HikCentral Professional Web Client

User Manual

Legal Information

About this Manual

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

Trademarks

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

Disclaimer

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

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

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

Symbol Conventions

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

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

Contents

Chapter 1 About Web Client

1.1 About This Document

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

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

1.2 Introduction

The platform is developed for the management of surveillance 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, alarm linkage, access control, time and attendance, face comparison, 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 surveillance 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.

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 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. For setting the time period, refer to ***System Security Settings*** .

2.1 Recommended Running Environment

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

CPU

Intel® Core™ I3 and above

Memory

4 GB and above

Web Browser

Internet Explorer® 11 and above, Firefox® 84 and above, Google Chrome® 84 and above, Safari® 11 and above， Microsoft® Edge 89 and above.

Note

You should run the web browser as the administrator.

2.2 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.

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

2. Enter the password and confirm password for the admin user in the pop-up Create Password window.

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 ***System Security Settings*** .

Caution

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

3. Click **OK**.

   Web Client home page displays after you successfully creating the admin password.

Result

After you logging 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.

2.2.2 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. For setting minimum password strength, refer to ***System Security Settings*** .

   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.

2.3 Login via Web Client

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. Enter the user name and password.
3. 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. For setting failed login attempts and locking duration, refer to ***System Security Settings*** .
   - 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.
   - 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. For setting minimum password strength, refer to ***System Security Settings*** .
   - If your password is expired, you will be asked to change your password when login. For setting maximum password age, refer to ***System Security Settings*** .

Result

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

2.4 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. For setting minimum password strength, refer to ***System Security Settings*** .

   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.

2.5 Forgot Password

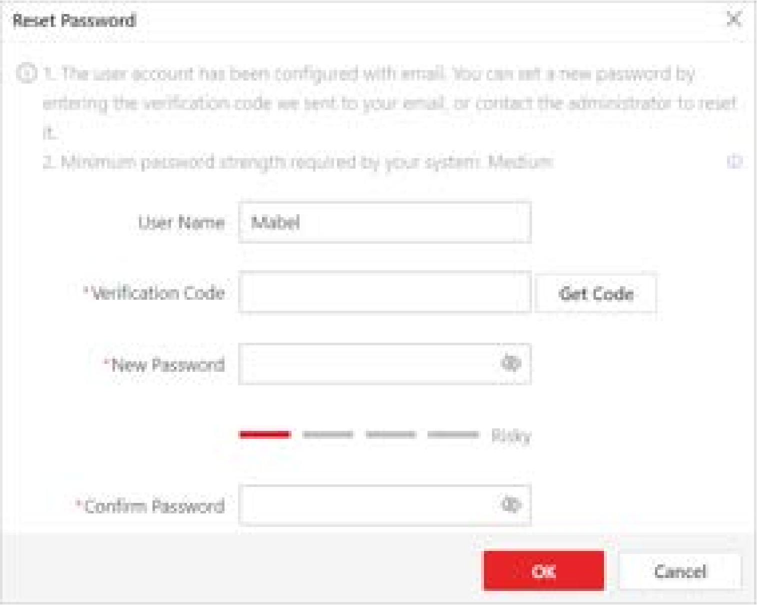
If you forgot the your account's password, you can reset the password and set a new password.

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, enter a user name in the User Name field.
2. Click **Forgot Password**.

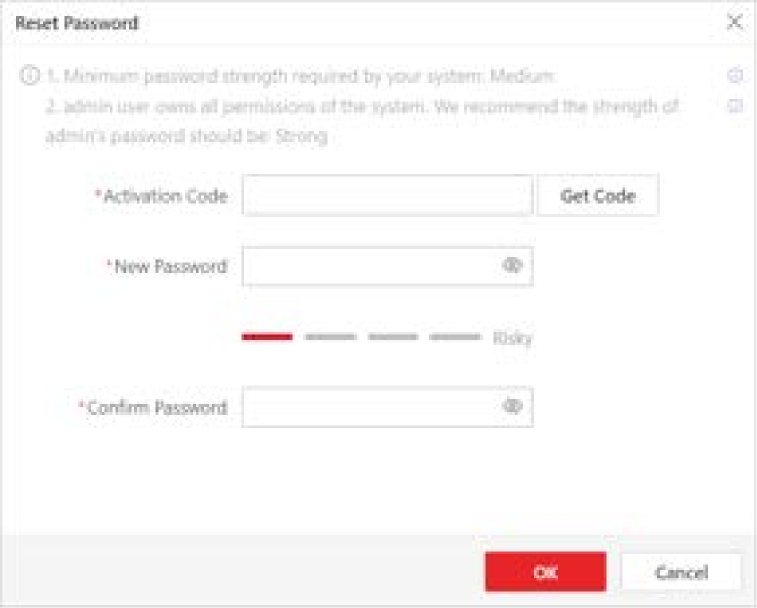


Reset Password

1. The user account has been configured with email. You can set a new password by entering the verification code we sent to your email, or contact the administrator to reset it.
2. Minimum password strength required by your system: Medium

User Name: Mabel

Figure 2-1 Reset Password for Normal User



Reset Password

1. Minimum password strength required by your system: Medium
2. admin user owns all permissions of the system. We recommend the strength of admin's password should be: Strong

Figure 2-2 Reset Password for admin User

3. Enter the required information on the Reset Password pane.
   - For the admin user, enter the License activation code, new password, and confirm password.

Note

If you forget the License activation code, you can click **Get Code** to send the activation code to the email address configured when activating the License in online mode. For setting an email for the admin user, refer to ***Activate License - Online*** .

- For normal users, click **Get Code** to send the verification code to the email address configured when adding the user. And then enter the received verification code, new password, and confirm password within 10 minutes.

  Note

  If the email address is not set for the normal user, contact the admin user to reset the password and change the password when login.

- For domain user, contact the admin user to reset 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. For setting minimum password strength, refer to ***System Security Settings*** .

⚠ **Caution**

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

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

4. Click **OK**.

Chapter 3 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.

Chapter 4 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, e.g., live view, playback, and searching online devices. 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.

Chapter 5 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 in the top of the Web Client, you can click tabs to quickly switch modules. You can also click ⟳ or ✕ in the tab area to refresh or exit from the module.

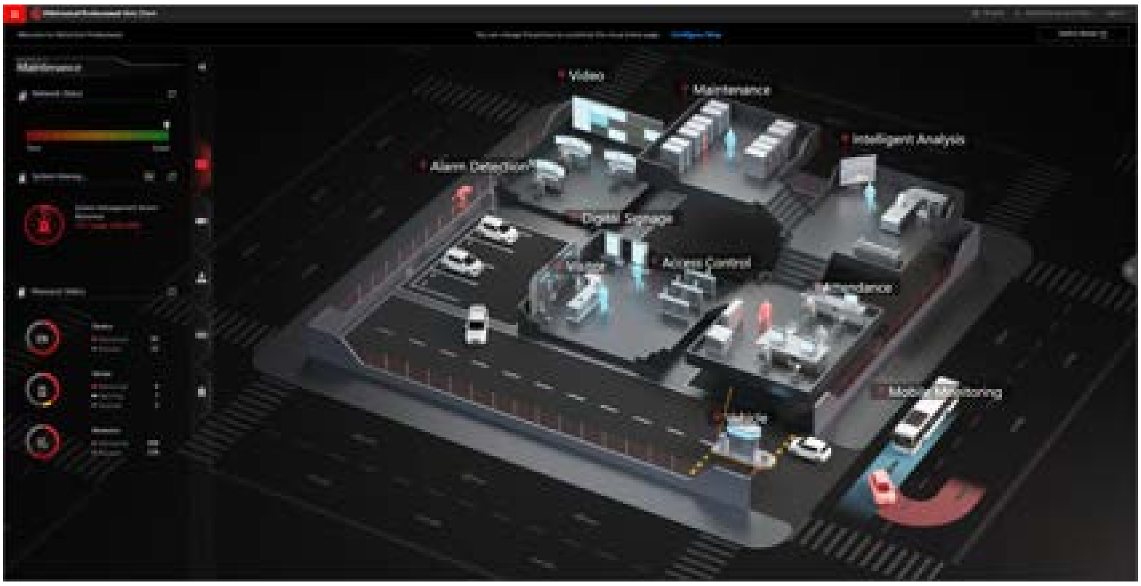


Figure 5-1 Default Home Page

Table 5-1 Default 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*** .
	Wizard	**Video** A wizard which guides you through the management and applications of video. You can also view the flow

Section	Module	Description
		chart which introduces the video resource management, recording configurations, and video application in ***Flow Chart of Video Management*** . **Access Control** A wizard which guides you through the basic configurations of access control. You can also view the flow chart which introduces the configurations and operations of access control and elevator control in ***Flow Chart*** . **Mobile Monitoring** A wizard which guides you through the configuration and applications of mobile monitoring. You can also view the flow chart which introduces the management of mobile devices and vehicles, the configuration of GIS map and driving rules, driving monitoring, vehicle route and driving event search, and the report management in ***Mobile Monitoring*** . **Vehicle and Parking** A wizard which guides you through the management and applications of vehicle and parking. You can also view the flow chart which introduces the management of parking lots, vehicles, and entry & exit rules, parking fee rules, parking guidance, and vehicle & record search in ***Flow Chart of Vehicle and Parking Management*** . **Alarm Detection** A wizard which guides you through the management and configurations of alarm detection. You can also view the flow chart which introduces the management of security control panels and alarm inputs, defense template configuration, and event & alarm management in ***Flow Chart of Alarm Detection*** . **Digital Signage** A wizard which guides you through the management and configurations of digital signage. You can also view the flow chart which introduces the management of digital signage terminals, materials, programs, and

Section	Module	Description
		schedules, program approval, and program release in ***Flow Chart*** . **Attendance** A wizard which guides you through the management and configurations of attendance. You can also view the flow chart which introduces the management of devices, person groups, and persons, basic attendance configuration, attendance rule configuration, and record search and handling in ***Flow Chart*** .
	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. 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 File*** . **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.
	Account	**Change Password** Change the password of the current user.

Section	Module	Description
		For more details, refer to ***Change Password of Current User*** . **Logout** Log out of the system and back to the login page.
Default Home Page	Switch to Map Configuration	Configure a map for displaying resources on the map. For more information, refer to ***Map Management*** .
	Switch Home Page Mode	Four predefined modes are provided, including Default Mode, System Installation and Management Mode, Security Control and Management Mode, and Attendance Management Mode, for different scenarios. You can also customize the Home page mode as needed. See more details in ***Customize and Switch Home Page Mode*** .
	Left Overview Pane	**Maintenance** The Maintenance module provides the overview of device network status, service running status, and health checking results. You can refresh to view the real-time status or results. See more details in ***Maintenance*** . **Intelligent Analysis** The Intelligent Analysis module provides the report overview of people feature analysis, people counting, and heat analysis. You can refresh to view the real-time analysis results, or export them in different formats. See more details in ***Intelligent Analysis Report*** . **Access Control** The Access Control module provides today's access record statistics, today's access trend, today's top 5 abnormal record types, and regional counting statistics of people stayed. You can refresh to view the real-time trend, top 5 types, and statistics, or export them in different formats. See more details in ***Access and Elevator Control Management*** .

Section	Module	Description
		Vehicle The Vehicle module provides the real-time status of parking spaces, today's occupancy rate of parking spaces, today's parking duration distributions, and today's vehicle passing trend. You can refresh to view the real-time information and export it in different formats. See more details in ***Vehicle and Parking Management*** . **Alarm** The Alarm module provides today's alarm statistics, the last 7 days' alarm trend, today's top 5 alarm categories, and today's top 5 alarm areas. You can refresh to view the trend, top 5 categories, and top 5 alarm areas, or export them in different formats. See more details in ***Event and Alarm Configuration*** .
	Quickly Access to Modules	On the scene graph of the default Home page, you can click the module names to quickly go to the corresponding configuration and management page.

5.1 Customize and Switch Home Page Mode

You can switch to the default Home page mode to three predefined modes (that are, System Installation and Management, Security Control Management, and Attendance Management) for different scenarios or customize a mode as needed.

Steps

1. In the top right corner of Home page, click **Switch Mode** to enter the mode switch page.

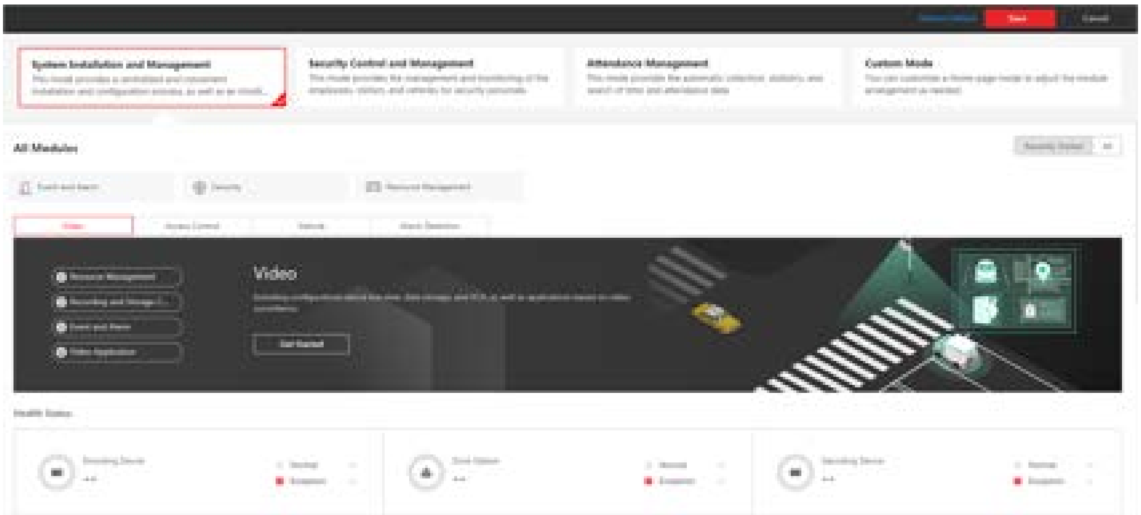

System Installation and Management
Security Control and Management
Attendance Management
Custom Mode
All Modules
Video
Health Status

Figure 5-2 Customize and Switch Home Page Mode

2. **Optional:** In the **All Modules** field, click **Recently Visited** or **All** to show and quickly access to the recently visited modules or all available modules.

Note

The displayed modules in the **Recently Visited** tab will keep refreshing according to the modules visited by the current user.

3. **Optional:** Customize a mode.
   1) In the top right corner, click **Custom Mode** to display mode configuration panel.
   2) In the module name field, click + to add module(s) to the mode.

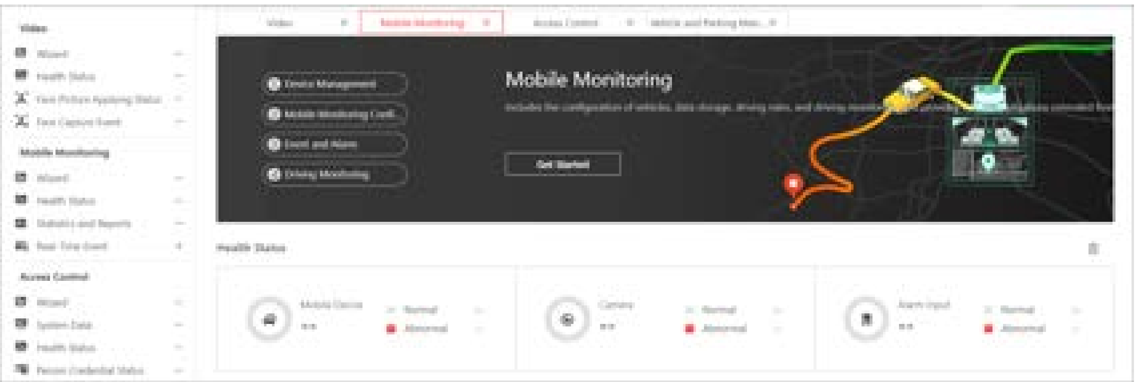


Figure 5-3 Customize Home Page Mode

   The added module(s) are displayed under the **All Modules** field.
   3) **Optional:** Click 🗑 or ✕ to remove the module(s) or section(s) from the mode.
4. At the top of the page, click a predefined or custom mode to switch the Home page mode.

   The modules contained in the mode are displayed under the **All Modules** field. You can click the tabs to switch the detailed and visual views of different modules.

5. **Optional:** In the top right corner of mode switching page, click **Cancel** to cancel setting mode.
6. **Optional:** In the top right corner of mode switching page, click **Restore Default** to switch to the default mode.
7. In the top right corner of mode switching page, click **Save** to save the mode settings.

5.2 Customize Navigation Bar

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

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** to display the navigation bar and the All Modules pane.

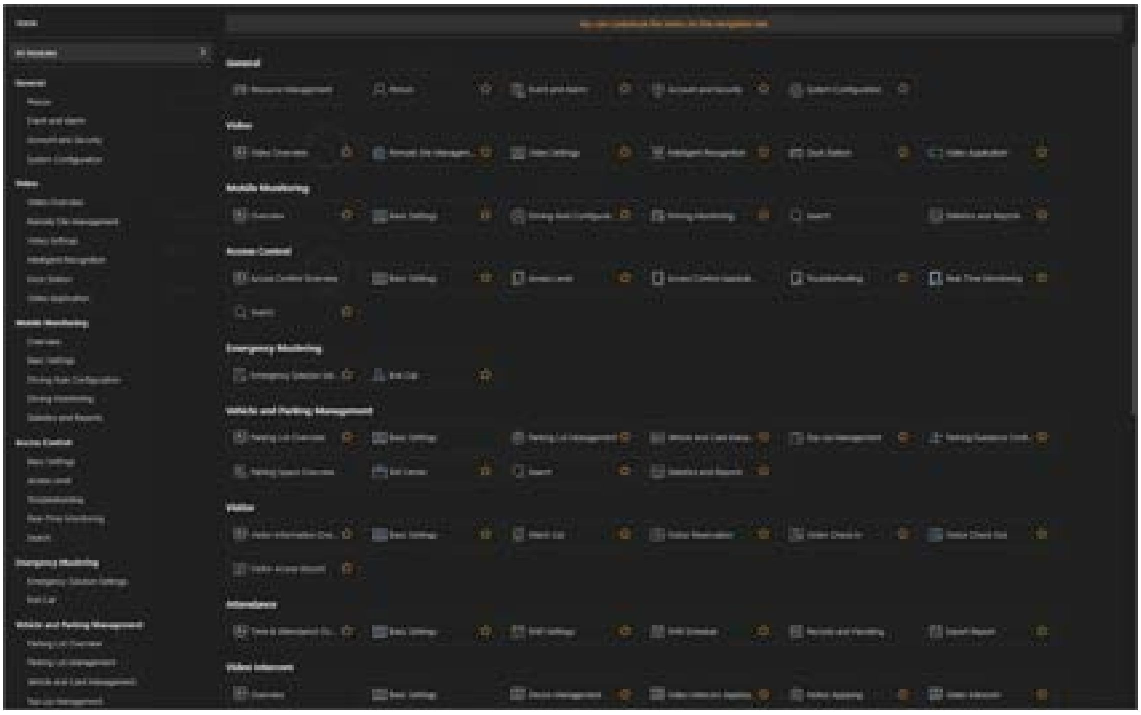


Figure 5-4 Navigation Bar and All Modules Panel

2. On the All Modules panel, move the cursor to a module item.

   An icon ☆ appears beside the module name.
3. Click ☆ to add the selected module to the navigation bar.

   The icon ☆ of the corresponding module turns to ★ .
4. **Optional:** Click ★ to remove the module from the navigation bar.

Chapter 6 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 (encoding devices, access control devices, recording server, and so on) 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*** .

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 ***Resource 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 ***Configure Storage and Recording*** .

Configure Event and Alarm

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

Configure Users

Specify who should be able to access the platform, and how. You can set different permissions for the users to limit their operations. Refer to ***Role and User Management*** .

Chapter 7 License Management

After installing HikCentral Professional, you have a temporary License for a specified number of cameras 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 (e.g., connect more cameras), you can purchase an expanded License to get additional features.

Note

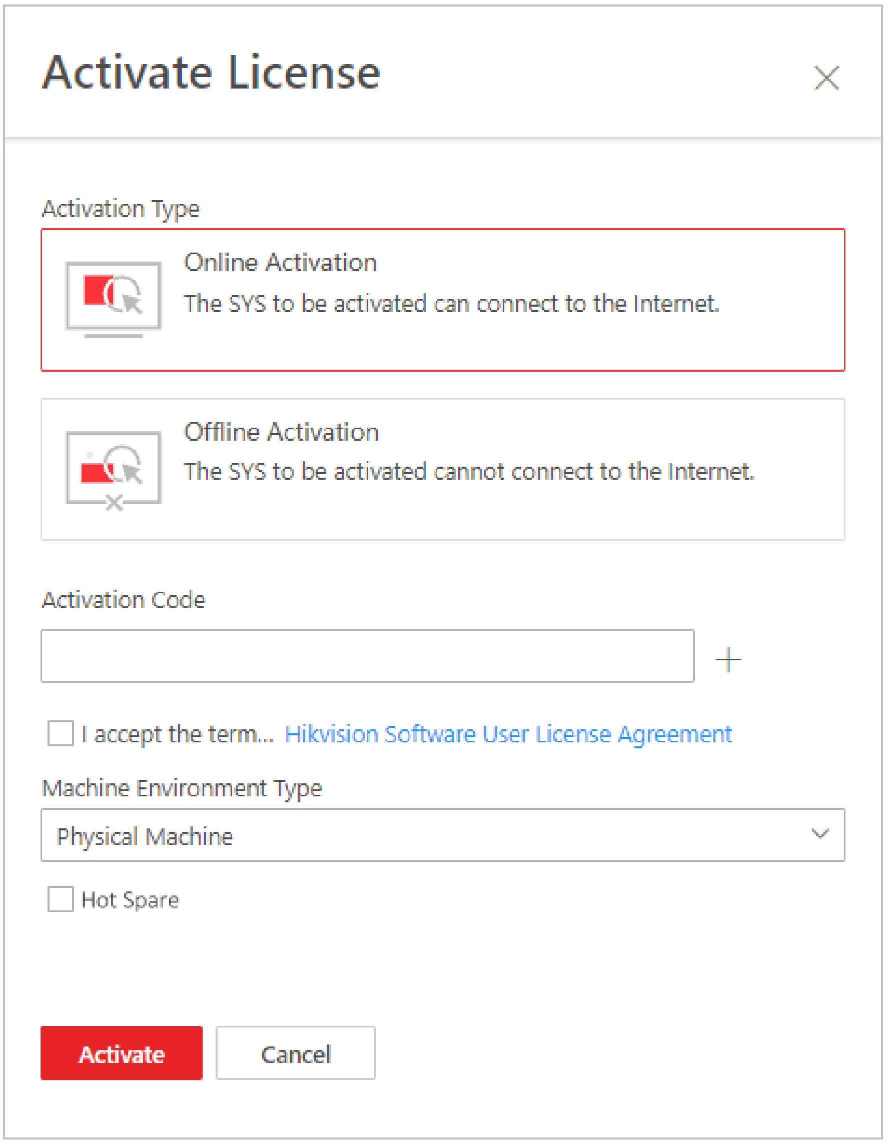
- Only the admin user can perform the activation, update, and deactivation operation.
- If you encounter any problems during activation, update, and deactivation, please send the server logs to our technical support engineers.

7.1 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*** .
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Online Activation** to activate the License in online mode.



Activate License

Activation Type

Online Activation
The SYS to be activated can connect to the Internet.

Offline Activation
The SYS to be activated cannot connect to the Internet.

Activation Code

□ I accept the term... Hikvision Software User License Agreement

Machine Environment Type

Physical Machine

□ Hot Spare

Figure 7-1 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 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 **Activate**.

   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.

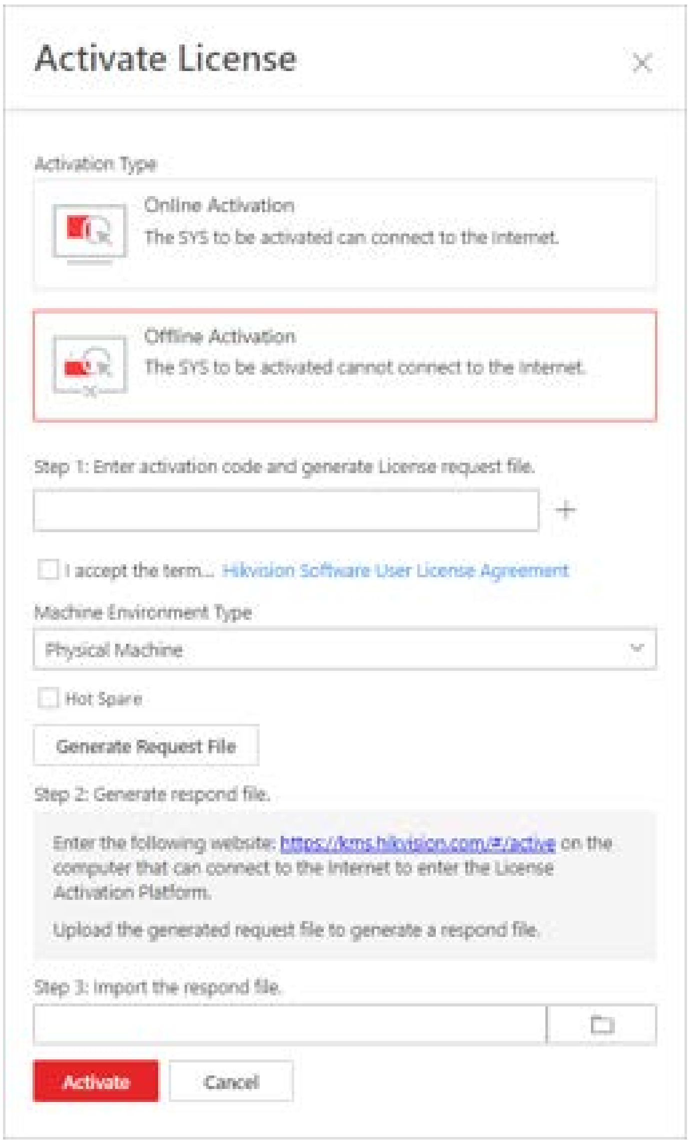
10. Set the email server parameters. See details in ***Configure Email Account*** .
11. Click **OK** to save the email settings.

7.2 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.



Activate License

Activation Type

Online Activation

The SYS to be activated can connect to the Internet.

Offline Activation

The SYS to be activated cannot connect to the Internet.

Step 1: Enter activation code and generate License request file.

□ I accept the term... Hikvision Software User License Agreement

Machine Environment Type

Physical Machine

□ Hot Spare

Generate Request File

Step 2: Generate respond file.

Enter the following website: https://kms.hikvision.com/#/active on the computer that can connect to the Internet to enter the License Activation Platform.

Upload the generated request file to generate a respond file.

Step 3: Import the respond file.

Activate Cancel

Figure 7-2 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.

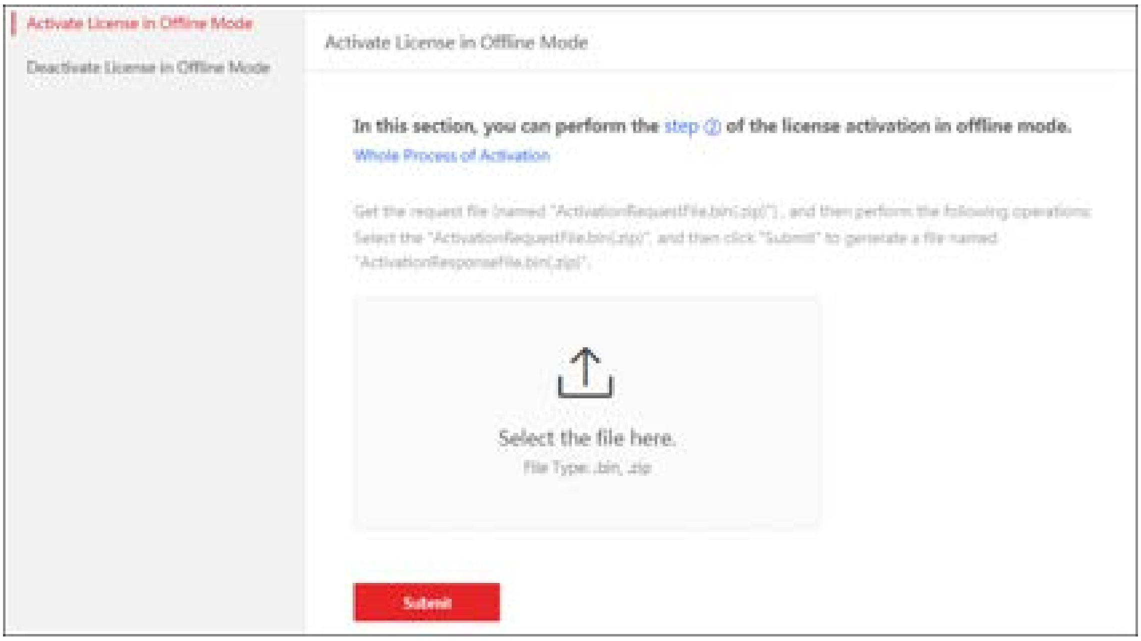
7. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

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.



Activate License in Offline Mode
Deactivate License in Offline Mode
Activate License in Offline Mode

In this section, you can perform the step ② of the license activation in offline mode.

Whole Process of Activation

Get the request file (named "ActivationRequestFile.bin(.zip)") , and then perform the following operations: Select the "ActivationRequestFile.bin(.zip)", and then click "Submit" to generate a file named "ActivationResponseFile.bin(.zip)".

Select the file here.
File Type: .bin, .zip
Submit

Figure 7-3 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.

7.3 Update License - Online

As your project grows, you may need to increase the connectable number of resources (e.g., cameras) 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. Refer to ***Login via Web Client*** for details.
2. In the top right corner of Home page, move the cursor to the **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License panel.
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 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 **Update**.

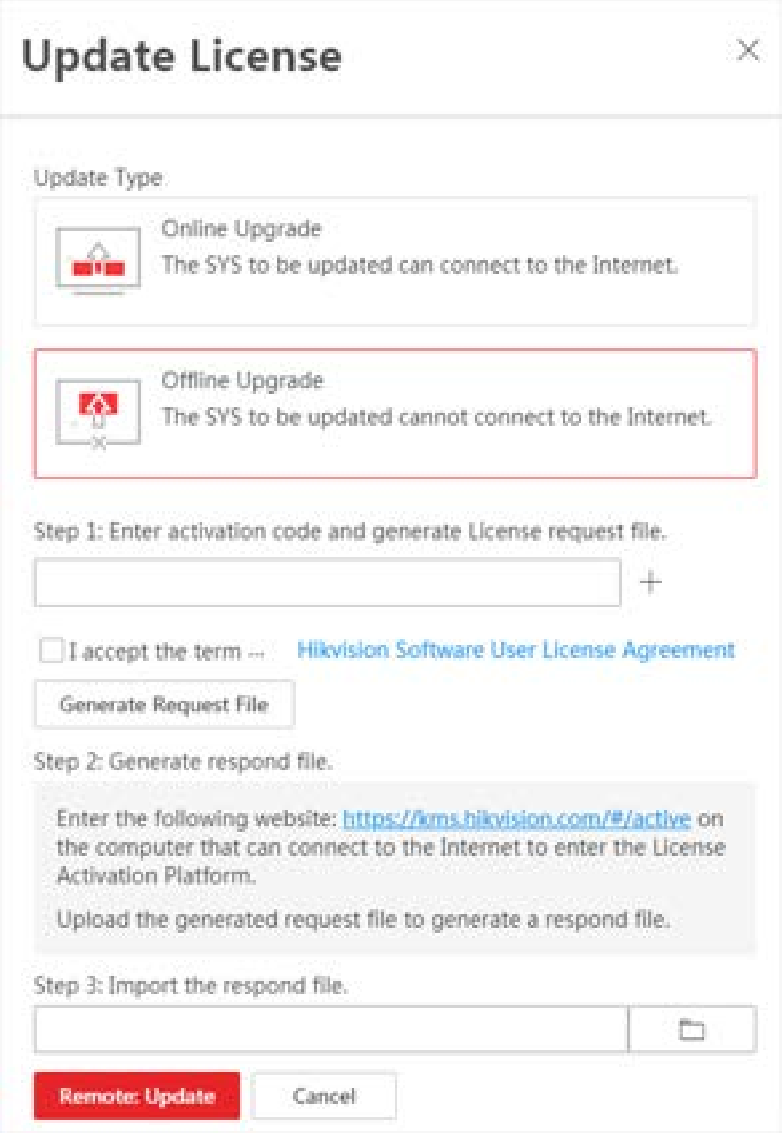
7.4 Update License - Offline

As your project grows, you may need to increase the connectable number of cameras 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. In the top right corner of Home page, 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.



Update License

Update Type

Online Upgrade
The SYS to be updated can connect to the Internet.

Offline Upgrade
The SYS to be updated cannot connect to the Internet.

Step 1: Enter activation code and generate License request file.

□ I accept the term ... Hikvision Software User License Agreement

Generate Request File

Step 2: Generate respond file.

Enter the following website: https://kms.hikvision.com/#/active on the computer that can connect to the Internet to enter the License Activation Platform.

Upload the generated request file to generate a respond file.

Step 3: Import the respond file.

Remote: Update | Cancel

Figure 7-4 Update License in Offline Mode

5. Enter the activation code of your additional License.

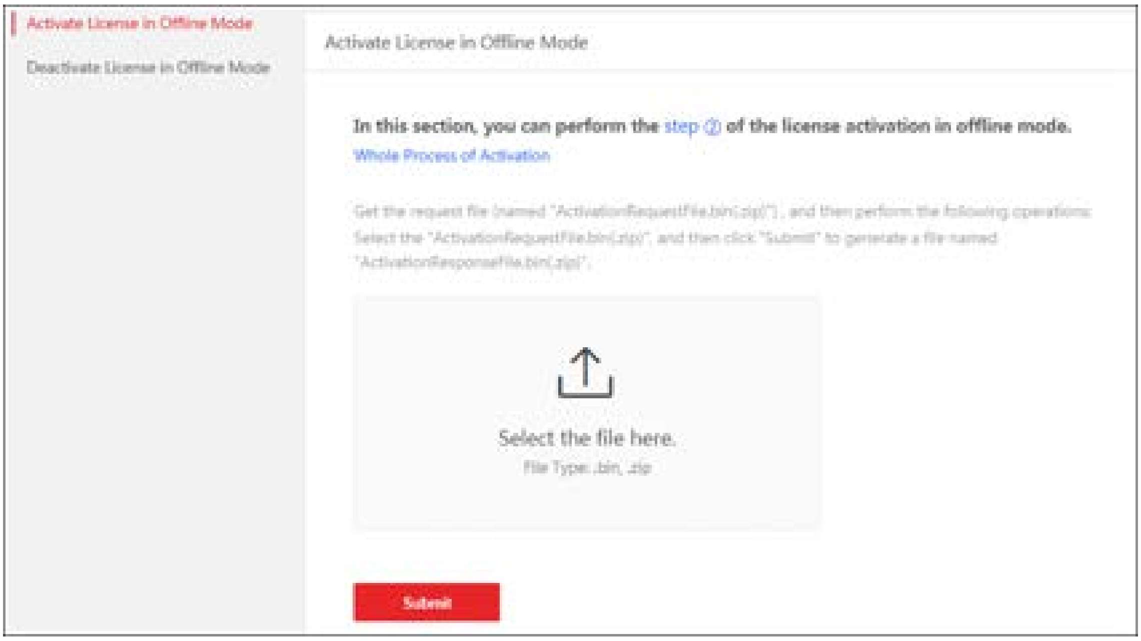
Note

- 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.


Activate License in Offline Mode
Deactivate License in Offline Mode
Activate License in Offline Mode
Whole Process of Activation
Select the file here.
File Type: .bin, .zip
Submit

In this section, you can perform the step ② of the license activation in offline mode.

Get the request file (named "ActivationRequestFile.bin(.zip)") , and then perform the following operations: Select the "ActivationRequestFile.bin(.zip)", and then click "Submit" to generate a file named "ActivationResponseFile.bin(.zip)".

Figure 7-5 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**.

7.5 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. Refer to ***Login via Web Client*** .
2. In the top right corner of Home page, move the cursor to the **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.

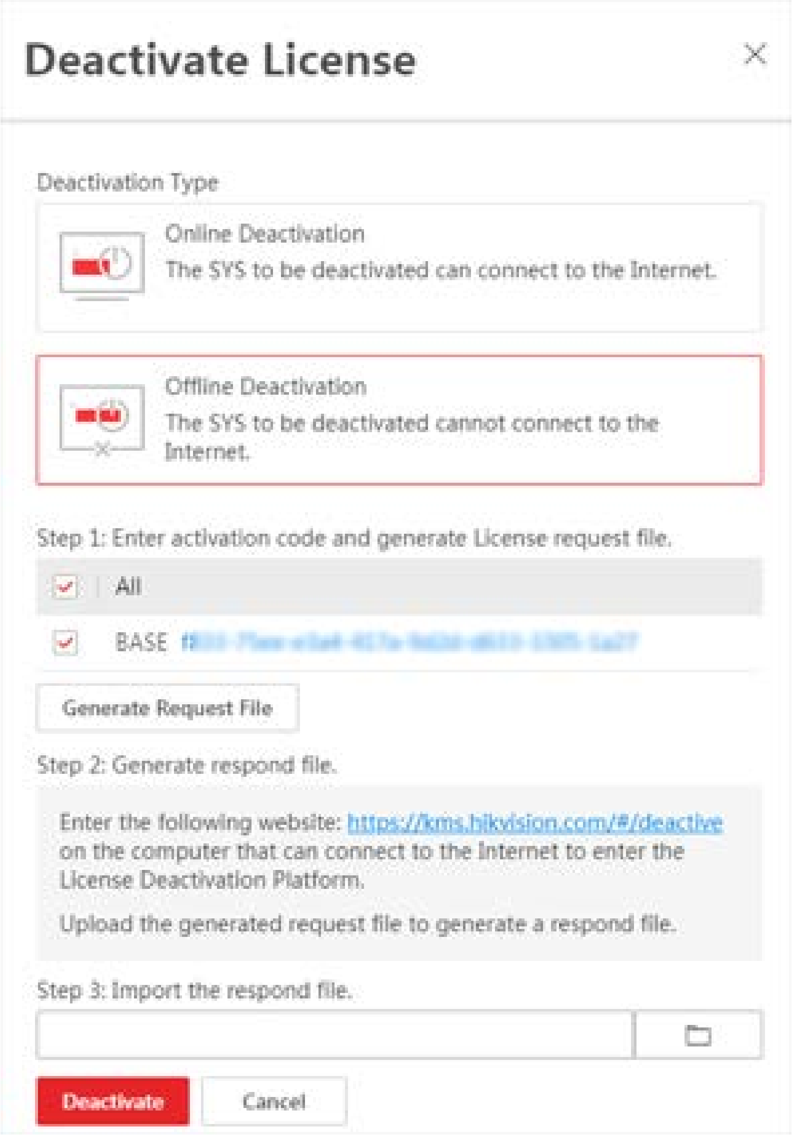
6. Click **Deactivate**.

7.6 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. In the top right corner of the Client, move the cursor to the **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.



Deactivate License

Deactivation Type

Online Deactivation
The SYS to be deactivated can connect to the Internet.

Offline Deactivation
The SYS to be deactivated cannot connect to the Internet.

Step 1: Enter activation code and generate License request file.

☑ All

☑ BASE [redacted]

Generate Request File

Step 2: Generate respond file.

Enter the following website: https://kms.hikvision.com/#/deactive on the computer that can connect to the Internet to enter the License Deactivation Platform.

Upload the generated request file to generate a respond file.

Step 3: Import the respond file.

Deactivate Cancel

Figure 7-6 Deactivate License in Offline Mode

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

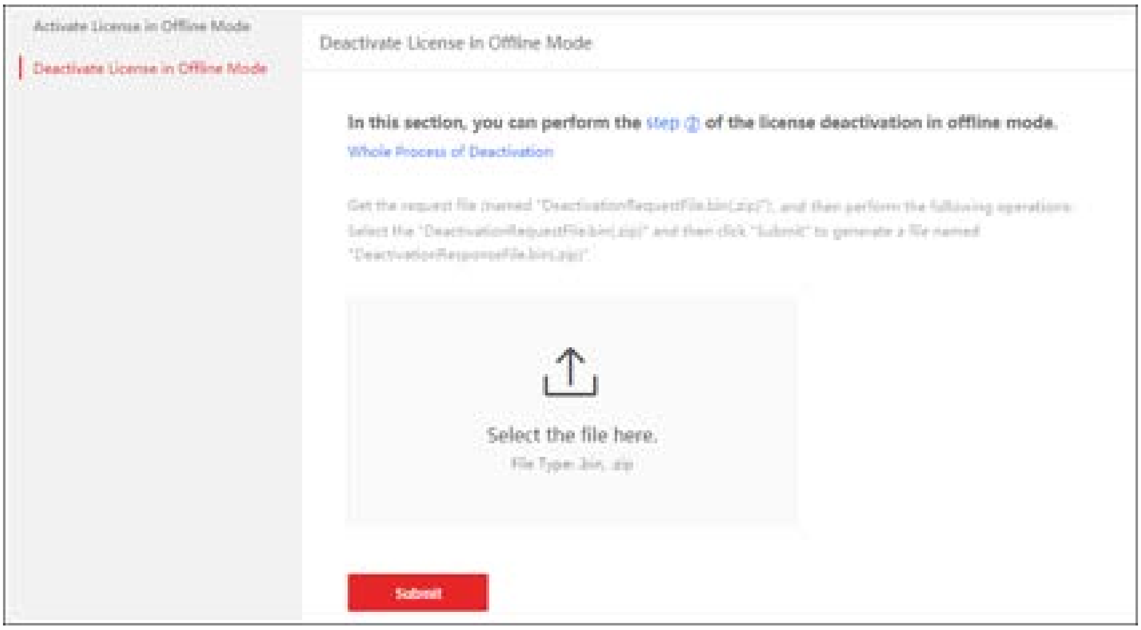
Note

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.


Activate License in Offline Mode
Deactivate License in Offline Mode
Deactivate License in Offline Mode
Whole Process of Deactivation
Select the file here.
File Type: .bin, .zip
Submit

In this section, you can perform the step ② of the license deactivation in offline mode.

Get the request file (named "DeactivationRequestFile.bin(.zip)"), and then perform the following operations: Select the "DeactivationRequestFile.bin(.zip)" and then click "Submit" to generate a file named "DeactivationResponseFile.bin(.zip)".

Figure 7-7 Select Request File

10. Click **Submit**.

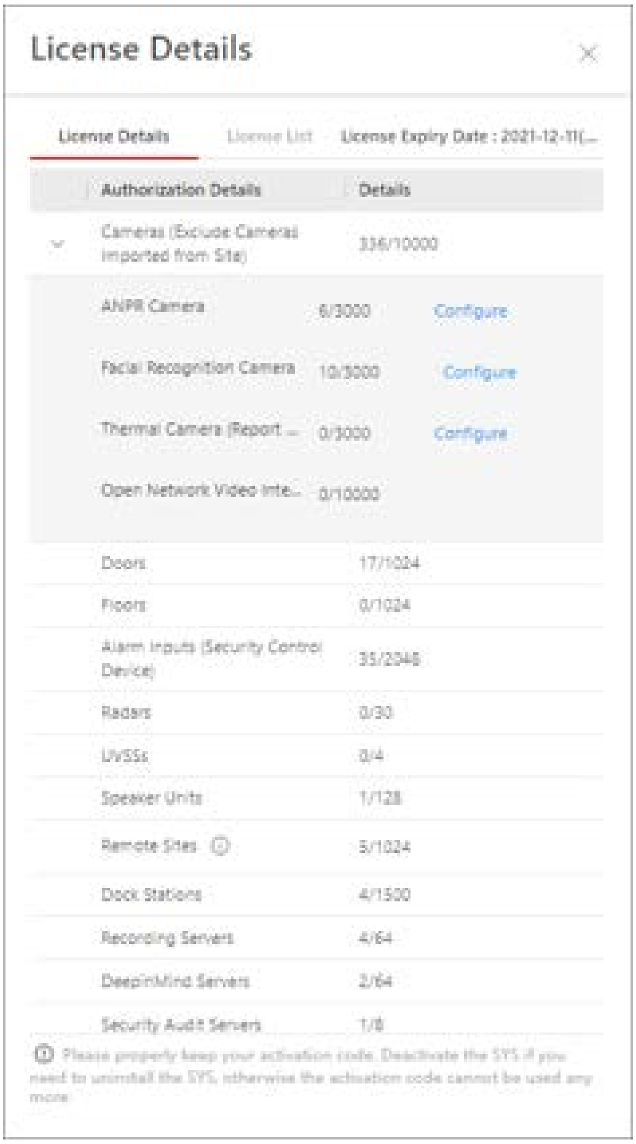
    A respond file named "DectivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
12.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

7.7 View License Details

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

Steps

1. Log in to the HikCentral Professional via Web Client. See ***Login via Web Client*** for details.
2. In the top right corner of Home page, click **Maintenance and Management** to show the drop-down menu.
3. Click **License Details** in the drop-down menu to open the License Details panel.



License Details

License Details | License List | License Expiry Date : 2021-12-11(...

Authorization Details	Details	
Cameras (Exclude Cameras Imported from Site)	336/10000	
ANPR Camera	6/3000	Configure
Facial Recognition Camera	10/3000	Configure
Thermal Camera (Report ...	0/3000	Configure
Open Network Video Inte...	0/10000	
Doors	17/1024	
Floors	0/1024	
Alarm Inputs (Security Control Device)	35/2048	
Radars	0/30	
UVSSs	0/4	
Speaker Units	1/128	
Remote Sites	5/1024	
Dock Stations	4/1500	
Recording Servers	4/64	
DeepinMind Servers	2/64	
Security Audit Servers	1/8	

Please properly keep your activation code. Deactivate the SYS if you need to uninstall the SYS, otherwise the activation code cannot be used any more.

Figure 7-8 License Details Page

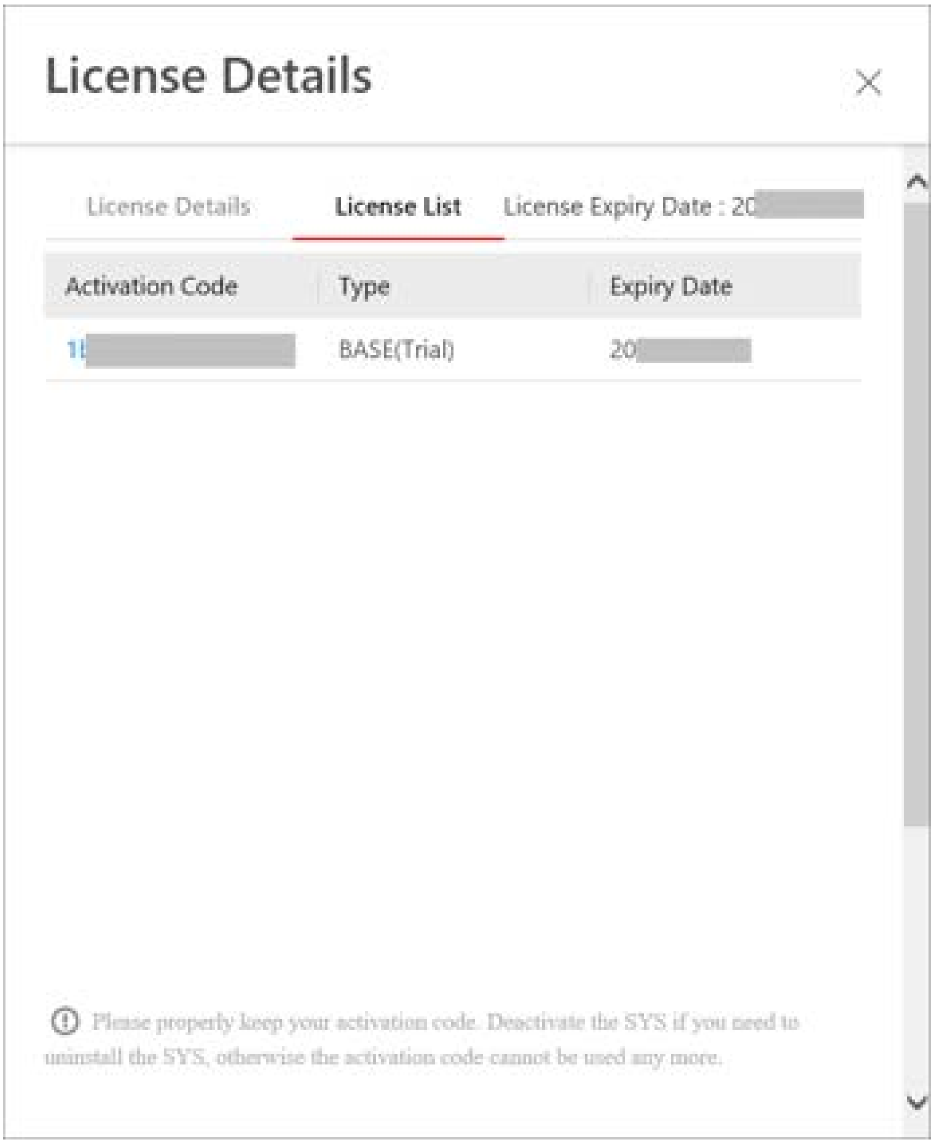
You can view the authorization details and check the expiry date of the trial License or the License you purchased.

4. **Optional:** Click › besides the Cameras(Exclude Cameras Imported from Site) to show the number of facial recognition cameras/ANPR cameras/thermal cameras (report supported)/Open Network Video Interface cameras and click **Configuration** to select the added cameras as these types of cameras, respectively.

Note

- Configuration of Open Network Video Interface cameras is not supported.
- If you do not configure the facial recognition camera/ANPR camera/thermal camera, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the platform.

5. **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.



License Details

License Details | **License List** | License Expiry Date : 20[redacted]

Activation Code	Type	Expiry Date
1[redacted]	BASE(Trial)	20[redacted]

Please properly keep your activation code. Deactivate the SYS if you need to uninstall the SYS, otherwise the activation code cannot be used any more.

Figure 7-9 License List Page

7.8 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. In the top right corner of the client, select **Maintenance and Management → License Details** to open the License Details panel.
2. Go to the bottom of details list and click ⚙ to enter the SSP Expiration Prompt Settings panel.
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 8 Resource Management

HikCentral Professional supports multiple resource types, such as encoding device, access control device, Remote Site, decoding device and Smart Wall. After adding them to the system, you can manage them, configure required settings and perform further operations. For example, you can add encoding devices for live view, playback, recording settings, event configuration, etc., add access control devices for access control, time and attendance management, etc., add Remote Site for central management of multiple systems, add Recording Server for storing the videos, add Streaming Server for getting the video data stream from the server, and add Smart Wall for displaying decoded video on smart wall.

8.1 Create Password for Inactive Device(s)

Because of simple default password, the devices may be accessed by the unauthorized user easily. For more security purpose, the default password is not provided for some devices. You are required to create the password to activate them before adding them and performing some operations on them via the platform. Besides activating the device one by one, you can also deal with multiple ones at the same time. The devices which are batch activated should have the same password.

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.

Perform this task when you need to activate the detected online devices. Here we take creating password for the encoding device as an example.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules → General → Resource Management** .
2. Click **Device and Server → Encoding Device** on the left.
3. View the device status (shown on Security column) and select one or multiple inactive devices.
4. Click 💡 to open the Device Activation window.
5. 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 installer and/or end-user.

6. Click **Save** to create the password for the device.

   An **Operation completed.** message is displayed when the password is set successfully.
7. Click in the Operation column to change the device's IP address, subnet mask, gateway, etc., if needed.

   Note

   For details, refer to ***Edit Online Device's Network Information*** .

8.2 Edit Online Device's Network Information

The online devices, which have IP addresses in the same local subnet with SYS server 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. Here we take creating password for the encoding device as an example.

Steps

1. In the top left corner of Home page, select → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. 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 be listed.

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
4. View the device status on Security column, and click in the Operation column of an active device.
5. Change the required parameters, such as IP address, device port, HTTP port, subnet mask, and gateway.

   Note

   The parameters may vary for different device types.

6. Click ✓ .
7. Enter device's password.
8. Click **Save**.

8.3 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,

8.3.1 Add Detected Online Encoding Devices

The system can perform an automated detection for available encoding devices 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.

Note

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

Add a Detected Online Encoding Device

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

Before You Start

- Make sure the devices (cameras, DVRs, etc.) 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. Refer to ***Create Password for Inactive Device(s)*** for details.

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
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 Web Client will be listed in the Online Device area.

4. In the Online Device area, select **Hikvision Private Protocol**/ **Hikvision ISUP Protocol**/**Open Network Video Interface Protocol** to filter the detected online devices.

Note

- Select **Hikvision Private Protocol**/**Hikvision ISUP Protocol** to add a Hikvision device and select **Open Network Video Interface Protocol** to add a third-party device.
- To display the devices which are added to the platform via Open Network Video Interface/ ISUP protocol, you can go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and check **Access via Open Network Video Interface Protocol**/**Allow ISUP Registration**.

5. In the Online Device area, select the active device to be added.
6. Click **Add to Device List** to open the Add Online Device window.

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. See ***Set NTP*** for details.

7. 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 8000.

Mapped Port

This function is only available when you select **Hikvision Private Protocol** to filter the detected online devices. If you want to download pictures from the device, switch on **Mapped Port** and enter the picture downloading port. By default, the port number is 80.

Verify Stream Encryption Key

Switch on **Verify Stream Encryption Key**, and enter stream encryption key in **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored in SYS server for security purpose.

Note

This function should be supported by the devices. Refer to the user manual of the device for getting the key.

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 installer and/or end-user.

8. **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.
9. **Optional:** Switch on **Add Resource to Area** to import the channels of the added devices to an area.

   Note

   - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import channels to area, you cannot perform operations such as live view, playback, event settings, etc., for the cameras.
10. **Optional:** Select a Streaming Server to get the video stream of the channels via the server.

    Note

    - The camera(s) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it.
    - You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting 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.

    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.

    Cloud Storage Server

    The video files will be stored in the Cloud 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.

    Note

    - For adding the encoding device by domain name, the video files can only be stored in the local storage of the device.
    - Configure the Hybrid Storage Area Network, Cloud Storage Server or pStor in advance, or its storage location cannot display in the drop-down list. You can click **Add New** to add a new Hybrid Storage Area Network, Cloud Storage Server or pStor.

12. **Optional:** Set the quick recording schedule for added channels.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type, etc. Refer to ***Configure Recording for Cameras on Current Site*** for details.
13. Click **Add**.
14. **Optional:** Perform the following operations after adding the online device.

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.

Replace Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

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.

What to do next

For facial recognition cameras/ANPR cameras/thermal cameras (report supported), click **Maintenance and Management → License Details → → Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally on the platform.

Add Detected Online Encoding Devices 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 (cameras, DVRs, etc.) 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. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
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 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.
4. In the Online Device area, select **Hikvision Private Protocol**/ **Hikvision ISUP Protocol**/**Open Network Video Interface Protocol** to filter the detected online devices.

   Note

   - Select **Hikvision Private Protocol**/**Hikvision ISUP Protocol** to add a Hikvision device and select **Open Network Video Interface Protocol** to add a third-party device.
   - To display the devices which are added to the platform via Open Network Video Interface/ ISUP protocol, you can go to ▦ → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and check **Access via Open Network Video Interface Protocol**/**Allow ISUP Registration**.
5. In the Online Device area, select the active devices to be added.
6. Click **Add to Device List** to open the Add Online Device dialog.

   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. See ***Set NTP*** for details.
7. **Optional:** Switch on **Mapped Port** and enter the picture downloading port if you want to download pictures from the device.

   Note

   This function is only available when you select **Hikvision Private Protocol** to filter the detected online devices. By default, the port No. is 80.
8. **Optional:** Switch on **Verify Stream Encryption Key**, and enter stream encryption key in **Stream Encryption Key on Device** field.

   Note

   This function should be supported by the devices. Refer to the user manual of the device for getting key.

   When starting live view or remote playback of the camera, the client will verify the key stored in SYS server for security purpose.

9. 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 installer and/or end-user.

10. **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.
11. **Optional:** Switch **Add Resource to Area** to on to import the channels of the added devices to an area.

    Note

    - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
    - You can create a new area by the device name or select an existing area.
    - If you do not import channels to area, you cannot perform operations such as live view, playback, event settings, etc., for the cameras.
12. **Optional:** Select a Streaming Server to get the video stream of the channels via the server.

    Note

    - The camera(s) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it.
    - You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.
13. Click **Add**.
14. **Optional:** Perform the following operations after adding the online devices in a batch.

Remote Configurations

Click ⚙ in the Operation column 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 **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.

Replace Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

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.

What to do next

For facial recognition camera/ANPR camera/thermal camera (report supported), click **Maintenance and Management → License Details → → Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.2 Add Encoding Device by IP Address/Domain

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 (cameras, DVRs, etc.) 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 ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding 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. See ***Set NTP*** for details.

4. Select **Hikvision Private Protocol/Open Network Video Interface Protocol** as the Access Protocol.

Note

- Select **Hikvision Private Protocol** to add a Hikvision device and select **Open Network Video Interface Protocol** to add a third-party device.
- To display the devices which are added to the platform via Open Network Video Interface protocol, you can go to ⊞ → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and check **Access via Open Network Video Interface Protocol**.

5. Select **IP Address/Domain** as the adding mode.
6. Enter the required information.

Device Address

The IP address or domain name of the device.

Add via TLS Protocol

This function is for **Hikvision Private Protocol** only. If you want to add the device via TLS protocol, check **Add via TLS Protocol**, and the SDK service port will be encrypted.

Device Port

By default, the device port No. is 8000.

Mapped Port

This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port No. that you have configured in the remote configuration page of the device. The default port No. is 80.

Verify Stream Encryption Key

This function is for **Hikvision Private Protocol** only. Switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored in SYS server for security purpose.

Note

This function should be supported by the devices. For details about getting the key, refer to the user manual of the device.

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 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 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 installer 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 channels of the added devices to an area.

Note

- You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform operations such as live view, playback, event settings, for the cameras.

9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the channels via the server.

Note

- The camera(s) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it.
- You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.

10. **Optional:** If you choose to add resources to area, switch on **Video Storage** and select a storage location for recording.

    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.

    Cloud Storage Server

    The video files will be stored in the Cloud 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.

Note

- For adding the encoding device by domain name, the video files can only be stored in the local storage of the device.
- You should 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. You can click **Add New** to add a new Hybrid Storage Area Network, Cloud Storage Server or pStor.

11. **Optional:** Set the quick recording schedule for added channels.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.
12. 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.

13. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations

Click ⚙ in the Operation column 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 **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.

Replace Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

What to do next

For facial recognition camera/ANPR camera/thermal camera (report supported), click **Maintenance and Management → License Details → › → Configuration → View** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.3 Add Encoding Devices by IP Segment

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 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 ⊞ **→ All Modules → General → Resource Management** .

2. Click **Device and Server → Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding 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. See ***Set NTP*** for details.

4. Select **Hikvision Private Protocol/Open Network Video Interface Protocol** as the Access Protocol.

Note

- Select **Hikvision Private Protocol** to add a Hikvision device, while select **Open Network Video Interface Protocol** to add a third-party device.
- To display devices which can be added to the platform via Open Network Video Interface Protocol, you need to go to 🟥 **→ All Modules → General → System Configuration → Network → Device Access Protocol** and check **Access via Open Network Video Interface Protocol**.

5. Select **IP Segment** as the adding mode.
6. Enter the required information.

Device Address

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

Add via TLS Protocol

If you want to add the device via TLS protocol, check **Add via TLS Protocol**, and the SDK service port will be encrypted.

Device Port

By default, the device port No. is 8000.

Mapped Port

This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port No. that you have configured in the remote configuration page of the device. The default port No. is 80.

Verify Stream Encryption Key

This button is for **Hikvision Private Protocol** only. You can switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored inSYS server for security purpose.

Note

This function should be supported by the devices. Refer to the User Manual of the device for getting key.

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 installer 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 on **Add Resource to Area** to import the resources of the added devices to an area.

   Note

   - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) 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 the live view, playback, event settings, for the resources.
9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.

   Note

   - The camera(s) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it.
   - You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.
10. Set the quick recording schedule for added resources.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.

- Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.

11. 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.
12. **Optional:** Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ in the Operation column 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 **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.

Replace Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

What to do next

For facial recognition camera/ANPR camera/thermal camera (report supported), click **Maintenance and Management → License Details → › → Configuration → View** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.4 Add Encoding Devices by Port Segment

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 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 ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding 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. See ***Set NTP*** for details.
4. Select **Hikvision Private Protocol/Open Network Video Interface Protocol** as the access protocol.

   Note

   - Select **Hikvision Private Protocol** to add Hikvision devices and select **Open Network Video Interface Protocol** to add third-party devices.
   - To display devices which can be added to the platform via Open Network Video Interface Protocol, you need to go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and check **Access via Open Network Video Interface Protocol**.
5. Select **Port Segment** as the adding mode.
6. Set the required information.

   Device Address

   Enter the IP address to add the devices which have the same IP address.

   Add via TLS Protocol

   If you want to add the device via TLS protocol, check **Add via TLS Protocol**, and the SDK service port will be encrypted.

   Device Port

   Enter the start port number and the end port number

   Mapped Port

   This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port number that you have configured on the remote configuration page of the device. The default port number is 80.

   Verify Stream Encryption Key

This button is for **Hikvision Private Protocol** only. You can switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **Stream Encryption Key on Device** field. Then when you start live view or remote playback of the device, the client will verify the key stored in SYS server for security purpose.

Note

This function should be supported by the devices. Refer to the user manual of the device for getting the key.

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 installer 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 on **Add Resource to Area** to import the channels of the added devices to an area.

   Note

   - You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import channels to area, you cannot perform live view, playback, event settings, etc., for the channels.
9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the channels via the server.

Note

- The camera(s) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it.
- You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.

10. **Optional:** Set the quick recording schedule for added channels.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.
11. Finish adding the device.
    - Click **Add** to add the devices of which the port number is between the start port number and end port number and back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add other devices.
12. **Optional:** Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ in the Operation column 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 **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.

Replace Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

What to do next

For facial recognition camera/ANPR camera/thermal camera (report supported), click **Maintenance and Management → License Details → › → Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.5 Add Encoding Device by Hik-Connect DDNS

You can add encoding 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 devices (cameras, DVRs, etc.) 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 Hik-Connect service for devices to be added on the remote configuration page of the device. For details, refer to the user manual of Hik-Connect.

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding 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. See ***Set NTP*** for details.

4. Select **Hikvision Private Protocol** as the Access Protocol.
5. Select **Hik-Connect DDNS** as the adding mode.
6. **Optional:** Switch on **Mapped Port** and enter the picture downloading port No. that you have configured on the remote configuration page of the device. The default port No. is 80.
7. Select a device source.

New Device

Add a new device to HikCentral Professional by Hik-Connect service.

Hik-Connect DDNS Device List

For users with a Hik-Connect account, you can add devices managed in your Hik-Connect account to HikCentral Professional in a batch.

Note

You can hover your cursor onto ⓘ to view details.

8. Enter the required information.

Hik-Connect DDNS Server Address

Enter the address of the Hik-Connect service. By default, it's ***https://open.ezvizlife.com***.

Serial No.

Enter the serial No. of the device.

Verification Code

Enter the verification code of the device.

Stream Encryption Key on Device

After switching on **Verify Stream Encryption Key**, you should enter stream encryption key in **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the camera, the client will verify the key stored in the SYS server for security purpose.

Note

This function should be supported by the devices. Refer to user manual of the device.

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 installer and/or end-user.

9. **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.
10. Switch on **Add Resource to Area** to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the live view, playback, event settings, etc., for the channels.

11. **Optional:** If you choose to add resources to an area, select a Streaming Server to get the video stream of the channels via the server.

Note

- The camera(s) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it.
- You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.

12. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
13. 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.
14. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations

Click ⚙ in the Operation column 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 **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.

Replace Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

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.

What to do next

For facial recognition camera/ANPR camera/thermal camera (report supported), click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.6 Add Encoding Device by Device ID

For the encoding devices supporting ISUP, you can add them by specifying a predefined device ID, key, etc. This is a cost-effective choice when you need to manage an encoding device without fixed IP address by HikCentral Professional.

Before You Start

- Make sure the encoding 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.
- 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. For details, refer to ***Device Access Protocol*** .

Steps

1. In the top left corner of Home page, select ⊞ **→ All Modules → General → Resource Management** .
2. Click **Device and Server → Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding 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. See ***Set NTP*** for details.
4. Select **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To display devices which can be added to the platform via ISUP, you need to go to ⊞ **→ All Modules → General → System Configuration → Network → Device Access Protocol** and enable **Allow ISUP Registration**.

5. Select **Device ID** as the adding mode.
6. Enter the required parameters, including the device ID and device name.

   Note

   For devices supporting accessing the platform via ISUP 5.0, you should enter the ISUP login password.

7. **Optional:** Switch on **Verify Stream Encryption Key** if the device supports and enables stream encryption, and enter the stream encryption key on device.
8. **Optional:** Switch on **Picture Storage** and set the location for picture storage.

   Note

   - You can select Local Storage, Hybrid Storage Area Network, Cloud Storage Server, pStor, or Network Video Recorder as the storage location.
   - If you select **Local Storage** as **Storage Location**, you can click **Configuration** to configure **Storage on SYS Server** for the captured pictures. For detailed information, see ***Configure Storage for Imported Pictures and Files*** .

9. **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.
10. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

    Note

    - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
    - For video access control terminal of a device, the camera on the terminal will also be imported 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 operations such as live view, playback, event settings, for the cameras.
11. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.

    Note

    - The camera(s) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it.
    - You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.

12. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.
13. 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.
14. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations

Click ⚙ in the Operation column 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 **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.

Replace Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

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.

What to do next

For facial recognition cameras/ANPR cameras/thermal cameras (report supported), click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally on the platform.

8.3.7 Add Encoding Devices by Device ID Segment

If you need to add multiple encoding devices which have no fixed IP addresses and support ISUP Protocol 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 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.
- Before adding devices supporting ISUP 2.6/4.0 protocol to the system, you need to set related configuration to allow these devices to access the system. For details, refer to ***Device Access Protocol*** .

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding 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. See ***Set NTP*** for details.
4. Select **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To display devices which can be added to the platform via ISUP, you need to go to ⊞ → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and enable **Allow ISUP Registration**.
5. Select **Device ID Segment** as the adding mode.
6. Enter the required parameters, including the start device ID and end device ID.

   Note

   For devices supporting accessing the platform via ISUP 5.0, you should enter the ISUP login password.
7. **Optional:** Switch on **Verify Stream Encryption Key** if the device supports, and enter the stream encryption key on device.
8. **Optional:** Switch on **Picture Storage** and set the location for picture storage.

Note

- You can select Local Storage, Hybrid Storage Area Network, Cloud Storage Server, pStor, or Network Video Recorder as the storage location.
- If you select **Local Storage** as **Storage Location**, you can click **Configuration** to configure **Storage on SYS Server** for the captured pictures. For detailed information, see ***Configure Storage for Imported Pictures and Files*** .

9. **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.
10. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

    Note

    - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
    - For video access control terminal of a device, the camera on the terminal will also be imported 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 operations such as live view, playback, event settings, for the cameras.
11. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.

    Note

    - The camera(s) related to the selected server will be displayed, you can view their information and can click the name of a camera to edit it.
    - You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.
12. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.
13. 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.
14. **Optional:** Perform the following operation(s) after adding devices.

Remote Configurations	Click ⚙ in the Operation column to set the remote configurations of the corresponding device.

Note

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

Change the 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.

Replace the Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

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.

What to do next

For facial recognition cameras/ANPR cameras/thermal cameras (report supported), click **Maintenance and Management → License Details → → Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally on the platform.

8.3.8 Add Encoding Devices 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 (cameras, DVR, etc.) 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. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding 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. See ***Set NTP*** for details.
4. Select **Hikvision Private Protocol/Hikvision ISUP Protocol**/ as the access protocol.

   Note

   - Select **Hikvision Private Protocol/Hikvision ISUP Protocol** to add a Hikvision device and select **Open Network Video Interface Protocol** to add a third-party device.
   - To display devices which can be added to the platform via ISUP, you need to go to ⊞ → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and enable **Allow ISUP Registration**.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined template (excel file) on your PC.
7. Open the exported template file and enter the required information of the devices to be added in the corresponding column.
8. Click and select the edited file.
9. **Optional:** Switch on **Picture Storage** and set the location for picture storage.

   Note

   - You can select Local Storage, Hybrid Storage Area Network, Cloud Storage Server, pStor, or Network Video Recorder as the storage location.
   - If you select **Local Storage** as **Storage Location**, you can click **Configuration** to configure **Storage on SYS Server** for the captured pictures. For detailed information, see ***Configure Storage for Imported Pictures and Files*** .
10. **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.

11. 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.
12. **Optional:** Perform the following operation(s) after adding devices in a batch.

Remote Configurations

Click ⚙ in the Operation column 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 **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.

Replace Device

If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

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.

What to do next

For facial recognition camera/ANPR camera/thermal camera (report supported), click **Maintenance and Management → License Details → › → Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.9 Limit Bandwidth for Video Downloading

You can limit bandwidth for video downloading of specific NVRs to save video on the total bandwidth, and thus ensuring the fluency of main features such as live view.

Note

The NVR should be of V4.1.50 or later versions.

In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Device and Server** → **Encoding Device** to enter the encoding device management page, select encoding device(s) and click **Edit Bandwidth for Video Downloading** to set the bandwidth upper-limit for video downloading of the selected device(s).

8.3.10 Set N+1 Hot Spare for NVR

You can form an N+1 hot spare system with several NVRs (Network Video Recorder). The system consists of several host servers and a spare server. When the 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.

Before You Start

- At least two online NVRs should be added to form an N+1 hot spare system. For details about adding NVR, see ***Manage Encoding Device*** .
- Make sure the NVRs 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.

If the N+1 hot spare settings have already been configured on the NVR, select 🟥 → **All Modules** → **General** → **Resource Management** → **Device and Server** → **Encoding Device** → **N+1 Hot Spare** → **Get Hot Spare Settings from Device** to upload the hot spare settings from the device to HikCentral Professional. If the N+1 hot spare settings haven't been configured on the device, perform the following task to set N+1 hot spare for the NVR.

Steps

Note

- The N+1 hot spare function is only supported by NVRs and Hybrid Storage Area Networks. For details about configuring N+1 hot spare system with Hybrid Storage Area Networks, see ***Set N+1 Hot Spare for Hybrid SAN*** .
- 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. In the top left corner of Home page, select ■ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** → **N+1 Hot Spare** to enter the N+1 Configuration page.
3. Click **Add** to set N+1 hot spare.
4. Select a NVR in the **Spare** drop-down list to set it as the spare server.
5. Select the NVR(s) in the **Host** field to set them as the host server.
6. Click **Add**.

   Note

   The recording schedules configured on the NVR will be deleted after setting it as the spare Recording Server.
7. Click **Apply Hot Spare Settings to Device** to apply the Hot Spare settings to the devices to take effect.
8. **Optional:** Perform the following operations after setting the hot spare.

Edit Hot Spare	Click ✎ on the Operation column, and you can edit the spare and host settings.
Delete Hot Spare	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.

8.4 Manage Access Control Device

You can add the access control devices to the system for access permission configuration, time and attendance management, etc.

8.4.1 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 🟥 → **All Modules** → **General** → **Resource Management** .
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. You can go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** 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 installer 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 select **Hikvision ISUP Protocol** in the Online Device area.
  - You 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 (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. **Optional:** Check **Restore Default** 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 Device Parameters*** 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
Select the added device(s) and click **Restore** 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.

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*** .

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 🟥 → **All Modules** → **General** → **Resource Management** .
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. You can go to 🟥 → **All Modules → General → System Configuration → Network → Device Access Protocol** 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 installer 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.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. **Optional:** Check **Restore Default** 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 Device Parameters*** 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

    You can configure privacy settings for online access control devices. For details, refer to ***Privacy Settings*** .

    Restore Default

    Select the added device(s) and click **Restore** 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.

8.4.2 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. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
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.
5. Select **IP Address/Domain** as the adding mode.
6. Enter the required parameters.

Note

By default, the device port number is 8000 when the access protocol is **Hikvision Private Protocol**, while the device port number is 80 when the access protocol is **Hikvision ISAPI Protocol**.

Caution

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

7. **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 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.

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. 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 Device Parameters*** 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

Select the added device(s) and click **Restore** 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.

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

If the original device malfunctions, you can replace it with a new device using the same IP address. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

8.4.3 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. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
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** or **Hikvision ISAPI Protocol** as the access protocol.
5. Select **IP Segment** as the adding mode.
6. Enter the required information.

Note

By default, the device port number is 8000 when the access protocol is **Hikvision Private Protocol**, while the device port number is 80 when the access protocol is **Hikvision ISAPI Protocol**.

⚠ **Caution**

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

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

7. **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 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.

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. See ***Configure Device Parameters*** 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

Select the added device(s) and click **Restore** 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.

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

If the original device malfunctions, you can replace it with a new device using the same IP address. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

8.4.4 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 🟥 → **All Modules** → **General** → **Resource Management** .
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. You can go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** 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 comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configuration** to enable **Local Storage** and set the storage locations for pictures and files as needed.

Note

If the selected access protocol is Hikvision Private Protocol, you can skip this step.

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 Device Parameters*** 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
Select the added device(s) and click **Restore** 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.

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

If the original device malfunctions, you can replace it with a new device using the same IP address. After you replace it, move the cursor on ⓘ on the right of the device name, and click **Replace Device** to confirm the replacement.

8.4.5 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 🟥 → **All Modules** → **General** → **Resource Management** .
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. You can go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** 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 comparison. The storage location of captured pictures and face picture libraries cannot be the same.

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

Note

If the selected access protocol is Hikvision Private Protocol, you can skip this step.

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 Device Parameters*** 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

Select the added device(s) and click **Restore** 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.

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*** .

8.4.6 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 🟥 → **All Modules** → **General** → **Resource Management** .
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. You can go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** →

Device Access Protocol 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 comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configuration** to enable **Local Storage** and set the storage locations for pictures and files as needed.

   Note

   If the selected access protocol is Hikvision Private Protocol, you can skip this step.
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 Device Parameters*** 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

Select the added device(s) and click **Restore** 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.

Replace Device

If the original device malfunctions, you can replace it with a new device using the same IP address. After you replace it, move the cursor on on the right of the device name, and click **Replace Device** to confirm the replacement.

8.4.7 Configure Device Parameters

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

Configure 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.

Before You Start

Make sure you have wired the third-party card readers to the access control device or elevator control device.

Steps

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.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** or **Device and Server** → **Elevator Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.

4. Switch on **Custom Wiegand**.
5. Configure the Wiegand parameters.

   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

Configure Device Actions for Access Event

You can set the linkage actions of an access control device or elevator control device for the device's events, so that when a specific event occurs, the device can execute actions such as capturing a picture, recording video footage, triggering alarm output, triggering buzzer, arming/disarming zones, locking/unlocking access points, etc.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** or **Device and Server** → **Elevator Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.

4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Event Linkage** as the linkage type.
   2) Select an event type from the **Event Type** drop-down list and then select a specific event.

   Note

   - If you select **Alarm Input Event**, you need to select an alarm input.
   - If you select **Door Event**, you need to select an access point.
   - If you select **Card Reader Event**, you need to select a card reader.
6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point 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.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for Card Swiping

You can set the linkage actions of an access control device or elevator control device for card swiping, so that when the device detects a specific card, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc. In this way, you can monitor the behaviors and whereabouts of the card holder.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** or **Device and Server** → **Elevator Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Card Linkage** as the linkage type.
   2) Select a card from the **Card Number** drop-down list.
   3) Select a card reader from the **Card Reader** drop-down list.
6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point 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.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for Person ID

You can set the linkage actions of an access control device or elevator control device for person ID, so that when the device detects the credentials of the person, it can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc. In this way, you can monitor the behaviors and whereabouts of the person.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** or **Device and Server** → **Elevator Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Person Linkage** as the linkage type.

2) Select a person ID from the **Person** drop-down list.

3) Select a card reader from the **Card Reader** drop-down list.

6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point 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.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for MAC Address

You can set access control device's linkage actions for MAC address of mobile devices, so that when the device detects a specific MAC address, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Select **MAC Linkage** as the linkage type, and then edit the MAC address.
6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point 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.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Card Swiping Parameters

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

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** or **Device and Server** → **Elevator Control Device** on the left.
3. Click ⚙ on the Operation column to enter the configuration page of a device.
4. In Card Swiping section, configure card swiping parameters.

Note

Parameters vary with different device types and models.

Reader Communication Protocol

Select the reader communication protocol.

Input Card Number On Keypad

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

Enable NFC Card

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

Mifare Encryption

If it is enabled, only the card with the same encrypted sector can be granted access.

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.

Note

For details about linking a camera to an access point, see ***Edit Door for Current Site*** or ***Edit Elevator for Current Site*** .

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*** or ***Edit Elevator 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.

Configure Other Parameters

You can configure other parameters for an access control device or elevator control device and restore or reboot the device on the device configuration page.

Note

- Device support required. Parameters vary with different device types and models.
- For more remote configurations, click **Configuration** at the end of the device configuration page. For detailed instructions, refer to the user manual of the device.

Time

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

Device Time

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

Sync with Server Time

Synchronize the device time with the server of the platform.

Skin-surface Temperature

Set **Temperature Screening** 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 must be higher than the minimum temperature.

Open Door When Temperature is Abnormal

If 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.

Mask Settings

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

Do Not Open Barrier when No Mask

If checked, the barrier will still open for persons without a mask.

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

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

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 **Configuration** to open the remote configuration page of the device and configure more parameters.

8.4.8 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.

In the top of top left corner of Home page, select → **All Modules** → **General** → **Resource Management** → **Device and Server** → **Access Control Device** .

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.

You can switch on the **Health Code** and enter the server address of the health code. When switched on, the health code will be available in **Result Display** area. The the server address of the health code will be applied to the devices.

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.

8.5 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.

8.5.1 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. 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 🟥 → **All Modules** → **General** → **Resource Management** .
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 Device List** to open the Add Elevator Control Device window.
6. 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 installer 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 select **Hikvision ISUP Protocol** in the Online Device area.
  - You select **Hikvision Private Protocol** in the Online Device area, and device port is 0.

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** 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 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 Device Parameters*** 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

Select the added device(s) and click **Restore** 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.

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. 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 🟥 → **All Modules** → **General** → **Resource Management** .
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 installer 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** 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. 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 Device Parameters*** 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

Select the added device(s) and click **Restore** 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.

8.5.2 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. 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 🟥 → **All Modules** → **General** → **Resource Management** .
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 installer 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. See ***Configure Device Parameters*** 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	Select the added device(s) and click **Restore** 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.

8.5.3 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. 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 🟥 → **All Modules** → **General** → **Resource Management** .
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 installer 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. See ***Configure Device Parameters*** 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

Select the added device(s) and click **Restore** 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.

8.5.4 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. 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 ▦ → **All Modules** → **General** → **Resource Management** .
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. See ***Configure Device Parameters*** 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

Select the added device(s) and click **Restore** 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.

8.6 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.

8.6.1 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. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

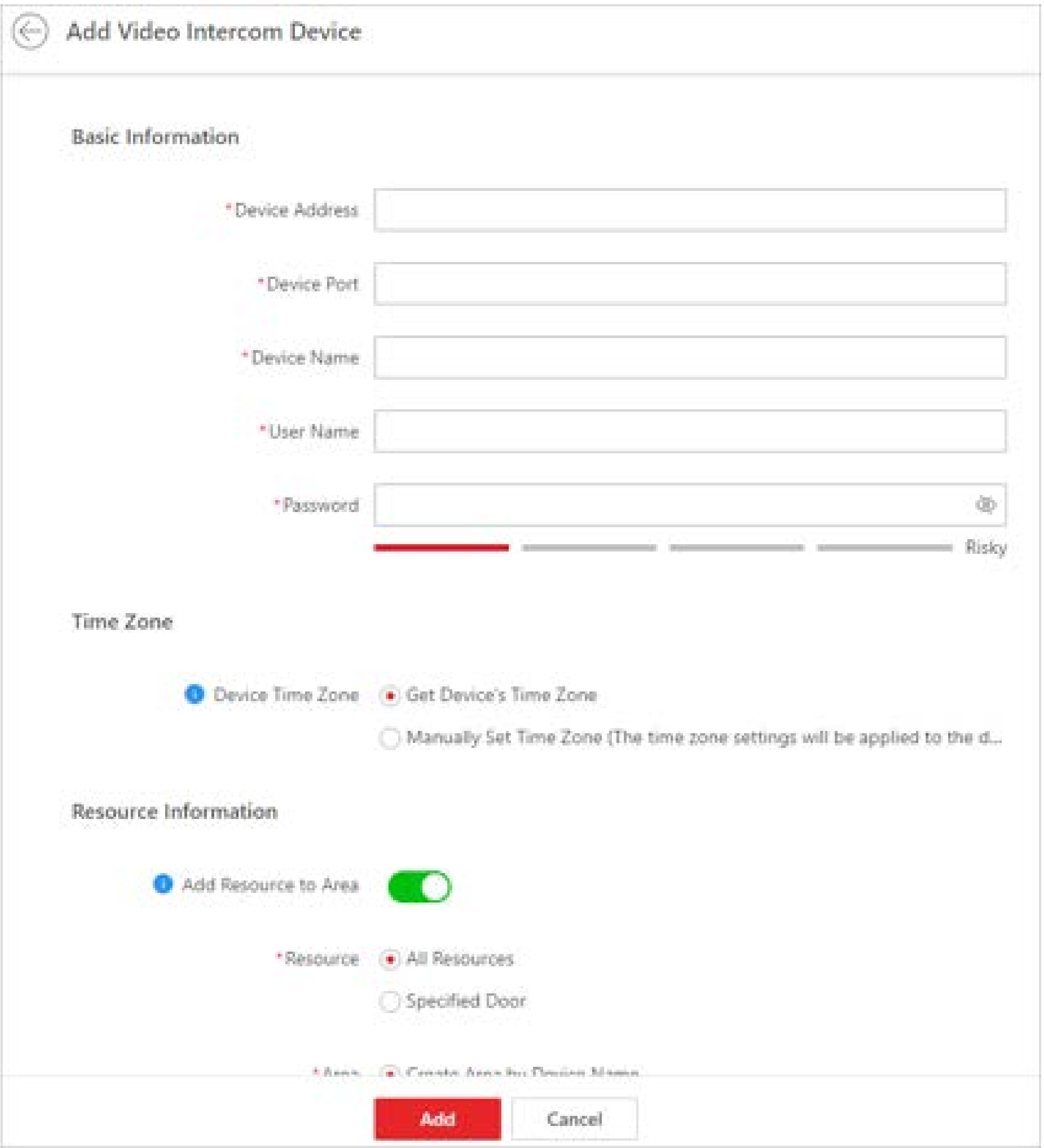
1. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. In the Online Device area, select a network type.

   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.



Add Video Intercom Device

Basic Information

*Device Address

*Device Port

*Device Name

*User Name

*Password

Risky

Time Zone

Device Time Zone ● Get Device's Time Zone

○ Manually Set Time Zone (The time zone settings will be applied to the d...

Resource Information

Add Resource to Area

*Resource ● All Resources

○ Specified Door

*Area ● Create Area by Device Name

Add Cancel

Figure 8-1 Add Video Intercom Device Page

6. Enter the required information.

   Device Address

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

   Device Port

   The port No. of the device, which is shown automatically. The default 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 installer 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** 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. 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

Select the added device(s), and click to restore the configured device parameters.

Note

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

Filter Device

Click **All Devices** at the upper-left corner on the Device List page, and then select a desired group to filter the devices.

8.6.2 Add a Video Intercom Device by IP Address

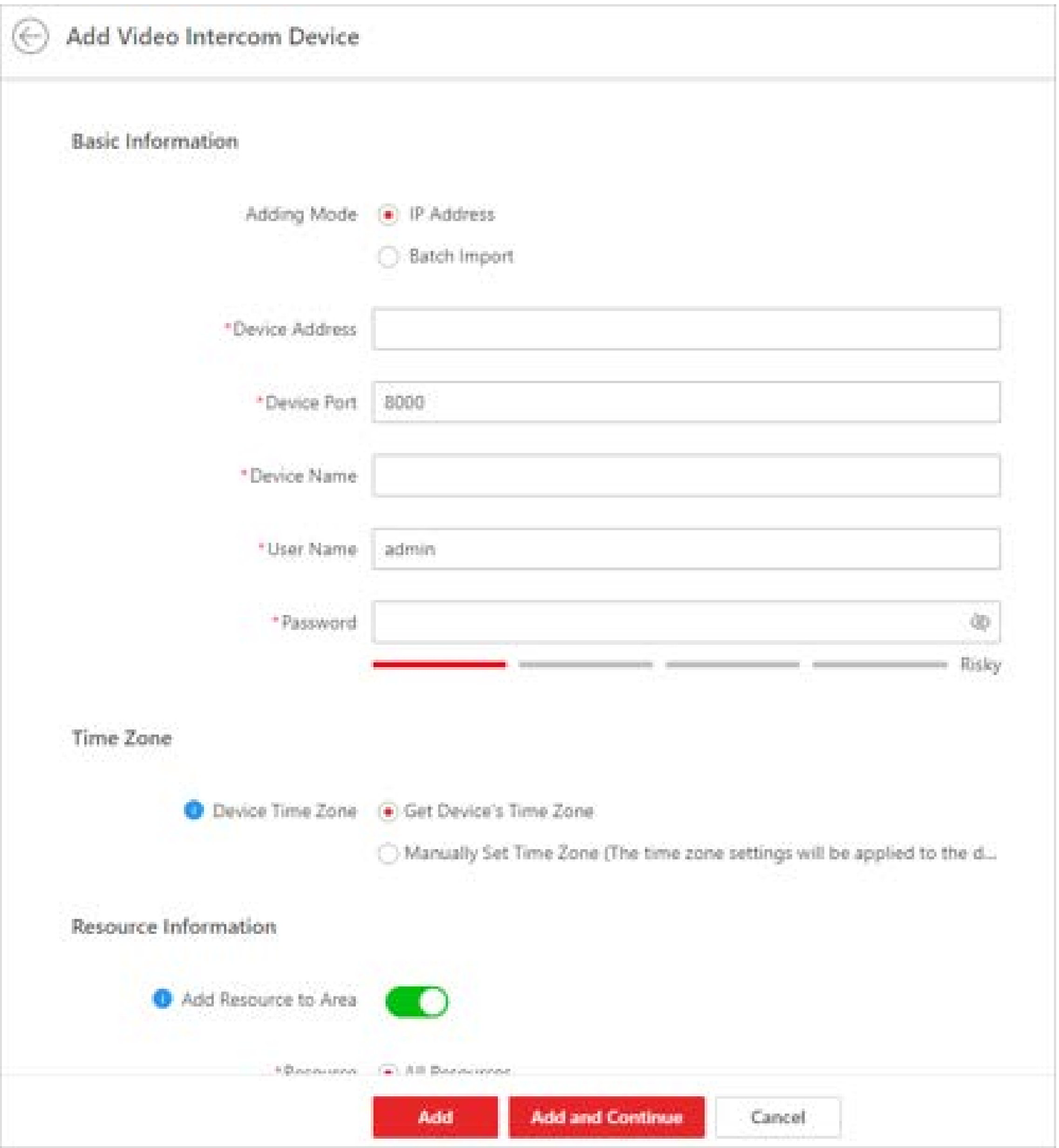
When you know the IP address of a video intercom device, you can add it to the system by specifying the IP address, user name, password, etc. for management and further video intercom applications.

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 ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **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.



Add Video Intercom Device

Basic Information

Adding Mode ● IP Address ○ Batch Import

*Device Address

*Device Port 8000

*Device Name

*User Name admin

*Password

Risky

Time Zone

Device Time Zone ● Get Device's Time Zone ○ Manually Set Time Zone (The time zone settings will be applied to the d...

Resource Information

Add Resource to Area (on)

Figure 8-2 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 installer and/or end-user.

6. **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.
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** so that all the parameters of the device configured on the system will be restored 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. 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.

Filter Device

Click **All Devices** at the upper-left corner on the Device List page, and then select a desired group to filter the devices.

8.6.3 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 ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **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 **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 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. 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.

Filter Device

Click **All Devices** at the upper-left corner on the Device List page, and then select a desired group to filter the devices.

8.7 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.

8.7.1 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 device one by one to HikCentral Professional by specifying its 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 to be able to connect the devices to the HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Visitor Terminal** on the left.
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 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 **Add to Device List** to open the Add Online Device window.
6. 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 installer 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 manually select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Check **Restore Default** 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 finish adding the device.
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 detailed operation steps about remote configuration, see the user manual of the device.
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. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Visitor Terminal** on the left.
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 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.

4. In the Online Device area, check the active devices to be added.
5. Click **Add to Device List** to open the Add Online Device dialog.
6. 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 installer 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 manually select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Check **Restore Default** 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 the following operations after adding the online 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.

Refresh Device Information

Select the added device and click ⟳ to refresh information of the device.

8.7.2 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. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Visitor Terminal** on the left.
3. Click **Add** to enter the Add Visitor Terminal page.
4. Select **IP Address** as the adding mode.
5. 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 installer 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** 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. 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.

9. **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.
Refresh Device Information	Select the added device and click ⟳ to refresh information of the device.

8.7.3 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. In the top left corner of Home page, select ⊞ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Visitor Terminal** on the left.
3. Click **Add** to enter the Add Visitor Terminal 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 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 installer 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. 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.

8. **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.

Refresh Device Information

Select the added device and click ⟳ to refresh information of the device.

8.7.4 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. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Visitor Terminal** on the left.
3. Click **Add** to enter the Add Visitor Terminal page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and 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 on the corresponding column.
7. Click 🗀 and select the edited file.
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 manually select a time zone of the device. The settings will be applied to the device automatically.

9. 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.
10. **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.

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

8.8 Manage Mobile Devices

Mobile devices are used for driving monitoring. They support live view, playback, remote configuration, alarm notification, GPS data collection, GPS positioning, etc. With mobile 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 mobile devices, including adding, editing, deleting, and remotely configuring them.

8.8.1 Add Detected Online Mobile Devices

The active online mobile 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 Mobile Device

The Web Client automatically searches for online mobile devices on the same local subnet with it or the SYS server. You can add detected online mobile 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 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 the Client, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Mobile Device** on the left.
3. Select a detected online mobile device from the Online Device list.
4. Click **Add to Device List** to enter the Add Mobile Device page.

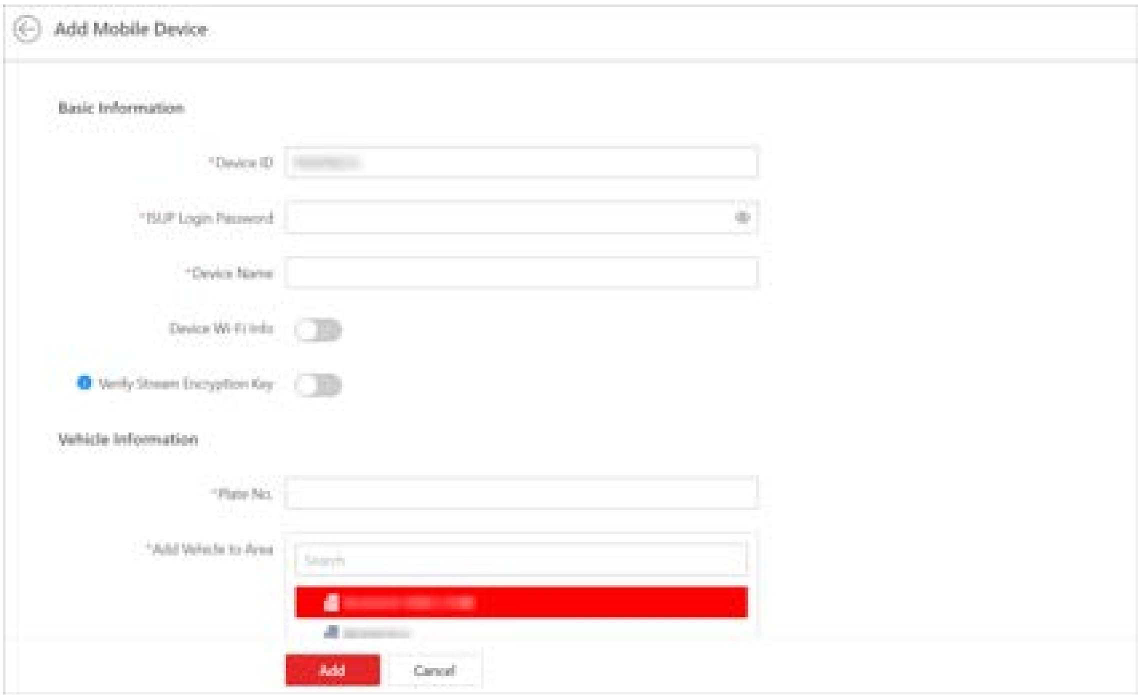


Figure 8-3 Add a Detected Online Mobile Device

5. Set basic information.
   1) Enter the ISUP login password and name of the mobile 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 installer and/or end-user.

2) **Optional:** Switch on **Device Wi-Fi Info** and enter the address and port of the mobile device as well as the user name and password of the Wi-Fi.

   Once a vehicle reaches its destination and the mobile 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 mobile device.

   Note

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

   When starting live view or remote playback of the cameras related to the mobile device, the Client will verify the key stored in the SYS server for security purpose.

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

   Note

   - If you select **Local Storage**, you need to click **Configuration** 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.
8. 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.
9. 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 mobile device.

10. Click **Add**.
11. **Optional:** Perform the following operations after adding the mobile device.

Edit Mobile Device	On the device list, click the name of a mobile device to edit it.
Configure Mobile Device Remotely	On the device list, click ⚙ in the Operation column to configure a mobile device remotely.
Reset Device's Time Zone	On the device list, select one or multiple mobile devices and click **Time Zone** to edit their time zones.
Delete Mobile Device	Select one or multiple devices and click **Delete** to delete them.
Search for Mobile Device	Enter key words in the search box and click 🔍 to search for specified mobile device.

Add Detected Online Mobile Devices in a Batch

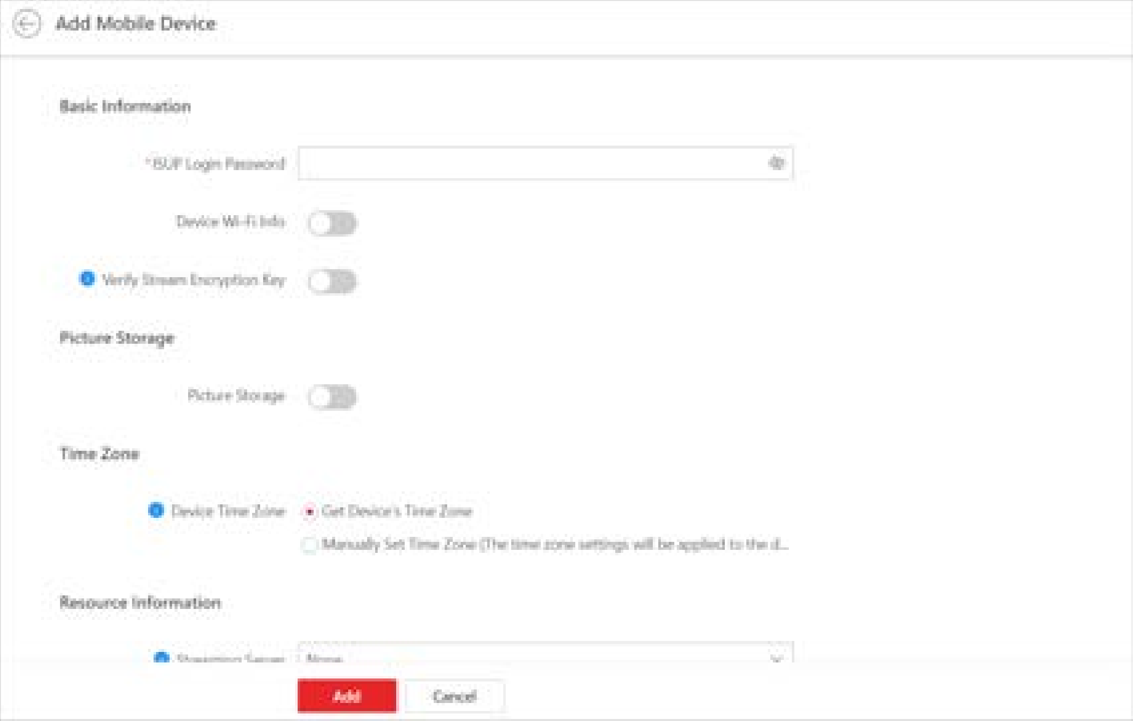
The Web Client automatically searches for online mobile devices on the same local subnet with it or the SYS server. You can batch add multiple detected online mobile devices to the platform if they share the same user account.

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 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 the Client, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Mobile Device** on the left.
3. Select some detected online mobile devices from the Online Device list.
4. Click **Add to Device List** to enter the Add Mobile Device page.



Add Mobile Device

Basic Information

*ISUP Login Password

Device Wi-Fi Info

Verify Stream Encryption Key

Picture Storage

Picture Storage

Time Zone

Device Time Zone
● Get Device's Time Zone
○ Manually Set Time Zone (The time zone settings will be applied to the d...

Resource Information

Streaming Server: None

Figure 8-4 Batch Add Detected Online Mobile Devices

5. Set basic information.
   1) Enter the ISUP login password of the mobile 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 installer and/or end-user.

   2) **Optional:** Switch on **Device Wi-Fi Info** and enter the address and port of the mobile devices as well as the user name and password of the Wi-Fi.

   Once a vehicle reaches its destination and the mobile 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 mobile devices.

Note

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

When starting live view or remote playback of the cameras related to the mobile devices, the Client will verify the key stored in the SYS server for security purpose.

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 **Configuration** 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 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.
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 mobile device.
9. Click **Add**.
10. **Optional:** Perform the following operations after adding these mobile devices.

Delete Mobile Device	Select one or multiple devices and click **Delete** to delete them.
Search for Mobile Device	Enter key words in the search box and click 🔍 to search for specified mobile device.

8.8.2 Add a Mobile Device by Device ID

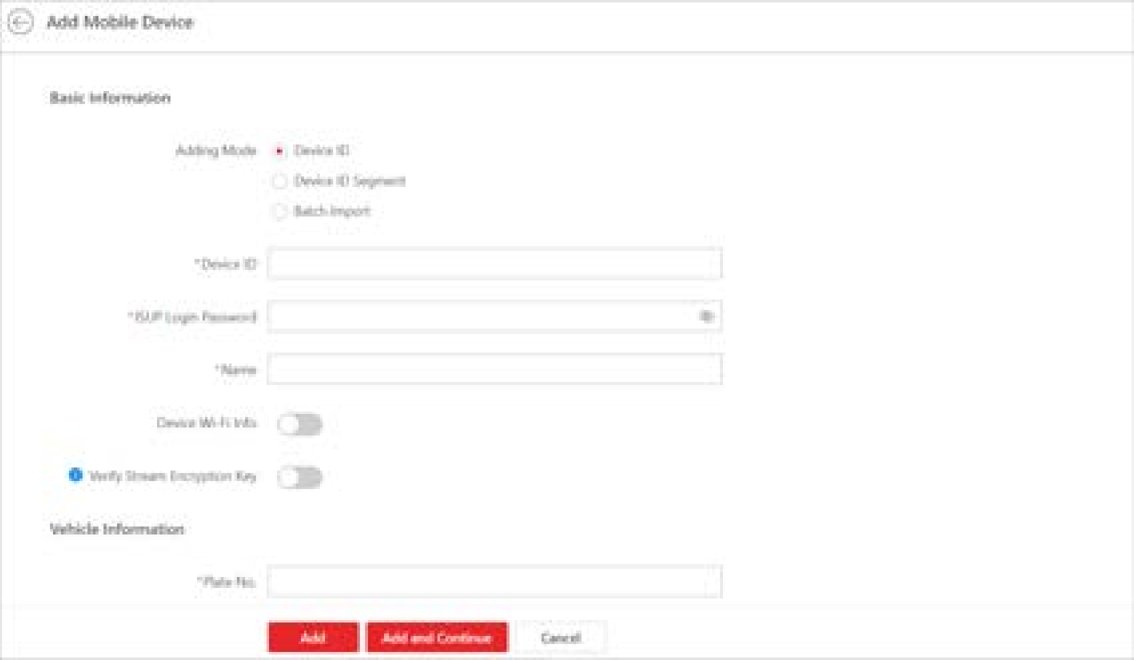
If a mobile device supports the ISUP protocol, you can add it to the platform by its device ID. This way is cost-effective when you need to manage a mobile device in the public network without a fixed IP address.

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 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 the Client, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Mobile Device** on the left.
3. Click**Add** to enter the Add Mobile Device page.


Add Mobile Device

Basic Information

Adding Mode ● Device ID ○ Device ID Segment ○ Batch Import

*Device ID

*ISUP Login Password

*Name

Device Wi-Fi Info

Verify Stream Encryption Key

Vehicle Information

*Plate No.

Figure 8-5 Add Mobile Device

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

Once a vehicle reaches its destination and the mobile 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 mobile device.

Note

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

When starting live view or remote playback of the cameras related to the mobile 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 the mobile device is related to.
   2) Add the vehicle to an existing area or click **Add New** 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 **Configuration** 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 mobile device.

9. Click **Add** to finish or click **Add and Continue** to add another mobile device.
10. **Optional:** Perform the following operations after adding the mobile device.

Edit Mobile Device	On the device list, click the name of a mobile device to edit it.

Configure Mobile Device Remotely
On the device list, click ⚙ in the Operation column to configure a mobile device remotely.

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

Delete Mobile Device
Select one or multiple devices and click **Delete** to delete them.

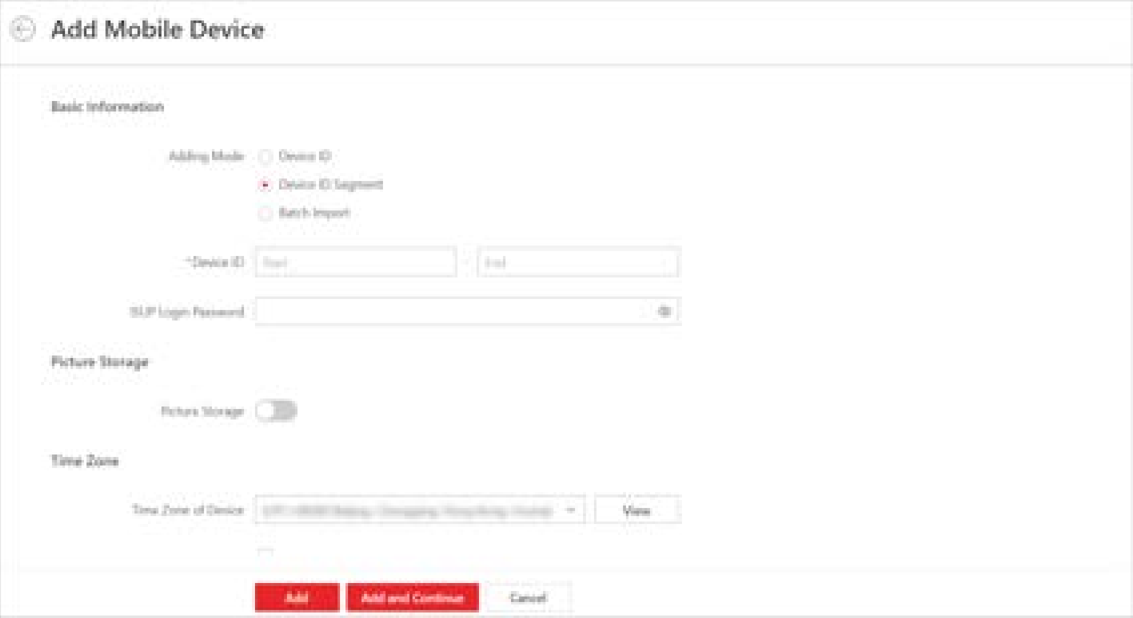
Search for Mobile Device
Enter key words in the search box and click 🔍 to search for specified mobile device(s).

8.8.3 Add Mobile Devices by Device ID Segment

You can add mobile device(s) to the platform by device ID segment, and perform further operations, such as editing device settings, configuring devices remotely, deleting devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Mobile Device** on the left.
3. Click **Add** to enter the Add Mobile Device page.
4. Select **Device ID Segment** as the adding mode.



Add Mobile Device

Basic Information

Adding Mode ○ Device ID ● Device ID Segment ○ Batch Import

*Device ID Start - End

ISUP Login Password

Picture Storage

Picture Storage

Time Zone

Time Zone of Device (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Figure 8-6 Add Mobile Device by Device ID Segment

5. 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.

6. 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.
7. Configure the time zone of the device(s).
   1) Select a time zone from the drop-down list.

   Note

   You can click **View** to see the Daylight Saving Time (DST) of the time zone if DST is observed by it.

   2) Check **Apply to Device**.
8. Configure the resource information.
   1) Switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

   Create Area by Device Name

   The name of the to-be-created area is the same with that of the device you add.

   Note

   When an added device is online, it will trigger the platform to create an area named after it, and add its related resource(s) to the area.

   Existing Area

   The device's logical resource(s) will be added to an existing area.

   Note

   If there is no area added, you need to click **Add New Area** to add the device's related resource(s) to the area.

   3) Select a streaming server from the drop-down list.
   4) 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.

   5) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the device.
9. Click **Add** to finish, or click **Add and Continue** to add other device(s).

10. **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.

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 must 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.

8.8.4 Add Mobile Devices in a Batch

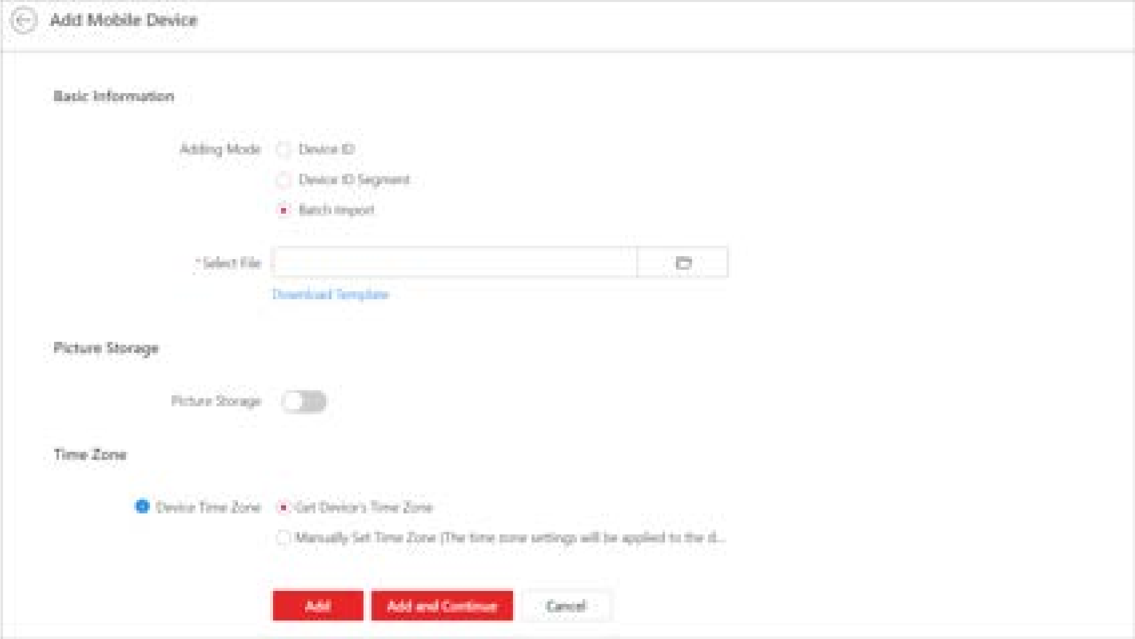
You can fill in required information of to-be-added mobile devices in an Excel file and upload it onto the platform to batch add them for management.

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 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 the Client, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Mobile Device** on the left.
3. Click **Add** to enter the Add Mobile Device page.



Add Mobile Device

Basic Information

Adding Mode ○ Device ID
○ Device ID Segment
● Batch Import

*Select File

Download Template

Picture Storage

Picture Storage

Time Zone

Device Time Zone ● Get Device's Time Zone
○ Manually Set Time Zone (The time zone settings will be applied to the d...

Figure 8-7 Batch Add Mobile Devices

4. 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 in required information.
   3) Click 🗀 to select the file and upload it to the platform.
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 **Configuration** 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. Click **Add** to finish or click **Add and Continue** to add another batch of mobile devices.
8. **Optional:** Perform the following operations after adding these mobile devices.

Edit Mobile Device	On the device list, click the name of a mobile device to edit it.

Configure Mobile Device Remotely
On the device list, click ⚙ in the Operation column to configure a mobile device remotely.

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

Delete Mobile Device
Select one or multiple devices and click **Delete** to delete them.

Search for Mobile Device
Enter key words in the search box and click 🔍 to search for specified mobile device(s).

8.9 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. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Query Terminal** on the left.
3. Click **Add** to enter the Add Query Terminal page.

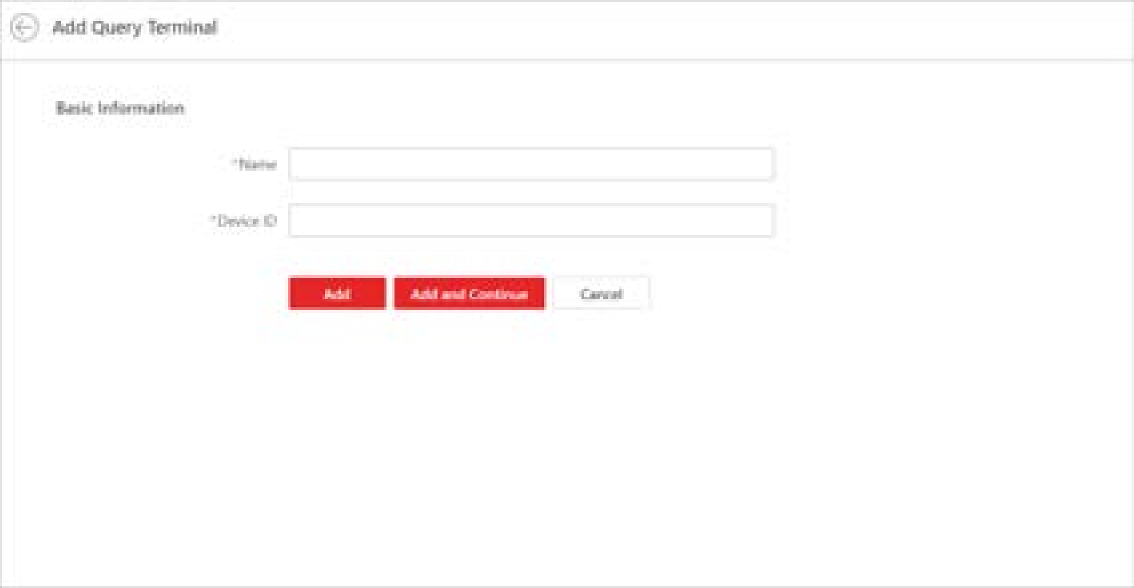


Figure 8-8 Add Query Terminal

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.

8.10 Add an Entrance/Exit Station

An entrance/exit station 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 station, the station will control the barrier gate to open and let the vehicle enter; after the vehicle returns the ticket or card, the station will allow the vehicle to exit. Besides, if an entrance/exit station assigns cards instead of tickets, its guidance screen is configurable, which means you can configure the information displayed on it.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Sever** → **Entrance/Exit Station** on the left.
3. Click **Add** to enter the Add Entrance/Exit Station page.

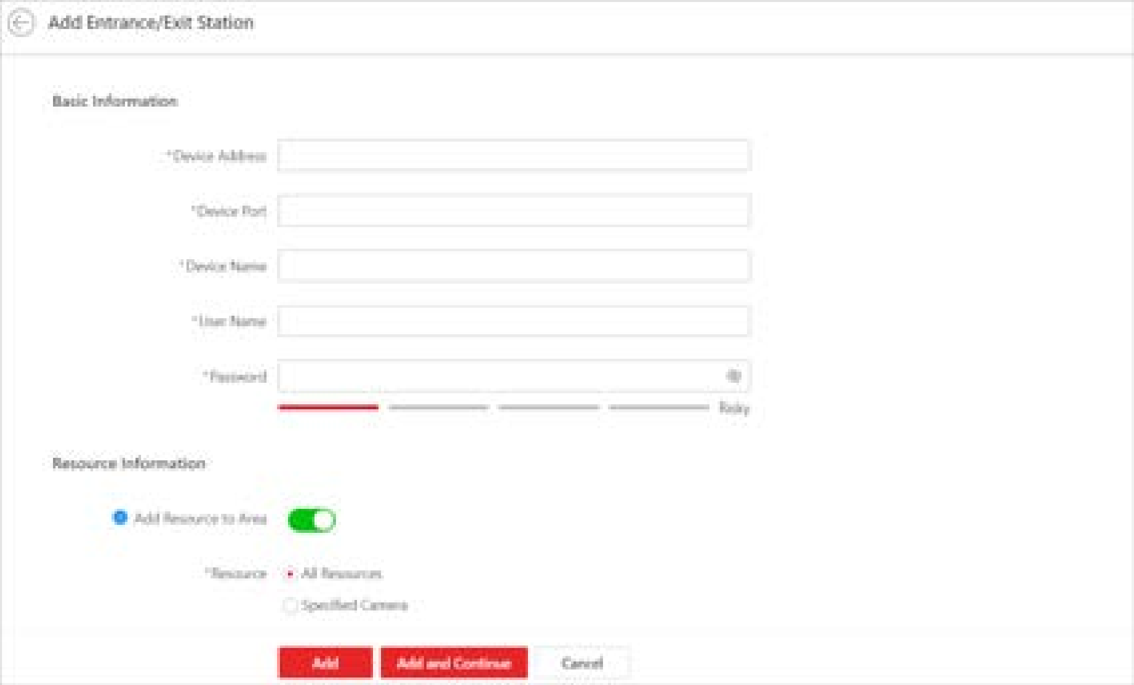


Figure 8-9 Add Entrance/Exit Page

4. In the Basic Information area, enter the IP address, port No., name, user name, and password of the entrance/exit station.
5. **Optional:** Add the entrance/exit station'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 station 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 station will be created, and the resource(s) will be added to the area; if you select **Existing Area**, you need to select an area to add the resource(s) to.

   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 can click the name of a camera to edit it.

   5) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the entrance/exit station.

6. Click **Add** to finish or click **Add and Continue** to add another entrance/exit station.
7. **Optional:** Perform the following operations.

Edit an Entrance/Exit Station
In the Device Name column, click the name of an entrance/exit station to edit it.

Delete an Entrance/Exit Station
Select an entrance/exit station, and click **Delete** to delete it. You can also select multiple entrance/exit stations, and click **Delete** to delete them at once.

Configure an Entrance/Exit Station Remotely
In the Operation column, click ⚙ to configure the entrance/exit station remotely.

8.11 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*** .

8.11.1 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 have 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 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Guidance Terminal** 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 activated device that you want to add.
5. Click **Add to Device List**.
6. In the Basic Information area, edit device login information.

   Device Address

   IP address of the device, which is acquired automatically.

   Device Port

   Port number of the device. The default port number is 8000.

   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 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 installer and/or end-user.
7. **Optional:** Switch on **Add Resource to Area** to import the resources of the device to an area.

Note

- You can import all the resources including cameras, alarm inputs, and alarm outputs, or specific cameras to the corresponding area.
- You can create a new area named after the device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the cameras.

8. **Optional:** If you choose to add resources to area, select a server in **Streaming Server** to get the video stream of the cameras via the server.

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.

9. **Optional:** If you choose to add resources to area, switch on **Video Storage** and select a storage location for recording.

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 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.

Note

- Configure the Hybrid Storage Area Network, Cloud Storage Server or pStor in advance, or its storage location cannot display in the drop-down list. You can click **Add New** to add a new Hybrid Storage Area Network, Cloud Storage Server, or pStor.

10. Set the recording schedule for the cameras.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the cameras of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type, etc. Refer to ***Configure Recording for Cameras on Current Site*** for details.

11. Click **Add**.
12. **Optional:** Perform further operations after adding the online device.

Configure Device

Click ⚙ in the **Operation** column to enter the remote configuration page of the device.

Note

For detailed instructions on remote configuration, see the user manual of the device.

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 change the password for them together.

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. 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 ■ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Guidance Terminal** 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 activated devices that you want to add.
5. Click **Add to Device List**.
6. 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 installer and/or end-user.

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

Note

- You can create a new area named after the device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the cameras.

8. **Optional:** If you choose to add resources to area, select a server in **Streaming Server** to get the video stream of the cameras via the server.

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.

9. **Optional:** If you choose to add resources to area, switch on **Video Storage** and select a storage location for recording.

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 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.

Note

Configure the Hybrid Storage Area Network, Cloud Storage Server, or pStor in advance, or its storage location cannot display in the drop-down list. You can click **Add New** to add a new Hybrid Storage Area Network, Cloud Storage Server, or pStor.

10. Set the recording schedule for the cameras.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the cameras of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.
11. Click **Add**.
12. **Optional:** Perform further operations after adding the online devices.

Configure Device	Click ⚙ in the **Operation** column to enter the remote configuration page of the device. **Note** For detailed instructions on remote configuration, see the user manual of the device.
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 change the password for them together.

8.11.2 Add a Guidance Terminal by IP/Domain

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 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Guidance Terminal** on the left.
3. Click **Add**.
4. Set **Adding Mode** to **IP/Domain**.
5. Edit device connection and login information.

   Device Address

   IP address of the device.

   Device Port

   Port number of the device. The default port number is 8000.

   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 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 installer and/or end-user.

6. **Optional:** Switch on **Add Resource to Area** to import the resources of the device to an area.

Note

- You can import all the resources including cameras, alarm inputs, and alarm outputs, or specific cameras to the corresponding area.
- You can create a new area named after the device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the cameras.

7. **Optional:** If you choose to add resources to area, select a server in **Streaming Server** to get the video stream of the cameras via the server.

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.

8. **Optional:** If you choose to add resources to area, switch on **Video Storage** and select a storage location for recording.

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 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.

Note

Configure the Hybrid Storage Area Network, Cloud Storage Server, or pStor in advance, or its storage location cannot display in the drop-down list. You can click **Add New** to add a new Hybrid Storage Area Network, Cloud Storage Server, or pStor.

9. Set the recording schedule for the cameras.
   - Check **Get Device's Recording Settings** to get the recording schedule from the device and the cameras of the device will start recording according to the schedule.

- Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.

10. Finish adding the device.
    - Click **Add** to add the device and return to the device list page.
    - Click **Add and Continue** to add the device and continue to add other devices.
11. **Optional:** Perform further operations after adding the device.

Configure Device

Click ⚙ in the **Operation** column to enter the remote configuration page of the device.

Note

For detailed instructions on remote configuration, see the user manual of the device.

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 change the password for them together.

8.11.3 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/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. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Guidance Terminal** on the left.
3. Click **Add**.
4. Set **Adding Mode** to **IP Segment**.
5. Edit device connection and login information.

Device Address

Start IP address and end IP address.

Device Port

Port number of the devices. The default port number is 8000.

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 installer and/or end-user.

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

Note

- You can import all the resources including cameras, alarm inputs, and alarm outputs, or specific cameras to the corresponding area.
- You can create a new area named after the device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the cameras.

7. **Optional:** If you choose to add resources to area, select a server in **Streaming Server** to get the video stream of the cameras via the server.

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.

8. Set the recording schedule for the cameras.
   - Check **Get Device's Recording Settings** to get the recording schedule from the devices and the cameras of the devices will start recording according to the schedule.

- Uncheck **Get Device's Recording Settings** and set up recording schedule later. Refer to ***Configure Recording for Cameras on Current Site*** for details.

9. Finish adding the devices.
   - Click **Add** to add the devices and return to the device list page.
   - Click **Add and Continue** to add the devices and continue to add other devices.
10. **Optional:** Perform further operations after adding the devices.

Configure Device

Click ⚙ in the **Operation** column to enter the remote configuration page of the device.

Note

For detailed instructions on remote configuration, see the user manual of the device.

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 change the password for them together.

8.11.4 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 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. 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Guidance Terminal** on the left.
3. Click **Add**.
4. Set **Adding Mode** to **Port Segment**.
5. Edit device connection and login information.

   Device Address

Devices' IP address.

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 installer and/or end-user.

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

Note

- You can import all the resources including cameras, alarm inputs, and alarm outputs, or specific cameras to the corresponding area.
- You can create a new area named after the device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the cameras.

7. **Optional:** If you choose to add resources to area, select a server in **Streaming Server** to get the video stream of the cameras via the server.

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.

8. Set the recording schedule for the cameras.
   - Check **Get Device's Recording Settings** to get the recording schedule from the devices and the cameras of the devices will start recording according to the schedule.
   - Uncheck **Get Device's Recording Settings** and set up recording schedule later. Refer to ***Configure Recording for Cameras on Current Site*** for details.

9. Finish adding the devices.
   - Click **Add** to add the devices and return to the device list page.
   - Click **Add and Continue** to add the devices and continue to add other devices.
10. **Optional:** Perform further operations after adding the devices.

Configure Device

Click ⚙ in the **Operation** column to enter the remote configuration page of the device.

Note

For detailed instructions on remote configuration, see the user manual of the device.

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 change the password for them together.

8.11.5 Batch Add Guidance Terminals by Template

You can download a predefined template (a spreadsheet) 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. 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Guidance Terminal** on the left.
3. Click **Add**.
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. Finish adding the devices.

- Click **Add** to add the devices and return to the device list page.
- Click **Add and Continue** to add the devices and continue to add other devices.

9. **Optional:** Perform further operations after adding the devices.

Configure Device

Click ⚙ in the **Operation** column to enter the remote configuration page of the device.

Note

For detailed instructions on remote configuration, see the user manual of the device.

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 change the password for them together.

8.12 Add Guidance Screen

Guidance 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 guidance screen to the platform by specifying its LAN IP address.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Guidance Screen** on the left.
3. Click **Add**.
4. Select the type of the guidance screen in **Device Type**.
5. Specify the information about the guidance screen.

Note

Parameter items vary among different device types.

LAN IP Address

Specify the IP address of the device.

Device Port

Specify the port number of the device.

Name

Create a descriptive name for the device.

Manufacturer

Select the manufacturer of the device.

Note

Currently, the platform only supports Hikvision guidance screens.

Model

Select the model of the device.

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.

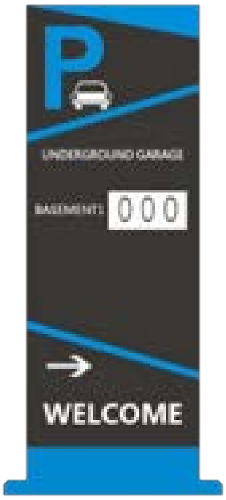


Figure 8-10 Entrance Guidance Screen - One Row

Number of Directions

The number of directions supported by the indoor 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.

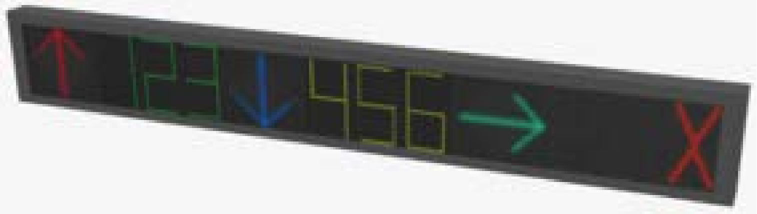


Figure 8-11 Indoor Guidance Screen - Three Directions

6. Click **Add** to finish adding the guidance screen, or click **Add and Continue** to continue adding another guidance screen.

What to do next

- After adding an entrance and exit guidance 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. See details in ***Add Lane*** .
- After adding an indoor guidance screen, you can set up a parking guidance system for your parking lot in Parking Guidance Configuration. See details in ***Parking Guidance Configuration*** .

8.13 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. In the top left corner of Home page, click ■ → **All Modules** → **General** → **Device Management** → **Devices and Servers** → **UVSS** to enter the UVSS management page.

   Note

   If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Device Management** on navigation bar to enter the device management page.

2. Click **Add** to enter the Add Under Vehicle Surveillance System page.
3. Set the required basic information such as device address, device port number, and device name.

   Device Address

   IP address of the UVSS.

   Device Port

   The device port of the UVSS. By default, the port is 8000.

Device Name

Enter name for the UVSS.

User Name

Enter the user name that can log into UVSS.

Password

Enter the password of the user that can log into UVSS.

4. **Optional:** Set the **Add Resource to Area** switch to on to import the resources of the added UVSS 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 area, you cannot perform the further configurations for the resources.

5. Finish adding the UVSS.
   - Click **Add** to finish adding the UVSS.
   - Click **Add and Continue** to add the current UVSS and continue to add more.
6. **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.
Delete Device	Check one or more added UVSS, and click **Delete** to delete the selected devices.
Search Device	Enter a keyword in the search box on the upper right corner of the page to quickly search the target device(s).

8.14 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.

8.14.1 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. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control 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 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.

5. In the Online Device area, select an active device to be added.
6. Click to open the Add Security Control Device window.
7. 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 installer 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 (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.

10. Click **Add**.

11. **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.

Add Detected Online Security Control Devices in a Batch

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. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select ☰ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. 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.
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 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.

5. In the Online Device area, select the active devices to be added.
6. Click to open the Add Security Control Device window.
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 installer 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 (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.

10. Click **Add**.
11. **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.

8.14.2 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. In the top left corner of Home page, 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 **Hikvision Private Protocol** as the Access Protocol.
5. Select **IP Address** as the adding mode.
6. Enter the required information.

   Note

   - By default, the device port is 8000.
   - For wireless security control panel, the default port is 80.

   Caution

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

   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
7. **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.
   - 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.

9. 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.

10. 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.

8.14.3 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. In the top left corner of Home page, 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 **Hikvision Private Protocol** as the Access Protocol.
5. Select **Hik-Connect DDNS** as the adding mode.
6. Select a device source.

   New Device

   Add a new device to both Hik-Connect and the system.

   Hik-Connect Device List

   Add devices managed by Hik-Connect to the system in a batch by getting the device list.
7. Set required parameters.

   Hik-Connect Server Address

   Enter the address of the Hik-Connect service. By default, it's ***https://open.ezvizlife.com***.

   Note

   If you select Hik-Connect Device List as 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.
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 (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.

10. 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.
11. **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.

8.14.4 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. In the top left corner of Home page, 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 **Hikvision Private Protocol** as the Access Protocol.

5. Select **IP Segment** as the adding mode.
6. 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 installer 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. 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.

8.14.5 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. In the top left corner of Home page, 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 **Hikvision Private Protocol** as the Access Protocol.
5. Select **Port Segment** as the adding mode.
6. 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 installer 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. 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.

8.14.6 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. In the top left corner of Home page, 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 **Hikvision ISUP Protocol** as the access protocol.

   Note

   To allow device registration via ISUP, you need to go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.
5. Select **Device ID** as the adding mode.
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 installer and/or end-user.
7. **Optional:** In the Recording Settings field, switch on **Video Storage** and select the storage location from the drop-down list.
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 (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.
10. 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.

11. 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.

8.14.7 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. In the top left corner of Home page, 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 **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To allow device registration via ISUP, you need to go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.
5. Select **Device ID Segment** as the adding mode.
6. Enter the required information, including the start device ID, the end device ID, and the ISUP login password.

7. **Optional:** In the Recording Settings field, set the **Video Storage** switch to on, and select the storage location from the drop-down list to store videos.
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 (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.
10. 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.
11. 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.

8.14.8 Add Security Control Devices in a Batch

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. In the top left corner of Home page, 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 **Hikvision Private Protocol** or **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To allow device registration via ISUP, you need to go to 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined template (excel file) in your PC.
7. Open the exported template file and edit the required information of the devices to be added on the corresponding column.
8. Click ... and select the template file.
9. **Optional:** In the Video Storage field, set the **Video Storage** switch to on, and select the storage location from the drop-down list to store video.

   Note

   This field displays when you select **Hikvision ISUP Protocol** as the access protocol.
10. **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.
11. 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.
12. 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.

8.15 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*.

8.15.1 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 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Dock Station** 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 5651.

   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. Two types of recording servers are supported: Hybrid Storage Area Network and pStor.

   Note

   You should configure the Hybrid Storage Area Network and pStor in advance, or its storage location cannot be displayed in the drop-down list.

   Backup Time

   The backup schedule of files uploaded by the dock station.

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 alias on the device list to edit the dock station.

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.

Copy Settings In the upper right corner of dock station editing panel, 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).

8.15.2 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 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 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Dock Station** 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. **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. Two types of recording servers are supported: Hybrid Storage Area Network and pStor.

   Note

   You should configure the Hybrid Storage Area Network and pStor in advance, or its storage location cannot be displayed in the drop-down list.

8. 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.
9. **Optional:** Perform the following operations.

   Edit Dock Station
   Click the dock station name on the device list to edit the dock station.

   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.

   Copy Settings
   In the upper right corner of dock station editing panel, 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).

8.15.3 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 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Dock Station** 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. **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. Two types of recording servers are supported: Hybrid Storage Area Network and pStor.

Note

You should configure the Hybrid Storage Area Network and pStor in advance, or its storage location cannot be displayed in the drop-down list.

Backup Time

The backup schedule of files uploaded by the dock station.

8. 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.
9. **Optional:** Perform the following operations.

Edit Dock Station	Click the dock station alias on the device list to edit the dock station.
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.

Copy Settings	In the upper right corner of dock station editing panel, 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).

8.15.4 Add Dock Stations in a Batch

When there are multiple dock stations to be added to HikCentral Professional, you can download a predefined template and fill in 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 in order to be able to connect the device to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Dock Station** 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 in the device list to edit the dock station.
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.

Copy Settings	On the upper right corner of dock station editing panel, 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).

8.15.5 Add Dock Station Group

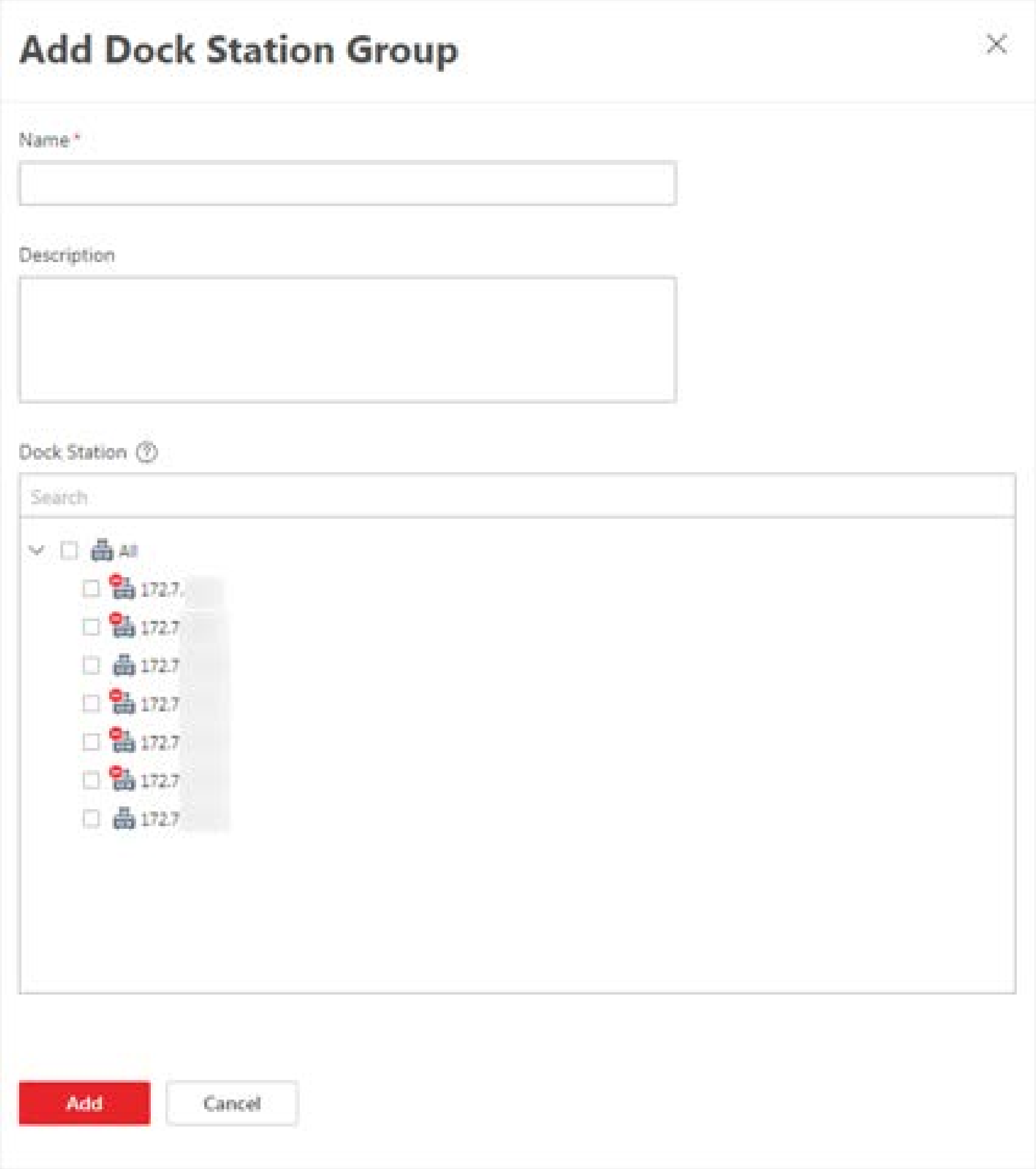
Dock station group is a group of persons who are linked to the same dock station(s). After linking persons to dock station(s), the videos and pictures on the persons' body cameras can be copied to these dock station(s).

Steps

Note

Up to 64 dock station groups can be added.

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Video** → **Dock Station** .
2. Click + to open Add Dock Station Group panel.



Add Dock Station Group

Name *

Description

Dock Station

Figure 8-12 Add Dock Station Group

3. Enter the basic information.

Name

Create a name for the dock station group.

Description

Enter the descriptive information for the group. E.g., This dock station group is for security guards in Team A.

Dock Station

Select dock station(s).

4. Click **Add**.

   The dock station group will be displayed in the dock station group list.

5. Add person(s) to the dock station group.

   Note

   Up to 200 persons can be added to one dock station group.

   1) Click **Add** to open the Add Person/Person Group window.
   2) Select a person group from the person group list in the window.
   3) Select specific person(s) or check **Select All** to select all persons in the group.
   4) Click **Add**.

      The person(s) will be displayed in the person list.

      Note

      If applying person(s) failed, the **Applying Failed** tag will be displayed on the person profile card. You can click the person profile card to view the failure details.

6. **Optional:** Perform following operations for added dock station groups.

   Edit Dock Station Group

   Select a dock station group in the dock station group list and click ✎ to edit it.

   Delete Dock Station Group

   Select a dock station group in the dock station group list and click 🗑 .

   Check Person Applying Failure Details

   Hover the cursor onto the ❗ and click **Details** to view the person applying failure details.

   Re-Apply Person(s)

   Hover the cursor onto the ❗ and click **Retry** to re-apply the person(s) to the dock station(s).

   Delete Person(s)

   Select person(s) from the person list, and then click **Delete** to delete the selected person(s). Or hover the cursor onto ⌄ next to **Delete**, and then click **Delete All** to delete all persons in the group.

   Only Display Person(s) Failed to Be Applied

   Check **Only Display Persons Failed to Be Applied** to filter the persons whose information is failed to be applied.

   Apply All Person(s)

   Click **Apply All** to apply the person(s) in the person list to the dock station(s) linked to the group.

8.16 Manage Digital Signage Terminals

On the Resource Management module, you can add digital signage terminals to the platform and perform further management and operation. There are two physical forms for the digital signage terminal. One is a terminal with screen, such as vertical digital signage and wall-mounted digital signage; the other (called digital signage player) is a station which integrate the function of information release, and it can connect with LED screen, LCD screen or jointed screen as the displaying screen.

8.16.1 Add Terminal

You can add terminals to the platform by multiple methods: adding online terminals, adding terminals by IP address, adding terminals by device serial No., and adding terminals by authentication code. After adding terminals to the platform, you can configure, manage and control the terminals.

Add Online Terminals

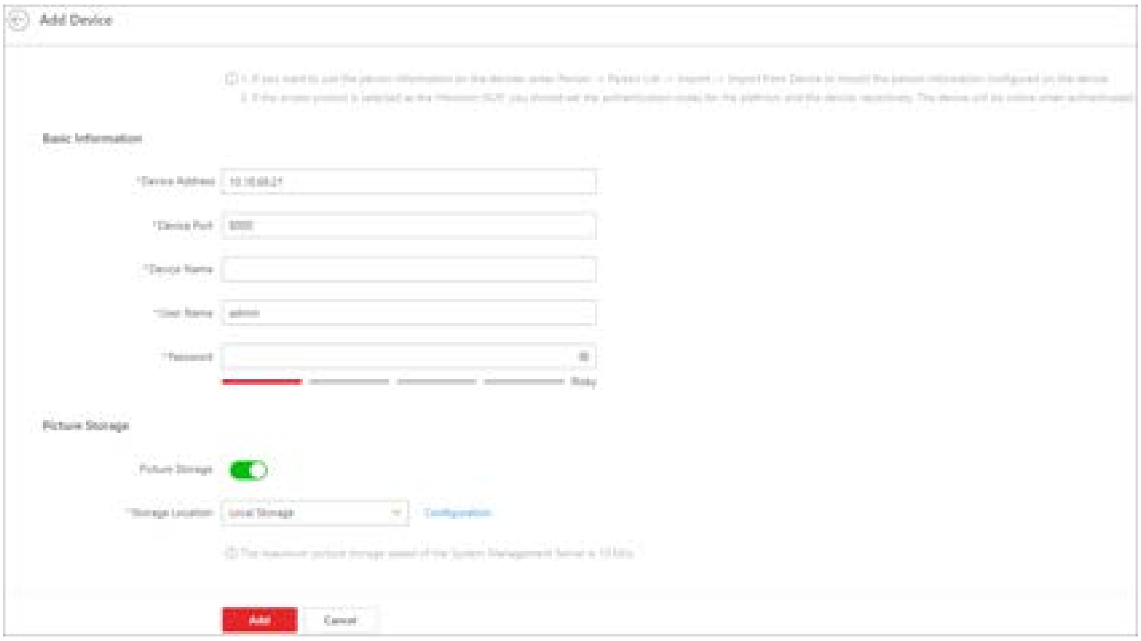
The platform can detect the online terminals (referred to as device in the following pages) in the same LAN as the server, and detect the device IP addresses. Based on this function, you can add the devices to the platform quickly. When the detected devices use the same user name and password, you can add the devices to the platform simultaneously.

Before You Start

Make sure you have downloaded and installed the Web Control on the login page.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Device and Server** → **Digital Signage Terminal** .
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 Device page.



Add Device

1. If you want to use the person information on the device enter Person -> Person List -> Import -> Import from Device to import the person information configured on the device.
2. If the access protocol is selected as the Hikvision ISUP, you should set the authentication mode for the platform and the device respectively. The device will be online when authenticated.

Basic Information

*Device Address: 10.16.68.21

*Device Port: 8000

*Device Name:

*User Name: admin

*Password: Risky

Picture Storage

Picture Storage: On

*Storage Location: Local Storage Configuration

The maximum picture storage speed of the System Management Server is 10 Mb/s.

Figure 8-13 Add Single Online Device

3. Set the basic information.

Device Address

The IP address of the device, which can be obtained automatically.

Note

If you add multiple devices simultaneously, this parameter will not be displayed.

Device Port

The port number of the device, which can be obtained automatically.

Note

If you add multiple devices simultaneously, this parameter will not be displayed.

Device Name

The name of the device, which can be used to describe the device function, location, etc.

Note

If you add multiple devices simultaneously, this parameter will not be displayed.

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 of the user 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 installer and/or end-user.

4. **Optional:** Enable **Picture Storage** to configure the storage location.

Local Storage

The pictures are stored in the SYS server.

Note

You can click **Configuration** to configure the storage location for pictures and files respectively. For details, refer to ***Configure Storage for Imported Pictures and Files*** .

pStor

The pictures are stored in the pStor server.

Note

In the attendance application scene, you should enable **Picture Storage**.

5. **Optional:** Set the time zone of the device.
   - Select **Get Device's Time Zone** to get the time zone of the device.
   - Select **Manually Set Time Zone (The time zone settings will be applied to the device automatically.)** to manually set the time zone of the device.
6. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add New** to add new area(s). For details, refer to ***Add Area for Current Site*** .

7. Click **Add**.
8. **Optional:** Perform the following operations after adding devices.

Change Password	Select one or more devices, and click **Change Password** to change the password of the selected devices.

Note

- You can only change the password of the online Hikvision devices.
- If multiple devices have the same password, you can change the password for multiple devices simultaneously.

Delete Devices

Select one or more devices, and click **Delete** to delete the selected devices.

Note

If the device which has been linked to the video wall is deleted, the corresponding video wall program cannot be released.

Set Time Zone

Select one or more devices, and click **Time Zone** to configure the time zone of the selected devices.

You can select **Get Device's Time Zone** or **Manually Set Time Zone (The time zone settings will be applied to the device automatically.)** according to your requirements.

Add Terminal by IP Address

If you know the IP address of the terminal (refereed to as device in the following pages) to be added, you can add the device to the platform by specifying the IP address, user name, password, etc.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Device and Server** → **Digital Signage Terminal** .
2. Click **Add** to enter the Add Device page.
3. Select the Access Protocol as **Hikvision Private Protocol**.

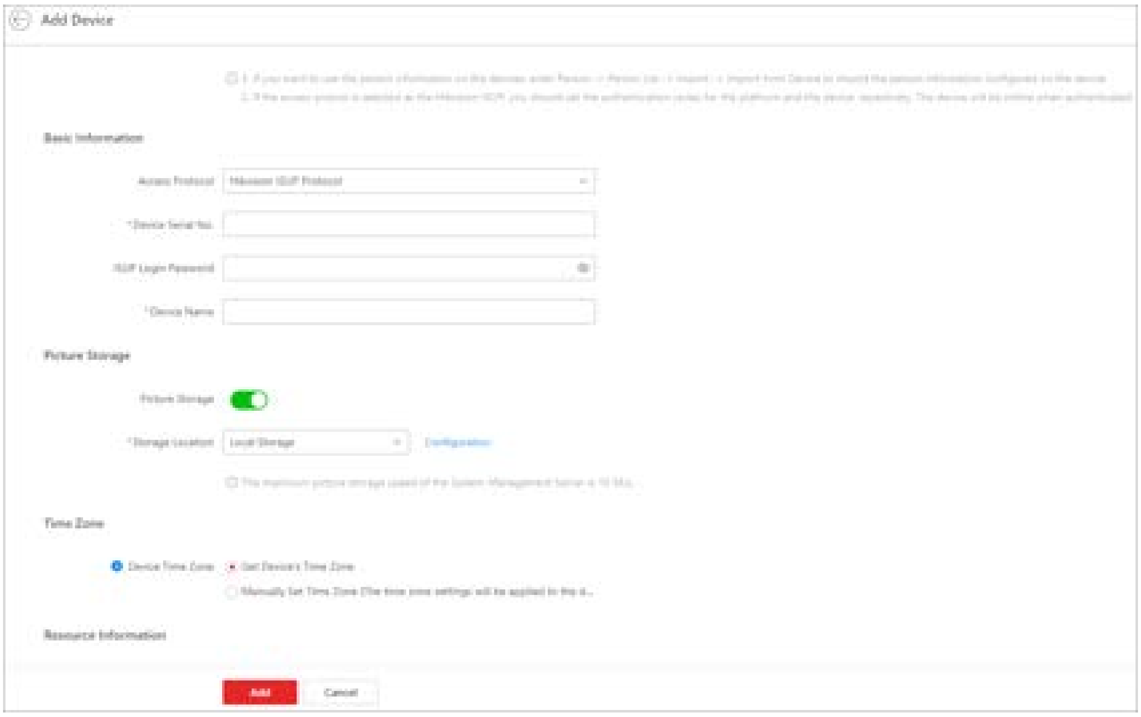


Figure 8-14 Add Terminal by IP Address

4. Set the basic 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.

Note

If you add multiple devices simultaneously, this parameter will not be displayed.

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 of the user 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 installer and/or end-user.

5. **Optional:** Enable **Picture Storage** to configure the storage location.

   Local Storage

   The pictures are stored in the SYS server.

   Note

   You can click **Configuration** to configure the storage location for pictures and files respectively. For details, refer to ***Configure Storage for Imported Pictures and Files*** .

   pStor

   The pictures are stored in the pStor server.

   Note

   In the attendance application scene, you should enable **Picture Storage**.
6. **Optional:** Set the time zone of the device.
   - Select **Get Device's Time Zone** to get the time zone of the device.
   - Select **Manually Set Time Zone (The time zone settings will be applied to the device automatically.) to manually set the time zone of the device.**
7. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

   Note

   You can create a new area by the device name or select an existing area. Also, you can click **Add New** to add new area(s). For details, refer to ***Add Area for Current Site*** .
8. Click **Add**.
9. **Optional:** Perform the following operations after adding devices.

   Change Password
   Select one or more devices, and click **Change Password** to change the password of the selected devices.

Note

- You can only change the password of the online Hikvision devices.
- If multiple devices have the same password, you can change the password for multiple devices simultaneously.

Delete Devices

Select one or more devices, and click **Delete** to delete the selected devices.

Note

If the device which has been linked to the video wall is deleted, the corresponding video wall program cannot be released.

Set Time Zone

Select one or more devices, and click **Time Zone** to configure the time zone of the selected devices.

You can select **Get Device's Time Zone** or **Manually Set Time Zone (The time zone settings will be applied to the device automatically.)** according to your requirements.

Add Terminal by Device Serial No.

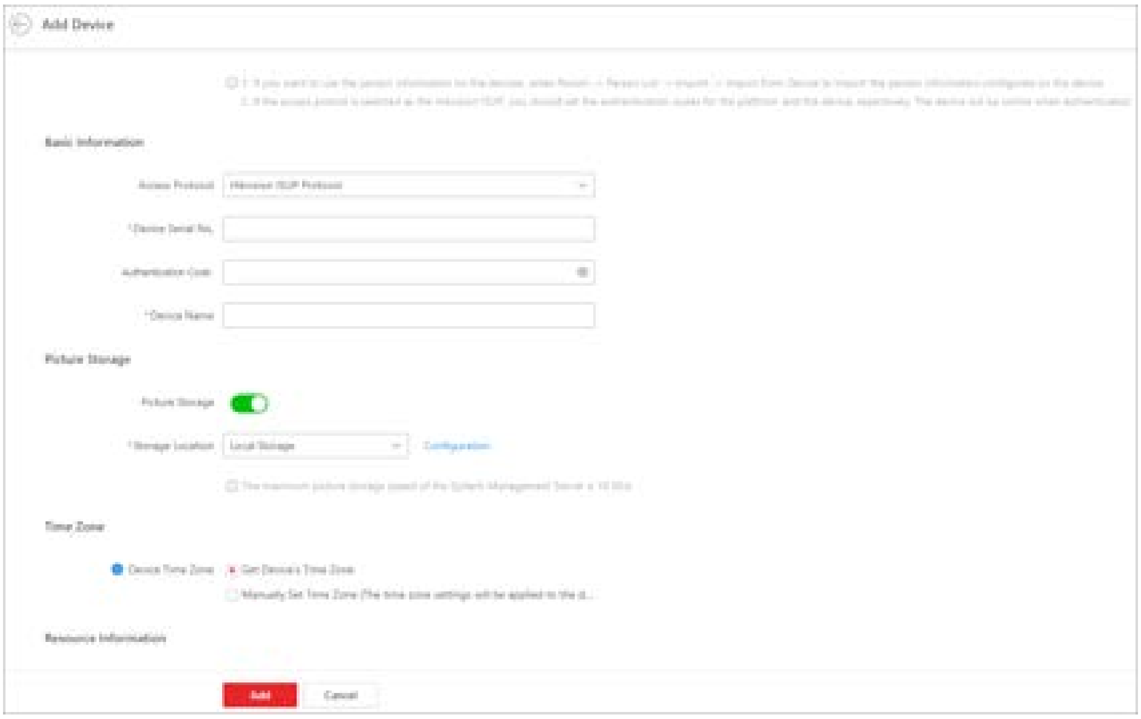
For the terminal (referred to as device in the following pages) supports ISUP protocol, you can add it to the platform by entering the device serial No., the authentication code, etc.

Before You Start

- Make sure you have activated the device. For details, refer to ***Create Password for Inactive Device(s)*** .
- Make sure you have configured the IP address for receiving device information on the platform, and select the current NIC as the address for receiving device information. Refer to ***Set IP Address for Receiving Device Information*** for details.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Device and Server** → **Digital Signage Terminal** .
2. Click **Add** to enter the Add Device page.



Access Protocol: Hikvision ISUP Protocol

*Device Serial No.

Authentication Code

*Device Name

Picture Storage: ●

*Storage Location: Local Storage Configuration

□ Manually Set Time Zone (The time zone settings will be applied to the d...

Figure 8-15 Add Terminal by Device Serial No.

3. Select **Hikvision ISUP Protocol** as the access protocol.
4. Set the basic information.

Device Serial No.

Enter the device serial No.

Authentication Code

Enter the authentication code of the device.

Note

The authentication code should contain 8 to 16 characters, including at least two of the following categories: upper case letters, lower case letters, and numbers.

Device Name

Name for the device, which can be used to describe the device function and location.

5. **Optional:** Enable **Picture Storage** to configure the storage location.

Local Storage

The pictures are stored in the SYS server.

Note

You can click **Configuration** to configure the storage location for pictures and files respectively. For details, refer to ***Configure Storage for Imported Pictures and Files*** .

pStor

The pictures are stored in the pStor server.

Note

In the attendance application scene, you should enable **Picture Storage**.

6. **Optional:** Set the time zone of the device.
   - Select **Get Device's Time Zone** to get the time zone of the device.
   - Select **Manually Set Time Zone (The time zone settings will be applied to the device automatically.) to manually set the time zone of the device.**
7. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add New** to add new area(s). For details, refer to ***Add Area for Current Site*** .

8. Click **Add**.
9. **Optional:** Perform the following operations.

Change Password

Select one or more devices, and click **Change Password** to change the password of the selected devices.

Note

- You can only change the password of the online Hikvision devices.
- If multiple devices have the same password, you can change the password for multiple devices simultaneously.

Delete Device

Select one or more devices, and click **Delete** to delete the selected devices.

Note

If the device which has been linked to the video wall is deleted, the corresponding video wall program cannot be released.

Set Time Zone

Select one or more devices, and click **Time Zone** to configure the time zone of the selected devices.

You can select **Get Device's Time Zone** or **Manually Set Time Zone (The time zone settings will be applied to the device automatically.)** according to your requirements.

What to do next

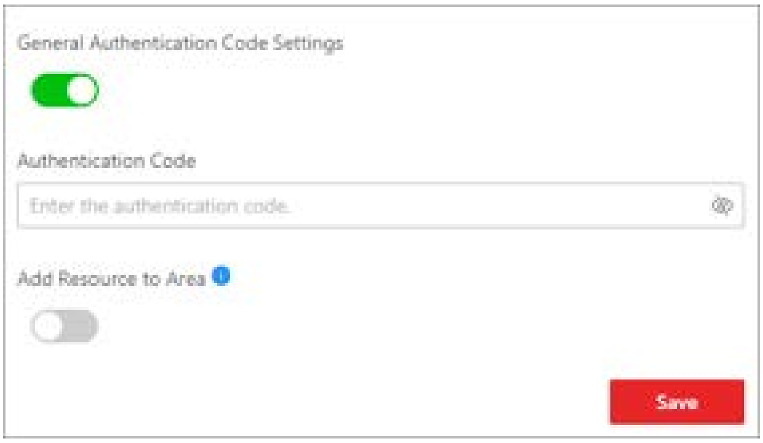
Enter the IP address of the platform, registration port No. (7600 by default), and the authentication code on the device's registration interface. Then the device will be added to the platform automatically.

8.16.2 Enable General Authentication Code

For the terminal which supports ISUP, you can set general authentication code on the platform. The authentication code is used for the terminal to register on the platform by ISUP. After enabling general authentication code on the platform, you should enter the authentication code on the terminal, which can then be added to the platform automatically.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** → **Device and Server** → **Digital Signage Terminal** .
2. Click **General Authentication Code Settings**.
3. Switch on **General Authentication Code Settings**.



General Authentication Code Settings

Authentication Code

Enter the authentication code.

Add Resource to Area

Figure 8-16 Set General Authentication Code

4. Enter the authentication code.

Note

The authentication code should contain 8 to 16 characters, including at least two of the following categories: upper case letters, lower case letters, and numbers.

5. **Optional:** Switch on **Add Resource to Area** to import the resources of the device to the area.
6. **Optional:** Select **Create Area by Device Name** or **Existing Area**.

Create Area by Device Name

Create a new area by the device name.

Existing Area

Select an existing area from the area list.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add New** to add new area(s). For details, refer to ***Add Area for Current Site*** .

7. Click **Save**.

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

Change Password

Select one or more devices, and click **Change Password** to change the password for the selected devices.

Note

- You can only change the password for online Hikvision devices.
- If multiple devices have the same password, you can change the password for them simultaneously.

Delete Device

Select one or more devices, and click **Delete** to delete the selected devices.

Note

If the device which has been linked to the video wall is deleted, the corresponding video wall program cannot be released.

Set Time Zone

Select one or more devices, and click **Time Zone** to configure the time zone of the selected devices.

You can select **Get Device's Time Zone** or **Manually Set Time Zone (The time zone settings will be applied to the device automatically.)** according to your requirements.

What to do next

After setting the general authentication code on the platform, you should enter the IP address of the platform, registration port number (7600 by default), and the authentication code on the terminal's registration interface. Then the terminal will be added to the platform automatically.

8.16.3 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 luminance, starting up Logo, etc.

Before You Start

Make sure at least one terminal is added to the platform, and make sure the terminal is online. Refer to ***Add Terminal*** for details.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules → Resource Management → Device and Server → Digital Signage Terminal**
2. Select one or multiple device(s), and then click **Display Settings** to enter the Display Settings page.
3. Set the device operation 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.

Starting Up Logo

After enabled, the logo will be displayed when the terminal starts up. The logo is set on the terminal locally.

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.

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 be entered to unlock the screen. The password is set on the terminal locally.

4. 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.

Timed Volume

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:** Click **Restore** to restore the displaying parameters to the default parameters.
6. Click **Save** to save the configuration.

8.16.4 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 terminal to the platform, you should configure the built-in camera parameters, such as device name, function, face similarity, etc.

Before You Start

Make sure at least one terminal is added to the platform, and make sure the terminal is online.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules → Resource Management → 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, select the channel No. of the built-in camera.
4. In the **Linked Device** area, the built in camera is displayed by default, click **Built in Camera** to enter the camera parameters settings page.
5. Set the parameters.

Device Name

The device name of the built-in camera.

Function

In the drop-down list, select **Attendance Check**,**Live View** or **Temperature Screening**.

Attendance Check

The attendance check function will be enabled, and the attendance data will be displayed in the attendance programs.

Live View

The live view of the camera will be displayed in the live view window of the normal programs.

Temperature Screening

Enable the temperature screening function of the camera. The real-time temperature screening is displayed on the temperature screening program.

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.

Enable Temperature Prompt

Check **Enable Temperature Prompt**, then when the camera detects abnormal temperature, the corresponding prompt will be displayed on the terminal.

Enable Mask Prompt

Check **Enable Mask Prompt**, then when the camera detects people without masks, the corresponding prompt will be displayed on the terminal.

Enable Face Location Prompt

Check **Enable Face Location Prompt**, then when the camera detects a face, a frame will be displayed on the terminal.

6. Click **Save** to save the above settings.

Link External Device to Terminal

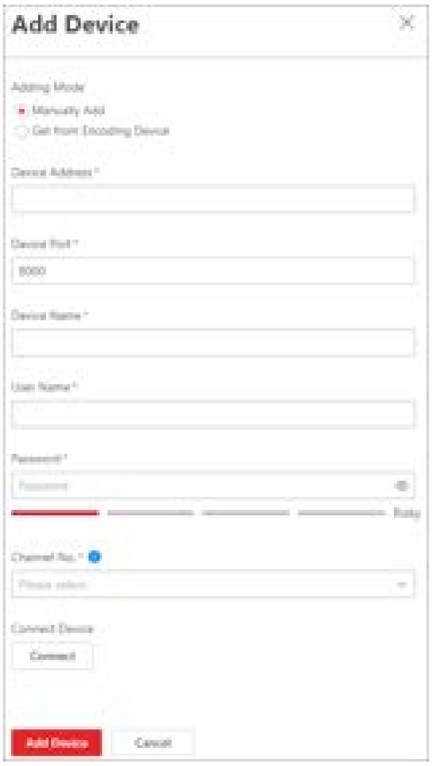
After adding terminals to the platform, you can link external devices such as cameras to the terminals for attendance, live view, or temperature screening.

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. In the top left corner of the Home page, select ▦ → **All Modules** → **Resource Management** → **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.



Add Device

Adding Mode

● Manually Add

○ Get from Encoding Device

Device Address *

Device Port *

8000

Device Name *

User Name *

Password *

Channel No. *

Please select

Connect Device

Figure 8-17 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 if you need to connect to the device.
- 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 Mode 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.

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.

8.16.5 Upgrade Old Device Firmware

For the terminal whose firmware version is old, the platform can automatically detect this terminal need to be upgraded, and you can manually upgrade the terminal's firmware.

In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Device and Server** → **Digital Signage Terminal** .

⚠ beside the terminal name indicates this terminal's firmware is old and firmware upgrade is required. Click ⚠ to enter the Upgrade Device page.

Select the terminal(s) you want to upgrade, and then click **Local File** to select the firmware package and then click **Upgrade** to finish upgrading.

8.17 Manage Smart Wall

Smart wall can provide security personnel with a rich visual overview of the areas you want to keep an eye on. Before displaying the video on smart wall, you need to set up smart wall firstly, and you can also edit, delete smart wall or manage decoding devices here.

This mainly includes the following:

- Decoding devices that can be added to the system and used for decoding the video stream from the encoding devices.
- Virtual smart wall that defines the layout and the name of the smart wall.
- Link between the decoding outputs of the decoding device and the windows of the smart wall.

8.17.1 Add Decoding Device

The decoding devices can be added to the system for linking with the smart wall. You can add online decoding devices with the IP addresses within SYS server's or Web Client's subnet, and can also add decoding devices by IP address, IP segment, or by port segment.

Add Online Decoding Device

The system can perform an automated detection for available decoding devices on the network where the Web Client or SYS 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.

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

Note

- For Google Chrome, you should install the SADP service according to the instructions and then the online device detection function is available.
- For Firefox, you should install the SADP service and import the certificate according to the instructions and then the online device detection function is available.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Smart Wall** on the left.
3. Click **Add** on Decoding Device panel to enter the Add Decoding Device page.
4. Select **Online Devices** as Adding Mode.
5. 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.
6. Select the device(s) to be added.

Note

- For the inactive device, you need to create the password for it before you can add it properly. For detailed steps, see .
- If the detected devices have the same password and user name, you can add multiple devices at a time. Otherwise, you can add them one by one.

7. Enter the required information.

   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 installer and/or end-user.

8. Finish adding the decoding device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
9. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output

Click › to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .

Edit Decoding Device

Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is.

Remote Configuration

Click ··· → ⚙ to set the remote configurations of the device.

Note

For detailed operations, see the user manual of the device.

Delete

Click ··· → ✕ to delete the device.

Add Decoding Device by IP Address

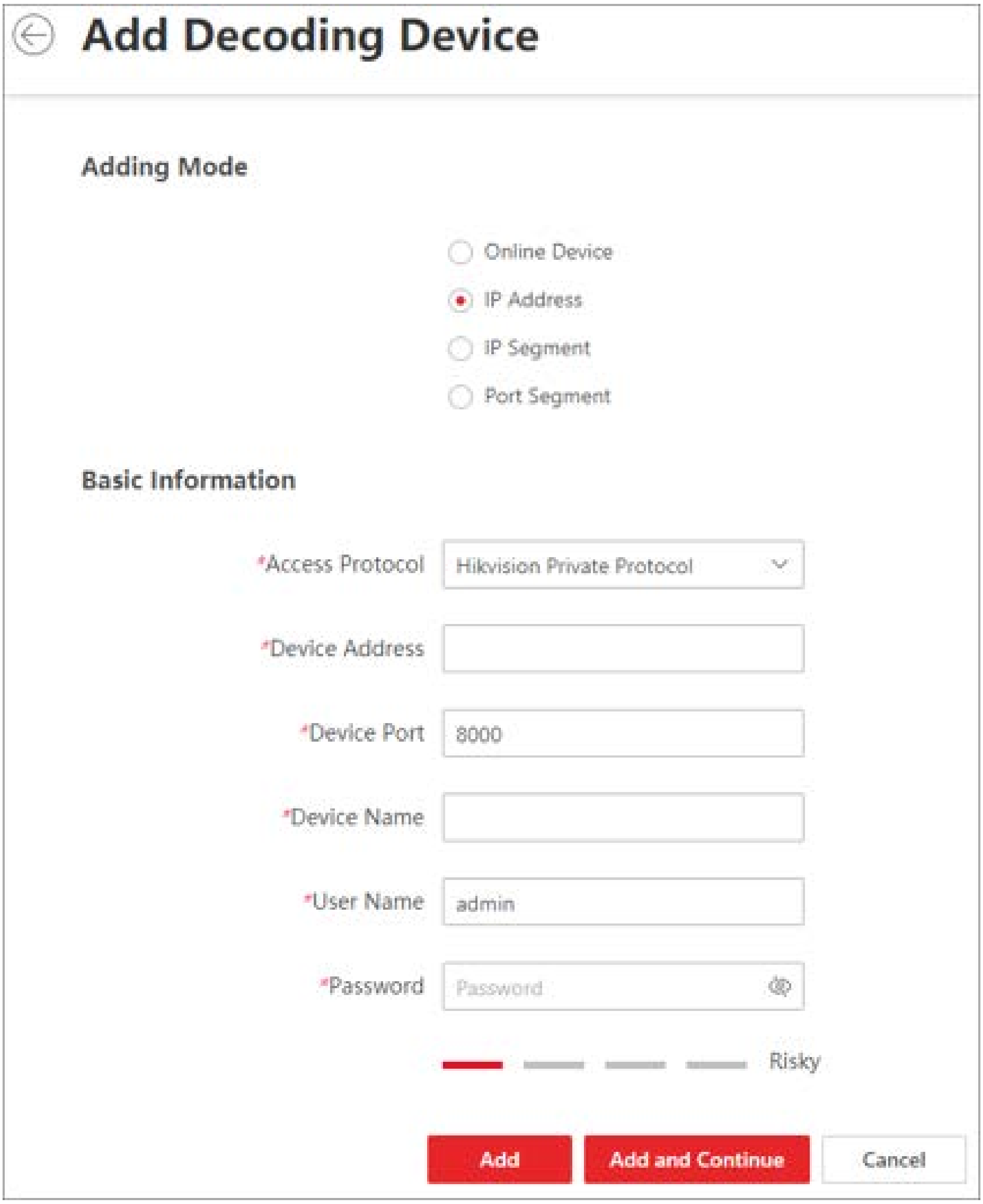
When you know the IP address of the decoding device to add, you can add the device to your system by specifying IP address, user name, password and other related parameters. This adding mode requires you to add the devices one by one, so it is a good choice if you only want to add a few devices and know all the details mentioned above.

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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Smart Wall** on the left.
3. Click **Add** to enter the Add Decoding Device page.



Add Decoding Device

Adding Mode

○ Online Device

● IP Address

○ IP Segment

○ Port Segment

Basic Information

*Access Protocol	Hikvision Private Protocol
*Device Address	
*Device Port	8000
*Device Name	
*User Name	admin
*Password	Password

Risky

Figure 8-18 Add Decoding Device Page

4. Select **IP Address** as Adding Mode.
5. Enter the required information.

   Access Protocol

   Select **Hikvision Private Protocol** to add the devices.

Device Address

The IP address of the device.

Device Port

The port number on which to scan. The default is 8000.

If the device is located behind a NAT (Network Address Translation)-enabled router or a firewall, you may need to specify a different port number. In such cases, remember to configure the router/firewall so it maps the port and IP address used by the device.

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 installer and/or end-user.

6. Finish adding the device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
7. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output
Click › to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .

Edit Decoding Device
Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is.

Remote Configuration
Click ··· → ⚙ to set the remote configurations of the device.

Note

For detailed operations, see the user manual of the device.

Delete	Click ··· → ✕ to delete the device.

Add Decoding Devices by IP Segment

If multiple decoding devices to add have the same port number, user name and password, but have different IP addresses, which are within a range, you can select this adding mode, and specify the IP range where your devices are located, and other related parameters. The system will scan from the start IP address to the end IP address for the devices in order to add them quickly.

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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Smart Wall** on the left.
3. Click **Add** to enter the Add Decoding Device page.
4. Select **IP Segment** as Adding Mode.
5. Enter the required information.

   Access Protocol

   Select **Hikvision Private Protocol** to add the devices.

   Device Address

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

   Device Port

   The same port number of the devices. By default, the device port No. is 8000.

   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 installer and/or end-user.

6. Finish adding the device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
7. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output

Click › to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .

Edit Decoding Device

Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is.

Remote Configuration

Click ··· → ⚙ to set the remote configurations of the device.

Note

For detailed operations, see the user manual of the device.

Delete

Click ··· → ✕ to delete the device.

Add Decoding Devices by Port Segment

When multiple decoding devices to add have the same IP address, user name and password, but have different port numbers, which are within a range, you can select this adding mode and specify the port range, IP address, user name, password, and other related parameters to add them.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. 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 ■ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Smart Wall** on the left.
3. Click **Add** to enter the Add Decoding Device page.
4. Select **Port Segment** as Adding Mode.
5. Enter the required information.

Access Protocol

Select **Hikvision Private Protocol** to add the devices.

Device Address

The same IP address where the devices are located.

Device Port

Enter the start port number and the end port number on which to scan.

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 installer and/or end-user.

6. Finish adding the device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.

   After adding the decoding device, the device will display in the list on Decoding Device panel.
7. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output

Click › to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .

Edit Decoding Device

Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is.

Remote Configuration

Click ··· → ⚙ to set the remote configurations of the device.

Note

For detailed operations, see the user manual of the device.

Delete	Click ··· → ✕ to delete the device.

8.17.2 Configure Cascade

In some actual scenarios for large screen display, the screen number of the smart wall will exceed the decoding output number of one decoder, or the cross-decoder functions such as roaming and spanning are required. You can cascade two decoders with video wall controller to meet various display demands.

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 decoders' interfaces have be connected with the video wall controller's using the matched wires.
- The decoders and video wall controller are added to the HikCentral Professional. Refer to ***Add Decoding Device*** for details.

Perform this task when you need to configure cascade for the decoding devices as follows.

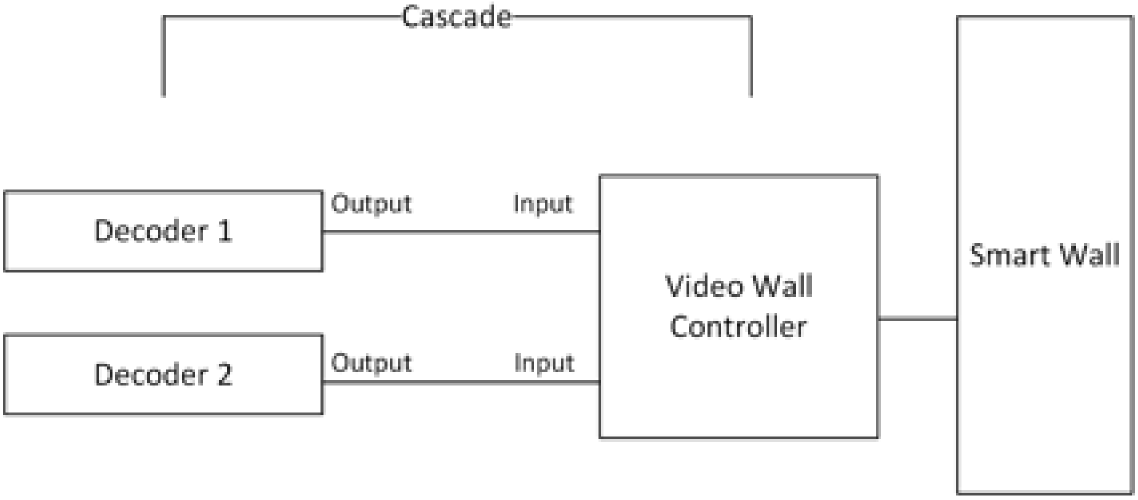


Figure 8-19 Cascade

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Smart Wall** on the left.
3. Click ⧉ behind the added video wall controller to enter the Cascading page.

Note

Only video wall controller DS-C10S and DS-C10S-T can support this function.

4. Select the signal channel of the video wall controller and click .
5. Select the decoding output of the decoders to set it as the signal input of the video wall controller.

Note

If the decoders are cascaded with video wall controller, the spared decoding outputs of the decoders cannot be used to display on smart wall any more.

6. Click **Save** to save the cascade.

Result

After configuring cascade, you need to add a smart wall and link the decoding outputs of the video wall controller to display the signal outputs of the two decoders on the smart wall.

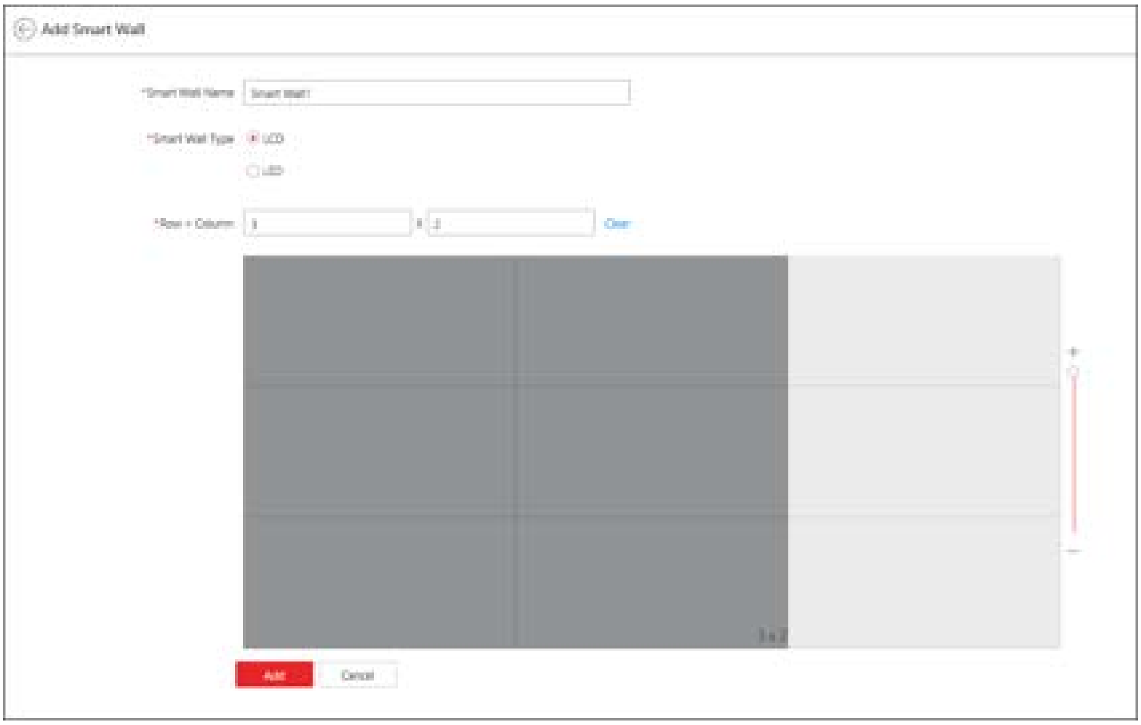
8.17.3 Add Smart Wall

You can add the smart wall to the system and configure its row and column.

Perform this task when you need to add a smart wall to the system.

Steps

1. In the top left corner of Home page, select → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Smart Wall** on the left.
3. Click **Add** on Smart Wall panel to open the Add Smart Wall dialog.



*Smart Wall Name: Smart Wall1

*Smart Wall Type: ● LCD ○ LED

*Row × Column: 3 × 2

Figure 8-20 Add Smart Wall Dialog

4. Set the name for the smart wall.
5. If the smart wall type is **LED**, select the max. resolution of the single output in the drop-down list.

Note

You can also select **Customize** to customize the resolution.

6. Set the row number and the column number.
7. Click **Add**.
8. **Optional:** Perform the following operations after adding the smart wall.

Link Decoding Output with Window	For details about the operations, see ***Link Decoding Output with Window*** .
Edit Smart Wall	Click ✎ to edit the name of the smart wall.
Delete Smart Wall	Click × to delete the smart wall.
Set Default Stream Type	For details about setting the default stream type for cameras, refer to ***Set Default Stream Type for Cameras on Smart Wall*** .

8.17.4 Link Decoding Output with Window

After adding the decoding device and smart wall, you should link the decoding device's decoding output to the window of the smart wall.

Perform this task when you need to link the decoding output to the smart wall.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Smart Wall** on the left.
3. Click › in front of the decoding device to show the decoding outputs.
4. Click › in front of the smart wall to show the windows.
5. Drag the decoding output from the Decoding Device panel to the display window of the smart wall, to configure the one-to-one correspondence.

Note

You can also press the Ctrl key and Alt key at the same time, and select two decoding outputs. All decoding outputs between the two outputs will also be selected, then you can drag all outputs to the display window.

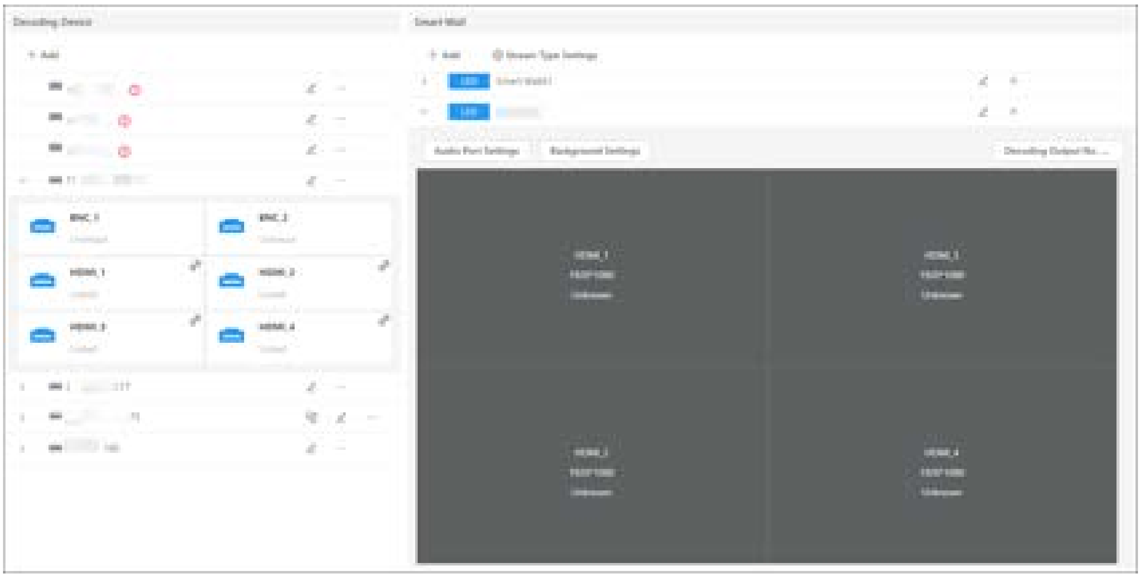


Figure 8-21 Link Decoding Device with Window

6. **Optional:** Perform the following operations after linking the decoding output with the window.

Cancel Linkage	Click ☒ to release the linkage.
Set Audio Port	Click **Audio Port Settings** to select the audio port.

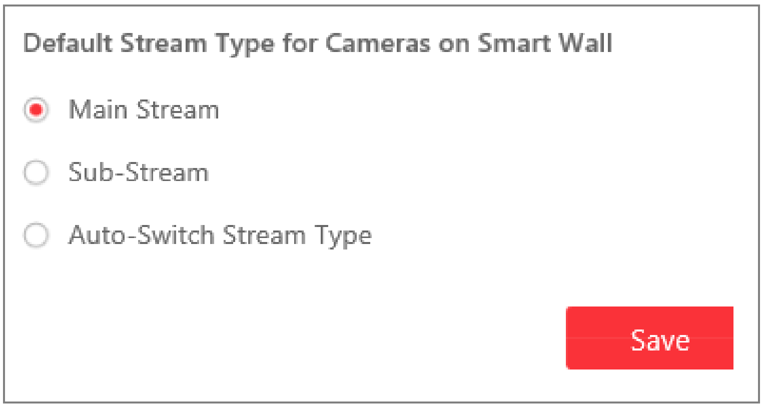
Set Background
Click **Background Settings** to set the background color of the smart wall.

Set Decoding Output No. Displayed on Screen
Click **Decoding Output No. Displayed on Screen**. After clicking, the displaying duration of decoding output No. on the screen is from 30 to 60 seconds.

8.17.5 Set Default Stream Type for Cameras on Smart Wall

According to the actual screen size, display effect, network bandwidth, or other requirements, you can set the default stream type for cameras displayed on smart wall, including main stream and sub-stream. You can also set a threshold about window division mode to switch between main stream and sub-stream automatically. The default stream type is effective for all cameras decoded and displayed on smart wall firstly.

In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** . Click **Device and Server** → **Smart Wall** on the left to enter the smart wall management page. On the Smart Wall area, click **Stream Type Settings** to select the default stream type as follows.



Default Stream Type for Cameras on Smart Wall

● Main Stream

○ Sub-Stream

○ Auto-Switch Stream Type

Figure 8-22 Set Default Stream Type for Cameras on Smart Wall

Main Stream

Main stream provides higher quality video, higher resolution, but brings about higher bandwidth usage. If you select main stream as default type, the live video streams of all cameras will be decoded and displayed on smart wall in main stream mode.

Sub-Stream

Sub-stream can save on bandwidth, but the video quality is lower than main stream. If you select sub-stream as default type, the live video streams of all cameras will be decoded and displayed on Smart Wall in sub-stream mode.

Auto-Switch Stream Type

If a window's proportion of the smart wall is larger than the configured threshold, the stream type will be main stream. If the proportion is smaller than the threshold, it will be switched to sub-stream. For example, if you set the threshold as ¼, when the window division turns to 5-window from 2-window, the stream type will be switched from main-stream to sub-stream.

8.18 Manage IP Speakers

You can add the IP speakers to the platform via multiple methods such as adding by IP address and IP segment. After that, you can manage the added IP speakers, including editing and deleting devices, configuring devices remotely, changing devices' passwords, etc.

8.18.1 Add IP Speaker by IP Address

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

Before You Start

Make sure the IP speakers to be added 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 ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **IP Speaker** on the left.
3. Click **Add** to enter the Add IP Speaker page.
4. Select **Hikvision Private Speaker Protocol** as the Access Protocol.
5. Select **IP Address** as the Adding Mode.
6. Enter the required information.

   Device Address

   The IP address of the device.

   Device Port

   The port number of the device. By default, it 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.

   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 the platform 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 installer and/or end-user.

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

Note

- You can import all resources (including alarm inputs, alarm outputs, and speaker units) to the area, or click **Specified Speaker Units** and select one or more speaker units from the list to add the selected resources to the area.
- You can create a new area by the device name or select an existing area from the area list. Also, you can click **Add New Area** to add a new area. For details about adding a new area, refer to ***Add Area*** .

8. Add the device.
   - Click **Add** to add the current device and return to the device list.
   - Click **Add and Continue** to add the current device and continue to add other device(s).
9. **Optional:** Perform the following operations.

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.

Format SD Card

Click 💾 to format the SD card of the IP speaker.

Search 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).

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.

8.18.2 Add IP Speakers in a Batch

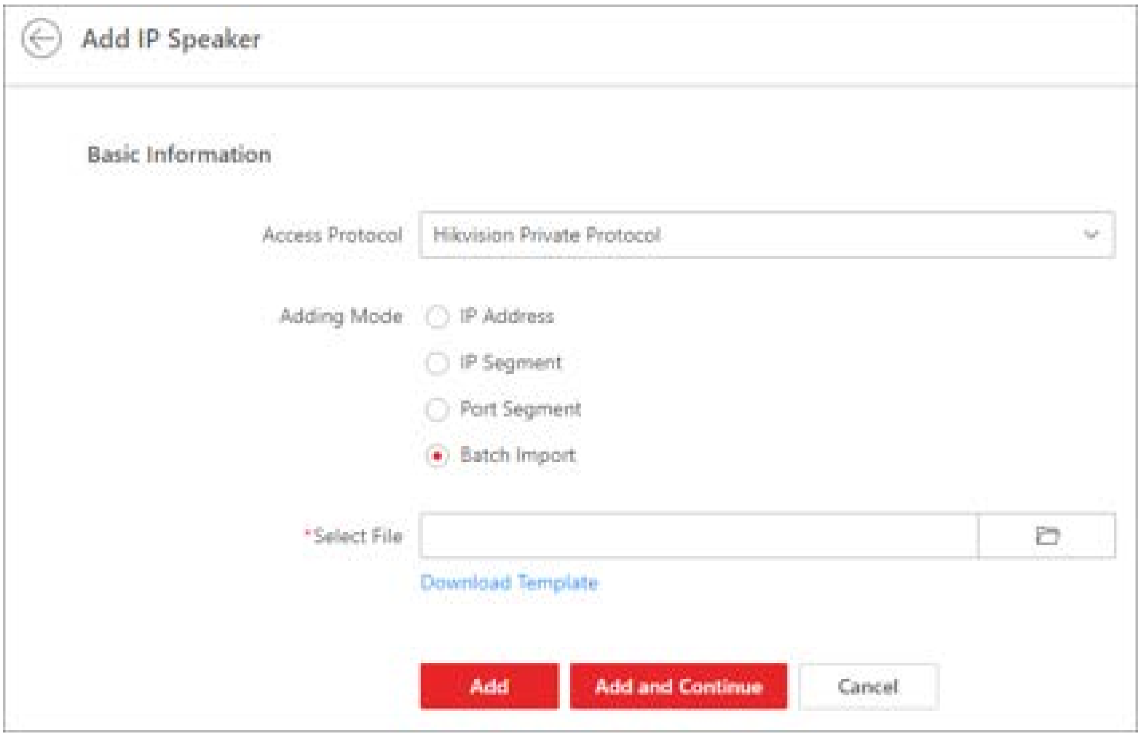
When there are multiple IP speakers to be added, you can edit the predefined template containing the required device information, and import the template to HikCentral Professional to add devices in a batch.

Before You Start

Make sure the IP speakers to be added 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 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **IP Speaker** on the left.
3. Click **Add** to enter the Add IP Speaker page.
4. Select **Hikvision Private Speaker Protocol** as the Access Protocol.
5. Select **Batch Import** as the Adding Mode.



Add IP Speaker

Basic Information

Access Protocol: Hikvision Private Protocol

Adding Mode: ○ IP Address ○ IP Segment ○ Port Segment ● Batch Import

*Select File:

Figure 8-23 Batch Add IP Speakers

6. Click **Download Template** and save the predefined template to your PC.
7. Open the template file and enter the required information of the devices in the corresponding column.
8. Click 🗀 and select the edited file.
9. Add the devices.
    - Click **Add** to add the current devices and return to the device list.
    - Click **Add and Continue** to add the current devices and continue to add other devices.
10. **Optional:** Perform the following operations.

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.

Format SD Card

Click to format the SD card of the IP speaker.

Search Device

Enter a keyword in the search box in the top 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.

8.19 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.

8.19.1 Add a Detected Online Security Inspection Device

You can add a single detected online security inspection device to the platform.

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. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **General** → **Resource Management** .
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 🟥 → **All Modules** → **General** → **System Configuration** → **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 installer 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.

Cloud Storage Server

The video files will be stored in the Cloud 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. Refer to ***Configure Recording for Cameras on Current Site*** for details.
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.
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.

8.19.2 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. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the upper-left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Inspection Device** .
3. Click **Add** to enter the Add Security Inspection Device page.
4. Select **Walk-Through Metal Detector** or **Analyzer** 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 🟥 → **All Modules** → **General** → **System Configuration** → **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 installer 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.

   Cloud Storage Server

   The pictures will be stored in the Cloud 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.

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.

8.19.3 Add Security Inspection Device by IP/Domain

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. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the upper-left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Inspection Device** .
3. Click **Add** to enter the Add Security Inspection Device page.
4. Select **Walk-Through Metal Detector** or **Analyzer** 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 installer 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.

    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.

    Cloud Storage Server

    The video files will be stored in the Cloud 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. Refer to ***Configure Recording for Cameras on Current Site*** for details.
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.
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.

8.20 Network Transmission Device Management

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 Control Client 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).

8.20.1 Add Detected Online Network Transmission Devices

The system can perform an automated detection for available network transmission device s 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.

Note

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

Add a Detected Online Network Transmission Device

When you want to add one of the detected online devices or add some of these devices with different user names and passwords, you need to select only one device every time to add it to HikCentral Professional. The IP address, port number and user name will be recognized automatically, which can reduce some manual operations in a way.

Before You Start

Make sure the network device (switch, bridge or fiber converter) you are going to use is 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 device to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Network Transmission Device** on the left panel.
3. 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 be listed.

   Local Network

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

   Device Address

   The IP address of the device, which is filled in automatically.

   Device Port

   The port number of the device, which is filled in automatically.

   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 installer and/or end-user.

Country Code

The country code defines the country/region where device will be used.

Note

- You should read and agree the disclaimer to set the country code.
- The country code is required for wireless bridges.
- You cannot edit the country code of the added device on its details page.

7. Click **Add**.
8. **Optional:** Perform the following operations after adding the device.

Remote Configuration

Click ⚙ in the Operation column 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 **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.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

Add Detected Online Network Transmission Devices in a Batch

For the detected online transmission network devices, if they have the same user name and password, you can add multiple devices to HikCentral Professional at a time.

Before You Start

Make sure the network devices (switches, bridges or fiber converters) 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Network Transmission Device** on the left.
3. 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 be listed.

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
4. In the Online Device area, select the devices to be added.
5. Click **Add to Device List** to enter the Add Online Device window.
6. Enter the user name, password, and country code.

   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 installer and/or end-user.

Country Code

The country code defines the country/region where device will be used.

Note

- You should read and agree the disclaimer to set the country code.
- The country code is required for wireless bridges.
- For the added device, its country code cannot be edited on the device details page.

7. Click **Add**.
8. **Optional:** Perform the following operations after adding devices.

Remote Configuration

Click ⚙ in the Operation column 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 **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.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

8.20.2 Add Network Transmission Device by IP Address

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

Before You Start

Make sure the network device (switch, bridge or fiber converter) you are going to use is 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 device to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Network Transmission Device** on the left panel.
3. Click **Add** to enter the Add Network Transmission Device window.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

   Device Address

   IP address of the device.

   Device Port

   The default device port number 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.

   User Name

   The administrator account which is created when activating the device, or the non-administrator account, such as operator. When adding device by non-administrator, the permission 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 installer and/or end-user.

Country Code

The country code defines the country/region where device will be used.

Note

- You should read and agree the disclaimer to set the country code.
- The country code is required for wireless bridges.
- Once the device is added, its country code cannot be edited on the device details page.

6. Finish adding the device.
   - Click **Add** to add the current device and back to the device list page.
   - Click **Add and Continue** to finish adding the current device and continue adding other devices.
7. **Optional:** Perform the following operations after adding devices.

Remote Configuration

Click in the Operation column 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 **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.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

8.20.3 Import Network Transmission Devices in a Batch

If there are a large number of devices to be added, you can enter the device information in the pre-defined template and upload the template to add the network transmission devices in a batch.

Before You Start

Make sure the network devices (switches, bridges or fiber converters) 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Network Transmission Device** on the left panel.
3. Click **Add** to enter the Add Network Transmission Device window.
4. Select the adding mode as **Batch Import**.
5. Click **Download Template** to download the template to the local PC.
6. Open the downloaded template file, and enter the required device information.
7. Click 📁 to select the edited template file.
8. Finish adding the device.
   - Click **Add** to add the current device and back to the device list page.
   - Click **Add and Continue** to finish adding the current device and continue adding other devices.
9. **Optional:** Perform the following operations after adding devices.

Remote Configuration
Click ⚙ in the Operation column 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 **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.

Set the System Connected Device
Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

8.21 Upgrade Device Firmware

You can upgrade the firmwares of the devices added to the system via the current Web Client or Hik-Connect.

Via Current Web Client

The following devices are supported to be upgraded the firmwares via the current Web Client:

Table 8-1 Device List

No.	Device Type
1	Camera
2	NVR (Network Video Recorder)
3	DVR (Digital Video Recorder)
4	Decoding Device
5	Access Control Device
6	Card Reader
7	Security Control Panel (including AX Security Control Panel)
8	Security Radar
9	Indoor Station
10	Door Station **Note** Upgrading the card reader linked to the door station is not supported.
11	Main Station
12	Guidance Terminal

Note

You can also upgrade the cameras access to the NVR in a batch.

Via Hik-Connect

The following devices are supported to be upgraded the firmwares via Hik-Connect:

Table 8-2 Device List

No.	Device Type
1	Camera
2	NVR
3	DVR
4	Indoor Station
5	Door Station **Note** Upgrading the card reader linked to the door station is not supported.
6	Main Station
7	Digital Signage Terminal

Note

You can also upgrade the cameras linked to the NVR in a batch.

8.21.1 Upgrade Device Firmware via Current Web Client

You can upgrade device firmware via the current Web Client.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Firmware Upgrade** on the left.
3. Select the **Via Current Web Client** tab.
4. In **Upgrade By** field, select the upgrade method.
5. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.
6. Select a upgrade package from the local computer and then click **Next**.

   The upgradable devices will be displayed.
7. **Optional:** Filter devices by device type, device firmware version, or device model.
8. Select device(s) and then click **Next**.
9. Select a upgrade schedule to upgrade the selected device(s).
   - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.
   - Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).

10. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be open.
11. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

8.21.2 Upgrade Device Firmware via Hik-Connect

You can upgrade device firmware via Hik-Connect, which is a cloud service.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Firmware Upgrade** on the left.
3. Select the **Via Hik-Connect** tab.
4. In **Upgrade By** field, select the upgrade method.
5. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.
6. Click **Next**.
7. 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.

   The upgradable devices will be displayed.
8. Select device(s) and click **Next** to enter the upgrade schedule page.
9. Select a upgrade schedule to upgrade the selected device(s).
   - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.
   - Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).
10. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be open.
11. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

8.21.3 Upgrade Device Firmware via FTP

You can upgrade device firmware via FTP.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Firmware Upgrade** on the left.
3. Select the **Upgrade Firmware via FTP** tab.
4. Set the basic information.

   FTP Server Address

   The address of FTP server, where you have uploaded the firmware upgrade package.

   Port

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

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

   Path

   If you saved 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.
5. Click **Next**.
6. Select an upgrade package from the local PC and then click **Next**.

   The upgradable device list will be displayed.
7. **Optional:** Filter devices by device type, device firmware version, or device model.
8. Select the device(s) and then select **Upgrade Schedule** from the drop-down list as upgrade now or custom.
9. Click **OK** to save the firmware upgrade settings.

   The upgrade task list will be displayed.
10. **Optional:** In the upper-right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.
11. **Optional:** In the upgrade task list, click ✕ in the Operation column to delete the upgrade task.

8.22 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*** .

8.22.1 Reset Device Password

If you forget the password you use to access the online device, you can request to have 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. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
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 icon ↺ in the Operation column of an active device.

   The Reset Password window pops up.
4. Click **Export File** to save the device file on your PC.
5. Send the file to the technical support.

Note

For the following operations about resetting the password, contact the technical support.

Caution

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

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

8.22.2 Restore Device's Default Password

For some encoding 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 (cameras, DVR, etc.) 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.

Steps

1. In the top left corner of Home page, select → **All Modules** → **General** → **Resource Management** .
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 installer and/or end-user.

8.23 Manage Recording Server

You can add the Recording Server to the system for storing the videos and pictures. Currently, the Recording Server supports 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

NVR can only be used to store pictures.

8.23.1 Add pStor

You can add a pStor server as a recording server to the HikCentral Professional for storing the videos and pictures.

Before You Start

- Make sure the pStor servers 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Recording Server** on the left panel.
3. Click **Add** to enter the Add Recording Server page.

   Note

   If the NTP server is not configured, a prompt message will appear on the top of the page. You can click **Configure** to set the time synchronization.
4. Select **pStor**.
5. Enter the network parameters.

   Address

   The pStor server's IP address in LAN that can communicate with SYS.

   Control Port

   The control port No. of the pStor server. If it is not changed, use the default value.

   Network Port

   The network port No. of the pStor server. If it is not changed, use the default value.

Signaling Gateway Port

The signaling gateway port No. of the pStor server. If it is not changed, use the default value.

6. Enter the user's access key and secret key of the pStor server for downloading pictures via Control Client.

Note

You can download these two keys on the pStor server's Web Client page.

7. **Optional:** Switch on **Enable Picture Storage** for storing pictures in this pStor.

Note

You should set picture downloading port No., which is used to download pictures via Control Client.

8. **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.
9. Enter the name, user name, and password of the pStor 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 installer and/or end-user.

10. **Optional:** In Storage Information field, switch on **Custom Video Copy-Back** and set the start time for copy-back.
11. Finish adding the server.
    - Click **Add** to add the server and back to the server list page.
    - Click **Add and Continue** to save the settings and continue to add other servers.
12. **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 and view its storage and camera information.

Delete Server
Select the server(s) from the list, and click **Delete** to remove the selected server(s).

Configure Server
Click ⚙ in the Operation column to enter the login page of the pStor server. You can log in and configure the pStor server.

Search Server
Enter keyword(s) in the search box in the top right corner to search for the target server(s).

8.23.2 Add Hybrid Storage Area Network

You can add the Hybrid Storage Area Network (hereafter simplified as Hybrid SAN) as a recording server to the HikCentral Professional for storing the video files and pictures.

Before You Start

Make sure the Hybrid SANs 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Recording Server** on the left panel.
3. Click **Add** to enter the Add Recording Server 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.
4. Select **Hybrid Storage Area Network**.
5. Enter the network parameters.

   Address

   The server's IP address in LAN that can communicate with SYS.

   Control Port

   The control port No. of the server. If it is not changed, use the default value.

   Network Port

   The network port No. of the server. If it is not changed, use the default value.

   File Transmission Port

   The file transmission port number of the server. If it is not changed, use the default value.
6. **Optional:** Enable picture storage function for storing pictures in this Hybrid SAN.
   1) Switch on **Enable Picture Storage**.
   2) Set picture downloading port number for downloading pictures via the Control Client. If the picture downloading port No. is not changed, use the default value.
   3) Set signaling gateway port number. If the picture downloading port number is not changed, use the default one.
   4) Enter the access key and secret key.

   Note

   The access key and secret key are used to download pictures via the Control Client. If required, you can contact the technical support to get them.
7. **Optional:** Switch on **Enable WAN Access** to access the server via WAN.

Note

When enabled, you should set the corresponding parameters including IP address of the server, the control port No., the network port No., etc.

8. Enter the name, user name, and password of the 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 installer and/or end-user.

9. **Optional:** In Storage Information field, switch on **Custom Video Copy-Back** and set the start time and end time for copy-back.
10. **Optional:** In Storage Information field, switch on **Video Expiration** and set the video expiration day(s).

    The oldest videos will be deleted automatically after the specified retention period.
11. Finish adding the server.
    - Click **Add** to add the server and back to the server list page.
    - Click **Add and Continue** to save the settings and continue to add other servers.
12. **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 and view its storage and camera information.

    Delete Server Select the server(s) from the list, and click **Delete** to remove the selected server(s).

    Configure Server Click ⚙ in the Operation column, and the login interface of the Hybrid SAN displays. You can log in and configure the Hybrid SAN.

    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.

8.23.3 Add Network Video Recorder

You can add an Network Video Recorder (NVR) as a recording server to HikCentral Professional for storing pictures.

Before You Start

Make sure the NVRs 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 Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Recording Server** on the left panel.
3. Click **Add** to enter the adding server 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. See ***Set NTP*** for details.
4. Select **Network Video Recorder** as the server type.
5. Set the required information.

   Address

   The server's IP address in LAN that can communicate with SYS.

   Control Port

   The control port No. of the NVR. If it is not changed, use the default value.

   Network Port

   The network port No. of the NVR. If it is not changed, use the default value.

   Picture Download Port

   The picture downloading port of the NVR. If it not changed, use the default value.

   Signaling Gateway Port

   The signaling gateway port No. of the NVR. If it is not changed, use the default value.
6. Enter the user's access key and secret key of the NVR for downloading pictures via Control Client.

   Note

   You can download these two keys on the NVR's remote configuration page.
7. **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.
8. Enter the name, user name, and password of the NVR.

   Caution

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

characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

9. Finish adding the NVR.
   - Click **Add** to add the NVR and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other NVRs.
10. **Optional:** Perform the following operations after adding the NVR.

Edit NVR Click **Name** field of the NVR and you can edit the information of the NVR and view its storage and camera information.

Delete NVR Select the NVR(s) from the list, and click **Delete** to remove the selected server(s).

Configure NVR Click ⚙ in the Operation column, and the login interface of the NVR will be displayed. You can log in and configure the NVR.

8.23.4 Manage Cloud Storage Server

You can add a Cloud Storage Server as a Recording Server to the HikCentral Professional for storing the video files.

Import Service Component Certificate to Cloud Storage Server

For data security purpose, the Cloud Storage Server's certificate should be same with the SYS server's. Before adding the Cloud Storage Server to the platform, you should import the certificate stored in the SYS server to the Cloud Storage Server.

Before You Start

Make sure the Cloud 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.

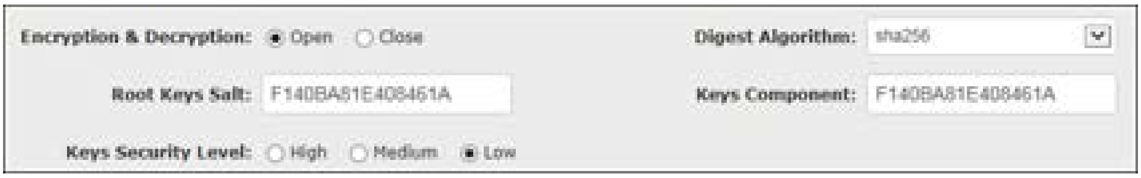
Steps

Note

If the service component certificate is updated, you should export the new certificate and import it to the Cloud Storage Server again to update.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** .
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 Cloud Storage Server via web browser.
5. Click **System → Configuration → Cloud Configuration** .
6. Input the root keys salt and keys component according to the parameters in the certificate you export in Step 3.



Encryption & Decryption: ● Open ○ Close

Digest Algorithm: sha256

Root Keys Salt: F140BA81E408461A

Keys Component: F140BA81E408461A

Keys Security Level: ○ High ○ Medium ● Low

7. Click **Set**.

What to do next

After importing the certificate to the Clout Storage Server, you can add the server to the platform for management. See ***Add Cloud Storage Server*** for details.

Add Cloud Storage Server

You can add Cloud Storage Server as recording server to the HikCentral Professional for storing the video files and pictures.

Before You Start

- Make sure the Cloud Storage Servers 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.
- You should import the service component certificate to the Cloud Storage Server first before adding it to the system. See ***Import Service Component Certificate to Cloud Storage Server*** for details.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules → General → Recourse Management** .
2. Click **Device and Server → Recording Server** on the left panel.
3. Click **Add** to enter the adding server 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. See ***Set NTP*** for details.

4. Select **Cloud Storage**.
5. Enter the network parameters.

Address

The server's IP address in LAN that can communicate with SYS server.

Control Port

The control port No. of the server. If it is not changed, use the default value.

Network Port

The network port No. of the server. If it is not changed, use the default value.

Signaling Gateway Port

The signaling gateway port No. of the server. If it is not changed, use the default value.

6. Enter the user's access key and secret key of the Cloud Storage Server for searching the video files stored in this Server via the HikCentral Professional Mobile Client or downloading pictures via Control Client.

Note

You can download these two keys on the Cloud Storage Server's configuration page (click **Virtualizing → User Management**).

7. **Optional:** Switch on **Enable Picture Storage** for storing pictures in this Cloud Storage Server.

Note

If this function is enabled, you need to set picture downloading port No., which is used to download pictures via Control Client.

8. **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.
9. Enter the name, user name, and password of the 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 installer and/or end-user.

10. Finish adding the Server.
    - Click **Add** to add the server and back to the server list page.
    - Click **Add and Continue** to save the settings and continue to add other servers.
11. **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 and view its storage and camera information.
Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Configure Server	Click ⚙ in the Operation column, and the login interface of the Cloud Storage Server displays. You can log in and configure the Cloud Storage Server.

8.23.5 Add pStor Cluster Service

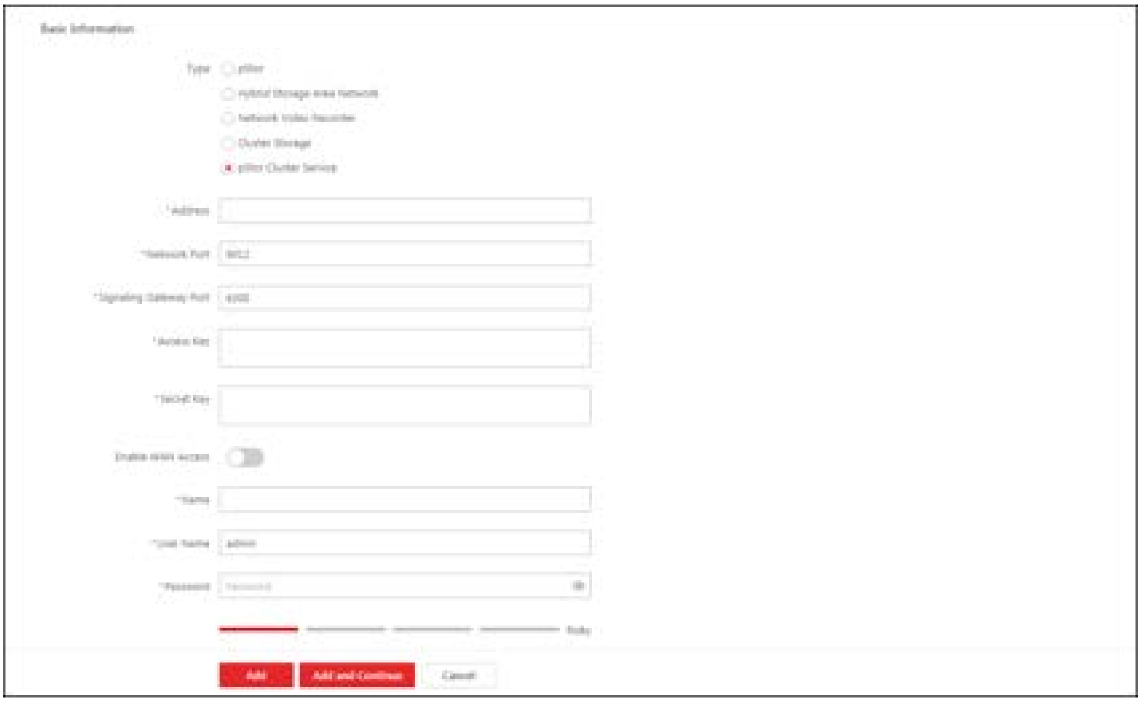
pStor cluster service is a service that can manage multiple pStors and the connected disks of pStors. When there are multiple pStors storing a large number of video files, you can add pStor cluster service to the HikCentral Professional for managing pStors. It is also an efficient way to add multiple pStors.

Before You Start

Make sure the pStor cluster services 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 ▦ → **All Modules** → **General** → **Recourse Management** .
2. Click **Device and Server** → **Recording Server** on the left panel.
3. Click **Add** to enter the Add Recording Server page.



Basic Information

Type ○ pStor
○ Hybrid Storage Area Network
○ Network Video Recorder
○ Cluster Storage
● pStor Cluster Service

*Address

*Network Port 8012

*Signaling Gateway Port 6300

*Access Key

*Secret Key

Enable WAN Access

*Name

*User Name admin

*Password Password

Risky

Figure 8-24 Add Recording Server 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. See ***Set NTP*** for details.

4. Select **pStor Cluster Service**.
5. Enter the required network parameters.

Address

The server's IP address in LAN that can communicate with SYS.

Network Port

The network port No. of the pStor cluster service. If it is not changed, use the default value.

Signaling Gateway Port

The signaling gateway port No. of the pStor cluster service. If it is not changed, use the default value.

6. Enter the user's access key and secret key of the pStor cluster service.

Note

You can download these two keys on the Web Client page (enter ***device's IP address: 9012*** in the browser) of pStor cluster service.

7. **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.
8. Enter the name, user name, and password of the pStor cluster service.

Caution

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

9. Finish adding the server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other servers.
10. **Optional:** Perform the following operations after adding the server.

Edit Server	Click **Name** field of the server and you can edit the basic information of the server, view its connected device(s) storage information.
Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Configure Server	Click ⚙ in the Operation column to enter the login interface of the pStor cluster service. You can log in and configure the pStor cluster service.

8.23.6 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, thus increasing the video storage reliability of HikCentral Professional.

Before You Start

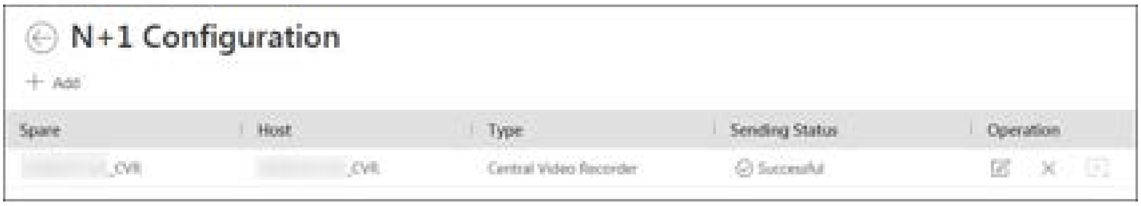
- Make sure the Hybrid Storage Area Networks you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- At least two online 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. For details about configuring N+1 hot spare system with NVRs, see ***Set N+1 Hot Spare for NVR*** .
- 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. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Recording Server** → **N+1 Hot Spare** to enter the N+1 Configuration page.



N+1 Configuration

+ Add

Spare	Host	Type	Sending Status	Operation
[redacted]_CVR	[redacted]_CVR	Central Video Recorder	Successful	

Figure 8-25 N+1 Configuration Page

3. Click **Add** to set the N+1 hot spare.
4. Select a Hybrid Storage Area Network in the Spare drop-down list to set it as the spare server.
5. Select the Hybrid Storage Area Network(s) in the Host field as the host server(s).
6. Click **Add**.

   Note

   The recording schedules configured on the Hybrid Storage Area Network will be deleted after setting it as the spare Recording Server.

7. **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.

8. **Optional:** If the host server sending the recording schedule to spare server failed, you can click on the Operation column to send the recording schedule on the host server to the spare one again.

8.24 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.

8.24.1 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.

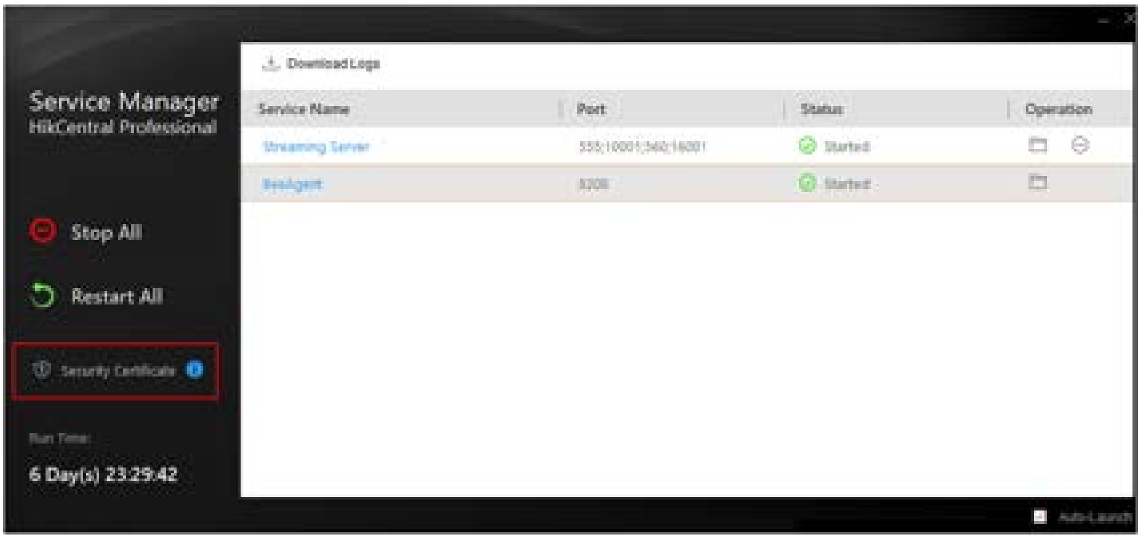
1. Log into the Web Client on the SYS server locally.

   You will enter the Home page of the Web Client.
2. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** .
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 installed with Streaming Service, open the Service Manager.
6. Click **Security Certificate**.



Service Name	Port	Status	Operation
Streaming Server	555;10001;560;16001	Started	
BeeAgent	8208	Started	

Figure 8-26 Enter Security Certificate

7. Enter the certificate information you generate in step 4.

8.24.2 Add Streaming Server

You can add a Streaming Server to the system to forward the video stream.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Streaming Server** on the left panel.
3. Click **Add** to enter the Add Streaming Server page.
4. Enter the required information.

   Name

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

   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.

Video File Streaming Port

It is used for Streaming Service to get stream for playback. 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

It is used for security certificate authentication. If it is not changed, use the default value.

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.

Note

The **Enable WAN Access** switch is available when you set Network Location as **LAN IP Address**.

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).

8.25 Add DeepinMind Server

When you know the related parameters such as IP address and port No. of the DeepinMind server, you can add it to the platform for intelligent functions, such as facial recognition, behavior analysis, and intrusion detection.

Before You Start

Make sure the DeepinMind server you are going to use is 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **DeepinMind Server** on the left.
3. Click **Add** to enter the Add DeepinMind Server page.
4. Set the required basic information such as device address, device port number, and WAN access.

   Address

   IP address of the DeepinMind server.

   Enable WAN Access

   Enable the DeepinMind 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 DeepinMind server for WAN access.
5. Finish adding the DeepinMind 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 **Alias** 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.

8.26 Add Security Audit Server

You can add the security audit server to the system to receive the security audit exception logs (e.g., injection attack logs, XSS events) of encoding devices from the server and trigger related alarms in the system.

Before You Start

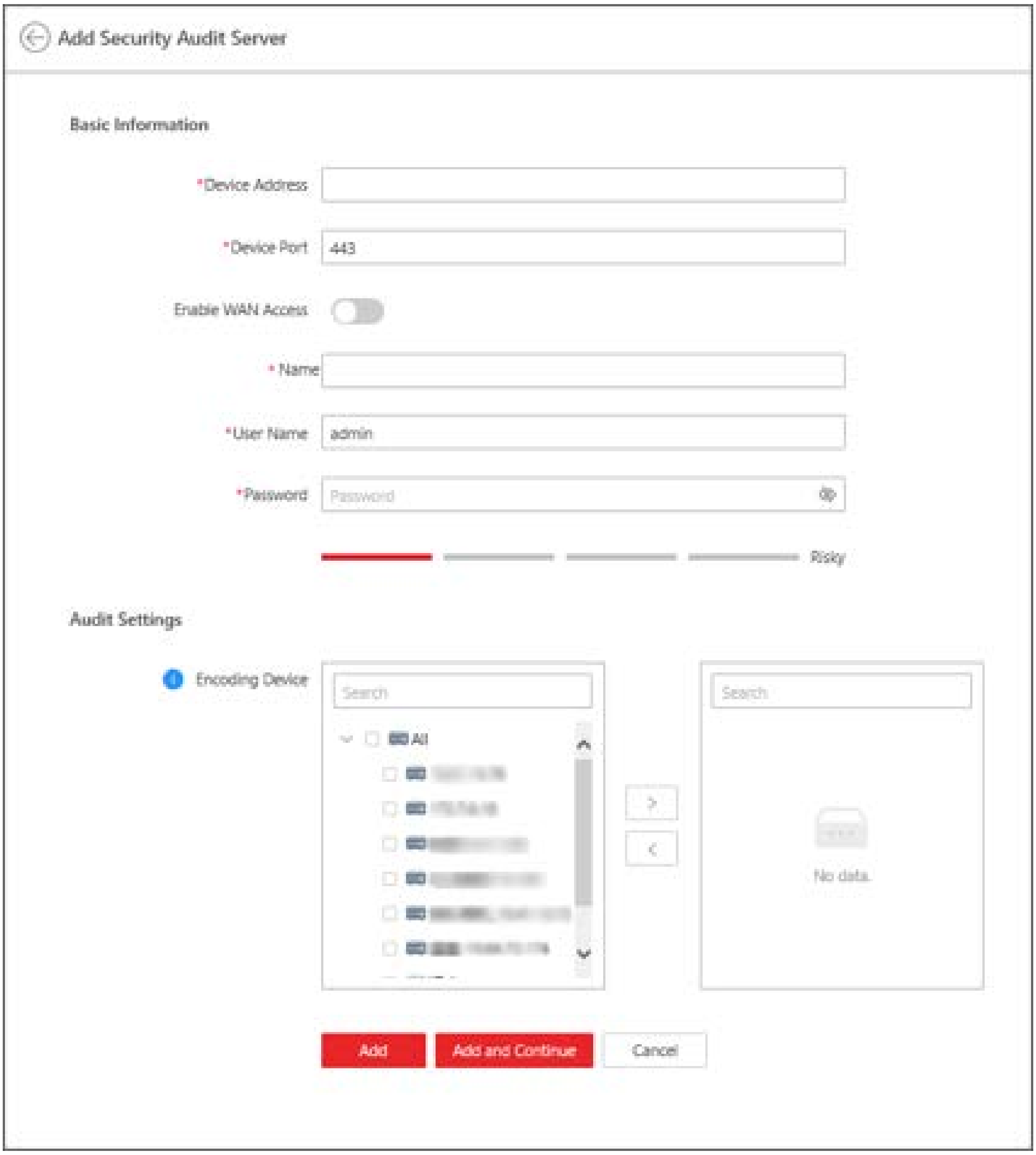
Make sure the security audit servers you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

- Adding security audit server is controlled by the system's license.
- Up to 8 security audit servers can be added to the system if the license permits.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .

2. Click **Device and Server → Security Audit Server** on the left panel.
3. Click **Add** to enter the Add Security Audit Server page.



Add Security Audit Server

Basic Information

*Device Address:

*Device Port: 443

Enable WAN Access

*Name:

*User Name: admin

*Password: Password

Risky

Audit Settings

Encoding Device

Figure 8-27 Add Security Audit Server Page

4. Set the required basic information such as device address, device port number, and WAN access.

   Address

   IP address of the security audit server.

   Device Port

The device port of the security audit server. By default, the port is 443, which means the security audit server access to HikCentral Professional by HTTPS.

Enable WAN Access

Enable the security audit server to access WAN.

Note

After enabling the WAN Access, you need to set the WAN IP address and log collection port for WAN access.

Name

Create a descriptive name for the security audit server. For example, you can use an alias that can show the feature of the server.

User Name

Enter the user name that has the privilege to log into the security audit server.

Password

Enter the password of the user that has the privilege to log into the security audit server.

5. Select the encoding devices for security audit.

Note

The system can receive the security audit exception logs (e.g., injection attack logs, XSS events) of selected encoding devices from the server, and trigger related alarms in the system.

6. Finish adding the security audit server.
   - Click **Add** to finish adding the server.
   - Click **Add and Continue** to add the server and continue to add more.
7. **Optional:** Perform the following operations after adding the security audit server.

Edit a Server	Click **Name** field of the server and you can edit the basic information of the server.
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).

8.27 Manage Remote Site

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.

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.

8.27.1 Add Remote Site by IP Address or Domain Name

If you know the IP address or domain name of the Remote Site to be added, you can add the site to the Central System by specifying the IP address (or domain name), user name, password, and other related parameters.

Steps

Note

- When adding Remote Site, the site's cameras and area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. In the top left corner of Home page, select ▦ → **All Modules** → **Video** → **Remote Site Management** .
2. Enter the Add Remote Site page.
   - 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.

Figure 8-28 Add Remote Site

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.

3. Select **IP Address/Domain** as the adding mode.
4. Enter the required information.

Site Address

The IP address or domain name of the Remote Site.

Site Port

Enter the port No. of the Remote Site.

Name

Edit a name for the Remote Site as desired. You can check **Get Name** to synchronize the Remote Site's name automatically.

User Name

The user name for the Remote Site, such as admin user and normal user.

Password

The password required to access the Remote Site.

⚠ **Caution**

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

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

Description

Optionally, you can enter the descriptive information for the Remote Site, such as location and deployment.

5. **Optional:** Enable receiving the alarms configured on the Remote Site.

1) Set the **Select Alarm** switch to **ON** to display all the configured alarms on a Remote Site.

[redacted]

Figure 8-29 Receive Alarm from Site Page

2) **Optional:** Click ▽ to filter the configured alarms by the alarm source, area, triggering event, etc.
3) 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.
- You can view and edit alarms in Event and Alarm module. For details about setting the event and alarm, refer to ***Event and Alarm Configuration*** .

6. 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.

Max. Number of Backups

Define the maximum number of backup files available on the platform.

7. **Optional:** Enable backing up the Remote Site's database in schedule.

1) Switch on **Scheduled Database Backup**.
2) 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.

3) Select what time of a day to start backup.

8. Click **Add** to add the remote site.

8.27.2 Add Remote Site Registered to Central System

If the Remote Sites have been registered to the Central System and the Central System also enabled the receiving site registration function, the registered Remote Sites will display in the site list. You can add them to the Central System by entering user names and passwords.

Before You Start

- The Remote Site must be registered to the Central System by entering the Central System's network parameters (see ***Set Network Parameters*** for details).
- Make sure the receiving site registration function has been enabled on the Central System. (see ***Set Network Parameters*** for details).

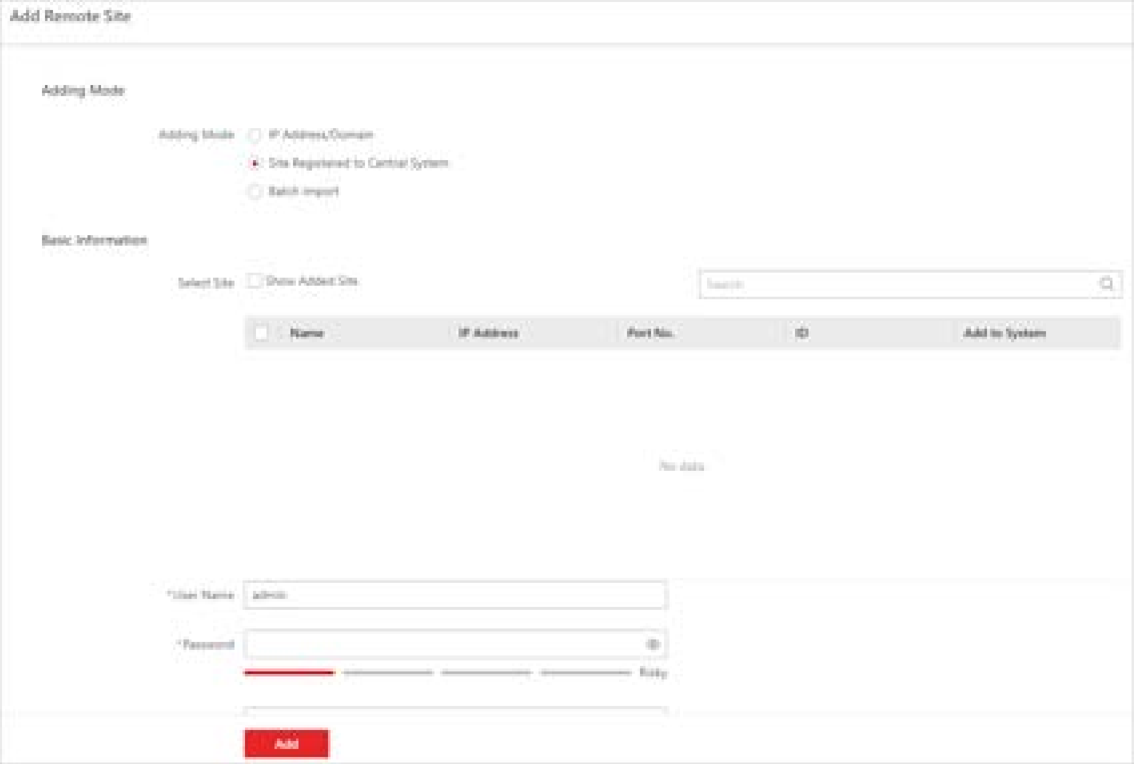
Perform this task when you need to add the site which has registered to the Central System.

Steps

Note

- When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Video** → **Remote Site Management** .
2. Enter the adding Remote Site page.
   - If no Remote Site 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.



Add Remote Site

Adding Mode

Adding Mode ○ IP Address/Domain
● Site Registered to Central System
○ Batch Import

Basic Information

Select Site □ Show Added Site

Search

□	Name	IP Address	Port No.	ID	Add to System

No data

*User Name admin

*Password

Risky

Figure 8-30 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.

3. Select **Site Registered to Central System** as the adding mode.

   The sites which have already registered to the Central System will display in the list.

4. Select the Remote Site(s) and enter the user name and password of the Remote Site(s).

Caution

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

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

5. 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.

Max. Number of Backups

Define the maximum number of backup files available on the system.

Note

The value of maximum number of backups ranges from 1 to 5.

6. **Optional:** Back up the Remote Site's database in schedule.
   1) Set the **Scheduled Database Backup** switch to **ON** to enable the scheduled backup.
   2) 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.

   3) Select what time of the day to start backup.
7. Click **Add** to add the Remote Site and go back to the Remote Site list page.

8.27.3 Add Remote Sites in a Batch

When you want to add multiple Remotes Sites at a time for convenience, you can edit the predefined template by entering the sites' parameters and import the template to the Central System to add them.

Steps

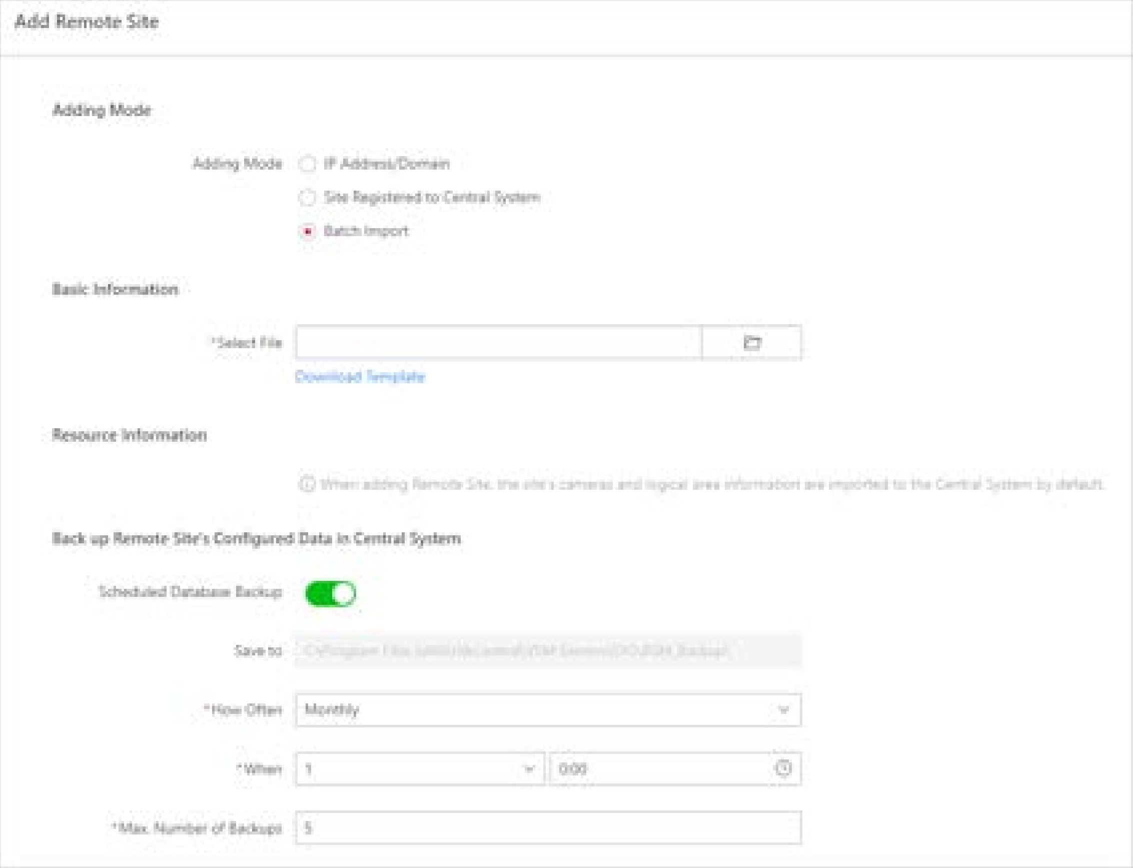
Note

- When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Video** → **Remote Site Management** .

   Note

   If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Remote Site Management** on navigation bar to enter the Remote Site management page.
2. Enter the adding Remote Site page.
   - If no Remote Site 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.



Add Remote Site

Adding Mode

Adding Mode ○ IP Address/Domain
○ Site Registered to Central System
● Batch Import

Basic Information

*Select File

Download Template

Resource Information

When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.

Back up Remote Site's Configured Data in Central System

Scheduled Database Backup: ON

Save to: [illegible]

*How Often: Monthly

*When: 1 0:00

*Max. Number of Backups: 5

Figure 8-31 Add Remote Site

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.

3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template on your PC.
5. Open the exported template file and input the required information of the Remote Sites to be added on the corresponding column.
6. Click 🗀 and select the template file.
7. 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.

   Max. Number of Backups

   Define the maximum number of backup files available on the system.
8. **Optional:** Back up the Remote Site's database in schedule.

   1) Set the **Scheduled Database Backup** switch to **ON** to enable the scheduled backup.

   2) 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.

3) Select what time of the day to start backup.

9. Click **Add** to add the Remote Site and go back to the Remote Site list page.

8.27.4 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.

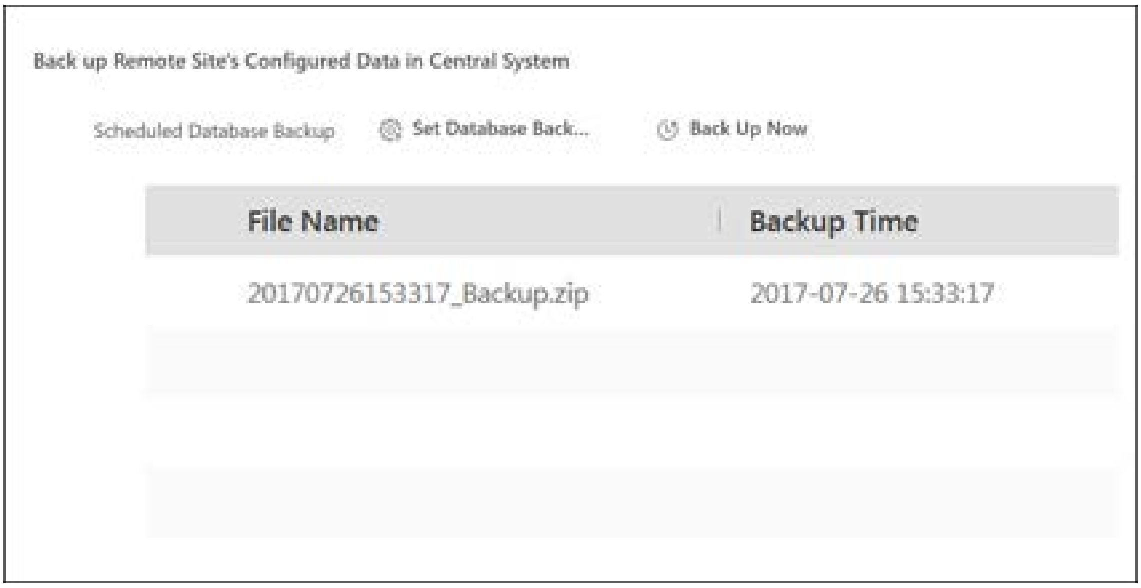
Steps

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Video** → **Remote Site Management** .

Note

If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Remote Site Management** on navigation bar to enter the Remote Site management page.

2. In the site list on the left, click the Remote Site name to view its details.



Back up Remote Site's Configured Data in Central System

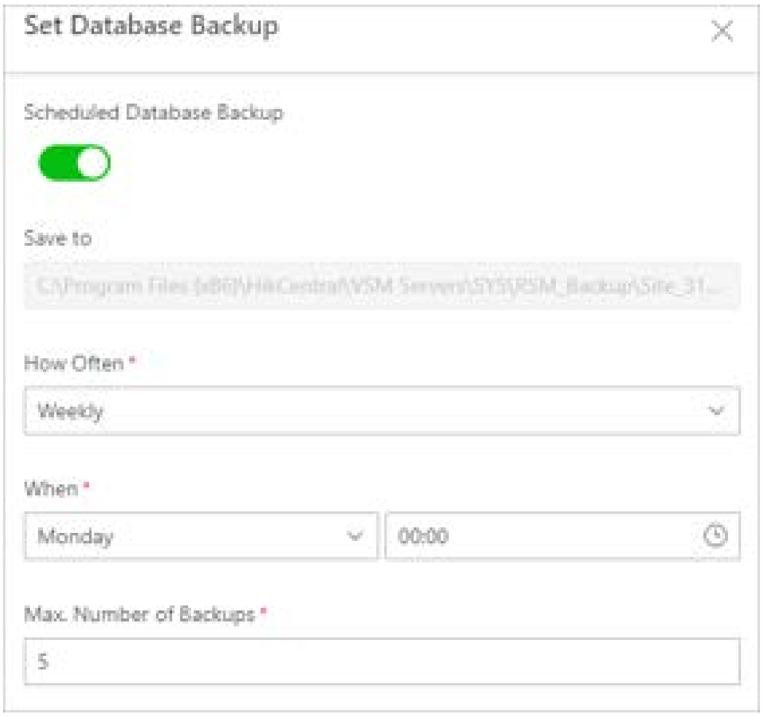
Scheduled Database Backup　Set Database Back...　Back Up Now

File Name	Backup Time
20170726153317_Backup.zip	2017-07-26 15:33:17

Figure 8-32 Back up Remote Site Database in Central System

3. Click **Back Up Now** to back up the Remote Site's database manually.
4. **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.



Set Database Backup

Scheduled Database Backup

Save to: C:\Program Files (x86)\HikCentral\VSM Servers\SYS\RSM_Backup\Site_31...

How Often *: Weekly

When *: Monday 00:00

Max. Number of Backups *: 5

Figure 8-33 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.

8.27.5 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 top left corner of Home page, select 🟥 → **All Modules** → **Video** → **Remote Site Management** .

   Note

   If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Remote Site Management** on navigation bar to enter the Remote Site management page.

2. In the site list on the left, click the Remote Site name to view its details.
3. View and edit the basic information of the Remote Site, including IP address, port, alias, etc.

   Note

   You cannot edit the address and port of the site registered to the Central System.

4. In the original information field, view the Remote Site's site name, system ID, system version, and GPS location.

   Note

   If the GPS location is not configured, click **Configuration** to set its location in Map module. See ***Map Management*** for details.

5. **Optional:** Click **Configuration on Site** to open the Web Client of the Remote Site and log in for further configuration.

   Note

   The site must be online if you need to enter its Web Client.

6. Click **Save**.

8.27.6 View Remote Site's Changes

When there are changed resources on the Remote Site, such as newly added cameras, deleted cameras, and name changed cameras, you can view the changed 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.

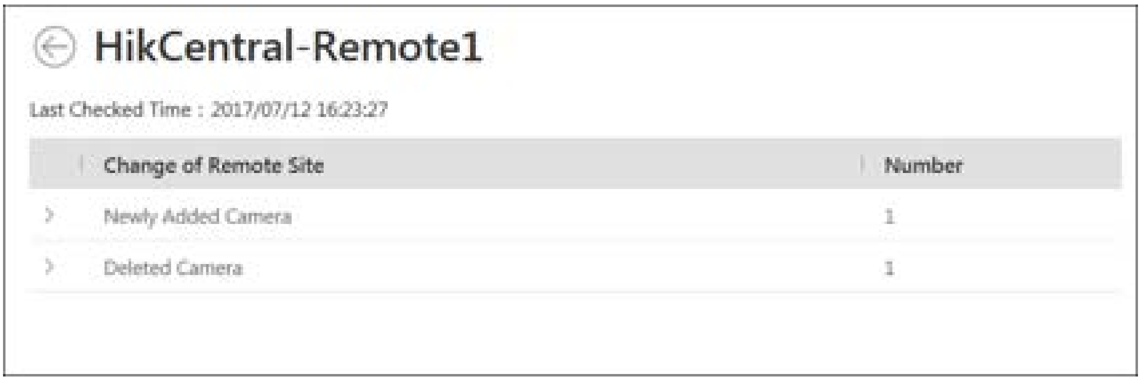
1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Video** → **Remote Site Management** .

   Note

   If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Remote Site Management** on navigation bar to enter the Remote Site management page.

2. Click ⟳ in the site list on the left to get the latest status of the Remote Sites.

3. Click the site name whose resources are changed to enter its details page.
4. Click **Changes of Remote Site** to view the changes.



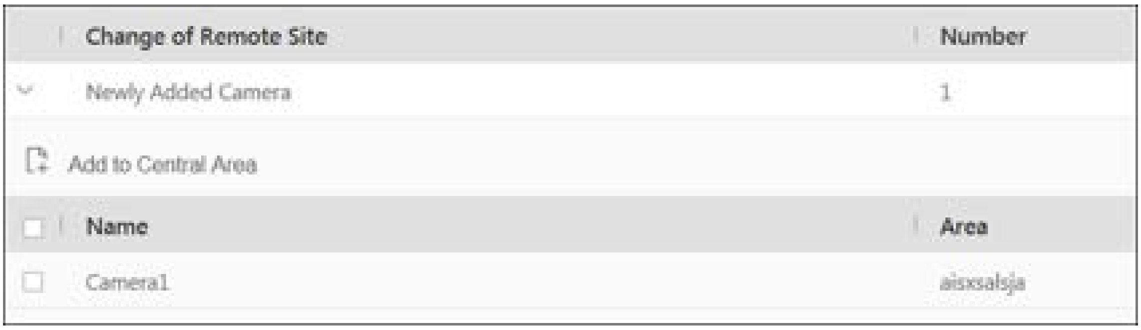
HikCentral-Remote1

Last Checked Time : 2017/07/12 16:23:27

Change of Remote Site	Number
Newly Added Camera	1
Deleted Camera	1

Figure 8-34 Remote Site Management

5. When there are newly added cameras on the site, you can view the added cameras and add them to the area in Central System.
   1) If there are some newly added cameras on Remote Site, click **Newly Added Camera** to expand the newly added camera list.

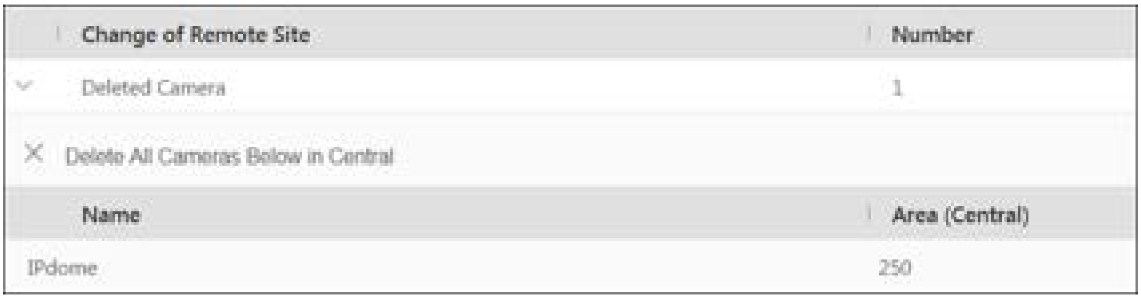


Change of Remote Site	Number
Newly Added Camera	1

□ Name	Area
□ Camera1	aisxsalsja

Figure 8-35 Changes of Remote Site

   You can view the camera name and area name on the Remote Site.
   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**.
6. When there are some cameras deleted from the site, you can view the deleted cameras and remove them from Central System.
   1) If there are some cameras deleted from Remote Site, click **Deleted Camera** to expand the deleted camera list.



Change of Remote Site	Number
Deleted Camera	1

× Delete All Cameras Below in Central

Name	Area (Central)
IPdome	250

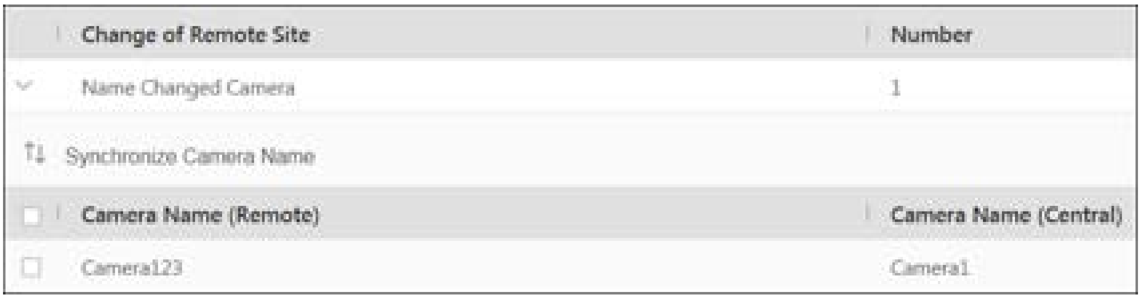
Figure 8-36 Change of Remote Site

You can view the camera name and its area in Central System.

2) Click **Delete All Cameras Below in Central** to delete the deleted cameras in Central System.

7. When there are some cameras whose names are changed on the site, you can view the name changed cameras and synchronize them to Central System.

   1) If the name of camera of Remote Site is changed, click **Name Changed Camera** to expand the name changed camera list.



Change of Remote Site	Number
Name Changed Camera	1

⇅ Synchronize Camera Name

□ Camera Name (Remote)	Camera Name (Central)
□ Camera123	Camera1

Figure 8-37 Name Changed Camera

You can view the camera names in Remote Site and Central System.

2) Select the cameras and click **Synchronize Camera Name** to synchronize the camera name in Central System.

Chapter 9 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, on the 1st floor, there mounted 64 cameras, 16 access points, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one area (named 1st Floor) for convenient management. You can get the live view, play back the video files, and 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.

9.1 Add Area

You should add an area before managing the elements by areas.

9.1.1 Add Area for Current Site

You can add an area for the current site to manage the devices.

Steps

1. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. **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.
4. Click + on the area list panel to open the Add Area panel.

Figure 9-1 Add Area for Current Site

5. Select the parent area to add a sub area.
6. Create a name for the area.
7. **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.
8. **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.
9. **Optional:** Click **Expand** to expand and set the additional area information as needed.

   Note

   For details about customizing fields of the additional area information, refer to ***Customize Additional Information*** .
10. Click **Add**.
11. **Optional:** After adding the area, you can do one or more of the following:

Edit Area
Click ✎ to edit the area.

Delete Area
Click 🗑 to delete the selected area, or press **Ctrl** on your keyboard, select multiple areas, and then click 🗑 to delete areas in a batch.

Note

After deleting the area, the resources (cameras, doors, elevators, radars, alarm inputs, alarm outputs, UVSSs, and digital signage terminals) 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 child area.

9.1.2 Add Area for Remote Site

You can add an area for the Remote Site to manage the devices in the Central System.

Steps

1. In the top-left corner of the Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. In the area list 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. Click + on the area list panel to open the Add Area panel.

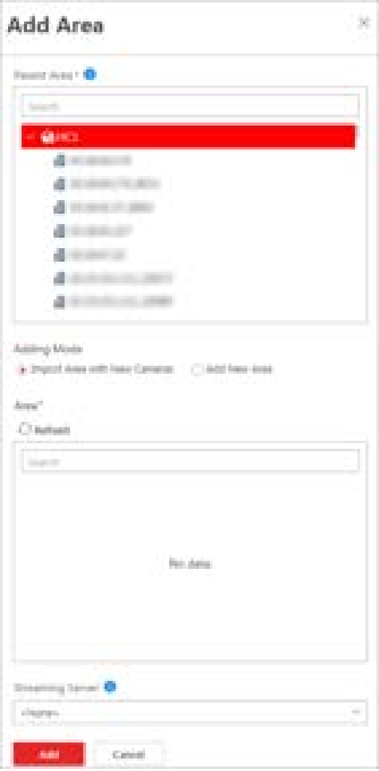


Figure 9-2 Add Area for Remote Site

5. Select the parent area to add a sub-area.
6. Set the adding mode for adding the area.

Import Area with New Cameras

If there are some cameras newly added to the areas on a Remote Site, you can import the areas as well as those newly added cameras. The areas with newly added cameras will be displayed and you can select the areas to add.

Add New Area

Add a new area to the parent area.

7. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.
8. **Optional:** If you select a Streaming Server for the area, check **Wall Display via Streaming Server** if you want to display the area's resources on the smart wall via this Streaming Server.
9. **Optional:** Click **Expand** to expand and set the additional area information as needed.

Note

For details about customizing the additional area information, refer to ***Customize Additional Information*** .

10. Click **Add**.
11. After adding the area, you can do one or more of the following:

Edit Area
Click ✎ to edit the area.

Delete Area
Click 🗑 to delete the selected area, or press **Ctrl** on your keyboard, select multiple areas, and then click 🗑 to delete areas in a batch.

Note

After deleting the area, the cameras will be removed from the area, as well as the corresponding recording settings and event 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 child area.

9.1.3 Customize Additional Information

You can customize the area information which is not included in the basic information according to actual needs, e.g., description. After customizing, you can enter the additional area information to make the area information complete when adding or editing an area.

In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Area** .

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.

You can also click ✎ to edit the additional information or click 🗑 to delete it.

9.2 Add Element to Area

You can add elements including cameras, alarm inputs, alarm outputs, access points, and under vehicle surveillance systems into areas for management.

9.2.1 Add Camera to Area for Current Site

You can add cameras to areas for the current site. After managing cameras into areas, you can 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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding cameras to.

   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.

4. Select the **Camera** tab.
5. Click + on the element page to enter the Add Camera page.
6. Select the device type.
7. Select the camera(s) to add.
8. **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.

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:

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 used to display a certain camera's live view on the smart wall via the network keyboard.

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.

Get PTZ Configuration

Select the cameras and click to get the details of PTZ Configuration from the devices in a batch.

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 Child Areas

Check **Include Sub-Area** to display the cameras of child areas.

9.2.2 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.

Before You Start

Encoding devices need to be added to HikCentral Professional for area management. Refer to ***Manage Encoding Device*** for details about adding devices.

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 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. In the area list 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. 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.

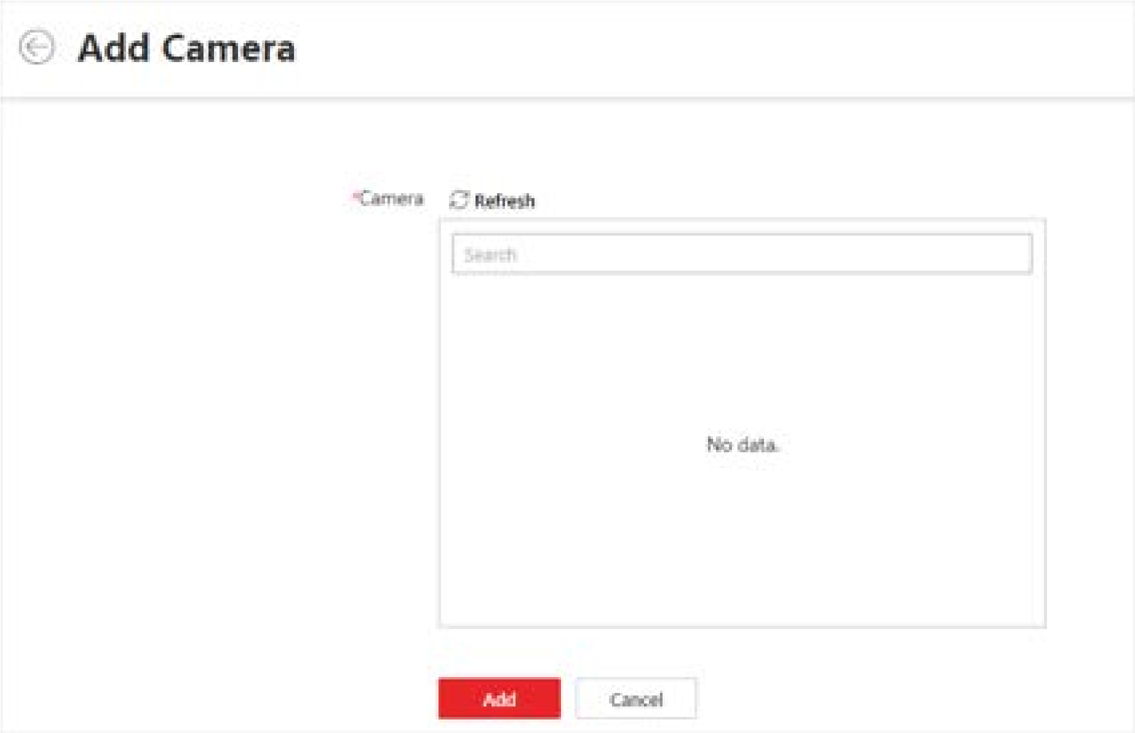


Figure 9-3 Add Camera to Area for Remote Site

7. Select the camera(s) to add.

   Note

   Up to 64 cameras can be added to one area.
8. Click **Add**.

The added camera(s) will be displayed in the list.

9. **Optional:** After adding the camera(s), you can do one or more of the following:

   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.

   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 Child Areas
   Check **Include Sub-Area** to display the cameras of child areas.

9.2.3 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 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding doors to in the area list panel.

   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 current site.

4. Select the **Door** tab.
5. Click + on the element page to enter the Add Door page.

6. Select the device type.
7. Select the door(s) to be added.
8. Click **Add**.

   The added door(s) will be displayed in the list.
9. **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 Child Areas	Check **Include Sub-area** to display the doors in child areas.

9.2.4 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 Home page, select → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding elevators to in the area list panel.
4. Select the **Elevator** tab.
5. Click + to enter the Add Elevator page.
6. In the Elevator Control Device field, all the added elevator control devices are displayed. Select the device to add the elevator to.

7. 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.
8. Click **Add**.
9. 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**.

   Add Elevator to Map
   Click to enter Map Settings page and drag the elevator to the map. See ***Add Hot Spot on Map*** for details.

   Display Elevators of Child Areas
   Check **Include Sub-area** to display the elevators of child areas.

9.2.5 Add Vehicle to Area for Current Site

You can add vehicles to areas for the current site for management. Only vehicles linked with mobile devices can be added to areas and one vehicle can only be added to one area.

Before You Start

The mobile devices need to be added to HikCentral Professional for area management. Refer to ***Manage Mobile Devices*** for details.

Steps

1. In the top-left corner of the Home page, select → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding vehicles to in the area list panel.

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.

4. Select the **Vehicle** tab.

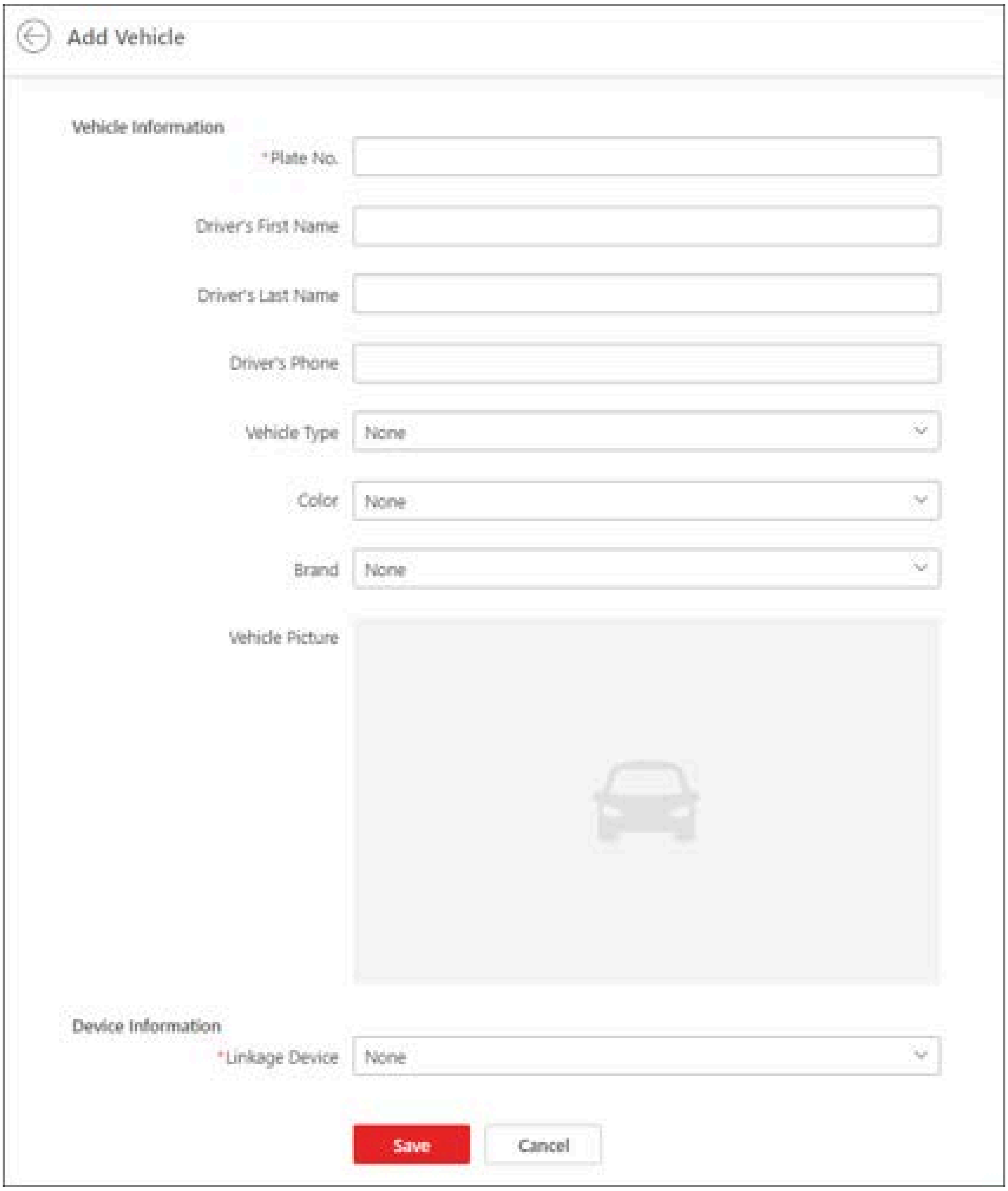


Figure 9-4 Add Vehicle to Area

5. Click **Add** on the element page to enter the Add Vehicle page.
6. Set the vehicle information, including the plate number, driver information, vehicle type, color, brand, and vehicle picture.
7. Select the mobile device linked with the vehicle from the Linkage Device drop-down list.
8. Click **Save**.

The added vehicle will be displayed in the list.

9. **Optional:** After adding the vehicle(s), you can do one or more of the following:

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.
Move to Other Area	Select the vehicle(s) and click **Move to Area**. Then select the target area to move the selected vehicle(s) to and click **Move**.
Display Vehicles of Child Areas	Check **Include Sub-Area** to display the vehicles in child areas.
Remotely Configure Linkage Device	Click ⚙ to go to the remote configuration page of the mobile device. **Note** This function is supported when the transfer protocol between the Web Client and the SYS server is HTTPS.

9.2.6 Add Radar to Area for Current Site

You can add 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 ***Resource Management*** for details.

Steps

Note

You cannot add a radar to multiple areas.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. In the area list 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. Select an area for adding radars to.
5. Click **Radar** tab.
6. Click + to enter the Add Radar page.
7. Select a radar in the **Radar** field.
8. Click **Add**.

9. **Optional:** After adding the radars, you can do one or more of the followings

   Arm/Disarm Radar
   Select the radar(s) and click / to arm/disarm the selected radar(s).

   Note

   An event will be triggered if anybody or an object enters an armed radar's detection area.

   Move to Other Area
   Select the radars and click . Then select the target area to move the selected radars to and click **Move**.

   Add Radar to Map
   Click to enter Map Settings page and drag the radar to the map. See ***Add Hot Spot on Map*** for details.

   Display Radars of Child Areas
   Check **Include Sub-area** to display the radars of child areas.

9.2.7 Add Alarm Input to Area

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 ***Resource 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 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding alarm inputs to.

   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 current site.
4. Select the **Alarm Input** tab.
5. Click + to enter the Add Alarm Input page.
6. Select the device type.
7. 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.

8. Click **Add**.
9. **Optional:** After adding the alarm inputs, you can do one or more of the followings.

Move to Other Area
Select the alarm inputs 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 Map Settings page and drag the alarm input to the map. See ***Add Hot Spot on Map*** for details.

Display Alarm Inputs of Child Areas
Check **Include Sub-area** to display the alarm inputs of child areas.

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.

9.2.8 Add Alarm Output to Area

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, the alarm devices (e.g., the siren, alarm lamp, etc.) connected with 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 ***Resource 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 Home page, select → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding alarm outputs to.

   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 current site.
4. Select the **Alarm Output** tab.
5. Click + to enter the Add Alarm Outputs page.
6. Select the device type.
7. Select the alarm outputs to add.
8. Click **Add**.
9. **Optional:** After adding the alarm outputs, you can do one or more of the followings.

   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**.

   Add Alarm Output to Map Click to enter Map Settings page and drag the alarm output to the map. See ***Add Hot Spot on Map*** for details.

   Display Alarm Outputs of Child Areas Check **Include Sub-area** to display the alarm outputs of child areas.

9.2.9 Add UVSS to Area for Current Site

You can add Under Vehicle Surveillance Systems (UVSSs) to areas for the current site for management.

Before You Start

The UVSS devices need to be added to the HikCentral Professional for area management. Refer to ***Add Under Vehicle Surveillance System*** for details.

Steps

Note

One UVSS can only belong to one area. You cannot add a UVSS to multiple areas.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding UVSSs to.

   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 current site.
4. Select the **UVSS** tab.
5. Click + to enter the Add UVSS page.
6. Select the UVSSs to add.
7. Click **Add**.
8. **Optional:** After adding the UVSSs, you can do one or more of the followings.

   Move to Other Area
   Select the UVSSs and click ⧉ . Then select the target area to move the selected UVSSs to and click **Move**.

   Add UVSS to Map
   Click 📍 to enter Map Settings page and drag the UVSS to the map. See ***Add Hot Spot on Map*** for details.

   Display UVSSs of Child Areas
   Check **Include Sub-area** to display the UVSSs of child areas.

9.2.10 Add Digital Signage Screen to Area for Current Site

You can add digital signage screens to areas for the current site for management.

Before You Start

The digital signage screens need to be added to HikCentral Professional for area management. Refer to ***Manage Digital Signage Terminals*** for details.

Steps

Note

One digital signage screen can only belong to one area. You cannot add one digital signage screen to multiple areas.

1. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.

3. Select an area for adding digital signage screens to.

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.

4. Click **Digital Signage Screen** tab.
5. Click **Add** to enter the Add Digital Signage Screen page.
6. Select the digital signage screens to add them.
7. Click **Add**.
8. **Optional:** After adding the digital signage screens, you can do one or more of the followings:

Delete Digital Signage Screen(s)
Select the digital signage screen(s) in the list and click **Delete**.

Move to Other Area
Select the digital signage screens and click **Move to Other Area**. Then select the target area to move the selected digital signage screens to and click **Move**.

Display Digital Signage Screens of Child Areas
Check **Include Sub-Area** to display the digital signage screens of child areas.

9.2.11 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.

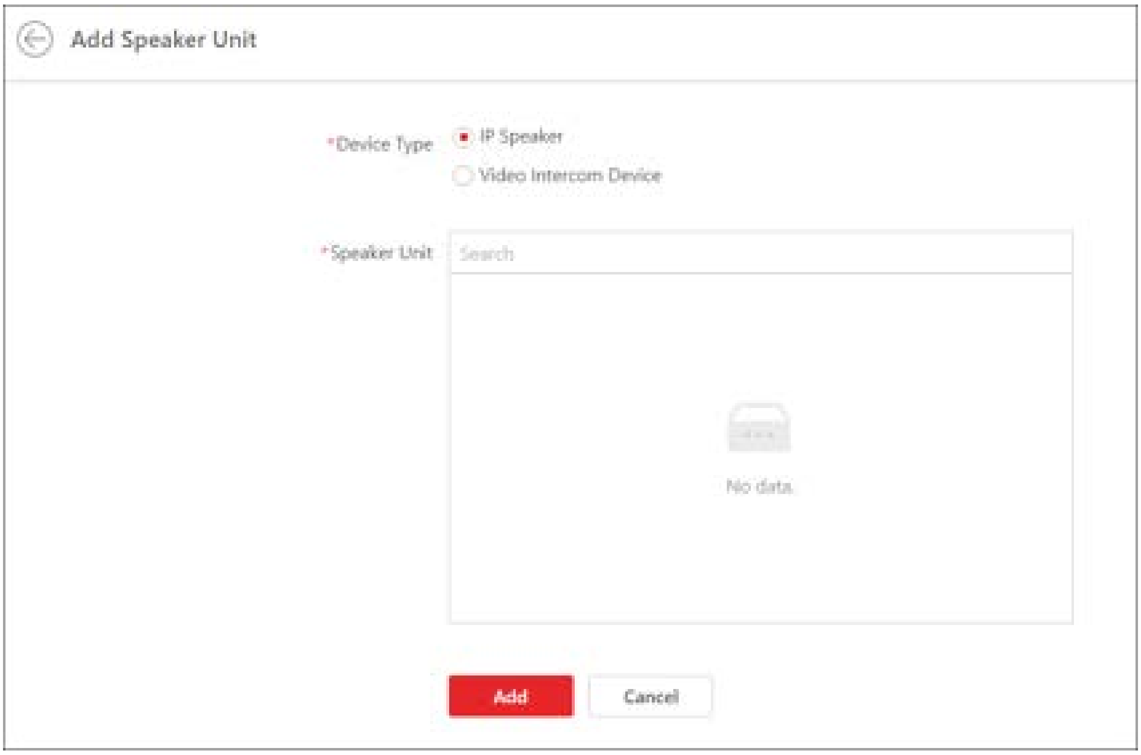
Steps

1. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding speaker units to.

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.

4. Select the **Speaker Unit** tab.
5. Click **Add** on the element page to enter the Add Speaker Unit page.



Add Speaker Unit

*Device Type ● IP Speaker ○ Video Intercom Device

*Speaker Unit Search

No data

Figure 9-5 Add Speaker Unit

6. Select the device type.
7. Select the speaker unit(s) to be added.
8. Click **Add**.

   The added speaker unit(s) will be displayed in the list.
9. **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 Child Areas
   Check **Include Sub-Area** to display the speaker units in child 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).

9.3 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 attendance settings for doors, and so on.

9.3.1 Edit Camera for Current Site

You can edit basic information, recording settings, and picture storage settings of the camera for current site.

Steps

1. In the top left corner of Home page, select → **All Modules** → **General** → **Resource Management** .
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. 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 changes 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 hover over the window and click in the lower-right corner to switch to playback.
9. Edit the recording settings of the camera. See ***Configure Storage and Recording*** for details.

   Note

   - If no recording settings have been configured for the camera, you can click **Configuration** 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.
10. **Optional:** Set the **Picture Storage** 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

- Refer to ***Configure Storage for Uploaded Pictures*** for details.
- For cameras added by ISUP protocol, this function is not available. You should click **Configuration** to edit the picture storage configurations.

11. **Optional:** Click **Configuration on Device** in the top right corner of 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 camera editing panel, click **Copy to** to select configuration item and copy the settings of this camera to other cameras.
13. Click **Save**.

9.3.2 Edit Door for Current Site

You can edit basic information, related cameras, picture storage settings, card reader settings, and face recognition terminal settings of the door on current site.

Steps

1. In the top left corner of Home page, select → **All Modules** → **General** → **Resource Management** .
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 and select one area.
4. Select the **Door** tab to show the added doors in this area.
5. Click a door's name in the **Name** column to enter the Edit Door page.
6. Edit the door's basic information.

   Name

   Edit the name for the door.

   Note

   If you changes 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.

   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 enabled.

Door Open Timeout Alarm

After enabled, if the door has configured with 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 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.

7. Relate cameras to the door, and you can view its live view, recorded video, captured pictures via the Control Client.

Note

- Up to 2 cameras can be related to one door.
- You can click ↑ or ↓ to adjust the displaying priority of its auto capture.
- You can switch on **Auto Capture** to realize the function of capturing automatically.

8. **Optional:** Switch on **Picture Storage** and select the storage location from the drop-down list for storing the pictures (captured by the device's camera) to the specified location. Refer to ***Configure Storage for Uploaded Pictures*** for details.

Note

- For details, refer to ***Configure Storage for Uploaded Pictures*** .
- If error occurred during picture storage configuration, ⚠ appears on the right of the door name.

9. 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.

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.

10. **Optional:** For the turnstile, set **Face Recognition Terminal** switch to on and add the face recognition terminals to link the selected turnstile.
    1) Click **Add** to enter 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 turnstile.
11. **Optional:** Click **Copy to** in the upper right corner to apply the current settings of the door to other door(s).
12. Click **Save**.

9.3.3 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. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Resource Management** .
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. Select the **Elevator** tab to show the added elevators in this area.
5. Click an elevator's name in the **Name** column to enter the elevator editing page.
6. 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.

Open Duration

The time interval between the elevator door is open and closed again.

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.

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.

7. 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.

8. 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.

9. 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.

10. **Optional:** Click **Copy to** in the upper right corner to apply the current settings of the elevator to other elevator(s).

11. Click **Save**.

9.3.4 Edit Vehicle for Current Site

After adding vehicles to areas of the current site, you can edit the basic vehicle information (plate number, driver information, vehicle type, color, brand, and vehicle picture) for the current site as needed.

Steps

1. In the top-left corner of the Home page, select ■ → **All Modules** → **General** → **Resource Management** .
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. Select an area.
5. Select the **Vehicle** tab to show the added vehicles.
6. Click a vehicle's plate number in the **Plate No.** column.
7. Edit the vehicle information (plate number, driver's name, driver's phone, vehicle type, color, brand, and vehicle picture).
8. Click **Save**.

9.3.5 Edit Radar for Current Site

After adding a radar to an area of the current site, you can edit the radar name, view the drawn zones or trigger lines, and view the related calibrated cameras.

Steps

1. In the top left corner of Home page, select ■ → **All Modules** → **General** → **Resource Management** .
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. Select an area.
5. Select the **Radar** tab to show the added radars.
6. Click a radar's name in the **Name** column to enter the Edit Radar page.
7. Edit the radar's name.
8. **Optional:** In the **Zone** field, view the drawn zones of the radar.

Note

If there is no zone drawn for the radar, you should go to Map Settings module to draw. Refer to ***Draw Zone or Trigger Line for Radar*** for details.

9. **Optional:** In Related Calibrated Camera field, view the calibrated cameras related to the radar.

Note

If there is no calibrated camera related to the radar, you should go to Map Settings module to configure. Refer to ***Relate Calibrated Camera to Radar*** for details.

10. Click **Save** to save the settings for the radar.

9.3.6 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 🟥 → **All Modules** → **General** → **Resource Management** .
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. Select the **Alarm Input** tab to show the added alarm inputs.
5. Click an alarm input name in the **Name** column to enter the Edit Alarm Input page.
6. Edit the alarm input name.
7. **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 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** .

8. Click **Save**.

9.3.7 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 🟥 → **All Modules → General → Resource Management** .
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. Select the **Alarm Output** tab to show the added alarm outputs.
5. Click an alarm output name in the **Name** column.
6. Edit the alarm output name in the pop-up window.
7. Click **Save**.

9.3.8 Edit Under Vehicle Surveillance System for Current Site

You can edit name of the Under Vehicle Surveillance System (UVSS) and relate cameras to the UVSS for current site.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules → General → Resource Management** .
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. Select an area.
5. Select the **UVSS** tab to show the added UVSSs.
6. Click an UVSS name in the **Name** column.
7. Edit the name of UVSS.

8. Relate cameras to the UVSS.
   1) Set the **Relate Camera** switch to ON.
   2) Select the camera(s).
9. Click **Save**.

9.3.9 Edit Digital Signage Screen for Current Site

You can edit the name of a digital signage screen for the current site.

Steps

1. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
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. Select an area.
5. Select the **Digital Signage Screen** tab to show the added digital signage screens.
6. Click a digital signage screen's name in the **Name** column.
7. Edit the name in the pop-up window.
8. Click **Save**.

9.3.10 Edit Speaker Unit for Current Site

You can edit basic information, related cameras settings of the speaker unit on current site.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
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. 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. Relate camera(s) to the broadcast.

- Up to 4 related cameras are allowed.
- Click ↑ or ↓ to adjust the displaying sequence of the cameras.

8. Click **Save**.

9.3.11 Edit Third-Party Integrated Resource for Current Site

After integrating the resources on third-party system to the HikCentral Professional via Optimus, the third-party resources are added to the areas.

In the top left corner of Home page, select 🟥 → **Resource Management** → **Area** → **Third-Party Integrated Resource** .

Click the name of third-party resource to enter the details page.

You can view the basic information of the resource, such as name, device type, and manufacturer.

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

- For details about locating resource on map, refer to ***Add Hot Spot on Map*** .
- The **Third-Party Integrated Resource** tab is available only when the **Integrate via Optiums** switch in System Configuration module is set to ON. For details, refer to ***Set Third-Party Integration*** .

9.3.12 Edit Element for Remote Site

If the current system is a Central System with a Remote Site Management module, you can edit the cameras added from the Remote Site.

Steps

1. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. In the area list 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. Select an area to show its cameras.
5. Click a camera's name in the **Name** column to enter the camera editing page.
6. 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.

7. **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.

Note

Double authentications is required for live view and playback on the camera editing page. For details about configuring double authentications, refer to ***System Security Settings*** .

8. 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 (for details, refer to ***Configure Recording for Cameras on Remote Site***).

9. **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.

10. **Optional:** Click **Copy to** to copy the current camera's specified configuration parameters to other cameras of the Remote Site.
11. Click **Save**.

9.4 Remove Element from Area

You can remove the added cameras, alarm inputs, alarm outputs, doors, and Under Vehicle Surveillance Systems (UVSSs) from the area.

9.4.1 Remove Element from Area for Current Site

You can remove the added cameras, doors, elevators, radars, alarm inputs, alarm outputs, UVSSs, speaker unit, and digital signage terminals from the area for current site.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area in the area list panel to show its added elements.

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.

4. Select the **Camera**, **Door**, **Elevator**, **Radar**, **Alarm Input**, **Alarm Output**, **UVSS**, **Digital Signage Screen** or **Speaker Unit** tab to show the added elements.
5. Select the elements.
6. Click 🗑 to remove the cameras from the area for current site.

9.4.2 Remove Element from Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can remove the added cameras from its area.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. In the area list 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. Select an area to show its added cameras.
5. Select the cameras.
6. Click 🗑 to remove the cameras from the area for remote site.
7. **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 10 Person Management

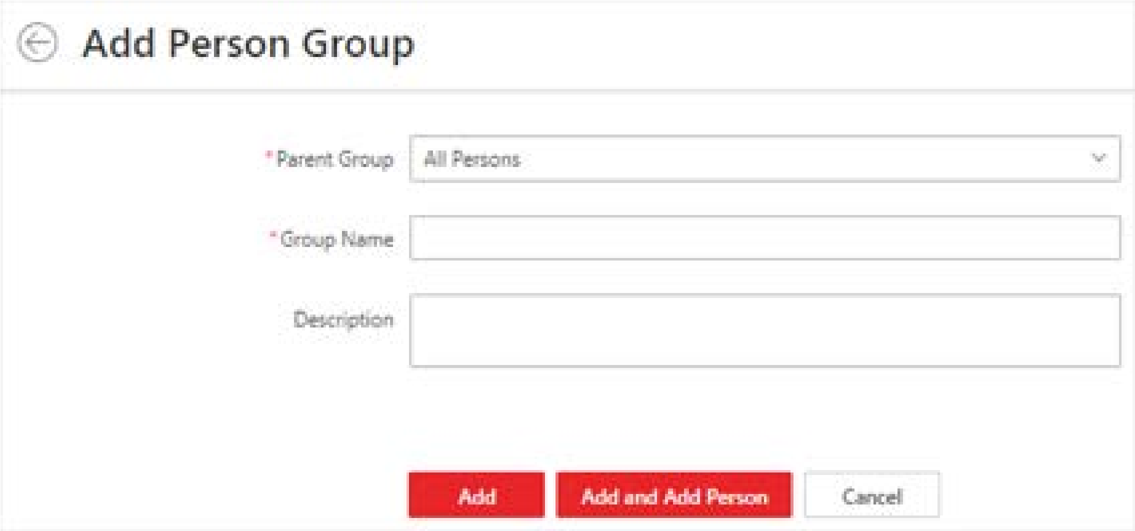
You can add person information to the platform for further operations such as access control (linking a person to an access level), face comparison (adding a person to a face comparison group), time and attendance (assign a shift schedule to a person), etc. After adding the persons, you can edit and delete the person information if needed.

10.1 Add Person Groups

When there are a large number of persons managed in the platform, you can put the persons into different person groups. For example, you can group employees of a company to different departments.

Steps

1. In the top left corner page of the Client, select ▦ → **All Modules** → **General** → **Person** .
2. Click + at the top of the person group list to enter the Add Person Group page.
3. Set the person group information, including the parent group, group name, and description.


Add Person Group

*Parent Group: All Persons

*Group Name:

Description:

Figure 10-1 Add Person Group

4. Add person group.
   - Click **Add** to add the person group and go back to the person management page.
   - Click **Add and Add Person** to add the person group and enter the Add Person page.
5. **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 Person Manually*** .

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 and attendance results will be affected.

6. **Optional:** Perform the following operations after adding person groups.

Edit Person Group

Select a person group, and click ✎ at the top of the person group list to edit the parent group, group name, or remarks.

Delete a Person Group

Select a person group and click 🗑 at the top of the person group list to delete the selected one.

Note

The root person group cannot be deleted.

Delete All Person Groups

Click ⌄ beside 🗑 at the top of the person group list to delete all added person groups.

10.2 Set Person ID Rule

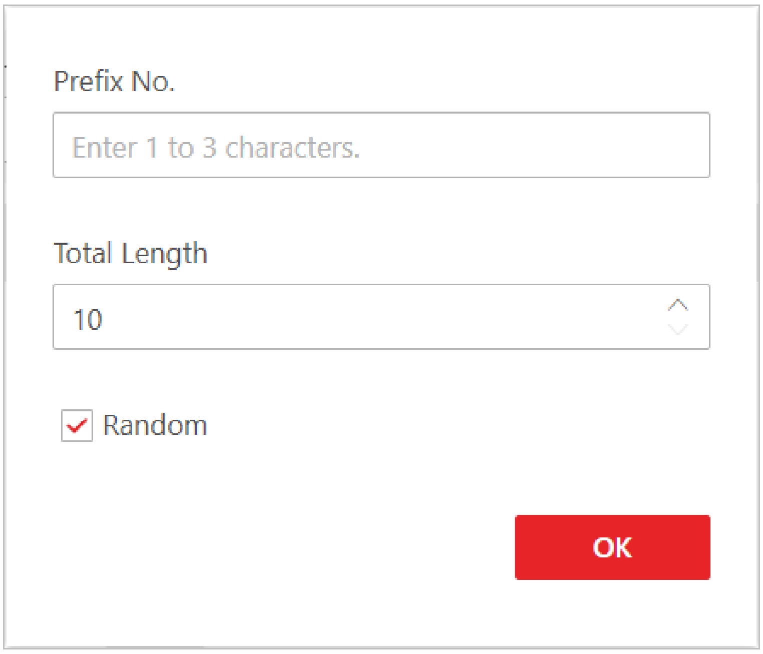
Before adding persons, you should configure a rule to define the prefix No., total length, and whether using random digits for the person ID.

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 top left corner of the Client, select 🟥 → **All Modules** → **General** → **Person** .
2. Click ▨ at the top of person list to open the ID rule settings pane.



Prefix No.

Enter 1 to 3 characters.

Total Length

10

☑ Random

Figure 10-2 ID Rule Settings Pane

3. Enter a prefix No. and select the total length.
4. **Optional:** Check **Random** to generate the ID (excepts the fixed prefix No.) with random digits.

   Example

   If you enter ***10*** as the prefix No. and set the total length to 8, all the person IDs will start from "10", such as "10125454" (when **Random** is checked) and "10000001" (when **Random** is unchecked).
5. Click **OK**.

10.3 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.

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*** .

10.3.1 Add a Person Manually

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, the elevator control application, the attendance management application, and the video intercom application.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Person** .
2. Select a person group from the person group list on the left.

   All persons in the selected person group will be displayed on the right. You can check **Include Sub-Group** to display the persons in sub person groups (if any).
3. Click ＋ at the top of person list to enter the Add Person page.

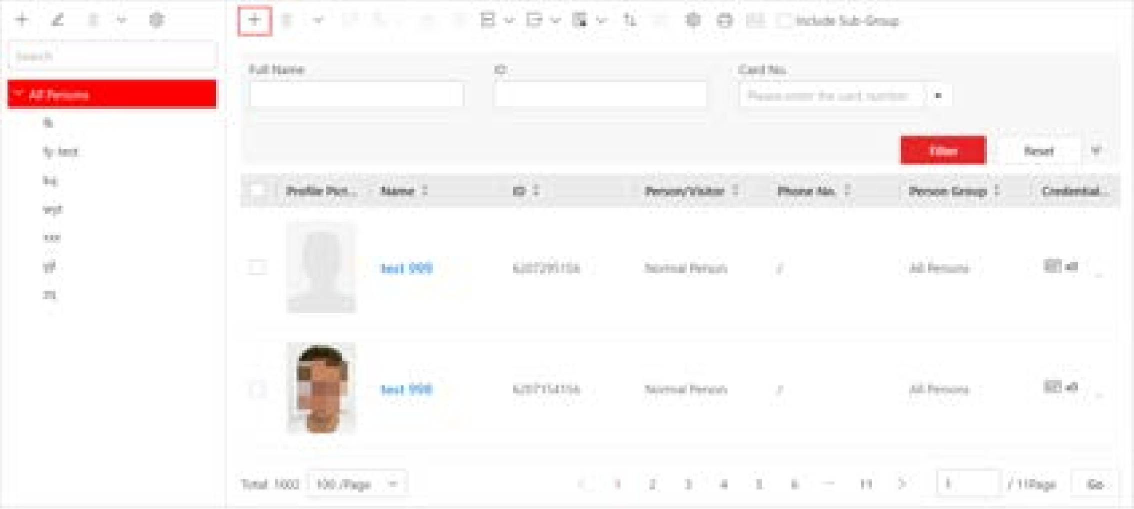
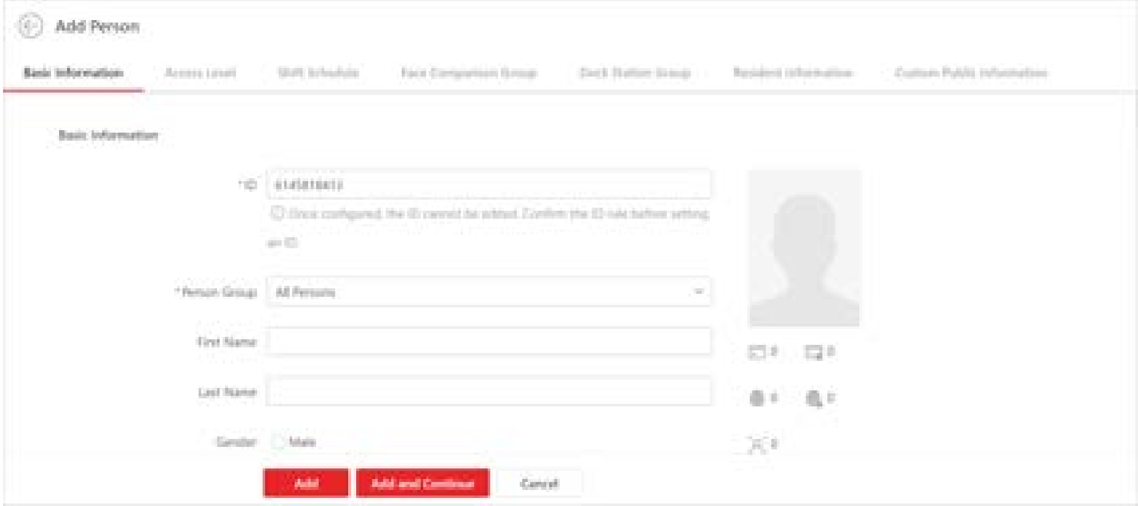


Figure 10-3 The Entry for Adding a Person



Add Person

Basic Information | Access Level | Shift Schedule | Face Comparison Group | Dock Station Group | Resident Information | Custom Public Information

Basic Information

*ID

Once configured, the ID cannot be edited. Confirm the ID rule before setting an ID.

*Person Group: All Persons

First Name

Last Name

Gender: ○ Male

Add | Add and Continue | Cancel

Figure 10-4 Add Person Page

4. Set the person's basic information, such as first name, last name, and gender.

ID (Required)

The default ID is generated by the platform. You can edit it if needed.

Note

- If the person is a police officer or a security guard with body cameras, make sure the person ID is same with the police ID configured on the body camera.
- The ID cannot be edited after finishing adding a person, so you should ensure its correctness at the beginning.

Person Group (Required)

Select a person group for the person.

Note

See ***Add Person Groups*** for details about how to add a person group.

Profile Picture

Hover the cursor onto , and you can select from three modes to add a picture.

From Device

You can select **Access Control Device**, **Video Intercom Device**, or **Enrollment Station** and set parameters (if required) to connect the device to the platform, and then collect the face picture via the 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.

Take a Picture

Click **Take a Picture** and then select one of the PC's webcams to take a picture.

Upload Picture

Click **Upload Picture** to select a picture from your PC.

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.
- You can switch on **Verify Profile Picture Quality** and select a device to check the quality of the profile picture. Click **Save** to start checking. You will be informed if the picture is not qualified.

Skin-Surface Temperature/Skin-Surface Temperature Status

Enter the person's skin-surface temperature and select the corresponding temperature status.

Note

For example, if a person's skin-surface temperature is 37 °C, then you can select her/his temperature status as normal.

Effective Period (Required)

Set the effective period for the person in applications such as access control application and time & attendance application, to determine the period when the person can access the specified access points with credentials. For example, if the person is a visitor, you can set a short effective period for the person.

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***.

Super User

If the person is set as a super user, the person 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.

PIN Code

Set the PIN code for access authentication. 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 Person Groups*** .

5. Add credential information for the person. See ***Manage Credentials*** for details.
6. Assign access levels to the person to define the access points where the person can access during the authorized period.
   1) Click **Assign**.
   2) Select one or more access levels for the person.
   3) 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.

7. **Optional:** View shift schedule of the person in the table.

Note

You can click ‹ or › to switch the time (month).

8. **Optional:** Add the person to the existing face comparison group(s) which will be used for face recognition and comparison.

Note

After adding the person to the face comparison group(s), you should apply the face comparison group(s) to a device to make the settings effective. For details about applying face comparison group to the device, refer to ***Apply Face Comparison Group to Device*** .

9. **Optional:** Add the person to the existing dock station group(s), and then set the login password which is used for the dock station(s) in the group to log into the body cameras.

   Note

   By default, the login password is 123456.

   The videos and pictures stored on the person's body camera can be copied to the person's linked dock station(s).

10. **Optional:** Set resident information to link the person with the indoor station and room number.

    Note

    - Make sure you have added indoor stations to the platform.
    - 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. In Custom Public Information area, select custom information to be applied.

    Note

    Make sure you have set the custom public information. See ***Customize Additional Information*** for details.

12. Finish adding the person.
    - Click **Add**.
    - 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.

13. **Optional:** After adding persons, 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 🗑 to delete the selected person(s).

    Delete All Persons
    Hover the cursor onto ⌄ beside 🗑 , and then click **Delete All** to delete all persons.

Clear Profile Pictures

Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Move Person

Follow the steps below to move the persons to another person group. Once moved, the access levels and shift schedules of the selected persons will be changed.

a. Select one or more persons, click .
b. Select the target person group to which the persons are about to be moved.
c. Click **Move**.

Clear Access Levels

Select one or more persons, click 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 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.

Export Person Information

Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

You can check **Linked Access Levels** or **Linked Shift Schedules** to export the additional information at the same time.

Export Profile Pictures

Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to **General → System Configuration → Security → Export Profile Pictures** page to check the **Export Profile Pictures**.

Link Persons to Indoor Stations

Select one or more persons, click and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

	Note • Make sure you have added indoor stations to the platform. • Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations. • Make sure the room number is consistent with the actual location information of the indoor station.
Filter Displayed Persons	Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required. **Note** When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

Manage Credentials

When adding a person, you can add the required credential information for the person. The supported credentials include normal cards, fingerprints, and special cards. These credentials can be used for the access authentication in applications such as access control and elevator control.

Steps

1. In the top left corner of the Client, select ■ → **All Modules** → **General** → **Person** .
2. On the adding or editing person page, click **Credential Management** under the profile picture to open the Add Credential pane.
3. 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.

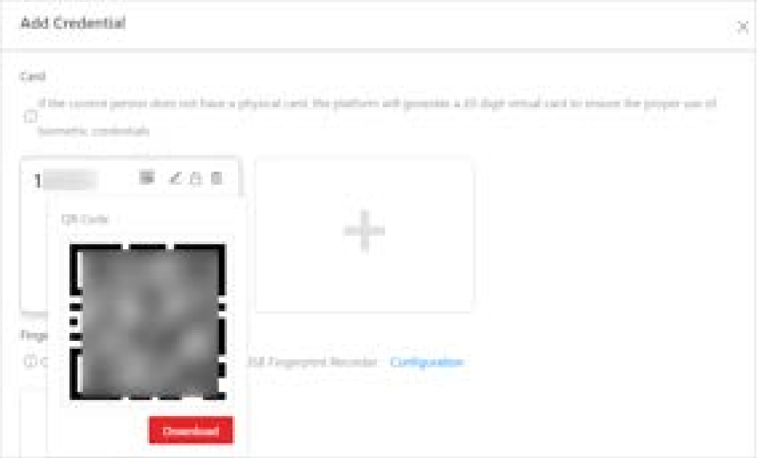


Figure 10-5 View QR Code of Card

4. In the Fingerprint area, click **Configuration** 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.
5. **Optional:** Switch on **Special Credential** and then add special cards and corresponding fingerprint information.
6. **Optional:** Perform the following operation(s).

Edit Card / Fingerprint Information	Hover the cursor onto an added card or fingerprint, and then click ✎ .
View and Download QR Code of Card	
Delete Card / Fingerprint	Hover the cursor onto an added card or fingerprint, and then click 🗑 .

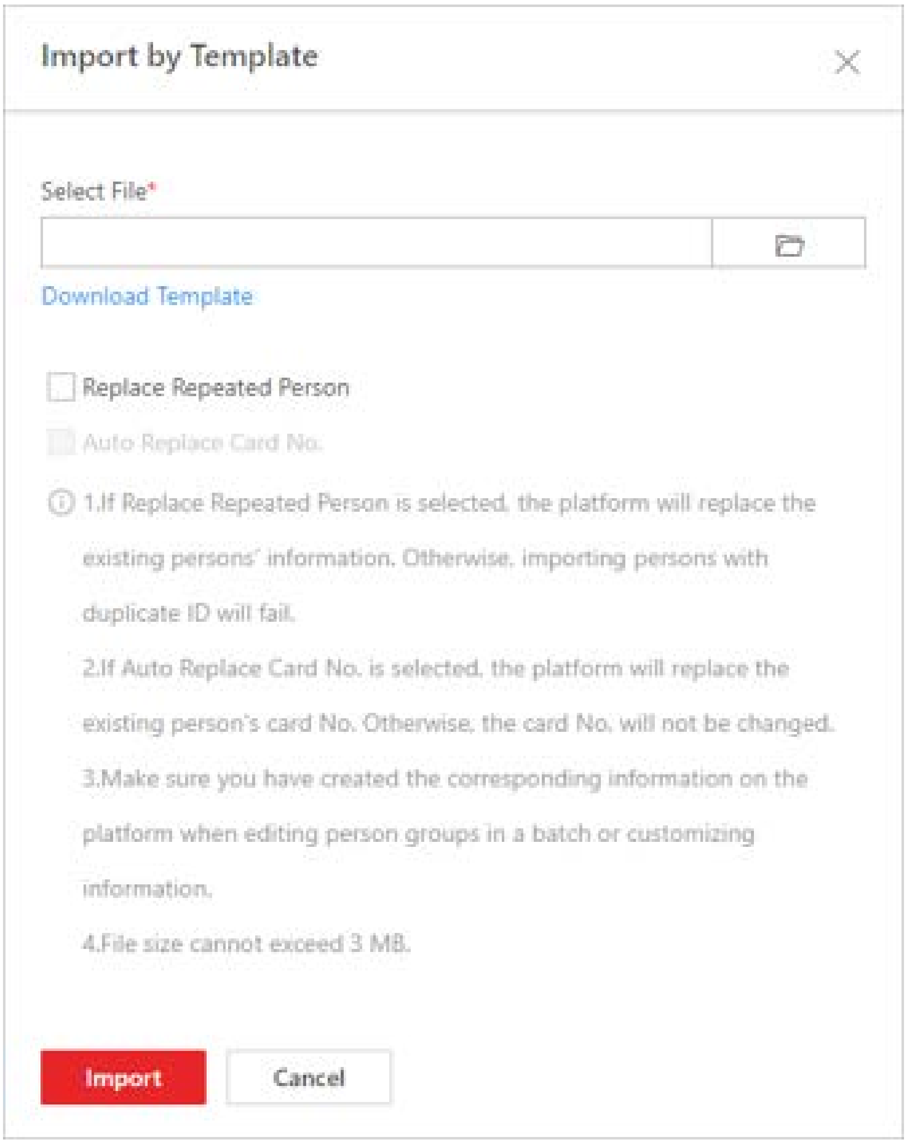
7. Click **Save**.

10.3.2 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 person group and the access levels.

Steps

1. In the top left corner of the Client, select → **All Modules** → **General** → **Person** .
2. Click → **Import by Template** .



Import by Template

Select File*

Download Template

□ Replace Repeated Person

□ Auto Replace Card No.

1.If Replace Repeated Person is selected, the platform will replace the existing persons' information. Otherwise, importing persons with duplicate ID will fail.

2.If Auto Replace Card No. is selected, the platform will replace the existing person's card No. Otherwise, the card No. will not be changed.

3.Make sure you have created the corresponding information on the platform when editing person groups in a batch or customizing information.

4.File size cannot exceed 3 MB.

Figure 10-6 Batch Add Persons by Template

3. In the pop-up window, click **Download Template** to save the template to your PC.

4. In the downloaded template, enter the person information following the rules shown in the template.
5. Click ▨ , and then select the template from your PC.
6. **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.
7. **Optional:** Check **Auto Replace Card No.** to replace the card No. automatically if it already exists in the platform.
8. 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.

9. **Optional:** After adding persons, 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 🗑 to delete the selected person(s).

Delete All Persons

Hover the cursor onto ⌄ beside 🗑 , and then click **Delete All** to delete all persons.

Clear Profile Pictures

Hover the cursor onto ⌄ beside 🗑 , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Move Person

Follow the steps below to move the persons to another person group. Once moved, the access levels and shift schedules of the selected persons will be changed.

a. Select one or more persons, click ✎ .
b. Select the target person group to which the persons are about to be moved.
c. Click **Move**.

Clear Access Levels

Select one or more persons, click ▨ 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 to enter the 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.

Export Person Information

Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

You can check **Linked Access Levels** or **Linked Shift Schedules** to export the additional information at the same time.

Export Profile Pictures

Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to **General → System Configuration → Security → Export Profile Pictures** page to check the **Export Profile Pictures**.

Link Persons to Indoor Stations

Select one or more persons, click and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to 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.

Filter Displayed Persons

Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

10.3.3 Import Profile Pictures

You can add multiple persons' profile pictures to the persons in a person group. 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.
   - 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. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Person** .
4. Click ✎ → **Import Profile Pictures** .
5. Select the profile 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.

6. Select a person group from **Person Group**.
7. **Optional:** Switch on **Verify Face Quality by Device** and then select a device for verifying the face quality.
8. Click **Import** to start importing.

   The importing progress shows and you can check the results.
9. **Optional:** After importing profile pictures, click **Export Failure Details** to export an Excel file to the local PC and view the failure details.

10.3.4 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. See ***Set Active Directory*** for details.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **General** → **Person** .
2. Click ⇥ → **Import Domain Persons** to enter the Import Domain Persons page.
3. Select the importing mode.

   Person

   Import the 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.

   Group

   Import all the persons in the organization unit. The person information will be synchronized based on each group.

   Security Group

   Import the selected security groups in the AD domain.

   Note

   Make sure you have set security groups.
4. **Optional:** When selecting **Person** or **Security Group** as the importing mode, select a person group to which the selected items (persons or security groups) need to be imported.
5. Set the effective period for the persons as needed.
6. Complete importing the domain persons.
   - Click **Add**.
   - Click **Add and Continue** to save the settings and continue to add persons.

7. **Optional:** Click the person name shown in the person list to view and edit the person information.

   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. For linking the person information in the domain to the person information in the platform, refer to ***Set Active Directory*** .
   - 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. For linking the person information in the domain to the person information in the platform, refer to ***Set Active Directory*** .

8. **Optional:** After adding persons, 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 🗑 to delete the selected person(s).

   Delete All Persons

   Hover the cursor onto ⌄ beside 🗑 , and then click **Delete All** to delete all persons.

   Clear Profile Pictures

   Hover the cursor onto ⌄ beside 🗑 , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

   Move Person

   Follow the steps below to move the persons to another person group. Once moved, the access levels and shift schedules of the selected persons will be changed.

   a. Select one or more persons, click ⇄ .
   b. Select the target person group to which the persons are about to be moved.
   c. Click **Move**.

   Clear Access Levels

   Select one or more persons, click ▨ 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 to enter the 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.

Export Person Information

Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

You can check **Linked Access Levels** or **Linked Shift Schedules** to export the additional information at the same time.

Export Profile Pictures

Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to **General → System Configuration → Security → Export Profile Pictures** page to check the **Export Profile Pictures**.

Synchronize Domain Persons

Select person(s) whose information has changed in the AD domain and click at the top of person list to get the latest person information.

Link Persons to Indoor Stations

Select one or more persons, click and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

Filter Displayed Persons

Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

10.3.5 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. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Person** .
2. Click ☰ → **Import from Device** .
3. Select **Access Control Device** or **Video Intercom Device** as the device type.
4. Select one or more devices from the device list.

   Note

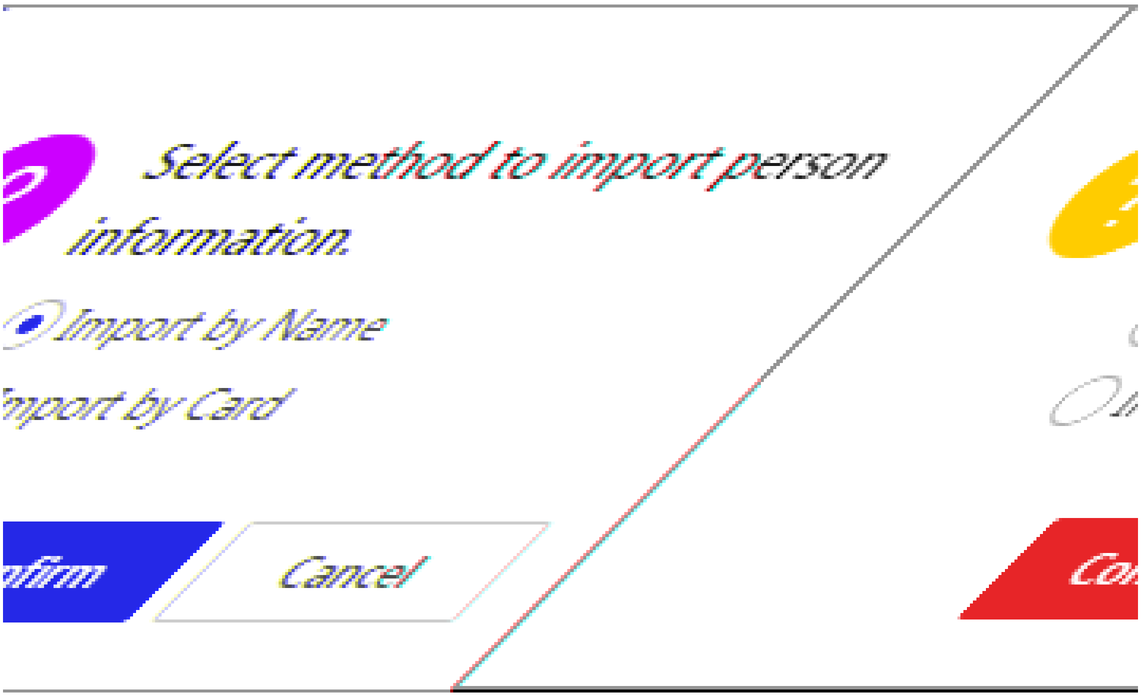
   You can enter a key word (fuzzy search supported) in the search box to search the target device(s) quickly.
5. Select a person group to which the persons will be imported.
6. **Optional:** Check **Replace Profile Picture** to replace the existed person profile pictures with the new ones from the devices.
7. 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.
8. If the following window pops up, select a method to import the person information.

   Note

   If not, skip this step.



Select method to import person information.

● Import by Name

mport by Card

nfirm

Cancel

Figure 10-7 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.

9. **Optional:** 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 Person

Select one or more persons and click 🗑 to delete the selected person(s).

Or hover the cursor onto beside , and then click **Delete All** to delete all persons.

Export Added Person Information

Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Export Profile Pictures

Click → **Export Profile Pictures** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

This function is available after you have enabled exporting profile pictures. Go to **System Configuration → Security → Export Profile Pictures** to enable this function.

Filter Person

Set conditions such as full name and ID, and then click **Filter**.

Move Persons

Follow the steps below to move the persons to another person group. Once moved, the access levels and shift schedules of the selected persons will be changed.

a. Select one or more persons, click .
b. Select the target person group to which the persons are about to be moved.
c. Click **Move**.

Link Persons to Indoor Stations

Select one or more persons, click and then select an indoor station for each person to apply the person information to the indoor station.

Note

- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to 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.

Clear Access Levels

Select one or more persons, click to clear the access levels of the selected persons.

Note

The cleared access levels of the persons cannot be restored.

Clear Profile Pictures

Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Check Person Authorization

Select one or more persons, click 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.

10.3.6 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. In the top left corner of Home page, select → **All Modules** → **General** → **Person** .
2. Click → **Import 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. Select **Enrollment Station** from the device list.
6. Set device address, port No., user name and password for accessing the enrollment station.
7. 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 person group 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 person group to which the person and credential information will be imported to.

8. Click **Import** to start importing.
9. **Optional:** 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 Person

Select one or more persons and click 🗑 to delete the selected person(s).

Or hover the cursor onto ⌄ beside 🗑 , and then click **Delete All** to delete all persons.

Export Added Person Information

Click ⇥ → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Export Profile Pictures

Click ⇥ → **Export Profile Pictures** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

This function is available after you have enabled exporting profile pictures. Go to **System Configuration → Security → Export Profile Pictures** to enable this function.

Filter Person

Set conditions such as full name and ID, and then click **Filter**.

Move Persons

Follow the steps below to move the persons to another person group. Once moved, the access levels and shift schedules of the selected persons will be changed.

a. Select one or more persons, click .
b. Select the target person group to which the persons are about to be moved.
c. Click **Move**.

Link Persons to Indoor Stations

Select one or more persons, click and then select an indoor station for each person to apply the person information to the indoor station.

Note

- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to 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.

Clear Access Levels

Select one or more persons, click to clear the access levels of the selected persons.

Note

The cleared access levels of the persons cannot be restored.

Clear Profile Pictures

Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Check Person Authorization

Select one or more persons, click 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.

10.4 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

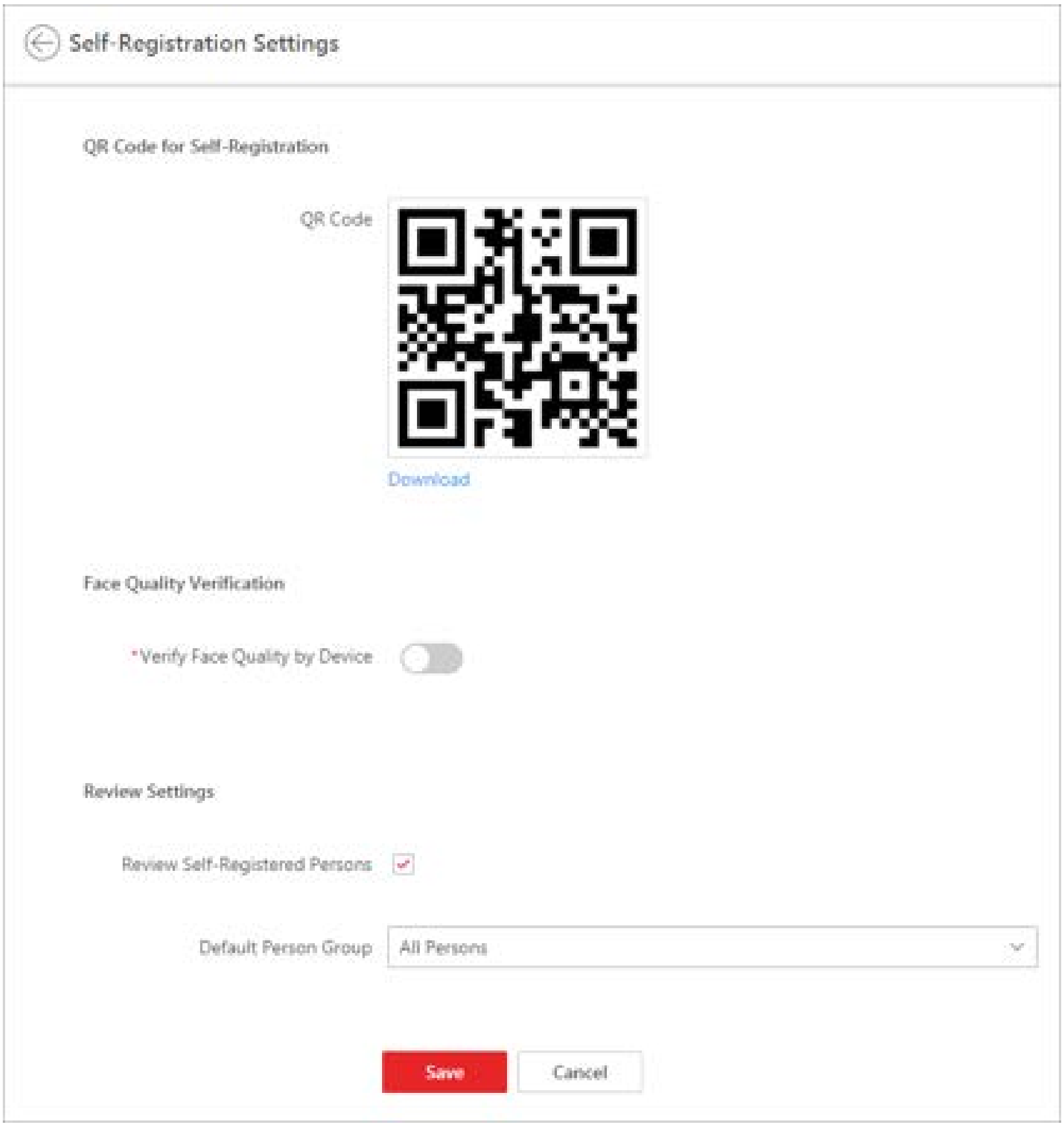
You should set self-registration parameters beforehand. See ***Set Self-Registration Parameters*** for details.

10.4.1 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.

In the top left corner of Home page, select ■ → **All Modules** → **General** → **Person** , and click ∨ beside ▤ , and then click **Self-Registration Settings** to enter the Self-Registration Settings page.

1.



Self-Registration Settings

QR Code for Self-Registration

QR Code

Download

Face Quality Verification

*Verify Face Quality by Device ○

Review Settings

Review Self-Registered Persons ☑

Default Person Group: All Persons

Figure 10-8 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 person group. 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 person group. See ***Review Self-Registered Person Information*** for details about how to review.

10.4.2 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, gender, 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.

10.4.3 Review Self-Registered Person Information

If you have enabled **Review Self-Registered Persons** 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 person group.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **General** → **Person** , and click ⌄ beside , and then click **Persons to be Reviewed** to enter the Persons to Be Reviewed page.
2. **Optional:** Click ▽ to filter registered persons by name, ID, gender, or status to quickly find your wanted persons.
3. 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.

Note

Approved persons will be added to the target person group; rejected persons will not be added to the target person group, but they will stay in the Persons to be Reviewed list.

10.5 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. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Person** .
2. Select persons to whom the cards will be issued.
3. Hover the cursor onto ▦ , and then click **Batch Issue Cards to Persons**.
4. 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*** .
5. 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.
6. Click **Start** to start issuing cards.
7. Repeat step 5 to issue the cards to the persons in the list in sequence.

   Note

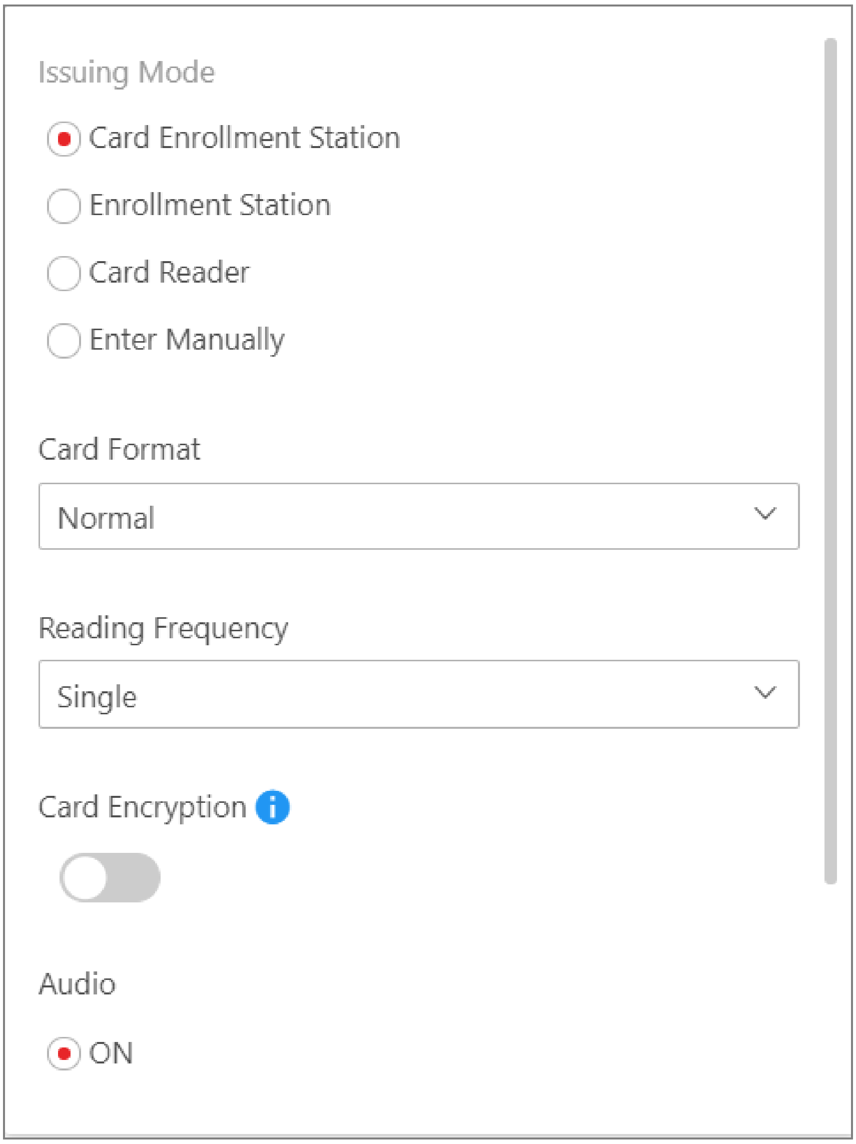
   You cannot change the card issuing mode once you issue one card to one person.
8. Click **Save**.

10.5.1 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. In the top left corner of the Client, select 🟥 → **All Modules** → **General** → **Person** .
2. 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.



Issuing Mode

● Card Enrollment Station

○ Enrollment Station

○ Card Reader

○ Enter Manually

Card Format: Normal

Reading Frequency: Single

Card Encryption: off

Audio

● ON

Figure 10-9 Card Issuing Settings Window Opened when Batch Issuing Cards to Persons

3. 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 Format

If the card 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 format, 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

4. Click **Save** (for Credential Management) or **Start** (for Batch Issue Cards to Persons).

10.6 Report Card Loss

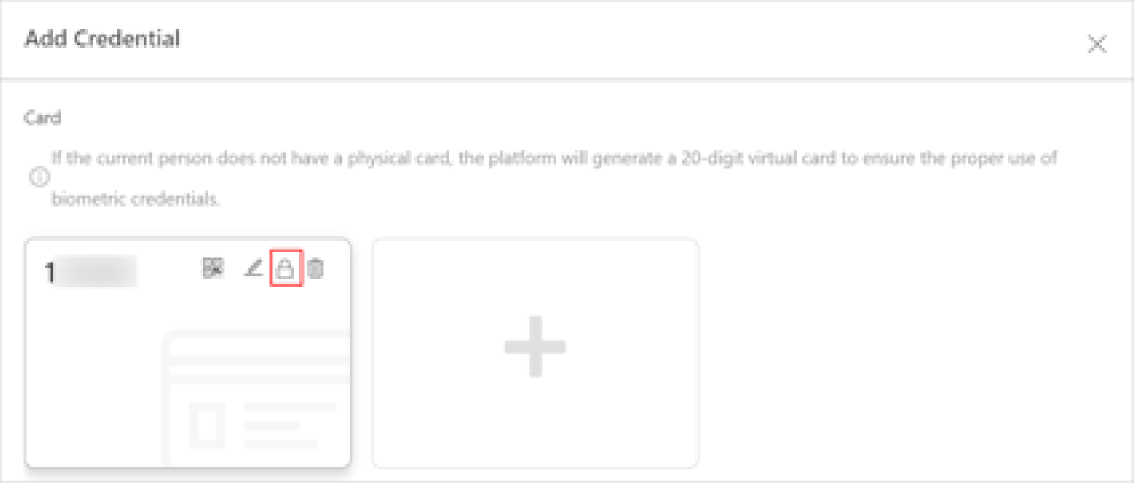
If a person cannot find her/his card, he/she should contact the card issuer as quickly as possible and the card issuer should report card loss via Web Client immediately to freeze the access level of the lost card. The card issuer can issue a temporary card with effective period and access level to the 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.

10.6.1 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. In the top left corner of the Client, select 🟥 → **All Modules** → **General** → **Person** .
2. **Optional:** On the Filter pane, click ▾ and set more conditions to search for persons for whom you want to report card loss.
3. 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.



Add Credential

Card

If the current person does not have a physical card, the platform will generate a 20-digit virtual card to ensure the proper use of biometric credentials.

Figure 10-10 Add Credential Panel

4. In the Card area, move the cursor onto the lost card and then click 🔒 .
5. Click **OK** to confirm the operation.
6. Click **Save**.

   After you report card loss, the access levels of the lost card will be inactive.
7. **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.

10.6.2 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. In the top left corner of the Client, select ☰ → **All Modules** → **General** → **Person** .
2. **Optional:** On the Filter pane, click ▾ and set more conditions to search for the person to whom you want to issue the temporary card.
3. Click the name of the person in the person list to enter the basic information page.
4. Click **Credential Management** to open the Add Credential pane.
5. In the Card area, click + .
6. Click **OK** to confirm the operation.

7. Enter the card number.
8. 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 Person Manually*** .

9. 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.

10. 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 .

10.6.3 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. In the top left corner of Home page, select → **All Modules** → **General** → **Person** .
2. **Optional:** On the Filter pane, click and set more conditions to search for the persons for whom you want to cancel card loss reports.
3. Select the persons in the person list.
4. Move the cursor onto , and then click **Cancel Card Loss**.

   The persons' temporary cards will be deleted.

10.7 Customize Additional Information

You can add additional information items as the options for configuring a person's basic information. The platform allows you to customize two types of additional information items: custom private information items and custom public information items. 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.

The following figure shows the custom private information items (marked in red rectangles) on the Add Person page. See ***Add a Person Manually*** for details about how to add a person.

Figure 10-11 Custom Private Information Item as Configuration Option

Steps

Note

- You can customize up to 20 private information items and 20 public information items.
- The system administrator can define whether a user has the permission to view the custom private information when setting permissions for a user (see ***Add Role***). For information security, the system administrator needs to make sure the custom private information is only viewable to specific users.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Person** .
2. Click ⚙ **Customize Additional Information** to enter the customizing addition information page.
3. Click **Add**.
4. Create a name for the item.

Note

You can enter up to 32 characters.

5. Select the type to restrict the format of the contents of the item.

Example

For example, if you select **General Text**, entering text information as the content of the item is required 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).

Figure 10-12 If You Select Date as the Type

6. Click **Save**.
7. **Optional:** Perform the following operation(s) if needed.

Edit Name Click ✎ to edit the name of the additional information item.

Delete Click 🗑 to delete the additional information item.

Note

You cannot delete the additional information item linked with person information in the domain.

10.8 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. For details, see ***Set Printer*** .
- Make sure you have added card templates to the platform. For details, see ***Set Card Template*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Person** .
2. **Optional:** Set conditions to search for the target persons.
3. Select the persons for whom you need to print cards.
4. Click ✎ to open the Print Card window.
5. Select a card template from **Card Template**.
6. Select a printer from **Printer**.
7. Select person(s) from the Selected Person list.
8. Click **Front** and **Back** to preview the information to be printed on the front and back of the physical cards.
9. Click **Print**.

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 Person Manually

Chapter 11 Role and User Management

The system allows you to add users and assign user's permissions for accessing and managing the system. Before adding users to the system, you should create roles to define the user's access rights to system resources and then assign the role to the user for granting the permissions to the user. A user can have many different roles.

11.1 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.

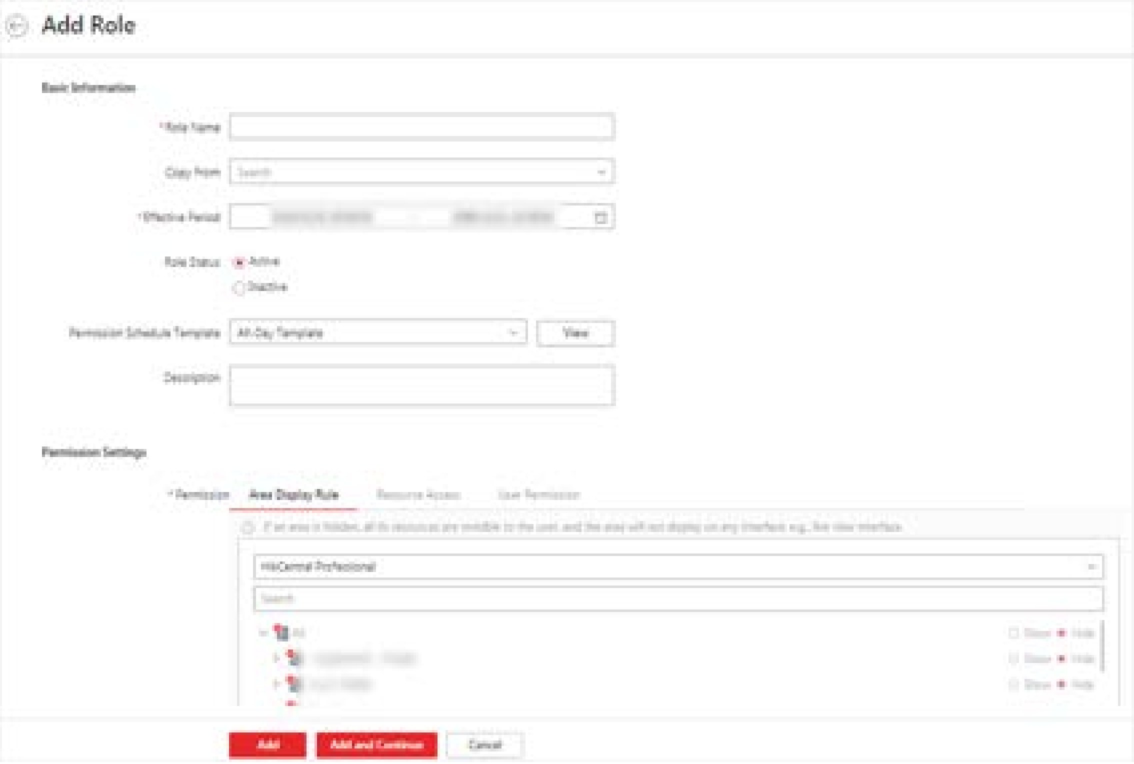
Administrator

Role that has all permissions of the platform.

Operator

Role that has all permissions for operating the Control Client and has the permission for operating the Applications (Live View, Playback, and Local Configuration) on the Web Client.

1. On the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Account and Security** .
2. Click **Roles** on the left.
3. Click **Add**.



Add Role

Basic Information

*Role Name

Copy From: Search

*Effective Period

Role Status: ● Active ○ Inactive

Permission Schedule Template: All-Day Template

Description

Permission Settings

*Permission: Area Display Rule | Resource Access | User Permission

If an area is hidden, all its resources are invisible to the user, and the area will not display on any interface e.g., live view interface.

HikCentral Professional

Search

All

Figure 11-1 Add Role Page

4. 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.

   Effective Period

   Set the time range within which the role takes effect. The role is inactive outside the effective period.

   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 New** 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.

5. 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.

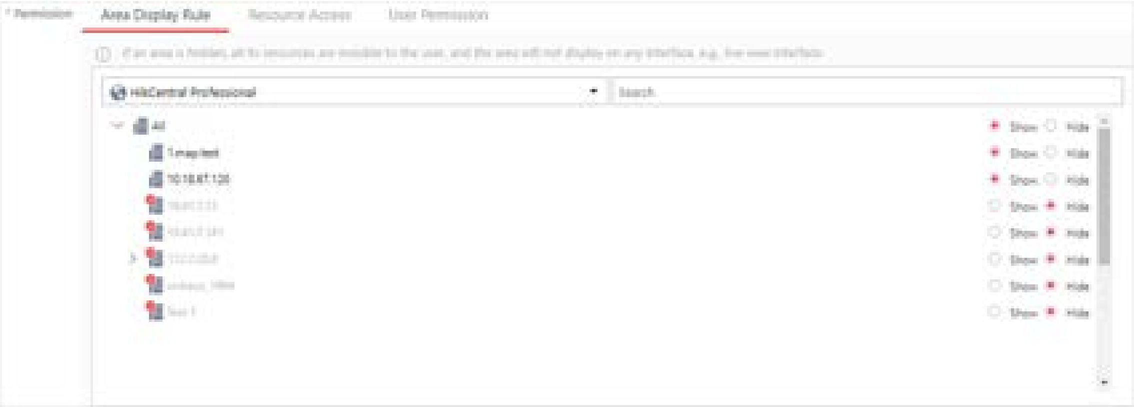


Figure 11-2 Area Display Rule

Resource Access Permission

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.

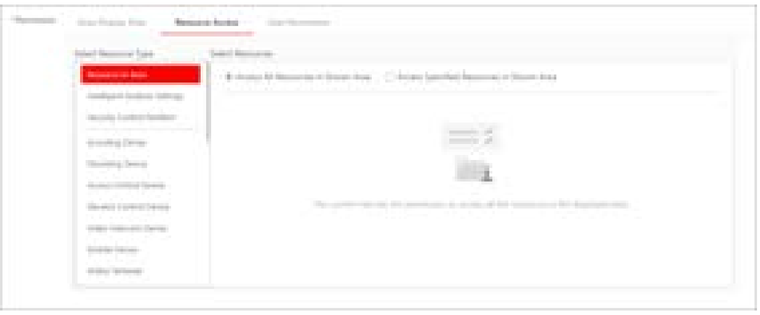


Figure 11-3 Resource Access Permission

User Permission

Assign resource permissions, configuration permissions, and operation permissions to the role.

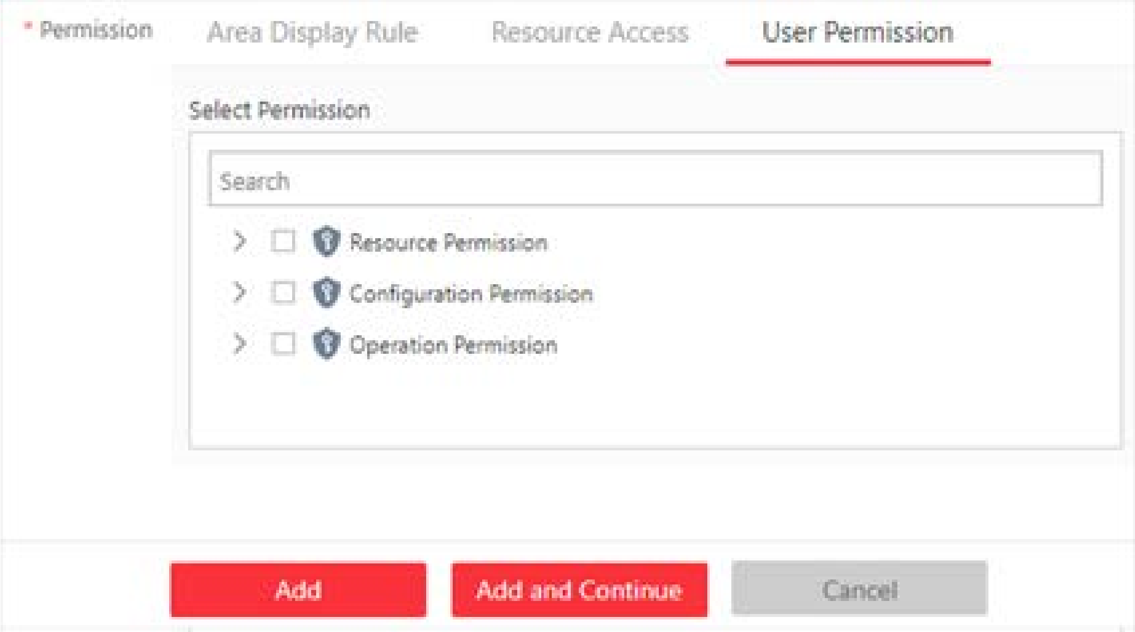


Figure 11-4 User Permission

Note

In **Resource Permission**, you can set time restriction for video playback permission. Once set, the role's permission of viewing and downloading video playback will be restricted within the configured time period. For example, if you set restriction for recent video to 6 minutes, the role can only view video playback of the last 6 minutes.

Figure 11-5 Playback Permission

6. Do one of the following to complete adding the role.
   - Click **Add** to add the role and return to the role management page.
   - Click **Add and Continue** to save the settings and continue to add another role.
7. **Optional:** Perform further operations on added roles.

Edit Role	Click role name to view and edit role settings.
Delete Role	Check a role and click **Delete** to delete the role.

Inactivate Role Check a role and click **Inactivate** to set the role status to **Inactive**.

Activate Role Check an inactive role and click **Activate** to set the role status to **Active**.

Refresh Role Click **Refresh All** to get the latest status of the roles.

Filter Role Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the roles according to the set conditions.

11.2 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. On the top left corner of Home page, select ■ → **All Modules** → **General** → **Account and Security** .
2. Click **Users** on the left.
3. Click **Add**.
4. Set basic information for the user.

User Name

Can contain letters (a-z, A-Z), digits (0-9), and "-" only.

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.

Note

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

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

If you select **Inactive**, the user account will be inactivated until you activate it.

Restrict Concurrent Logins

To limit the maximum IP addresses logged in to the system using the user account, switch on **Restrict Concurrent Logins** and set the maximum number of concurrent logins.

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 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.

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.

11.3 Import Domain Users

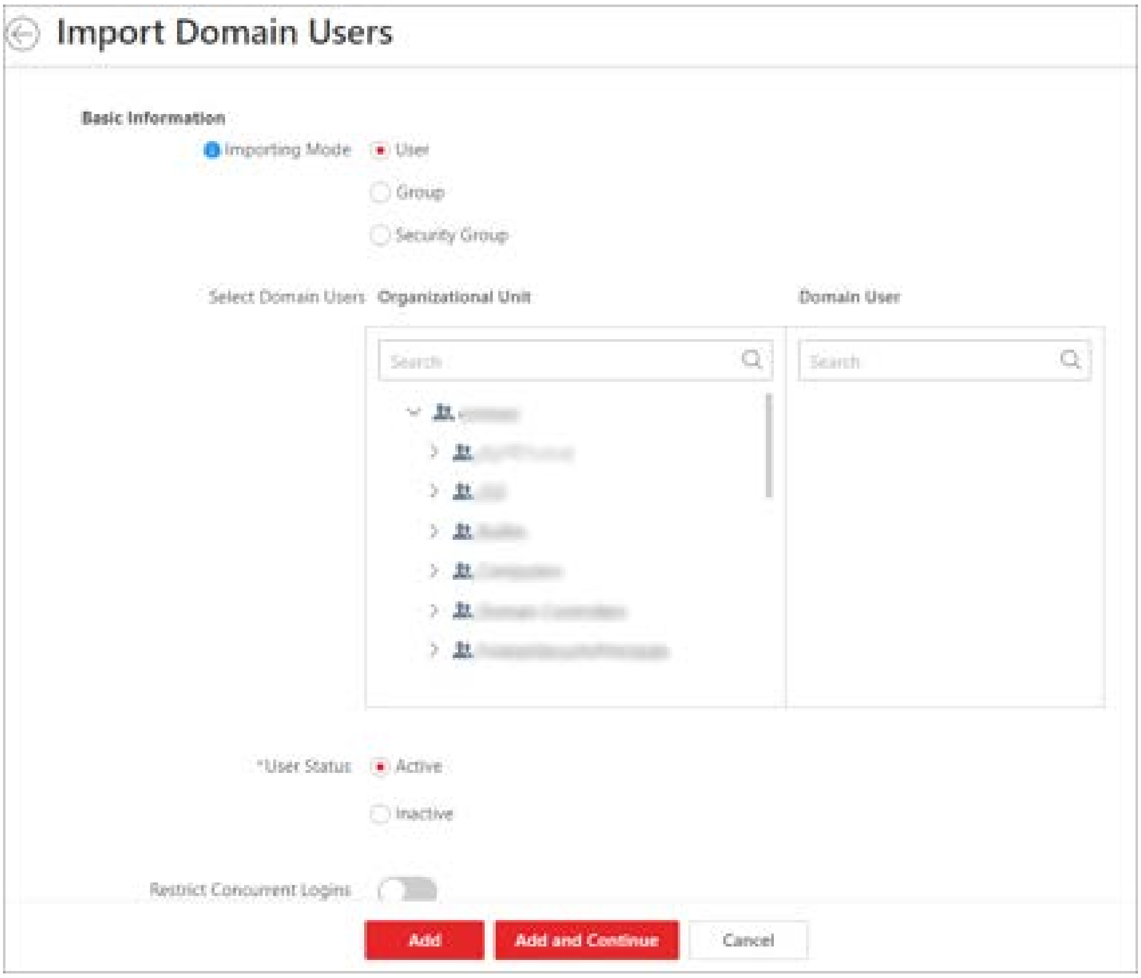
You can batch import the users (including the user name, real name, and email) in the AD domain to the platform and assign roles to the domain users.

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 🟥 → **All Modules** → **General** → **Account and Security** .
2. Click **Users** on the left.
3. Click **Import Domain Users**.



Import Domain Users

Basic Information

Importing Mode ● User ○ Group ○ Security Group

Select Domain Users Organizational Unit Domain User

*User Status ● Active ○ Inactive

Restrict Concurrent Logins

Figure 11-6 Import Domain Users

4. 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.

   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.

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

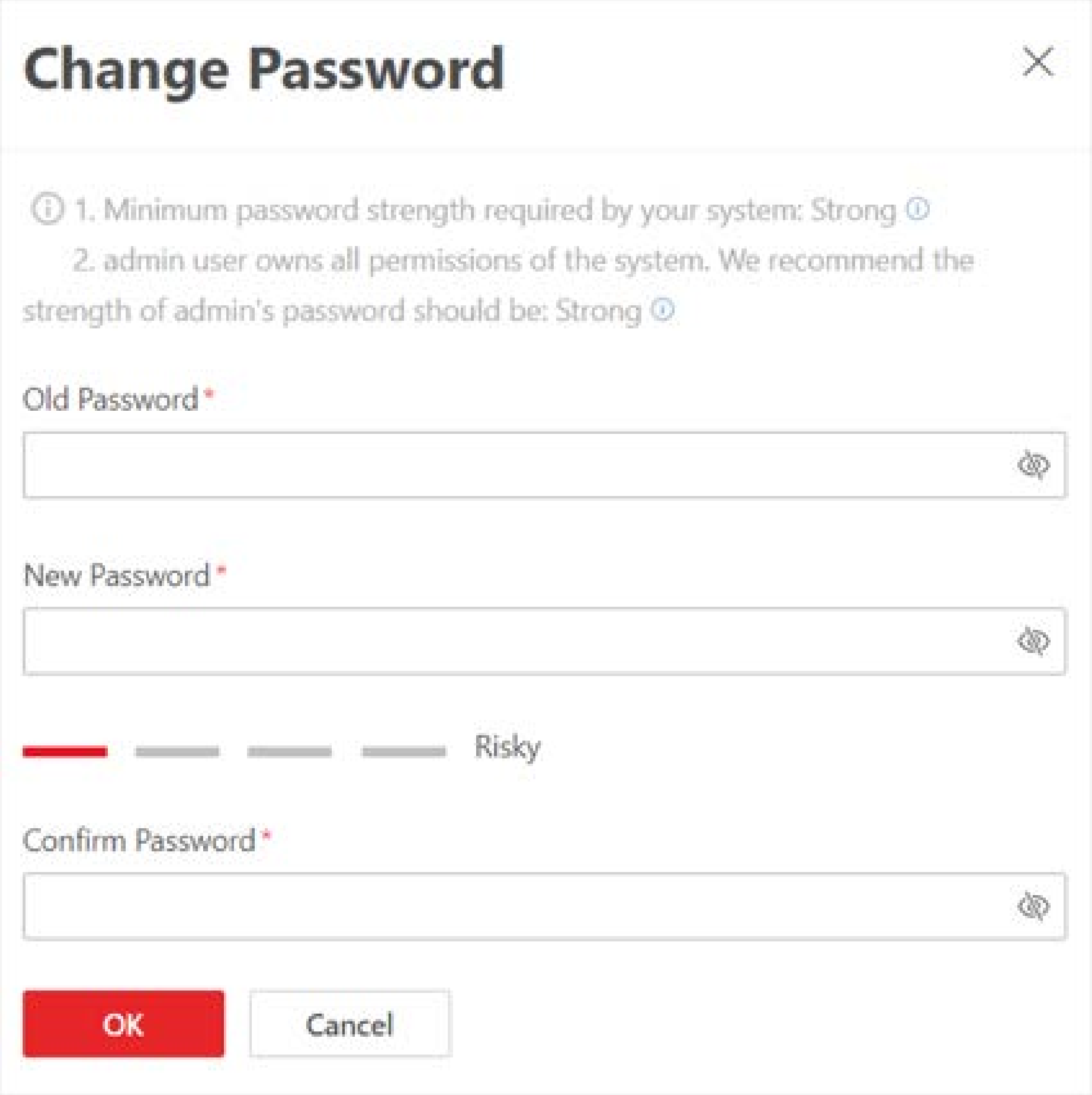
After successfully adding the domain users, the users can log in to the HikCentral Professional via the Web Client, Control Client, and Mobile Client with their domain accounts and passwords.

11.4 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.



Change Password

ⓘ 1. Minimum password strength required by your system: Strong ⓘ

2. admin user owns all permissions of the system. We recommend the strength of admin's password should be: Strong ⓘ

Old Password *

New Password *

Risky

Confirm Password *

Figure 11-7 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.

11.5 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, Weekday Template, and Weekend Template. You can add new templates according to actual needs.

Steps

1. In the top left corner of Home page, select ■ → **All Modules** → **Account and Security** .
2. Click **Permission Schedule Template** on the left.
3. Click + to create a blank template.
4. 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.
5. 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.
6. **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.
7. Click **Add** to add the permission schedule template.
8. **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

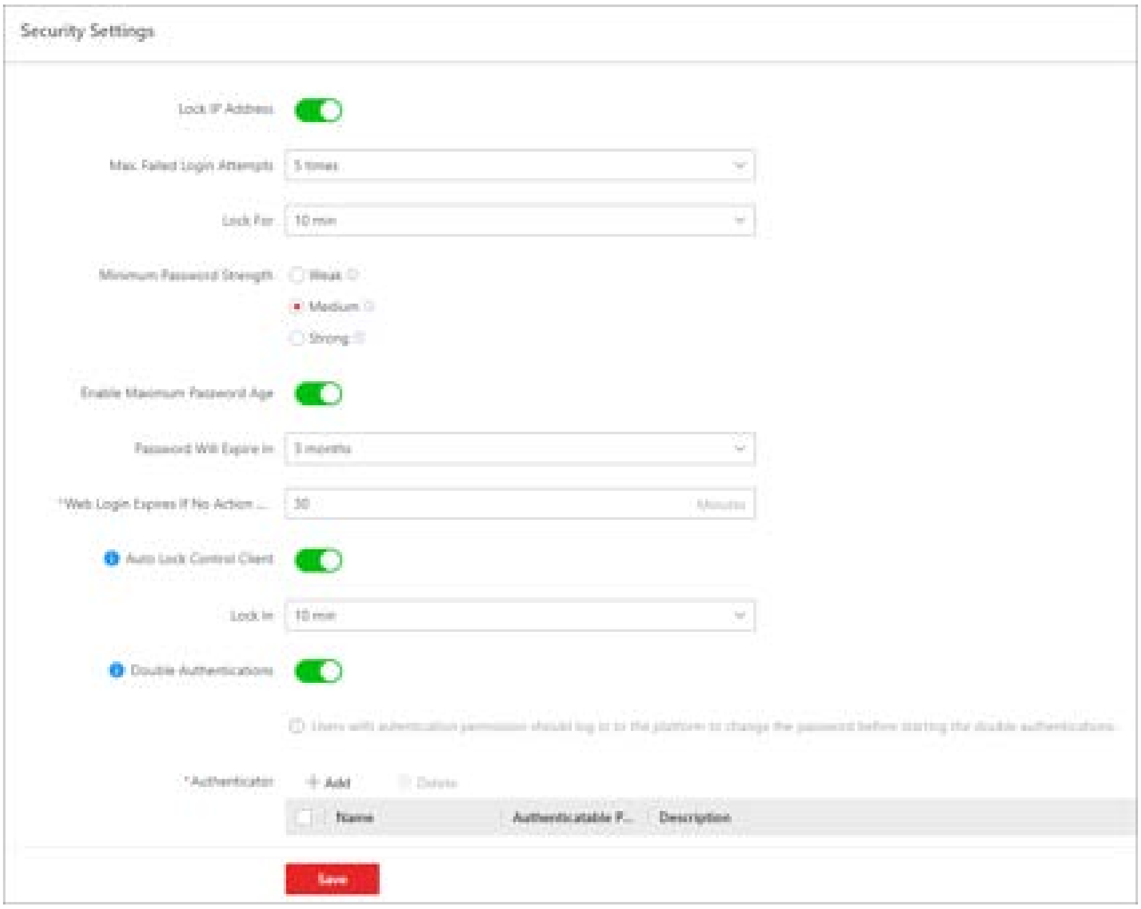
Set permission schedules for roles to define in which period the permissions for the roles are valid. For details, refer to ***Add Role*** .

Chapter 12 System Security Settings

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. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Account and Security** .
2. Click **Security Settings** on the left.



Security Settings

Lock IP Address: ●
Max. Failed Login Attempts: 5 times
Lock For: 10 min
Minimum Password Strength: ○ Weak ● Medium ○ Strong
Enable Maximum Password Age: ●
Password Will Expire in: 3 months
*Web Login Expires If No Action ...: 30 Minutes
Auto Lock Control Client: ●
Lock In: 10 min
Double Authentications: ●
Users with authentication permission should log in to the platform to change the password before starting the double authentications.
*Authenticator: + Add Delete

□	Name	Authenticatable P...	Description

Figure 12-1 Security Settings Page

3. Switch on **Lock IP Address** to limit the number of failed login attempts.
   1) Select the allowable login attempts for accessing HikCentral Professional.

Note

Failed login attempts include failed password attempt and failed verification code attempt.

2) Set the locking duration for this IP address. During the locking duration, the login attempt via this IP address is not allowed.

The number of login attempts is limited.

4. Select the **Minimum Password Strength** to define the minimum complexity requirements that the password should meet.
5. Set the maximum password age.
   1) Switch on **Enable Maximum Password Age** 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.
6. Set minutes after which the Web login will expire if there is no actions during the set minutes.
7. 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.
8. 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.
9. Click **Save** to save the above settings.

Chapter 13 Event and Alarm Configuration

You can set the linkage actions for the detected events and alarms. The detailed information of the events and alarms can be received and checked via the Control Client and the Mobile Client.

Event

Events can be divided into:

Generic Event

The signal that resource (e.g., other software, device) sends when something occurs, and can be received in the form of TCP or UDP data packages, which the system can analyze, and generate events if they match configured expression.

User-Defined Event

The user-defined event can be used to:

- The user can trigger a user-defined event manually in Monitoring and Alarm Center module on the Control Client when viewing the video or checking the alarm information.
- A user-defined event can trigger an alarm if configured.
- An alarm will be armed or disarmed when the user-defined event is triggered.
- An alarm can trigger a user-defined event as alarm actions.

Alarm

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. An alarm can trigger a series of linkage actions (e.g., popping up window) for notification and alarm handling.

Linkage Actions

You can set linkage actions for both events and alarms.

- An event's linkage actions are used to record the event details (such as recording and capturing) and trigger basic actions (such as linking access point to lock or unlock, triggering alarm output, sending email, etc.).
- An alarm's linkage actions are used to record the alarm details and provide the recipients multiple ways to view alarm information for alarm acknowledgment and handling, such as popping up alarm window, displaying on smart wall, audible warning, etc.

13.1 About Event and Alarm

Event

Event is the signal that resource (e.g., device, camera, server) sends when something occurs. System can receive and record event 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, pop-up window on the Control Client, etc.). You can check the event related video and captured pictures via the Control Client if you set the recording and capturing as event linkage.
The rule of an event includes four elements, namely, "**event source**" (i.e., the device which detects the event), "**triggering event**" (specified event type), "**what to do**" (linkage actions after this alarm is triggered), and "**when**" (during specified time period, the linkage actions can be triggered).

Example
The event can be defined as intrusion (**triggering event**) which happens in the bank vault and be detected by cameras mounted in the bank vault (**event source**) on weekend (**when**), and trigger the camera to start recording (**what to do**) once happened.

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 on the Control Client, showing the alarm details) for notification and alarm handling. You can check the received real-time alarm message via the Control Client and search the history alarms.
The rule of an alarm includes six elements, namely, "**alarm source**" (i.e., the device which detects the triggering event), "**triggering event**" (specified event type occurred on the alarm source and triggers the alarm), "**when**" (during specified time period, the alarm can be triggered), "**recipient**" (the user in the system who can receive this alarm), "**priority**" (the priority of this alarm), and "**what to do**" (linkage actions after this alarm is triggered). Besides these five elements, you can also set other properties for this alarm such as alarm description, etc.

Example
The alarm can be defined as intrusion (**triggering event**) which happens in the bank vault and be detected by cameras mounted in the bank vault (**alarm source**) on weekend (**when**), and trigger the camera to start recording (**what to do**) once happened. this alarm is marked as High priority (**priority**), and users including admin and operators (**recipient**) can receive this alarm notification and check the alarm details.

13.1.1 Supported Events and Alarms

Currently, the system supports events and alarms for the following types of resources:

Video

Camera

The video exception or the events detected in the monitoring area of the camera, such as motion detection, line crossing, and so on.

Alarm Input

The event or alarm triggered by the alarm input of the video device in the system.

Face

The event or alarm detected by facial recognition camera or temperature screening cameras, such as face matched event or alarm, face mismatched event or alarm, rarely appeared event or alarm, abnormal skin-surface temperature, no mask event or alarm, etc.

Access Control

Door

The access control event or alarm triggered at the doors (doors of access control devices and video intercom devices), such as access event, door status event, etc.

Elevator

The elevator control event or alarm triggered in the elevators, such as card swiping event, elevator status event, etc.

Alarm Input

The event or alarm triggered by the alarm input of the access control device in the platform.

Person

The event triggered by card number or person matched with that in the platform.

Vehicle

Vehicle Features

The event triggered by license plate number and vehicle types matched with that in the platform, and license plate number mismatched with that in the platform.

Parking Lot

The events or alarms triggered by different parking lots.

Alarm

Security Radar

The radar arming event or alarm and the event ot alarm detected by the radars, such as auto-arming event, line crossing event, etc.

Alarm Input

The event or alarm triggered by the alarm input of the resources in the system, such as a smoke detector and zones of a security control panel.

Intelligent Analysis Group

The alarm or pre-alarm triggered when people amount in a region is more/less than the threshold.

Maintenance

The operating exceptions of the resources (e.g. camera, door, UVSS, dock station, recording server, security audit server) added to the system, such as camera offline, server exception, and so on.

User-Defined Event

The event or alarm triggered by the user-defined event added in the system.

Generic Event

You can customize the expression to create a generic event to analyze the received TCP and/or UDP data packages, and trigger events when specified conditions are met. In this way, you can easily integrate your system with a very wide range of external sources, such as access control systems and alarm systems. See ***Configure Generic Event*** for details.

Digital Signage

The event or alarm triggered in the Digital Signage, such as abnormal temperature and person amount more than threshold.

Visitor

The alarm triggered by visitors not checked out in effective period.

Note

You should enable the alarm detection frequency of auto checkout for visitor after effective period. See ***Set Basic Parameters*** for details.

Broadcast

The event triggered by alarm input linked with the IP speaker. When an event is triggered in the alarm input, the IP speaker will start broadcasting.

Security Inspection

The alarms triggered by walk-through metal detectors.

Mobile Monitoring

The alarms triggered by ADAS (advanced driver assistance system) events, driver behavior, and vehicles.

13.1.2 Define Alarm Priority, Alarm Category, and Alarm Icon

The system predefines several alarm priorities, alarm categories, and alarm icons for basic needs. You can edit the predefined alarm priority and alarm category, and set customized alarm priority and alarm category according to actual needs.

Steps

Note

Alarm Priority

Define the priority for the alarm when add the alarm and filter alarms in the Control Client.

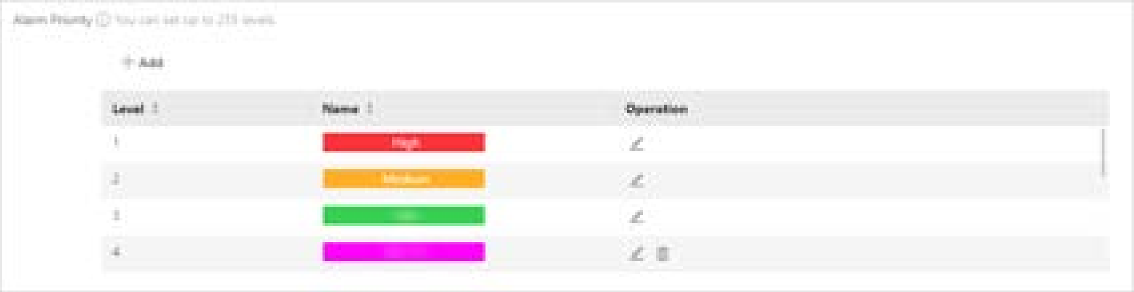
Alarm Category

Alarm category is used when the user acknowledges the alarm in the Control Client and categories what kind of alarm it is, e,g., false alarm, or alarm to be verified. You can search the alarms by the alarm type in the Alarm Center of Control Client.

Alarm Icon When Alarm Occurs

The system pre-defines some icons of resources for several special alarms.
For example, it pre-defines 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 the users.

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **Alarm Custom Settings** to enter the alarm custom settings page.
2. Set the alarm priority according to actual needs. By default, three kinds of alarm priority exist.



Alarm Priority ⓘ You can set up to 255 levels.

+ Add

Level	Name	Operation
1	High	✎
2	Medium	✎
3	Low	✎
4	[illegible]	✎ 🗑

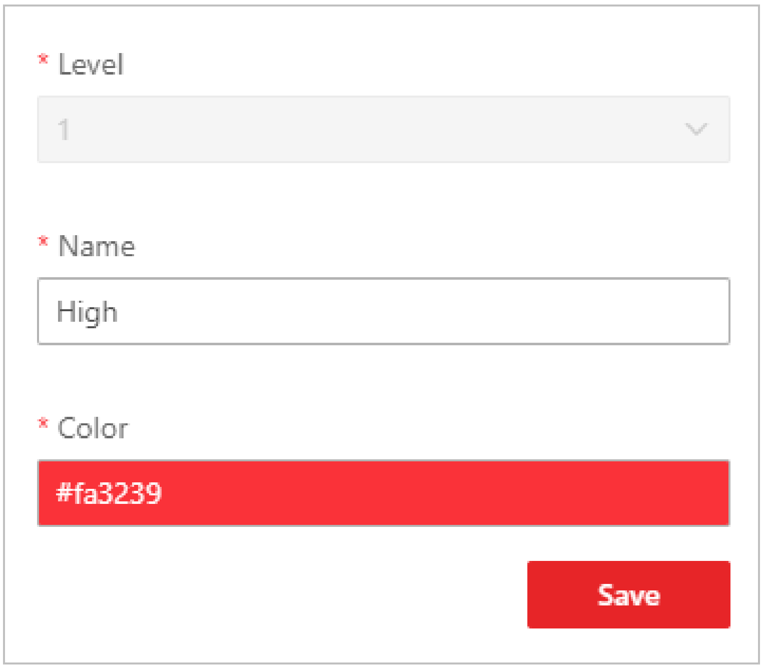
Figure 13-1 Alarm Priority

1) Click **Add** to add a customized priority.

Note

Up to 255 levels of alarm priority can be added. The priority levels can be used for sorting alarms in Alarm Center of Control Client.

2) Select a level No. for the priority.
3) Enter a descriptive name for the priority.
4) Select the color for the priority.



* Level

1

* Name

High

* Color

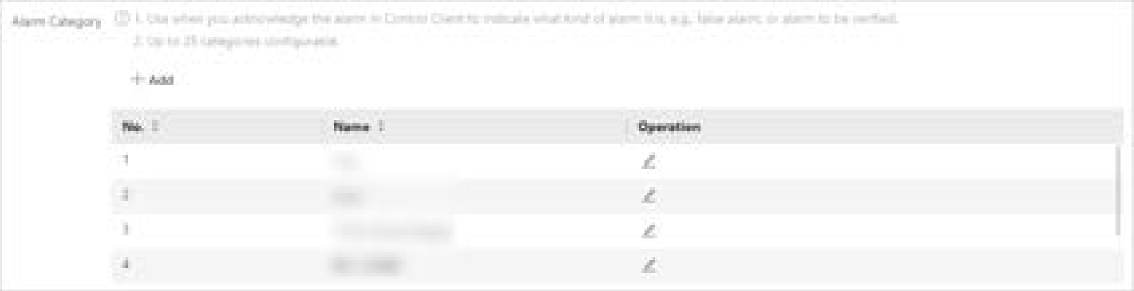
#fa3239

Figure 13-2 Alarm Priority Settings Window

5) Click **Save** to add the priority.

   The priority will be displayed on the alarm priority list.

3. Set the alarm category according to actual needs. By default, four alarm categories exist.



Alarm Category

1. Use when you acknowledge the alarm in Control Client to indicate what kind of alarm it is, e.g. false alarm, or alarm to be verified.
2. Up to 25 categories configurable.

No.	Name	Operation
1	[illegible]	✎
2	[illegible]	✎
3	[illegible]	✎
4	[illegible]	✎

Figure 13-3 Alarm Category

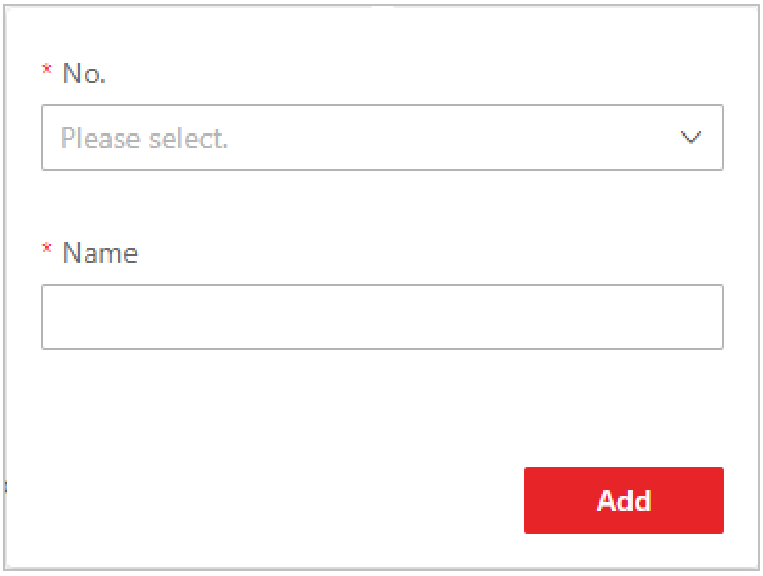
1) Click **Add** to add the customized alarm category.

Note

Up to 25 alarm categories can be added.

2) Select a No. for the alarm category.

3) Enter a descriptive name for the alarm category.



* No.

Please select.

* Name

Figure 13-4 Alarm Category Settings Window

4) Click **Save** to add the alarm category.

The alarm category will be displayed on the alarm category list.

4. In the Alarm Icon When Alarm Occurs field, you can view the alarm icons provided by the system which are used to notify the users that the alarm is triggered.

Note

These pre-defined alarm icons cannot be edited and deleted.

5. 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.

13.1.3 Add Event and Alarm

In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Event and Alarm** → **Event and Alarm Configuration** → **Normal Event and Alarm** and click **Add** to add an alarm or event.

Triggering Event and Source

The following fields indicate two elements in the rule: "triggering event" and "event or alarm source".

Triggering Event

The specific event type detected on the event source will trigger an event or alarm.

Source

This field refers to the specific entity (such as cameras, devices, servers, etc.) which can trigger this event and alarm.

When setting a thermal related event and alarm for thermal cameras, you can select areas, points, or lines as event and alarm sources.

Note

Triggering event type including **Camera**, **Alarm Input**, and **Face** in **Video** and **Camera**, **Encoding Device**, **Decoding Device**, **Recording Server**, and **Streaming Server** in **Maintenance** supports selecting sources in remote sites. For different device types, the labels vary.

Name

After selecting the source(s), you need to name the event or source. 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 Comparison Group

If the triggering event you select is **Face**, you need to select the face comparison group so that the platform can compare the detected face pictures with face pictures in the group.

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 **Person Amount More/Less than Threshold** and **Person Amount More/Less than Threshold (Pre-Alarm)** for 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

If the source type you selected is **Parking Lot** and the triggering event is **Frequently Appeared Vehicle**, 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 for more than 3 times in one day, an alarm will be triggered.

Vehicle List

If you select triggering events related with 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 with the one(s) you selected here, a vehicle type matched alarm will be triggered.

For example, if 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

Click the color to select the color to indicate this event or alarm, which will be displayed in the event center. 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 Recurred Event/Alarm

This function is used to avoid the same event or alarm occurs frequently in a short time. You need to set the **Ignore Events Recurred in (s)** which is the threshold of the recurring events or alarms.

For example, if you set **Ignore Events Recurred in (s)** to ***30 s***, the events or alarms of the same type occurred on the same camera within 30 s will be regarded as one event or alarm.

Note

The **Ignore Events Recurred in (s)** is 15 s by default. You can set it from 15 s to 1800 s.

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 system. After this duration, if the source still detects this triggering event, the triggering event will be uploaded to the system and trigger an alarm.

With this function, when the system 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.

What to Do

The fields defines what actions the system will take to record the alarm details and notify security personnel.

Trigger Recording

Select the related camera to record the alarm video when the alarm is triggered. You can view the live video and play back these video files in the Alarm Center of the Control Client.

- To relate the source camera itself for recording, select **Source Camera** and select the storage location for storing the video files.
- 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 video for after the alarm stops.
- **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.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Capture Picture

Select cameras to capture pictures during the alarm, and you can view the captured pictures when checking the alarm in the Event & Alarm Search of the Control Client.

- If the alarm source is a camera, you can set 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 When: 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 three 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).

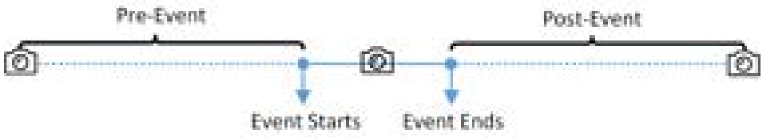


Figure 13-5 Capture Pictures

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 (Cloud Storage Server, Hybrid SAN, or pStor).

Create Tag

Select the cameras to record video when the event occurs and set the storage location for storing the video files. The system will add a tag to the event triggered video footage for convenient search. The tagged video can be searched and checked via the Control Client.

- If the event source is a camera, you can set to trigger the source camera itself for tagged recording by selecting **Source Camera**.
- 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 to record the tagged video started from 5 seconds before the event and lasted 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 (including doors and floors).

For doors, the doors can be locked, unlocked, remained locked, or remained unlocked when the alarm occurs.

For floors, the elevators can access the floors freely, with credentials, temporarily, or access forbidden.

For example, you can set to trigger all the doors remaining locked and all the floors access forbidden when intrusion of suspicious person is detected.

- **All Access Points:** When the alarm occurs, the system will trigger all the doors and floors to take certain action.
- **Specified Access Point:** Click **Add** to select specified access points or emergency operation groups as the linkage targets. When the alarm occurs, the system will trigger these doors, floors, or doors/floors in the emergency operation groups to take certain action.

Link Alarm Input

Select alarm inputs and these alarm inputs will be armed or disarmed when the alarm 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 intrusion alarm, these PIR detectors will be armed and trigger other events or alarms (if rules configured), so that the security personnel will get to known where the suspect goes.

Link Alarm Output

Select alarm output (if available) and the external device connected can be activated when the alarm occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the time period (unit: s) after which that the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected cameras when the alarm 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 third-party platform and set the control about detailed operations that will happen when the alarm occurs.

Send Email

Select an email template to send the alarm information according to the defined email settings. If you have purchased the license of emergency mustering, you can select an emergency counting group in the drop-down list of **Send Data of Emergency Counting Groups**. When the event occurs or the alarm is triggered, the platform will send the data of the selected emergency counting group to the email in a PDF file.

Note

For details about setting 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 the information such as the number of people still in the building, their names and profiles, phone numbers, and locations of last access.

Link Printer

If the source type you selected is **Alarm Input**, you can link to print the entry & exit counting report of 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 in the system so that they can get the information such as how many people are still in the building, their names and profiles, phone numbers, and locations of last access.

For details about printer settings, refer to ***Set Printer*** .

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

You can select the pre-defined user-defined event(s) in the event list.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

Link Speaker Unit

After linking speaker units to an event or alarm and selecting an audio file to be played, the selected audio file will be played by the selected speaker units when the event or alarm is triggered.

Trigger Remaining Open for Entrance and Exit

When the event occurs or the alarm is triggered, 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.

When

The field defines a time period when the event or alarm can be triggered.

Receiving Schedule

The event or alarm source is armed during the receiving schedule and when the source detects the triggering event, an alarm will be triggered and link the configured linkage actions. The system provides two types of receiving schedule:

- **Schedule Template:** Select a receiving schedule template for the event or alarm to define when the event or alarm can be triggered. For setting customized template, refer to ***Configure Receiving Schedule Template*** .
- **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the receiving schedule. When the user defined event or alarm input is triggered, the receiving schedule will start or end. You can set the **Auto-End Arming** switch to on and set the specified time to automatically end arming for this event or alarm even if the end event does not occur.

Note

For example, assume that you have set event A as start event, event B as end event, and set the value of **Auto-End Arming in** 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).

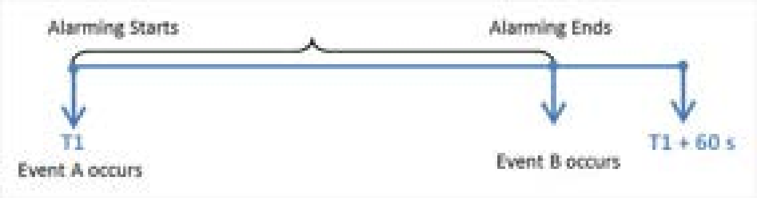


Figure 13-6 Receiving Schedule 1

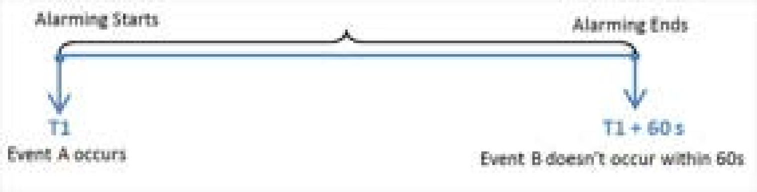


Figure 13-7 Receiving Schedule 2

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.

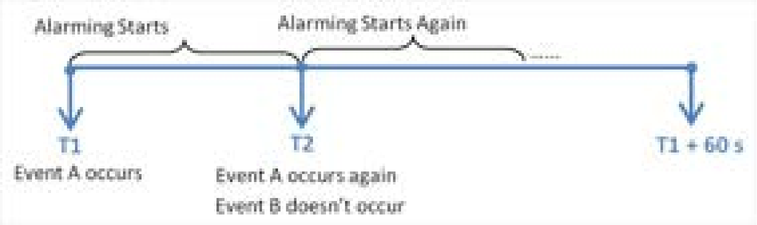


Figure 13-8 Receiving Schedule 3

Alarm Settings

Recipient

The field defines users who can receive the alarm notification and check the alarm details when the alarm is triggered.

Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to HikCentral Professional via the Control Client or Mobile Client.

Note

By default, the admin user and the users configured with the permission of receiving alarms will be automatically selected as the recipients and cannot be unselected.

Alarm Priority

The field defines the priority for the alarm. Priority can be used for filtering alarms in the Control Client.

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 alarm occurs.

Trigger Emergency

When the event occurs or the alarm is triggered by an emergency (such as fire), the platform automatically switches to the In Emergency mode or End Emergency mode.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window and set the alarm video's stream type.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Wall Related to Graphic Card:** Display the alarm video on the wall which adopts graphic card of the PC that running the Control Client to decode video.
- **Wall Related to Decoding Device:** Display the alarm video on the wall which adopts decoding device (namely the wall that related to the decoding device) to decode the video.
- **Smart Wall No.:** Select the No. of smart wall window to display the alarm video.
- **Stream Type:** Select the stream type of the alarm video displaying on the smart wall.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Related Map

Select a map to show the alarm information and you should add the camera to the map as a hot spot (refer to). You can check the map in the Alarm Center and Alarm & Event Search of the Control Client.

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Other Operations After Adding an Alarm

After adding an alarm, you can perform the following operations if needed.

Table 13-1 Other Operation

Operation	Description
Edit Alarm	Click ✎ in the Operation column to edit the alarm.
Copy to Other Alarms	You can copy the current alarm's specified parameters to other added alarms for batch configuration. Click ✎ in the Operation column to enter the alarm details page and click **Copy to**. Specify the settings of the source alarm, select target alarm(s), and click **OK**.
Delete Alarm	Select alarms and click **Delete** to delete the selected alarms.
Delete All Invalid Alarms	Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.
Enable Alarms	Select an alarm and click **Enable → Enable** to enable the alarm, or click **Enable → Enable All** to enable all the added alarms..
Disable Alarm	Select an alarm and click **Disable → Disable** to disable the alarm. Set a time when the alarm is disabled and the duration how long the alarm will be disabled for.
Disable All Alarms	Click **Disable → Disable All** to disable all the added alarms. Set a time when the alarms are disabled and the duration how long the alarms will be disabled for.
Test Alarm	Click **Test** to trigger this alarm automatically. You can test if the linkage actions work properly.

13.1.4 Add Combined Alarm

For some complicated scenarios, the alarm should be triggered when multiple events or alarms are detected or triggered. For example, the system detects intrusion in area B, then the arming of area

A starts. After that, if the system detects intrusion in area A, then an alarm will be triggered to notify the security personnel.

In this section, we suppose the combined alarm is alarm A, the triggering event is event B. (The system detects event B, the arming of alarm A starts.)

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **Event and Alarm** → **Event and Alarm Configuration** → **Combined Alarm** .
2. Click **Add Combined Alarm** to open the Add Combined Alarm window.
3. Set the parameters on the page and save.

   Alarm Triggered Area

   Select the area of the alarm (alarm A) happened.

   Alarm Priority

   The priority including low, medium, high and custom level which indicates the urgent degree of this alarm (alarm A).

   Alarm Name

   Create a name for this alarm (alarm A).

   Description

   Describe the alarm (alarm A) according to your requirements.

   Ignore Recurring Alarms

   Enable **Ignore Recurring Alarms** and set the time. After enabled, the system will ignore the recurring alarm(alarm A) within the time period.
4. Click the name of an added combined alarm to enter the Alarm Configuration page.
5. Configure the Schedules, which defines the receiving schedule of this alarm (alarm A).

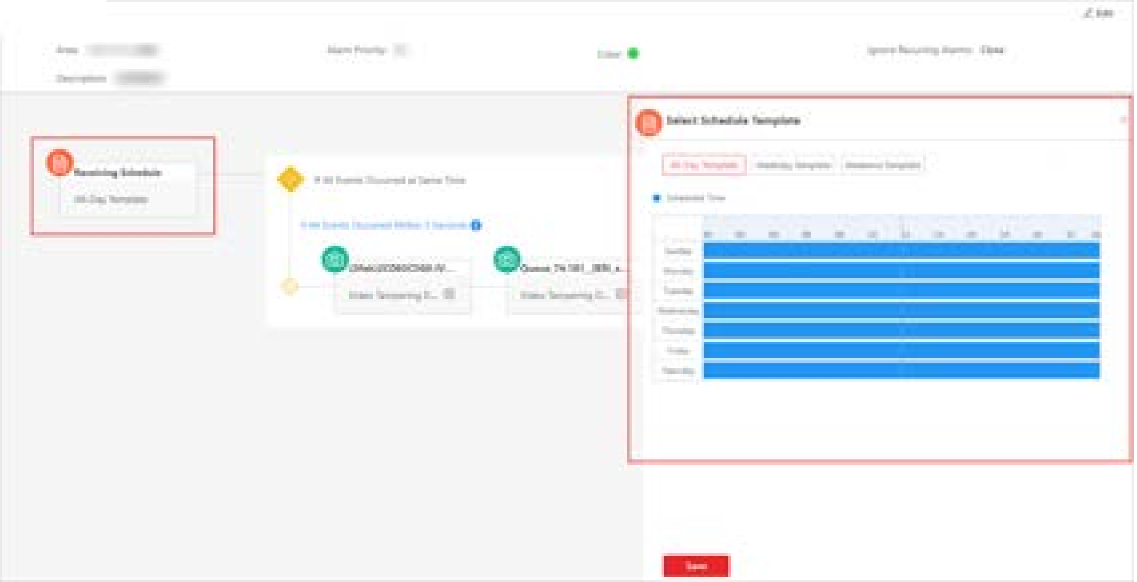


Figure 13-9 Receiving Schedule

1) Click **Receiving Schedule** to show the Select Receiving Schedule panel.
2) Select the schedule template as **All-Day Template**, **Weekday Template**, **Weekend Template**, or a customized template. See ***Configure Receiving Schedule Template*** for details.
3) Click **Save**.

Note

You can click 🗑 appeared on the top right of the **Receiving Schedule** button to delete it. If the schedule is deleted, all related conditions and actions will also be deleted.

6. Select the alarm triggering logic and configure the condition, which defines the triggering condition of this alarm (alarm A).
   1) Click the area in the following image to show the Select Alarm Triggering Logic panel.

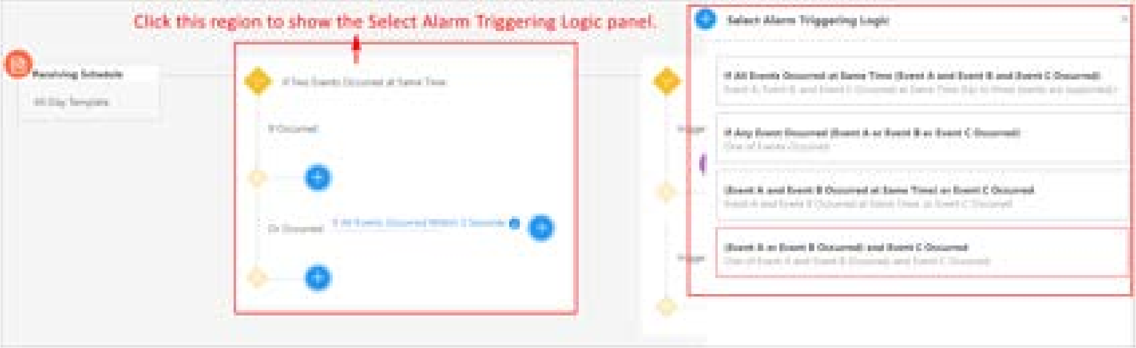

Click this region to show the Select Alarm Triggering Logic panel.
Receiving Schedule
All-Day Template
Select Alarm Triggering Logic

Figure 13-10 Select Triggering Logic

2) Select the triggering logic on the Select Alarm Triggering Logic panel.
3) Click ⊕ to select the event type and event source (event B) that trigger this alarm (alarm A).
4) Click **Save**.

5) **Optional:** Click ⊕ at the right of selected event type and source panel to select more event types and sources.

6) **Optional:** Click ⚙ to open the remote configuration page of the triggering source to configure the source. For details about remote configuration, refer to the device user manual.

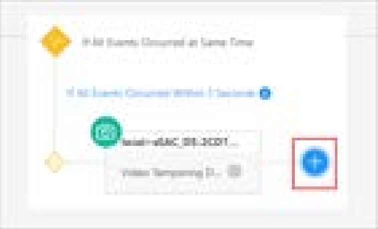

If All Events Occurred at Same Time
If All Events Occurred Within 3 Seconds
local - iSAC_DS-2CD7...
Video Tampering D...

Figure 13-11 Add New Event Type and Source

Note

You can click the configured Condition panel to edit all conditions, or move the cursor to the Condition panel and click 🗑 appeared in the top right corner to delete all configured conditions at the same time. If the conditions are deleted, all related actions will also be deleted.

7. Configure the Actions, which defines the linkage action (such as triggering recording, capturing picture, and creating tag) and recipient after this alarm (alarm A) is triggered.

1) Click ⊕ to open the Select Alarm Linkage Action panel.

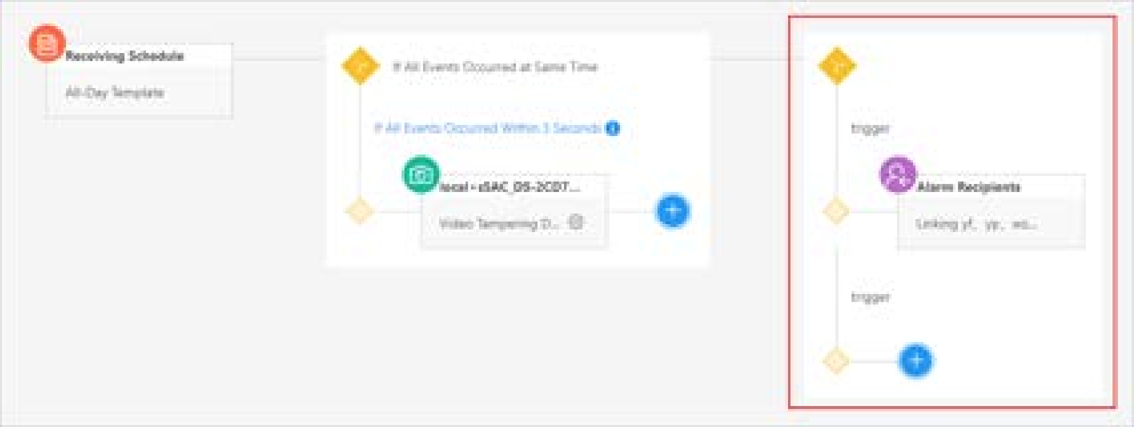


Figure 13-12 Action

2) Click **Alarm Recipients** and select the Alarm Recipients.

Note

If **Automatically Receive Alarm** is enabled for some users (refer to ***Add Normal User*** for details), an action panel of **Alarm Recipients** will be automatically generated after setting the conditions, and the users will be selected as the recipient. You can click the generated action panel to edit the alarm recipients, but the selected users cannot be unselected.

3) Click **Save**.

4) **Optional:** Click ⊕ below the Alarm Recipients panel to add more linkage actions and configure action parameters. See ***Add Event and Alarm*** for details about linkage actions.

8. Click **Save** in the top right corner of this page, and this alarm (alarm A) will be added to the platform.

Note

If the alarm recipients are not configured for this combined alarm, you cannot save the combined alarm.

9. **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 in 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) to copy, 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 receive the notification.

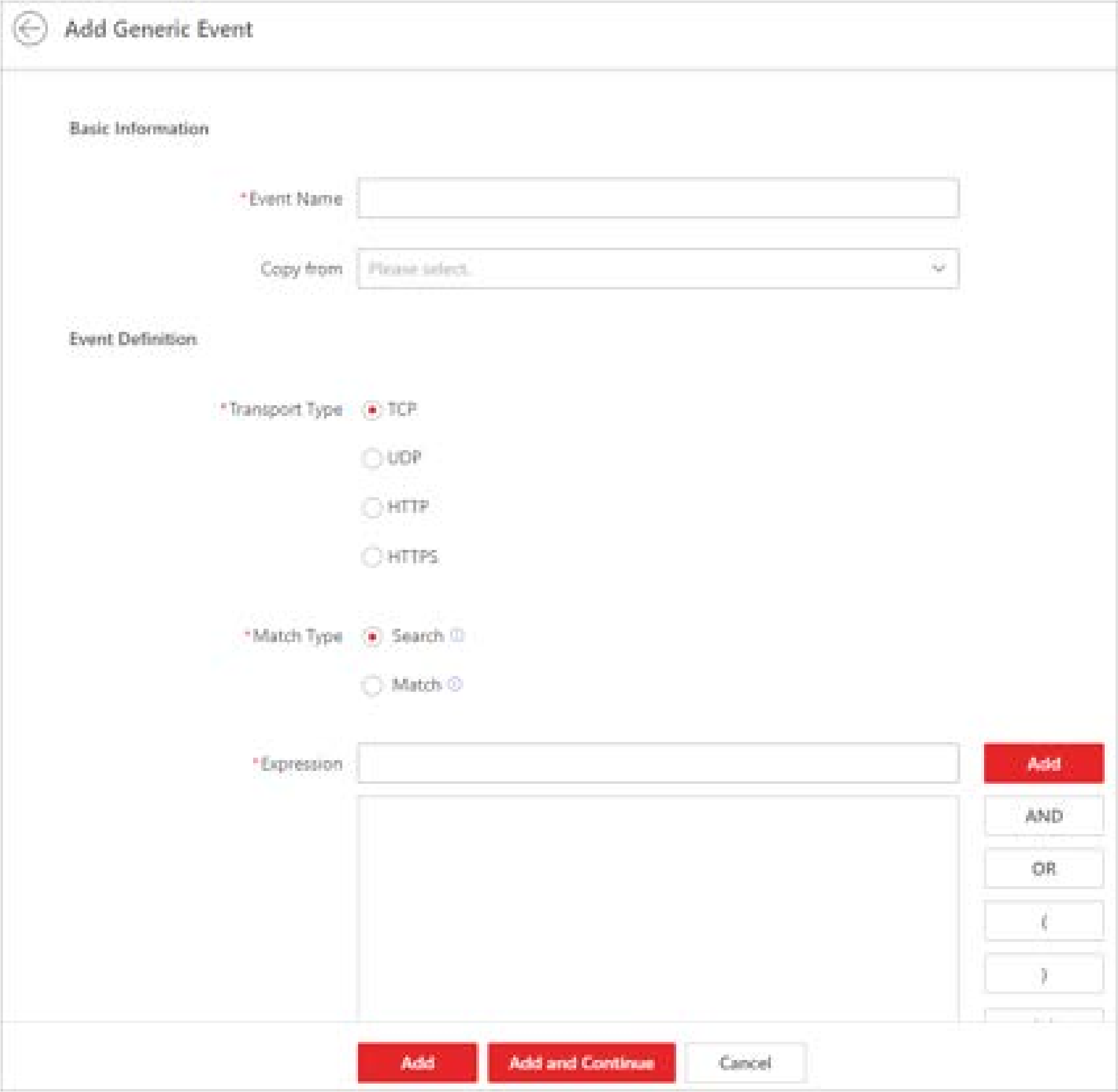
Enable/Disable
Switch on the button beside **Status** to enable or disable this alarm. After the alarm is enabled, it can be received by the platform. If you disable this alarm, you will be required to set the time and duration of disabling and the plaform cannot receive the alarm in the duration.

13.2 Configure Generic Event

You can customize the expression to create a generic event to analyze the received TCP and/or UDP data packages, and trigger events when specified conditions are met. In this way, you can easily integrate your system 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 🟥 → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **Generic Event** to enter the generic event settings page.
2. Click **Add** to enter the Add Generic Event page.



Add Generic Event

Basic Information

*Event Name

Copy from: Please select.

Event Definition

*Transport Type: ● TCP ○ UDP ○ HTTP ○ HTTPS

*Match Type: ● Search ○ Match

*Expression

Figure 13-13 Add Generic Event Page

3. Set a name for the event in the Event Name field.
4. **Optional:** Copy the settings from other defined generic events in the **Copy from** field.
5. Select **TCP**, **UDP**, **HTTP**, or **HTTPS** as the package transmission protocol.
6. Select the match type which indicates how particular your system should be when analyzing the received data packages:

   Search

   The received package must contain the text defined in the Expression field.

   For example, if you have defined that the received packages should contain "Motion" and "Line Crossing", the alarm will be triggered when the received packages contain "Motion", "Intrusion" or "Line Crossing".

Match

The received package must exactly contain the text defined in the Expression field, and nothing else.

7. Define the event rule for analyzing the received package in the Expression field.
   1) Enter the term which should be contained in the expression in the text field.
   2) Click **Add** to add it to the expression.
   3) Click parenthesis or operator button to add it to the expression.
   4) To add a term, parenthesis or operator to the expression, position the cursor inside the expression field in order to determine where a new item (term, parenthesis or the operator) should be included, and click Add or one of the parenthesis or operator buttons.
   5) To remove an item from the expression, position the cursor inside the field in order to determine where an item should be removed, and click ✕ . The item immediately to the left of the cursor will 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.

8. 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.
9. View in the Generic Event list to check whether the event has been added successfully.
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.
Delete Event Settings	Select the event(s) and click **Delete** to delete the selected event settings.
Delete All Event Settings	Check the check box in the heading row, and click **Delete** to delete all the event settings.
Receive Generic Event	After creating a generic event to analyze the received TCP, UDP, HTTP, or HTTPS data packages from a very wide range of external systems, you can select the event(s), and click **Receive Generic Event** to enable receiving the generic event.

13.3 Configure User-Defined Event

If the event you need is not in the provided system-monitored event list, or the generic event cannot properly define the event received from third-party system, you can customize a user-defined event.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **User-Defined Event** to enter the user-defined event management page.
2. Click **Add** to open the following window.

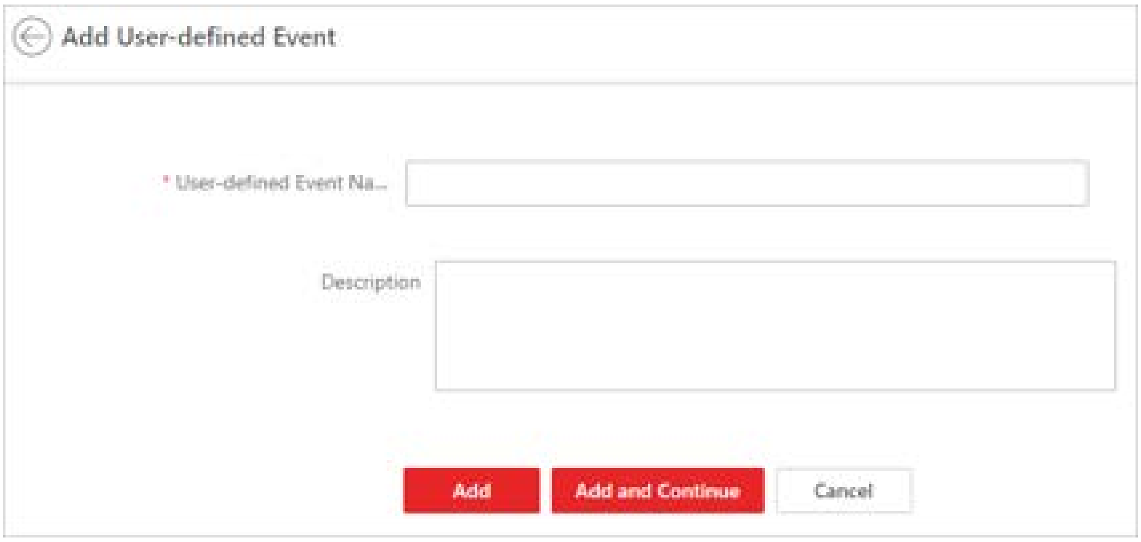


Figure 13-14 Add User-Defined Event

3. Create a name for the event.
4. **Optional:** Enter the description information to describe the event details.
5. 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 event.

   With the customized user-defined event, it provides the following functions:

   - The user can trigger a user-defined event manually in Monitoring and Alarm Center module on the Control Client when viewing the video or checking the alarm information.
   - A user-defined event can trigger an alarm if configured.
   - You can define the arming time period by the user-defined event: An alarm's arming schedule will start or end when the user-defined event is triggered.
   - An alarm can trigger a user-defined event as alarm actions.
   - Integrate other third-party systems with HikCentral Professional by using the data received from the third-party system. You can trigger the user-defined events outside the HikCentral Professional. For details, contact our technical support.

Note

- For configuring the alarm source, arming schedule, and alarm action, refer to ***Event and Alarm Configuration*** .
- For triggering the user-defined event on the Control Client, refer to *User Manual of HikCentral Professional Control Client*.

13.4 Configure Receiving Schedule Template

When setting event and alarm, you can select the pre-defined receiving schedule template to define when the event or alarm can be triggered and notifying the recipients. The system predefines three default receiving schedule templates: All-Day Template, Weekday Template, and Weekend Template. You can also add a customized template according to actual needs.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **Receiving Schedule Template** .
2. Click **+** to enter the add receiving schedule template page.

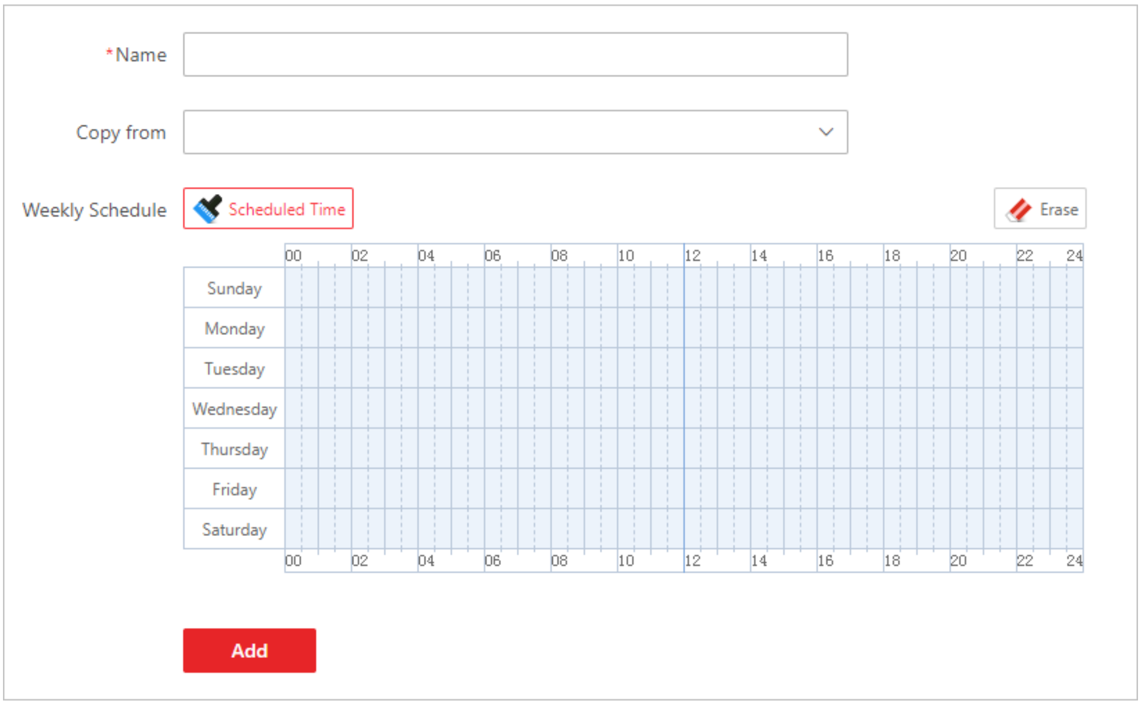


Figure 13-15 Add Receiving Schedule Template

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. Click **Scheduled Time** and drag on the time bar to set the time periods. During the time periods, the event can be triggered on the event source and notify the recipients in HikCentral Professional.

   Note

   Up to 4 time periods can be set for each day.
5. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
6. Click **Add** to add the template and go back to the receiving schedule template list page.

   The receiving schedule template will be displayed on the receiving schedule template list.
7. **Optional:** Perform the following operations after adding the receiving schedule template.

View Template Details	Click the template to view its details.
Edit Template	Click the name of a customized template to edit template details.
Delete Template	Select a template and click 🗑 to delete the template.

13.5 Add Alarm Recipient Group

Enter a short description of your task here (optional).

Before You Start
Enter the prerequisites here (optional).
Enter the context of your task here (optional).

Steps

1. Enter your first step here.
   Enter the result of your step here (optional).

Example
Enter an example that illustrates the current task (optional).

What to do next
Enter the tasks the user should do after finishing this task (optional).

13.6 Event and Alarm Search

On the event & alarm search module, you can view the alarm overview, search the historical event or alarm by setting search condition as required.

13.6.1 Alarm Overview

In the alarm overview module, it gives you an overview of the alarm distribution, top 5 alarms and top 5 warning zones.

In the top left corner of Home page, select ▦ → **All Modules** → **General** → **Event and Alarm** → **Search** → **Overview** to enter the Alarm Analysis page.

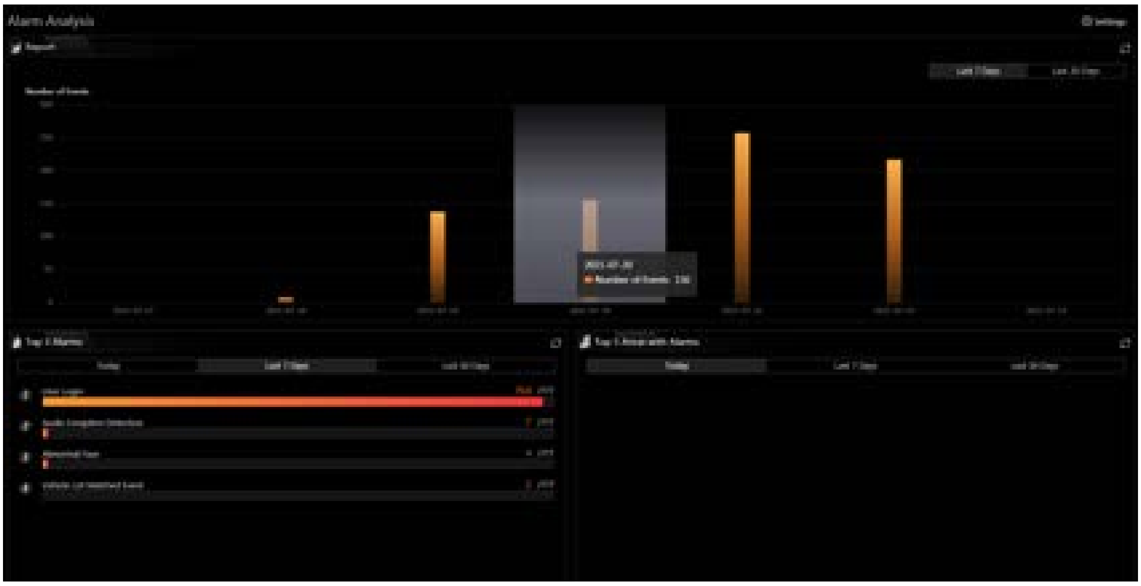


Figure 13-16 Alarm Analysis

You can click **Settings** in the upper-right corner to customize the event, alarm, or event and alarm types to be calculated in the overview page.

In the upper area of the page, the number of events triggered in the last 7 days or last 30 days are displayed in vertical bar chart.

In the lower-left area of the page, the top 5 alarms triggered in today, last 7 days or last 30 days are displayed in horizontal bar chart. The type of information displayed here 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 Top 5 Alarms will only display data of the alarms. Click the number of an alarm to jump to the Event and Alarm Search page. Also, the **Trigger Alarm** field will also change according to your selection on the Settings pane.

In the lower-right area of the page, the top 5 areas with alarm in today, last 7 days or last 30 days are displayed in horizontal bar chart.

13.6.2 Search Event and Alarm Logs

You can search the event and alarm log files of the added resource for checking.

Before You Start

You should configure the event and alarm settings first.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules → General → Event and Alarm → Search → Event and Alarm Search** to enter the Event & Alarm Search page.
2. Set the time range for search.
   - Select a predefined time period for search.

- Select **Custom Time Interval** and specify the start time and end time for search.

3. Select the event type as **All**, **Not Trigger Alarm** or **Trigger Alarm**.

   All

   Both events and alarms.

   Not Trigger Alarm

   The events happened but were not triggered as alarms.

   Trigger Alarm

   The events happened and were triggered as alarms.

4. **Optional:** If you select **Trigger Alarm**, you can set the following filter conditions.

   Marking Status

   Switch **Marking Status** on and select **Marked** or **Unmarked** to filter the marked or unmarked alarms/events.

   Acknowledging Status

   Switch **Acknowledging Status** on and select **Acknowledged** or **Unacknowledged** to filter the acknowledged or unacknowledged alarms/events.

   Alarm Priority

   Select the priority level to filter the alarms/events by priority.

   Category

   Select the category to filter the alarms/events by category.

5. Enable **Area** and then click □ to select the area of the source.
6. Enable **Triggered By** and then 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).

7. **Optional:** If you select events of the Access Control category, enter the entered/exited person's name.
8. **Optional:** If you have entered the additional information about the alarm on the third-party system, enter the additional information in the **Third-Party Additional Information** when searching for a third-party event or alarm.
9. Enable **Event & Alarm Name** to select the event/alarm name in the drop-down list.
10. Click **Search**.

    The matched event or alarm logs display on the list.

11. **Optional:** Perform the following operation(s) after searching for alarms and events.

Export Events and Alarms	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.

13.7 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 daily or weekly, 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 ***Set Email Template*** .
- 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 🟥 → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **Scheduled Report** .
2. Click **+**.
3. Create a name for the report.
4. Set the event(s) or alarms contained in the report.
   1) In the Report Target field, click **Add**.

      All the added events and alarms are displayed.
   2) (Optional) Filter the events by event source type and triggering event.
   3) Select the event(s).

      Note

      Up to 32 events can be added in one report rule.
   4) Click **Add**.
5. Set the report type as **Daily** or **Weekly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains information of the events triggered on the day (24 hours) before the current day.

For example, if you set the sending time as 20:00, the system will send a report at 20:00. every day, containing details of all the events triggered between 00:00. and 24:00. before the current day.

Weekly Report

As compared to daily report, weekly report can be less time-consuming, since it is not to be submitted every day. The system will send one report at the sending time every week, which contains information of the events triggered on the last 7 days before the sending date.

For example, if you set the sending time as 6:00 on Monday, the system 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.

6. Select the 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 ***Set Email Template*** .

7. Select Excel or PDF as the report format.
8. Select the **Report Language**.
9. Click **Add** to add the report and go back to the report list page.

Chapter 14 Video Management

After adding encoding devices to the system, you need to set video related parameters to ensure the security personnel can not only view live videos streamed from these devices via the Control Client, Web Client and Mobile Client, but also access other important functions such as playback and intelligent recognition. These functions can provides great help and convenience for their works such as security surveillance and investigation.

14.1 Flow Chart of Video Management

The two flow charts below show the process of configurations and operations required for viewing videos of encoding devices and other related functions on current site and remote site respectively.

View Videos of Encoding Devices on the Current Site

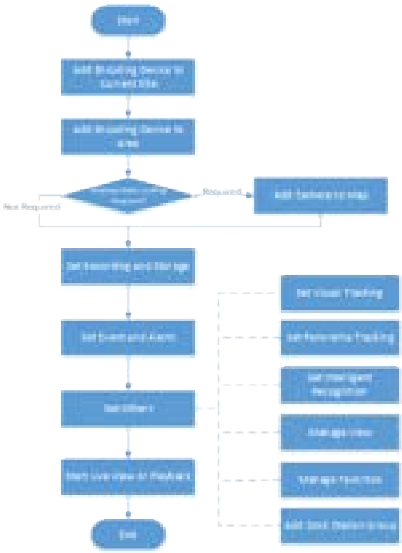

Start
Add Encoding Device to Current Site
Add Encoding Device to Area
Required
Not Required
Add Camera to Map
Set Recording and Storage
Set Event and Alarm
Set Others
Start Live View or Playback
End
Set Visual Tracking
Set Panorama Tracking
Set Intelligent Recognition
Manage View

Table 14-1 Flow Chart Description

Procedure	Description
Add Encoding Device to Current Site	Add encoding device to the current HikCentral Professional site by online detection, IP address, port segment, **Hik-Connect DDNS**, device ID, device ID segment, etc.

Procedure	Description
	For details, see ***Manage Encoding Device*** .
Add Encoding Device to Area	Group encoding devices to different areas according to the locations of the devices for convenient management. For details, see ***Area Management*** .
Add Camera to Map	Add cameras to a map as hot spots to view videos on map. After that, you can get the video information and camera location information at the same time. For details about adding cameras to map, see ***Add Hot Spot on Map*** .
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). For details about configuring recording and storage, see ***Configure Storage and Recording*** .
Configure Event and Alarm	Configure linkage actions for the events detected by the encoding devices. For details, see ***Event and Alarm Configuration*** .
Configure Others	You can configure other video related functions including visual tracking, panorama tracking, intelligent recognition, and dock station group. • Configure Visual Tracking: Visual tracking is a target tracking function that allows you to track a target (e.g., a suspect) moving across fields of view of multiple cameras by switching views of camera nearly seamlessly. For details about the configuration, see ***Configure Visual Tracking*** . • Configure Panorama Tracking: Panorama Tracking is a target tracking function based on the linkage between a box/bullet camera and a speed dome. When a VCA event is detected or a target is selected manually, the bullet/box camera, through its video analysis function, can work together with the speed dome to locate, zoom in, and track the target. For details about configuring this function, see ***Configure Panorama Tracking*** . • Configure Intelligent Recognition: Intelligent recognition refers to the recognition of faces, body features, or behaviors, etc., by

Procedure	Description
	intelligent analysis devices added to the platform. For details configuring this function, see ***Intelligent Recognition*** . • Configure Dock Station Group: A dock station group refers to a group of persons (e.g., police officers) related to a same dock station — a data collector which can automatically detect and back up law-enforcement data and evidence data from body camera(s) connected to it. After relating persons to a dock station, the videos and pictures stored on the persons' body cameras can be copied to the dock station. For details about configure dock station group, see ***Add Dock Station Group*** .
Start Live View or Playback	Start playing live videos or video footage of the encoding devices. You can also manage view and favorites. For details, see ***Video Application*** .

View Videos of Encoding Devices on Remote Site

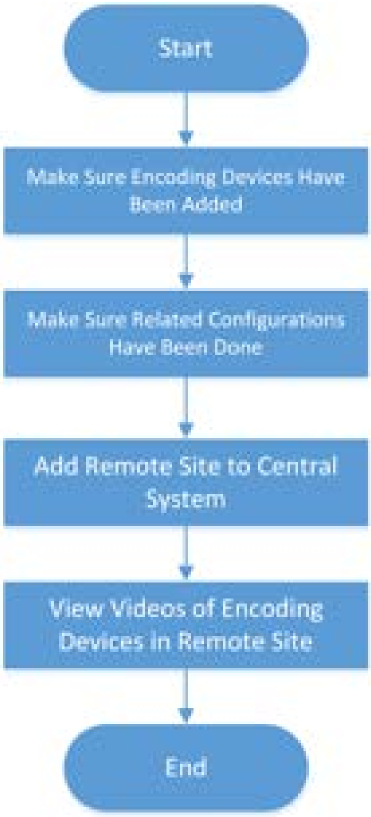

Start
Make Sure Encoding Devices Have Been Added
Make Sure Related Configurations Have Been Done
Add Remote Site to Central System
View Videos of Encoding Devices in Remote Site
End

Table 14-2 Flow Chart Description

Procedures	Description
Make Sure Encoding Devices Have Been Added	Make sure encoding devices has been added to a remote site by the administrator of the site.
Make Sure Related Configurations Have Been Done	Make sure recording and storage configurations and other required configurations (refer to configuration descriptions in ***Table 14-1***) have been done by the administrator of the site.
Add Remote Site to Central System	Add the remote site to the current site under the prerequisite that the latter has the Remote Site Management (RSM) module. The HikCentral Professional site with the RSM module is also called the Central System. For details about adding remote site to a Central System, see ***Add Remote Site by IP Address or Domain Name*** , ***Add Remote Site Registered to Central System*** , or ***Add Remote Sites in a Batch*** .
View Videos of Encoding Devices on Remote Site	Select the remote site and then select an encoding device on it to view the live video and video footage of the device. For details, see ***Video Application*** .

14.2 Configure Storage and Recording

Before you can play back video files recorded by cameras, you need to set the time periods for video recording and the location for storing video files and pictures first. Also, before you can import pictures (e.g., static e-map picture) and view pictures (e.g., alarm-related pictures) uploaded from devices, you need to set storage locations for these pictures and set related parameters.

HikCentral Professional provides four storage locations (encoding devices, Hybrid Storage Area Network, Cloud Storage Server, and pStor) for storing the recorded video files of the cameras.

Encoding Device

Store video files on the encoding devices (i.e., DVR, NVR, and network camera) locally. Take NVR for an example, the video files recorded by the cameras linked to it will be stored in its storage medium (e.g., HDDs, Net HDDs, and SD/SDHC cards) if you select **Encoding Device** as the storage location.

To store video files in this way, you need to make sure the encoding device is equipped with a storage medium and the storage medium should have been formatted.

Perform the following operations to format storage medium if required:

Go to the remote configuration page of the encoding device (🟥 → **All Modules** → **General** → **Resource Management** → **Encoding Device** → ⚙), and then click **Storage** → **Storage Management** → **HDD Management** → **Format** to initialize the selected storage device.

Hybrid Storage Area Network

Store the video files in the added Hybrid Storage Area Network. For details about adding Hybrid Storage Area Network, refer to ***Add Hybrid Storage Area Network*** .

Cloud Storage Server

Store the video files in the added Cloud Storage Server. For details about adding Cloud Storage Server, refer to ***Add Cloud Storage Server*** .

pStor

Store the video files in the added pStor, which is the storage access service used for managing local HDDs and logical disks. For details about adding pStor, refer to ***Add pStor*** .

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. For details about adding pStor Cluster Service, refer to ***Add pStor Cluster Service*** .

14.2.1 Configure Recording for Cameras on Current Site

For the cameras on the current site, HikCentral Professional provides five storage methods (storing on encoding devices, Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service) for storing the video files of the cameras according to the configured recording schedule. You can get device's recording settings when adding camera to an area.

Before You Start

Encoding devices need to be added to the HikCentral Professional for area management. Refer to ***Resource Management*** for detailed configuration about adding devices.

Steps

1. Enter the **Recording Setting** tab.
   1) In the top left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Area** .
   2) Select an area to show its cameras.

   Note

   For Central System with Remote Site Management module, you can select the current site (marked with 🌐 icon) from the drop-down site list to show its cameras.

   3) Select a camera and click its name to enter camera settings page.
   4) Select the **Recording Settings** tab.
2. Turn on **Main Storage**.
3. Select the storage location for storing the recorded video file.

4. Select the storage type and configure other required parameters.
   - 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**, **Cloud Storage Server**, **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 **Cloud Storage Server**, and the command-based recording schedule can not be configured for the **Cloud Storage Server** and **pStor**.

Stream Type

Select the stream type as main stream, sub-stream or dual-stream.

Note

For storing on Hybrid Storage Area Network, Cloud Storage Server, 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, Cloud Storage Server, 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 Expiration

If you select **Encoding Device** as the storage location , set **Video Expiration** switch to on 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

- Make sure you have configured recording schedule stored in the device local storage or pStor for auxiliary storage first. Otherwise, the scheduled copy-back is not configurable.
- The recordings can be copied only from the encoding device to Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service, or from pStor to another pStor.

Copy in

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.

5. **Optional:** Set the **Auxiliary Storage** switch to ON and configure another storage location for the video files.

Note

- If Cloud Storage Server, 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, Cloud Storage Server, pStor or pStor Cluster Service, or from pStor to another pStor.

6. Click **Save**.

14.2.2 Configure Recording for Cameras on Remote Site

You can set recording schedule to record the video of cameras on Remote Sites and stores in the Central System's Recording Servers (Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service).

Steps

1. Go to the **Recording Settings** tab.
   1) In the top left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Area** .
   2) Select the added Remote Site form the drop-down list.

   Note

   The icon 🌐 indicates that the site is Remote Site.

   3) Select an area to show the cameras added to it.
   4) Select a camera and click its name to enter the camera settings page.
   5) Select **Recording Settings** tab.
2. In the Recording Settings area, turn on **Storage in Central System**.
3. Select the storage location for storing the recorded video file.
4. Select the storage type and configure the required parameters.
   - Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location at the real time.

   Note

   You can select **Hybrid Storage Area Network**, **Cloud Storage Server**, **pStor**, or **pStor Cluster Service**, specify a server and (optional) select a Streaming Server to get the video stream of the camera via it.

   Recording Schedule Template

   Set the template which defines when 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.

Stream Type

Select the stream type as main stream, or sub-stream.

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 Cloud Storage Server, pStor, or pStor Cluster Service, and it is available for the camera that is configured with event-based recording.

Post-Record

Start recording the video from periods following detected events.

This field displays when the storage location is set as Hybrid Storage Area Network, and it is available for the camera that is configured with event-based recording.

Streaming Server

Optionally, select a **Streaming Server** to get the video stream of the camera via it.

Enable ANR

If you select the Storage Location as Hybrid Storage Area Network, check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network disconnects and transport the video to Hybrid Storage Area Network when network recovers.

- Select **Scheduled Copy-Back** as the storage type and specify period, main/auxiliary storage, recording type and uploading speed to upload the recorded video files from the device local storage or pStor on the Remote Site to the specified storage location according to scheduled period.

Note

Make sure you have configured recording schedule stored on encoding device or pStor for the camera on the remote site.

5. Click **Save**.

14.2.3 Configure Storage for Imported Pictures and Files

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 the HDD of SYS server. You can configure the storage locations and the corresponding quotas for them.

Steps

Note

You can configure the storage only when the current Web Client is running on SYS server.

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Storage** → **Storage on SYS Server** .

   The disks of the SYS server 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**.

14.2.4 Configure Storage for Uploaded Pictures

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, Cloud Storage Server, pStor, or NVR (Network Video Recorder).

Steps

1. Enter the picture storage setting page.

1) In the top left corner of the Home page, select 🟥 → **All Modules** → **General** → **Resource Management** → **Area** → **Camera** .
2) Select an area to show its cameras.

Note

For Central System with Remote Site Management module, you can select the current site (marked with 🌐 icon) from the drop-down site list to show its cameras.

3) Select a camera and click its name to enter the camera settings page.

2. Select the **Picture Storage Settings** tab.
3. Switch on **Picture Storage**.
4. 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 **Configuration** 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 ***Configure Storage for Imported Pictures and Files*** for details.
- You cannot configure the storage location for the captured undercarriage pictures, which are stored on the UVSS device.

5. Click **Save** to save the uploaded pictures to the specified location.

14.2.5 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 🟥 → **All Modules** → **Video** → **Video Settings** → **Recording Schedule Template** .
2. Click + to enter the Adding Recording Schedule page.

Note

Up to 32 templates can be added.

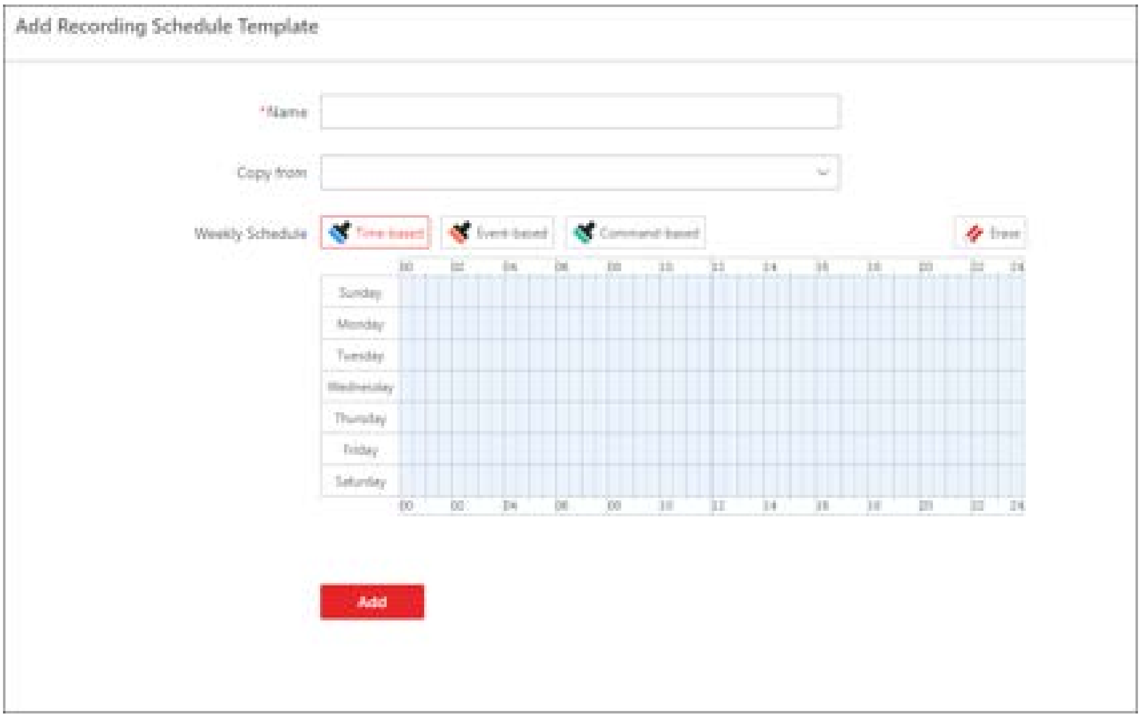


Figure 14-1 Adding Recording Schedule Template Page

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.

14.3 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 Home page, select 🟥 → **All Modules** → **Video** → **Video Settings** → **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. More the cursor to one of the thumbnail, and then click the appeared **Set Visual Tracking** to open visual tracking settings page.
5. **Optional:** Click **Refresh** to get the latest view of the camera.
6. Click **Add Related Camera** to open the camera list panel, and select a camera from the camera list or search for a specific camera by keywords, and then click **OK**.

   The icon representing the related camera will be displayed on the view of the current camera. And the thumbnail of the view of the related camera will be listed on the right side.
7. Drag the icon to a proper position on the view according to its actual mounting position.
8. **Optional:** Hover the cursor over the thumbnail list on the right side, and then click **Set Visual Tracking** to set visual tracking for the related camera.

Note

You can repeat this step to set visual tracking for more cameras. After that, you can view the visual tracking route of different cameras. You can click one camera to view its corresponding visual tracking image.

Figure 14-2 Set Visual Tracking

9. **Optional:** Hover the cursor over the thumbnail list on the right side, and then click **Delete** to cancel the association between the current camera and its related camera.
10. Click in the upper-left corner to save the above settings and back to the visual tracking page.

    The security personnel will be able to use the video tracking function on the Control Client.

Example

Visual Tracking in Hallway

The following picture shows the surveillance 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 surveillance 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.

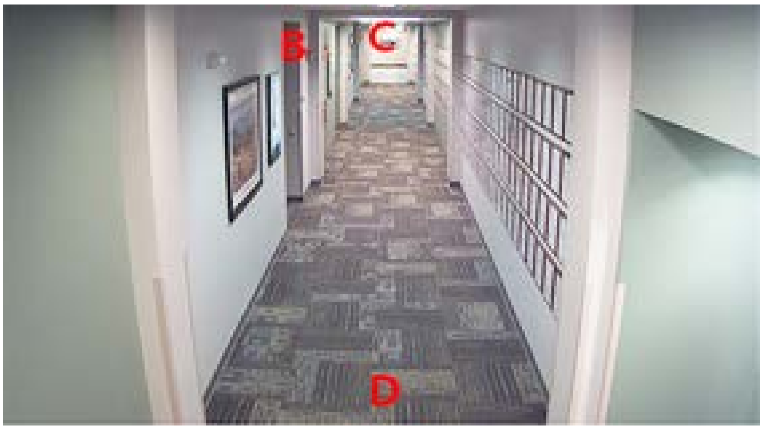


Figure 14-3 Surveillance Image of Camera A

14.4 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 🟥 → **All Modules** → **Video** → **Video Settings** → **Network** .
2. Set network parameters.

Register to Central System

Switch on **Register to Central System** and enter the IP address and port No. of Central System to allow the system without Remote Site Management module (as we called Remote Site) to be registered to the Central System. Central System is the system that has Remote Site Management module and can group multiple Remote Sites together to form a larger-scale union. The purpose of grouping Central System and Remote Sites is to allow Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same system.

Note

- Before registering to the Central System, make sure you have enabled the Central System to receive the site registration. Refer to the parameter **Receive Site Registration** for details.
- Registering to Central System is only available for the system without Remote Site Management module.
- Open Service Manager (installed on the PC running central system's SYS service), and click **System Management Service** if you need to view or edit the Central System's port.

Receive Site Registration

Check the **Receive Site Registration** to allow the system with Remote Site Management module (or Central System) to receive the registration from Remote Sites. Remote Site is the system that does not have Remote Site Management module and can register to Central System to form a larger-scale union. The purpose of joining Central System and Remote Sites is to allow Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same system.

Note

- If a remote site needs to register to the Central System, it should open the Remote Site's Web Client and enter **Register to Central System** to configure the Central System's parameters. See ***Set Network Parameters*** for details.
- Allowing remote site registration is only available for the system with Remote Site Management module.

Device Access Mode

Set the device access mode as 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**.

14.5 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 ▦ → **All Modules** → **Video** → **Video Settings** → **Panorama Tracking Settings** .
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. Select a speed dome from the list for linking the camera to the speed dome.
5. Select **Manual Calibrating** or **Auto Calibrating** as calibration mode and click **Next**.
6. 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.

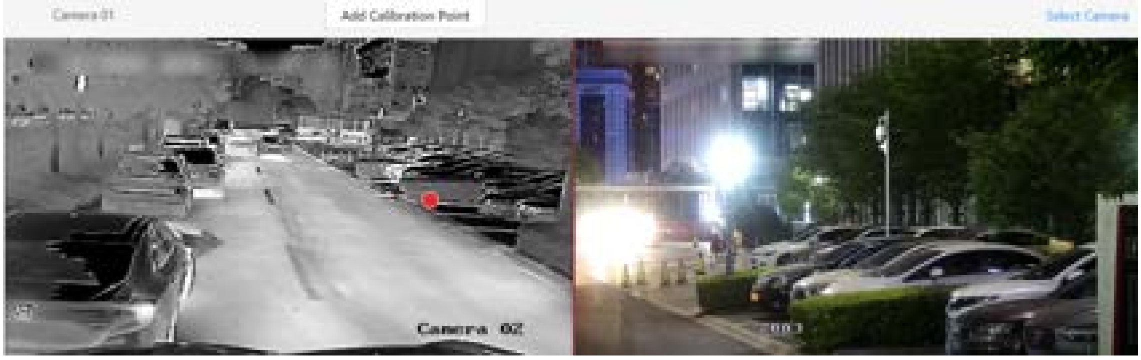


Figure 14-4 Manual Calibrating

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.

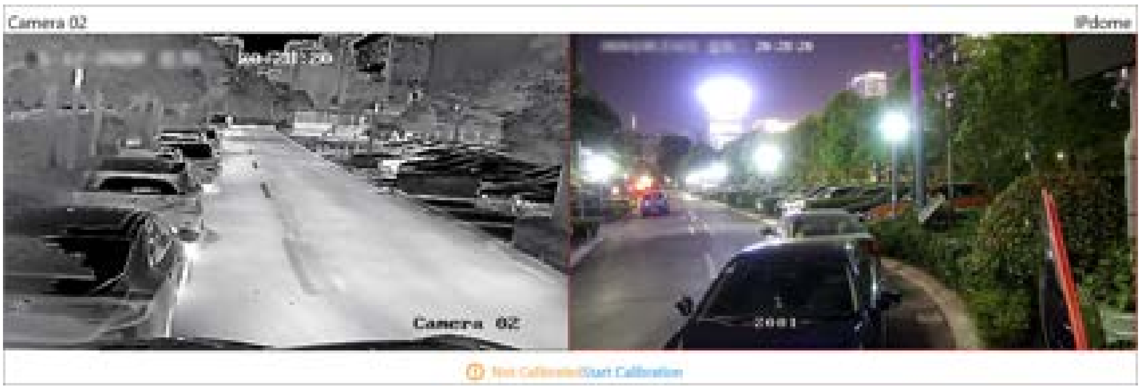


Figure 14-5 Auto Calibrating

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).

7. 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.

8. 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.

9. **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.

14.6 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 Manage Face Comparison Group

HikCentral Professional 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.

On the Web Client, after adding the persons to the person group, the administrator should create a face comparison group, and then add persons (selected from the person list) to the group before you can perform face comparison. Finally, the administrator should apply the face comparison group with person information to the face recognition device to take effect.

When a person's face is detected and it matches or mismatches the person information in the face comparison group, an event/alarm (if configured) will be triggered to notify the security personnel and you can view the face comparison information during live view on the Control Client.

Add a Face Comparison Group

You need to add a face comparison group and add persons to the group for face comparison for further configurations such as intelligent recognition task settings.

Steps

Note

For details about intelligent recognition task settings, see ***Manage Intelligent Recognition Task*** .

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Click + to open the Add Face Comparison Group pane.
3. Create a name for the face comparison group.
4. **Optional:** Enter a description about the face comparison group.

5. Click **Add**.

   The face comparison group will be displayed in the group list.
6. **Optional:** Perform further operations.

   Edit Face Comparison Group

   Select a group from the group list and then click ✎ to edit its name and description.

   Delete Face Comparison Group

   Select a face comparison group and click 🗑 to delete it.

   Add Persons to Face Comparison Group

   Select a face comparison group and click **Add** to add new or existing persons on the platform to the group.

   See details in ***Add Persons to a Face Comparison Group*** .

   Import Persons to Face Comparison Group

   Select a face comparison group and click **Import** to batch import persons to the group.

   Choose the method of importing persons. See details in ***Import Person Information by Template*** , ***Import Persons Using Zipped Profile Pictures*** , and ***Import Face Information from Enrollment Station*** .

   Delete Persons from Face Comparison Group

   Select persons in the group and click **Delete** to delete them from the group.

   Or click ⌄ → **Delete All** to delete all persons in the group.

   Delete Profile Pictures

   Select persons in the group and click ⌄ → **Delete Profile Picture Only** to delete the profile pictures of selected persons.

   Export All Face Information in a Group

   a. Click **Export**.
   b. Create a password for decompressing the exported file, and then confirm it.

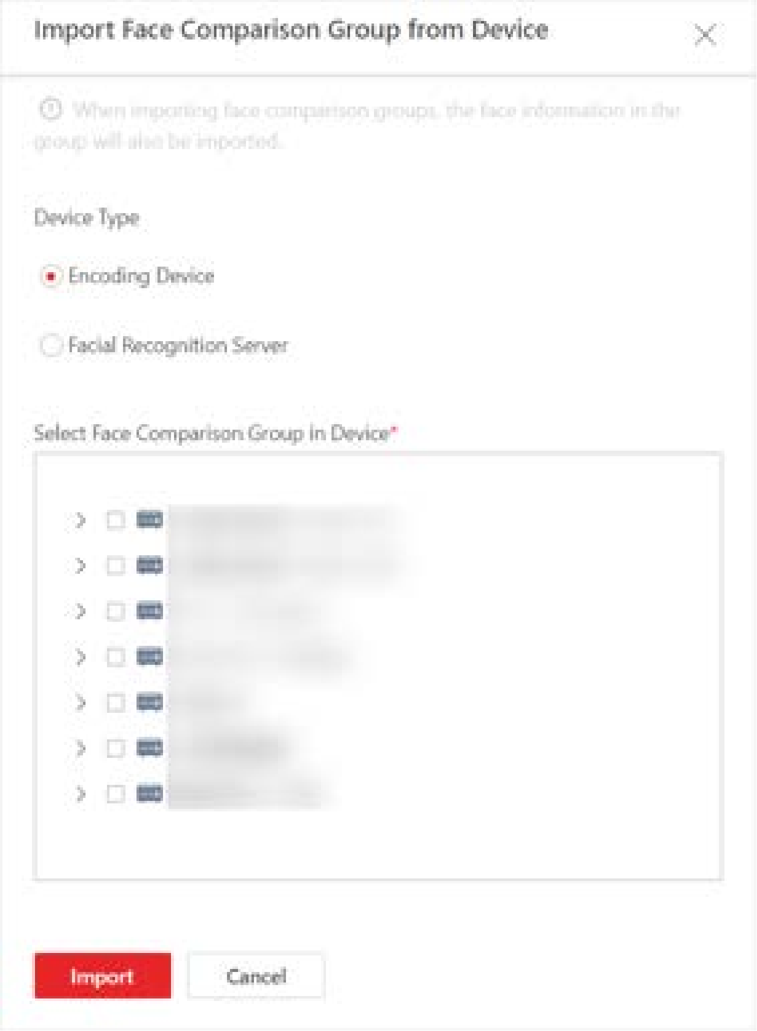
Import Face Comparison Group from Device

You can import face picture libraries from an encoding device or a facial recognition server to the platform as face comparison groups. After you importing the face picture libraries, the face information contained in them will also be imported.

Steps

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Click ⇤ to open the Import Face Comparison Group from Device pane.
3. Select **Encoding Device** or **Facial Recognition Server** from the Device Type field.

   All available devices will be displayed.



When importing face comparison groups, the face information in the group will also be imported.

Device Type

● Encoding Device

○ Facial Recognition Server

Select Face Comparison Group in Device*

Figure 14-6 Import Face Comparison Group from Device

4. Click › to show the face comparison group(s) of a device.
5. Select face comparison group(s), and the click **Import**.

   The Import Face Comparison Group window pops up, displaying the import results.

   Note

   If a face picture library fails to be imported, you can view the failure details such as library name, device name, and the failure reason.

Add Persons to a Face Comparison Group

You can add new persons manually to a face comparison group, or add existing persons on the platform to the group.

Steps

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Select a group from the group list.
3. Click **Add** → **Add New Person** or **Add Existing Person** to add persons to the group.

   Add New Person
   Enter the required person information including ID, first name, and last name, and then click **Add** or **Add and Continue** to add the person to the group.

   Add Existing Person
   Select persons from the person list, and then click **Add**.

   Note

   You can check **Include Sub-Group** to include the persons in the sub-groups.

4. 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.
5. **Optional:** Perform further operations.

   Delete Persons from Face Comparison Group
   Select persons in the group and click **Delete** to delete them from the group.

   Or click ⌄ → **Delete All** to delete all persons in the group.

   Delete Profile Pictures
   Select persons in the group and click ⌄ → **Delete Profile Picture Only** to delete the profile pictures of selected persons.

Import Person Information by Template

HikCentral Professional provides a template (an XLSX file) for batch importing person information from the local PC. You can use the template to import large amount of person information to a specific face comparison group with minimum efforts.

Steps

1. In the top left of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Select the face comparison group that needs importing person information.
3. Click **Import** → **Import by Template** to open the Import by Template pane.
4. Click **Download Template** on the pane to download the template.
5. Fill required information into the template, and then click 🗀 to select the filled-in template from the local PC.

6. **Optional:** Check **Replace Repeated Person** to allow the system to overwrite the person information already exists in the face comparison group when you import the information.
7. Click **Import**.

Import Persons Using Zipped Profile Pictures

You can batch import persons to the face comparison group by importing profile pictures in a compressed (zipped) file.

Before You Start

Make sure you have named the to-be-imported profile pictures in the following rules: "First Name + Last Name" (e.g., David Lennon), "ID" (e.g., 777816547), or "First Name + Last Name_ID" (e.g., David Lennon_777816547).

Steps

Note

The platform only supports importing photos in the format of JPG, JPEG, or PNG.

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Select a face comparison group from the group list.
3. Hover the cursor over **Import**, and then click **Import Zipped Profile Picture** to open the Import Zipped Profile Picture pane.
4. Click 🗀 to select a ZIP file from the local PC.
5. Click **Import**.

   Note

   The imported persons will also be added to the All Persons group of the platform.

Import Face Information from Enrollment Station

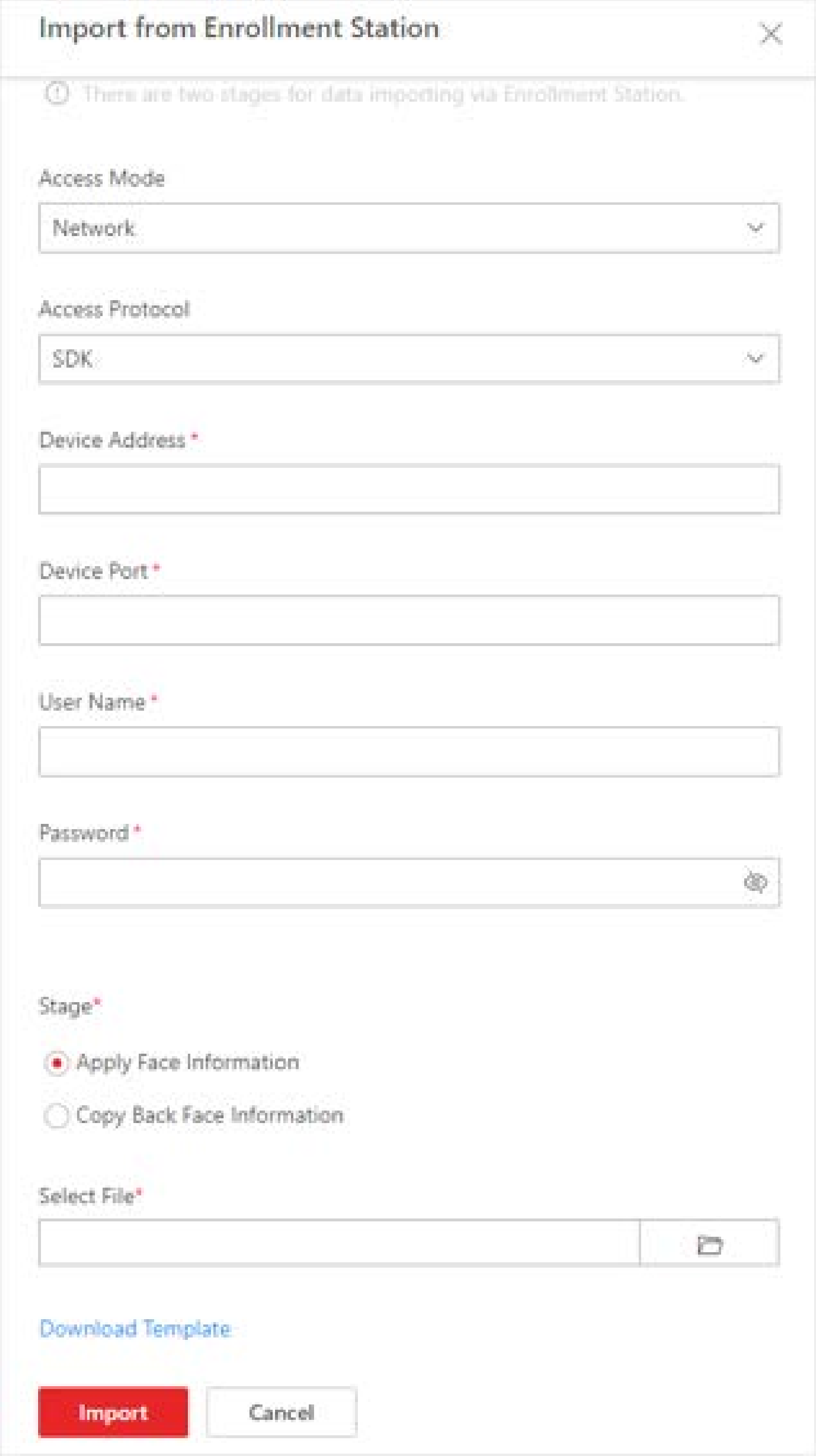
You can import face information from an enrollment station if you know its IP address, device port, user name, and password.

Before You Start

Make sure you have added the enrollment station to the platform.

Steps

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group**
2. Select a face comparison group.
3. Click **Import** → **Import from Enrollment Station** to show the Import from Enrollment Station pane.



Import from Enrollment Station

There are two stages for data importing via Enrollment Station.

Access Mode: Network

Access Protocol: SDK

Device Address *

Device Port *

User Name *

Password *

Stage*

● Apply Face Information

○ Copy Back Face Information

Select File*

Figure 14-7 Import from Enrollment Station

4. Set the required information, such as device IP address, device port, and password.

Stage

Apply Face Information

Import specific face information from the enrollment station to the face comparison group.

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 comparison group.

Copy Back Face Information

Copy back all the face information acquired by the enrollment station to the selected face comparison group.

5. Click **Import**.

Apply Face Comparison Group to Device

After setting the face comparison group and adding person(s) to the group, you need to apply the group settings to the device which supports face comparison so that the camera can compare the detected faces with the face pictures in the face comparison group and trigger alarms (if configured). After applying the face comparison group 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 comparison groups 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 🟥 **→ All Modules → Video → Intelligent Recognition → 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 camera(s) to apply the selected face comparison group(s) to.
6. Click **Apply** to start applying.

14.6.2 Manage Intelligent Recognition Task

You can add an intelligent recognition task to define the conditions such as the device and time for intelligent recognition. The task types include face comparison, people feature analysis, frequently appeared person analysis, rarely appeared person analysis, archive analysis, and behavior analysis.

Add Face Comparison Task

You can add face comparison task to define the time, device, face comparison group, similarity threshold, and so on, for face comparison. Once a face comparison task is added, the security personnel can view real-time matched face information during live view and search face comparison records via the Control Client and Mobile Client.

Before You Start

Make sure you have set face comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Face Comparison** .
2. Click **Add** to enter the Add Face Comparison Task page.
3. Set parameters, such as task name, description, and task schedule template.

   Note

   The parameter marked with a red asterisk is required.

   Task Schedule Template

   Select a task schedule template from the drop-down list to define the time when the face comparison functionality is activated.

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

   Note

   For details about adding task schedule template, see ***Add Task Schedule Template*** .

   Device for Analysis

   Select a type of face comparison device.

   Camera

   Select camera(s) from the Available list, and then click › to add selected one(s) to the Selected list.

Face Comparison Group

Select face comparison group(s). 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 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 comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.

   The face information in the selected face comparison group(s) will be applied to the selected camera(s).
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add People Feature Analysis Task

You can add a people feature analysis task to define conditions such as time, device(s), and detection area, for people feature analysis, which recognizes and records body features of the people appeared in the fields of view of the cameras linked to the people feature analysis device. Once a people feature analysis task is added, the security personnel can search and view people feature analysis records via the Control Client and Mobile Client.

Steps

1. In the top left of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **People Feature Analysis** .
2. Click **Add** to enter the Add People Feature Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when the people feature analysis functionality is activated.

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

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select a type of people feature analysis device for the execution of people 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.

4. Complete adding the task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add Frequently Appeared Person Analysis Task

You can add a frequently appeared person analysis task to define the time, device(s), appeared times threshold, and so on, for frequently appeared person analysis, which searches 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.

Before You Start

Make sure you have set facial comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select ▦ → **All Modules → Video → Intelligent Recognition → Intelligent Recognition Task → Frequently Appeared Person Analysis** .
2. Click **Add** to enter the Add Frequently Appeared Person Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when frequently appeared person analysis is activated.

You can click **View** to view detailed scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select the device type for frequently appeared person analysis.

Camera

Select camera(s) for detecting persons.

Face Comparison Group

Select face comparison group(s). 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

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 comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.

Filter Tasks	Click and set filter conditions such as task name, and then click **Filter**.

Add Rarely Appeared Person Analysis Task

You can add a rarely appeared person analysis task to define the time, device(s), appeared times threshold, and so on, for searching 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.

Before You Start

Make sure you have set facial comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Rarely Appeared Person Analysis**
2. Click **Add**to enter the Rarely Appeared Person Analysis Task page.
3. Set related information, such as task name, description, and task schedule template.

Note

The information marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when rarely appeared person analysis is activated.

You can click **View** to view detailed scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select the device type for rarely appeared person analysis.

Camera

Select camera(s) for detecting persons.

Face Comparison Group

Select face comparison group(s). 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.

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 comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add Archive Analysis Task

You can add an archive analysis task to define conditions such as time, device, and face comparison group for archive analysis. 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.

Before You Start

Make sure you have set face comparison group. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select ■ → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Archive Analysis** .
2. Click **Add** to enter the Add Archive Analysis Task page.

3. Set parameters, such as task name, description, and task schedule template.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when rarely appeared person analysis is activated.

You can click **View** to view detailed scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select the device type for archive analysis.

Camera

Select camera(s) for detecting persons.

Face Comparison Group

Select face comparison group(s). 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 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 comparison group(s) reaches the threshold, the detected face will be compared and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add Behavior Analysis Task

Behavior analysis refers to the analysis of behaviors of people, vehicle, and other objects for purposes such as finding out security threat. The available behavior analysis types include perimeter protection (e.g., intrusion detection), street behavior analysis, prisoner behavior analysis, and people density analysis. You can add a behavior analysis task to define conditions such as time, device, and detection area for behavior analysis. Once a behavior analysis task is added, the specified device will perform behavior analysis in the specified detection area during the specified periods.

Before You Start

Make sure you have added behavior analysis server to the system. For details, see ***Add DeepinMind Server*** for details.

Steps

1. In the top left of the Home page, select 🟥 → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Behavior Analysis** .
2. Click **Add** to enter the Add Behavior Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

   Note

   - The parameter marked with a red asterisk is required.
   - The parameters vary with different behavior types. Here we only introduce part of the parameters. For details about the settings of each type of behavior analysis, see the user manual of the device.

   Behavior Type

   Select a behavior type.

   The behavior types are categorized into different groups based on their usage scenarios, including people density analysis, perimeter protection, prison behavior, and street behavior.

   Task Schedule Template

   Select a task schedule template from the drop-down list to define the time when behavior analysis is activated.

   Device for Analysis

   Select a device for behavior analysis.

   Camera

   Select camera(s) for detecting behaviors.

   Detection Area

   Draw an area or line for behavior analysis.

   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.
4. Complete adding this task.
   - Click **Add** to complete adding this task.

- Click **Add and Continue** to complete adding this task and continue adding more.

5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add 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 specified detection area during the configured time.

Before You Start

Make sure you have added DeepinMind server to the platform. For details, see ***Add DeepinMind Server*** .

Steps

1. In the top left of the Home page, select ▦ → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Vehicle Analysis** .
2. Click **Add** to enter the Add Vehicle Analysis Task page.
3. Set the related parameters.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when the vehicle analysis functionality is activated.

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

Note

For details about adding a new task schedule template, see ***Add Task Schedule Template*** .

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 **Draw Area in Full Screen** to make the whole video image as a detection area.

4. Adding the task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more task(s).
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task
Select a task from the task list, and then click **Delete**.

Delete All Tasks
Click ⌄ next to **Delete**, and then click **Delete All**.

Filter Tasks
Click ▽ , set filter conditions such as task name and device for analysis, and then click **Filter**.

View Exception Details
If the device for vehicle analysis or the camera is abnormal, a red icon will appear beside the corresponding device, hover the mouse cursor on the icon to view the exception details.

14.6.3 Applying Center

In Applying Center, you can apply the face comparison group settings to the face recognition cameras to make the these settings take effect on the cameras. You can also view the cameras that fail to receive the settings and the face information that fails to be applied to the cameras, and then apply the face information again.

View Applying Status

You can view the status of the applying of face comparison groups from different perspectives, including the cameras failed to receive face comparison group, the cameras to which certain face comparison groups need to be applied, the person information failed to be applied, and the person information to be applied.

In the top left of the Home page, select ■ → **All Modules** → **Video** → **Intelligent Recognition** → **Applying Center** .

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 comparison group, analysis device, and exception details (e.g., the device reaches its maximum face comparison group capacity, the face comparison group 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 comparison groups: the applying status of each face comparison group 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 comparison group 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 comparison group 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.

Steps

1. In the top left of the Home page, select ■ → **All Modules → Video → Intelligent Recognition → Applying Center** .
2. 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 comparison group 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 comparison group 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.

14.6.4 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.

Perform the following operations to add a custom template.

Steps

1. In the top left of the Home page, select ▦ → **All Modules** → **Video** → **Intelligent Recognition** → **Task Schedule Template** .
2. Click ＋ to add a schedule template.
3. Create a name for the template.
4. **Optional:** Select an existing template from the **Copy to** drop-down list.
5. Edit weekly schedule.

   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 .

   Erase Task Time
   Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period.
6. Click **Add**.
7. **Optional:** Select a task from the task list, and then click 🗑 to delete it.

14.7 Video Application

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 Application 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.

14.7.1 Manage View

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.

Perform this task when you need to get quick access to a certain set of channels for live view or playback.

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.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Video** → **Video Application** .
2. Click **View** to enter the View page.
3. **Optional:** Add a custom view group.
   1) 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.

   2) Click .
   3) Create a name for the group or use the default name.
   4) Click **OK** to add this view group.
4. Add a view.
   1) Select a view group.
   2) Click + .
   3) Create a name for the view or use the default name.
   4) Click **Add** to select cameras.
   5) Select a stream type for each camera in the Stream Type column, or you can click **Set Stream Type** to select a stream type.
   6) Select a preset you want to switch to for each camera.
   7) **Optional:** Click **Up** or **Down** to adjust the camera order.
   8) **Optional:** Select camera(s) and click **Delete** to delete them.
   9) Select a layout for the view.

10) Select a switching interval or click **Custom Time Interval** to set the switching interval among the selected cameras.
11) Click **Add** to add this view.

5. **Optional:** You can also Drag the channels to the window or double-click the channels to start live view or playback. Save the view with the displayed view division and channels.
   - Click 💾 → **Save View** to save the current window division mode and displayed channels and (or) map as the selected view.
   - Click 💾 → **Save as View** to save the current window division mode and displayed channels and (or) map as a new view by creating view name (optional) and selecting the view saving path.

Note

If the added view is not selected before, you can also save the current window division and displayed channels as a new view.

6. **Optional:** Perform the following operations after adding the view.

Edit View	Click ✎ to edit the view settings, such as the view name and camera's stream type.
Add Camera/Map to the Existing View	a. Go to **Monitoring**. b. Select camera(s) or map. **Note** You can press Ctrl on the keyboard to select multiple cameras. c. Click 💾 → **Save View** to save the camera(s) or map to an existing view.
Delete Camera/Map from View	a. Move the cursor to a camera or a map in a view. b. Click × to close the current camera or map window. c. Click 💾 → **Save View** to save the current view.
Live View/ Playback in View Mode	Select a view, and click ··· → **Play** to start live view or playback in view mode. See ***Start Live View in View Mode*** and ***Start Playback in View Mode*** for details.
Delete View or View Group	Click 🗑 to delete the custom view or view group.
Reset View	Click ↺ to restore the view to its initial settings.
Search View	Click 🔍 , and enter keywords in the search box to search for target view(s).

14.7.2 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, and so on.

Start Live View in Area Mode

You can start the live view of cameras grouped in an area.

Before You Start

Make sure you have grouped cameras into areas. Refer to the ***Add Camera to Area for Current Site*** or ***Add Camera to Area for Remote Site*** for details.

Steps

1. In the top left corner of the Client, select ■ → **All Modules** → **Video** → **Video Application** .

   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.

   Note

   For setting the user permission, refer to ***Role and User Management*** .

2. **Optional:** Click ▦ in the upper-right corner to change live view window division.

   Average

   All the divided windows are distributed in average.

   Highlighted

   The highlighted window is used to display the live video of the critical camera.

   Horizontal

   The divided windows are distributed horizontally in the window.

   Vertical

   The divided windows are distributed vertically in the window.

   Others

   Other types of window division besides the types above.

3. Start live view.

   For One Camera

   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.

   For All Cameras in The Same Area

   Drag an area to a display window, and click **Play in Batch**, or double-click the area to start the live view of all camera in the area.

   Note

   The display windows automatically adapt to the number of cameras in the area.

4. **Optional:** When an alarm is triggered on a resource, the title bar of the resource's live view window will turn red. Click the red title bar to view the alarm information and acknowledge the alarm.

Start Live View in View Mode

You can quickly start the live view of the cameras managed in a view.

Before You Start

Make sure you have added at least a view. Refer to ***Manage View*** for details.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Video** → **Video Application** .
2. Select **View** on the left.
3. Start the live view of the cameras related to the view.
   - Double click a view.
   - Move the mouse cursor to a view, and click → **Play** beside the view name.

   Note

   You can switch the added views from the drop-down list above the live view window.
4. **Optional:** Perform further operations after starting live view.

   View Alarm Information
   When an alarm is triggered on a resource, the title bar of the resource's live view window will turn red. Click the red title bar to view the alarm information and acknowledge alarm.

   Adjust Windows' Sequence
   Drag the windows to adjust the sequences.

   Note

   The changed sequence will be restored after restarting live view in view mode.

   Stop Live View
   Click that appears in the upper-right corner when the mouse pointer is over the display window. You can also click above the display window to stop the live view of all the display windows.

Auto-Switch Cameras in an Area

You can play the live view of all cameras in an area in turn in one window and perform further operations after auto-switch starts.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Video** → **Video Application** .

   The areas which the current user has permission to access are listed and cameras which the user has permission to access are shown in each area.

   Note

   For setting the user permission, refer to ***Role and User Management*** .

2. 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.
3. **Optional:** Move the cursor to the live view window and perform further operations after auto-switch starts.

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.

PTZ Control

The Control Client provides PTZ control for cameras with pan/tilt/zoom functionality. You can set the preset, patrol and pattern for the cameras on the PTZ control panel.

Note

The PTZ control function should be supported by the camera.

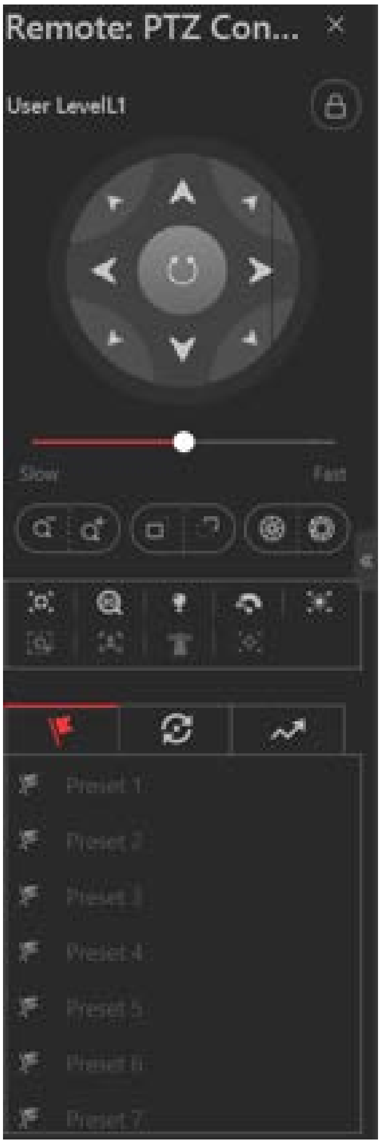


Figure 14-8 PTZ Control Panel

The following buttons are available on the PTZ control panel:

🔒	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*.
	Cancel the PTZ lock.

	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 **Focus +** move the focal point forward, and click **Focus -** to move the focal point backward.

In the live video display window, you can also click the icon to enable window PTZ control. Move the cursor to the direction you desired and click on the image to pan or tilt. You can also click and drag the cursor with a white arrows to the direction you desired for a quick direction control.

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.

Steps

1. In the top left corner of Control Client, select → **All Modules** → **Surveillance** → **Monitoring** .
2. Start live view of the PTZ camera.
3. Click to enter the PTZ Control mode.
4. Click to enter the PTZ preset configuration panel.
5. Use the direction buttons and other buttons to control the PTZ movement.
6. Select a PTZ preset number from the preset list and click .
7. Create a name for the preset in the pop-up window.
8. Click **OK** to save the settings.

Note

- Up to 256 presets can be added.
- The unconfigured preset is gray.
- The configured preset is highlighted.

9. **Optional:** After adding the preset, you can do one or more of the followings:

Call Preset Double-click the preset, or select the preset and click .

Edit Preset Select the preset from the list and click .

Delete Preset Select the preset from the list and click .

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

Two or more presets for one PTZ camera need to be added. Refer to ***Configure Preset*** for details about adding a preset.

Steps

1. In the top left corner of Control Client, select ▦ → **All Modules** → **Surveillance** → **Monitoring** .
2. Start live view of the PTZ camera.
3. Click ▣ to enter the PTZ Control mode.
4. Click ▣ to enter the PTZ patrol configuration panel.
5. Add presets to the patrol.
   1) Click ✎ on the right side of a patrol.
   2) Select **Device Preset** or **Virtual Preset** as the preset type.
   3) Click + to add a configured preset, and set the dwell time and patrol speed.

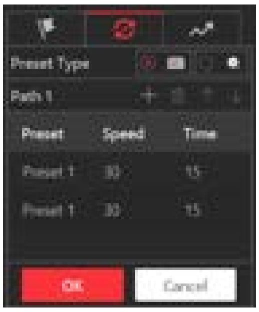
   Note

   - The preset dwell time ranges from 15 to 30s.
   - The patrol speed ranges from 1 to 40.
   - The unconfigured patrol is gray.
   - The configured patrol is highlighted.

   4) Repeat the above steps to add other presets to the patrol.

   Note

   By default, the first preset is added to the patrol list. Double-click the preset, speed, and dwell time to access a drop-down configuration list.



Preset	Speed	Time
Preset 1	30	15
Preset 1	30	15

Figure 14-9 Configure Patrol

6. **Optional:** Perform the following operations after you add the preset.

Edit Added Preset
Double-click the corresponding field of the preset to edit the settings.

Remove Preset from Patrol
Click 🗑 to remove the preset from the patrol.

Adjust Preset Sequence
Click ↑ or ↓ to adjust the presets sequence.

7. Click **OK** to save the patrol settings.

Note

Up to 8 patrols can be configured.

8. **Optional:** After setting the patrol, you can do one or more of the followings:

Call Patrol
Click to start the patrol.

Note

When the patrol is working, it will stop if you start performing PTZ control including direction button control, zoom in/out, focus +/-, iris +/-, etc. The patrol will continue working after you have stopped PTZ control for 15 seconds.

Stop Calling Patrol
Click to stop the patrol.

Configure Pattern

Patterns can be set to record the movement of the PTZ.

Steps

1. In the top left corner of Control Client, select → **All Modules** → **Surveillance** → **Monitoring** .
2. Start live view of the PTZ camera.
3. Click to enter the PTZ Control mode.
4. Click to enter the PTZ pattern configuration panel.
5. Click to start recording the movement path of the pattern.
6. Use the direction buttons and other buttons to control the PTZ movement.
7. Click to stop and save the pattern recording.

Note

Only one pattern can be configured, and the newly-defined pattern will overwrite the previous one.

8. **Optional:** After setting the pattern, you can do one or more of the followings:

Call Pattern
Click to call the pattern.

Note

When the pattern is working, it will stop if you perform PTZ control including direction button control, zoom in/out, focus +/-, iris +/-, etc. The pattern will continue working after you have stopped PTZ control for 15 seconds.

Stop Calling Pattern
Click ■ to stop calling the pattern.

Delete Pattern
Click 🗑 to clear the recorded pattern.

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

During live view, you can record the live video manually and you can export the video as video evidence.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Video** → **Video Application** .
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

   - You can change the saving path of video files in System. For details, see ***Set File Parameters*** .
   - 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

During live view, you can take a quick snapshot of the live video via the Control Client.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Video** → **Video Application** .
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

   - You can change the saving path of video files in System. For details, see ***Set File Parameters*** .
   - 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).

   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.

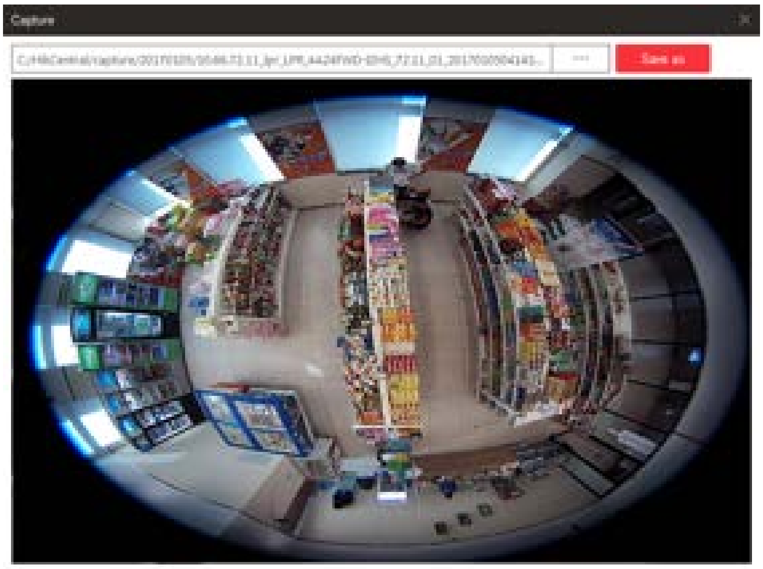


Figure 14-10 Capture Window

   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.

   Note

   The picture cannot be saved if the free space on your disk is less than 512 MB.

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.

   Note

   For details, refer to ***Start Live View in Area Mode*** and ***Start Live View in View Mode*** .

2. On the toolbar of display window, click to enter the fisheye dewarping mode and view live view.

Figure 14-11 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.

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 Client, select 🟥 → **All Modules** → **Video** → **Video Application** .
2. In the top right corner of Live View page, click ⬛ → **Toolbar** .
3. In **Live View Toolbar** 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 14-3 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 **Search by Picture** 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.
	Switch Stream Type	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.
	Video Enhancement	Adjust the video image including brightness, saturation, etc.
	Rotate Image	Rotate a 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).

Note

The icons on the toolbar in the live view window vary with the device's capabilities.

5. **Optional:** Check **Always Display Toolbar** to always show the toolbar on the live view window.
6. Click **Save**.

14.7.3 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.

Normal Playback

You can search video files by area or camera for the Normal Playback and download found video files to local PC. You can also add a tag to mark important video footage, and so on.

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.

Search Video File

You can search video files by camera, by area, or by time for normal playback. And you can also filter the searched video files by recording type, tag type, target type and storage location.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Video** → **Video Application** .
2. Click **Playback** to enter the playback page.
3. Drag the camera or area to the display window, or double-click the camera or area to play the recording of the specified camera(s) in selected window.

   Note

   The playback window supports up to 16 channels.

   Today's recorded video files of the selected camera will be played.
4. Click ▦ on the toolbar to set the date and time.

   Note

   In the calendar, the date with video files will be marked with a triangle.

   After selecting the date and time, the matched video files will start playing in the display window.
5. **Optional:** Click ▼ on the toolbar to select recording type, tag type, target type and storage location for playback.

   Note

   To set the storage location for recording, refer to ***Configure Storage and Recording*** .

Play Video File

After searching the video files for the normal playback, you can play the video via timeline or thumbnails.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Video** → **Video Application** .
2. Click the **Playback** tab to enter the playback page.
3. Select a date with videos to start playing video and show the timeline after searching the video files.

   Note

   The video files of different types are displayed in different colors on the timeline.
4. Play video in specified time period by timeline or thumbnails.
   - Drag the timeline forward or backward to position the desired video segment.
   - Move the cursor over the timeline to take a quick view of video thumbnails (if supported by the device) and click the appearing thumbnail to play the specific video segment.

   Note

   - Click ⊞ / ⊟ on the right of the timeline bar, or use the mouse wheel to zoom in or zoom out the timeline.
   - Click ▥ / ▣ to show or hide the thumbnail bar.
   - Move the cursor to the top border of the thumbnail bar and drag to adjust the height of the thumbnails when the cursor changes into ÷ . You can also click ▨ to lock the thumbnail bar above the playback timeline, and click ▨ to hide the thumbnail bar automatically.

Start Playback in View Mode

You can quickly access the playback of the cameras managed in a view.

Before You Start

Make sure you have added a view. For details, refer to ***Manage View*** .

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Video** → **Video Application** .
2. Click **View** on the left navigation bar.
3. Click the **Playback** tab to enter the playback page.
4. Click a view to quickly start the playback of all the cameras related to the view.

   Note

   You can also quickly switch the added view from the drop-down view list above the display windows.

Synchronous Playback

You can play the video files of different cameras synchronously. Synchronous playback allows you to synchronize the display of video from multiple cameras.

Steps

Note

Video files from up to 16 cameras can be played simultaneously.

1. In the top left corner of the Client, select ■ → **All Modules** → **Video** → **Video Application** .
2. Click the **Playback** tab to enter the playback page.
3. Start normal playback of at least two cameras.

   Note

   For detailed configuration about normal playback and playback control, refer to ***Normal Playback*** . Some icons may not be available for synchronous playback.
4. Click **Synchronous Playback** on the playback toolbar to enable the synchronous playback.

   The cameras displayed in Playback will start synchronous playback.
5. **Optional:** Click **Asynchronous Playback** on the playback toolbar to disable synchronous playback.
6. **Optional:** Click ◁ and ▷ to perform normal and reverse playback.
7. **Optional:** Click ◁ and ▷ to perform single-frame normal and reverse playback.

   Note

   - No more than 16 cameras are allowed in single-frame normal and reverse playback.
   - If you pause one camera, others will be paused in the synchronous playback mode.
8. **Optional:** Move the cursor to the lower edge of the playback window to access the icons for further operations.

   Note

   For details, refer to ***Customize Icons on Playback Window*** .

Fisheye Playback

Fisheye playback function allows you to play the fisheye camera's video in fisheye dewarping mode. Fisheye dewarping mode refers to the process of perspective correction of an image, to reverse the effects of geometric distortions caused by the fisheye camera lens. Dewarping allows you to cover a wide area with a single device and have a normal view of an otherwise distorted or reversed image.

Steps

1. In the top left corner of the Client, select ■ → **All Modules** → **Video** → **Video Application** .

2. Click the **Playback** tab to enter the playback page.
3. Select a fisheye camera from the camera list to start playback.

Note

For detailed configuration about playback and playback control, refer to ***Normal Playback*** .

4. Move the cursor to the display window, and click on the appearing toolbar to enter the fisheye dewarping mode.
5. Drag on the video to adjust the view angle.
6. Scroll the mouse wheel to zoom in or zoom out the view.

Customize Icons on Playback Window

You can customize the icons shown on the toolbar of the playback window, adjust the icon order and set whether to always display toolbar on the playback window.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Video** → **Video Application** .
2. In the top right corner of Playback page, click → **Toolbar** .
3. In **Playback Toolbar** section, add or remove the icons to show or hide the icons on the live view toolbar.
4. Customize playback toolbar.
   - Click an icon in the list to add it to the gray frame below to hide the icon. Icons in the gray frame will be hidden in the toolbar of the playback window.
   - Click the icon in the gray frame to add it back to the playback toolbar to show an icon on the toolbar.
5. Drag the icons in the icon list to adjust icon order.

Table 14-4 Icons on Playback Toolbar

🔊	Audio Control	Turn off/on the sound and adjust the volume.
📷	Capture	Take a snapshot of the current video and save in the current PC. **Note** After capturing a picture, a thumbnail will pop up on the upper-right corner. You can click **Search by Picture** to search the captured picture, archive, and identity verification related with the captured picture.
✂	Clip	Clip the video files for current playback and save in the current PC. You can save the clipped video as evidence, and set the saving path for the clipped video files. For

		details about saving video files as evidence and setting saving path, see ***Manual Recording*** .
	Add Tag	Add custom tag for the video file to mark the important video point. You can also edit the tag or go to the tag position conveniently.
	Lock Video	Lock the video file and set the locking duration to avoid deleting the video file and protect the video file from being overwritten when the HDD is full. **Note** For the camera imported from Remote Site, if the video files are stored on the encoding device locally, you cannot lock the video files.
	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. **Note** When in software decoding mode, you can also capture the zoomed in picture after enabling digital zoom function.
	Fisheye Expansion	Available for fisheye camera for entering the fisheye dewarping mode. See ***Fisheye Playback*** .
	Stream Switch	Switch the stream to main stream, sub-stream (if supported), or smooth stream (if supported). If the device supports transcoding playback, start transcoding and you need to set the resolution, frame rate and bitrate for transcoding. **Note** • The smooth stream will show if device supports. You can switch to smooth stream when in low bandwidth situation to make playback more fluent. • Only video files stored in DVR and I-series NVR support transcoding playback.
	Video Enhancement	Adjust the video image including brightness, saturation, etc.

🎙	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.
⟳	Rotate Image	Rotate a image.

Note

The icons shown on the toolbar in the display window will vary with the device's capabilities.

6. **Optional:** Check **Always Display Toolbar** to always display the toolbar on the playback window.
7. Click **Save** to save the above settings.

14.7.4 Set Video Parameters

You can set network parameters, picture file format, image parameters, people counting display parameters, icons on live view and playback toolbar, and shortcuts for keyboard and joystick.

Set Network Parameters

You can set global stream type for live view and window divisions for main stream.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Video** → **Video Application** .
2. In the top right corner of Live View or Playback page, click ⚙ → **Network** to enter network settings page.
3. Configure network parameters.

   Global Stream

   Select the default stream type for live view for global usage. If the network is in good condition, select main stream or sub-stream. If the network is in poor condition, select smooth stream.

   If the device doesn't support smooth stream, it will use sub-stream. If the device doesn't support sub-stream, it will use main stream.

   If you don't want to adopt global stream settings for certain encoding device, you can go to **Maintenance** → **Health Monitoring** → **Encoding Device** and switch its stream type (refer to ***Resource Status*** for details). The Control Client will get this stream type to start live view of the encoding device's resources.

   Window Divisions for Main Stream

   When the number of divided windows is smaller than the number you set, the live video will be displayed by main stream.

   Note

   This parameter is invalid for playback.

Network Timeout

Network timeout duration refers to the default waiting time for the configurations on the Web Client. The configuration will be regarded as failure if there is no response within the configured timeout time.

The minimum default waiting time of the interactions between the configurations and SYS server is 60s, the minimum time between SYS server and devices is 5s, and the minimum time between the configurations and devices is 5s.

Note

This parameter affects all the Web Clients accessing the current SYS server.

4. Click **Save**.

Set File Parameters

You can set the file format of pictures captured during live view and playback.

In the top-left corner of the Client, select ■ → **All Modules** → **Video** → **Video Application** . And then in the top-right corner of the Live View or Playback page, click ■ → **File** to enter the file settings page.

Select the file format for pictures captured during live view or playback.

Set the saving path for the files you will download to your computer (manually recorded video files, captured pictures, etc.).

Click **Save** to save the settings.

Set Display Parameters

You can set display parameters, including view scale, video caching, etc.

Steps

1. In the top left corner of the Client, select ■ → **All Modules** → **Video** → **Video Application** .
2. In the top right corner of Live View or Playback page, click ■ → **Display** to enter display settings page.
3. Configure the display parameters.

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 set as 4:3 or 16:9.

Display Window No.

Display the No. of each window in Monitoring module.

Display VCA Rule

When On, displays the VCA rule in the live view and playback.

Video Caching

Larger frame caching will result in better video performance. It is determined based on network performance, computer performance, and bit rate.

Continuous Decoding

Decode continuously when switching window division between one window and multiple windows.

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.

Note

It is not supported when GPU hardware decoding is enabled.

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. When the performance of the graphic card is good, you can enable GPU decoding to lower the computer's performance consumption. It is not recommended to enable this function if the graphic card's performance is poor.

Note

- Your computer must support GPU decoding.
- After enabling GPU decoding, restart live view and playback for GPU decoding to take effect.
- If the client shows a blurred screen after enabling GPU decoding, disable GPU decoding.
- If GPU decoding is enabled, overlaying transaction information on live view and playback image is not supported.

4. Click **Save**.

14.7.5 Manage Favorites

You can add and manage Favorites on the client. For camera(s) added to the Favorites, you can quickly view the live view or start the playback.

Before You Start

Make sure you have added camera(s) to area(s). Refer to the ***Add Camera to Area for Current Site*** or ***Add Camera to Area for Remote Site*** for details.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Video** → **Video Application** .
2. Click **Favorites** on the left navigation bar.

Note

In the Favorites list, two default root Favorites (**Favorites** and **Favorites Shared by Others**) are displayed. You can click › to view the sub Favorites and cameras added in these two root Favorites.

3. Select a parent Favorites.

Note

You can either select the root Favorites or the sub Favorites added under the root one.

4. Add a Favorites under the parent Favorites.
   1) Click + .
   2) Enter the name for Favorites.
   3) **Optional:** Select a parent node from the drop-down list.
   4) **Optional:** Check **Online Resource Only** to display online resources only on the list.
   5) Select the camera(s) to be added to Favorites.
   6) Click **Save**.

Note

Up to 5 levels of Favorites can be added.

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

Edit Favorites

Select a Favorites, and click ⋯ → **Edit** on the right side of Favorites' name to edit its name and add more camera(s) to it if needed.

Share Favorites

Select a Favorites, and click ⋯ → **Share** on the right side of Favorites' name to share it with others.

Note

For details about adding user(s), refer to the *User Manual of HikCentral Professional Web Client*.

Delete Favorites

Select a Favorites, and there are two methods to delete it.

- Click 🗑 on the top of the Favorites list, and click **OK**.
- Click ⋯ → **Delete** on the right side of Favorites' name.

View Live View/Playback of All Cameras

- 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.
- When in Playback window, select a Favorites, and click ⋯ → **Play All** to start viewing the playback of all the camera(s) added in Favorites.

Search Camera in Favorites

Enter keywords in the search box above the Favorites list to search for the target camera(s) or Favorites.

Delete Camera in Favorites	Select a camera in Favorites, and click 🗑 to delete it.

Chapter 15 Mobile Monitoring

The Mobile Monitoring function 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 routes vehicles have traveled along, and searching for events and alarms triggered by vehicles. You can configure fence rules and deviation 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.

15.1 Flow Chart

The flow chart introduces the process of mobile monitoring configuration.

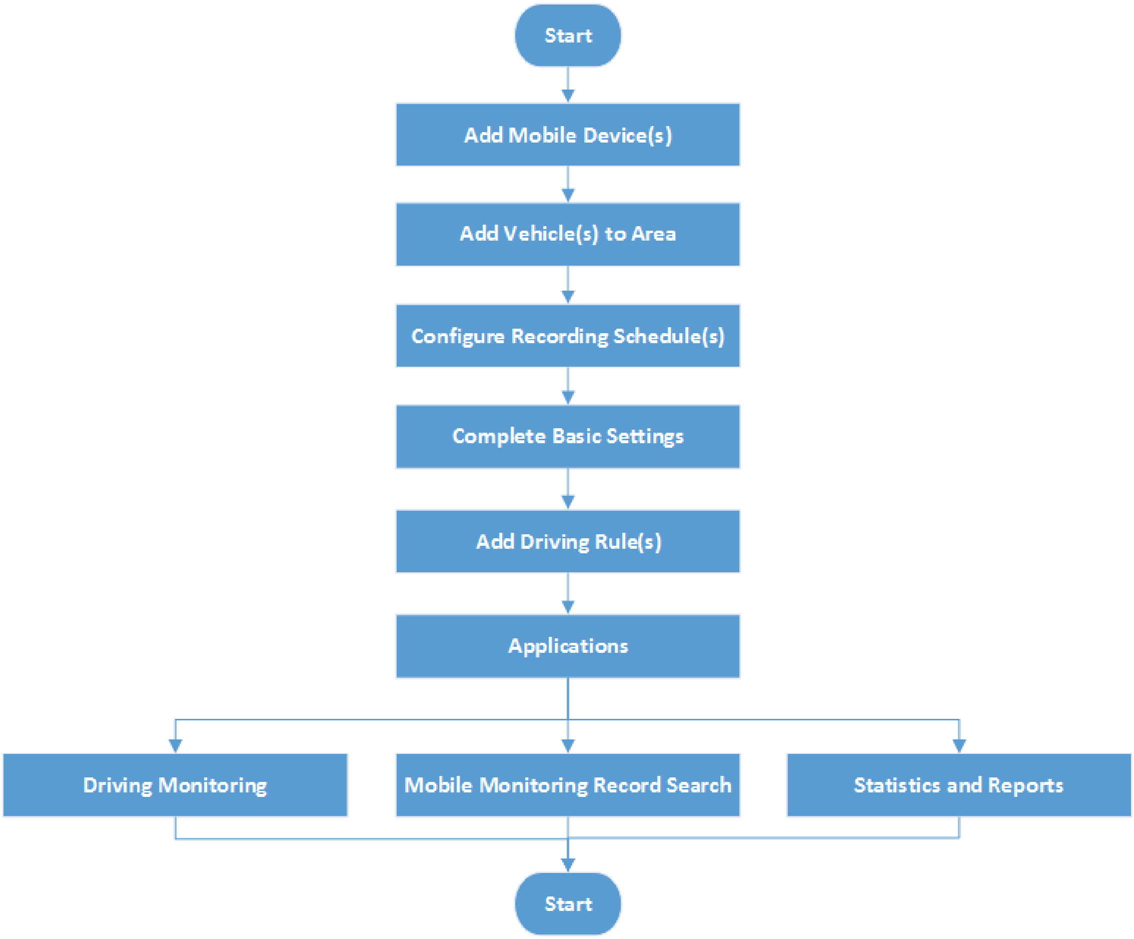


Figure 15-1 Flow Chart of Mobile Monitoring Configuration

15.2 Mobile Monitoring Overview

The Overview page displays the major steps of Mobile Monitoring configuration and presents brief information such as the health of devices and real-time driving events.

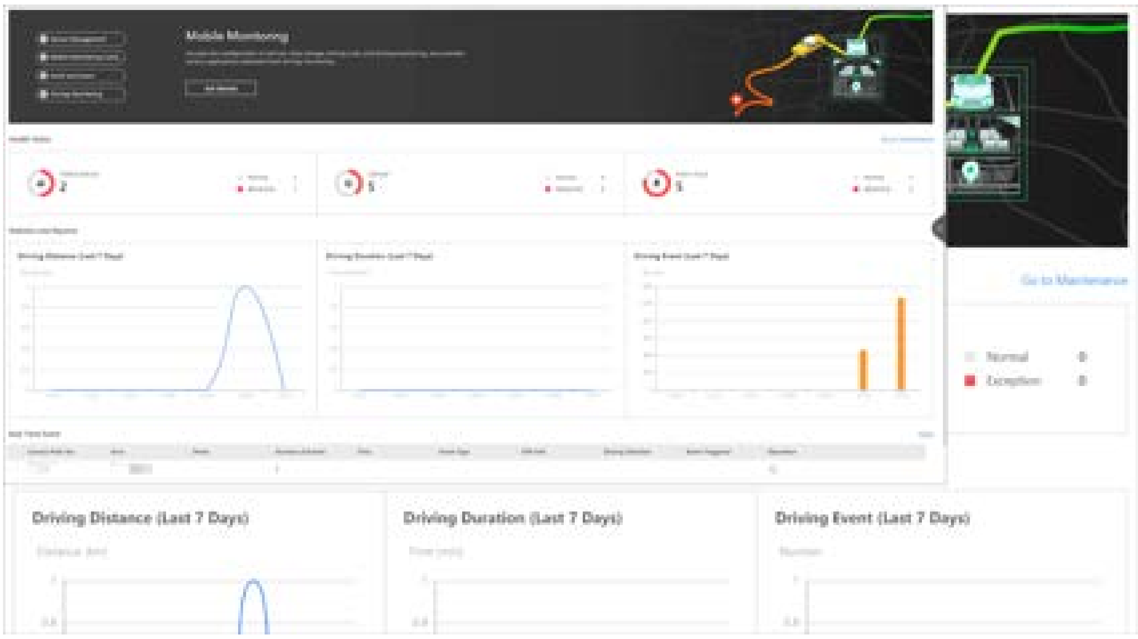

Mobile Monitoring
Go to Maintenance
Normal
Exception
Driving Distance (Last 7 Days)
Distance (km)
Driving Duration (Last 7 Days)
Time (min)
Driving Event (Last 7 Days)
Number

Figure 15-2 Mobile Monitoring Overview

Banner

The banner briefly introduces the Mobile Monitoring function and the major steps of configuration. You can click each button to complete a relevant step, or click **Get Started** and then click to follow the wizard to complete configuration including adding mobile devices, adding vehicles, configuring recording settings, etc.

Health Status

You can view the health of devices including mobile devices, cameras, and alarm inputs. You can click **Go to Maintenance** to view more details.

Statistics and Reports

You can view some of the mobile monitoring statistics generated in the last 7 days, including the driving distance, driving duration, and driving event. See ***Statistics and Reports*** for how to view more details and reports.

Real-Time Event

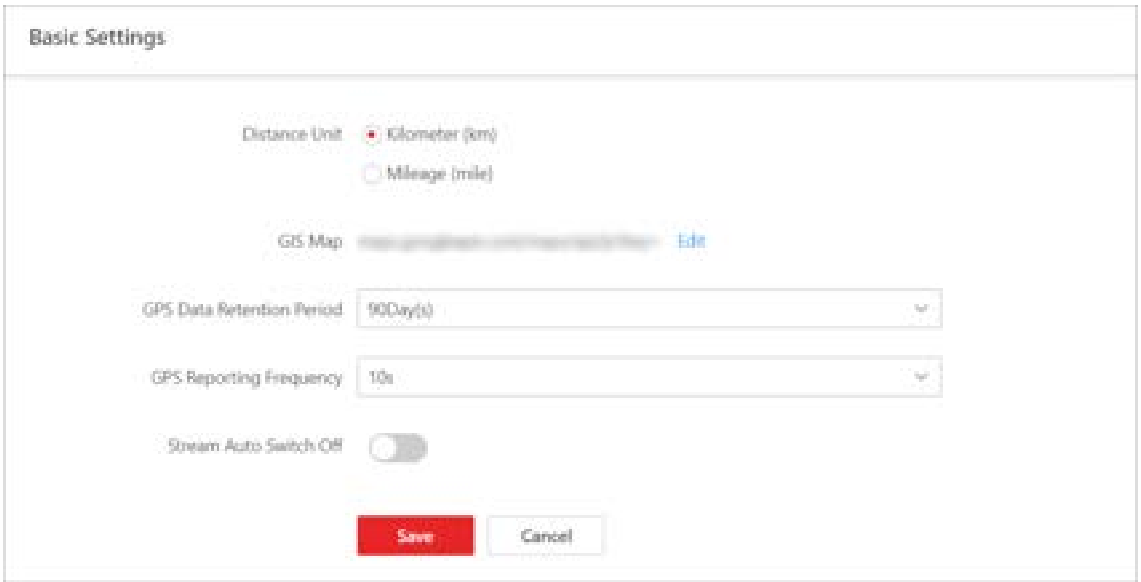
You can view the events triggered by monitored vehicles. Detailed information of each record is also provided, including the vehicle's license plate number, the area where an event was triggered, driver information, etc. You can click **More** to go to the Driving Event Search page to search for more driving events. See ***Search for Driving Events*** for details.

15.3 Basic Settings

You can configure basic setting including the distance unit, GIS map, retention period of GPS data, etc.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Mobile Monitoring** .
2. Select **Basic Settings** on the left to enter the Basic Settings page.



Basic Settings

Distance Unit ● Kilometer (km)
○ Mileage (mile)

GIS Map [illegible] Edit

GPS Data Retention Period 90Day(s)

GPS Reporting Frequency 10s

Stream Auto Switch Off

Figure 15-3 Basic Settings

3. Select a distance unit.
4. Click **Edit** to edit the GIS map.

Note

If you have not configured a GIS map, you should click **Configure GIS Map** to configure a GIS map first. See ***Set GIS Map and Icons*** for details.

5. Select the retention period of GPS data.
6. Set the frequency at which the GPS information is reported to the platform.
7. **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.

15.4 Driving Rule

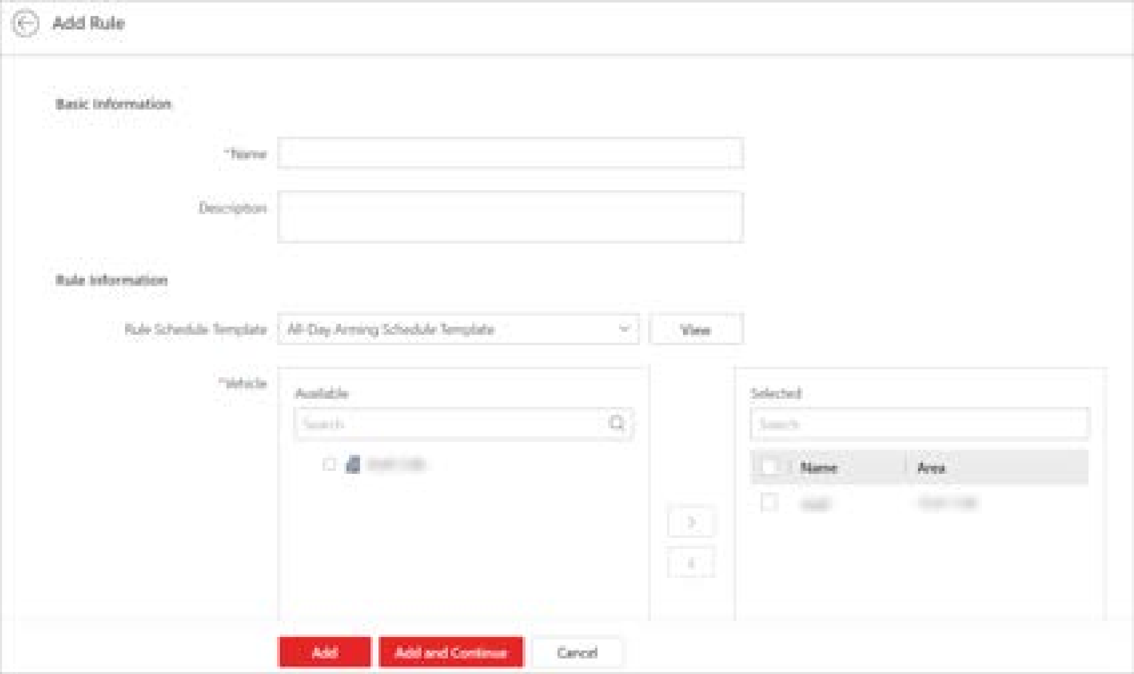
There are two types of driving rule: fence rule and deviation rule. A fence rule specifies the area where vehicles are allowed or not allowed to drive and a deviation rule specifies the route that vehicles should drive along. Besides, you can configure rule schedule templates to define when the rules should take effect. As a result, if a vehicle breaks an effective rule, an alarm will be triggered and uploaded to the platform.

15.4.1 Configure a Fence Rule

You can add a fence rule to specify the area where vehicles are allowed or not allowed to drive.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Mobile Monitoring** .
2. Select **Driving Rule Configuration** → **Fence Rule** on the left.
3. Click **Add** to enter the Add Rule page.



Rule Schedule Template: All-Day Arming Schedule Template

Figure 15-4 Add a Fence Rule

4. Set the basic information.
   1) Create a name for the fence rule.
   2) **Optional:** Enter the description of the fence rule.
5. 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) Click to draw a fence area on the map.

6. Click **Add** to finish or click **Add and Continue** to add another fence rule.
7. **Optional:** Perform the following operations after configuring the fence rule(s).

Manage Fence Area

- Select a fence area and drag its edges to adjust it shape or size.
- Select a fence area and click to delete it.

Manage Map

- Click to display the map in full-screen mode.
- Click to place selected vehicle(s) in the center of the map.
- Click + / - to zoom in/out on the map.

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

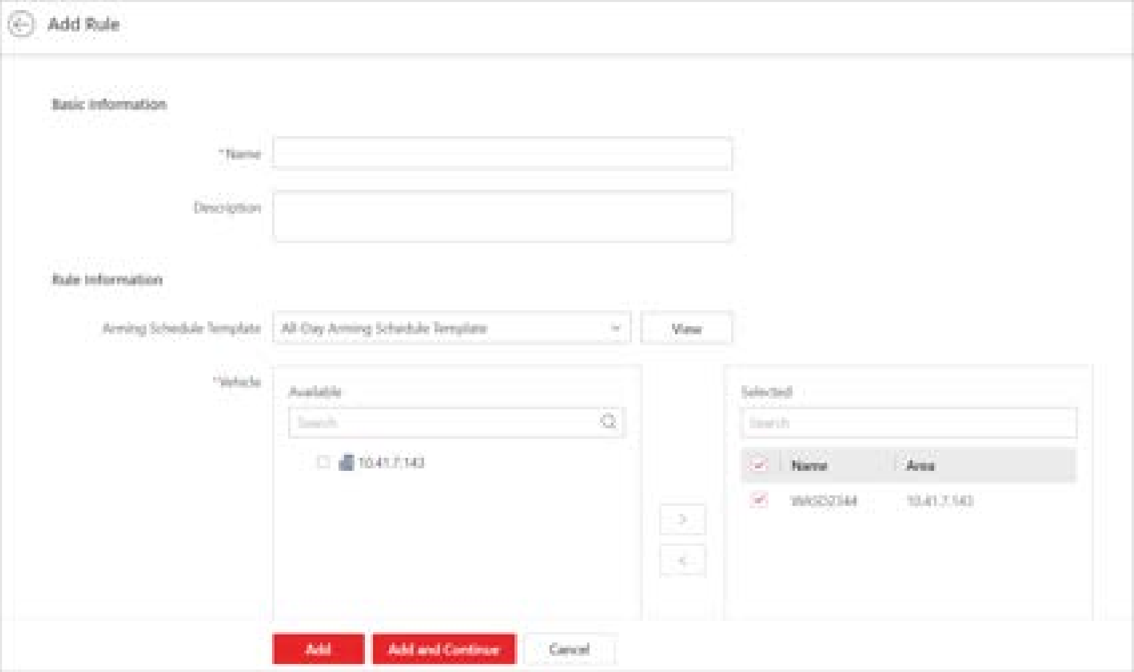
On the rule list, select one or multiple fence rules and click **Delete** to delete them.

15.4.2 Configure a Deviation Rule

You can add a deviation rule to specify the route that vehicles should drive along.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Mobile Monitoring** .
2. Select **Driving Rule Configuration** → **Deviation Rule** on the left.
3. Click **Add** to enter the Ad Rule page.



Basic Information

*Name

Description

Rule Information

Arming Schedule Template: All-Day Arming Schedule Template

*Vehicle

Available

Search

□ 10.41.7.143

Selected

Search

☑	Name	Area
☑	WASD2344	10.41.7.143

Figure 15-5 Add a Deviation Rule

4. Set basic information.
   1) Create a name for the deviation rule.
   2) **Optional:** Enter the description of the deviation rule.
5. 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) Click to draw a route on the map.
6. Click **Add** to finish or click **Add and Continue** to add another deviation rule.
7. **Optional:** Perform the following operations.

Manage Route	• Select a route and drag a point to move the route. • Select a route and click to delete it.

Manage Map	• Click ⛶ to display the map in full-screen mode. • Click ▣ to place selected vehicle(s) in the center of the map. • Click + / - to zoom in/out on the map.
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.

15.4.3 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. In the top left corner of the Client, select ▦ → **All Modules** → **Mobile Monitoring** .
2. Select **Driving Rule Configuration** → **Rule Schedule Template** on the left.
3. Click + to enter the Add Rule Schedule Template page.

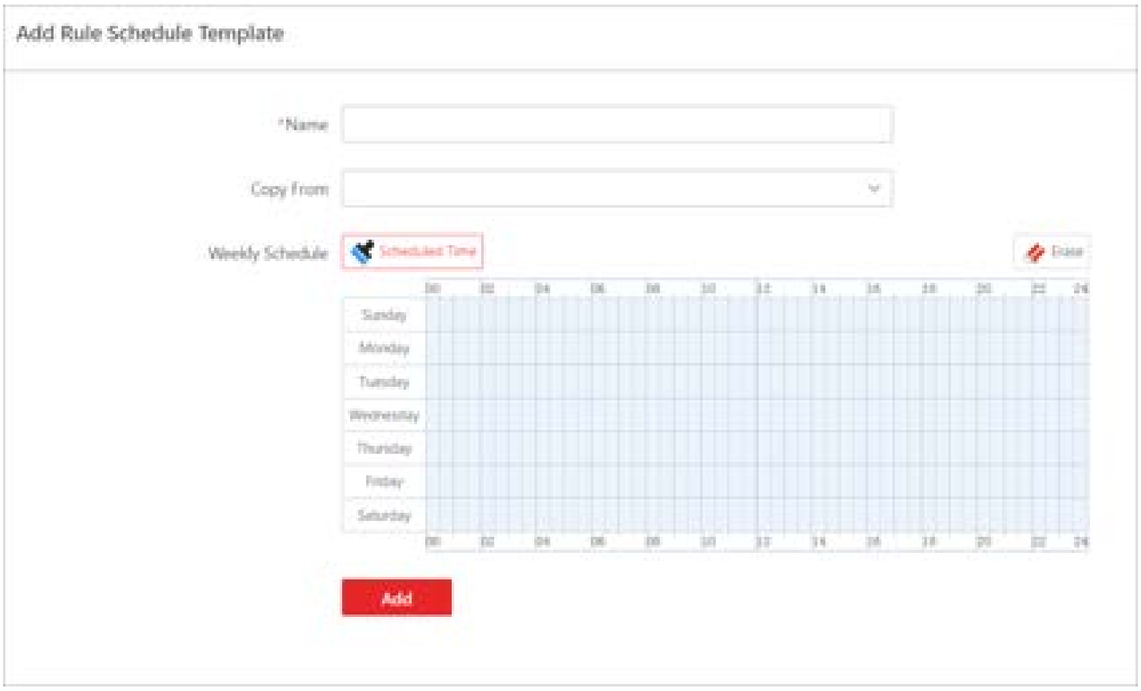


Figure 15-6 Add Rule Schedule Template

4. Create a name for the rule schedule template.

5. **Optional:** In the **Copy from** field, select an existing template to copy its weekly schedule to the current one.
6. 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.

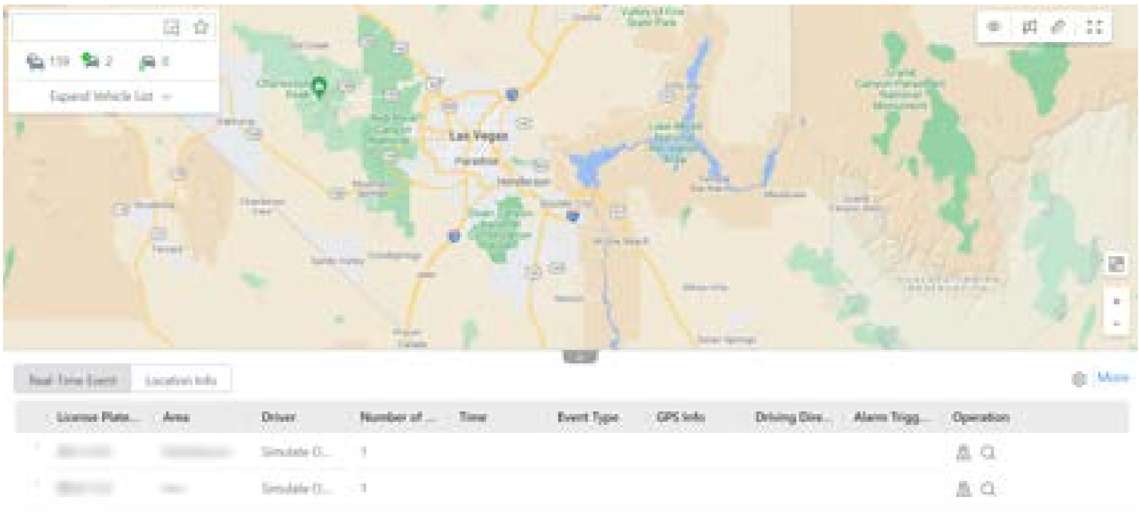
7. **Optional:** Click **Erase** and click or drag on the formerly selected rectangle(s) to remove them from the scheduled time.
8. **Optional:** Perform the following operations.

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.

15.5 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 routes vehicles have traveled along, and add vehicles to the Favorites list for quick and easy management.

In the top left corner of the Client, select ▦ → **All Modules** → **Mobile Monitoring** → **Driving Monitoring** to enter the Driving Monitoring page.



License Plate...	Area	Driver	Number of ...	Time	Event Type	GPS Info	Driving Dire...	Alarm Trigg...	Operation
[redacted]	[redacted]	Simulate D...	1						
[redacted]	[redacted]	Simulate D...	1						

Figure 15-7 Driving Monitoring Page

Vehicle List Pane

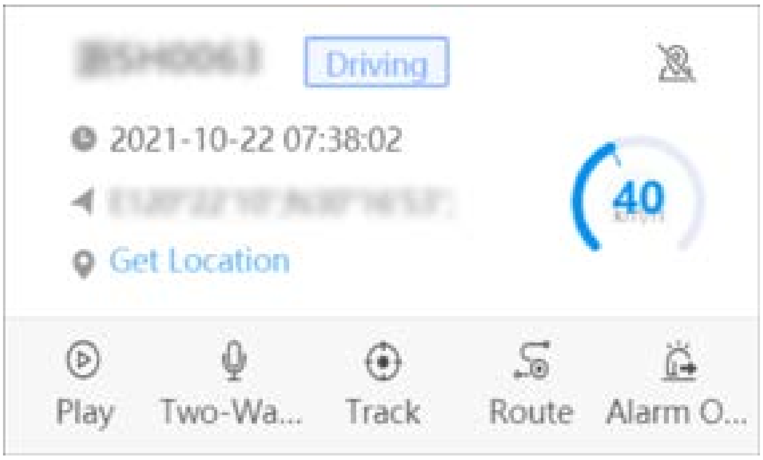
On the vehicle list pane, you can click **Expand Vehicle List** and then click / / to view all/ online/located vehicles.

You can move the cursor onto a vehicle to view its real-time information, including its location, speed, etc, and can perform the following operations:

Operation	Step
Search for Vehicle	Enter key words in the search box and click to search for the specified vehicle.
Locate Vehicle	Click to locate the vehicle on the map and click again to cancel locating it.
Play Back Route	Click to play back the route the vehicle has traveled along.
Other	Click ··· to open the operation menu and you can choose to play video, talk to a driver via two-way audio, track a vehicle in real time, play back traveled route, control alarm outputs, and add/remove a vehicle from the Favorites list. **Note** You can click ☆ to display the Favorites list.

Driving Monitoring Pane

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:



Driving

2021-10-22 07:38:02

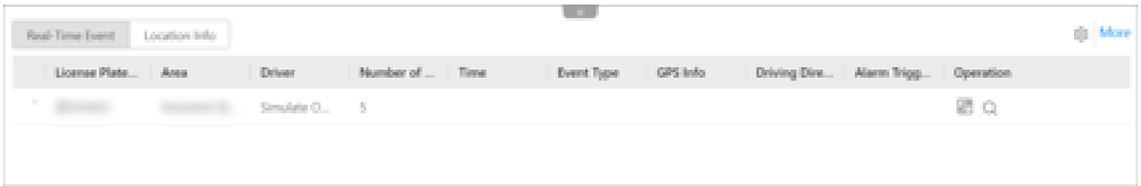
Get Location

Figure 15-8 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 videos or play back video recordings streamed from vehicle-mounted cameras.
Talk to Driver	Click **Two-Way Audio** to talk to the driver.
Track Vehicle	Click **Track** 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 Route	Click **Route** and select a period and camera to play back the route recorded by the camera in the specified period.
Control Alarm Output	Click **Alarm Output Control** and then click / to enable/disable the alarm output related to the vehicle.

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. Besides, you can perform the following operations:



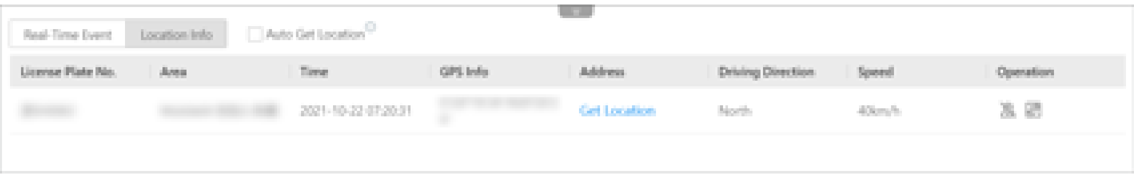
License Plate...	Area	Driver	Number of ...	Time	Event Type	GPS Info	Driving Dire...	Alarm Trigg...	Operation
[redacted]	[redacted]	Simulate O...	5						

Figure 15-9 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 Route	Click in the Operation column to go to the Vehicle Route Search page to search for the route a vehicle has traveled along.
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:



License Plate No.	Area	Time	GPS Info	Address	Driving Direction	Speed	Operation
[redacted]	[redacted]	2021-10-22 07:20:31	[redacted]	Get Location	North	40km/h	

Figure 15-10 Location Info Table

Operation	Step
Get Vehicle's Location	Click **Get Location** in the 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 to cancel locating a vehicle.
Center Vehicle	Click to place a vehicle in the center of the map.

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 fence area or/and route on the map.
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.
Zoom Map	Click + / - to zoom in/out on the map.

15.6 Mobile Monitoring Record

Mobile monitoring records include the routes vehicles have traveled along and the events triggered by them in a specified period. You can search for each of the two types of records, view the details of each record, and export records to your PC for further use.

15.6.1 Search for Vehicle Routes

You can search for the routes that vehicles have traveled along in the specified period, view detailed information of each record, play back routes, and export records to the PC.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Mobile Monitoring** .

2. Select **Search → Vehicle Route Search** on the left.
3. Set search conditions.
   1) Specify the period you want to search for vehicle routes in.
   2) Select vehicle(s).
   3) **Optional:** Switch on **Speed Range** and set a speed range.
   4) **Optional:** Switch on **Event Type** and click ⎘ to select event type(s).

   Note

   All event types have been selected by default.
4. Click **Search**.

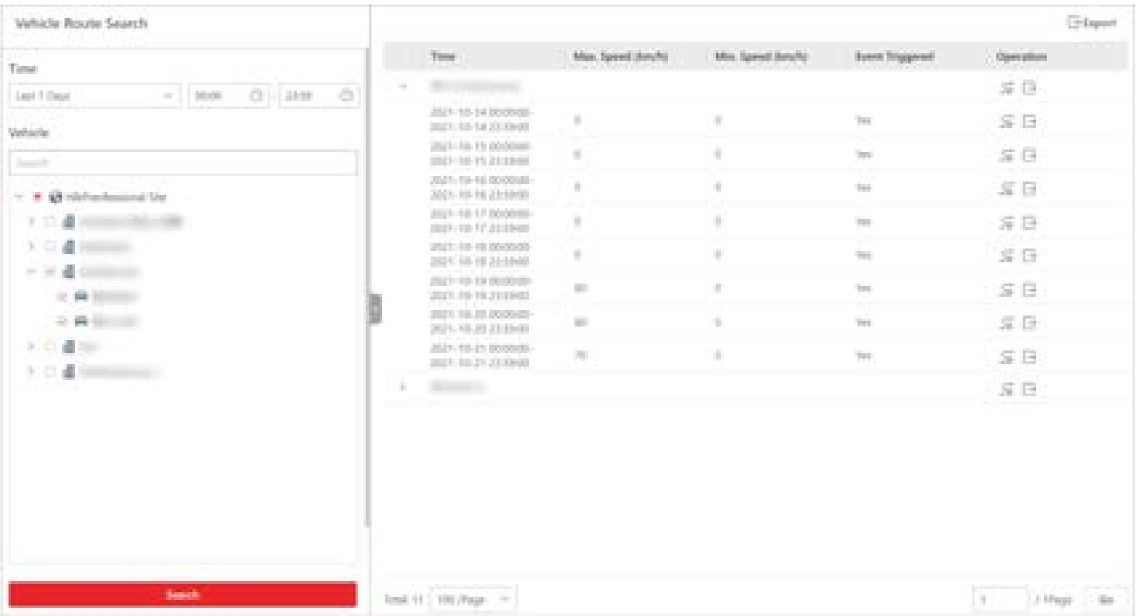


Figure 15-11 Vehicle Route Search

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

Play Back Route	Click ⇆ to play back a route.
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 route and click ⇥ to export a record to the PC.

15.6.2 Search for Driving Events

You can search for the event triggered by vehicles, view detailed information of each record, and export records to the PC.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Mobile Monitoring** .
2. Select **Search** → **Driving Event Search** on the left.
3. Set search conditions.
   1) Specify the period you want to search for driving events in.
   2) Click to select vehicle(s).

   Note

   All vehicle(s) have been selected by default.

   3) Click to select event type(s).

   Note

   All event types have been selected by default.

   4) Click **Specify Area on Map** and draw an area on the map.

   The platform will search for events triggered in the specified area.
4. Click **Search**.

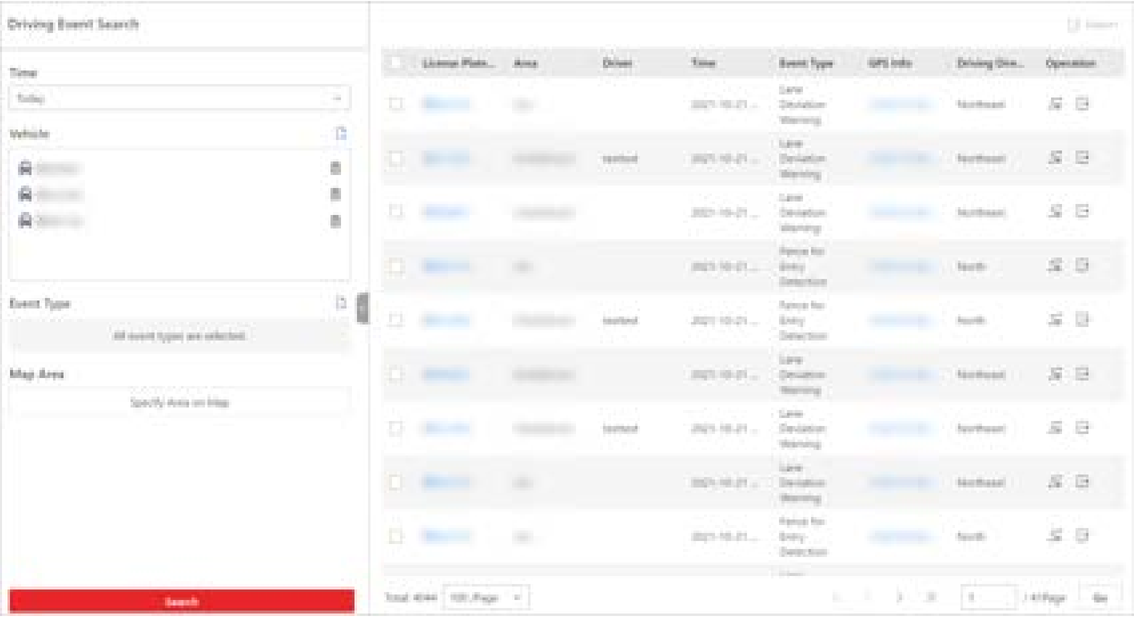


Figure 15-12 Driving Event Search

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

Play Back Route Click to play back a route.

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.

15.7 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.

15.7.1 Overview

You can have an overview of mobile monitoring data in the last 7 days on one page, including the GPS information, driving distance, driving duration, overspeed times, driving events, and device online rate.

In the top left corner of the Web Client, select → All Modules → Mobile Monitoring → Statistics and Reports → Overview to enter the overview page.

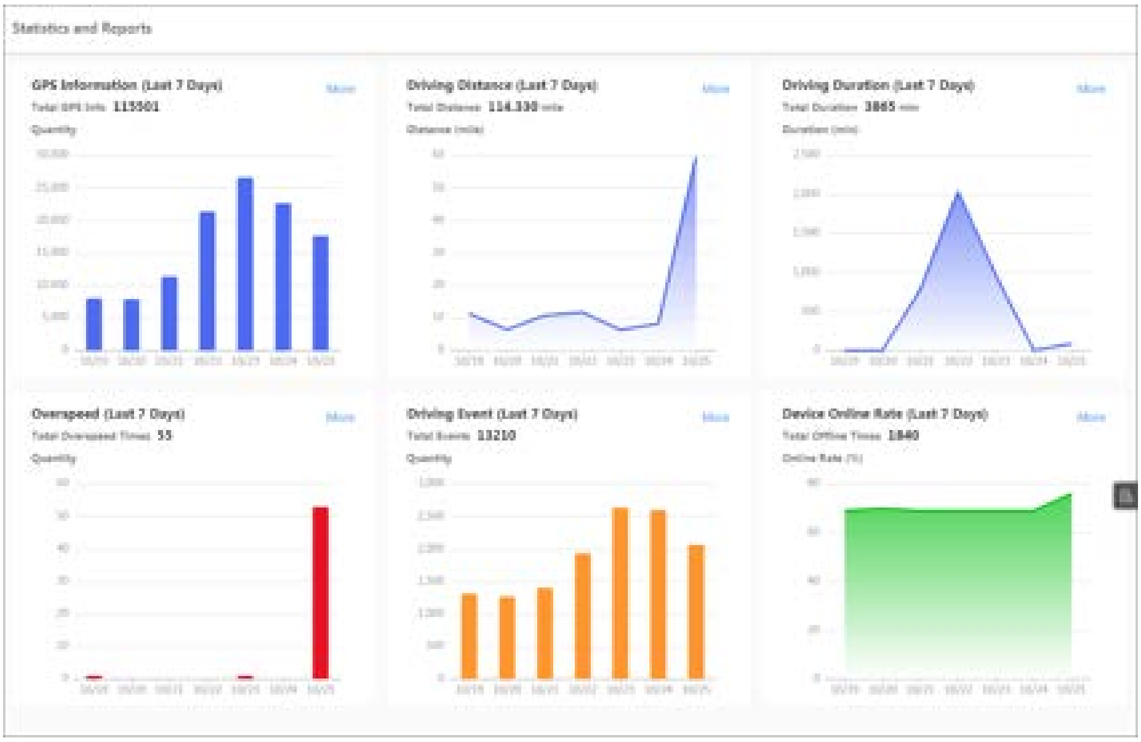


Figure 15-13 Statistics Overview

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.

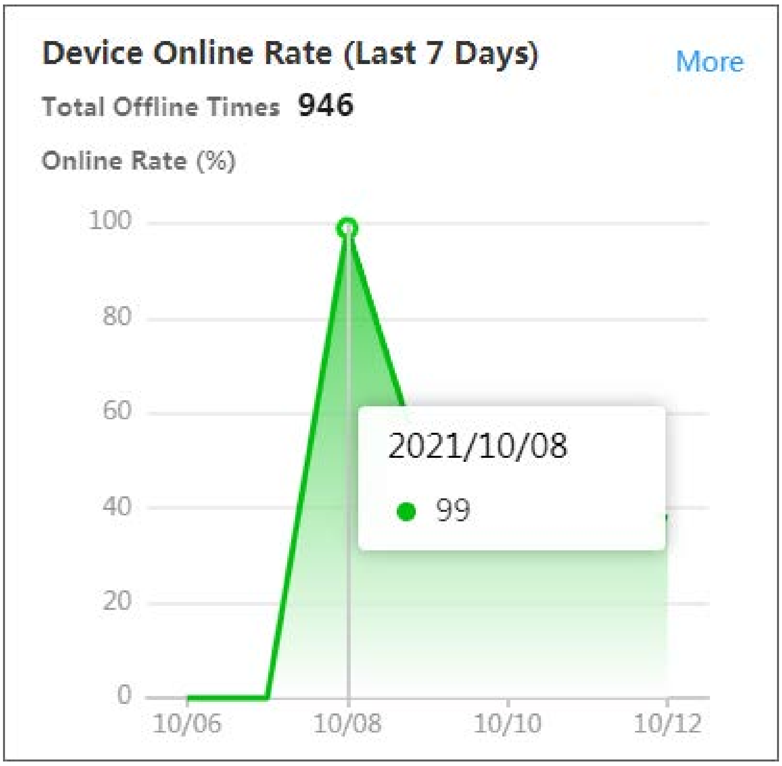


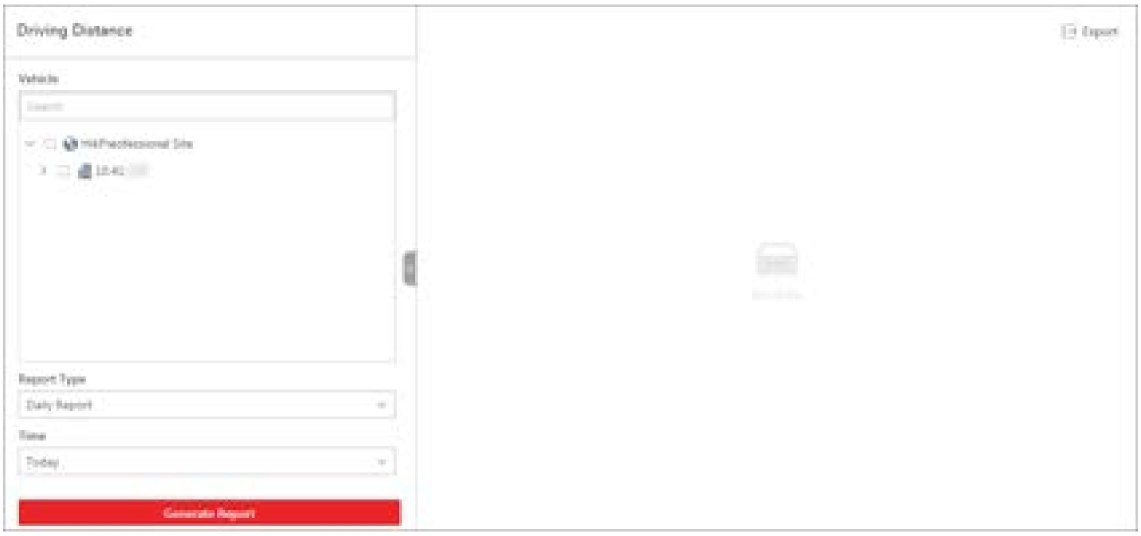
Figure 15-14 Example

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.

To know more information about how to generate reports related to mobile monitoring, see the following topics:

- ***Generate a GPS Information Report***
- ***Generate a Driving Distance Report***
- ***Generate a Driving Duration Report***
- ***Generate an Overspeed Report***
- ***Generate a Driving Event Report***
- ***Generate a Device Online Rate Report***



Report Type: Daily Report

Time: Today

Figure 15-15 Generate Report

15.7.2 Generate a GPS Information Report

You can generate a GPS information report showing the GPS-related 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. In the top left of the Web Client, select ▦ → **All Modules** → **Mobile Monitoring** → **Statistics and Reports** , and then select **GPS Information** from the navigation pane on the left to enter the GPS Information page.
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

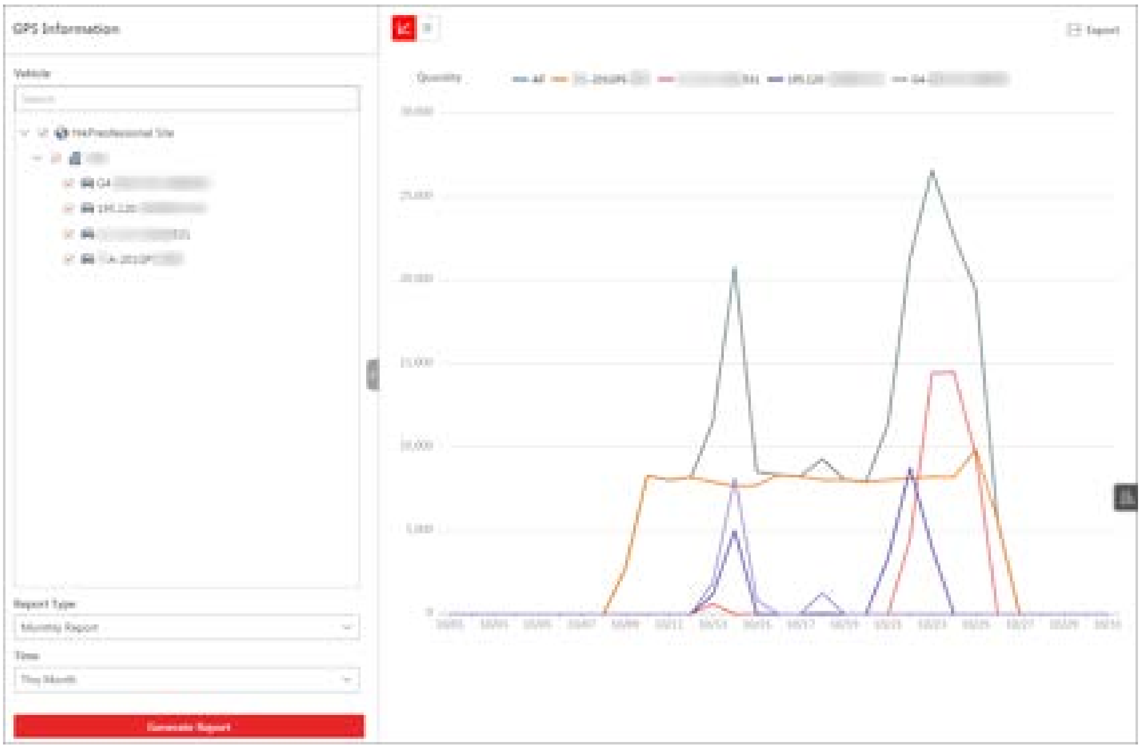
The data of the selected period will be shown in the report.

- 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**.

The data will be shown on the right side of the page.

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.



Report Type: Monthly Report

Time: This Month

Figure 15-16 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.
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 Vehicle, Time, Export By, and Export In. For the Export By parameter, you can set the content (brief or detailed) of the report to be exported. For Export In, you can set the format of the report.

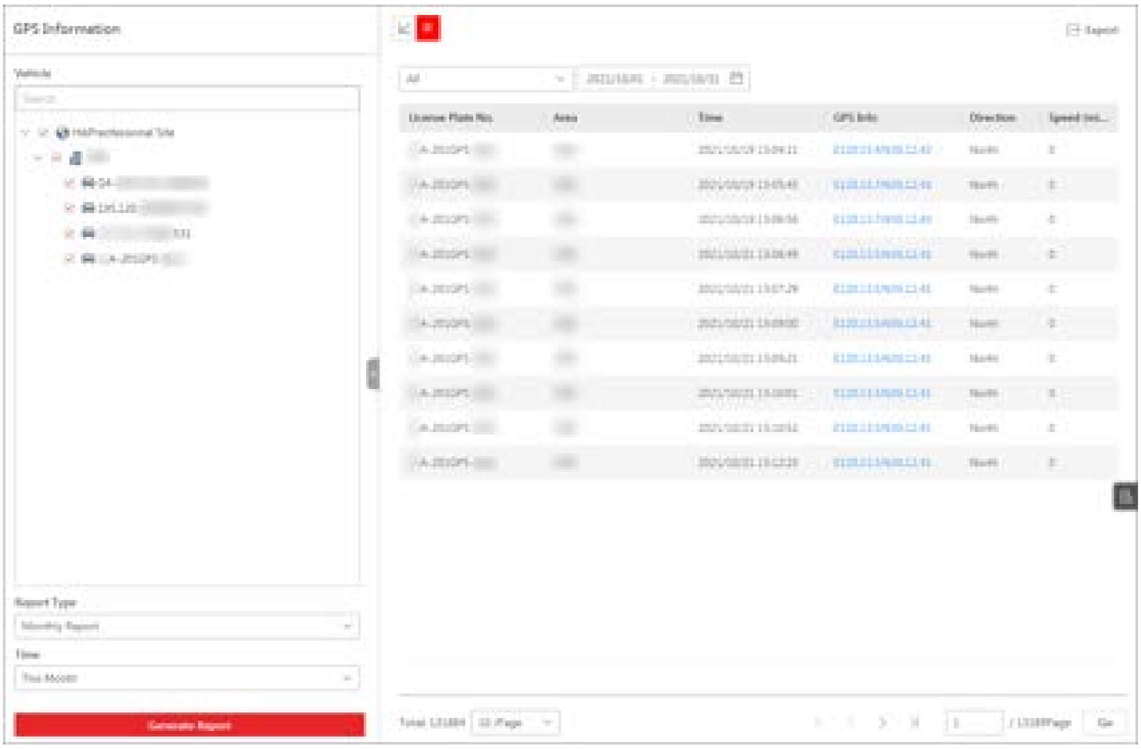


Figure 15-17 View Data in Table

15.7.3 Generate a Driving Distance Report

You can generate a driving distance report to view the driving distance of specific vehicles in a certain period.

Steps

1. In the top left of the Web Client, select ▦ → **All Modules** → **Mobile Monitoring** → **Statistics and Reports** , and then select **Driving Distance** from the navigation pane on the left to enter the Driving Distance page.
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 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**.

The data will be shown on the right side of the page.

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.

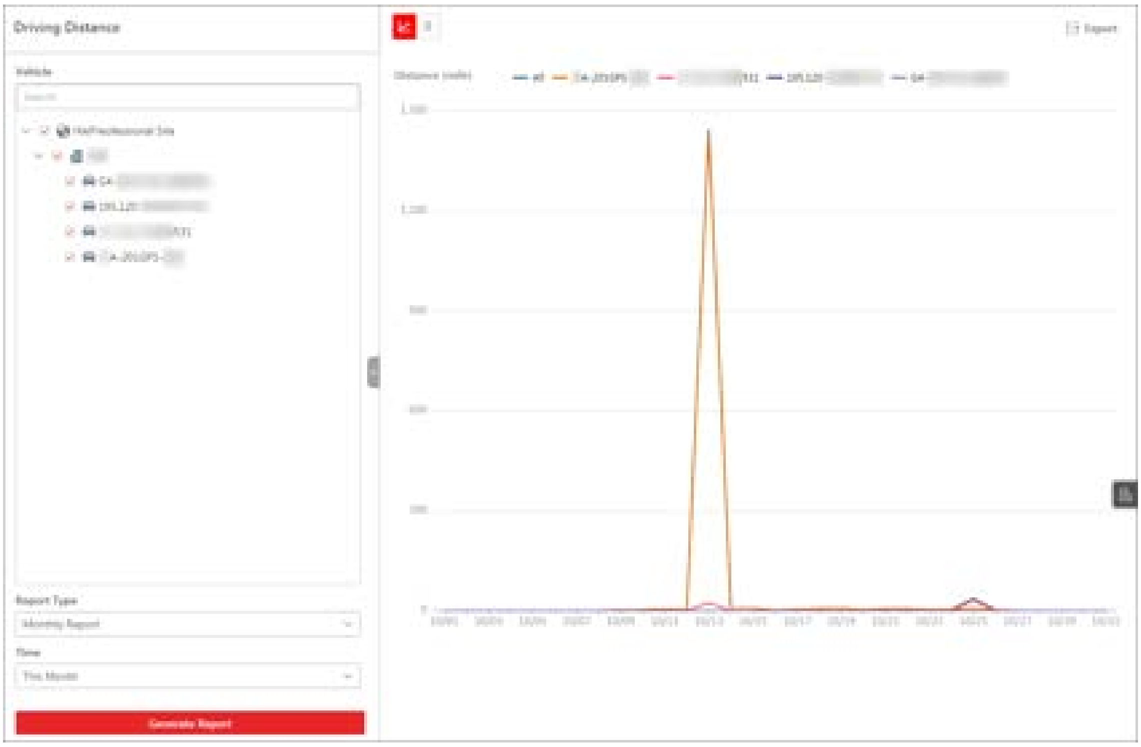


Figure 15-18 View Data in Line Chart

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 the corresponding data.
View Data in Table	Click ≡ to view the data in a table that shows the license plate number, area, time, and driving distance. 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 Vehicle, Time, and Export In. For Export In, you can set the format of the report.

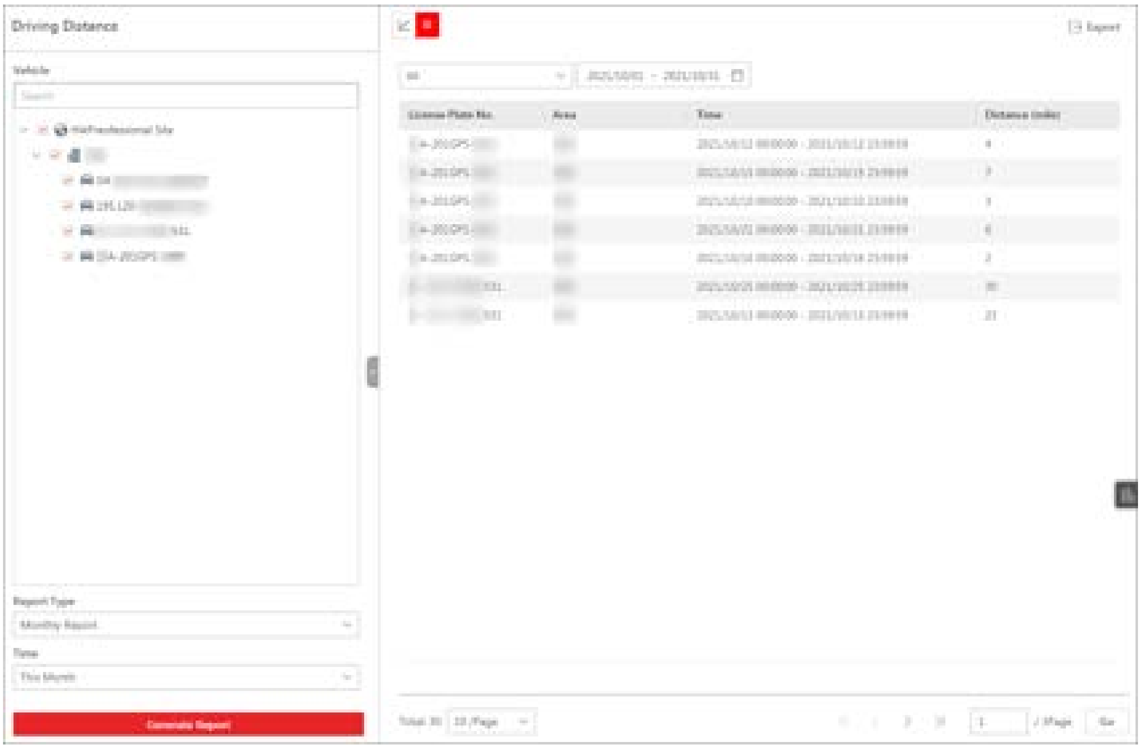


Figure 15-19 View Data in Table

15.7.4 Generate a Driving Duration Report

You can generate a driving duration report to view the driving duration of specific vehicles at a certain speed in a certain period.

Steps

1. In the top left of the Web Client, select ▦ → **All Modules** → **Mobile Monitoring** → **Statistics and Reports** , and then select **Driving Duration** from the navigation pane on the left to enter the Driving Duration page.
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.

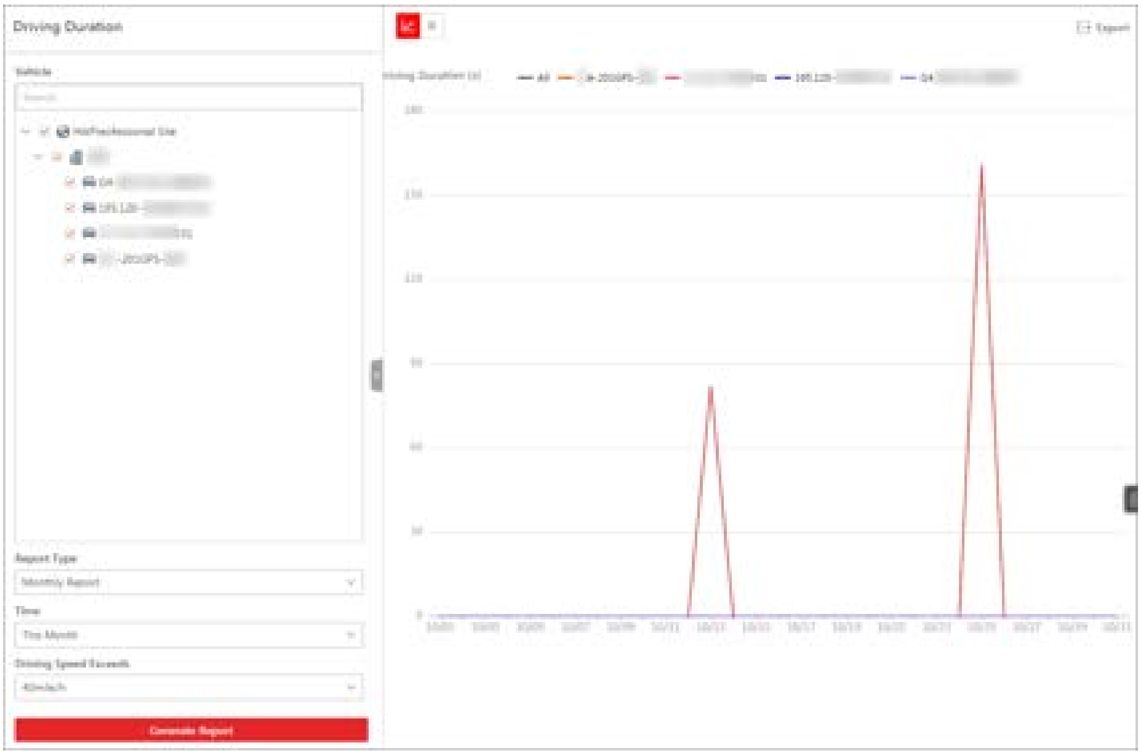
Driving Speed Exceeds

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**.

The data will be shown on the right side of the page.

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.



Driving Duration

Vehicle

Search

Report Type

Monthly Report

Time

This Month

Driving Speed Exceeds

40km/h

Generate Report

Figure 15-20 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 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, start time, end time, driving duration, maximum speed, minimum speed, start location, and end location. 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 Vehicle, Time, Export By, and Export In. For the **Export By** parameter, you can set the content (brief or detailed) of the report to be exported. For **Export In**, you can set the format of the report.

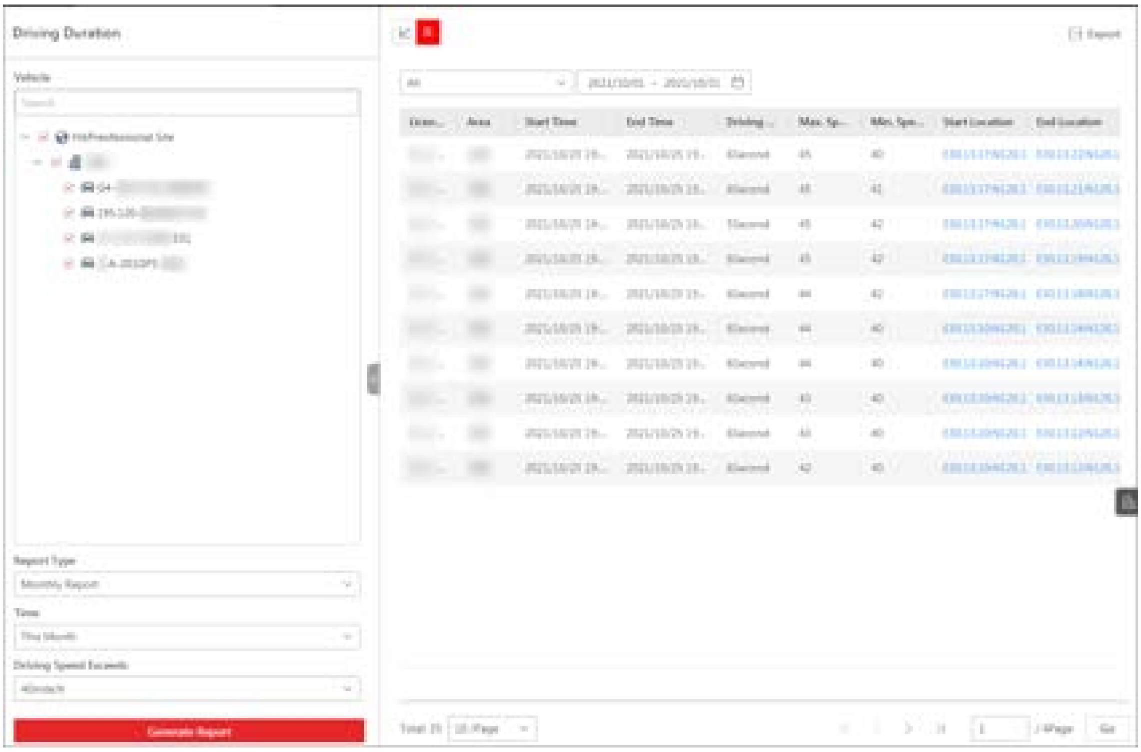


Figure 15-21 Switch Report to Table

15.7.5 Generate an Overspeed Report

You can generate an overspeed report to view the times that specific vehicles overspeed in a specific period.

Steps

Note

You can define the overspeed threshold for vehicles in a specific area. For details, see ***Add Vehicle to Area for Current Site*** .

1. In the top left of the Web Client, select ▦ → **All Modules** → **Mobile Monitoring** → **Statistics and Reports** , and then select **Overspeed** from the navigation pane on the left to enter the Overspeed page.
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**.

The data will be shown on the right side of the page.

By default, the data will be shown in a line chart, on which the Y-axis represents the overspeed times and the X-axis the time.

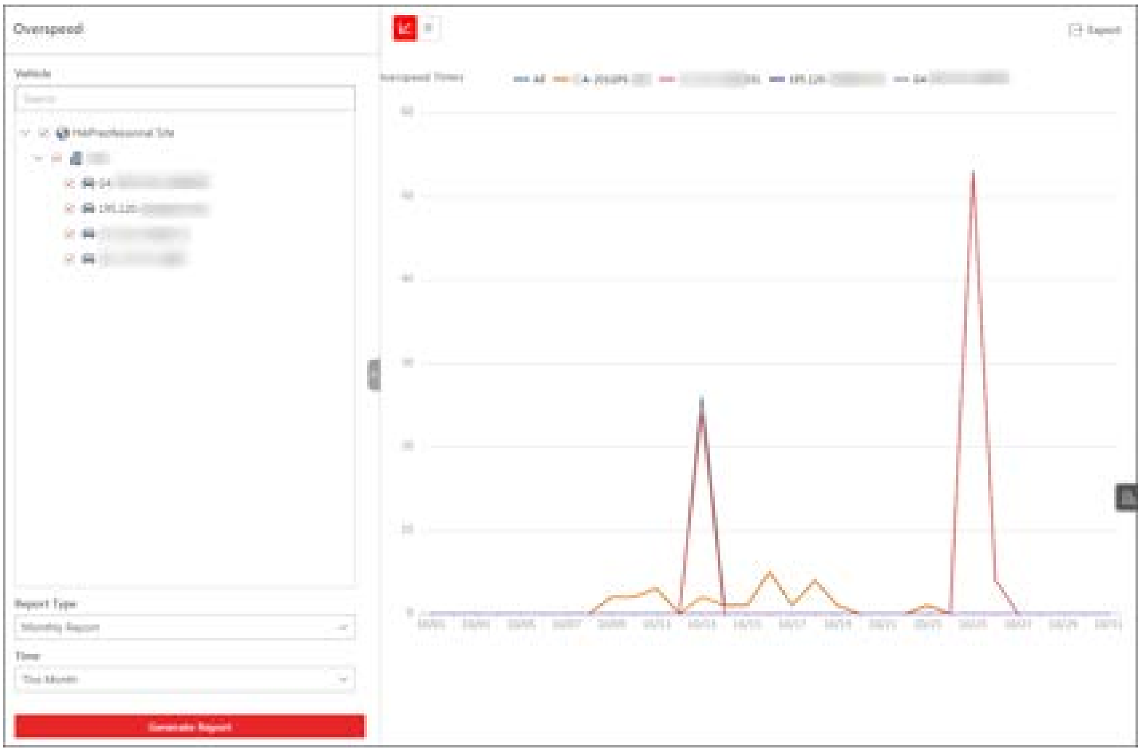


Figure 15-22 View Data in Line Chart

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.

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 Vehicle, Time, Export By, and Export In.

For the Export By parameter, you can set the content (brief or detailed) of the report to be exported.

For Export In, you can set the format of the report.

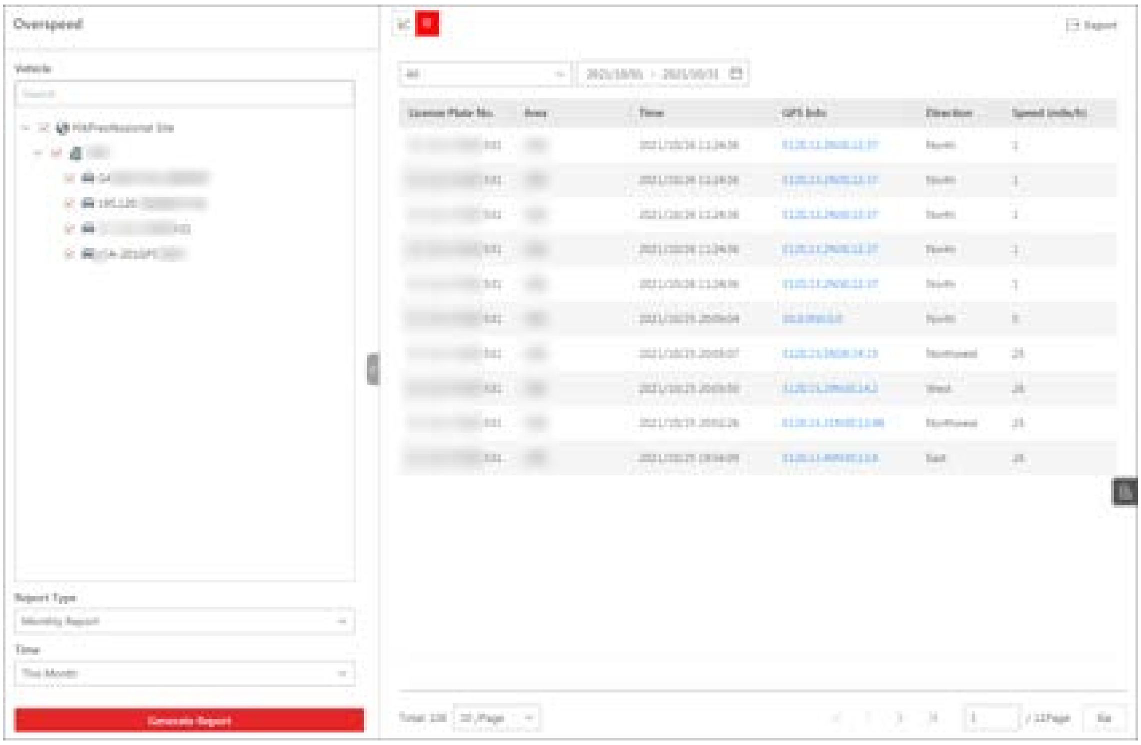


Figure 15-23 View Data in Table

15.7.6 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. In the top left of the Web Client, select ▦ → **All Modules** → **Mobile Monitoring** → **Statistics and Reports** , and then select **Driving Event** from the navigation pane on the left to enter the Driving Event page.
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

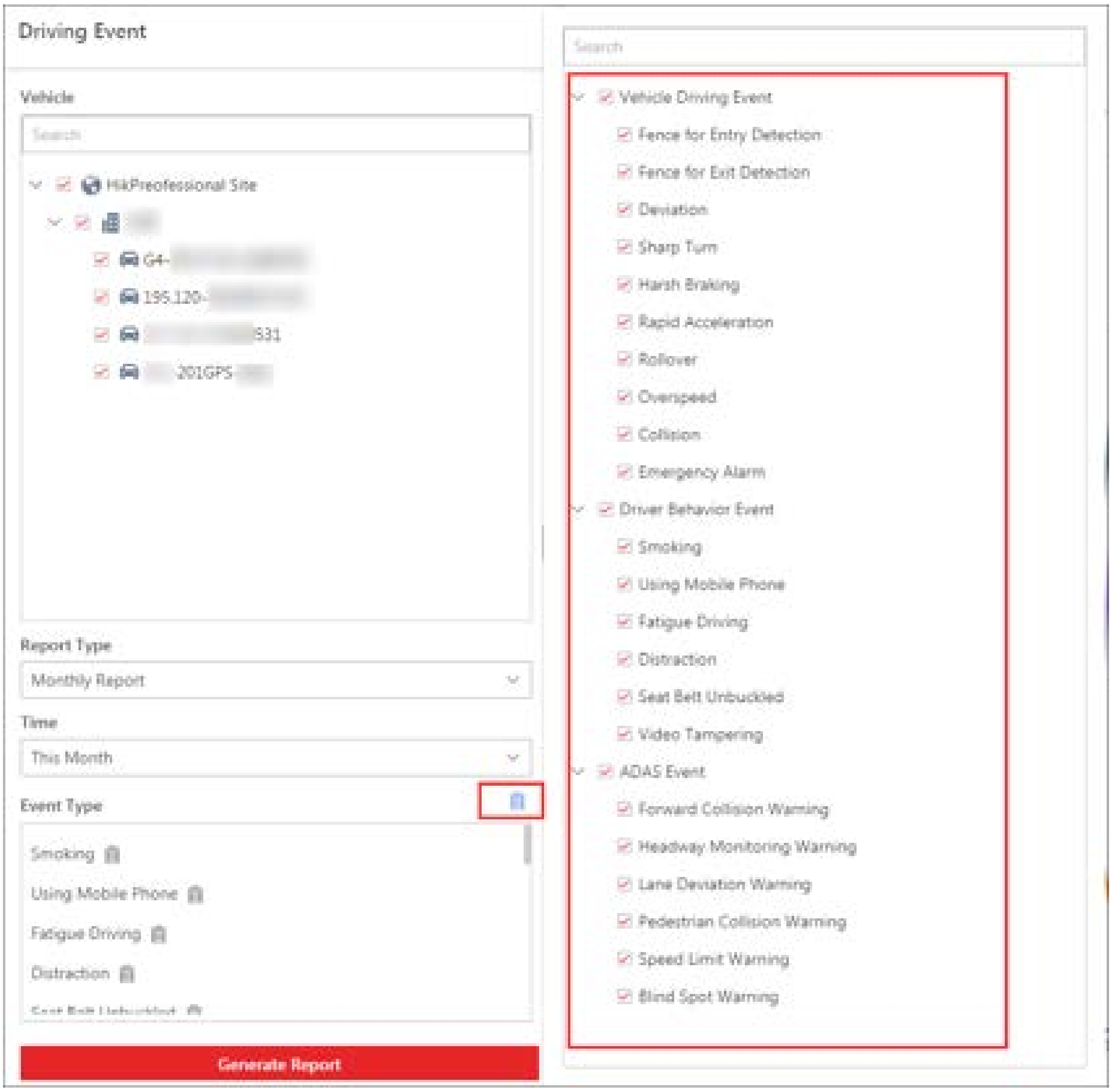
The data of the selected period will be shown in the report.

- 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.

Event Type

By default, all event types are selected.

You can click to select the events whose detection times will be calculated.



Driving Event

Vehicle

Search

☑ HikPreofessional Site

☑ [redacted]

☑ G4-[redacted]

☑ 195.120-[redacted]

☑ [redacted]531

☑ [redacted]201GPS-[redacted]

Report Type: Monthly Report

Time: This Month

Event Type

Smoking

Using Mobile Phone

Fatigue Driving

Distraction

Seat Belt Unbuckled

Generate Report

Search

- ☑ Vehicle Driving Event
  - ☑ Fence for Entry Detection
  - ☑ Fence for Exit Detection
  - ☑ Deviation
  - ☑ Sharp Turn
  - ☑ Harsh Braking
  - ☑ Rapid Acceleration
  - ☑ Rollover
  - ☑ Overspeed
  - ☑ Collision
  - ☑ Emergency Alarm
- ☑ Driver Behavior Event
  - ☑ Smoking
  - ☑ Using Mobile Phone
  - ☑ Fatigue Driving
  - ☑ Distraction
  - ☑ Seat Belt Unbuckled
  - ☑ Video Tampering
- ☑ ADAS Event
  - ☑ Forward Collision Warning
  - ☑ Headway Monitoring Warning
  - ☑ Lane Deviation Warning
  - ☑ Pedestrian Collision Warning
  - ☑ Speed Limit Warning
  - ☑ Blind Spot Warning

Figure 15-24 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.

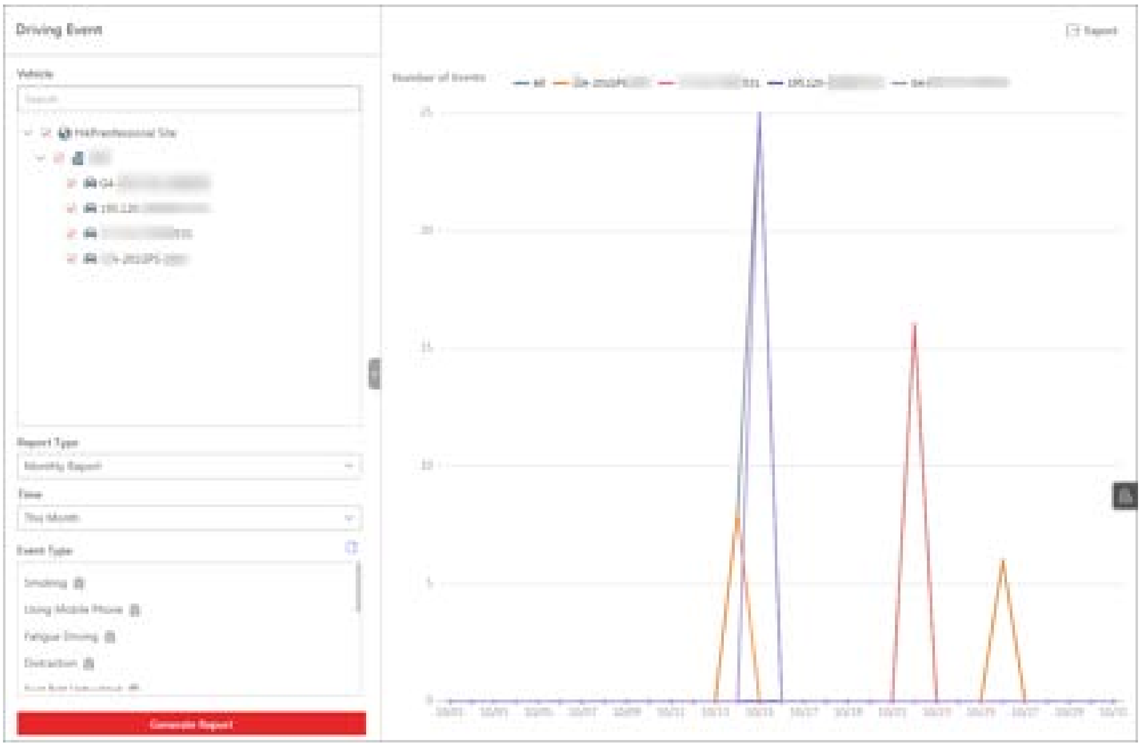


Figure 15-25 View Data in Line Chart

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 including Vehicle, Time, Event Type, and Export In. For Export In, you can set the format of the report.

15.7.7 Generate a Passenger Counting Report

You can generate a passenger counting report to view the number of passengers who got on or (and) off specific vehicles in a specific period.

Steps

1. In the top left of the Client, select ▦ → **All Modules** → **Mobile Monitoring** → **Statistics and Reports** , and then select **Passenger Counting** from the navigation pane on the left to enter the Passenger Counting page.
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 passengers and the X-axis the time.

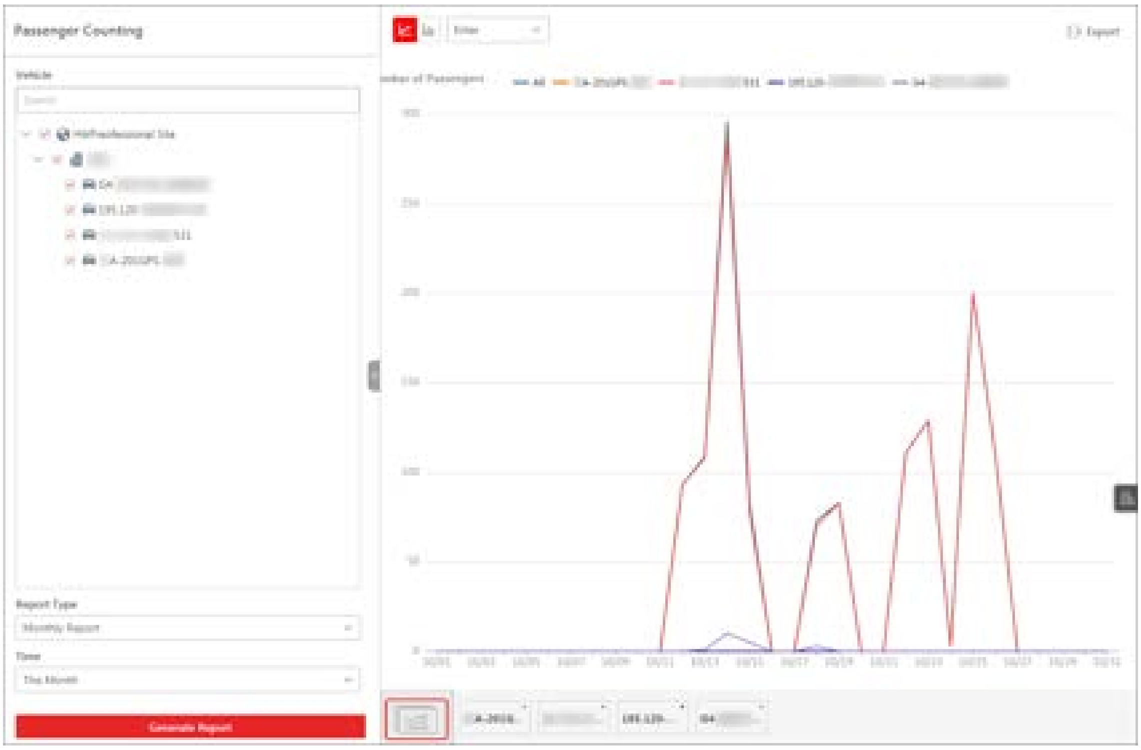


Figure 15-26 View Data in Line Chart

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 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.

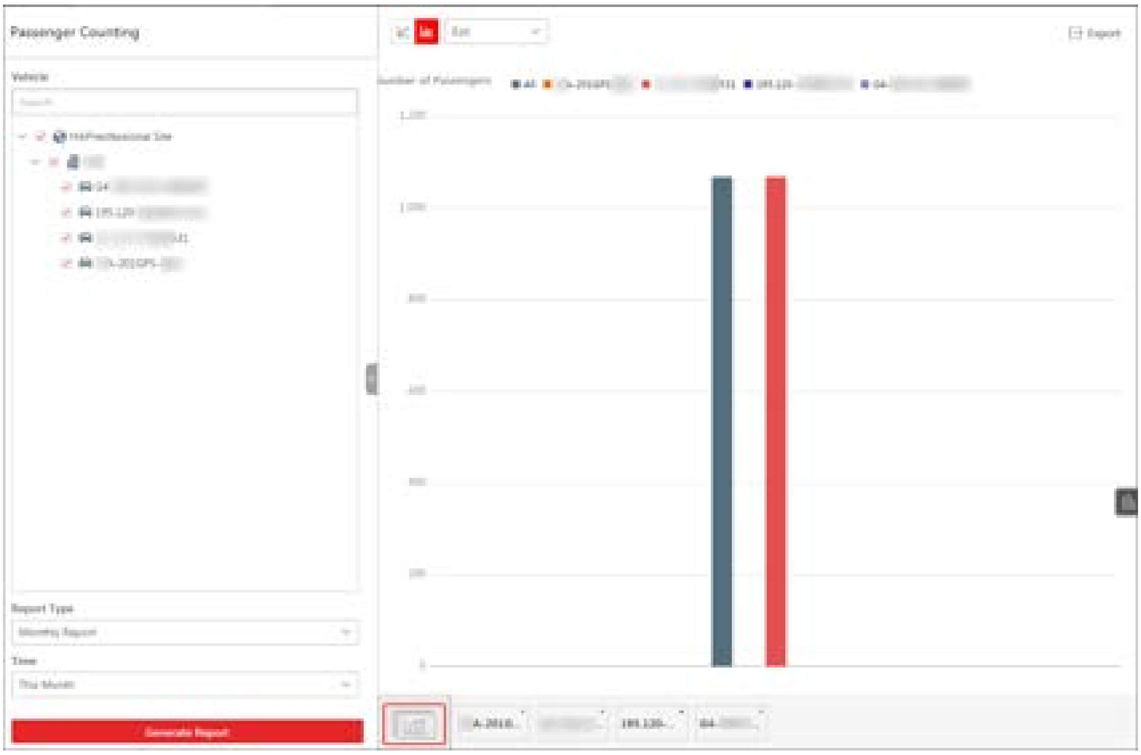
For example, if you select **Enter**, the report only shows the number of passengers who get on the selected vehicles in the selected period.

Filter by Vehicle
Click a vehicle at the bottom of the chart to view the number of passengers who got on and (or) off the vehicle in the selected period.

Export Report
Click **Export** to open the Export pane, and then set parameters including Vehicle, Time, and Export In.

For Time, you can select **By Hour**, **By Day**, or **By Month** to let the export report show the number of passengers by hour, by day, or by month respectively.

For Export In, you can set the format of the report.



Report Type: Monthly Report

Time: This Month

Figure 15-27 View Data in Histogram Chart

15.7.8 Generate a Device Online Rate Report

You can generate a report to view the online rate of the mobile devices mounted on the selected vehicles in a specific period.

Steps

1. In the top left of the Web Client, select ▦ → **All Modules** → **Mobile Monitoring** → **Statistics and Reports** , and then select **Device Online Rate** from the navigation pane on the left to enter the Device Online Rate page.
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.

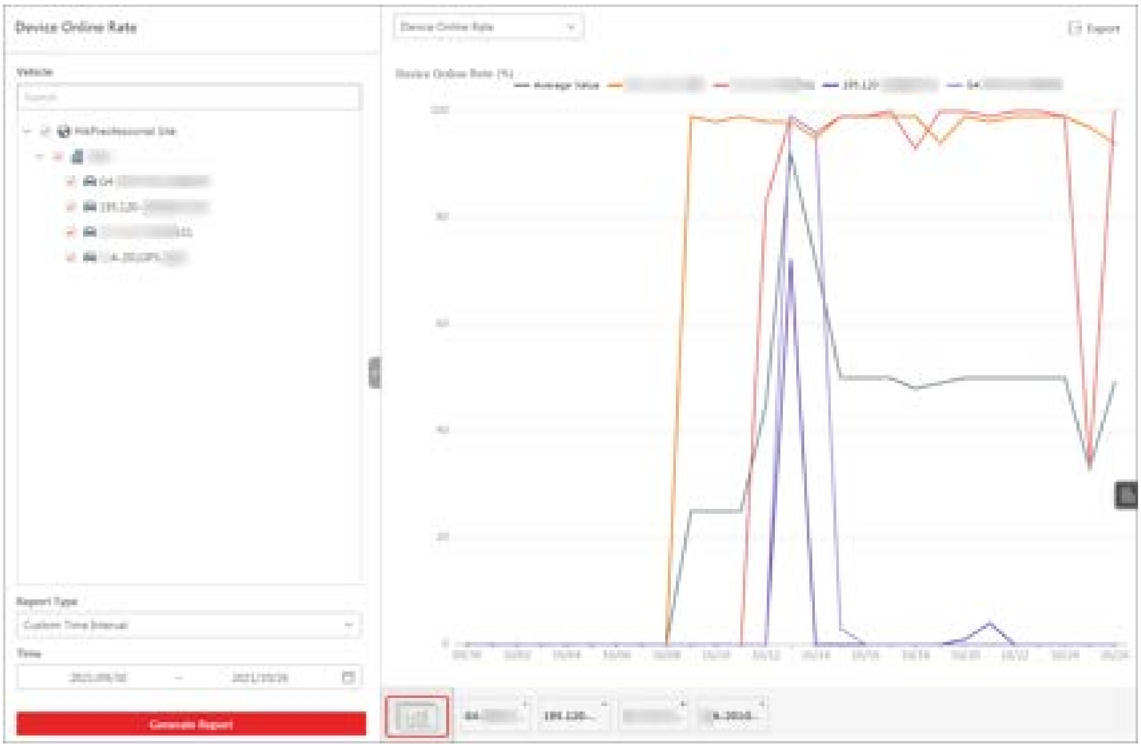


Figure 15-28 View Data in Line Chart

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 the corresponding data.

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 Vehicle, Time, and Export In.

For Export In, you can set the format of the report.

Chapter 16 Access and Elevator Control Management

The system supports access control and elevator control functions. Access control is a security technique that can be used to regulate who can get access to the specified doors and elevator control can be used to regulate who can get access to the specified floors by taking the elevator.

On the Web Client, the administrator can add access control devices, elevator control devices, and video intercom devices to the system, group resources (such as doors and elevators) into different areas, and define access permissions by creating an access level to group the doors/floors 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 and floors in the access level with their credentials during the authorized time period.

16.1 Flow Chart

The following flow chart shows the process of the configurations and operations of access control and elevator control. For access control, you can also enter the **Access Control Overview** module on the Home page of the Web Client to go through the basic configurations.

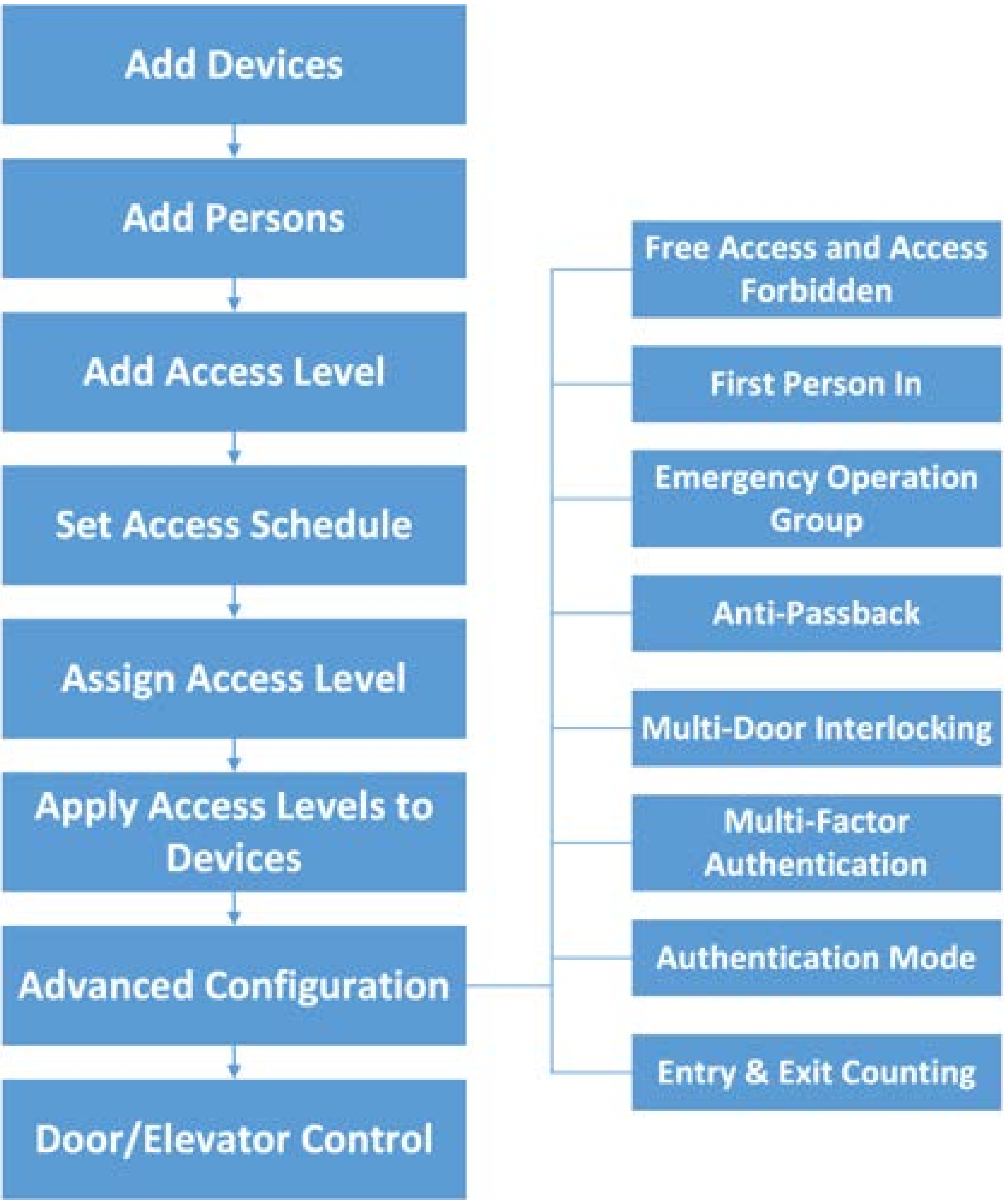


Figure 16-1 Flow Chart of Access Control and Elevator Control

- **Add Device**: You need to add the access control devices, video intercom devices, and elevator control devices to the system. The system provides multiple methods for adding them. For details, refer to ***Manage Access Control Device*** , ***Manage Video Intercom Device*** , and ***Manage Elevator Control Device*** .
- **Add Persons**: Add person information and set person's credentials (such as PIN, issuing a card, fingerprint, etc.). For details, refer to ***Person Management*** .

- **Add Access Level**: An access level is a group of doors and floors. After assigning access level, the assigned objects can get access to these doors and floors during the authorized time period. For details, refer to ***Manage Access Level*** .
- **Set Access Schedule**: The access schedule defines when the person can access the access point with credentials. For details, refer to ***Set Access Schedule Template*** .
- **Assign Access Level**: 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 person group. For details, refer to ***Assign Access Level*** .
- **Apply Access Levels to Device**: After setting the linkage between the persons and the access level, you need to apply the person's access level settings to the access control device or elevator control device of the doors/floors linked to the access level to take effect. After that, the persons can access these doors/floors during the authorized time period defined by the related access level. For details, refer to ***Apply Persons' Access Levels to Device*** .
- **Advanced Configuration**: The system provides some advanced configurations such as free access and access forbidden rule, first person in rule, emergency operation group, anti-passback, multi-door interlocking, multi-factor authentication, authentication mode, and entry & exit counting. For details about these configurations, refer to ***Configure Free Access and Access Forbidden Rules*** , ***Configure First Person In Rule*** , ***Add Emergency Operation Group*** , ***Configure Area Anti-Passback Rules*** , ***Configure Multi-Door Interlocking*** , ***Configure Multi-Factor Authentication Rule*** , ***Configure Authentication Mode*** , and ***Add Entry and Exit Counting Group*** .
- **Door/Elevator Control**: After the above configurations on the Web Client, you can control the door/floor's status during live view, view real-time access events, search for history access records, etc. See ***Door and Elevator Control*** for details.

16.2 Manage Access Level

In access control, access level is a group of doors and floors. Assigning access level to persons, person groups, or access groups can define the access permission that which persons can get access to which doors and floors during the authorized time period.

16.2.1 Add Access Level

To define access permission, you need to add an access level to group the access points (doors and floors).

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **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(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.

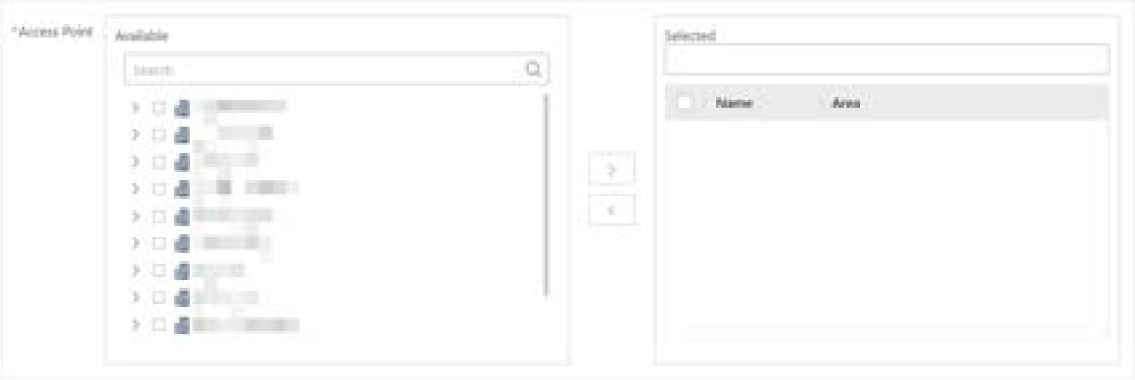


Figure 16-2 Select Access Points

7. 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*** .

8. Click **Add** to add the access level and return to the access level management page.
9. **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 ***Assign Access Level*** .

16.2.2 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, person group, 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. In the top left corner of Home page, select 🟥 → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Access Level** on the left.
3. Click on the access level that you want to assign to persons.

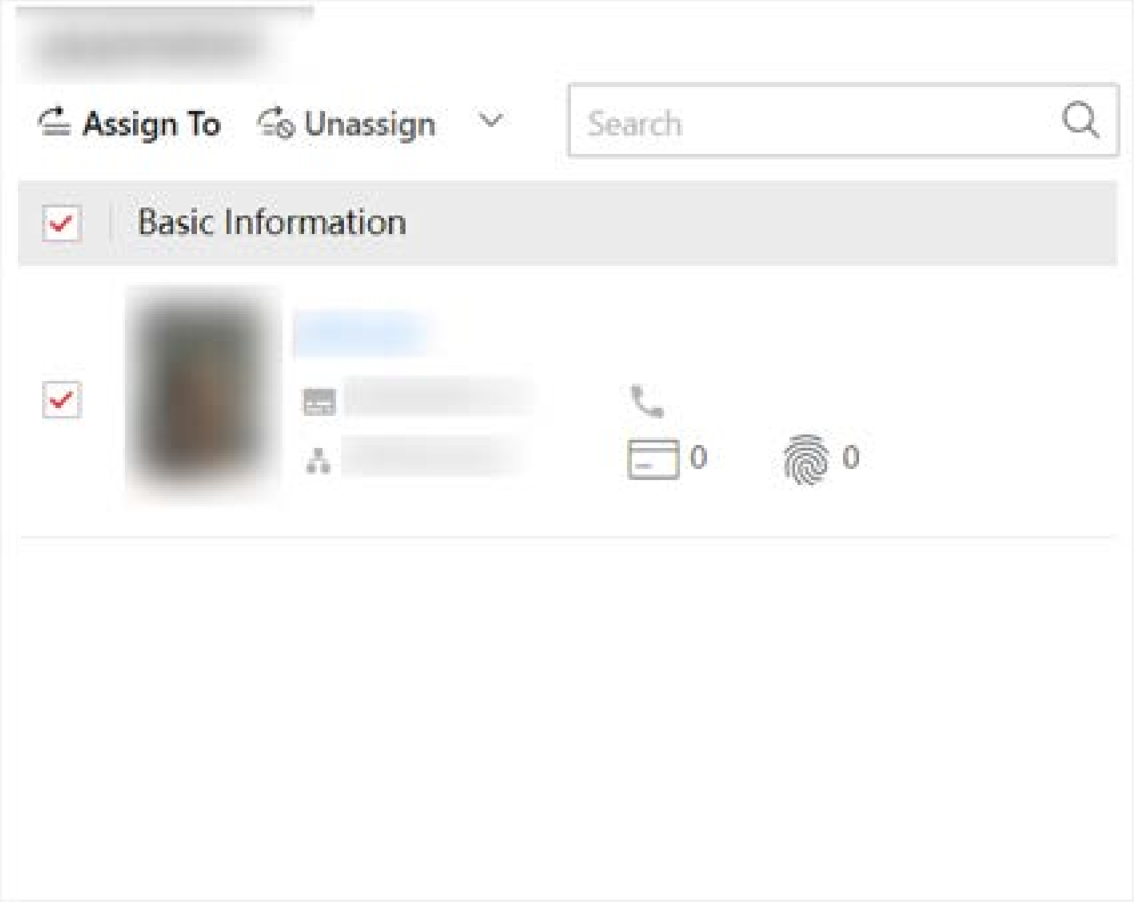


Figure 16-3 Assignee Panel

4. On the assignee panel, click **Assign To** to show person list.
5. Select the persons whom you want to assign the access level to and click **Add**.
6. Do one of the following to apply access level settings to devices.

- In the pop-up window, click **Apply Now** to apply the settings immediately.
- In the pop-up window, click **Apply Later**. When ready, click to apply the settings. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .

7. **Optional:** To unassign a person from the access level, select the person and click **Unassign**. To unassign all, click → **Unassign All** .

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. In the top left corner of Home page, select → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Person** on the left.
3. In the person group list, click a person group.
4. In the person information panel on the right, select the persons to whom you want to assign access levels.

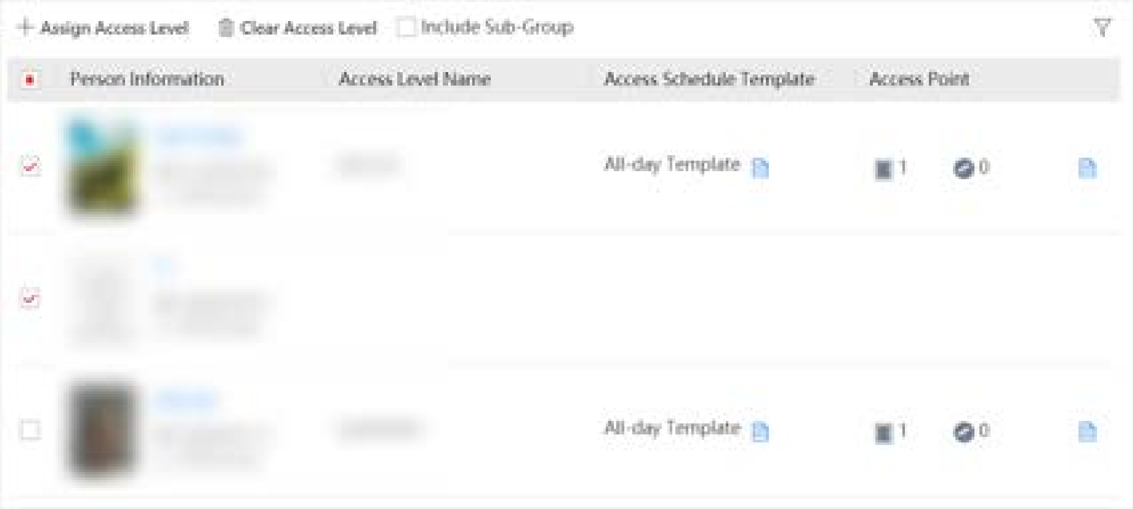


Figure 16-4 Person Information Panel

Note

You can click on person's name to view the details about the person.

5. Click **Assign Access Level**.
6. In the Assign Access Level panel, select the access levels that you want to assign to the selected persons.
7. Click **Add**.
8. Do one of the following to apply access level settings to devices.
   - In the pop-up window, click **Apply Now** to apply the settings immediately.
   - In the pop-up window, click **Apply Later**. When ready, click to apply the settings. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .
9. **Optional:** To clear a person's access levels, select the person and click **Unassign**. For details, refer to ***Clear Persons' Access Levels*** .

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 Group

You can assign access levels to person groups, so that the persons in the person group can have the access to the access points in the access levels.

Before You Start

- Make sure you have added person groups and 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 person groups.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Person Group** on the left.
3. Do one of the following to assign access levels to person groups.
   - Assign access levels to each person group one by one.
     a. In the person group list, click on a person group.
     b. In the assigned access level panel on the right, click **Assign Access Level**.
     c. In the Assign Access Level panel, select the access levels you want to assign to the selected person group.
     d. Click **Add**.
   - Assign access levels to multiple person groups at a time.
     a. Click .
     b. In the person group list, select the person groups where you want to assign access levels.

> **Note**
>
> Sub-groups are excluded from selection by default. To include all sub-groups of each person group, check **Select Sub-Groups**.

c. In access level list, select the access levels you want to assign to the person groups.
d. Click **Save**.

> **Note**
>
> After assigning access levels to a person group, you can still modify the access levels for each person in the group, and it will not affect the settings for the person group. For details, refer to ***Assign by Person*** .

4. Do one of the following to apply access level settings to devices.
   - In the pop-up window, click **Apply Now** to apply the settings immediately.
   - In the pop-up window, click **Apply Later**. When ready, click to apply the settings. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .
5. **Optional:** To unassign an access level from the person group, select the access level and click **Unassign**. To unassign all access levels, click ⌄ → **Unassign All** .

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 permission (In the specified time period, they have the permission to access the specified access points and floors). 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. One or multiple access levels can be assigned 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 platform. 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. In the upper-left corner of the Home page, select ⊞ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Access Group** on the left.
3. Perform one of the following operations to enter the Add Access Group page.

- Click at the top of the access group list to enter the Manage Access Group page, and then click **Add** to enter the Add Access Group page.
- 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.

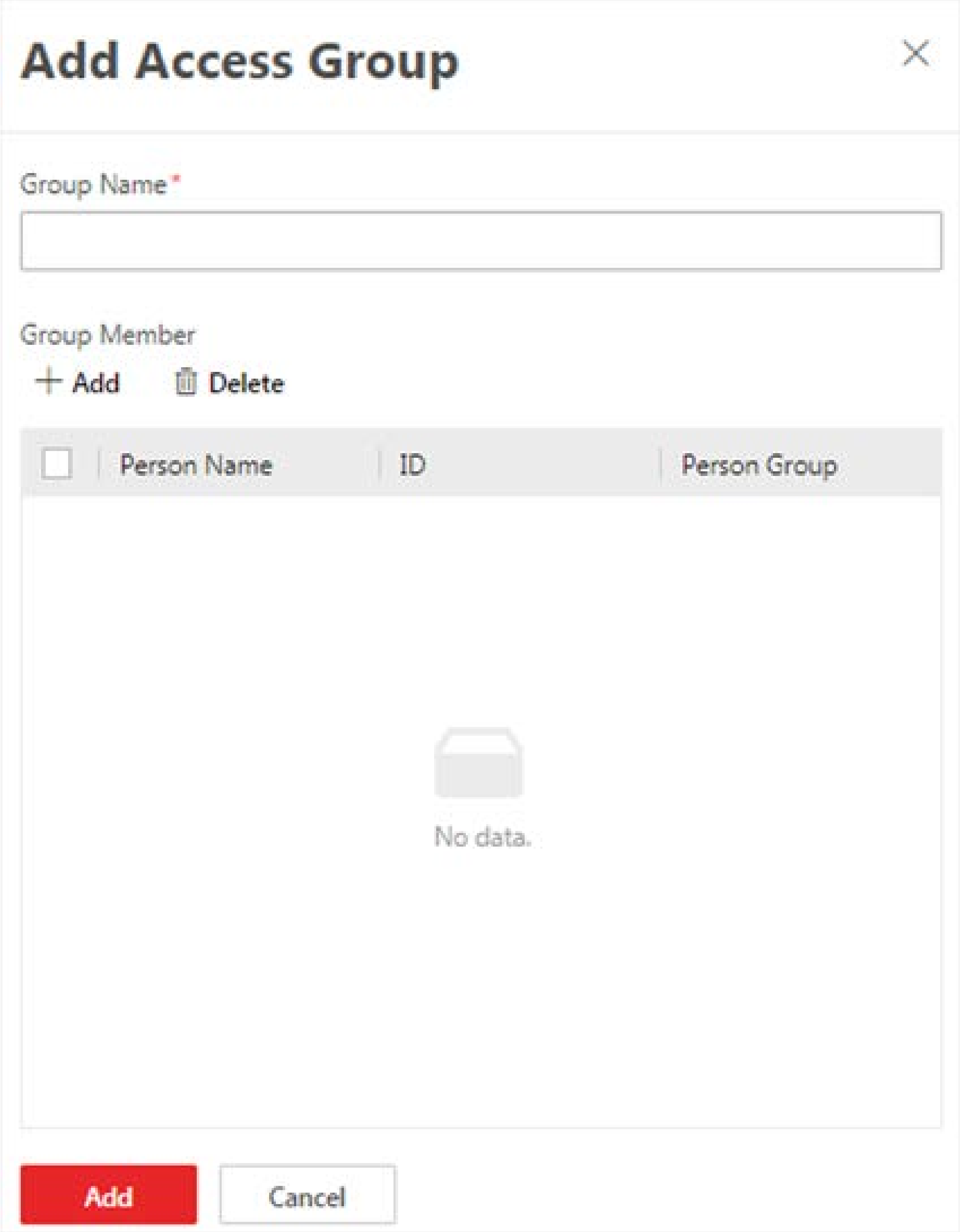


Figure 16-5 Add Access Group Page

4. In the **Group Name** field, enter the name of the access group.
5. In the **Group Member** area, click **Add** to open the person list, select the person(s) to be added to the access group.

6. Click **Add** to add the selected person(s) to the access group.
7. After configuration, click **Add** at the bottom.
8. Select an access group to assign access levels to.
9. Click **Assign Access Level** on the right.
10. In the Add Access Level page, select the access level(s) to be assigned to.
11. Click **Add**.
12. Perform one of the following operations to apply access level settings to devices.
    - In the pop-up window, click **Apply Now** to apply the settings immediately.
    - In the pop-up window, click **Apply Later**. When ready, click to apply the settings. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .
13. **Optional:** Unassign access level(s) from the access group.
    - In the assigned access level list, select the access level(s) and click **Unassign** to unassign the access level(s) from the access group.
    - In the assigned access level list, click → **Unassign All** to unassign all access levels from the access group.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

16.2.3 Apply Persons' Access Levels to Device

After setting or modifying the linkage between persons and access levels, you need to apply the access level settings to the access control devices or elevator control devices to take effect. After that, the persons can access these doors/floors during the authorized time period defined by the related access level.

Manually Apply Access Level Settings to Device

After setting access levels and assigning access levels to persons, person groups, or access groups, you need to apply the relations between persons and access points to the devices.

Before You Start

Make sure you have assigned access levels to persons in the system. For details, refer to ***Assign Access Level*** .

Steps

1. In the top left corner of Home page, select → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Access Level**, **Assign by Person**, **Assign by Person Group**, or **Assign by Access Group** on the left.
3. Click .
4. In the Apply Access Level Settings panel, select the persons to apply the access level settings.
    - To apply the access level settings of all persons, select **All Persons**.

- To apply the access level settings of specific persons, select **Specified Persons**, click , select the persons, and click **Add**.

5. Select the access points to apply the persons' access level settings.
   - To apply the access level settings of all access points, switch off **Specified Access Point**.
   - To apply the access level settings of specific access points, switch on **Specified Access Point** and select the access points.
6. Apply access level settings to devices.
   - To clear all persons' access level configurations on the devices first and then apply the configurations in the system to the devices, check **Apply (Initial)** and click **Apply**.

     Note

     - Only available when you select **All Persons** previously.
     - During the initialization process, the devices will be offline, and persons cannot access these access points.
   - To apply changed (newly added, edited, deleted) access level settings to the devices, uncheck **Apply (Initial)** and click **Apply**.
7. **Optional:** If persons' access level settings (such as linked access levels, person credentials, etc.) are changed or the applying process failed, will appear next to , indicating some access level settings are pending to be applied to the devices. You can hover the cursor over to view the details.

   Note

   For troubleshooting the applying process, refer to ***Access Control Test*** .

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 ***Assign Access Level*** .

Steps

1. In the top left corner of Home page, click → **All Modules** → **Access Control** → **Basic Settings** .
2. Click **Apply to Device (Scheduled)** on the left.
3. Switch on **Apply to Device (Scheduled)**.
4. 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 **Auto-Apply** drop-down list.

5. Click **Save**.

16.2.4 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.

In the top left corner of Home page, click 🟥 → **All Modules** → **Access Control** → **Access Level** .

Click **Assign by Person** on the left.

Select a person group to show all persons in the group. You can filter the target persons by setting search conditions.

Select the target persons and click **Unassign**.

Note

After clearing, the previous access level settings of the persons cannot be restored. You need to re-assign access levels for them again when needed.

After clearing the access level settings of the selected persons, these persons will be removed from the related access groups. You need to apply the access level settings of these persons to the devices to take effect. You can click **Apply Now** in the pop-up window to apply the settings immediately. Or click **Apply Later**. When ready, click . For details, refer to ***Manually Apply Access Level Settings to Device*** for details. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .

After applying to the devices, the access level settings of the persons will be deleted on the devices.

16.2.5 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 🟥 → **All Modules** → **Access Control** → **Basic Settings** .
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.
   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*** .

16.2.6 Enable Authentication via Password

Authentication via password allows you to authenticate only via your password. After this function is enabled, all the passwords in the platform should be different from each other. You can update the password manually or automatically.

Steps

1. Click ⊞ → **All Modules** → **Access Control** → **Basic Settings** .
2. Click **General** on the left to enter the General page.
3. Switch on **Authenticate via Password**.
4. Select **Manual** or **Auto** as the PIN code update mode.

   Manual Mode

You need to export users whose passwords are duplicated or not configured from the Person module, and then notify these users to update the passwords by themselves. A password should consist of 4 to 8 characters.

Auto Mode

The platform will change the duplicate password to a unique one or customize a unique password for each user whose password is not configured, and then notify these users.

5. Click **Save**.

16.3 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, elevator control, and video intercom) are set correctly and completely and whether the devices are running properly.

In the top left corner of Home page, click ▦ → **All Modules** → **General** → **Access Control** → **Troubleshooting** .

Check Credential Status

Select **Credential Status** tab to view the status of the added credentials.

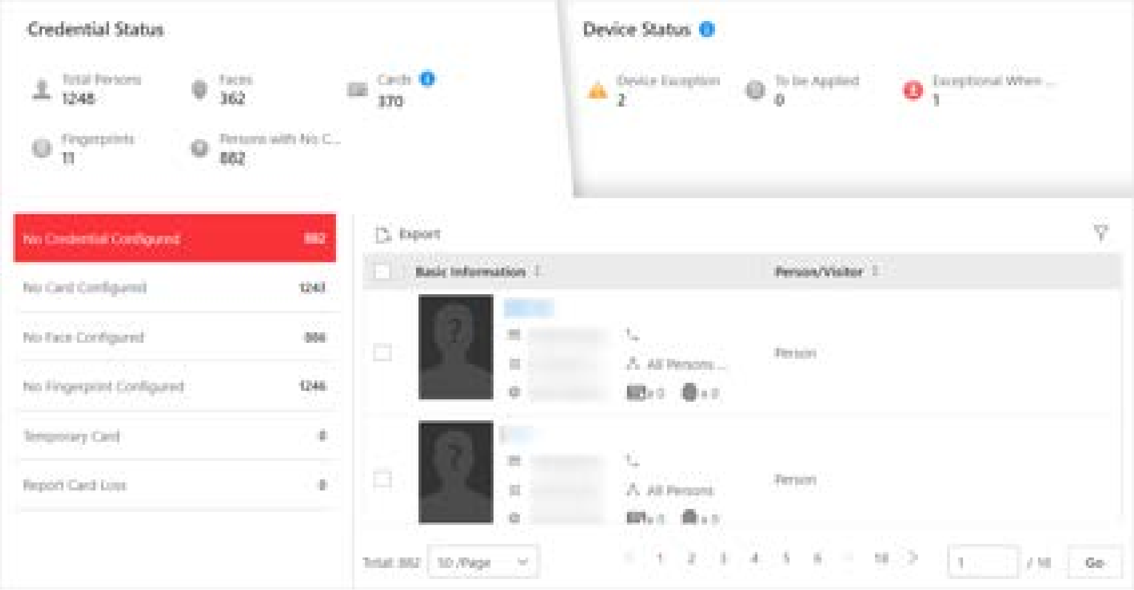


Figure 16-6 Credential Status

There are 6 types of exceptions on credential settings in the system. The number next to each exception type indicates the number of persons and visitors whose credential settings are exceptional.

Click each exception type to view the information about the persons and visitors with exceptions. You can click person's name to edit the credentials if necessary.

Check Device Status

Select **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, failed to apply, and persons to be applied to the devices.

Note

Only the status of the devices which have been configured with access levels are shown.

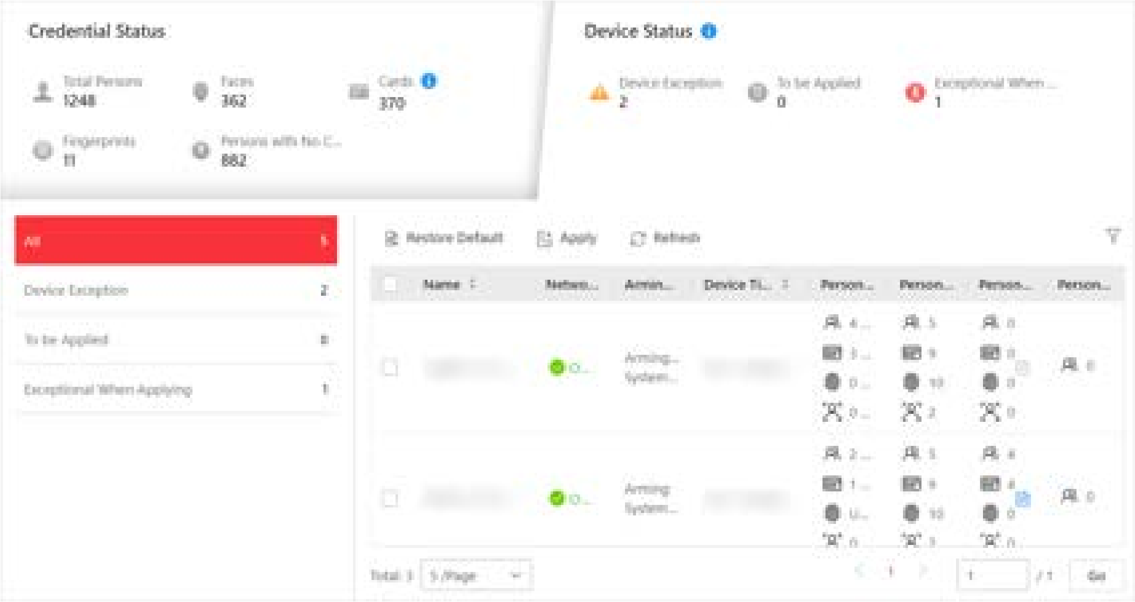


Figure 16-7 Device Status

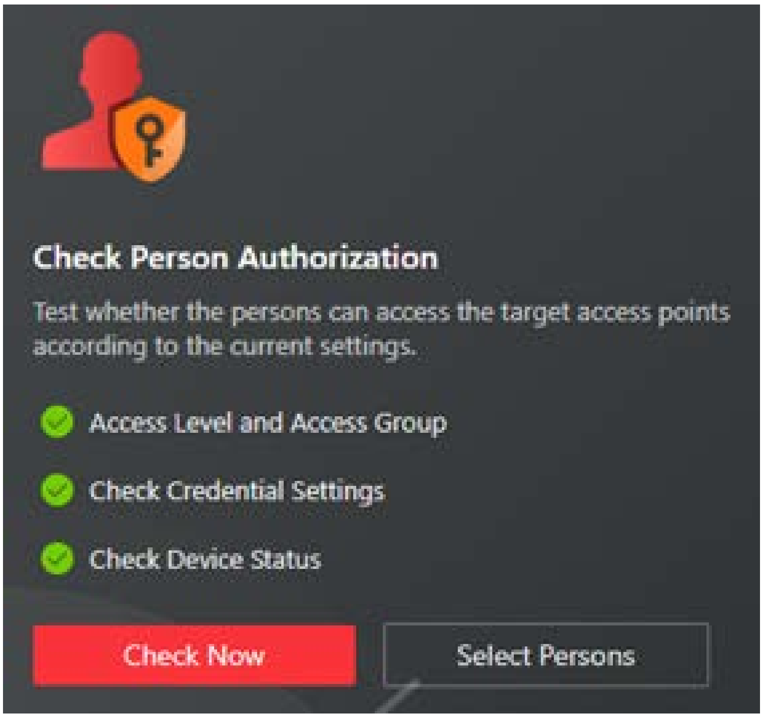
Click each exception type to view the information about the persons and visitors with exceptions. You can select the devices and click the following buttons to solve device issues.

Restore Default	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/Visitors

You can check the authorization settings (such as access levels and access group settings, credential settings, and applying status) of specific persons or visitors 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.



Check Person Authorization

Test whether the persons can access the target access points according to the current settings.

- ✓ Access Level and Access Group
- ✓ Check Credential Settings
- ✓ Check Device Status

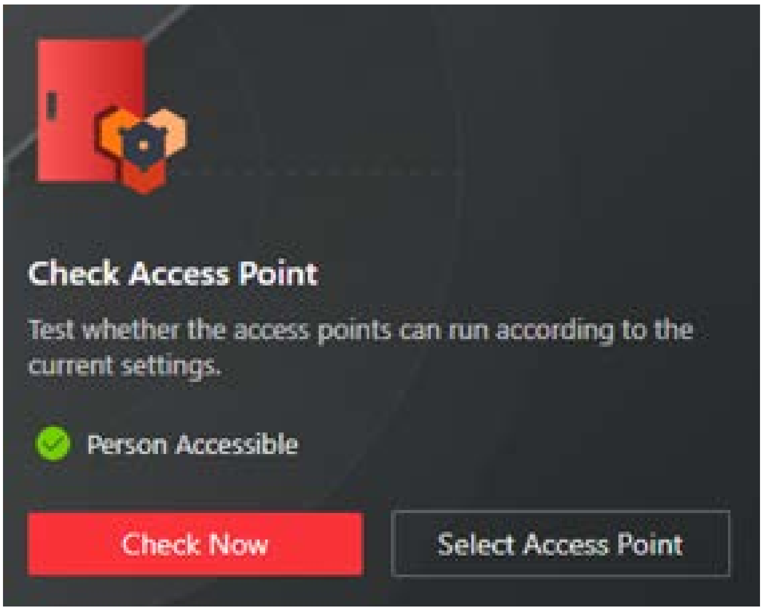
Figure 16-8 Check Authorization Settings

In the **Check Person Authorization** section, select the item(s) of information you want to check.
Click **Check Now** to test the authorization settings of all existing persons and visitors.
Or click **Select Persons** to select the persons or visitors you want to test and then click **Check Now** to test the authorization settings of the selected persons or visitors.

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.



Check Access Point

Test whether the access points can run according to the current settings.

✓ Person Accessible

Figure 16-9 Check Access Point Settings

In the **Check Access Point** section, select the item(s) of information 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.

16.4 Advanced Functions

16.4.1 Configure Free Access and Access Forbidden Rules

You may need to set doors and floors accessible or inaccessible during certain periods. To perform this function, you need to configure free access and access forbidden rule for certain doors or floors.

Steps

Note

This function should be supported by the device.

1. In the top left corner of Home page, select → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Free Access and Access Forbidden** on the left.

3. Click **Add** to enter the Add Free Access and Access Forbidden Rule page.
4. Enter the rule name.
5. Select an access point from the following area list.
6. Select free access schedule or access forbidden schedule.

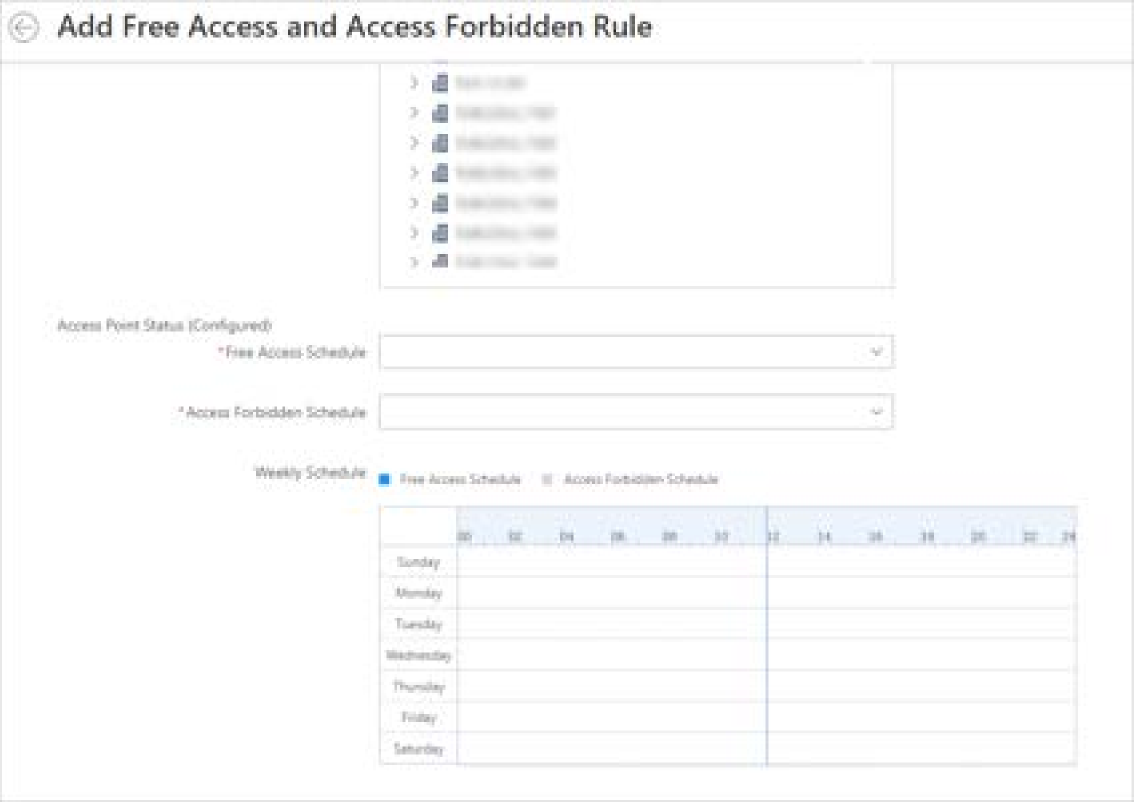


Figure 16-10 Add Free Access and Access Forbidden Rule Page

Free Access Schedule

During free access period, all persons can access the selected doors and floors without credentials required.

Access Forbidden Schedule

During access forbidden period, no persons can access the selected doors or floors even if he/she has the authorized credentials, except the super users.

Note

- You can click **Add New** to add a custom access schedule or holiday schedule. See ***Set Access Schedule Template*** for details.

7. Click **Add**.

   The system will automatically apply the schedule(s) to devices.

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

   View Schedule Details Click to show the schedule details.

Copy Schedule to Other Access Point
Click a rule name to enter the rule page. Click **Copy to** on the top right to copy the schedule to other access points.

16.4.2 Configure First Person In Rule

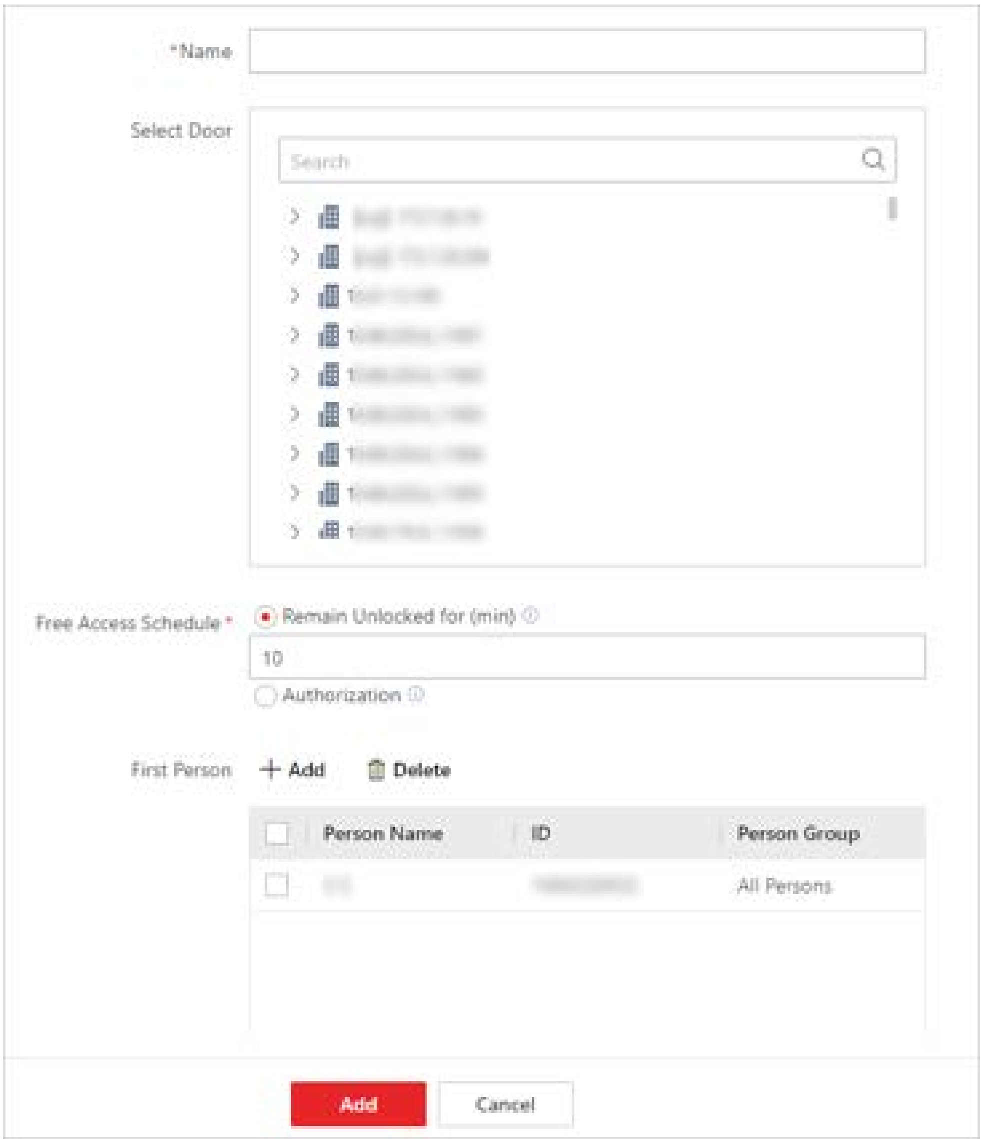
First Person In refers to a rule that only after the first person is authorized to enter with his or her card, fingerprint, or face, can other people's permission be activated. There are two modes for First Person In, the Remaining Open after First Person and the Authorization by First Person.

Steps

Note

This function should be supported by the device.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **First Person In Rules** on the left.
3. Click **Add** to enter the Add First Person In Rules page.
4. Enter the rule name.
5. Select a door from the following area list.
6. Set **Free Access Schedule**.



*Name

Select Door

Search

Free Access Schedule*

● Remain Unlocked for (min)

10

○ Authorization

First Person + Add Delete

□	Person Name	ID	Person Group
□	[redacted]	[redacted]	All Persons

Figure 16-11 Add First Person In Rule Page

Remain Unlocked for

When the door is locked, if the first person swipes card, the door will remain unlocked during the configured period.

Authorization

The door is locked and access is denied with any credentials (except during the free access schedule) until you swipe the first card. After the first person swipes card, the door is authorized and the persons with corresponding access level are granted to access. The authorization will be invalid at 00:00 a.m. every day.

7. Click **Add** to select first person(s).
8. Click **Add** to add the rule.

16.4.3 Add Emergency Operation Group

An emergency operation group is a group for access points which need to be operated (remaining locked/unlocked) 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 Control Client, so that the school closes and no one can get into the school except for high level admins. This function would block out teachers, custodians, students, etc.

Before You Start

Add the access points into different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the top left corner of Home page, select → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Access Control Rule** → **Emergency Operation Group** on the left.
3. Click **Add**.

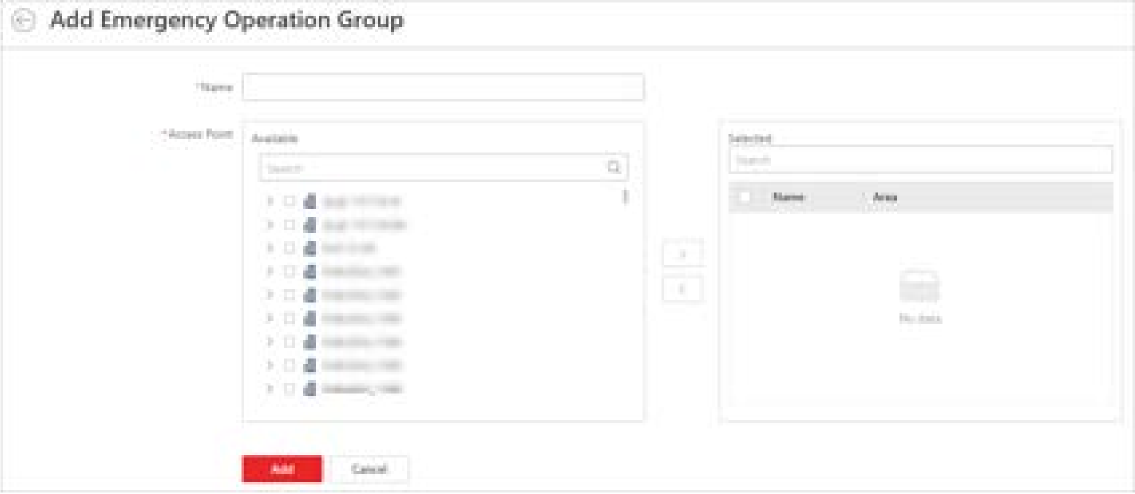


Figure 16-12 Add Emergency Operation Group Page

4. Create a name for the group.
5. Select the access points and click **>** to add them to the group.

Note

You can add doors of access control devices, doors of video intercom devices, and floors of elevator control devices to the emergency operation group.

6. Click **Add**.

   The emergency operation group is added in the table and you can view the access points in the group.

16.4.4 Configure Anti-Passback Rules

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 to enhance the access security of some important or specific places (e.g., laboratories, offices).

Configure Area Anti-Passback Rules

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 he/she enters the area via the door in the group, and he/she 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. In the upper-left corner of the Home page, click ⊞ → **All Modules** → **Access Control** → ▣ **Access Control Application** .
2. Click **Anti-Passback** on the left and click **Area Anti-Passback** on the right.
3. Click **Add** to open the Add Area Anti-Passback page.
4. Create a name for the door group.
5. Select doors in the Available list and click › to add them to the Selected list.
6. **Optional:** Switch on **Forgive Anti-Passback Regularly** and 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. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven.
7. Click **Add**.
8. **Optional:** Perform the following operations after adding the 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

   When a person attempts to use a card without following the rule, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven.

	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).
Delete Anti-Passback Group	Select the group(s) and click **Delete** to delete the anti-passback group(s).

Configure Route Anti-Passback Rules

The route anti-passback depends on the card swiping route. This function establishes a specific card reader sequence in which cards must be used in order to grant access. You should set the first card reader and the subsequent ones. It will authenticate the anti-passback according to the entrance and exit information stored in the card reader.

Steps

1. In the upper-left corner of the Home page, click ⊞ → **All Modules** → **Access Control** → ▣ **Access Control Applications** .
2. Click **Anti-Passback** on the left and click **Route Anti-Passback** on the right.
3. Click **Add** to enter the Add Route Anti-Passback page.
4. Create a name for the route anti-passback rule in the **Name** field.
5. Set the card reader order in the Card Reader Order area.
   1) Click **Add**, select a card reader in the list, and click **Add** to add a card reader.
   2) Hover the cursor on the added card reader and click ⊕ to add another card reader.

   Note

   You can repeat this step to add card readers according to a specific sequence as needed.

   3) **Optional:** Click the card reader and click **Change Card Reader** to select another card reader to replace it.
   4) **Optional:** Click the card reader and click **Delete** to delete the card reader and its subsequent card reader(s).
6. **Optional:** Switch on **First Card Reader** and select a card reader from the drop-down list to set it as the first card reader.

   Note

   If you violate the route anti-passback rule, you should swipe the card again from the first card reader.
7. **Optional:** Switch on **Forgive Anti-Passback Regularly** to set a fixed time so that the platform can forgive the anti-passback violations automatically everyday.
   Anti-Passback Violation

When a person attempts to use a card out of the route anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven.

8. Click **Add**.
9. **Optional:** Perform the following operations after adding the route anti-passback rule.

View Card Reader Order

Click 👁 in the Operation column to view the card reader order of the rule.

Edit Anti-Passback Rule

Click the rule name to edit the anti-passback rule settings.

You can edit the name of the rule, add, change, or delete card readers in the order, change the first card reader, or change the settings of forgiving anti-passback violation regularly.

Set/Cancel Forgiving Anti-Passback Regularly

When a person attempts to use a card out of the route anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven.

Select the rule(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 rule(s) at that time everyday.

You can also select the rule(s) and click **Cancel Forgiving Anti-Passback Regularly** to cancel the settings of the selected rule(s).

Delete Anti-Passback Rule

Select the rule(s) and click **Delete** to delete the route anti-passback rule(s).

16.4.5 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 into different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Multi-Door Interlocking** on the left.
3. Click **Add**.
4. Create a name for the group.
5. Select doors and click **>**.
6. Click **Add**.

16.4.6 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 Home page, select ▦ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Access Control Rule** → **Multi-Factor Authentication** on the left.
3. Click **Add** to enter the Add Multi-Factor Authentication Rule page.
4. Enter the rule name.
5. Select a door from the following area list.
6. 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 on the Control Client. The operator of the Control Client 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.
7. 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 New** to customize a new schedule. For details, refer to ***Set Access Schedule Template*** .

8. 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.
9. Click **Add** to set the access group(s) to define who have the permission to access the door.

   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.

   Card Swiping Order

   Click ↑ or ↓ in the **Operation** column to set the authentication order of different access groups.
10. Click **Save**.

Add Multi-Factor Authentication Group

To perform 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 Home page, select 🟥 → **All Modules** → **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 number from the person list.
7. Click **Add**.

Add Person to Receive Remote Door Open Request

To handle remote door open request on the Control Client, you need to appoint persons to receive these request beforehand.

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Multi-Factor Authentication** on the left.
3. Click **Persons to Receive Remote Door Open Request** on the top.
4. Click **Add** to open the Add Persons to Receive Remote Door Open Request panel.
5. Select persons from the person list.
6. Click **Add**.

16.4.7 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.

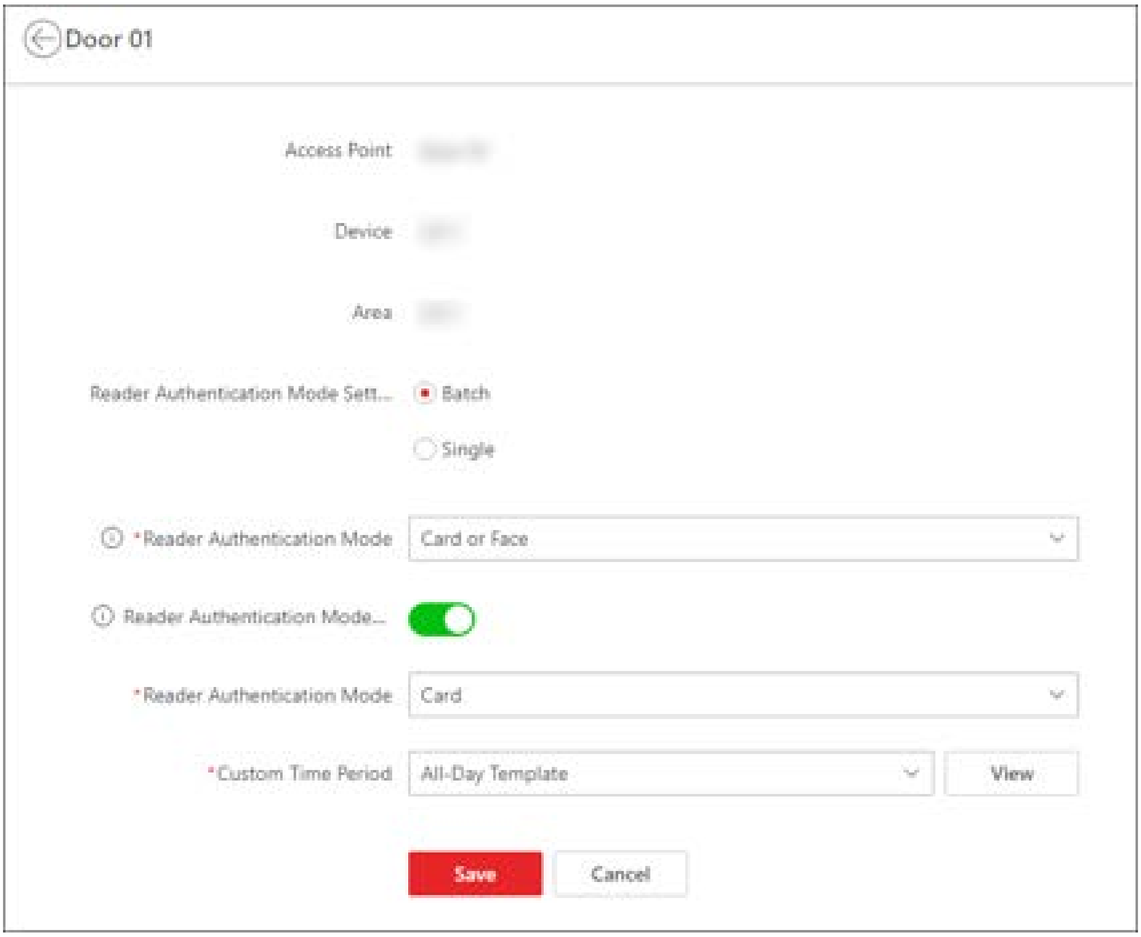
1. In the upper-left corner of the Home page, select ⊞ → **All Modules** → **Access Control** → ▣ **Access Control Application** .
2. Click **Authentication Mode** on the left and click **Reader Authentication Mode** on the right.
3. Select an area from the area list.
4. Click a door name on the right.
5. Select the 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.



Door 01

Access Point [redacted]

Device [redacted]

Area [redacted]

Reader Authentication Mode Sett... ● Batch ○ Single

*Reader Authentication Mode: Card or Face

Reader Authentication Mode...: on

*Reader Authentication Mode: Card

*Custom Time Period: All-Day Template

Figure 16-13 Set Reader Authentication Mode Page

6. Select the 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 → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Authentication Mode** on the left and click **Private Authentication Mode** on the right.
3. Select a person group from the left list.

   All persons in the person group will be listed on the right panel.
4. Click in the Operation column to open the Device for Authentication page.
5. Click **Add**, select 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 editing 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 **Configure All**, 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.

16.4.8 Add Entry and Exit Counting Group

The entry and exit counting group is used to group the access points in certain region. You can set some access points as the region border. Only the persons accessing these access points are counted, and other access points inside the region are ignored. By grouping these access points, the system 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 scene. 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

Note

After setting entry & exit counting group, you can perform entry & exit counting in **Access Control Retrieval → Entry & Exit Counting** on the Control Client to count the number of people who are still in the region and view who enters/exits this region.

1. In the top left corner of Home page, select 🟥 → **All Modules → Access Control → Access Control Application** .
2. Click **Entry and Exit Counting Group** on the left.
3. Click **Add**.
4. Create a name for the group.
5. Click **Add** and select access points from the area list.
6. Set the entering or exiting direction of the card readers of the selected access points.

   The access records on the entering card reader will be counted as person entering this region while the access records on the exiting one will be counted as person exiting this region.
7. Click **Add**.

   The entry & exit counting group is added in the table and you can view the access points in the group.

16.5 Door and Elevator Control

With emergency operation group, you can control door and elevator 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.

You can control all or part of the doors and floors in the selected site and area according to your need. When the emergency is over, you can restore the status to Access with Credential.

Note

Only the users with Administrator or Operator role can control all doors/floors in a batch.

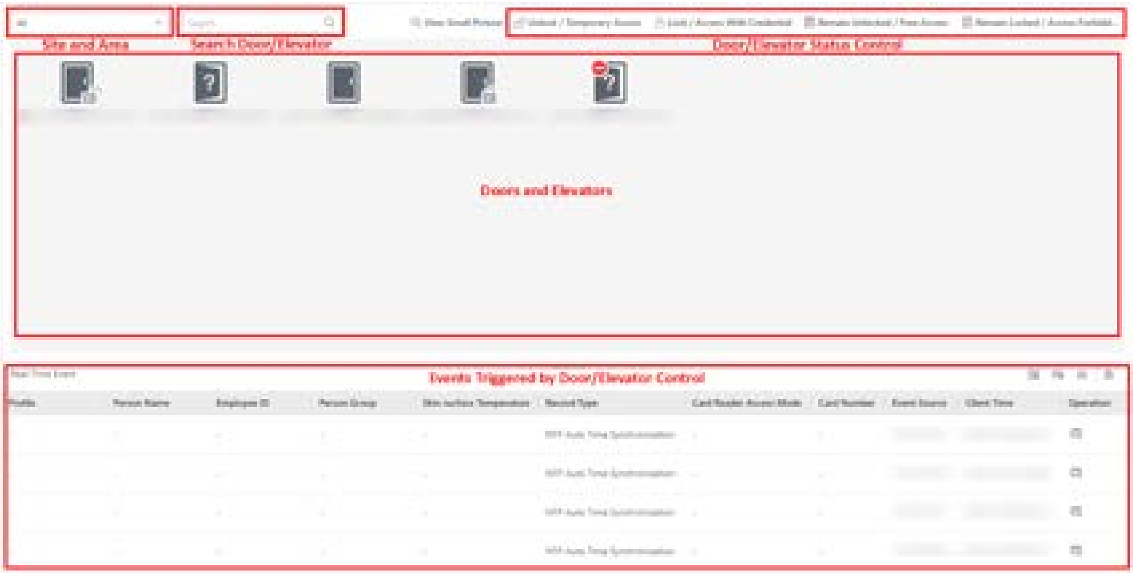

Site and Area
Search Door/Elevator
Door/Elevator Status Control
Doors and Elevators
Events Triggered by Door/Elevator Control

Figure 16-14 Access Control Real-time Monitoring

16.5.1 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 more event information, and so on.

In the top left corner of Home page, select → **All Modules** → **Access Control** → **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 Device Recorded Data Retrieval page to search records by customizing searching 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 column to only show the most relevant event information.

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-switch to the Latest Record** to display the person/visitor information contained in the newest access record. If you uncheck the **Auto-switch to the Latest Record**, the platform will display the person/visitor information contained in the historical access records. The platform supports hiding the window.

16.5.2 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 Emergency Operation Group*** .

In the top left corner of Home page, select 🟥 → **All Modules** → **Access Control** → **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 / Temporary Access** → **All** to unlock all doors in the current site.

Click **Unlock / Temporary Access** → **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. Person who has the access permission can access the door with credentials.

Click **Lock / Access with Credential** → **All** to lock all doors in the current site.

Click **Lock / Access with Credential** → **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 (free access). 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 / Free Access → All** and all doors in the current site will remain unlocked.

Click **Remain Unlocked / Free Access → 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 super users, can access the door even with authorized credentials. This function is applicable for situations such as preventing a theft in the building from getting away.

Click **Remain Locked / Access Forbidden → All** to lock down all the doors in the site.

Click **Remain Locked / Access Forbidden → Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain locked.

Note

For setting person's super user privilege, refer to ***Role and User Management*** .

16.5.3 Elevator 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. See details in ***Add Emergency Operation Group*** .

In the top left corner of Home page, select 🟥 **→ All Modules → Access Control → Real-Time Monitoring** .

Control all or part of floors in the current site.

Temporary Access

During the temporary access time, the 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 super users, can access this floor even with authorized credentials. This function is applicable for situations such as preventing a theft 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.

Note

For setting person's super user privilege, refer to ***Role and User Management*** .

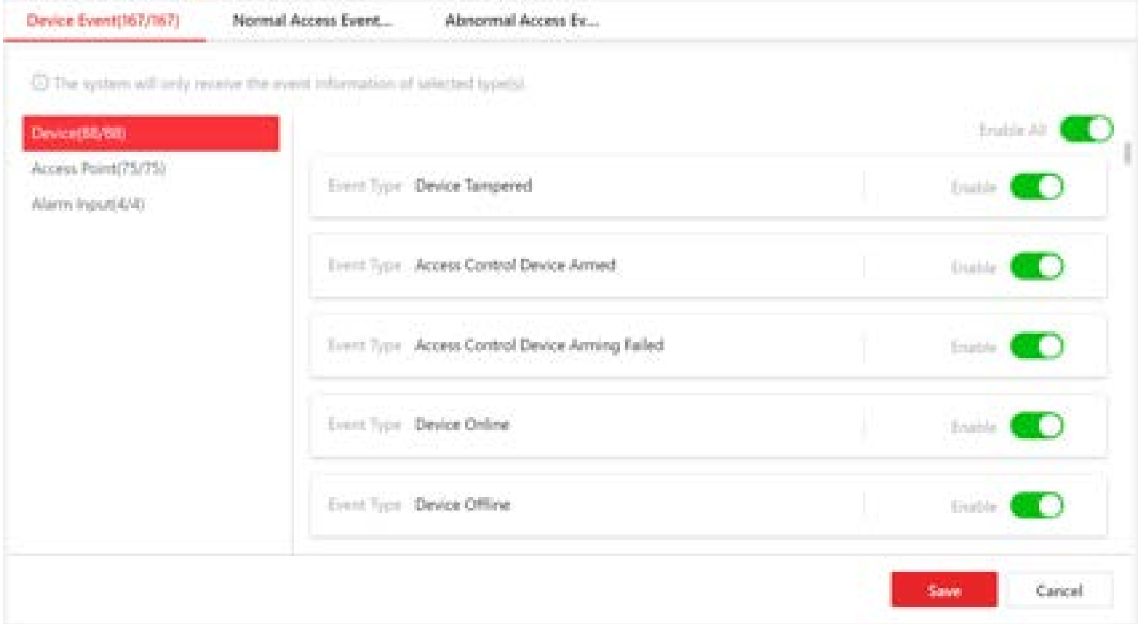
16.6 Subscribe for Device and Access Events

You can subscribe for 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 for device and access events.

Steps

1. In the top left corner of Home page, select 🟥 **→ All Modules → Access Control → Basic Settings** .
2. Click **Device Event Subscription** on the left.



ⓘ The system will only receive the event information of selected type(s).

Enable All: on

Event Type: Device Tampered — Enable: on

Event Type: Access Control Device Armed — Enable: on

Event Type: Access Control Device Arming Failed — Enable: on

Event Type: Device Online — Enable: on

Event Type: Device Offline — Enable: on

Figure 16-15 Device and Access Event Subscription

3. Select an event category from **Device Event**, **Normal Access Event**, and **Abnormal Access Event**.
4. Switch on the event types to subscribe for these events.
5. **Optional:** Switch off the event types whose real-time event records you do not want to receive.

> **Note**
>
> If you switch off a 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 Access Records*** and ***Search Data Recorded on Device*** .

6. 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 for. For details, see ***View Real-Time Access Event*** .

16.7 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 Home page, select ▦ → **All Modules** → **Access Control** → **Basic Settings** → **Call Recipient Settings** .

Click **Add** to select user(s) to receive access control calls on the Control Client.

16.8 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 ⊞ → **All Modules** → **Access Control** → **Basic Settings** .

Click **General** to enter the General page.

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.

16.9 Search Access Records

You can search for persons' access records triggered on specified access points (including doors and elevators) via the Client 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 Event and Alarm*** .

Steps

1. In the upper-left corner of the Home page, select ⊞ → **All Modules** → **Access Control** → **Access Control Retrieval** .
2. Select **Access Record Retrieval** on the left.
3. **Optional:** Import access records to the system.
   - Import access records 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 access records generated in the specified time period.

     Note

     - If the device has uploaded access record(s) to the system before, switching on **Specified Time Range** is not required and access 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 access record to the system before, you must switch on **Specified Time Range** for importing access 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 access records 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**.

4. In the **Time** drop-down list, select the time during which the access records are generated.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

5. **Optional:** In the **Access Point** area, click and select door(s) and elevator(s) from the resource list.
6. **Optional:** In the **Record Type** area, click to select record type(s).
7. In the **Access Result** drop-down list, select an access result type to quickly filter access granted records or access denied records.
8. Set the searching mode.
   - a. Select **Person/Visitor** as the searching mode.
     b. Select **All**, **Person**, or **Visitor** as the person type.
     c. Select **Select Persons** or **Fuzzy Matching** as the searching mode.

     Select Persons

     Select persons in the person list.

     Fuzzy Matching

     Enter a keyword to search for persons whose name contains the keyword.

     d. Click **Add** to select the person(s), or enter the keywords of the person name for fuzzy matching.
   - a. Select **Card No.** as the searching mode.
     b. Enter the card number.
9. **Optional:** Switch on **Skin-Surface Temperature Status** and select **Normal** or **Abnormal**.
10. **Optional:** Switch on **Wearing Mask or Not** and select **Wearing Mask** or **No Mask**.
11. Click **Search**.

    Matched access records are listed on the right.
12. **Optional:** Perform the following operations after searching for access records.

View Record Details Click the person name in the Full Name column to view the record details, such as the recorded video or captured picture of the related camera (if configured), person information, and access information. If the person is a visitor, you can view the detailed visitor information and host information, including name, person profile, visit reason, belongings picture (if any), etc.

Filter Search Results by Person Type

Click 🝖 next to the column name **Person/Visitor** and select **Person** or **Visitor** to filter the search results.

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 file in 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 access record details (including person name, person ID, event time, access result, etc.) in your PC as an Excel or a CSV file. If you select **Excel**, you can check **Export Picture** to save the captured pictures as well.

Note

Up to 500 records can be exported each time.

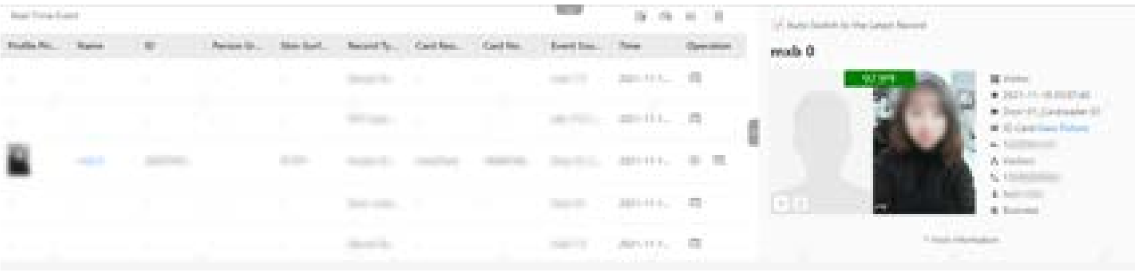


Figure 16-16 Real-Time Events

16.10 Search Data Recorded on Device

Data recorded on devices are records (e.g., triggered events/alarms, card-swiping records, etc.) stored in access control devices, elevator control devices, and video intercom devices. The records can be events/alarms triggered by human behaviors detected by devices and those triggered by devices (such as device faults). You can search for the records in different dimensions according to your needs.

Steps

1. In the upper-left corner of the Home page, select ⊞ → **All Modules** → **Access Control** → 🔍 **Access Control Retrieval** .

2. Click **Device Recorded Data Retrieval** on the left.
3. In the Time drop-down list, select a time range for searching.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

4. 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 records can be access records, operation records, and alarms triggered by human behaviors.

Device

Devices include access control devices, elevator control devices, and video intercom devices. The data recorded in these devices covers all events triggered by devices (such as device faults).

Alarm Input

The alarm inputs included in devices. The records are arming status changes.

5. Select the record source(s) and record type(s).
6. Click **Search**.

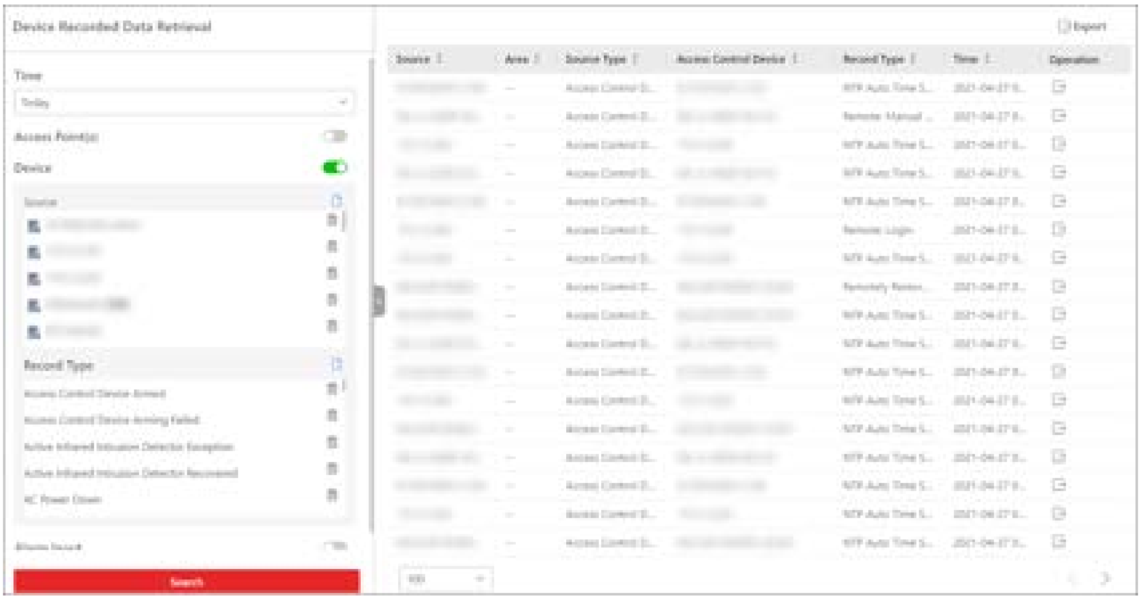

Device Recorded Data Retrieval
Time
Today
Access Point(s)
Device
Source
Record Type
Access Control Device Armed
Access Control Device Arming Failed
Active Infrared Intrusion Detector Exception
Active Infrared Intrusion Detector Recovered
AC Power Down
Alarm Input
Search
Export
Source
Area
Source Type
Access Control Device
Record Type
Time
Operation

Figure 16-17 Device Recorded Data Retrieval

7. **Optional:** Perform further operations on the searched records.

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 or a CSV file.

Chapter 17 Emergency Mustering

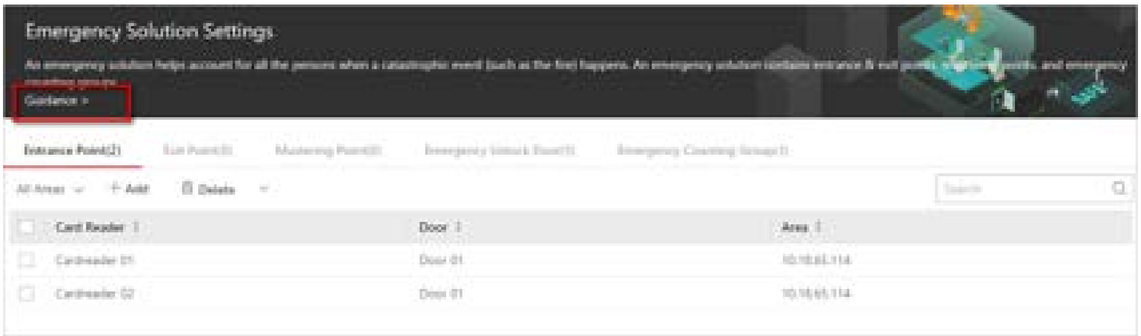
The emergency mustering helps users get prepared to account for all staff in a quick and efficient manner in an emergency situation, such as a fire.

You can configure an emergency solution beforehand and start a roll call by one click. In an emergency, the users can:

- Conduct a roll call with real-time data.
- Get immediate access to personal contact information.
- Filter persons based on status (In, Out & Not Check In, Checked In, and Unknown)

Based on the information provided by the platform, users can rescue persons who are still in the place.

Click **Guidance** to and configure the emergency solution following the guidance.



Emergency Solution Settings

An emergency solution helps account for all the persons when a catastrophic event (such as the fire) happens. An emergency solution contains entrance & exit points, mustering points, and emergency counting groups.

Guidance >

Card Reader	Door	Area
Cardreader 01	Door 01	10.18.65.114
Cardreader 02	Door 01	10.18.65.114

Figure 17-1 Entrance Point List

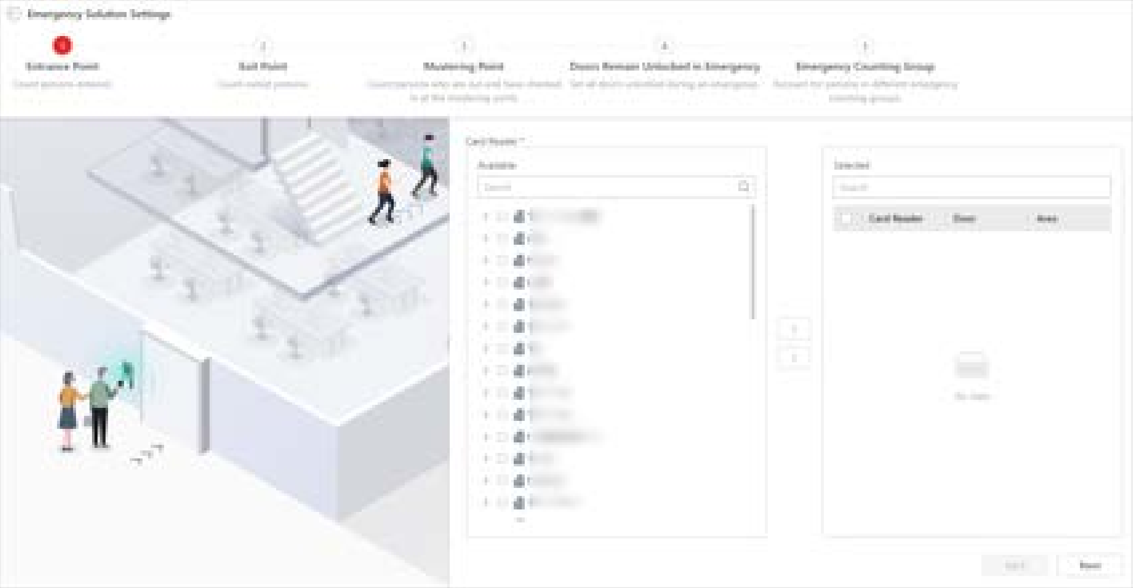


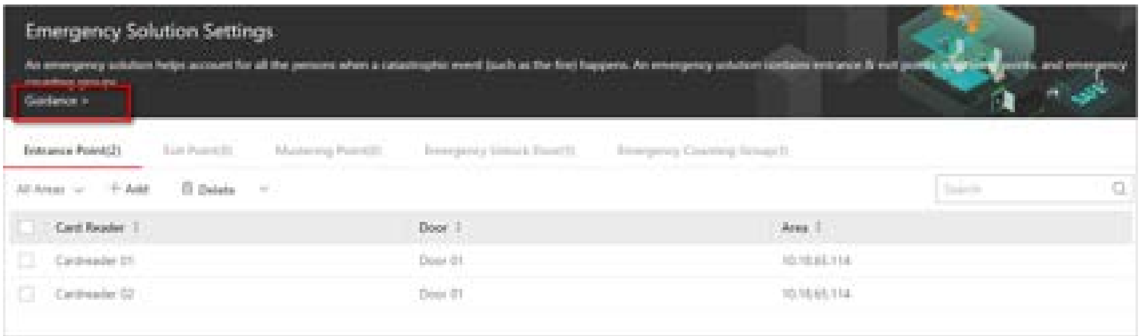
Figure 17-2 Guidance for Setting the Emergency Solution

17.1 Emergency Solution Settings

An emergency solution refers to the preparation settings before a roll call. The emergency solution includes the settings of entrance points, exit points, mustering points, doors remain unlocked in an emergency, and emergency counting groups. After setting the emergency solution, users can start a roll call by one click once an emergency happens.

In the top left corner of Home page, select ▦ → **All Modules** → **Emergency Mustering** → **Emergency Solution Settings** . Configure the following items according to your needs.

1. Add Entrance Points



Card Reader	Door	Area
Cardreader 01	Door 01	10.18.65.114
Cardreader 02	Door 01	10.18.65.114

Figure 17-3 Entrance Point List

An entrance point is the card reader by which persons authenticate to check in before entering a place. If a person authenticates by an entrance point, the person's status is In.

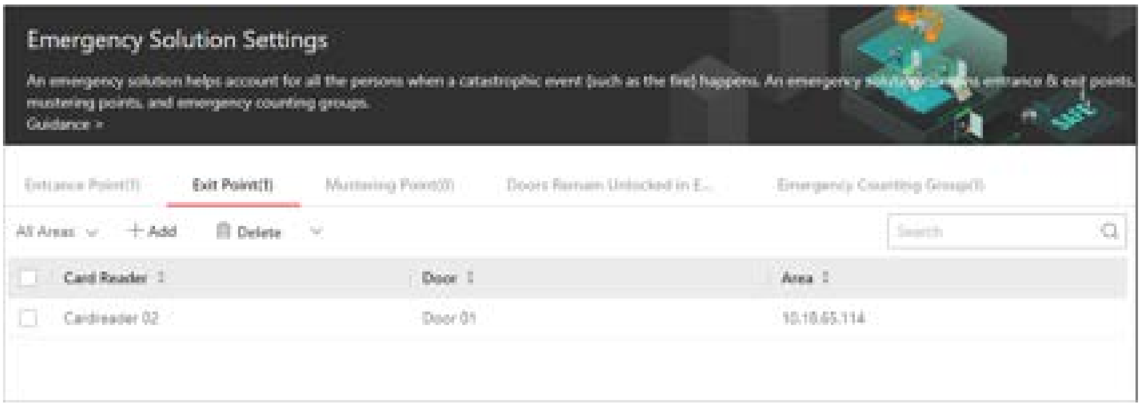
Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as entrance points of the area.

You can check card readers and click **Delete** to cancel setting them as entrance points, or click ⌄ → **Delete All** to cancel setting all card readers as entrance points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the entrance points.
- To delete the entrance points, you should end the emergency first.

2. Add Exit Points



Emergency Solution Settings

An emergency solution helps account for all the persons when a catastrophic event (such as the fire) happens. An emergency solution contains entrance & exit points, mustering points, and emergency counting groups.

Guidance >

Card Reader	Door	Area
Cardreader 02	Door 01	10.10.65.114

Figure 17-4 Exit Point List

An exit point is the card reader by which persons authenticate for exiting from a place. If a person authenticates by an exit point, the person's status is Out.

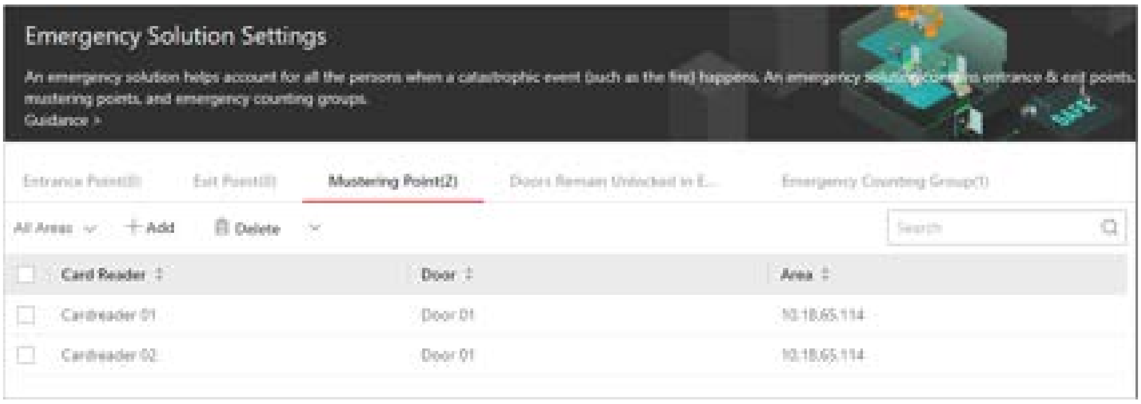
Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as exit points in the area.

You can check card readers and click **Delete** to cancel setting them as exit points, or click ⌄ → **Delete All** to cancel setting all card readers as exit points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the exit points.
- To delete the exit points, you should end the emergency first.

3. Add Mustering Points



Emergency Solution Settings

An emergency solution helps account for all the persons when a catastrophic event (such as the fire) happens. An emergency solution contains entrance & exit points, mustering points, and emergency counting groups.

Guidance >

□	Card Reader	Door	Area
□	Cardreader 01	Door 01	10.18.65.114
□	Cardreader 02	Door 01	10.18.65.114

Figure 17-5 Mustering Point List

A mustering point is the card reader locating in a refuge. When an emergency happens, persons exit from the place where they are, go to the refuge, and check in by the mustering point. The status of persons who have checked in at the mustering point is Out & Checked In.

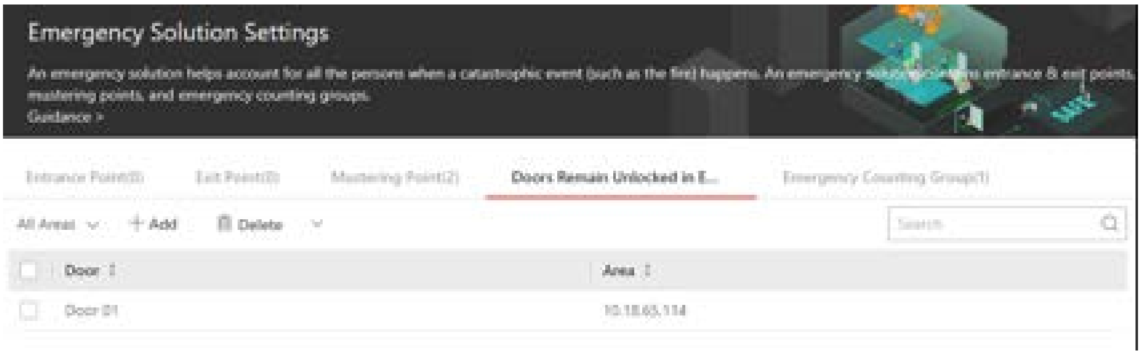
Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as mustering points in the area.

You can check card readers and click **Delete** to cancel setting them as mustering points, or click ⌄ **→ Delete All** to cancel setting all card readers as mustering points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the mustering points.
- To delete the mustering points, you should end the emergency first.

4. Add Doors Remain Unlocked in Emergency



Emergency Solution Settings

An emergency solution helps account for all the persons when a catastrophic event (such as the fire) happens. An emergency solution contains entrance & exit points, mustering points, and emergency counting groups.

Guidance >

□	Door	Area
□	Door 01	10.18.65.114

Figure 17-6 Doors Remain Unlocked in Emergency

A door remain unlocked in an emergency refers to the the door that will be turned to the status of Remain Unlocked once an emergency happens. Thus the persons inside the place can exit from the place without authentication at the card reader.

Click ⌄ besides **All Areas** and select an area. Click **Add** and select doors to set them as doors remain unlocked in an emergency in the area.

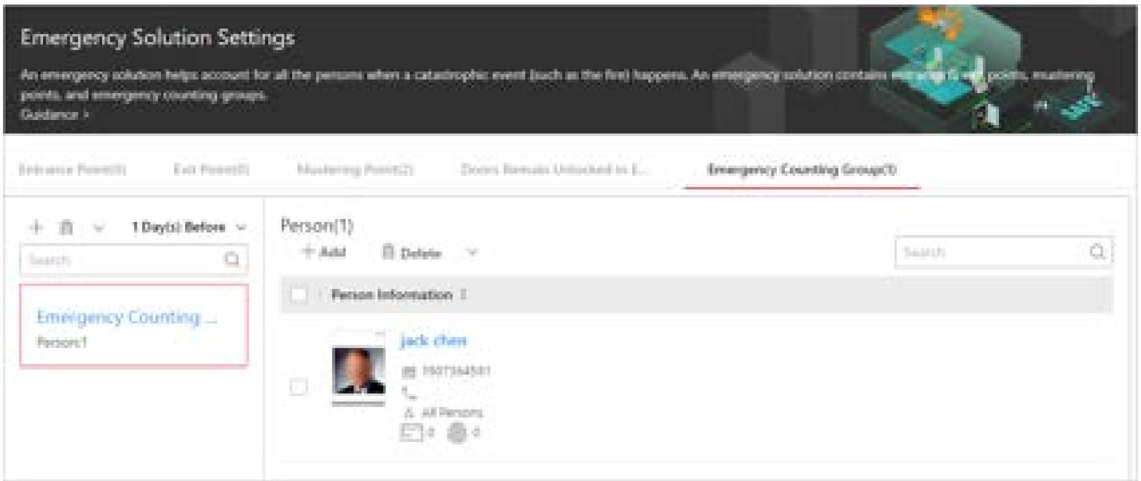
You can check doors and click **Delete** to delete them, or click ⌄ → **Delete All** to delete all doors.

You can also enter a door name on the top right to search for it.

Note

- Make sure you have added the door to the platform before selecting the doors.
- To delete the doors, you should end the emergency first.

5. Add Emergency Counting Groups



An emergency solution helps account for all the persons when a catastrophic event (such as the fire) happens. An emergency solution contains entrance & exit points, mustering points, and emergency counting groups.

Figure 17-7 The Emergency Counting Group

An emergency counting group refers to a person group based on which you can know how many persons are in, out, or out & checked in when the platform is in an emergency.

Click + to open the Add Emergency Counting Group pane. Enter a name for the group and click ⊕ to add persons to the group. Click **Add** to add more persons to the group after adding the group.

Note

Make sure you have added the persons to the platform beforehand.

You can perform the following operations.

- Click ⌄ besides the **1 Day Before** to update the persons in the group.
- Click a person name to view person details.
- Select a group and click 🗑 to delete it, or click ⌄ → **Delete All** to all groups.
- Check persons and click **Delete** to remove the selected persons from the group, or click ⌄ → **Delete All** to remove all the persons from the group.

17.2 Start a Roll Call

After configuring the emergency solution, you can start a roll call by one click once an emergency happens.

In the top left corner of Home page, select ▦ → **All Modules** → **Emergency Mustering** → **Roll Call** . Click **In Emergency** to display the data of emergency counting groups.

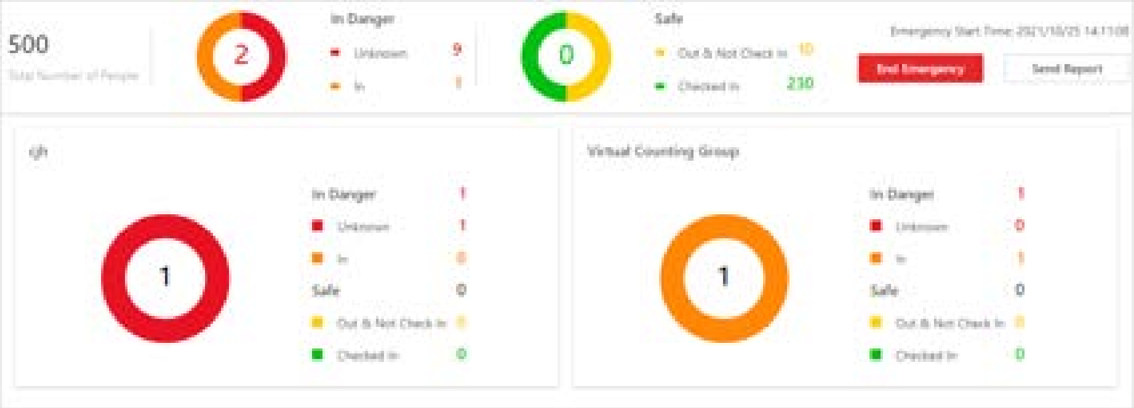


Figure 17-8 Data of Emergency Mustering

On the top left, the total number of persons in emergency counting groups are displayed. On the right of the total number of persons, the number of persons in danger and safe are both displayed. The persons in danger refer to persons who are still inside (checked in at the entrance point but did not check out at the exit point) the place where the emergency happens and the persons who did not check in at the entrance point. The persons who are safe refer to persons who have checked out at the exit point but not checked in at the mustering point and persons who have checked in at the mustering point.

The data of each emergency counting group is also displayed. You can click a group name to enter the page of the group for details. Click 👤 to check in a person who shows at the mustering point but the person status is not Checked In.

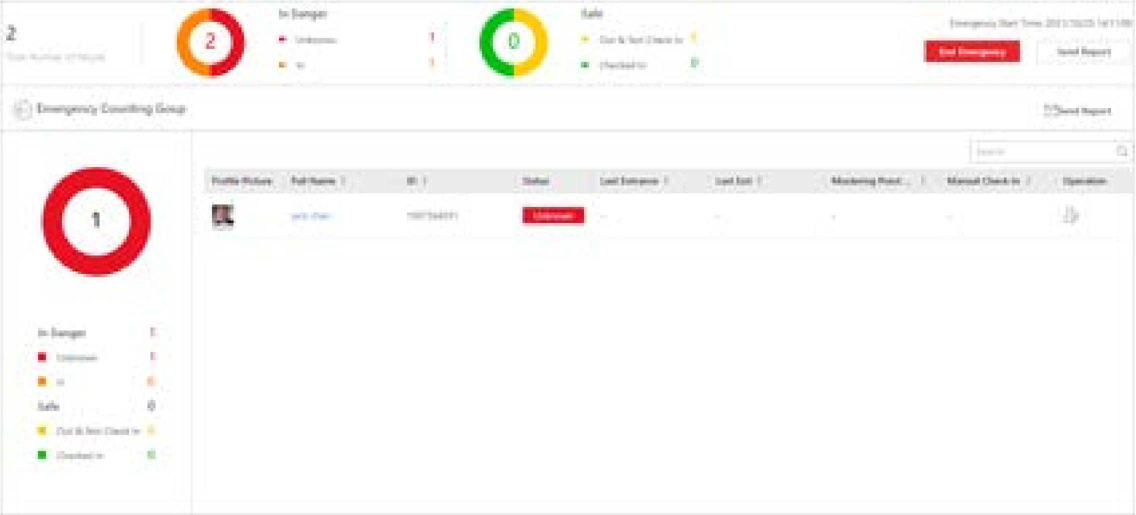


Figure 17-9 Data of an Emergency Counting Group

The virtual counting group refers to a group consisting of persons who are not added to any emergency counting group.

Perform the following operations if you need.

- Click **End Emergency** to end the emergency status of the platform.
- Click **Send Report** and select an email template to send the data of the emergency counting group to the recipients.

Note

- It is extremely important to remember that the data displayed and the reports contained in the email can only ever be accurate if all users follow the conventions of the system. All users must read in and out of all controlled areas; running a logical anti-passback system can help to enforce this.
- During the emergency, editing the emergency solution is not allowed. You should end the emergency before editing it.

Chapter 18 Vehicle and Parking Management

HikCentral Professional provides vehicle and parking management services covering vehicle management, entry & exit rule management, parking fee rule management, etc. 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. Meanwhile, you need to import vehicle information to the platform and categorize vehicles into different types if needed, so that you can predefine parking fee rules and entry & exit rules for them. For the 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.

18.1 Flow Chart of Vehicle and Parking Management

The following flow chart shows the process of configuring and managing vehicle and parking.

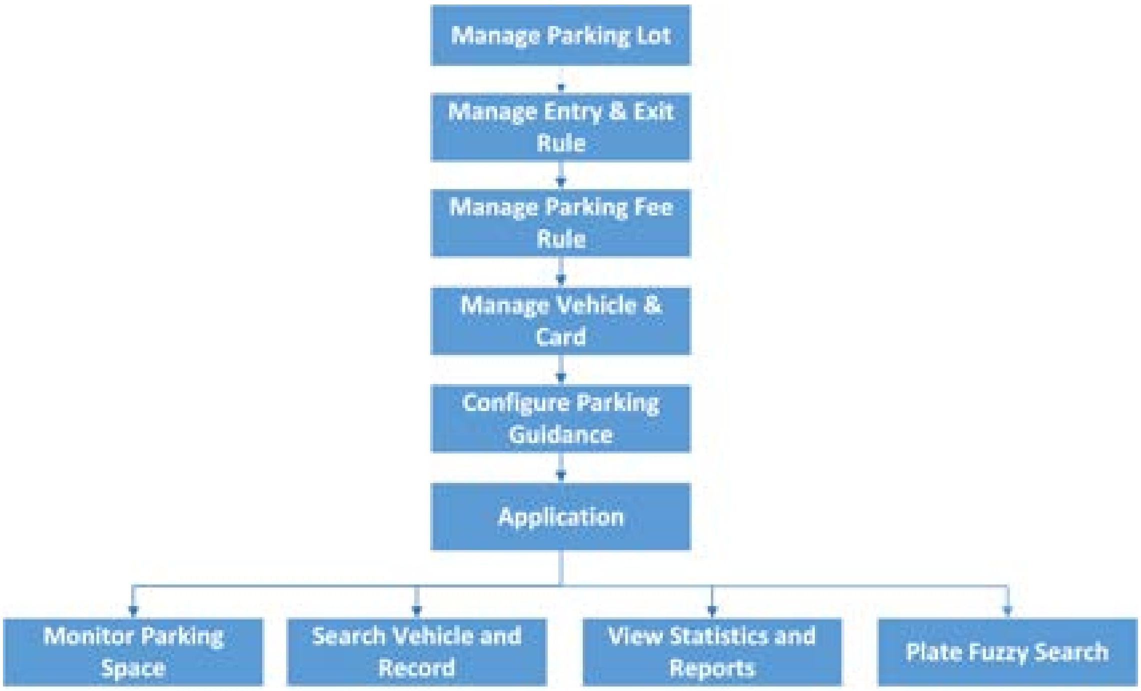


Figure 18-1 Flow Chart of Vehicle and Parking Management

- **Parking Lot Management**: Parking lot is a parking facility that is intended for parking vehicles. You need to create a parking lot in the platform and set its entrances and exits as well as lanes according to actual needs.
- **Vehicle and Card Management**: On the Web Client, the administrator can add vehicle information to the platform, and set events and alarms to define whether an event or alarm will

be triggered when the recognized license plate number matches or mismatches with that managed in the platform, or whether an event or alarm will be triggered when the recognized vehicle type matches the specified one. For entrance and exit control, the administrator can set entry & exit rules for the vehicles managed in the platform to define whether to allow the vehicles to enter or exit the parking lot. In addition, the administrator can issue temporary cards to temporary vehicles for parking management.

- **Entry & Exit Rule Management**: An entry & exit rule defines how to open barrier gate when the platform detects a vehicle at the lane. The platform can open the barrier automatically when detects a vehicle, or you can also open it manually by clicking **Allow** button on the Control Client after verifying its identity.
- **Parking Fee Rule Management**: A parking rule defines how vehicles are charged for parking. On the Web Client, the administrator can set parking fee rules for parking lots, including the parking fee rule for a specific type of vehicles, the parking pass rule, the discount rule, etc.
- **Parking Guidance Configuration**: Parking guidance is performed by two types of devices: the guidance terminal and the guidance screen. The guidance terminal can relate multiple parking cameras for management, and the guidance screen displays the number of vacant parking spaces in a parking lot and guides the drivers to the area where there are vacant parking spaces.
- **Application**: After completing the above-mentioned configurations, you can perform operations including monitoring parking spaces, searching for vehicles and records, viewing statistics and reports, and license plate fuzzy search.

18.2 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.

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.

Device Monitoring: You can view the health of devices related to the parking lot, including guidance terminals, parking cameras, and guidance screens.

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.

You can click **Parking Space Overview** to go to the Parking Space Overview page and view more detailed statistics of parking spaces. You can also click **Maintenance** to go to the Maintenance page and view more detailed statistics of the health of devices. See ***Parking Space Monitoring*** and ***Maintenance*** for details.

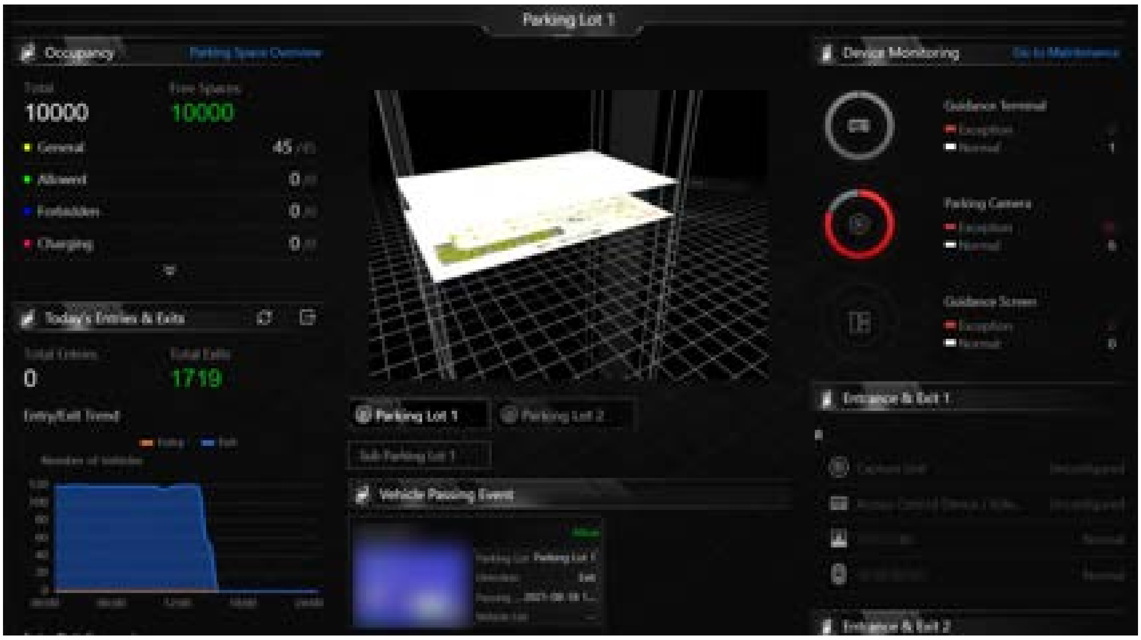


Figure 18-2 Parking Lot Overview Page

18.3 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.

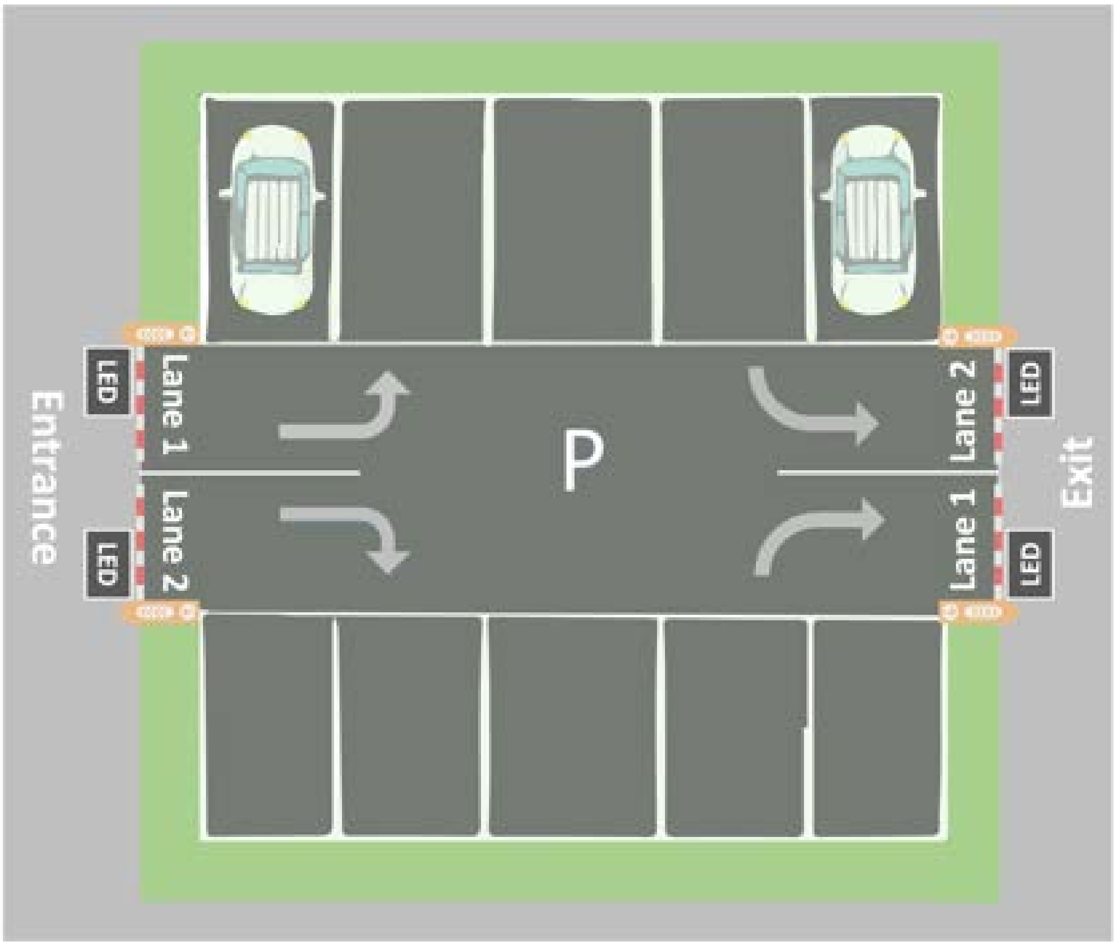
Entrance & Exit

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.


Entrance
LED
Lane 1
LED
Lane 2
P
Lane 2
LED
Lane 1
LED
Exit

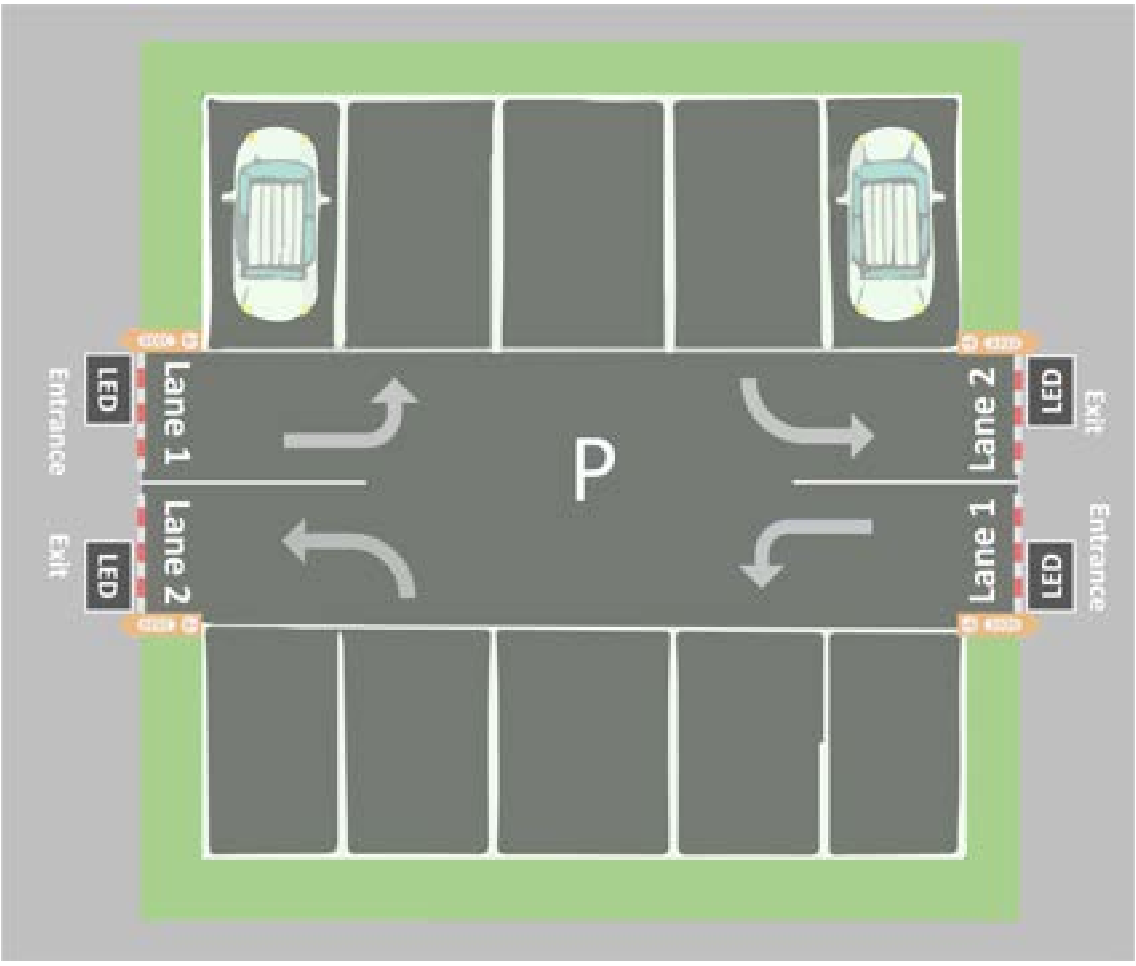


Figure 18-3 Parking Lot

18.3.1 Add Parking Lot

In the Parking Lot Management module, 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. Go to ▦ → **All Modules** → **Vehicle** → **Parking Lot Management** .
2. Click **Add Parking Lot** to open the Add Parking Lot window.

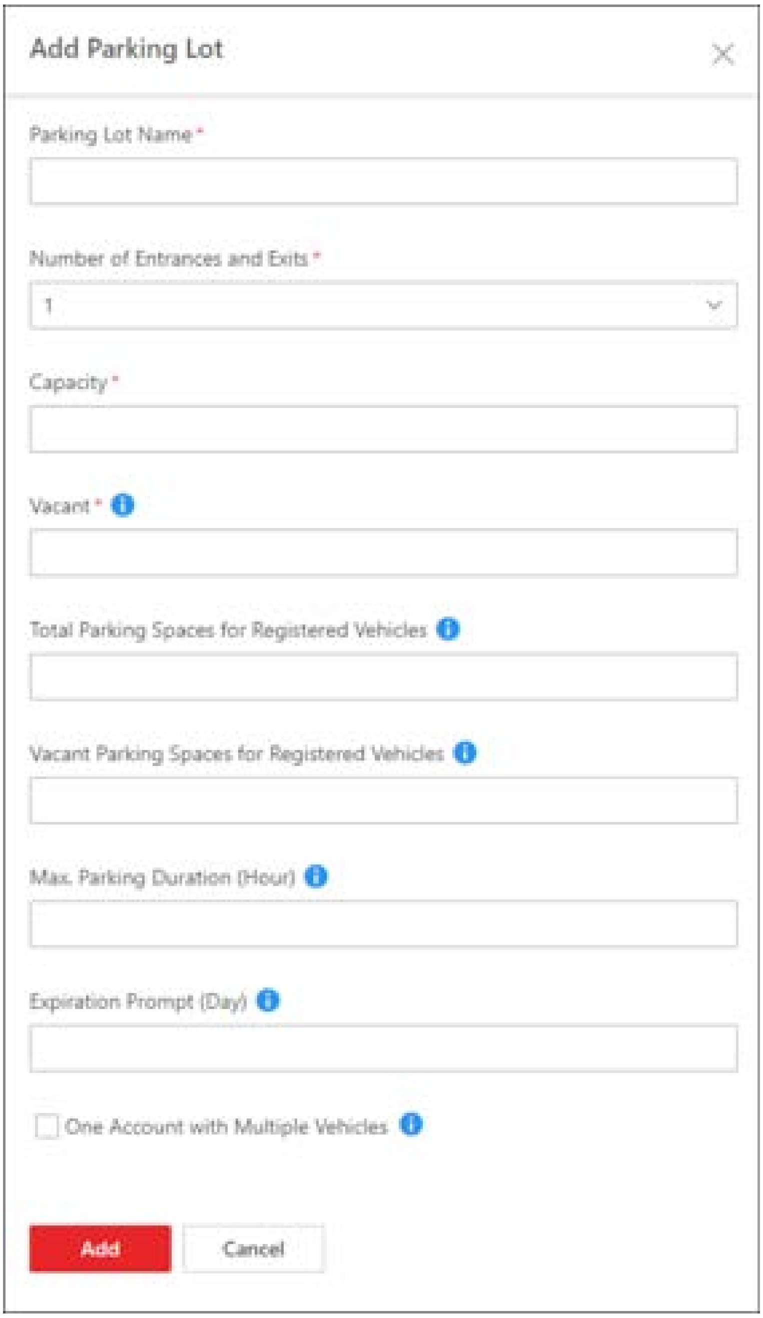

Add Parking Lot
Parking Lot Name *
Number of Entrances and Exits *
1
Capacity *
Vacant *
Total Parking Spaces for Registered Vehicles
Vacant Parking Spaces for Registered Vehicles
Max. Parking Duration (Hour)
Expiration Prompt (Day)
□ One Account with Multiple Vehicles
Add
Cancel

Figure 18-4 Create Parking Lot Window

3. Enter the parking lot information.

Number of Entrances and Exits

The number of entrances and exits in the created parking lot.

Capacity

The total number of parking spaces in the created parking lot.

Vacant

The number of parking spaces without parked vehicles.

Total Parking Spaces for Registered Vehicles

The total number of parking spaces for registered vehicles.

Note

Only registered vehicles are allowed to park in these parking spaces.

Vacant Parking Spaces for Registered Vehicles

The number of vacant parking spaces for registered vehicles.

Max. Parking Duration (Hour)

The maximum parking duration of a car parked in the created parking lot. You can configure an event or alarm which will be triggered when a vehicle's parking is due. For example, you enter 12, an event or alarm (if any) will be triggered if a vehicle has parked for more than 12 hours.

Expiration Prompt (Day)

Take a vehicle which expires at Jan. 6th, 2020 as an example, if you enter 5, the expiration prompt will be displayed on the LED screen linked to the parking lot from Jan. 1st, 2020 to Jan. 5th, 2020.

Multiple Vehicles Under One Account

One vehicle owner account with multiple vehicles related.

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** to enter the page of this parking lot. b. In the upper-right corner, click **Edit** to open the Edit Parking Lot panel. **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/Edit/Delete a Sub Parking Lot

In a parking lot area, click **Settings** 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.

18.3.2 Add Entrance and Exit

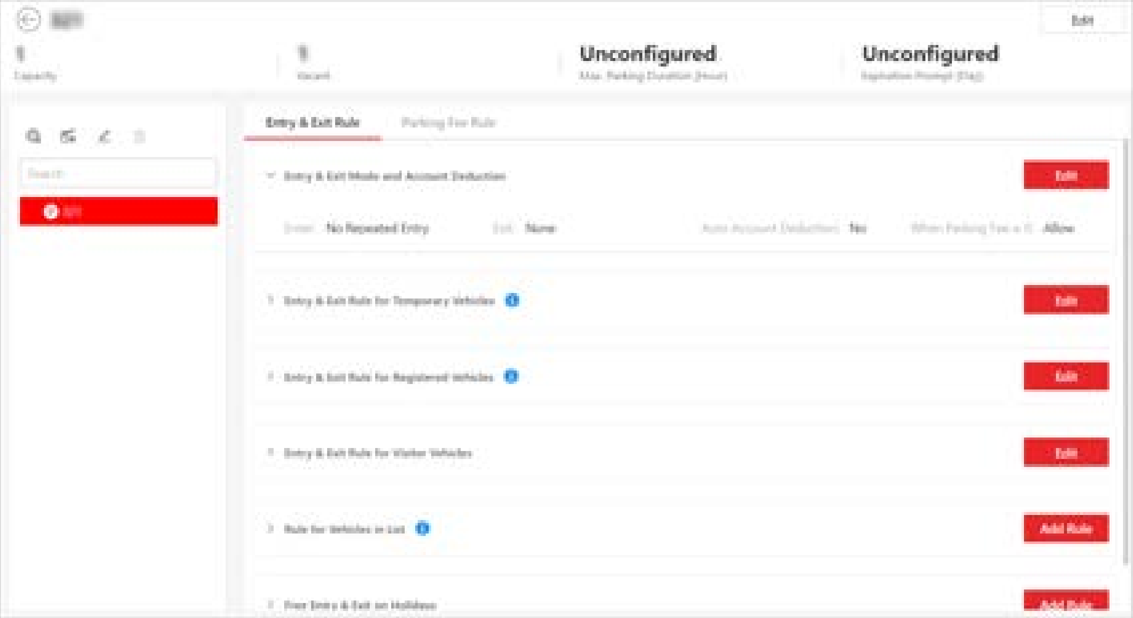
An entrance or exit helps control vehicles to enter/exit the parking lot or prevent vehicles from entering/exiting the parking lot. For example, the entrance or exit allows a vehicle in the VIP list to enter/exit the parking lot, and prevent a vehicle in the blocklist from entering the parking lot. You 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. Go to → **All Modules** → **Vehicle** → **Parking Lot Management** .
2. In a parking lot area, click **Settings** to enter the page of this parking lot.


Edit
Capacity
Vacant
Unconfigured
Max. Parking Duration (Hour)
Unconfigured
Expiration Prompt (Day)
Search
Entry & Exit Rule
Parking Fee Rule
Entry & Exit Mode and Account Deduction
Edit
Entry & Exit Rule for Temporary Vehicles
Edit
Entry & Exit Rule for Registered Vehicles
Edit
Entry & Exit Rule for Visitor Vehicles
Edit
Rule for Vehicles in List
Add Rule
Free Entry & Exit on Holidays
Add Rule

Entry: No Repeated Entry Exit: None Auto Account Deduction: No When Parking Fee ≠ 0: Allow

Figure 18-5 Parking Lot Page

3. On the top of the left list, click .
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.

18.3.3 Add Lane

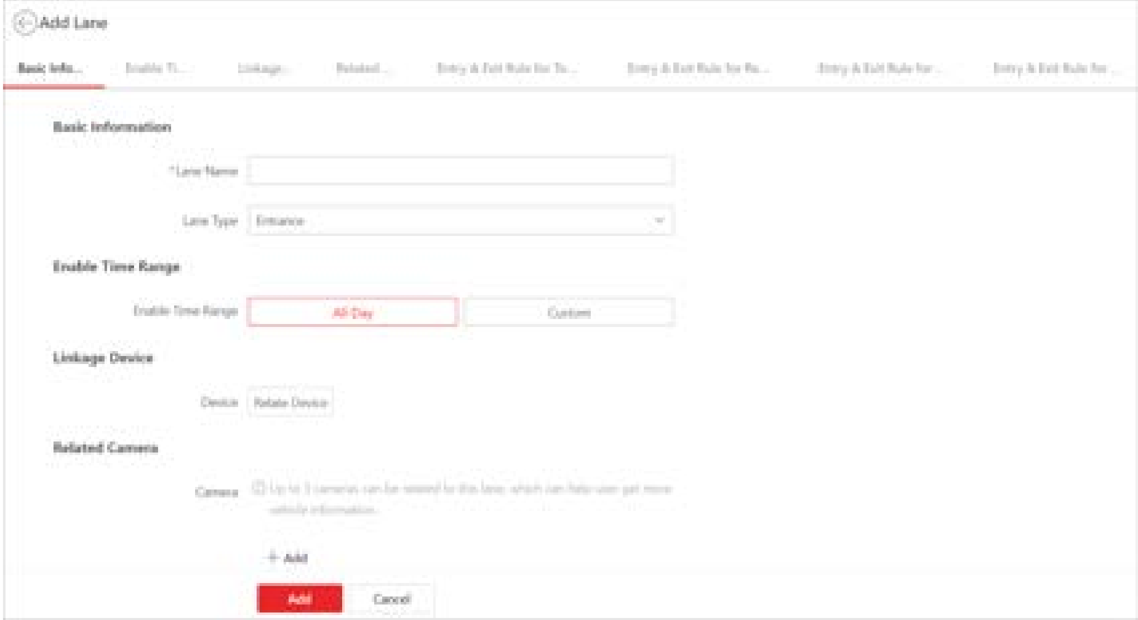
A lane linked with a capture unit or card-swiping device is used for controlling the barrier. A capture unit linked to a lane can recognize a vehicle at the lane, and compare the vehicle information with vehicles in a vehicle list. Then, the capture unit opens the barrier automatically to allow the vehicle to enter/exit according to entry and exit rule of the vehicle list if the vehicle has been added to a vehicle list. An access control device/video intercom device opens the barrier when a vehicle owner swipes card on it to open the barrier to allow the vehicle to enter or exit the parking lot. Meanwhile, the capture unit does not open the barrier for the recognized license plate number which is added to the blocklist; the access control device/video intercom device cannot control the barrier without swiping a card specialized for the parking lot. You can also relate a camera with the lane. The camera will capture a picture (it can be a vehicle, human face, or other) which will be displayed on the Control Client. You can view the pictures captured by the related camera on the Control Client if needed.

Before You Start

- Make sure you have added at least an entrance/exit for the parking lot. See ***Add Entrance and Exit*** for details.
- You may need to have added a capture unit to the system for barrier control.

Steps

1. Go to → **All Modules** → **Vehicle** → **Parking Lot Management** .
2. In a parking lot area, click **Settings** to enter the page of this parking lot.
3. Select an entrance & exit from the left list.
4. Click + to enter the Add Lane page.


Add Lane
Basic Info...
Enable Ti...
Linkage...
Related...
Entry & Exit Rule for Te...
Entry & Exit Rule for Re...
Entry & Exit Rule for ...
Entry & Exit Rule for ...
+ Add
Add
Cancel

Basic Information

*Lane Name

Lane Type: Entrance

Enable Time Range

Enable Time Range: All Day | Custom

Linkage Device

Device: Relate Device

Related Camera

Camera: Up to 3 cameras can be related to this lane, which can help user get more vehicle information.

Figure 18-6 Add Lane Page

5. Set the lane.
   1) In the Basic Information area, create a name for the lane, and select a lane type from the drop-down list.
   2) In the Enable 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 Linkage Device area, click **Relate Device** to select device(s) to be related to the lane, and set one device as the barrier control unit according to actual needs.

   Entrance/Exit Station

   An entrance/exit station 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 station, the station will control the barrier gate to open and let the vehicle enter; after the vehicle returns the ticket or card, the station will allow the vehicle to exit. Besides, if an entrance/exit station assigns cards instead of tickets, its guidance screen is configurable. See ***Set Contents Displayed on Guidance Screen*** 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 ***Manage Entry & Exit Rules for Parking Lots*** for details about setting an entry & exit rule.

Note

You can relate 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.

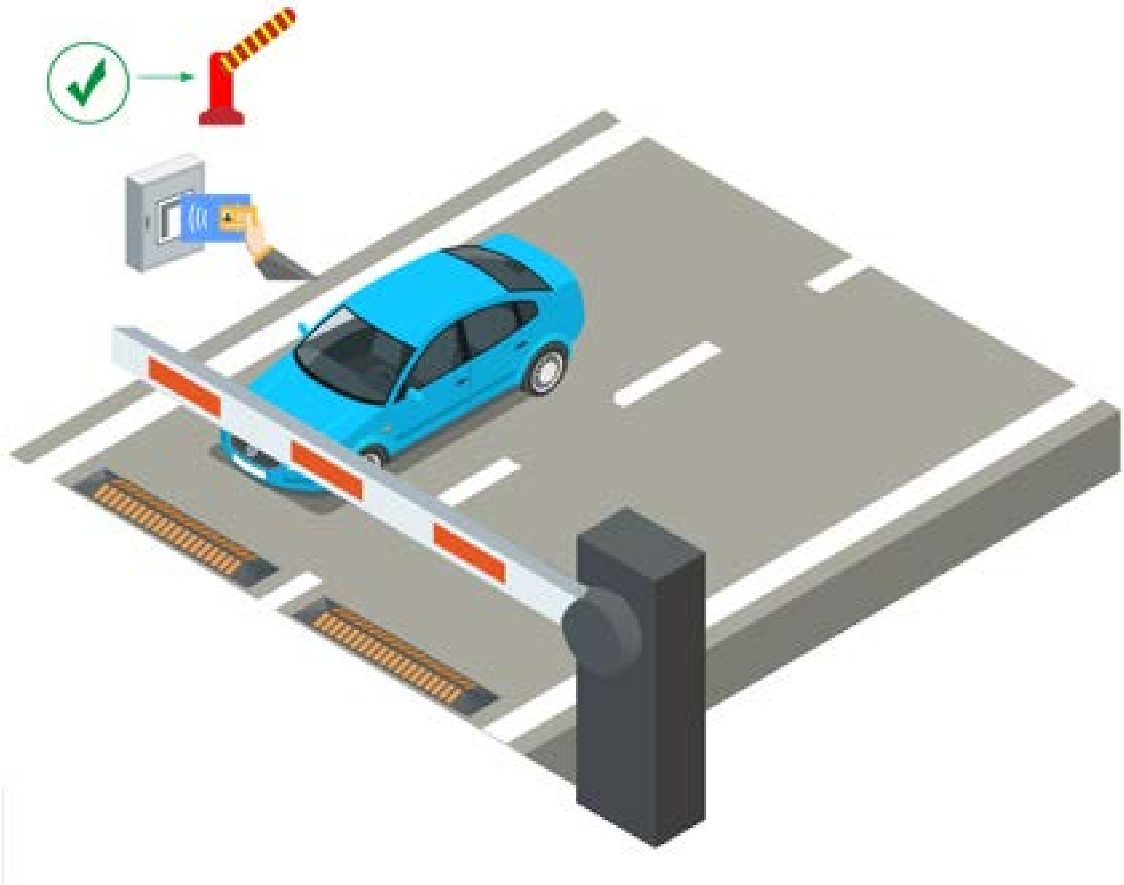


Figure 18-7 Opening Barrier by Card Swiping

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.

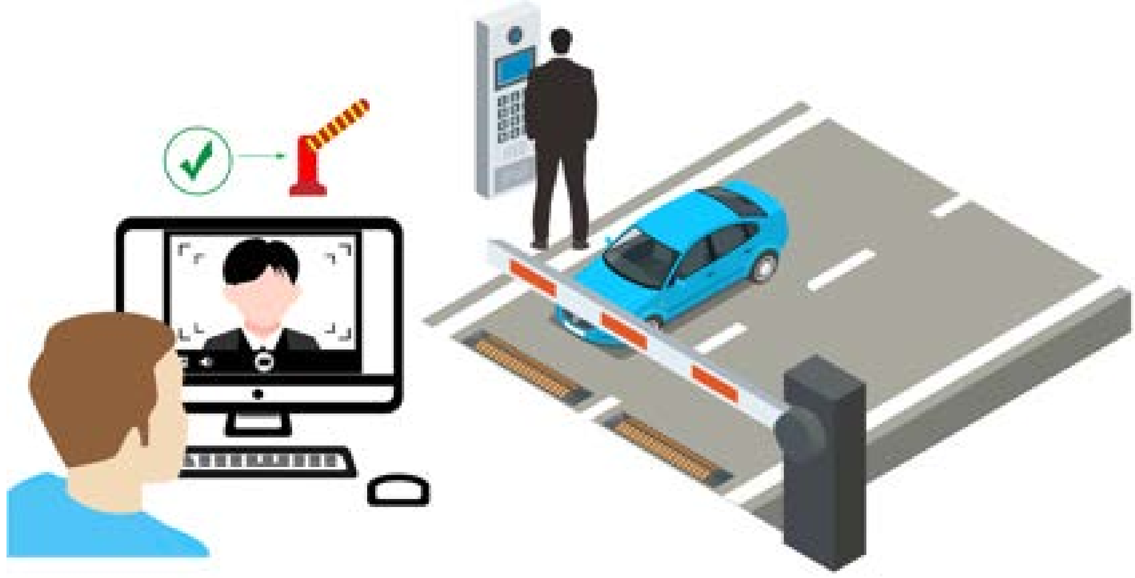


Figure 18-8 Opening Barrier by Video Intercom

Guidance Screen

A guidance screen is used for displaying information such as the number of vacant parking spaces, vehicle expiration date. See ***Set Contents Displayed on Guidance Screen*** for details.

4) In the Related Camera area, select camera(s) to be related to the lane.

Note

- Make sure you have enabled picture storage for the camera. Otherwise, you cannot see the captured pictures on the Control Client. See ***Area Management*** for details about how to enable picture storage for a camera.
- Up to three different cameras can be related to the lane.
- One camera can be related to multiple lanes.
- You can view the pictures captured by the related camera when viewing the vehicle-passing information on the Web Client and Control Client.

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.

6. Click **Add**.

18.3.4 Set Contents Displayed on Guidance Screen

The guidance screen related to a lane and the guidance screen on an entrance/exit station can be used for displaying information including the date and time, parking duration, license plate number, expiration prompt, etc.

Before You Start

Make sure you have related a guidance screen to a lane. See ***Add Guidance Screen*** for details about how to add a guidance screen.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **Parking Lot Management** .
2. Click **Settings** to enter the parking lot settings page.
3. Select an entrance or exit from the left list.
4. Click the name of the guidance screen to open the Screen Configuration pane.

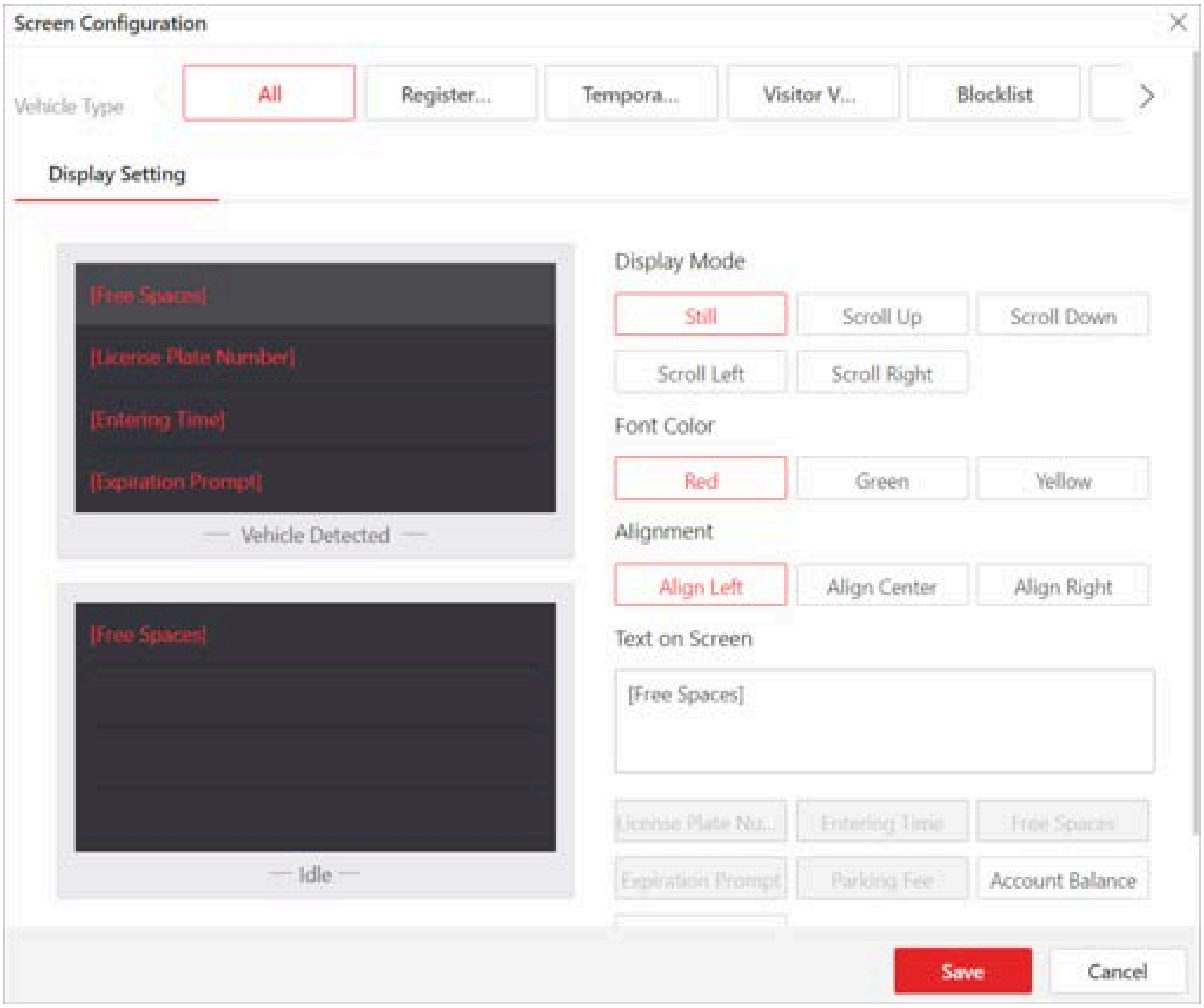


Figure 18-9 Screen Configuration for Common Guidance Screen

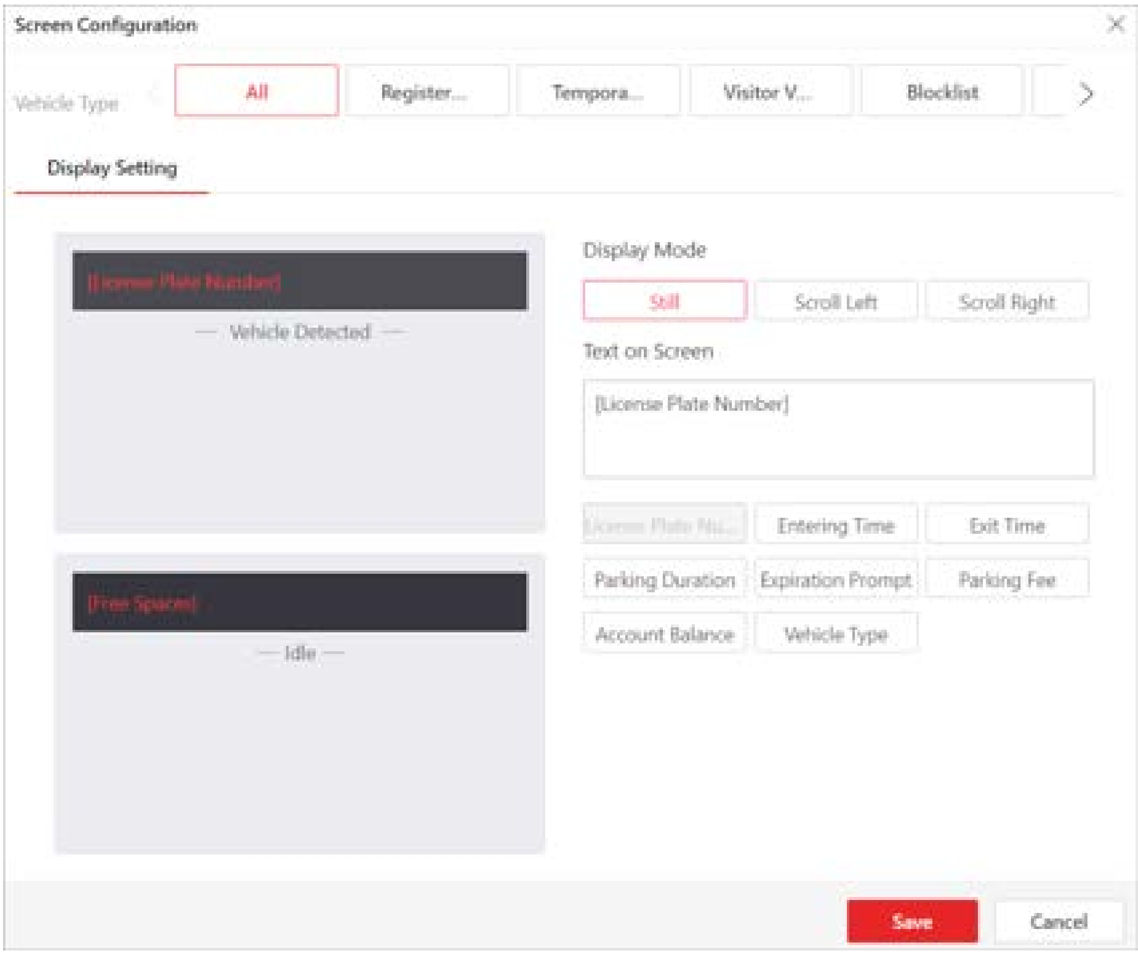


Figure 18-10 Screen Configuration for Entrance/Exit Station's Screen

5. Select a vehicle type.
6. Configure the Vehicle Detected screen.
   1) Click a line to set its **Display Mode**, **Font Color**, and **Alignment**.

   Note

   Font color and text alignment is not configurable for the screen of an entrance/exit station.

   2) Select the information to be displayed on the line from **Text on Screen**.

   Plate No.

   Used for displaying the license plate number recognized by the capture unit. Click to add it to the **Text on Screen** area.

   Free Spaces

   The number of vacant parking spaces in the floor the guidance screen is related to.

Note

If a guidance screen is related to more than one floor, instead of displaying the number of vacant parking spaces of each floor, the total number of vacant parking spaces of all floors will be displayed.

Entering Time

The time when a recognized vehicle enters 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.

Account Balance

The balance in the vehicle owner's account.

3) **Optional:** Configure other lines in the same way.

Note

There is only one line for displaying information on the screen of an entrance/exit station.

7. Configure the Idle screen in the same way you configure the Vehicle Detected screen.

Vacant Parking Spaces in Vehicle List

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.

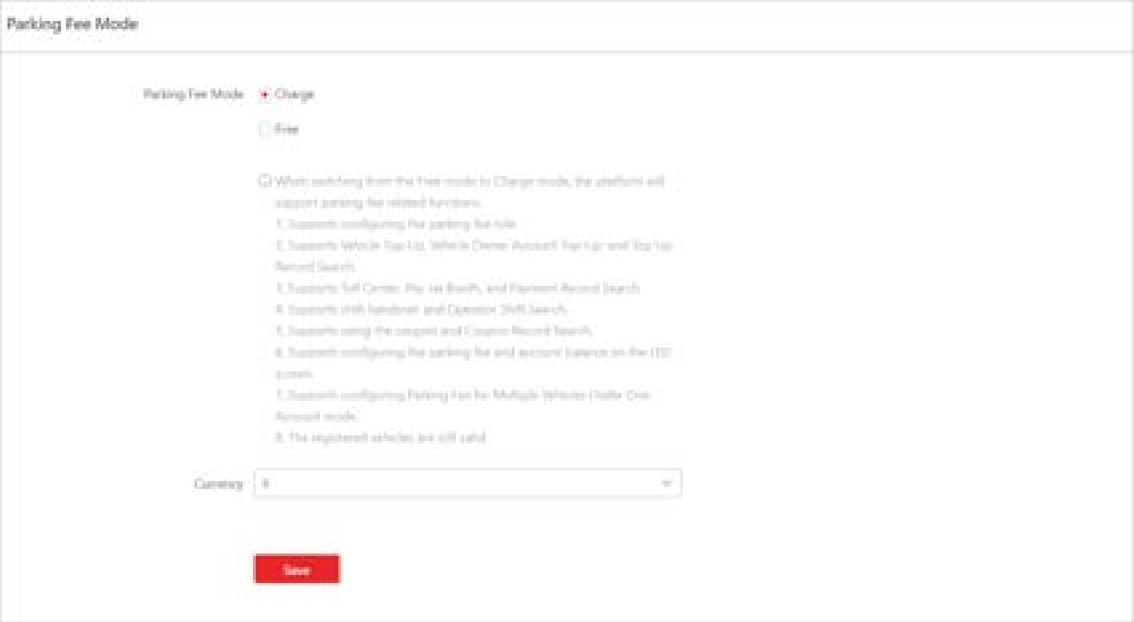
8. Click **Save**.

18.3.5 Set Parking Fee Mode for Parking Lots

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. Go to 🟥 → **All Modules** → **Vehicle** → **Basic Settings** → **Parking Fee Mode** .



Parking Fee Mode

Parking Fee Mode ● Charge

○ Free

When switching from the Free mode to Charge mode, the platform will support parking fee related functions.
1. Supports configuring the parking fee rule.
2. Supports Vehicle Top-Up, Vehicle Owner Account Top-Up and Top-Up Record Search.
3. Supports Toll Center, Pay (at) Booth, and Payment Record Search.
4. Supports shift handover and Operator Shift Search.
5. Supports using the coupons and Coupon Record Search.
6. Supports configuring the parking fee and account balance on the LED screen.
7. Supports configuring Parking Fee for Multiple Vehicles Under One Account mode.
8. The registered vehicles are still valid.

Currency

Figure 18-11 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 will not be able to configure.

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**.

18.4 Manage Entry & Exit Rules for Parking Lots

The entry & exit rule defines how to open the barrier gate when a vehicle is detected at the lane. In the Parking Lot Management module, you can set entry & exit rules for different types of vehicles, including temporary vehicles, registered vehicles, visitor vehicles, and vehicles in list. Besides, 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.

18.4.1 Set Entry & Exit and Deduction Mode

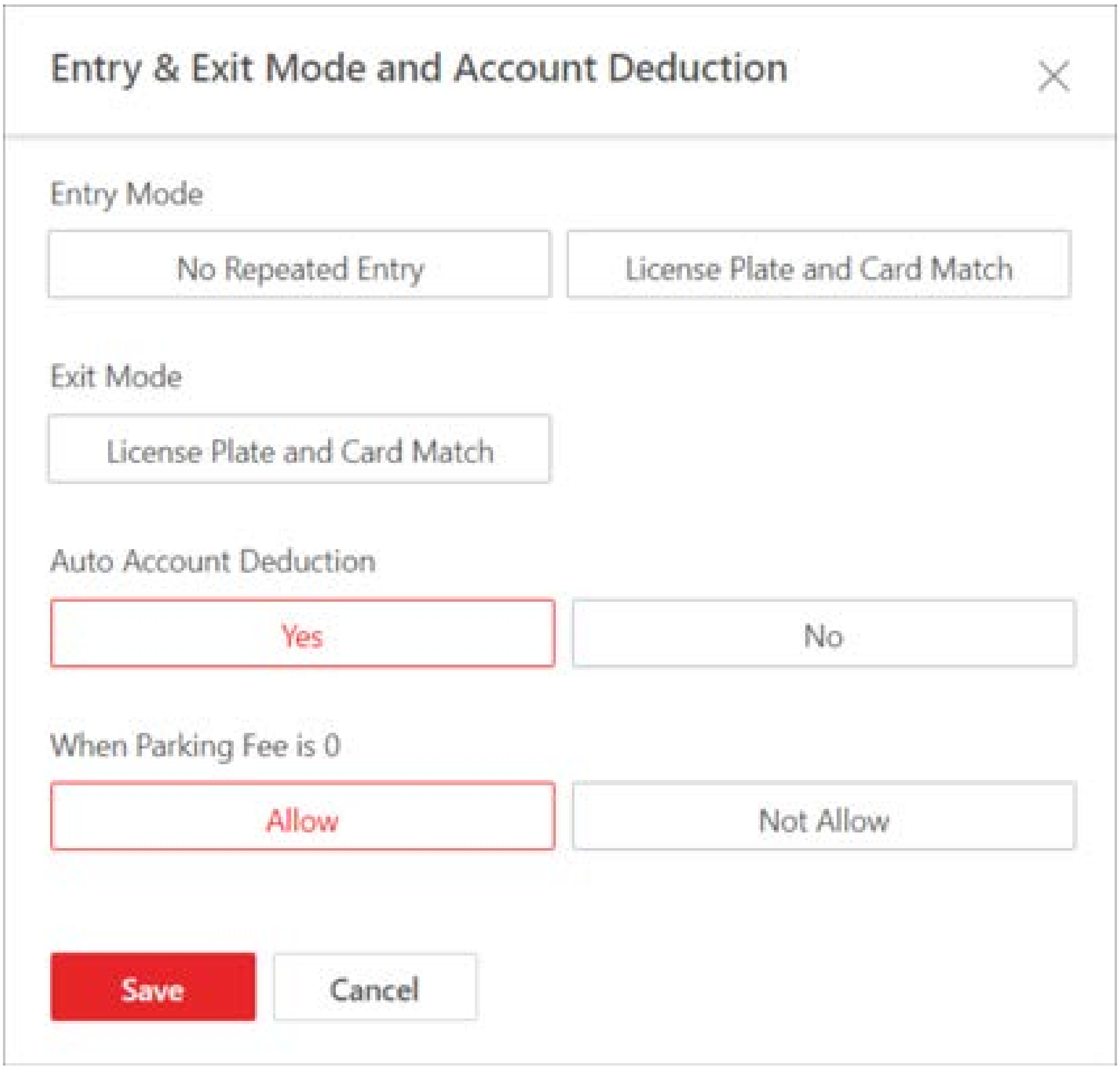
In the Parking Lot Management module, you can set the entry & exit mode and account deduction mode for a parking lot, which can help you to manage the entry and exit of vehicles as well as the payment of parking fee more easily.

Before You Start

Make sure that the parking fee mode has been set to **Charge**.

Steps

1. Go to → **All Modules** → **Vehicle** → **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 Mode and Account Deduction** to open the following panel.



Entry & Exit Mode and Account Deduction

Entry Mode: No Repeated Entry | License Plate and Card Match

Exit Mode: License Plate and Card Match

Auto Account Deduction: [✓ Yes] No

When Parking Fee is 0: [✓ Allow] Not Allow

Figure 18-12 Entry & Exit Mode and Account Deduction

5. Set the mode.

   Entry Mode

   The condition in which a vehicle is allowed to enter.

   Exit Mode

The condition in which a vehicle is allowed to exit.

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**.

18.4.2 Set Entry & Exit Rule for Registered Vehicles

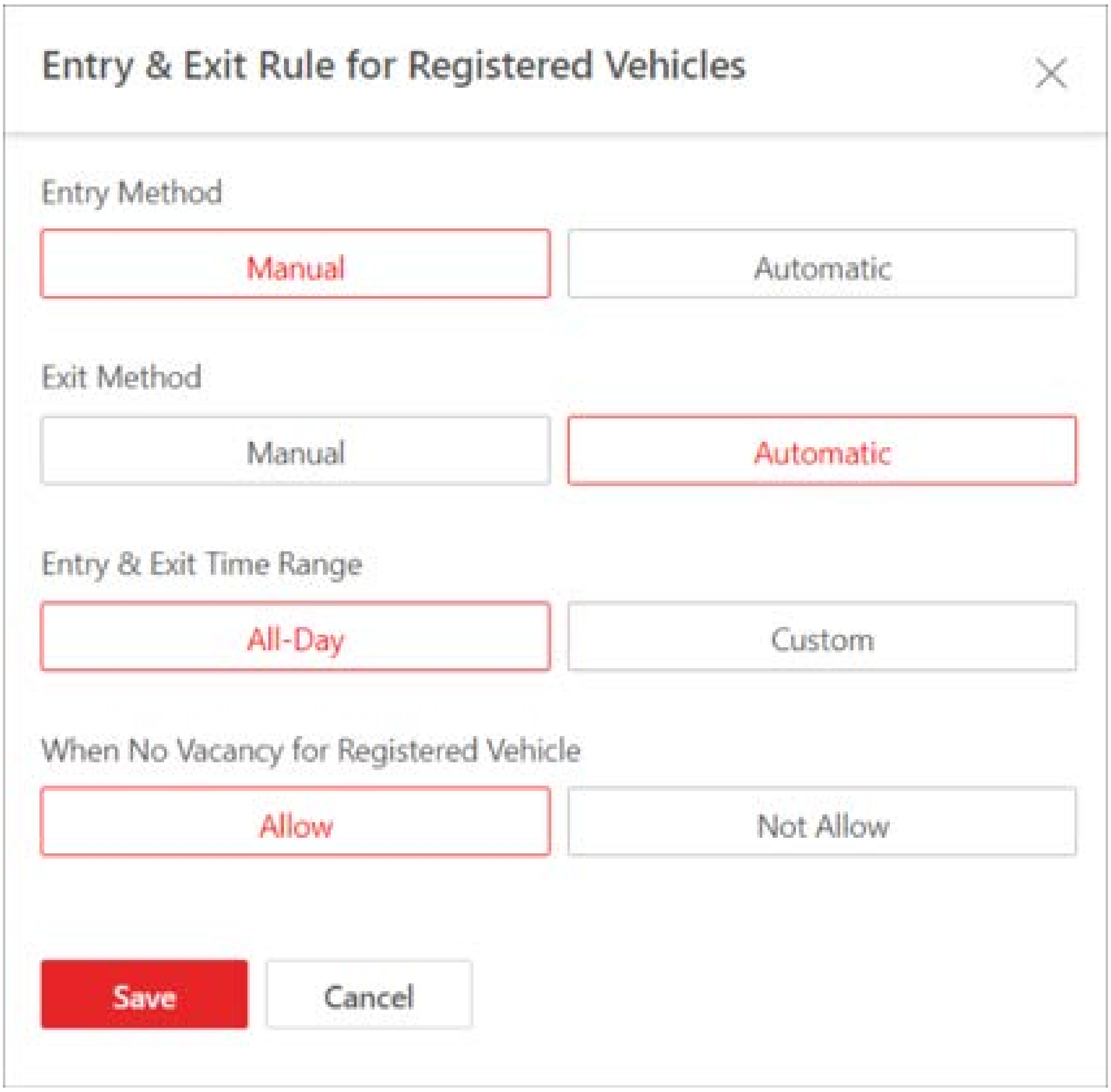
Registered vehicles are the ones that have been added to the platform. In the Parking Lot Management module, you can set the entry & exit rule for registered vehicles, which can help you to manage the entry and exit of them more easily.

Before You Start

Make sure that at least one vehicle has been added to the platform. See ***Add a Registered Vehicle*** or ***Batch Import Registered Vehicles*** for details.

Steps

1. Go to → **All Modules** → **Vehicle** → **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 panel.



Entry & Exit Rule for Registered Vehicles

Entry Method
[✓ Manual] Automatic

Exit Method
Manual [✓ Automatic]

Entry & Exit Time Range
[✓ All-Day] Custom

When No Vacancy for Registered Vehicle
[✓ Allow] Not Allow

Figure 18-13 Entry & Exit Rule for Registered 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 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.

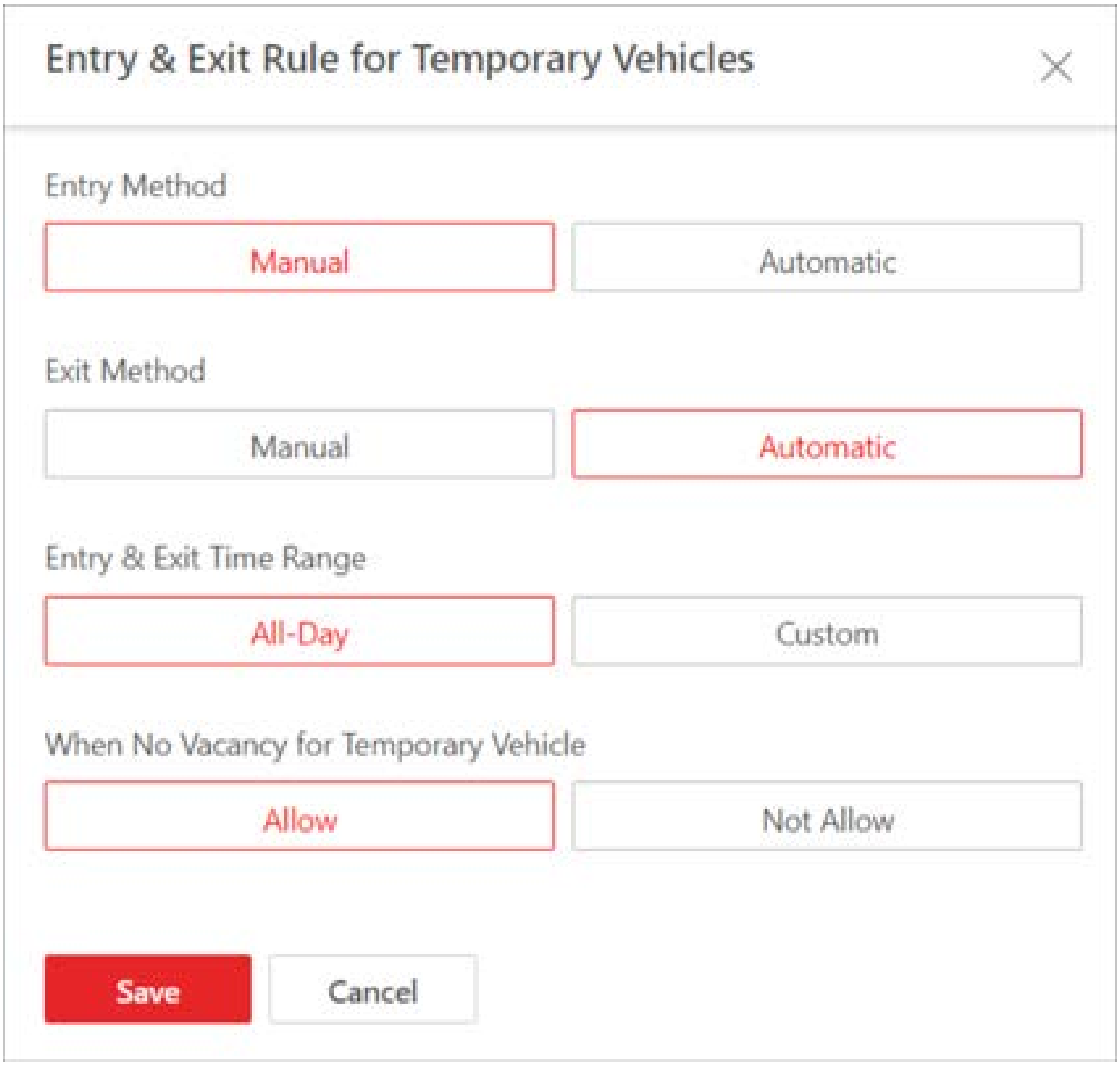
6. Click **Save**.

18.4.3 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. In the Parking Lot Management module, 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. Go to → **All Modules** → **Vehicle** → **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 panel.



Entry & Exit Rule for Temporary Vehicles

Entry Method

[✓ Manual] Automatic

Exit Method

Manual [✓ Automatic]

Entry & Exit Time Range

[✓ All-Day] Custom

When No Vacancy for Temporary Vehicle

[✓ Allow] Not Allow

Figure 18-14 Entry & Exit Rule for Temporary 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 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.

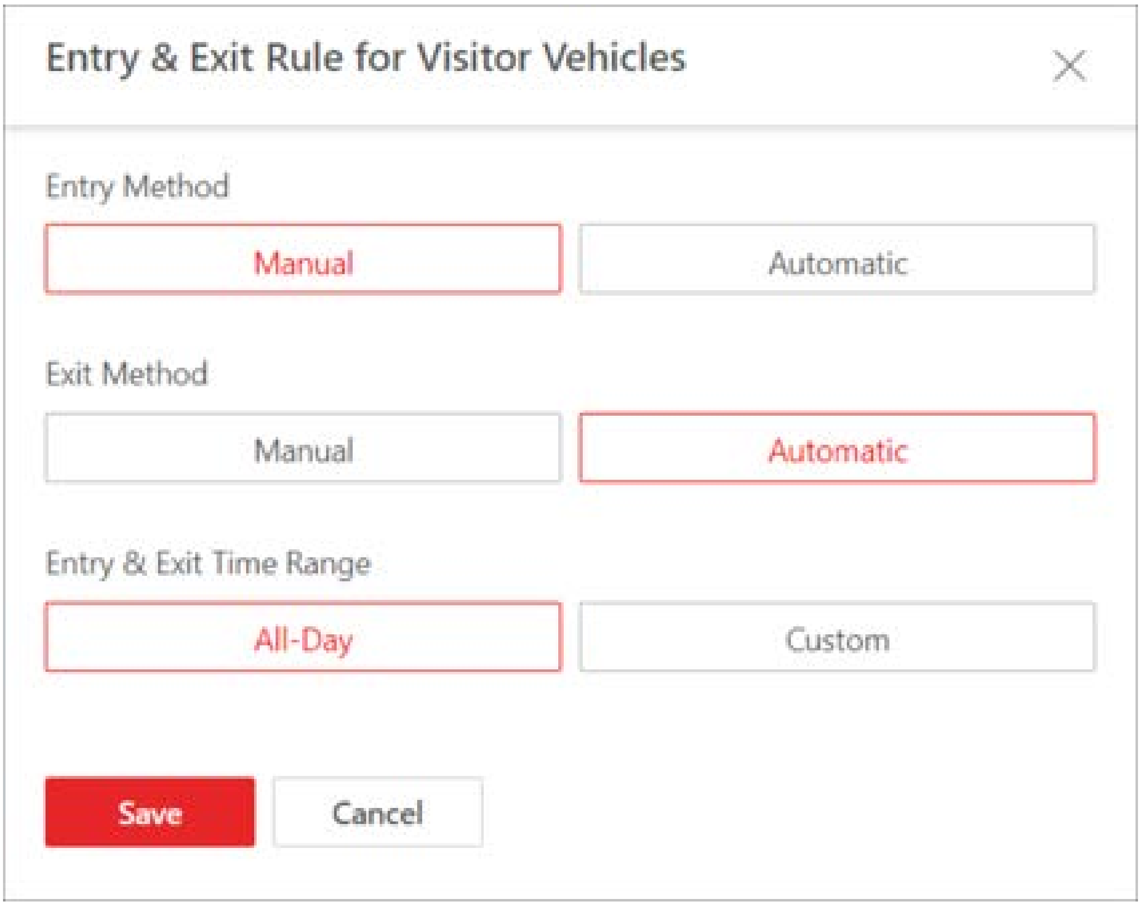
6. Click **Save**.

18.4.4 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. In the Parking Lot Management module, 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. Go to 🟥 → **All Modules** → **Vehicle** → **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 panel.



Entry & Exit Rule for Visitor Vehicles

Entry Method: Manual (selected) / Automatic

Exit Method: Manual / Automatic (selected)

Entry & Exit Time Range: All-Day (selected) / Custom

Figure 18-15 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**.

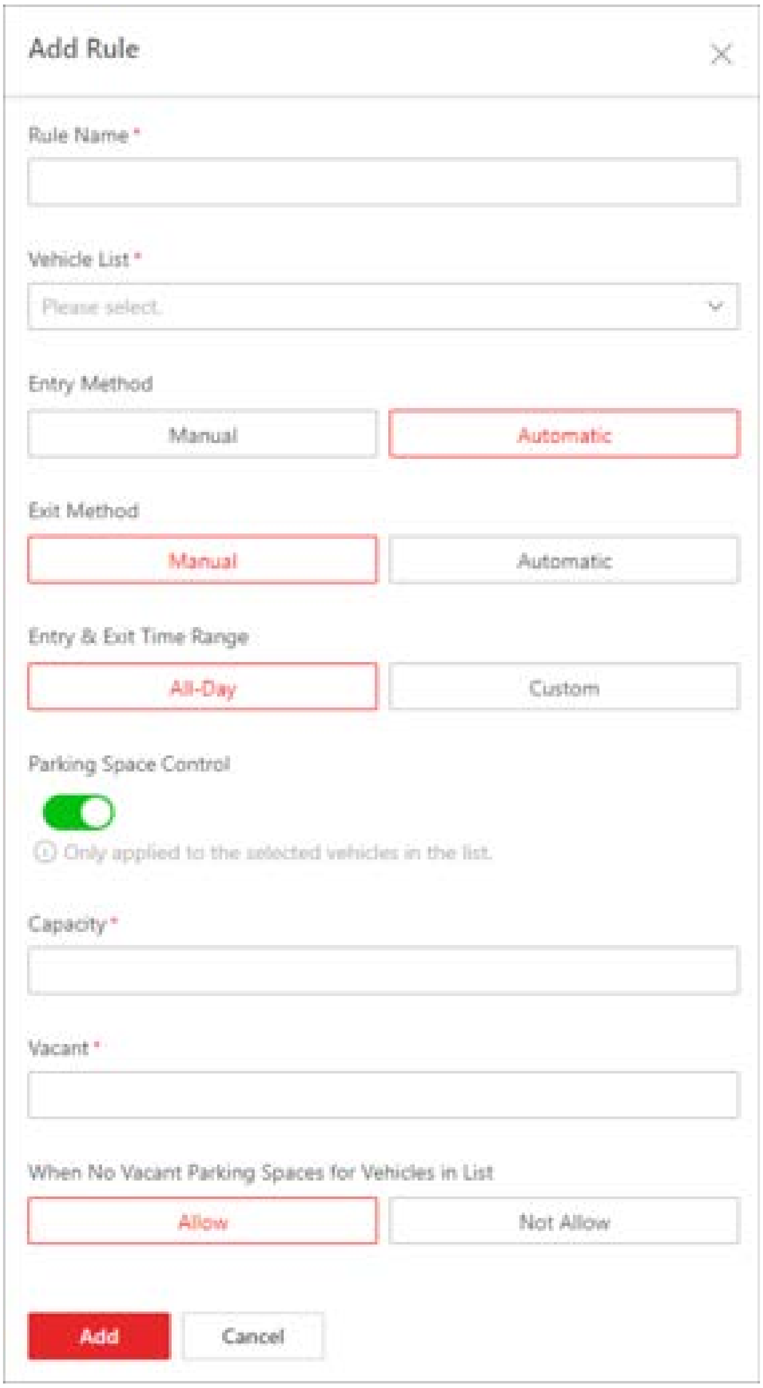
18.4.5 Add Entry & Exit Rule for Vehicles in List

Vehicles in list are the ones that have been added to the platform and managed in the list you created. In the Parking Lot Management module, 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. See ***Add Vehicle List*** for details.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **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 panel.



Add Rule

Rule Name *

Vehicle List *

Please select.

Entry Method

Manual [✓ Automatic]

Exit Method

[✓ Manual] Automatic

Entry & Exit Time Range

[✓ All-Day] Custom

Parking Space Control

Only applied to the selected vehicles in the list.

Capacity *

Vacant *

When No Vacant Parking Spaces for Vehicles in List

[✓ Allow] Not Allow

Figure 18-16 Add Rule

5. Set the rule.

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:** Perform the following operations if needed.

Edit a Rule	Click ✎ to edit a rule.
Delete a Rule	Click 🗑 to delete a rule.

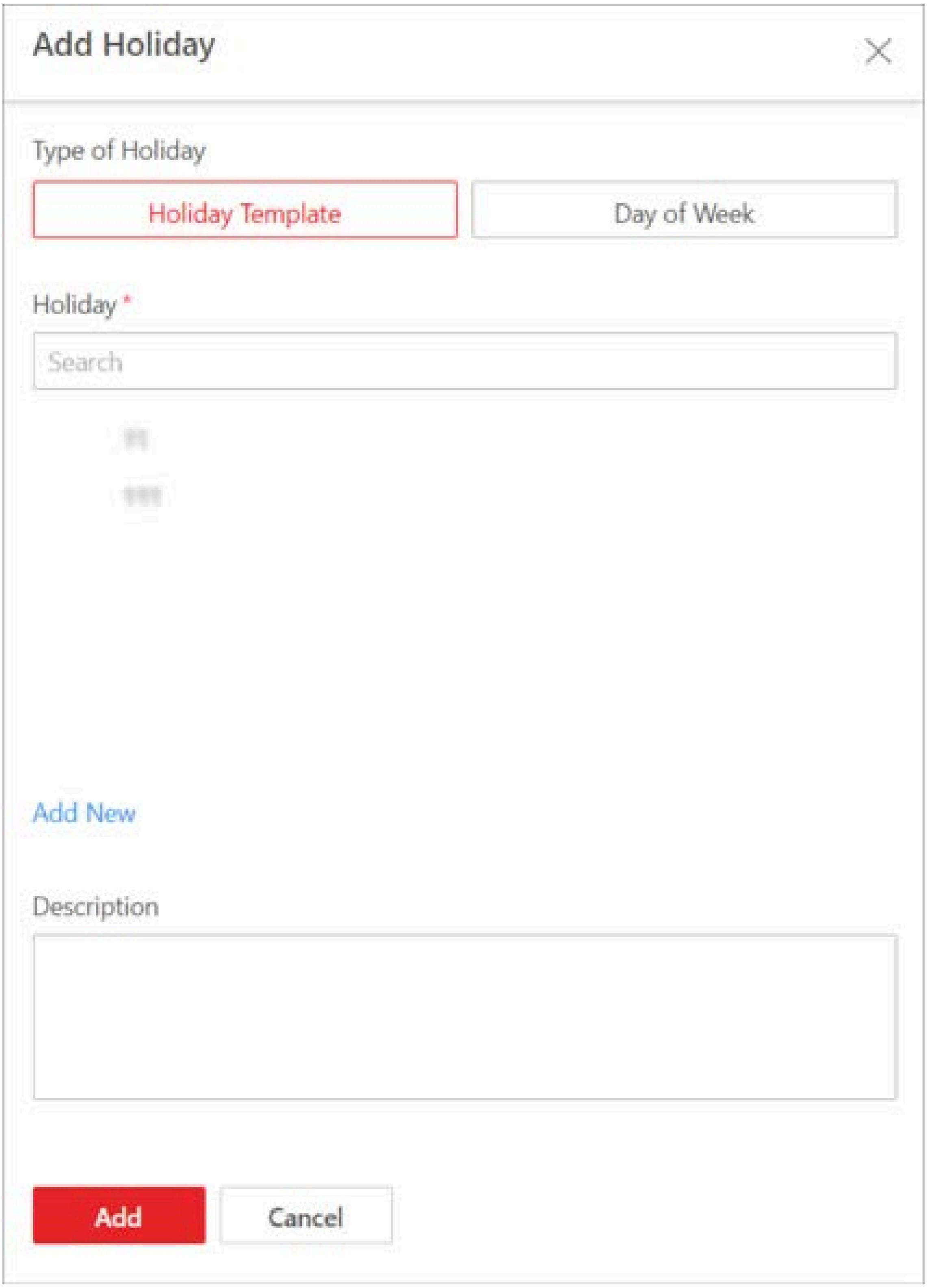
18.4.6 Add Entry & Exit Rule for Holidays

In the Parking Lot Management module, 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. Go to ▦ → **All Modules** → **Vehicle** → **Parking Lot Management** .
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Add** beside **Free Entry & Exit on Holidays** to open the Add Holiday panel.
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**.



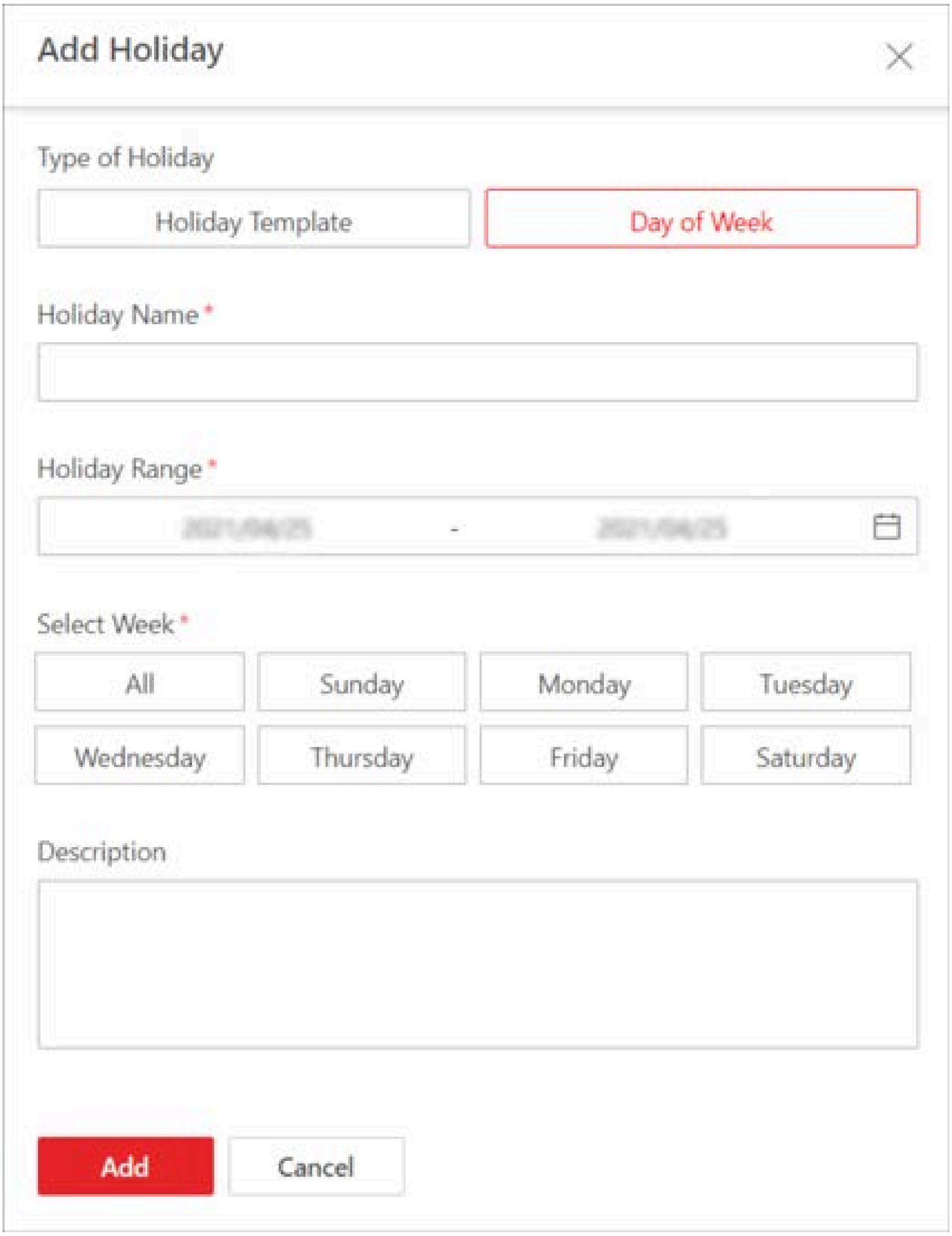
Add Holiday

Type of Holiday

Holiday *

Description

Figure 18-17 Holiday Template



Add Holiday

Type of Holiday

Holiday Template | Day of Week

Holiday Name *

Holiday Range *

2021/04/25 - 2021/04/25

Select Week *

All | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday

Description

Figure 18-18 Day of Week

6. **Optional:** Perform the following operation(s) if needed.

Edit a Rule Click ✎ to edit a rule.

Delete a Rule Click to delete a rule.

18.5 Manage Parking Fee Rules for Parking Lots

In the Parking Lot Management module, 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 ***Set Parking Fee Mode for Parking Lots*** for details.

18.5.1 Add Parking Fee Rule for Temporary Vehicles

In the Parking Lot Management module, you can add parking fee rule for temporary vehicles, which can help you to calculate parking fee more easily.

Before You Start

Make sure that the parking fee mode has been set to **Charge**.

Steps

1. Go to → **All Modules** → **Vehicle** → **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 panel.
5. Create a name for the rule.
6. Select a type of vehicle that the rule is applied to.
7. Select a time unit that the parking fee is charged by and complete relevant 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 parking.

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 New** to add different time ranges and fees.

c. (Optional) Switch on **Daily Max. Fee**, and enter the fee.
d. Enter the fee for the duration beyond the maximum duration allowed.

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 New** 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.

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 New** 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 this rule.
9. Click **Add**.
10. **Optional:** Perform the following operations if needed.

Copy a Rule to Other Parking Lot(s)	Click ⧉ and select the parking lot(s) that the rule is copied to.
Edit a Rule	Click ✎ to edit a rule.
Delete a Rule	Click 🗑 to delete a rule.

18.5.2 Add Parking Fee Rule for Vehicles in List

In the Parking Lot Management module, you can add parking fee rule for vehicles in list, which can help you to calculate parking fee more easily.

Before You Start

- Make sure that the parking fee mode has been set to **Charge**.
- Make sure that at least one vehicle list has been added. See ***Add Vehicle List*** for details.

Steps

1. Go to ■ → **All Modules** → **Vehicle** → **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 panel.
5. Create a name for the rule.
6. Select a type of vehicle that the rule is applied to.
7. Select a time unit that the parking fee is charged by and complete relevant 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 parking.

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 New** to add different time ranges and fees.

c. (Optional) Switch on **Daily Max. Fee**, and enter the fee.
d. Enter the fee for the duration beyond the maximum duration allowed.

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 New** 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.

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 New** 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 this rule.
9. Click **Add**.
10. **Optional:** Perform the following operations if needed.

Copy a Rule to Other Parking Lot(s)	Click ⧉ and select the parking lot(s) that the rule is copied to.
Edit a Rule	Click ✎ to edit a rule.
Delete a Rule	Click 🗑 to delete a rule.

18.5.3 Add Parking Pass Rule

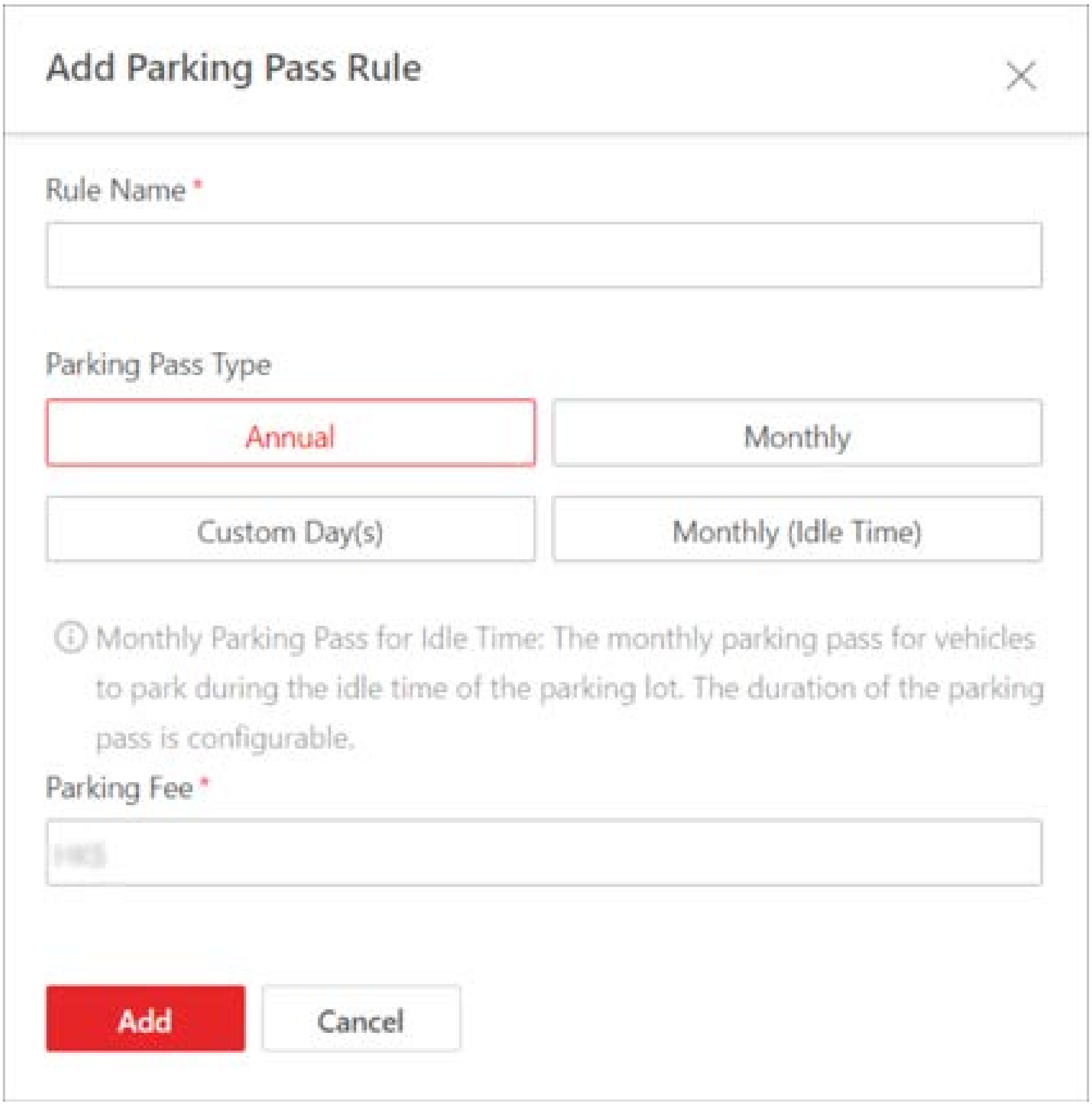
A parking pass charges a certain amount of money. Within the validity period of a parking pass, the vehicle can enter and exit a specific parking lot as a registered vehicle, so that it can park in that parking lot without paying any fee. In the Parking Lot Management module, you can add rule for parking pass.

Before You Start

Make sure that the parking fee mode has been set to **Charge**.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **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 Pass Rule for Registered Vehicle** to enter the Add Parking Pass Rule panel.



Add Parking Pass Rule

Rule Name *

Parking Pass Type

ⓘ Monthly Parking Pass for Idle Time: The monthly parking pass for vehicles to park during the idle time of the parking lot. The duration of the parking pass is configurable.

Parking Fee *

Figure 18-19 Add Parking Pass Rule Panel

5. Create a name for the rule.
6. Select a type for the parking pass and complete relevant 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 (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**.
8. **Optional:** Perform the following operations if needed.

Copy a Rule to Other Parking Lot(s)	Click and select the parking lot(s) that the rule is copied to.
Edit a Rule	Click to edit a rule.
Delete a Rule	Click to delete a rule.

18.5.4 Add Discount Rule

In the Parking Lot Management module, 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**.

Steps

1. Go to → **All Modules** → **Vehicle** → **Parking Lot Management** .
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add Rule** 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.

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.

18.5.5 Add Parking Fee Rule for Abnormal Entry & Exit

In the Parking Lot Management module, you can add parking fee rule for abnormal entry & exit (e.g., a vehicle with an entry record but without an exit record), which can help you to manage abnormal entries and exits more easily.

Before You Start
Make sure that the parking fee mode has been set to **Charge**.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **Parking Lot Management** .
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Add Rule** beside **Parking Fee Rule for Abnormal Parking** to enter the following panel.
5. Create a name for the rule.
6. Enter the parking fee for abnormal entry & exit.
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**.
11. **Optional:** Perform the following operations as needed.

Copy a Rule to Other Parking Lot(s)	Click ⧉ and select the parking lot(s) that the rule is copied to.
Edit a Rule	Click ✎ to edit a rule.
Delete a Rule	Click 🗑 to delete a rule.

18.5.6 Additional Configuration

In the Parking Lot Management module, 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**.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **Parking Lot Management** .
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Parking Fee Rule**.
4. Click **Edit** beside **Additional Configuration** to enter the Additional Configuration panel.
5. Enter the parking duration that is free of charge after paying the parking fee.
6. **Optional:** Switch on **Parking Fee Rule for Multiple Vehicles Under One Account**, and select **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**.

18.6 Manage Vehicle

HikCentral Professional supports adding the information of vehicles to the platform and categorizing the vehicles into different types. The platform also provides ANPR (Automatic Number-Plate Recognition) functions. After adding cameras which support ANPR, the cameras can recognize the license plate number of the detected vehicles. In addition, the platform provides entrance and exit management and it can control the entry and exit of the detected vehicles.

On the Web Client, the administrator can add vehicle information to the platform, categorize the vehicles into different types (including registered vehicles, temporary vehicles, visitor vehicles, and vehicles in list), and set events and alarms to define whether an event or alarm will be triggered when the recognized plate number matches or mismatches with the license plate numbers of the vehicles managed in the platform, or whether an event or alarm will be triggered when the recognized vehicle type matches the specified vehicle type. For entrance and exit control, the administrator can set entry & exit rules for the vehicles managed in the platform to define whether to allow the vehicles to enter or exit the parking lot.

18.6.1 Add Registered Vehicles

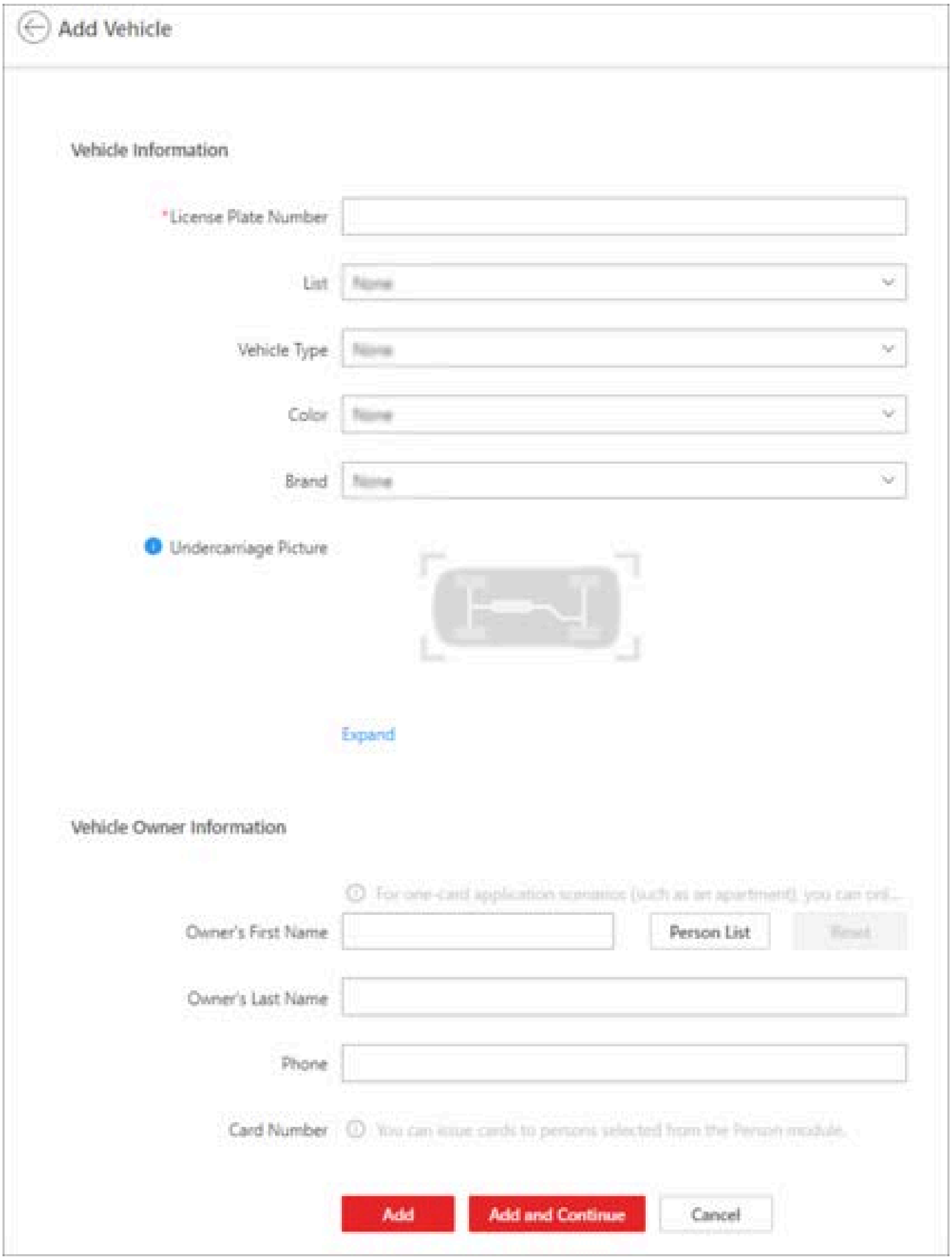
A registered vehicle can park in a specific parking lot without paying any fee. To make a vehicle become a registered vehicle, you need to add its information (including the license plate number, vehicle type, etc) to the platform first, and then you need to relate a parking pass to it, so that the vehicle can enter and exit the parking lot as a registered vehicle. After adding a registered vehicle, you can set entry & exit rule and parking fee rule for it.

Add a Registered Vehicle

In the Vehicle and Card Management module, you can add the information of one vehicle to the platform as a registered vehicle at one time.

Steps

1. Go to 🟥 → **All Modules** → **Vehicle** → **Vehicle and Card Management** → **Registered Vehicle** → **Vehicle** .
2. Click **Add** to enter the Add Vehicle page.



Add Vehicle

Vehicle Information

*License Plate Number

List: None

Vehicle Type: None

Color: None

Brand: None

Undercarriage Picture

Expand

Vehicle Owner Information

For one-card application scenarios (such as an apartment), you can onl...

Owner's First Name

Owner's Last Name

Phone

Card Number: You can issue cards to persons selected from the Person module.

Figure 18-22 Add Vehicle Page

3. Set vehicle information.

1) Enter the license plate number.

2) **Optional:** Select the list that the vehicle is added to from the drop-down list.

Note

If you have not added any vehicle list to the platform, you can click **Add New** to create one.

3) **Optional:** Select the type, color, and brand of the vehicle from the drop-down list.
4) **Optional:** Click **Expand** and enter the custom vehicle information.
5) **Optional:** Upload an undercarriage picture for this vehicle.
   a. Move the cursor to the image area and click **Upload**.
   b. In the pop-up panel, select the undercarriage picture to upload it.

   After uploading an undercarriage picture, you can view both the current vehicle's captured undercarriage picture and this uploaded picture for comparison on the Control Client.

4. **Optional:** Enter the owner's first name, last name, and phone number, or select a person from the person list as the vehicle owner through the following steps.
   1) Click **Person List** to open the following panel.

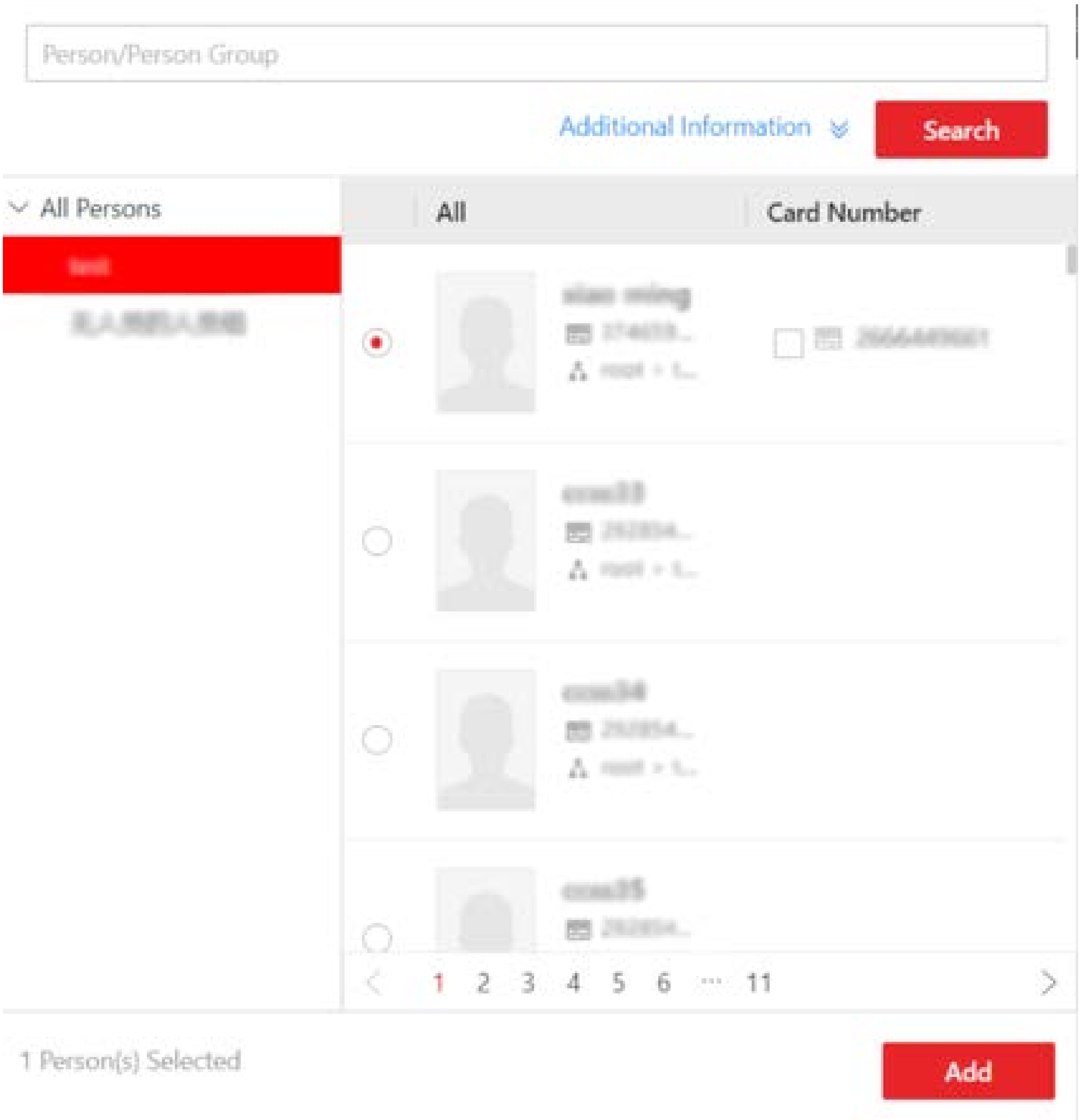


Figure 18-23 Add Person in Person List as Vehicle Owner

2) Select a person list from the left list.

The person(s) in the list will be displayed.

3) Select a person from the right list.

Note

To select a person, you can also search for a person by entering the person's name. You can click **Additional Information** to enter the person's personal information so that the search result will be more accurate.

4) **Optional:** Select a card number for the owner from the Card Number list. The owner can swipe the selected card on the access control device or video intercom device when entering or exiting the parking lot.

5) Click **Add**.

5. Finish adding the vehicle information.
   - Click **Add** to add the vehicle information.

     Note

     Only the vehicle with a parking pass can enter and exit the parking lot as a registered vehicle. Therefore, on the pop-up panel, you need to click **Parking Pass Top-Up** to add a parking pass to the vehicle. Or you can click **Return to Vehicle List** and add a parking pass to the vehicle in Top-Up Management module later, see ***Top Up for Vehicles*** for more details.
   - Click **Add and Continue** to save the settings and continue to add other vehicles.

   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 a new one.
6. **Optional:** Perform the following operations after adding the vehicle information.

Edit Vehicle Information	Click the plate number in License Plate Number column to edit the vehicle information
Delete Vehicle Information	Check the vehicle information and click **Delete** to delete the selected vehicle information.
Delete All Vehicle Information	Click ⌄ beside the **Delete** icon, and click **Delete All** to delete all vehicle information in the current vehicle list.
Delete Expired Vehicle Information	Click **Delete Expired Vehicle** to delete all expired vehicle information from the current vehicle list.
Export Vehicle Information	Click **Export All** to save the vehicle information of the list (CSV file) to your PC, which can be imported to other vehicle list. Click ▽ to filter vehicles and then click **Export All** to export the information of filtered vehicles to the PC.
Search for Vehicle(s)	Click ▽ and set search conditions to search for specific vehicle(s).

Batch Import Registered Vehicles

In the Vehicle and Card Management module, you can import the information of multiple vehicles into the platform as registered vehicles at one time.

Steps

1. Go to ■ → **All Modules** → **Vehicle** → **Vehicle and Card Management** → **Registered Vehicle** → **Vehicle** .

2. Click **Import**.

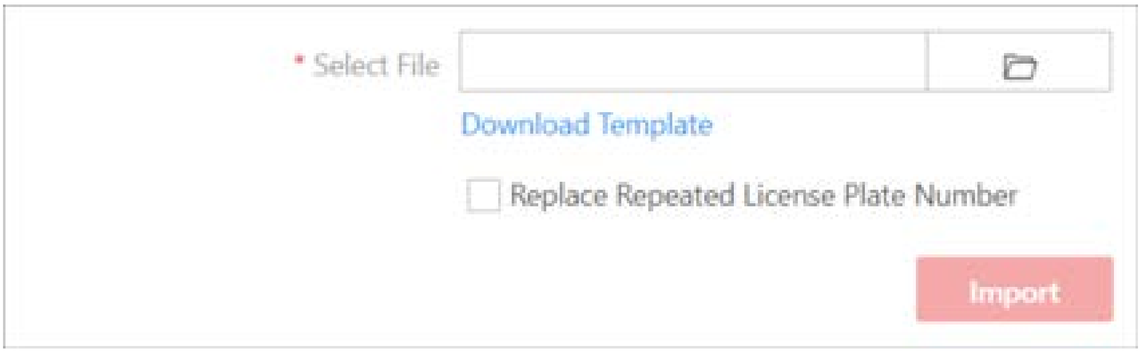


Figure 18-24 Import File

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**.
8. **Optional:** Perform the following operations after importing the vehicle information.

Edit Vehicle Information	Click the plate number in License Plate Number column to edit the vehicle information.
Delete Vehicle Information	Check the vehicle information and click **Delete** to delete the selected vehicle information.
Delete All Vehicle Information	Click ⌄ beside the **Delete** icon, and click **Delete All** to delete all vehicle information from the current vehicle list.
Delete Expired Vehicle Information	Click **Delete Expired Vehicle** to delete all expired vehicle information from the current vehicle list.
Export Vehicle Information	Click **Export All** to save the vehicle information of the list (CSV file) to your PC, which can be imported to other vehicle list. Click ▽ to filter vehicles and then click **Export All** to export the information of filtered vehicles to the PC.
Search for Vehicle(s)	Click ▽ and set search conditions to search for specific vehicle(s).

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 the information of multiple vehicles into the platform, you need to relate a parking pass to each of them in the Top-Up Management module later. See ***Top Up for Vehicles*** for more details.

18.6.2 Add Vehicle List

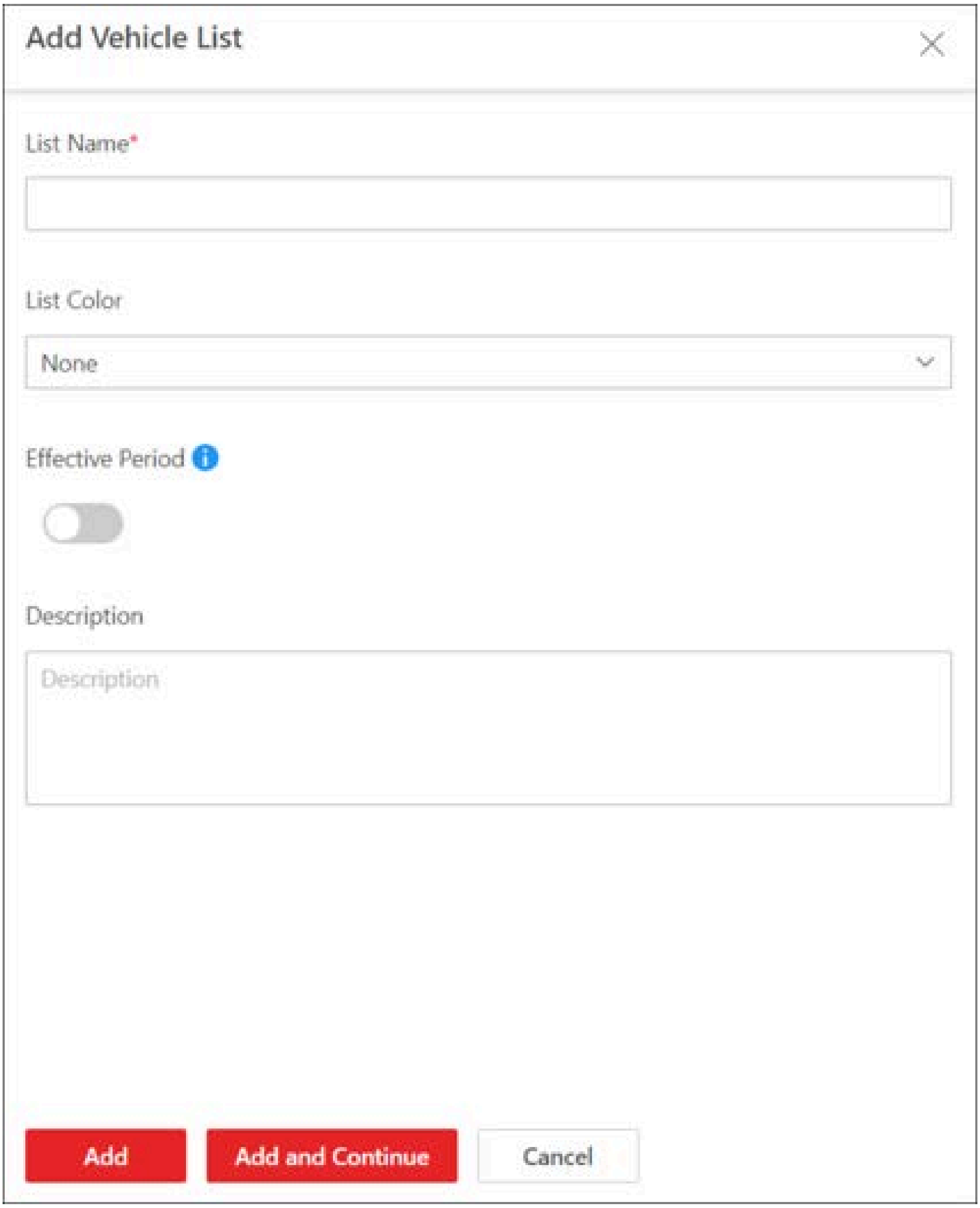
A vehicle list can group multiple vehicles so that you can manage them more easily. In the Vehicle and Card Management module, you can add vehicle lists to the platform.

Steps

Note

Up to 100 vehicle lists can be added.

1. Go to 🟥 → **All Modules** → **Vehicle** → **Vehicle and Card Management** → **List Management** .
2. On the top left, click + to enter the Add Vehicle List panel.


Add Vehicle List

List Name*

List Color

None

Effective Period

Description

Description

Figure 18-25 Add Vehicle List Page

3. Create a name for the vehicle list.
4. **Optional:** Select a color for the vehicle list.

Note

You can use different colors to mark different types of vehicle lists.

5. **Optional:** Switch on **Effective Period** and set the effective period for the vehicle list.

Note

- Vehicles in the list will not be allowed to enter the parking lot after the vehicle list expires.
- When you are adding 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 with that of the vehicle list.

6. **Optional:** Enter a description of the vehicle list if needed.
7. Click **Add** to add the vehicle list, or click **Add and Continue** to add the current vehicle list and start adding another one.
8. **Optional:** Perform the following operations if needed.

Note

You need to go to 🟥 → **All Modules** → **Account and Security** → **Roles** to select or create a role and then select vehicle list(s) allowing for further management by the role. See ***Add Role*** for details on permission settings.

Edit Vehicle List
Select a vehicle list and click ✎ to edit it.

Delete Vehicle List
Select a vehicle list and click 🗑 to delete it.

Export Vehicle List
Select a vehicle list and click **Export** to export it to the PC.

Add Vehicle(s) to Vehicle List
Select a vehicle list and click **Add** to add vehicle(s) to it.

Note

You can search for vehicles by entering the custom vehicle information. See ***Customize Vehicle Information*** for more details.

Remove Vehicle(s) from Vehicle List
Select a vehicle list, check vehicle(s), and click **Delete** to remove them from the current list.

18.6.3 Add Vehicle to Blocklist

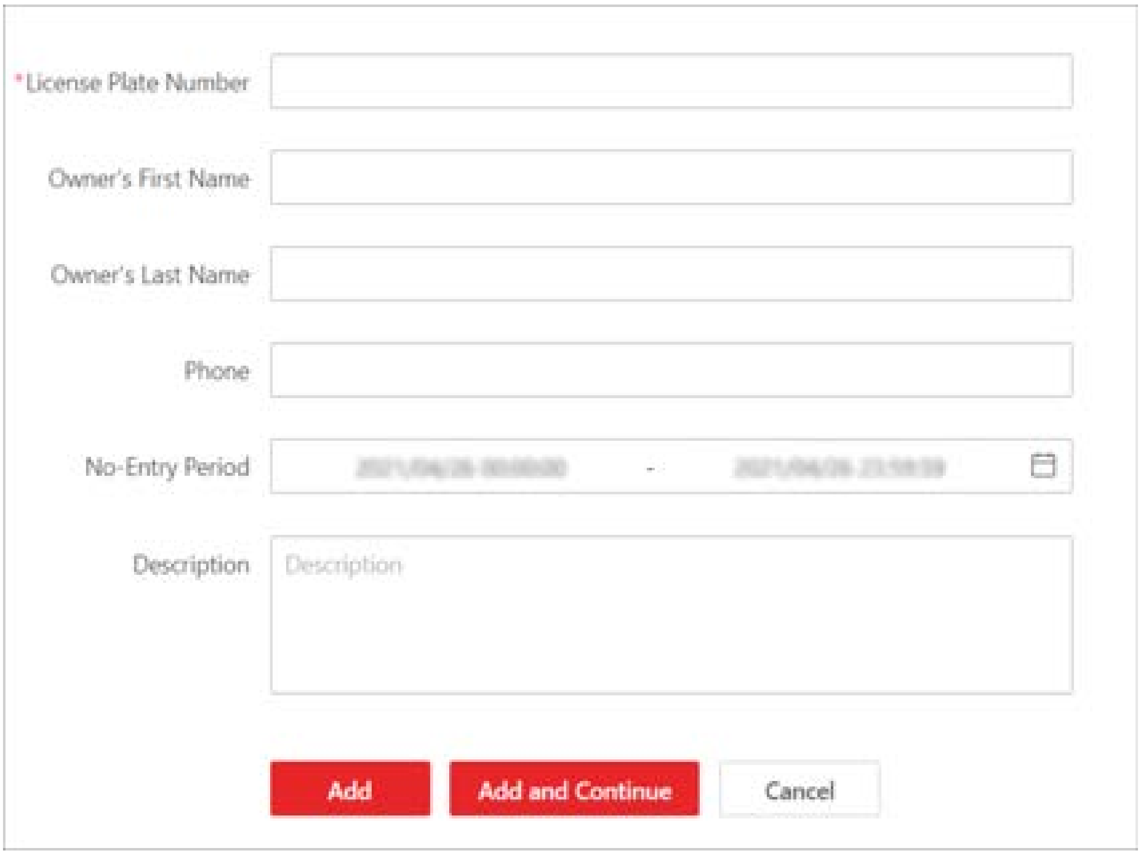
The vehicles added to the blocklist cannot enter the parking lot as its license plate number will be recognized at the lane. When adding a vehicle to the blocklist, the administrator can set a certain period during which the vehicle is not allowed to enter the parking lot. The vehicles can be added to the blocklist one by one or in a batch.

Add a Vehicle to Blocklist

In the Vehicle and Card Management module, you can add one vehicle to the blocklist at one time. Once added, the vehicle cannot enter the parking lot during the period you set.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **Vehicle and Card Management** → **Blocklist** .
2. Click **Add** to enter the following panel.



*License Plate Number

Owner's First Name

Owner's Last Name

Phone

No-Entry Period: 2021/04/26 00:00:00 - 2021/04/26 23:59:59

Description: Description

Figure 18-26 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.
8. **Optional:** Perform the following operations if needed.

Remove Vehicle(s) from Blocklist	Check vehicle(s) and click **Delete** to remove the vehicle(s) from the blocklist one by one or in a batch.

Export Vehicle Information	Check vehicle(s) and click **Export All** to save the information of the vehicle(s) to your PC.

Batch Import Vehicles to Blocklist

In the Vehicle and Card Management module, 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. Go to ▦ → **All Modules** → **Vehicle** → **Vehicle and Card Management** → **Blocklist** .
2. Click **Import**.

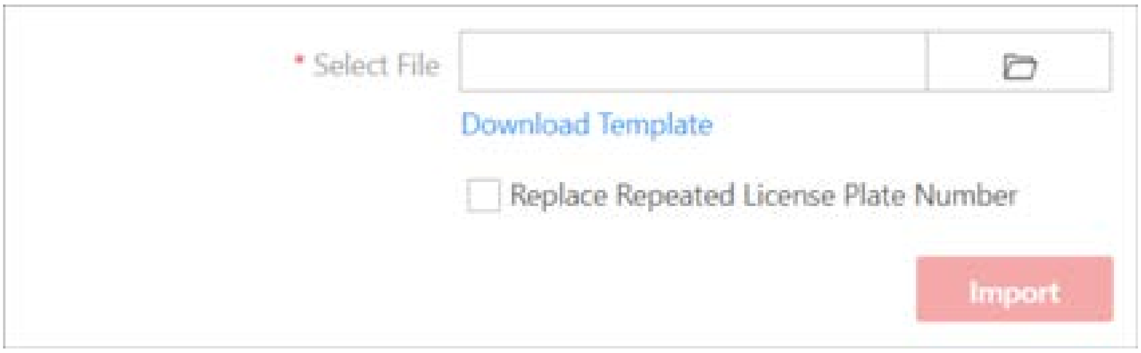


Figure 18-27 Import File

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**.
7. **Optional:** Perform the following operations if needed.

Remove Vehicle(s) from Blocklist	Check vehicle(s) and click **Delete** to remove the vehicle(s) from the blocklist one by one or in a batch.
Export Vehicle Information	Check vehicle(s) and click **Export All** to save the information of the vehicle(s) to your PC.

18.6.4 Issue Temporary Cards

In the Vehicle and Card Management module, 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. Go to ▦ → **All Modules** → **Vehicle** → **Vehicle and Card Management** → **Temporary Card** .

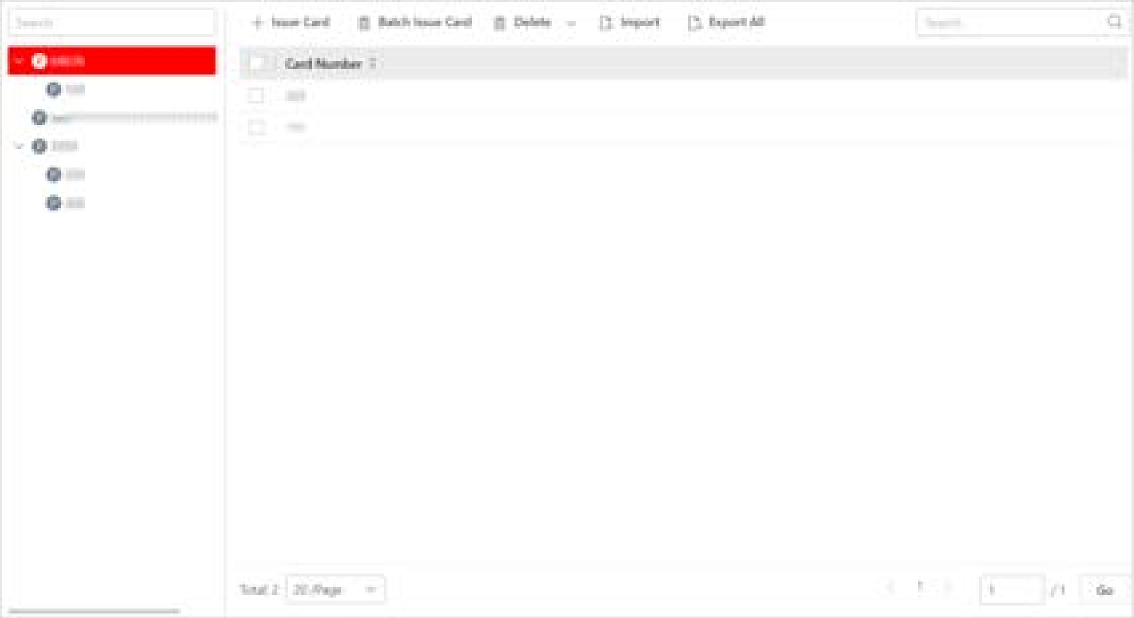


Figure 18-28 Issue Temporary Card Page

2. Select a parking lot from the left list.
3. Click **Issue Card** to open the Issue Card panel.

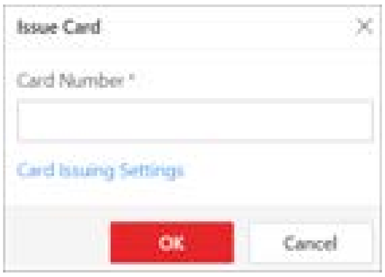


Figure 18-29 Issue Card Panel

4. Enter the card number.
5. **Optional:** Click **Card Issuing Settings** to set card issuing parameters. See ***Set Card Issuing Parameters*** for more details.
6. Click **OK**.

   The card will be added to the selected parking lot.
7. **Optional:** Perform the following operations if needed.

Delete Selected Card(s)	Check the temporary card(s) and click **Delete** to delete the selected card(s).

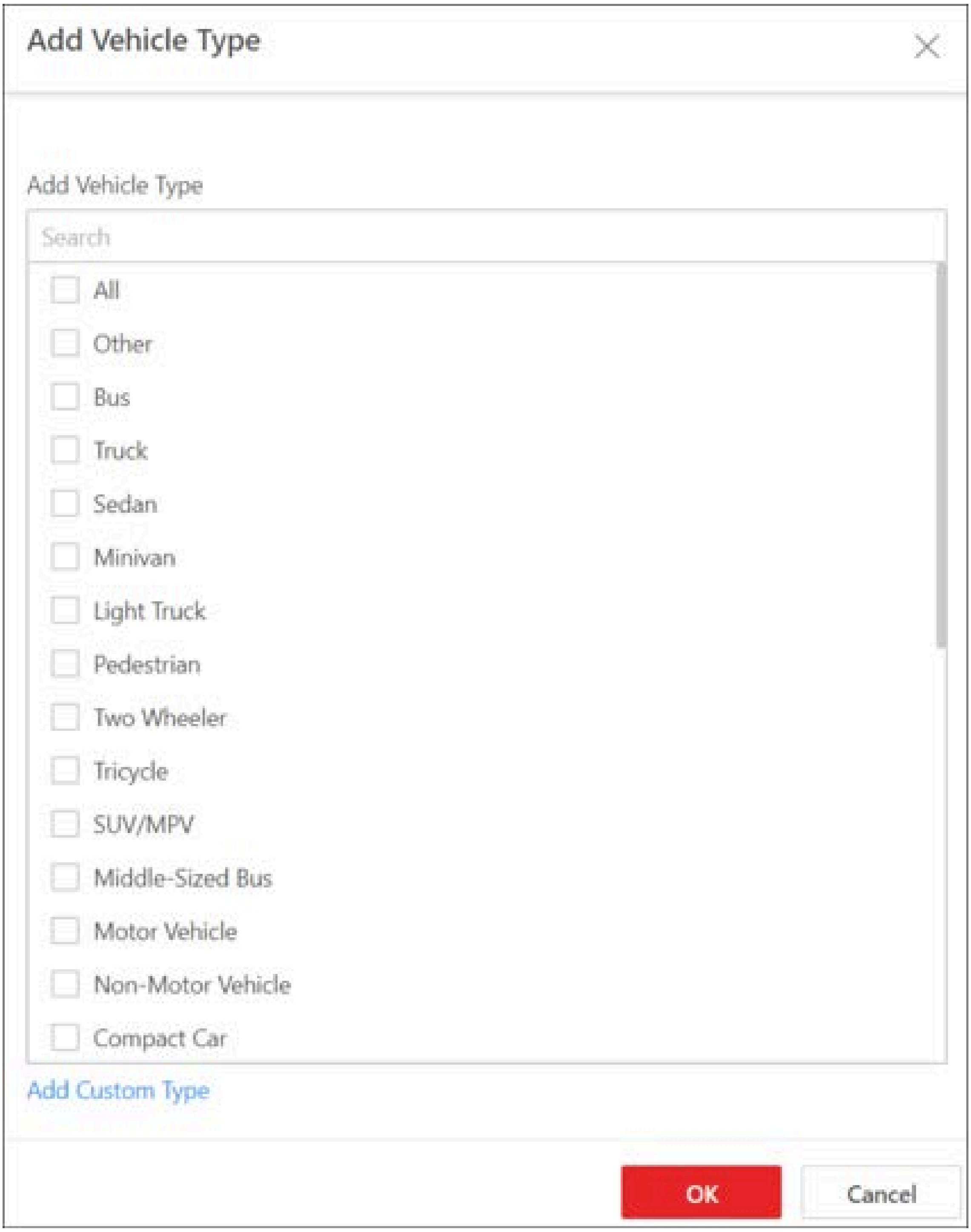
Delete All Cards	Click ⌄ beside **Delete**, and click **Delete All** to delete all temporary cards in the list.
Export Temporary Card Information	Click **Export All** to save the information of the card(s) to your PC.

18.6.5 Customize Vehicle Information

You can customize different items of vehicle information (such as vehicle model) which are not predefined in the basic information. The custom vehicle information can help to recognize vehicles or search for vehicles more accurately.

Steps

1. Go to ■ → **All Modules** → **Vehicle** → **Basic Settings** → **Customize Vehicle Information** .
2. Add vehicle type.
   1) Click **Add** in Vehicle Type area to enter the following panel.



Add Vehicle Type

Add Vehicle Type

Search

□ All

□ Other

□ Bus

□ Truck

□ Sedan

□ Minivan

□ Light Truck

□ Pedestrian

□ Two Wheeler

□ Tricycle

□ SUV/MPV

□ Middle-Sized Bus

□ Motor Vehicle

□ Non-Motor Vehicle

□ Compact Car

Figure 18-30 Add Vehicle Type Panel

2) Check vehicle type(s) in the list.

Note

If you cannot find the vehicle type you want in the list, you can click **Add Custom Type** to customize a vehicle type.

3) Click **OK**.

3. Add custom information.

1) Click **Add** in Custom Information area to enter the following panel.

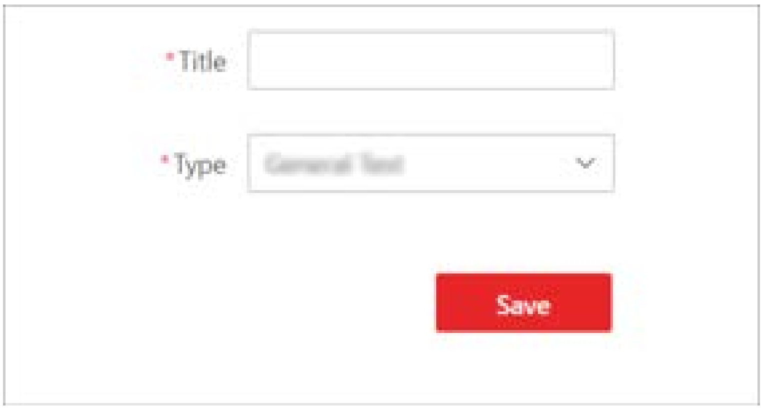


Figure 18-31 Customize Information Panel

2) Create a title for the information.

3) Select an information type from the drop-down list.

Note

The custom information can be used as filtering conditions when you are searching for specific vehicle(s).

General Text

1 to 32 characters are allowed except certain special characters.

Number

Only 1 to 32 digits are allowed.

Date

Select a data from the calendar.

Single Selection

You need to set options for the information. When adding a vehicle, you can select from the options.

4) Click **Save**.

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

Delete Vehicle Type	Click 🗑 to delete a vehicle type.
Edit Custom Information	Click ✎ to edit the custom information.
Delete Custom Information	Click 🗑 to delete the custom information.

18.7 Top Up for Vehicles

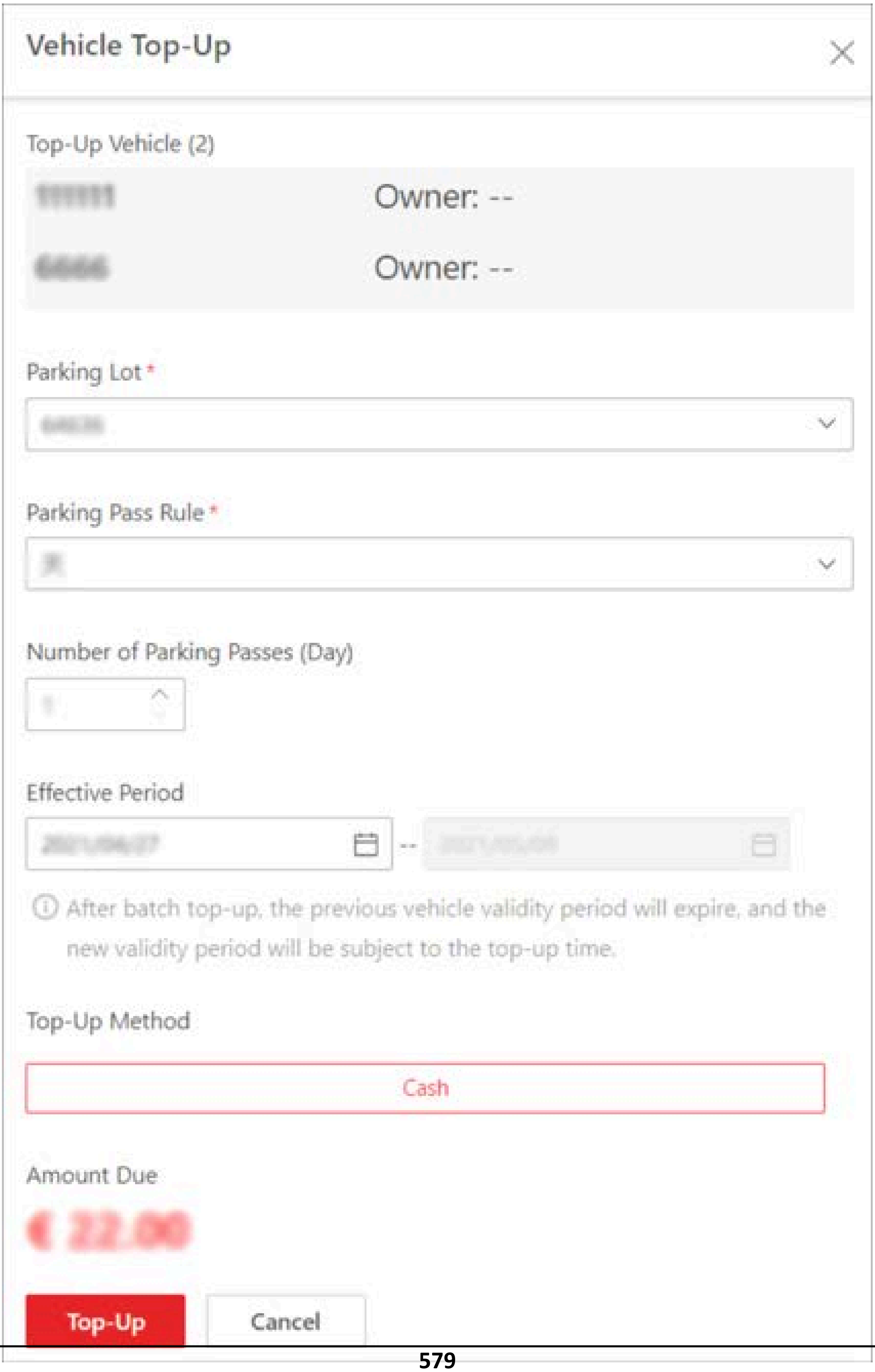
In the Top-Up Management module, you can top up the parking pass for vehicles.

Before You Start

Make sure that you have added parking pass rule(s) to the platform. See ***Add Parking Pass Rule*** for more details.

Steps

1. Go to 🟥 → **All Modules** → **Vehicle** → **Top-Up Management** .
2. Check one or multiple vehicles in the list.
3. In the upper-left corner, click **Top-Up**.



Vehicle Top-Up

Top-Up Vehicle (2)

111111 Owner: --

6666 Owner: --

Parking Lot *

[illegible]

Parking Pass Rule *

[illegible]

Number of Parking Passes (Day)

1

Effective Period

2021/04/27 -- [illegible]

After batch top-up, the previous vehicle validity period will expire, and the new validity period will be subject to the top-up time.

Top-Up Method

Cash

Amount Due

€ 22.00

Figure 18-32 Vehicle Top-Up Window

4. Select a parking lot for the vehicle(s) to park.
5. Select a parking pass rule from the drop-down list.

   Custom Day(s)

   The parking pass is valid during the day(s) you set.

   Monthly

   The parking pass is valid for one month.

   Yearly

   The parking pass is valid for one year.
6. Select the number of parking passes.

   Example

   If you select **Yearly** as the parking pass rule and set the number of parking passes to 2, 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 of the parking pass, and the end date will be automatically calculated by the platform according to the parking pass rule you set.
8. Select the top-up method.

   Note

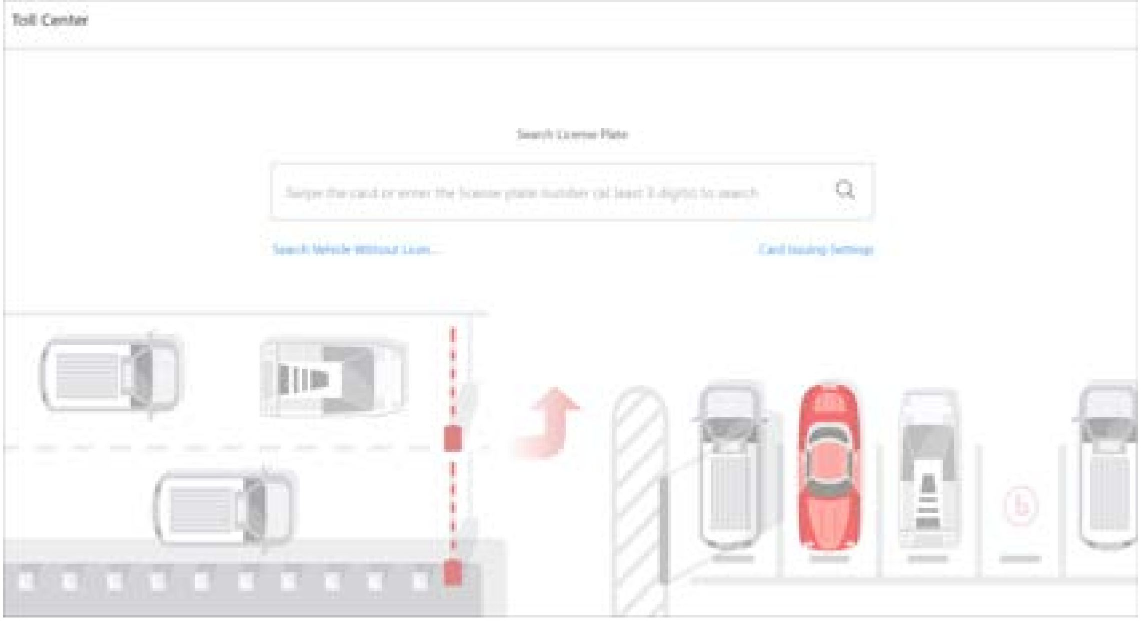
   Currently, the platform only support topping up in cash, so **Cash** is automatically selected. And the amount due will be automatically calculated according to the parking pass rule and number of parking passes you set.
9. Click **Top-Up**.

18.8 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, parking fee, etc. Once all the information is confirmed, the vehicle owner can pay the parking fee in the toll center.

Steps

1. Go to 🟥 → **All Modules** → **Vehicle** → **Toll Center** .



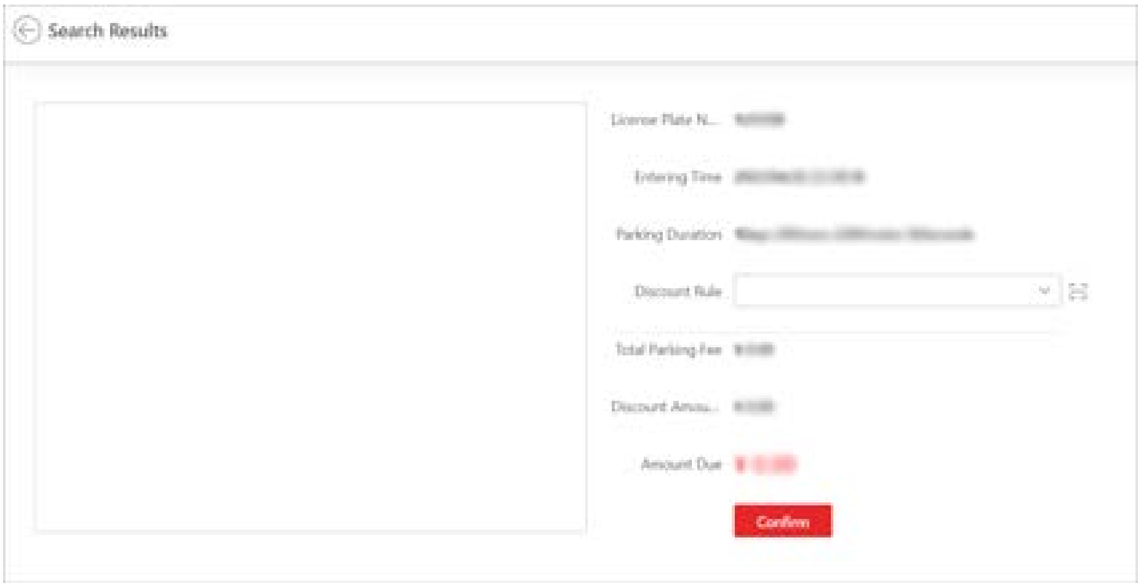
Toll Center

Search License Plate

Swipe the card or enter the license plate number (at least 3 digits) to search

Figure 18-33 Toll Center Page

2. Swipe the temporary card or enter the license plate number to search for a specific vehicle.
   - If the vehicle's license plate is not captured and recorded, you can click **Search Vehicle Without License Plate No.**, and select the target vehicle from the displayed picture(s).
   - If you choose to swipe the temporary card, you can click **Card Issuing Settings** to set card issuing parameters. See ***Set Card Issuing Parameters*** for more details.



Search Results

License Plate N... [illegible]

Entering Time [illegible]

Parking Duration [illegible]

Discount Rule

Total Parking Fee [illegible]

Discount Amou... [illegible]

Amount Due [illegible]

Figure 18-34 Search Result Page

3. Set the discount rule.
   - 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 panel, click **Print Receipt** to print the receipt.

18.9 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 guidance screen. The guidance terminal can relate multiple parking cameras for management, and the guidance 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.

18.9.1 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 guidance screens, configuring the types of parking spaces.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **Parking Guidance Configuration** .

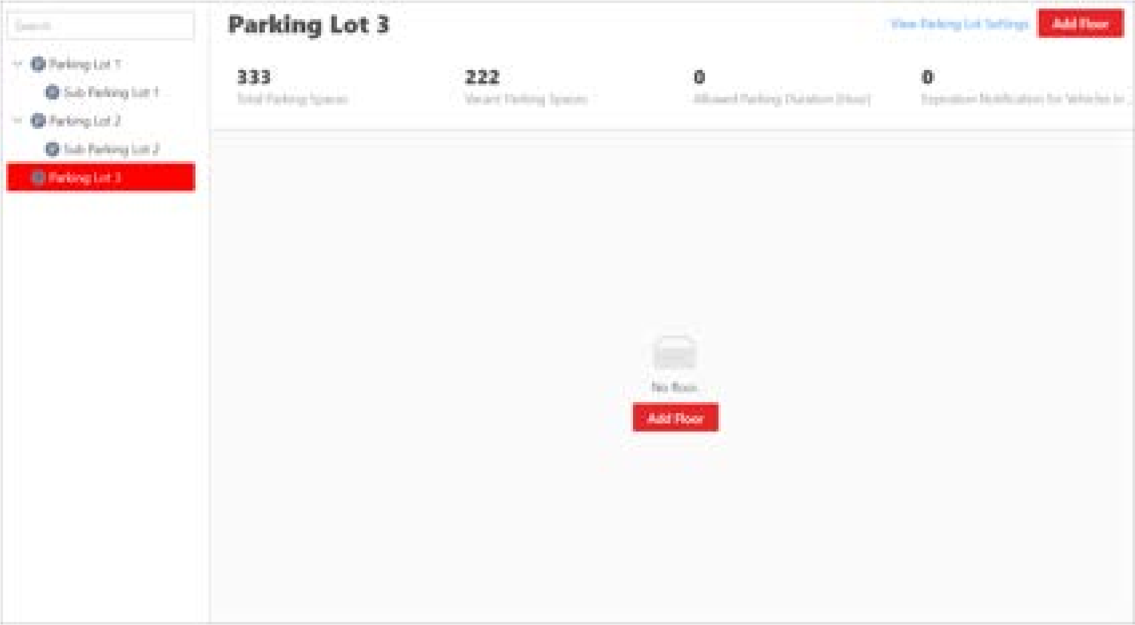


Figure 18-35 Add Floor Page

2. Select a parking lot from the left list.
3. Click **Add Floor**.

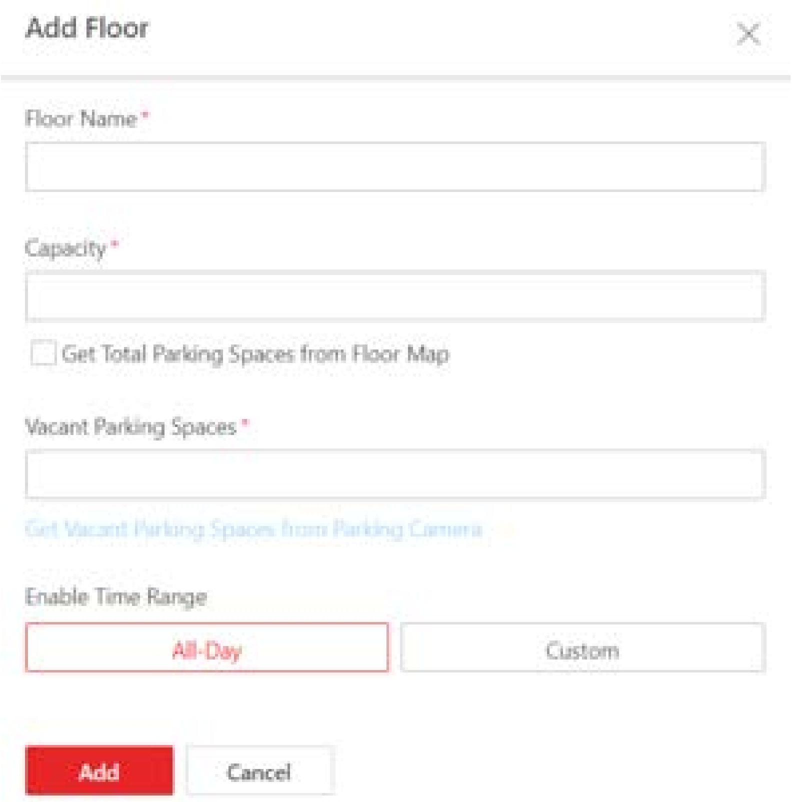


Figure 18-36 Add Floor Pane

4. Set the floor.
   1) Create a name for the floor.
   2) 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.

   3) 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.

4) Set the period during which the floor is available for parking. Click **All-Day**, or click **Custom** to customize a period.

5. Click **Add**.

   You will enter the page where you can relate devices, configure a map, mark guidance screen, and configure types for parking spaces.

What to do next

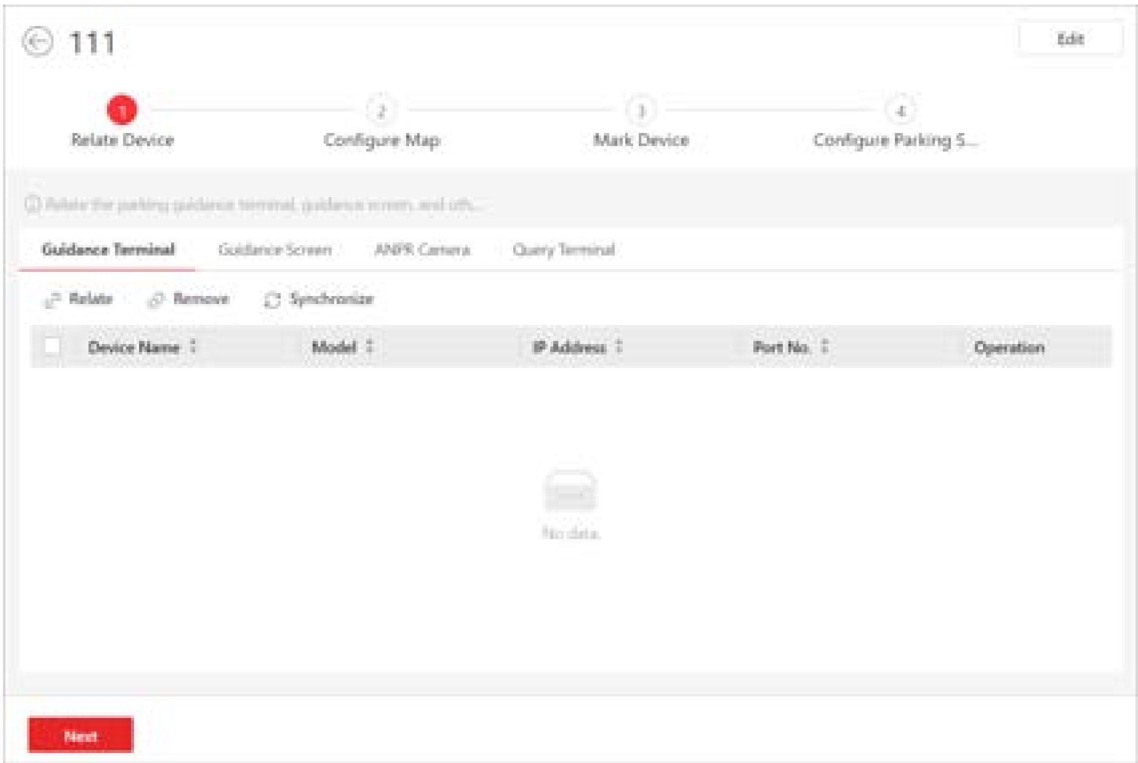
Relate devices to the floor. See ***Relate Devices to the Floor*** .

18.9.2 Relate Devices to the Floor

In the Parking Guidance Configuration module, after adding a floor to the parking lot, you can relate devices (guidance terminal, 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 related 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 count the number of vacant and occupied parking spaces.

Steps

1. After adding a floor, you will enter the following page.



Relate the parking guidance terminal, guidance screen, and oth...

Figure 18-37 Relate Device

2. Click **Relate Device**.

3. Relate device(s) to the floor.

1) Click **Guidance Terminal → Relate** , and select guidance terminal(s) to relate.

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 related to the terminal(s).
- Click 🗎 to view the parking camera(s) related to a guidance terminal, and the parking spaces monitored by the parking camera(s).
- Click ⚙ to edit the settings of a guidance terminal.

2) Click **Guidance Screen → Relate** , and select guidance screen(s) to relate.

Entrance Guidance Screen

An entrance guidance screen displays the welcome message and the number of vacant parking spaces in the parking lot.

Note

If an entrance guidance screen is related to more than one floor, it displays the total number of vacant parking spaces of all floors.

Indoor Guidance Screen

An indoor guidance screen displays the number of vacant parking spaces and guides vehicles to the area where there are vacant parking spaces.

Note

If both of the ANPR cameras and parking cameras are related to a parking lot, the entrance guidance screen and indoor guidance screen display the number of vacant parking spaces counted by ANPR cameras and parking cameras respectively.

3) Click **ANPR Camera → Relate** , and select ANPR camera(s) to relate. 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 related to different floors.
- The number of vacant parking spaces on the top floor is counted by the ANPR camera.

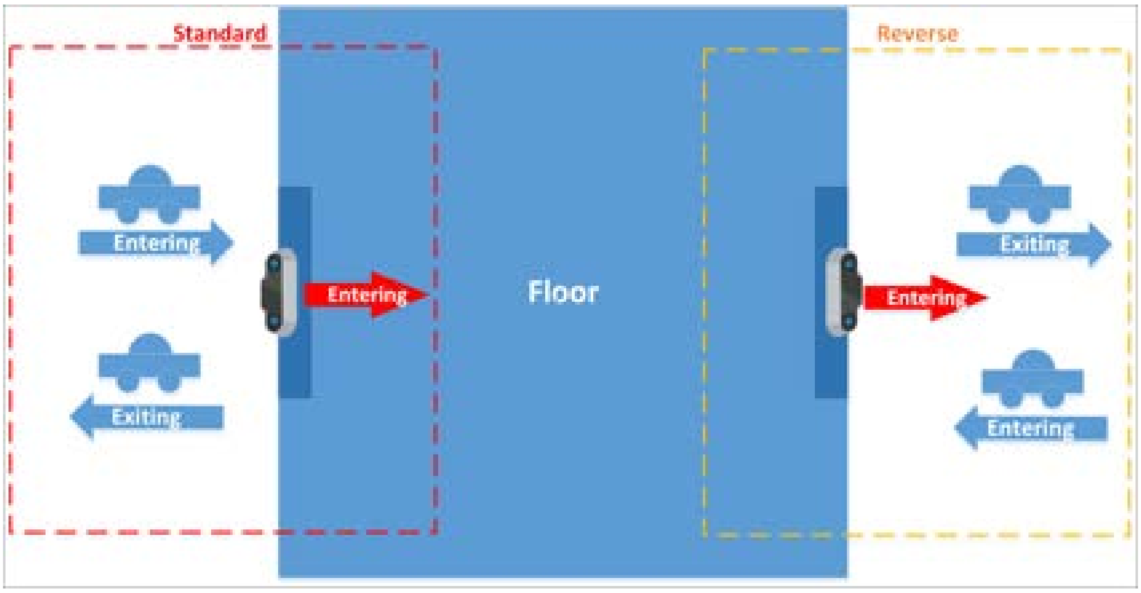


Figure 18-38 Schematic Diagram of Calculation Mode

4) Click **Query Terminal** and select query terminal(s) to relate.

Query Terminal

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.

What to do next

Click **Next** to configure a map for the floor. See ***Configure a Map for the Floor*** .

18.9.3 Configure a Map for the Floor

In the Parking Guidance Configuration module, you can add a map to the floor, add parking spaces to the map, and configure the layout of parking spaces.

Steps

1. After relating device(s) to the floor, you will enter the following page.

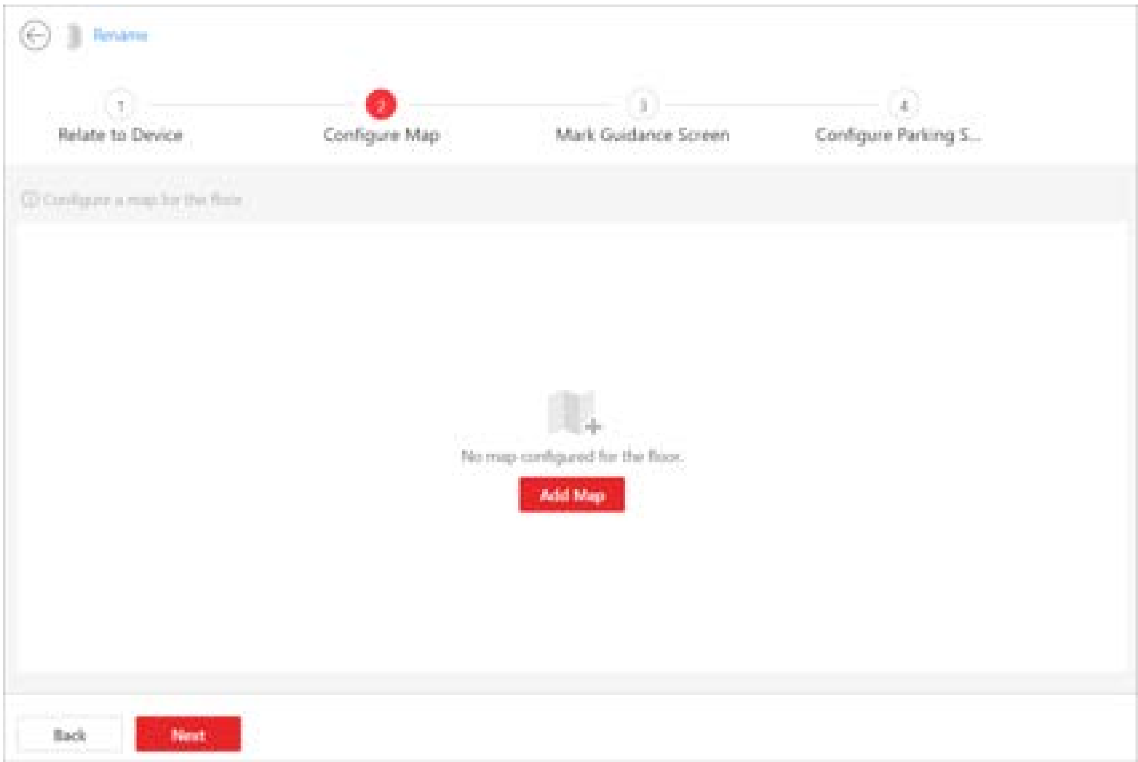


Figure 18-39 Add a Map

2. Click **Add Map**.
3. Select a map from your PC and add it to the floor.

Note

You can click + or − to adjust the size of the map.

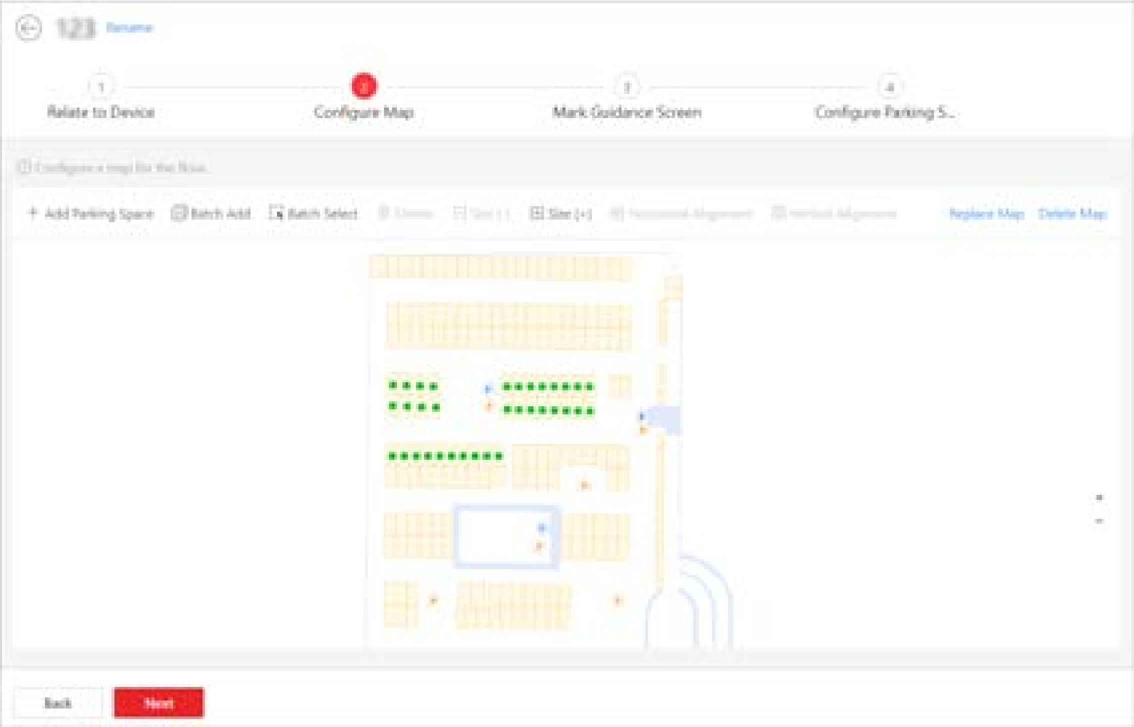


Figure 18-40 Configure the Map

4. Add parking space(s).
   - Add parking spaces one by one.
     a. Click **Add Parking Space** 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 **Batch Add**.
     b. Click on the map to draw a line.
     c. On the pop-up panel, enter the number of parking spaces to be added.
     d. Enter the No. of the first parking space.
     e. Select the order of parking space No. from **Ascend** (e.g., 1, 2, 3) and **Descend** (e.g., 3, 2, 1).
     f. Click **Save**.
5. **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 **Delete** to delete it.
- Click **Batch Select**, drag you cursor to select multiple parking spaces, and click **Delete** to batch delete them.

Adjust the Size of the View of Parking Space(s)

- Click one parking space and click **Size (+)** or **Size (-)** to make it bigger or smaller.
- Click **Batch Select**, drag you cursor to select multiple parking spaces, and click **Size (+)** or **Size (-)** to make them bigger or smaller.

Align Parking Spaces Horizontally

Click **Batch Select**, drag you cursor to select multiple parking spaces, and click **Horizontal Alignment** to align them in a horizontal line.

Align Parking Spaces Vertically

Click **Batch Select**, drag you cursor to select multiple parking spaces, and click **Vertical Alignment** to align them in a vertical line.

Replace Map

Click **Replace Map** to change the map.

Delete Map

Click **Delete Map** to delete the map.

6. **Optional:** Click **Back** to edit former configuration.

What to do next

Click **Next** to mark guidance screen(s) on the map. See ***Mark Guidance Screens on the Map*** .

18.9.4 Mark Guidance Screens on the Map

In the Parking Guidance Configuration module, you can relate the guidance screen to the parking spaces at a specific direction in the parking lot. Once related, the guidance screen can display the number of vacant parking spaces and guide vehicles to them.

Steps

1. After configuring a map for the floor, you will enter the following page.

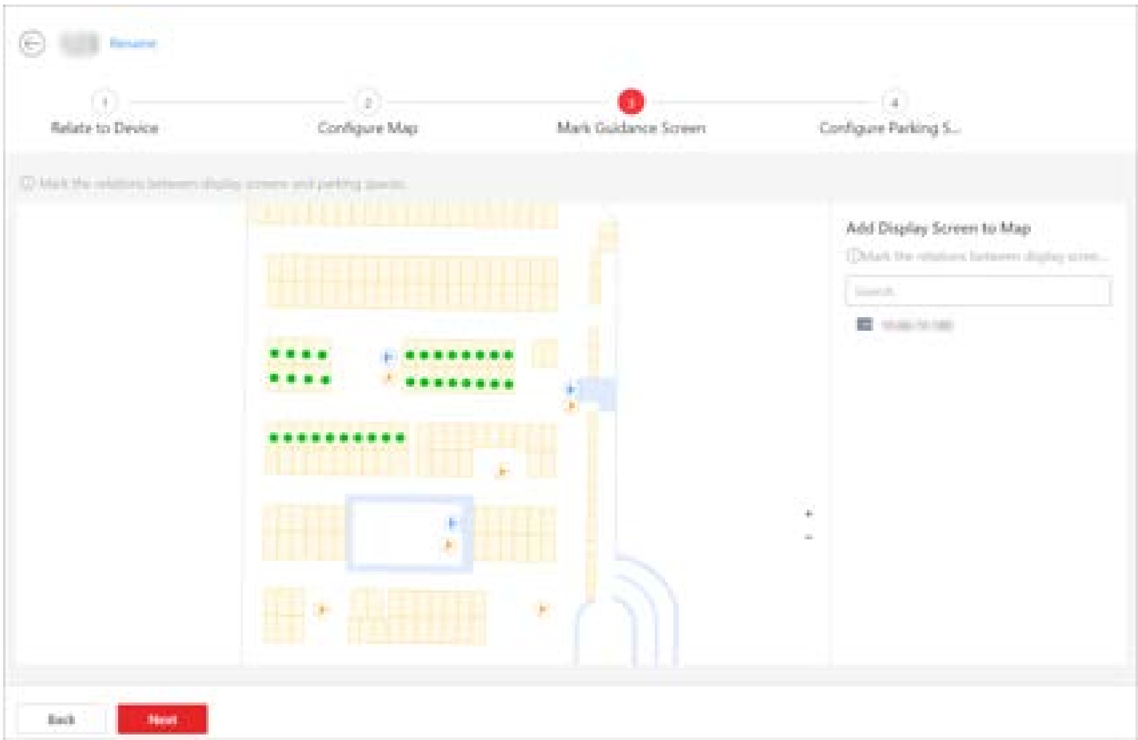

Rename
1
Relate to Device
2
Configure Map
3
Mark Guidance Screen
4
Configure Parking S...
Mark the relations between display screens and parking spaces.
Add Display Screen to Map
Mark the relations between display scree...
Search
+
-
Back
Next

Figure 18-41 Mark Guidance Screen

2. Move a guidance screen from the left list to the map.

Note

Only the indoor guidance screen can be marked. The entrance guidance screen will not be displayed in the list.

3. Relate the guidance screen to the parking space(s) at a specific direction. Take relating the parking space(s) at left as an example.
   1) Click or **Relate Parking Space(s) at Left**.
   2) Click one parking space to relate, click **Batch Select** and drag to select multiple parking spaces to relate, or check **Select All Parking Spaces** to relate all parking spaces on the map.
   3) Click **OK**.

Note

You can also mark the parking space(s) at right or in the middle via the same steps.

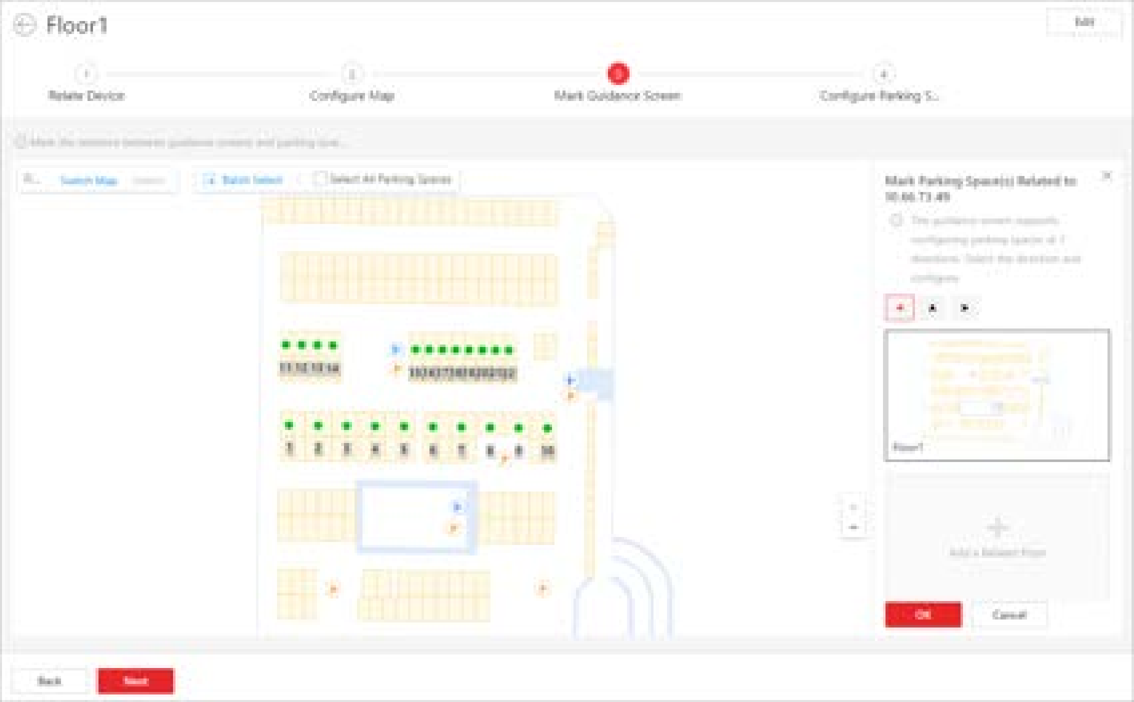


Figure 18-42 Relate Guidance Screen with Parking Spaces

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

Cancel the Relation Between Parking Space and Guidance Screen	Take canceling the relation between the parking space at left and the guidance screen as an example. a. Click ◀ . b. Click anywhere on the map. **Note** The color of the related parking space(s) turns into green. c. Click **OK**.
Add a Related Floor	Click **Add a Related Floor** and select a floor to relate it with the indoor guidance screen.
Cancel the Relation with a Floor	Select a floor and click **Delete** to cancel the relation with it.
Switch Map	Click **Switch Map** and select another map to display.

What to do next

Click **Next** to configure the types of parking spaces. See ***Set Types for Parking Spaces on the Map*** .

18.9.5 Set Types for Parking Spaces on the Map

In the Parking Guidance Configuration module, you can set types for parking spaces and managing the types according to actual needs.

Steps

1. After marking the guidance screen, you will enter the following page.

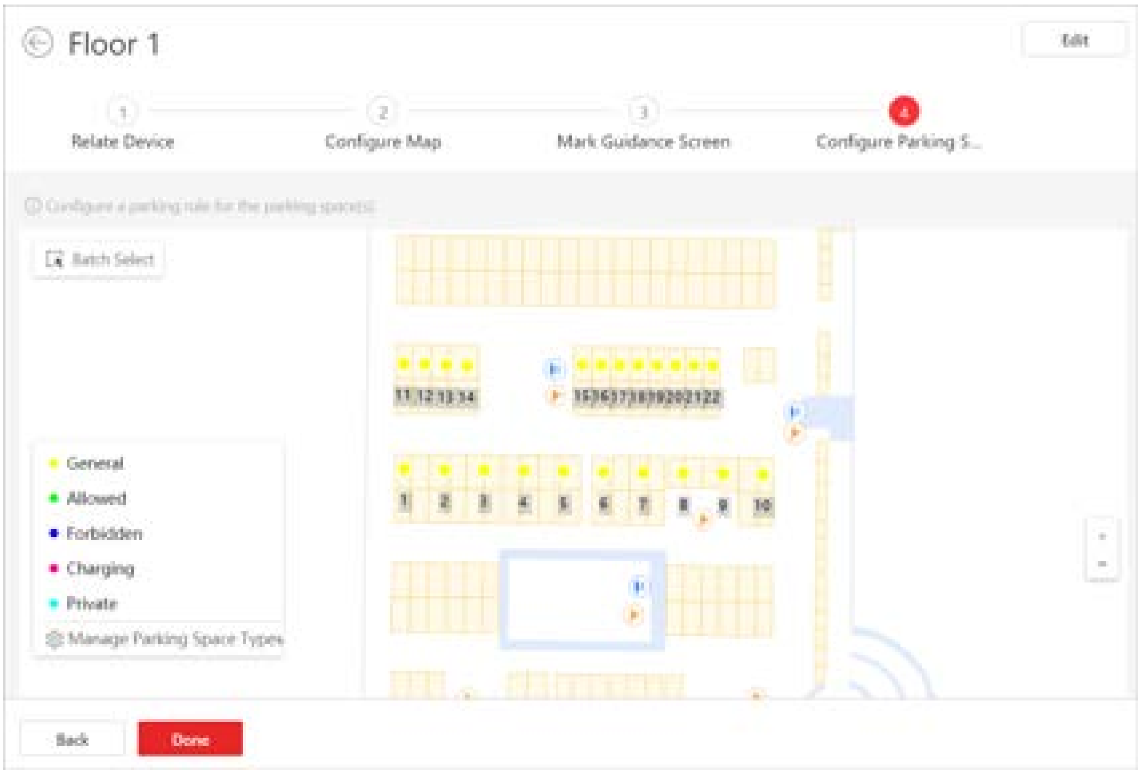
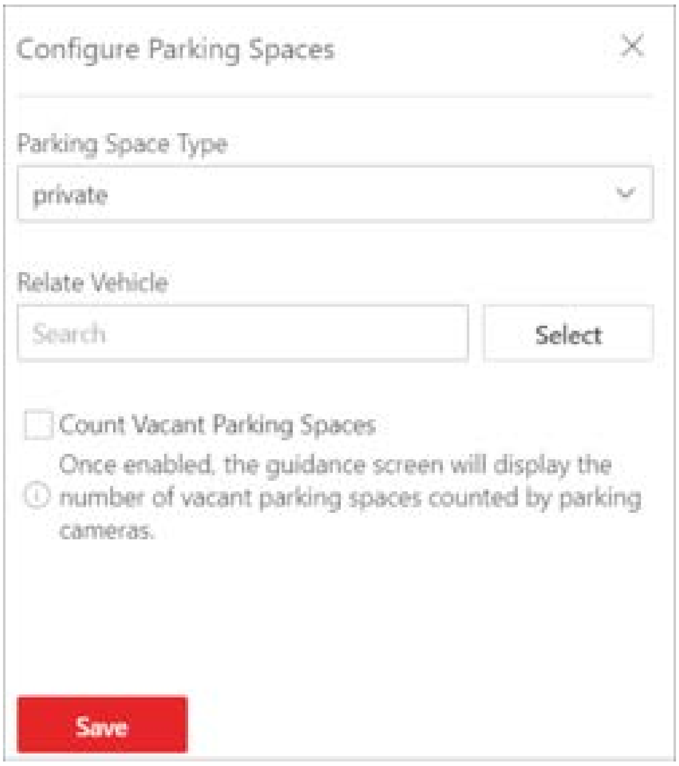


Figure 18-43 Set Types for Parking Spaces

2. Click a parking space to open the Configure Parking Spaces pane.



Configure Parking Spaces

Parking Space Type

private

Relate Vehicle

Search

Select

□ Count Vacant Parking Spaces

Once enabled, the guidance screen will display the number of vacant parking spaces counted by parking cameras.

Save

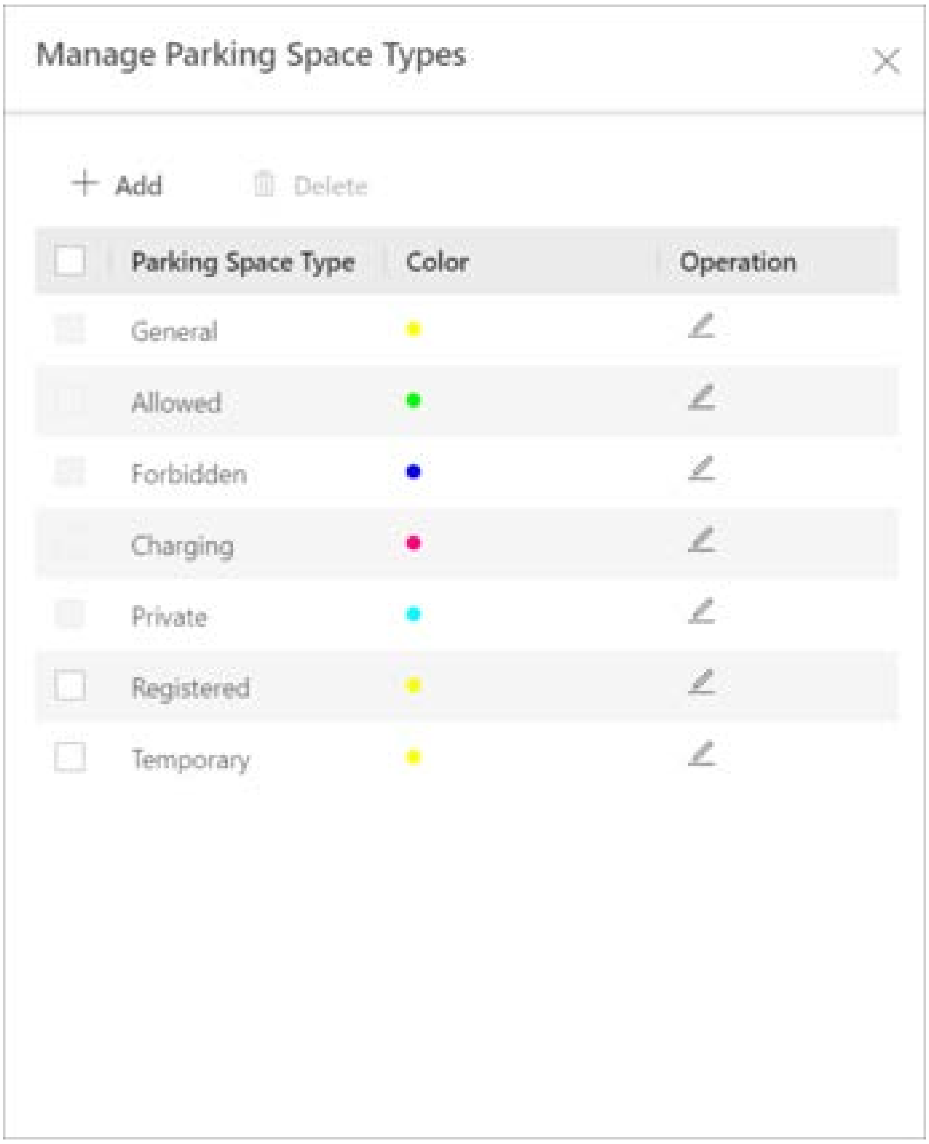
Figure 18-44 Configure Parking Spaces Pane

3. Select a type for the parking space from the drop-down list.
4. Relate vehicle(s) or vehicle list(s) to the parking space.

Note

Skip this step if you select **General** or **Charging** as the parking space type.

5. **Optional:** Check **Count Vacant Parking Spaces** to display the number of vacant parking spaces on the guidance screen.
6. **Optional:** Click **Manage Parking Space Types** and perform the following operations if needed.



Manage Parking Space Types

+ Add   Delete

□	Parking Space Type	Color	Operation
□	General	●	✎
□	Allowed	●	✎
□	Forbidden	●	✎
□	Charging	●	✎
□	Private	●	✎
□	Registered	●	✎
□	Temporary	●	✎

Figure 18-45 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 types (general, allowed, forbidden, charging, private) cannot be edited.
Delete Parking Space Type(s)	Select one or multiple types and click **Delete** to delete them. **Note** The default types cannot be deleted.

7. Click **Done**.
8. **Optional:** Click **Back** to edit former configuration.

18.10 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 number, 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, and parking spaces with unknown status, and the number of overtime parking and parking violations.

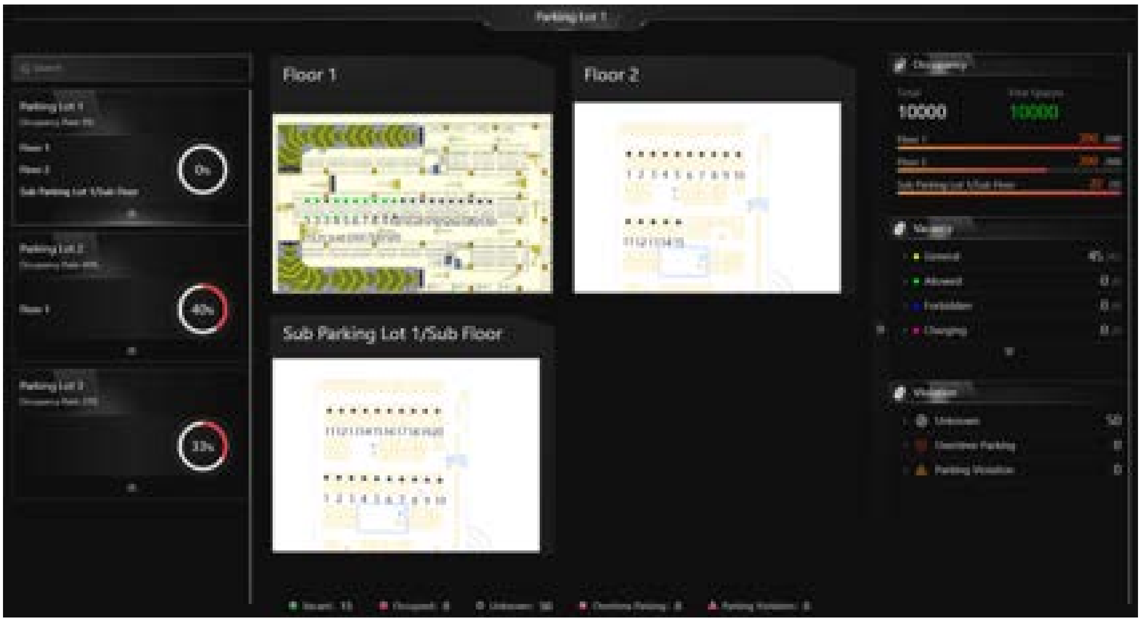


Figure 18-46 Parking Space Overview

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.

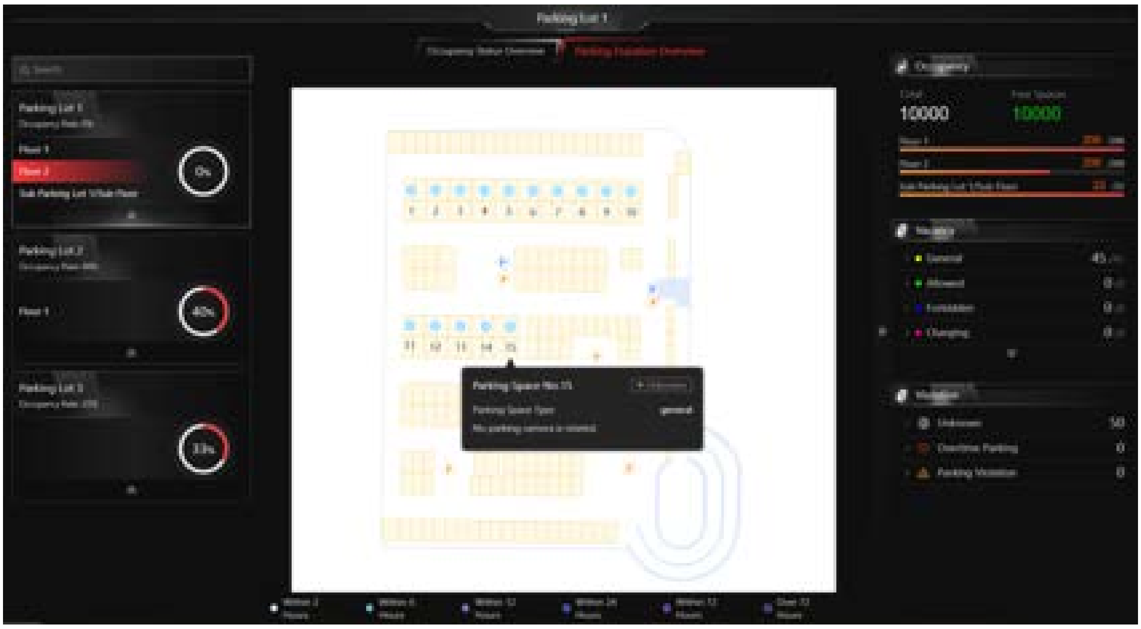


Figure 18-47 Floor Parking Space Overview

18.11 Vehicle and Record Search

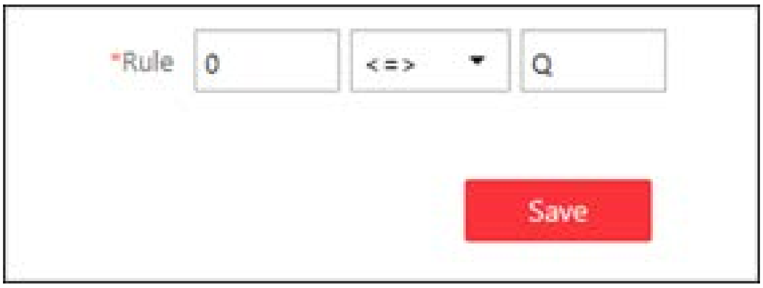
In the Vehicle module, you can search for various types of records, including the vehicle passing records, parking records, payment records, etc. Each record is attached with highly detailed information related to it, which can give the vehicle owner and the administrator a whole picture of the vehicle's activity in a parking lot. Therefore, these records can help you to manage vehicles and parking lots much better.

18.11.1 Add Fuzzy Matching Rules for License Plate Search

When searching 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. By default, the system provides 6 ready-made rules including 0<=>Q, 0<=>O, Q<=>O, 1<=>I, G<=>6, and D<=>O.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Basic Settings** → **Plate Fuzzy Search** .
2. Click **Add**.



*Rule 0 <=> Q

Save

Figure 18-48 Add a 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

- By default, 6 rules are added when you log in for the first time.
- Up to 16 rules can be added.

4. Click **Save**.
5. **Optional:** After adding the rules, you can do one or more of the followings.

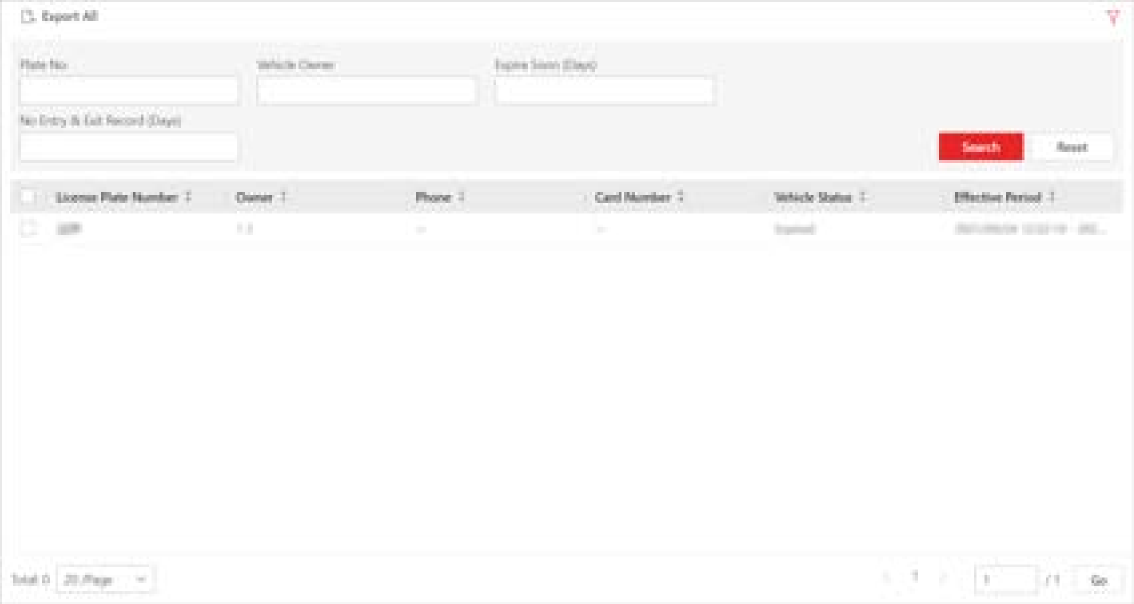
Edit Rule	Click ✎ in the Operation column to edit this rule.
Enable/Disable Rule	Click ✓ / ⊖ in the Operation column to enable/disable this rule.
Delete Rule	Click × in the Operation column to delete this rule.

18.11.2 Search for Visitor Vehicles

In the Vehicle and Card Management module, you can search for visitor vehicles. The information of the vehicles (such as the license plate number, vehicle owner, etc) will be displayed, and you can export the information to your PC.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **Vehicle and Card Management** → **Visitor Vehicle** .
2. Click ▽ to open the panel of search conditions.



	License Plate Number	Owner	Phone	Card Number	Vehicle Status	Effective Period
□	[illegible]	[illegible]	--	--	Expired	[illegible]

Figure 18-49 Search Visitor Vehicle Page

3. Set search conditions, 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 entered or exited the parking lot.

4. Click **Search**.

   The matched result(s) will be displayed.

18.11.3 Search for Vehicle Passing Records

If the added Automatic Number-Plate Recognition (ANPR) camera, Under Vehicle Surveillance System (UVSS), and entrance and exit are properly configured, and the vehicle license plate number is recognized by the cameras or capture units linked to the entrance and exit, you can search the related vehicle passing information.

Steps

Note

Make sure your license supports ANPR function. Otherwise, ANPR function cannot perform normally in the system.

1. In the top left corner of the Client, select ▦ → **All Modules** → **Vehicle** → **Search** → **Vehicle Passing Record Search** .

2. Set a time range.
   - Select to search the vehicle passing records generated today, yesterday, current week, last 7 days, or last 30 days.
   - Click **Custom Time Interval** to set the search time range.
3. Select **Camera**, **UVSS** or **Entrance and Exit** as the source of passing vehicle records.

   The camera, UVSS, or entrance/exit will be automatically displayed under the Source.

   Note

   For camera, you can click , select the current site or a Remote Site from the drop-down list and select the ANPR camera(s).
4. Set searching conditions according to your needs.

   Marking Status

   Search marked or unmarked vehicles' passing records.

   Country/Region

   Select the country/region where the vehicle's license plate number is registered.

   License Plate Number

   Select **No License Plate** to search vehicles without license plate number; select **With License Plate** and enter a vehicle's license plate number or key word of license plate number.

   Vehicle Owner

   Enter the vehicle owner's name or keyword of name.

   Vehicle Type

   Select the type of the vehicle from the drop-down list.

   Brand

   Select the brand of the vehicle from the drop-down list.

   Color

   Select the color of the vehicle from the presented colors.

   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 the camera in other directions.

   Driving Speed

   Set a range of driving speed.

   Vehicle List

   Search vehicle passing records of vehicles in certain vehicle list(s).

   Custom Information

   The custom items of vehicle information you added.
5. Click **Search**.

The vehicle passing records that match the search conditions will be displayed in the right area.

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

View Vehicle Information
Click a license plate number in the list to view the detailed information of the vehicle.

Sort Records
Click **Sort by Time** or **Sort by Vehicle Passing Times** in the upper-right corner to sort vehicle passing records.

Sort by Time

Sort records by the time vehicles passed through the entrance & exit.

Sort by Vehicle Passing Times

Sort records by the number of times vehicles passed through the entrance & exit.

Export Vehicle Passing Records

a. Click **Export** in the upper-right corner to open the Export panel.
b. Select **Excel**, **CSV**, or **PDF** as the format of the exported file. Check **Export Picture** to save vehicles' pictures in your PC with the Excel file.
c. Click **Browse** to select a saving path.
d. Click **Save**.

Note

- Up to 500 vehicle passing records with captured pictures can be exported at one time. If the number of records with captured pictures exceeds 500, you need to go to the Control Client to export them.
- Up to 100,000 vehicle passing records without captured pictures can be exported at one time.

18.11.4 Search for Parking Records

On the platform, you can search for the parking records generated in a specific parking lot or the record 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. In the top left corner of the Client, select 🟥 → **All Modules** → **Vehicle** → **Search** → **Parking Record Search** .
2. Set search conditions according to actual needs.

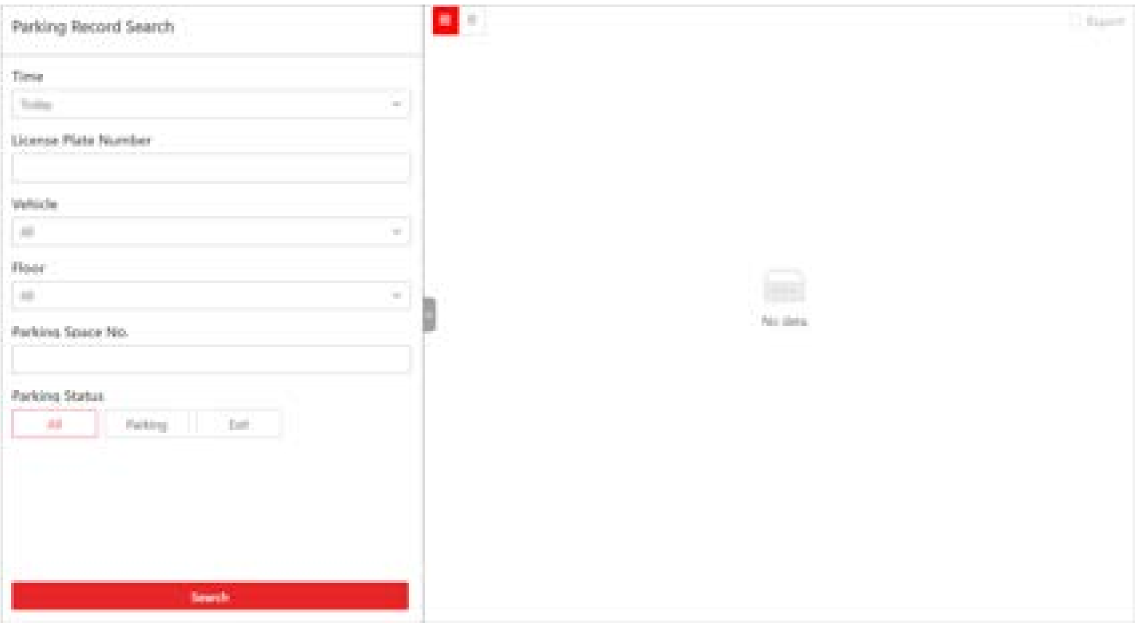


Figure 18-51 Parking Record Search Page

1) Set a time range.

Note

You can select today, yesterday, current week, last 7 days, or last 30 days from the drop-down list to search for the records generated in a relevant period, or click **Custom Time Interval** to customize a time range.

2) **Optional:** Enter the license plate number of the vehicle.
3) Select a parking lot or **All** from the drop-down list.
4) Select a floor or **All** from the drop-down list.
5) **Optional:** Enter the parking space No.
6) Select the status of parking.

3. Click **Search**.

The matched record(s) will be displayed in the right area.

Note

You can click ≡ or ⊞ to switch between list mode and thumbnail mode.

4. **Optional:** In the upper-right corner, click **Export** to export the record(s) to your PC.

Note

- Up to 500 parking records with captured pictures can be exported at one time. If the number of records with captured pictures exceeds 500, you need to go to the Control Client to export them.
- Up to 100,000 parking records without captured pictures can be exported at one time.

18.11.5 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. In the top left corner of the Client, select ▦ → **All Modules** → **Vehicle** → **Search** → **Parked Vehicle Search** .
2. Set searching conditions according to actual needs.

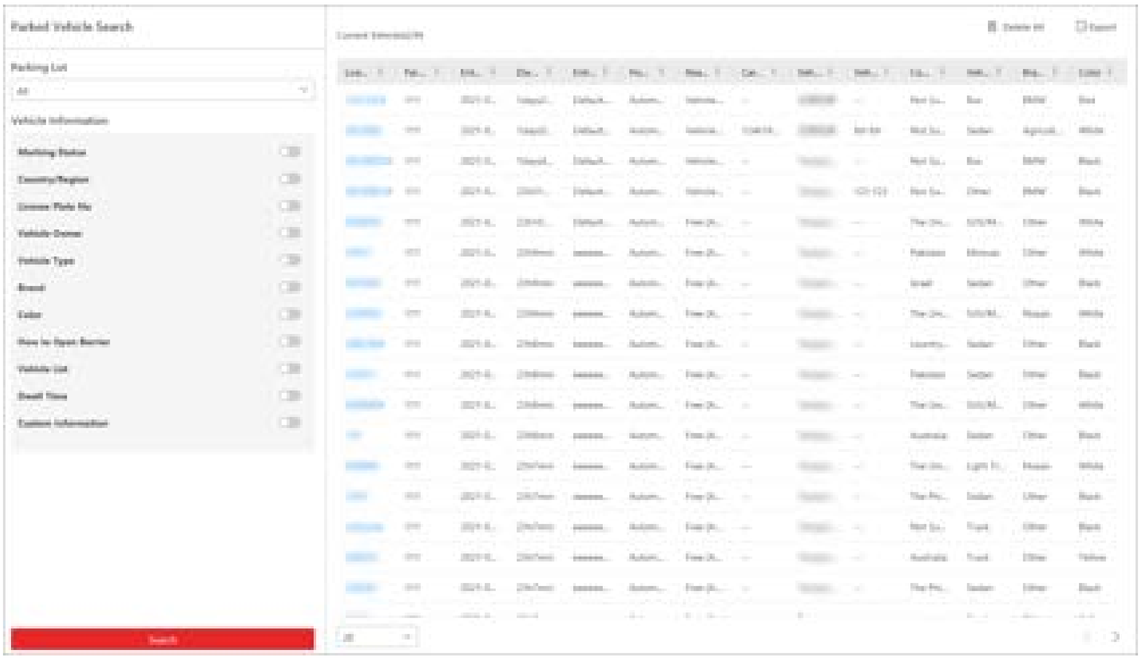


Figure 18-52 Search Vehicles in Parking Lot

1) Select a parking lot from the drop-down list.
2) **Optional:** Set vehicle information.

Label

Search marked or unmarked vehicles in the parking lot.

Country/Region

Select the country/region where the vehicle's license plate number is registered.

License Plate Number

Select **No License Plate** to search vehicles without license plate number; select **With License Plate** and enter a vehicle's license plate number or key word of license plate number.

Vehicle Owner

Enter the vehicle owner's name or keyword of name.

Vehicle Type

Select the type of the vehicle from the drop-down list.

Brand

Select the brand of the vehicle from the drop-down list.

Color

Select the color of the vehicle from the presented colors.

How to Open Barrier

It refers to how the barrier gate was opened when a vehicle exits the parking lot. **Manual** indicates that the a security guard manually controls the barrier gate to open after identifying the vehicle owner; **Automatic** indicates that the barrier gate was opened automatically after the capture unit recognizing the license plate number; **Barrier Not Open** indicates that the barrier gate was not opened after the capture unit recognizing the license plate number.

Vehicle List

Search vehicle passing records of vehicles in certain vehicle list(s).

Dwell Time

The parking duration of the searched vehicles in the parking lot.

Additional Information

The custom items of vehicle information you added.

3. Click **Search**.

   The matched vehicles will be displayed in the right area.

4. Perform the following operations if you need.

Delete Vehicles from Parking Lot	• Click **Delete All** to delete all searched vehicles from the parking lot. **Note** After deleting a vehicle in the list, there will be one more vacant parking space in the parking lot.
Export Vehicle Information to PC	• Save information of all searched vehicles as a file in PC. a. In the top right corner, click **Export** to open the Export panel. b. Select **Excel** or **CSV** as the format of the exported file. Check **Export Picture** to save vehicles' pictures in your PC with the Excel file.

c. Click **Browse** to select a saving path.

d. Click **Save**.

Note

- Up to 500 records of parked vehicles with captured pictures can be exported at one time. If the number of records with captured pictures exceeds 500, you need to go to the Control Client to export them.
- Up to 100,000 records of parked vehicles without captured pictures can be exported at one time.

View Vehicle Information	Click a license plate number in the list to view the detailed information of the vehicle.

18.11.6 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 to manage the parking lots better.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Vehicle** → **Search** → **Payment Record Search** .

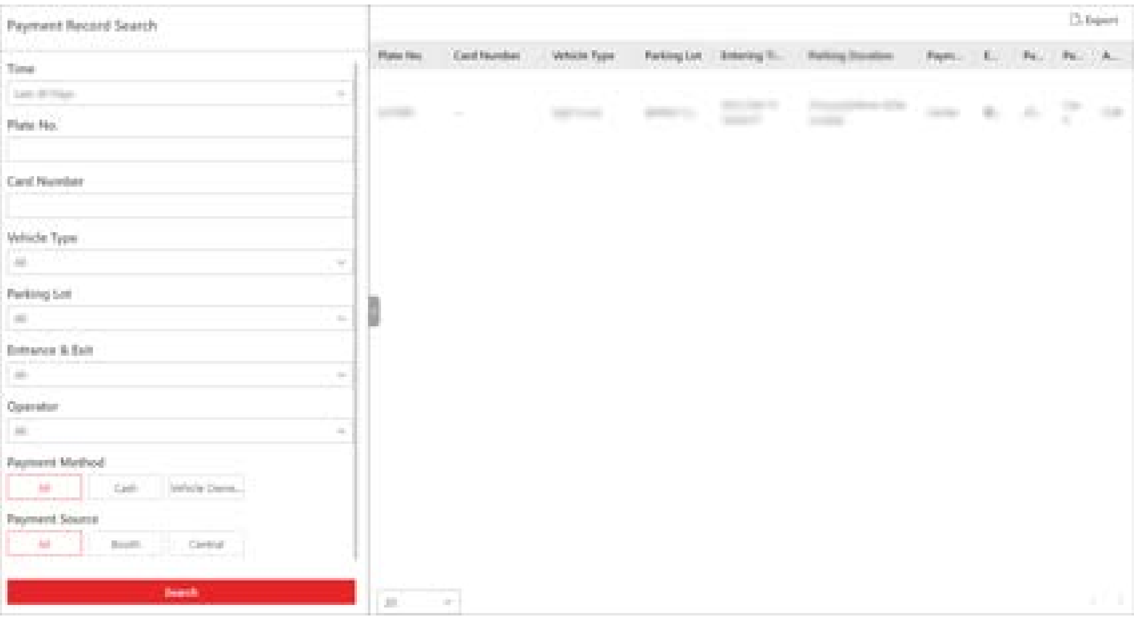


Figure 18-53 Payment Record Search Page

2. Set search conditions according to actual needs.
   1) Set a time range.

      Note

      You can select today, yesterday, current week, last 7 days, or last 30 days from the drop-down list to search for the records generated in a relevant period, or click **Custom Time Interval** to set a time range by yourself.

   2) **Optional:** Enter the license plate number of the vehicle.
   3) **Optional:** Enter the card number of the vehicle.
   4) Select the type of the vehicle or **All** from the drop-down list.
   5) Select a parking lot or **All** from the drop-down list.
   6) Select an operator (the person responsible for collecting the fee) or **All** from the drop-down list.
   7) Select the payment method from **All**, **Cash**, and **Vehicle Owner Account**.
   8) Select the source of payment from **All**, **Booth**, and **Toll Center**.
3. Click **Search**.

   The matched record(s) will be displayed in the right area.
4. **Optional:** In the upper-right corner, click **Export** to export the record(s) to your PC.

18.11.7 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 exporting the records to your PC. With the statistics, you can monitor some of the transactions happened in the parking lots, which can help you to manage the parking lots better.

Steps

1. Go to ▦ → **All Modules** → **Vehicle** → **Search** → **Top-Up and Refund Record Search** .

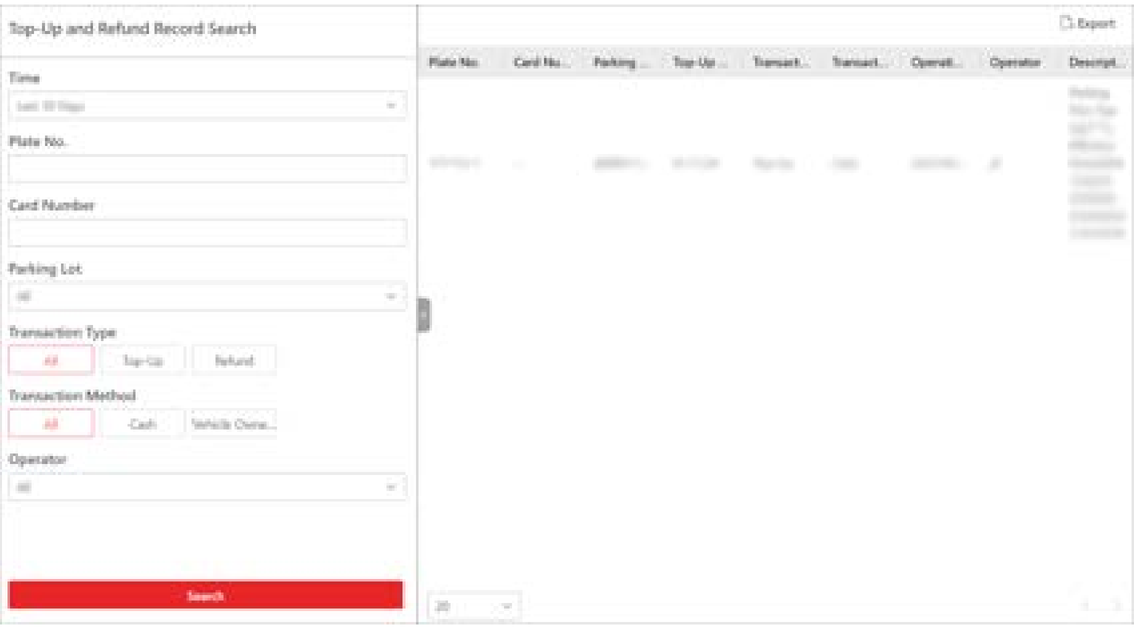


Figure 18-54 Top-Up and Refund Record Search Page

2. Set search conditions according to actual needs.
   1) Set a time range.

   Note

   You can select today, yesterday, current week, last 7 days, or last 30 days to search for the records generated in relevant period, or click **Custom Time Interval** to set a time range by yourself.

   2) **Optional:** Enter the license plate number of the vehicle.
   3) **Optional:** Enter the card number of the vehicle.
   4) Select a parking lot or **All** from the drop-down list.
   5) Select the transaction type from **All**, **Top-Up**, and **Refund**.
   6) Select the transaction method from **All**, **Cash**, and **Vehicle Owner Account**.
   7) Select an operator (the person responsible for collecting the fee) or **All** from the drop-down list.
3. Click **Search**.

   The matched record(s) will be displayed in the right area.
4. **Optional:** In the upper-right corner, click **Export** to export the record(s) to your PC.

18.11.8 Search for Transaction Records of Vehicle Owner Account

In the Search module, you can search for the transaction records of a specific vehicle owner account, and exporting 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. Go to 🟥 → **All Modules** → **Vehicle** → **Search** → **Account Transaction Record Search** .
2. Set search conditions according to actual needs.

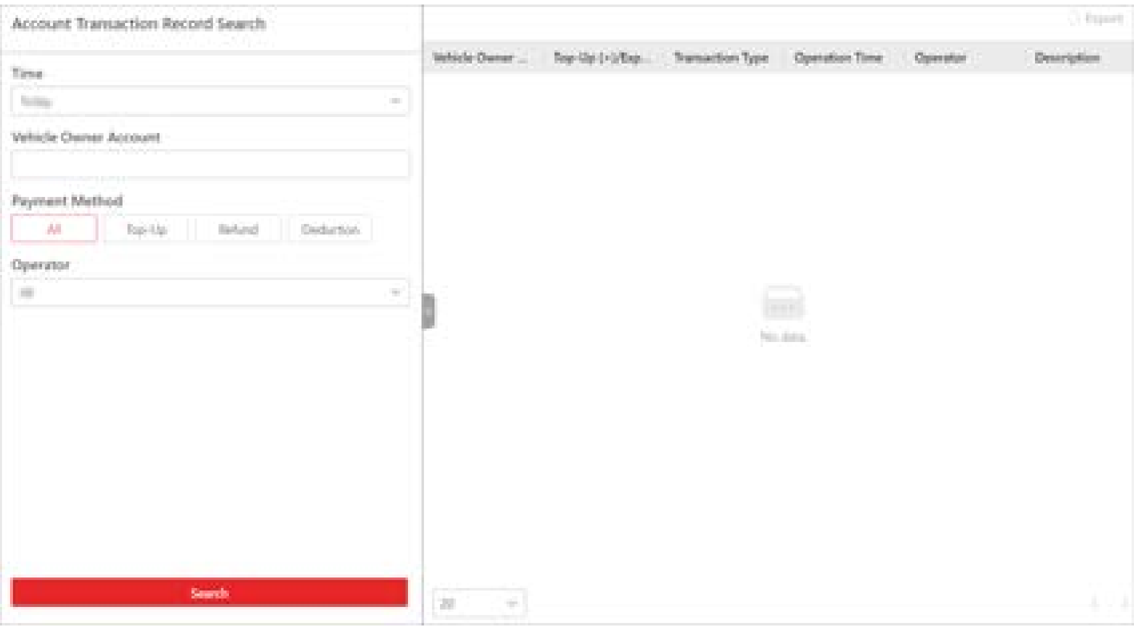


Figure 18-55 Account Transaction Record Search Page

1) Set a time range.

Note

You can select today, yesterday, current week, last 7 days, or last 30 days to search for the records generated in relevant period, or click **Custom Time Interval** to set a time range by yourself.

---

2) Enter the account of the vehicle owner.
3) Select the transaction type from **All**, **Top-Up**, **Refund**, and **Deduction**.
4) Select an operator (the person responsible for collecting the fee) or **All** from the drop-down list.

3. Click **Search**.

   The matched record(s) will be displayed in the right area.
4. **Optional:** In the upper-right corner, click **Export** to export the record(s) to your PC.

18.11.9 Search for the Work Records of Operators

In the Search module, you can search for the work records of operators (i.e., the persons responsible for payment management). You can view 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. Go to 🟥 → **All Modules** → **Vehicle** → **Search** → **Operator Shift Search** .
2. Set search conditions according to actual needs.

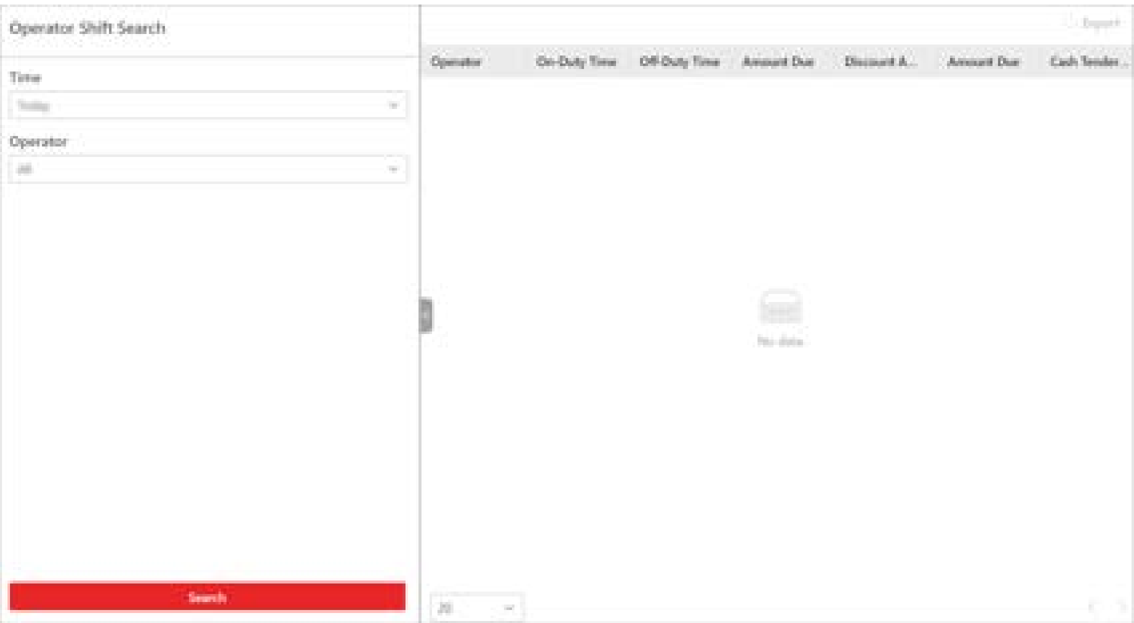


Figure 18-56 Operator Shift Search Page

1) Set a time range.

Note

You can select today, yesterday, current week, last 7 days, or last 30 days to search for the records generated in relevant period, or click **Custom Time Interval** to set a time range by yourself.

2) Select an operator (the person responsible for collecting the fee) or **All** from the drop-down list.

3. Click **Search**.

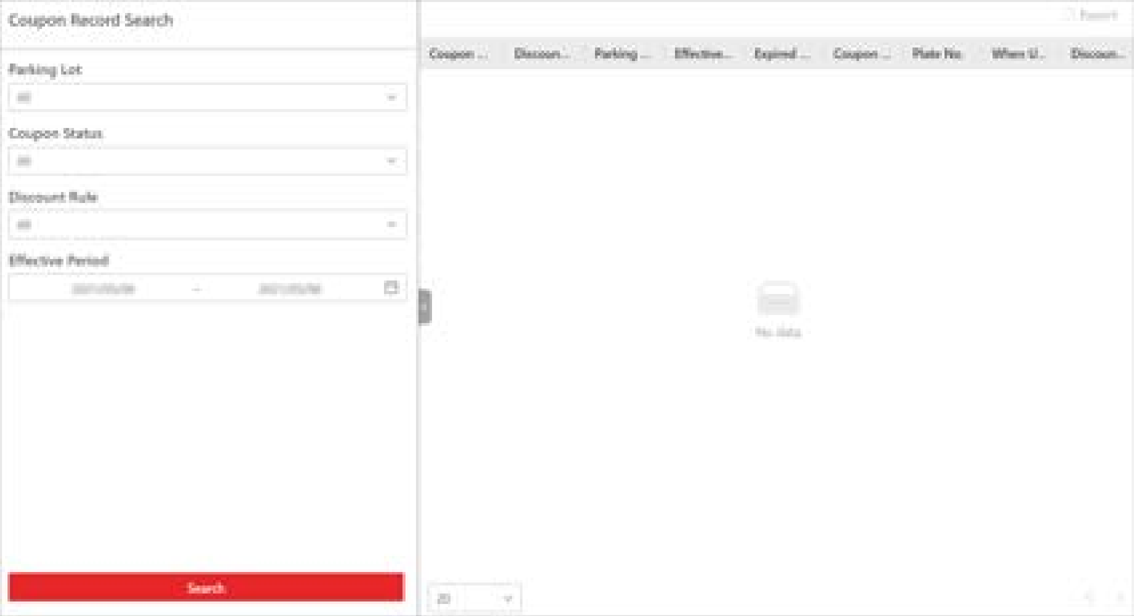
   The matched record(s) will be displayed in the right area.
4. **Optional:** In the upper-right corner, click **Export** to export the record(s) to your PC.

18.11.10 Search for Coupon Records

In the Search module, you can search for coupon records and view the detailed information of the coupons, such as the discount rule, expiration time, coupon status.

Steps

1. Go to 🟥 → **All Modules** → **Vehicle** → **Search** → **Coupon Record Search** .
2. Set search conditions according to actual needs.



Coupon Record Search

Parking Lot: All

Coupon Status: All

Discount Rule: All

Effective Period

Figure 18-57 Coupon Record Search Page

1) Select a vehicle or **All** from the drop-down list.
2) Select a status of the coupon from the drop-down list.
3) Select a discount rule or **All** from the drop-down list.
4) **Optional:** Click 📅 to set the effective period of the coupon(s) to be searched for.

3. Click **Search**.

   The matched record(s) will be displayed in the right area.

4. **Optional:** In the upper-right corner, click **Export** to export the record(s) to your PC.

18.12 Set 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 the further operations for the vehicles, such as correcting license plate number and manually allowing passing.

In the top left corner of Home page, select ▦ → **All Modules** → **Vehicle** → **Basic Settings** → **Call Recipient Settings** .

Click **Add** to select user(s) to receive entrance & exit calls on the Control Client.

18.13 Export Operation Reports of Parking Lots

In the Statistics and Reports module, you can view the statistics related to the operations of parking lots, such as the parking lot occupation rate, parking duration distribution, traffic flow statistics. With the statistics, you can have a general understanding of the situation of parking lots.

Steps

1. Go to → **All Modules** → **Vehicle** → **Statistics and Reports** → **Parking Lot Operation Analysis** .

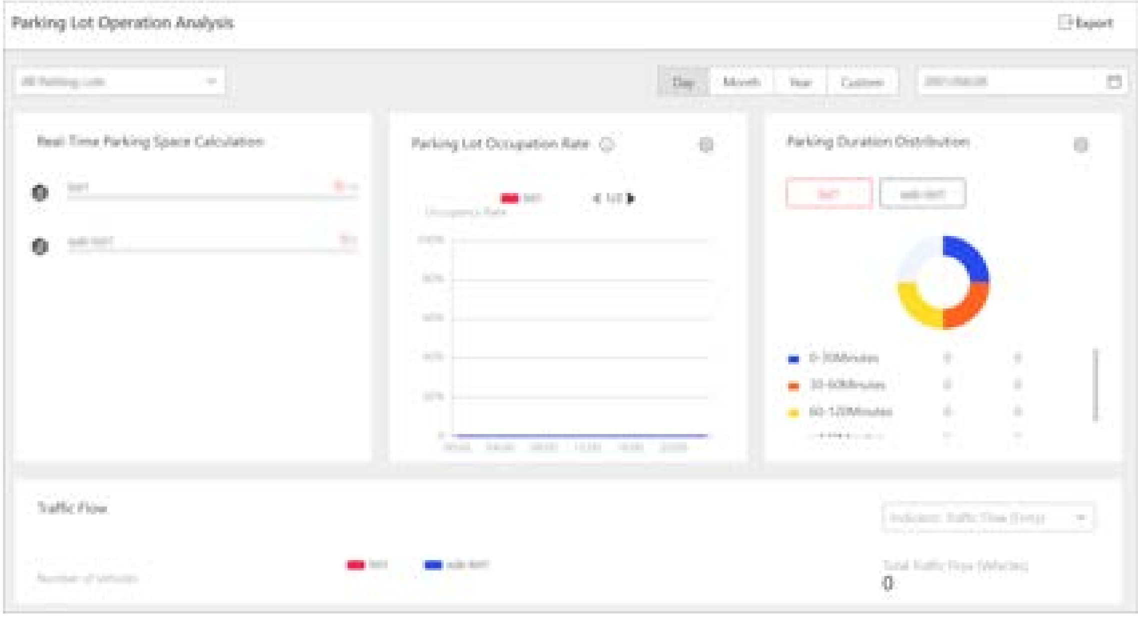

Parking Lot Operation Analysis
Export
All Parking Lots
Day
Month
Year
Custom
Real-Time Parking Space Calculation
Parking Lot Occupation Rate
Occupancy Rate
Parking Duration Distribution
0-30Minutes
30-60Minutes
60-120Minutes
Traffic Flow
Indicator: Traffic Flow (Entry)
Number of Vehicles
Total Traffic Flow (Vehicles)
0

Figure 18-58 Parking Lot Operation Analysis 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 in the custom period.
4. **Optional:** Click ⚙ beside **Parking Lot Occupation Rate** to set a time period.

   The statistics generated in the set period will be displayed.
5. Click ⚙ beside **Parking Duration Distribution** to set the parking duration(s) to be calculated.

   The distribution of the selected parking duration(s) will be displayed.
6. In the Traffic Flow area, select one or multiple indicators from the drop-down list.

   Traffic Flow (Entry)

   The number of vehicles entered the parking lot.

   Traffic Flow (Exit)

   The number of vehicles exited the parking lot.
7. **Optional:** In the upper-right corner, click **Export** to save the analysis report to your PC.

18.14 Export Transaction Reports of Parking Lots

In the Statistics and Reports module, 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. Go to → **All Modules** → **Vehicle** → **Statistics and Reports** → **Transaction Analysis** .

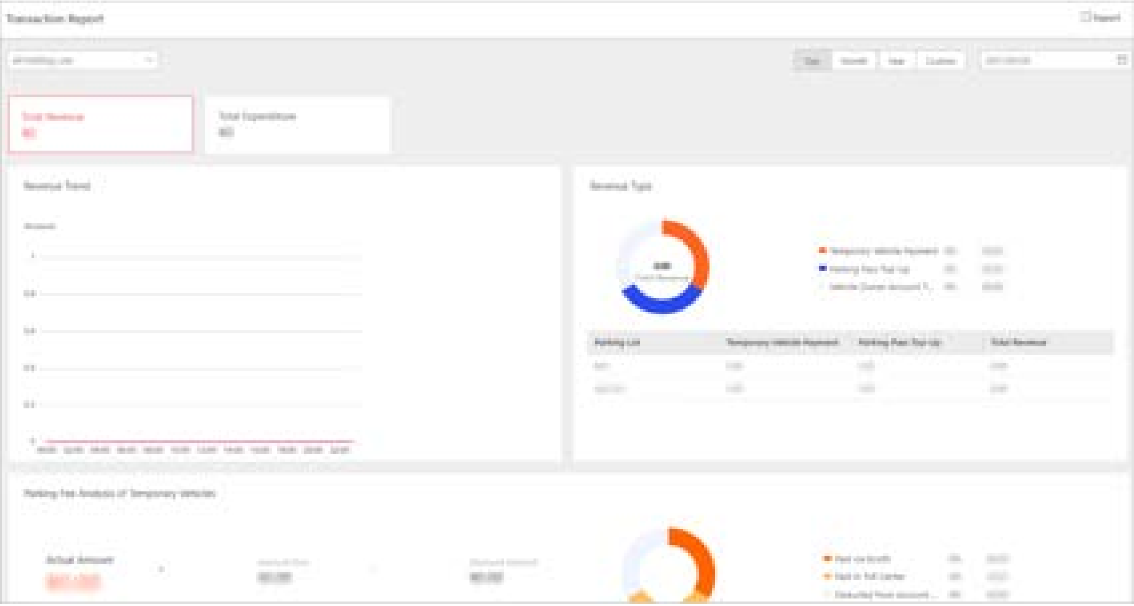


Figure 18-59 Transaction Analysis Page

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 in 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:** In the upper-right corner, click **Export** to save the analysis report to your PC.

18.15 Send Overtime Parking Report Regularly

You can set a regular overtime parking report rule for the parking lot added to the system, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the records of overtime parking vehicles detected by ANPR cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .
- Make sure the parking lot has been added to the system. For details, refer to ***Add Parking Lot*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Vehicle** → **Overtime Parking Report** .
2. Click **+** to enter the Create Report page.
3. Create a name for the report.
4. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the records of overtime parking vehicles detected between 00:00 and 24:00 before the current day.

   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 system will send one report at the sending time every week or every month, which contains the records of overtime parking vehicles detected 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 system will send a report at 6:00 in the morning on every Monday, containing the records of overtime parking vehicles detected between last Monday and Sunday.
5. Select the 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 ***Set Email Template*** .
6. Select the **Report Language**.
7. Click **Add** to add the report and go back to the report list page.

18.16 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 number, 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.

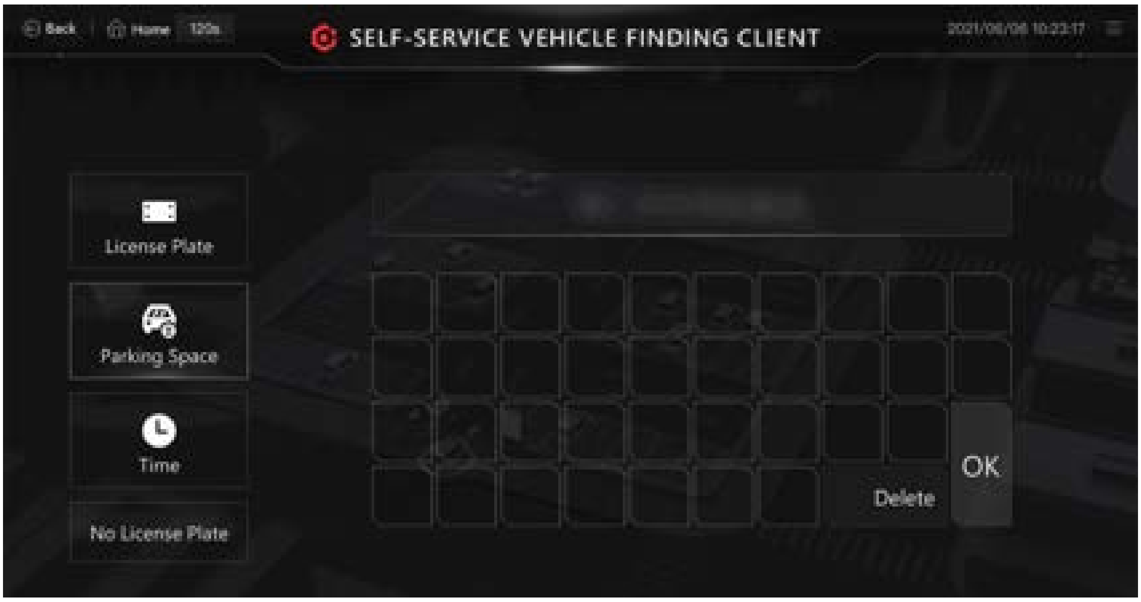


Figure 18-60 Self-Service Vehicle Finding Client

Chapter 19 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 with 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 floor the visitors can access with credentials.

The Visitor Information Overview page shows the wizard for the Visitor module, the current day visit statistics, and current day visit trend.

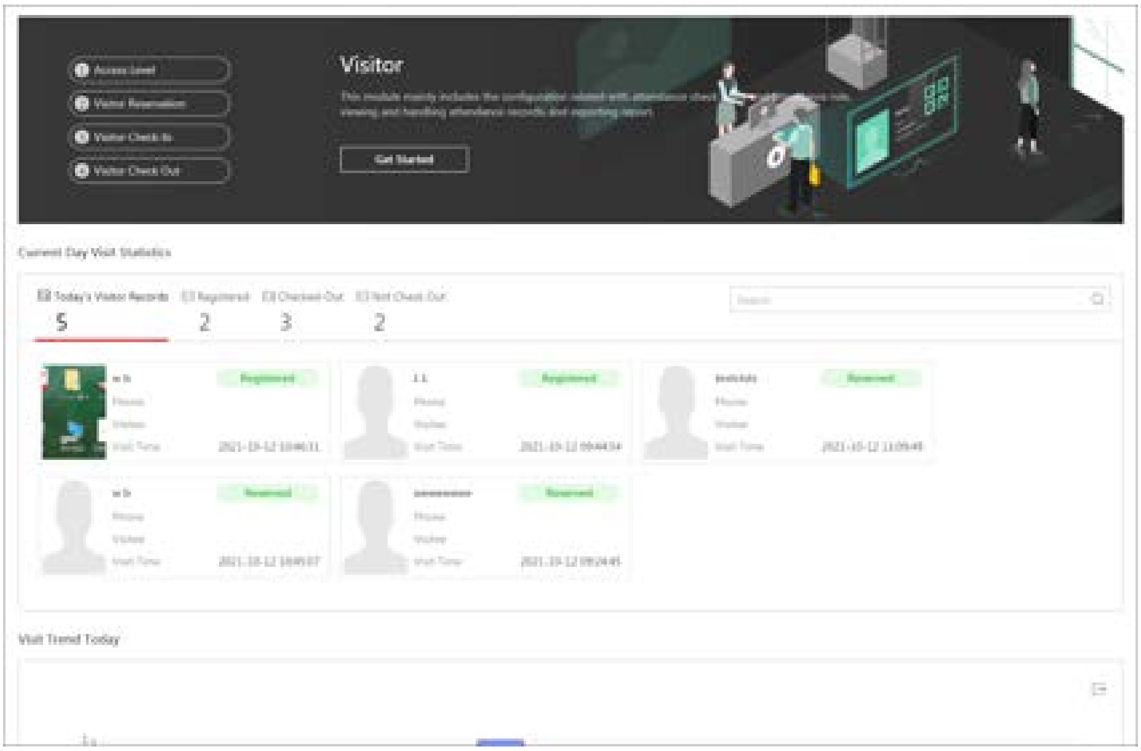


Figure 19-1 Visitor Information Overview

Current Day Visits Statistics

You can search for a specific visitor by the keywords of their name and view the following four types of visitor information:

- **Today's Visit Records**: All the visitors on the current day.
- **Checked In**: The visitors who have checked in on the current day and the basic information about each of these visitors, such as their phone numbers and hosts.

- **Checked Out**: The visitors who have checked out on the current day and the basic information about each of these visitors, such as their phone numbers and check-out time.
- **Not Checked Out**: The visitors who have checked in and not checked out until the current day and the basic information about each of these visitors, such as their phone number and hosts.

Visit Trend Today

You can view the variation trend of the number of visitors on the current day through a line chart. On the line chart, you can perform the following operations:

- Hover the cursor onto 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.

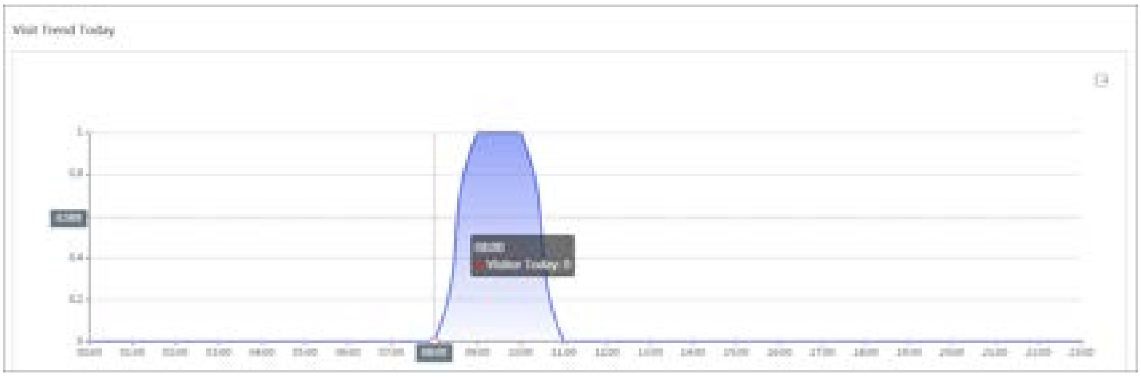


Figure 19-2 Visit Trend Today

19.1 Flow Chart of Visitor Management

The flow chart below shows the process of visitor settings management.

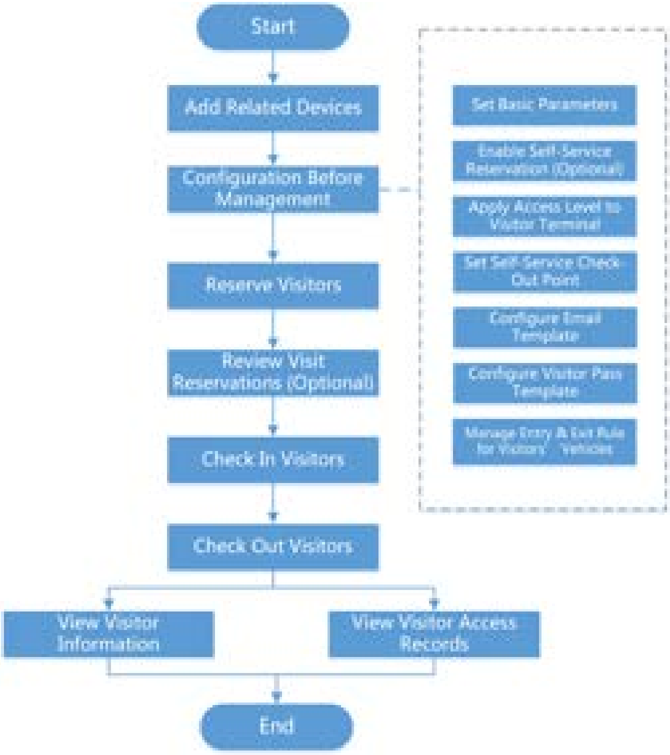

Start
Add Related Devices
Configuration Before Management
Reserve Visitors
Review Visit Reservations (Optional)
Check In Visitors
Check Out Visitors
View Visitor Information
View Visitor Access Records
End
Set Basic Parameters
Enable Self-Service Reservation (Optional)
Apply Access Level to Visitor Terminal
Set Self-Service Check-Out Point
Configure Email Template
Configure Visitor Pass Template
Manage Entry & Exit Rule for Visitors' Vehicles

Figure 19-3 Flow Chart of Visitor Management

Table 19-1 Flow Chart Description

Procedure	Description
Add Related Devices	Add devices used for visitor reservation, check-in, check-out, authentication, etc. See ***Manage Visitor Terminals*** , ***Manage Access Control Device*** , 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 registered 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*** .

19.2 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.

19.2.1 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. In the top left of the Web Client, select ▦ → **All Modules** → **Visitor** → **Visitor Check-In** → **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. For details about permission settings, see ***Add Role*** .

4. **Optional:** Perform the following operations after adding the visitor group.

Edit Visitor Group	Click ✎ to change the visitor group's information.
Delete Visitor Group	Select a visitor group and click 🗑 to delete it.

19.2.2 Set Self-Service Check-Out Point

After setting self-service check-out point, visitors can check out by credentials at the self-service check-out points without the help of receptionist. If you have issued a card to a visitor when registering, after checking out, the visitor should put the card in the place for card collection. The access level of 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.

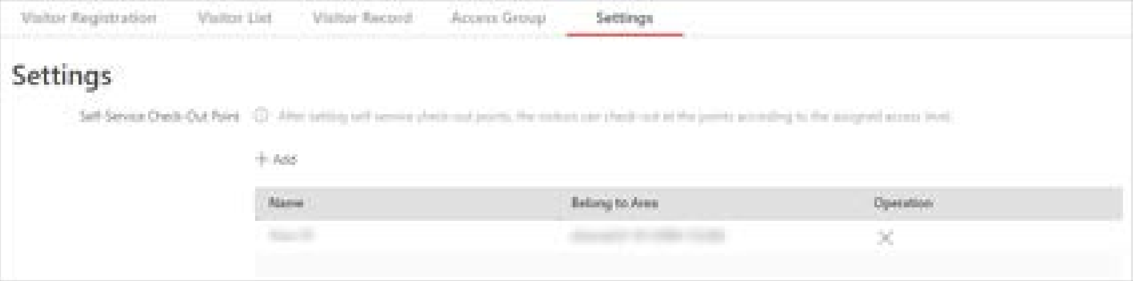
1. In the top left of the Home page, select ▦ → **All Modules → Visitor → Visitor Settings → Basic Settings → Self-Service Check-Out Point** .
2. Click **Add** to show the resource list.

   Note

   You can enter a keyword of a door name in the searching bar to search wanted doors.
3. Select one or more door and click **Add**.

   Note

   After setting self-service check-out points, the visitors can check-out at the points according to the assigned access level by swiping card or fingerprint/face authentication.



Self-Service Check-Out Point ⓘ After setting self-service check-out points, the visitors can check-out at the points according to the assigned access level.

Figure 19-4 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.

19.2.3 Add Access Level for Visitors

An access level contains access points that are accessible during certain period. If you select an access level for a visitor for registration and apply the settings to devices, the visitor can access the access point(s) during authorized period with credentials.

Before You Start

Make sure you have added at least one access level in the Access Control module. See details in ***Add Access Level*** .

Steps

1. In the top left of the Home page, select → **All Modules** → **Visitor** → **Visitor Settings** → **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 periods.
5. **Optional:** Perform the following operations after adding access level.

   View Access Schedule Template Details
   Click in the Access Schedule Template column to view when the access point is accessible for the visitor. See ***Set Access Schedule Template*** for details about setting access schedule template.

   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 herself/himself, under the precondition that you have enabled the Self-Service Reservation feature (see ***Set Self-Service Reservation Parameters***).

   Delete Access Levels for Visitors
   Select access levels and click **Delete** to delete the selected access group.

   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.

19.2.4 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 on the latter.

Before You Start

Make sure you have added access levels for visitors. See ***Add Access Level for Visitors*** for details.

Steps

1. In the top left of the Web Client, select 🟥 → **All Modules** → **Visitor** → **Visitor Settings** → **Basic Settings** → **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 hover the cursor onto it and then click **View** or **Apply Again** to view the failure details or apply the access levels again respectively.

19.2.5 Set Self-Service Reservation Parameters

Self-service reservations refer to visit reservations made by visitors themselves. You can 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 her/him. For details, see ***Reserve a Visitor*** .

1. In the top left of the Home page, select 🟥 → **All Modules** → **Visitor** → **Basic Settings** → **Self-Service Reservation** .
2. 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.
3. **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

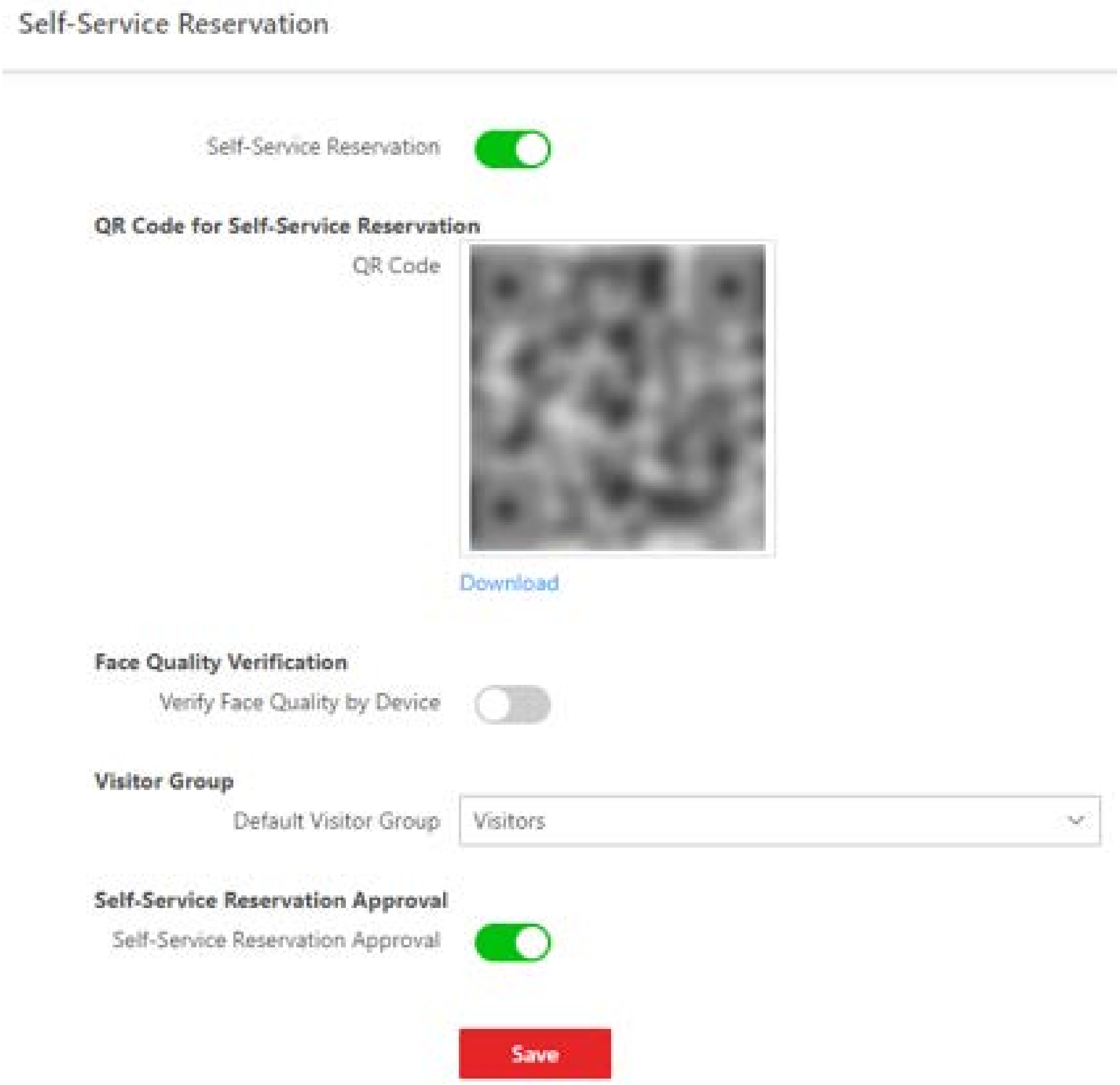
To use this function properly, make sure you have added an access control device or video intercom device to the platform beforehand.

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 by default.

Self-Service Reservation Approval

If you enable this, after the visitor self-service reservation, you need to review the visitor information on the Visitor to be Approved page. After review, the visitor will be added to the selected visitor group. See ***Review Visitor Reservations*** for details about how to review.


Self-Service Reservation

Self-Service Reservation

QR Code for Self-Service Reservation

QR Code

Face Quality Verification

Verify Face Quality by Device

Visitor Group

Default Visitor Group: Visitors

Self-Service Reservation Approval

Self-Service Reservation Approval

Figure 19-5 Self-Service Reservation

4. Click **Save**.

19.2.6 Add Visitor Email Template

You can set email templates (including specifying email type, email subject, and content) for sending emails automatically so that the platform can send emails to the specified recipient according to the predefined email template.

Before You Start

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Visitor** → **Basic Settings** → **Email Template** .
2. Click **Add**.
3. Enter the required parameters.

   Email Type

   Define when the platform automatically sends an email containing the information you predefined to the specified recipient.

   Send Email When Reservation Approved

   The platform automatically sends an email to the specified recipient when a visit reservation is approved.

   Send Email When Checked-In

   The platform automatically sends an email to the specified recipient when a visitor checks in.

   Send Email When Reservation Rejected

   The platform automatically sends an email to the specified recipient when a visit reservation is rejected.

   Recipient

   Set the type of the email recipient (visitor or host).

   Assume that you have set **Email Type** to **Send Email when Reservation Approved** and **Recipient** to **Visitor**, a visitor will receive an email when their visit reservation is approved, as long as their email address is provided in the reservation.

   Name

   Create a name for the template.

   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 report content to be sent. You can also click the buttons below the **Content** parameter 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.
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:** Perform the following operation(s) after adding the email template:

Edit Template	Click ✎ in the Operation column to edit template details.
Delete All Templates	Click **Delete All** to delete all the added templates.

Note

On the email template list page, there are two default templates. You can view or edit default templates but not delete them.

19.2.7 Add a Visitor Pass Template

The platform offers a default visitor pass template that defines a default style for the visitor passes. If the default style does not meet your needs, you can add a visitor pass template to customize the style.

Steps

1. In the top left of the Home page, select ▦ → **All Modules** → **Visitor** → **Basic Settings** → **Visitor Pass Template** .
2. Click + to enter the Create Visitor Pass page.

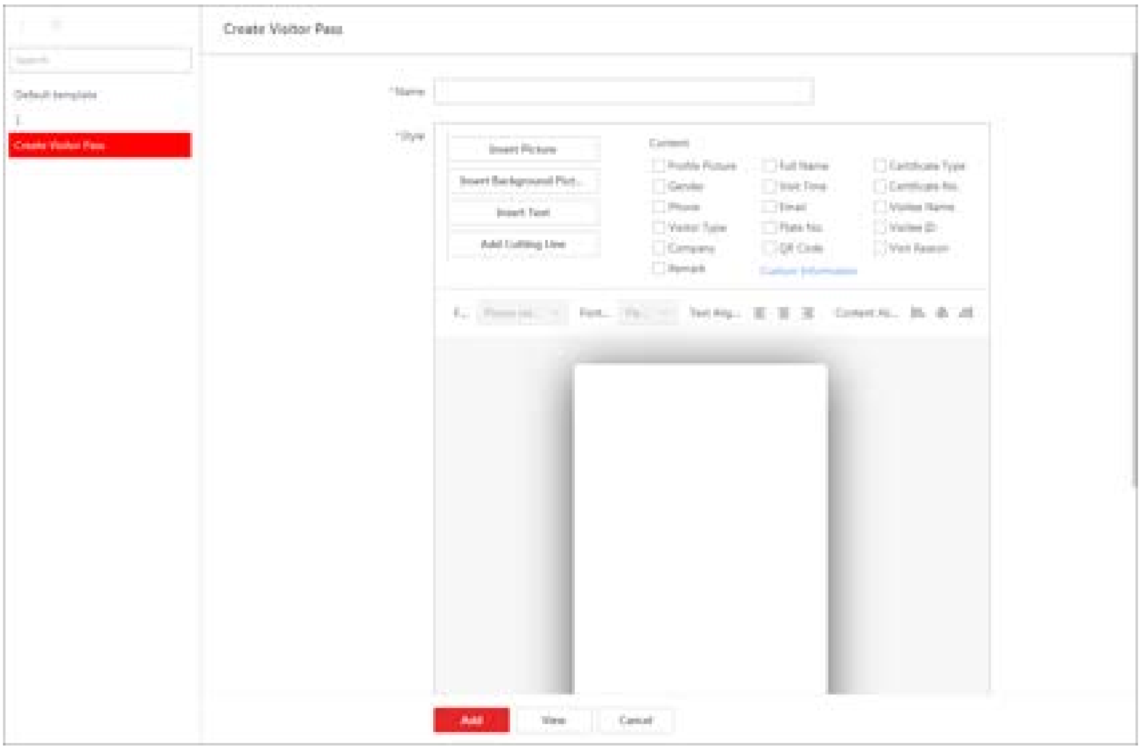


Figure 19-6 Create Visitor Pass Page

3. Create a name for the visitor pass.
4. Perform one or more of the following operations to add elements to the visitor pass template.

Insert Background Picture Click **Insert Background Picture** to select a picture from the local PC and set it as the background of the visitor pass template.

Set Content Check the check-box(es) to add the content elements. 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 visitor pass template.

Insert Text Click **Insert Text** to add a text box onto the visitor pass 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 onto the visitor pass template.

5. Adjust positions of 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 to Top**, **Stick at Bottom**, **Move Up**, **Move Down**.

6. **Optional:** Right click an element and then click **Delete** in the right-click menu.
7. **Optional:** Click **View** to preview the visitor pass template.
8. Click **Add** to add the visitor pass 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 🗑 .

19.2.8 Set Basic Parameters

To manage visitors in actual scenarios, you can set basic parameters such as Default Check-Out Time, Take Photo of Visitor's Belongings, Auto Checkout for Visitor After Effective Period, Visit Purpose, Email Template, Visitor Reservation Code format.

Steps

Note

If you do not configure basic parameters, the platform will manage visitors via the default value.

1. In the top left of the Home page, select ■ → **All Modules** → **Visitor** → **Basic Settings** → **Basic Parameters** .
2. Configure the following parameters according to your need.

   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 need.

   Auto Checkout for Visitor After Effective Period

   With the **Auto Checkout for Visitor After Effective Period** enabled, if the visitor does not check-out before the end time of the visit, the platform will automatically check out for the visitor. You can set a frequency for detecting whether the visitors have checked out. For example, you set 30 min as the detection frequency, the platform will check the visiting status of all visitors every 30 minutes on the platform. If the platform discovers visitors who have not checked out before the end time of visit, it will check out the visitors. Note that the **Alarm Detection** will be disabled if you enable **Auto Checkout for Visitor After Effective Period**.

   Alarm Detection

   With **Alarm Detection** enabled, if a visitor does not check-out before the end time of visit, an alarm will be triggered for notification. You can set a frequency for detecting whether the visitors have checked out. For example, you set 3 min as the alarm detection frequency, the platform will check the visiting status of all visitors on the platform. If the platform discovers visitors who have not checked out before the end time of visit, an alarm will be triggered. Note that the **Auto Checkout for Visitor After Effective Period** will be disabled if you enable **Alarm Detection**. By default, the **Detection Frequency** should range from 3 to 10 minutes.

   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 for the visitor.

   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 reserving, the visitor will receive the reservation code by email and text message. When checking in, the visitor should provide the reservation code.

   Print Visitor Pass When Check-In

   When enabled, the printer connected to your PC will automatically print a visitor pass once a visitor is checked in.

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 a Visitor Pass Template*** .

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.

Check-In Not Required if Reservation Confirmed

Applicable to reception areas where neither receptionist nor visitor terminal is deployed. If the option is selected, visitors will be automatically checked in when reservations are made for them.

Visit Purpose

You define visit purposes as options on the Reserve page. Click **Add** to add a new visit purpose. You can also edit the names of visit purpose, delete a visit purpose, or search a visit purpose.

Email Template

You can select an email template to let the platform automatically send an email based on selected email template to the specified recipient (the host or visitor) in the following cases.

Note

- If the recipient is the host, make sure that the host's email address is provided when add the host the platform. For details, see ***Add a Person Manually*** .
  If the recipient is the visitor, make sure that the visitor's email address is provided when make a reservation for or check in the visitor.
- You can customize email templates according to your need. See ***Add Visitor Email Template*** for details.

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 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.

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.

Custom Configuration

Customize visitor attributes and the fields that will be displayed on the visitor reservation page and visitor check-in page.

Custom Visitor Attribute

Click **Add** to add custom visitor attributes. The added ones will be displayed as fields on the visitor reservation page and 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 visitor reservation page as shown in the figure below.

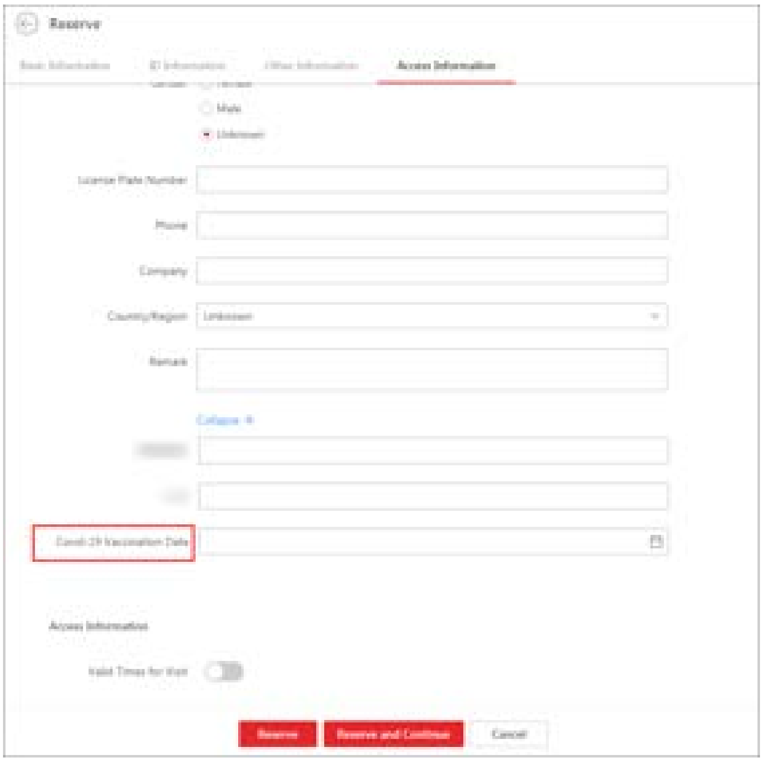


Figure 19-7 Example

Custom Field for Reservation & Check-In

Select additional fields that can be displayed on the visitor reservation page and visitor check-in page from the Available area.

For example, you can check **All** in the Available area and then click › to set all the available fields as the additional fields that will be displayed on the visitor reservation page and visitor check-in page. Moreover, you can turn on the switches in the Set as Required column to set corresponding fields as required fields.

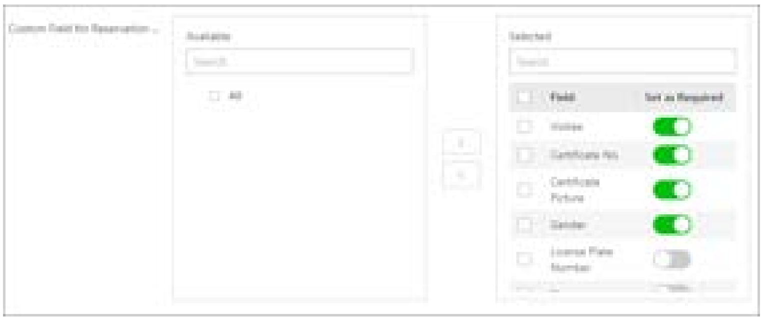


Figure 19-8 Set All Available Fields as Additional Fields

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 hover the cursor onto the icon and then click **View** or **Apply Again** to view the failure details or apply the authorization code to visitor terminals again.

19.3 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.

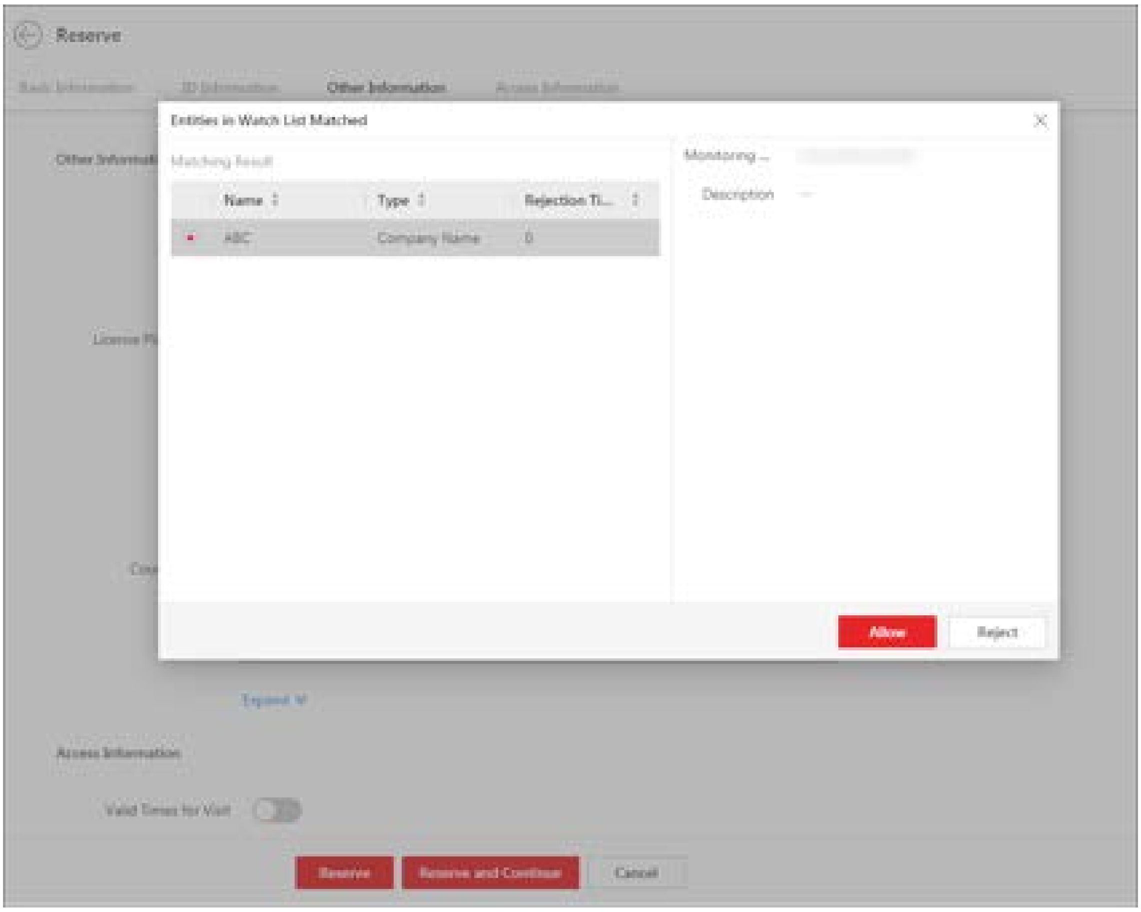


Figure 19-9 The Entities in Watch List Window

19.3.1 Configure Category and Match Method

You can define the categories of entities to be monitored and the methods to determine that attributes (e.g., name and ID) of a visitor match the entities in the watch list.

Steps

1. In the top left of the Home page, select ▦ → **All Modules** → **Visitor** → **Watch List** to enter the Watch List page.
2. Click **Category and Match Method** to open the Category and Match Method pane.
3. Add entity categories.
   1) Click **Add** on the Category and Match Method pane to open the category-adding window.
   2) Create a category name.
   3) **Optional:** Enter a remark for the category.
   4) Click **Add**.
   5) **Optional:** Perform one or more of the following operations.

- Edit Category: Click a category name to edit the category information.
- Delete Types: Select categories and then click **Delete** to delete the selected ones. Or hover the cursor onto ⌄ and then click **Delete All** to delete all categories.

4. Set the method(s) for matching entities in the watch list during reservations or checked-in.

Match via Name

If the name of a visitor 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 ID

If the ID number of a visitor 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 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.

5. Configure name matching settings.

Note

To make the name matching 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.

6. Click **OK**.

19.3.2 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. In the top left of the Web Client, select 🟥 → **All Modules** → **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 first name, last name, category, effective period, ID type, ID number, and ID picture.
- For **Company**, set other information including company name, category, and effective period.
- For **Country/Region**, set other information including country/region, category, and effective period.

Category

Select a category that the entity belongs to. Or click **Create New Category** to create a new one.

You can manage categories in **Category and Match Method**. For details, see ***Configure Category and Match Method*** .

Effective Period

If enabled, you can determine the period when the platform monitors the entity. If disabled, the platform monitors the entity indefinitely.

5. **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 return to be 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.

19.3.3 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. In the top left of the Home page, select ■ → **All Modules** → **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.

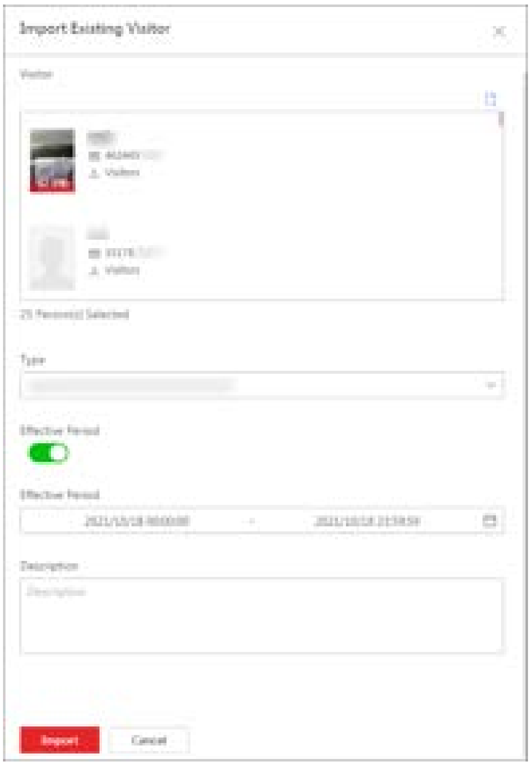


Figure 19-10 The Import Existing Visitor Pane

4. Set other information, including category, effective period, and description.

   Category

   Select a category to which the entity belongs.

   Make sure you have added categories in **Category and Match Method**. For details, see ***Configure Category and Match Method*** .

   Effective Period

   Determine the period that 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 return to be 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.

19.4 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.

19.4.1 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. In the top left of the Home page, select ▦ → **All Modules** → **Visitor** → **Visitor Reservation** .
2. Click **Reserve** on the top left to enter the Reserve page.
3. Set basic information for the visitor, such as name, host, visit purpose, visit time, visitor types. You can also upload a profile picture for the visitor.

   Note

   You can customize parameters such as visit purpose, visitor type, etc. See ***Set Basic Parameters*** .
4. Set ID information for the visitor, including ID type, ID No., and ID picture.
5. Set other information.
   1) Set license plate number, gender, and email, etc.

      License Plate Number

      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.

      Email

      Enter the visitor the email address for receiving an email containing the reservation code or notification that the visit reservation is approved/rejected.
   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

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 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.

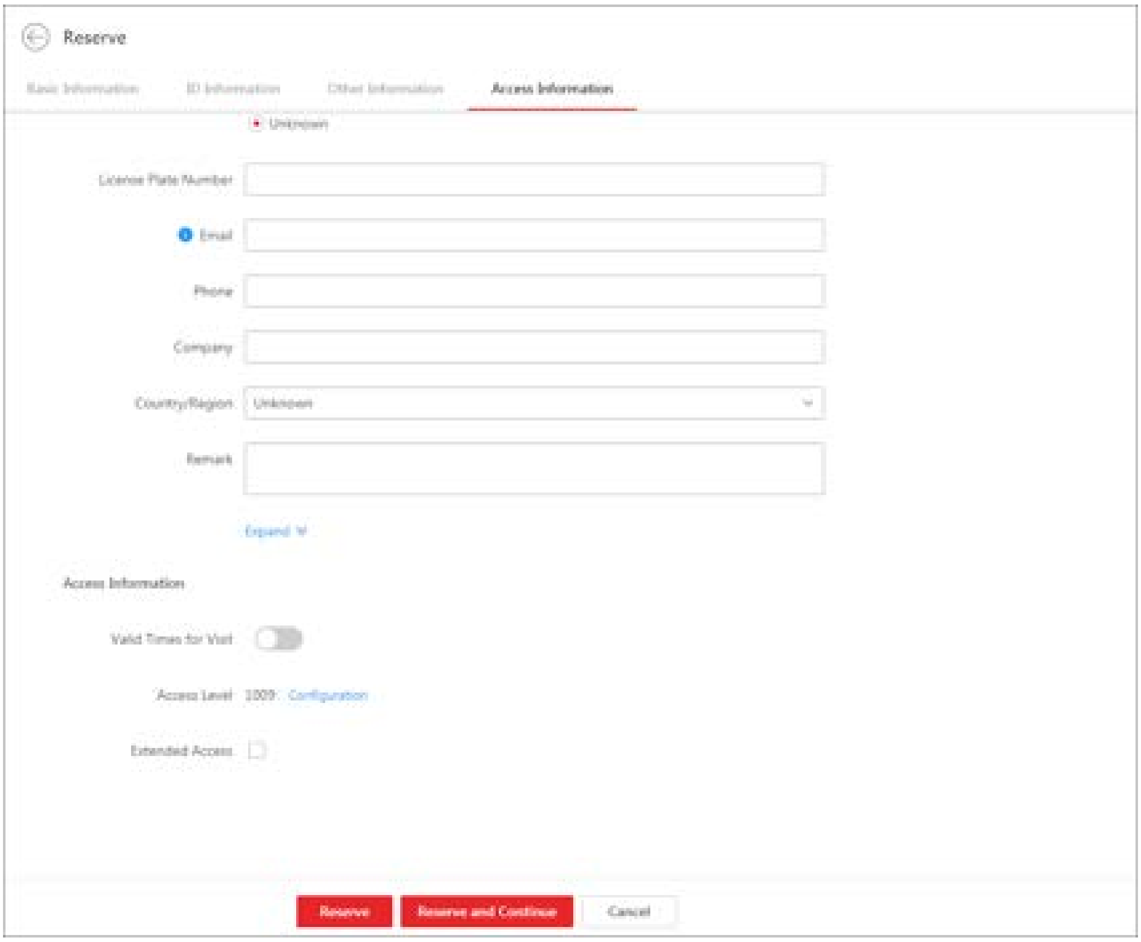


Figure 19-11 Set Access Information

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.
- Send emails to notify the specified recipient that the visitor is checked in (if the email information 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 phone and estimated entry time, and then click **Filter** to filter reservations. For the **Status** condition, you can click ⌄ to select one or more reservation status (reserved, expired, and checked in) 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.

19.4.2 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

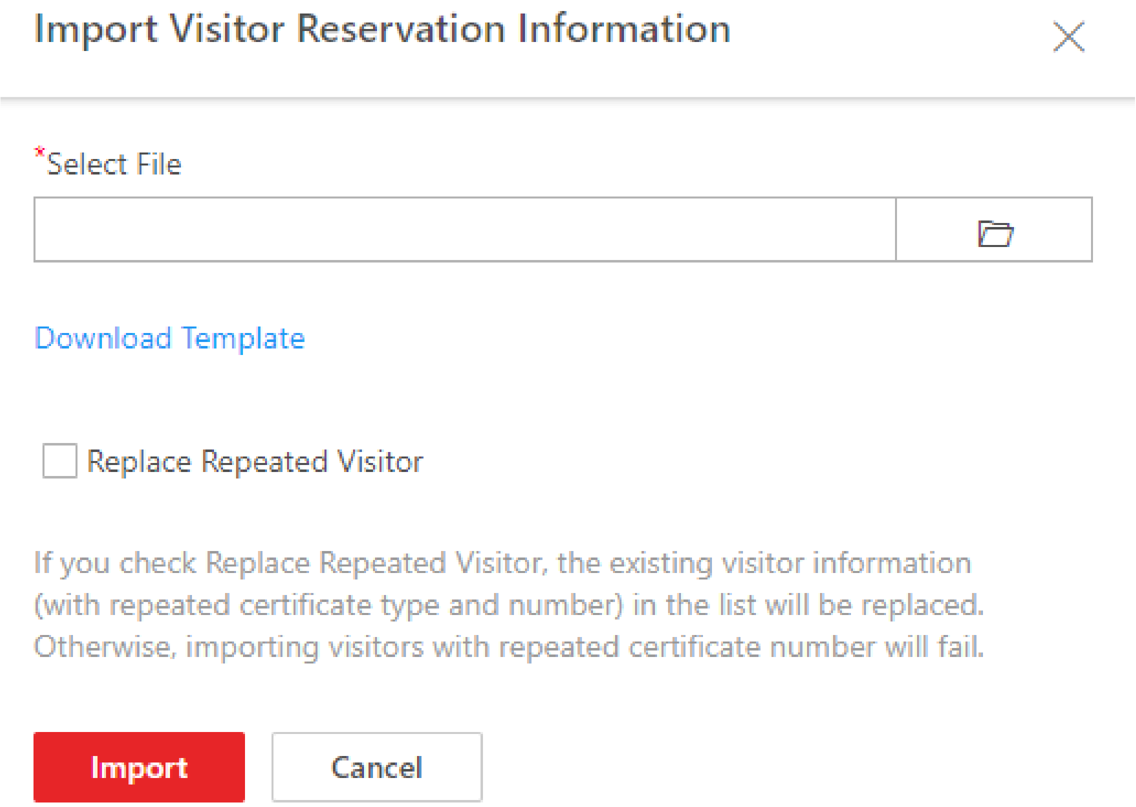
Before any operations in the visitor system, you can set the parameters according to actual situation such as setting basic parameters to define the scenario for the visiting process, managing visitor types, assigning access levels for visitors, etc. See ***Configurations Before Visitor Management*** for details.

Steps

1. In the top left of the Home page, select 🟥 → **All Modules** → **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.



Import Visitor Reservation Information

*Select File

Download Template

□ Replace Repeated Visitor

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 19-12 Import Visitor Reservation Information

7. Click **Import**.
8. **Optional:** Check one or more visitor 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 deleting.

19.4.3 Review Visitor Reservations

If you have enabled Self-Service Reservation Approval function when you set visitor self-service registration 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 Self-Service Reservation Parameters*** for details.

Steps

Note

You need to have the permission (**User Permission → Configuration Permission → Visitor → Reservation Approval**) shown in the picture below before you can review reservations.

Figure 19-13 The Permission for Reviewing Reservations

1. In the top left of the Home page, select 🟥 **→ All Modules → Visitor → Visitor Reservation** .

   Note

   If there are visitors to be approved, the number of the to-be-approved visitors will be displayed.

   Figure 19-14 The Number of The To-Be-Approved Visitors

2. Click **To Be Reviewed** on the top to enter the following page.

   On the page, you can view the information of the to-be-approved visitors, such as their companies and whether their attributes match entities in the watch list.

[redacted]

Figure 19-15 Visitor To Be Approved

3. **Optional:** Click ▿ to filter reserved visitors by name, ID, gender, 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-Registered 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.

19.5 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.

19.5.1 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 fingerprint and face picture) or QR code, and be able to access the predefined doors and floors.

Steps

1. In the top left of the Home page, select → **All Modules** → **Visitor** → **Visitor Check-In** .
2. Click **Unreserved Visitor Check-In**.
3. Edit basic visitor information, including name, profile picture, host, visit purpose, check-out time, and visitor type.

   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 set the visitor profile picture in three ways: collecting a face picture from devices, taking a picture by the camera of your computer, or uploading a picture saved in your computer.
   - Hover the cursor on the uploaded profile picture and click **×** to delete it.

4. Click **Credential Management** to set the credentials for the visitor, including 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.

   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 19-16 Read Card

Note

Only one card can be issued to a visitor.

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 **Configuration** to set the collection mode as follows.

USB Fingerprint Recorder

Collect fingerprint 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 fingerprint 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 fingerprint 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 fingerprint on the device and it will enroll your fingerprint automatically.

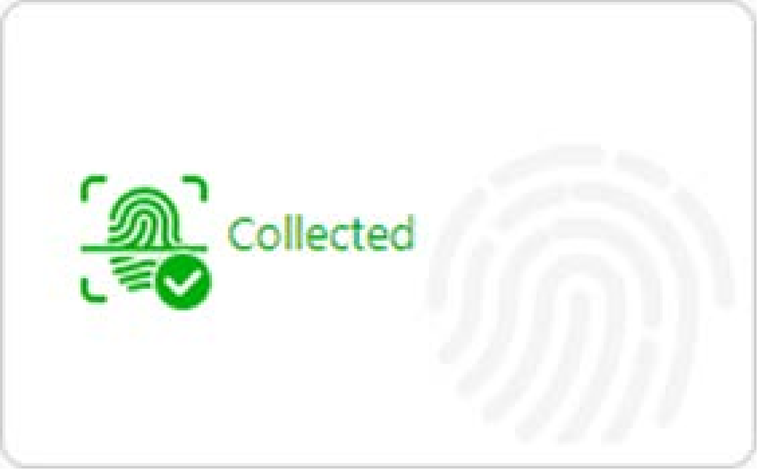


Figure 19-17 Fingerprint Recorded

Note

- No more than one fingerprint can be collected for 1 visitor.
- You can configure either cards or fingerprints.

5. **Optional:** Edit the ID information, including selecting certificate type, entering certificate No., and taking/uploading a certificate photo.
6. **Optional:** Take belongings photo.

Note

Make sure you have enabled this function. See ***Set Basic Parameters*** for details.

7. Set other information.

   1) Set other information, such as license plate number, gender, and skin-surface temperature.

   License Plate Number

   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 from the parking lot.

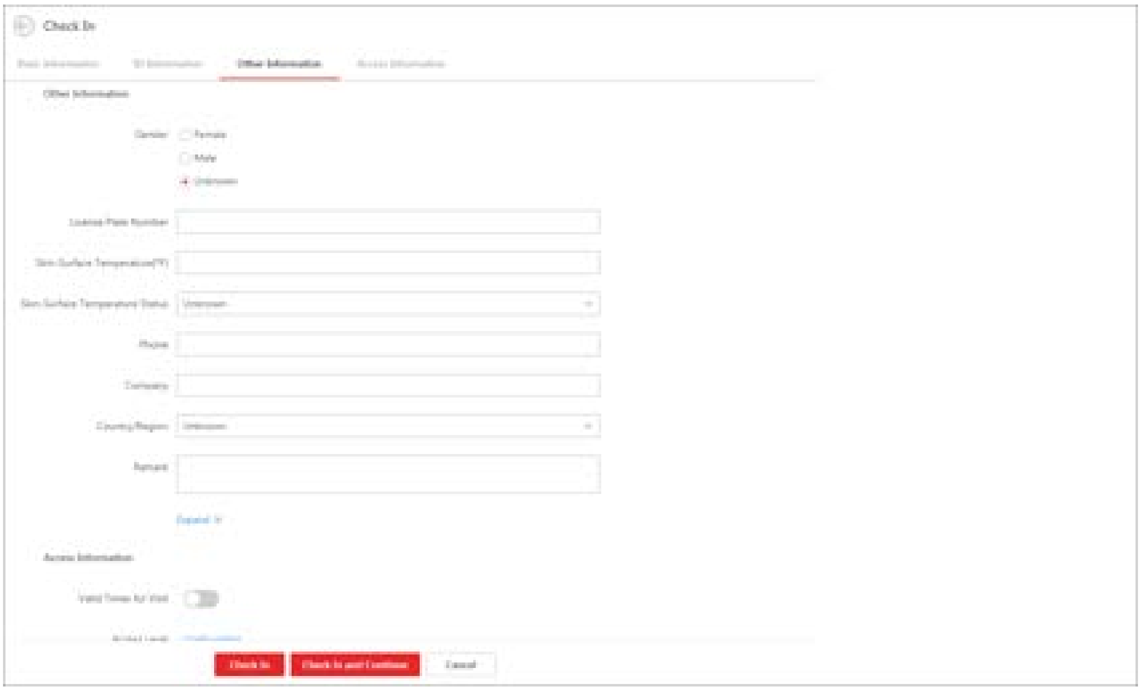
   Email

   Enter the visitor's email address for receiving an email containing the QR code or notification that the visitor has checked in.

   2) 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*** .



Other Information

Gender: ○ Female ○ Male ● Unknown

License Plate Number:

Skin-Surface Temperature(°F):

Skin-Surface Temperature Status: Unknown

Phone:

Company:

Country/Region: Unknown

Remark:

Expand

Access Information

Valid Times for Visit:

Access Level:

Figure 19-18 Set Other Information

8. 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

   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 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.

9. Complete checking in the visitor.
   - Click **Check In**.

     If the operation succeeds, 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.
   - Click **Check In and Continue** to check in the visitor and continue to check in another.

10. Go back to the Visitor Check-In page to check whether the visitor information fails to be applied to the visitor terminal(s). If fails, check failure details, troubleshoot, and apply again.

Note

If there is visitor information fails to be applied to visitor terminal(s), a notification will show at the top of the Visitor Check-In page (see the area marked in red in ***Figure 19-19***). In this case, you can click the notification to open the ***Figure 19-20*** to view the failure details and troubleshoot according to the failure reason shown on the window, and then apply the visitor information to visitor terminal(s) again.

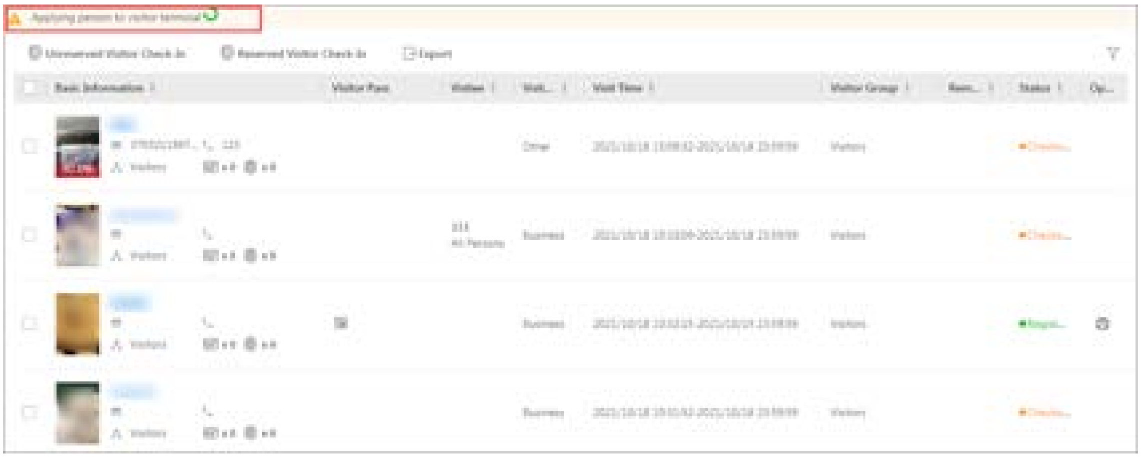
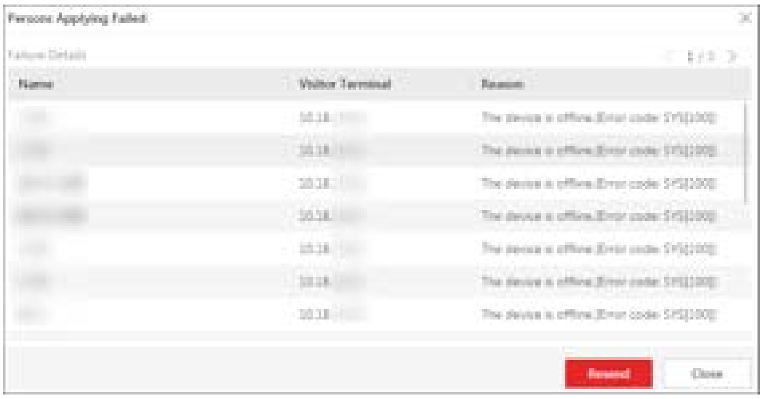


Figure 19-19 Notification on Applying Failures



Name	Visitor Terminal	Reason
[illegible]	10.18.[illegible]	The device is offline.(Error code: SYS[100])
[illegible]	10.18.[illegible]	The device is offline.(Error code: SYS[100])
[illegible]	10.18.[illegible]	The device is offline.(Error code: SYS[100])
[illegible]	10.18.[illegible]	The device is offline.(Error code: SYS[100])
[illegible]	10.18.[illegible]	The device is offline.(Error code: SYS[100])
[illegible]	10.18.[illegible]	The device is offline.(Error code: SYS[100])
[illegible]	10.18.[illegible]	The device is offline.(Error code: SYS[100])

Figure 19-20 Persons Applying Failed Window

11. **Optional:** Perform the following operations on the Visitor Check-In page if needed.

Filter Visitors

Click ▽ to filter visitors by conditions including ID No., name, phone, and company.

For the **Status** condition, you can click ⌄ to select one or more reservation status (reserved, expired, and checked in) to filter visitors.

You can also click **Select Additional Information** to filter visitors.

Export Visitors

Select visitors and click **Export** to export registered visitors to the computer 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 **Visitor Pass** 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*** .

19.5.2 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. In the top left of the Home page, select 🟥 → **All Modules** → **Visitor** → **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 certificate type and enter the certificate No.

   The Reserved Visitor Check In page will show.
5. Configure the visitor information. See ***Check In a Visitor Without Reservation*** for details.
6. Click **Check In**.

   Note

   If the operation succeeds, 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 fails, check failure details, troubleshoot, and apply again.

Note

If there is visitor information fails to be applied to visitor terminal(s), a notification will show on the top of the Visitor Check-In page (see the area marked in red in ***Figure 19-19***). In this case, you can click the notification to open the ***Figure 19-20*** to view the failure details and troubleshoot according to the failure reason shown on the window, and then apply the visitor information to visitor terminal(s) again.

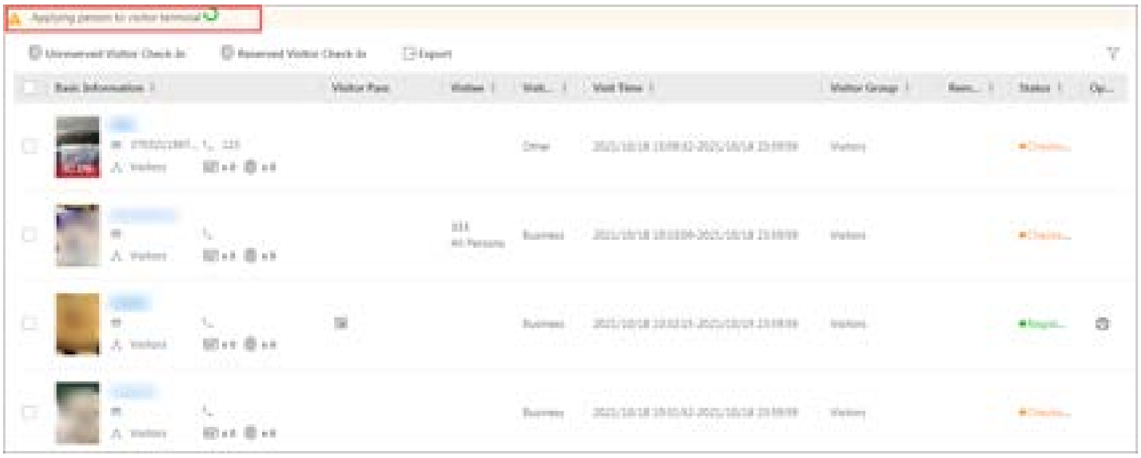

Applying persons to visitor terminal
Unreserved Visitor Check-In
Reserved Visitor Check-In
Export
Basic Information
Visitor Pass
Visitor Group
Status
Op...

Figure 19-21 Notification on Applying Failures

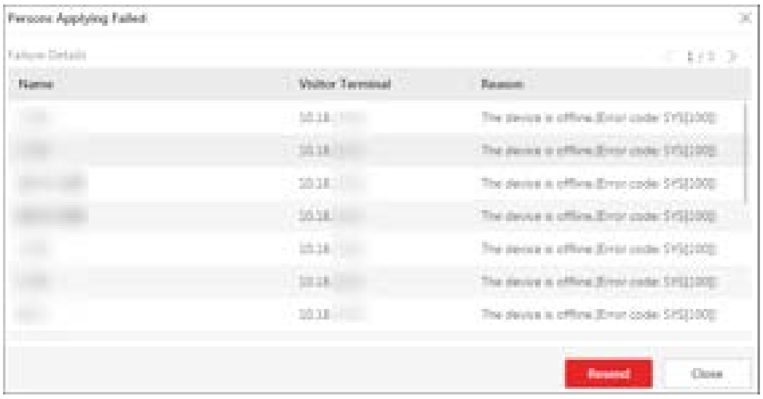


Figure 19-22 Persons Applying Failed Window

8. **Optional:** Perform the following operations on the Visitor Check-In page if needed.

Filter Visitors

Click to filter visitors by conditions including ID No., name, phone, and company.

For the **Status** condition, you can click to select one or more reservation status (reserved, expired, and checked in) to filter visitors.

You can also click **Select Additional Information** to filter visitors.

Export Visitors

Select visitors and click **Export** to export registered visitors to the computer 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 **Visitor Pass** 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.

19.5.3 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.

In the top left of the Home page, select ■ → **All Modules** → **Visitor** → **Visitor Check-In** → **Visitor Information** to view the list of all the checked-in 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.
- **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.

19.6 Manage Entry & Exit Rule for Visitors' Vehicles

If one visitor comes by driving a vehicle, when registering, you need to enter the license plate number so that the platform can control the barrier to open when the capture unit of the parking lot detects this license plate.

Default Vehicle List for Visitors

There is one default vehicle list which is for the vehicles of visitors only in the Vehicle module. After visitor registration, 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 information 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 registered visitors on the **Entry & Exit Rule** page.
By default, the rule is: Whenever the vehicles in the vehicle list for visitors entering the parking lot, the platform will automatically open the barrier; Whenever the vehicles in the vehicle list for visitors exiting the parking lot, the platform will automatically open the barrier. You can edit this rule according to actual needs.

Note

For details about editing entry & exit rule, see ***Manage Entry & Exit Rules for Parking Lots*** .

Note

This rule cannot be deleted.

19.7 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 he/she leaves.

In the top left of the Home page, select ▦ → **All Modules** → **Visitor** → **Visitor Check-Out** to enter the Visitor Check-Out page.

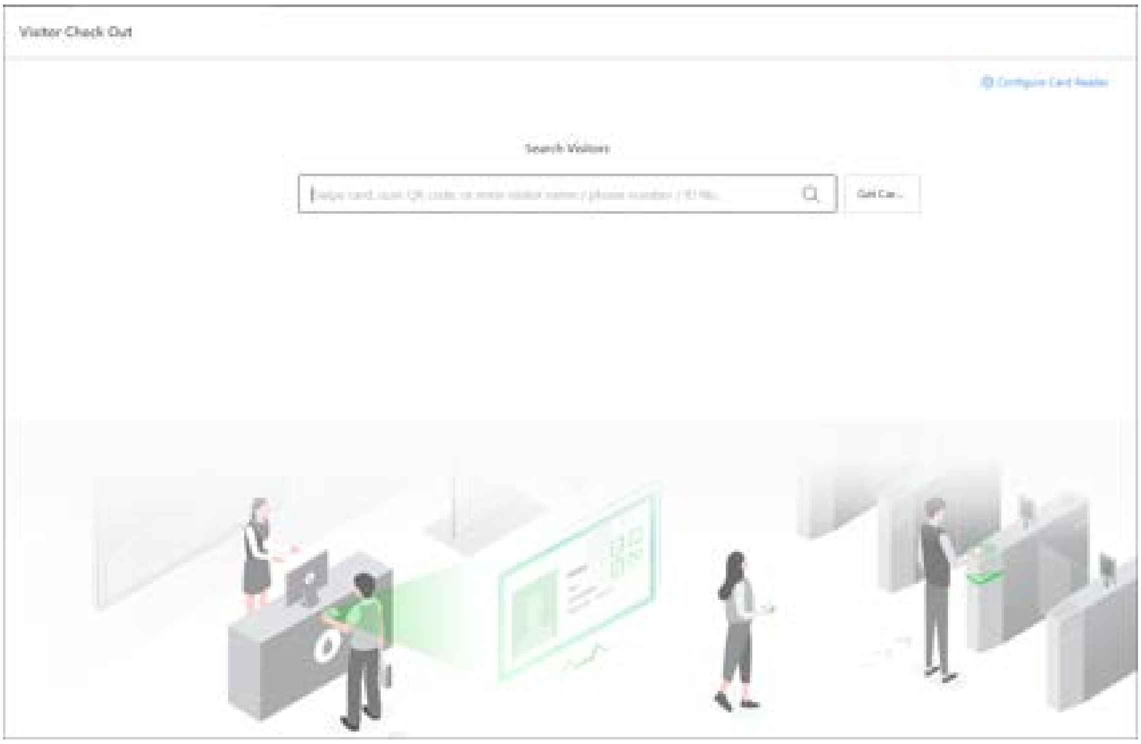

Visitor Check Out
Configure Card Reader
Search Visitors
Swipe card, scan QR code, or enter visitor name / phone number / ID No.
Get Car...

Figure 19-23 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 registering, 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.
For details about how to configure the card reader, see ***Set Card Issuing Parameters*** .

Search for and Check out a Visitor

You can enter the name, phone number, ID number of a visitor on the Visitor Check-Out page, and click 🔍 to search for the visitor, and then click **Check Out** on the search result page to check out her/him.

Check out a Visitor by Scanning QR Code

If a barcode reader has been plugged into the PC where the platform runs, you can use the barcode reader to scan the QR code on the visitor pass of a visitor to check out the visitor.

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 **Auto Checkout for Visitor After Effective Period** is enabled on the Basic Parameters page. For details, see ***Set Basic Parameters*** .

19.8 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 time.

In the top left corner of the Home page, select ■ → **All Modules → 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 reason, visit time, status, and skin-surface temperature. 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 (reserved, expired, and checked in) to filter visitors.

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 20 Time & Attendance

In the Attendance module, you can easily manage the time & attendance system of your organization and track your employees' attendance.

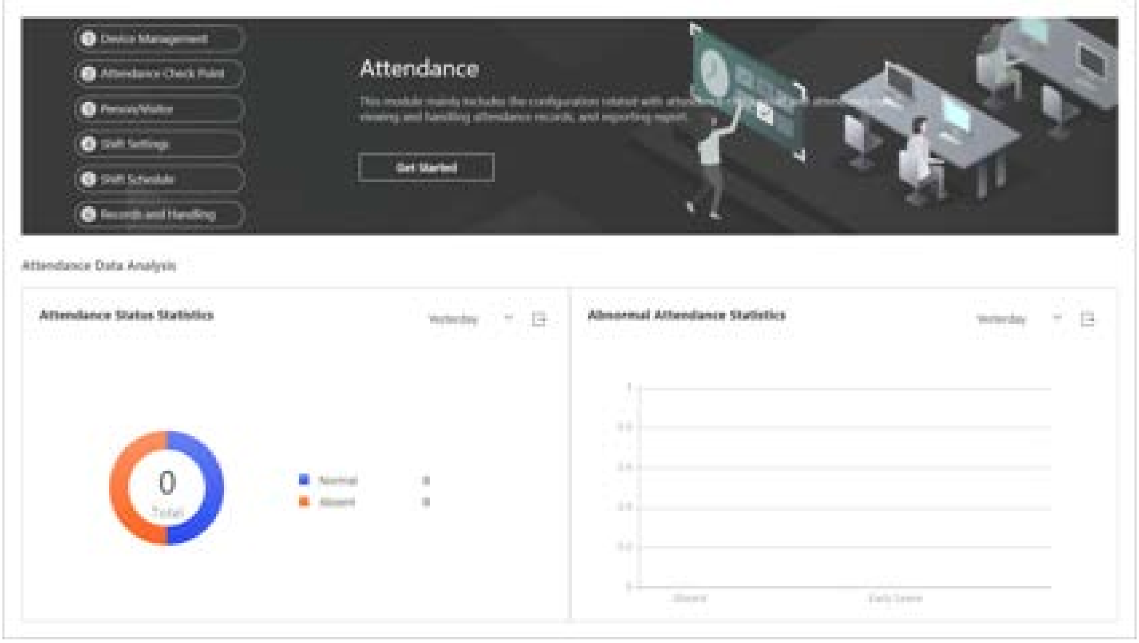


Figure 20-1 Time & Attendance Overview

The overview page shows the most recent attendance statistics:

- **Attendance Status Statistics**: Displays attendance status data in a doughnut chart.
- **Abnormal Attendance Statistics**: Displays abnormal attendance records in a bar chart.

Note

- You can select the time range from **Yesterday**, **Last 7 Days**, and **Last 30 Days**.
- You can export the current chart to local PC.

To set up a time & attendance system from the start, click **Get Started** and follow the instructions on screen.

Note

You can move cursor to ◀ on the right to browse through all steps.

To get detailed instructions on each step, refer to ***Flow Chart*** .

20.1 Flow Chart

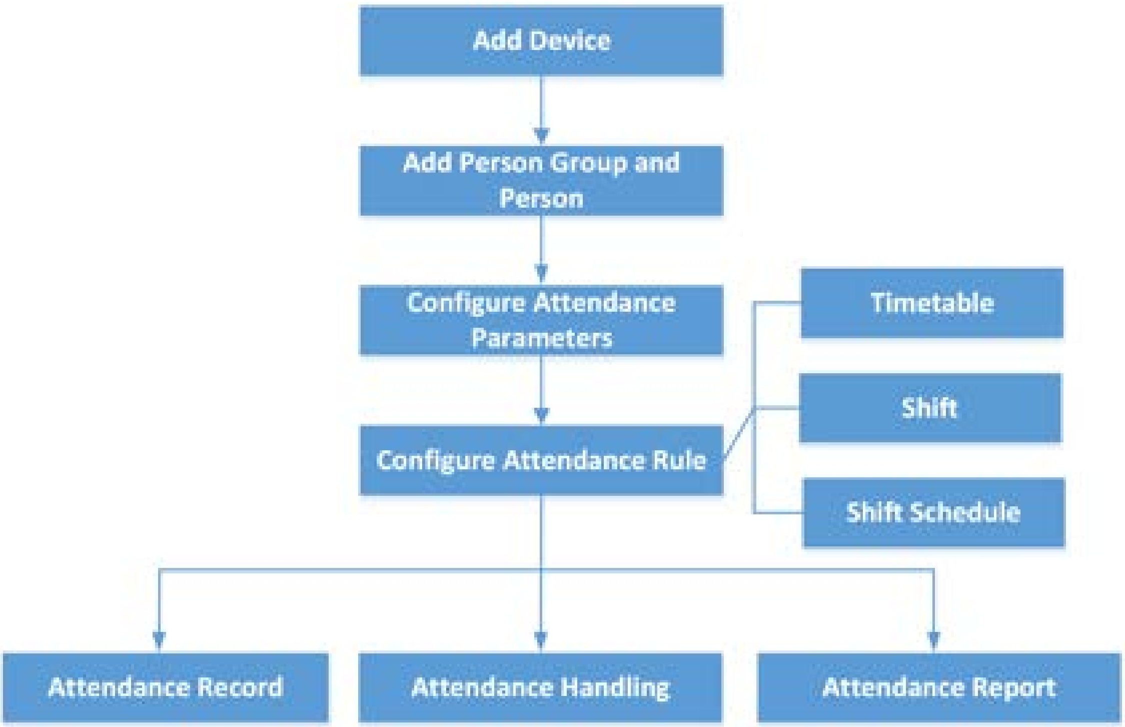


Figure 20-2 Flow Chart for Time & Attendance

- **Add Device**: Add devices (e.g., access control devices) to the platform. For more details, refer to ***Resource Management*** .
- **Add Person Group and Person**: Add person groups and persons. For more details, refer to ***Add Person Groups*** and ***Add Person*** .
- **Configure Attendance Parameters**: Configure attendance check points, general rule, overtime rule, leave types, display rule for report, third-party database, etc. For more details, refer to ***Configure Attendance Parameters*** , ***Set Display Rules for Attendance Report*** and ***Synchronize Card Swiping Records to Third-Party Database*** .
- **Configure Attendance Rule**: Add timetable (including break timetable and work timetable), shift, and shift schedule. For more details, refer to ***Add Timetable*** , ***Add Shift*** or ***Manage Shift Schedule*** .
- **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 ***Manage Attendance Record*** .
- **Attendance Report**: Export attendance report to local PC or send it via email regularly. For more details, refer to ***Manage Attendance Reports*** .

20.2 Configure Attendance Parameters

You can configure the attendance parameters, including the weekends, absence rule, overtime parameters, attendance check point, leave type, etc.

20.2.1 Add Attendance Check Point

You can set the access points (or linked card readers), cameras which support facial recognition (such as DeepinView series camera, and the camera connected with DeepinMind series NVR), or terminals as attendance check points, 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. In the upper-left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Basic Settings** .
2. Click **Attendance Check Point** on the left to enter the attendance check point management page.
3. Click **Add**.
4. Select the type of the attendance check point.

   Check-In & Out

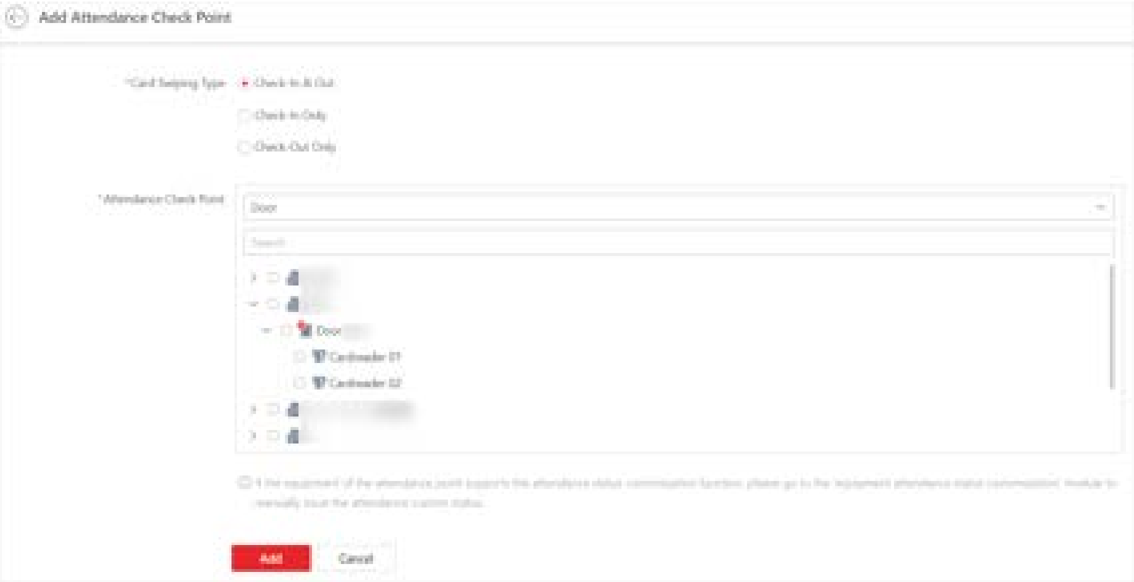
   The attendance records of check-in or check-out on the attendance check point are both valid.

   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.
5. Select the resource type (e.g., door) from the drop-down list.



Add Attendance Check Point

*Card Swiping Type ● Check-In & Out

○ Check-In Only

○ Check-Out Only

*Attendance Check Point: Door

Search

□ Door

□ Cardreader 01

□ Cardreader 02

If the equipment of the attendance point supports the attendance status customization function, please go to the 'equipment attendance status customization' module to manually issue the attendance custom status.

Figure 20-3 Add Attendance Check Point

All the resources which have not been set as attendance check point will be displayed.

6. 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.

7. Click **Add**.

The selected resources will be displayed in the attendance check point list.

8. 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.

20.2.2 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.

In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Basic Settings** → **General Rule** .

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.

20.2.3 Define Absence

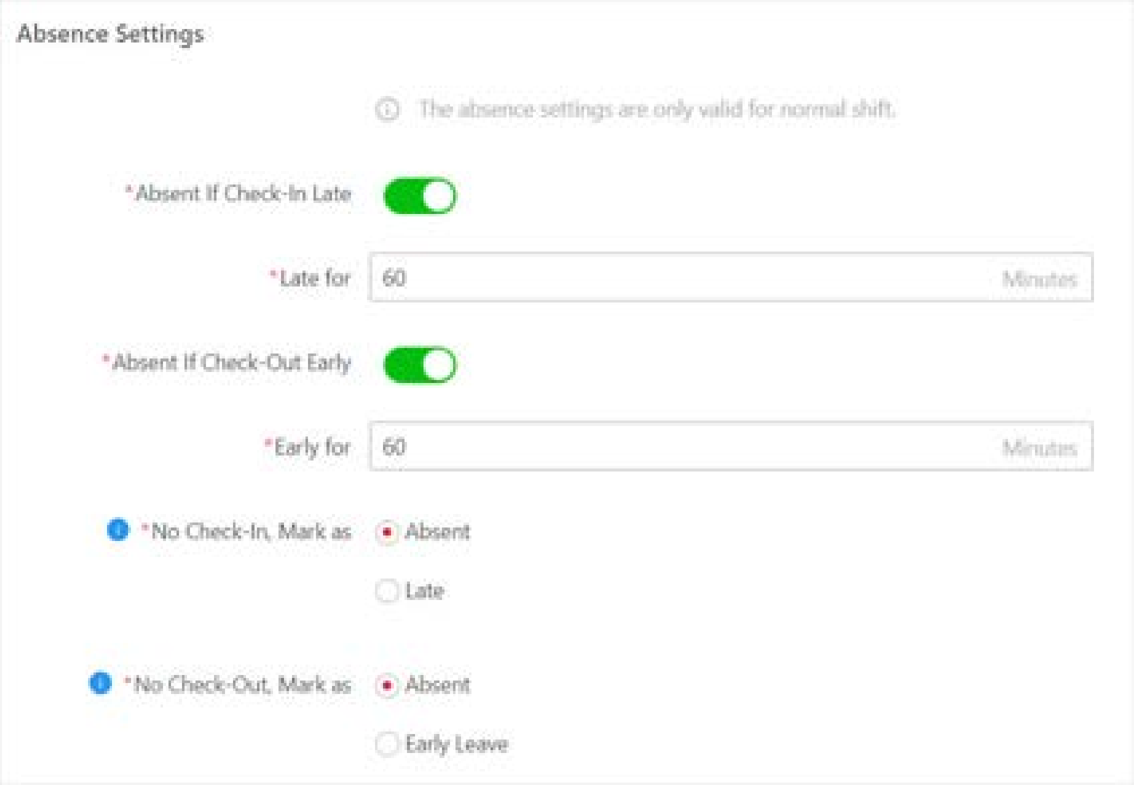
You can define a global rule for absence. When the employee's attendance conforms to the absence rule, the attendance record will be marked as absent or other status you define.

In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Basic Settings** → **General Rule** .

In the Absence Settings area, you can define the absence rules.

Note

The absence settings are only valid for normal shift.



Absence Settings

ⓘ The absence settings are only valid for normal shift.

*Absent If Check-In Late: On

*Late for: 60 Minutes

*Absent If Check-Out Early: On

*Early for: 60 Minutes

*No Check-In, Mark as: ● Absent ○ Late

*No Check-Out, Mark as: ● Absent ○ Early Leave

Figure 20-4 Absence Settings

Set Absence Rule for 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.

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 for** 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.

Set Absence Rule for Check-Out

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.
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 16:00-21:00 (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*** .

20.2.4 Configure Authentication Mode

You can configure authentication modes, including card, fingerprint, and face. After setting authentication mode, you can get attendance records of the configured authentication mode and calculate attendance data of the configured authentication mode.

In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Basic Settings** → **General Rule** .

Switch on **Customize Authentication Mode**, and select card, fingerprint, or/and face as the authentication mode.

Note

This function requires device capability.

20.2.5 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. In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Basic Settings** → **General Rule** .
2. In the Auto-Calculate Attendance area, select a time in **Calculate at**.

3. Click **Save**.

20.2.6 Configure Attendance Result Accuracy

You can control the degree of accuracy of each attendance statistic data, such as late duration, break duration, overtime duration, and actual work hours.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Attendance** → **Basic Settings** → **General Rule** .
2. In the Advanced Settings area, set the parameters for each attendance statistics type in **Attendance Result Accuracy**.

   Min. Unit

   Set the minimum unit for the result item.

   You can set the minimum unit to 1 Minute, 0.5/1 Hour, or 0.5/1 Day.

   Rounding

   Rounding means replacing the number with a neighboring value that fits the minimum unit.

   You can choose to round up, round down, or round to the nearest value.

   Display Format

   Choose the display format of the time.

   Example

   For example, you set **Min. Unit** to 0.5 Hour, set **Rounding** to Round Up, and set **Display Format** to HH:MM.

   - If the actual duration is 1 to 30 minutes, the statistic data displayed will be *0h30min*.
   - If the actual duration is 31 to 60 minutes, the statistic data displayed will be *1h0min*.
3. Click **Save**.

   You can see the attendance results according to your accuracy settings in attendance records or attendance reports.

20.2.7 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. In the upper-left corner of Home page, select → **All Modules** → **Attendance** → **Basic Settings** .
2. Select **Overtime** on the left to enter the overtime settings page.
3. Set **Work Hour Rate** for each overtime level (work hours = work hour rate × actual overtime).

Note

When a person works outside the scheduled work time on workdays, the person will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3. You can set different work hour rates for three overtime levels.

Example

For example, a person's actual overtime is 1 hour (in overtime level 1), and the work hour rate of overtime level 1 is set to 2.50, so the work hours will be calculated as 2.50 hours.

4. In the Overtime in Workdays area, switch on **Calculate Overtime** to set the calculation mode of overtime duration on workdays.

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 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

Select the overtime levels and drag on the time slot to set the range of the selected overtime levels. The total work hours will be calculated according to the work hour rate of each overtime level.

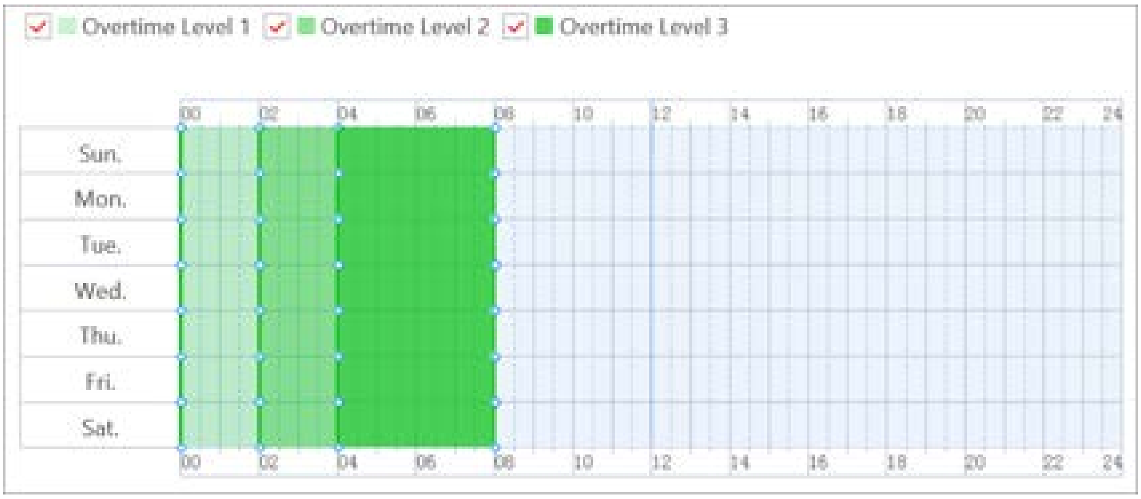


Figure 20-5 Overtime Level Settings

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.

5. In the Overtime on Holidays area, set the overtime rule for holidays.

If Overtime 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 time 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

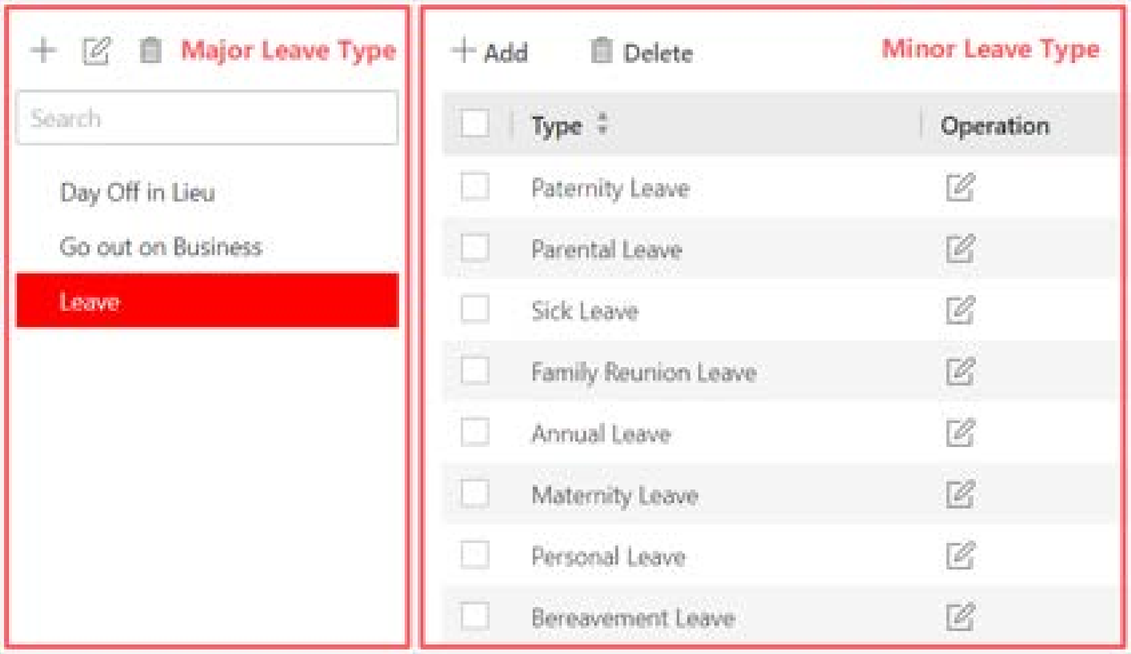
- To add a new holiday, click **Add Holiday**.
- To edit holidays, click **Holiday Settings**.

6. **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.
7. Click **Save**.

20.2.8 Manage Leave Type

A leave type represents the reason for a leave. You can customize the leave types (major leave types and minor leave types) in advance and select them as the leave reason when applying for leave for persons in the platform. You can also edit or delete the leave types.

In the top left corner of Home page, select ■ → **All Modules** → **Attendance** → **Basic Settings** → **Leave Type** to enter leave type management page.



□	Type	Operation
□	Paternity Leave	✎
□	Parental Leave	✎
□	Sick Leave	✎
□	Family Reunion Leave	✎
□	Annual Leave	✎
□	Maternity Leave	✎
□	Personal Leave	✎
□	Bereavement Leave	✎

Figure 20-6 Leave Type Management Page

In the Major Leave Type area, you can add, edit, or delete the major leave types.

- Add Major Leave Type: Click + and create a name to add a new major leave type.
- Edit Major Leave Type Name: Select a major leave type and click ✎ to edit its name.
- Delete Major Leave Type: Select a major leave type and click 🗑 to delete the major leave type and all minor types in it.

Select a major leave type, the minor leave types of the major leave type are listed in the Minor Leave Type area. You can add, edit, or delete the minor leave types.

- Add Minor Leave Type: Click **Add** and create a name to add a new minor leave type under the major leave type.
- Edit Minor Leave Type Name: Click ✎ on the Operation column to edit the name of the minor leave type.
- Delete Minor Leave Type: Select the minor leave type(s) and click **Delete** to delete the selected minor leave type(s).

Note

After setting the leave types, you can select the leave type(s) from a list when applying for leave for persons. See details in ***Apply for Leave for a Single Person*** or ***Apply for Leave for Multiple Persons*** .

20.2.9 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 ■ → **All Modules** → **Attendance** → **Basic Settings** .
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 Check Name

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.

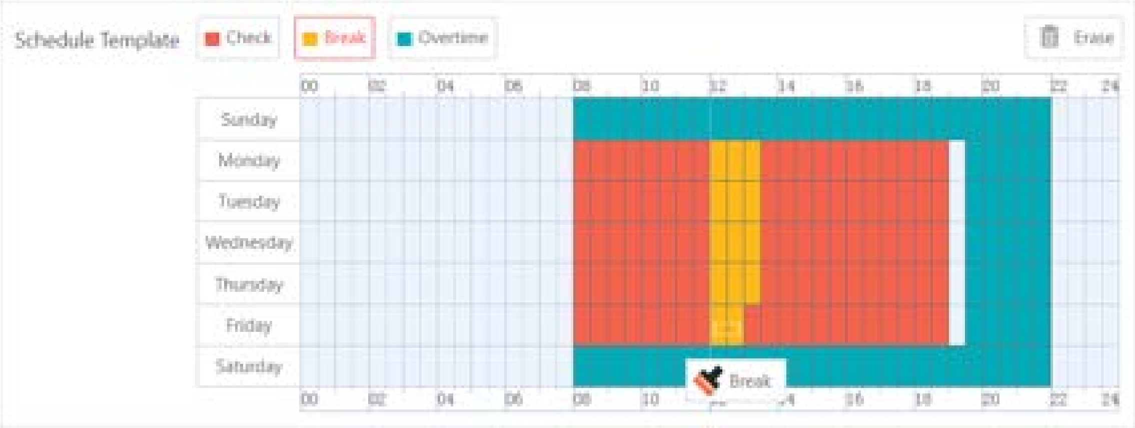


Figure 20-7 Schedule Template

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 ***Add Attendance Check Point*** .
- 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.

20.3 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 man-hour 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.

20.3.1 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. In the upper-left corner of Home page, select 🟥 → **All Modules → Attendance → Shift Settings** .
2. Select **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. **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 Man-Hour Shift*** .

20.3.2 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. In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Shift Settings** .
2. Click **Timetable** on the left to enter the timetable management page.
3. Click **Add**.
4. In **Basics**, set the following parameters.

Name

Create a descriptive name for the timetable.

Color

Click on the **Color** field and set the color for the timetable. Different colors represent the corresponding timetables when drawing for Shift Schedule in time bar.

Set Calculation Mode

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.

5. In **Attendance**, select **Normal Shift** as the timetable type.
6. Set the detailed rules for work time and check-in/out.

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.

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.

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**.

7. In **Break Time**, click **Add** to select the break timetables to define the break time in the timetable.

Note

- You can click **Add New** to create a new break timetable. See details in ***Add Break Timetables*** .
- Check **Count Break Time in Work Hours** to include the break time into work hours.

8. **Optional:** In **Timetable Overview**, view the timetable in a timeline.

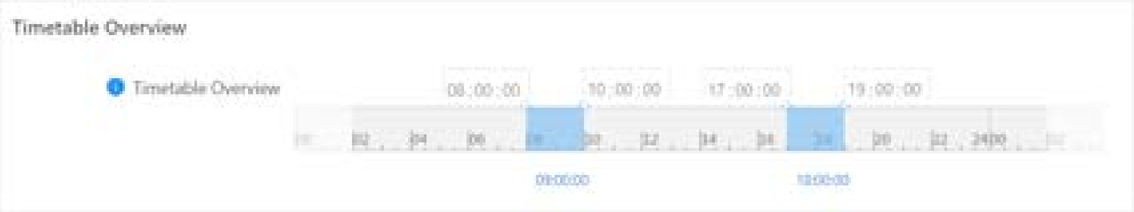


Figure 20-8 Timetable Overview

Note

You can drag the timeline to the left or right.

9. **Optional:** Switch on **Absence Settings** to 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.

10. 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*** .

20.3.3 Add Timetable for Man-Hour Shift

Man-hour 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. In the top left corner of Home page, select ▦ → **All Modules** → **Attendance** → **Shift Settings** .
2. Click **Timetable** on the left to enter the timetable management page.
3. Click **Add**.
4. In **Basics**, set the following parameters.

   Name

   Create a descriptive name for the timetable.

   Color

   Click on the **Color** field and set the color for the timetable. Different colors represent the corresponding timetables when drawing for Shift Schedule in time bar.

   Set Calculation Mode

   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.
5. In **Attendance**, select **Man-Hour Shift** as the timetable type.
6. Set the rules for work time and check-in/out.

   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.
7. In **Break Time**, click **Add** to select the break timetables to define the break time in the timetable.

Note

- You can click **Add New** to create a new break timetable. See details in ***Add Break Timetables*** .
- Check **Count Break Time in Work Hours** to include the break time into work hours.

8. **Optional:** In **Timetable Overview**, view the timetable in a timeline.

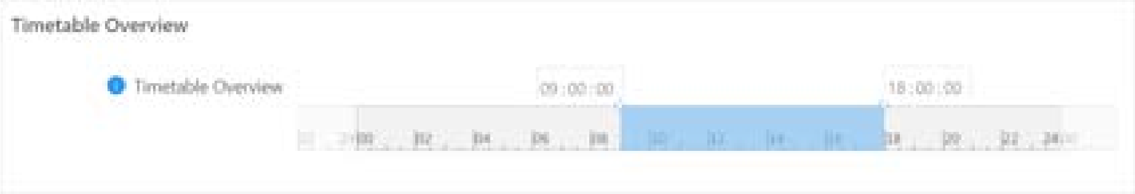


Figure 20-9 Timetable Overview

Note

You can drag the timeline to the left or right.

9. 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*** .

20.4 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 Man-Hour Shift*** .

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Attendance** → **Shift Settings** .
2. Click **Shift** on the left to enter the shift management page.
3. Click **Add**.
4. Set the shift's basic information, including creating a descriptive name and editing its description.
5. **Optional:** Select another shift from the drop-down list of **Copy from** field to copy the shift information to the current shift.
6. Set the shift's repeating pattern.

   Week

   The shift will repeat every 1 to 52 weeks based on your selection. If you select 2 or more weeks, you need to set the start week.

Day

The shift will repeat every 1 to 31 days based on your selection. You need to set a start date to define when the shift starts.

Month

The shift will repeat every 1 to 12 months based on your selection. If you select 2 or more months, you need to set the start date.

7. Select **Normal Shift** or **Man-Hour Shift** as the shift type.

   The corresponding timetables of normal shift or man-hour shift will be displayed.

8. Select a timetable and click on the table below to apply the timetable on each day.

Note

- For **Normal Shift**, you can apply more than one timetable in one day which requires the employees to check in and check out according to each timetable. The start and end work time and the valid check-in and out time in different timetables can not be overlapped.
- You can use up to 8 different timetables in one shift.

9. Select a general calculation mode for the shift.

Note

You can set a unique calculation mode for each timetable in the timetable settings page. General calculation mode only applies to the timetables without a calculation mode.

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/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

- If a timetable in the shift is not enabled with T&A Status on Device, it will be enabled if you enable this function for the shift.
  If a timetable in the shift is already enabled with T&A Status on Device, this setting will not change even if you disable the function for the shift.
- To configure the rule of T&A status on device, see ***Customize Attendance Status on Device*** for details.

10. **Optional:** Switch on **Enable Overtime** set a different overtime rule instead of using the general overtime rule.

Note

See instructions on setting a general overtime absence rule in ***Configure Overtime Parameters*** . You can also refer to this topic for explanations for the parameters in the overtime rule.

11. Select the holidays. On holidays, the shift will not be effective.

Note

For setting the holiday, refer to ***Set Holiday*** .

12. Click **Add** to finish adding the shift.

What to do next

Assign shift to persons or person groups. See details in ***Assign Shift Schedule to Person*** or ***Assign Shift Schedule to Person Group*** .

20.5 Manage Shift Schedule

Shift 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 person group or persons, or add a temporary schedule, so that it will calculate the attendance records for persons according to this shift schedule.

20.5.1 Shift Schedule Overview

The shift schedule overview shows the shift schedule information of each person in the person group. You can also view the detailed schedule of one person for each day in one month.

In the top left corner of Home page, click 🟥 → **All Modules** → **Attendance** → **Shift Schedule** → **Shift Schedule Overview** to enter the shift schedule overview page.

Select a person group on the left, you can view the schedule information about every person in the person group.

Click the person name to enter the detailed schedule of this person for each day in one month, such as effective period, shift name, and so on. You can click **Edit** or **Delete** to edit the shift schedule or delete the shift schedule.

Note

If any shift is not assigned to the person, you can click **Set Shift Schedule** to assign a shift to him/her.

20.5.2 Assign Shift Schedule to Person Group

After setting the shift, you need to assign it to the person group so that it will calculate the attendance records for persons in the person group according to this shift schedule.

Before You Start

Make sure you have added person groups, persons, and shifts. For details, refer to ***Add Person Groups*** , ***Add Person*** , and ***Add Shift*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Shift Schedule** .
2. Click **Assign to Person Group** on the left.
3. Do one of the following to set the shift schedule.

   Assign One by One On the left, select a person group you want to assign shift to, and switch on **Set Shift Schedule**.

   Batch Assign Click ▤ to open the Set Shift Schedule panel. Select the person groups.
4. Set schedule parameters.

   Effective Period

   The shift is effective within the period you set.

   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.
5. Select a shift for the person group(s) you select.

   Note

   - You can click **View** to preview the shift.
   - You can click **Add New** to assign another shift to the persons in the person group(s). The persons can check in/out in any of the timetables which are applied to the shifts and the attendance will be effective.
6. Click **Save**.

20.5.3 Assign Shift Schedule to Person

You can add a person shift schedule and assign a shift to one or more persons, so that it will calculate the attendance records for the persons according to this shift schedule.

Before You Start

Make sure you have added the person(s) and the shift. For details, refer to ***Add Person*** and ***Add Shift*** .

Steps

Note

The person schedule has the higher priority than person group schedule.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Shift Schedule** .
2. Click **Assign to Person** on the left to enter the person shift schedule management page.
3. **Optional:** Select a person group on the left, enter keywords in text field, or check **Include Sub-Group** to filter the persons.
4. Select the persons you want to assign the shift to.
5. Click **Set Shift Schedule** to enter the Set Shift Schedule page.
6. Set required parameters.

   Effective Period

   Within the period you set, the shift is effective.

   Check-In Not Required

   Persons in this schedule do not need to check-in when they come to work.

   Check-Out Not Required

   Persons in this schedule do not need to check-out when they end work.

   Effective for Overtime

   The persons' overtime will be recorded for this schedule.
7. Select a shift to be assigned.

   Note

   You can click **Add New** to assign another shift to the person(s). The person(s) can check in/out in any of the timetables which are applied in the shifts and the attendance will be effective.
8. Click **Save**.

20.5.4 Add Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift 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 Person*** and ***Add Shift*** .

Steps

Note

The temporary schedule has the higher priority than other schedules.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Shift Schedule** .
2. Click **Temporary Schedule** tab to enter the temporary schedule page.
3. Click **Add** to enter adding temporary schedule page.
4. Set required parameters.

   Name

   Customize a name for the schedule.

   Effective Period

   Within the period you set, the shift is effective.

   Check-In Not Required

   Persons in this schedule do not need to check-in when they come to work.

   Check-Out Not Required

   Persons in this schedule do not need to check-out when they end work.

   Effective for Overtime

   The persons' overtime will be recorded for this schedule.
5. Select a shift to be assigned.

   Note

   You can click **Add New** to assign another shift to the person(s). The person(s) can check in/out in any of the timetables which are applied in the shifts and the attendance will be effective.
6. Click to select the person(s) you want to assign the shift to.
7. Click **Save**.

20.6 Manage Attendance Record

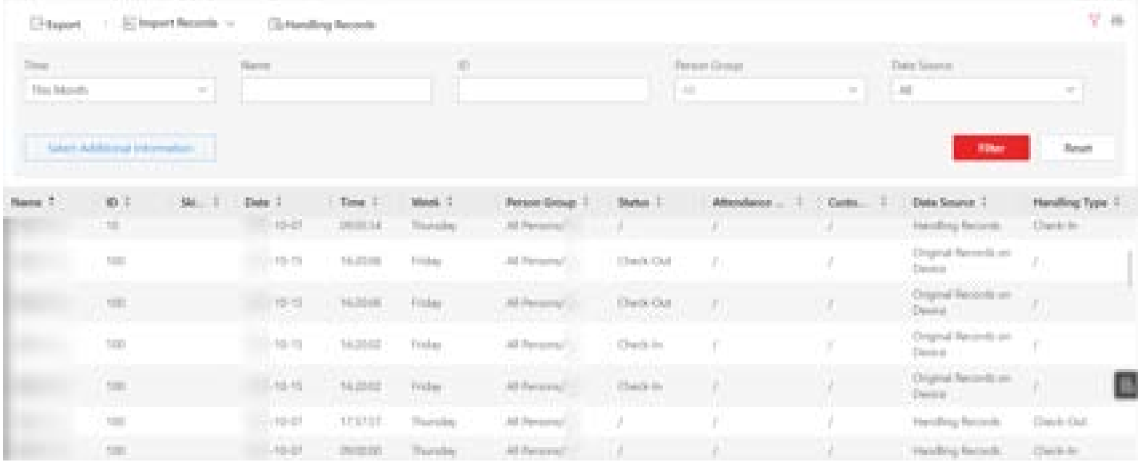
The persons' attendance records will be recorded and stored in the system. You can search the records by setting the search conditions to view the attendance details and view the person's attendance report. You can also correct check-in/out time for the exceptional records according to actual needs.

20.6.1 Search Raw Records

You can search the raw attendance records with conditions such as time, person information, and data source. Raw records refer to the original records on attendance check devices (access records) and handling records (manually corrected attendance records).

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Raw Records** on the left.



Name	ID	Ski...	Date	Time	Week	Person Group	Status	Attendance ...	Custo...	Data Source	Handling Type
	10		10-07	09:00:14	Thursday	All Persons/	/	/	/	Handling Records	Check-In
	100		10-15	16:20:08	Friday	All Persons/	Check Out	/	/	Original Records on Device	/
	100		10-15	16:20:06	Friday	All Persons/	Check Out	/	/	Original Records on Device	/
	100		10-15	16:20:02	Friday	All Persons/	Check In	/	/	Original Records on Device	/
	100		10-15	16:20:02	Friday	All Persons/	Check In	/	/	Original Records on Device	/
	100		10-07	17:57:37	Thursday	All Persons/	/	/	/	Handling Records	Check Out
	100		10-07	09:00:00	Thursday	All Persons/	/	/	/	Handling Records	Check-In

Figure 20-10 Raw Records

3. **Optional:** In the filter area, set the search conditions.

   Time

   Set the time range of the raw records you want to search. You can set up to one year's time range.

   Name

   Name of the person you want to search.

   ID

   Person ID of the person you want to search.

   Person Group

   Select the person group to view the raw records of the persons in the group.

   Data Source

   Select the type of raw records you want to search.

   - **Original Records on Device**: access and authentication records generated by the attendance check points.
   - **Handling Records**: manually corrected attendance records.

   Select Additional Information

   You can search the raw records with more custom conditions. Click **Select Additional Information** to select the additional search conditions.

Note

For more details about adding additional condition, refer to ***Customize Additional Information*** .

4. Click **Filter** to show all matched raw records.
5. **Optional:** Perform further operations.

Select Display Items	Click and select the items displayed in the search result.
Import Raw Records	Click **Import Records** to import raw records from an attendance check device or a file exported from an attendance check device. **Note** See details in ***Import Raw Attendance Records*** .
Export Raw Records	Click **Export** to export the filtered attendance records to your PC. **Note** See details in ***Export Attendance Records*** .
Handle Raw Records	You can click **Handle Records** to correct the check-in/out records if necessary.

20.6.2 Import Raw Attendance Records

Attendance data 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 attendance data on the platform. You can use this function to get the latest access records from the devices.

In the upper-left corner of Home page, select ▦ → **All Modules → Attendance → Records and Handling → Raw Records** .

Click **Import Records** > **Import from Device** or **Import from File**.

Import from Device

Applicable to getting the latest data on the attendance check devices that are added to the platform.
Select the devices that store the attendance check data, and then select the time range to be imported. Click **OK** to import the records 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' attendance check events. You can import the file to the platform so that the attendance check data 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.

20.6.3 Search Attendance Result

You can search attendance results to view the person's attendance status by setting the search conditions such as attendance group, person name, status, and skin-surface temperature status.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance Result** on the left.
3. In the filter area, set the search conditions.

   Time Period / Time

   Set the time range of the attendance results you want to search. You can set one year's time range at most and search the persons' attendance results recorded within three years.

   Name

   Enter the person name to view the attendance results.

   ID

   Enter the person's ID to view the attendance results.

   Person Group

   Select the person group to view the attendance results.

   Status

   You can search the attendance results of certain status. For example, if you want to view the late arrival records, you can select **Late** to search.

   Skin-Surface Temperature Status

You can search the attendance results by setting skin-surface temperature status, including All, Normal, Abnormal, and Unknown.

Select Additional Information

You can search the attendance results with more custom conditions. Click **Select Additional Information** to select the additional search conditions.

Note

For more details about adding additional conditions, refer to ***Customize Additional Information*** .

4. Click **Filter** to show all matched attendance results.
5. **Optional:** Perform further operations.

Sort Results

Click ⇅ and select a sorting rule to sort the matched results in order.

Select Display Items

Click 🎚 and select the items displayed in the search result.

View Person's Attendance Results

Click the person name to view the person's attendance results.

Note

Hover the cursor on the date to view the detailed work time, including scheduled work time and actual work time.

Export Attendance Results

Click **Export** to export the filtered attendance results and save in your PC.

Note

For more details, refer to ***Export Attendance Records*** .

Recalculate Attendance Results

Click **Calculate Again** to calculate the results with the latest raw records and handled records.

Note

See details in ***Manually Calculate Attendance Results***

Handle Attendance / View Handling Records

You can correct the check-in/out records or apply for leave for persons if necessary. You can also view the history handling records. For details, refer to ***Correct Check-In/Out for a Single Person*** / ***Correct Check-In/Out for Multiple Persons*** , ***Apply for Leave for a Single Person*** / ***Apply for Leave for Multiple Persons*** , and ***View Attendance Handling Records*** .

20.6.4 Correct Check-In/Out for a Single Person

After searching the person's attendance results, you can correct one person's check-in/out time according to actual needs.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance Result** on the left.
3. Search the attendance results.

   Note

   For details, refer to ***Search Attendance Result*** .
4. Click the name in the list of attendance results to enter the attendance details page of the person.
5. Hover the cursor over the date with abnormal attendance result and click **Handle Records**.
6. Select **Correct Check-in/out** as the handling type.
7. Set the correction type and time.
8. **Optional:** Enter the remarks, such as correction reason.
9. Click **Save**.

   Note

   The platform will start recalculating the attendance results according to the corrected records.

20.6.5 Correct Check-In/Out for Multiple Persons

You can batch correct multiple persons' check-in/out time according to actual need (e.g., the employees forgot to check in or check out).

Steps

1. In the top left corner of Home page, select → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Raw Records** → **Handle Records** or **Attendance Result** → **Batch Handle** .
3. Select **Correct Check-in/out** as the handling type.
4. Choose one of the following operations for handing.
   - **Filtered Person(s)**: Correct the check-in/out time of the persons whose attendance records are filtered when searching attendance records. You need to set correction type and time.

     Note

     Not available when you are searching raw records.
   - **Select Person(s)**: Select one or more persons in person groups, and set correction type and time.

Note

Up to 10,000 persons can be selected.

- **Batch Import**: Click **Download Template** and edit the related information in the downloaded template, then click and import the template with the corrected attendance records.

  Note

  If failed, you can export the error information, and import the edited information again.

5. Click **Save**.

20.6.6 Apply for Leave for a Single Person

After searching the person's attendance results, you can apply for leave according to actual needs.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance Result** on the left.
3. Search the attendance results.

   Note

   For details, refer to ***Search Attendance Result*** .
4. Click the name in the list of attendance results to enter the attendance details page of the person.
5. Hover the cursor over the date with abnormal attendance result and click **Handle Records**.
6. Select **Apply for Leave** as the handling type.
7. Set the leave type and time.
8. **Optional:** Enter the remarks, such as leave reason.
9. Click **Save**.

   Note

   The platform will start recalculating the attendance results according to the leave records.

20.6.7 Apply for Leave for Multiple Persons

You can apply for leave for multiple persons when they ask for leave or go on a business trip.

Before You Start

Make sure the required leave type have been defined. For more details, refer to ***Manage Leave Type*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance Result** on the left.
3. Click **Batch Handle**.
4. Select **Apply for Leave** as the handling type.
5. Choose one of the following operations for handing.
   - **Filtered Person(s)**: Apply leave for the persons whose attendance records are filtered when searching attendance results. You need to set leave type and time.
   - **Select Person(s)**: Select one or more persons in person groups, and set leave type and time.

   Note

   Up to 10,000 persons can be selected.
6. **Optional:** Enter remarks, such as leave reasons.
7. Click **Save**.

20.6.8 Manually Calculate Attendance Results

If person group or shift 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 pount (4 o'clock by default) every day. You can edit the time point in **Attendance** → **Basic Settings** → **General Rule** → **Auto-Calculate Attendance** .

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance Result** on the left.
3. Click **Calculate Again** to show the calculation settings window.
4. Set the start time and end time for attendance data.
5. Select **All Persons** or **Specific Persons** for attendance calculation.
6. Click **OK**.

   Note

   It can only calculate the attendance data recorded within three months.

20.6.9 View Attendance Handling Records

Attendance handling records show the added attendance handling information, including check-in/out correction and leave application. You can view the handling details, undo the handling operations, or export the records here.

In the top left corner of Home page, select ▦ → **All Modules** → **Attendance** → **Records and Handling** → **Handling Records** to view the attendance handling records.

You can perform the following operations.

- **Filter Handling Records**: Click ▽ and set conditions (e.g., Name, ID, Time, etc.) to filter the handling records.
- **Undo Handling Operations**: Select the handling record(s) and click **Undo** to cancel the handling operations. The correction records will be deleted in the page and the previous attendance status will also be restored.
- **Export Handling Records**: Click **Export** to save the handling records in CSV or Excel format to the local PC.

20.6.10 Export Attendance Records

The attendance results and raw records can be exported in Excel, PDF, or CSV format and be saved to the local PC. You can select the items to be included in the exported file.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance Result** or **Raw Records** on the left.
3. In the filter panel, set the search conditions to filter attendance records.

   Note

   For more details, refer to ***Search Attendance Result*** or ***Search Raw Records*** .
4. Click **Export** in the upper-left corner.
5. Select the format of the exported file from Excel, PDF and CSV.
6. Select the data items to be exported.
7. **Optional:** Click ↑ or ↓ to adjust the order of the data items.
8. Click **Export** to export the attendance records and save to your PC.

20.7 Manage Attendance Reports

Attendance report is the statistics of the attendance results of the specific person group(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, and manually export report.

20.7.1 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, and marks of different attendance status.

In the top left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Attendance 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.

Marks of Different Status

In the report, different marks indicate different status respectively, including late, absent, no schedule, holiday, etc. You can customize these marks according to actual needs.

20.7.2 Send Attendance Report Regularly

You can set a regular report rule for specific person groups, 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 person groups during specific 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 parameters 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 records in total.
- The report is an Excel file.

1. In the upper-left corner of Home page, select 🟥 → **All Modules** → **Attendance** → **Basic Configuration** .
2. Select **Scheduled Report** on the left to enter the report setting page.
3. Click **Add** (for first time) or click + .
4. Create a descriptive name for the report.
5. In **Report Type**, select the report content, such as Daily Report, Start/End Work Time, etc.

   Note

   - You can select **Custom Report** as the report type and select a customized report from the **Custom Report** drop-down list.
   - You can click **Add New** to create a new custom report. See instructions in ***Add a Semi-Custom Report*** or ***Add a Custom Report*** .

6. In **Person Group**, select the person group(s) and click > to include the persons in the person group(s) in this report.
7. In **Person**, click ▢ to include individual persons in this report.
8. Set the statistics type to **Daily**, **Weekly**, or **Monthly** 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. Select the 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 ***Set Email Template*** .

10. Select **CSV**, **Excel**, or **PDF** as the format.

Note

You can select **TXT** as the format if the report type is **Access Records**.

11. Select a report language.
12. Select and enable the way of sending the report from **Send Report via Email**, **Upload to SFTP**, and **Local Storage**.

Note

To set up the SFTP or local storage, click ⚙ > **SFTP Settings** or **Configure Local Storage**.

13. Click **Add** to save the report schedule.

The report will be generated and sent to the recipient at the specified sending time.

20.7.3 Export Attendance Report

HikCentral Professional supports multiple report types and you can export a series of attendance reports manually to view the employees' attendance data.

Steps

1. Select 🟥 → **All Modules** → **Attendance** → **Export Report** .
2. Select **Attendance Report** on the left.
3. Select a report type.
4. Select the person groups and individual persons to be included in the report.

Note

For Department Report, you can only select person groups.

5. Set the time range of this report according to the report type.

Monthly Reports

- **By Calendar Month**: Select a calendar month as the report time range.
- **Custom Time Period**: Report time range is 30 days from the start date you specify.

Weekly Reports

- **By Week**: Select a calendar week as the report time range.
- **Custom Time Period**: Report time range is 7 days from the start date you specify.

Other Report Types

Select the start date and end date of the report.

6. Select **CSV**, **Excel**, or **PDF** as the format of the report.

Note

You can select **TXT** as the format if the report type is **Access Records**.

7. Click **Export**.

   The report will be generated and downloaded to the local PC.

20.7.4 Custom Report

If the predefined attendance report types in the platform cannot meet your needs, you can customize your own report types.

- ***Add a Semi-Custom Report*** : Customize a report based on a predefined report.
- ***Add a Custom Report*** : Create a completely new report with more flexibility on data selection and presentation.

Add a Semi-Custom Report

You can create a semi-custom attendance report based on the predefined report type in the platform. After creating a semi-custom report, you can export the report manually or set a schedule to send the report to your email regularly.

Steps

1. Select 🟥 → **All Modules** → **Attendance** → **Export Report** .
2. Select **Custom Report** on the left.
3. Select the **Semi-Custom Report** tab.
4. Click **Add**.
5. Create a descriptive name for the report in the **Report Name** field.
6. Select a predefined report type from the **Report Source Type** drop-down list.

   Example

   For example, if you want to customize a report based on the Department Report, you can select **Department Report** and then customize it in the following steps.
7. Select the data items you want to include in the report from **Available 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. Select a sorting rule for records from the **Table Display Rule** drop-down list.
9. Click **Add** to save the semi-custom report, or click **Add and Continue** to add another one.
10. **Optional:** Perform further operations.

Edit Report	Click on report name to edit it.
Delete Report	Select the report(s) and click **Delete** to delete the selected report(s).
Export Report	Click and specify the 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*** .

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. Select → **All Modules** → **Attendance** → **Export Report** .
2. Select **Custom Report** on the left.
3. Select the **Custom Report** tab.
4. Click **Add**.
5. Create a descriptive name for the report in the **Report Name** field.
6. Choose whether to merge the data of the same person/department/date.
7. Select a sorting rule for records from the **Table Display Rule** drop-down list.
8. Select the data items you want to include in the report from **Available 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.

9. Click **Add** to save the custom report, or click **Add and Continue** to add another one.
10. **Optional:** Perform further operations.

Edit Report	Click on report name to edit it.
Delete Report	Select the report(s) and click **Delete** to delete the selected report(s).
Export Report	Click and specify the 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*** .

Chapter 21 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.

21.1 Customize Report Dashboard

The report dashboard provides an at-a-glance view for the reports supported by the system, such as people counting report, vehicle analysis report, and queue analysis report. You can customize the report dashboard as required.

Steps

1. In the top left corner of the Client, select ■ → **All Modules** → **Intelligent Analysis** → **Intelligent Analysis Overview** .
2. **Optional:** Click ⌄ → **Add Dashboard** on the report dashboard page to add a new dashboard.

   Note

   You can add up to 100 dashboards.

   The new dashboard appears and it is 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.
3. **Optional:** Edit dashboard(s).
   1) Click ⌄ to expand the added dashboard(s).
   2) Click ✎ to edit the dashboard name or click 🗑 to delete the dashboard.
4. Add report(s) to a dashboard and edit the report(s).
   1) Select a report type and generate the report.
   2) Click **Add** on the report page to add the report to dashboard.

      The report appears on the selected dashboard.
   3) Perform the following operations.
      - Add More Reports: Click **Add Report** to add more reports to the dashboard.
      - View Report in Larger Window: Click ⤢ to view the report in larger window.
      - Edit Report Name: Click ⋯ and then click **Edit**.
      - Delete Report from Dashboard: Click ⋯ and then click **Delete**.

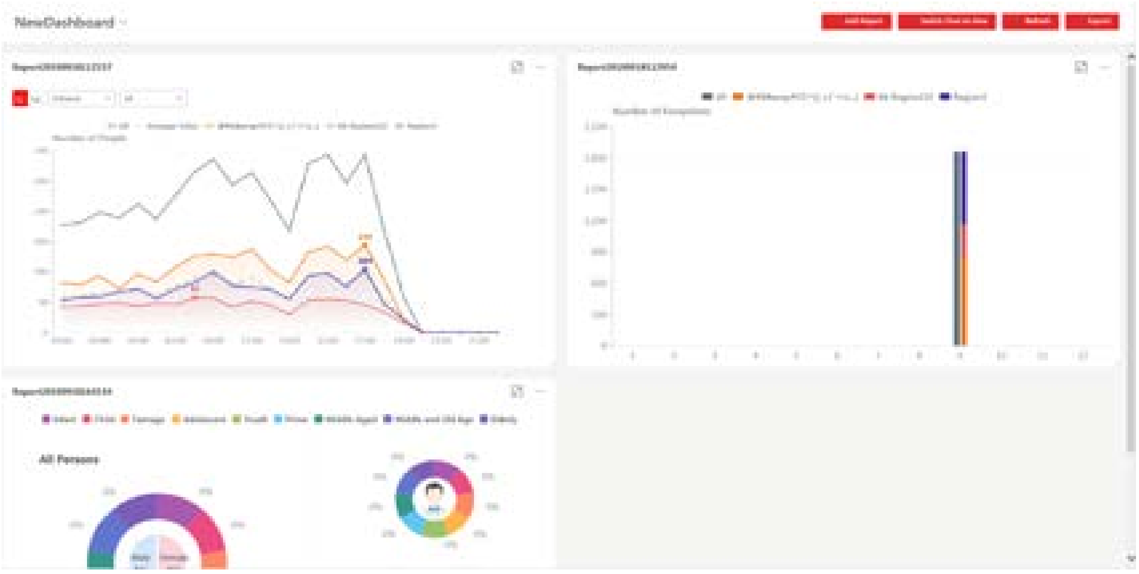


Figure 21-1 Report Dashboard

5. Switch time to view report data.
   1) 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.
   2) 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.
6. **Optional:** Export report(s) on the dashboard to the local PC.
   1) Click **Export** to display the Export panel.
   2) Select report(s) from the report list.
   3) Select **Excel**, **CSV**, or **PDF** as the format of the exported report(s).
   4) Click **Export**.

21.2 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.

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 border. 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.

For details about adding a people counting group, refer to ***Add People Counting Group*** .

21.2.1 Add 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 border. 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.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **People Counting Group** .
2. Click **Add**.
3. Create a name for the group.
4. Select a site.
5. In the **Resource for People Counting**, click **Add** to select the resources (including doors and people counting cameras) for calculating the number of people stayed in this region.
6. Set the entry or exit direction of the selected cameras and readers related to the selected doors.

Note

- For doors, the access records on the entry reader will be calculated as person entered this region while the access records on the exit one will be calculated as person exited this region.
- For cameras, the people crossing along the entry direction will be calculated as person entered this region while the people crossing along the exit one will be calculated as person exited this region.

7. **Optional:** Switch on the **Regularly Clear All** and set a time for clearing all data regularly.
8. **Optional:** Switch on the **Maximum Capacity** and enter the maximum number of persons that can enter the area monitored by this group.
9. Click **Add**.

   The people counting group is added in the table and you can view the resources in the group.

10. **Optional:** Locate the people counting group on the map by setting the locations of the doors and cameras in the group and setting the border of the region for detection.
    1) Click **Set Geographic Location** to enter the Map Settings page.
    2) Drag the people counting group from the Resource Group list on the right to the map.

       The region as well as the doors and cameras in the group will be added on the map.
    3) Drag to draw the region according to the actual needs.
    4) Drag the icons of the doors and cameras onto the map to set the their locations on the map.
    5) Right click to finish.

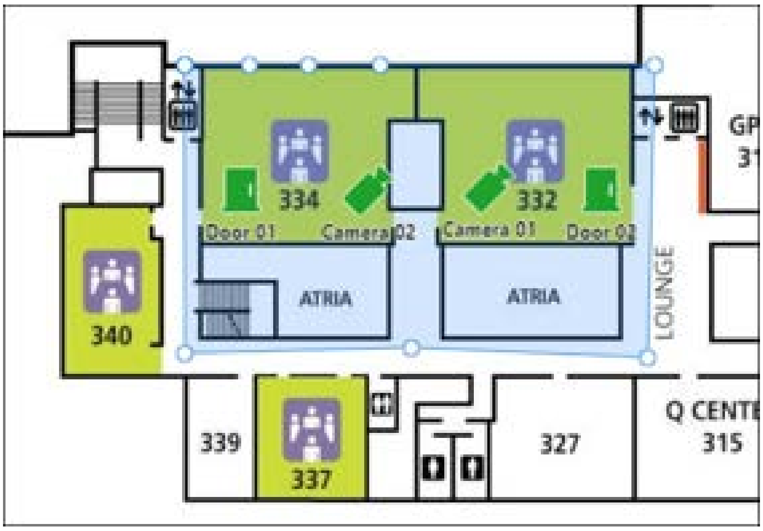


Figure 21-2 Draw People Counting Group on Map

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 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.

21.2.2 Generate People Counting Report

You can manually generate an entry & exit counting report to view the entry & exit statistics in a line chart or histogram. You can also export the report to the local PC.

Before You Start

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.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Intelligent Analysis** → **Analysis Report** → **People Counting** .
2. Select the analysis type.

   People Counting for One 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.

People Counting in One Region

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

Make sure you have added people counting groups. See ***Add People Counting Group*** for details.

3. Select people counting camera(s) or people counting group(s) based on the analysis type you set in the previous step.
   - Select Camera(s):
     a. Click .
     b. Select a current site or Remote Site from the drop-down list to show its people counting cameras.

     Note

     - Only people counting cameras and people counting groups will be displayed here.
     - Only the online cameras on the Remote Site will be displayed.

     c. Check the people counting camera(s) for statistics and click any position outside the selection region to go back to the Camera list.
     d. Check the cameras in the Camera list.

     Note

     Up to 20 people counting cameras can be selected for statistics at the same time.
   - Select Group(s):

     Check the added people counting group(s) for statistics.
4. Set the report type to daily report, weekly report, monthly report, annual report, or customize the time interval for a report.

   Daily Report

   The daily report shows data on a daily basis. The system will calculate the number of people in each hour of one day.

   Weekly Report, Monthly Report, 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 system will calculate the number of people in each day of one week, in each day of one month, and in each month of one year.

   Custom Time Interval

   Users can customize the days in the report to analyze the number of people in each day or month of the custom time interval.
5. In the Time field, 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.

6. Click **Generate Report**.

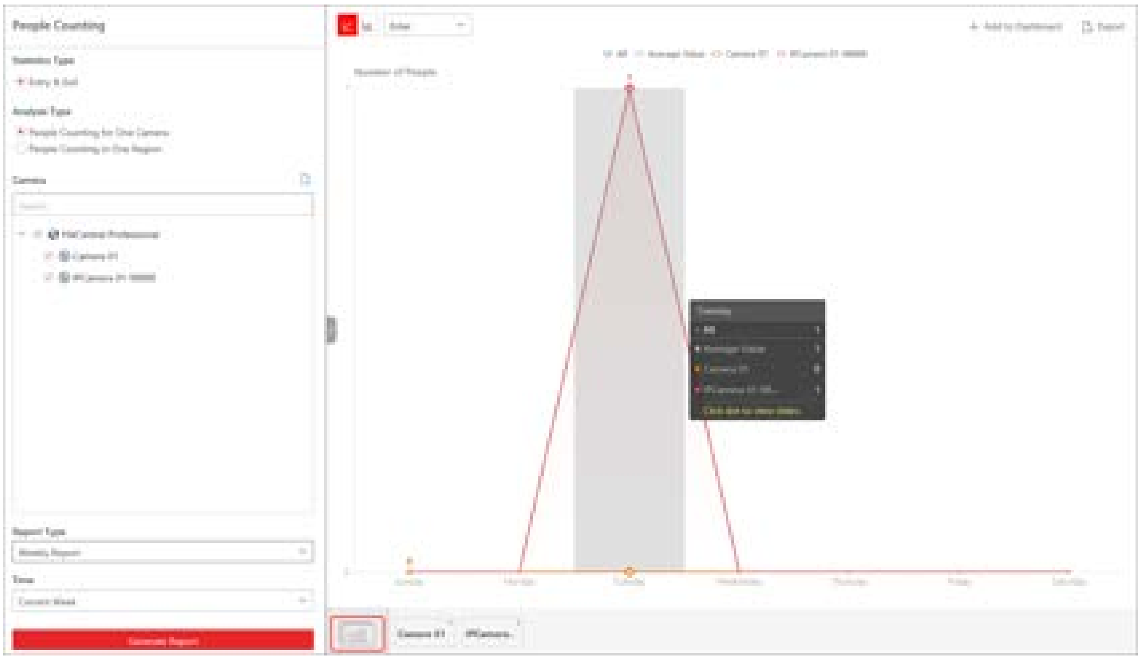


Figure 21-3 People Counting Report (Entry & Exit)

The statistics of all the selected item(s) are displayed in the right panel.

7. **Optional:** Perform the following operation(s) after generating the people counting report.

Show/Hide Certain Data
Click the legend to show or hide the data of a certain element, such as a certain camera.

View Entered/Exited/ Both Entered and Exited Statistics
Select **Enter**, **Exit**, or **Enter and Exit** from the drop-down list. The total statistics and all the selected cameras' statistics are displayed and marked with different colors.

View Both Entered and Exited Statistics of a Camera or Group
Click the camera or group name on the page below to view the chart of a camera or group.

View Linked Video
For line chart, if the selected report type is daily report, weekly report, or monthly report, click the line on the line chart to play the linked video.

For histogram, if the selected report type is daily report, click the rectangle on the histogram to play the linked video.

Switch Between Line Chart and Histogram
Select 📈 or 📊 on the upper-left corner to switch between line chart (displaying the trend for the number of people on different time points) and histogram (for comparison).

8. **Optional:** Export the report to the local PC.
   1) Click **Export**.

      The Export panel will display camera selected and time configured according to the range you defined previously.
   2) (Optional) Select the camera or group and set the report type and report time if needed.
   3) Select shorter time period to view more detailed data of each camera.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1or 24 records respectively for each camera.

      Note

      If you select **By Minute**, the records amount depends on the configuration on the device. For example, if the device reports people counting data to the system every minute, it will export 24*60 records for each camera.
   4) Set the format of the exported file as Excel, CSV, or PDF.
   5) Click **Export**.

21.2.3 Send People Counting Report Regularly

You can set a regular report rule for specified people counting cameras or specified people counting groups, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the number of people entered or exited detected by people counting cameras, or the number of people stayed calculated by the people counting cameras and doors in the same region.

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 the sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select ☰ → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Scheduled Report** .
2. Click **Add** to open the Create Report page.

3. Select the report category as **People Counting**.
4. Select the statistics type as the **Entry & Exit**.

Note

This statistics type will count the number of people entered and exited, and calculate the number of people stayed in a region by the formula of "number of people entered - number of people exited".

5. Select the analysis type.

People Counting for One Camera

The report contains the number of people entered and exited detected by the people counting camera(s). You need to select the camera(s) as the Report Target.

For example, if you select the people counting type as **People Counting for One Camera** and select two people counting cameras as the **Report Target**, the platform will generate two reports of the cameras respectively, including the number of people entered and exited detected by the two cameras.

People Counting for One Region

The report contains the number of people stayed in one region, which is calculated by the detected people from the people counting camera(s) and the statistic people from the doors in the region. You need to select the people counting group(s) as the Report Target.

Note

The **Analysis Type** is available only when the statistics type is selected as **Entry & Exit**.

6. Create a name for the report.
7. Select the people counting camera(s) or groups contained in the report.

Note

If you select **People Counting for One Camera** as the analysis type, you should select camera(s). If you select **People Counting for One Region**, you should select people counting group(s).

8. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

Daily Report

The 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.

Weekly Report and Monthly Report

As compared to the daily report, the 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 the weekly report, if you set the sending time as 6:00 on Monday, the platform will send a report at 6:00 on every Monday morning, containing the number of people detected between last Monday and Sunday.

9. Set how the report will present the results analyzed in the specified time period.

   Example

   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 analysis results in each hour or each minute for one camera.
10. Set the report time and sending time according to the report type.
11. **Optional:** Set the effective period (start time and end time) in which the reports will be regularly sent.
12. 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.
13. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .
14. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** 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 ⚙ at the top of report list and click **SFTP Settings** from the drop-down list to enter the configuration pane.
15. **Optional:** Switch on **Save to Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

    Note

    You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.
16. Click **Add**.

21.3 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.

21.3.1 Generate People Density Analysis Report

You can manually generate a people density report to view the people density data in a line chart. You can also export the report to the local PC if required.

Before You Start

- Make sure you have purchased the License that supports people density analysis, or the function will be unavailable.
- Make sure you have added the behavior analysis server to the HikCentral Professional and linked cameras to the server.
- Make sure you have configured people density analysis on the behavior analysis server. For details, see the user manual of the server.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Report** → **People Density Analysis** .
2. Select camera(s) to search for people density data.
   1) Click to open the camera list.
   2) **Optional:** Check **Include Sub-Area** to allow the display of camera(s) in sub-areas.
   3) Select a current site or Remote Site from the drop-down site list.
   4) Select areas and then select the camera(s) in these areas.

   Note

   - Only the online cameras will be displayed.
   - You can also enter keywords of the camera name to search for cameras.

   5) Check camera(s) appeared in the camera list for statistics.
3. Set the report type to daily report, weekly report, monthly report, annual report, or customize the time interval for a report.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the peak amount of people appeared in the images of the camera in each hour of one day.

   Weekly Report, Monthly Report, Annual Report

   Compared to generating daily report, generating weekly report, monthly report, and annual report can be less time-consuming. The system will calculate the peak amount of people in each day of one week, in each day of one month, and in each month of one year respectively.

Custom Time Interval

Users can customize the days in the report to analyze the peak amount of people in each day or month of the custom time interval.

4. Select a pre-defined time period or customize a time period for search.
5. Click **Generate Report**.

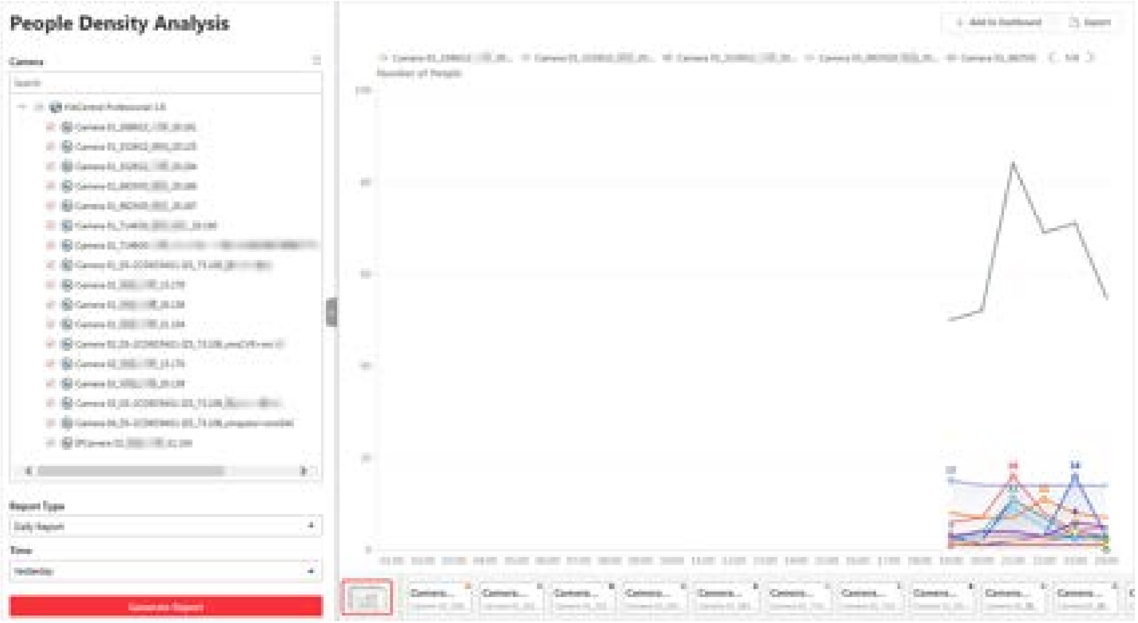


Figure 21-4 People Density Analysis Report

The statistics of all the selected camera(s) will be displayed on a line chart.

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

Add Report 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**.

Show/Hide Certain Data

Click the legend to show or hide the data of certain element, such as certain camera.

View Statistics of a Camera

Select a camera at the bottom of the line chart to view its statistics in the line chart.

View Detailed Data in Each Time Segment

Hover the cursor onto the line chart to view the detailed data.

For a daily report, you can view the peak amount of people appeared in the images of each camera in each hour; For a weekly report, in each day; For a monthly report, in each day; For a monthly report, in each month.

View Linked Video

Click the dot on the line chart to view the video of the time period that the dot represents.

Note

Viewing linked videos is not supported by annual report.

View Detailed Data in Each Minute

Note

Viewing detailed data in each minute is only supported by daily report.

a. Generate a daily report.
b. Select a camera at the bottom of the line chart to display its statistics only.
c. Hover the cursor onto the line chart and then click **Details** on the pop-up floating window.
   The line chart that shows statistics in each minute will be displayed.
d. Hover the cursor onto the newly-displayed line chart to view the peak amount of people appeared in the images of the camera in each minute.

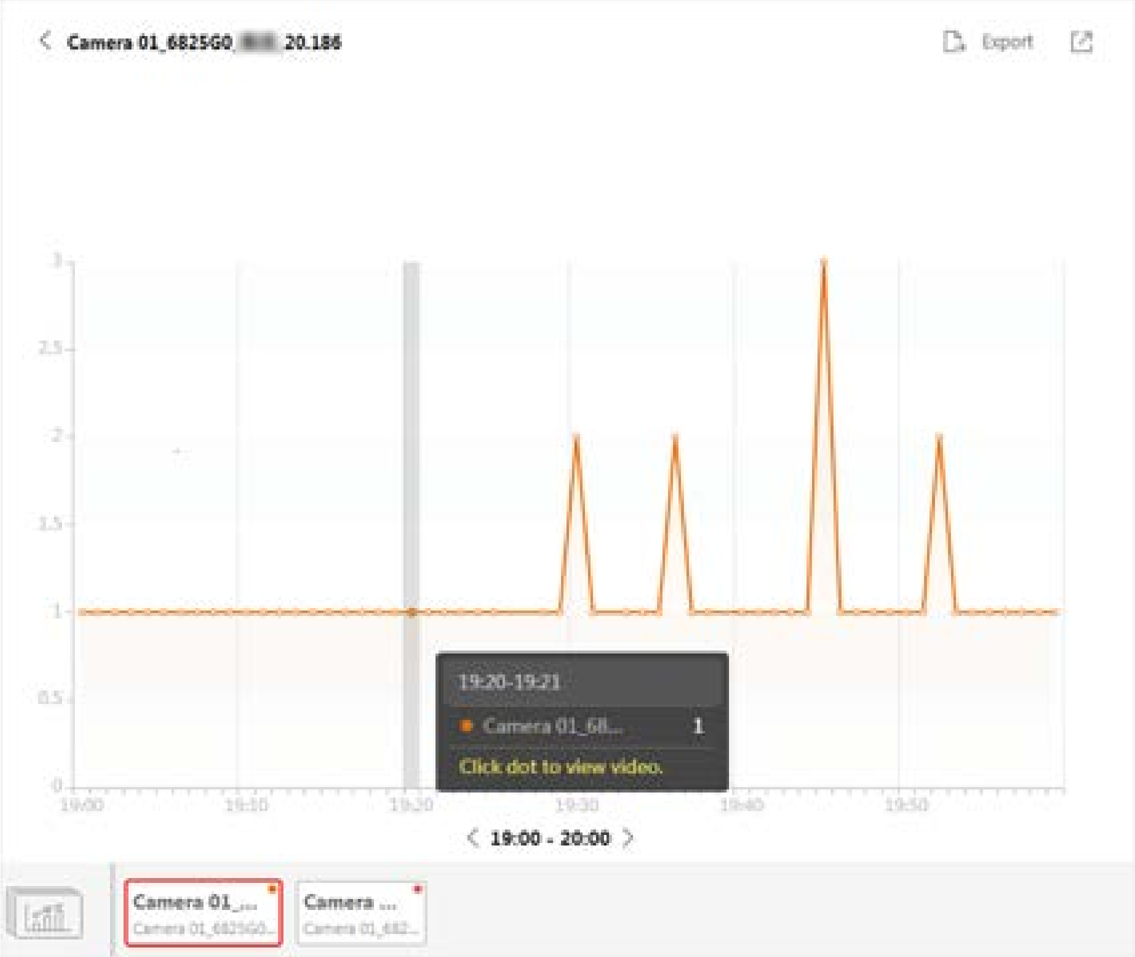


Figure 21-5 View Detailed Data In Each Minute

7. **Optional:** Export the report(s) on the dashboard to the local PC.
   1) Click **Export**.

      The Export panel will display the camera selected and time configured according to the range you defined previously.
   2) **Optional:** (Optional) Select the camera and set the report type and report time if needed.
   3) Select a shorter time period to view more detailed data of each camera.

      Example

      For example, if you select the daily report, you can select **By Day** or **By Hour**, and it will export 1or 24 records respectively for each camera.

      Note

      If you select **By Minute**, the number of records depends on the configuration on the device. For example, if the device reports the data to the platform every minute, it will export 24*60 records for each camera.
   4) Set the format of the exported file as Excel, CSV, or PDF.

5) Click **Export**.

21.3.2 Send People Density Analysis Report Regularly

You can set a regular people density analysis report rule for specified cameras, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the variation trend of people density data in line chart, which is calculated by behavior server.

Before You Start

- Add behavior analysis server to the platform, and configure people density analysis task for specified camera(s). For details, refer to ***Add DeepinMind Server*** .
- 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. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Scheduled Report** .
2. Click **Add** to open the Create Report page.
3. Select the report category as **People Density Analysis**.
4. Create a name for the report.
5. Set the camera(s) contained in the report.

   Note

   Make sure you have configured people density analysis for the camera(s). For details, refer to ***Add DeepinMind Server*** .
6. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   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.

   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.

7. Set how the report will present the results analyzed in the specified time period.

   Example

   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 analysis results in each hour or each minute for one camera.
8. Set the report time and sending time according to the report type.
9. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
10. 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.
11. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .
12. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

    Note

    You can also click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.
13. **Optional:** Switch on **Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

    Note

    You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.
14. Click **Add**.

21.4 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.

21.4.1 Generate 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.

Before You Start

Add 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.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Report** → **Queue Analysis** .
2. Select camera(s) for statistics.
   1) Click in the camera panel.
   2) Select a current site or Remote Site from the drop-down site list to show its cameras.

   Note

   Only the online cameras which support queue management will be displayed here.

   3) Check the camera(s) for statistics.

   The cameras will be added to the camera list.
3. Select the queue regions configured on the camera and the platform will collect the queue data in these queue regions.

   Note

   For configuring the queue, refer to the user manual of the camera.
4. Select the report type as daily report, weekly report, monthly report, or annual report.

   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, 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 system will calculate the queue data detected in each day of way week, in each day of one month, and in each month of one year.

5. Set the time or time period for statistics.
6. Select the analysis type and set the report range for daily report, weekly report, or monthly report.

Queuing-Up Time Analysis

The report will show the persons' queuing-up durations in different queues.

For example, if you set the report range to 300s and 600s, the report will show that in each queue, how many persons have waited for less than 300s, how many persons have waited for 300 to 600s, and how many persons have waited for more than 600s.

Queue Status Analysis

The report will show the number of queuing-up persons within different queuing-up durations.

For example, if you set the report range as 5 persons and 10 persons, the report will show that in each queue, how many seconds the status lasts when there are less then 5 persons, how many seconds the status lasts when there are 5 to 10 persons, and how many seconds the status lasts when there are more than 10 persons.

7. Click **Generate Report**.

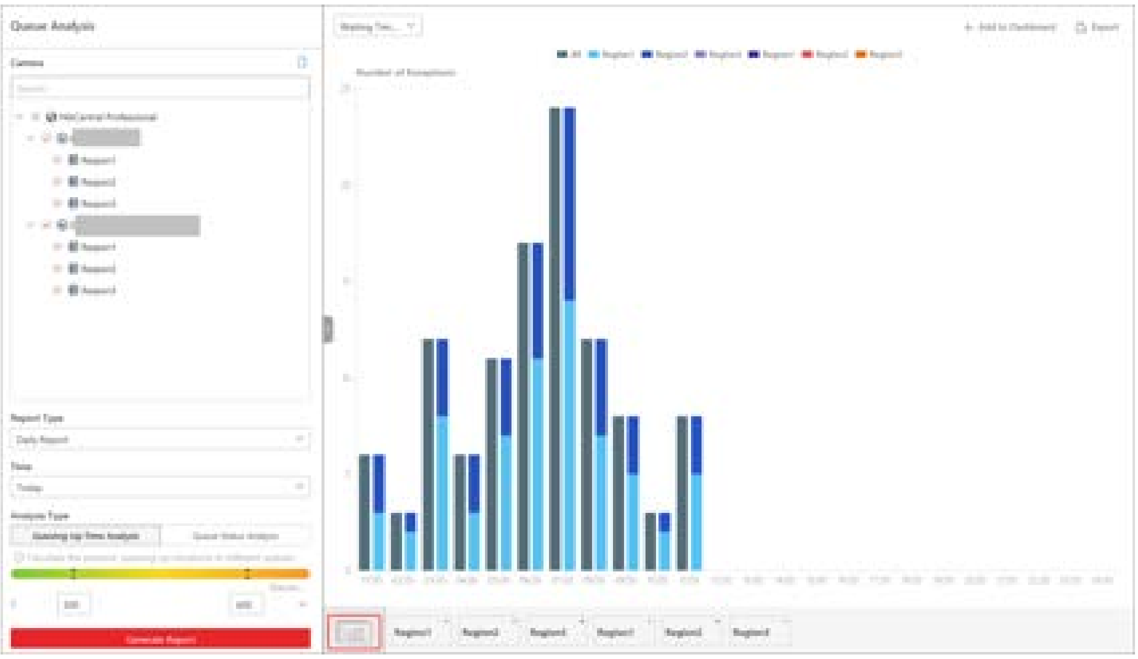


Figure 21-6 Queue Analysis Report

A chart is displayed in the right panel, showing the number of exceptions (waiting timeout or people amount exceeding) of different queues.

8. **Optional:** Perform the following operation(s) after generating the report.

Show/Hide Certain Data	Click the legend to show or hide the data of certain element, such as queue.
View Queue Analysis Report of a Queue	Click the queue icon on the page below to view the report of a queue, including the number of exceptions, number of people in the queue, and waiting durations .
Switch Between Number of Exceptions, Number of People, and Queue Length	Click on the page below to view the report of all the selected queues. If you select the report type as **Daily Report**, **Weekly Report**, or **Monthly Report**, and set the analysis type as **Queue Status Analysis**, click the drop-down list to view the number of waiting timeout exceptions, or number of people in different and all queues. If you select the report type as **Annual Report**, and set the analysis type as **Queue Status Analysis**, click the drop-down list to view the number of waiting timeout exceptions or number of people in all queues. If you select the report type as **Daily Report**, **Weekly Report**, or **Monthly Report** and set the analysis type as **Queuing-Up Time Analysis**, click the drop-down list to view the number of people amount exceeding exceptions or queue length of different queues. If you select the report type as **Annual Report**, and set the analysis type as **Queuing-Up Time Analysis**, the people amount exceeding exceptions will show.

9. **Optional:** Export the report to the local PC.

   1) Click **Export**.

      The Export panel will display with camera and queue selected and time configured according to the range you defined previously.

   2) **Optional:** (Optional) Select the camera and queue, and set the report type and report time if needed.
   3) Select shorter time period to view more detailed data of each queue.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour** and it will export 1 or 24 records respectively for each queue.

   4) Select the content to export.

      Queue Exception

      The number of exceptions (people amount exceeding and waiting timeout) of each queue.

      People Amount Exceeding

      The number of persons in the queue exceeds the configured threshold.

Waiting Timeout

The waiting duration for the persons in the queue exceeds the configured threshold.

Person Amount in Queue

The number of persons in each queue.

Queue Status

The status of each queue, including persons' waiting duration and number of persons (queue length) in the queue.

5) For daily report, weekly report or monthly report, select analysis type.
6) Set the format of the exported file as Excel, CSV, or PDF.
7) Click **Export**.

21.4.2 Send Queue Analysis Report Regularly

You can set a regular report rule for specified cameras which support queue management, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing queue exceptions, number of persons in the queue, and queue status including waiting duration and queue length, detected by these cameras during the specified 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. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select ▦ → **All Modules → Intelligent Analysis → Analysis Group Settings → Scheduled Report** .
2. Click **Add** to open the Create Report page.
3. Select the report category as **Queue Analysis**.
4. Create a name for the report.
5. Select the camera(s) which support queue management contained in the report.

   Note

   Only cameras which support queue management will be displayed here.

   The report will show the data of all the queues configured on the cameras.

Note

For configuring the queue, refer to the user manual of the camera.

6. Set the report type as **Daily**, **Weekly**, or **Monthly**.

   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.

   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.

7. Set the content in the report.

   Queue Exception

   The number of exceptions (people amount exceeding and waiting timeout duration) of each queue, including the number of persons in the queue exceeds the configured threshold and the waiting duration for persons in the queue exceeds the configured threshold.

   Person Amount in Queue

   The number of persons in each queue.

   Queue Status

   The status of each queue, including persons' waiting duration and number of persons in the queue.

   If you select **Queue Status**, you should select the **Analysis Type** as queue length or waiting duration, and set the range.

   Queue Length

   The report will show how many seconds each queue status (number of persons in different ranges) lasts.

   For example, if you set the report range as ***Range 1 < 5 ≤ Range 2 ≤ 10 < Range 3***, the report will show that in each queue, how many seconds the status lasts when there are less then 5 persons, how many seconds the status lasts when there are 5 to 10 persons, and how many seconds the status lasts when there are more than 10 persons.

   Waiting Duration

The report will show the number of persons in each queue who have waited for specified duration.

For example, if you set the report range as ***Range 1 < 300 ≤ Range 2 ≤ 600 < Range 3***, the report will show that in each queue, how many persons have waited for less than 300s, how many persons have waited for 300 to 600s, and how many persons have waited for more than 300s.

8. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

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.

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.

9. Set how the report will present the results analyzed in the specified time period.

Example

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 analysis results in each hour or each minute for one camera.

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. 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.

13. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

14. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

Note

You can also click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

15. **Optional:** Switch on **Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

Note

You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.

16. Click **Add**.

21.5 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.

For details about adding a heat analysis group, refer to ***Add Heat Analysis Group*** .

21.5.1 Add 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.

Steps

1. In the top left corner of the client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Heat Analysis Group** .
2. Click **Add**.
3. Create a name for the group.
4. Select a site.

5. In the **RES for Dwell Time CALC** field, select the cameras for calculating the dwell time of the people stayed in this region.
6. **Optional:** To calculate the average dwell time of each people, you need to add resources (including doors and cameras) to the group to calculate the number of people stayed in this region.

   Note

   Average Dwell Time = Total Dwell Time/Number of People in This Region

   1) Set the switch **Average Dwell Time Statistics** to on.
   2) In the **Resource for People Stayed Calculation** field, click **Add** to select the doors and camera to the group for calculating the number of people stayed in this region.
   3) Set the entering or exiting direction of the card readers of the selected doors and the entering or exiting direction of the cameras.

      Note

      Number of People Stayed in Region = Number of People Entered - Number of People Exited

      For doors, the access records on the entering card reader will be calculated as person entering this region while the access records on the exiting one will be calculated as person exiting this region.

      For cameras, the people crossing along the entering direction will be calculated as person entering this region while the people crossing along the exiting one will be calculated as person exiting this region.
7. Click **Add**.

   The heat analysis group is added in the table and you can view the resources in the group.
8. **Optional:** Locate the group on the map by setting the locations of the doors and cameras in the group and setting the border of the region for detection.
   1) Click **Set Geographic Location** to enter the Map Settings page.
   2) Drag the heat analysis group from the Resource Group list on the right to the map.

      The region as well as the doors and cameras in the group will be added on the map.
   3) Drag to draw the region according to the actual needs.
   4) Drag the icons of the doors and cameras to set the their locations on the map.
   5) Right click to finish.

   After adding the heat analysis group on the map, you can know the dwell time of the people stayed in the region, how many persons stayed in the region, and average dwell time of each people on the Control Client.

21.5.2 Generate Heat Analysis Report

You can generate a heat analysis report to track consumer movements and analyze the visit times and dwell time in a configured area.

Before You Start

- Add 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.
- Add 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*.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Intelligent Analysis** → **Analysis Report** → **Heat Analysis** .
2. Select analysis type.

   Heat Analysis for One Camera

   A heat analysis report based on the data from the selected cameras will be generated. The data of different cameras will be displayed and you can compare the data of different cameras.

   Heat Analysis in One Region

   A heat analysis report based on the data from the selected heat analysis groups will be generated. The data of different groups will be displayed and you can compare the data from different groups.

   Note

   You should have added heat analysis group(s). For details, see ***Add Heat Analysis Group*** .
3. Select heat analysis camera(s) or heat analysis group(s) for statistics.

   1) Click .

   Note

   - Only the online heat analysis camera(s) or heat analysis group will be displayed here.
   - Up to 20 heat analysis cameras can be selected for statistics at the same time.

   2) Check the heat analysis camera(s) or heat analysis group(s) for statistics.
4. Set the report type to daily report, weekly report, monthly report, annual report, or customize the time interval for a report.

   Daily Report

   Daily report shows data on a daily basis. The platform will calculate the number of people or people dwell time in each hour of one day.

   Weekly Report, Monthly Report, 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.

   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.

5. **Optional:** Set the time or time period in the Time field for statistics.

Note

For custom time interval report, you need to set the start time and end time to specify the time period.

6. Set the analysis type.

Dwell Time

The minutes that the people stay at the same location during each time period for each camera.

People Amount

The number of people detected during each time period for each camera.

Note

This analysis type is only supported by the second generation of heat analysis cameras.

Average Dwell Time

The average dwell time for the each person stay at the same location during each time period for each camera.

7. Click **Generate Report**.

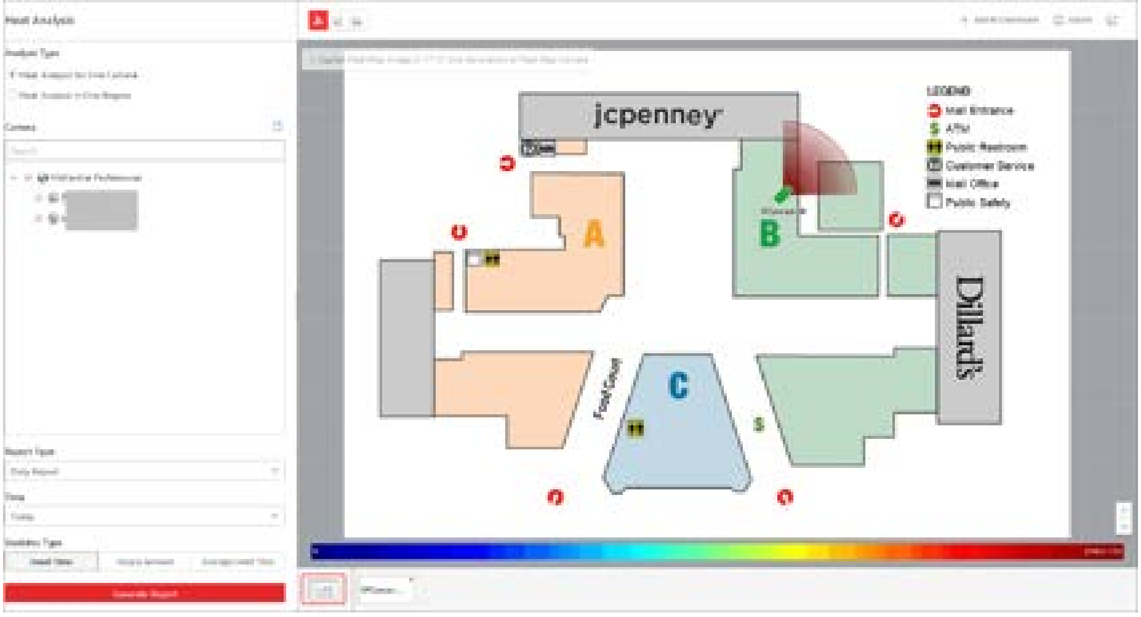


Figure 21-7 Static Map of Selected Cameras

The static maps of the selected cameras will appear.

8. Click the map to view the detailed heat data of the cameras on the map. You can view each camera's field of view, and the fields are color coded. The red color block (255, 0, 0) indicates the

most welcome region (most persons detected or longest dwell time), and blue color block (0, 0, 255) indicates the less-popular region (least persons detected or shortest dwell time).

Note

Move the cursor to the field of view to view the detected value, including people amount or dwell time.

9. **Optional:** Click the camera icon on the page below to view heat analysis of a camera.

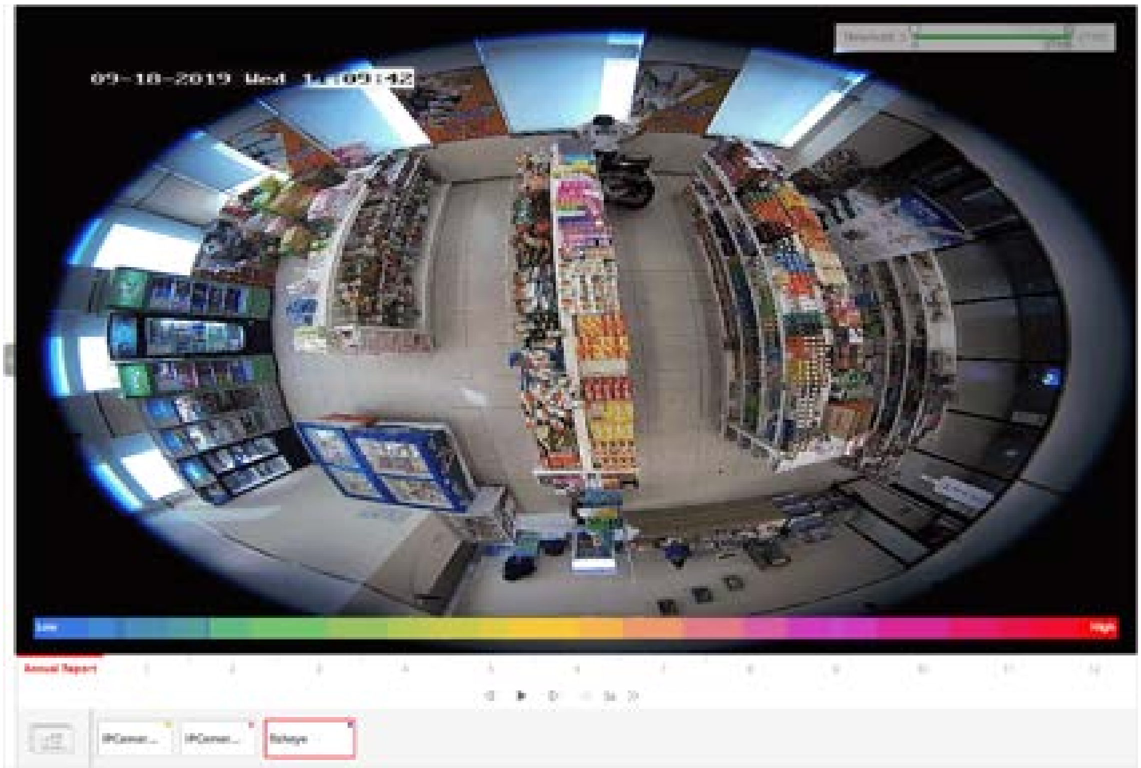


Figure 21-8 Heat Map of a Camera

The image of the camera is color coded. The red color block (255, 0, 0) indicates the most welcome region (most persons detected or longest dwell time), and blue color block (0, 0, 255) indicates the less-popular region (least persons detected or shortest dwell time).

You can drag the slider on the upper-right to adjust the range of the heat value. The heat data out of the range will not be displayed.

10. **Optional:** Click to switch among heat map, histogram, line chart to view the details.

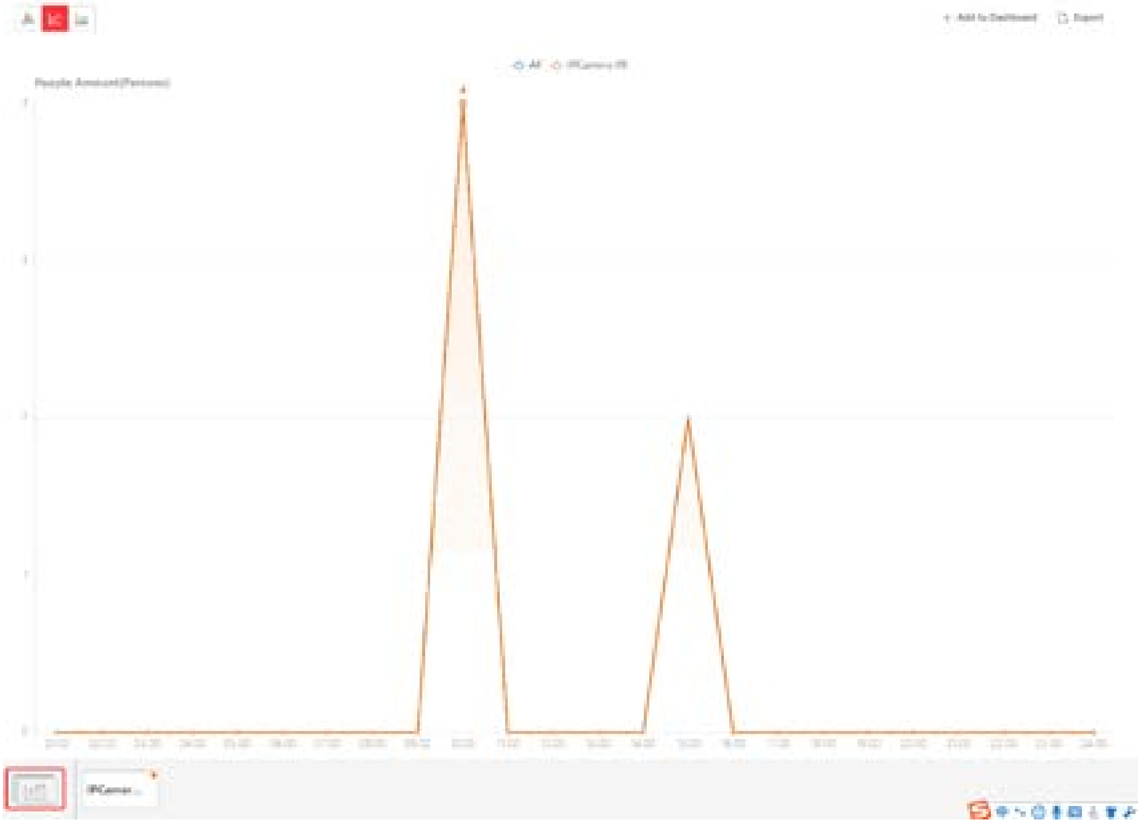


Figure 21-9 Line Chart of Heat Analysis

11. **Optional:** Export the report to the local PC.
    1) Click **Export**.

       The Export panel will display with camera selected and time configured according to the range you defined previously.
    2) (Optional) Select the camera, and set the analysis type and report time if needed.
    3) Select shorter time period to view more detailed data of each camera.

       Example

       For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1, 24 records respectively for each camera.
    4) Set the format of the exported file as Excel, CSV, or PDF.
    5) Click **Export**.

21.5.3 Send Heat Analysis Report Regularly

You can set a regular report rule for specified heat map cameras, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the heat map data (people dwell time at each location and number of people detected) during the specified 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. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Scheduled Report** .
2. Click **Add** to open the Create Report page.
3. Select **Heat Analysis** as the report category.
4. 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 Heat Analysis Group*** .
5. Create a name for the report.
6. Select the 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).
7. Set the report type as **Daily**, **Weekly**, or **Monthly**.

   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.

   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.

8. After setting the report type, set how the report will present results analyzed in the specified time period.

   Example

   For example, if you select the report type as **Weekly**, you can select **Calculate by Day** or **Calculate by Hour**. There will be 7 or 7×24 records for each camera respectively in the report, showing the people amount or dwell time detected on each day or each hour for one camera.

9. Set the content in the report.

   Dwell Time

   The minutes that the people stay at the same location during each time period for each camera.

   People Amount

   The number of people detected during each time period for each camera.

   Note

   This content can be selected only when the analysis type is selected as **Heat Analysis for One Camera**.

   Average Dwell Time

   The average time that each people stay at a same location during each time period for each camera. The value is calculated by dividing the dwell time by the number of people who appear at the location.

   Note

   - The Number of People who Appear at a Location= The Number of People who Stay at the Location at the End of Previous Time Period + The Number of People who Visit the Location at the Current Time Period.
   - The number of people who appears at a location refers to the number of people who visits the location from 00:00:00 to 23:59:59.

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. 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.

13. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

14. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

Note

You can also click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

15. **Optional:** Switch on **Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

Note

You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.

16. Click **Add**.

21.6 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.

For details about adding a pathway analysis group, refer to ***Add Pathway Analysis Group*** .

21.6.1 Add 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.

Steps

Note

This function is only supported by the second generation of fisheye cameras. You should have configured intersection analysis rule for the fisheye camera. If not, click **Configuration** to set that on the remote configuration page of the device.

1. In the top left corner of the client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Pathway Analysis Group** .
2. Click **Add**.
3. Create a name for the group.
4. Select the fisheye cameras for calculating the number of people on different directions in specific pathway.
5. Click **Add**.

   The pathway analysis group is added in the table and you can view the cameras in the group.
6. **Optional:** Locate the pathway analysis group on the map by setting the locations of the fisheye cameras in the group and setting the directions for camera's exits.

   Note

   To define the camera's exits, refer to the user manual of the camera.

   1) Click **Set Geographic Location** to enter the Map Settings page.
   2) Drag the pathway 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.
   3) Drag the icons of the cameras to set the their locations on the map.
   4) Click an exit of the fisheye camera as starting point and then draw a line, indicating the direction of the pathway.
   5) Enter the pathway name and select an exit for this pathway.
   6) Click **Save** to save the pathway.
   7) Perform the above sub-steps to draw other pathways.

Note

You can also draw a line to link the exits of two fisheye cameras if there are two cameras in the pathway.

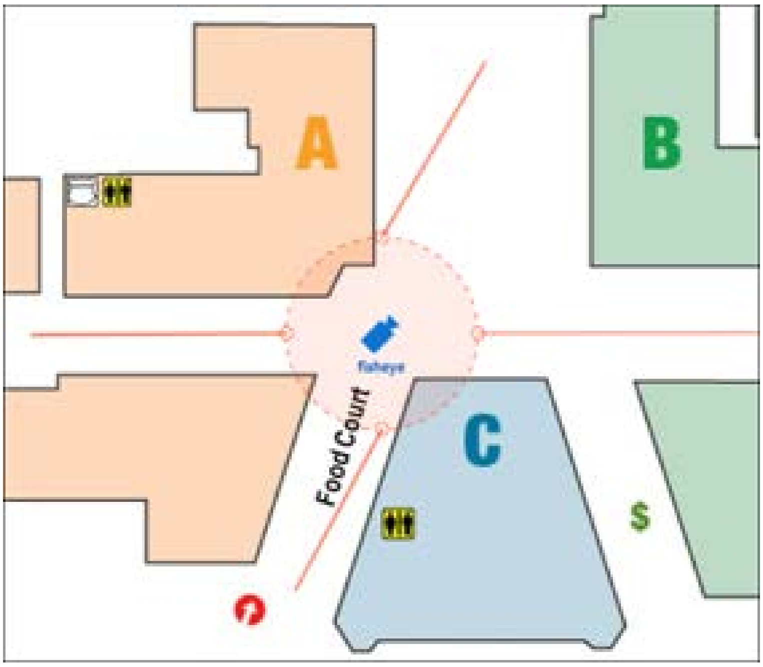


Figure 21-10 Add Pathway Analysis Group

8) **Optional:** Click the camera icon and select **Edit Direction Area** to set radius, view angle and direction.
9) Right click to finish.

After adding the pathway analysis group on the map, you can view the real-time number of people walking by on the Control Client.

21.6.2 Generate 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.

Before You Start

- Properly add 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*.
- You should have added pathway analysis groups. For details, see ***Add Pathway Analysis Group*** .

Steps

Note

This function is only supported by the second generation of fisheye cameras.

1. In the top left corner of the Client, select 🟥 → **All Modules → Intelligent Analysis → Analysis Report → Pathway Analysis** .
2. Select path analysis group(s) for statistics.
3. Select the report type as daily report, weekly report, monthly report, annual report, or customize the time interval for a report.

   Daily Report

   Daily report shows data on a daily basis. The platform will calculate the number of people or people dwell time in each hour of one day.

   Weekly Report, Monthly Report, 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.

   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 in the Time field for statistics.

   Note

   For custom time interval report, you need to set the start time and end time to specify the time period.
5. Click **Generate Report**.

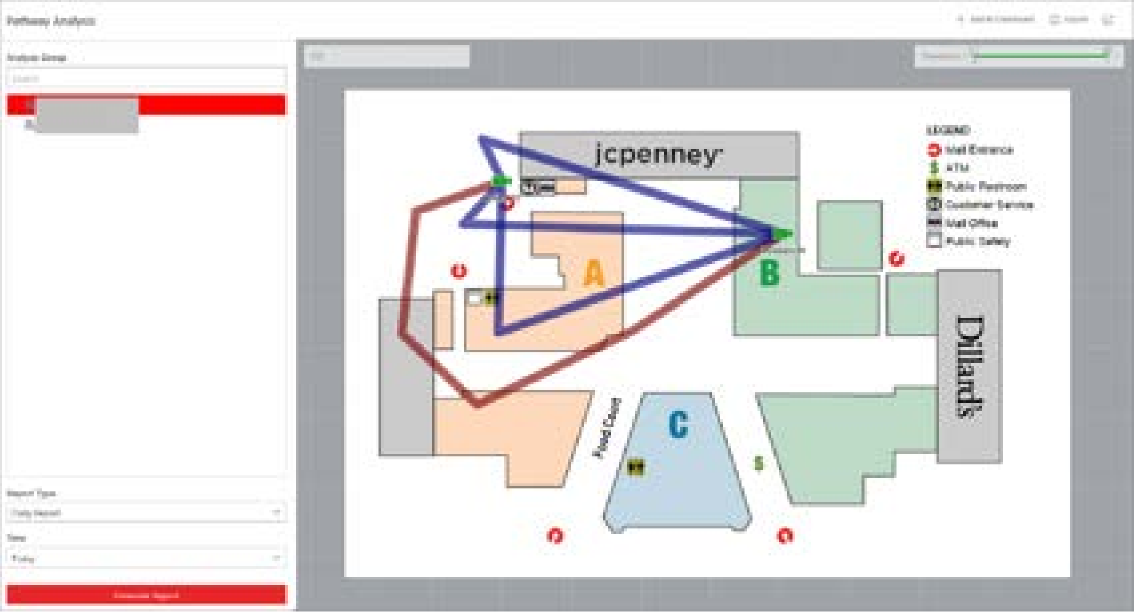


Figure 21-11 Pathway Analysis Report

The static map with the cameras and pathways color coded on the map will be displayed. The red color block (255, 0, 0) indicates the most welcome pathway (most persons detected or longest dwell time), and blue color block (0, 0, 255) indicates the less-popular pathway (least persons detected or shortest dwell time).

6. Move the cursor to the camera hot spot to view the line chart or heat map of the people amount and people dwell time in the pathways during this time period.

Figure 21-12 View Heat Map or Line Chart

7. **Optional:** Export the report to the local PC.
   1) Click **Export**.

      The Export panel will display with camera selected and time configured according to the range you defined previously.
   2) (Optional) Select the pathway analysis group and set the report type and report time if needed.
   3) Select shorter time period to view more detailed data of each camera.

Example

For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1, 24 records respectively for each camera.

4) Set the format of the exported file as Excel, CSV, or PDF.
5) Click **Export**.

21.6.3 Send Pathway Report Regularly

You can set a regular report rule for specified fisheye cameras which support pathway analysis, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the people counting data (people dwell time at each location and number of people) on the configured pathways, detected by these fisheye cameras, during the specified 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. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Scheduled Report** .
2. Click **Add** to open the Create Report page.
3. Select the report category as **Pathway Analysis**.
4. Create a name for the report.
5. Select the pathway analysis group(s) contained in the report.
6. Set the report type as **Daily**, **Weekly**, or **Monthly**.

   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.

   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.

7. Set how the report will present results analyzed in the specified time period.

   Example

   For example, if you select the report type as **Weekly**, you can select **Calculate by Day** or **Calculate by Hour**. There will be 7 or 7×24 records for each camera respectively in the report, showing analysis results on each day or each hour for one camera.

8. Set the report time and sending time according to the report type.
9. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
10. 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.

11. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

12. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

    Note

    You can also click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

13. **Optional:** Switch on **Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

    Note

    You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.

14. Click **Add**.

21.7 Person Feature Analysis Report

Person feature analysis report shows the proportion of persons with different features detected by cameras which support facial recognition. The person features refers to the gender and age group of the detected persons, such as male, female, child, the elderly, and teenager.

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.

For details about adding a person feature analysis group, refer to ***Add Person Feature Analysis Group*** .

21.7.1 Add Person Feature Analysis Group

Person feature analysis is a group of cameras which support facial recognition and feature analysis (such as gender and age group). 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.

Steps

1. In the top left corner of the client, select ■ → **All Modules → Intelligent Analysis → Analysis Group Settings → Person Feature Analysis Group** .
2. Click **Add**.
3. Create a name for the group.
4. Select a site.
5. Select the cameras for analyzing the detected persons' age and gender.
6. Click **Add**.

   The feature group is added in the table and you can view the cameras in the group.
7. **Optional:** Locate the person feature analysis group on the map by setting the locations of the cameras in the group and setting the border of the region for detection.
   1) Click **Set Geographic Location** to enter the Map Settings page.
   2) 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.
   3) Drag to draw the region according to the actual needs.
   4) Drag the icons of the cameras to set the their locations on the map.
   5) Right click to finish.

After adding the person feature analysis group on the map, you can view the features of the persons appeared on the Control Client.

21.7.2 Generate Person Feature Analysis Report

The platform supports saving features (including age and gender) of recognized human faces and generating reports in various time periods. The reports tells the percentage and number of people of different gender and age groups in different time period. It can be used in places such as shopping mall to analyze interests of people in different gender and age.

Before You Start

Make sure you have added a person feature analysis group if you want to perform feature analysis in one region. See ***Add Person Feature Analysis Group*** for details about adding a person feature analysis group.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Report** → **Person Feature Analysis** .
2. Select analysis type.

   Feature Analysis for One Camera

   Compare percentage and number of people of different gender and age groups detected by specified camera(s).

   Feature Analysis in One Region

   Compare percentage and number of people of different gender and age groups detected by the cameras in specified person feature analysis group(s) of multiple regions.
3. Select camera(s)/person feature analysis group(s).

   Note

   - Only online cameras will be displayed.
   - Up to 20 cameras/groups can be selected for statistics at the same time.
   - The platform supports selecting one group of a Remote Site.
4. Select the report type as daily report, weekly report, monthly report, annual report, or customize the time interval for a report, and the platform will generate statistics of the selected camera(s)/group(s) of the current day/week/month/year or the customized period.
5. Set the time or time period in the Time field for statistics.

   Note

   For custom time interval report, you need to set the start time and end time to specify the time period.
6. Click **Generate Report**.

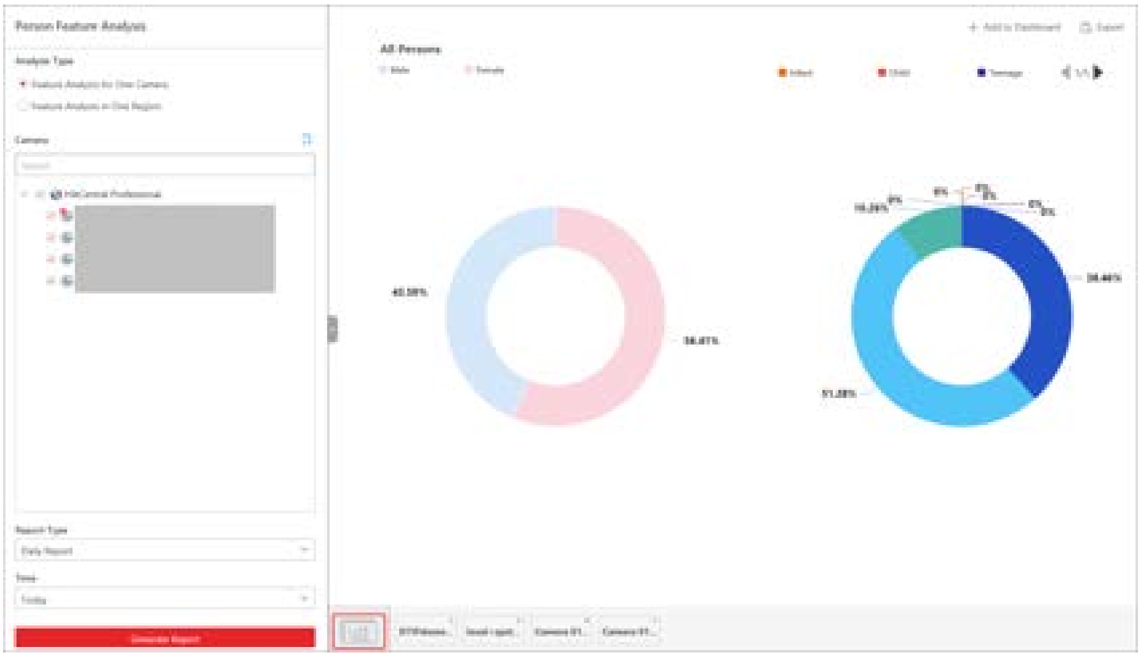


Figure 21-13 Person Feature Analysis

The statistics of all the selected cameras/groups are displayed on the right panel.

7. **Optional:** Click **Add to Dashboard** to display the report on the Dashboard.
8. **Optional:** Export the report to the local PC.
   1) Click **Export**.

      The Export panel will display with camera selected and time configured according to the range you defined previously.
   2) (Optional) Select the camera or group and set the report type and report time if needed.
   3) Select shorter time period to view more detailed data of each camera.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1or 24 records respectively for each camera.
   4) Set the format of the exported file as Excel, CSV, or PDF.
   5) Click **Export**.

21.7.3 Send Person Feature Analysis Report Regularly

You can set a regular report rule for specified cameras of person feature analysis, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the percentage and number of people of different genders and ages during the specified 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. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Scheduled Report** .
2. Click **Add** to open the Create Report page.
3. Select **Person Feature Analysis** as the report category.
4. Select person feature type.

   Feature Analysis for One Camera

   Compare percentage and number of people of different gender and age groups detected by specified camera(s).

   Feature Analysis in One Region

   Compare percentage and number of people of different gender and age groups detected by the cameras in specified person feature analysis group(s) of multiple regions.
5. Create a name for the report.
6. Select the camera(s) or person feature analysis groups contained in the report.

   Note

   If you select **Feature Analysis for One Camera** as person feature type, you should select camera(s). If you select **Feature Analysis in One Region**, you should select feature analysis group(s).
7. Set the report type as **Daily**, **Weekly**, or **Monthly**.

   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.

   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.

8. Set how the report will present results analyzed in the specified time period.

   Example

   For example, if you select the report type as **Weekly**, you can select **Calculate by Day** or **Calculate by Hour**. There will be 7 or 7×24 records for each camera respectively in the report, showing the percentage and number of people of different gender and age groups detected on each day or each hour for one camera.

9. Set the report time and sending time according to the report type.
10. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
11. 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.

12. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

13. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

    Note

    You can also click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

14. **Optional:** Switch on **Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

    Note

    You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.

15. Click **Add**.

21.8 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.

21.8.1 Generate 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 thermometry points on different presets.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Intelligent Analysis** → **Analysis Report** → **Temperature Analysis** .
2. Select thermal camera(s) for statistics.
   1) Click in the camera panel.
   2) Select a current site or Remote Site from the drop-down site list to show its thermal cameras.

      Note

      Only the online thermal cameras will be displayed here.

   3) Check the thermal camera(s) for statistics.

      The cameras will be added to the camera list.
3. Select the preset(s) configured on the camera and the platform will collect the data on the thermometry point in these presets.

   Note

   For configuring the thermometry point with temperature measurement rules, refer to the user manual of the thermal camera.
4. Select the report type as daily report, weekly report, monthly report, annual report, or customize the time interval for a report.

   Daily Report

   Daily report shows data on a daily basis. The platform will calculate the temperature data detected in each hour of one day.

   Weekly Report, Monthly Report, 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 temperature data detected in each day of way week, in each day of one month, and in each month of one year.

   Custom Time Interval

   Users can customize the days in the report to analyze temperature data detected in each day or month of the custom time interval.
5. Set the time or time period in the Time field for statistics.

Note

For custom time interval report, you need to set the start time and end time to specify the time period.

6. Click **Generate Report**.

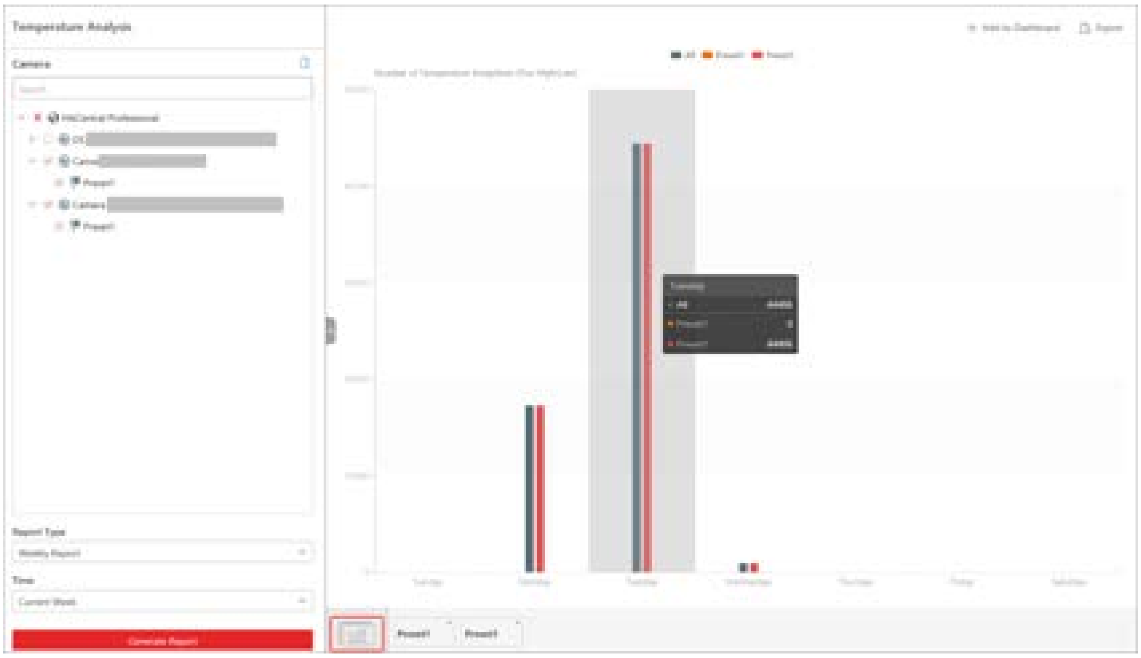


Figure 21-14 Temperature Analysis Report

The temperature statistics of all the selected presets are displayed in the right panel.

7. **Optional:** Perform the following operation(s) after generating the temperature report.

Show/Hide Certain Data
Click the legend to show or hide the data of certain element, such as certain preset or thermometry point.

View Temperature Report of Single Preset
Click the preset icon on the page below to view the report in the single preset.

View Temperature Report of Single Thermometry Point

a. Click the preset icon on the page below to view the report in the single preset.
b. In the **Item for Comparison** field, select one thermometry point.
c. In the **Item for Comparison** field, select the indicator you want to view in the chart.

High/Low Temperature

Shows the number of exceptions that the temperature at this thermometry point is higher or lower than the pre-defined temperature.

Max. Temperature

Shows the maximum temperature at this thermometry point during the set time period.

The temperature is displayed in line chart, indicating the trend.

Min. Temperature

Shows the minimum temperature at this thermometry point during the set time period.

The temperature is displayed in line chart, indicating the trend.

8. **Optional:** Export the report to the local PC.
   1) Click **Export**.

      The Export panel will display with camera selected and time configured according to the range you defined previously.
   2) (Optional) Select the camera and preset, and set the report type and report time if needed.
   3) Select shorter time period to view more detailed data of each camera.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour**, or **By Minute** and it will export 1, 24, or 24×60 records respectively for each thermometry point.
   4) Select the content to export.

      Temperature Exception

      Export the number of exceptions on temperature (temperature too high or too low) of each thermometry point.

      Temperature Status

      Export the maximum temperature and minimum temperature of each thermometry point.
   5) Set the format of the exported file as Excel, CSV, or PDF.
   6) Click **Export**.

21.8.2 Send Temperature Analysis Report Regularly

You can set a regular report rule for specified thermal cameras, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing temperature exceptions or min./max. temperature, detected by these thermal cameras during the specified 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. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Scheduled Report** .
2. Click **Add** to open the Create Report page.
3. Select the report category as **Temperature Analysis**.
4. Create a name for the report.
5. Select the thermal camera(s) and presets contained in the report.

   The report will show the temperature exceptions (including temperature too high or too low) or maximum and minimum temperature of different thermometry points on these presets.
6. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   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 the temperature exceptions or min./max. temperature detected between 00:00 and 24:00 before the current day.

   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 the temperature exceptions or min./max. temperature detected 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 temperature exceptions or min./max. temperature detected between last Monday and Sunday.
7. Set how the report will present results analyzed in the specified time period.

   Example

   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 thermometry point respectively in the report, showing the temperature exceptions or min./max. temperature detected in each hour or each minute.
8. Set the content in the report.

   Temperature Exception

   The number of exceptions on temperature (temperature too high or too low) of each thermometry point.

   Temperature Status

The maximum temperature and minimum temperature of each thermometry point.

9. Set the report time and sending time according to the report type.
10. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
11. 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.

12. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

13. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

Note

You can also click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

14. **Optional:** Switch on **Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

Note

You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.

15. Click **Add**.

21.9 Vehicle Analysis Report

Vehicle analysis report shows the number of passing vehicles detected by the specified cameras during specified time period.

You can set a regular report rule for the specified ANPR cameras, and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a vehicle analysis report at any time to view the data if required.

21.9.1 Generate Vehicle Analysis Report

For ANPR cameras and entrances & exits, you can generate a report to show the number of passing vehicles detected by specified cameras during specified time periods.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Report** → **Vehicle Analysis** .
2. Select **ANPR** or **Entrance & Exit** for the statistical type.
3. Select ANPR camera(s) or entrance(s) & exit(s) for analysis.
   - Select ANPR Camera:
     a. Click in the camera panel.
     b. Select a current site or Remote Site from the drop-down list to show its ANPR cameras which support this function.

     Note

     Only the online ANPR cameras will be displayed here.

     c. Check the camera(s) for analysis.
     d. Select the camera(s) for the report in the camera list.

     Note

     Up to 20 ANPR cameras can be selected for statistics at the same time.

   - Select Entrance & Exit:

     Check the entrance(s) & exit(s) for analysis.
4. Select the report type as daily report, weekly report, monthly report, 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 to 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 will calculate the number of vehicles in each day of way week, in each day of one month, and in each month of one year.

   Custom Time Interval

   Users can customize the days in the report to analyze the number of vehicles in each day or month of the custom time interval.
5. Set the time or time period for statistics.

   Note

   For the custom time interval report, you need to set the start time and end time to specify the time period.
6. Click **Generate Report**.

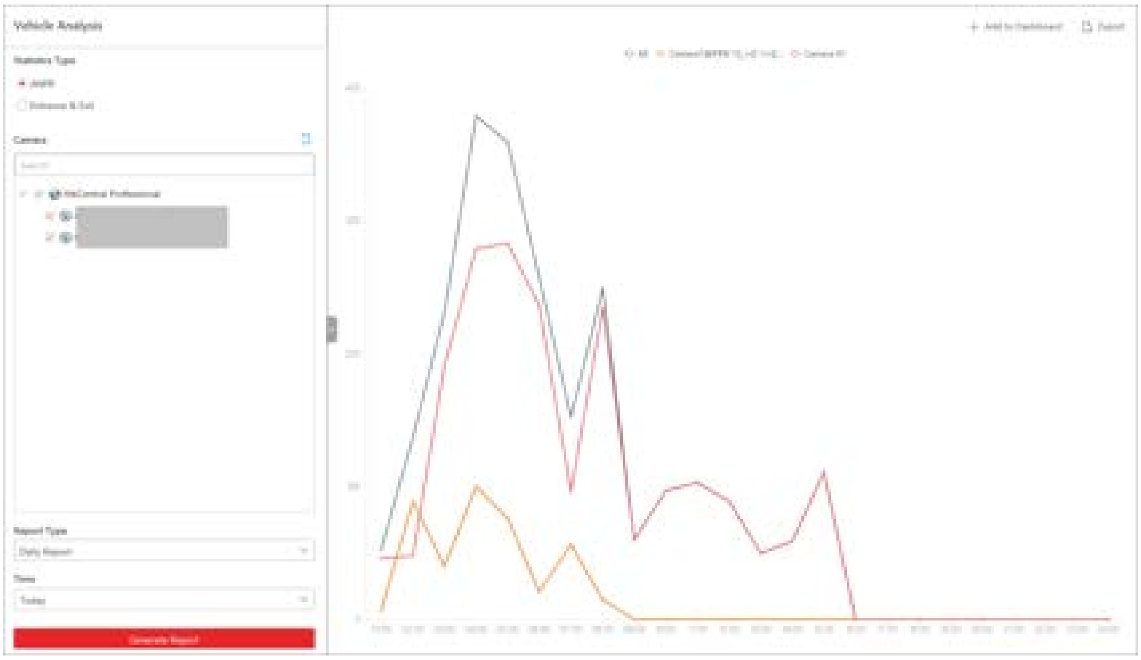


Figure 21-15 Vehicle Analysis Report

The passing vehicles statistics detected by all the selected cameras are displayed in the right panel.

7. **Optional:** Export the report to the local PC.
   1) Click **Export**.

      The Export panel will display camera selected and time configured according to the range you defined previously.
   2) **Optional:** Select the camera and set the report type and report time if needed.
   3) Select a shorter time period to view more detailed data of each camera.

      Example

      For example, if you select the daily report, you can select **By Day** or **By Hour**, and it will export 1or 24 records respectively for each camera.

      Note

      If you select **By Minute**, the number of records depends on the configuration on the device. For example, if the device reports vehicle analysis data to the platform every minute, it will export 24*60 records for each camera.
   4) Set the format of the exported file as Excel, CSV, or PDF.
   5) Click **Export**.

21.9.2 Send Vehicle Analysis Report Regularly

You can set a regular report rule for specified ANPR cameras, and the platform can 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 specified 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. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select 🟥 → **All Modules → Intelligent Analysis → Analysis Group Settings → Scheduled Report** .
2. Click **Add** to open the Create Report page.
3. Select the report category as **Vehicle Analysis**.
4. Create a name for the report.
5. Select the ANPR camera(s) contained in the report.
6. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   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 the number of passing vehicles detected between 00:00 and 24:00 before the current day.

   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 the number of passing vehicles detected 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 number of passing vehicles detected between last Monday and Sunday.
7. Set how the report will present results analyzed in the specified time period.

Example

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.

8. Set the report time and sending time according to the report type.
9. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
10. 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.

11. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

12. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

Note

You can also click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

13. **Optional:** Switch on **Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

Note

You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.

14. Click **Add**.

21.10 Skin-Surface Temperature Screening Report

The skin-surface temperature screening report shows the number of people with abnormal skin-surface temperature or who do not wear face masks during different time periods.

You can set a regular report rule for specified temperature screening cameras or access control devices with temperature screening function, and then the platform will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a skin-surface temperature screening report at any time to view the data if required.

21.10.1 Generate Skin-Surface Temperature Analysis Report

You can generate the skin-surface temperature analysis report to view the variation trend of the number of people with abnormal skin-surface temperature.

Before You Start

- Make sure you have added devices that support temperature screening to HikCentral Professional.
- Make sure you have enabled temperature screening on the device. For details, see the user manual of the device.

Steps

1. In the top left corner of the Client, select 🟥 → **All Modules** → **Intelligent Analysis** → **Analysis Report** → **Skin-Surface Temperature** .
2. Select the analysis type.

   Temperature Screening Point

   A skin-surface temperature report based on data from temperature screening points (e.g. cameras and visitor terminals) you select will be generated.

   Person Group

   A skin-surface temperature report based on the data from the person groups you select will be generated.
3. Select temperature screening point(s) or person group(s) for analysis.
   - Select Temperature Screening Point:
     a. Click to open the camera list panel.

     Note

     Only the online cameras will be displayed.

     b. (Optional) Check **Include Sub-Area** to select the sub-areas of the area that you have selected.
     c. Select an area in the area list to show the related temperature screening points.
     d. Check the temperature screening point(s) for screening.
     e. Select temperature screening point(s) for the report in the temperature screening point list.
   - Select Person Group:

     Check the person group(s) for screening.

   Note

   You can check **Select Sub-Groups** to select the sub-groups of the person group that you have selected.
4. Set the report type to daily report, weekly report, monthly 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 peak amount of people appeared in the images of the camera in each hour of one day.

Weekly Report, Monthly Report

Compared to generating the daily report, generating the weekly report and monthly report can be less time-consuming. The platform will calculate the peak amount of people on each day of one week and on each day of one month respectively.

Custom Time Interval

Users can customize the days in the report to analyze the peak amount of people in each day or month of the custom time interval.

5. In the Time field, select a predefined time period or customize a time period for search.
6. Click **Generate Report**.

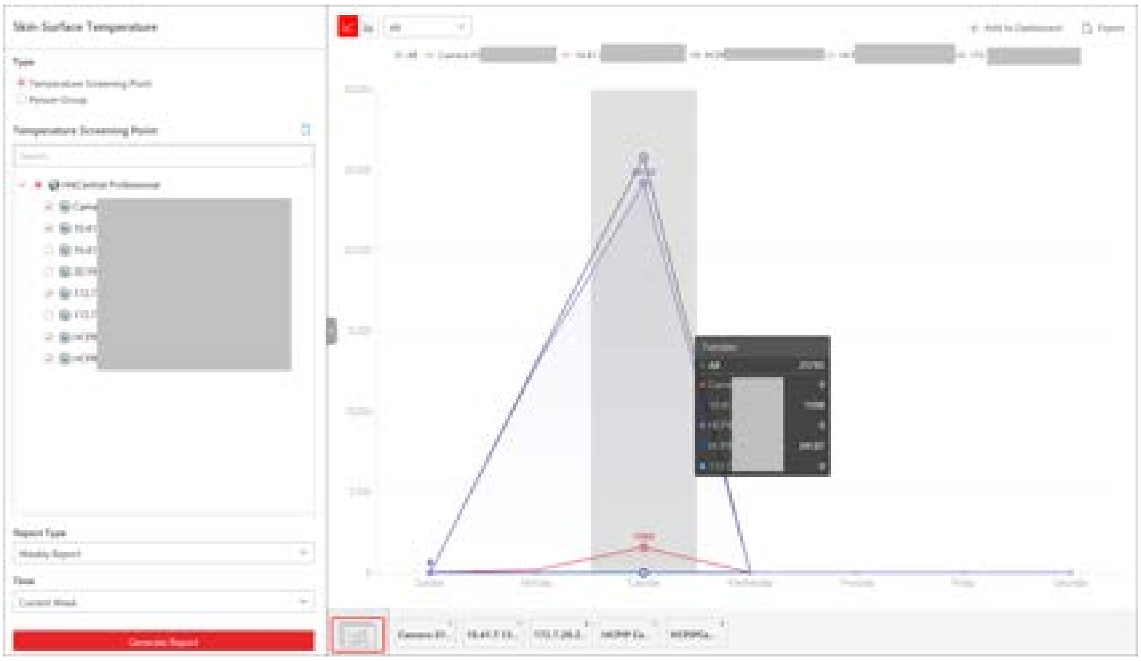


Figure 21-16 Skin-Surface Temperature Analysis Report

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 data of certain element, such as certain camera.
View Abnormal Temperature or No Mask Statistics	In the top left corner of the chart, select Abnormal Temperature or No Mask from the drop-down list to display the statistics of people with abnormal temperature and without wearing face mask, respectively.
Switch Between Line Chart and Histogram	Click 📈 / 📊 to switch between line chart and histogram.

	Note Daily report only supports histogram.
Add a Report 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**.

8. **Optional:** Export the report to the local PC.
   1) Click **Export**.
   2) **Optional:** Select the temperature screening point(s) or person group(s) and set the report type and report time if needed.
   3) Select shorter time period to view more detailed data of each camera.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1or 24 records respectively for each camera.
   4) Set the format of the exported file as Excel, CSV, or PDF.
   5) Click **Export**.

21.10.2 Send Skin-Surface Temperature Screening Report Regularly

You can set a report-sending rule for specified cameras. Once set, the platform will send an email containing the skin-surface temperature screening report to the target recipients daily, weekly, or monthly, showing the variation trend of the number people whose skin-surface temperatures are abnormal.

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 the sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select ■ → **All Modules** → **Intelligent Analysis** → **Analysis Group Settings** → **Scheduled Report** .
2. Click **Add** to open the Create Report page.
3. Select the report category as **Skin-Surface Temperature**.

4. Select the analysis type.

   Temperature Screening Point

   The report contains the skin-surface temperature data from temperature screening points (e.g. cameras). You need to select the temperature screening point(s) as the Report Target.

   Person Group

   The report contains the skin-surface temperature data from the person groups. You need to select the person group(s) as the Report Target.
5. Create a name for the report.
6. Select temperature screening point(s) or person group(s).
7. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   Daily Report

   The daily report shows data on a daily basis. The platform will send one report at the sending time every day, which contains the 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 the analysis results between 00:00 and 24:00 before the current day.

   Weekly Report and Monthly Report

   As compared to the daily report, the 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 the weekly report, if you set the sending time as 6:00 on Monday, the platform will send a report at 6:00 on every Monday morning, containing the analysis results between last Monday and Sunday.
8. Set how the report will present the analysis results generated in the specified time period.

   Example

   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 results analyzed in each hour or each minute by one camera.
9. Set the report time and sending time according to the report type.
10. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
11. 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.
12. **Optional:** Switch on **Send Report 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 New** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

13. **Optional:** Switch on **Upload to SFTP**, and click **Configuration** beside **SFTP Address** to configure the SFTP settings, including SFTP address, port, user name, password, and saving path.

Note

You can also click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

14. **Optional:** Switch on **Local Storage**, and click **Configuration** beside **Saving Path** to configure the saving path of local storage.

Note

You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.

15. Click **Add**.

Chapter 22 Digital Signage Management

Digital signage management includes managing materials, programs, schedules, release, etc. It is widely applied to the industries of entertainment, finance, and traffic for information release. You can upload local and dynamic materials to the platform for creating programs. The programs can be released and played on the terminals according to the configured schedule. Also, the platform supports more other functions including cutting in programs and cutting in text messages.

22.1 Flow Chart

For the first time, you can follow the flow chart below.

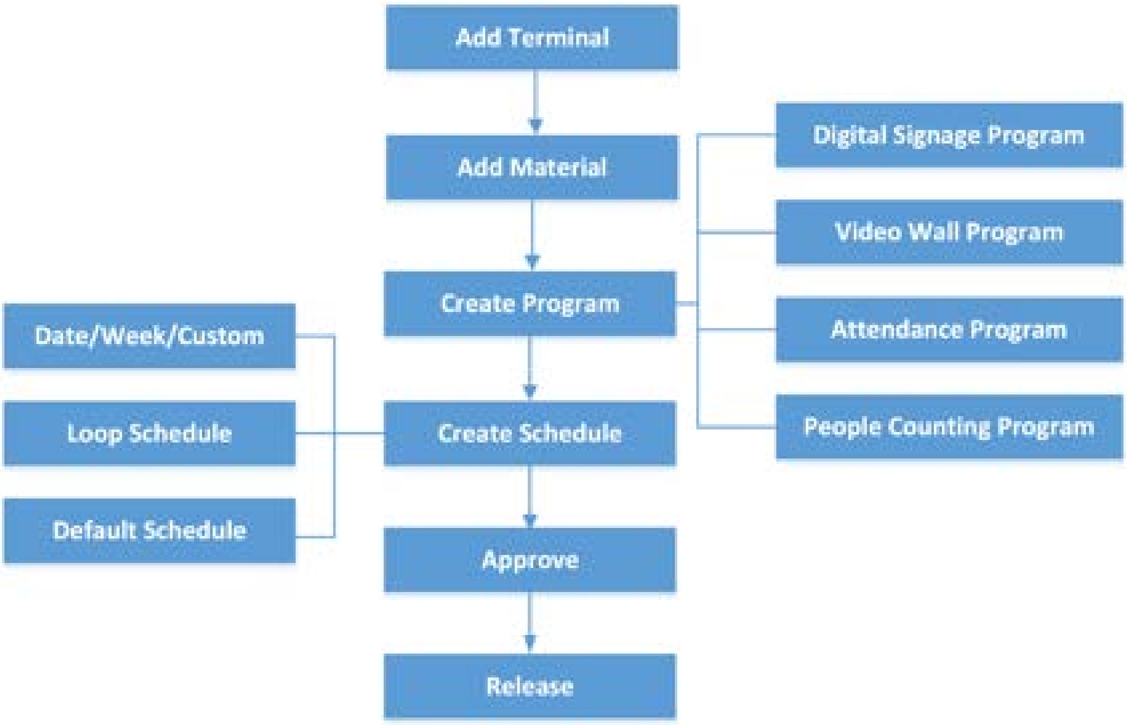


Figure 22-1 Flow Chart

- **Add Terminal & pStor:** You should add digital signage terminals and pStor to the platform. For details, refer to ***Manage Digital Signage Terminals*** and ***Add pStor*** .
- **Add Material:** Material is used for creating programs. You can upload local materials from local PC, or create dynamic materials in the platform. For details, refer to ***Material Management*** .
- **Create Program:** You can create different programs including digital signage program, video wall program, attendance program, and people counting program in the platform according to the required application scenarios. For details, refer to ***Program Management*** .

- **Create 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 ***Schedule Management*** .
- **Approve:** The added materials, programs and schedules should be approved before they are used. For details, refer to ***Approve*** .
- **Release:** You can view the release details and release progress of multiple tasks such as schedule releasing. After being released, the related task can take effect on the terminals. For details, refer to ***Release Management*** .

22.2 Material Management

Material is used for creating programs. The platform supports various types of materials such as picture, video, and audio to meet with different program requirements. You can upload materials from local PC to the platform, or create dynamic materials in the platform. After uploading the materials, you can mange them including editing, searching, replacing, etc.

22.2.1 Upload Local Material

You can upload local materials which can be used for creating programs. The materials supported to be uploaded include picture, video, audio, document, APP, etc. For the uploaded materials, you can perform more operations, including adding to favorites, editing, downloading, deleting, etc.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Digital Signage** → **Materials** .
2. Click **Upload Local Material** and select one or more materials to be uploaded from the local PC.

Table 22-1 Supported Material Types and Formats

Material Types	Formats
Picture	BMP, JPG, PNG, GIF, JPEG
Video	ASF, AVI, MPG, 3GP, MOV, MKV, WMV, FLV, MP4, RM, RMVB
Audio	MP3, WAV, WMA
Document	TXT, PDF, EXCEL, WORD, PPT
Webpage	HTML, HTM
APP	APK, ZIP

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.

3. Click **Open**.

   The selected local materials start to be uploaded. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails).

Note

- 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.

4. **Optional:** After uploading the materials, perform the following operations if needed.

Add to/Cancel Favorites
Click ☆ to add the material to favorites or move it from favorites.

Edit Material
Check one or multiple materials, and click **Edit** to edit the selected materials, such as editing the name and the property.

Delete Material
Check one or multiple 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 in the process of releasing.

Download Material
Click to download single material to the local PC.

View Large Picture
Click to view large picture of the material.

Refresh Material
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 Material
You can search the added materials via the three methods below.

- Enter a keyword on the upper right corner of the page, and click 🔍 to quickly find the target materials.
- Click ▼ , and filter the added materials according to the uploaded time, status, sharing property, etc.
- Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter the materials.

22.2.2 Create Dynamic Material

You can create and upload dynamic materials used for creating programs to the platform. The material types supported include webpage, network picture, stream media server, and network camera. For the uploaded materials, you can perform more operations, including adding to favorites, editing, downloading, deleting, etc.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Digital Signage** → **Materials** .
2. Click **Create Dynamic Material**, select the material type, and configure other parameters.

Material Type

Webpage

When selecting this type, you should enter the URL address of the webpage.

URL Picture

When selecting this type, you should enter the URL address of the picture.

Stream Media Server

Receive streams from the stream media server. You should enter the URL address of the stream media server.

IPC

Get video streams from network camera. You should enter the required information of network camera such as IP address, port No., and channel No.

Name

Define a material name that is easy to identify. Up to 64 characters can be entered.

Sharing Property

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.

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.

Description

Enter the detailed description of the material to be uploaded.

Area

Set the area which the material belongs to.

3. Finish uploading the material to the platform.
   - Click **Upload**.
   - Click **Upload and Continue** to upload the current material and continue to upload other materials.
4. **Optional:** Perform the following operations if needed.

Add to Favorites/Cancel
Click ☆ to add the material to favorites or move it from favorites.

Edit Material
Check one or multiple materials, and click **Edit** to edit the selected materials, such as editing the name and the property.

Delete Material
Check one or multiple 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 in the process of releasing.

View Large Picture
Click 🔍 to view large picture of the material.

Refresh Material
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 Material
You can search the added materials via the three methods below.

- Enter a keyword on the upper right corner of the page, and click 🔍 to quickly find the target materials.
- Click ▼ , and filter the added materials according to the uploaded time, status, sharing property, etc.
- Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter the materials.

22.3 Program Management

Program is composed of various materials. When released, the program will be played on the terminal to function as a prompt, notice, etc. You can add programs (including digital signage program, video wall program, attendance program, and people counting program) to the platform according to different application scenarios. When creating programs, you can custom the layout of the program and add materials to the program as needed. You can also manage the added programs such as previewing, releasing, and cutting in.

22.3.1 Create Digital Signage Program

Digital signage program can be used in multiple application scenarios (e.g., playing a program related with commodity information at the entrance of a chain supermarket), helping to spread information in a convenient and efficient way.

Before You Start

You have added materials to the platform and the materials have been approved. For details, refer to ***Material Management*** and ***Approve*** .

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **Digital Signage** → **Programs** → **Digital Signage** .
2. Click **Add**.
3. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

   Screen Size

   Select the screen size as Landscape Mode, Portrait Mode, or Custom.

   Sharing Property

   Public

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

   Private

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

   Area

   Set the area which the program belongs to.

   Description

   Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.
4. Click **Next**.
5. Select a template type and the corresponding template as needed.

Note

- You can click ☆ to add the template to Favorites. Up to 1,000 templates can be added to Favorites.
- You can click ☆ **My Favorites** in the lower-left corner to view and select the template that has been added to Favorites.

6. Click **OK** to enter the creating program page.

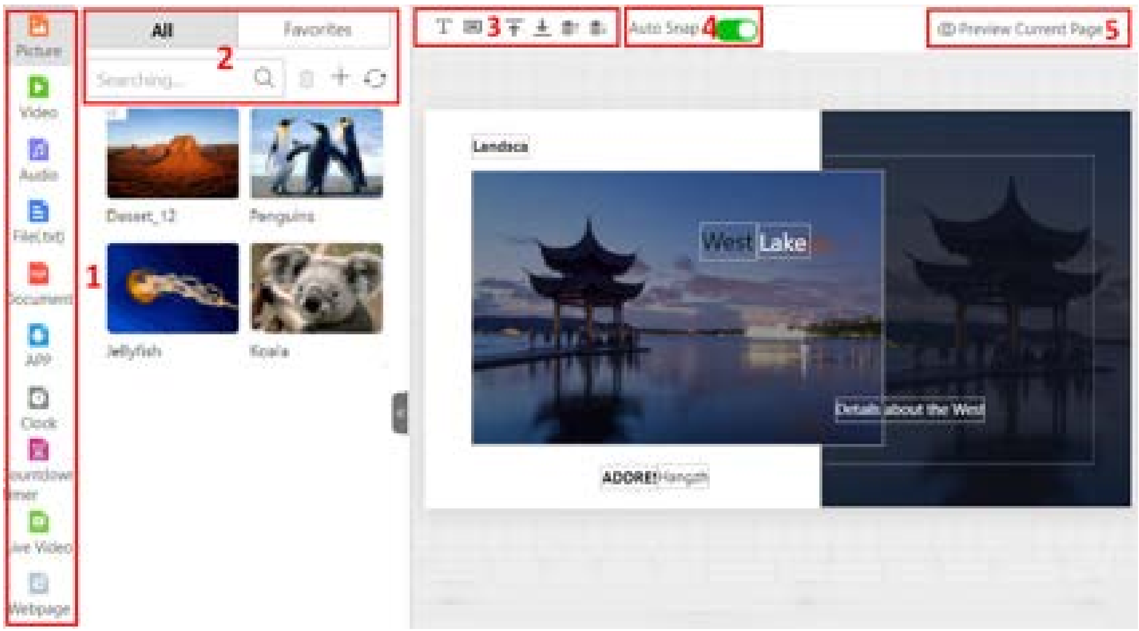


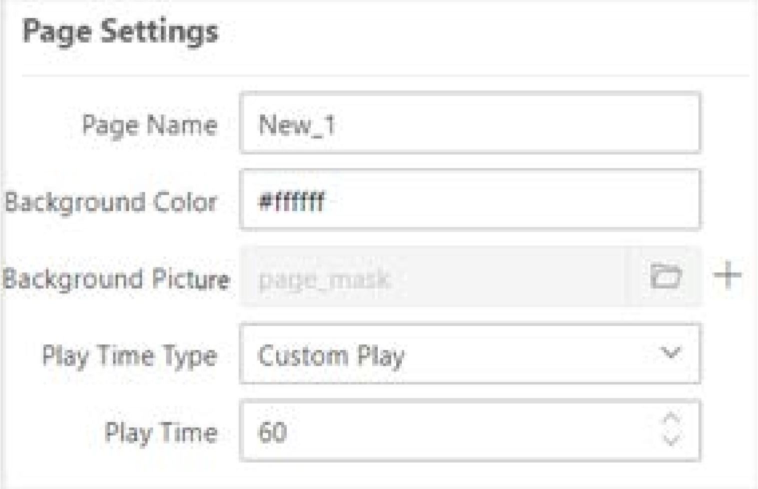
Figure 22-2 Create Program

Table 22-2 Page Description

Number	Description
1	There are 10 types of windows. An audio window cannot be added with a video window or live video window at the same time. Up to 16 windows can be added for one page.
2	You can select materials from **All** or **My Favorites** list. Click + to add other materials from local PC to the platform. Also, you can search materials, delete materials, and refresh material list.
3	You can click T to add a text window in the template; click ▭ to add a button window in the template (only available for touchscreen terminals); click ↑ / ↓ / ⤒ / ⤓ to make the window layer move up / move down / stick on top / stick at bottom.

Number	Description
4	You can enable **Auto Snap**, and the two windows will be connected when they are near enough.
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 fullscreen.

7. Edit page properties, including page name, background, and play time.



Page Settings

Page Name: New_1

Background Color: #ffffff

Background Picture: page_mask

Play Time Type: Custom Play

Play Time: 60

Figure 22-3 Page Settings

8. **Optional:** Add, delete, or adjust program pages at the bottom side.

Add	Click + / ⊕ to add new page(s).
Delete	Put the cursor on the page, and click ⊗ on the upper right corner to delete the current page.
Adjust Sequence	Click a page and drag it to the desired location to adjust the sequence of program pages.

9. Select a material from the left list and drag it to the corresponding window in the template to add the selected material.
10. Set window properties, including window position, window type, switching method, etc.

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.

No 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.

Move Window Layer

Click ↑ / ↓ / ⤒ / ⤓ to make the window layer move up / move down / stick on top / stick at bottom.

Switching Effect

Select the switching effect from the drop-down list for the current window. There are 11 types of switching effect.

Play Time

Set the playing duration for the current window.

Note

The playing time of a window can not exceed the playing time of a page, or the exceeding part of the program will not be played.

11. **Optional:** On the current editing program page, perform the following operations.

Edit Program	Click ✎ to edit program parameters in the pop-up window. For details, refer to Step 3.
Preview Program	Click **Preview** to preview the program.

Figure 22-4 Preview 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.

Cut-In

Click **Cut-in** to cut in the current program.

Note

For details, refer to ***Cut in Program*** .

Create Schedule

Click **Next** to enter the managing schedules page and create a schedule for the program.

Note

For details, refer to ***Schedule Management*** .

12. Click **Save** to save the current program.
13. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode

Click ▦ / ☰ to view the added programs in the thumbnail mode or in the list mode.

Add Program to Favorites

Click ☆ to add the current program to Favorites.

Preview Program

Click 👁 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

Click ⧉ 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.

Cut-In

Click ▶ to cut in the current program. For details, refer to ***Cut in Program*** .

Create Schedule

Click ▦ to enter the managing schedules page and create a schedule for the program. For details, refer to ***Schedule Management*** .

Enlarge Program Page

Click 🔍 to enlarge the program page and view it.

Filter Program

You can filter programs via the following three methods:

- Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter to filter programs according to whether they have been added to Favorites or not.
- Enter a keyword in the search field on the upper right corner, and click 🔍 to quickly search for the target programs.
- Click ⏷ , and filter programs by conditions such as status and sharing property.

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 or more programs, and click **Delete** to delete the selected programs. **Note** Programs that are releasing or cutting in cannot be deleted.

22.3.2 Create Video Wall Program

You can create video wall programs on the platform. The program can be used to display programs of multiple terminals joined in the video wall. The platform provides multiple layout choices for video wall programs. You can select a layout according to the actual scene and edit it as needed. After creating the program, you can preview the program, cut in program, etc.

Before You Start

You have configured video wall before applying the video wall programs. For details, refer to ***Configure Video Wall*** .

Steps

1. In the upper-left corner of the Home page, select 🟥 → **All Modules** → **Digital Signage** → **Programs** → **Video Wall** .
2. Click **Add**.
3. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

   Video Wall Dimension

   Set the video wall dimension.

   Note

   The maximum dimension is 1 × 10 or 10 × 1.

   Digital Signage Screen Type

   Select **Landscape Mode** or **Portrait Mode** as needed.

   Sharing Property

   Public

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

   Private

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

   Area

Set the area which the program belongs to.

Description

Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.

4. Click **Next**.
5. **Optional:** Select video wall layout according to actual need.
   - When the dimension is no bigger than 1 × 5 or 5 × 1 (i.e., 1 × 2, 2 × 1, 1 × 3, 1 × 4, 1 × 5), select a predefined video wall layout from the list.
   - When the dimension is bigger than 1 × 5 or 5 × 1 (i.e., 1 × 6, 1 × 7, 1 × 8, 1 × 9, 1 × 10), select **No Layout** or **Custom Layout**.
6. Click **OK**to enter the creating program page.

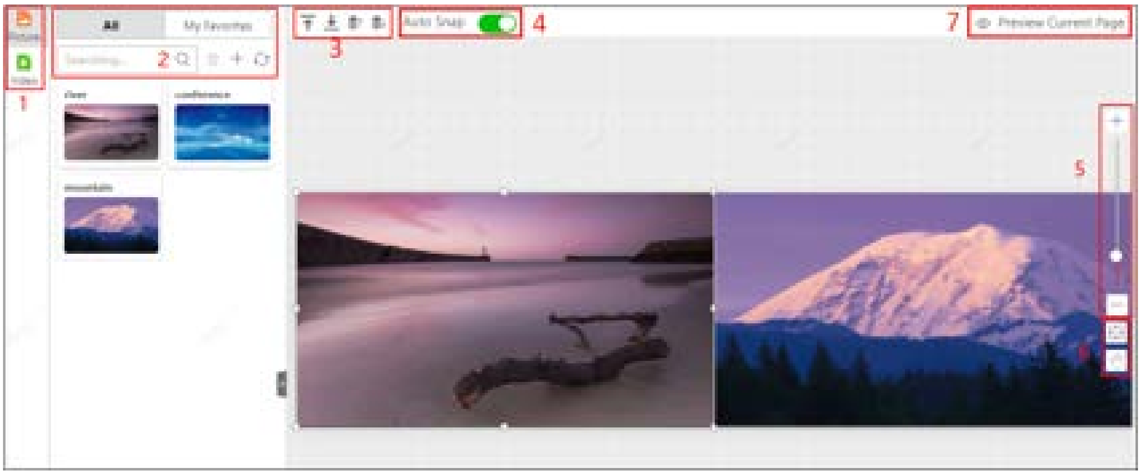


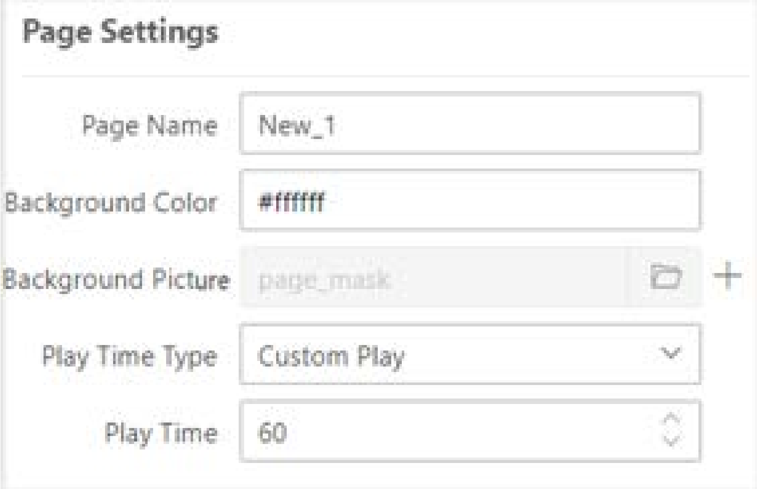
Figure 22-5 Create Program

Table 22-3 Page Description

Number	Description
1	There are 2 types of windows, including picture windows and video windows.
2	You can select materials from **All** or **My Favorites** list. Click + to add other materials from local PC to the platform. Also, you can search materials, delete materials, and refresh material list.
3	You can click ⤒ / ⤓ / ⬆ / ⬇ to make the window layer move up / move down / stick on top / stick at bottom.
4	You can enable **Auto Snap**, and the two windows will be connected when they are near enough. Also, the division lines will be connected when they are near enough.

Number	Description
5	You can click + / − or drag the slider to zoom in or zoom out the current page.
6	You can click ✋ / ⊡ to pan or reset the current page.
7	• 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 fullscreen.

7. Edit page properties, including page name, background, and play time.



Page Settings

Page Name: New_1

Background Color: #ffffff

Background Picture: page_mask

Play Time Type: Custom Play

Play Time: 60

Figure 22-6 Page Settings

8. **Optional:** Add, adjust, or delete program page(s) at the bottom side.

Add

Click + / ⊕ to add new page(s).

Delete

Put the cursor on the page, and click ⊗ on the upper right corner to delete the current page.

Adjust Sequence

Click a page and drag it to the desired location to adjust the sequence of program pages.

9. Select a material from the left list and drag it to the corresponding window to add the selected material.

10. Set window properties, including window position, window type, switching method, etc.

Current Window

Select the material added to the current window.

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.

No Skip

When the Window A played on the terminal, there is no other pop-up window or page.

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.

Move Window Layer

Click ↑ / ↓ / ⤒ / ⤓ to make the window layer move up / move down / stick on top / stick at bottom.

Switching Effect

Select the switching effect from the drop-down list for the current window. There are 11 types of switching effect.

Play Time

Set the playing duration for the current window.

Note

The playing time of a window can not exceed the playing time of a page, or the exceeding part of the program will not be played.

11. **Optional:** On the current editing program page, perform the following operations if needed.

Edit Program

Click ✎ to edit program parameters in the pop-up window. For details, refer to Step 3.

Preview Program

Click **Preview** to preview the current program.

Figure 22-7 Preview 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 current page 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.

Cut-In

Click **Cut In** to cut in the current program.

Note

For details, refer to ***Cut in Program*** .

Create Schedule

Click **Next** to enter the managing schedules page and create a schedule for the program.

Note

For details, refer to ***Schedule Management*** .

12. Click **Save** to save the current program.
13. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode

Click ▦ / ☰ to view the added programs in the thumbnail mode or in the list mode.

Add Program to Favorites

Click ☆ to add the current program to Favorites.

Preview Program

Click 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

Click 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.

Cut-In

Click ▶ to cut in the current program. For details, refer to ***Cut in Program*** .

Create Schedule

Click to enter the managing schedules page and create a schedule for the program. For details, refer to ***Schedule Management*** .

Enlarge Program Page

Click 🔍 to enlarge the program page and view it.

Filter Program

You can filter programs via the following three methods:

- Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter to filter programs according to whether they have been added to Favorites or not.
- Enter a keyword in the search field on the upper right corner, and click 🔍 to quickly search for the target programs.
- Click ⏷ , and filter programs by conditions such as status and sharing property.

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 or more programs, and click **Delete** to delete the selected programs. **Note** Programs that are releasing or cutting in cannot be deleted.

22.3.3 Create Attendance Program

You can create attendance programs on the platform. The program can be used to display the persons' basic information (name and gender), check-in time and temperature information. You can also configure welcoming words for persons when they check in. The platform provides two types of program templates including Attendance and Temperature Screening Template and Attendance Template. You can select one template according to the actual scene and edit the predefined template as needed. After creating the program, you can preview the program, cut in program, etc.

Before You Start

You have added terminal(s) to the platform and have linked a device that supports face attendance with the terminal. For details, refer to ***Add Terminal*** and ***Link External Device to Terminal*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Digital Signage** → **Programs** → **Attendance** .
2. Click **Add**.
3. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

   Screen Size

   Select the screen size as landscape mode or portrait mode.

   Sharing Property

   Public

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

   Private

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

   Area

   Set the area which the program belongs to.

   Description

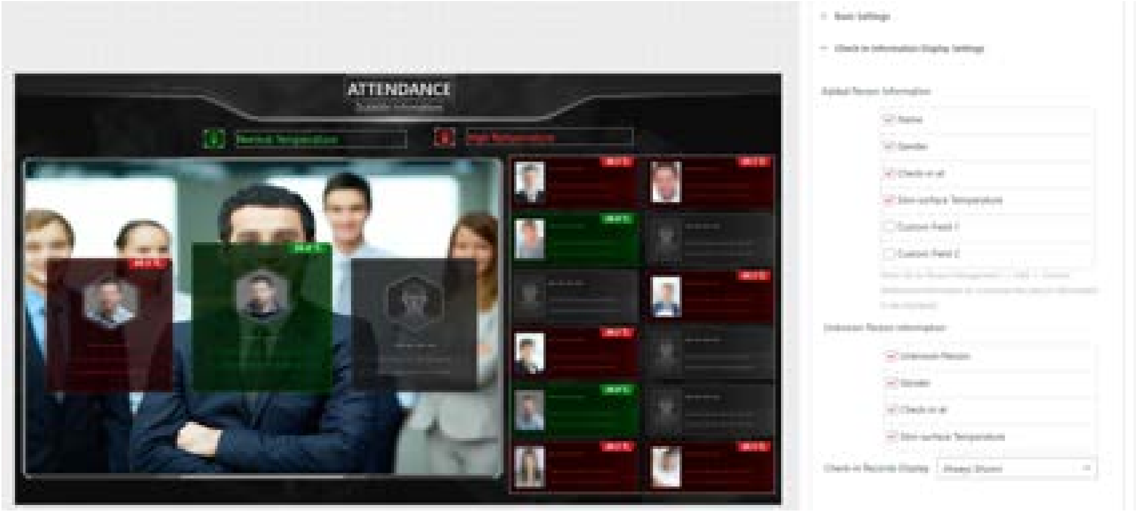
Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.

4. Click **Next**.
5. Select a template type and the corresponding template as needed.

Note

- You can click ☆ to add the template to My Favorites. Up to 1,000 templates can be added to Favorites.
- You can click ☆ **My Favorites** in the lower-left corner to view and select the template that have been added to Favorites.

6. Click **OK** to enter the creating program page.



Basic Settings

Check-in Information Display Settings

Added Person Information

☑ Name

☑ Gender

☑ Check-in at

☑ Skin-surface Temperature

□ Custom Field 1

□ Custom Field 2

Unknown Person Information

☑ Unknown Person

☑ Gender

☑ Check-in at

☑ Skin-surface Temperature

Check-in Records Display: Always Shown

Figure 22-8 Create Program

Basic Settings

Configure the content and font size for main title and sub title; enable Welcome Words and configure the content of welcome words; enable Audio Announcement and configure the related settings such as announcement speed, the content of person's voice and voice prompt; and set the Alarm Temperature Threshold.

Check-in Information Display Settings

Added Person Information

Configure whether to display the added person information, including name, gender, check-in time, and skin-surface temperature. You can also add custom fields.

Unknown Person Information

Configure whether to display the unknown person information, such as gender, check-in time, and skin-surface temperature. You can also configure the time period of displaying the check-in records.

Note

Added persons refers to persons that have been added to the platform, while unknown persons refers to persons that have not been added to the platform.

More

Click 🗀 to set the background picture for the current program.

Note

Make sure you have added picture materials to the platform and the materials have been approved. For details, refer to ***Material Management*** and ***Approve*** .

Advertisement Settings

You can add advertisements (pictures, videos, etc.) to the program, and configure switching effect and playing time for the advertisements.

Note

Only when selecting **Attendance Template**, you can configure advertisements.

7. **Optional:** On the current editing program page, perform the following operations if needed.

Edit Program
Click ✎ to edit program parameters in the pop-up window. For details, refer to Step 3.

Preview Program
Click **Preview** to preview the current program.

Figure 22-9 Preview 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.

Cut-In
Click **Cut-in** to cut in the current program.

Note

For details, refer to ***Cut in Program*** .

Create Schedule
Click **Next** to enter the managing schedules page and create a schedule for the program.

Note

For details, refer to ***Schedule Management*** .

8. Click **Save** to save the current program.
9. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode

Click ▦ / ☰ to view the added programs in the thumbnail mode or in the list mode.

Add Program to Favorites

Click ☆ to add the current program to Favorites.

Preview Program

Click 👁 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 current page in fullscreen.

Copy Program

Click ⧉ 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.

Cut-In

Click ▶ to cut in the current program. For details, refer to ***Cut in Program*** .

Create Schedule

Click 📅 to enter the managing schedules page and create a schedule for the program. For details, refer to ***Schedule Management*** .

Enlarge Program Page

Click 🔍 to enlarge the program page and view it.

Filter Program

You can filter programs via the following three methods:

- Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter to filter programs according to whether they have been added to Favorites or not.
- Enter a keyword in the search field on the upper right corner, and click 🔍 to quickly search for the target programs.
- Click ⊻ , and filter programs by conditions such as status and sharing property.

Refresh Program List

Click **Refresh** to refresh the program list. The programs will be listed according to the time they were added.

Delete Program

Check one or more programs, and click **Delete** to delete the selected programs.

Note

Programs that are releasing or cutting in cannot be deleted.

22.3.4 Create People Counting Program

You can create people counting program on the platform. The program is used to display the people counting information (the remaining people and people stayed) in a certain location, mask information, and skin-surface temperature information. For people with no masks or whose temperature is abnormal, you can enable voice alarm for them. The platform provides two types of templates for different application scenarios: People Counting & Temperature Screening template, and Temperature Screening template. You can select a template according to the actual scene and edit the predefined template. After creating the program, you can preview the program, cut in program, etc.

Before You Start

You have added terminal(s) to the platform and have linked a device that supports people counting or temperature screening function with the terminal. For details, refer to ***Add Terminal*** and ***Link External Device to Terminal*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Digital Signage** → **Programs** → **People Counting** .
2. Click **Add**.
3. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

   Screen Size

   Select the screen size as landscape mode or portrait mode.

   Sharing Property

   Public

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

   Private

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

Area

Set the area which the program belongs to.

Description

Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.

4. Click **Next**.
5. Select a template type and the corresponding template as needed.

Note

- You can click ☆ to add the template to My Favorites. Up to 1,000 templates can be added to Favorites.
- You can click ☆ **My Favorites** in the lower-left corner to view and select the template that have been added to Favorites.

6. Click **OK** to enter the creating program page.

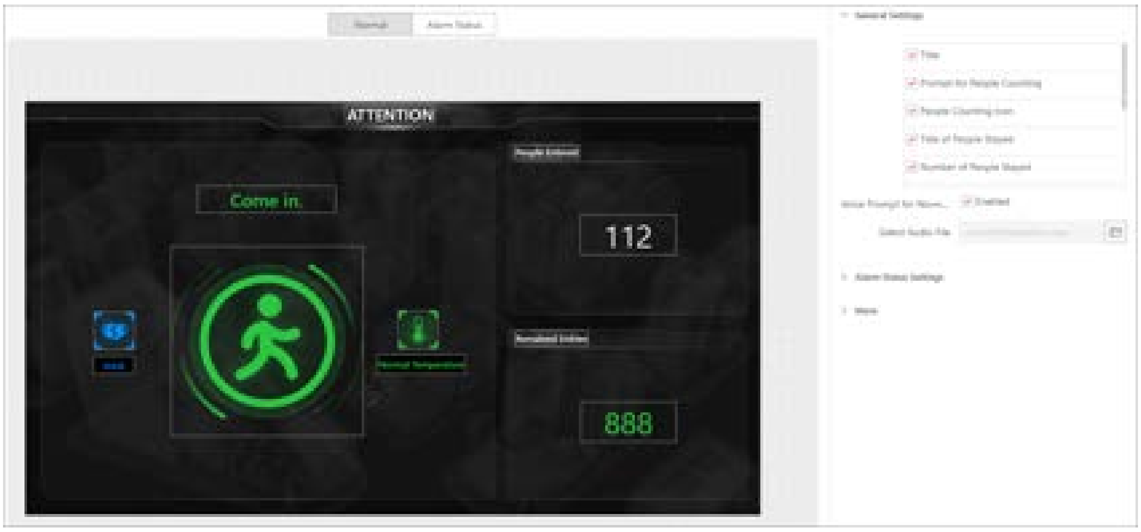


Figure 22-10 Create Program

Normal

The program only contains the people counting related information, such as remaining entry and people stayed.

Alarm Status

The program contains mask information, abnormal temperature information, and people counting related information.

General Settings

You can check whether to display people counting related information, such as prompt for people counting, people counting icon, and the number of people stayed. You can enable audio prompt for normal temperature and select the corresponding audio file. The configurations in this area will be applied to **Normal** and **Alarm Status** simultaneously.

Alarm Status Settings

You can check whether to display alarm status related information, such as prompt for abnormal temperature; set maximum people stayed; enable voice alarm for no mask, abnormal temperature and people full, and configure the corresponding audio file for them.

Advertisement Settings

You can add advertisements (pictures, videos, etc.) to the program, and configure switching effect and playing time for the advertisements.

Note

Only when selecting **People Counting & Temperature Screening Template**, you can configure advertisements.

More

Click 🗀 to set the background picture and the alarm picture for the current program.

Note

Make sure you have added picture materials to the platform and the materials have been approved. For details, refer to ***Material Management*** and ***Approve*** .

7. **Optional:** On the current editing program page, perform the following operations if needed.

Edit Program
Click ✎ to edit program parameters in the pop-up window. For details, refer to Step 3.

Preview Program
Click **Preview** to preview the program.

Figure 22-11 Preview 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.

Cut-In
Click **Cut In** to cut in the current program.

Note

For details, refer to ***Cut in Program*** .

Create Schedule

Click **Next** to enter the managing schedules page and create a schedule for the program.

Note

For details, refer to ***Schedule Management*** .

8. Click **Save** to save the current program.
9. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode

Click ▦ / ☰ to view the added programs in the thumbnail mode or in the list mode.

Add Program to Favorites

Click ☆ to add the current program to Favorites.

Preview Program

Click ● 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 current page in fullscreen.

Copy Program

Click ⧉ 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.

Cut-In

Click ▶ to cut in the current program. For details, refer to ***Cut in Program*** .

Create Schedule

Click ■ to enter the managing schedules page and create a schedule for the program. For details, refer to ***Schedule Management*** .

Enlarge Program Page

Click 🔍 to enlarge the program page and view it.

Filter Program

You can filter programs via the following three methods:

- Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter to filter programs according to whether they have been added to Favorites or not.
- Enter a keyword in the search field on the upper right corner, and click to quickly search for the target programs.
- Click , and filter programs by conditions such as status and sharing property.

Refresh Program List
Click **Refresh** to refresh the program list. The programs will be listed according to the time they were added.

Delete Program
Check one or more programs, and click **Delete** to delete the selected programs.

Note

Programs that are releasing or cutting in cannot be deleted.

22.4 Schedule Management

You can create a schedule and define a playing schedule to play the added programs on the terminals according to the scheduled time or method. The platform supports default schedule, loop schedule, or you can customize your schedule including playing by date or by week. For the added schedules, you can perform more operations such as editing, releasing, searching, exporting, and adding to favorites.

22.4.1 Create a Schedule

You can create schedules for the added programs so that the programs will be played on the terminals according to the scheduled time or method. For the added schedule(s), you can perform more operations such as editing, adding to favorites, exporting, and releasing the schedule.

Before You Start
Make sure you have created programs in the platform. For details, refer to ***Program Management*** .

Steps

1. Enter the Create Schedules page.
   - After creating a program, click **Next**.
   - In the top right corner of the Home page, select → **All Modules** → **Digital Signage** → **Schedules** → **Add** .
2. In the pop-up Create Schedules window, set the related information, and click **OK**.

   Name

   Define a schedule name that is easy to identify.

   Program Type

Select **Other Program** or **Video Wall Program**.

Sharing Property

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.

Area

Set the area which the schedule belongs to.

Description

Enter the schedule description.

3. Select the play mode as **Play by Date**, **Play by Week** or **Custom Play**.

Play by Date/Week

Play the program according to a daily/weekly schedule.

Custom

Customize the schedule within up to 90 days.

4. Select program(s) from the program list and drag to the timeline on the right side.

Note

- You can click **All** or **My Favorites** to display all programs or programs that have been added to favorites.
- You can select **Landscape Mode**, **Portrait Mode**, or **Custom** from the drop-down list to filter programs.
- If you have selected the program type as video wall program in Step 2, you can filter programs by setting the video wall dimension.
- If you have selected the program type as other program in Step 2, you can select programs from the lists of digital signage programs, attendance programs, or people counting programs.
- You can enter keywords in the search box to filter programs.

5. Move the cursor to the timeline, and drag the cursor on the timeline to specify the playing time of the program.

Note

When hovering the cursor on the program's playing time, you can view the thumbnail of the program.

6. **Optional:** Adjust the program schedule.
   - Move the cursor to the program bar on the timeline and drag the right and left edges to adjust the beginning time and end time of the program.
   - Click the program bar on the timeline, and adjust the beginning time and end time of the program in the input box.

- Click to copy the program to other time periods.
- Click to delete the program in this time period.

7. Click **Save** to save the current schedule.
8. **Optional:** Click **Release** to enter the release page.

Note

For details, refer to ***Release a Program Schedule*** .

9. **Optional:** After creating schedules, perform the following operations as needed.

Edit Schedule

Click the name of the schedule and then click to enter Arrange Schedule page and you can edit the schedule information.

Delete Schedule

Select one or more schedules, click **Delete** to delete the selected schedules.

Release Schedule

Click to release the selected schedule. For details, refer to ***Release a Program Schedule*** .

Export Schedule

Click to export the schedule.

Add to Favorites/ Cancel

Click ☆ or ★ to add the schedule to favorites or move it from favorites.

Note

You can add up to 1,000 schedules to favorites.

Refresh Schedule

Click **Refresh** to refresh the schedule list.

Search Schedule

You can search the added schedules via the three methods.

- Enter a keyword on the upper right corner of the page, and click to quickly find the target schedules.
- Click on the upper right corner of the page, and set the search conditions such as status and sharing property to quickly filter the target schedules.
- Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter the schedules.

22.4.2 Create a Loop Schedule

You can create a loop schedule for the added programs. With loop schedule configured, the added programs will be played repeatedly according to the play mode, including normal mode and period mode. You can add multiple playlists to meet different requirements.

Before You Start

Make sure you have created programs on the platform. For details, refer to ***Program Management*** .

Steps

1. Enter the Create Schedules page.
   - After creating a program, click **Next**.
   - In the top right corner of the Home page, select → **All Modules → Digital Signage → Schedules → Add** .
2. In the pop-up Create Schedules window, set the related information, and click **OK**.

   Name

   Define a schedule name that is easy to identify.

   Program Type

   Select **Other Program** or **Video Wall Program**.

   Sharing Property

   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.

   Area

   Set the area which the schedule belongs to.

   Description

   Enter the schedule description.
3. Select the play mode as **Play in Loop**.
4. Select a program in the program list and drag the program to the playlist.

   Note

   - You can click **All** or **My Favorites** to display all programs or programs that have been added to favorites.
   - You can select **Landscape Mode**, **Portrait Mode**, or **Custom** from the drop-down list to display corresponding programs.
   - If you have selected the program type as video wall program in Step 2, you can filter programs by setting the video wall dimension.
   - If you have selected the program type as other program in Step 2, you can select programs from the lists of digital signage programs, attendance programs, or people counting programs.
   - You can enter keywords in the search box to filter programs.
   - You can add up to 8 programs to a single playlist.
5. Set the play mode.

   Normal Mode

   Play the program orderly and repeatedly.

   Period Mode

Play the programs orderly and repeatedly in specific time period. The time periods for different playlists cannot be overlapped.

Note

The priority of Period Mode is higher than that of Normal Mode. Only one playlist can be set to normal mode.

6. **Optional:** Click **Add Playlist** to add more playlists.

Note

You can add up to 8 playlists.

7. Click **Save** to save the current schedule.
8. **Optional:** Click **Release** to enter the release page.

Note

For details, refer to ***Release a Program Schedule*** .

9. **Optional:** After creating schedules, perform the following operations as needed.

Edit Schedule	Click the name of the schedule and then click ✎ to enter Arrange Schedule page and you can edit the schedule information.
Delete Schedule	Select one or more schedules, click **Delete** to delete the selected schedules.
Release Schedule	Click ◁ to release the selected schedule. For details, refer to ***Release a Program Schedule*** .
Export Schedule	Click ⇥ to export the schedule.
Add to Favorites/ Cancel	Click ☆ or ★ to add the schedule to favorites or move it from favorites. **Note** You can add up to 1,000 schedules to favorites.
Refresh Schedule	Click **Refresh** to refresh the schedule list.
Search Schedule	You can search the added schedules via the three methods. • Enter a keyword on the upper right corner of the page, and click 🔍 to quickly find the target schedules. • Click ▽ on the upper right corner of the page, and set the search conditions such as such as status and sharing property to quickly filter the target schedules. • Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter the schedules.

22.4.3 Create a Default Schedule

With the default schedule enabled, the terminal will play the default video automatically if there is no program or cut-in. After creating a default schedule, you can perform more operations such as editing, adding to favorites, exporting, and releasing the schedule.

Before You Start

Make sure you have created programs in the platform. For details, refer to ***Program Management*** .

Steps

1. Enter the Create Schedules page.
   - After creating a program, click **Next**.
   - In the top right corner of the Home page, select ▦ **→ All Modules → Digital Signage → Schedules → Add** .
2. In the pop-up Create Schedules window, set the related information, and click **OK**.

   Name

   Define a schedule name that is easy to identify.

   Program Type

   Select **Other Program** or **Video Wall Program**.

   Sharing Property

   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.

   Area

   Set the area which the schedule belongs to.

   Description

   Enter the schedule description.
3. Select the play mode as **By Default**.
4. Select a program in the program list, and drag the program to the right.

Note

- You can click **All** or **My Favorites** to display all programs or programs that have been added to favorites.
- You can select **Landscape Mode**, **Portrait Mode**, or **Custom** from the drop-down list.
- If you have selected the program type as video wall program in Step 2, you can filter programs by setting the video wall dimension.

- If you have selected the program type as other program in Step 2, you can select programs from the lists of digital signage programs, attendance programs, or people counting programs.
- You can enter keywords in the search box to filter programs.

5. Click **Save** to save the current schedule.
6. **Optional:** Click **Release** to enter the release page.

Note

For details, refer to ***Release a Program Schedule*** .

7. **Optional:** After creating schedules, perform the following operations as needed.

Edit Schedule
Click the name of the schedule and then click ✎ to enter Arrange Schedule page and you can edit the schedule information.

Delete Schedule
Select one or more schedules, click **Delete** to delete the selected schedules.

Release Schedule
Click ◁ to release the selected schedule. For details, refer to ***Release a Program Schedule*** .

Export Schedule
Click ⇨ to export the schedule for offline view.

Add to Favorites/ Cancel
Click ☆ or ★ to add the schedule to favorites or move it from favorites.

Note

You can add up to 1,000 schedules to favorites.

Refresh Schedule
Click **Refresh** to refresh the schedule list.

Search Schedule
You can search the added schedules via the three methods.

- Enter a keyword on the upper right corner of the page, and click 🔍 to quickly find the target schedules.
- Click ▽ on the upper right corner of the page, and set the search conditions such as status and sharing property to quickly filter the target schedules.
- Select **All**, **Added to Favorites**, or **Not Added to Favorites** from the drop-down list on the upper side of the page to filter the schedules.

22.5 Approve

The added materials, programs and schedules should be approved before they are used.

Note

Only users with the permission to approve materials, programs and schedules can approve the related contents.

In the top left corner of Home page, select 🟥 → **All Modules** → **Digital Signage** → **Approval** .

Select the content to be approved, including **Material**, **Program**, and **Schedule**, select the approval result, and give suggestions.

- **Approve One by One:** In the **Operation** column, click ✓ to pass the approval; click ⊗ to deny the approval.
- **Batch Approval:** Check multiple materials, programs or schedules, click **Pass** to pass the approval; click **Deny** to deny the approval.

Note

- You can enter up to 128 characters for the approval suggestions.
- There are three types of check status: **Passed**, **Denied**, and **To be Checked**. When the check status of a material is changed from Passed to Denied, the status of its related programs and schedules is changed into To be Checked.

22.6 Release Management

You can view the release details and release progress of multiple tasks (such as schedule releasing and cutting in program). After being released, the above tasks can take effect on the terminals.

22.6.1 View Release Records

You can view release records of all the tasks (such as releasing schedules and cut-in text messages) and the details of their release status.

Click ▦ → **All Modules** → **Digital Signage** → **Release** . You can view release details of all the tasks in the platform, including task name and type, release time and status (Released or Failed), etc. Also, you can perform more of the following operations.

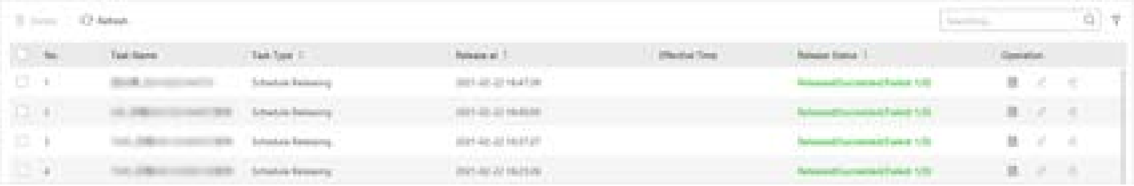


Figure 22-12 View Release Records

- **View Release Details**: click ▫ to view release status details of each task, including terminal device, release progress, and status.

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.
- When there are multiple pieces of release status, you can enter a keyword in the search box to search for the target release status.

- **Release Schedule**: For unreleased schedules, click to enter releasing schedules page. For details, refer to ***Release a Program Schedule*** .
- **Delete Task**: Click to delete single release task; Check multiple tasks, and click **Delete** to batch delete the selected tasks.
- **Release Again**: For a task that failed to be released, you can click to release the task again.

22.6.2 Release a Program Schedule

For the approved program schedule, you should release the schedule to the terminals. When releasing a schedule, you can set the release mode, effective mode, and the terminal(s). The program will then be played according to the configured method on the terminals.

Before You Start

- You have added terminals to the platform. For details, please refer to ***Add Terminal*** .
- The program schedules to be released should have been approved. For details, refer to ***Approve*** .

Steps

1. Enter the releasing schedule page.
   - After creating the programs, click **Next**. For details about creating programs, refer to ***Program Management*** .
   - Select → **All Modules** → **Digital Signage** → **Programs** , select a program type, move the cursor to a program, click to enter the adding schedules page, and click **Release** on the upper right corner.
   - Select → **All Modules** → **Digital Signage** → **Schedules** to enter managing schedules page, and click .
2. Enter the task name.
3. 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.

4. Select the effective mode as **Take Effect Immediately** or **Take Effect Later**.

Note

When selecting **Take Effect Later**, you should set the effective time. Only after the program takes effect, it can be played on the terminal.

5. Select an area, and check one or more devices in the selected area.

Note

You can enter a keyword in the search box to quickly find the target area or device.

6. Click **OK**.

22.6.3 Cut in Text Message

You can cut in text message(s) for one or more terminals. When configuring cut-in text message(s), you can set the playing time, location, etc., of the text message and preview the displaying effects of them in the platform. The terminals will play the cut-in text message according to the configured time and method.

Before You Start

You have added terminal(s) to the platform. For details, refer to ***Add Terminal*** .

Steps

1. In the top left corner of Home page, select → **All Modules** → **Digital Signage** → **Device Control** → **Digital Signage Control** .
2. Check one or more online devices in the list.

Note

You can enter a keyword in the search box on the upper right corner to quickly find the target device(s).

3. Click **Cut In Message** to enter the Cut In Message page.
4. Enter the customized task name.
5. In **Edit Text Message** area, enter the text content and the corresponding play time.

Note

- The playing time for different cut-in text messages can be overlapped.
- You can click in the Operation column to view the playing effect of the current text message on the right side of the page.

6. In **Text Message Property** area, set the configuration mode, front size and color, background, etc., for the text message.
7. Click **Cut-in**.

Note

Cut-in text messages do not need to be approved.

22.6.4 Cut in Program

You can cut in a program when creating or managing programs in the platform. The cut-in program will precede other programs and play on the terminal in the configured method.

Before You Start

- Make sure you have added terminal(s) to the platform. For details, please refer to ***Add Terminal*** .
- The program schedules to be released should have been approved. For details, refer to ***Approve*** .

Steps

1. Enter Cut-in Program page.
   - Select 🟥 → **All Modules** → **Digital Signage Management** → **Programs** , select a program type, move the cursor to a program, and click ▶ .
   - After creating a program, click **Cut-in** on the upper right corner of the page.
2. Enter the task name.
3. Select the cut-in mode as **Play Duration (h/m/s)** or **End Time**.
4. Select one or more terminals for the cut-in programs.

   Note

   You can enter a keyword in the search box to quickly find the target device(s).
5. Click **OK**.

22.7 Digital Signage Overview

You can have an overview of the functions about digital signage and statistics for materials, programs, etc.

In the top left corner of Home page, select 🟥 → **All Modules** → **Digital Signage** → **Digital Signage Overview** .

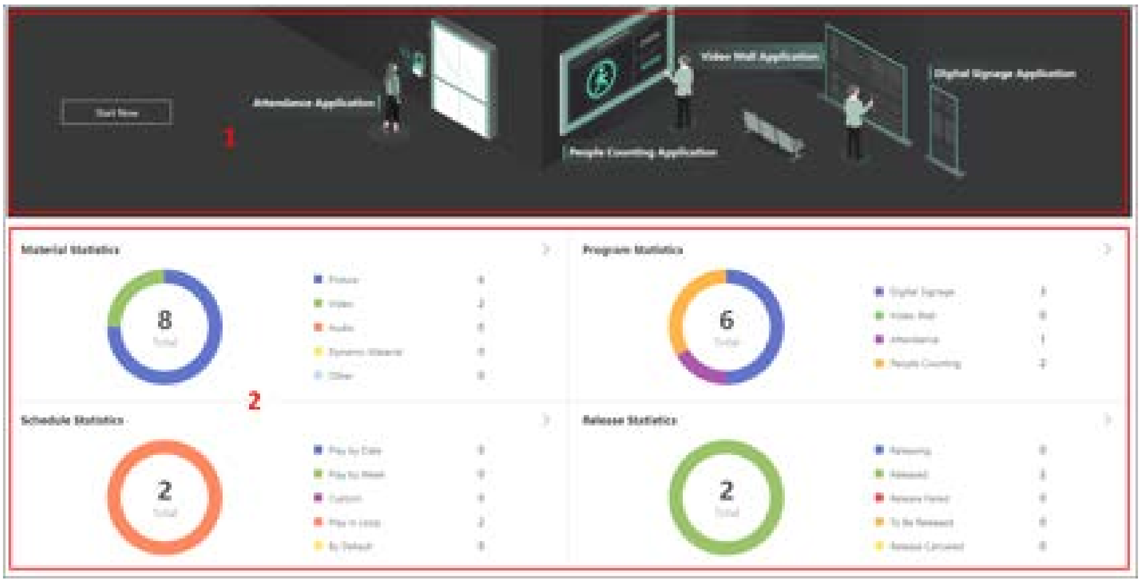


Figure 22-13 Digital Signage Overview

Table 22-4 Home Page Description

Number	Description
1	Displays different applications of the digital signage module, including attendance application, people counting application, etc. Click **Start Now** to pop up the Digital Signage Wizard on the right side of the page, and you can use the digital signage function according to the wizard.
2	An overview of resources added to the platform, including material statistics, program statistics, schedule statistics, and release statistics. • **Material Statistics**: Displays the total number and the types of the added materials, as well as the corresponding number and proportion of each type of materials. • **Program Statistics**: Displays the total number and the types of the created programs, as well as the corresponding number and proportion of each type of programs. • **Schedule Statistics**: Displays the total number and the types of the schedules as well as the corresponding number and proportion of each type of schedules. • **Release Statistics**: Displays different releasing status such as Releasing, Released and Releasing Failed, and their corresponding number and proportion.

22.8 Device Control

After adding terminals to the platform or configuring video walls on the platform, you can control the terminals or video walls, such as starting up, shutting down, playing programs, setting the volume, etc.

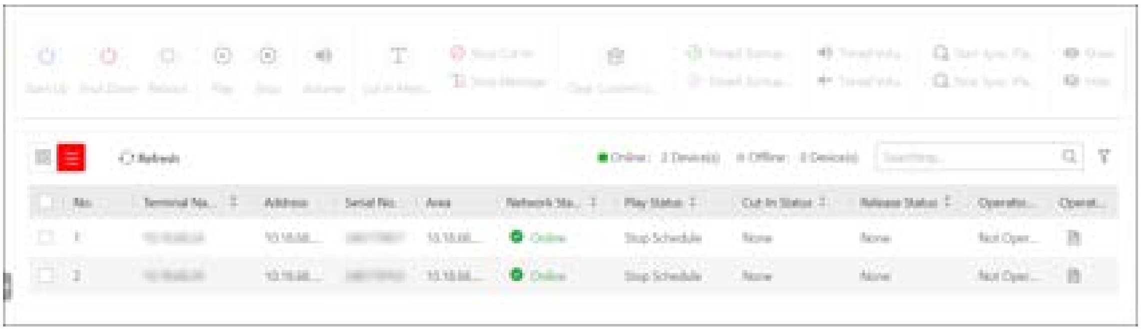
22.8.1 Control Terminal

After adding terminals to the platform, you can control the terminals on the platform, such as starting up, shutting down, playing programs, setting the volume, etc.

Note

Make sure you have added terminals to the platform. See details in ***Add Terminal*** .

In the top left corner of Home page, select ▦ → **All Modules** → **Digital Signage** → **Device Control** → **Digital Signage Control** .



□	No.	Terminal Na...	Address	Serial No.	Area	Network Sta...	Play Status	Cut-In Status	Release Status	Operatio...	Operat...
□	1	[illegible]	10.16.6…	[illegible]	10.16.6…	● Online	Stop Schedule	None	None	Not Oper...	
□	2	[illegible]	10.16.6…	[illegible]	10.16.6…	● Online	Stop Schedule	None	None	Not Oper...	

Figure 22-14 Digital Signage Control

Perform the following operations as needed.

Functions	Operations
Switch Display Mode	Click ▦ / ☰ to display the added terminals in thumbnail/list mode.
Refresh Terminal List	Click **Refresh** to refresh the terminal list.

Functions	Operations
View Terminal Details	Click in the Operation column to view the details of the terminal, such as software version, system version, IP address, MAC address, CPU usage, HDD usage, etc.
Search Terminals	• Click , set the search conditions (such as network status, cut-in status, release status, playback status) and click **Search** to search for the target terminals. • Enter a keyword in the search box to search for the target terminals.

Select one or multiple devices and perform the following operations as needed.

Start UP / Shut Down / Reboot

Remotely start up/shut down/reboot the terminal(s).

Play/Stop

Play/stop the programs on the screen of the terminal(s).

Set Volume

Set the output volume of the terminal.

Cut in Message

Go to the Cut in Message page to customize the cut-in messages displayed on the screen of the terminal(s).

Stop Cut-In/Stop Message

Stop cutting in programs. / Stop cutting in messages.

Clear Content on Terminal

Clear all the contents to be played on the terminal(s), including programs, cut-in programs/ message, etc.

Timed Startup/Shutdown Enabled
Timed Startup/Shutdown Disabled

Enable/Disable start up/shut down terminal(s) according to the schedule.

Note

For details about timed start up/shut down, refer to ***Configure Device Display Settings*** .

Timed Volume On
Timed Volume Off

Turn on/off the volume of the terminal(s) based on the schedule you set.

Note

For details about timed volume on/off, refer to ***Configure Device Display Settings*** .

Start Sync. Playing on Terminal
Stop Sync. Playing on Terminal

Start or stop synchronous playing on terminals.

Show/Hide

Show or hide the release progress.

Valid Default Schedule/Invalid Default Schedule

If you create default video schedule for the terminal(s), you can manually control the schedule valid or invalid.

Note

For details about creating default video schedule, refer to ***Create a Default Schedule*** .

Screenshot

Generate the screenshot(s) of the terminal(s), which is/are in JPG format.

NTP Time Sync.

The time synchronization of NTP server should be enabled when starting synchronous playing on the terminals. See details in ***Set NTP*** .

Restore Default

Restore the parameters of the terminal(s) to the default settings.

Remote Debugging

Enable the Android debug bridge for the terminal(s), and enter the debugging contents.

Log Export

Export the logs of the terminal(s) in ZIP format.

22.8.2 Control Video Wall

You can control the video walls after adding them to the platform.

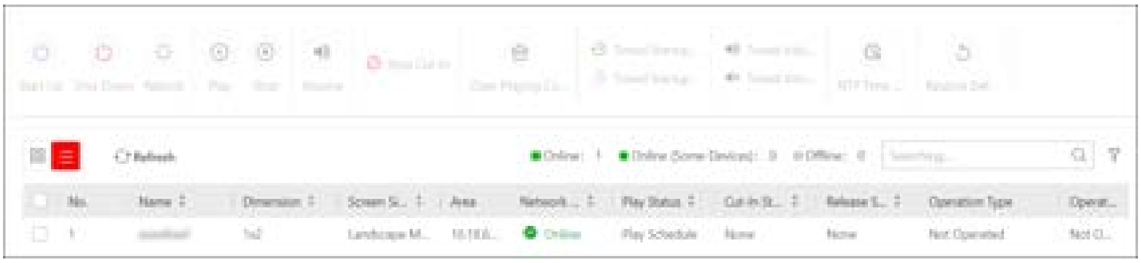
Before You Start
Make sure you have added video walls. See details in ***Configure Video Wall*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Digital Signage** → **Device Control** → **Video Wall Control** .

Note

The multiple terminals that constitute the video wall should be controlled as a whole, or the playing status of different terminals will not be the same.



	No.	Name	Dimension	Screen S...	Area	Network ...	Play Status	Cut-in St...	Release S...	Operation Type	Operat...
□	1	[illegible]	1x2	Landscape M...	10.18.6...	Online	Play Schedule	None	None	Not Operated	Not Cl...

Figure 22-15 Video Wall Control

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

Switch Display Mode
Click ▦ / ☰ to display the added video walls in thumbnail/list mode.

Refresh Video Wall List
Click **Refresh** to refresh the video wall list.

Search Video Walls
- Click ▽ , set the search conditions (dimension, screen type, network status, play status, cut-in status, release status) and click **Search** to search for the target video walls.
- Enter a keyword in the search box to search for the target video walls.

3. **Optional:** Select one or multiple video walls and perform the following operations.

Start UP / Shut Down / Reboot
Remotely start up, shut down, or reboot the video walls.

Play/Stop
Play or stop the programs or cut-in messages on the video walls.

Volume
Set the volume of the video walls.

Stop Cut-In
Stop cutting in programs.

Clear Playing Content
Clear all contents to be played on the video walls.

Timed Startup/ Shutdown Enabled

Timed Startup/ Shutdown Disabled
Enable or disable startup/shutdown according to the schedule.

Note

For details about timed startup/shutdown, see details in ***Configure Device Display Settings*** .

Timed Volume On

Timed Volume Off
Turn on/off the volume of the video walls based on the configured schedule.

	Note For details about timed volume on/off, see details in ***Configure Device Display Settings*** .
NTP Time Sync.	The time synchronization of NTP server should be enabled when starting synchronous playing on the terminals. See details in ***Set NTP*** .
Restore Default	Restore the parameters of the terminals to the default settings.

22.9 Set Material Storage Location

The materials uploaded can be saved to the local storage or pStor server.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Digital Signage** → **Basic Settings** → **Material Storage Location** .
2. Select a storage location from the drop-down list.

   Note

   To select **pStor** as the storage location, make sure you have added pStor servers to the platform. For details, refer to ***Add pStor*** .
3. Click **Save** to save the above settings.

22.10 Configure 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 Terminal*** and ***Set NTP*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Digital Signage** → **Basic Settings** → **Video Wall Configuration** .
2. Click **Add**.

Figure 22-16 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 descriptions 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 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.

Set Video Wall Display Parameters	Select one or multiple added video walls, click **Video Wall Display Control** to set the display parameters.
Refresh Video Wall List	Click **Refresh** to refresh the video wall list.
Search Video Walls	• Click ▽ , set the search conditions (video wall dimension and screen type), and click **Search** to search for the target video walls. • Enter a keyword in the search box to search for the target video walls.

Chapter 23 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.

23.1 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. In the top left corner of the Home page, select 🟥 → **All Modules** → **Speaker Unit** → **Basic Settings** .
2. In Audio File area, select **Local Storage** or **pStor** as the location to save the audio file, and select the corresponding storage pool.

   Note

   When selecting pStor as the storage location, make sure you have added pStor to the platform. For details, refer to ***Add pStor*** .
3. In Live Broadcast Recording area, check **Live Broadcast Recording**.
4. Select **Local Storage** or **pStor** as the location to save the recording file, and select the corresponding storage pool.

   Note

   When selecting pStor as the storage location, make sure you have added pStor to the platform. For details, refer to ***Add pStor*** .
5. 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 Connection

   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.

6. Click **Save** to save the above settings.

23.2 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. In the top left corner of the Home page, select → **All Modules** → **Speaker Unit** → **Speaker Unit Group** .
2. Create a speaker unit group.
   1) Click .
   2) Enter the name for the group.
   3) Click **Add**.
3. 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**.
4. **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 and/or alarm-triggered broadcast for the selected devices.

Note

For Hikvision devices, you can only adjust the volume of live broadcast.

23.3 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. In the top left corner of the Home page, select → **All Modules** → **Speaker Unit** → **Media Library** .

2. 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.
3. Click **Add**.
4. 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.
5. Click **Upload**.

   Note

   You can view the uploading progress and results.

   The uploaded media file(s) are displayed in the list.
6. **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.

23.4 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). Refer to ***Add Speaker Unit to Area for Current Site*** for details.
- Make sure you have added media file(s) to the media library. Refer to ***Manage Media Files*** for details.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **Speaker Unit** → **Live Broadcast and Recording** .
2. Select **Live Broadcast**.
3. Select the online speaker unit(s) for live broadcast.
   - Check **Group**, and select one or more speaker units from speaker unit group(s).

     Note

     You can click **Display Not Grouped** to display the speaker unit(s) that are not grouped.
   - Check **Area**, and select one or more speaker units from the area(s) where the speaker units are added.

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 will broadcast fluently and correctly.

5. Click **Start**.

What to do next

Speak to the PC microphone or play the audio file.

23.5 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. In the top left corner of the Home page, select ■ → **All Modules** → **Speaker Unit** → **Live Broadcast and Recording** .
2. Set the start time.
3. Set the end time.
4. Select a broadcaster from the drop-down list.
5. 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, and the file size.
6. **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.

23.6 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). Refer to ***Add Speaker Unit to Area for Current Site*** for details.

Steps

1. In the top left corner of the Home page, select 🟥 → **All Modules** → **Speaker Unit** → **Scheduled Broadcast** .
2. Click **Add** to enter Add Scheduled Broadcast page.
3. Enter the name for the scheduled broadcast task.
4. Select the speaker unit(s) to execute the task.
   - Check **Group**, and select one or more speaker units from speaker unit group(s).
   - Check **Area**, and select one or more speaker units from the area(s) where the speaker units are added.
5. Configure the Period Type.
   - When selecting **Every Day**, you should set the start date and end date.
   - When selecting **One Time**, you should set the start time.
   - When selecting **Every Week**, you should set the start date, end date, and the repetition day of the week.
6. Configure the Broadcast Time.
7. 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.
8. 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*** .
9. Set **Once** or **Specified Duration** as the Play Mode.

   Note

   When selecting **Specified Duration**, you should configure the time duration for playing media file(s).
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, play mode, the number of speaker units, etc.

Note

You can click to view the names of speaker unit(s) and the media file(s).

Play / Stop Audio

- Click **Listen** 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.

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 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**.

   Match Detected Package with Face(s) Captured Within (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 behavior type(s) for behavior analysis, and the alarm type(s) for metal detection.

24.2 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. Select an area from the area list.
3. Click **Add** to enter the Add Security Inspection Channel page.
4. Enter the channel name and description.

5. **Optional:** In the Linkage 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. Click **Add**.

24.3 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

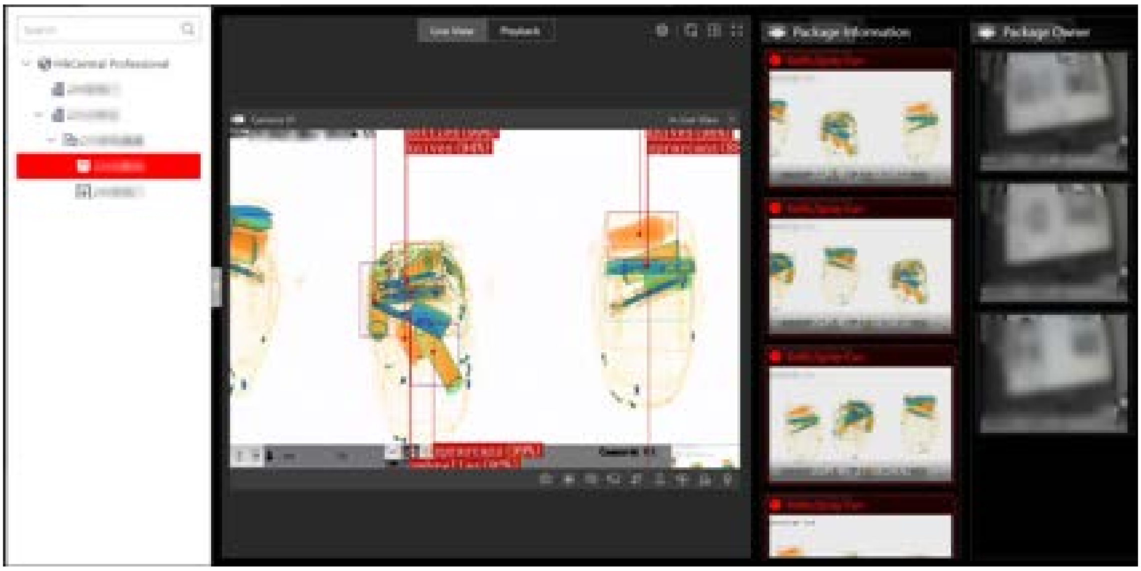


Figure 24-1 Live View

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.

Icon	Function	Description
	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

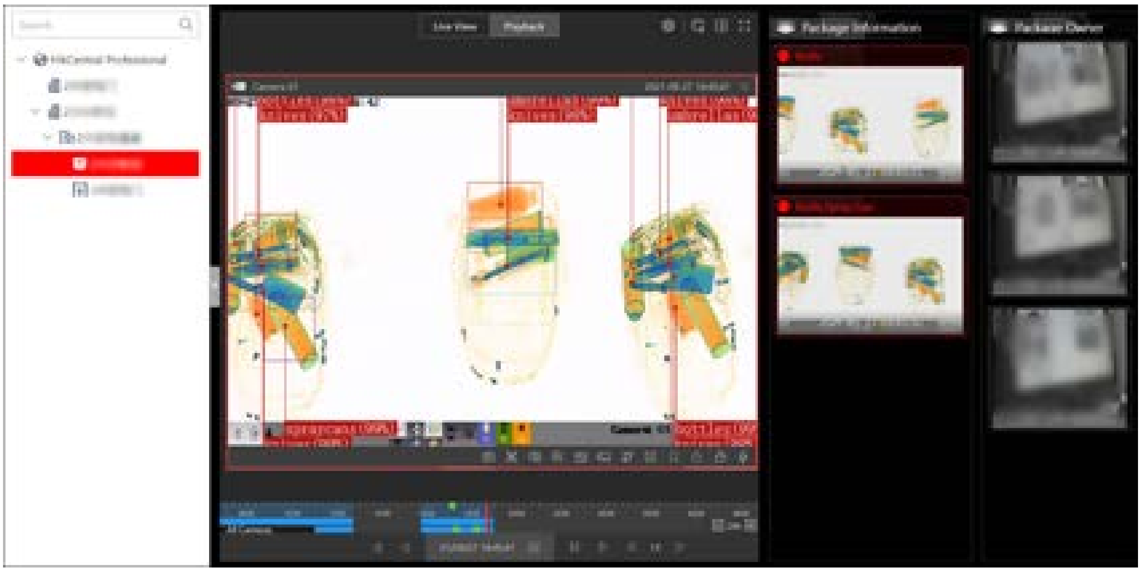


Figure 24-2 Playback

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.

Icon	Function	Description
	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.

24.4 Historical Data Search

You can search for the historical data of security inspection, including package detection records, metal detection records, and inspector absence records.

24.4.1 Search for Package Detection Records

You can set search conditions, including time, article type, and location, to search for the package detection records.

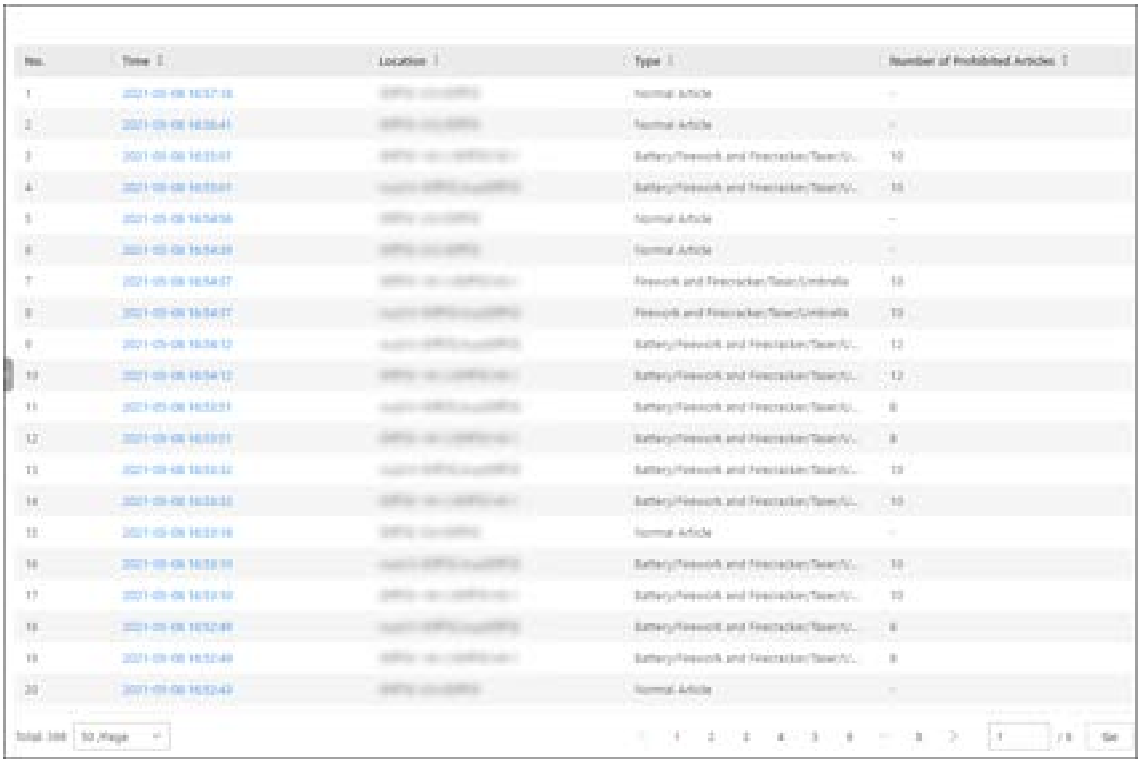
Steps

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	[illegible]	[illegible]	Normal Article	--
2	[illegible]	[illegible]	Normal Article	--
3	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
4	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
5	[illegible]	[illegible]	Normal Article	--
6	[illegible]	[illegible]	Normal Article	--
7	[illegible]	[illegible]	Firework and Firecracker/Taser/Umbrella	10
8	[illegible]	[illegible]	Firework and Firecracker/Taser/Umbrella	10
9	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	12
10	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	12
11	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	8
12	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	8
13	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
14	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
15	[illegible]	[illegible]	Normal Article	--
16	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
17	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	10
18	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	8
19	[illegible]	[illegible]	Battery/Firework and Firecracker/Taser/U...	8
20	[illegible]	[illegible]	Normal Article	--

Figure 24-3 Search for Package Detection Records

24.4.2 Search for Metal Detection Records

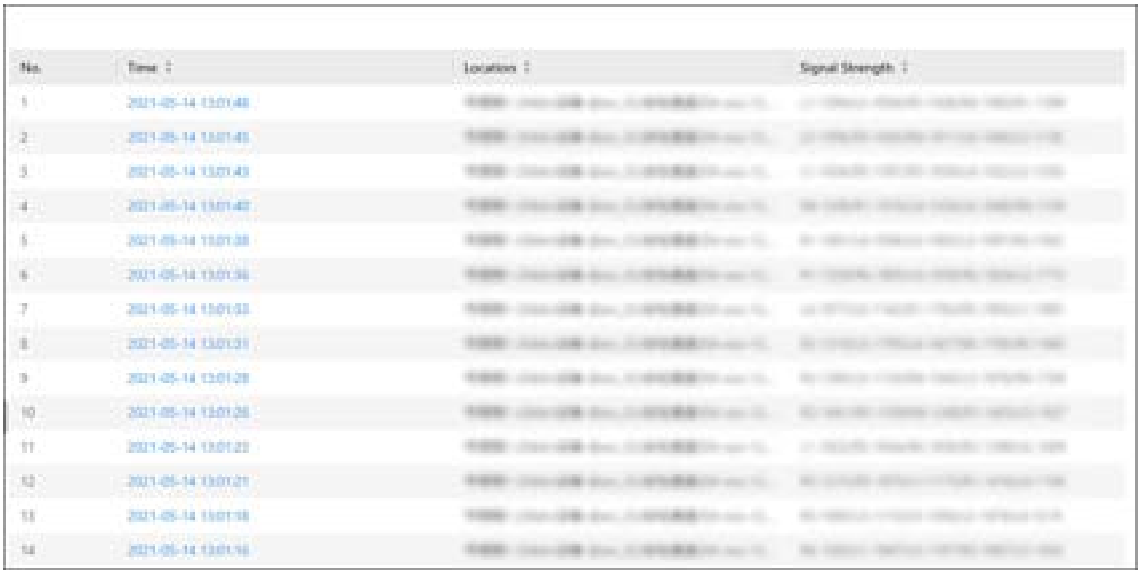
You can set the search conditions, including time and location, to search for the metal detection records.

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 24-4 Search for Metal Detection Records

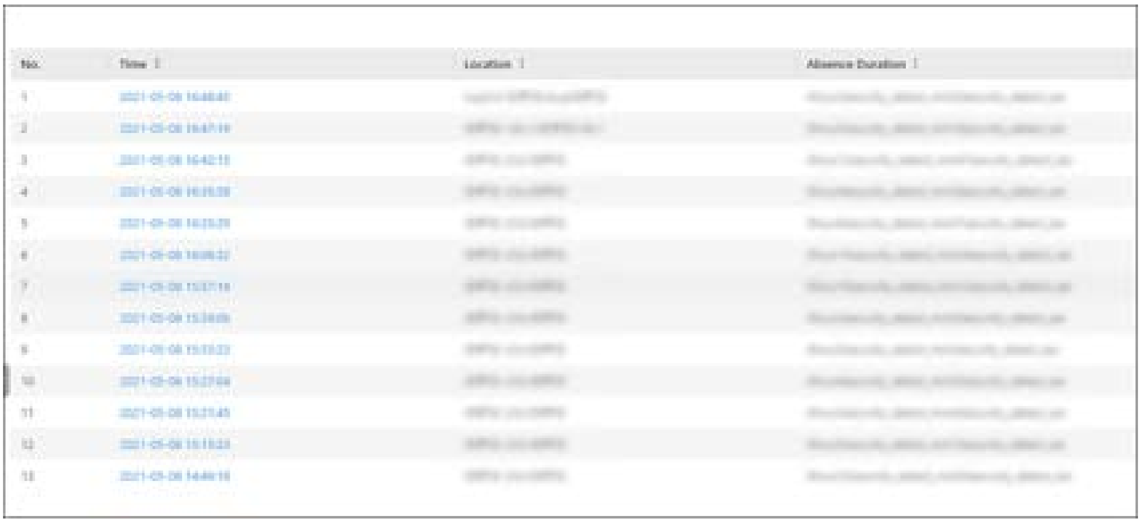
24.4.3 Search for Absence Records

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 16:48:40	[illegible]	[illegible]
2	2021-05-08 16:47:19	[illegible]	[illegible]
3	2021-05-08 16:42:15	[illegible]	[illegible]
4	2021-05-08 16:26:38	[illegible]	[illegible]
5	2021-05-08 16:23:29	[illegible]	[illegible]
6	2021-05-08 16:08:32	[illegible]	[illegible]
7	2021-05-08 15:37:16	[illegible]	[illegible]
8	2021-05-08 15:34:06	[illegible]	[illegible]
9	2021-05-08 15:33:23	[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 14:44:16	[illegible]	[illegible]

Figure 24-5 Search for Absence Records

24.5 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.

24.6 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 Alarm Detection

A security control device detects people, vehicles, etc., entering a predefined region, triggers events and alarms, and reports events/alarms information (such as location) to security personnel.

On the Web Client, after adding a security control device to the system, the administrator needs to group the device's alarm inputs into security control partitions in the system. You also need to set one arming schedule for the alarm inputs in a security control partition which defines when and how to arm the alarm inputs in this security control partition.

For example, area 1 is created for the first floor, and all the resources on the first floor are managed in area 1. If there is one security control device mounted on the first floor, you should add its zones (alarm inputs) into area 1 first, then link the zones into security control partitions and set an arming schedule to these security control partitions. After that, the zones can be armed according to the schedules respectively.

25.1 Flow Chart of Alarm Detection

The following flow chart shows the process of the configurations and operations of alarm detection.

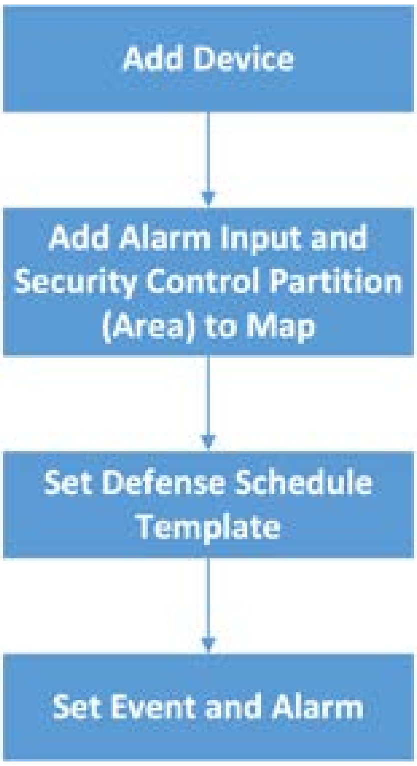

Add Device
Add Alarm Input and Security Control Partition (Area) to Map
Set Defense Schedule Template
Set Event and Alarm

Figure 25-1 Flow Chart of Alarm Detection

- **Add Device**: Add security control devices to detect persons, vehicles, or other emergency events in the detection region to trigger alarms and then notify the security personnel of alarm information. And then, add alarm inputs and partitions (areas) to areas for management. Refer to ***Manage Security Control Device*** , ***Add Alarm Input to Area*** , and ***Add Security Control Partitions (Area) from Device*** for details.
- **Add to Map**: Add alarm inputs and partitions (areas) on map to view their geographic locations, arm or disarm zones, bypass zones, and clear alarms. Refer to ***Add Hot Spot on Map*** for details.
- **Set 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.
- **Event and Alarm**: Set event and alarm parameters and linkage actions to view event and alarm details on the Client or Mobile Client, timely remind the security personnel to handle related issues, or search history events and alarms when an emergency occurs. Refer to ***Event and Alarm Configuration*** for details.

25.2 Add Security Control Partitions (Area) from Device

HikCentral Professional provides areas to manage the added resources in different groups. You can group the resources into different areas according to the locations of the resources. After adding security control devices to the platform, you need to import the partitions (area) configured on the devices to different areas as well as group the alarm inputs (zones) in the partitions (area) into different areas for further operations.

Steps

1. In the upper-left corner of the Home page, select 🟥 → **All Modules → Alarm Detection → Security Control Partition (Area)** .
2. Select an area and 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** if you want to add the alarm inputs (zones) in the selected partitions (areas) to the area.

   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 Security Control Partition (Area) list.
6. **Optional:** Perform one or more of the following operations after adding the security control partitions (areas) to the area.

   Edit Security Control
   Click the name of a partition (area) to display the partition (area) details and then edit its name, partition No., or set the arming schedule for it (see details in ***Configure Arming Schedule Template***).

Partition (Area)

Note

For the partition (area) of AX security control panel, you cannot edit the arming schedule via the platform. Only editing on the device is supported.

Delete Security Control Partitions (Areas)

Select one or multiple partitions (areas) and click **Delete**.

Bypass Zone

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. To bypass the zone, click ⌄ to expand the partition (area) details, and click in the Operation column of the Alarm Input list to bypass the alarm input.

When you want to recover the zone that is bypassed to make it work normally, click in the Operation column to recover it.

Arm or 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**: When all people in the detection area leave, turn on the Away mode to arm all 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**: It is used after people leave the detection area. The zone will be armed immediately without delay.

In the Security Control Partition (Area) list, select the partitions (areas) and click these buttons to arm the partitions (areas), or click **Disarm** to disarm them.

Clear Alarms

Select one or multiple partitions (areas) and click **Clear Alarms** to clear the generated alarms.

Add Partition (Area) on Map

Select a partition (area) and click **Set Geographic Location** to add it on the map. See details in ***Add Hot Spot on Map*** .

25.3 Configure Arming Schedule Template

The arming schedule defines the arming mode in different periods for the partitions of the added security control devices. You can set a weekly schedule to specify periods for arming in Instant mode, arming in Away mode, or arming in Stay mode. The system predefines two default arming schedule templates: All-Day Template and Weekday Template. You can also add a customized template as needed.

Steps

1. In the upper-left corner of the Home page, select 🟥 → **All Modules** → **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 a defined 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 Arming

   It is used after people leave the detection area. The zone will be armed immediately without delay.

   Away Arming

   When all people in the detection area leave, turn on the Away mode to arm all zones in the area after the defined dwell time.

   Stay Arming

   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.
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 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 (such as 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.

26.1 Flow Chart of Video Intercom

For the first time, you can follow the flow chart to perform configurations and operations.

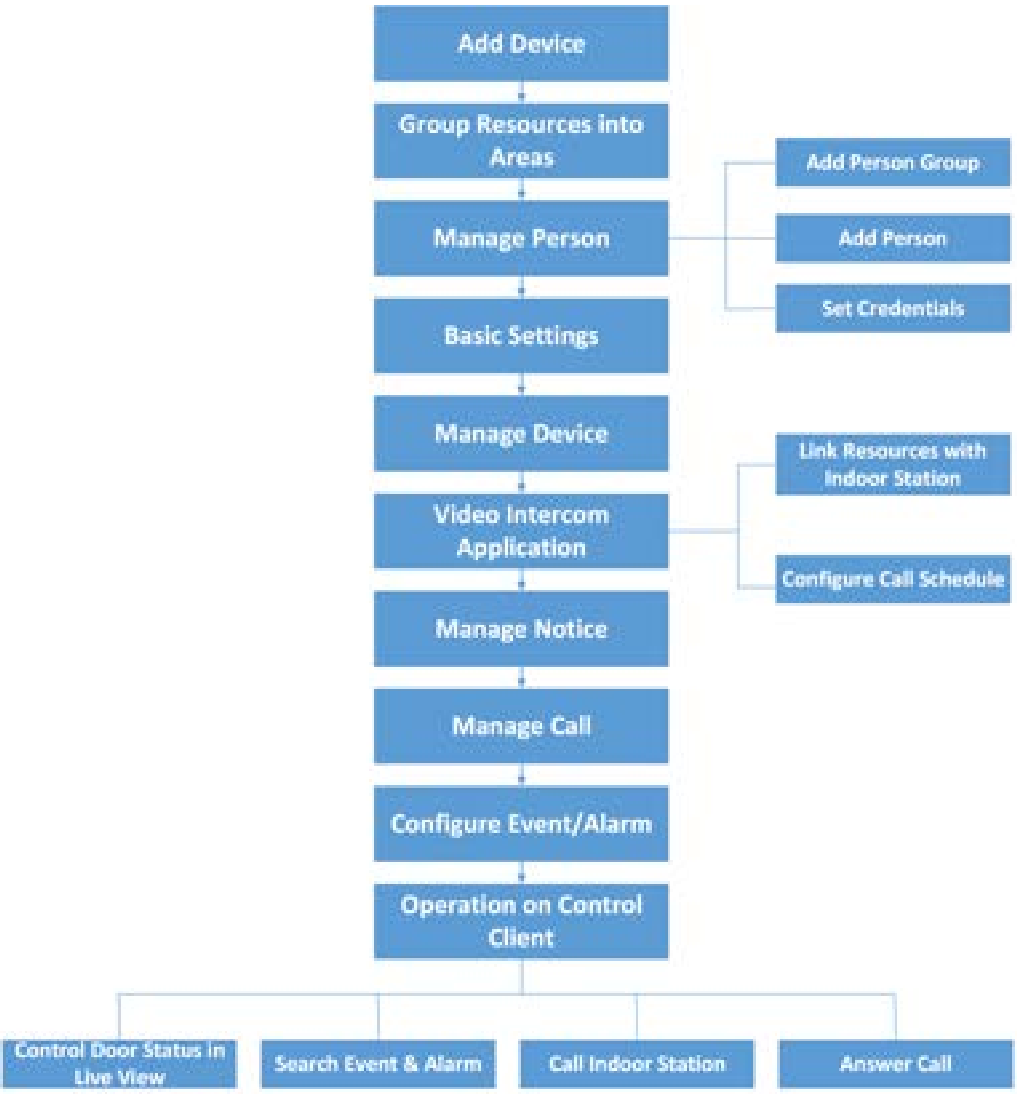


Figure 26-1 Flow Chart of Video Intercom

- **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 and cameras) into different areas according to the resources' locations. For details, refer to ***Area Management*** .
- **Manage Person**: Add person group and person to the system, and set credential information. For details, refer to ***Person Management*** .
- **Basic Settings**: Add call recipients and call schedule templates, and configure call parameters. For details, refer to ***Basic Settings of the Platform*** .
- **Manage Device**: Set location information for video intercom devices and apply the settings to devices. For details, refer to ***Manage Video Intercom Device*** .

- **Video Intercom Application**: Add call schedules and apply them to devices, link resources (camera, person, and doorbell) to indoor stations. For details, refer to ***Video Intercom Application*** .
- **Manage Notice**: Add notices and apply them to indoor stations. For details, refer to ***Manage Notices*** .
- **Manage Call**: Call indoor stations and view recents. Fore details, refer to ***Call & Talk*** .
- **Configure Event / Alarm**: Configure event and alarm for video intercom resources. For more details, refer to ***Event and Alarm Configuration*** .
- **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. For more details about related configurations and operations of the doors, refer to ***Flow Chart*** .

26.2 Video Intercom Overview

On the Video Intercom Overview page, you can view resource health status and alarm input details. You can also view and export statistics of calls and talks, and of notices in a specific period.

In the upper-left corner of the Home page, select ▦ → **All Modules** → **Video Intercom** → **Overview** .

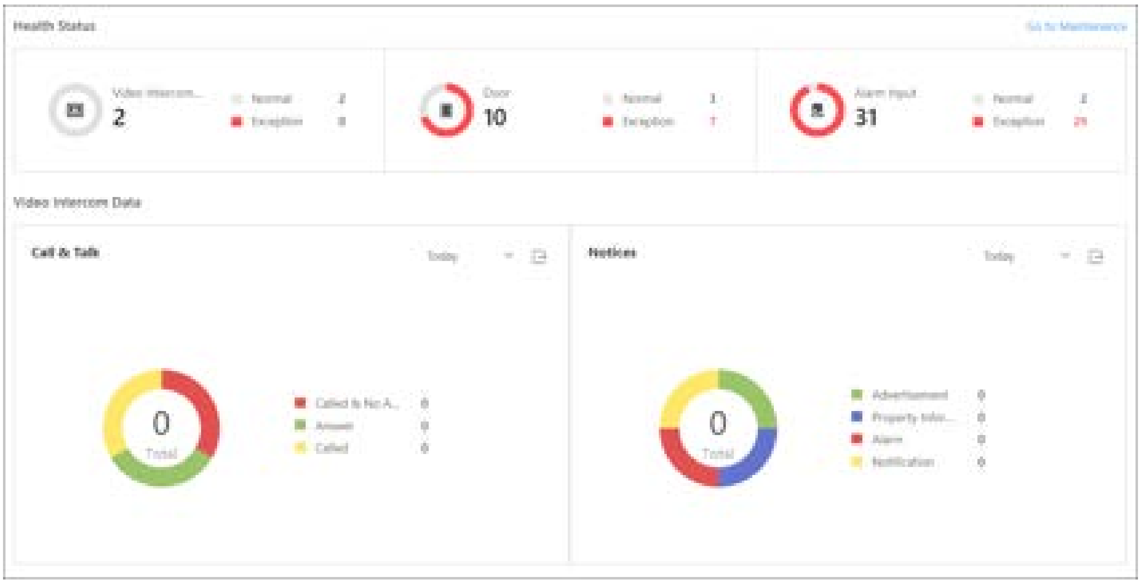


Figure 26-2 Video Intercom Overview

Perform the following operations as needed.

Operation	Description
View Resource Status	In Health Status, click on the number under the resource type or the number besides **Abnormal** to go to the Maintenance page to view details of resources status or alarm input.
Go to Maintenance	In the upper-left corner, click **Go to Maintenance** to enter the Maintenance module. For more about the Maintenance module, refer to ***Maintenance*** .
Filter Video Intercom Data	Click ⌄ and select a period to view the data of this period.
Export Video Intercom Data	Click ⧉ to select a file format and click **Export** to export the data generated in the selected period.

26.3 Basic Settings of the Platform

You can add platform users as recipients of calls from devices. After adding recipients, when someone calls the platform, the recipient can receive the call. You can also add a call schedule template which defines when door stations can call indoor stations or call center. Besides, you can configure call parameters, such as the ring tone and the max. speaking duration with the device.

26.3.1 Add Call Recipients

After adding call recipients, when someone calls the system, the added recipient can receive and answer the call.

Note

Before recipients can receive calls form devices on the platform, you need to enable **Receive Calls** on the Call Parameter page. For details about enabling this function, refer to ***Configure Call Parameters*** .

In the upper-left corner of the Home page, select ▦ → **All Modules** → **Video Intercom** → **Basic Settings** → **Call Recipient Settings** .

Click **Add** to add recipients.

Select users to receive calls and click **Add**.

On the Call Recipients Settings page, perform the following operations as needed.

- Check one or more users and click **Delete** to delete the user(s).
- In the upper-right corner, enter the keyword to search for specific users.

26.3.2 Add Call Schedule Template

Call schedule template defines when door stations can call indoor stations or call center. For example, if a resident is absent from home during workdays, while he/she is at home during weekends and holidays, the resident can customize a schedule template which call the management center during workdays and call the indoor station during weekends and holidays.

Steps

1. In the upper-left corner of the Home page, select → **All Modules** → **Video Intercom** → **Basic Settings** → .
2. Click + to add a schedule template.

   The two default templates, namely All-Day Call Schedule Template for Indoor Station and All-Day Call Schedule Template for Indoor Station, cannot be edited or deleted.
3. Create a name for the template.
4. **Optional:** Select an existing template from the **Copy from** drop-down list.
5. Select **Indoor Station** or **Management Center**.

   Note

   Select **Indoor Station** if there is someone indoor who can answer the call from door station while select **Management Center** if there is no one can answer the call.
6. Edit weekly schedule.

   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 .

   Erase Task Time
   Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period.
7. **Optional:** Click **Add Holiday** to select an existed holiday template, or click **Add New** to add a new template. For detailed information, see ***Set Holiday*** .
8. Click **Add** to save the template.
9. **Optional:** Select a task from the task list, and then click 🗑 to delete it.

What to do next

Set call schedule for indoor stations and call center to define in which time period door stations can call indoor stations or call center. For details, refer to ***Add Call Schedule for Door Stations*** .

26.3.3 Configure Call Parameters

You can configure call parameters, including the ring tone and maximum speaking duration with indoor stations, and enable or disable the Always Receive Calls function.

In the upper-left corner of the Home page, select → **All Modules** → **Video Intercom** → **Basic Settings** → **Call Parameters** .

Configure the following parameters as needed.

Ringtone

Click to select a ring tone and click **Play** to play the ring tone.

Auto Hang Up After(s)

The call will be hung up automatically after the duration.

Max. Speaking Duration with Indoor Station(s)/Door Station(s)/Access Control Device(s)

Enter the maximum duration during which you can speak with the device.

Receive Calls

After enabling the function, you can receive the calling notification from the device to the platform.

26.4 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

Card Swiping

For outer door station and door station which supports Mifare encryption, you can enable **Mifare 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 **Configuration** to go to Remote Configuration page of the device.

26.5 Manage Video Intercom Device

You can set location information for video intercom devices. After setting location information, you need to apply settings to all devices or the specified device(s).

26.5.1 Set Locations for Video Intercom Devices

You can add single device or batch add devices that have been added to the platform, and set location information for the added device(s).

Before You Start

Make sure you have added video intercom devices to the system.

Steps

1. In the upper-left corner of the Home page, select ☰ → **All Modules** → **Video Intercom** → **Device Management** .
2. Add the device(s).
   - Add single device.
     a. Click **Add** to add the device which has been added to the platform.
     b. Set the basic information and location of the device, and click **Add** to add device.
   - Add devices in a batch.
     a. Click ⌄ → **Batch Add** to add devices which have been added to the platform.
     b. Select the adding mode to add device and set required information.

Note

- If the community is divided into different sections, enter the corresponding number. If not,enter 1.
- If the building is composed of only one unit, enter 1.

Manually Select

You can select devices manually in the drop-down list.

Batch Import

You can batch add devices that have been added to the platform.

i. Click **Download Template** to download and save the template file to your PC.
ii. Open the downloaded template file and enter the required information.
iii. Click 🗀 to select the file, and click **Add** to add devices.

c. Click **Add**.

3. Click a device name.
4. In Device Location Information area, set parameters as needed.

Note

- If the community is divided into different sections, enter the corresponding number. If not,enter 1.
- If the building is composed of only one unit, enter 1.
- The parameters displayed vary with device types.

26.5.2 Apply Location to Video Intercom Devices

After setting location information for video intercom devices, you need to apply settings to devices.

In the upper-left corner of the Home page, select ▦ → **All Modules** → **Video Intercom** → **Device Management** .

Check one or more devices and click **Apply Settings**.

Select the device(s) to apply.

All Devices

By default, the changed settings will be applied to all devices. If you check **Apply (Initial)**, first clear all former information applied to the devices, and then apply all settings configured on the platform this time to the devices.

Specified Device(s)

Click 🗋 to select devices. The changed settings will be applied to the selected device(s).

Apply (Initial)

First clear all former linkages applied to the devices, and then apply all linkages configured on the platform this time to the devices. This mode is mainly used for first-time deployment.

Click **Apply** to apply settings to the device(s).

The procedure of applying information will be displayed in the pop-up window, and the reasons for failures will be displayed in the Reason column. Move the cursor over ●, and click **Retry** to apply the settings to devices again. Also, move the cursor over ●, and click **View Details** to view the details. You can also click **Retry** to re-apply settings to devices.

26.6 Video Intercom Application

You can configure call schedule templates to define when indoor stations and call centers can receive the call from door stations. After you configure the templates, you can add the templates for door stations so that they will distribute calls to indoor stations or call centers as configured in the schedule template. Finally, you can apply call schedule to devices, so devices such as indoor/ door stations and call centers can execute commands from the platform. Besides, after adding indoor station to the system, you can link camera with the added indoor station to view video of the related camera(s) on the indoor station. You can also link single person to indoor stations for calling residents. In addition, you can 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 Add Call Schedule for Door Stations

You can add call schedule for door stations to define when door stations can call indoor stations or call centers.

Before You Start

Make sure you have configured call schedule templates. For detailed information, see ***Add Call Schedule Template*** .

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **Video Intercom** → **Video Intercom Application** → **Door Station Call Schedule Settings** .
2. Click **Add** to add a door station call schedule.
3. Select a door station in the list.
4. Select a schedule template and room number for each button.

   Note

   As long as a template contains calling the call center, the Room can not be selected. See ***Add Call Schedule Template*** for details about how to set a call schedule template.
5. **Optional:** Click ▫ to view the schedule details.
6. Click **Add** to save the schedule.

   The added schedule will be displayed in the list.
7. **Optional:** Perform the following operations.

Filter Door Stations	• Click on the top right to set conditions such as Door Station, Location Information, or Application Status to filter door stations. • Click **Reset** to reset search conditions.
Delete Door Stations	Select door stations and click **Delete** or click → **Delete All** to delete the door stations.

What to do next

You can apply call schedules to devices. For detailed information, see ***Apply Call Schedule to Devices*** .

26.6.2 Apply Call Schedule to Devices

You can apply call schedules to door stations so that the communication between devices and the platform will be supported.

Before You Start

Make sure that you have added call schedules for door stations. For detailed information, see ***Add Call Schedule for Door Stations*** .

Steps

1. In the top left corner of Home page, select → **All Modules** → **Video Intercom** → **Video Intercom Application** → **Door Station Call Schedule Settings** .
2. Click **Apply Settings** on top of the device list page.
3. Select **All Door Stations** or **Specified Door Station(s)**.
4. **Optional:** If you choose **Specified Door Station(s)**, select door station(s) or click to batch select the door station(s) that you want to apply the call schedule to.

   Note

   Only the door stations with added call schedules will be displayed.
5. Click **Add**.
6. **Optional:** Check **Apply (Initial)** to clear all former call schedules applied to the devices, and then apply all call schedules configured on the platform.
7. Click **Apply**.

   The procedure of applying information will be displayed in the pop-up window, and the reasons will be displayed in the Reason column. Move the cursor over , and click **Retry** to apply the schedules to devices again. Also, you can move the cursor over , and click **View Details** to view the details. You can also click **Retry** to re-apply the schedule to devices.

26.6.3 Link Resources with Indoor Stations

After adding an indoor station to the system, 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 single person with an indoor station or multiple persons with the indoor station(s) at a time, so that linked persons can calling residents. Besides, you can relate a doorbell with an indoor station.

Link Cameras to an Indoor Station

After adding indoor station to the system, you can relate camera with the added indoor station to view video of the related camera(s) on the indoor station. Up to 16 cameras can be related to one indoor station.

Before You Start

Make sure you have added indoor station(s) to the system. For details, refer to ***Add a Video Intercom Device by IP Address*** .

Make sure the camera(s) to be related are correctly installed and are added to the system by Hikvision Private Protocol/Open Network Video Interface Protocol.

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **Video Intercom** → **Video Intercom Application** → **Linkage Camera to Indoor Station** .
2. Click **Add**.

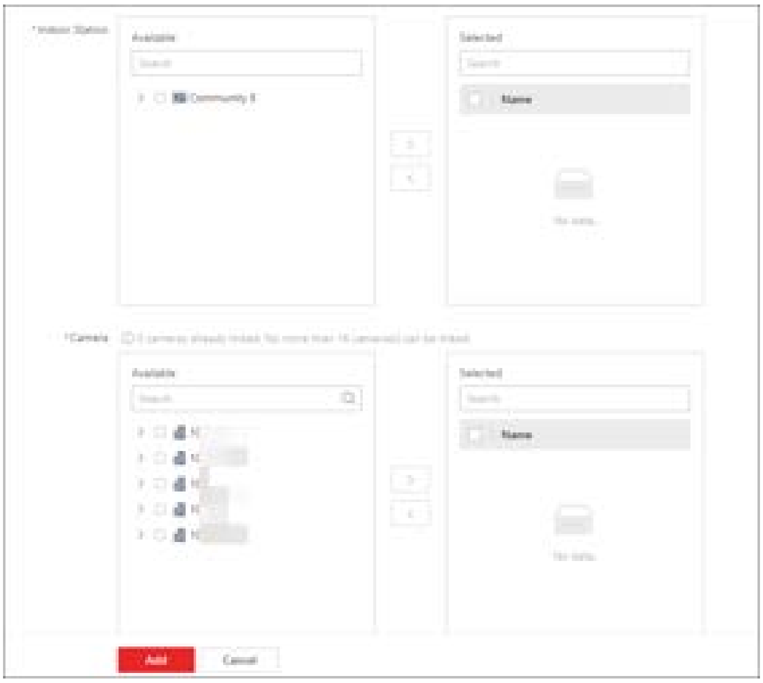


Figure 26-3 Add Related Camera

Note

You can also relate camera with 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.

Note

You can enter a keyword to search for the target indoor station(s). And the keyword of corresponding device(s) will be displayed in red.

4. In the Camera list, check one or more cameras.

Note

No more than 16 cameras can be linked. You can enter a keyword to search for the target camera(s). And the keyword of corresponding camera(s) will be displayed in red.

5. Click **Add**.

Note

You can also delete the related camera(s) in the configuration page of the indoor station.

6. Click **Apply Settings** to apply the settings to devices.
7. **Optional:** Perform the following operations.

Filter Door Stations
- Click on the top right to set conditions such as Door Station, Location Information, or Application Status to filter door stations.
- Click **Reset** to reset search conditions.

Delete Door Stations
Select door stations and click **Delete** to delete the door stations.

View Linked Cameras
On the page of the added indoor station list, click › to view linked cameras.

Change Linked Cameras
On the page of the added indoor station list, click on the IP address of the indoor station to change linked cameras.

Link Persons to an Indoor Station

The person needs to be linked with an indoor station, which is used for calling residents. You can link single person with an indoor station or multiple persons with indoor station(s) at a time. Here we introduce you how to batch link persons with indoor station(s).

Steps

Note

For more details about linking single person with an indoor station, refer to ***Add a Person Manually*** .

1. In the top left corner of Home page, select → **All Modules** → **Video Intercom** → **Video Intercom Application** → **Link Person to Indoor Station** .
2. Click **Add**.

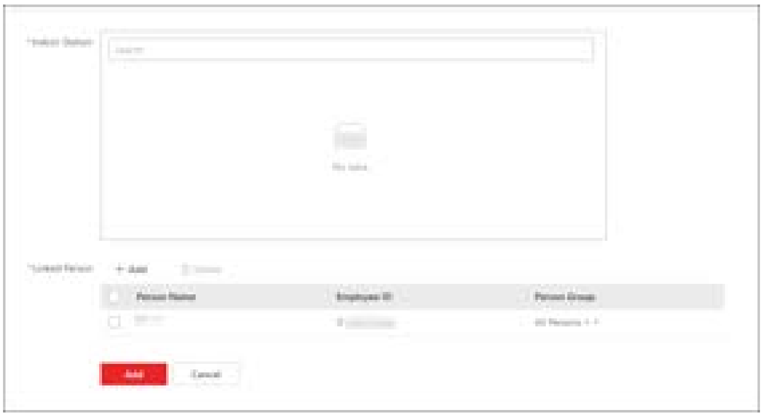


Figure 26-4 Add Linked Person

3. Select an indoor station.

Note

Up to 10 persons can be linked with one indoor station and the person cannot be linked with multiple indoor stations.

4. Click **Add** to select persons to be linked with the indoor station.
5. **Optional:** Check one or more persons and click **Delete** to delete the person(s).
6. Click **Add**.

   The linked person information will be applied to the indoor station(s).
7. **Optional:** Perform the following operations.

Filter Door Stations	• Click 🝖 on the top right to set conditions such as Door Station, Location Information, or Application Status to filter door stations. • Click **Reset** to reset search conditions.
Delete Door Stations	Select door stations and click **Delete** to delete the door stations.
View Linked Person	On the page of the added indoor station list, click › to view linked persons.
Change Linked Persons	On the page of the added indoor station list, click on the IP address of the indoor station to change linked persons.

Link Doorbell to an Indoor Station

You can relate a doorbell with an indoor station. If Call Management Center function of this doorbell is disabled, you can call the related indoor station by the doorbell.

If you have added the doorbell to the system, you can relate the doorbell with an indoor station as the following steps. If not, you can also relate the doorbell with an indoor station when adding the doorbell (see ***Manage Video Intercom Device*** for more details).

Steps

1. In the top left corner of Home page, select ▦ → **All Modules → Video Intercom → Video Intercom Application → Link Doorbell to Indoor Station** .
2. Click **Add** to enter Link Doorbell with Indoor Station page.

   The added doorbells are displayed in the list.
3. From drop-down list, select the doorbell to be related with the indoor station.
4. From drop-down list, select the corresponding indoor station that the doorbell is to be related with.

   Note

   The location information of the indoor station is same as that of the doorbell.
5. Click **Add**.
6. **Optional:** Check one or more doorbells and click **Delete** to delete the doorbell(s).

Result

The doorbell will be related with the selected indoor station.

26.7 Manage Notices

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. Before applying the copied notice, you can also edit the notice.

26.7.1 Add and Apply a Notice

You add and apply notices to indoor stations. After adding and applying notices, you can delete, filter, and export them.

Steps

1. In the upper-left corner of the Home page, select ▦ → **All Modules → Video Intercom → Notice Applying** .
2. Click **Add** to add a notice.
3. Create a title of the notice.
4. Select a notice type.
5. **Optional:** Click + to add pictures.

   Note

   Up to 6 pictures can be added, and each picture should be no larger than 512 KB. The picture format should be JPG.

6. Enter the content of the notice.
7. Select indoor stations to receive the notice.
8. Click **Preview** to preview the notice.
9. Click **Apply** to apply the notice to indoor stations.
10. Perform the following operations.

Delete Notice
Check one or more notices and click **Delete**.

Export Notice
Check one or more notices and click **Export** to export notice information to the Excel/CVS file.

Filter Notices
In the upper-right corner, click to set filter conditions and click **Filter**.

View Notice Details
Click to view the basic information (title, notice type, etc.) and application status.

Note

In the Application Status page, you can also apply or search notices.

26.7.2 Copy and Apply Notice to Indoor Stations

You can copy a notice and apply it to indoor stations conveniently. Before application, you can also edit the copied notice.

Note

Make sure you have added and applied a notice to indoor stations.

In the upper-left corner of the Home page, select → **All Modules** → **Video Intercom** → **Notice Applying** .

The following are two methods for copying and applying the notice(s).

1. If notice information needs no change, check one or more notices, and click **Copy and Apply**. The checked notice(s) will be copied and applied to indoor stations directly.
2. If notice information needs change, click to copy the current notice and edit the notice as needed. Click **Apply** to apply the notice to indoor stations.

26.8 Call & Talk

In Call & Talk module, you can view contacts of indoor stations in a specific unit and call an indoor station conveniently. You can also view and export recents which include details such as the device name, call status, and device location. Besides, you can download recorded audios to the local PC.

26.8.1 Call an Indoor Stations

You can view names and locations of indoor stations, and person information. You can also call indoor stations directly on the platform in situations such as when the call the to the door station is failed and when an emergency occurs.

In the upper-left corner of the Home page, select 🟥 → **All Modules** → **Video Intercom** → **Call & Talk** → **Contacts** .

On the left, select an unit. The indoor stations in this unit will be listed on the right. In the upper-right corner, you can also set conditions and enter the keyword to search indoor stations.

Click ☎ to call the indoor station.

26.8.2 View Recents

You can view and export call logs which include details such as the device name, call status, and device location. You can also download recorded audios to the local PC.

In the upper-left corner of the Home page, select 🟥 → **All Modules** → **Video Intercom** → **Call & Talk** → **Recents** .

Perform the following operations as needed.

Operation	Description
Export Logs	Check one or more devices and click **Export** to export call logs to in Excel/CSV file format.
Filter Logs	Click ▽ to set conditions and click **Filter** to search logs.
Download Recorded Audio	Click ⤓ to download the recorded audio in MP4 format to the local PC.

Chapter 27 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. For details, refer to ***Set User Preference*** .

27.1 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.

27.1.1 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. In the top left corner of Home page, select ▦ → **All Modules → Temperature Screening → Configuration** .
2. 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 **Save**.
3. 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**.

4. **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.

27.1.2 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. For details, refer to ***Configure Other Parameters*** .

27.2 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.

In the top left corner of Home page, select ▦ → **All Modules** → **Temperature Screening** → **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.

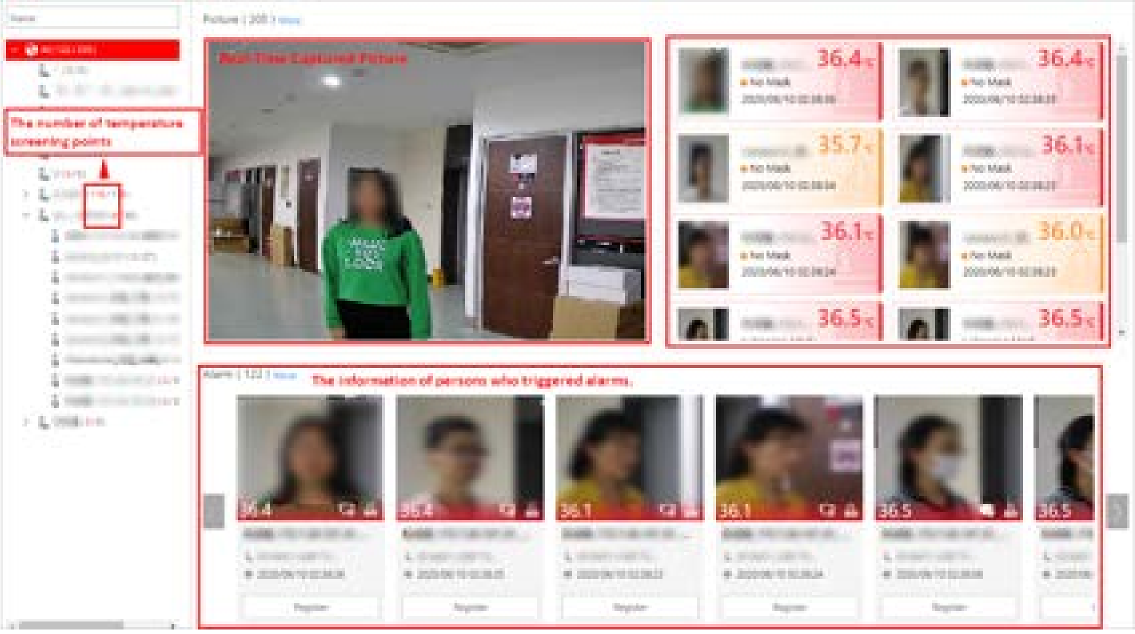

Real-Time Captured Picture
The number of temperature screening points
The information of persons who triggered alarms.
36.4
36.4
35.7
36.1
36.1
36.0
36.5
36.5
No Mask
Register

Figure 27-1 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.

27.3 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

Temperature screening data has been generated in real-time skin-surface temperature monitoring.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Temperature Screening** → **History** .
2. Select a temperature screening point group or a temperature screening point from the list.
3. Click to unfold the Filter panel.
4. Set the search condition(s) including start time, end time, skin-surface temperature, etc.
5. Click **Filter**.

   History temperature screening data that meets the search condition(s) will be displayed below.
6. **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.

27.4 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.

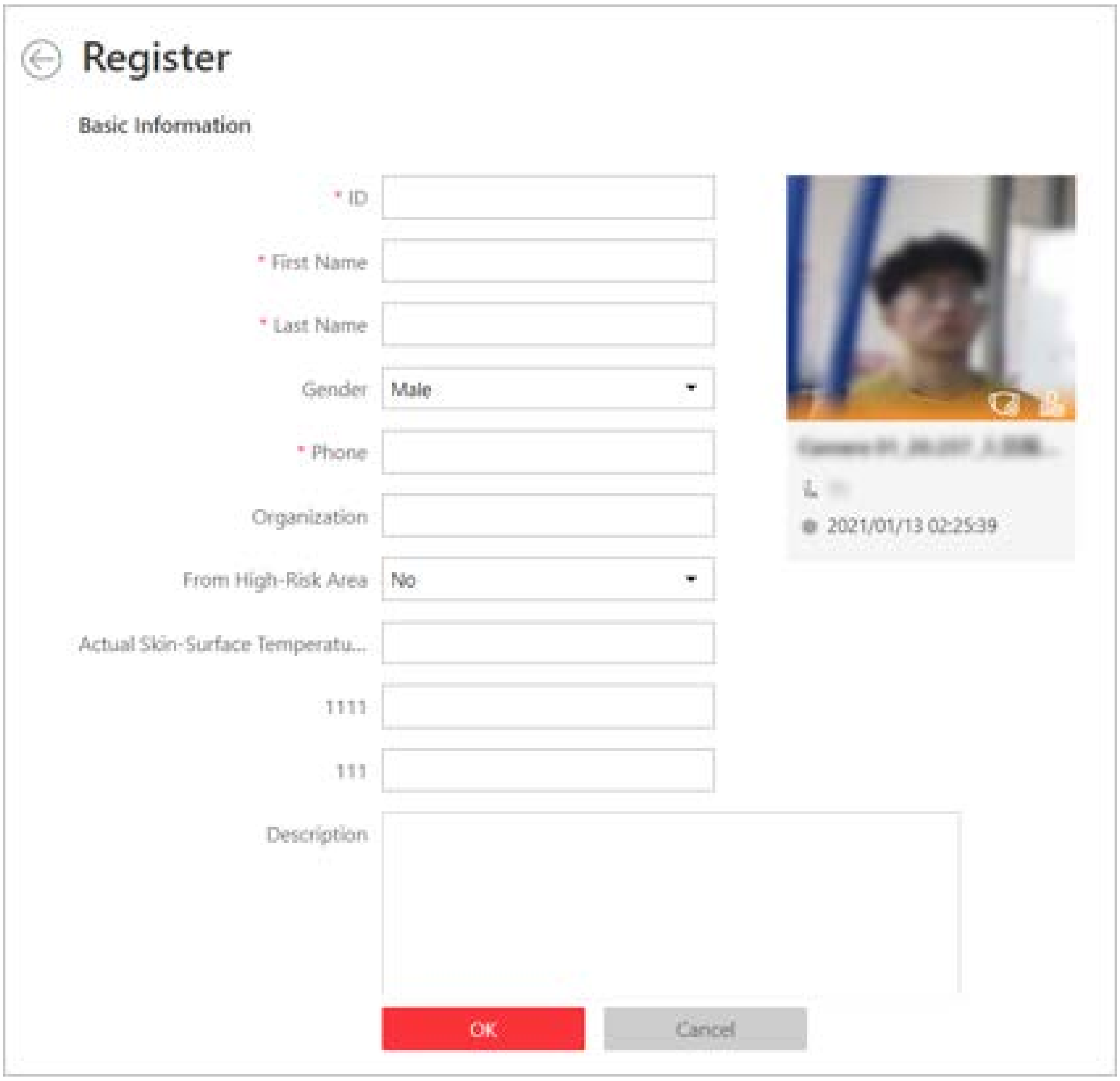
27.4.1 Register Person Information

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. In the top left corner of Home page, select ▦ → **All Modules** → **Temperature Screening** → **Skin-Surface Temperature** (or **History**).

   The skin-surface temperature screening information will be displayed.
2. If a screened person is not registered, you can click **Register** to enter the Register page to register for the person.



Register

Basic Information

* ID

* First Name

* Last Name

Gender: Male

* Phone

Organization

From High-Risk Area: No

Actual Skin-Surface Temperatu...

1111

111

Description

2021/01/13 02:25:39

Figure 27-2 Register Page

3. 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.

4. 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.

27.4.2 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. In the top left corner of Home page, select 🟥 → **All Modules** → **Temperature Screening** → **Registration** .
2. Click ⚙ **Registration Template** to enter the Registration Template page.
3. Click **Add**.
4. In the Title field, create a name for the additional item.

   Note

   Up to 32 characters are allowed for the name.
5. 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.
6. Click **Save**.
7. **Optional:** Perform one or more of the following operations.

Edit Name	Click ✎ to edit the name.
Delete	Click × to delete the additional item.

27.4.3 View Registered Person Information

For the registered persons, you can view their detailed information including person name, ID, gender, phone, skin-surface temperature, wearing mask or not, etc.

In the top left corner of Home page, select 🟥 → **All Modules** → **Temperature Screening** → **Registration** .

You can view person name, ID, gender, 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.

27.5 Generate Report

Skin-surface temperature report gives you an overview of skin-surface temperature, mask-wearing detecting results, and registered person information. Based on the temperature status and mask-wearing detecting 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 to learn their detailed information including name, location, face picture, from high-risk area or not, etc.

In the top left corner of Home page, select ▦ → **All Modules** → **Temperature Screening** → **Report** .

Select a temperature screening point group or temperature screening point, set time range at the bottom and click **Generate Report**.

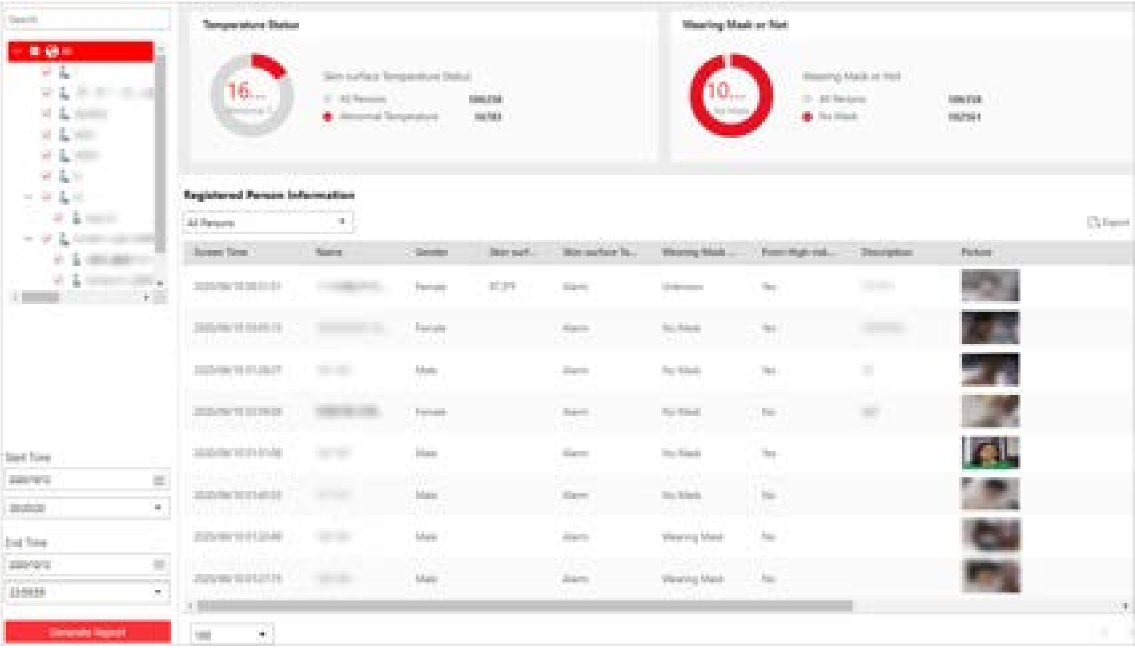


Figure 27-3 Skin-Surface Temperature Report

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 who had been detected whether they are wearing a mask, and the number of persons wearing no mask.

Registered Person Information

You can filter persons with abnormal skin-surface temperature or wearing no mask quickly to view their detailed information. For example, If a person with abnormal skin-surface temperature does not wear 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 a 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.

Chapter 28 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 GIS map, you can see the geographic locations of your surveillance system. This type of map uses a geographic information system to accurately show all the hot spots' (resources (e.g., camera, alarm input) placed on the map are called hot spots) geographic locations in the real world. GIS map lets you view and access cameras 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 (e.g., camera, alarm input) 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.

28.1 Set GIS Map and Icons

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. In the top left corner of Home page, select 🟥 → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. 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, 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**.

3. Click **Icon Settings** to set the customized icons.
   1) Click **Hot Region** or the following device types 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 path.

   Note

   The icon picture format can only be PNG, JPG, or JPEG.

   4) **Optional:** Click to constrain the aspect ratio.
   5) Click **Save**.

Result

You can view the GIS map on Map Monitoring page and perform the following operations in the map area.

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.

28.2 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.

Before You Start

Make sure you have disabled the GIS Map function. See ***Set GIS Map and Icons*** for details.

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. Open the Add Map panel.
   - 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.
4. Select an adding mode.
5. Select 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.
6. Click **Add**.
7. **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 **Calibrate** 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.

8. **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.

9. **Optional:** Perform the following operations after adding map in the map area.

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	Drag the map or the red window in the lower part to adjust the map area for view.

28.3 Search Locations on GIS Map

You can search the locations on the GIS map.

Before You Start

You should enable the GIS Map function and set the GIS Map API URL properly. For details, refer to ***Set GIS Map and Icons*** .

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. **Optional:** On the top left of the map, click ▦ to display the GIS map.
3. On the top left of the map, enter a location name you want to search in the 🔍 field.

   The related locations display in the search field.
4. Click to select the location you want to locate from the related locations.

Result

The location will be located on the map.

28.4 Add Hot Spot on Map

You can add elements (e.g., cameras, access points, alarm inputs, etc.) as the hot spot and place the hot spot on the e-map or GIS map. Then you can view the elements on the map and perform further operations via Control Client. For example, you can get the live view, actual access points, and alarm information of the surveillance scenarios, lock access point, unlock access point, and so on.

Before You Start

A map should have been added. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

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** 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 setting GPS location (only available when parent map is GIS map, and refer to ***Search Locations on GIS Map*** for details), and selecting icon style).

For camera and radar hot spot, you can also edit the detection area, including radius, direction, and angle, or drag the displayed sector on the map to directly adjust the detection area.

Delete Hot Spot Click the hot spot icon on the map and click **Delete** to remove the hot spot from the map.

28.5 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. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding maps.

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.

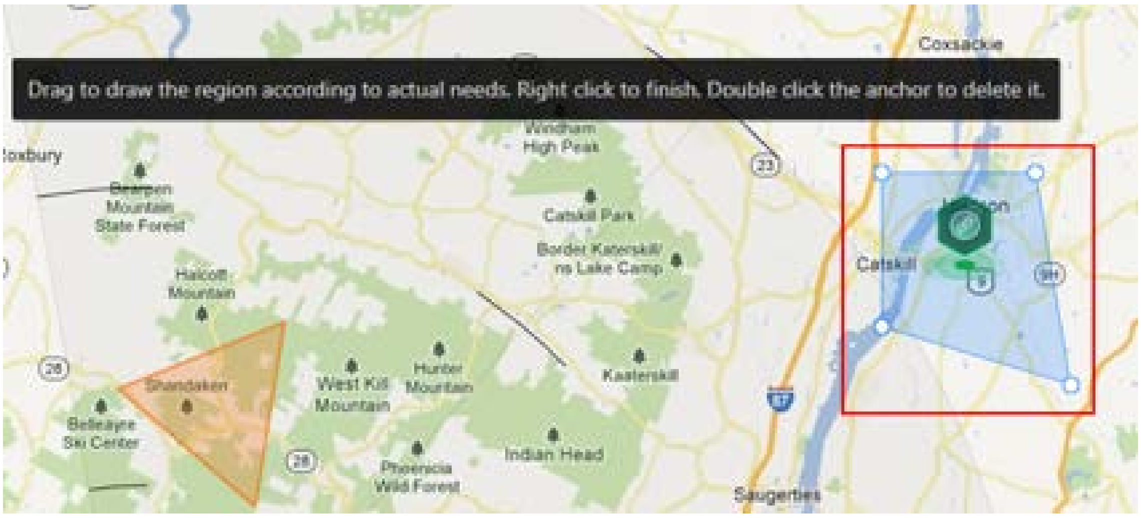
   The added hot region icon will be displayed on the parent map.
8. **Optional:** Perform the following operation(s) after adding the hot region.

   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, and refer to ***Search Locations on GIS Map*** for details), 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.



Drag to draw the region according to actual needs. Right click to finish. Double click the anchor to delete it.

Figure 28-1 Edit Hot Region Area

28.6 Add Label on Map

You can add labels with description on the map.

Before You Start

At least one map should have been added. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

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 **Label** icon on the right.
5. Click on the map where you want to place the label.
6. Customize a name for the label, and you can input content for the label as desired.
7. Click **Save**.

   The added label icon will be displayed on the map.
8. **Optional:** Perform the following operation(s) after adding the label.

Adjust Label Location	Drag the added label on the map to the desired locations.
Edit Label	Click the added label icon on the map to view and edit the detailed information, including name and content on the appearing dialog.
Delete Label	Click the label icon on the map and click **Delete** on the appearing dialog to delete the label.

28.7 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 border of the region for detection.

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.

For details about how to add a people counting group on the map, refer to ***Add People Counting Group*** .

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.

For details about adding a heat analysis group, refer to ***Add Heat Analysis Group*** .

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.

For details about how to add a pathway analysis group, refer to ***Add Pathway Analysis Group*** .

Person Feature Analysis Group

After adding the person feature analysis group, the cameras which support facial recognition and feature analysis (such as gender and age group) 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.

For details about adding a person feature analysis group, refer to ***Add Person Feature Analysis 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 Control Client.

For details about how to add an anti-passback group on the map, refer to ***Configure Area Anti-Passback Rules*** .

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 Control Client.

For details about how to add a multi-door interlocking group on the map, refer to ***Configure Multi-Door Interlocking***

Entry & Exit 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 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.

For details about how to add an entry &exit counting group on the map, refer to ***Add Entry and Exit Counting Group*** .

Emergency Operation 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 Control 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 Emergency Operation Group*** .

Security Control Partition (Area)

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.

For details about adding a security control partition, refer to ***Add Security Control Partitions (Area) from Device*** .

28.8 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. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

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 **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 refer to ***Search Locations on GIS Map*** for details), 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.

28.9 Add Combined Alarm on Map

You can add the combined alarms on map to locate the alarm for a visualized monitoring.

Before You Start

Make sure you have added a map. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

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 **Combined Alarm** on the right.
5. Drag a combined alarm to the map.

   The combined alarm is displayed on the map.
6. **Optional:** Perform the following operations after adding the combined alarm.

Adjust Combined Alarm Location	Drag the added combined alarm on the map to the desired locations.
Edit Combined Alarm	Click the added combined alarm 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 refer to ***Search Locations on GIS Map*** for details), and selecting icon style).

Delete Combined Alarm Click the combined alarm icon on the map and click **Delete** to remove the combined alarm from the map.

28.10 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.

Before You Start

Make sure you have configured a GIS map. See ***Set GIS Map and Icons*** for details.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **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.

28.11 Operate Hot Spot

The resources (including cameras, alarm inputs, alarm outputs, access points, elevators, radars, UVSS, and digital signage) added on the map are called the hot spots. The hot spots show the locations of the resources. You can operate the hot spot, such as starting live view of the camera, UVSS, and door, arming or disarming the resources.

28.11.1 Preview Hot Spot

You can view locations of hot spots including cameras, alarm inputs, alarm outputs, access points, elevators, radars, sites, Under Vehicle Surveillance Systems (UVSS), etc. on the map. Also, you can set the arming control and view history alarms of surveillance scenarios through the hot spots.

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 → **All Modules** → **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 occupacy rate and parking floor details.

6. Operate in the dialog.
   - For camera and UVSS hot spot: Check the live view and playback of the camera, view its status, area, and remark, set the arming control, and view the history alarms.

     Note

     - To view the live view and playback of the camera, the user should be assigned with permissions of live view and playback of the camera. For details, refer to the *User Manual of HikCentral Professional Web Client*.
     - For details about arming control, see ***Arm or Disarm Hot Spot*** .
     - For details about viewing history alarms, see ***View History Alarm*** .
   - For alarm input hot spot: View its status, area, and remark, set the arming control, and view the history alarms.
   - For alarm output hot spot: Turn on or off the linked alarm output.

- For access point hot spot: View the access point status, check the live view and playback of the access point's related camera(s), view the access point's basic information, control the door status, set the arming control, and view the history alarms and access records.
- For elevator hot spot: View the elevator status, area and remark, check the live view and playback of the elevator's related camera(s), control the floor status, set the arming control, and view the history alarms and access records.
- For radar hot spot: View the radar status, area and remark, check the live view and playback of the radar's related camera(s), set the arming control, view the history alarms.
- For radar PTZ camera hot spot: View camera's field of view and view the object's moving pattern.
- For site hot spot: View the site's resources and alarms which are not handled.
- For partition hot spot: Set the arming control including alarm clearing, disarming, away arming, stay arming, instant arming. For details, refer to ***Arm or Disarm Hot Spot*** .
- For parking lot hot spot: Click a certain floor and you will go to the paking lot management module so you can view the details of the the parking floor in the parking lot.

  Hover your cursor on a parking lot, you can view the details of the parking lot. If nothing appears, you can click **Configure Now** to configure the parking lot.

28.11.2 Broadcast via Hot Spot

You can broadcast via hot spot through real-time speaking or playing the saved audio files.

Before You Start

Make sure you have added broadcast resources on the map.

Steps

1. In the top left corner of Home page, select ⊞ → **All Modules** → **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. Click the broadcast icon to view details such as Status, Area, and Remark.
4. Click **Broadcast** to select the broadcast mode.
5. Select **Speak** or **Play Audio** as the broadcast mode.

   Note

   Speak

   Speak in real-time, and the audio will be recorded and uploaded to the server.

   Play Audio

   Play the files saved in the server.
6. **Optional:** If you select **Play Audio** as the adding mode, you can search or select a desired audio file to play.

Note

Click **Download** to download a selected audio file. The speed of playing the audio file will be faster if you downloaded them.

7. Click **Enabled**.
   - After you enable speaking, it will start broadcasting immediately.
   - After you enable 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.

28.11.3 Draw Zone or Trigger Line for Radar

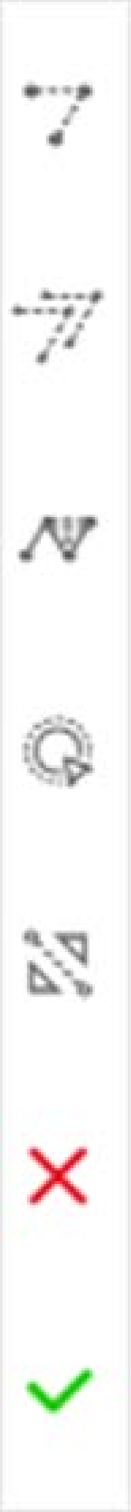
You can draw zones or trigger lines for radar, so if an object is detected to have crossed the trigger line or entered the area shaped by the dual-trigger line or zone, the event and alarm will be triggered.

Before You Start

A radar has been added to the area and map. Refer to ***Add Radar to Area for Current Site*** and ***Add Hot Spot on Map*** for details.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **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.

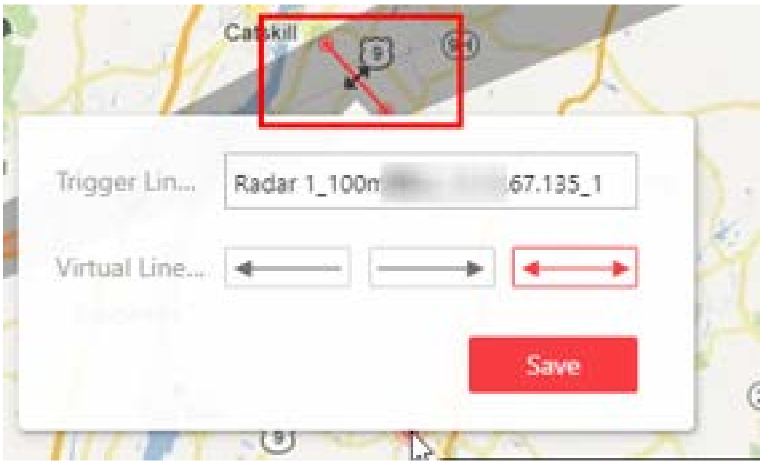


Draw Trigger Line

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.



Trigger Lin... Radar 1_100m[redacted]67.135_1

Virtual Line... ← → ↔

Figure 28-3 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.

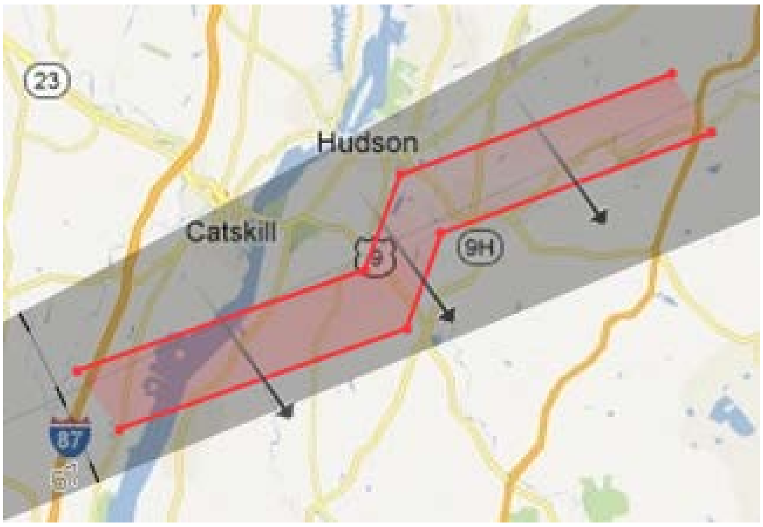


Figure 28-4 Dual-Trigger Line in the Detection Area

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.

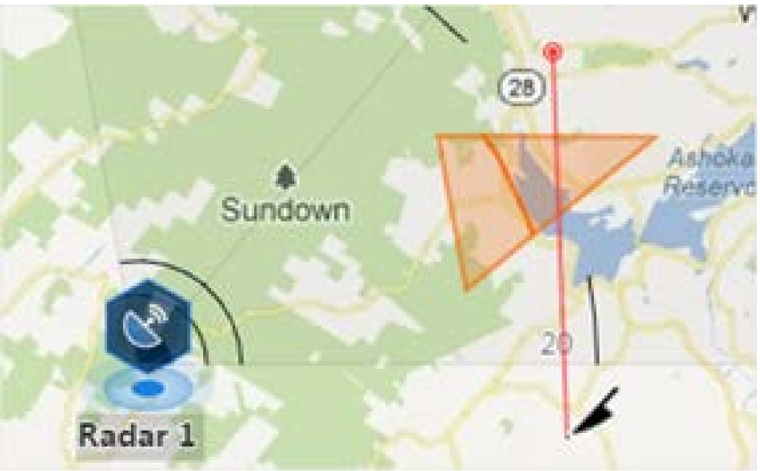


Figure 28-5 Zone Segmentation

Distance Segmentation

Split a zone into two smaller zone by an arc.

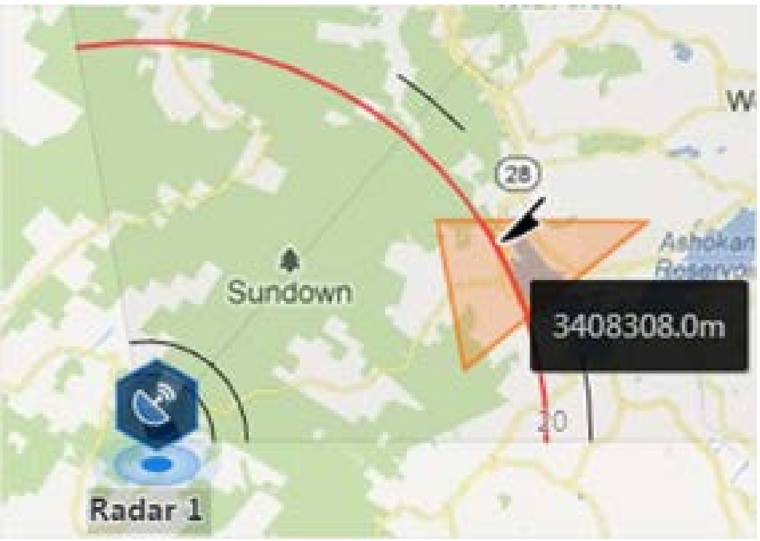


Figure 28-6 Distance Segmentation

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.

28.11.4 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 Radar to Area for Current Site*** and ***Add Hot Spot on Map*** for details.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **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.

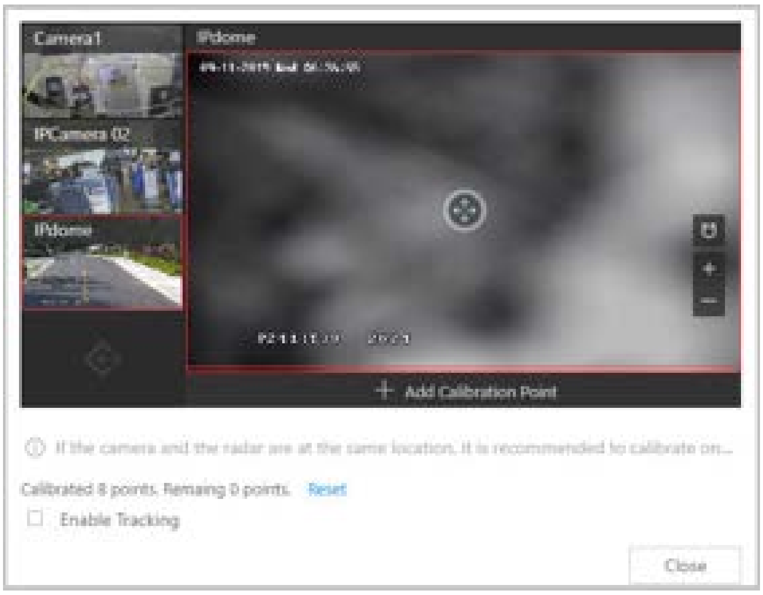
4. Click the radar's icon first, and then click camera icon(s) to relate the camera(s) with the radar.

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.



ⓘ If the camera and the radar are at the same location, it is recommended to calibrate on...

Calibrated 8 points. Remaing 0 points. Reset

□ Enable Tracking

Close

Figure 28-7 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.

28.11.5 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.

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 🟥 → **All Modules** → **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 to select a map.
4. Click the hot spot.

   A window on which the related functions of the hot spot display is opened.
5. Click **Arm/Disarm** to arm/disarm the hot spot.

28.11.6 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.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Map** → **Map Monitoring** .
2. Click the hot spot.

   A dialog pops up on which the related functions of the hot spot display.
3. Click ■ to enter the event and alarm search page.
4. Search history alarms of the hot spot. See ***Search Event and Alarm Logs*** for details.

28.12 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 🟥 → **All Modules** → **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.

28.13 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 🟥 → **All Modules** → **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.

28.14 View Remote Site Alarm

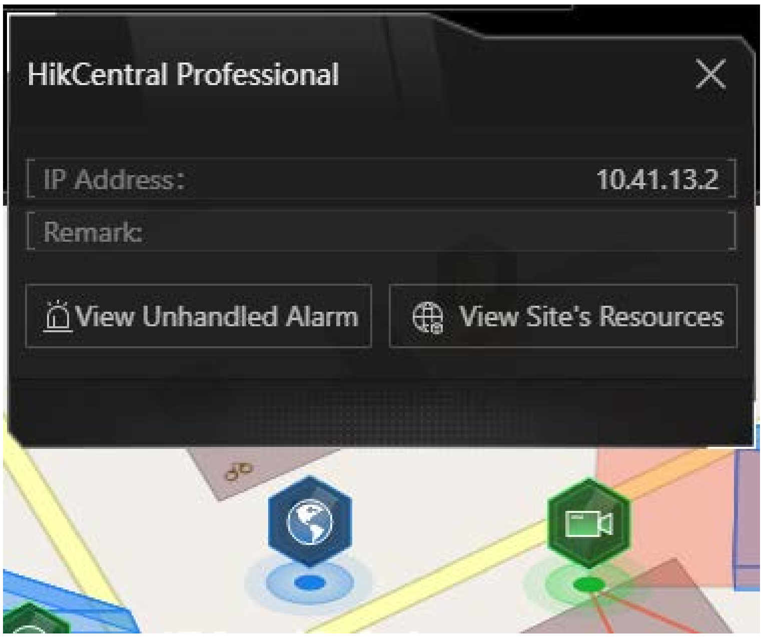
If you have added a remote site on a GIS map, you can view the information of alarms triggered on the remote site. Even if there is no alarm triggered at the current time, you can also view history alarms of the site.

Before You Start

Make sure you have added a remote site on the GIS map. See ***Add Remote Site on GIS Map*** for details.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **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.



HikCentral Professional

IP Address: 10.41.13.2

Remark:

Figure 28-8 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.

28.15 Operate Map

After opening map, you can perform one or more operations of the followings, such as zooming in or out map, selecting resource(s) on map, adding label, printing map, displaying map in full screen mode, and so on.After opening map, you can perform one or more operations of the followings, such as zooming in or out map, adding label, displaying map in full screen mode, and so on.

Zoom in/Zoom out Map

Use the mouse wheel or click + or − to zoom in or zoom out on the map.

Filter

Click ◉ and select the resource type you want to show on the map.

Add Label

Click ▣ to add a label with description to the map.

Search Location

By the search bar on the top of the map, you can search locations on GIS map and hot spot/hot region on the e-map by entering keyword(s).

Chapter 29 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.

29.1 Health Monitoring

Health monitoring 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.

29.1.1 Real-Time Health Status Overview

In the Health Monitoring 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.

In the top left corner of the client, select 🟥 → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

Click **Real-Time Overview** tab at the top to enter the Real-Time Overview page.

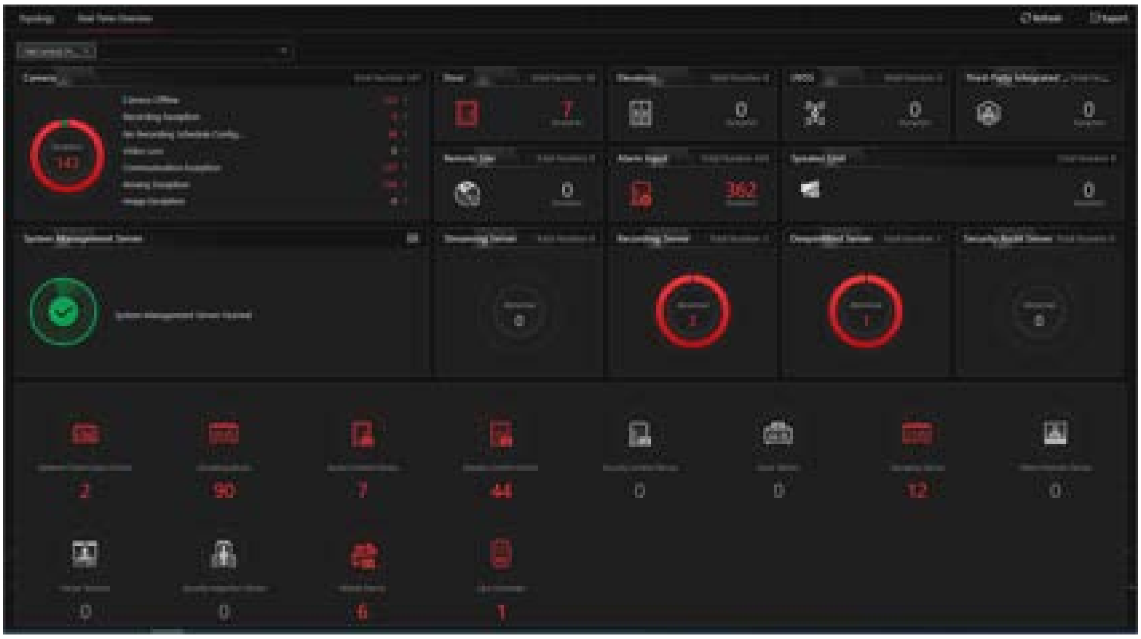
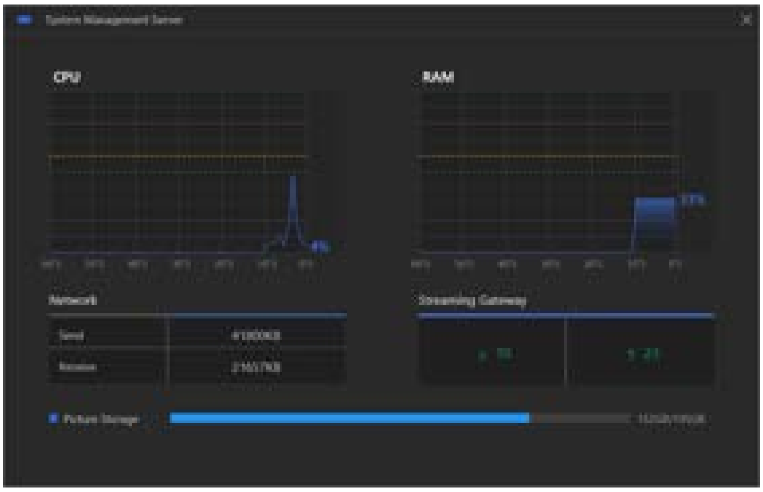
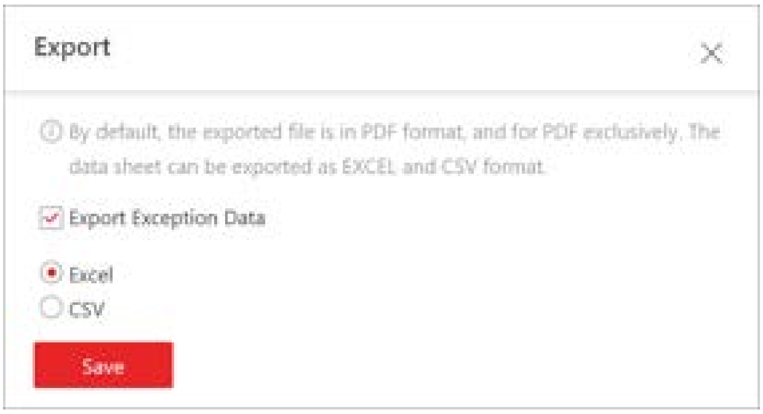


Figure 29-1 Real-Time Health Status Overview

Table 29-1 Real-Time Health Status Page

Section	Description
Resource Status	View the abnormal data of different resources (e.g., cameras, doors, elevators, or alarm inputs) added to areas of Central System in the graphical way. You can click the numbers and status types on the chart to view the real-time status details of resources or Remote Sites. **Note** The Remote Site status is only available for the Central System with Remote Site Management module (based on the License you purchased).
System Management Server Status	View the network health status and server running status. Click ▪ in the upper right corner of System Management Server panel to view the running status details of the server, including CPU usage, RAM usage, etc.

Section	Description
	 System Management Server CPU RAM Network Send Receive Streaming Gateway Picture Storage **Figure 29-2 System Management Server Status Details**
Server Status	View the status (i.e., exception, warning, normal) of servers added on Central System. You can click the numbers and status types on the chart to view the real-time status details of servers.
Device Status	View the abnormal data of different devices (e.g., encoding devices, decoding devices, or access control devices) added on Central System. You can click the numbers on the chart to view the real-time status details of devices. 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*** .
Select Sites	Select one or multiple Sites (including Remote Sites) from the drop-down list in the upper left corner of Real-Time Overview page to display the status of resources on the selected Site(s).
Refresh	• 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 Settings → Health Check Frequency** to set the interval for automatically refreshing the resource status on the page. See details in ***Set Health 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.  Export ⓘ By default, the exported file is in PDF format, and for PDF exclusively. The data sheet can be exported as EXCEL and CSV format. ☑ Export Exception Data ● Excel ○ CSV Save **Figure 29-3 Export Overview Page or Exception Data**

29.1.2 Real-Time Health Status Overview (Topology)

In the Health Monitoring 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, surveillance 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.

In the top left corner of the client, select ▣ → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

Click **Topology** tab at the top to enter the Topology page.

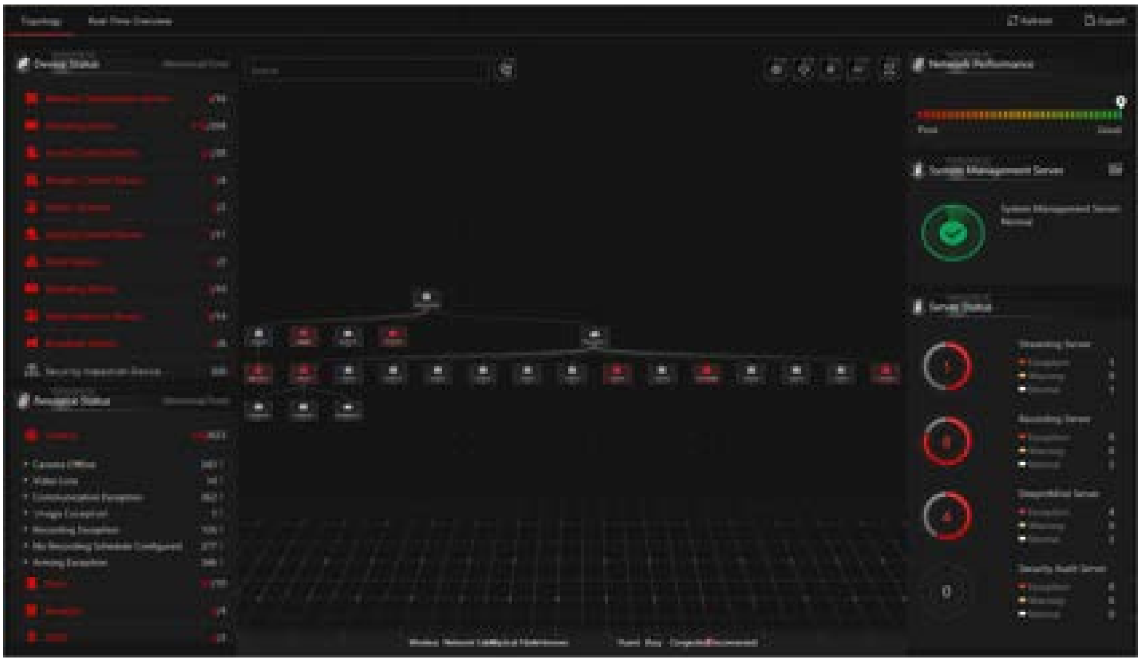
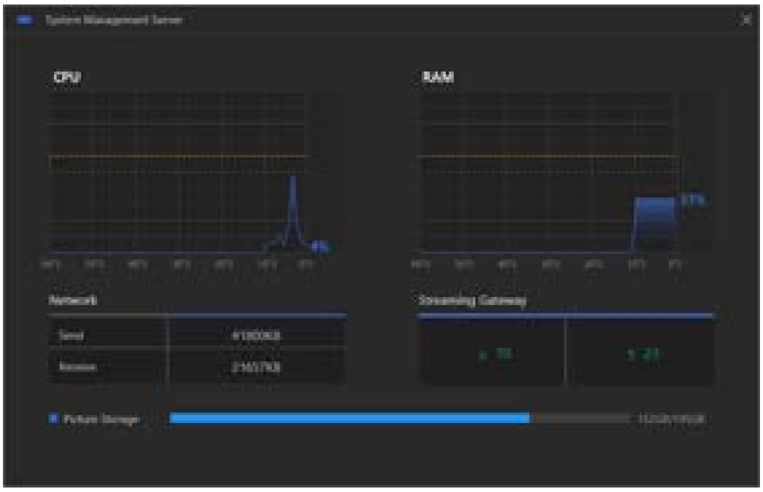
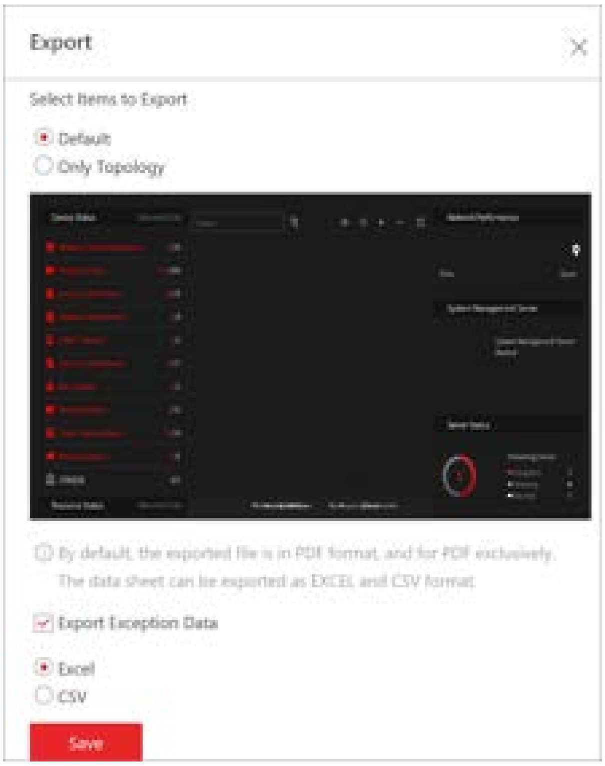


Figure 29-4 Topology Overview

Table 29-2 Topology Page

Section	Description
Device Status	View the abnormal data of different devices (e.g., encoding devices, decoding device, or access control devices) added on the Central System. 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 (e.g., cameras, doors, elevators, or alarm inputs) added to the areas of the Central System. You can click the number to view the real-time status details of resources or Remote Sites. **Note** The Remote Site status is only available for the Central System with the Remote Site Management module (based on the License you purchased).

Section	Description
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 (i.e., poor or good) of the System Management Server.
System Management Server Status	View the network health status and server running status. Click ▪ in the upper right corner of the System Management Server panel to view the running status details of the server, including its CPU usage, RAM usage, etc.  System Management Server CPU RAM Network Send Receive Streaming Gateway Picture Storage **Figure 29-5 System Management Server Status Details**
Server Status	View the status (i.e., exception, warning, normal) of servers added on the Central System.
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 Health 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

Section	Description
	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.  Export Select Items to Export ● Default ○ Only Topology By default, the exported file is in PDF format, and for PDF exclusively. The data sheet can be exported as EXCEL and CSV format. ☑ Export Exception Data ● Excel ○ CSV Save **Figure 29-6 Export Topology**

Topology Details

The topology of devices will display the hierarchical relationships among the devices, device information, link status, alarm information, etc.

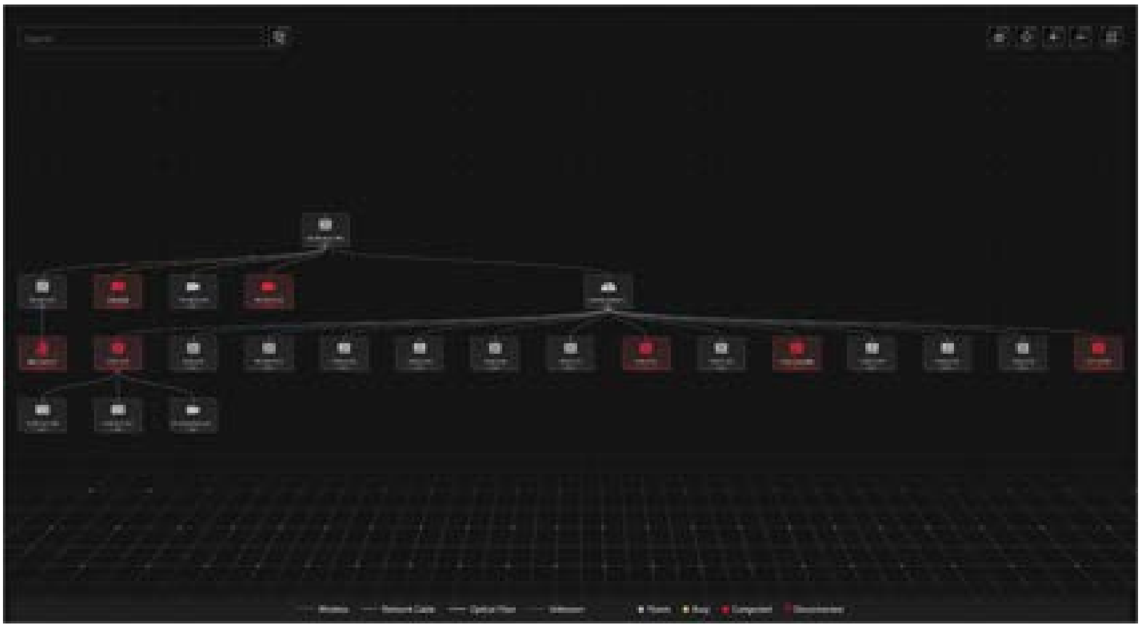


Figure 29-7 Topology Details

Device Node

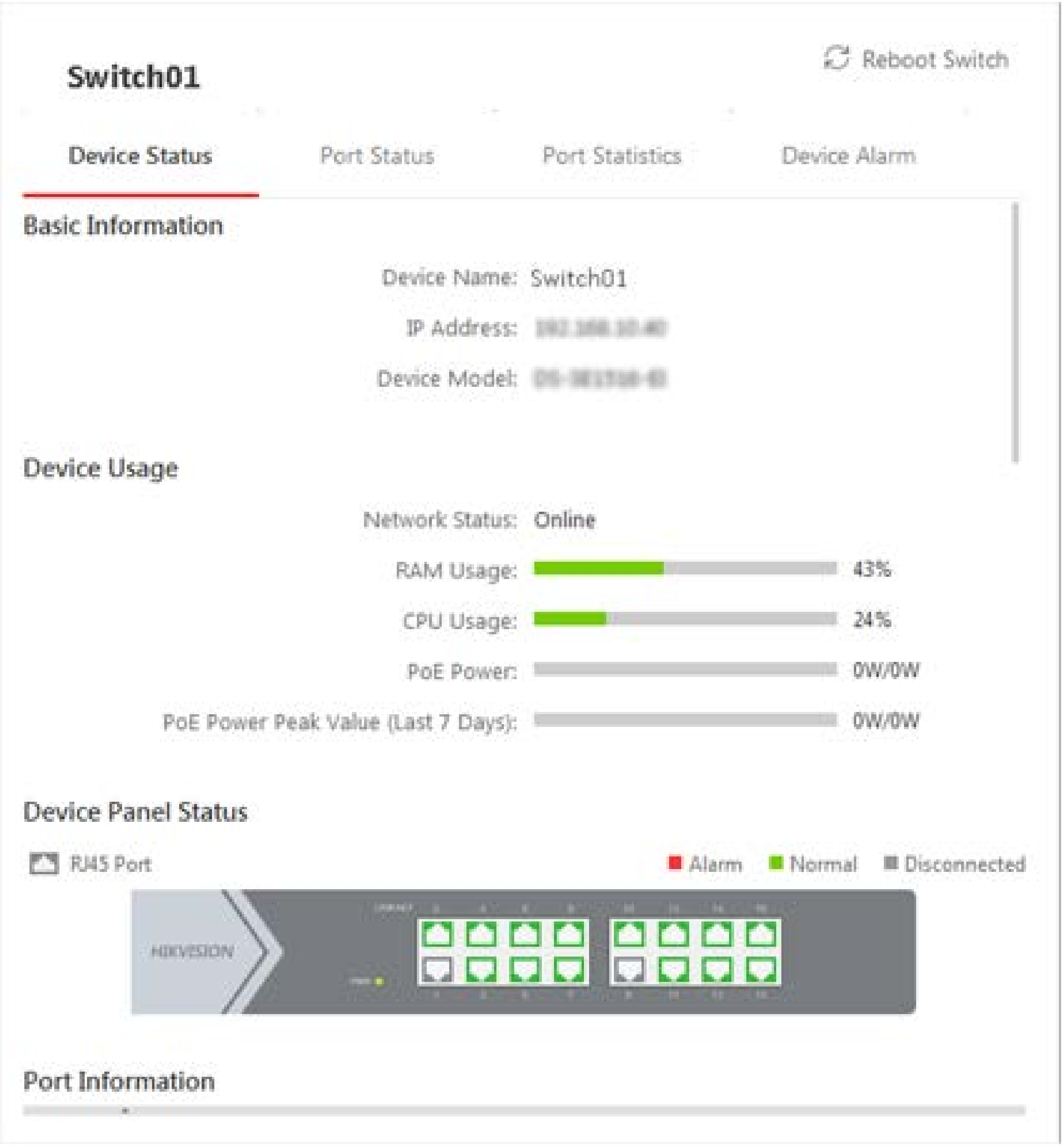
The device nodes are displayed by icons, including the System Management Server, Recording Server, network transmission device, encoding device, access control device, video intercom device, network bridge, fiber converter, etc. Each device node displays the device name and IP address.

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).



Switch01

Reboot Switch

Device Status | Port Status | Port Statistics | Device Alarm

Basic Information

Device Name: Switch01

IP Address: [redacted]

Device Model: [redacted]

Device Usage

Network Status: Online

RAM Usage: 43%

CPU Usage: 24%

PoE Power: 0W/0W

PoE Power Peak Value (Last 7 Days): 0W/0W

Device Panel Status

RJ45 Port

🟥 Alarm 🟩 Normal ▨ Disconnected

Port Information

Figure 29-8 View Device Details

Note

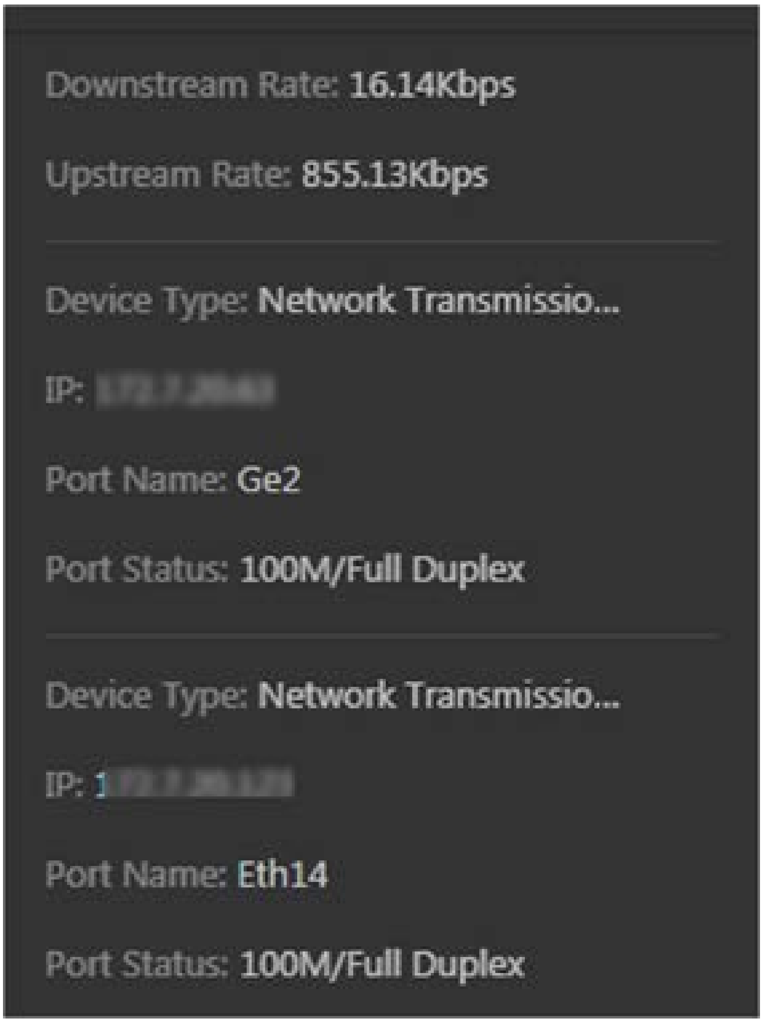
The device details vary with different device models.

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.



Downstream Rate: 16.14Kbps

Upstream Rate: 855.13Kbps

Device Type: Network Transmissio...

IP: [redacted]

Port Name: Ge2

Port Status: 100M/Full Duplex

Device Type: Network Transmissio...

IP: [redacted]

Port Name: Eth14

Port Status: 100M/Full Duplex

Figure 29-9 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.

29.1.3 Historical Health Data Overview

You can view the historical online rate of resources and devices, or the recording integrity rate.

In the top left corner of Home page, select ▦ → **All Modules** → **Maintenance** → **Health Monitoring** → **History Overview** .

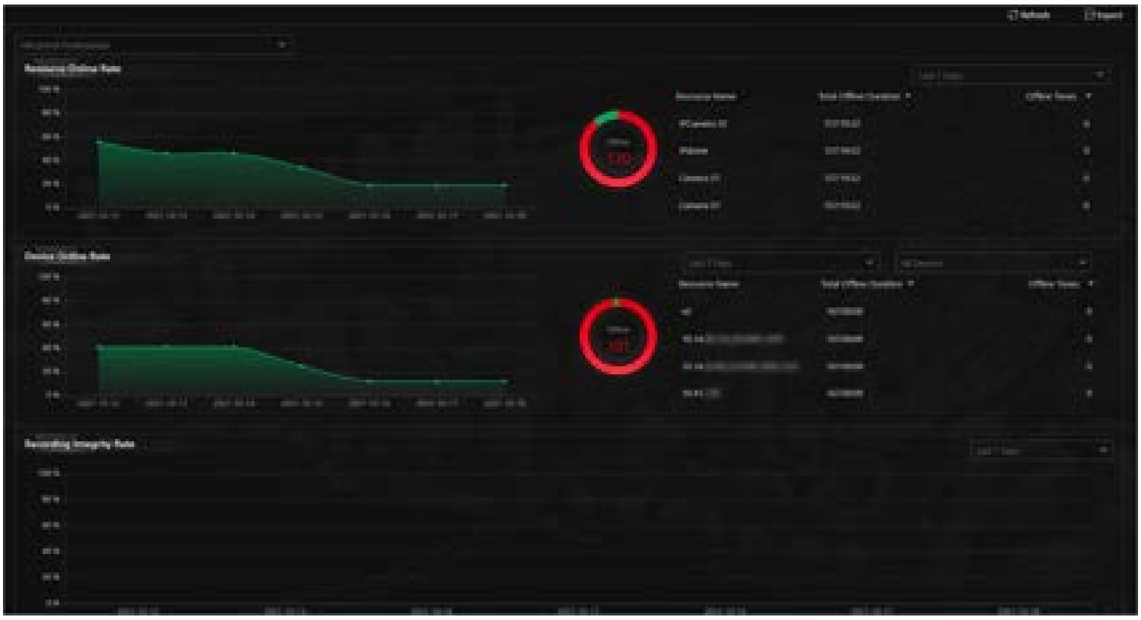
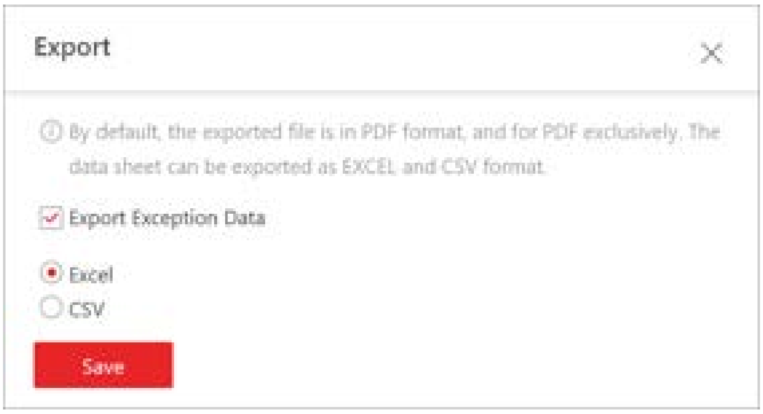


Figure 29-10 Historical Health Data Overview

Table 29-3 Historical Health Data Page

Section	Description
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: ◦ 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:

Section	Description
	◦ 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.
Recording Integrity Rate	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 Device Log page to view the detailed resource status of devices at that time point.
Select Site	Select a Current or Remote Site from the drop-down list in the upper left corner of History Overview page to display the historical data of resources on the Site.

Section	Description
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 Settings → Health Check Frequency** to set the interval for automatically refreshing the data on the page. See details in ***Set Health 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.  ⓘ By default, the exported file is in PDF format, and for PDF exclusively. The data sheet can be exported as EXCEL and CSV format. ☑ Export Exception Data ● Excel ○ CSV **Figure 29-11 Export Overview Page or Exception Data**

29.2 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.

29.2.1 Send Log Report Regularly

You can configure parameters to send device and resource log reports to specified users regularly via email. Device log reports contain information on the online/offline status of device, and resource log reports contain the online/offline status of resources as well as the recording status.

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

- Make sure you have set an email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Make sure you have configured 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 records in total.
- The report is an Excel file.

1. In the top left corner of Home page, select ▦ → **All Modules** → **Maintenance** → **Basic Settings** .
2. Select **Scheduled Report** on the left.
3. 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.
4. In **Report Category**, select **Resource Logs**.
5. Edit the report rule.

   Report Name

   Create a name for the report.

   Report Target

   Specify the resources that you want to add into the report.

   Report Content

   Select the log content to be included in the report.

   Statistics Type

   Select the generation frequency of the report. You can set a sending time in **Send At**.

   Daily

   Daily 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) as **Send 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.

Weekly/Monthly

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, 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 **Recent One Week**.

Report Time

Set the time period during which the logs will be recorded.

Send Date

Set the report sending date(s) if you have set **Statistics Type** as the daily report.

Send At

Set a report sending time.

Effective Period

Set the effective period for the report rule.

Report Language

Select a report language.

Send Report via Email

Switch on to send the report via email.

Email Template

Select an email template to define the recipient information and content if you have switched on **Send Report via Email**.

Note

You can click **Add New** to add a new email template. For setting email template, refer to ***Set Email Template*** .

Upload to SFTP

Switch on to upload the report to SFTP.

Note

You can click **Configuration** to set the SFTP.

Local Storage

Switch on to save the report to the local PC.

Note

You can click **Configuration** to set the saving path.

6. Click **Add** to save the report rule.

Send Device Log Report Regularly

You can set report sending rules for encoding devices, and the platform can send emails with device log reports to specified users daily, weekly, or monthly.

Before You Start

- Make sure you have set an email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Make sure you have configured 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 records in total.
- The report is an Excel file.

1. In the top left corner of Home page, select 🟥 → **All Modules** → **Maintenance** → **Basic Settings** .
2. Select **Scheduled Report** on the left.
3. 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.
4. In **Report Category**, select **Device Logs**.
5. Edit the report rule.

   Report Name

   Create a name for the report.

   Report Target

   Specify the devices that you want to add into the report.

   Report Content

   Select the log content to be included in the report.

   Statistics Type

   Select the generation frequency of the report. You can set a sending time in **Send At**.

   Daily

   Daily 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) as **Send 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.

Weekly/Monthly

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, 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 **Recent One Week**.

Report Time

Set the time period during which the logs will be recorded.

Send Date

Set the report sending date(s) if you have set **Statistics Type** as the daily report.

Send At

Set a report sending time.

Effective Period

Set the effective period for the report rule.

Report Language

Select a report language.

Send Report via Email

Switch on to send the report via email.

Email Template

Select an email template to define the recipient information and content if you have switched on **Send Report via Email**.

Note

You can click **Add New** to add a new email template. For setting email template, refer to ***Set Email Template*** .

Upload to SFTP

Switch on to upload the report to SFTP.

Note

You can click **Configuration** to set the SFTP.

Local Storage

Switch on to save the report to the local PC.

Note

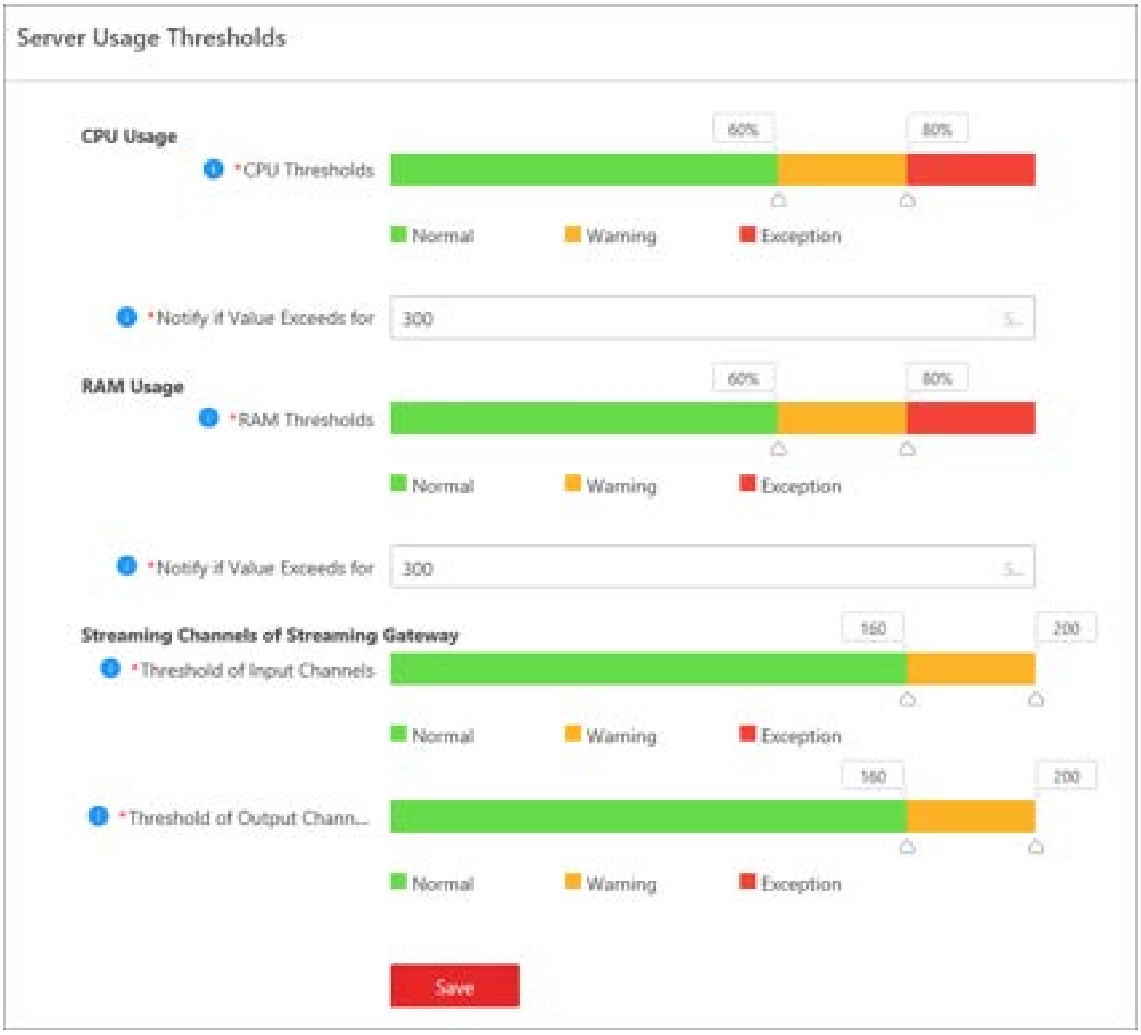
You can click **Configuration** to set the saving path.

6. Click **Add** to save the report rule.

29.2.2 Set Warning Threshold for SYS Usage

An alarm can be triggered if the SYS's CPU usage and RAM usage reaches a predefined warning threshold and lasts for a predefined duration, or if the channel usage of Streaming Gateway reaches a predefined warning threshold. The related threshold value can be checked via the Control Client.

In the top left corner of Home page, select ☰ → **All Modules** → **General** → **Maintenance** → **Basic Settings** → **Server Usage Thresholds** .



Server Usage Thresholds

CPU Usage

*CPU Thresholds: 60% 80%

*Notify if Value Exceeds for: 300 s

RAM Usage

*RAM Thresholds: 60% 80%

*Notify if Value Exceeds for: 300 s

Streaming Channels of Streaming Gateway

*Threshold of Input Channels: 160 200

*Threshold of Output Chann...: 160 200

Figure 29-12 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 (see ***Add Event and Alarm***), the alarm will be triggered when the CPU usage reaches 60% and lasts for 20 seconds.

Streaming Channels of Streaming Gateway

Drag the to adjust the threshold value for the number of input or output channels of Streaming Gateway.

Example

If you set the Warning threshold value to 160 for the number of input channels of Streaming Gateway, 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.

29.2.3 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.

In top left corner of Home page, select → **All Modules** → **Maintenance** → **Basic Settings** → **Network Timeout** .

Table 29-4 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.

29.2.4 Set Health 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 Health Status Overview module, such as the devices' online/offline status, recording status, etc. You can set the frequency which controls how often the platform gets the latest status of the devices, servers, and resources.

In the top left corner of Home page, select ▦ → **All Modules** → **Maintenance** → **Basic Settings** → **Health Check Frequency** .

Device Health Status

You can set the health check frequency for different devices, including visitor terminals, encoding devices, access control devices, elevator control devices, video intercom devices, security control devices, dock stations, network transmission devices, IP speakers, decoding devices, security inspection devices, and lane controllers, 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.

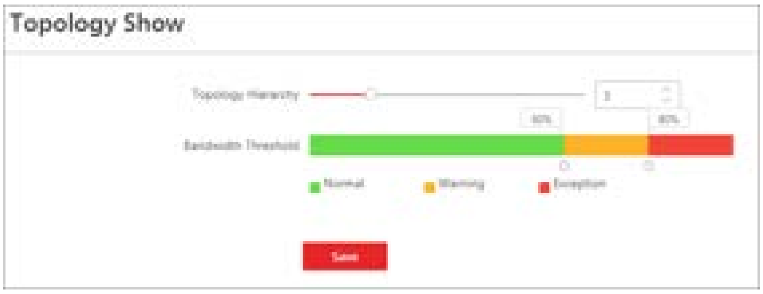
29.2.5 Set Topology Show Parameters

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 Monitoring*** .

In the top left corner of Home page, select ▦ → **All Modules** → **Maintenance** → **Basic Settings** → **Topology Show**



Topology Show

Topology Hierarchy

Bandwidth Threshold

Figure 29-13 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.

29.3 Resource Status

You can monitor the status of the added resources, such as cameras, encoding devices, Recording Servers, Streaming Servers, etc., 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 left corner of the client, select ▦ → **All Modules** → **Maintenance** → **Resource Status** , and select a resource type on the navigation panel on the left.

Note

You can view the status of cameras, UVSSs, Streaming Servers, Recording Servers, encoding devices, dock stations, and decoding devices added on the Remote Sites via the Resource Status module of Central System.

Camera Status

On the camera status page, you can view camera status, such as network status, arming status, and recording status.

You can also perform the following operations.

- Select a Remote Site from the drop-down list in the camera list panel to display the status of cameras on the Remote Site.
- Click the camera name to view its status and basic information.
- Click the IP address to view the status of the device to which the camera is related.
- Click in the Operation column to go to the Area page to configure the parameters of the specified camera. See details in ***Edit Camera for Current Site*** or ***Edit Element for Remote Site*** .
- Click in the Operation column to view the online/offline records of the specified camera. For details, see ***Search for Online/Offline Logs of Resource*** .

  Note

  This operation is not available for the cameras added on Remote Sites.
- Click in the Operation column to view the recording status of the camera. For details, see ***Search for Recording Status of Resource*** .

  Note

  This operation is not available for the cameras added on Remote Sites.
- 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.
- Select the device type(s) from the first drop-down list on the top to filter the camera status by device type.
- Check the check box and select the exception type from the second drop-down list on the top to filter the camera status by exception type.

Note

Contact the admin user to edit the abnormal configurations of camera's event or alarm via the Web Client if an icon ⓘ appears near the camera name.

Door Status

On the door status page, you can view the information such as the network status of related devices and door status.

Note

For the door linked to the video intercom device, the door status is not available to be displayed.

You can also perform the following operations.

- Click the door name to view the status details and basic information.
- Click the device name to view the status of the device to which the door is related.
- Click in the Operation column to go to the Area page to configure the parameters of the specified door. See details in ***Edit Door for Current Site*** .
- 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).

      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 super users.
- Check the check box and select the exception type from the drop-down list on the top to filter the door status by exception type.

Elevator Status

On the elevator status page, you can view information, such as the network status of elevator control devices and the card reader status.
You can also perform the following operations.

- Click the name to view the status details and basic information.
- Click the device name to view the status of the device to which the elevator is related.
- Click in the Operation column to go to the Area page to configure the parameters of the specified elevator. See details in ***Edit Elevator for Current Site*** .
- Check the check box and select the exception type from the drop-down list on the top to filter the elevator status by exception type.

Alarm Input Status

You can view the alarm input status including resource usage status (online or offline), arming status, bypass status, fault status, alarm status, detector connection status, battery status, and so on.
You can also perform the following operations.

- Click the device name to view the status of the device to which the alarm input is related.
- Select the device type(s) from the first drop-down list on the top to filter the alarm input status by device type.
- Check the check box and select the exception type from the second drop-down list on the top to filter the alarm input status by exception type.

UVSS Status

On the UVSS status page, you can view the information such as line scan camera status and capture camera status.

You can also perform the following operations.

- Click the UVSS name to view the status details and basic information.
- Select a Remote Site from the drop-down list at the top of UVSS status page to display the status of UVSSs on the Remote Site.
- Click in the Operation column to go to the Area page to configure the parameters of the specified UVSS. See details in ***Edit Under Vehicle Surveillance System for Current Site*** .

  Note

  This operation is not available for the UVSSs added on Remote Sites.
- Check the check box and select the exception type from the drop-down list on the top to filter the UVSS status by exception type.

Speaker Unit Status

On the speaker unit status page, you can view the status and information of speaker units, such as the network status and health check time.

You can also perform the following operations.

- Click the speaker unit name to view the status details and basic information.
- Click the device name to view the status of the device to which the speaker unit is related.
- Click in the Operation column to go to the Area page to configure the parameters of the specified speaker unit. See details in ***Edit Speaker Unit for Current Site*** .
- Check the check box and select the exception type from the drop-down list on the top to filter the speaker unit status by exception type.

Remote Site Status

You can view the Remote Site status such as the network status and health check time, and click the Remote Site name to view the status details and basic information.

Streaming Server Status

You can view the streams via each added Streaming Server (including incoming streams and outgoing streams), and view the hardware status such as network status, CPU usage, and RAM usage.

You can also perform the following operations.

- Click the Streaming Server name to view the status details and basic information.
- Check the check box and select the exception type from the drop-down list on the top to filter the Streaming Server status by exception type.

Recording Server Status

You can view the status and information of Recording Server, such as the recording status, CPU usage, RAM usage, HDD status, and so on.
You can also perform the following operations.

- Click the Recording Server name to view the status details and basic information.
- Select a Remote Site from the drop-down list at the top to display the status of Recording Servers on the Remote Site.
- Click the status in Recording Status column to view the recording status of the channels configured to store the video files in this Recording Server.
- Click the status in Hardware Status or HDD Status column to view the hardware status and HDD exception details if the status is exceptional.
- Check the check box and select the exception type from the drop-down list on the top to filter the Recording Server status by exception type.

DeepinMind Server Status

You can view the network status, CPU usage, and RAM usage, etc., of the DeepinMind Servers, and click the server name to view the status details and basic information.
You can also check the check box and select the exception type from the drop-down list on the top to filter the DeepinMind Server status by exception type.

Security Audit Server Status

You can view the HDD status, network status, and first added time, etc., of the Security Audit Server, and click the server name to view the status details and basic information.
You can also check the check box and select the exception type from the drop-down list on the top to filter the Security Audit Server status by exception type.

Encoding Device Status

You can view the encoding device status including the recording status, HDD usage, arming status, etc.
You can perform the following operations.

- Select a Remote Site from the drop-down list at the top to display the status of encoding devices on the Remote Site.
- Click the device name to view the status and basic information of the encoding device and the related cameras.
- Click the status in **Recording Status** column to view the recording status of channels configured to store the video files on this encoding device.
- Click ⚙ in the Operation column to go to the Device and Server page to configure the parameters of the specified encoding device.
- Click 🔔 to wake up the encoding device if it is in sleep mode.

- Click in the Operation column to view the online/offline records of the encoding device. For details, see ***Search for Online/Offline Logs of Device*** .
- Check the check box and select the exception type from the drop-down list on the top to filter the encoding device status by exception type.

Access Control Device Status

You can view the status and information such as network status and battery status of the added access control devices. If the device is turnstile, you can view the status of master lane controller, slave lane controller, and component.
You can perform the following operations.

- Click the device name to view the status and basic information of the access control device, and the related doors and cameras.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified access control device.
- Check the check box and select the exception type from the drop-down list on the top to filter the Access Control Device status by exception type.

Elevator Control Device Status

You can view the information such as network status, arming status, and distributed elevator controller status.

- Click the device name to view the status and basic information of the elevator control device, and the related floors and cameras.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified elevator control device.
- Check the check box and select the exception type from the drop-down list on the top to filter the elevator control device status by exception type.

Video Intercom Device Status

You can view the status information of the video intercom device such as network status, arming status, and the status of calling center from device (whether the device is able to call the surveillance center of the platform).
You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Click the device name to view the status and basic information of the video intercom device, and the related doors and cameras.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified video intercom device.
- Select the device type(s) from the first drop-down list on the top to filter the video intercom device status by device type.
- Check the check box and select the exception type from the second drop-down list on the top to filter the video intercom device status by exception type.

Security Control Device Status

You can view the managed devices' network status, battery status, and so on.
You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Check the check box and select the exception type from the drop-down list on the top to filter the security control device status by exception type.
- Click the device name to view the status and basic information of the security control device, and the related alarm inputs and cameras.
- Click ⚙ in the Operation column to go to the Device and Server page to configure the parameters of the specified security control device.

Dock Station Status

You can view the network status, HDD status, file backup status, and so on, of the added dock station.
You can perform the following operations.

- Select a Remote Site from the drop-down list at the top to display the status of dock stations on the Remote Site.
- Click the device name to view the status and basic information of the dock station.
- Click ⚙ in the Operation column to go to the Device and Server page to configure the parameters of the specified dock station.
- Check the check box and select the exception type from the drop-down list on the top to filter the dock station status by exception type.

IP Speaker

You can view the IP speakers' network status, serial No., address, and so on.
You can perform the following operations.

- Click the device name to view the status and basic information of the IP speaker.
- Click ⚙ in the Operation column to go to the Device and Server page to configure the parameters of the specified IP speaker.

Network Transmission Device

You can view the network transmission devices' CPU usgae, RAM usage, PoE usage, occupied ports, and so on.
You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Check the check box and select the exception type from the drop-down list on the top to filter the network transmission device status by exception type.
- Click the device name to view the basic information, device usage, and port information of the network transmission device.
- Click ⚙ in the Operation column to go to the Device and Server page to configure the parameters of the specified network transmission device.

Decoding Device Status

You can view the status information such network status, first added time, and checking time.
You can perform the following operations.

- Select a Remote Site from the drop-down list at the top to display the status of decoding devices on the Remote Site.
- Click the device name to view the status and basic information of the decoding device.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified decoding device.

Security Inspection Device

You can view the security inspection devices' network status, IP address, serial No., and so on.
You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Check the check box and select the exception type from the drop-down list on the top to filter the security inspection device status by exception type.
- Click the device name to view the status and basic information of the security inspection device.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified security inspection device.
- Click in the Operation column to view the online/offline records of the security inspection device. For details, see ***Search for Online/Offline Logs of Device*** .

Common Operations

You can perform the following operations for different resource types.

- Check **Include Sub-area** to display the resources of child areas.
- 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.
- Click **Export** to export the status data as CSV or Excel to the local PC.
- 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 (see details in ***Set Health Check Frequency***).

29.4 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 the Remote Site; 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 and online status.
You can search the log files, view the log details and backup the log files.

29.4.1 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. In the top left corner, select ■ → **All Modules** → **Maintenance** → **System Log** → **Server Logs** .

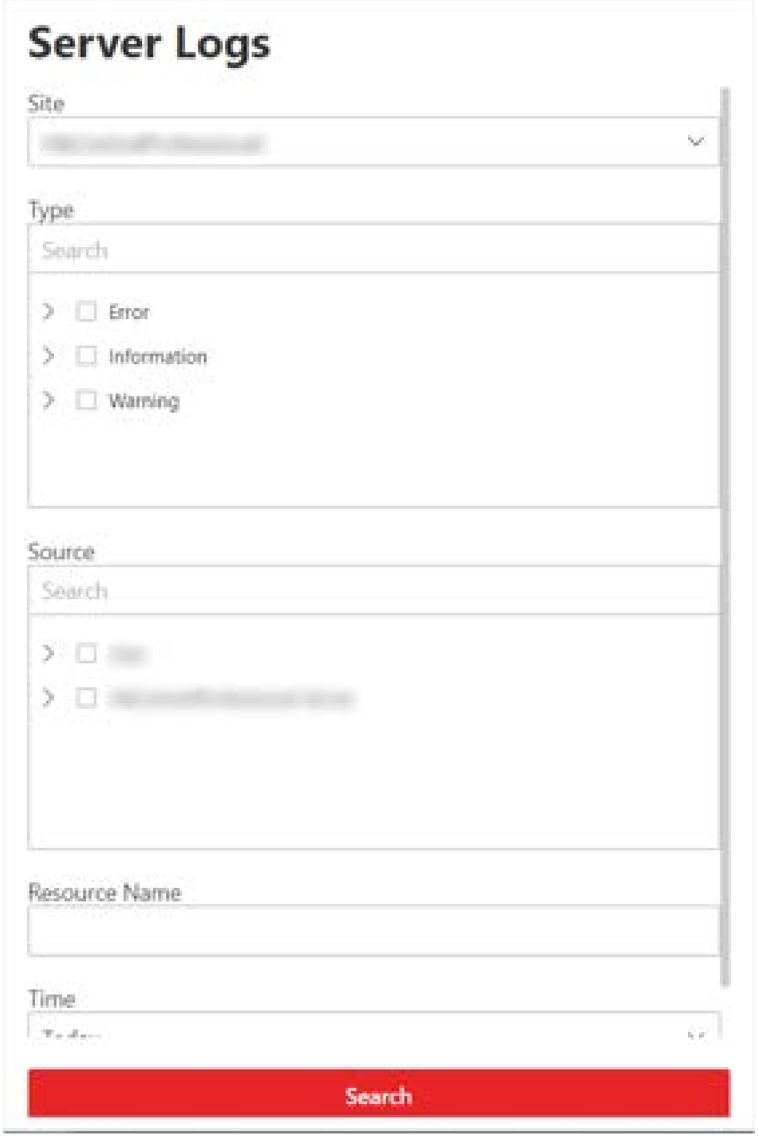


Figure 29-14 Search for Server Logs

2. In **Site**, select the current site or a Remote Site.
3. In **Type**, 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 **Source**, select user and server to set the source of the logs that you want to search for.
5. **Optional:** In **Resource Name**, enter the name of a resource to search the logs of the resource.
6. In **Time**, select the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

7. Click **Search**.

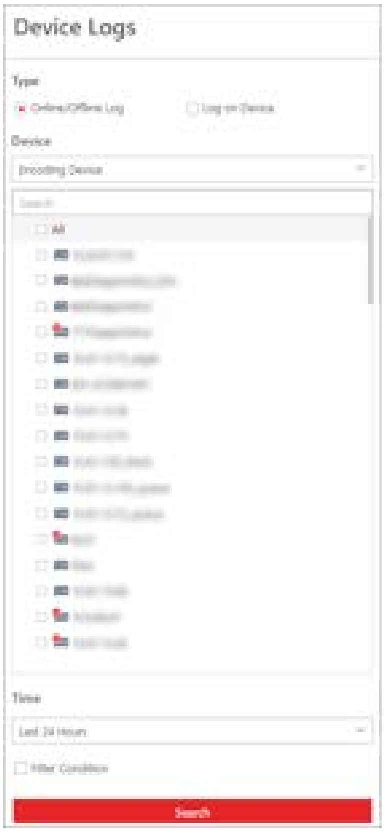
   All matched logs are listed with details on the right.
8. **Optional:** Check all or specific logs, click **Export**, and then select a file format (i.e., Excel or CSV) to download the searched logs as a single file to your local PC.

29.4.2 Search for Online/Offline Logs of Device

You can search for the online/offline logs of encoding devices, security inspection devices, and mobile devices. The online/offline logs provide information on the current device status (online or offline), latest offline time, total offline duration, etc.

Steps

1. In the top left corner, select ▦ → **All Modules** → **Maintenance** → **System Log** → **Device Logs** .



Device Logs

Type

● Online/Offline Log ○ Log on Device

Device

Encoding Device

Search

□ All

Time

Last 24 Hours

□ Filter Condition

Search

Figure 29-15 Search for Device Online/Offline Logs

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, check **Filter Condition** 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.

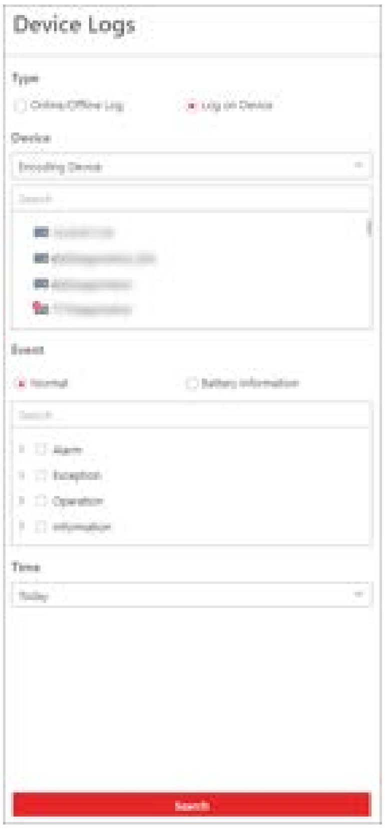
Export Logs Click **Export** and then select a file format (i.e., Excel or CSV) to download the searched logs as a single file to your local PC.

29.4.3 Search for Logs Stored on Device

You can search for the logs stored on encoding devices, security control devices, decoding device, access control devices, elevator control devices, and network transmission devices.

Steps

1. In the top left corner, select ▦ → **All Modules** → **Maintenance** → **System Log** → **Device Logs** .



Device Logs

Type

○ Online/Offline Log ● Log on Device

Device

Encoding Device

Search

Event

● Normal ○ Battery Information

Search

□ Alarm

□ Exception

□ Operation

□ Information

Time

Today

Search

Figure 29-16 Search for Logs Stored on Device

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**.

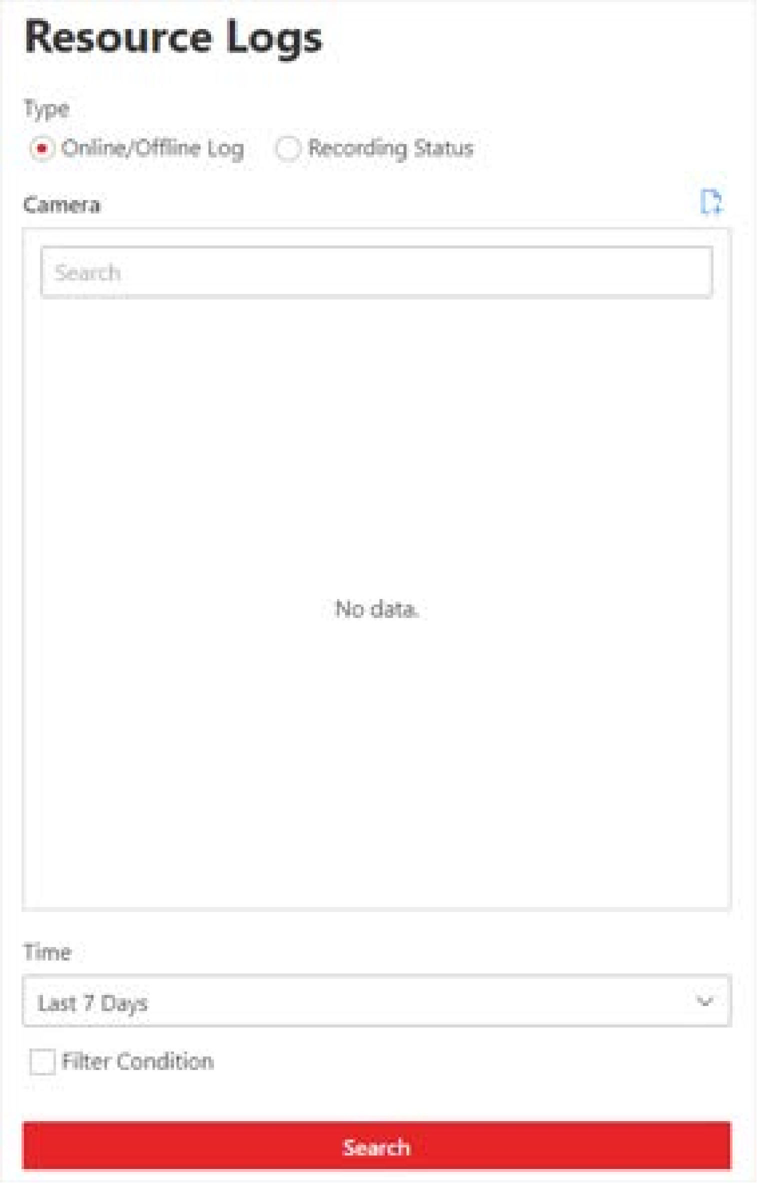
   All matched logs are listed with details on the right.
7. **Optional:** Click **Export** and then select a file format (i.e., Excel or CSV) to download the searched logs as a single file to your local PC.

29.4.4 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. In the top left corner, select ▦ → **All Modules** → **Maintenance** → **System Log** → **Resource Logs** .



Resource Logs

Type

● Online/Offline Log ○ Recording Status

Camera

Search

No data.

Time

Last 7 Days

□ Filter Condition

Figure 29-17 Search for Resource Online/Offline 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 resources, check **Filter Condition** to set a range of total offline times during the specified time range to filter the resources.
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.

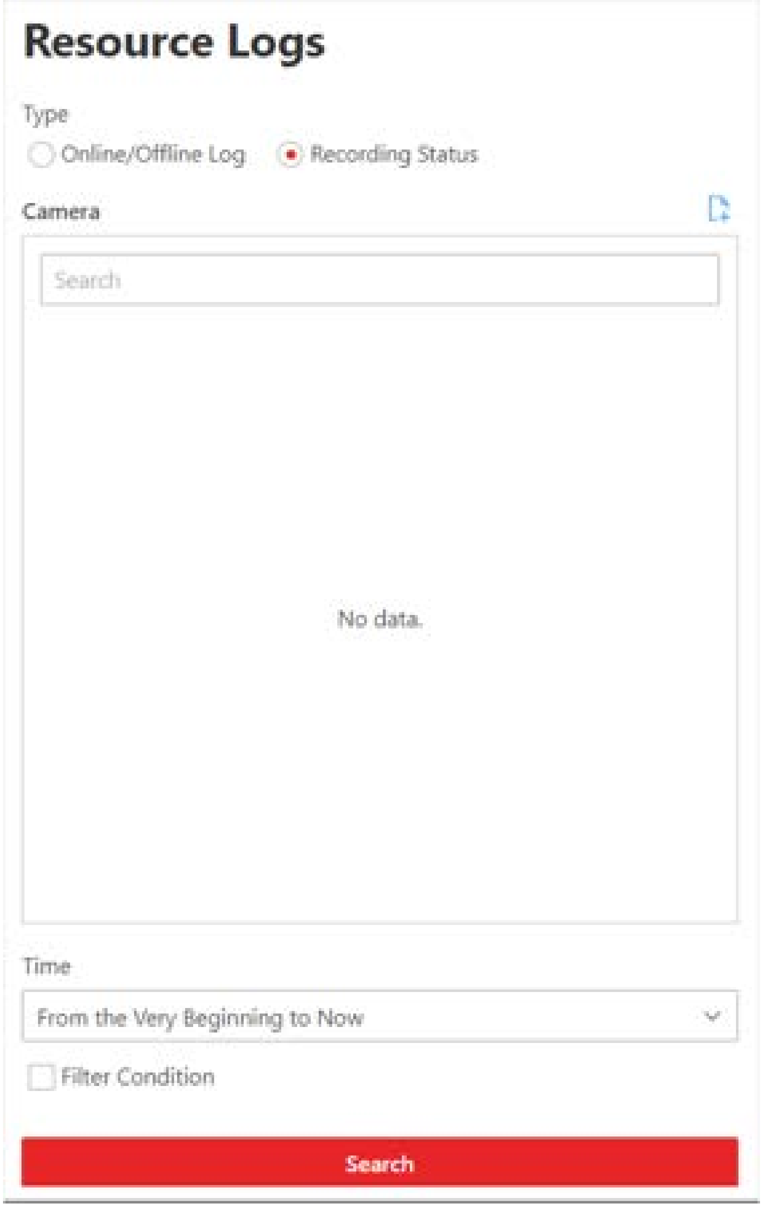
   Export Logs
   Click **Export** and then select a file format (i.e., Excel or CSV)to download the searched logs as a single file to your local PC.

29.4.5 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. In the top left corner of the Client, select 🟥 → **All Modules** → **Maintenance** → **System Log** → **Resource Logs** .



Resource Logs

Type

○ Online/Offline Log ● Recording Status

Camera 🗋

Search

No data.

Time

From the Very Beginning to Now

□ Filter Condition

Search

Figure 29-18 Search for Resource Recording Status

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

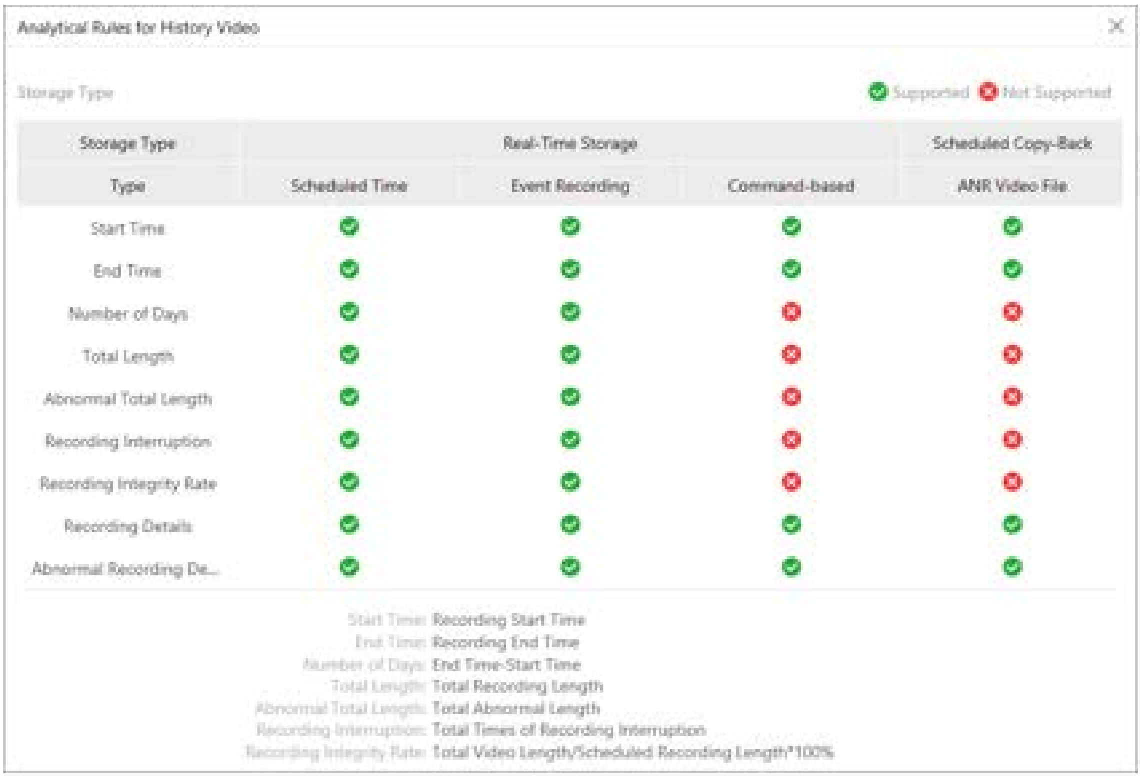
   The total time length of the video loss within the scheduled time.

   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

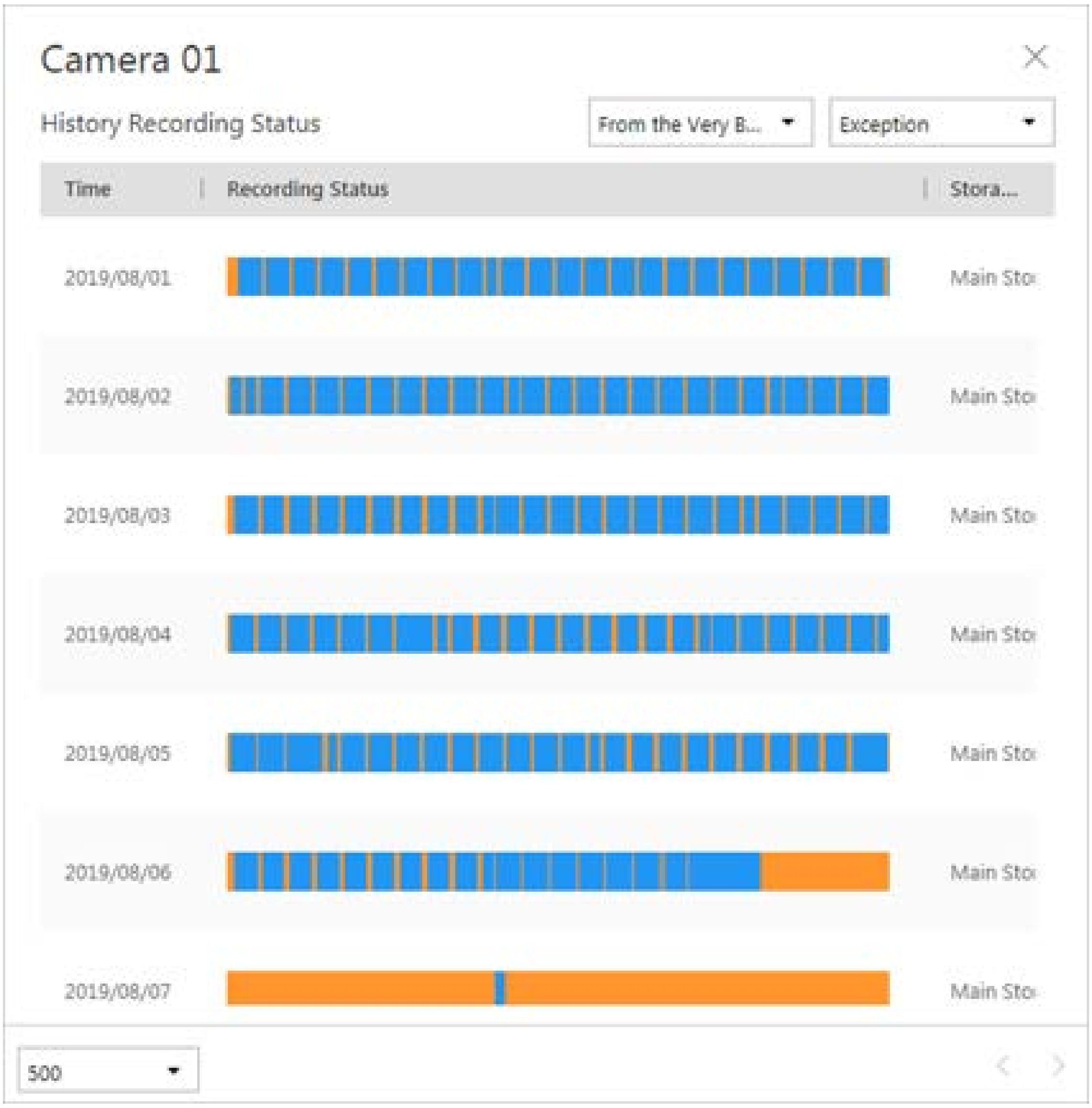
✓ Supported ✗ Not Supported

Storage Type	Real-Time Storage			Scheduled Copy-Back
Type	Scheduled Time	Event Recording	Command-based	ANR Video File
Start Time	✓	✓	✓	✓
End Time	✓	✓	✓	✓
Number of Days	✓	✓	✗	✗
Total Length	✓	✓	✗	✗
Abnormal Total Length	✓	✓	✗	✗
Recording Interruption	✓	✓	✗	✗
Recording Integrity Rate	✓	✓	✗	✗
Recording Details	✓	✓	✓	✓
Abnormal Recording De...	✓	✓	✓	✓

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 29-19 Analytical Rules for History Video

2) Click a camera name to open the History Recording Status panel.



Camera 01

History Recording Status

From the Very B... ▾ | Exception ▾

Time	Recording Status	Stora...
2019/08/01		Main Sto
2019/08/02		Main Sto
2019/08/03		Main Sto
2019/08/04		Main Sto
2019/08/05		Main Sto
2019/08/06		Main Sto
2019/08/07		Main Sto

500 ▾

Figure 29-20 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 (exception 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.

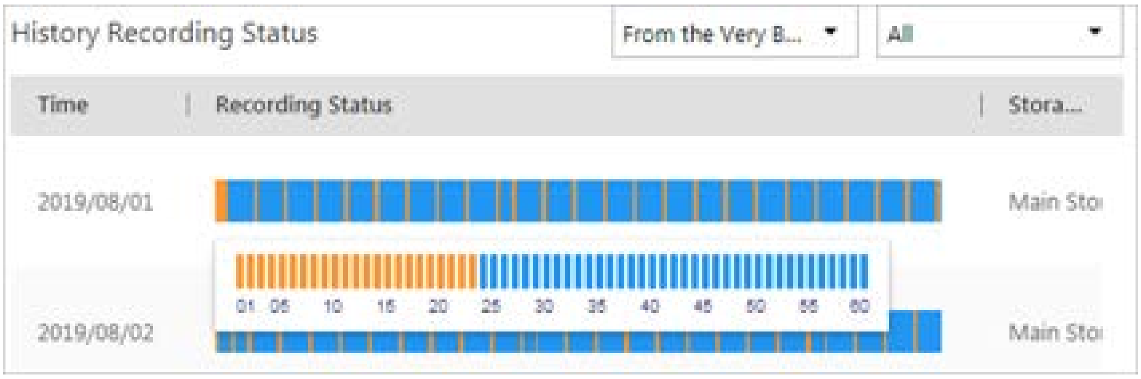


Figure 29-21 Recording Status Details within One Hour

9. **Optional:** Click **Export** and then select a file format (i.e., Excel or CSV) to download the recording status as a single file to your local PC.

29.5 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.

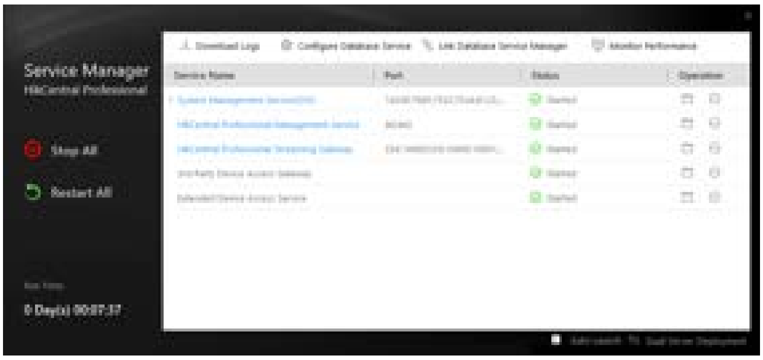


Figure 29-22 Service Manager Main Page

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:** Check **Auto-Launch** to enable launching the Service Manager automatically after the PC started up.
4. Click ■ **Dual-Server Deployment** to deploy the database on another server.

29.6 Set System Data Backup

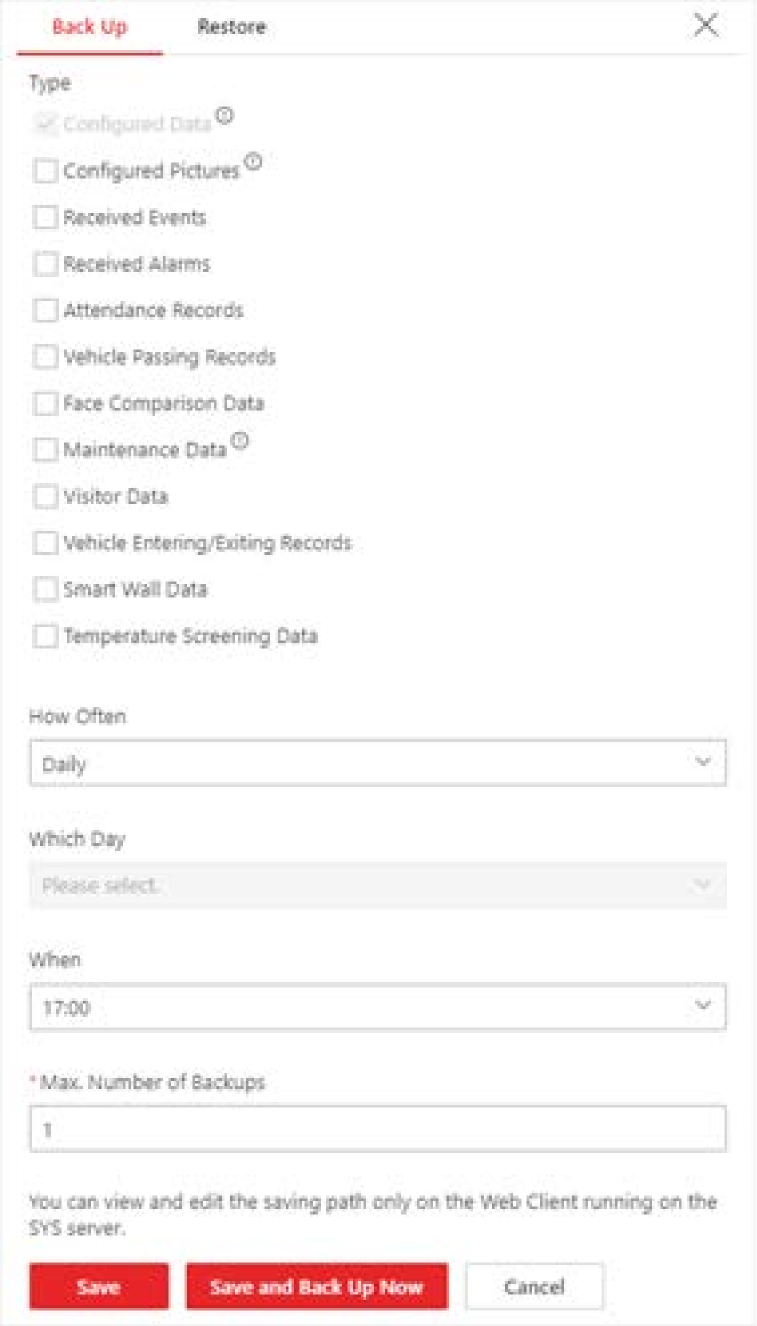
For purpose of restoring the original system data after a data loss event or recovering data from an earlier time, you can manually back up system data, or configure a schedule to back up regularly. System data includes data configured in the system, pictures, received events and alarms, face comparison data, card swiping data, maintenance data, etc.

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.



Back Up Restore

Type

☑ Configured Data

□ Configured Pictures

□ Received Events

□ Received Alarms

□ Attendance Records

□ Vehicle Passing Records

□ Face Comparison Data

□ Maintenance Data

□ Visitor Data

□ Vehicle Entering/Exiting Records

□ Smart Wall Data

□ Temperature Screening Data

How Often: Daily

Which Day: Please select.

When: 17:00

* Max. Number of Backups: 1

You can view and edit the saving path only on the Web Client running on the SYS server.

Figure 29-23 Set System Data Backup

3. In **Type**, select the system data that you want to back up.

   Configured Data

   Data configured via the Web Client, including resources, user permissions, etc. It is selected by default.

   Configured Pictures

Pictures uploaded when configuring maps, persons, vehicles, etc.

Maintenance Data

Maintenance data includes received events/alarms, attendance records, visitor data, etc.

Note

- Person access records are the access records on the card readers of doors with credentials.
- Device recorded data includes the data recorded by the access control devices, elevator control devices, video intercom devices and alarm inputs of these devices, and other records except access records on the doors.

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** if you need to back up the system data immediately.

29.7 Restore System Data

When an exception occurs, you can restore the system data if you have backed up system data before.

Before You Start

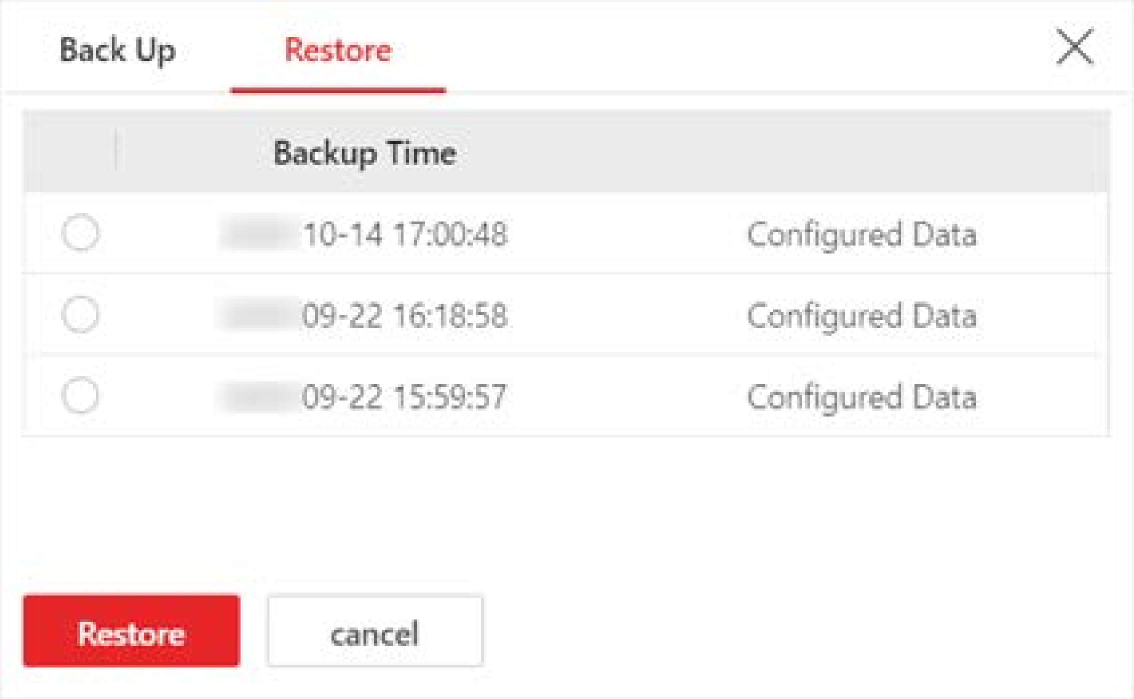
Make sure you have backed up system data. Refer to ***Set System Data Backup*** for details.

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 client, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Restore** tab.
3. Select a backup file to be restored.



	Backup Time	
○	[redacted]10-14 17:00:48	Configured Data
○	[redacted]09-22 16:18:58	Configured Data
○	[redacted]09-22 15:59:57	Configured Data

Figure 29-24 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.

29.8 Export Configuration File

You can export and save configuration data to local disk, including remote site configurations, 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.
3. Click **Export** to download the data to the local PC.

Note

The configuration data file is in CSV format.

Chapter 30 Evidence Management Center

In the Evidence Management Center, you can manage evidence and the unlinked files (including pictures, videos, audios and other files), which contain important information about incidents such as traffic accidents and violent crimes in case of the need for settling disputes or legal cases.

30.1 Basic Settings

You can set the storage location for evidence and set custom items to define the evidence type, on-site organization, and result/conclusion, all of which containing the information about evidence. This configuration will affect the functionality of evidence management on the Client.

In the top left corner of the Client, select 🟥 → **All Modules → Evidence Management Center → Basic Settings** .

Storage Location

Set the storage location to **Local Storage** or **SFTP**.

Note

- If **SFTP** is selected as the storage location, the following fields are required: address, port, user name, and password.
- If **Local Storage** is selected as the storage location, you can select the local resource pool.

Evidence Type

You can add or delete the type of accident or criminal incident recorded in the evidence, such as theft, robbery, attack, and missing person.

On-Site Organization

You can add or delete the organization or personnel on the site, which is responsible for collecting the evidence of the accident or criminal incident, such as police, ambulance, and fire department.

Result/Conclusion

You can add or delete the result/conclusion of incidents based on the evidence collected from the on-site organization, such as arrested, warned, and injured.

30.2 Add Evidence

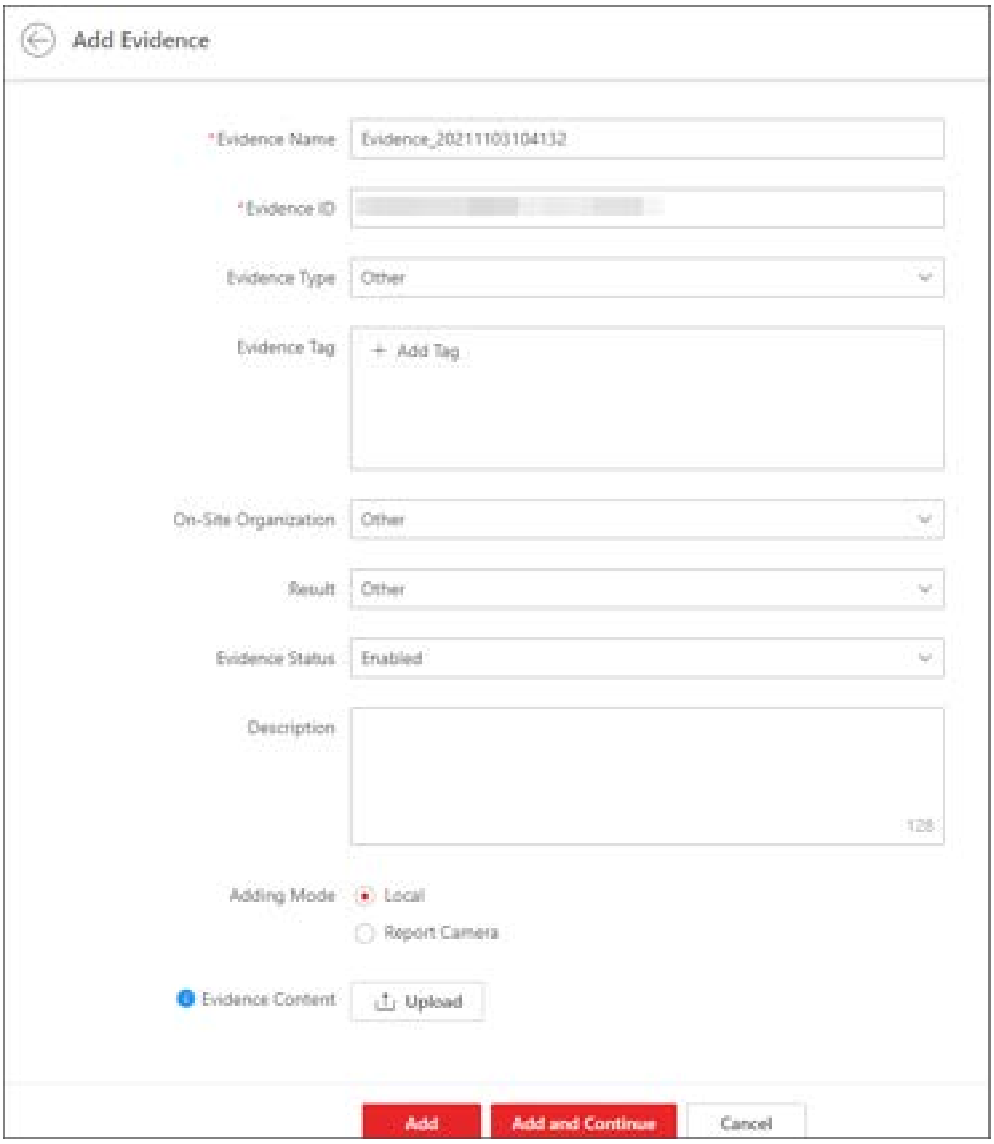
You can add evidence about incidents such as traffic accidents and violent crimes in case of the need for settling disputes or legal cases. You can set detailed information for the added evidence, including the evidence name, ID, type, tag, on-site organization, result/conclusion, and status. Also, you can upload the file (including pictures, audios, videos, Excel file, CSV file, PDF file, and others) as the evidence content from cameras or local PC.

Before You Start

Make sure you have configured basic settings. For details, refer to ***Basic Settings*** .

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Evidence Management Center** → **Evidence** .
2. Select **Evidence Management** on the left.
3. Click **Add** to enter the Add Evidence page.



Add Evidence

*Evidence Name: Evidence_20211103104132

*Evidence ID: [redacted]

Evidence Type: Other

Evidence Tag: + Add Tag

On-Site Organization: Other

Result: Other

Evidence Status: Enabled

Description: 128

Adding Mode: ● Local ○ Report Camera

Evidence Content: Upload

Figure 30-1 Add Evidence

4. Create a name for the evidence.

The evidence ID will be generated automatically on the Client. You can edit the evidence ID which should be 1 to 64 letters or digits.

5. Set the type, tag, on-site organization, result/conclusion, status, or description for the evidence.
6. **Optional:** Set the mode of adding files as the evidence.
   - Select **Local** and click **Upload** to upload files (such as pictures, audios, and videos) from the local PC for the evidence content.
   - Select **Camera**, check cameras in the Linked Camera list, select the uploading mode, and set the corresponding parameters for the selected uploading mode. If you select **Upload at Specified Time**, you should specify the start time and end time of file uploading and recording. If you select **Upload when Wi-Fi Detected**, the files will be automatically uploaded once the Wi-Fi is detected and connected, so you are only required to specify the start time and end time of file recording.

   Note

   When the uploading mode is **Upload when Wi-Fi Detected**, only supports uploading evidence from cameras linked to the same device.
7. Finish adding the evidence.
   - Click **Add** to add the evidence and back to the Evidence Management page.
   - Click **Add and Continue** to save the settings and continue to add other evidence.
8. **Optional:** Perform further operations after adding evidence(s) if needed.

Refresh Evidence
Click **Refresh** to refresh the latest view of evidence list.

View Details and Edit Evidence
Click the evidence name to view the details of evidence's basic information and operation record. You can also edit the basic information of the evidence, such as editing the evidence content, selecting the evidence type, and adding the evidence tag.

Delete Evidence
Select the evidence(s) and click **Delete** to delete the evidence(s).

Filter Evidence
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 evidence.

Enable/Disable Evidence
Click **Disable Evidence** to disable the evidence if the related case is settled, or click **Enable Evidence** to enable the selected evidence if the related-case is pending.

Export Evidence Record
Click **Export** to export the selected evidence record(s) in the Excel, CSV, or PDF format.

Note

You can check **Include Evidence File** to export the attached evidence file.

30.3 Manage Unlinked Files

The unlinked files refer to the files about incidents such as traffic accidents and violent crimes in case of the need for settling disputes or legal cases, but have not been linked with any evidence. You can manage the unlinked files, such as adding and viewing the files by category (pictures, videos, audios, and others). You can also link the added files with the specific evidence.

30.3.1 Add and View Unlinked Files

You can add the files which are unlinked with evidence(s). For the added unlinked file(s), you can perform more operations such as viewing the added files by category, filtering and exporting the unlinked files.

Steps

1. In the top left corner of the Client, select ▦ → **All Modules → Evidence Management Center → Evidence** .
2. Select **File Management** on the left.

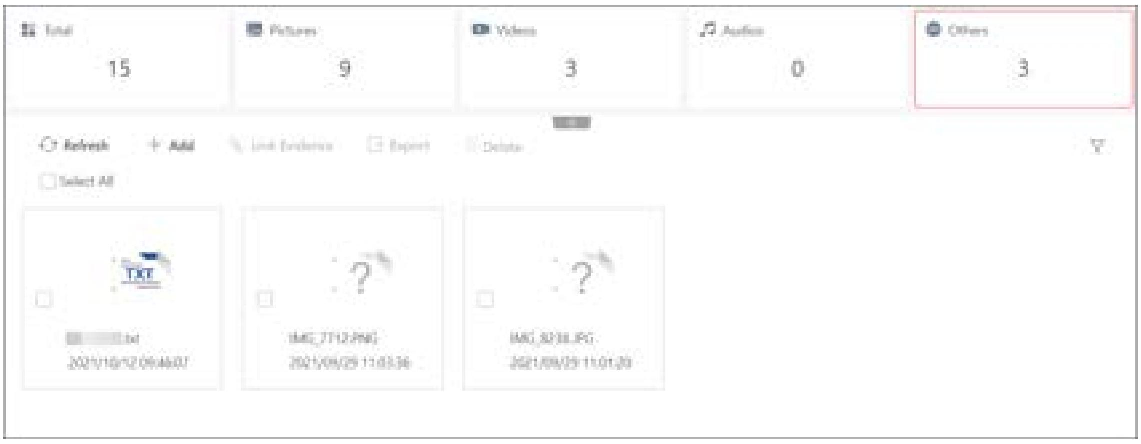


Figure 30-2 File Management Page

3. Click **Add**.
4. Select the pictures, videos, audios, or other files from local PC to add.
5. **Optional:** Perform further operations if needed.

View the Unlinked Files by Category	At the top of File Management page, you can view the total number of unlinked files or the number of categorized files, including pictures, videos, audios, and others. You can also click each category to view all of the corresponding files information, including the file name and uploading time.
Filter the Unlinked Files	Click ▽ in the upper right corner to unfold the filter pane, enter the evidence name in the search box or select the creation time, and then click **Filter** to filter the target evidence.

Refresh the Unlinked Files	You can click **Refresh** to refresh the file list.
Floating Window Display	Hover your cursor on the added picture to view the enlarged picture in a floating window.
Link the Unlinked Files to Evidence	For details, refer to ***Link Files with Evidence*** .
Export the Unlinked Files	Select the unlinked file(s) and click **Export** to export the file(s). **Note** For viewing the file exporting records, refer to ***Manage Operation Records*** .
Delete the Unlinked Files	Select the unlinked file(s) and click **Delete** to delete the selected file(s).

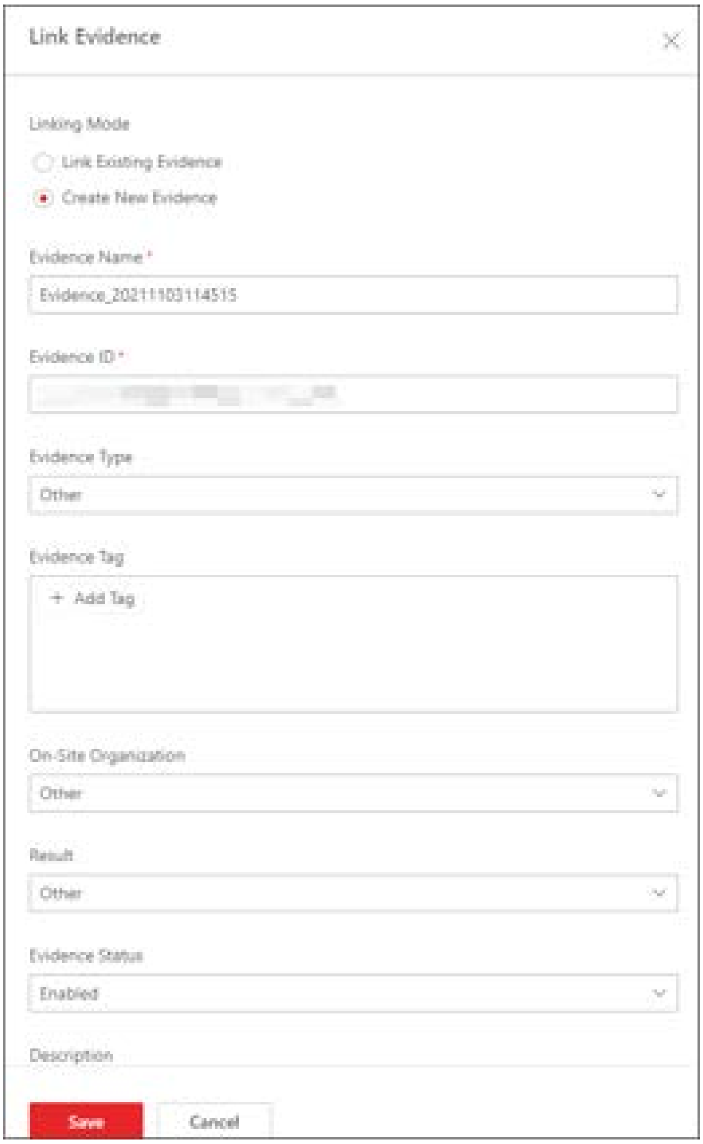
30.3.2 Link Files with Evidence

You can link the added file with the existing evidence or newly added evidence. The linked files recorded in the evidence can be used as materials in case of the need for settling disputes or legal cases.

Before You Start
Make sure you have added the file(s). For details, refer to ***Add and View Unlinked Files*** .

Steps

1. In the top left corner of the Client, select ▦ → **All Modules** → **Evidence Management Center** → **Evidence** → **File Management** .
2. Select the unlinked file(s) in the list.
3. Click **Link Evidence** to enter the Link Evidence pane.



Link Evidence

Linking Mode

○ Link Existing Evidence

● Create New Evidence

Evidence Name *

Evidence_20211103114515

Evidence ID *

[redacted]

Evidence Type

Other

Evidence Tag

On-Site Organization

Other

Result

Other

Evidence Status

Enabled

Description

Figure 30-3 Link Files with Evidence

4. Select the linking mode.
   - Select **Link Existing Evidence** and enter the evidence name/ID/tag/description in the Select Evidence box to select the existing evidence for linking.
   - Select **Create New Evidence** and create a new evidence for linking.

Note

For details about adding evidence, refer to ***Add Evidence*** .

5. Click **Save**.

   The linked files will not be displayed in the list.

30.4 Manage Operation Records

You can manage the evidence operation records, including viewing or deleting the upload/ download records of evidence or files from the local PC or cameras.

In the top left corner of the Client, select ▦ → **All Modules** → **Evidence Management Center** → **Operation Record** .

Upload Record

On the Upload Record page,you can view the records (including evidence or file size and upload status) of the evidence or files uploaded from local PC or related cameras.
You can also search for records by name, check a record and click ⏸ / ▶ / ↻ in the Operation column to pause/start/retry the upload task. Or you can check record(s) and click **Delete** to delete the selected record(s).

Download Record

On the Download Record page, you can view the records ((including evidence or file size and download status) of exporting evidence or files on the platform.
You can also search for records by name, check a record and click ⏸ / ▶ / ↻ in the Operation column to pause/start/retry the download task. Or you can check record(s) and click **Delete** to delete the selected record(s).

Chapter 31 System Configuration

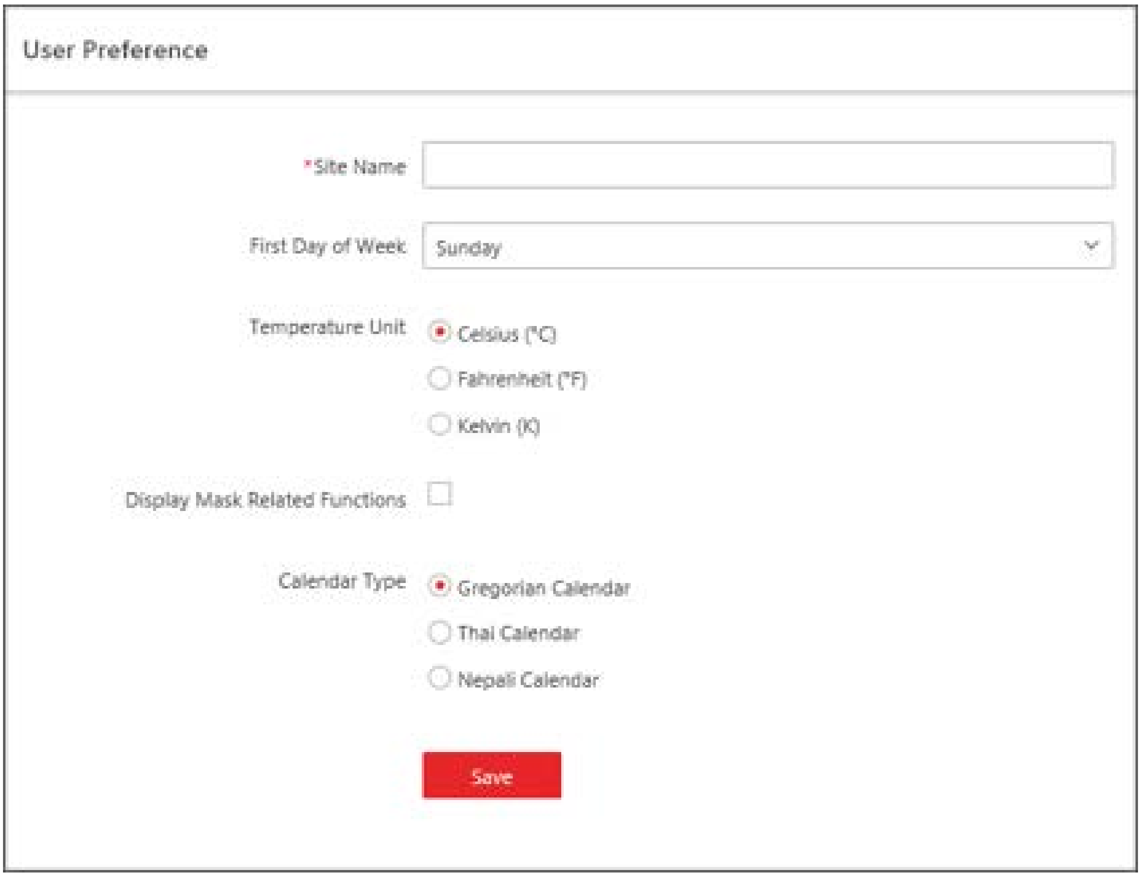
The System page allows you to set basic parameters for the system, such as defining a customized name for your site, setting the WAN IP address for allowing to access your system via WAN (Wide Area Network), and configuring NTP (Network Time Protocol) settings to synchronizing the time between the system and the NTP server.

- For the system with Remote Site Management module, you can enable it to receive the registration from Remote Site.
- For the system without Remote Site Management module, you can set to register it to the Central System as a Remote Site.

31.1 Set User Preference

For different nations, regions, cultures and enterprise backgrounds, the user preference might be different. You can set the user preference according to the actual scene, including the first day of a week and the temperature unit.

In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Normal** → **User Preference** to enter the User Preference page.



User Preference

*Site Name

First Day of Week: Sunday

Temperature Unit: ● Celsius (°C) ○ Fahrenheit (°F) ○ Kelvin (K)

Display Mask Related Functions □

Calendar Type: ● Gregorian Calendar ○ Thai Calendar ○ Nepali Calendar

Figure 31-1 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, attendance settings, 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.

31.2 Set Printer

You can set printer(s) for the system, which can be used to print the stranded person list in some urgent evacuation scenario, such as fire hazard.

Note

Make sure the printer(s) are installed in the same network with the SYS server.

In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Normal** → **Printer Settings** .

Click **Add** to select the printer(s) detected by the HikCentral Professional.

Note

After setting printer(s) for the system, you can link printer when configuring alarm/event whose source type is alarm input. For details, refer to ***Add Event and Alarm*** .

You can also click 🗑 in the Operation column to delete the printer.

31.3 Set NTP

You can set the NTP server for synchronizing the time between the resources (devices managed in the platform, recording servers, sites, SYS, etc.) and the NTP server.

Steps

Note

For devices added via Open Network Video Interface protocol, time synchronization will fail. Please configure the time on the device locally and make sure the device's NTP settings are the same as the platform's.

1. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **NTP** .
2. Switch on **Time Synchronization** to enable the NTP function.
3. Set the NTP server address and NTP port.

   Note

   If the local NTP service has been configured, you can click **Detect Local NTP** to fill in the NTP server address and NTP port automatically.
4. Enter the interval for the automatic time synchronization.
5. **Optional:** Click **Test** to test the communication between the resources and the NTP server.
6. **Optional:** Switch on **Configure WAN Mapping** and enter the IP address and port 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**.

31.4 Set Active Directory

If you have the 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 HikCentral Professional conveniently.

Steps

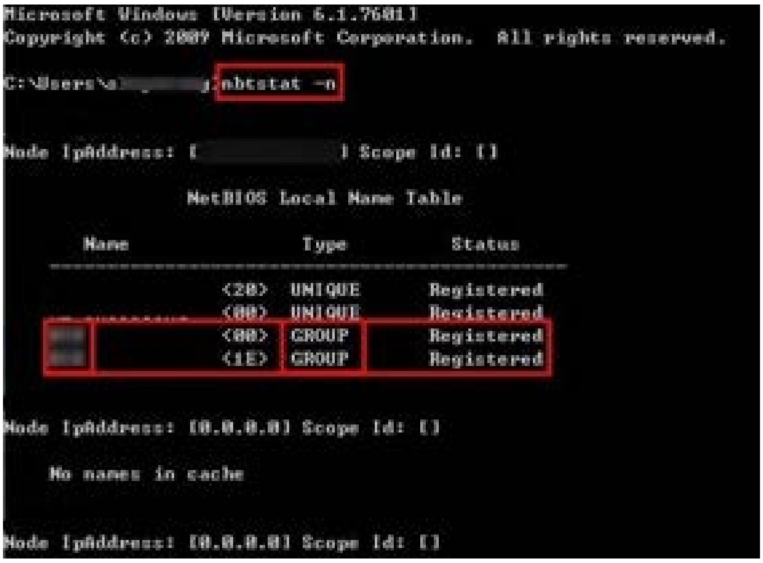
1. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Active Directory** to enter the Active Directory page.
2. Configure the basic information parameters to connect to the AD domain controller.

   Domain Name

   The domain name of the AD domain controller.

   Note

   - HikCentral Professional only supports the NetBIOS format, e.g., TEST\user, instead of the DNS Domain name format.
   - To get the NetBIOS domain name, open the CMD window and enter ***nbtstat – n***. The NetBIOS domain name is the one in **GROUP** type.

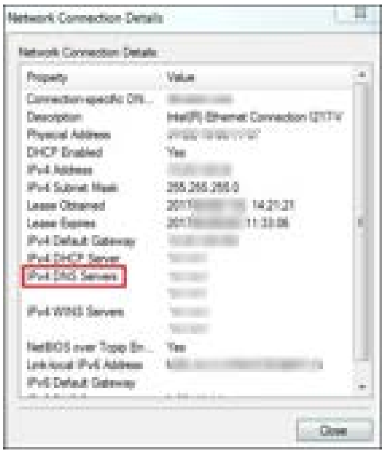


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\[redacted]>nbtstat -n

Node IpAddress: [[redacted]] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
                   <20>  UNIQUE      Registered
    [redacted]     <00>  UNIQUE      Registered
    [redacted]     <00>  GROUP       Registered
    [redacted]     <1E>  GROUP       Registered

Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Node IpAddress: [0.0.0.0] Scope Id: []
```

Figure 31-2 How to Get NetBIOS Domain Name

Host Name

The DNS server's IP address. You can get it in Network Connection Details.



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	[redacted]
Description	Intel(R) Ethernet Connection I217-V
Physical Address	[redacted]
DHCP Enabled	Yes
IPv4 Address	[redacted]
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	2017[redacted] 14:21:21
Lease Expires	2017[redacted] 11:33:06
IPv4 Default Gateway	[redacted]
IPv4 DHCP Server	[redacted]
IPv4 DNS Servers	[redacted]
	[redacted]
IPv4 WINS Servers	[redacted]
	[redacted]
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	[redacted]
IPv6 Default Gateway	

Figure 31-3 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

The user name of the AD domain controller. The user should be the domain administrator.

Password

The password of the AD domain controller.

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. Click **Fetch DN** to have the filter condition entered automatically.
- 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.

3. Set the time to automatically synchronize the users in the AD domain to the platform.
4. **Optional:** Link the person information you are concerned about in the domain to the person information in the system.

   1) Switch on **Linked Person Information**.

   The default and custom additional information items (see ***Customize Additional Information***) are displayed in the Person Information area by default. You can set the relationship for those or add new person information items as needed.

   2) **Optional:** Click **Add New** 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 new person information item is also displayed on the Custom Additional Information page, where you can edit or delete the items. Refer to ***Customize Additional Information*** for details.
   - The person information item is case-sensitive.

   3) **Optional:** Click + to show the person information items stored in the domain.

   4) Check the checkbox in the domain to link it to the added person information item when importing the domain's persons.

   5) **Optional:** Hover over the linked person information in the domain and click × to remove the relationship. You can also change the relationship between each other by clicking and dragging one item to another.
5. Click **Save**.

   After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on the User Management page.

   If the Linked Person Information function is enabled, the corresponding person information in the system will match the linked person information in the domain and cannot be edited.

31.5 Device Access Protocol

Before adding devices supporting ISUP 2.6/4.0 to the system, you need to set the related configuration to allow these devices to access the system.

In the upper-left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** to enter the Device Access Protocol page.

Check **Access via Open Network Video Interface Protocol** when the device is accessed via Open Network Video Interface protocol.

Switch on **Allow ISUP Registration**.

Check **Allow ISUP of Earlier Version**.

Note

The device may be attacked when accessing the system via ISUP of earlier versions.

Click **Save**.

31.6 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 enable it to access the SYS via WAN (Wide Area Network). For example, if the SYS is in a local area network, and you need to visit the platform via the Web Client or Control Client running in WAN, you should enable WAN access and set a static IP address or a domain name and ports for HikCentral Professional.

Steps

1. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Network** → **WAN Access** to enter the WAN Access page.
2. Switch on **Access WAN** to enable the WAN access function.
3. Enter a static IP address or a domain name of the server for WAN access.
4. Set the following ports.

   Client Communication Port

   Used for the Web Client and Control Client to access the platform via HTTP. By default, it is 80.

   Client SSL Communication Port

   Used for the Web Client and Control Client to access the platform via HTTPS. By default, it is 443.

   Real Time Streaming Port

   Used for getting the stream for live view via the Control Client. By default, it is 554.

   Video File Streaming Port

   Used for getting the stream for playback via the Control Client. By default, it is 10000.

Web Client Streaming Port

Used for getting the stream via the Web Client (for the web browser of Google Chrome, Firefox, or Safari). By default, it is 559.

Local Picture Storage Port on Server

Used for storing local pictures on the server. By default, it is 6123.

Local File Picture Storage Port on Server

Used for storing local files on the server. By default, it is 6203.

Broadcast Signaling Port

Used for signaling interaction when getting the stream via the Web Client. By default, it is 7662.

IP Speaker Registration Port

Used for the IP speakers registering to the platform. By default, it is 8877.

IP Speaker Communication Port

Used for the interaction between IP speakers and the platform. By default, it is 10015.

Guidance Terminal Event Port

Used for receiving the events reported by the guidance terminal. By default, it is 8686.

Schedule Releasing Port

Used for releasing schedules. By default, it is 6471.

5. **Optional:** If you adopt generic events to integrate HikCentral Professional with external sources, you need to set the TCP port, UDP port, HTTP port, and HTTPS port for receiving the TCP, UDP, HTTP, and/or HTTPS data packages.

Note

For setting the generic event, refer to ***Configure Generic Event*** .

6. **Optional:** For the platform with a Remote Site Management module, you can set the port to receive the registration from the Remote Site.

Note

This configuration item is only available for the Central System with a Remote Site Management module based on the License you purchased.

7. **Optional:** If you need to manage devices accessed via ISUP, you can set the ports for these ISUP devices, such as the registration port, alarm receiving port, and so on.

Port for Downloading Files from ISUP Devices

Used for downloading files from ISUP devices. By default, it is 8555.

ISUP Registration Port

Used for the ISUP devices registering to the platform. By default, it is 7660.

ISUP Alarm Receiving Port (TCP)

Used for receiving alarms from ISUP devices via TCP. By default, it is 7332.

ISUP Alarm Receiving Port (UCP)

Used for receiving alarms from ISUP devices via UCP. By default, it is 7334.

ISUP Streaming Port (via VAG)

Used for getting the stream from ISUP devices via the VAG server. By default, it is 7661.

ISUP Streaming Port (via Plugin)

Used for getting the stream from ISUP devices via the Plugin. By default, it is 16000.

ISUP Port for Two-Way Audio

Used for two-way audio between the platform and ISUP devices. By default, it is 16001.

Note

If the ISUP ports are disabled on the SYS, the ISUP related ports will not be displayed on the WAN Access page.

8. Click **Save**.

31.7 Set IP Address for Receiving Device Information

You can select the NIC of the current SYS so that the platform can receive the alarm information of the device connected via ISUP account, and to perform live view and playback for the devices connected via ISUP account.

Before You Start

Make sure the server's ports ranging from 8087 to 8097 are available.

Steps

1. In the top left corner of Home page, select ▦ → **All Modules** → **General** → **System Configuration** → **Network** → **Address for Receiving Device Info** .
2. Select **Get from NIC** or **Enter Manually**.

   Get from NIC

   Usually, you can select **Get from NIC** to get IP address from the NIC of SYS.

   Select the currently used NIC name of SYS in the drop-down list. The NIC information including description, MAC address, and IP address will display.

   Enter Manually

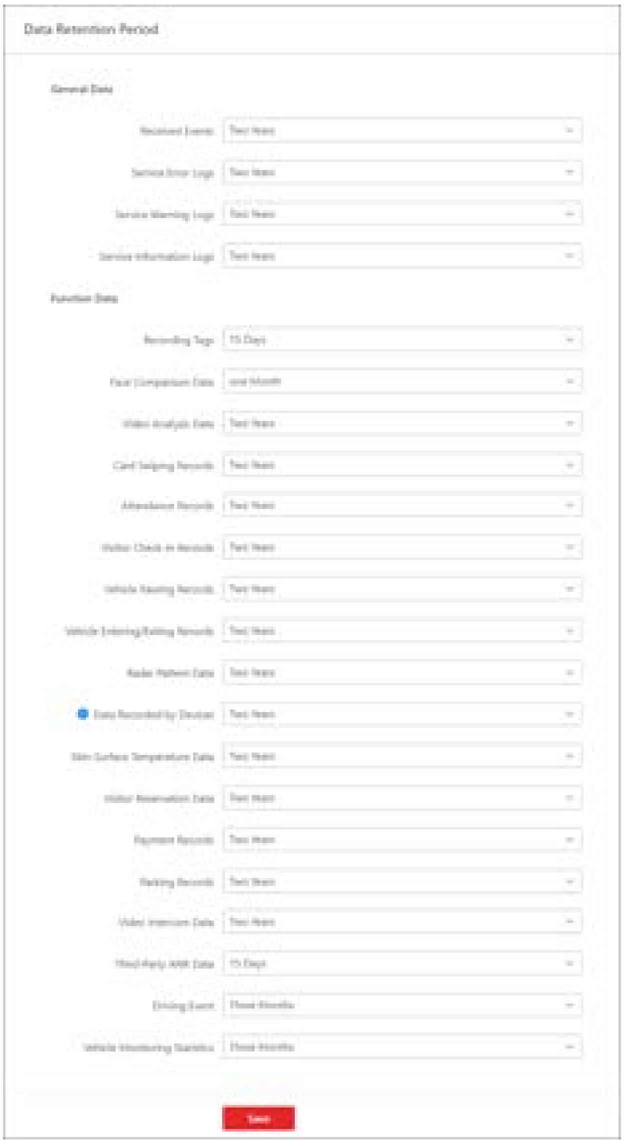
   If you have configured hot spare for the SYS. Manually enter the IP address for receiving device information.
3. Click **Save**.

31.8 Set Data Retention Period

The data retention period specifies how long you can keep the events, logs, and some records in the SYS server, such as recording tags and vehicle entering/exiting records.

Steps

1. In the top-left corner of the Home page, select ▦ → **All Modules** → **General** → **System Configuration** → **Storage** → **Data Retention Period** .
2. Set the data retention period from the drop-down list for the required data types.



Data Retention Period

General Data

Received Events	Two Years
Service Error Logs	Two Years
Service Warning Logs	Two Years
Service Information Logs	Two Years

Function Data

Recording Tags	15 Days
Face Comparison Data	One Month
Video Analysis Data	Two Years
Card Swiping Records	Two Years
Attendance Records	Two Years
Visitor Check-in Records	Two Years
Vehicle Passing Records	Two Years
Vehicle Entering/Exiting Records	Two Years
Radar Pattern Data	Two Years
● Data Recorded by Devices	Two Years
Skin-Surface Temperature Data	Two Years
Visitor Reservation Data	Two Years
Payment Records	Two Years
Parking Records	Two Years
Video Intercom Data	Two Years
Third-Party ANR Data	15 Days
Driving Event	Three Months
Vehicle Monitoring Statistics	Three Months

Figure 31-4 Set Data Retention Period

3. Click **Save**.

31.9 Set Holiday

You can add the holiday to define the special days that can adopt a different shift schedule or access schedule. You can set a regular holiday and an irregular holiday according to the actual scene.

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.

In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Normal** → **Holiday Settings** . Click **Add** to open the adding holiday dialog. Enter the holiday name and select **Regular Holiday** as the holiday type.

Set the parameters according to the following instructions:

Start Date

The start date of the holiday.

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 the VSM server.

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.

In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Normal** → **Holiday Settings** . Click **Add** to open the adding holiday dialog. Enter the holiday name and select **Irregular Holiday** as the holiday type.

Set the parameters according to the following instructions:

Start Date

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 the SYS server.

Note

If you check **Repeat Annually**, the specified date of this holiday will be generated automatically according to the current year of the SYS server.
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**.

31.10 Set Card Template

You can set the styles for card templates. After settings, the card will be applied in the format of the template.

Steps

1. In the top-left corner of the Home page, select → **All Modules** → **General** → **System Configuration** → **Normal** → **Card Template** .
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. You can set the font and the font size for the text after clicking the text field.

   Content
   Check the attribute(s) for the content of the template. You can also click **Customize** to customize the attributes for the template.

   Note

   - You can drag any edge or corner to adjust the size of the picture and text box.
   - You can select one or multiple text boxes on the template and click ≡ , ≡ , or ≡ to adjust the alignment of the text in the box.
   - You can select multiple elements on the template and click , , or to adjust these elements.
   - You can right-click on the element (except the background picture) and click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down** to adjust the layer of the element displayed on the template.

6. **Optional:** Set the back style of the template.

   Note

   You can set the back style according to step 5.

7. Click **Add** to add the template and go back to the card template list page.

   The email template will be displayed on the card template list.
8. **Optional:** Perform the following operation(s).

View Template	Click to view the template.
Edit Template	Click in the Operation column to edit template details.
Delete Template	Click in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

Note

On the card template list page, there are two default templates. You can view default templates but cannot edit or delete them.

31.11 Set Email Template

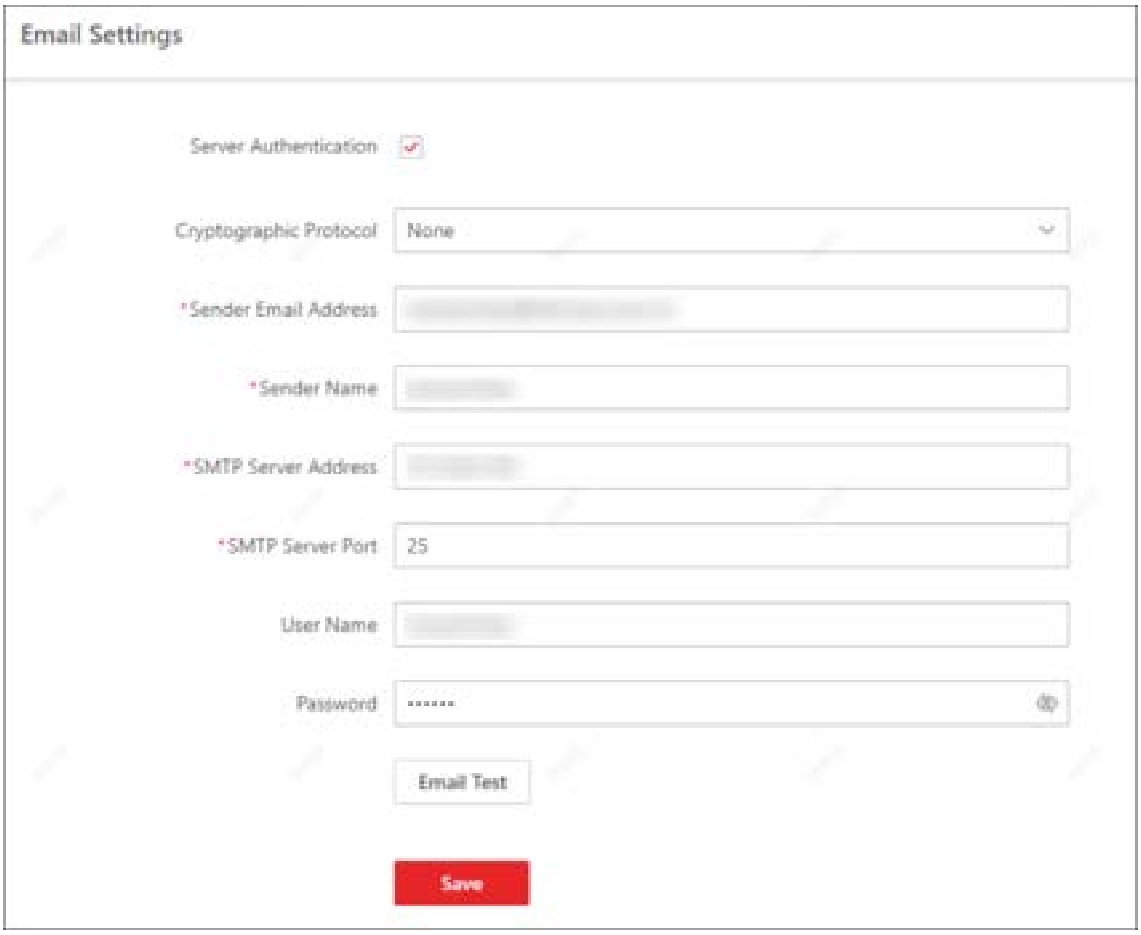
Before sending report or sending event message to the designate email account(s) as email linkage, you should set the email template properly. The email templates include template for sending report and template for sending event message as linkage action when the event is triggered. The email template specifies the recipient, email subject, and content.

31.11.1 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. In the top-left corner of the Home page, select → **All Modules** → **General** → **System Configuration** → **Email** → **Email Settings** .



Email Settings

Server Authentication ☑

Cryptographic Protocol: None

*Sender Email Address

*Sender Name

*SMTP Server Address

*SMTP Server Port: 25

User Name

Password: ••••••

Figure 31-5 Email Settings

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.

3. Click **Email Test** to test whether the email settings work or not.

   The corresponding attention message box will pop up.
4. Click **Save**.

31.11.2 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

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. In the top-left corner of the Home page, select 🟥 → **All Modules → General → System Configuration → Email → Report Email Template** .
2. Click **Add** to enter the Add Email Template page.
3. Enter the required parameters.

Name

Create a name for the template.

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 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 the report content to be sent. You can also click buttons above the **Email Content** parameter to add the related information to the content.

Note

If you add the time period 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.

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:** Perform the following operation(s) after adding the email template:

Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click 🗑 in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

31.11.3 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

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. In the top of top left corner of Home page, select ▦ → **All Modules** → **General** → **System Configuration** → **Email** → **Event and Alarm Email Template** .
2. Click **Add** to enter the Add Email Template page.
3. Enter the required parameters.

   Name

   Create a name for the template.

   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** to send email with image attachment.
5. Select a content language to define the language of the sent content.
6. 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 on the email template list.
7. Perform the following operation(s) after adding the email template:

Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click 🗑 in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

31.12 Set Transfer Protocol

You can set the SYS server's transfer protocol to define the access mode for the SYS (via Web Client, Control Client, or Mobile Client) as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Steps

1. In the top left corner of Home page, select ☰ → **All Modules** → **General** → **System Configuration** → **Security** → **Transfer Protocol** .
2. In the **Clients and SYS Transfer** field, select **HTTP** or **HTTPS** as the transfer protocol between the clients (Web Client, Control Client, and Mobile Client) and the SYS servers.

   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. If you select **HTTPS**, you are required to set the certificate. You can use the system provided certificate, or select **New Certificate** and click … to select a new certificate file.

Note

- The new certificate should be in PEM format.
- The public key and private key should be in the same certificate file.

4. Click **Save**.
   - The SYS server will reboot automatically after changing the clients and SYS server transmission settings.
   - All the users logged in will be forced to log out during reboot. The reboot takes about one minute and after that, the users can log in again.

31.13 Export Service Component Certificate

For data security, before adding the Streaming Server or Cloud Storage Server to the system, you should generate the service component certificate stored in the SYS server and input the certificate information to the Streaming Server you want to add, or export the service component certificate stored in the SYS and import the certificate to the Cloud Storage Server, so that the certificates of the Streaming Server, Cloud Storage Server and SYS server are the same.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Security** → **Service Component Certificate** .
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** beside **Certificate between System and Recording Server** to export the service component certificate in XML format and save it in the local PC.

   Note

   On the Cloud Storage Server you want to add, import the service component certificate you export. For more details, see ***Manage Cloud Storage Server*** .

31.14 Set Database Password

You can set the database password of the system on the Web Client running on the SYS server.

Note

Setting database password is only available when you access the Web Client on the SYS server locally.

In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Security** → **Database Password** .

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

31.15 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 the SYS service, you can enable the hot spare function and configure the hot spare property of the current SYS server 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. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Advanced** → **Hot Spare** .
2. Set the **Hot Spare Configuration** switch to ON to enable the hot spare function.

   The current SYS server's server name and available IP address will be displayed.
3. Set the server as host server or spare server in Hot Spare Property.
4. Click **Save**.

31.16 Set Third-Party Integration

HikCentral Professional supports integrating third-party resources (such as camera, door, etc.) via Optimus. Also, the system provides open platform to integrate the third-party system. By the Open APIs (application programming interface) provided on the open platform, the third-party system can obtain some functions (such live view, playback, alarm, etc.) of HikCentral Professional, to develop more customized features.

In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Third-Party Integration** .

Third-Party Integration

Note

- Setting open platform is only available when you access the Web Client on the SYS server locally.
- Only admin/administrator users have the permission to perform this function.

Switch on the **Integrate via Optimus**.
Configure related parameters in the Optimus software. For details, refer to the *User Manual of Optimus*.
The default icons of resources integrated from the third-party will be displayed. Hover the cursor over the default icon and click Click ✎ to change the resource icons according to your need.

Open Platform

Note

Setting open platform is only available when you access the Web Client on the SYS server locally.

Turn **Open API** to ON, set the IP address of the open platform, management port of the open platform and select the partner user.

Note

- The open platform should be deployed in the same network with the SYS server.
- The third-party system integrates the HikCentral Professional by the partner user(s) you select, which defines the permission(s) of resources and operations in the HikCentral Professional.

Click **Test** to test the service availability of the open platform.
Click **Save** to save the settings.

31.17 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.

31.17.1 Synchronize Card Swiping Records to Third-Party Database

You can enable synchronization function to apply the card swiping records of specified resources from HikCentral Professional to the third-party database automatically.

Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Third-Party Integration** → **Data Interchange** .
2. Switch on **Data Interchange** to enable data interchange function.
3. Click **Add** and select the resource(s) for card swiping records synchronization.

   Note

   You can click 🗑 on Operation column to delete the resource or click **Delete All** to delete all added resources.
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. Select **Notification Time** from the drop-down list to set the synchronization time.

8. Set the required parameters of the third-party database, including server IP address or domain name, server port, database name, user name, and password.
9. Click **Test Connection** to test whether database can be connected.
10. 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.
11. Click **Save**.

    The data will be written to the third-party database.

31.17.2 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. In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Third-Party Integration** → **Data Interchange** .
2. Switch on **Data Interchange** to enable the data interchange function.
3. Click **Add** and select the resource(s) for card swiping records synchronization.

   Note

   You can click in the Operation column to delete the resource or click **Delete All** to delete all added resources.
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 **Access Record Dump**.
7. In the Dump Rule area, click **Add** and set the required parameters.

   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 server. 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 server 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.

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 card swiping records.

Dump Time

The time when dumping card swiping records is started.

8. Click **Add**.

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**.

31.18 Diagnose Remote Fault

When faults occur in HikCentral Professional, you can get the system information using the authentication code generated by HikCentral Professional to help diagnose the system faults.

In the top-left corner of the Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Advanced** → **Diagnosis & Maintenance** to enter the Diagnosis & Maintenance page.

Switch on **Remote Fault Diagnosis** to generate an authentication code for remote diagnosis. It will be canceled automatically after 60 minutes.

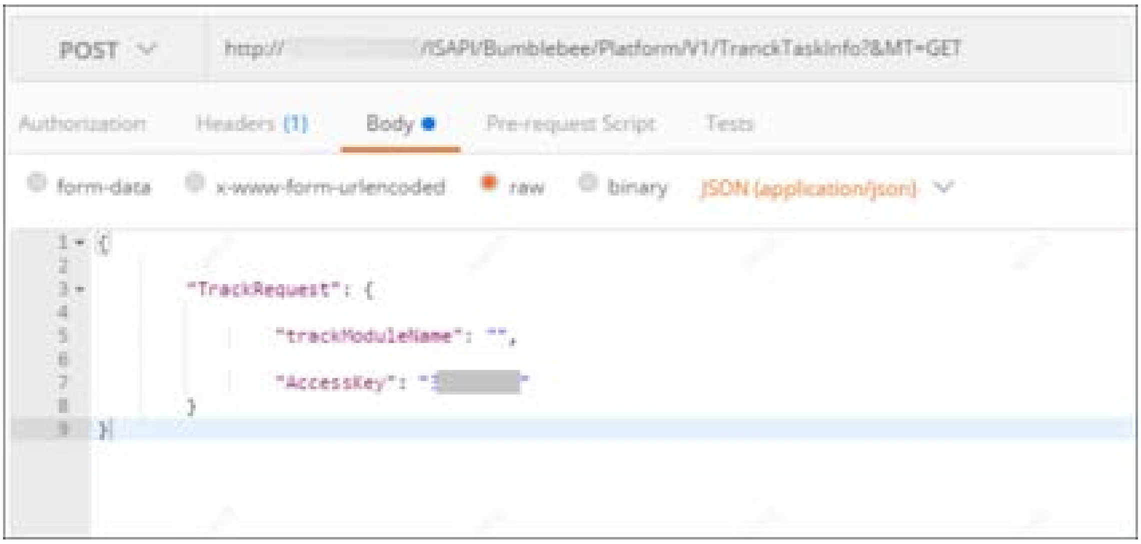
Note

The authentication code will be refreshed every time you switch on **Remote Fault Diagnosis**.

Launch Postman, create a new request, set the HTTP method to POST, and enter the request URL (format: ***http://<host>[:port]/ISAPI/Bumblebee/Platform/V1/TranckTaskInfo?&MT=GET***).

Then in the Body area, enter the request message in JSON format (set the **trackModuleNmae** to the module name and set the **AccessKey** to the authentication code generated on HikCentral Professional), and click **Send**.

The response message is returned in the Body area of Response and it shows the system running information. You can perform fault diagnosis remotely according to the information.



http://[redacted]/ISAPI/Bumblebee/Platform/V1/TranckTaskInfo?&MT=GET

```
{

        "TrackRequest": {

                "trackModuleName": "",

                "AccessKey": "[redacted]"
        }
}
```

Figure 31-6 Get System Running Information Using Postman

31.19 Reset Device Network Information

When system network domain changes (such as server migration), you must reset the network information of the added device to adapt to the new network environment. Otherwise the device live view, playback and other functions will be affected.

Perform this task when you need to reset the network information of the added device.

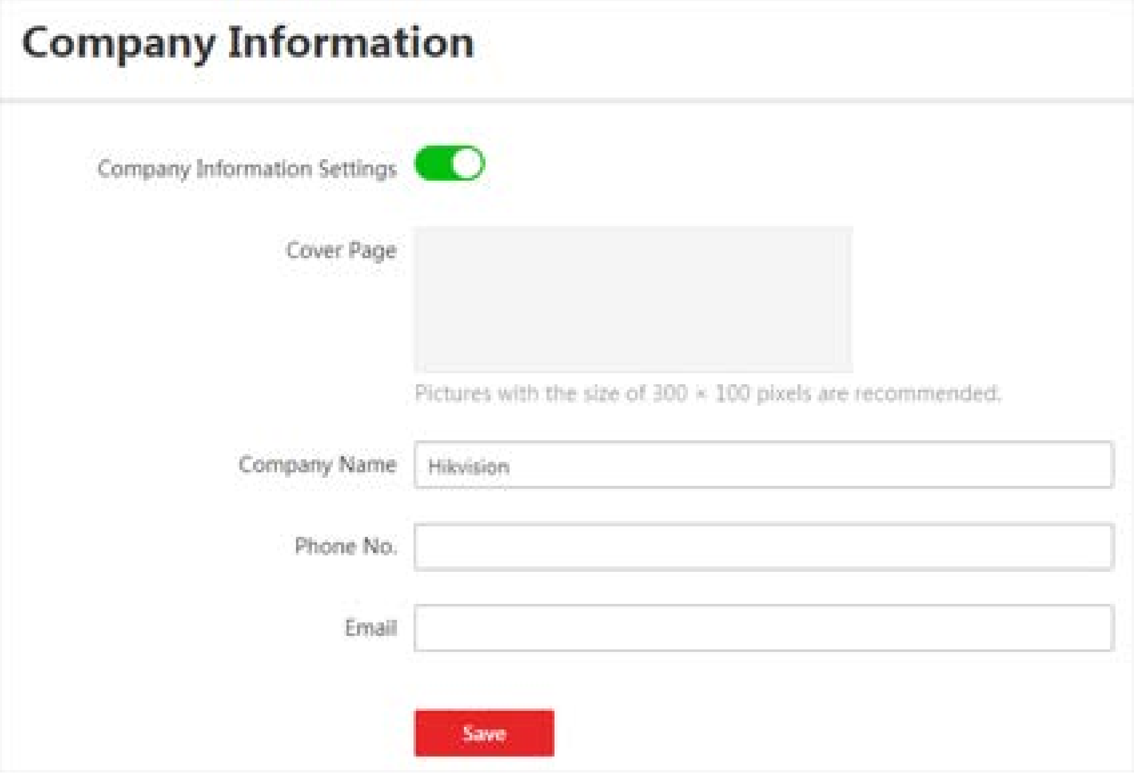
Steps

1. In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Advanced** → **Reset Network Information** .
2. Click **Reset** to one-touch reset the device network information.

31.20 Set Company Information

You can configure and show the company information on the Web Client for customization requirements.

In the top left corner of Home page, select 🟥 → **All Modules** → **General** → **System Configuration** → **Company Information** to enter the Company Information Settings page.



Company Information

Company Information Settings

Cover Page

Pictures with the size of 300 × 100 pixels are recommended.

Company Name: Hikvision

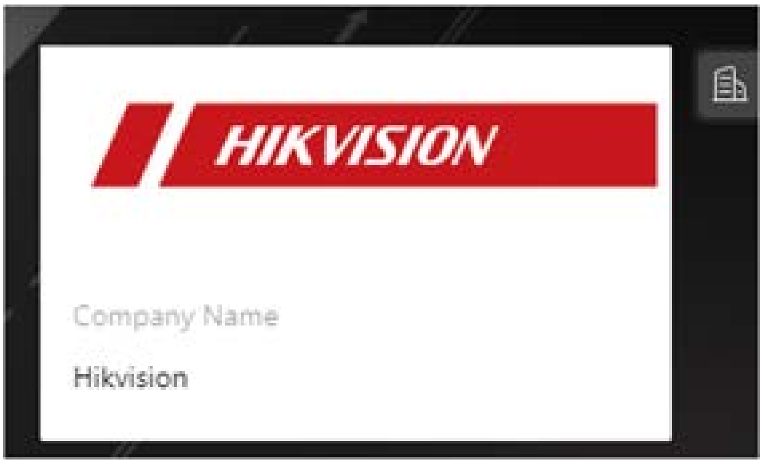
Phone No.

Email

Figure 31-7 Company Information Settings

Switch on **Company Information Settings** to enable displaying company information on the Web Client. And 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.



Company Name

Hikvision

Figure 31-8 Company Information Displayed on Web Client

See Far, Go Further