open the Export Settings page.
4. On the Person Selection Method area, select **Department** / **Attendance Group**.
5. Check the desired departments / attendance groups.

Note

If you select **Department**, you can check **Include Sub-Department** to display the persons of sub-departments. You can also click to filter persons by status (all, employed, or resigned).

6. **Optional:** Click **Select Extra Persons**, and click to include individual persons whose attendance data will be delivered in this report.

Note

- You can check **Include Sub-Department** to display the persons of sub-departments.
- You can click and select person status (all, employed, or resigned), or enable **Additional Information** and enter the keyword in the text field to search for matched persons.
- You can check **Select All** to select all persons.

7. Specify the time period by selecting the predefined time period, or clicking **Custom** to customize the start and end date.
8. Specify the report format.

Note

If you select PDF, you can customize the paper size and direction of printing.

9. Click **Export** to export the custom report to the local PC.

Chapter 31 Patrol Management

The system provides the service for patrol management, with which you can create patrol routes and arrange patrol persons to perform the patrols (by checking in at the patrol points offline) according to the shift schedules. You can monitor the patrol online in real time to conveniently know whether exceptions occur during patrols, and view and export patrol-related events records / statistics.

On the Web Client, you can set patrol points, patrol person groups, patrol schedule templates, patrol routes, etc., perform real-time monitoring, search for patrol-related event records, and view patrol statistics.

31.1 Patrol Overview

The Patrol Overview page shows the wizard for the Patrol Management module, and Today's Patrol Route Statistics (including Patrol Shift Status Statistics and Patrol Route Status Statistics).

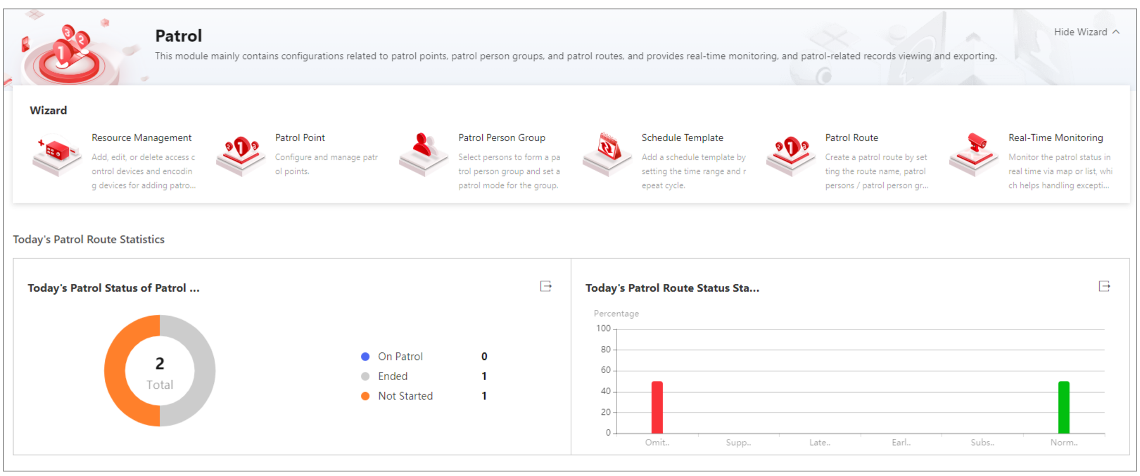


Figure 31-1 Patrol Overview

Patrol Shift Status Statistics (Today's Patrol Route Statistics)

You can view the total number of patrol routes which have shift(s) for the current day, and the numbers of patrol routes with different patrol shift status. You can also click the total number to switch to the Real-Time Monitoring page, or click to export the chart in PDF, PNG, or JPG format.

On Patrol

Shows the number of patrol routes of which the earliest shift has started/ended and the last shift is not ended.

Ended

Shows the number of patrol routes of which all the shifts for the current day have ended.

Not Started

Shows the number of patrol routes of which the earliest shift has not started.

Patrol Route Status Statistics (Today's Patrol Route Statistics)

You can view the percentages of patrol routes with different status (omitted patrol, supplemented patrol, etc.). You can also click to export the chart in PDF, PNG, or JPG format.

Omitted Patrol

Indicates that the patrol is not performed within the scheduled time period.

Supplemented Patrol

Indicates that the patrol is performed after the scheduled time period.

Late Patrol

Indicates that within one patrol shift, the patrol is first performed before the scheduled time period, and then performed again after the scheduled time period.

Early Patrol

Indicates that the patrol is performed before the scheduled time period.

Substitute Patrol

Indicates that the actual patrol person who performed the patrol is not the planned patrol person.

Normal Patrol

Indicates that the patrol is performed within the scheduled time period by the planned patrol persons.

31.2 Flow Chart of Patrol Management

The flow chart below shows the process of configuring and managing patrols.

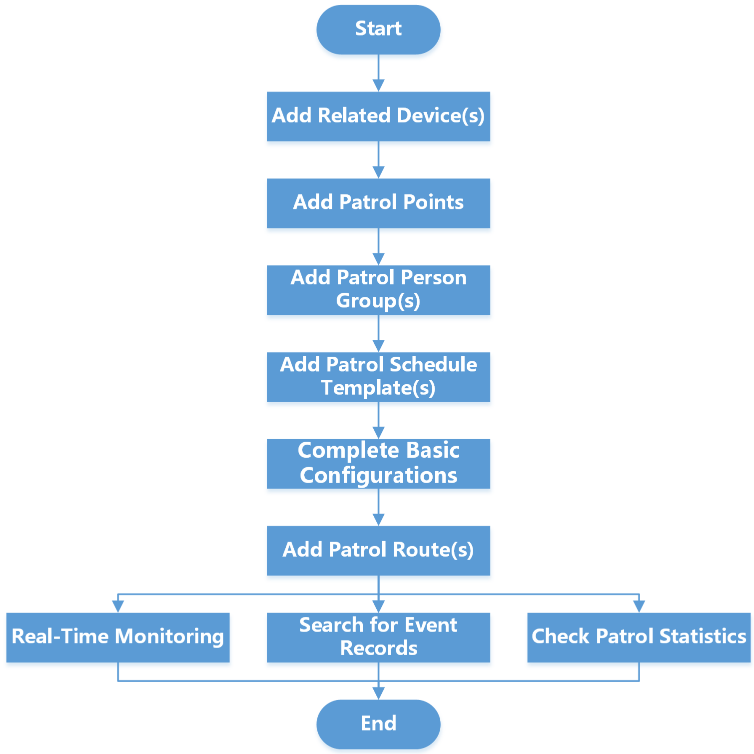


Figure 31-2 Flow Chart of Patrol Management

Table 31-1 Flow Chart Description

Step	Description
Add Related Device(s)	Add devices used for adding patrol points, real-time monitoring, etc.
Add Patrol Points	Before you create a patrol route and start a patrol, you need to add patrol points. You can set access points as patrol points, or generate QR codes to be patrol points. The patrol persons have to check in at the patrol points to perform the patrol. See ***Add Patrol Points*** for details.
Add Patrol Person Group(s)	Before adding a patrol route, you can select persons to form a patrol person group and set their patrol mode. See ***Add Patrol Person Group*** for details.

Step	Description
Add Patrol Schedule Template(s)	You need to set the schedule template first in order to schedule a patrol. See ***Add Patrol Schedule Template*** for details.
Complete Basic Configurations	To manage patrols, you need to set the parameters according to your needs. You can set the exception types for patrol persons to report, storage location of attachments, time for advance notification, and detection interval at which the server detects patrol route status. See ***Basic Configurations for Patrol Management*** for details.
Add Patrol Route(s)	Set the route name, patrol person / patrol person group, patrol schedule, patrol duration, patrol point, patrol pattern, shift schedule, etc., to form a complete patrol route. See ***Add Patrol Route*** for details.
Real-Time Monitoring	Monitor the patrol status in real time via map or list, to conveniently know whether an exception occurs during the patrol, which helps handling the exception in time. See ***Real-Time Patrol Monitoring*** for details.
Search for Event Records	Search for and export patrol-related event records including patrol events and exception reporting. See ***Search for Patrol-Related Event Records*** for details.
Check Patrol Statistics	Filter, check, and export patrol statistics by patrol route, patrol point, and patrol person. See ***Check Patrol Statistics*** for details.

31.3 Basic Configurations for Patrol Management

To manage patrols, you need to set the parameters according to your needs. You can set the exception types for patrol persons to report, storage location of attachments, time for advance notification, and detection interval at which the server detects patrol route status.

31.3.1 Add Exception Types for Patrol Management

You can add exception types for patrol persons to select from when they need to report exceptions via Mobile Client during patrols.

Before You Start

Make sure you have configuration permissions for patrol management.

Steps

1. On the top left of the Web Client, select → **Integrated Service → Patrol → Basic Configuration → Exception Type** .
2. On the top left of the page, click **Add**.

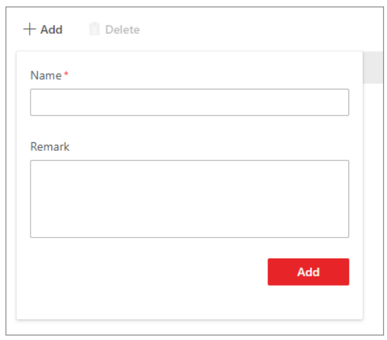


Figure 31-3 Add Exception Type

3. Enter a name for the exception type.
4. **Optional:** Enter the remark for the exception type.
5. Click **Add**.

   The added exception type will be displayed on the exception type list.
6. **Optional:** Perform the following operations according to your needs.

Edit an Exception Type	In the Operation column, click to edit the name and remark of the exception type.
Delete Exception Type(s)	Select the exception types to be deleted and click **Delete** on the top left of the page.

31.3.2 Set Parameters for Patrol Management

You can set parameters including Local Storage Configuration, Notification Time, and Detection Frequency to manage patrols and patrol-related attachment storage.

Note

Make sure you have configuration permissions for patrol management.

1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Basic Configuration** → **Parameter Configuration** .

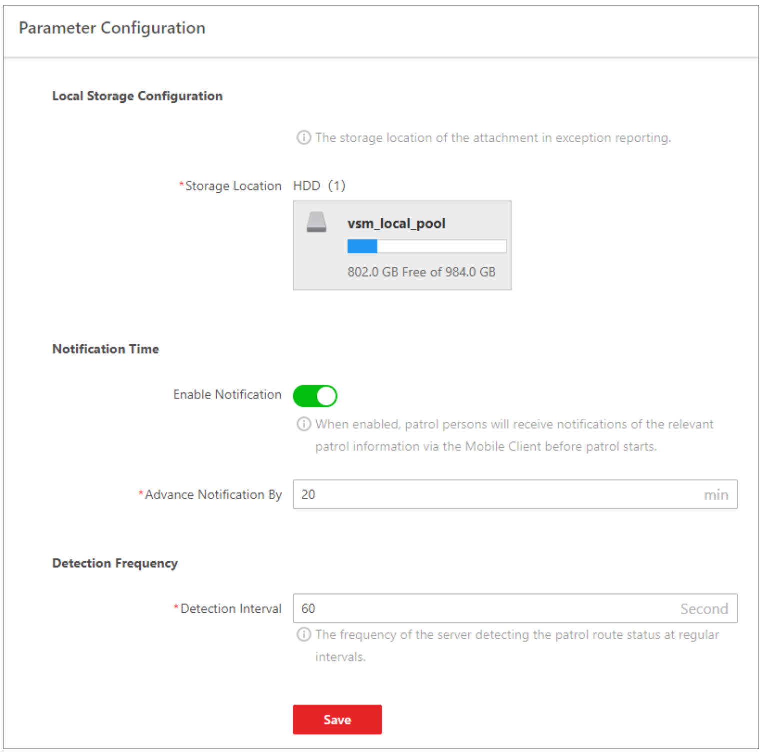


Figure 31-4 Parameter Configuration

2. Configure the following parameters according to your needs.

Local Storage Configuration

Configure the **Storage Location** for the attachments in exception reporting.

Notification Time

When the notification is enabled, patrol persons will receive notifications of the relevant patrol information via Mobile Client before patrols start. After it is enabled, you can edit the time by which the notification is advanced.

Detection Frequency

Set the **Detection Interval** at which the server detects the patrol route status.

GIS Configuration

Enable **GIS Map** so that you can configure patrol points on the GIS map.

Note

To use the basic functions of the GIS map, you need to subscribe to the Geocoding API, Maps JavaScript API, and Places API from Google Maps. If you want to search for geographic locations, you need to subscribe to the Geolocation API.

31.4 Add Patrol Points

Before you create a patrol route and start a patrol, you need to add patrol points. You can set access points as patrol points, or generate QR codes to be patrol points. The patrol persons have to check in at the patrol points to perform the patrol.

Before You Start

Make sure you have configuration permissions for patrol management and permissions for related resources.

Steps

1. 1. On the top left of the Web Client, select → **Integrated Service → Patrol → Patrol Management → Patrol Point** .
2. On the top left of the page, click **Add**.

Figure 31-5 Add Patrol Point

3. Select the patrol point type and add patrol points of either type according to your needs.
   - Add Patrol Points of Access Point Type:

     Select **Access Point** as the **Patrol Point Type**, click **Add**, select card readers, and click **Add** to add the patrol points to the list. Click **Add** again to add more patrol points to the list.

     Note

     - Only one patrol point will be added for each card reader.
     - The patrol point name is generated automatically based on the resource name. You can edit the name if required.
   - Add Patrol Points of QR Code Type:

     Select **QR Code** as the **Patrol Point Type**, click **Add**, and enter the name for the patrol point to add the patrol point to the list. Click **Add** again to add more patrol points to the list.
4. Click **Link** and select camera(s) to link to the patrol point.

   Note

   No more than 4 cameras can be linked to each patrol point.
5. **Optional:** For patrol points of QR code type, you can turn on **GPS Verification** to set the valid patrol scope.

   You can set the valid patrol scope by searching for the location or by manually drawing a circle.

6. **Optional:** Click **Delete All** to delete all patrol points, or click to delete one patrol point.
7. Click **Save**.

   The added patrol points will be displayed on the patrol point list.
8. Perform the following operations according to your needs.

Filter Patrol Points	On the top right of the page, click , set the conditions (patrol point name, patrol point type, linked cameras, resource, and area) according to your needs, and click **Filter**.
Delete Patrol Points	Select the patrol points to be deleted and click **Delete**.
Edit a Patrol Point	Click the name of a patrol point to enter the patrol point information page. You can edit the patrol point name and linked cameras.
View Thumbnails of Camera Views	In the Linked Camera(s) column, click to view the thumbnails of the latest views of the linked cameras.
View/Download the QR Code of a Patrol Point	For a patrol point of QR code type, click in the Patrol Point Type column to view and download the QR code.
Enable GPS Verification	For a patrol point of QR code type, turn on **GPS Verification** to enable the GPS verification. After this is enabled, patrols will be valid only if they are performed within this scope.

31.5 Add Patrol Person Group

You can select persons to form a patrol person group and set a patrol mode for the group.

Before You Start

Make sure you have configuration permissions for patrol management and permissions to access the related person groups.

Steps

1. On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Patrol Management** → **Patrol Person Group** .
2. Click **Add**.

Note

If you have already added a patrol person group before, click + on the top left of the page to add another one.

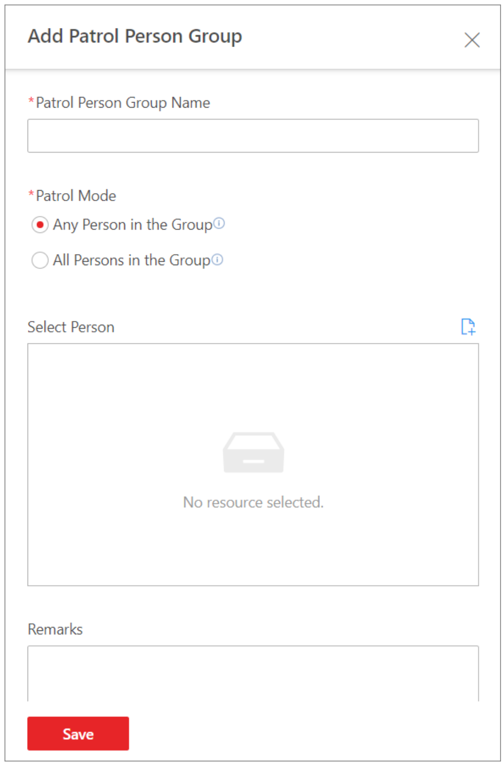


Figure 31-6 Add Patrol Person Group

3. Enter a name for the patrol person group.
4. Select a patrol mode.

   Any Person in the Group

   The patrol at a patrol point is performed when any person in the group checks in at the patrol point.

   All Persons in the Group

   The patrol at a patrol point is performed when all persons in the group check in at the patrol point.
5. Click to select persons to form the patrol person group.

Note

- No more than 100 persons can be selected for one patrol person group.
- You can also skip this step for now and add persons to the patrol person group later.

6. **Optional:** Enter remarks for the patrol person group.
7. Click **Save**.

Note

No more than 300 patrol person groups can be created for a system.

The added patrol person groups will be displayed on the left pane.

8. **Optional:** Perform the following operations according to your needs.

Edit a Patrol Person Group	On the left pane, select a patrol person group and click on the top to open the Edit Patrol Person Group pane. You can edit the name, patrol mode, person(s), and remarks of the group accordingly.
Delete Patrol Person Groups	On the left pane, select a patrol person group and click on the top to delete the selected group. Click → **Delete All** to delete all patrol person groups.
Search for Patrol Person Groups	On the left pane, enter keyword(s) in the search box to search for patrol person groups.
Add Persons to a Patrol Person Group	Select a patrol person group and click **Add** to add patrol persons to the patrol person group.
Search for Persons in a Patrol Person Group	Select a patrol person group and enter keyword(s) in the upper-right search box to search for patrol persons in the patrol person group.
Delete Persons from a Patrol Person Group	Select a patrol person group, select the patrol persons to be deleted, and click **Delete**. You can also click → **Delete All** to delete all patrol persons from the group.

31.6 Add Patrol Schedule Template

You need to set the schedule template first in order to schedule a patrol.

Before You Start
Make sure you have configuration permissions for patrol management.

Steps
1. On the top left of the Web Client, select → **Integrated Service → Patrol → Patrol Management → Schedule Template** .
2. Click **Add Schedule Template**.

Note

If you have already added a schedule template before, click on the top left of the page to add another one.

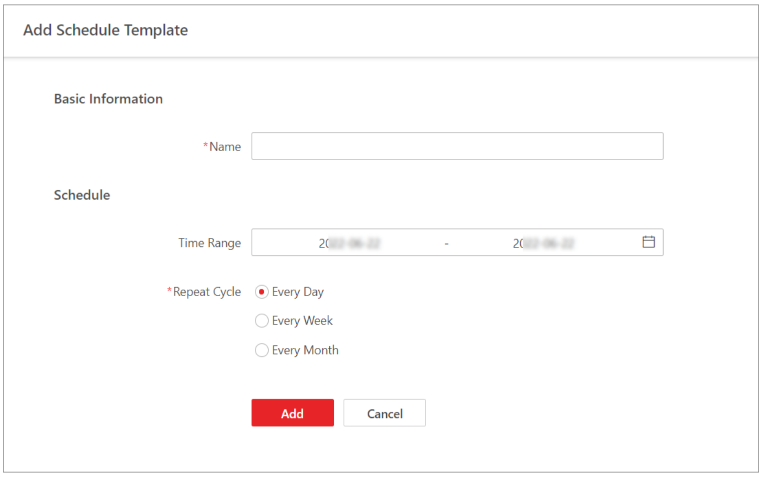


Figure 31-7 Add Schedule Template

3. Enter a name for the schedule template.
4. Set a validity period for the schedule template.
5. Choose a repeat cycle for patrol scheduling.

   Every Day

   Patrols will be scheduled for each day of the set time period.

   Every Week

   Patrols will be scheduled on the selected days of every week within the set time period.

   Every Month

   Patrols will be scheduled on the selected dates of every month within the set time period.
6. Click **Add**.

   The added schedule templates will be displayed on the left pane.
7. **Optional:** Perform the following operations according to your needs.

Edit a Schedule Template	Select a schedule template and edit its configuration accordingly, including the name, time range, and repeat cycle.
Delete a Schedule Template	Select a schedule template and click **Delete**. **Note** Schedule templates cannot be deleted if being linked with shift schedules of a patrol route.
Search for Schedule Templates	On the left pane, enter keyword(s) in the search box to search for schedule templates.

31.7 Add Patrol Route

To start a patrol, you need to create a patrol route. Set the patrol point(s), patrol pattern, patrol duration, and shift schedule(s) to form a complete patrol route.

Before You Start

- Make sure you have configuration permissions for patrol management and permissions to access the related patrol points and person groups.
- Make sure you have already added patrol points and patrol schedule templates to the system. For details about adding patrol points, see ***Add Patrol Points*** . For details about adding patrol schedule templates, see ***Add Patrol Schedule Template*** .

Steps

1. On the top left of the Web Client, select → **Integrated Service → Patrol → Patrol Management → Patrol Route** .
2. Click **Add Route**.
3. Enter a name for the patrol route.
4. **Optional:** Enter remarks for the route.
5. Click **Save** to open the patrol route configuration page.

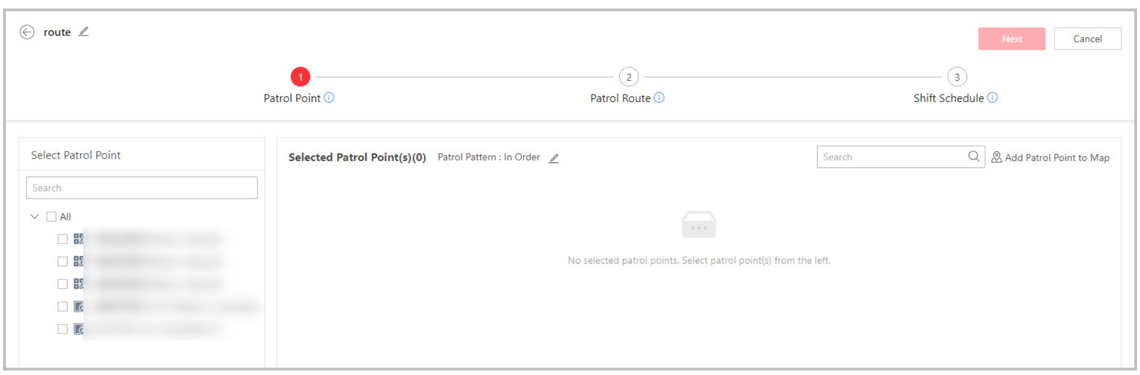


Figure 31-8 Patrol Route Configuration Page

6. Select the patrol point(s) that the patrol persons need to patrol on a route.
7. Click beside **Patrol Pattern: In Order** to set the patrol pattern for the route.

Note

- The patrol pattern is **In Order** by default.
- You can click ↑ and ↓ to rearrange the patrol list order as needed.

In Order

Patrol according to the order in the patrol list.

No Order

Patrol the patrol points on the route in no particular order.

First Point First and Last Point Last

Patrol the first patrol point on the patrol list at first and the last point on the list at last.

First Point First

Patrol the first patrol point on the patrol list at first.

Last Point Last

Patrol the last patrol point on the patrol list at last.

8. Click **Next**.

Note

If a patrol point has not been added to a map, you can click **Add Patrol Point to Map** and drag it onto a map. If there are points with GPS verification enabled, GIS map will be automatically selected for you to add points to it; otherwise, you will have to choose between **GIS Map** and **Static Map**.

9. Set the total patrol duration (in minutes) for the patrol route.
10. Set the time error and interval for patrolling the patrol points, and click **Next**.

Note

Time error and interval settings are for patrols of the "In Order" patrol pattern only.

Time Error

The time error allowed to pass a patrol point during actual patrol.

You can set a common time error for all patrol points, or set the time error for each patrol point individually by entering values in the table cells or the textboxes that appear when hovering over the Rule Preview pane.

Interval

The time interval of patrolling the current patrol point and the previous one.

You can set a common interval for all adjacent patrol points, or set each interval individually by entering values in the table cells or the textboxes that appear when hovering over the Rule Preview pane.

Note

The sum of all patrol intervals should be less than the set total duration of the patrol route.

11. Click **Add Schedule**.
12. Configure the parameters for adding a shift schedule.

Name

Enter a name for the shift schedule.

Copied From

If you have already added at least one shift schedule to the patrol route, you can select a shift schedule from the drop-down list to replicate its settings for schedule template and patrol person / patrol person group selection.

Schedule Template

Select a schedule template from the drop-down list.

Patrol Start Time

Set a start time for the patrol.

Note

The patrol time periods of shift schedules cannot overlap with one another.

Patrol Person or Patrol Person Group

Select persons or select an added patrol person group for the shift schedule. For details about adding patrol person groups, see ***Add Patrol Person Group*** .

13. Click **Add**.

Note

- If needed, click **Add Shift Schedule** again and repeat the step above to continue adding shift schedules. No more than 8 shift schedules can be added for a patrol route.
- You can edit an added shift schedule and delete one or delete all shift schedules according to your needs. The editing of a shift schedule will be applied to the route according to the time range and repeat cycle in the selected schedule template.

14. Click **Finish** to complete the patrol route configuration.
15. **Optional:** Perform the following operations according to your needs.

Switch Display Mode for Patrol Routes	On the top right of the page, click to view the added patrol routes in calendar mode, or click to view them in list mode. For the calendar mode, you can switch among day, week, and month views.
Filter Patrol Routes	On the top right of the page, click , set the conditions (route name, patrol points, persons, patrol person groups, schedule templates, patrol route status, and time range) according to your needs, and click **Filter**.
View Route Details	Click the name of a route to enter its route details page. You can view information such as patrol points, patrol pattern, patrol duration, and shift schedules configured for the route. You can also view maps to which the patrol points of the route are being added.
Edit a Patrol Route	Click the name of a patrol route, and click **Edit Route** on the top right of the page to enter the route configuration page. You can edit the route settings such as patrol points, patrol pattern, patrol duration, and shift schedules.
Disable Patrol Routes	Select the routes to be disabled and click **Disable Route**.
Enable Patrol Routes	Select the routes to be enabled and click **Enable Route**.

Delete Patrol Routes	Select the routes to be deleted and click **Delete**.

31.8 Real-Time Patrol Monitoring

You can monitor the patrol status in real time via map or list, to conveniently know whether an exception occurs during the patrol, which helps handling the exception in time.

Note

Make sure you have the operation permission for patrol monitoring.

On the top left of the Web Client, select → **Integrated Service → Patrol → Real-Time Monitoring** . On the patrol monitoring page, you can view the real-time status of patrol routes and information about real-time events related to the patrols.

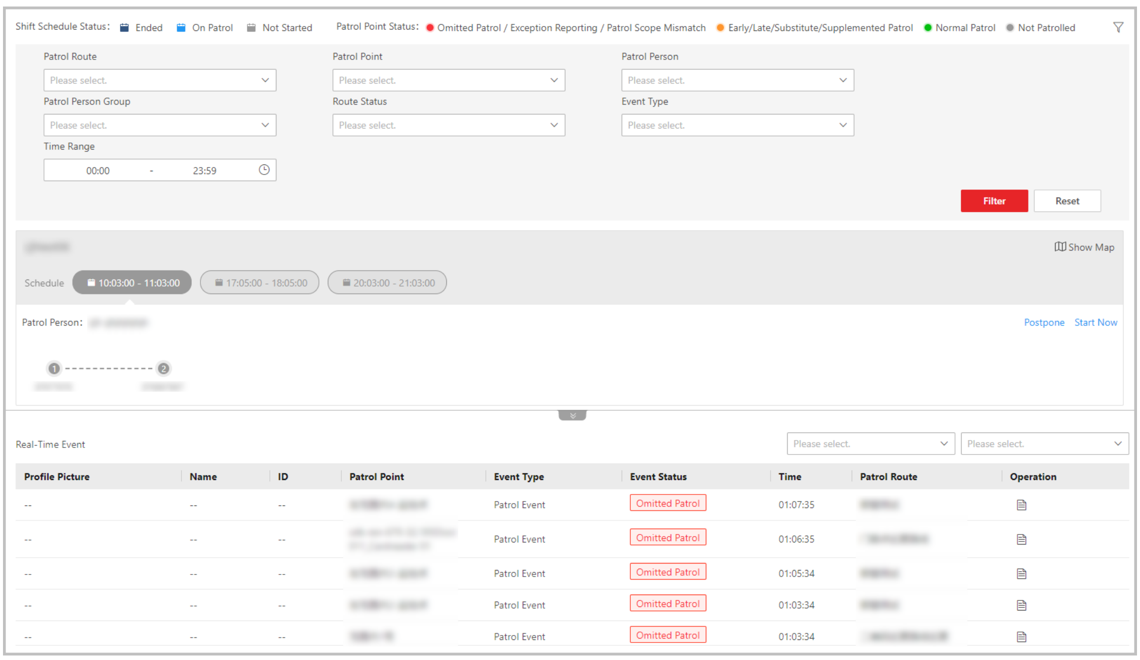


Figure 31-9 Real-Time Monitoring Page

Patrol Route Status

The real-time status of all enabled patrol routes with shifts scheduled for the current day are displayed by default. You can filter the routes by clicking on the top right of the page and setting the filter criteria (e.g., patrol route, patrol point, patrol person / patrol person group, route status, event type, and time range).

Information such as the route name, patrol person / patrol person group, scheduled time period for each shift, and a list of patrol points are displayed for each patrol route. The shift schedule status (e.g., ended, on patrol, and not started) and patrol point status (e.g., omitted patrol /

exception reporting, patrol scope mismatch, early patrol, late patrol, substitute patrol, supplemented patrol, normal patrol, and not patrolled) are indicated with different colors with respect to the legends on the top of the page.

You can click a patrol point already being patrolled to view its status and the related patrol event information. You can also hover over a shift to view its status and detailed information. If needed, you can manually start or postpone a shift not started yet by selecting the shift schedule and clicking **Start Now** or **Postpone** respectively.

For patrol routes with patrol points that have been added to maps, you can also click **Show Map** to switch to monitoring the patrol status in real time via maps.

Real-Time Event

The patrol monitoring page also supports showing information about real-time patrol-related events (e.g., patrol events, exception reporting, and patrol scope mismatch), including the patrol person information (e.g., profile picture, name, ID), event information (e.g., event type, event status), patrol information (e.g., patrol point, valid patrol scope, patrol route, shift schedule, scheduled/actual patrol time, and planned/actual patrol person), and related video/picture files and attachments.

Note

The actual information displayed may vary depending on the event type and patrol status.

You can filter the real-time events by event type and view details about each event by clicking in the Operation column.

31.9 Search for Patrol-Related Event Records

You can search for and export patrol-related event records, including patrol events and exception reporting.

Before You Start

Make sure you have the operation permission for patrol search.

Steps

1. On the top left of the Web Client, select → **Integrated Service → Patrol → Search → Event Record Search** .

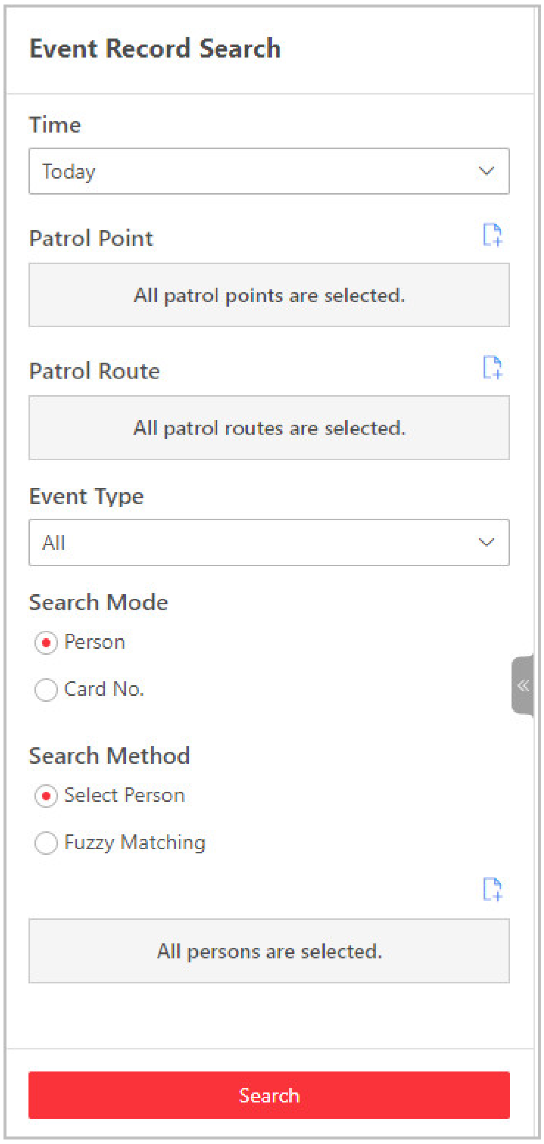


Figure 31-10 Event Record Search

2. Set the search conditions.

Time

Select from **Today**, **Yesterday**, **Current Week**, **Last 7 Days**, and **Last 30 Days**, or set a custom time interval of no more than 31 days.

Patrol Point

By default, all patrol points are selected. Click to select certain patrol point(s) to filter the search results.

Patrol Route

By default, all patrol routes are selected. Click to select certain patrol route(s) to filter the search results.

Event Type

By default, all patrol-related event records will be searched. Select **Patrol Event**, **Exception Reporting**, or **Patrol Scope Mismatch** from the drop-down list to search for the specified type of event records only.

Search Mode

Choose whether to search for the event records by **Person** or **Card No.**.

- Search by person: In the **Search Method** field, choose whether to search by person selections or fuzzy matching of persons' names.
- Search by Card No.: Enter the card No. in the search box.

3. Click **Search**.

The matched records will be shown on the right side of the page.

4. **Optional:** Perform the following operations according to your needs.

View Details of an Event Record	In the Operation column of an event record, click to view detailed information about the record. • For a patrol event, you can view the event information (e.g., patrol status), patrol information (e.g., patrol point, valid patrol scope, patrol route, shift schedule, scheduled/actual patrol time, and planned/actual patrol person) depending on the patrol status, and videos/pictures related to the patrol. • For an exception reporting, you can view the event information (e.g., exception type and description), patrol information (e.g., patrol point, patrol route, and patrol person), and the file(s) attached to this exception reporting.
Export an Event Record	In the Operation column of an event record, click to export the record.
Export All Matched Event Records	On the top right of the result page, click **Export** to export all matched results. You can choose whether to export in XLSX format or CSV format, and whether to export the event records with picture.

31.10 Check Patrol Statistics

You can filter, check, and export patrol statistics by patrol route, patrol point, and patrol person.

Note

Make sure you have the operation permission for patrol search.

On the top left of the Web Client, select → **Integrated Service** → **Patrol** → **Search** → **Patrol Statistics** to enter the patrol statistics page.

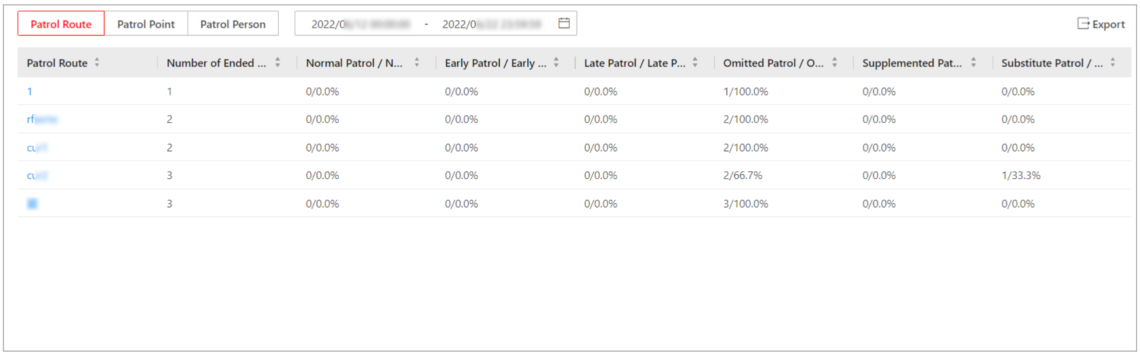


Figure 31-11 Patrol Statistics Page

You can select the type of patrol statistics to be displayed from **Patrol Route**, **Patrol Point**, and **Patrol Person**, and filter the results by specifying a time range. Information such as the number of shift schedules, number of patrols of a certain status (e.g. normal patrol, early patrol, late patrol, omitted patrol, supplemented patrol, and substitute patrol), and the percentage of each status will be displayed in a table. If needed, you can export the patrol statistics in either XLSX format or CSV format.

You can click the name of a patrol route, patrol point, or patrol person to view detailed information about each patrol in a list, including the patrol status, scheduled start time, actual start time, scheduled and actual patrol duration, shift schedule, and the person who performed the patrol. You can filter the patrol records by status and export the statistics in either XLSX format or CSV format.

Chapter 32 Commercial Display Management

In the Commercial Display module, you can use digital signage related functions and centralized device control functions. Digital signage management includes managing contents, schedules, release, materials, etc. You can select a proper method to create contents according to actual needs and set schedules to release the contents to the specific devices. The contents should be reviewed before they are released and played on the devices according to the configured schedule. Centralized device control management includes controlling digital signage terminals and interactive flat panels, managing applications, viewing flat panel usage statistics and other playing statistics.

In the top left corner of Home page, select → **Integrated Service → Commercial Display** .

32.1 Commercial Display Overview

The following is the overview of the Commercial Display module.

On the left, select **Overview**, and perform the following operations if needed.

Centralized Device Control

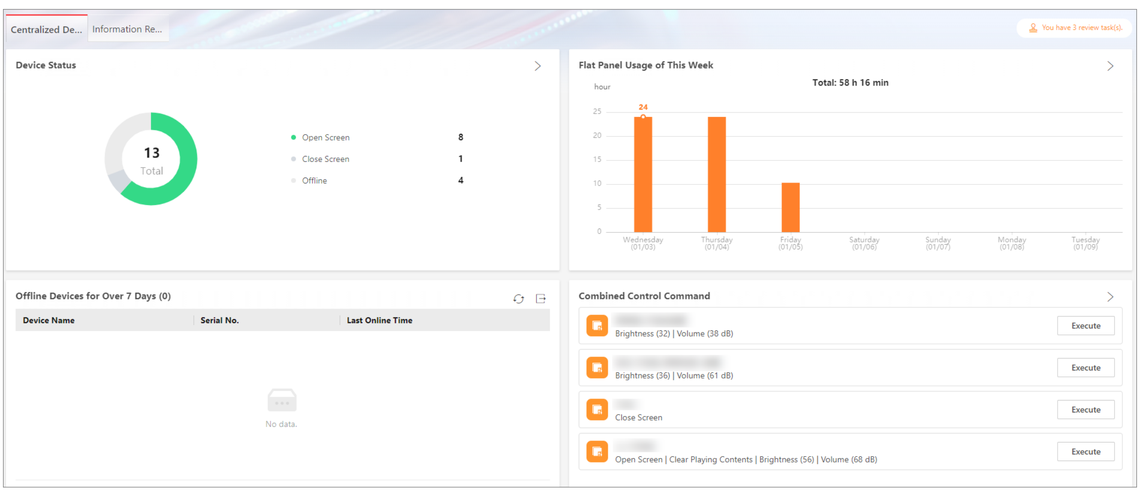


Figure 32-1 Centralized Device Control

The central device control mode supports viewing device status, flat panel usage of the this week, offline devices for over 7 days, and combined control command. You can also click › to go to the Device Control page or Flat Panel Usage Statistics page for details. In the Offline Devices for Over 7 Days area, you can refresh the list or export the information about the devices.

Information Release

In the Wizard area, click an application to perform the corresponding task.

Below the Wizard, Quick Release, Release by Template, and Material Library are displayed.

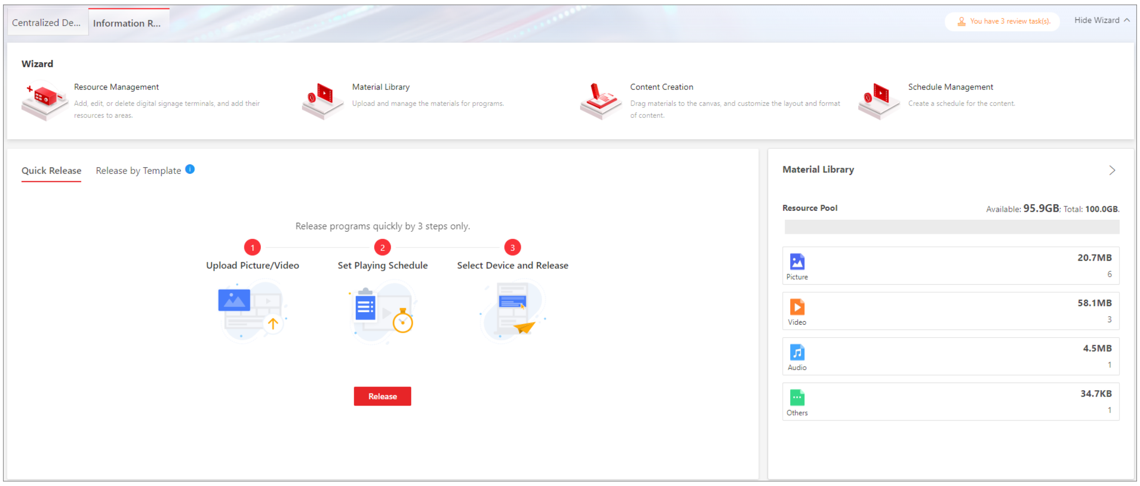


Figure 32-2 Information Release

32.2 Flow Chart of Digital Signage Management

You can follow the flow chart below for using the digital signage module for the first time.

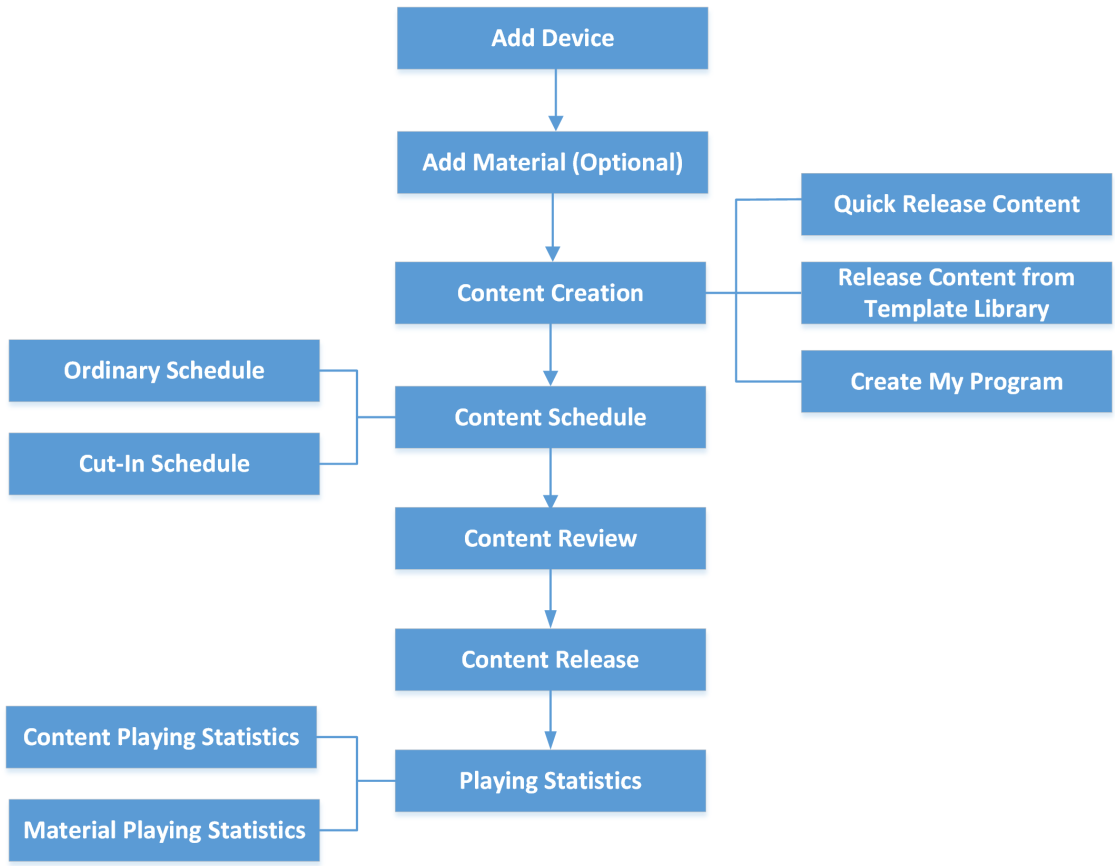


Figure 32-3 Flow Chart of Digital Signage Management

- **Add Device**: You should add devices to the platform. For details, refer to ***Manage Digital Signage Terminals*** and ***Manage Interactive Flat Panel*** .
- **Add Material**: Material is used for creating programs. You can upload materials to the platform. For details, refer to ***Material Library*** .
- **Content Creation**: You can create contents via three methods including quick releasing contents, creating contents from the template library, and creating my programs according to actual needs. For details, refer to ***Content Creation*** .
- **Content Schedule**: You should define a playing schedule for the added programs, which will then be played according to the scheduled time or method on the terminals. For details, refer to ***Create a Cut-In Schedule*** and ***Create an Ordinary Schedule*** .
- **Content Review**: The added contents should be reviewed before they are used. For details, refer to ***Review Management*** .
- **Content Release**: You can view release records of all the tasks and the details of their release status. For details, refer to ***View Release Records*** .

32.3 Content Creation

The platform supports creating contents and releasing them to the selected devices. Then the contents can be played on the devices to function as prompts, notices, etc. According to actual needs, you can select from three entries/methods to create contents, namely, quick releasing contents, creating contents from template library, and creating my programs. When creating contents via the latter two entries/methods, you can customize the layout of the program, add materials to the program, preview the program, etc.

32.3.1 Quickly Release Content

You can quickly release contents by selecting device type(s), selecting material(s) from local PC or material library, setting the content playing schedule, setting the release mode, and selecting device(s) to release the contents.

Before You Start

Make sure you have added device(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** , ***Manage Interactive Flat Panel*** , and ***Add LED Controller*** .

Steps

1. On the left, select **Content Creation**.
2. Click **Quick Release** on the left to enter the Quick Release page.

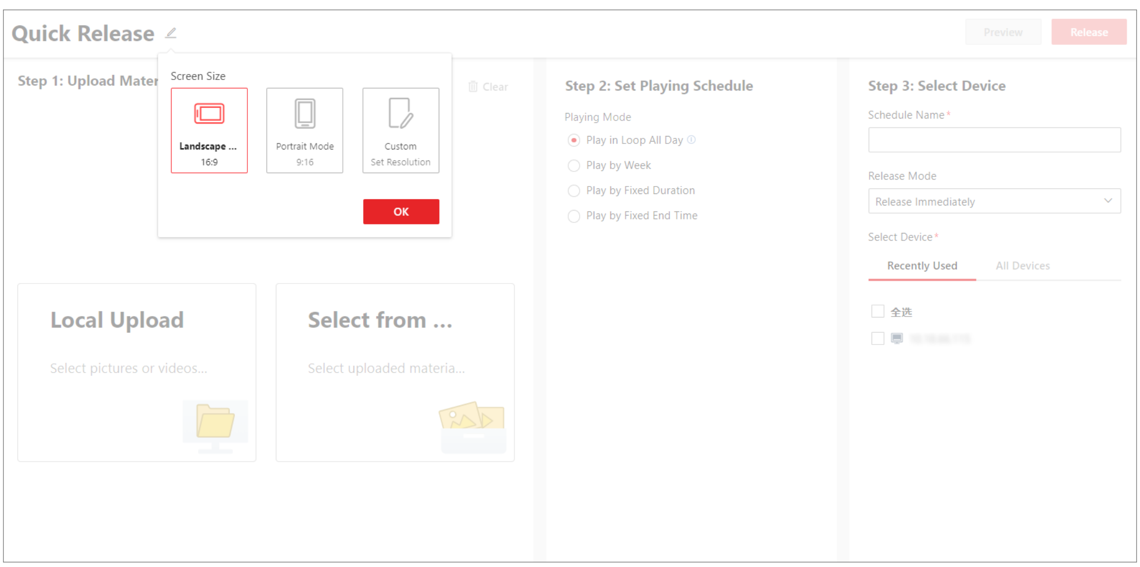


Figure 32-4 Quick Release Page

3. Select the device type and screen size, and click **OK**.
   - Click **Digital Signage Terminal** to select the screen size, and you can click **Custom** to enter the resolution manually.
   - Click **Interactive Flat Panel**.

- Click **Screen Controller**, enter the resolution manually or click **Get Device Screen Size** to get the screen size of the added device.

4. Upload the material(s).
   - Click **Local Upload**, and select picture(s) and/or video(s) form local PC.
   - Click **Select from Material Library**, select an area from the drop-down list, and select material(s) from the Material Library.

Note

- For the selected material, move the mouse cursor to it and you can click **Edit** to edit the material size, or click **Delete** to delete the material. You can also click **Clear** to delete all the selected materials.
- On the editing material page, you can check **Show Original Aspect Ratio** to view the material in its actual proportion (only picture material supports). After resizing the material, you can click **Reset** to revert the material size to its original size.

5. Set the playing schedule.
   1) For multiple uploaded materials, drag them to adjust the playing order, and set the switching effect as **Gradient** or **None**.
   2) Set the playing duration for picture materials.
   3) Set the playing schedule as **Play In Loop All Day**, **Play by Week**, **Play by Fixed Duration**, or **Play by Fixed End Time**.
6. Select the device(s) to release the content.
   1) Enter the schedule name.
   2) **Optional:** Select the release mode as **Release Later**, or select **Release Immediately** and set the release time.
   3) **Optional:** Switch on **Device Sync Playing** (for digital signage terminals only).

   Note

   Make sure you have enabled the time synchronization of NTP server. See details in ***Set NTP for Time Synchronization*** .

   4) Select device(s) from recently used devices or all devices.
7. **Optional:** Click **Preview** to preview the content.

Note

- During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the content in full screen.
- For the content with multiple materials, it will be played automatically according to the playing order you have set. Also, you can manually click or to preview the previous or the next material.

8. Click **Release** to start releasing the content.

   After the content is released, you will enter the Release page and view the quick release task in the list.

32.3.2 Manage Template Library

The platform provides multiple templates which can be used in different application scenarios such as chain retail and financial bank. You can preview the template, add it to My Template, and create my program based on the selected template according to actual needs.

On the left, select **Content Creation → Template Library** .

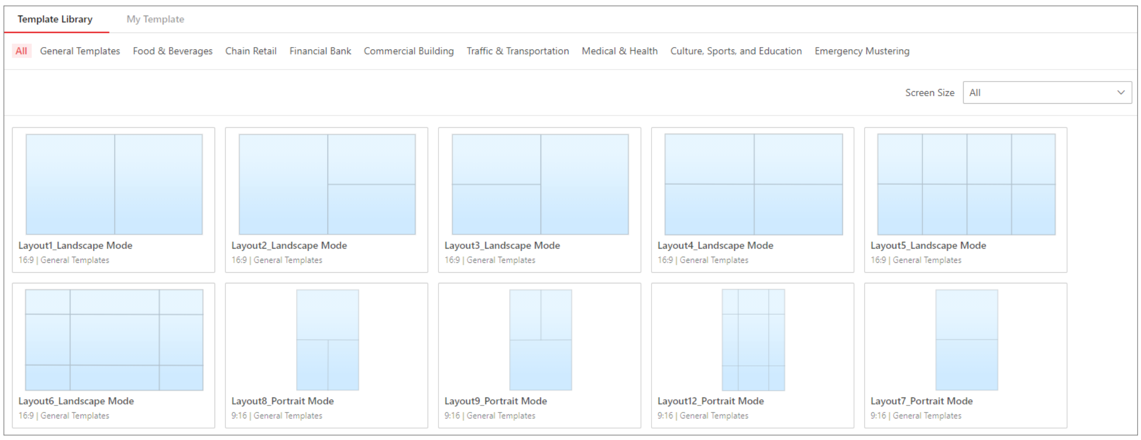


Figure 32-5 Template Library

You can perform the following operations.

- Hover over the target template, and click **Create** or **Preview → Create Program** to enter the creating content page. For details about creating contents, refer to ***Figure 32-6*** .
- Filter templates by the template types or the screen sizes.
- Hover over a template and click **Preview** to preview the template.

Note

You can click **Emergency Mustering** and select a template for creating the emergency mustering program. After being created, the program will be played on the device when the emergency is triggered.

- Hover over a template, and click **Add to My Template** to add it to My Template. On My Template page, you can also filter and preview the templates, and remove them from My Template.

32.3.3 Create My Program

The platform supports creating single-sided programs and video wall programs. Therefore, you can create programs according to the screen type (single-sided screen or video wall) of your devices. When creating the program, you can select the needed materials and design the layout to meet your requirements. After creating the programs, you can perform more operations such as previewing, copying, releasing, editing, and filtering programs.

Before You Start

Make sure you have added device(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** , ***Manage Interactive Flat Panel*** , and ***Add LED Controller*** .

Steps

1. On the left, select **Content Creation → My Program** .
2. Click **Add**.
3. Configure program parameters including name, device type, screen type, screen size, and description.
4. Click **OK** to enter the creating program page.

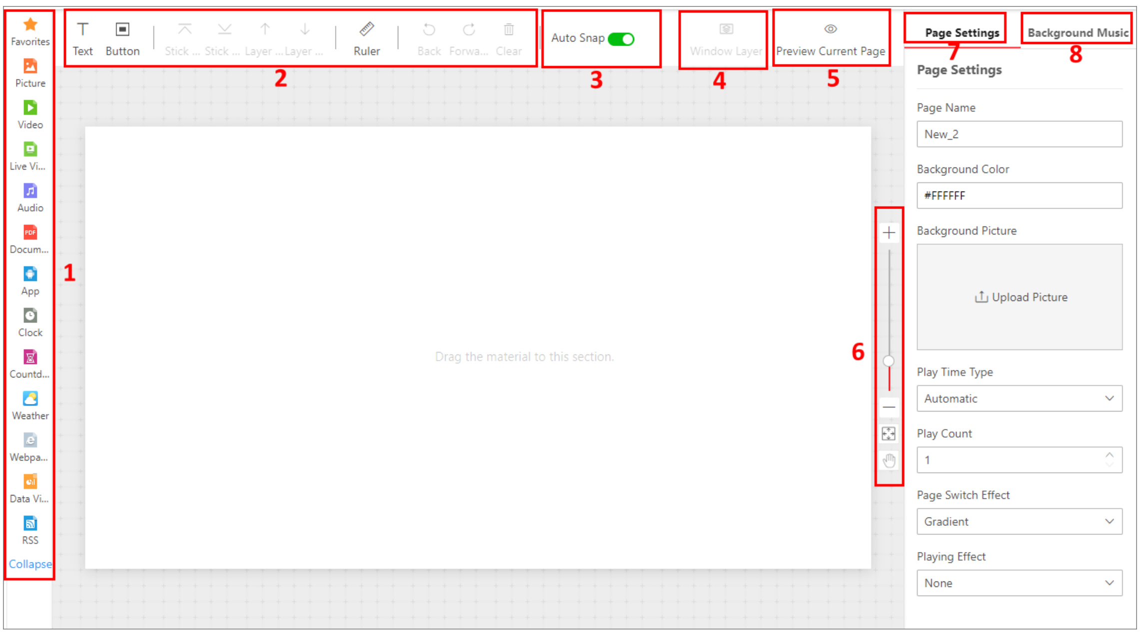


Figure 32-6 Create My Program

Table 32-1 Page Description

Number	Description
1	There are multiple types of material windows. For details about operations of different material types, refer to ***Table 32-2*** . **Note** • Up to 16 windows can be added for one page. • An audio window cannot be added with a video window or live video window at the same time. • You can add material(s) to Favorites in Material Library.
2	Here are meanings of tools.

Number	Description
	• : Add a text window in the template. • : Add a button window in the template (only available for touchscreen terminals). • / / / : Make the window layer move up / move down / stick on top / stick at bottom. • : Display rulers in the right side and top side. • / : Undo or redo the operation. • : Clear all the materials.
3	Enable **Auto Snap**, and the two windows will be connected when they are near enough.
4	Click **Window Layer** to view the number of current window layers and what each layer is.
5	• You can click **Preview Current Page** to preview the content of the current page. • During previewing, you can click or to pause or start playing. You can click or to adjust the playing speed as 1x, 2x, or 4x. Also, you can click to preview the current page in full-screen.
6	: Zoom in the canvas. : Zoom out the canvas. : Convert the canvas to its original size. : Drag the canvas.
7	Edit page settings, including page name, background, play time type, etc.
8	Click **Upload** to upload the background music from the local PC or Material Library. After uploading, you can enable the background music, which will be played on the current page. You can delete the background music if needed.

5. **Optional:** On the left side, perform operations such as adding, copying, deleting program pages.

Add
Click **Add** to add new page(s). Up to 32 pages can be added.

Copy
Put the cursor on the page, and click **Copy** to copy the current page.

Delete
Put the cursor on the page, and click **Delete** to delete the current page.

Note

You cannot delete the page when there is only one page.

Change Template
Put the cursor on the page, click **Change Template**, and select a new template from Template Library or My Library.

Adjust Sequence	Click a page and drag it to the desired location to adjust the sequence of program pages.

6. Select a material type and select the corresponding material(s) from the left list and drag it to the corresponding window in the template to add the selected material.

Table 32-2 Material Types and Corresponding Operations

Material Type	Operation
Picture/Video/Audio/ Text	• Click **Picture/Video**, move the mouse cursor to the upper-right corner of the material, and click to set its validity period. The material will be played within the validity period. • **Picture/Text**: On the right Window pane, set **Rotation Degree**, **Round Corner**, and **Micro Animation**. • **Picture/Video**: On the right Window pane, expand **Advanced Settings**, and check **Show Original Aspect Ratio** to display these materials in their original sizes. • **Text**: On the right Window pane, select the font provided by the platform or click **Upload** to custom the font. After uploading fonts, you can click **Font Library** to preview, delete, and search for fonts. You can set the background color and transparency, as well as the scrolling direction and speed.
Live Video	On the right Window pane, expand **Advanced Settings**, and check **Close Audio**, then the program will be played without audio. Besides, only one Device Channel 1 can be added to one program page.
Weather	On the right Window pane, set parameters such as **Weather Location** and **Refresh Interval** to specify the weather display effect. **Note** Make sure you have configured the weather web manufacturer. See ***Set Weather Web Manufacturer*** .
Webpage	On the right Window pane, set the display format according to actual needs.
Data View	Click **Data View**, and select table, chart, dynamic picture, and dynamic text. For details about adding data view materials, refer to ***Upload Materials*** . For dynamic pictures, and dynamic texts, supports setting **Rotation Degree**, **Round Corner**, and **Micro Animation**.

Material Type	Operation
RSS	On the right Window pane, enter the **RSS Feed URL** to subscribe to news or other information you interested in and specify other display parameters.
Signal Source	Select the signal source for LED controller such as HDMI1 and HDMI2.

Note

- When selecting materials, you can search for materials and refresh material list. Also, you can click **Local Upload** to add other materials from local PC to the platform.
- You can add the same or different types of materials to one window. When adding the same type of materials to one window, you can click **Create Window** to create a new window or click **Add More Material** to add more material to the current window.

7. Set window properties, including window position, window type, switching method, etc.

Note

You can set different parameters for different types of material windows.

Window Position

Set the window position by entering the width, height, and coordinate of the window.

Window Type

Normal

The normal window is displayed by default when the program is played. You can set a window jump link or page jump link for such a window.

Popup Window

The pop-up window is hidden by default. Only after setting a redirect link for a normal window and clicking the link, the hidden window will be popped up.

Switching Method

For Android touchscreen terminals, you can open the specified content by linking to a window or page.

Do Not Skip

There is no linked window or page to the current window which is played on the terminal.

Jump to Next Window

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked window.

Jump to Next Page

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked page.

Set Uniformly

Check **Set Uniformly** and set the following operations.

Switching Effect

Select the switching effect from the drop-down list for the current window. There are 11 types of switching effect.

Play Time (sec)

Set the playing duration for the current window.

Note

- The play time of a window can not exceed the playing time of a page, or the exceeding part of the program will not be played.
- For adding a webpage, you can set its play time as **Unlimited**.

8. **Optional:** On the current editing program page, perform the following operations.

Edit Program	Click to edit program parameters in the pop-up window.
Preview Program	Click **Preview** to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in full screen. For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click or to preview the previous or the next page of the program.
Create Schedule	Click **Next** to enter the Ordinary Schedule page and create a schedule for the program. **Note** For details, refer to ***Create an Ordinary Schedule*** .

9. Click **Save** to save the current program.
10. **Optional:** On the My Program page, perform the following operations.

View Program in List or Thumbnail Mode	Click / to view the added programs in the thumbnail mode or in the list mode.
Preview Program	Move the mouse cursor to a program, and click **Preview** to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen.

	For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click or to preview the previous or the next page of the program.
Copy Program	Move the mouse cursor to a program, and click **Copy** to enter editing program page. Click **Save** on the upper right corner to copy the current program, and a new program with the same content is created. **Note** When copying a program (e.g., Program A) for the first time, the name of the new program (Program A_1) will be generated automatically. If you need to copy this program (Program A) for a second or more times, you should manually edit its name, or the program cannot be created successfully.
Create Schedule	Move the mouse cursor to a program, and click **Release** to enter the Ordinary Schedule page and create a schedule for the program. For details, refer to ***Create an Ordinary Schedule*** .
Share / Cancel Sharing Program	Select one or more programs, click **Share** or **Cancel Sharing** to set the sharing property of programs as **Public** or **Private**. **Public** All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) and the higher-level organizations can see and use the schedule. **Private** All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) can see and use the schedule.
Filter / Search for Program	In the upper right corner, click to filter programs by the screen size, or enter keywords in the search box to search for the program(s).
Refresh Program List	Click **Refresh** to refresh the program list. The programs will be listed according to the time they are added.
Delete Program	Check one/more programs, or click **Select All** to select all programs, and click **Delete** to delete the selected programs.

Add Emergency Mustering Text Notification

You can add emergency mustering text notifications on the platform by configuring related parameters, and the added text notifications will be displayed on the digital signal terminals when the emergency is triggered.

Before You Start

Make sure you have added devices to the platform. For details, refer to ***Manage Digital Signage Terminals*** .

Steps

Note

For one device, only the latest added text notification can be displayed.

1. On the left, select **Content Creation → Template Library** .
2. Click **Emergency Mustering** on the top.
3. **Optional:** Click **Emergency Solution Settings** to enter Emergency Mustering module and view emergency solution settings.

   Note

   For details, refer to ***Add Emergency Solution*** .
4. Move the mouse cursor to the template of Text Notification for Emergency, and click **Create** to enter the adding text notification page.
5. Set the needed parameters, including text notification name and content.
6. Select an area and check device(s) under the area.

   Note

   Only the latest text notification can be displayed on one device. Therefore, if you select a device which has already been configured with a text notification, the previous text notification will be invalid and will not display any more.

   The text notification will be displayed on the selected devices.
7. Click **Release**.

   Note

   The text notification is released and will be displayed when the emergency is triggered.

   You can view the release status on the right side of the page.
8. **Optional:** Perform the following operations.

View Text Notification in List/Thumbnail Mode	Click / to view the added text notifications in the thumbnail mode or in the list mode.

Copy Text Notification	Move the mouse cursor to a text notification, and click **Copy** to enter the adding text notification page. A new text notification which is of the same content as the original one will be displayed. You can edit the content before releasing the new text notification, or click **Release** to release the current text notification directly. **Note** If you do not reselect device(s) for the new text notification, the previous text notification(s) configured on the device(s) will be invalid and will not display any more.
View Device Release Details	Move the mouse cursor to a text notification, and click **Device Status** to view release details of the text notification on the device.
Share / Cancel Sharing Text Notification	Select one or more text notifications, click **Share** or **Cancel Sharing** to set the sharing property of text notifications as **Public** or **Private**. **Public** All users in the current organization (i.e., the organization where the user who adds the text notification belongs to) and the higher-level organizations can see the text notification. **Private** All users in the current organization (i.e., the organization where the user who adds the text notification belongs to) can see the text notification.
Search for Text Notification	In the upper right corner, enter keywords in the search box to search for the text notification(s).
Refresh List	Click **Refresh** to refresh the text notification list.
Delete Text Notification	Check one or more text notifications, and click **Delete** to delete the selected text notifications.

32.4 Schedule Management

You can create a schedule and define a playing schedule to play the added programs on the devices according to the scheduled time or method. The platform supports two types of schedules: ordinary schedule and cut-in schedule. When creating schedules, you can select the needed programs and device(s) to release the programs. For the added schedules, you can perform more operations such as editing, releasing, searching, exporting, and filtering.

32.4.1 Create an Ordinary Schedule

You can create an ordinary schedule to play the added programs on the devices according to the scheduled time or method. The platform supports loop schedule, default schedule, or you can customize your schedule and play the programs by day or by week. For the added schedules, you can perform more operations such as editing, releasing, searching, exporting, etc.

Before You Start

- Make sure you have added program(s) to the platform. For details, refer to ***Create My Program*** .
- Make sure you have added device(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** , ***Manage Interactive Flat Panel*** , and ***Add LED Controller*** .

Steps

1. On the left, select **Schedule Management → Ordinary Schedule** .
2. Click **Add** to enter the Ordinary Schedule page.

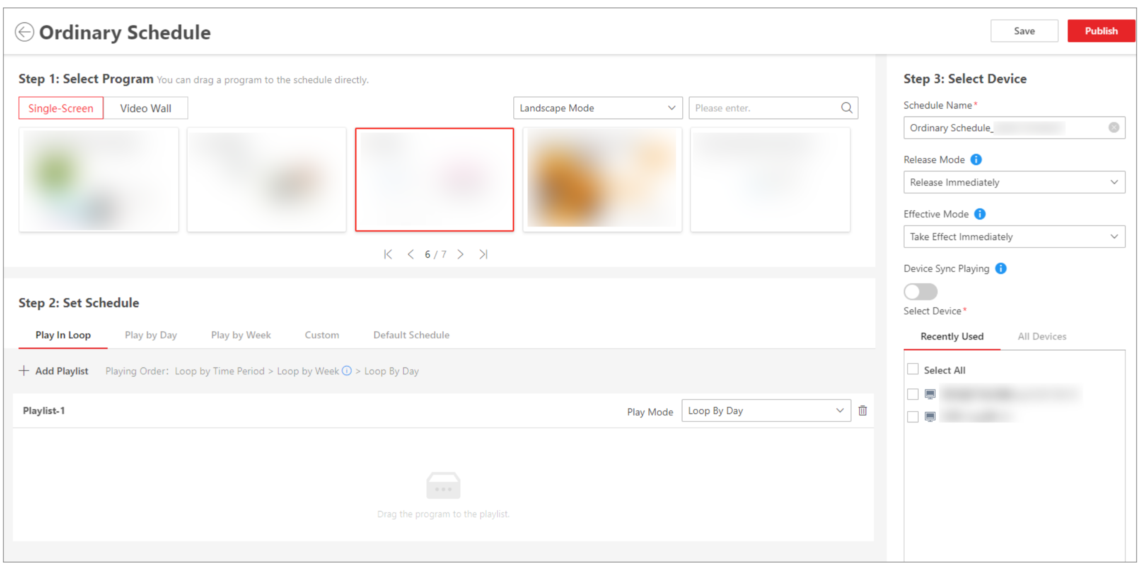


Figure 32-7 Ordinary Schedule

3. **Optional:** Filter the programs.
   - Select the program type as **Single-Screen** or **Video Wall**.
   - Select the screen size as **Landscape Mode**, **Portrait Mode**, or **Custom**.
   - Enter keywords in the search box to search for the program(s).
4. Select a program and set the schedule for it.

Play In Loop

a. Select a program in the program list and drag the program to the playlist.

Note

You can click **Add Playlist** to add more playlists as needed. Up to 8 playlists can be added, and up to 16 programs can be added to a single playlist.

b. Set the play mode.

Loop By Day

Play the program orderly and repeatedly by day. You can select the date to play.

Play By Week

Play the program orderly and repeatedly by week. You can set the playing day and time period.

Loop By Time Period

Play the program orderly and repeatedly by the selected time period.

Play by Day

Play the program according to a daily schedule.

a. Select a program from the program list and drag to the desired location on the timeline.

Note

You can add multiple programs to one day. When hovering the cursor on the program's playing time, you can view the thumbnail of the program.

b. Adjust the playing time of program(s).
c. Click on the right side of the timeline to delete all the selected programs.

Play by Week

Play the program according to a weekly schedule.

a. Select a program from the program list and drag to the desired location on the timeline.

Note

You can add multiple programs to one day. When hovering the cursor on the program's playing time, you can view the thumbnail of the program.

b. Adjust the playing time of program(s).
c. Click to copy the program to other day(s) in the week.
d. Click **Delete All** to delete all the selected programs.

Custom

Play the program according to a custom schedule.

a. Set the custom time.

Note

The time range should be within 90 days.

b. Select a program in the program list, and drag the program to the desired location on the timeline.

Note

You can add multiple programs to one day.

c. Adjust the playing time of program(s).
d. Click **Delete All** to delete all the selected programs.

Default Schedule	Play the default content automatically when no contents are scheduled on the device. Select a program in the program list, and drag the program to the playlist.

5. Select the device(s) to release the content.
   1) Enter the schedule name.
   2) **Optional:** Select the release mode as **Release Later** or **Release Immediately**.

   Note

   When selecting **Release Later**, you should set the release time, and the program schedule will be released at the configured time period.
   3) **Optional:** Select the effective mode as **Take Effect On Schedule** or **Take Effect Immediately**.

   Note

   When selecting **Take Effect On Schedule**, you should set the effective time. Only after the program takes effect, it can be played on the device.
   4) **Optional:** Switch on **Device Sync Playing**, select digital signage terminals and/or LED controllers.

   Note

   Make sure you have enabled the time synchronization of NTP server.
   5) Select device(s) from recently used devices or all devices.
   6) **Optional:** Enter the description.
6. Save or release the ordinary schedule.
   - In the upper-right corner, click **Save** to save the above settings and release the schedule later.
   - In the upper-right corner, click **Release** to start releasing the schedule to the selected device(s). After the schedule is released, you will enter the Release page and view the schedule releasing task in the list.

   Note

   • During releasing, you can click **Cancel Releasing** to cancel releasing.
   • You can view the release progress and the result on the right side of the page.
7. **Optional:** Perform the following operations if you save the schedule in the previous step.

Edit Schedule	Click the schedule name to enter Ordinary Schedule page and you can edit the schedule information.
Share / Cancel Sharing Schedule	Select one or more schedules, click **Share** or **Cancel Sharing** to set the sharing property of schedules as **Public** or **Private**.
Release Schedule	a. Click in the Operation column to open the Schedule Releasing window. b. Set the parameters including schedule name, release mode (optional), and effective mode (optional).

	c. Select the device(s) from the recently used devices or all devices. d. Click **Save and Release** to save the settings and release the schedule to the selected device(s).
Export Schedule	Click in the Operation column, and select the saving path to export the selected schedule to the local PC.
Refresh Schedule List	Click **Refresh** to refresh the schedule list. The schedules will be listed according to the time they are added.
Delete Schedule	Check one or more schedules, and click **Delete** to delete the selected schedules.
Filter Schedules	In the upper right corner, select one or more play modes, or enter keywords in the search box to filter the schedules which meet the conditions.

32.4.2 Create a Cut-In Schedule

You can create a cut-in schedule to cut in the specific programs or text messages on the specific devices according to the scheduled time. The cut-in programs or text messages will precede other contents. After creating schedules, you can perform more operations such as editing, releasing, searching, etc.

Before You Start

- Make sure you have added program(s) to the platform. For details, refer to ***Create My Program*** .
- Make sure you have added device(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** and ***Manage Interactive Flat Panel*** .

Steps

1. On the left, select **Schedule Management → Cut-In Schedule** .
2. Click **Add** to enter the Cut-In Schedule page.

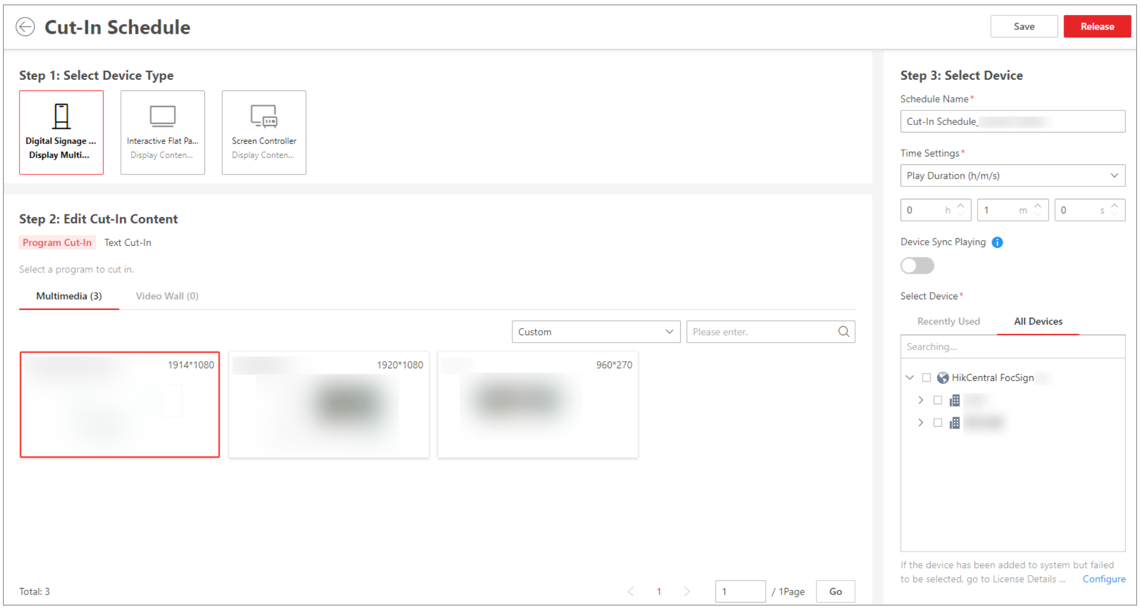


Figure 32-8 Cut-In Schedule Page

3. Select **Digital Signage**, **Interactive Flat Panel**, or **Screen Controller** as the device type.
4. Select the cut-in content.
   - Cut in a program: Click **Program Cut-In**, and select a program.
   - Cut in the text message:
     a. Click **Text Cut-In**, and select the screen size as **Landscape Mode** or **Portrait Mode**.
     b. In the Edit Text Message area, set the content and the corresponding play time.

     Note

     The play time for different text messages can be overlapped. You can click in the Operation column to view the playing effect of the current text message on the left side of the page.

     c. Set the configuration mode, front size and color, background, etc., for the text message.
5. Select the device(s) to release the content.
   1) Enter the schedule name.
   2) For **Program Cut-In**, set playing duration.
   3) **Optional:** Switch on **Device Sync Playing** (for digital signage terminals only).

   Note

   Make sure you have enabled the time synchronization of NTP server. See details in ***Set NTP for Time Synchronization*** .

   4) Select device(s) from recently used devices or all devices.
6. Save or release the cut-in schedule.
   - In the upper-right corner, click **Save** to save the above settings and release the schedule later.

- In the upper-right corner, click **Release** to start releasing the schedule to the selected device(s). After the schedule is released, you will enter the Release page and view the schedule releasing task in the list.

Note

- During releasing, you can click **Cancel Releasing** to cancel releasing.
- You can view the release progress and the result on the right side of the page.

7. **Optional:** Perform the following operations if you save the schedule in the previous step.

Edit Schedule	Click the schedule name to enter Cut-In Schedule page and you can edit the schedule information.
Share / Cancel Sharing Schedule	Select one or more schedules, click **Share** or **Cancel Sharing** to set the sharing property of schedules as **Public** or **Private**.
Release Schedule	a. Click in the Operation column to open the Schedule Releasing window. b. Set the schedule name. c. Select the device(s) from the recently used devices or all devices. d. Click **Save and Release** to save the settings and release the schedule to the selected device(s).
Refresh Schedule List	Click **Refresh** to refresh the schedule list. The schedules will be listed according to the time they are added.
Delete Schedule	Check one or more schedules, and click **Delete** to delete the selected schedules.
Filter Schedules	In the upper right corner, select the playing type, or enter keywords in the search box to filter the schedules which meet the conditions.

32.4.3 View Release Records

You can view release records of all the tasks and the details of their release status.

On the left, select **Schedule Management → Release** . You can view release details of all the tasks on the platform, including task name and type, release time, effective time, and release status (Released or Failed), etc. Also, you can perform more of the following operations.

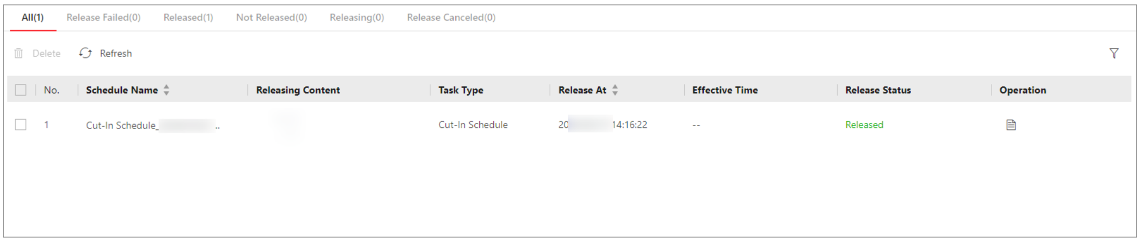


Figure 32-9 View Release Records

- **View Release Details**: Click in the Operation column to view release details such as device name and release progress.

> **Note**
>
> For a task that is releasing, you can click **Cancel Release** to cancel releasing the task. For a task that failed to be released or was canceled releasing, you can click **Release again** to release the task again.

- **Delete Task**: Check one or multiple tasks, and click **Delete** to delete the selected tasks.
- **Release Again**: For a task that failed to be released, you can click to release the task again.
- For tasks failed to be released due to network or electricity disconnection, they can continue to be released within the effective period (48 hours) if connected to the network or electricity again.
- **Filter Tasks**: On the top of the page, click **Release Failed**, **Released**, **Not Released**, **In Release**, or **Invalid Release** to filter tasks via release status; In the upper right corner, click , and filter tasks by conditions such as task name and type.

32.5 Review Management

The added contents should be reviewed before they are used. After being reviewed, the contents can be released automatically.

> **Note**
>
> The contents created by the user who has the review permission can be released directly, otherwise the contents should be reviewed by the user who has the review permission.

On the left, select **Review Management**.

Perform the following operations as needed.

Description	Operation
Review Content One by One	1. On the **All** and **To Be Reviewed** pages, click in the **Operation** column. 2. On the pop-up Content Review page, review the content.

Description	Operation
	3. Select the result as **Pass** or **Deny**. 4. Enter the comment. **Note** When the result is **Deny**, the comment is required. You can enter up to 128 characters. 5. Click **Preview** to preview the program. **Note** During previewing, you can adjust the playing speed, view in full screen, and switch program pages. 6. Click **OK**.
Batch Review Contents	• On the **All** and **To Be Reviewed** pages, check multiple contents to be reviewed, click **Pass**, and enter the comment (optional) to batch pass the selected contents. • On the **All** and **To Be Reviewed** pages, check multiple contents to be reviewed, click **Deny**, and enter the comment (required) to batch deny the selected contents. **Note** When entering the comment, you can enter up to 128 characters.
Delete Content	On the **Denied** and **Passed** pages, check one or more contents, click **Delete** to delete them.
Refresh Content	On the **All**, **To Be Reviewed**, **Denied** and **Passed** pages, click **Refresh** to refresh the content list.
Search for Content	On the **All**, **To Be Reviewed**, **Denied** and **Passed** pages, enter keywords in the search box in the upper right corner to search for the target contents.

32.6 Material Library

Material is used for creating programs. The platform supports various types of materials to meet different program requirements. You can upload local materials (such as picture and video) and other materials (such as webpage and picture URL) to the platform. After uploading the materials, you can mange materials including editing, searching, replacing, etc.

Note

On the left, select **Material Library** to enter the Material Library page.

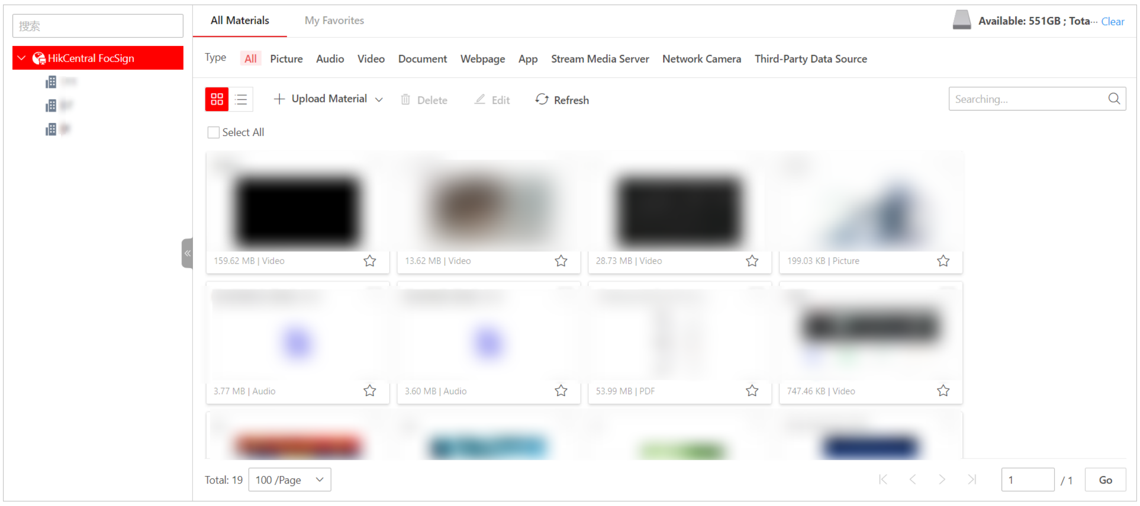


Figure 32-10 Material Library

32.6.1 Upload Materials

You can upload materials which can be used for creating programs. The materials supported to be uploaded include picture, video, audio, document, APP, webpage, network picture, stream media server, network camera, etc. For the uploaded materials, you can perform more operations, including adding to favorites, editing, downloading, deleting, etc.

Steps

1. Click **All** → **Upload Material** to select the uploading mode. Or select a material type as following methods an perform operations.

Table 32-3 Operations about Supported Material Types and Formats

Material Type	Format	Operation
Picture	BMP, JPG, PNG, GIF, JPEG	• Click **Picture** → **Upload Materiel** → **Create URL Picture Material** , enter the name and URL address of the picture. • Click **Picture** → **Upload Materiel** → **Local Upload** to upload the selected local materials. Meanwhile, the uploading

Material Type	Format	Operation
		progress and the failure details will be displayed (when uploading fails).
Video	ASF, AVI, MPG, 3GP, MOV, MKV, WMV, FLV, MP4	Click **Video/Audio/Document/App → Local Upload** to upload the selected local materials. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails).
Audio	MP3, WAV, WMA	
Document	TXT, PDF, EXCEL, DOC, DOCX, PPT, PPTX	
App	APK	
Webpage	HTML, HTM	• Click **Webpage → Upload Materiel → Local Upload** to upload the selected local materials. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails). • Click **Webpage → Upload Materiel → Create URL Picture Material** , enter the name and URL address of the webpage.
Streaming Media Service	/	Click **Streaming Media Service → Create Material** to receive streams from the streaming media server. If you disable **Built-In Steaming Media Service**, you should enter the URL of the streaming media server. If you enable **Built-In Steaming Media Service**, you should enter the IP address, port No., channel No., user name, and password of the network camera.
Network Camera	/	Click **Network Camera → Create Material** to get video streams from network camera. You should enter the required information of network camera such as IP address, port No., and channel No.
Third-Party Data Source	/	Click **Third-Party Data Source → Create Material** . There are two types of data source: Auto-Push Data Source and Third-Party Database. If you select **Auto-Push Data Source**, you should enter data source ID and select the data type; If you select **Third-Party Database**, you should set the basic information of the third-party database, including data source ID, database type, encoding format of data interchange, database name, IP address, etc.

Note

- A single material should be smaller than 4 GB. The names of any two materials cannot be the same.
- Up to 1,000 materials can be uploaded to the platform at a time. Up to 10,000 materials can be stored in the platform.
- For those materials that fail to be uploaded, click to upload again or click to replace the material. For those materials with the failure reason "duplicated material", you can replace the material or click **Close** to cancel uploading.
- If you set **Sharing Property** to **Public**, all users in the current organization (i.e., the organization where the user who creates the material belongs to) and the higher-level organizations can see and use the material. If you set **Sharing Property** to **Private**, all users in the current organization (i.e., the organization where the user who creates the material belongs to) can see and use the material.

2. **Optional:** After uploading the materials, perform the following operations.

Add to Favorites or Not	Click to add the material to **My Favorites**. Click again to remove it from **My Favorites**.
Edit Material	Check one/more materials, or check **Select All** to select all materials, and click **Edit** to edit the selected materials, such as editing the name and the property.
Delete Material	Check one/more materials, or check **Select All** to select all materials, and click **Delete** to delete the selected materials. **Note** You cannot delete materials that have been added to a program or materials that are being released.
Download Material	Click to download single material to the local PC.
View Large Picture	Click to view large picture of the material.
Refresh Materials	Click **Refresh** to refresh the material list.
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Search for Material	Enter keywords in the search box, and click to search for materials. You can also click tabs (**All**, **Picture**, **Audio**, etc.) on the top of the materials to filter materials.

32.6.2 Manage Materials in My Favorites

You can manage materials in **My Favorites**, such as editing materials, filtering materials, and deleting materials.

On the top, click **My Favorites**.

Table 32-4 Mange Materials

Description	Operation
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Add to Favorites or Not	Click or to add the material to **My Favorites** or remove it from **My Favorites**.
Edit Material	Select material(s) to be deleted, and click **Edit** to edit the selected materials, such as name and sharing property.
Refresh Material	Click **Refresh** to refresh the material list.
Download Material	Click to download the material to local PC. **Note** Only materials uploaded from local PC can be downloaded.
View Large Picture	Click to view the large picture of the material.
Search for Material	Enter keywords in the search box, and click to search for materials. You can also click tabs (**All**, **Picture**, **Audio**, etc.) on the top of the materials to filter materials.
Delete Material	Select material(s) to be deleted, and click **Delete** to delete the selected materials. **Note** You cannot delete materials that are added to a program or being released.

You can view statistics reports including flat panel usage statistics, content playing statistics and material playing statistics.

On the left, select **Statistics Report**. If you have added the target menu to the top navigation, click the menu on the top directly, and this entry will be introduced in the following.

32.7.1 View Flat Panel Usage Statistics

You can view daily/weekly/monthly/customized flat panel usage statistics.

Steps

1. On the left, select **Statistics Report → Flat Panel Usage Statistics** .
2. Select device(s).
3. Select report type as daily/weekly/monthly report, or customize a period.
4. Select the counting time.
5. Click **Generate Report**.

   The report will be displayed on the right pane, and you can view statistics in a bar chart and view device usage details in a table.

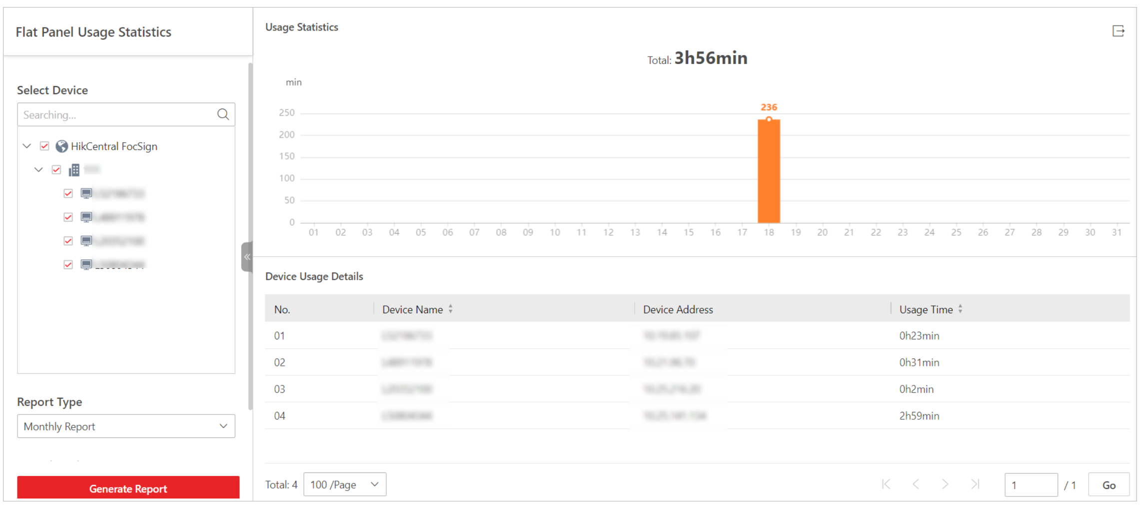


Figure 32-11 View Flat Panel Usage Statistics

32.7.2 Content Playing Statistics

You can set search conditions such as device and start time to search for content playing statistics. You can export the statistics to the local PC if needed.

Steps

1. On the left, select **Statistics Report → Content Playing Statistics** .
2. Set the search conditions including device, start time, and end time.
3. Click **Search**.

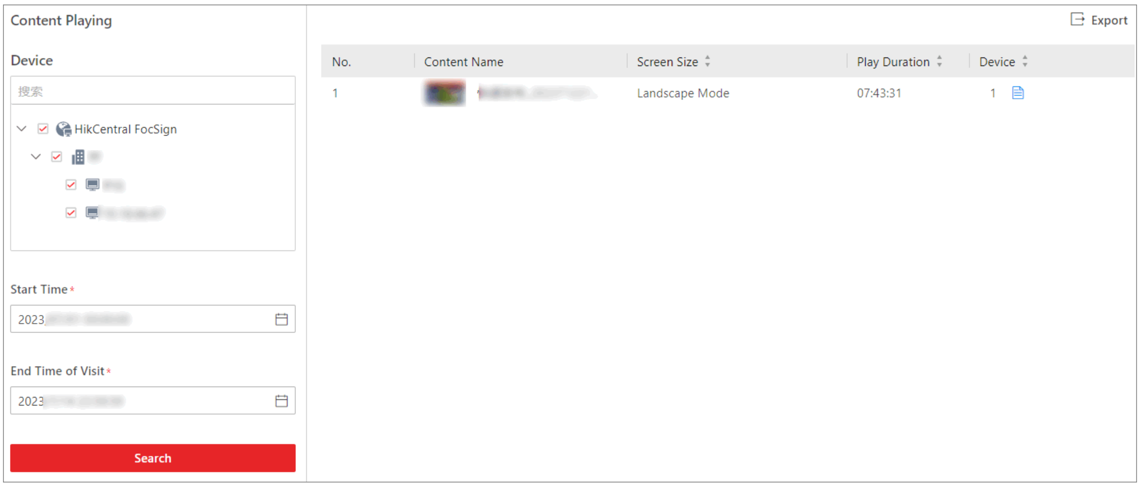


Figure 32-12 Content Playing Statistics

The search results will be displayed on the right. You can view the content name, screen size, etc.

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

View Device Information	Move the mouse cursor to in the Device column to view the name(s) and content playing duration of the device(s).
View Large Picture of Content	Move the mouse cursor to the picture in the Content Name column to view the large picture of the content.
Export Statistics	Click **Export** in the upper right corner and select a file type to export the searched statistics to the local PC.

32.7.3 Material Playing Statistics

You can set search conditions such as device and start time to search for material playing statistics. You can export the statistics to the local PC if needed.

Steps

1. On the left, select **Statistics Report → Material Playing Statistics** .
2. Set the search conditions including device, start time, end time, and material type.
3. Click **Search**.

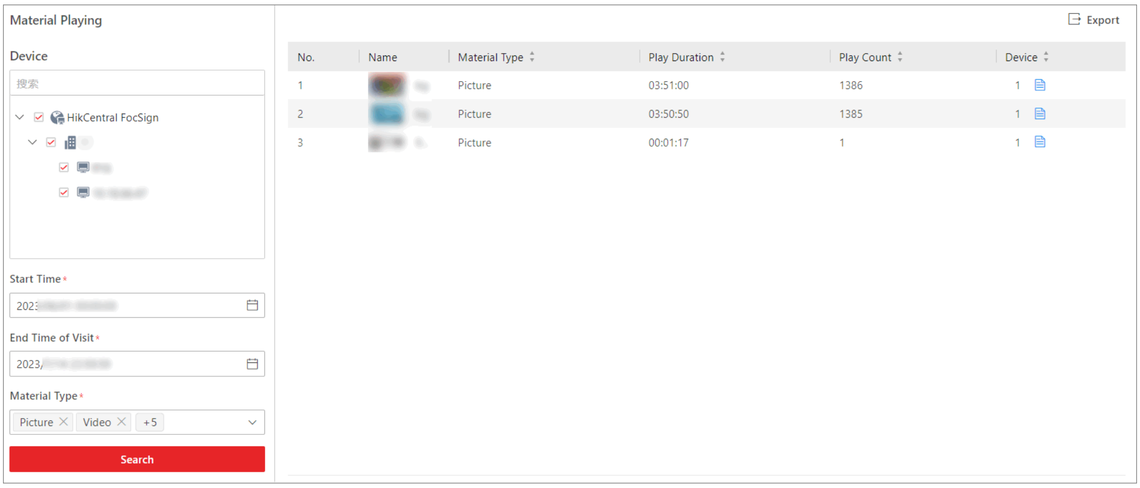


Figure 32-13 Material Playing Statistics

The search results will be displayed on the right. You can view the material name, material type, etc.

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

View Device Information	Move the mouse cursor to in the Device column to view the name(s) and content playing duration of the device(s).
View Large Picture of Material	Move the mouse cursor to the picture in the Name column to view the large picture of the material.
Export Statistics	Click **Export** in the upper right corner and select a file type to export the searched statistics to the local PC.

32.8 Basic Settings

In Basic Settings module, you can configure material storage location and configure video walls.

32.8.1 Set Weather Web Manufacturer

You can enable weather service and set the weather manufacturer for the programs including weather information. After enabled, you can add a weather window in the program and display the weather information provided by the manufacturer.

Select **Weather Web Manufacturer** on the left navigation bar, and enable **Weather Web Manufacturer**.

Select the manufacturer name, and then enter the authorization code.

Note

The user should buy the weather service from the weather manufacturer and get the authorization code.

32.8.2 Set Material Storage Location

The materials uploaded can be saved to the local storage or pStor server.

Steps

1. On the left navigation pane, click **Basic Settings → Material Storage Location** .
2. Set the storage location as **Local Storage** or **pStor**, and select a resource pool.

   Note

   To select **pStor** as the storage location, make sure you have added pStor servers to the platform.
3. Click **Save** to save the above settings.

32.8.3 Add Video Wall

A video wall is made up of multiple terminals. After adding more than one terminals to the platform, you can configure video walls with custom dimensions (row × column).

Before You Start

Make sure you have added at least two terminals to the platform and have enabled the time synchronization of NTP server. See details in ***Add Digital Signage Terminal*** .

Steps

1. On the left, select **Basic Settings → Video Wall Configuration** .
2. Click **Add**.

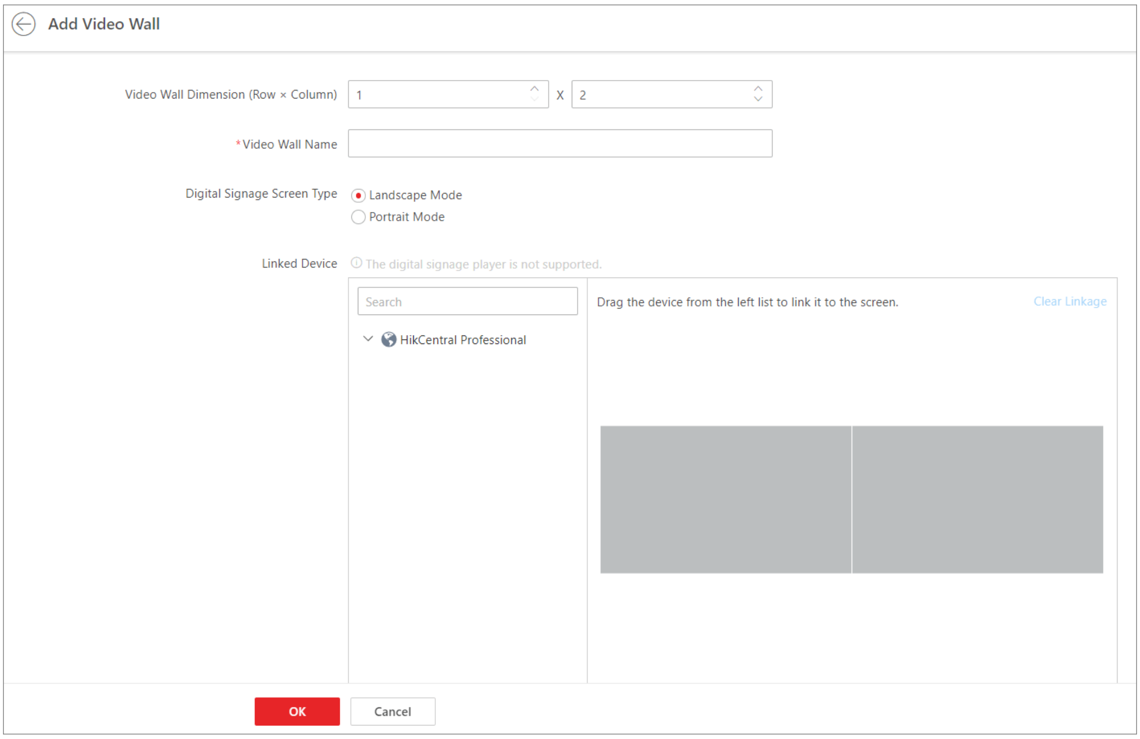


Figure 32-14 Add Video Wall

3. Specify the video wall dimension (row × column).
4. Enter the video wall name.
5. Select **Landscape Mode** or **Portrait Mode** as the screen type.
6. In Linked Device area, drag the devices from the device list to the screen on the right.

Note

The digital signage player is not supported.

7. **Optional:** Click **Clear Linkage** to clear the linked devices from the screen.
8. **Optional:** Enter the description of the video wall.
9. Click **OK**.
10. **Optional:** After adding video walls, you can perform the following operations.

Switch Display Mode	Click / to display the added video walls in the thumbnail/list mode.
Edit Video Wall Information	• In thumbnail mode, click the video wall card to enter the video wall information page and edit the information. • In list mode, click the name of the video wall to enter the video wall information page and edit the information.
Delete Video Walls	Select one or multiple added video walls and click **Delete** to delete the selected video walls.

Refresh Video Wall List	Click **Refresh** to refresh the video wall list.
Search Video Walls	Click ▽ , set the search conditions such as dimension and screen type, and click **Search** to search for the target video walls.

32.9 Device Control

The platform supports controlling selected devices (including digital signage terminals, interactive flat panels, LED controllers, and video walls) by clicking buttons of general functions, and creating a combined control command to control devices.

32.9.1 Control a Device

You can control the devices after adding them to the platform.

Note

Make sure you have added devices to the platform.

On the left, select **Device Control → Device Control** .

General Operations When Devices are Selected

Check devices of different types, and then click buttons on the top.

Open/Close Screen

Turn on/off the device sleep mode. If it is turned off, the screen will be woke up from the sleep mode.

Restart

Restart selected devices.

Play/Stop

Play/stop the programs on the terminal(s).

Stop Cut-In

Stop cutting in programs.

Clear Playing Contents

Clear all the contents to be played on the screen(s), including programs, cut-in programs, etc.

Volume

Set the output volume of the selected device(s).

Time Startup/Shutdown

The device(s) will start up / shut down according to the schedule.

Combined Control

When you need to control multiple devices in a batch, you can create a combined control command for the devices and then control them in a batch. See ***Create a Combined Control Command for Multiple Devices*** .

Restore Default Settings

Only available for digital signage terminals.

Enable/Disable Sync Playing

Enable/disable sync playing the same released contents on different digital signage terminals.

Note

Make sure you have enabled the time synchronization of NTP server.

Remote Debugging

Enable the Android debug bridge for the device(s), and enter the debugging contents.

Export Log

Export the logs of the device(s) in ZIP format.

Remote Control

Hover the cursor on a device, and click **Remote Desktop** to connect the device and operate on the device remotely.

Note

This should be supported by the device.

Note

The operations should be supported by the selected device type(s).

Other Operations

Switch Display Mode

Click / to display the added devices in thumbnail/list mode.

Filter by Device Type

In the drop-down list of the **Device Type**, select **Digital Signage Terminal** / **Interactive Flat Panel** / **Video Wall**.

Filter by Device Status

In the drop-down list of the **Device Status**, select **Open Screen** / **Close Screen** / **Offline** to filter devices by status.

Refresh Device List

Click **Refresh** to refresh the device list.

Search for a Device

In the text bar on the right of **Device Status**, enter a device name to search for it.

32.9.2 Create a Combined Control Command for Multiple Devices

When you need to send multiple control commands to devices at a time, you can create a combined control command for the devices. The platform supports controlling digital signage terminals, interactive flat panels, and video walls.

Before You Start
Make sure you have added devices to the platform.

Steps

1. On the left, select **Device Control → Combined Control Command** .
2. Click **Add** to enter the Create Combined Control Command page.
3. Enter a name for the command group.
4. Select a device type.
5. In the Select Control Command area, click the buttons under each tab to add it to the Command Details on the right.
6. Click **Save** to save the command, or click **Execute** to execute the command.

   The added command will be displayed in the command list.
7. **Optional:** Perform the following operations if needed.

Execute a Command	Click **Execute** to execute a command in the list.
Delete Command(s)	Click **Delete** behind a command to delete it, or check **All Commands**, and then click **Delete** on the top to delete all commands in the list.
Search for Command(s)	On the upper-right, enter the name of the combined control demand to search for it.

32.10 Application Management

You can give algorithm capabilities to devices by configuring device application packages. After you finish configuring, you can add and apply the applications to interactive flat panels and manage the applications.

32.10.1 Add Applications

You can add device applications to the platform, and then apply them to interactive flat panels.

Before You Start
Make sure the interactive flat panels you are going to use are added to the platform. For details, see ***Manage Interactive Flat Panel*** .

Steps

1. On the left, select **Application Management** to enter the Application Management page.
2. Click **Add**.
3. Click to upload an application package from the local PC, and add function descriptions if there are any.

   Note

   Only one application can be added at a time.
4. Click **Next**, and then select available device(s) to apply the application.
5. Click **Apply** to apply the application to the device.

   There will be a pop-up window showing the process of the application, and you can click **Cancel** to cancel the applying process. If the device loses power during the applying process, the platform will continue to apply the application after powering on the device again.
6. **Optional:** Perform the following operations after applying applications to device(s).

View Application Records	Click **Application Record** to open the Application Record page, you can specify conditions, and click **Search** to view the records about adding device applications in specific time period. **Note** The icon indicates that adding device application(s) failed.
Apply Application	Click to open the page for applying application to device. Select the device(s) and click **OK** to finish applying.

32.10.2 Manage Applications on Devices

You can manage device applications after adding the them.

Note

Make sure the devices you are going to use are added to the platform. For details about adding interactive flat panels, see ***Manage Interactive Flat Panel*** .

On the LEFT, select **Application Management** to enter the Application Management page.

You can perform the following operations.

Add Device Application to Specific Device	Select an interactive flat panel in the list, and click **Add** to add an application to the device.

	Note Only one application can be added at a time.
Uninstall Application	Select an interactive flat panel in the list, select applications on the right, and click **Uninstall** on the top to uninstall applications.
Refresh Device Application List	Click **Refresh** to refresh the application list.
View Application Records	Click **Application Record** to open the Application Record page, you can specify conditions, and click **Search** to view the records about adding device applications in specific time periods. **Note** The icon indicates that applying device application(s) failed.

Chapter 33 Emergency Mustering

The emergency mustering module facilitates the safe evacuation of people during a crisis or emergency situation. You can customize emergency solutions for various areas and then start a roll call to verify who is safely accounted for at evacuation sites and mustering points.

Take the following steps to configure the emergency mustering system.

1. In the upper left corner of the Home Page, select → **Integrated Service → Emergency Mustering** .
2. Customize your emergency solution by area. For details, see ***Add Emergency Solution*** .
3. Select area(s) to trigger an emergency and start a roll call. For details, see ***Start a Roll Call*** .

33.1 Add Emergency Solution

Take the following steps to add an emergency solution:

1. ***Select Areas***
2. ***Add Card Readers***
3. ***Add Doors Remaining Unlocked in Emergency***
4. ***Add Emergency Counting Groups***
5. ***Release Emergency Mustering Notifications***
    - ***Add Emergency Mustering Programs***
    - ***Add Text Notifications***
    - ***Set Broadcast Linkage***
6. ***Trigger Emergency Automatically***

33.1.1 Select Areas

- If you are configuring the emergency solution for the first time, select **Configure**, and then select area(s) for emergency mustering.
- If you have configured the emergency solution, select **Emergency Solution Settings → Add Solution for Emergency Evacuation** , and then select area(s) for emergency mustering.

33.1.2 Add Card Readers

To add an entrance & exit point and a mustering point, you should select card readers for authentication, headcounts or other measures. Authenticated individuals are marked as "In" at an entrance and "Out & Not Check in" at an exit. A mustering point is the designated location to assemble after an emergency evacuation. Those who have checked in at the mustering point are marked as "Checked In At Mustering Point". This part will guide you through adding mustering points.

Select **Mustering Point → Add → Card Reader → OK** .

Note

Ensure that you have added card reader(s) to the platform before setting the entrance point, exit point, and mustering point.

33.1.3 Add Doors Remaining Unlocked in Emergency

In an emergency, unlocked doors ensure that occupants can exit their work site quickly and efficiently and help emergency responders access the building rapidly to conduct rescue operations without authentication at the card reader.

To add doors remaining unlocked in emergency, select **Doors Remain Unlocked in Emergency → Add → Door → OK** .

33.1.4 Add Emergency Counting Groups

After setting the resource access permission and adding persons, you can add emergency counting groups for headcounts based on the authentication status.

Set Permissions

To access and manage emergency counting groups, set the resource access permission.

1. In the upper left corner of the Home Page, select **→ Account and Security → Roles → Add** , and set the basic information.
2. Select **Resource Access**, set the resource type to Emergency Counting Group, and select a group in an area as needed.

Add Emergency Counting Groups

To add an emergency counting group in the Emergency Solution Settings page, select **Emergency Counting Group →** + , enter the group name and description, select persons, and then select **Add**.

Note

You can also add persons to an emergency counting group before adding an emergency counting group. To add persons who have been added to the platform to a group, take the following steps:

1. In the upper left corner of the Home Page, select **→ Person** .
2. Click the personal ID, select **Emergency Counting Group**.
3. Select a group in an area, and then select **Add**.
4. (Optional) You can also select **Add → Emergency Counting Group** , and select a group in an area to add new persons to a group.

33.1.5 Release Emergency Mustering Notifications

To ensure safety, coordination, and effective communication during critical situations, you can configure emergency mustering programs and text notifications. These notifications will be displayed on digital signal terminals or disseminated by broadcasts when an emergency is triggered.

Add Emergency Mustering Programs

To add an emergency mustering program, take the following steps:

1. Select **Prompt by Digital Signage Terminal → Configure** .
2. Select a template, and click **Create**.
3. Set the page and background music, and select **Release → Select Device → OK** .

Add Text Notifications

To add a text notification, take the following steps:

1. Select **Prompt by Digital Signage Terminal → Configure** .
2. Select **Text Notification Emergency** and click **Create**.
3. Set the notification name and content.
4. Select the device.
5. Select **Release**.

Set Broadcast Linkage

To set the broadcast linkage, take the following steps:

1. Select **Prompt by Broadcast → Configure** .
2. Configure the following parameters: the broadcast name, area, speaker unit, broadcast content, audio file, and play mode.
3. Select **Save and Apply**.

33.1.6 Trigger Emergency Automatically

You can add events and alarms to allow the platform to automatically trigger an emergency by area when the event or alarm is triggered.

1. In the top left corner of Home page, select ▦ **→ Security Monitoring → Event and Alarm → Event and Alarm Configuration → Normal Event and Alarm → Add** .
2. Set the triggering condition.
3. Set the linkage action to **Send Email**, select a template, and then select emergency counting groups by area.
4. Enable **Trigger Alarm** to set the alarm priority and recipients.
5. Enable **Trigger Emergency** to set **Reaction of Platform** to **Trigger Emergency**, and to select an area.

33.2 Start a Roll Call

After configuring the emergency solutions, you can start a roll to check that all personnel have safely evacuated from a hazardous area or are present in designated mustering point. During emergencies, it is essential to manage information effectively. Roll call provides a systematic way to gather and relay information about individuals' whereabouts.

Take the following steps to start a roll call.

1. Select **Roll Call → Select Area for Triggering Emergency** .
2. View the detailed personnel information of all selected areas to ensure the safety and accountability of all individuals.
3. (Optional) Click a card to view the detailed personnel information of a single area, including the overall information, profile picture, name, phone number, and status.

   Note

   Click to check in a person who shows at the mustering point but the person status is not Checked In At Mustering Point.
4. (Optional) You can perform the following operations as needed.

Operation	Description
End the emergency status.	- Select **Turn off Emergency of All Areas** to end the emergency status of all areas. - Select **Turn Off Emergency** to end the emergency status of the selected area. Before you edit the emergency solution, end the emergency status.
Select person statuses.	Select **Set Statistics Type** on the upper-right corner.
Send emergency mustering report.	Select **Send Report** to select areas/groups, set sorting rules, select the report export mode, and confirm your password. If you set the report export mode to **Send Email**, you can select **New Email Template** to quickly configure a new email template.
Automatically print the emergency mustering report when you end the emergency status of a selected area.	Select **→ Security Monitoring → Event and Alarm → Event and Alarm Configuration → Normal Event and Alarm → Add** , enable **Trigger Alarm → Trigger Emergency** , set the reaction of platform to **Turn off Emergency**, enable **Print Report**, and select an emergency counting group for report printing.

Chapter 34 Broadcast Management

You can manage the added speaker units in the platform and configure the related functions for them. For example, you can group multiple speaker units, configure live broadcast, configure scheduled broadcast, etc.

34.1 Set Basic Settings for Broadcast

You can set locations to save the audio file and live broadcast recording file. Also, you can set parameters related with live broadcast, including broadcast mode and encoding format.

Steps

1. On the top navigation bar, select → **Integrated Service → Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Basic Configuration**.
3. In Audio File area, select **Local Storage** or **pStor** as the location to save the audio file, and select the corresponding resource pool.

   Note

   When selecting pStor as the storage location, make sure you have added pStor to the platform.
4. In Live Broadcast Recording area, check **Live Broadcast Recording**.
5. Select **Local Storage** or **pStor** as the location to save the recording file, and select the corresponding resource pool.

   Note

   When selecting pStor as the storage location, make sure you have added pStor to the platform.
6. In Live Broadcast Parameters area, select the broadcast mode and the encoding format from the drop-down list.

   Default

   The SYS server automatically judges via which method to send the broadcast data to the speaker unit according to the network domain of the Client (Web Client, Control Client, or Mobile Client).

   Via Streaming Server Proxy

   The Client sends the broadcast data to the speaker unit via the streaming server.

   Direct Access

   The Client directly sends the broadcast data to the speaker unit.

   Via Center Proxy

   The Client sends the broadcast data to the speaker unit via the SYS server.
7. Click **Save** to save the above settings.

34.2 Group Speaker Units

You can group multiple speaker units for convenient management. Take the scenario of an industrial park for example, if there are 10 speaker units on the first floor, you can group all these speaker units into a group.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Speaker Unit Group**.
3. Create a speaker unit group.
   1) Click .
   2) Enter the name for the group.
   3) Click **Add**.
4. Add speaker unit(s) to the speaker unit group.
   1) Click **Add**.
   2) In the pop-up device list, select speaker unit(s) to be added.
   3) Click **Add**.
5. **Optional:** Perform the following operations.

View Audio File	Click to view the audio file(s) of the corresponding speaker unit.
Delete Speaker Unit	Check one or more speaker units to be deleted, and click to delete the selected devices.
Adjust Volume	Check one or more speaker units, and click **Volume** to adjust the volume of live broadcast or alarm-triggered broadcast for the selected devices. **Note** For Hikvision devices, you can only adjust the volume of live broadcast.

34.3 Manage Media Files

You can upload and manage media files to the platform. The uploaded media files can be used for live broadcast, scheduled broadcast, etc.

Before You Start

Make sure you have saved the media files to be uploaded to your local PC.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Media Library**.

3. Select a media library (except the root library on the top) from the list, or click to add a new media library under the root library.

   You can view all the media file(s) in the selected media library.
4. Click **Add**.
5. Select one or more media files from local PC.

   Note

   The file should be in MP3 or WAV format, and no larger than 10 MB.
6. Click **Upload**.

   Note

   You can view the uploading progress and result(s).

   The uploaded media file(s) are displayed in the list.
7. **Optional:** Perform the following operations.

Add	Click **Add** to add more media files.
Delete	Select one or more media files, click **Delete** to delete the selected files.
Download	Click on the Operation column to download the media file to local PC.

34.4 Configure Live Broadcast

You can select the speaker unit(s) and the broadcast mode to configure live broadcast. The corresponding audio file or the user's voice will broadcast on the speaker unit(s) in real time.

Before You Start

- Make sure you have grouped speaker units. Refer to ***Group Speaker Units*** for details.
- Make sure you have added speaker unit(s) to area(s).
- Make sure you have added media file(s) to the media library. Refer to ***Manage Media Files*** for details.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Live Broadcast and Recording** → **Live Broadcast** .
3. Select the online speaker unit(s) for live broadcast.
   - Select **Group**, and select one or more speaker units from speaker unit group(s).

     Note

     You can click **Display Terminals Not Grouped** to display the speaker unit(s) that are not grouped.
   - Select **Area**, and select one or more speaker units from the area(s) where the speaker units are added.

Note

You can hover on a speaker unit, and click to listen to the live broadcast content. During listening, you can click to adjust the volume, and click to stop listening. This function should be supported by the device.

4. Select the broadcast mode.
   - Check **Speak**.
   - Check **Audio File**, and select an audio file from the media library.

     Note

     You can click **Download** to download and play the selected audio file beforehand to ensure the audio can broadcast fluently and correctly.
   - Check **Custom Broadcast Content**, select a language, and enter the broadcast content as needed.

     Select **Once** or **Specified Duration** as the play mode.
5. Click **Start**.

Note

After starting broadcasting, you can click in the Operation column to listen to the broadcast content; click to adjust the volume; and click to stop listening. This function should be supported by the device.

What to do next

Speak to the PC microphone, play the audio file, or play the custom broadcast content.

34.5 Search for Live Broadcast Records

You can set search conditions including the start time, end time, and the broadcaster to search for live broadcast records.

Before You Start

- Make sure you have finished live broadcast. Refer to ***Configure Live Broadcast*** for details.
- Make sure you have enabled the function of **Live Broadcast Recording**. For details, refer to ***Set Basic Settings for Broadcast*** .

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Live Broadcast and Recording** → **Live Broadcast Recording** .
3. Set the start time.
4. Set the end time.
5. Select a broadcaster from the drop-down list.
6. Click **Search**.

You can view the search results on the right side and view the details of each record, including the broadcaster, the number of the speaker units, the start time, the broadcast mode, and the file size.

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

Download	Click in the Operation column to download the broadcasted audio.
View Speaker Unit	Click › to view the speaker unit.
View Custom Broadcast Content	If the broadcast mode is **Custom Broadcast Content**, hover the mouse cursor over in the Operation column to view the custom broadcast content.

34.6 Add a Scheduled Broadcast Task

You can configure the parameters such as the period type and play mode to add a scheduled broadcast task in the platform and then apply the task to the speaker unit(s). After that, the audio file(s) you have selected will be played on the corresponding speaker unit(s) according to the schedule. For the added scheduled broadcast task(s), you can view the task details, search for target task(s), etc.

Before You Start

- Make sure you have grouped speaker units. Refer to ***Group Speaker Units*** for details.
- Make sure you have added speaker unit(s) to area(s).

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Scheduled Broadcast**.
3. Click **Add** to enter Add Scheduled Broadcast page.
4. Enter the name for the scheduled broadcast task.
5. Select the speaker unit(s) to execute the task.
   - Check **Group**, click **Add**, select one or more speaker units from speaker unit group(s), and click **Add**.

     Note

     You can click **Display Terminals Not Grouped** to display the speaker unit(s) that are not grouped.
   - Check **Area**, select one or more speaker units from the Available list, and add them to the Selected list.
6. Configure the period type.
   - When selecting **Every Day**, you should set the start date and end date.
   - When selecting **Every Week**, you should set the start date, end date, and the repetition day(s) of the week.
7. Configure the playing time.

1) Click **Add**.
2) Set the broadcast time as needed.
3) Set **Once** or **Specified Duration** as the play mode.
4) Click **Add** to finish adding.

8. Select the broadcast priority from the drop-down list.

Note

Broadcast priority ranges from 0 to 15. The larger the number, the higher the priority.

9. Click **Add** to add the audio file(s) from the media library.

Note

- For the added audio files, you can click ↑ or ↓ to adjust their playing sequences; click to delete an audio file.
- For details about adding media files, refer to ***Manage Media Files*** .

10. Click **Add** to save the above settings.

A prompt of selecting the applying method pops up.

11. Apply the task.
    - Click **Apply Now** to apply the task immediately.
    - Click **Apply Later** to apply the task later.
12. **Optional:** Perform the following operations.

View Details
View the details of the added scheduled broadcast task, including the broadcast time, start date and end date, period type, the number of speaker units, etc.

Note

You can click › to view more details.

Play/Stop Audio
- Click **Play** to play the audio of a corresponding scheduled broadcast task.
- Click **Stop** to stop playing the audio.

Apply
- Click **Apply All** to apply all the tasks to the speaker units.
- Select the tasks to be applied, click **Apply All** to apply the selected tasks to the speaker units.

Note

You can view the application process and the results. For the applying failed tasks, you can view the failure reasons.

Search
Enter keywords in the search box in the upper-right corner, and click to search for the target task(s).

Delete
Check one or more tasks, click **Delete** to delete the selected tasks.

34.7 Add a Linked Broadcast Task

You can configure the parameters such as the broadcast content and play mode to add a linked broadcast task in the platform and then apply the task to the speaker unit(s). After that, the broadcast content will be played when the emergency is triggered in the selected areas. For the added linked broadcast task(s), you can view the task details, search for target task(s), etc.

Before You Start

- Make sure you have grouped speaker units. Refer to ***Group Speaker Units*** for details.
- Make sure you have added speaker unit(s) to area(s).

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Linked Broadcast**.
3. Click **Add** to enter Add Broadcast Linkage page.
4. Enter the name for the linked broadcast task.
5. Select a broadcast area.
6. Select the speaker unit(s) to execute the task.
7. Select the broadcast content.
   - Check **Audio File**, and click **Add** to add the audio file(s) from the media library.

     Note

     - For the added audio files, you can click ↑ or ↓ to adjust their playing sequences; click to delete an audio file.
     - For details about adding media files, refer to ***Manage Media Files*** .
   - Check **Custom Broadcast Content**, and enter the broadcast content as needed.
8. Add an audio file as needed.
9. Select the play mode.

   Once

   The linked broadcast will only be played once.

   Specific Duration

   The linked broadcast will be played for the configured duration.

   Broadcast Until Recovery

   The linked broadcast will be played continuously until the status of emergency is recovered.
10. Click **Save and Apply**.

    You can view the applying progress and the result.
11. **Optional:** Perform the following operations.

Edit a Task	Click the broadcast name to edit its parameters as needed.

View Emergency Mustering Configuration	Click **View Emergency Mustering Configuration** to enter Emergency Mustering module and view the emergency mustering configuration.
View Applying Failed Task(s)	indicates that the broadcast task(s) are failed to be applied. • Move the mouse cursor to beside the broadcast name, and click **View Details** to view the failure details of the current task. • Move the mouse cursor to beside **Apply All**, and click **View Details** to view the failure details of all the tasks.
Apply Task Again	When there are task(s) that failed to be applied, you can apply the task(s) to the speaker units again. • Move the mouse cursor to beside the broadcast name, and click **Try Again** to apply the current task again. • Move the mouse cursor to beside **Apply All**, and click **Try Again** to apply all the tasks again. **Note** During the applying process,you can view the application process and the results. For the applying failed tasks, you can view the failure reasons.
Start/Stop Playing Broadcast Content	Click **Play/Stop** to start/stop playing the broadcast content of a task.
Search for Task(s)	Enter keywords in the search box in the upper-right corner, and click to search for the target task(s).
Delete a Task	Click **Delete** to delete a linked broadcast task. **Note** If a linked broadcast is taking effect as the emergency is triggered in the selected areas, it cannot be deleted.

See Far, Go Further

UD38379B