# 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

# Symbol Conventions

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

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

# Contents

# Chapter 1 About 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 system is developed for central management of surveillance system and features flexibility, scalability high reliability, and powerful functions.

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

**Note**

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

The complete system contains the following modules. You can install the modules according to actual needs.

| Module | Introduction |
| --- | --- |
| System Management Service (SYS) | • Provides the unified authentication service for connecting with the clients and servers.<br>• Provides the central management for the users, roles, permissions, devices, and services.<br>• Provides the configuration interface for surveillance and management module. |
| 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 system.

| Client | Introduction |
| --- | --- |
| Control Client | Control Client is a C/S software which provides multiple operating functionalities, including real-time live view, PTZ control, video playback and downloading, alarm receiving, log query, 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 system via Wi-Fi, 3G, and 4G networks with mobile device. It fulfills the functions of the devices connected to the system, such as live view, remote playback, PTZ control, and so on. |

# Chapter 2 Login

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

## 2.1 Recommended Running Environment

The following is recommended system requirement for running Web Client.

**CPU**

Intel Pentium IV 3.0 GHz and above

**Memory**

1 GB and above

**Video Card**

RADEON X700 Series

**Web Browser**

Internet Explorer® 11 and above, Firefox® 57 and above, Google Chrome® 61 and above, Safari® 11 and above (running on Mac OS X 10.3/10.4), Microsoft® Edge 89 and above.

**Note**

You should run the web browser as 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.

Perform this task when you forgot the user's password.

**Steps**

1. Open the login page.
2. Enter a user name in the User Name field.

**3.** Click **Forgot Password**.

**4.** Set the new password for the user.

- For admin user, enter the activation code, new password, and confirm password in the Reset Password window.
- For normal user, if the email address is set when adding the user and email server is tested successfully, click **Get Code**, and then you will receive an email with the verification code in your email address. Within 10 minutes, enter the received verification code, new password, and confirm password to set the new password for the normal user.

  **Note**

  If the email address is not set for the normal user, contact the admin user to reset the password for you and change the password when login. See ***Reset Password for Normal User*** for details.
- 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.

**5.** 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 or Google Play.

**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 Home page of the Web Client provides an overview of navigation and menu about the function modules. It contains several sections for the modules, such as Navigation, Overview Panel, Map Configuration on Home Page, Wizard, Maintenance and Management, Mode Switch, etc. You can access the modules you want quickly and conveniently via the Home page.

The HikCentral Professional Web Client is composed of the following modules.

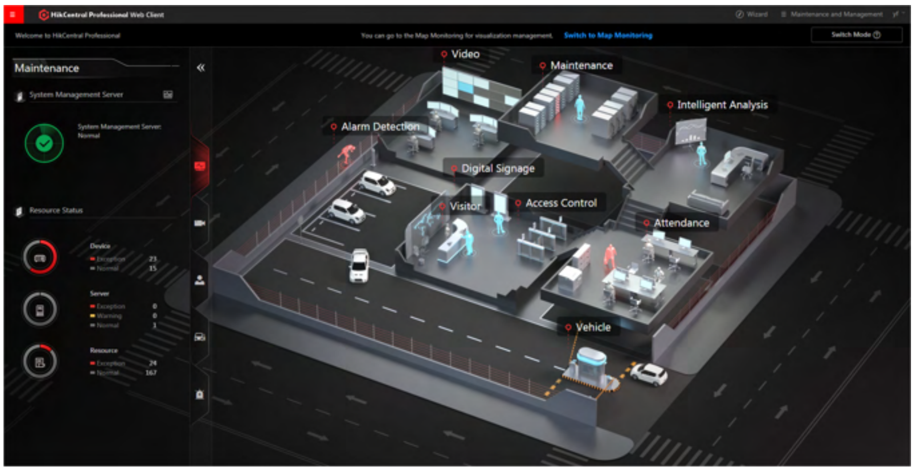



**Figure 5-1 Modules on Home Page**

**Table 5-1 Modules on Home Page**

| Section | Module | Description |
| --- | --- | --- |
| Navigation Icon | | The navigation bar shows the available functions determined by the Licenses you purchased.<br>You can add some frequently used or important modules to the navigation bar for convenient access. See details in ***Customize Navigation Bar*** . |
| Overview Panel | Maintenance | The Maintenance module provides the overview of device network status, service running status, and health checking results.<br>You can refresh to view the real-time service running status.<br>See more details in ***Maintenance*** . |
| | Intelligent Analysis | The Intelligent Analysis module provides the report overview of people feature analysis and people counting.<br>You can refresh to view the real-time analysis and counting results, or export them in different formats. |

| Section | Module | Description |
| --- | --- | --- |
| | | See more details in ***Intelligent Analysis Report*** . |
| | Access Control | The Access Control module provides today's access record statistics, today's access trend, and top 5 of today's abnormal record types.<br>You can refresh to view the real-time trend and top 5 of types, or export them in different formats.<br>See more details in ***Access and Elevator Control Management*** . |
| | Vehicle | The Vehicle module provides the real-time status of parking spaces, today's occupancy rate of parking spaces, and today's parking duration distributions.<br>You can refresh to view the real-time information and export it in different formats.<br>See more details in ***Parking Management*** . |
| | Alarm | The Alarm module provides today's alarm statistics, the last 7 days' alarm trend, top 5 of today's event and alarms, and top 5 of today's alarms in one region.<br>You can refresh to view the trend and top 5 of alarms, or export them in different formats.<br>See more details in ***Event and Alarm Configuration*** . |
| Map Configuration on Home Page | | The default Home page is a navigation map of the Web Client for accessing modules.<br>You can go to the Map Monitoring to configure the map for visualization management as needed. See more details in ***Map Management*** . |
| Wizard | Video | A wizard which guides you through the management and applications of Video. You can also view the flow chart which introduces the video resource management, recording configurations, and video application in ***Flow Chart*** . |
| | 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*** . |
| | Vehicle | A wizard which guides you through the management and applications of Vehicle. You can also view the flow chart |

| Section | Module | Description |
| --- | --- | --- |
| | | which introduces the management of parking lots, vehicles, and entry & exit rules, parking fee rules, parking guidance, and vehicle & record search in ***Flow Chart*** . |
| | 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*** . |
| | 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 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.<br>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.<br>When an exception occurs, you can restore the database if you have backed up the database.<br>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.<br>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. |

| Section | Module | Description |
|---|---|---|
| | | View the License Agreement and Open-Source License Agreement. |
| Home Page Mode Switch | | The Mode Switch module provides four predefined modes of Home page, i.e., Default Mode, System Installation and Management Mode, Security Control and Management Mode, and Attendance Management Mode, for different scenarios.<br>You can also customize the Home page mode as needed.<br>See more details in ***Customize and Switch Home Page Mode*** . |
| Others | Change Password | Change the password of the current user.<br>For more details, refer to ***Change Password of Current User*** . |
| | Logout | Log out of the system and back to the login 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.

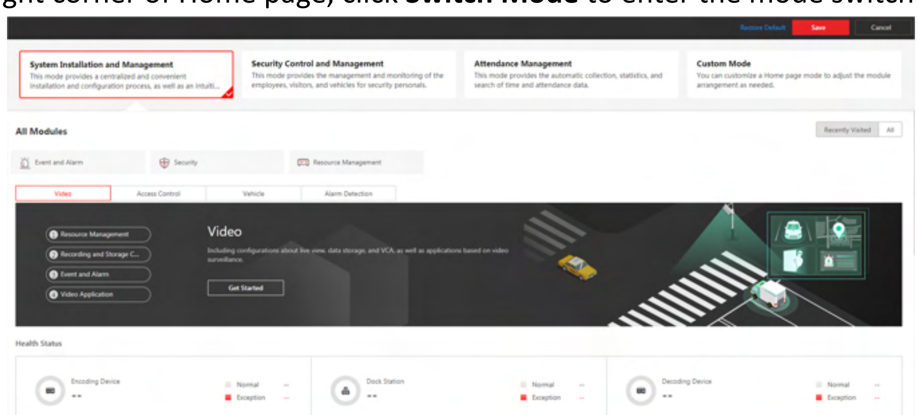



**Figure 5-2 Customize and Switch Home Page Mode**

**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) At the left, click **Custom Mode** to display mode configuration panel.
   2) In the module name field, click + to add module(s) to the mode.

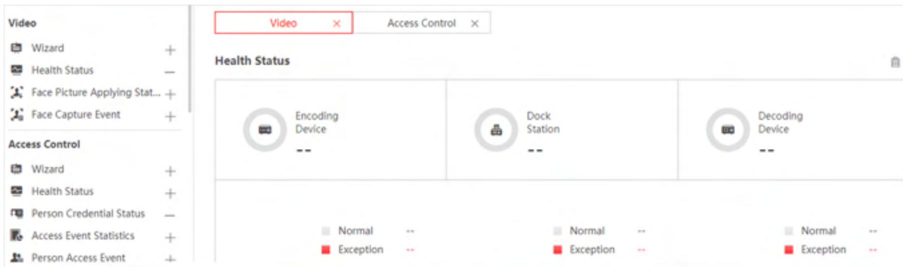



**Figure 5-3 Customize Mode for Home Page**

   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 Home page, select → **All Modules** to display the navigation bar and All Modules panel.

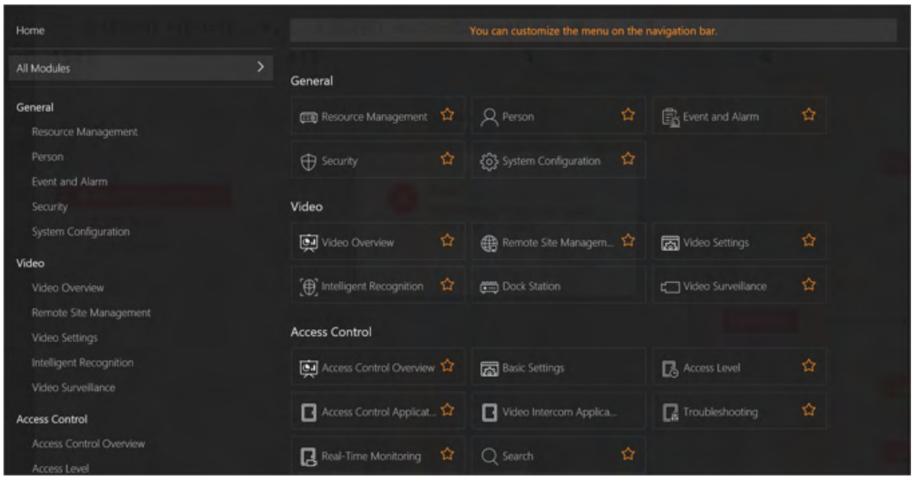



**Figure 5-4 Navigation Bar and All Modules Panel**

**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 system, make sure the devices (camera, DVR, recording server, and so on) 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 connect the devices to the system via network.

**Open Web Client and Login**

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

**Activate License**

Refer to ***License Management*** .

**Add Devices to Platform and Configure Area**

The system can quickly scan your network for relevant devices (camera, DVR, and so on), and add them to your system. 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, and alarm input can trigger linkage actions in the system. Refer to ***Event and Alarm Configuration*** .

**Configure Users**

Specify who should be able to access your system, and how. You can set the different permissions for the users to limit the operation of the system. 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.

**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:** 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.

**7.** Click **Activate**.

## 7.2 Activate License - Offline

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

**Steps**

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

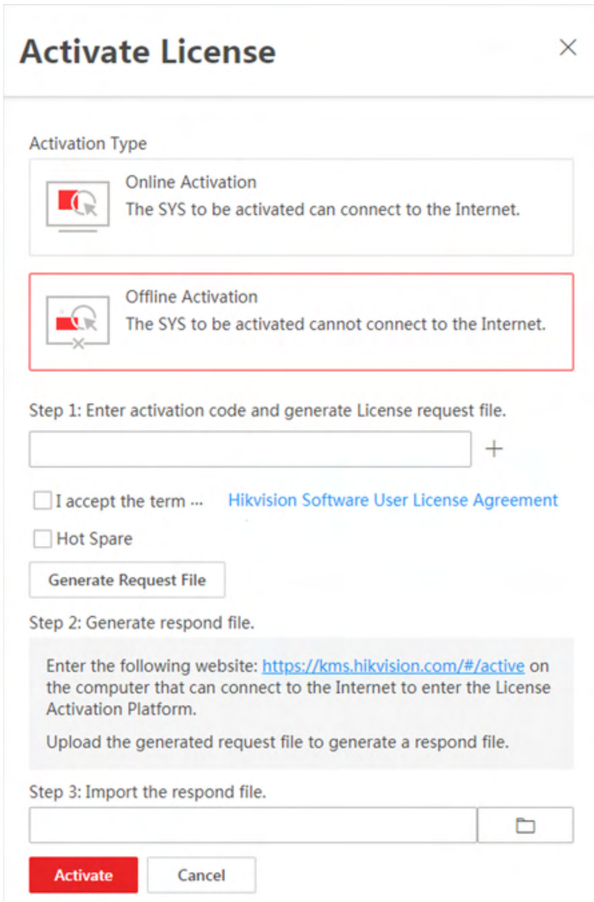



**Figure 7-1 Activate License in Offline Mode**

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:** 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.

7. Click **Generate Request File**.

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

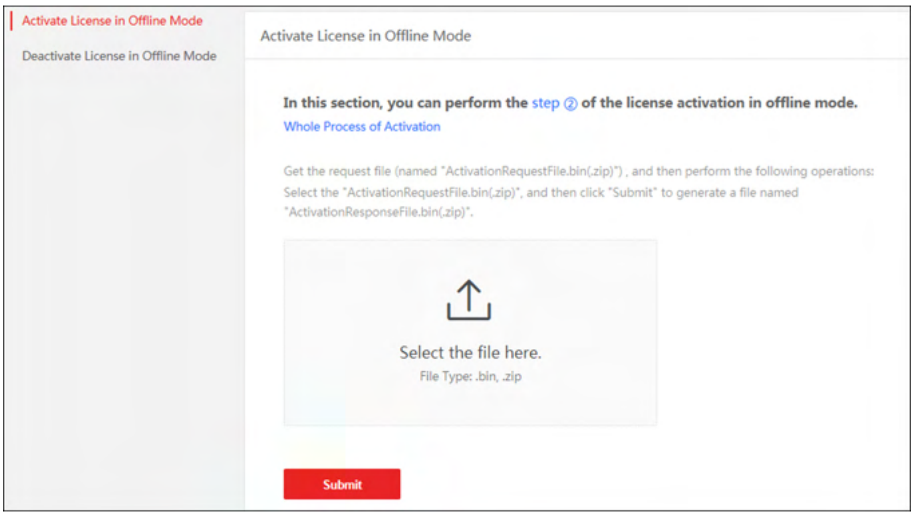



**Figure 7-2 Select Request File**

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 Activation panel, click and select the downloaded respond file.
14. Click **Activate**.

## 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 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 **Offline Update** to update the License in offline mode.

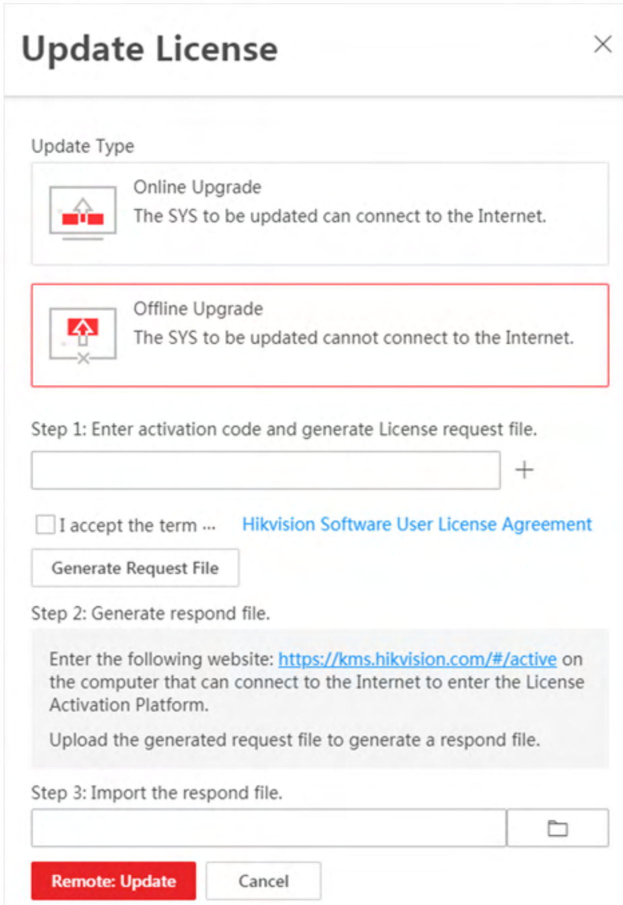



**Figure 7-3 Update License in Offline Mode**

5. Enter the activation code of your additional License.

**Note**

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

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

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

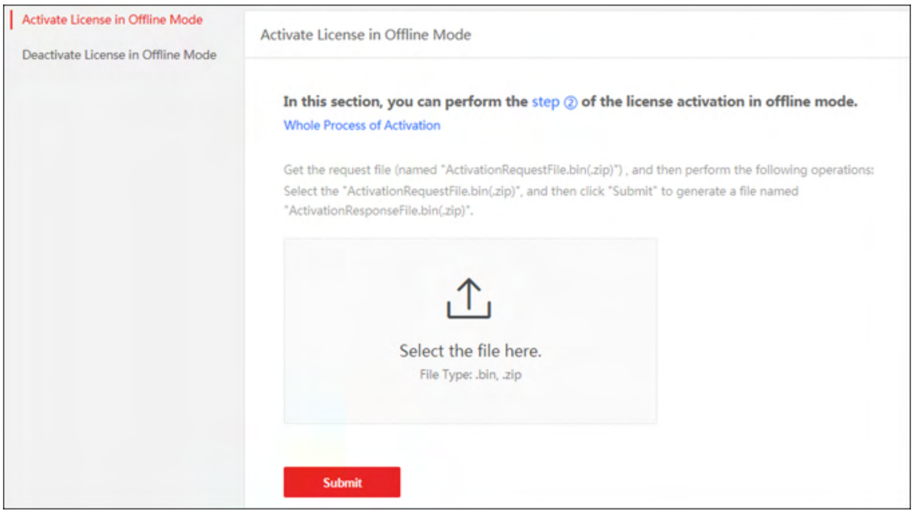



**Figure 7-4 Select Request File**

**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 computer or server, you should deactivate the SYS first and then activate the other SYS again. If the SYS to be deactivated 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 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 **Offline Deactivation** to deactivate the License in offline mode.

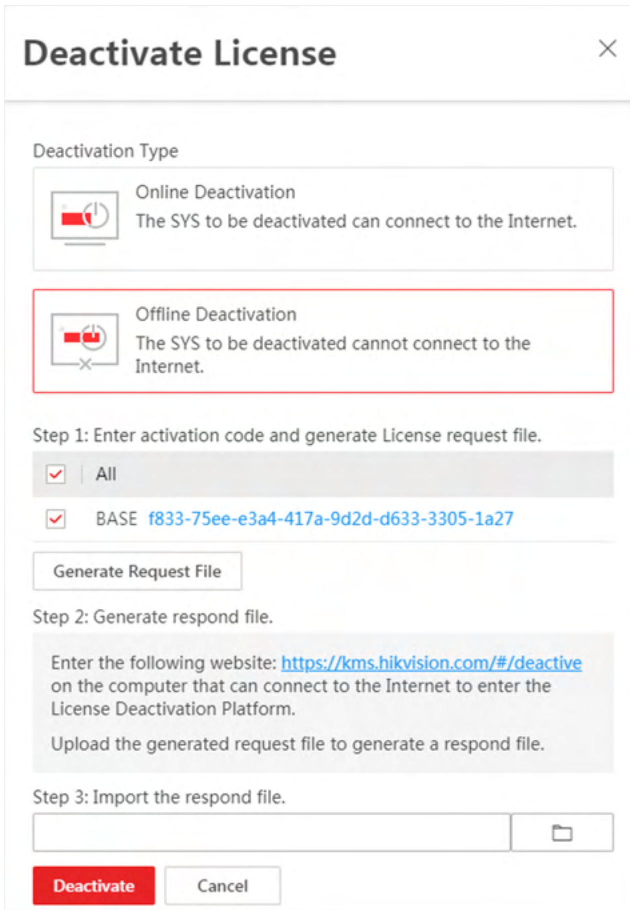



**Figure 7-5 Deactivate License in Offline Mode**

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

**Note**

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

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

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

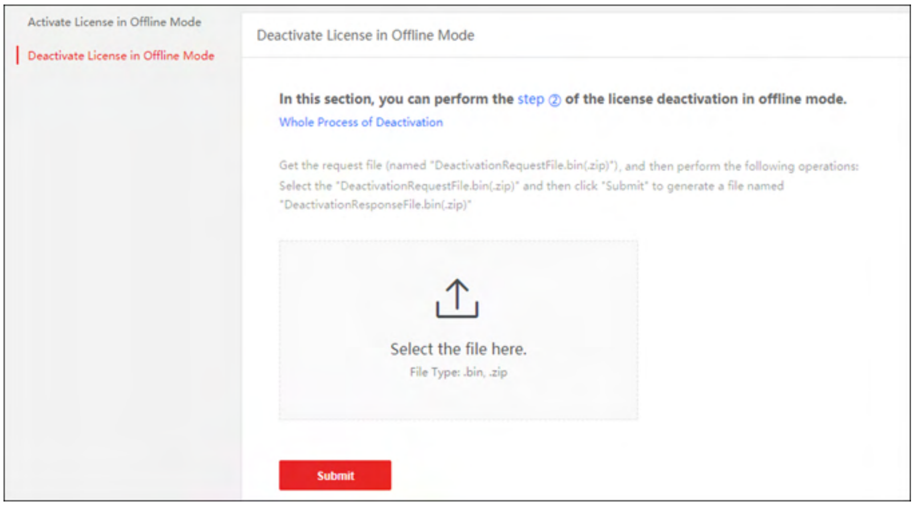



**Figure 7-6 Select Request File**

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 panel, 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.

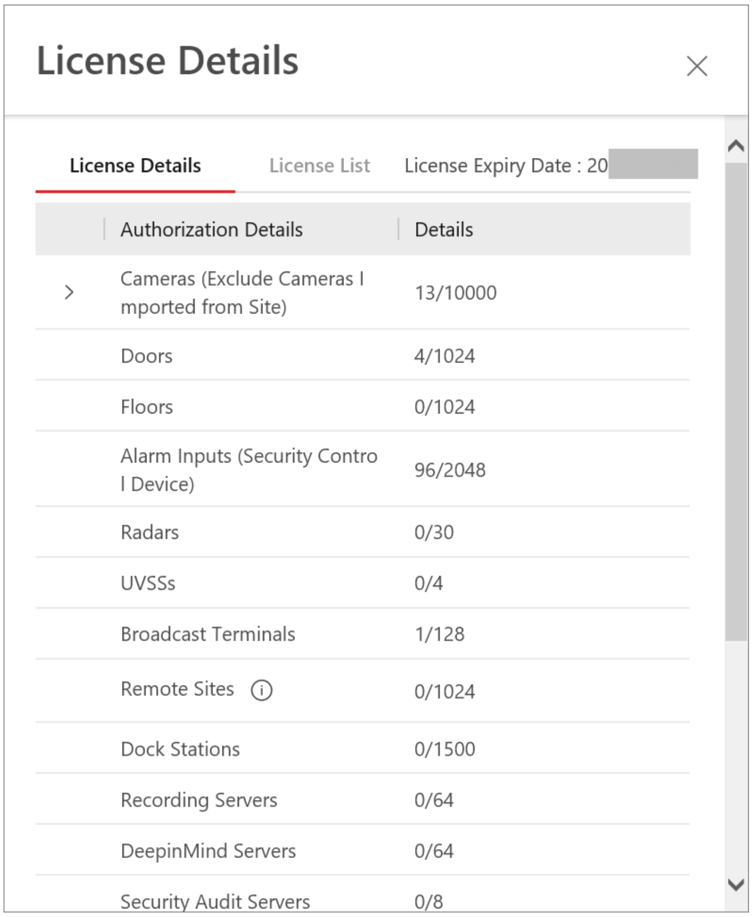



**Figure 7-7 License Details Page**

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 facial recognition cameras/ANPR cameras/thermal cameras (report supported) and click **Configuration** to select the added cameras as these three types of cameras, respectively.

**Note**

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.

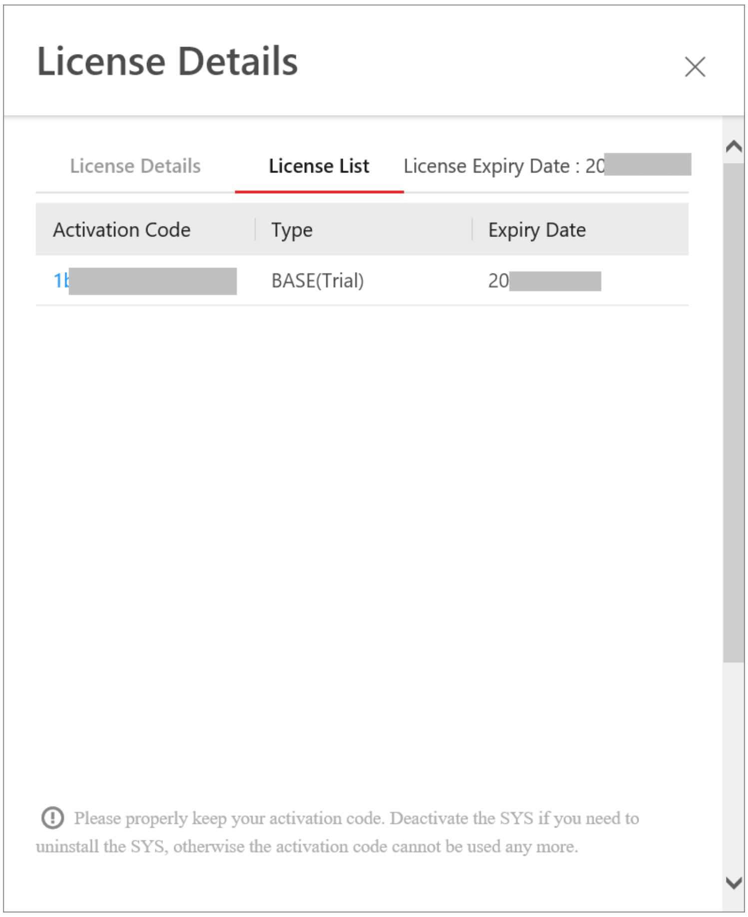



**Figure 7-8 License List Page**

## 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, 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 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.

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**/**ONVIF Protocol** to filter the detected online devices.

   **Note**

   Select **Hikvision Private Protocol**/**Hikvision ISUP Protocol** to add a Hikvision device and select **ONVIF Protocol** to add a third-party device.
   Only if you enable the access via ONVIF/ISUP protocol, can the corresponding devices be displayed. You can click **General → System Configuration → Network → Device Access Protocol** to configure it.
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.
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** in Step 3. If you want to download pictures from the device, switch **Mapped Port** to on and enter the picture downloading port. By default, the port No. is 80.

   **Verify Stream Encryption Key**

   Switch **Verify Stream Encryption Key** to on, 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 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 **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.
10. **Optional:** If you choose to add channels to area, select a Streaming Server to get the video stream of the channels 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.
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. 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 to set the remote configurations of the corresponding device.<br>**Note**<br>For detailed operation steps about remote configuration, see the user manual of the device. |
| **Change Password** | Select the added device(s) and click to change the password for the device(s). |

**Note**

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

**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 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, 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 to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Perform this task when you need to add the detected online devices in a batch.

**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**

   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/ONVIF Protocol** to filter the detected online devices.

**Note**

Select **Hikvision Private Protocol/Hikvision ISUP Protocol** to add Hikvision devices and select **ONVIF Protocol** to add third-party devices.
Only if you enable the access via ONVIF/ISUP protocol, can the corresponding devices be displayed. You can click **General → System Configuration → Network → Device Access Protocol** to configure it.

5. In the Online Device area, check the active devices to be added.
6. Click **Add to Device List** to open the Add Online Device dialog.
7. **Optional:** Switch **Mapped Port** to on 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** in Step 3. By default, the port No. is 80.

8. **Optional:** Switch **Verify Stream Encryption Key** to on, 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**

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 to set the remote configurations of the corresponding device.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |

**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 or Domain Name

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, 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.

**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. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol/ONVIF Protocol** as the Access Protocol.

**Note**

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

5. Select **IP/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**

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. 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.

**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, etc., 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**

You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying 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.
    - 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.

11. 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.
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 to set the remote configurations of the corresponding device.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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, 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.

**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. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol/ONVIF Protocol** as the Access Protocol.

**Note**

Select **Hikvision Private Protocol** to add a Hikvision device, while select **ONVIF Protocol** to add a third-party device.

To display devices which can be added to the platform via ONVIF Protocol, you need to go to → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and check **Access via ONVIF 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 **Add Resource to Area** to on 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, etc., 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**

   You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying 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, etc. 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 to set the remote configurations of the corresponding device.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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, 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.

**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. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol/ONVIF Protocol** as the access protocol.

**Note**

Select **Hikvision Private Protocol** to add Hikvision devices and select **ONVIF Protocol** to add third-party devices.

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

5. Select **Port Segment** as the adding mode.
6. Enter 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 No. and the end port No.

**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 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 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 **Add Resource to Area** to on 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.
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**

   You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when displaying live view on the smart wall.
10. 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.
11. Finish adding the device.
    - Click **Add** to add the devices of which the port No. is between the start port No. and end port No. 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  to set the remote configurations of the corresponding device.<br><br>**Note**<br><br>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).<br><br>**Note**<br><br>• You can only change the password for online HIKVISION devices currently.<br>• 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, 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.

Make sure you have enabled Hik-Connect service for devices to be added on device web page. 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.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol** as the Access Protocol.

5. Select **Hik-Connect DDNS** as the adding mode.
6. **Optional:** Set the **Mapped Port** switch to on 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 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**

   Move your cursor over ⓘ to view details.
8. Enter the required information.

   **Hik-Connect 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 **Verify Stream Encryption Key** to on, 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.

   **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 **Add Resource to Area** to on 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**

    You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying live view on 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 to set the remote configurations of the corresponding device.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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.

### 8.3.6 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.
3. Click **Add** to enter the Add Encoding Device page.
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 ISUP 5.0 to the system, you should enter the key.
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 strorage.

**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:** Select the storage location from the drop-down list.
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 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, etc., for the cameras.
12. **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**

    You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying live view on the smart wall.
13. **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.
14. 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.
15. **Optional:** Perform the following operation(s) after adding the devices.

| | |
|---|---|
| **Remote Configurations** | Click to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the remote configuration, see the user manual of the device. |

| | |
|---|---|
| **Change Password** | Select the added device(s) and click to change the password for the device(s).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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 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 Edit the Device page, and click **Wake Up** to wake the device up. If a device is in sleep mode, the communication between the solar camera and the platform is not supported. |

## 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 a 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.
3. Click **Add** to enter the Add Encoding Device page.
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 ISUP 5.0 protocol to the system, you should enter the key.

7. **Optional:** Switch on **Picture Storage** and set the location for picture strorage.

**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*** .

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 **Add Resource to Area** to on 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, etc., for the cameras.

10. **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**

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:** 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.

**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.

**What to do next**

- If the original device malfunctions, you can replace it with a new device. After you replace it, move the cursor on the icon on the right of the device name, and click **Replace Device** to confirm the replacement.
- After you add a solar camera, the network status will be displayed as offline, online(Asleep), or online(Waked up). You can click the icon in the **Operation** column to wake up an asleep camera. You can also click the the device name to enter the Edit the Device page, and click **Wake Up** to wake the device up. If a device is in sleep mode, the communication between the solar camera and the platform is not supported.

## 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.
3. Click **Add** to enter the Add Encoding Device page.
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 **ONVIF 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 on the corresponding column.

**8.** Click ... and select the edited file.

**9. Optional:** Switch on **Picture Storage** and set the location for picture strorage.

**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 to set the remote configurations of the corresponding device.<br><br>**Note**<br><br>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).<br><br>**Note**<br><br>• You can only change the password for online HIKVISION devices currently.<br>• 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.
- 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 the device name to enter the Edit the Device page, and click **Wake Up** to wake the device up. If a device is in sleep mode, the communication between the solar camera and the platform is not supported.

### 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.<br>**Note**<br>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**.
7. Configure settings for 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.

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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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.<br>**Note**<br>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**.
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

If you know the IP address 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** as the access protocol.
5. Select **IP Address** as the adding mode.
6. Enter the required parameters.

   **Note**

   By default, the device port 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.
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** 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.

   **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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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.<br>**Note**<br>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 the settings icon 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** or **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 **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**<br>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 settings for 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.
   - **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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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.<br>**Note**<br>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 master 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 master 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 master station. It is mainly applied in the community and office buildings.
- **Master Station:** The master 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 Detected Online Video Intercom Devices

The system can perform an automated detection for available video intercom devices (including indoor station, door station, outer door station, and master station) in the same local subnet with the current Web Client or SYS server. You can add one online device at a time to the system by specifying device name, password, device location information, etc.

### Add a Detected Online Indoor Station

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 open the Add Video Intercom Device window.

**6.** Select **Indoor Station** as the device type.

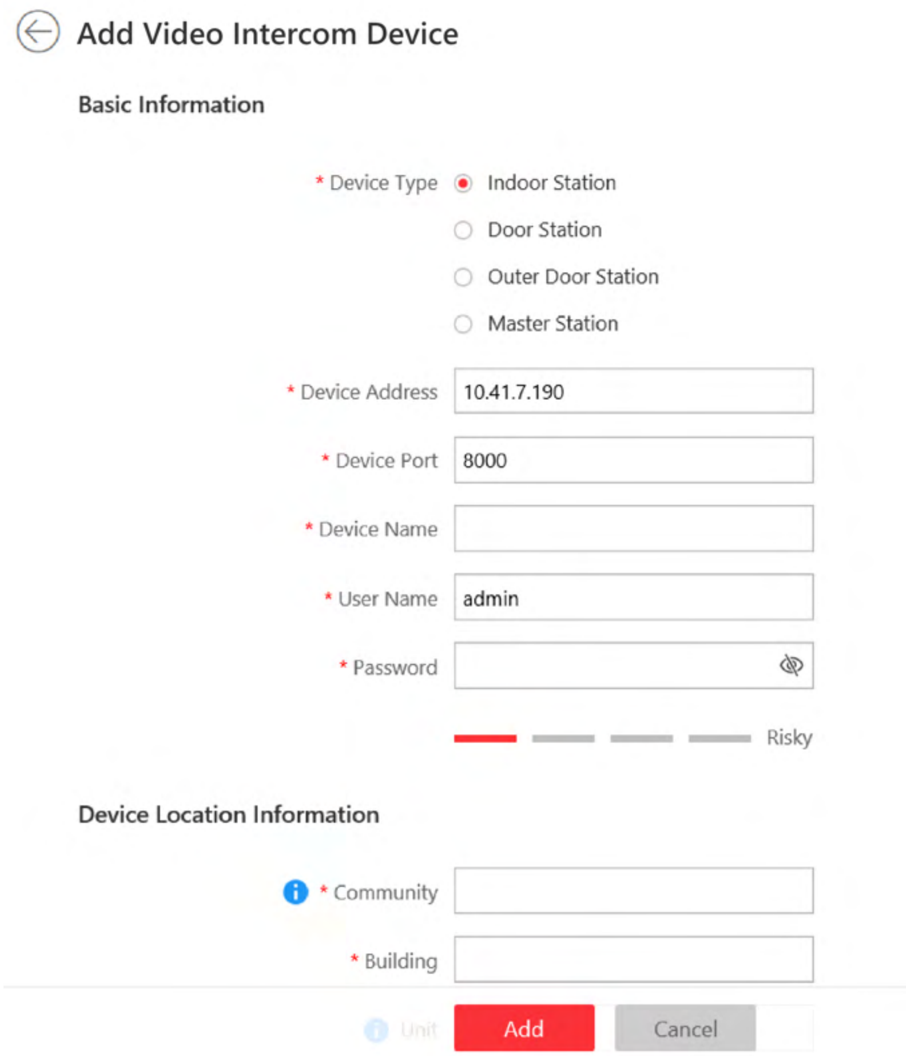



**Figure 8-1 Add Video Intercom Device**

**7.** 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.

8. Set the device location information, including community, building, unit (optional) and room.

**Note**

- You should enter an integer between 101 and 9999 in the **Room** Field. The room is composed of floor No. and room No. For example, for room 2 on the 12th floor, enter 1202.
- For example, if the device is located in community 1, building 2, unit 5, and room 305, you should enter 1, 2, 5, 305 respectively in the corresponding input box.

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 **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.
11. In the Resident Information Area, click to select resident(s) to be linked with the device.

    **Note**

    Up to 10 residents can be linked to the device.
12. **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.

13. Click **Add**.
14. 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).<br><br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| **Add Related Camera** | Click  to relate camera(s) with the added indoor station(s). For details, refer to ***Relate Camera with Indoor Station*** . |
| **Apply Device Settings** | If the parameters in the system are inconsistent with the parameters on the video intercom device(s) after the device location information or device IP address is edited,  will be displayed on the right side of the icon  . Click  to apply the current settings in the system to the device(s). |
| **Restore Default** | Select the added device(s), and click  to restore the configured device parameters.<br><br>**Note**<br>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. |
| **Link Doorbell with Indoor Station** | Click  to link the added doorbell(s) with indoor station(s). For details, refer to ***Relate Doorbell with Indoor Station*** . |
| **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. |

### Add a Detected Online Door Station

The online video intercom devices in the same local subnet with the current Web Client or SYS server can be displayed on the list, and you can add the detected door 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 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 the active device to be added.
5. Click in the Online Device area to open the Add Video Intercom Device window.
6. Select **Door Station** as the device type.

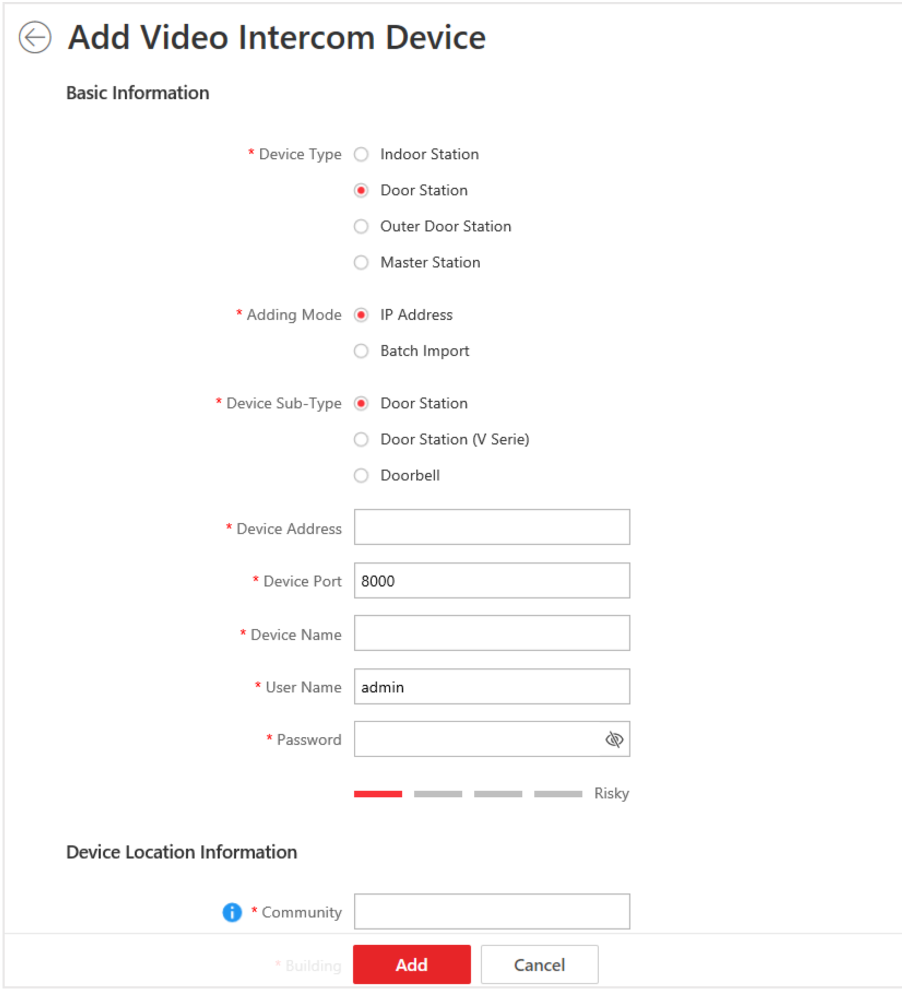



**Figure 8-2 Add Video Intercom Device**

7. Select **Door Station**, **Door Station (V Serie)**, or **Doorbell** as the device sub-type.
8. 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.

**9.** Set the device location information, including community, building and unit (optional).

**Note**

For example, if the device is located in community 1, building 2, unit 5, you should enter 1, 2, 5 respectively in the corresponding input box.

**10. Optional:** Select an indoor station from the drop-down list to link the doorbell with an indoor station.

**Note**

For details, refer to ***Relate Doorbell with Indoor Station*** .

**11. 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.

**12. 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 resources (including cameras and doors) or the specified door 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 such as such as live view, playback, etc., for the cameras.

**13.** Click **Add**.

**14.** 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.

**Apply Device Settings**

In some cases such as you have edited the device location information or device IP address, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon will display on the right side of the . Click to apply the current settings in system to the device(s).

**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.

## Add a Detected Online Outer Door Station

The online video intercom devices on the same local subnet with the current Web Client or SYS server can be displayed on the list, and you can add the detected outer door 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 open the Add Video Intercom Device window.
**6.** Select **Outer Door Station** as the device type.

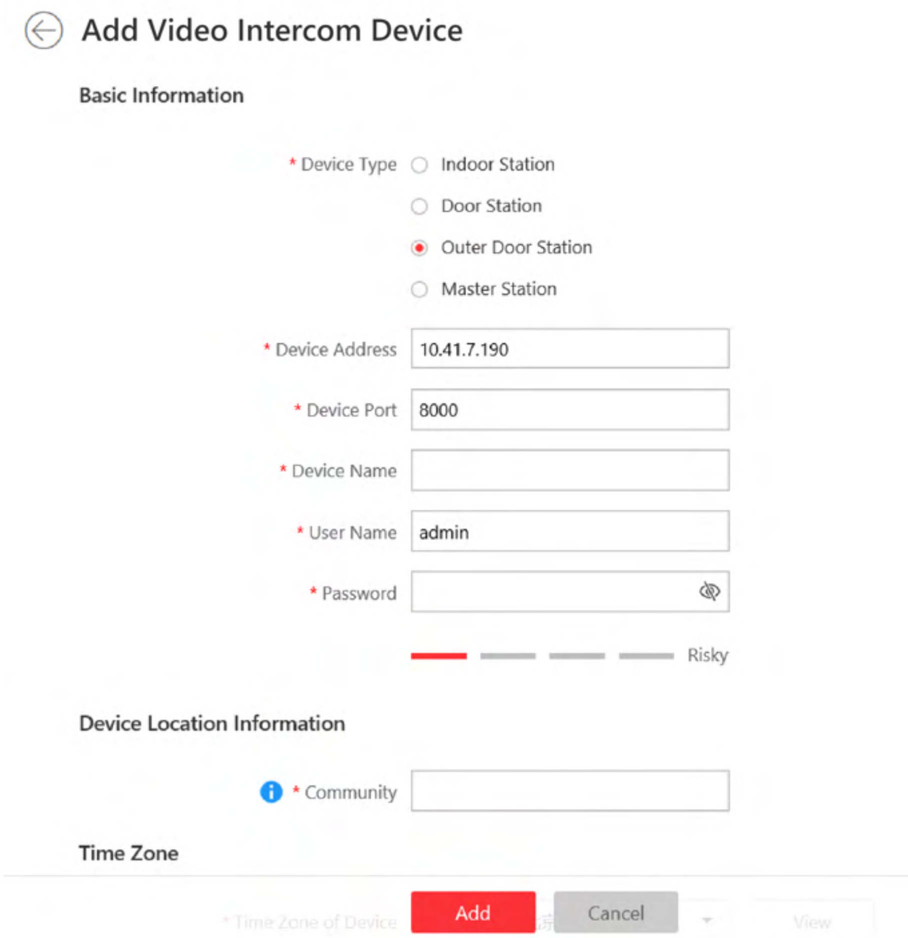



**Figure 8-3 Add Video Intercom Device**

**7.** 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.

8. Enter an integer in the **Community** field.

**Note**

If the community is divided into different sections, you should enter the corresponding number. If not, enter 1 in the input box.

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

    **Note**

    - You can import all the resources (including cameras and doors) or the specified door 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 such as live view, playback, etc., for the cameras.
11. **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.
12. Click **Add**.

**Note**

If you have checked **Restore Default** in Step 10, you should click **OK** confirm the settings.

13. 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).<br><br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| **Apply Device Settings** | When you have edited the device location information or device IP address, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon will be displayed on the right side of the . Click to apply the current settings in the system to the device(s). |
| **Restore Default** | Select the added device(s), and click to restore the configured device parameters.<br><br>**Note**<br>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. |

## Add a Detected Online Master Station

The online video intercom devices on the same local subnet with the current Web Client or SYS server can be displayed on 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 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 the active device to be added.
5. Click in the Online Device area to open the Add Video Intercom Device window.
6. Select **Master Station** as the device type.

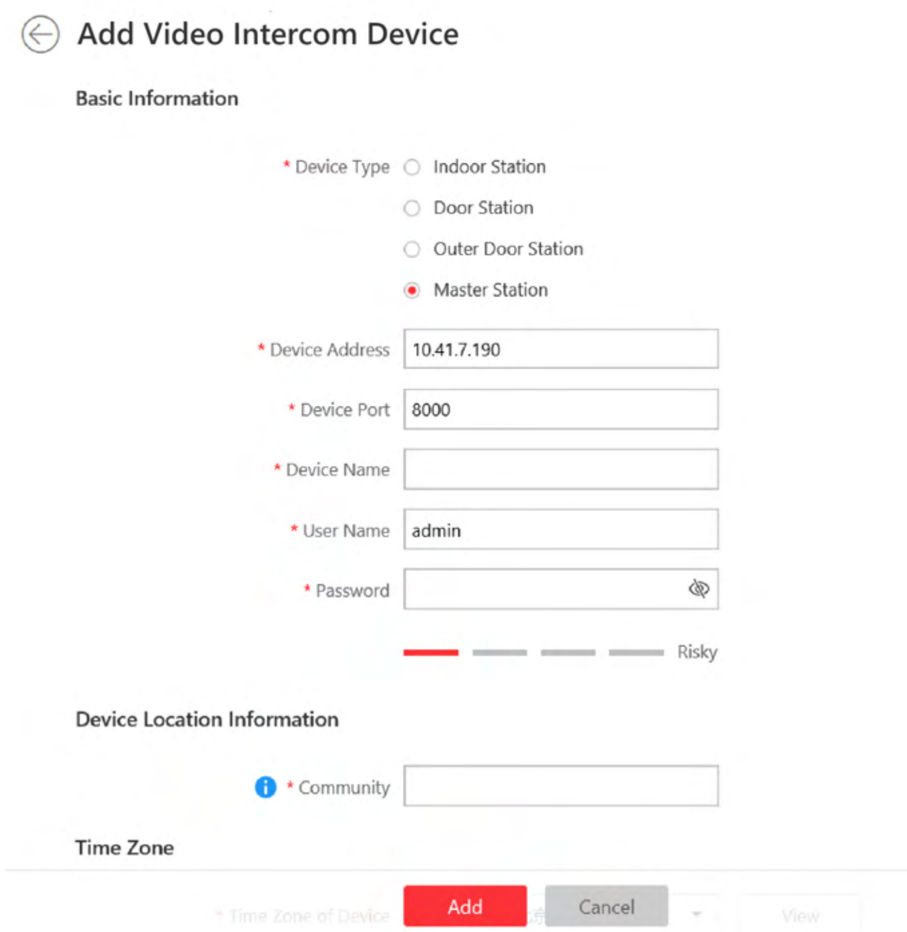



**Figure 8-4 Add Video Intercom Device**

**7.** 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.

8. Enter an integer in the **Community** field.

**Note**

If the community is divided into different sections, you should enter the corresponding number. If not, enter 1 in the input box.

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:** 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. 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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |

| | |
|---|---|
| **Apply Device Settings** | When you have edited the device location information or device IP address, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon will be displayed on the right side of the . Click to apply the current settings in the system to the device(s). |
| **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 Indoor Station by IP Address

When you know the IP address of a indoor station, 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.

The system supports configuring calling priority for indoor stations. By default, the first indoor station added to the system is the main indoor station and the others are the indoor extensions.

**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 + to enter Add Video Intercom Device page.
4. Select **Indoor Station** as the device type.

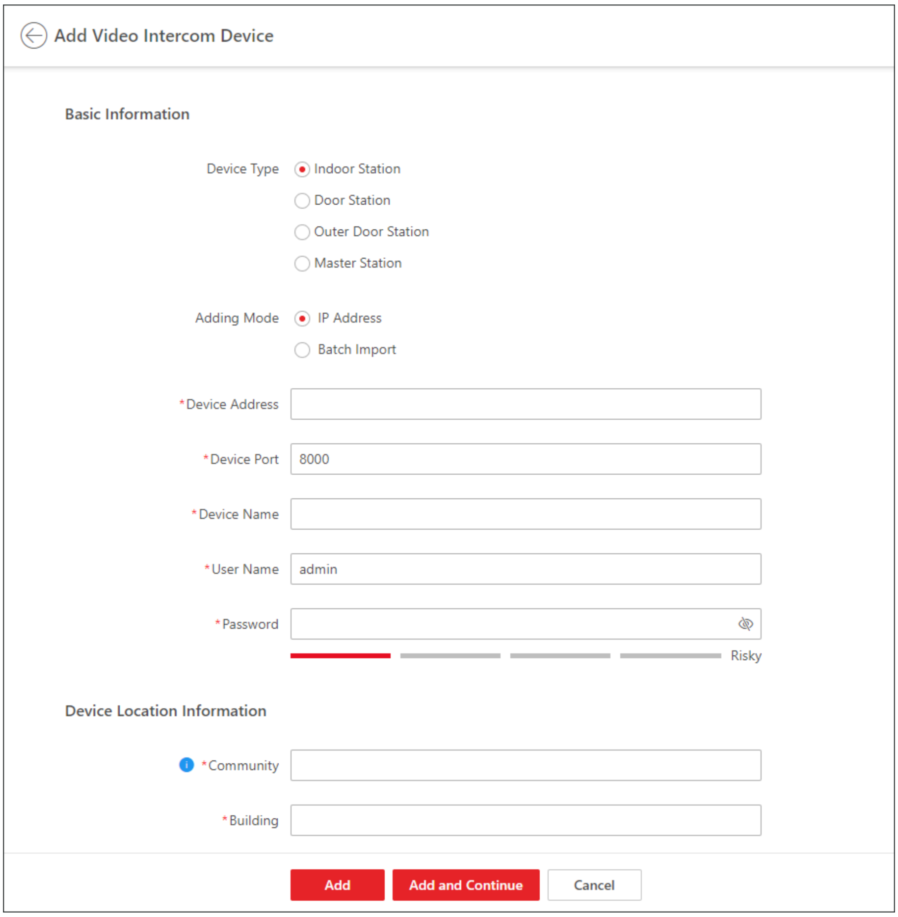



**Figure 8-5 Add Indoor Station**

**5.** Select **IP Address** as the adding mode.

**6.** 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.

7. Set the device location information, including community, building, unit (optional) and room.

**Note**

- You should enter an integer between 101 and 9999 in the **Room** Field. The room is composed of floor No. and room No. For example, for room 2 on the 12th floor, enter 1202.
- For example, if the device is located in community 1, building 2, unit 5, and room 305, you should enter 1, 2, 5, 305 respectively in the corresponding input box.

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 **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.

10. In the Resident Information Area, click to select resident(s) to be linked with the device.

**Note**

Up to 10 residents can be linked to the device.

11. **Optional:** Check **Restore Default** so that all the parameters of the device configured on the system will be restored to default settings.
12. Finish adding the device.
    - Click **Add** to add the indoor station and back to the video intercom device list page.
    - Click **Add and Continue** to save the settings and continue to add the next indoor station.
13. 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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| **Add Related Camera** | Click to relate camera(s) with the added indoor station(s). For details, refer to ***Relate Camera with Indoor Station*** . |
| **Apply Device Settings** | In some cases such as you have edited the device location information or device IP address, or the calling priority of the devices is changed, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon will be displayed on the right side of the . Click to apply the current settings in system to the device(s). |
| **Link Doorbell with Indoor Station** | Click to link the added doorbell(s) with indoor station(s). For details, refer to ***Relate Doorbell with Indoor Station*** . |
| **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 Door Station by IP Address

When you know the IP address of a door station, 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.

The system supports configuring calling priority for door stations. By default, the first door station added to the system is the main door station and the others are the sub door stations.

**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 + to enter Add Video Intercom Device page.
4. Select **Door Station** as the device type.

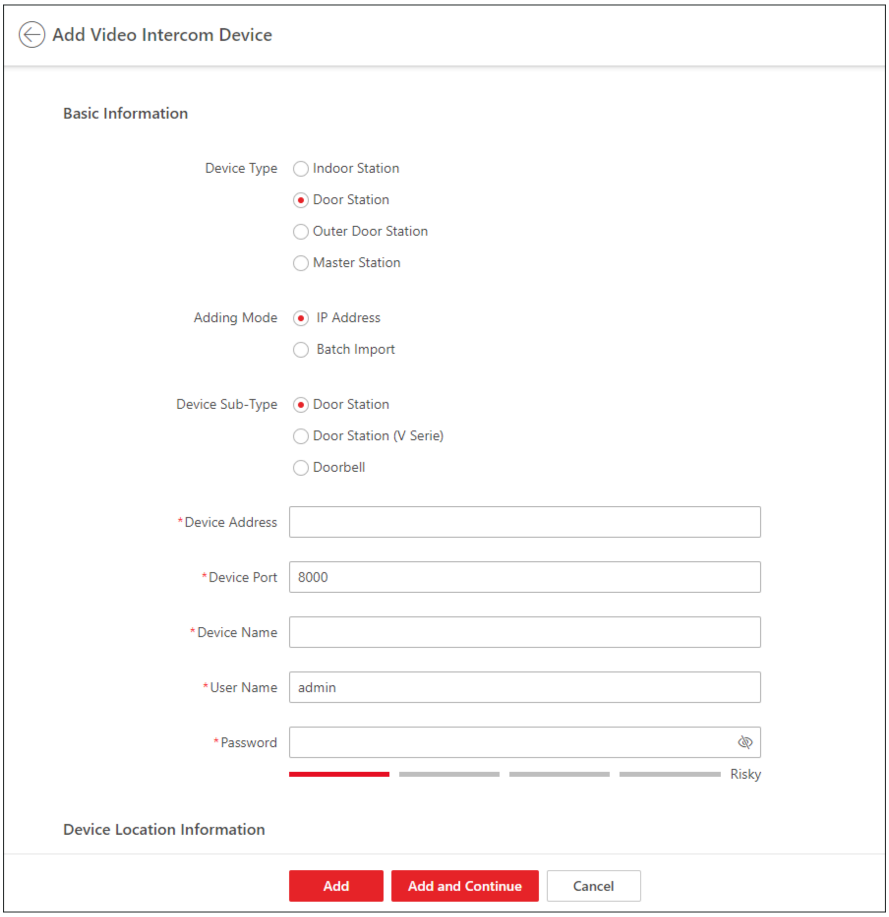



**Figure 8-6 Add Door Station**

**5.** Select **IP Address** as the adding mode.

**6.** Select **Door Station**, **Door Station (V Serie)**, or **Doorbell** as the device sub-type.

**7.** 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.

8. Set the device location information, including community, building and unit (optional).

**Note**

For example, if the device is located in community 1, building 2, unit 5, you should enter 1, 2, 5 respectively in the corresponding input box.

9. **Optional:** Select an indoor station from the drop-down list to link the doorbell with an indoor station.

**Note**

For details, refer to ***Relate Doorbell with Indoor Station*** .

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 resources of the added devices to an area.

**Note**

- You can import all the resources (including cameras and doors) or the specified door 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 such as such as live view, playback, etc., for the cameras.

12. **Optional:** Check **Restore Default** so that all the parameters of the device configured on the system will be restored to default settings.
13. Finish adding the device.
    - Click **Add** to add the door station and back to the video intercom device list page.
    - Click **Add and Continue** to save the settings and continue to add the next door station.
14. 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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| **Apply Device Settings** | When you have edited the device location information or device IP address, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon  will be displayed on the right side of the  . Click  to apply the current settings in the system to the device(s). |
| **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. |

## 8.6.4 Add Outer Door Station by IP Address

When you know the IP address of an outer door station, 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.

The system supports configuring calling priority for outer door stations. By default, the first outer door station added to the system is the main outer door station and the others are the sub outer door stations.

**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 + to enter Add Video Intercom Device page.
4. Select **Outer Door Station** as the device type.

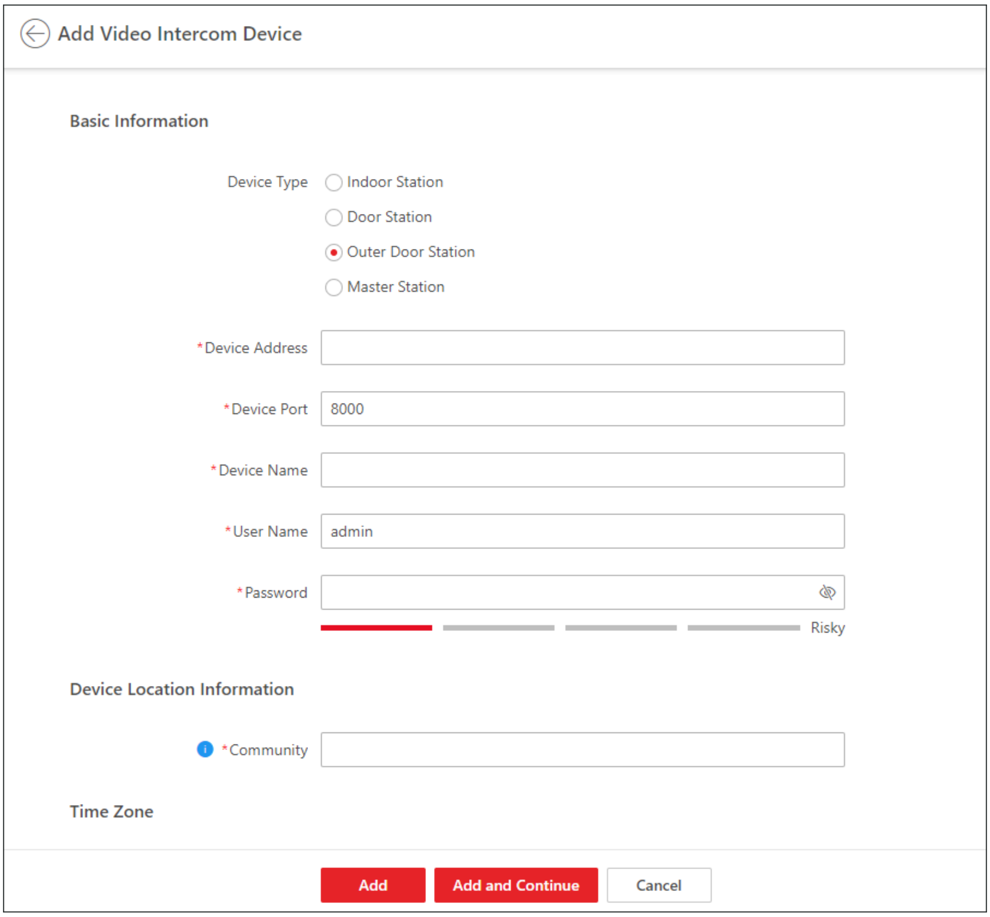



**Figure 8-7 Add Outer Door Station**

**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. Enter an integer in the **Community** field.

**Note**

If the community is divided into different sections, you should enter the corresponding number. If not, enter 1 in the input box.

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 resources (including cameras and doors) or the specified door 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 such as live view, playback, etc., for the cameras.

9. **Optional:** Check **Restore Default** so that all the parameters of the device configured on the system will be restored to default settings.
10. Finish adding the device.
    - Click **Add** to add the outer door station and back to the video intercom device list page.
    - Click **Add and Continue** to save the settings and continue to add the next outer door station.
11. 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.

| | |
|---|---|
| **Apply Device Settings** | In some cases such as you have edited the device location information or device IP address, or the calling priority of the devices is changed, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon will be displayed on the right side of the . Click to apply the current settings in system to the device(s). |
| **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. |

### 8.6.5 Add Master Station

When you know the IP address of a master station, 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.

The system supports configuring calling priority for master stations. By default, the first master station added to the system is the main master station and the others are the sub master stations. The main master station can be used as the SIP server.

**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 + to enter Add Video Intercom Device page.
4. Select **Master Station** as the device type.

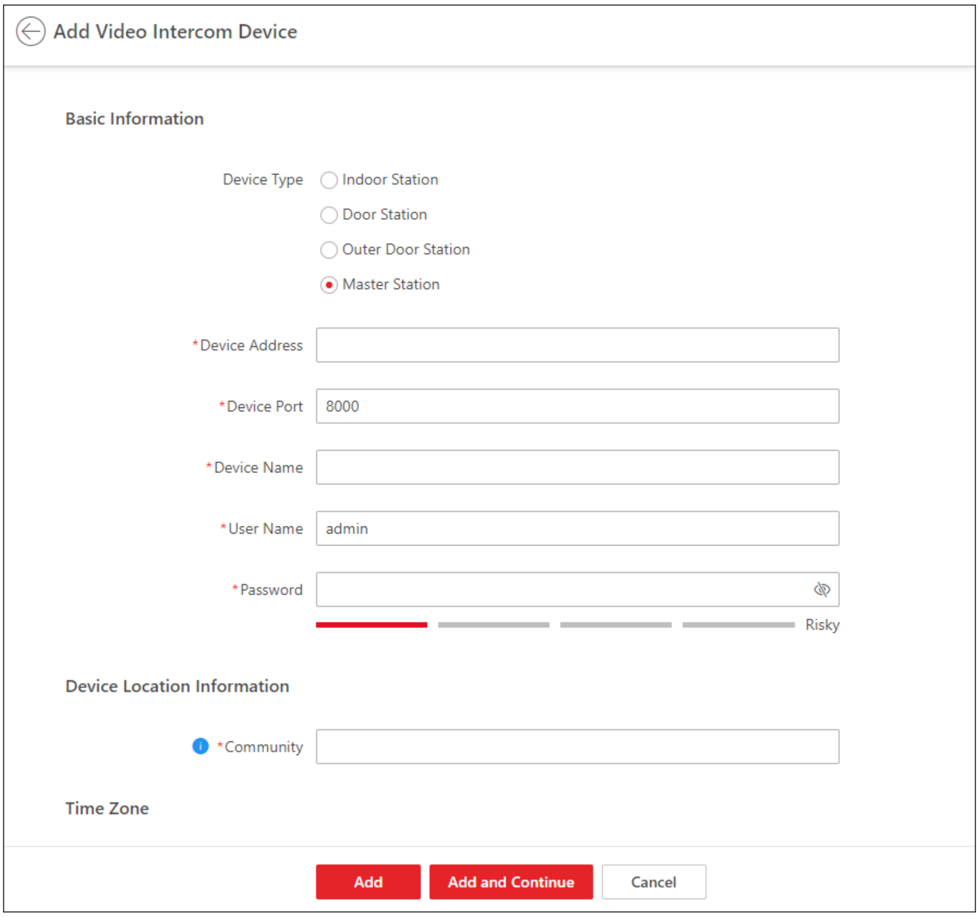



**Figure 8-8 Add Master Station**

**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. Enter an integer in the **Community** field.

**Note**

If the community is divided into different sections, you should enter the corresponding number. If not, enter 1 in the input box.

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:** 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 master station and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add the next master station.
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.

**Apply Device Settings**

In some cases such as you have edited the device location information or the device IP address, or the calling priority of the devices is changed, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon

| | |
|---|---|
| | will display on the right side of the . Click to apply the current settings in system to the device(s). |
| **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. |

## 8.6.6 Add Indoor Stations and Door Stations in a Batch

You can add indoor stations and door stations 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 + to enter Add Video Intercom Device page.
4. Select **Indoor Station** or **Door Station** as the device type.
5. Click **Batch Import** as the adding mode.
6. Click **Download Template** to 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.
8. Click ··· and select the template file.
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. Finish adding the devices.
    - Click **Add** to add the door stations/outer door stations 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 door stations/outer door stations.
11. 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.

**Add Related Camera**

Click to relate camera(s) with the added indoor station(s). For details, refer to ***Relate Camera with Indoor Station*** .

**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 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.

### 8.7.1 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.<br>**Note**<br>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.<br>**Note**<br>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.<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If multiple devices in the device list have the same password, you can change the password for them in a batch. |

### 8.7.2 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.

### 8.7.3 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.<br><br>**Note**<br><br>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).<br><br>**Note**<br><br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |

## 8.7.4 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.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |

### 8.7.5 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.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |

## 8.7.6 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**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |

## 8.7.7 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.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |

## 8.7.8 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.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |

## 8.8 Manage Dock Station

You can add a dock station to the system by IP/domain. You can also add multiple dock stations to the system by IP segment, port segment, or importing a pre-defined template which contains the required dock stations' information.

### 8.8.1 Add Dock Station by IP/Domain

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.
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.

   **User Name**

   User name of the dock station.

   **Password**

Password of the dock station.

**6. Optional:** Set time zone for the dock station.

- Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

**Note**

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

- Click **Get Device's Time Zone** to get the device's time zone.

**7.** Finish adding the dock 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.

**8. 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. |

## 8.8.2 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.

**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 of the device. By default, it is 5651.

**6. Optional:** Set time zone for the dock station.

- Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

**Note**

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

- Click **Get Device's Time Zone** to get the device's time zone.

7. Finish adding the dock stations.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and continue to add more dock stations.
8. **Optional:** Perform the following operations.

| | |
|---|---|
| **Edit Dock Station** | Click the dock station alias on the device list to edit the dock station. |
| **Delete Dock Station** | Select dock station(s) and then click **Delete** to delete them. |

## 8.8.3 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 need 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**

   The same password of the dock stations.
6. **Optional:** Set time zone for the dock station.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

**Note**

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

- Click **Get Device's Time Zone** to get the device's time zone.

7. Finish adding the device.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and add more dock stations by port segment.
8. **Optional:** Perform the following operations.

| | |
|---|---|
| **Edit Dock Station** | Click the dock station alias on the device list to edit the dock station. |
| **Delete Dock Station** | Select dock station(s) and then click **Delete** to delete them. |

### 8.8.4 Add Dock Stations in 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.
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 on 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 alias on the device list to edit the dock station. |
| **Delete Dock Station** | Select dock station(s) and then click **Delete** to delete them. |

## 8.9 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.<br>**Note**<br>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). |

## 8.10 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).

### 8.10.1 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 at present or add a few 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 may 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.
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 Encoding 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.

   **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.** Click **Add**.

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

**Remote Configuration**

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 **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 (switch, bridge or fiber converter) 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.

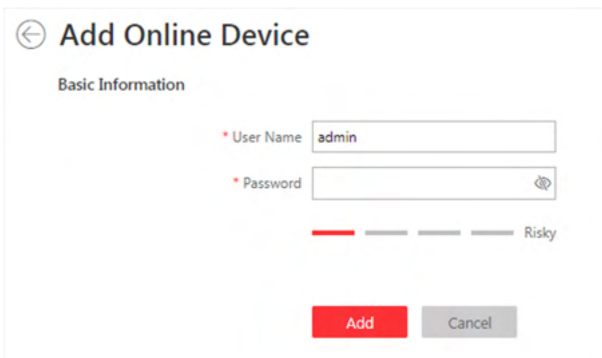



**Figure 8-9 Add Online Devices in a Batch**

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

| | |
|---|---|
| **Remote Configuration** | Click ⚙ to set the remote configurations of the corresponding device.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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.<br>**Note**<br>System connected switch is the switch that is directly connected with the SYS server. |

## 8.10.2 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.
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**

Enter the IP address of the device.

**Device Port**

The default device port 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.

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 to set the remote configurations of the corresponding device.<br>**Note**<br>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.<br>**Note**<br>System connected switch is the switch that is directly connected with the SYS server. |

### 8.10.3 Import Network Transmission Devices in a Batch

If there are 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 (switch, bridge or fiber converter) 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. 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 to set the remote configurations of the corresponding device. |

| | |
|---|---|
| | **Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• 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.<br>**Note**<br>System connected switch is the switch that is directly connected with the SYS server. |

## 8.11 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*** .

## 8.12 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.

### 8.12.1 Add Terminal

You can add terminal to the platform by multiple methods: adding online terminals, adding terminals by IP address, adding terminals by ISUP account. After the terminals are added to the platform, you can configure, manage and control the terminals. The terminal includes digital signage and digital signage player.

### Add Single or Multiple Online Terminals

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

**Before You Start**

Install the web controls first, and then the online devices can be detected.

**Steps**

1. On the Home page, select **General → Resource Management → Device and Server → Digital Signage Terminal** .
2. Click **Online Device** to display the online devices in the lower area.
3. 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.
4. Set the basic information.

**Device Address**

Device IP address, which can be obtained automatically.

**Note**

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

**Device Port**

Device port No., which can be obtained automatically.

**Note**

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

**Device Name**

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

**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 non-admin account to add device, the permissions might be limited.

**Password**

The password of the user name. And prompt the password strength.

**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, and then configure the face picture library storage location and capture storage location.

**Local Storage**

The pictures are stored in the local storage space of the server running the platform.

**Note**

Click **Configuration** to configure picture storage.

**pStor Server**

The pictures are stored in the pStor server.

**Note**

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

6. Set the time zone of device, 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.
7. **Optional:** Switch on **Add Resource to Area**, and then select **Create Area by Device Name** or **Existing Area**.
8. Click **Add**.
9. **Optional:** Perform the following operations after adding devices.

**Change Password**

Select one or more device(s), and then click **Change Password**.

**Note**

- Support changing 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 the added one or multiple device(s), and then click **Delete** to delete the selected devices.

**Set Time Zone**

Select the added one or multiple device(s), and then click **Time Zone** to configure the time zone of device. 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. When the time zone of device and the platform are not consistent, the platform will apply the time zone settings to the device.

## Add Terminal by IP Address

If you know the IP address of the terminal (called 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. On the Home page, select **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**.

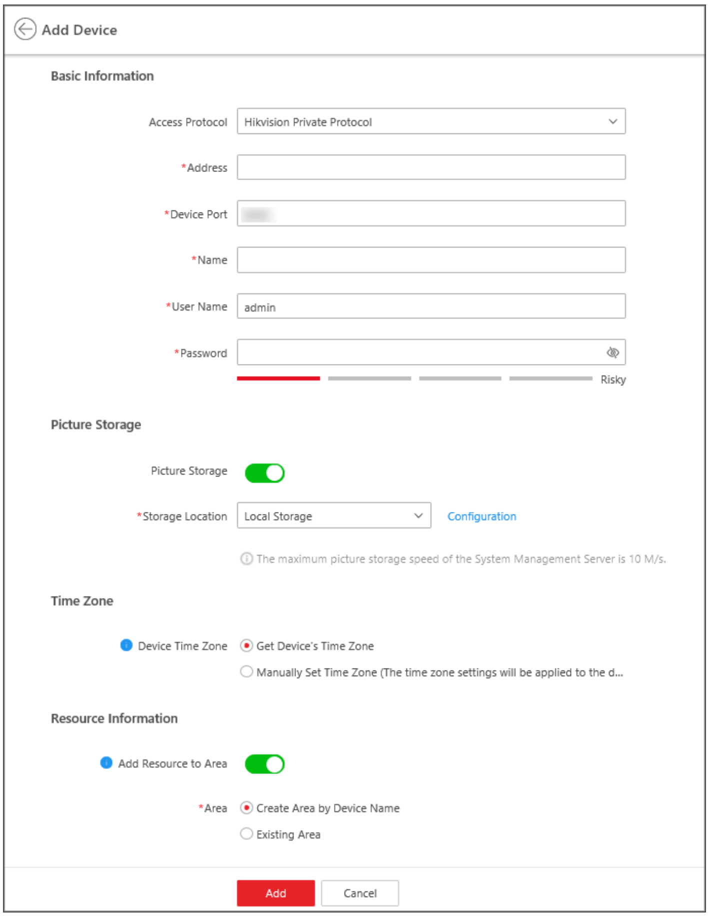



**Figure 8-12 Add Terminal by IP Address**

**4.** Set the basic information.

**Device Address**

Enter the device IP address.

**Device Port**

Enter the device Port No.

**Device Name**

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

**User Name**

The admin account (which is created when activating the device) or the non-admin account, such as operator. If you use non-admin account to add device, 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**, and then configure the storage location, and configure the face picture library storage location and capture storage location.

   **Local Storage**

   The pictures are stored in the local storage space of the server running the platform.

   **Note**

   Click **Configuration** to configure picture storage.

   **pStor Server**

   The pictures are stored in the pStor server. For more details about adding pStor server, refer to ***Add pStor*** .

   **Note**

   In the attendance application scene, you should enable **Picture Storage**.
6. Set the time zone of device, 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.
7. **Optional:** Enable **Add Resource to Area**, and then select **Create by Device Name** or **Existing Area**.
8. Click **Add**.
9. **Optional:** Perform the following operations after adding devices.

| | |
|---|---|
| **Change Password** | Select one or more device(s), and then click **Change Password**.<br>**Note**<br>• Support modifying the password of the online Hikvision devices.<br>• If multiple devices have the same password, you can change the password for multiple devices simultaneously. |
| **Delete Devices** | Select the added one or multiple device(s), and then click **Delete** to delete the selected devices. |
| **Set Time Zone** | Select the added one or multiple device(s), and then click **Time Zone** to configure the time zone of device. 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. When the time zone of device and the platform are not consistent, the platform will apply the time zone settings to the device.

## Add Terminal by ISUP Account

For the terminal (called device in the following pages) supports ISUP protocol, you can add it to the platform by ISUP protocol by entering the device ID and key.

**Before You Start**

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. On the Home page, select **General → Resource Management → Device and Server → Digital Signage Terminal** .
2. Click **Add** to enter the Add Device page.

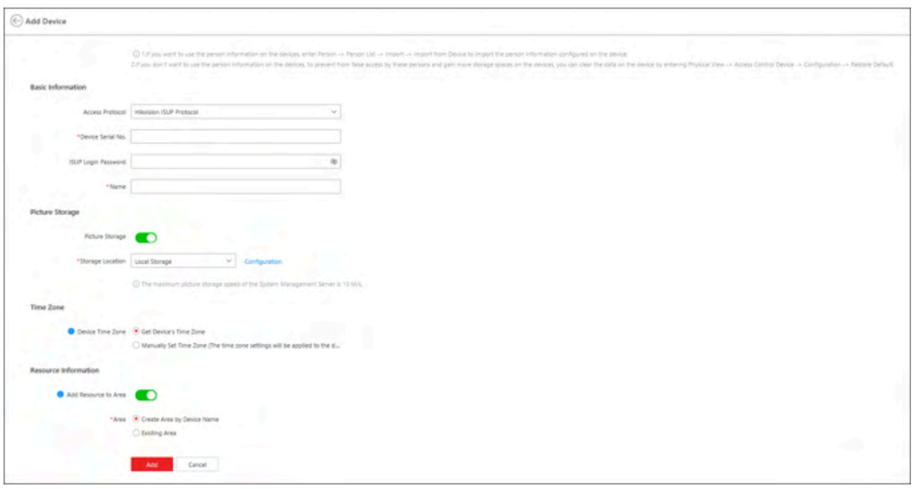


**Figure 8-13 Add Terminal by ISUP Account**

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

   **Device ID**

      Enter the device ID registered by ISUP protocol.

   **Key**

      Enter the device key.

   **Device Name**

      Name for the device, which can be used to describe the device function and location.
5. **Optional:** Enable **Picture Storage**, and then configure the storage location, and then configure the face picture library storage location and capture storage location.

**Local Storage**

The pictures are stored in the local storage space of the server running the platform.

**Note**

Click **Configuration** to configure picture storage.

**pStor Server**

The picture is stored in the pStor server. For more details about adding pStor server, refer to ***Add pStor*** .

**Note**

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

6. Set the time zone of device, 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.
7. **Optional:** Enable **Add Resource to Area**, and then select **Create by Device Name** or **Existing Area**.
8. Click **Add**.
9. **Optional:** Perform the following operations according to the requirements.

**Change Password**

Select one or multiple device(s), and then click **Change Password**.

**Note**

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

**Delete Devices**

Select the added one or multiple device(s), and then click **Delete**.

**Set Time Zone**

Select the added one or multiple device(s), and then click **Time Zone** to configure the time zone of device. 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. When the time zone of device and the platform are not consistent, the platform will apply the time zone settings to the device.

### 8.12.2 Enable General Authentication Code

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

**Steps**

1. In the top left corner of the Client, select → **All Modules** → **Resource Management** → **Device and Server** → **Digital Signage Terminal**
2. Click **General Authentication Code Settings**.
3. Enable **General Authentication Code Settings**.
4. Enter the authentication code.

**Note**

The length of authentication code is 8-16 bits, including at least two of upper or lower cases letters and digits.

**What to do next**

After setting general authentication code, you should enter the authentication code on the terminal.

### 8.12.3 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.

## 8.12.4 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.

**Face Similarity**

Set the face similarity for face comparison. When the captured face picture's similarity reaches the value, it will be regarded as comparison succeeded.

**Pupil Distance**

Set the pixel of face score. For example, if you set the face score as 1 pixel, when the face score of the person in the view is 1 pixel, it will trigger face capture. It is used to control the recognition distance between the person and camera.

**Face Score**

It is used to control the quality of face capture. The higher the value, the better the quality of captured picture will be.

**Face Comparison Mode**

**Compare Face in the Middle**

Compare the captured face in the middle of view.

**Compare Biggest Face**

Compare the captured biggest face in the view.

**Compare All Faces**

Compare all the captured faces in the view.

**Facial Recognition Mode**

**The Highest Similarity Face**

Upload the highest similarity face picture.

**The Frist Face Exceeds the Similarity Threshold**

Upload the first face picture exceeding the similarity threshold.

**All Faces Exceeds the Similarity Threshold**

Upload all the face pictures exceeding the similarity threshold.

**Face Recognition Interval**

Set the face recognition interval according to your requirements.

**6.** Click **Save**.

## Link External Device to Terminal

After adding terminal to the platform, you can link external devices (such as camera or DVR/NVR) to the terminal for attendance, live view or temperature screening.

**Before You Start**

- Make sure the external device has been installed properly.
- 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 in the Operation column of the online device to enter the remote configuration page of terminal.
3. In the **Linked Device** area, click **Add** to enter the Add Device page.
4. Set the parameters.

   **Device Address**

   Device IP address.

   **Device Port**

   Device Port No., by default, it is 8000.

   **Device Name**

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

   **User Name**

   The Login account of the device.

   **Password**

   The password of the Login account.

   **Channel No.**

   The channel No. of the device to be added to the terminal.
5. Click **Add Device** to finish adding.

## 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.

### 8.12.5 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** → **Resource Management** . Click **Device and Server** → **Digital Signage Terminal** on the left to enter the terminal list page.

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.

## 8.13 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.

### 8.13.1 Add Detected Online IP Speakers

The platform can automatically detect the available IP speakers on the same network where the Web Client or the SYS server is located, which makes the devices' information (e.g., IP address) recognized by the platform. Based on the information, you can add the devices quickly.

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

**Note**

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

### Add a Detected Online IP Speaker

For the detected online IP speakers, 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 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.
- 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** → **IP Speaker** on the left.
3. In the Online Device area, select a network type.

   **Server Network**

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

   **Local Network**

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
4. Select an 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 displays automatically.

   **Device Port**

   The port number of the device, which displays automatically. The default 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 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. Click **Add** to add the current device.
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.

**Search Device**

Enter a key word in the search box in the upper-right corner, and click (or press the Enter key) to search for the target device(s).

**View Error Message**

If there is an icon appearing beside the device name, hover the mouse cursor to the icon and view the error message. You can click **Edit**/ **Refresh** to edit/refresh the device if needed.

### Add Detected Online IP Speakers in a Batch

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

**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.
- 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. Select **Device and Server** → **IP Speaker** on the left.
3. In the Online Device area, select a network type.

   **Server Network**

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

   **Local Network**

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
4. Select the active devices to be added.
5. Click **Add to Device List** to open the Add Online Device window.
6. Set 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 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 (such as alarm inputs and alarm outputs) of the added devices to the area.

**Note**

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. Click **Add** to batch add these devices.
9. **Optional:** Perform the following operations.

| | |
|---|---|
| **Remote Configurations** | Click to configure the device remotely.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| **Search Device** | Enter a key word in the search box in the upper-right corner, and click or press the Enter key to search for the target device(s). |
| **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. |

## 8.13.2 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 Protocol/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.<br>**Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| **Search Device** | Enter a key word in the search box in the 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. |

### 8.13.3 Add IP Speaker by IP Segment

When multiple IP speakers 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 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 Protocol** as the Access 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.

   **Device Port**

   The port number of the device. By default, it is 8000.

   **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:** Switch on **Add Resource to Area** to import the resources (such as alarm inputs and alarm outputs) of the added devices to the area.

   **Note**

   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 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 device(s).
9. **Optional:** Perform the following operations.

| | |
|---|---|
| **Remote Configurations** | Click to configure the device remotely. |

| | |
|---|---|
| | **Note**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| **Search Device** | Enter a key word in the search box in the 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. |

### 8.13.4 Add IP Speaker by Port Segment

When multiple IP speakers 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 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 Protocol** as the Access Protocol.
5. Select **Port Segment** as the Adding Mode.
6. Enter the required information.

   **Device Address**

   Enter the IP address of the devices to be added.

   **Device Port**

Enter the start port No. and the end port No.

**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 (such as alarm inputs and alarm outputs) of the added devices to the area.

---

**Note**

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 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 device(s).
9. **Optional:** Perform the following operations.

| | |
|---|---|
| **Remote Configurations** | Click to configure the device remotely.<br>**Note**<br>For details about remote configuration, see the user manual of the device. |
| **Change Password** | Select the added device(s) and click to change the password(s) for the device(s). |

**Note**

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

| | |
|---|---|
| **Search Device** | Enter a key word in the search box in the 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. |

## 8.13.5 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 Protocol/Hikvision Private Speaker Protocol** as the Access Protocol.
5. Select **Batch Import** as the Adding Mode.
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**<br>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).<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If the devices have the same password, you can select multiple devices to change the password for them at the same time. |
| **Search Device** | Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s). |

## 8.14 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*** .

### 8.14.1 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.<br>**Note**<br>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.<br>**Note**<br>• You can change the password for online HIKVISION devices only.<br>• 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.<br><br>**Note**<br><br>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.

### 8.14.2 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.

### 8.14.3 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.

### 8.14.4 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 the settings icon 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.

### 8.14.5 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.

## 8.15 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.

### 8.15.1 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.<br>**Note**<br>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.<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If multiple devices in the device list have the same password, you can change the password for them in a batch. |

## 8.15.2 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.<br>**Note**<br>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.<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If multiple devices in the device list have the same password, you can change the password for them in a batch. |

### 8.15.3 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.<br>**Note**<br>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.<br>**Note**<br>• You can only change the password for online HIKVISION devices currently.<br>• If multiple devices in the device list have the same password, you can change the password for them in a batch. |

## 8.16 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 |

| No. | Device Type |
|---|---|
| | Note<br>Upgrading the card reader linked to the door station is not supported. |
| 11 | Master 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<br>Note<br>Upgrading the card reader linked to the door station is not supported. |
| 6 | Master Station |
| 7 | Digital Signage Terminal |

**Note**

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

## 8.16.1 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.

### 8.16.2 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.

### 8.16.3 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.

## 8.17 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*** .

### 8.17.1 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.

### 8.17.2 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.

## 8.18 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.

### 8.18.1 Add pStor

You can add pStor server as Recording Server to the HikCentral Professional for storing the video files 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.
3. Click **Add** to enter the Add Recording Server page.
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:** Set the **Enable Picture Storage** switch to ON for storing pictures in this pStor.

**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, set the **Enable WAN Access** switch to ON and set the corresponding parameters which are available when you access the server via WAN.
9. Enter the alias, 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. 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 **Alias** 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 ⚙, and the login interface of the pStor server displays. You can log in and configure the pStor server. |

### 8.18.2 Add Hybrid Storage Area Network

You can add the Hybrid Storage Area Network (hereafter simplyfied as Hybrid SAN) as Recording Server to the HikCentral Professional for storing the video files and pictures.

**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.

**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.
3. Click **Add** to enter the Add Recording Server page.
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.
6. **Optional:** Enable picture storage function for storing pictures in this Hybrid Storage Area Network.
   1) Set the **Enable Picture Storage** switch to ON.
   2) Set picture downloading port No. for downloading pictures via Control Client. If the picture downloading port No. is not changed, use the default one.
   3) Set signaling gateway port No.. If the picture downloading port No. 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:** Set the **Enable WAN Access** switch to ON 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 alias, 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. 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 **Alias** 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 , 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 to perform one-touch configuration before you can store the video files of the camera on the Hybrid Storage Area Network. |

## 8.18.3 Add Network Video Recorder

You can add an NVR (Network Video Recorder) as a Recording Server to HikCentral Professional for storing pictures.

**Before You Start**

Make sure the NVR 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.
3. Click **Add** to enter the adding server page.
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 Web Client 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 alias, 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 **Alias** 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 , and the login interface of the NVR will be displayed. You can log in and configure the NVR. |

## 8.18.4 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**

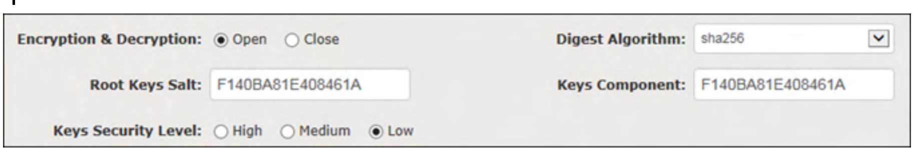
Make sure the Cloud Storage Server you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

**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.




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.
3. Click **Add** to enter the adding server page.
4. Select **Cloud Storage Server**.
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 Cloud Storage 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:** Set the **Enable Picture Storage** switch to ON 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, set the **Enable WAN Access** switch to ON and set the corresponding parameters which are available when you access the server via WAN.
9. Enter the alias, 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 **Alias** 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 , and the login interface of the Cloud Storage Server displays. You can log in and configure the Cloud Storage Server. |

## 8.18.5 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 service 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.
3. Click **Add** to enter the Add Recording Server page.
4. Select **pStor Cluster Service**.

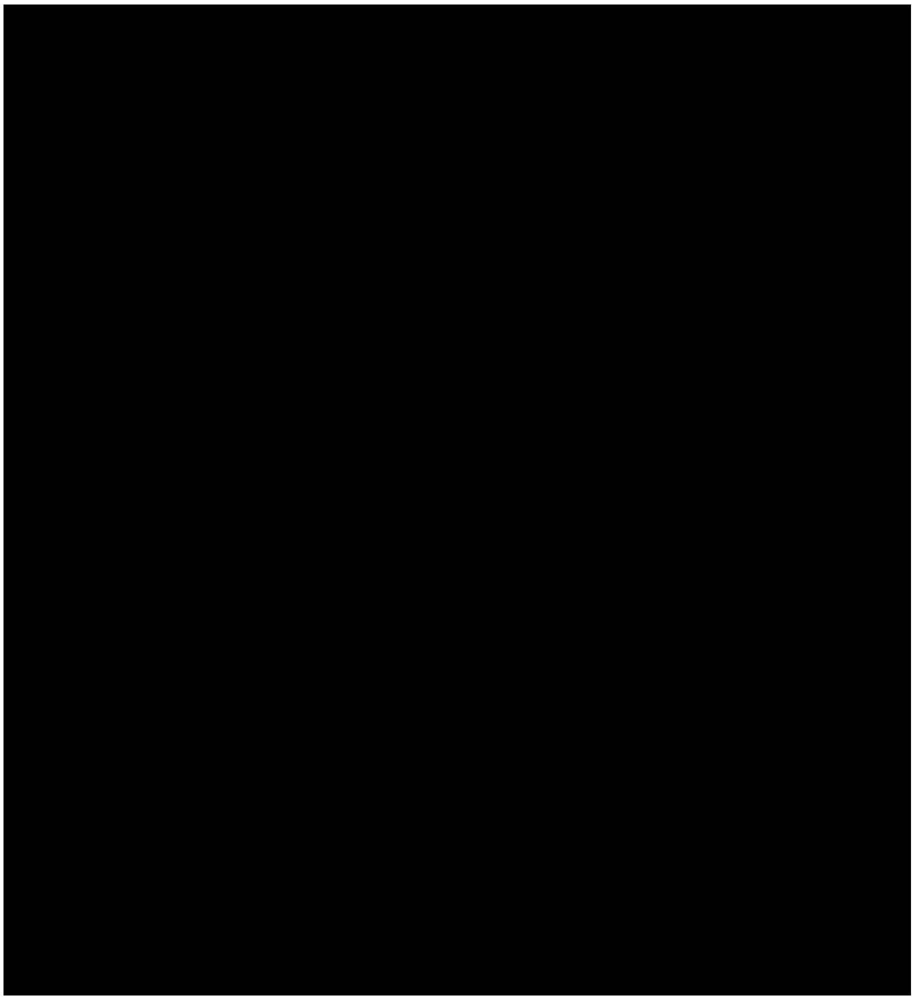


**Figure 8-14 Add pStor Cluster Service**

**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 device 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 **Alias** 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 to enter the login interface of the pStor cluster service. You can log in and configure the pStor cluster service. |

## 8.18.6 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.

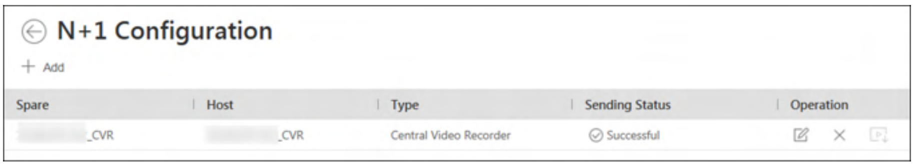



**Figure 8-15 N+1 Configuration Page**

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.

## 8.19 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.

### 8.19.1 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**.

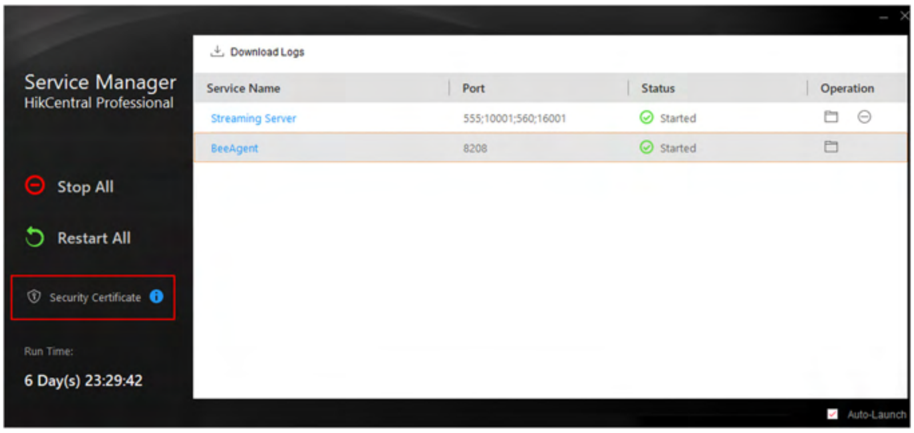



**Figure 8-16 Enter Security Certificate**

**7.** Enter the certificate information you generate in step 4.

## 8.19.2 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.

**3.** Click **Add** to enter the Add Streaming Server page.

**4.** Enter the required information.

**Alias**

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**.

**5. 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.

**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.

## 8.20 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.

   **Device 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. |

## 8.21 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 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**

- 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.
3. Click **Add** to enter the Add Security Audit Server page.

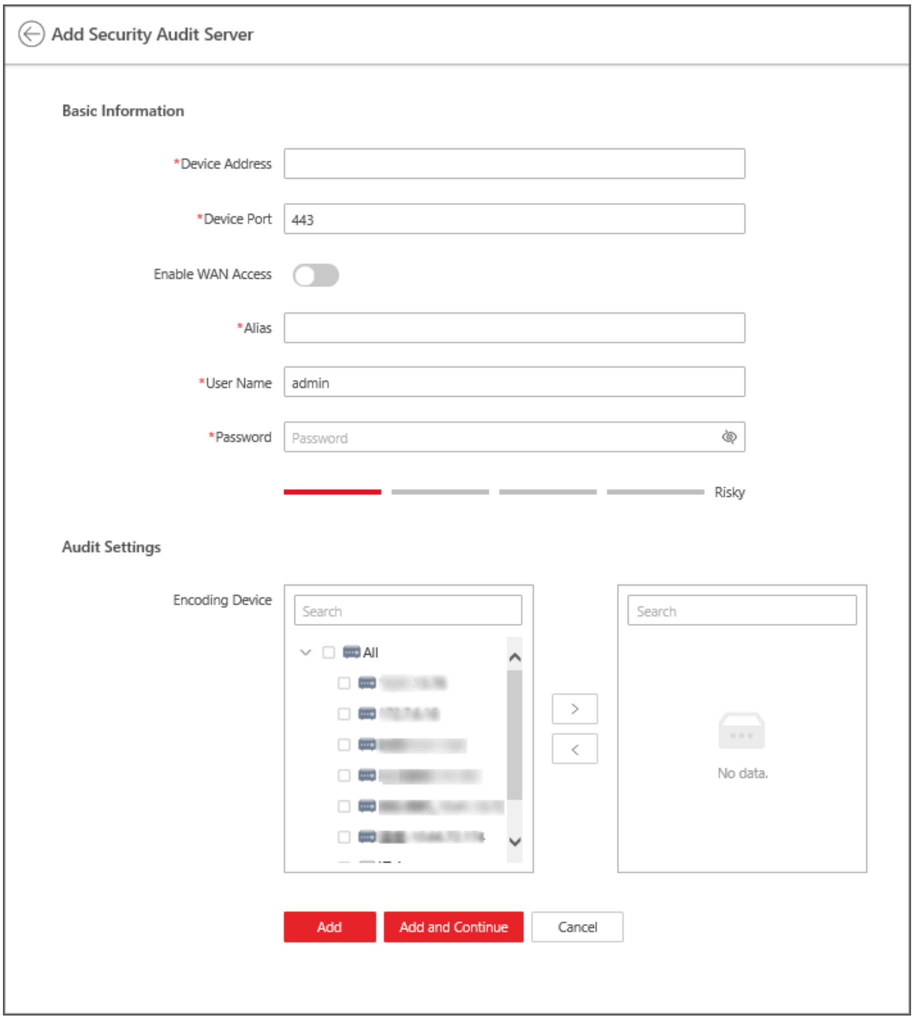



**Figure 8-17 Add Security Audit Server Page**

4. Set the required basic information such as device address, device port number, and WAN access.

**Device 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.

**Alias**

Enter an alias for the Security Audit 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.

## 8.22 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.

### 8.22.1 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.<br>**Note**<br>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.

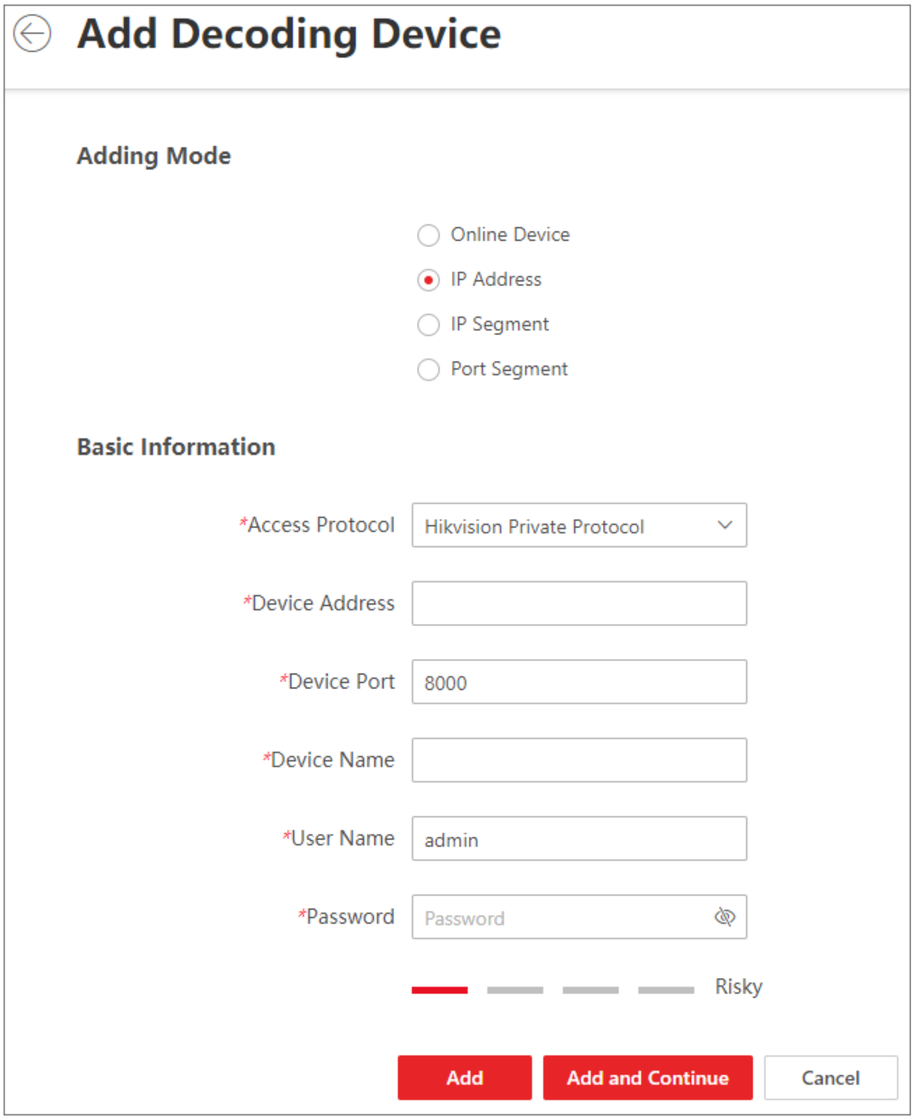



**Figure 8-18 Add Decoding Device Page**

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

**Access Protocol**

Select **Hikvision Private Protocol** to add the devices and select **ONVIF Protocol** to add the third-party 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.<br>**Note**<br>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 and select **ONVIF Protocol** to add the third-party 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 and select **ONVIF Protocol** to add the third-party 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.<br>**Note**<br>For detailed operations, see the user manual of the device. |
| **Delete** | Click ··· → × to delete the device. |

### 8.22.2 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.

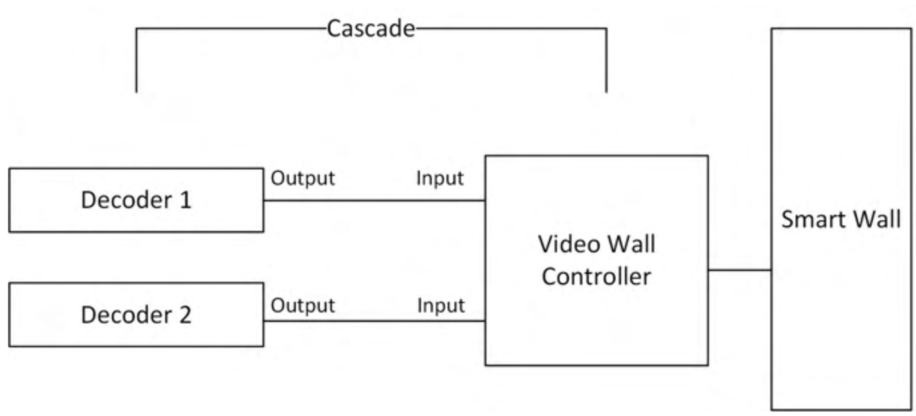



**Figure 8-19 Cascade**

**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.

### 8.22.3 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.

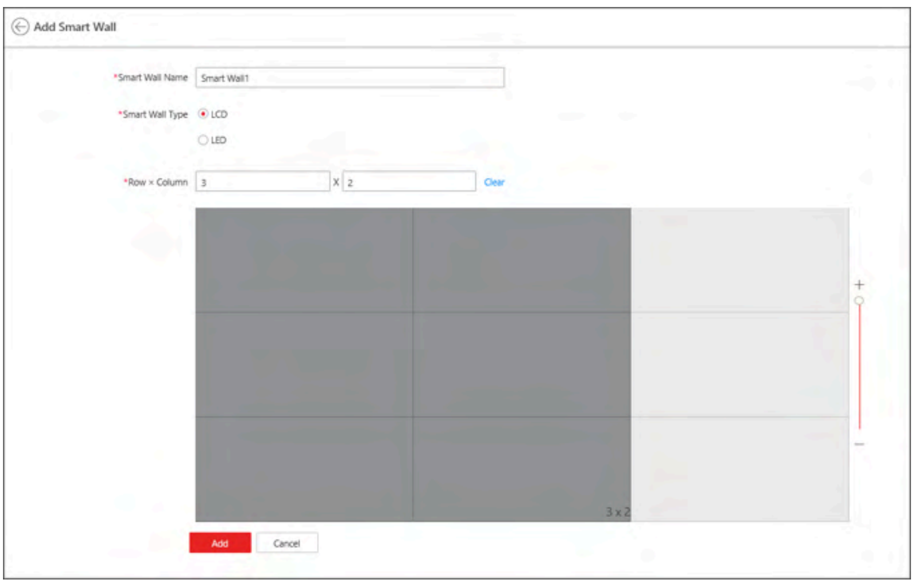



**Figure 8-20 Add Smart Wall Dialog**

4. Set the name for the smart wall.
5. Set the row number and the column number.
6. Click **Add**.
7. **Optional:** Perform the following operations after adding the decoding device.

| | |
|---|---|
| **Link Decoding Output with Window** | For details about the operations, see ***Link Decoding Output with Window*** . |

| | |
|---|---|
| **Edit Smart Wall** | Edit the name of the smart wall. |
| **Delete Smart Wall** | Delete the smart wall. |

### 8.22.4 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.

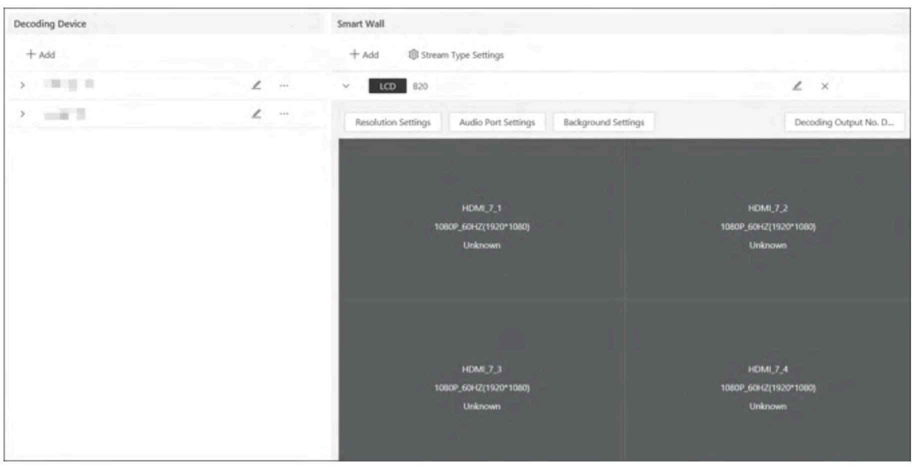



**Figure 8-21 Link Decoding Device with Window**

6. **Optional:** Click to release the linkage.

### 8.22.5 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.

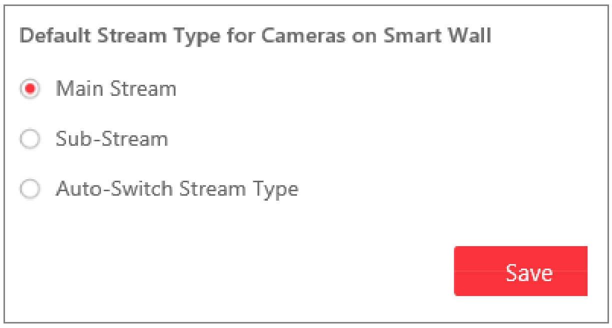



**Figure 8-22 Set Default Stream Type for Cameras on Smart Wall**

**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.

# 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 current site to manage the devices.

**Steps**

1. In the top left corner of 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 a current site.
4. Click + on the area list panel to open the Add Area panel.

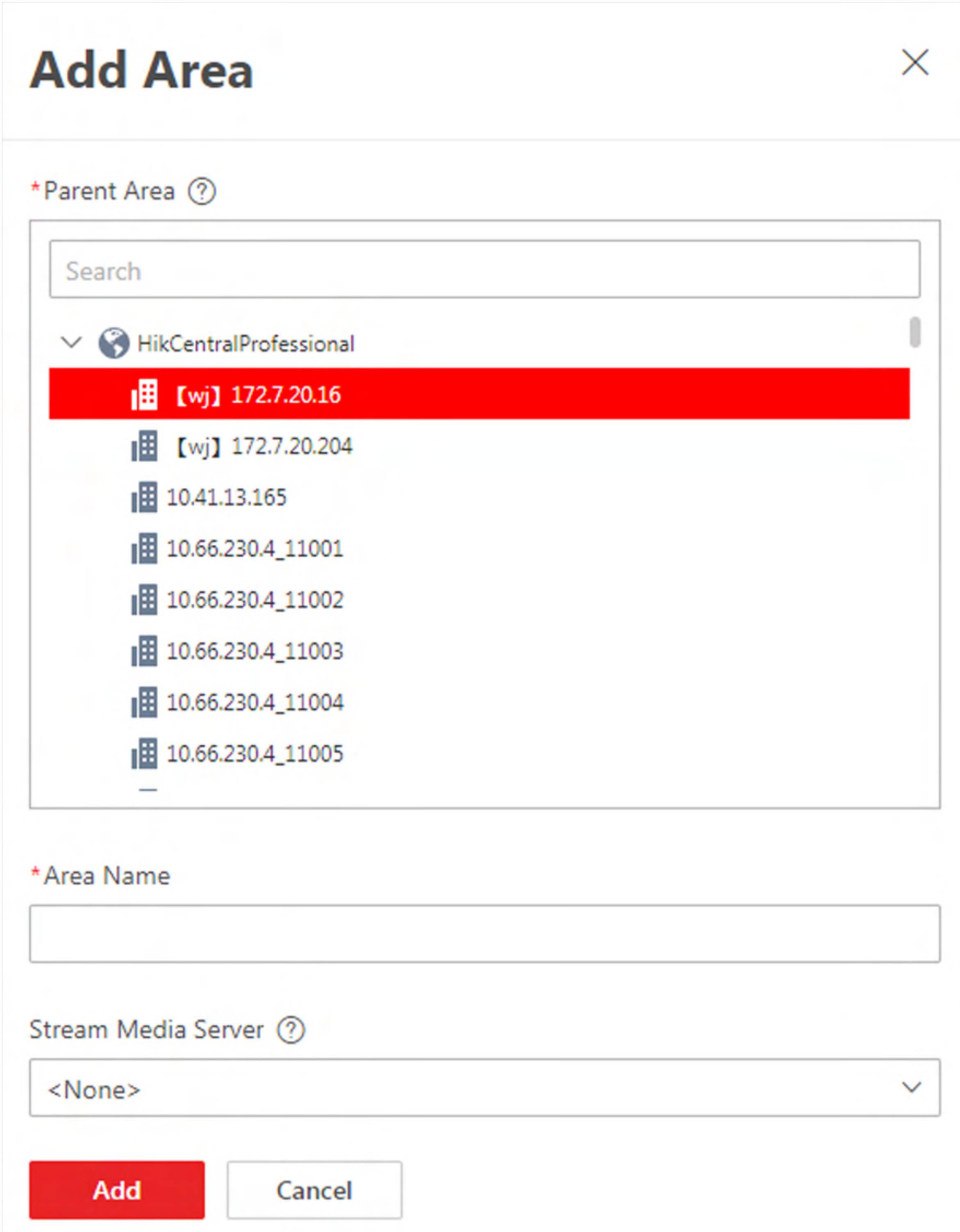



**Figure 9-1 Add Area for Current Site**

**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.
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. Click **Add**.
10. **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 a selected area, or press **Ctrl** on your keyboard and select multiple areas and then click to delete areas in a batch.<br>**Note**<br>After deleting the area, the resources in the area (cameras, doors, elevators, radars, alarm inputs, alarm outputs, UVSSs, and digital signage terminals) 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 the area. |
| **Move Area** | Drag the added area to other parent area as the child area. |

## 9.1.2 Add Area for Remote Site

You can add an area for Remote Site to manage the devices in the Central System.

**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 Remote Site.

4. Click + on the area list panel to open the Add Area panel.

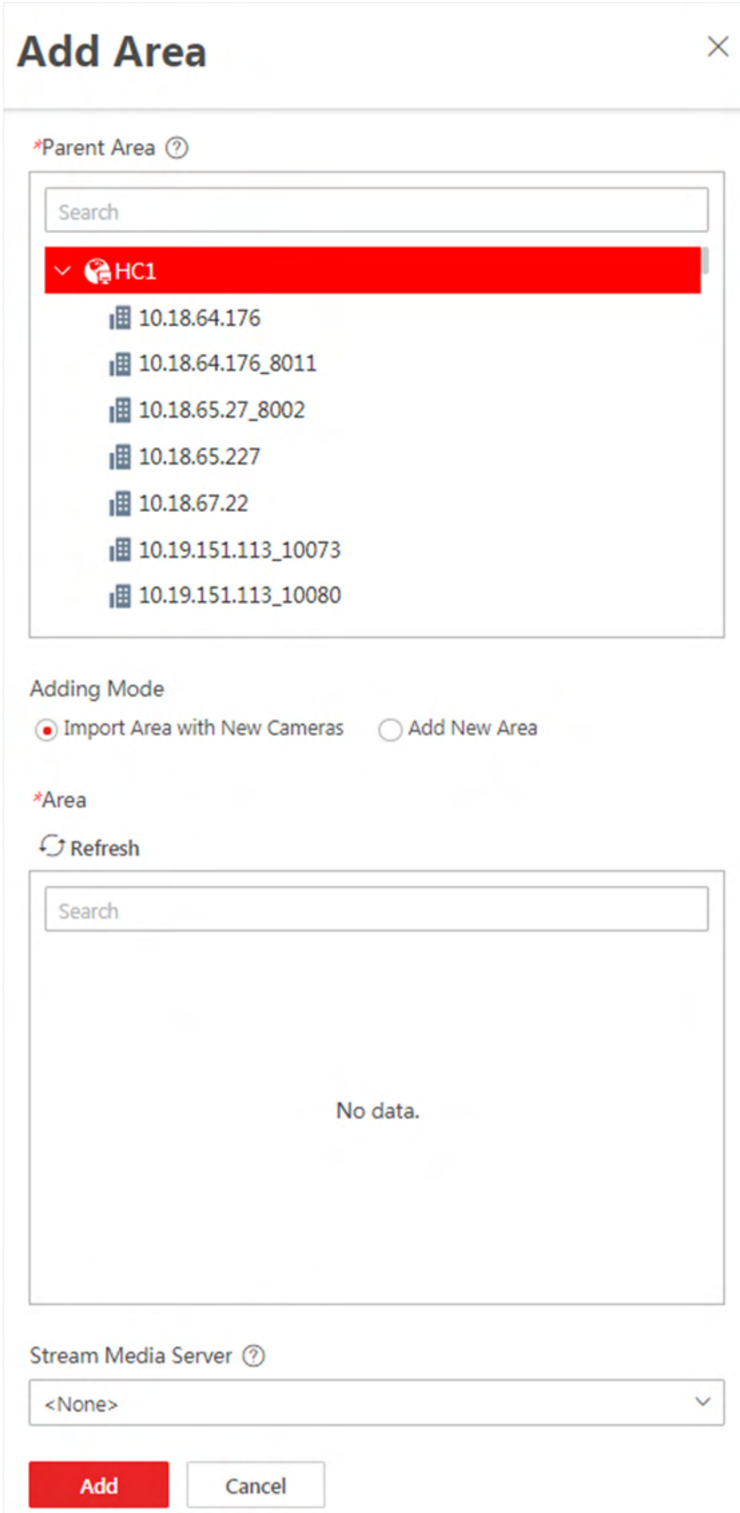



**Figure 9-2 Add Area for Remote Site**

**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 display 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. Click **Add**.
10. 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 and select multiple areas and then click to delete areas in a batch.<br>**Note**<br>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 the area. |
| **Move Area** | Drag the added area to other parent area as the child area. |

## 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 the 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 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 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:** Click in the Operation column to configure the camera.
9. Click **Add**.

   The added camera(s) will be displayed in the list.
10. **Optional:** After adding the cameras, you can do one or more of the followings.

| | |
|---|---|
| **Get Camera Name** | Select the cameras and click to get the cameras' names from the device in a batch.<br>**Note**<br>You can only synchronize the camera name of online HIKVISION device. |
| **Apply Camera Name** | Select the cameras and click to apply the cameras' names to the device 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 Camera ID page. Then edit the default identifier number in the **ID** column of each camera and click **Save**.<br>**Note**<br>The camera ID is unique and used to display certain camera's live view on smart wall via the network keyboard. |
| **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 Map Settings page and drag the camera to the map. See ***Add Hot Spot on Map*** for details. |
| **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 Remote Sites to areas in Central System for management.

**Before You Start**

Encoding devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Encoding Device*** for detailed configuration 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 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 Remote Site.
4. Select an area for adding cameras to in the area list panel.
5. Click + on the Camera page to enter the Add Camera page.

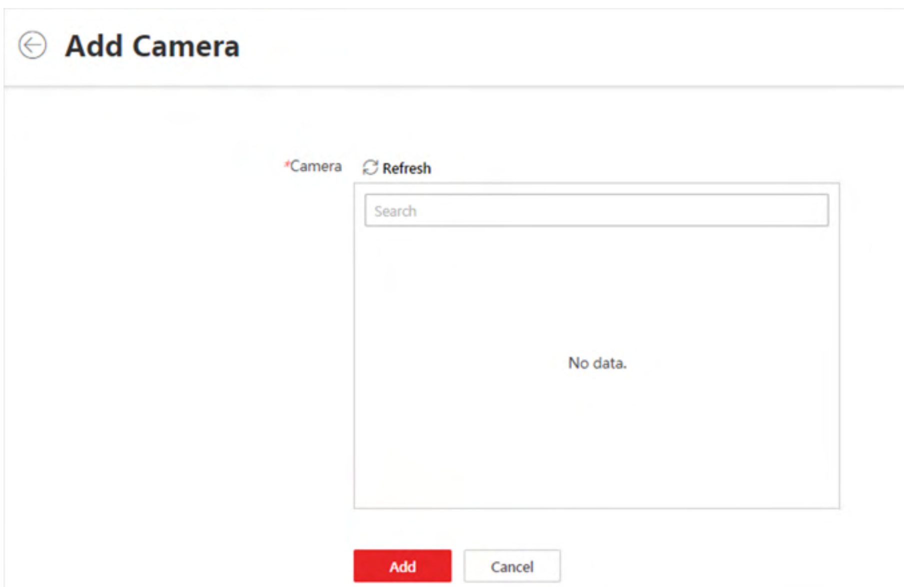



**Figure 9-3 Add Camera to Area for Remote Site**

6. Select the cameras to add.

**Note**

Up to 64 cameras can be added to one area.

7. Click **Add**.
8. **Optional:** After adding the cameras, you can do one or more of the following:

| | |
|---|---|
| **Synchronize Camera Name** | Select the cameras and click to get the cameras' names from the device in a batch. |
| **Set Camera ID** | Click to enter Camera ID page. Then edit the default identifier number in the **ID** column of each camera and click **Save**.<br>**Note**<br>The camera ID is unique and used to display certain camera's live view on smart wall via the network keyboard. |
| **Move to Other Area** | Select the cameras and click . Then select the target area to move the selected cameras to and click **Move**. |
| **Display Cameras of Child Areas** | Select **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.<br>**Note**<br>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 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).<br>**Note**<br>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. |

## 9.2.6 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.<br>• **Online Status**: indicates alarm input online; indicates alarm input offline.<br>• **Arming Status**: indicates alarm input armed; indicates alarm input disarmed.<br>• **Bypass Status**: indicates alarm input bypassed; indicates bypass restored.<br>• **Fault Status**: indicates alarm input exception.<br>• **Alarm Status**: indicates that the alarm input is alarming.<br>• **Detector Connection Status**: indicates alarm input not enrolled or offline; indicates detector online.<br>• **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. |

### 9.2.7 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. |

## 9.2.8 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. |

## 9.2.9 Add Digital Signage Terminal to Area for Current Site

You can add digital signage terminal to areas for the current site for management.

**Before You Start**

The digital signage terminals need to be added to the HikCentral Professional for area management. Refer to ***Manage Digital Signage Terminals*** for details.

**Steps**

**Note**

One digital signage terminal can only belong to one area. You cannot add an digital signage terminal 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 digital signage terminals 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. Click **Digital Signage Terminal** tab.
5. Click + to enter the Add Digital Signage Terminal page.
6. Select the digital signage terminals to add.
7. Click **Add**.
8. **Optional:** After adding the digital signage terminals, you can do one or more of the followings.

| | |
|---|---|
| **Move to Other Area** | Select the digital signage terminals and click . Then select the target area to move the selected digital signage terminals to and click **Move**. |
| **Display Digital Signage Terminals of Child Areas** | Check **Include Sub-area** to display the digital signage terminals of child areas. |

## 9.2.10 Add Speaker Unit to Area for Current Site

You can add speaker unit to areas for the current site for management.

**Before You Start**

The speaker units need to be added to the HikCentral Professional for area management. Refer to ***Group Speaker Units*** for details.

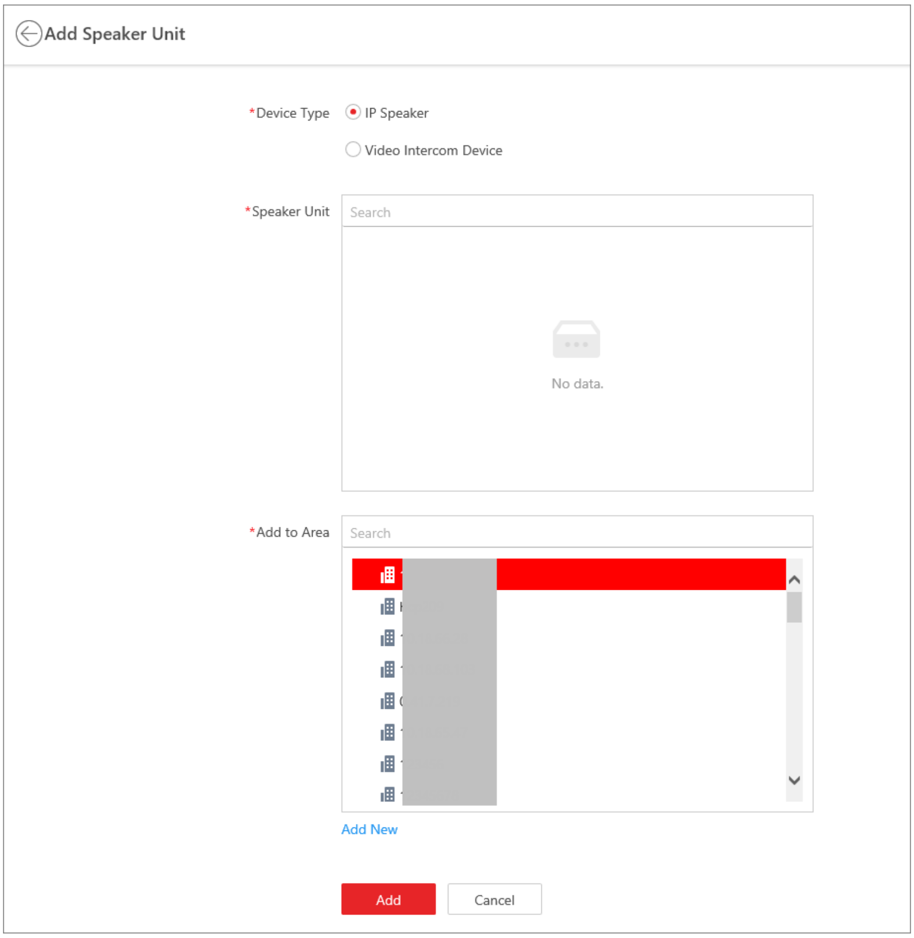
**Steps**

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 for adding speaker unit 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 **Speaker Unit** tab.
5. Click + on the element page to enter the Add Speaker Unit page.




**6.** Select the device type.

**7.** Select the speaker unit(s) to be added.

**8.** Click **Add**.

The 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 doors and click . Then select the target area to move the selected doors to and click **Move**. |
| **Adjust Broadcast Volume** | Select speaker unit(s) and click to adjust the broadcast volume. |
| **Set Geographic Location** | Click to enter Map Settings page. You can search the speaker unit(s) to be added to the 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 and click to search the speaker unit. |

| | |
|---|---|
| **Delete Speaker Unit** | Select the speaker unit(s) and click 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. Click **Save**.
12. **Optional:** Enter the Edit Door page again and click **Copy to** to apply the current settings of the door to other door(s).

### 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. Click **Save**.

11. **Optional:** If needed, enter the elevator editing page again and click **Copy to** to apply the current settings of the elevator to other elevator(s).

### 9.3.4 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.

### 9.3.5 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**.

### 9.3.6 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 input name in the **Name** column.
6. Edit the alarm output name in the pop-up window.

**7.** Click **Save**.

## 9.3.7 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**.

## 9.3.8 Edit Digital Signage Terminal for Current Site

You can edit the name of digital signage terminal for the 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 **Digital Signage Terminal** tab to show the added digital signage terminals.
**6.** Click an digital signage terminal's name in the **Name** column.
**7.** Edit the name in the pop-up window.
**8.** Click **Save**.

### 9.3.9 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**.

### 9.3.10 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*** .

### 9.3.11 Edit Element for Remote Site

If the current system is a Central System with Remote Site Management module, you can edit the cameras added from the Remote 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 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 changes the camera's name, you can click in the added cameras 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.
8. Edit the recording settings of the camera.

**Note**

For recording settings, if no recording settings have been configured for the camera, click **Configuration** 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 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 system for further operations such as access control (adding the person to access group), face comparison (adding the person to face comparison group), time and attendance (adding the person to attendance group), 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 Home Page, select → **All Modules** → **General** → **Person** to enter the person management page.

**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.

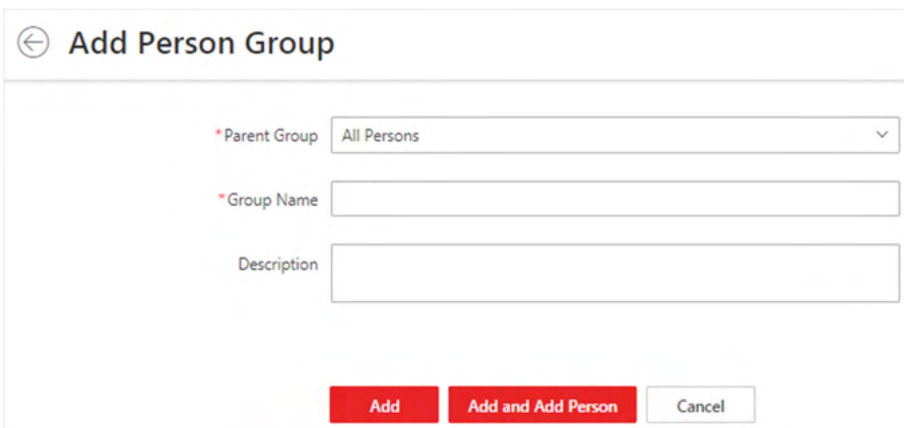



**Figure 10-1 Add Person Group**

**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 **Authenticate via PIN Code**.

1) Click to open the Authenticate via Password window.

2) Set parameters.

**Authenticate via PIN Code**

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.

**Note**

You can set a PIN code for a person when setting basic information for the person. For details, see ***Add a Person Manually*** .

**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 to change their PIN codes.

**Manual**

The system administrator needs to manually filter out persons who have no PIN code or have duplicated PIN codes, and then notify these persons to change their PIN codes.

**Note**

The system administrator needs to notify relevant persons to change their PIN codes in time. Otherwise these persons' access authentication and attendance results will be affected.

## 10.2 Add Person

### 10.2.1 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 and face comparison group. 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.

**3.** Click + .

**Note**

The entry for adding a person varies with your HikCentral Professional license.

[redacted]

**Figure 10-2 The Entry for Adding a Person**

You enter the adding person page.

4. Set the person's basic information, such as first name, last name, and gender.

**ID**

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.

**Person Group**

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 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 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℃, then you can select her/his temperature status as normal.

**Effective Period**

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.

**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 card 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.

**Administrator Permission**

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 1 to 8 digits.
- 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. 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. 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. Enter the custom public information.

**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 the person, you can perform one or more of the following operations.

| | |
|---|---|
| **Edit Person** | Click the person name to edit the person details.<br>**Note**<br>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** | Check the person(s) and click **Delete** to delete the selected person(s). |
| **Delete All Persons** | Hover the cursor onto beside , and then click **Delete All** to delete all persons. |
| **Export the 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 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. |
| **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.<br>a. Select one or more persons, click .<br>b. Select the target person group to which the persons are about to be moved.<br>c. Click **Move**. |

| | |
|---|---|
| **Clear Access Levels** | Select one or more persons, click to clear the access levels of the selected persons.<br>**Note**<br>The access levels of these persons cannot be restored once they are cleared. |
| **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. |

## 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 used for dismiss or used under duress. 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 Home page, select → **All Modules** → **General** → **Person** .
2. Click **Credential Management** to open the Add Credential panel.
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 reading card information via the enrollment station, card enrollment station, or card reader. For details, see ***Batch Issue Cards to Persons*** .
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. Click **Save**.
7. **Optional:** Perform the following operation(s).

| | |
|---|---|
| **Edit Card / Fingerprint Information** | Hover the cursor onto an added card or fingerprint, and then click . |
| **Delete Card / Fingerprint** | Hover the cursor onto an added card or fingerprint, and then click . |

## 10.2.2 Add a Person by Reading from the ID Card

You can add a person by reading the person name, ID photo, and ID number from the person's ID card. Once a person is added in this method, the person can use her/his ID card for access authentication at the access points.

**Before You Start**

Make sure your HikCentral Professional license supports this function. If the function is not supported, you can contact the technical support or after-sales to add the function to your license.

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **General** → **Person** .
2. Hover the cursor onto + , and then click **Read from ID**.

   For the first time operation, a window will pop up to remind you to configure the reading settings (e.g., ID card reader model) first.
3. Configure the reading settings.
   1) Select the model of your reader from **ID Card Reader Model**.
   2) Set **Verify Fingerprint**.

   **Verify Fingerprint**

   After switched on, reading the person information from the ID card will be allowed only when the person's fingerprint matches the fingerprint information contained in the ID card.

   **Fingerprint Security Level**

   Select the fingerprint security level. The higher the security level you set, the lower the False Acceptance Rate (FAR) and the higher the False Rejection Rate (FRR) will be.

   **Fingerprint Recognition Timeout**

   Set the timeout duration for fingerprint recognition.

3) Click **Save**.

The Read from ID panel will be displayed.

4. **Optional:** Click **Configuration** on the Read from ID panel to edit the reading settings.
5. Swipe the person's ID card on the ID card reader to read the person information.

   The person name, ID photo, and ID card No. will be automatically uploaded to the platform.
6. Set other person information, including person ID, effective period, and person group.

   **ID**

   Edit the unique ID for the person on the platform.

   **Effective Period**

   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.

   **Person Group**

   Select a person group to add the person to this group.
7. Click **Add**.
8. **Optional:** Perform the following operation(s).

| | |
|---|---|
| **Edit Person** | Click the person name to edit the person details.<br>**Note**<br>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).<br>Or hove 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 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. |
| **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 . <br> b. Select the target person group. <br> 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. <br><br> **Note** <br> • Make sure you have added indoor stations to the platform. <br> • Up to 10 persons can be linked to one indoor station. And a person cannot be linked to multiple indoor stations. <br> • 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. <br><br> **Note** <br> 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. |

### 10.2.3 Batch Add Persons by Importing Person Information File

You can batch add the information of multiple 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, the access group, and the face comparison group.

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **General** → **Person** .
2. Click → **Import an Excel File** .
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:** Perform the following operation(s).

| | |
|---|---|
| **Edit Person** | Click the person name to edit the person details.<br>**Note**<br>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).<br>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 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. |
| **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.<br>a. Select one or more persons, click .<br>b. Select the target person group to which the persons are about to be moved.<br>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**<br>• Make sure you have added indoor stations to the platform.<br>• Up to 10 persons can be linked to one indoor station. And a person cannot be linked to multiple indoor stations.<br>• 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.<br>**Note**<br>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. |

### 10.2.4 Import Domain Persons

You can batch import the users in the AD 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 Home page, 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:** Perform the following operation(s).

| | |
|---|---|
| **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 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. |
| **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.<br><br>**Note**<br>• Make sure you have added indoor stations to the platform.<br>• Up to 10 persons can be linked to one indoor station. And a person cannot be linked to multiple indoor stations.<br>• 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.<br><br>**Note**<br>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. |

### 10.2.5 Batch Add 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 server, 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 server, 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 by Importing Profile Pictures** .
5. Select the profiles.
   - If you access the platform via the Web Client running on the SYS server, 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 an access control device or a video intercom 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.

## 10.2.6 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.


**Figure 10-3 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.<br>**Note**<br>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).<br>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 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. |
| **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.<br>a. Select one or more persons, click .<br>b. Select the target person group to which the persons are about to be moved.<br>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.<br>**Note**<br>• Make sure you have added indoor stations to the platform.<br>• Up to 10 persons can be linked to one indoor station. And a person cannot be linked to multiple indoor stations.<br>• 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.<br>**Note**<br>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. |

### 10.2.7 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.<br>**Note**<br>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).<br>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 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. |
| **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 . <br>b. Select the target person group to which the persons are about to be moved. <br>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. <br><br>**Note** <br>• Make sure you have added indoor stations to the platform. <br>• Up to 10 persons can be linked to one indoor station. And a person cannot be linked to multiple indoor stations. <br>• 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. <br><br>**Note** <br>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 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.

## 10.3.1 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.

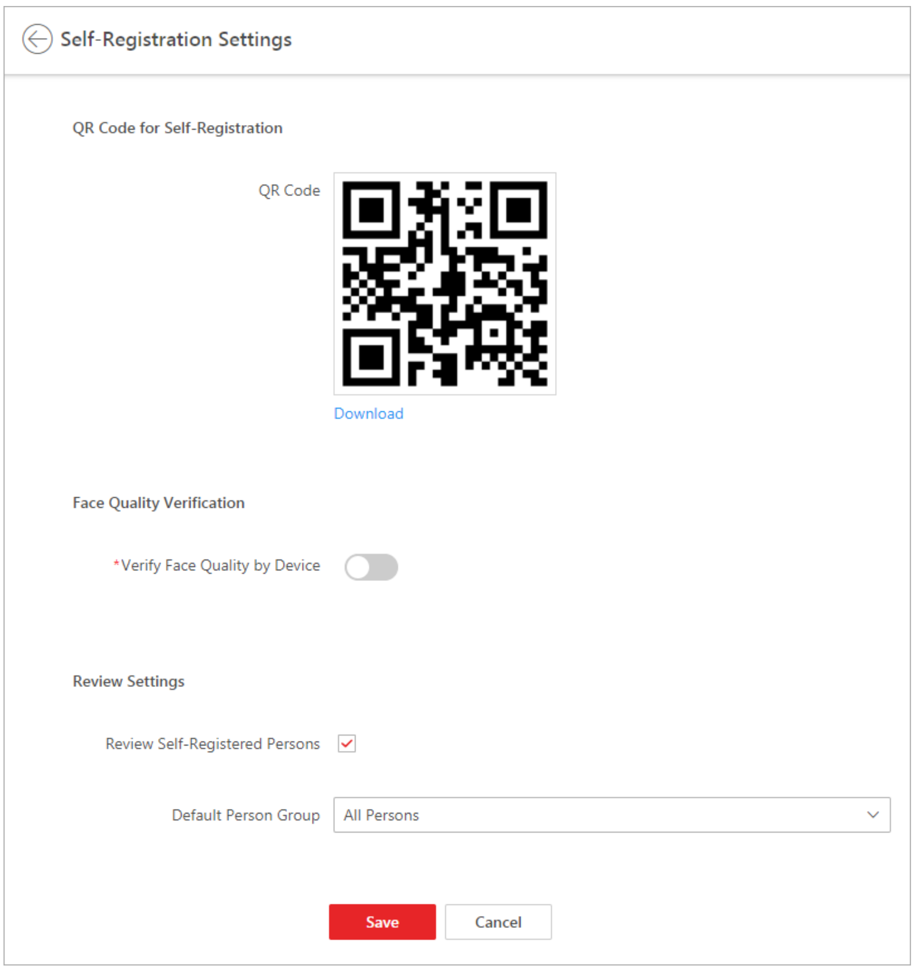



**Figure 10-4 Self-Registration Settings**

### 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.

## 10.3.2 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.

### 10.3.3 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 Home page, select → **All Modules** → **General** → **Person** → **Self-Registration** → **Persons to be Reviewed** .
**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.<br>• Select a registered person, and click to approve the person.<br>• 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.<br>• Select a registered person, and click to reject the person.<br>• 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.<br>• 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.

## 10.4 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 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) and manually entering card numbers.

**Steps**

**1.** In the top left corner of Home page, select → **All Modules** → **General** → **Person** .

**2.** Open the card issuing settings window when managing credentials or batch issuing cards to persons.
   - For opening the window when managing credentials, refer to ***Manage Credentials*** .
   - For opening the window when batch issuing cards to persons, refer to ***Batch Issue Cards to Persons*** .

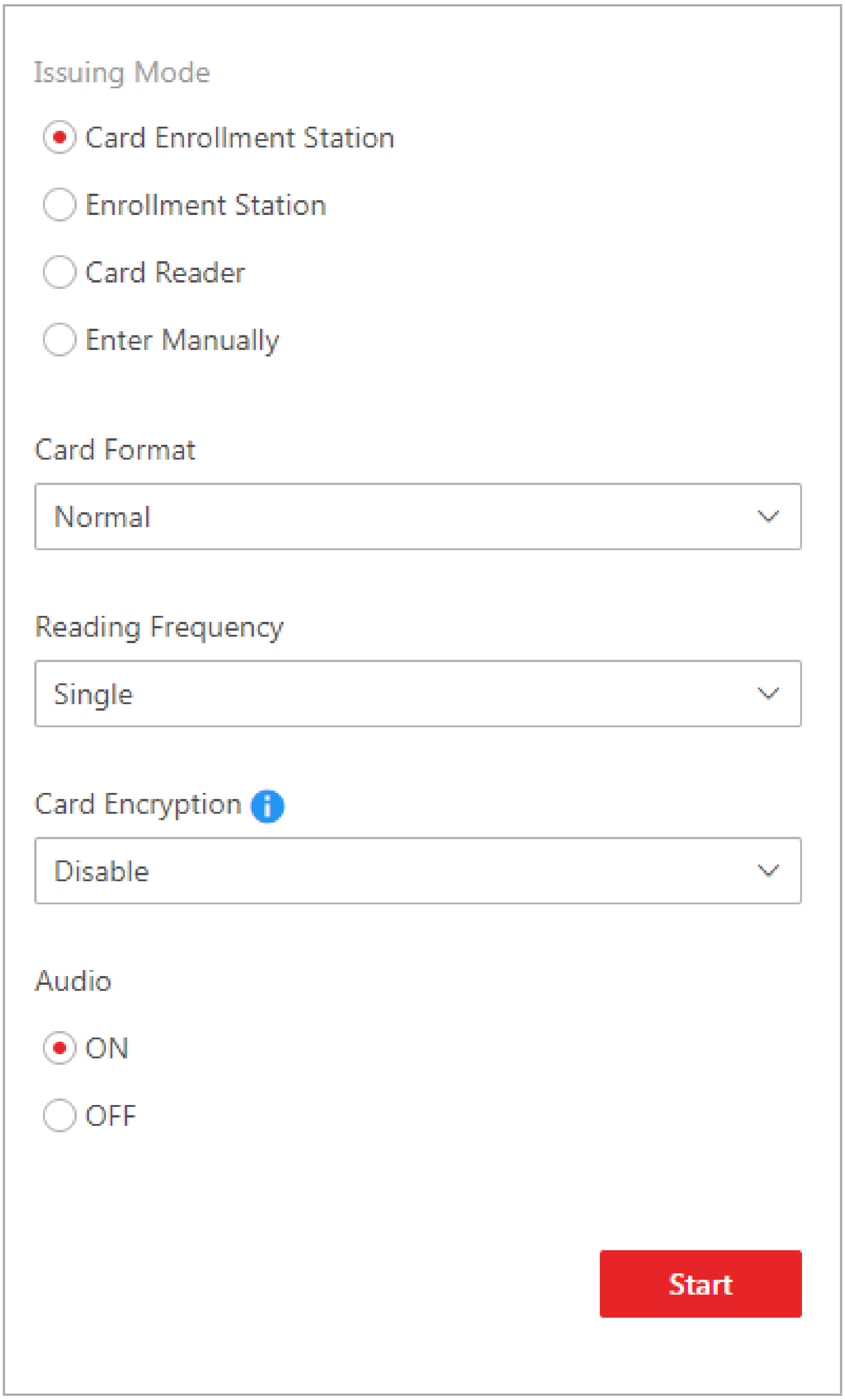



**Figure 10-5 Card Issuing Settings Window Opened when Batch Issuing Cards to Persons**

**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 number.

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 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.

**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.

**RF Card Type**

EM card, M1 card, and ID card are supported.

**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.

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 Home page, select → **All Modules** → **General** → **Person** .
2. **Optional:** Click and set conditions to search for the person 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.


**Figure 10-6 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 Home page, select → **All Modules** → **General** → **Person** .
2. **Optional:** Click and set 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 panel
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:** Click and then set 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 10-7 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).

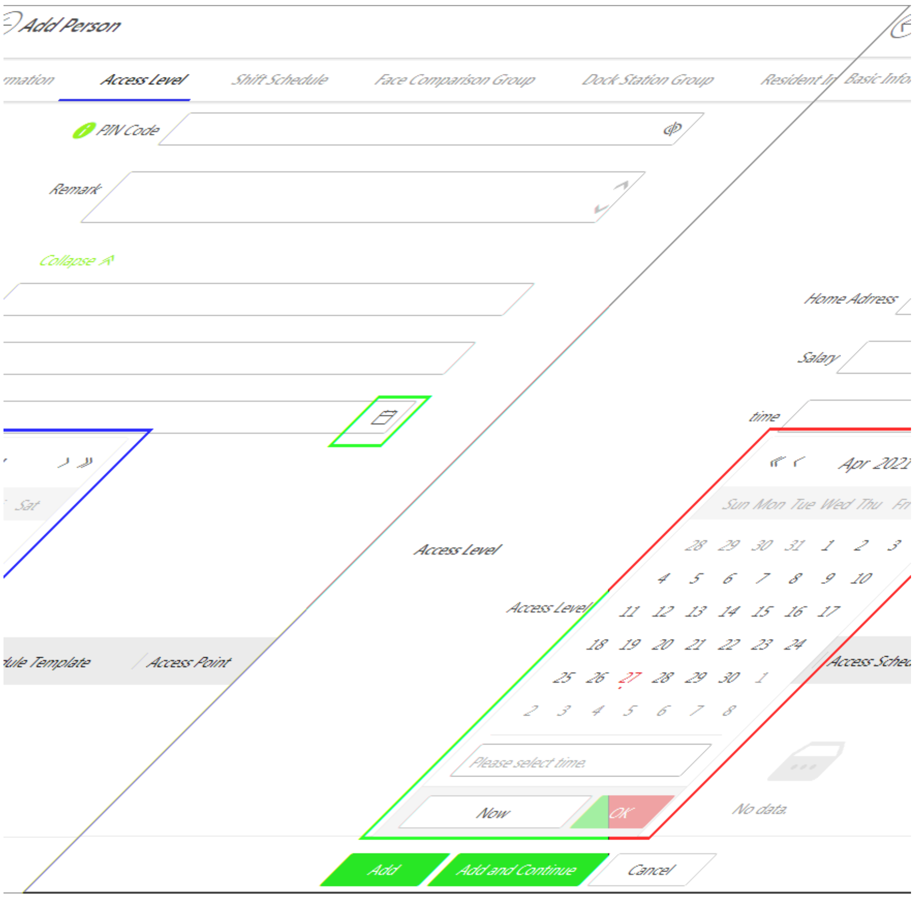



**Figure 10-8 If You Select Date as the Type**

**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** → **Security** .
2. Click **Roles** on the left.
3. Click **Add**.

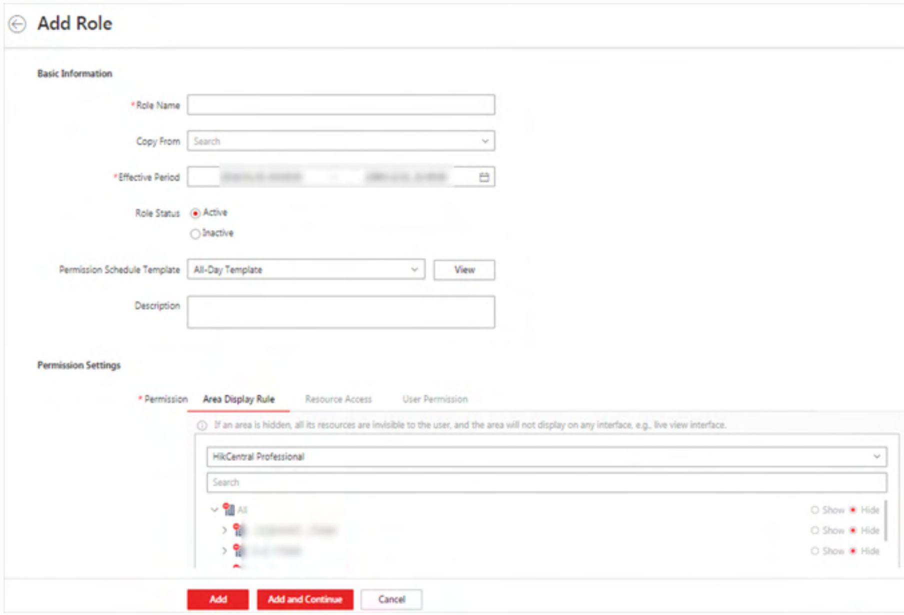


**Figure 11-1 Add Role Page**

**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.

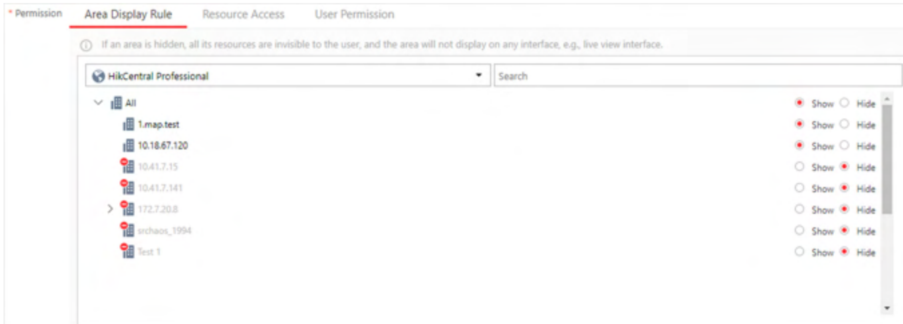



**Figure 11-2 Area Display Rule**

### 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.

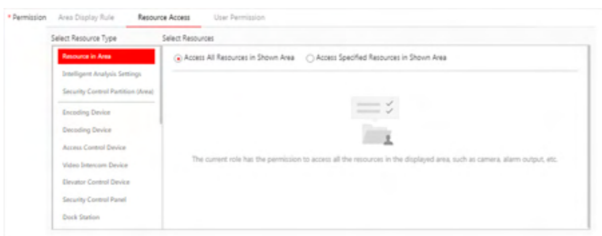


**Figure 11-3 Resource Access Permission**

### User Permission

Assign resource permissions, configuration permissions, and operation permissions to the role.

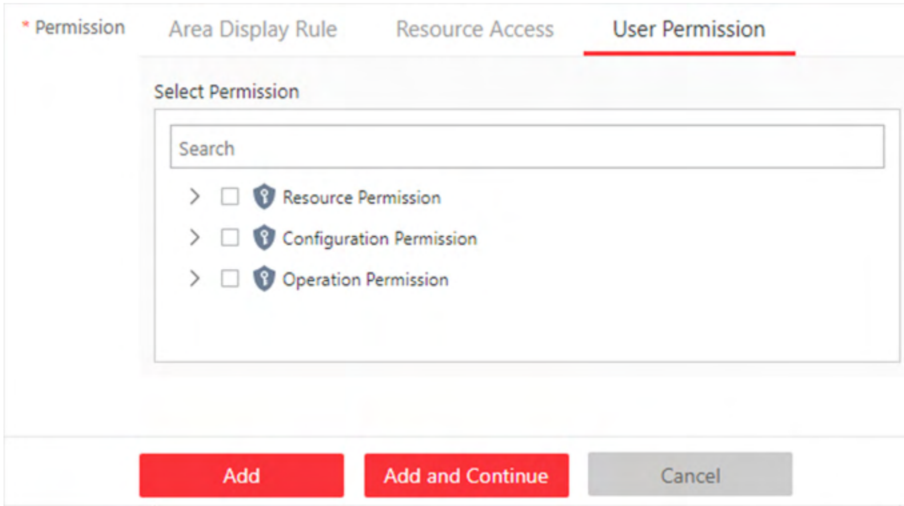



**Figure 11-4 User Permission**

**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.

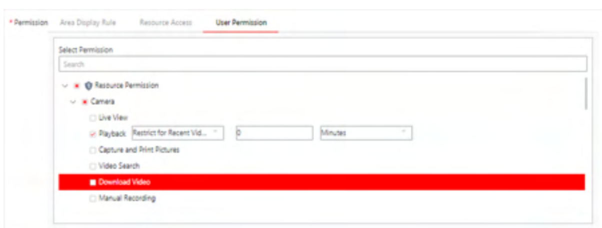


**Figure 11-5 Playback Permission**

**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** → **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.

**Automatically Receive Alarm**

Switch on and users with this role will receive resource alarms no matter configured as recipients of each alarm individually or not.

**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.

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.<br>**Note**<br>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. For details about changing password, refer to ***Change Password for Reset User*** . |
| **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.<br>• 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** → **Security** .

**2.** Click **Users** on the left.

**3.** Click **Import Domain Users**.

**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.

**Belong to**

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. Switch on **Automatically Receive Alarm**, and the users can receive all alarms of resources they have permission to access even if they are not configured as recipients when adding alarms.
9. 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.

10. 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.
11. **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.

## 11.3.1 Change Password of Current User

You can change the password of your currently logged-in user account via Web Client.

**Steps**

1. Move the cursor to the user name at the top-right corner of the Web Client.
2. In the drop-down list, click **Change Password** to open the Change Password panel.

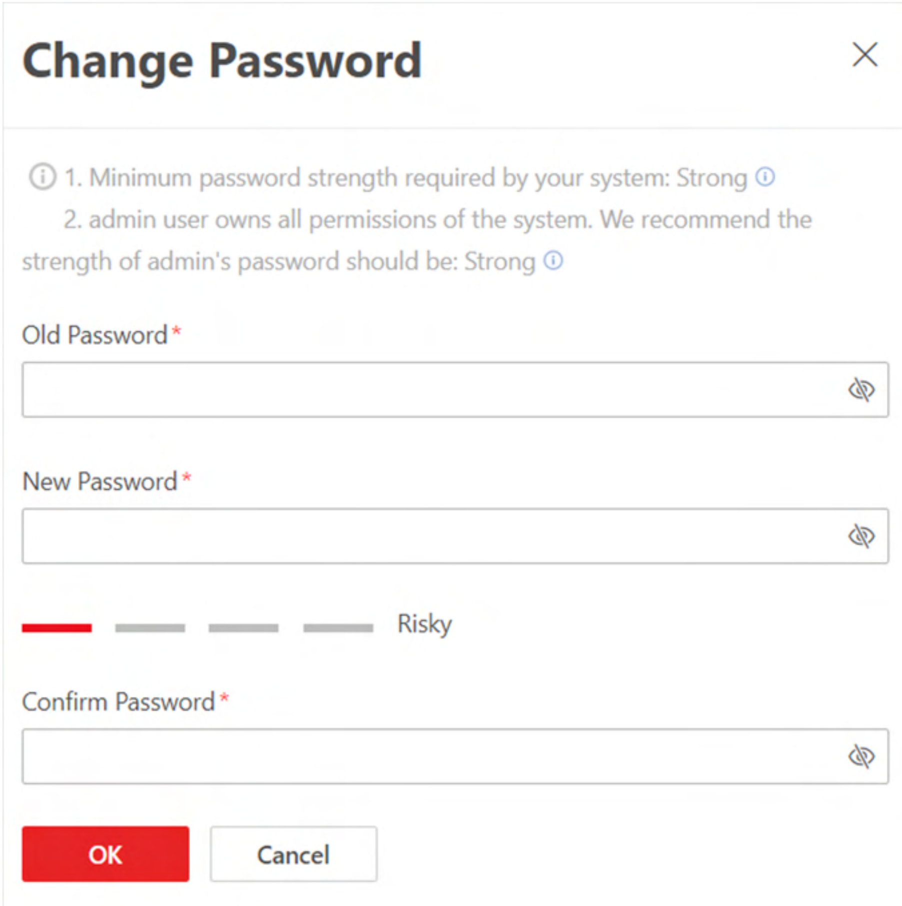



**Figure 11-7 Change Password Panel**

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.

## 11.4 Reset Password for Admin User

If you forget the password of the admin user, you can reset the password for the admin user.

**Steps**

**1.** Use a web browser to enter the IP address of the PC running SYS service.

**Example**

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

**Note**

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

**2. Optional:** When you log in for the first time, you need to install the plug-in before you can access the functions.

**Note**

If a new version of plug-in is detected, you should update it to ensure the proper usage and better user experience.

**3.** Enter ***admin*** in **User Name**.

**4.** Click **Forgot Password** to open the Reset Password panel.

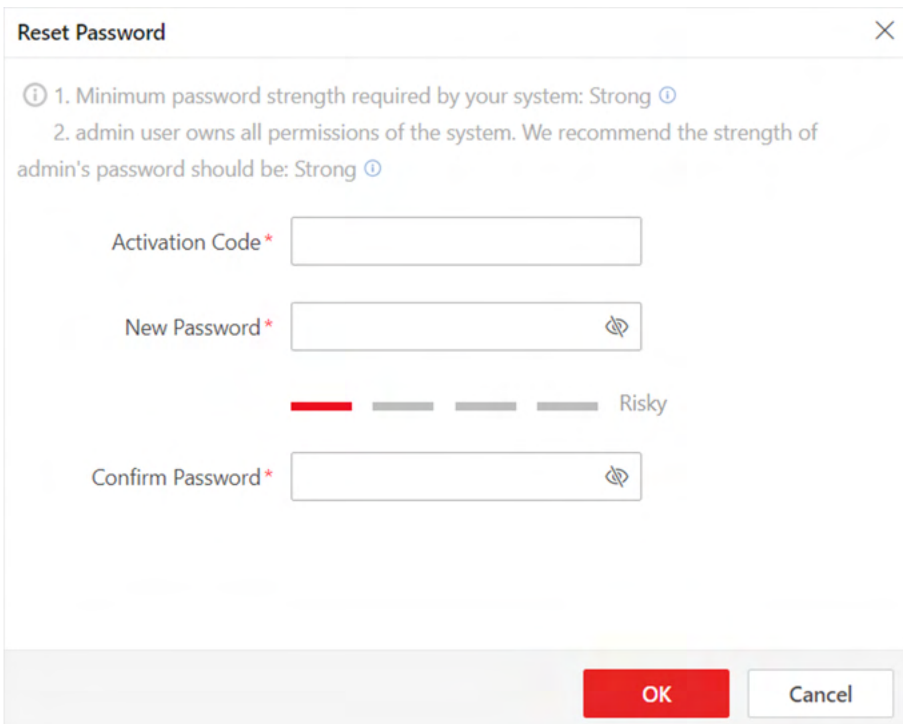



**Figure 11-8 Reset Password**

**5.** Enter the activation code 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.

6. Click **OK** to reset the password for admin user.

## 11.5 Reset Password for Normal User

If a normal user forget the password, the admin user or users with administrator role can reset the password for the normal user.

**Steps**

**Note**

If the normal user account is configured with an email address, the user can set a new password via email without requesting help from the admin user or user with administrator role. For details about setting user email address, refer to ***Add Normal User*** .

1. In the top left corner of Home page, select → **All Modules** → **Security** .
2. Click **Users** on the left.
3. Click the name of the user to enter the user detail page.
4. Click **Reset** and set a new password for the user.

## 11.6 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** → **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**

To copy the settings from another existing template, select the template from the drop-down list.

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:** Holiday schedule has a higher priority than weekly schedule. 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.
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. |
| **Delete Template** | Click a template, and click to delete it. |

**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** → **Security** .

**2.** Click **Security Settings** on the left.

**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.** 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.

5. 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.

6. 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.

   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.
7. 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.

### 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.

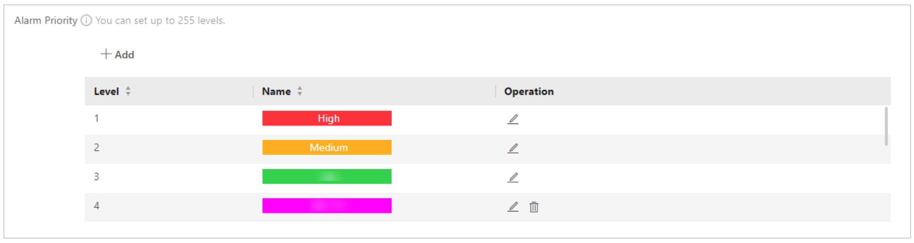



**Figure 13-1 Alarm Priority**

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.

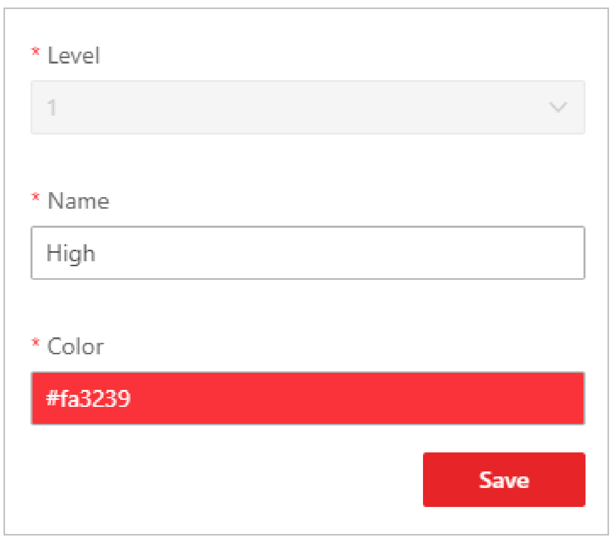



**Figure 13-2 Alarm Priority Settings Window**

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.


**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.

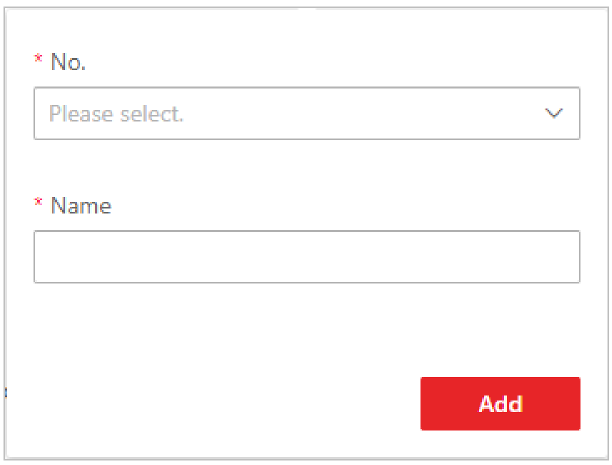



**Figure 13-4 Alarm Category Settings Window**

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.

**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.

## 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).

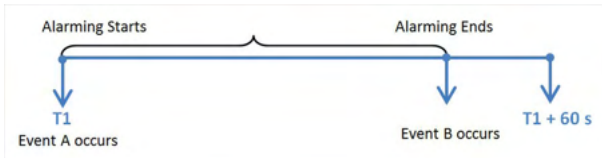



**Figure 13-6 Receiving Schedule 1**


**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.

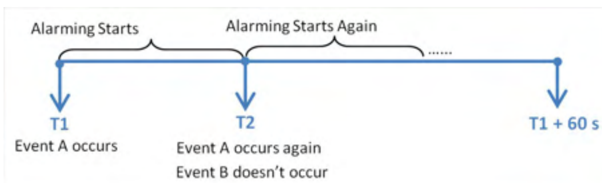



**Figure 13-8 Receiving Schedule 3**

## 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.

**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.<br>Click in the Operation column to enter the alarm details page and click **Copy to**.<br>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).

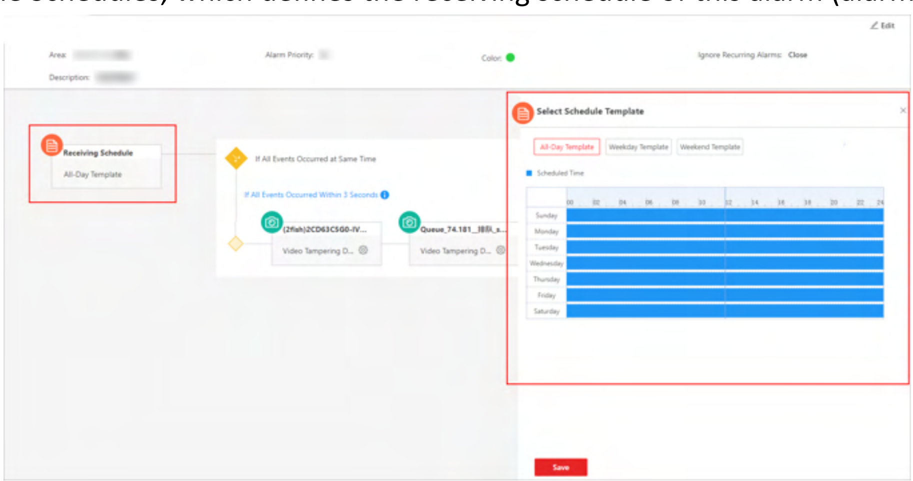



**Figure 13-9 Receiving Schedule**

   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.

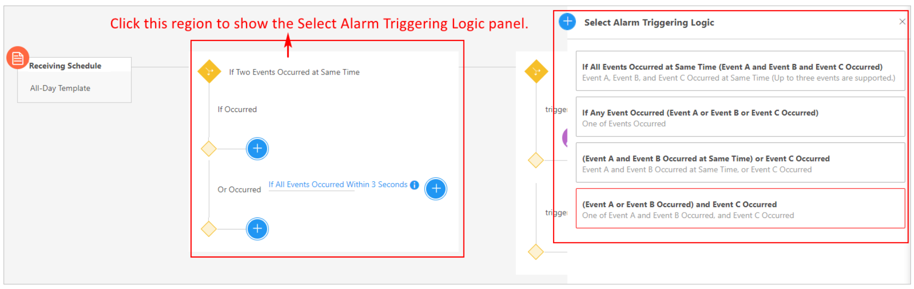



**Figure 13-10 Select Triggering Logic**

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.

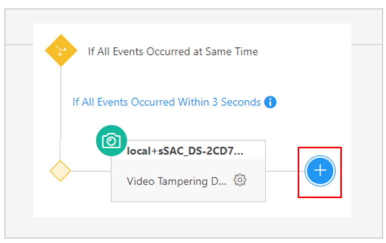



**Figure 13-11 Add New Event Type and Source**

**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.

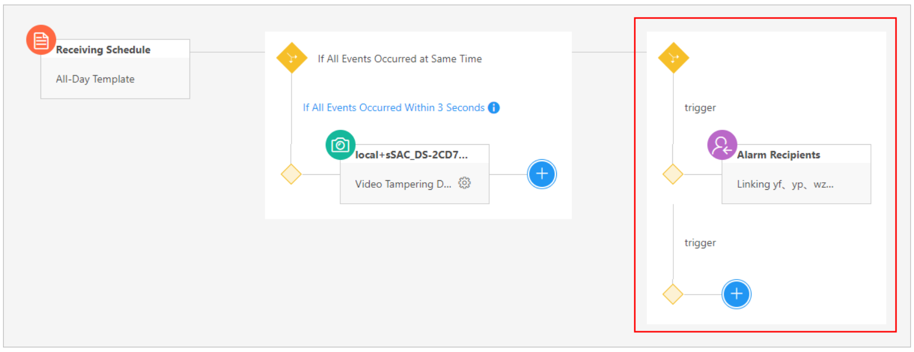



**Figure 13-12 Action**

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.

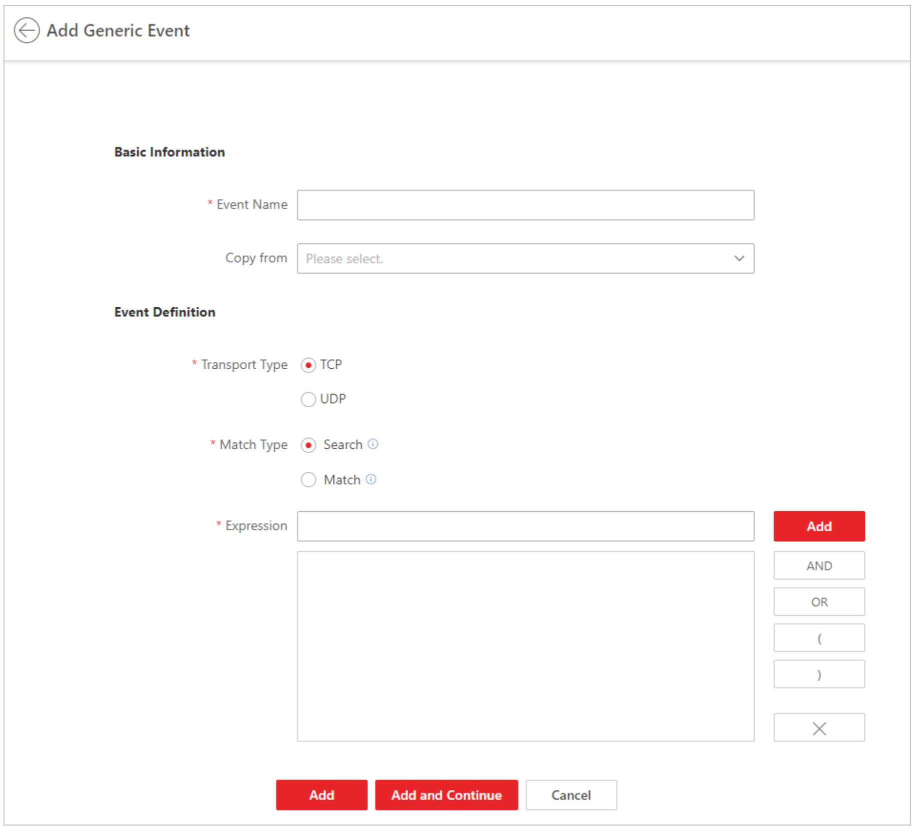



**Figure 13-13 Add Generic Event Page**

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** or **UDP** to select the package transmission method as TCP or UDP protocol.
6. Select the match type which indicating 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 search the results to look for the packages that contained 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 and/or UDP 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.

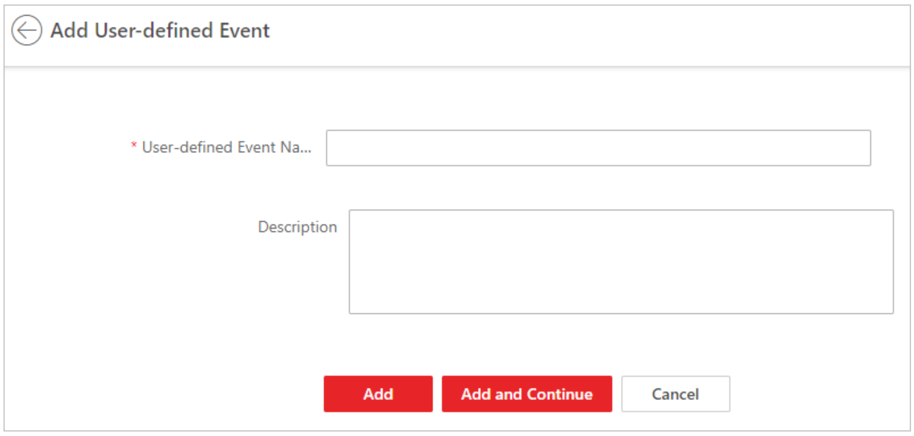



**Figure 13-14 Add User-Defined Event**

**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 pre-defines 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.

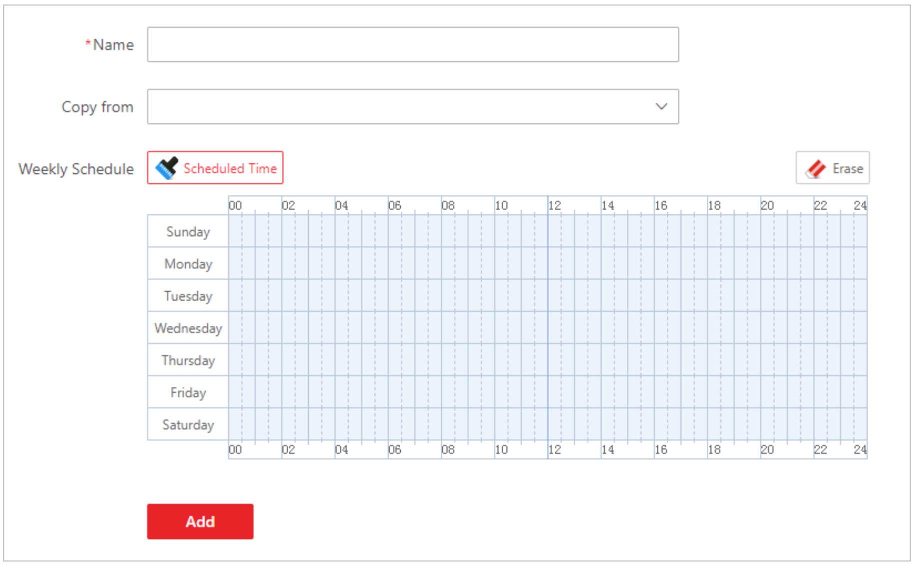



**Figure 13-15 Add Receiving Schedule Template**

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 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.

### 13.5.1 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 **Set** in the upper-right corner to customize the event or 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.

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.

### 13.5.2 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. Enable **Event & Alarm Name** to select the event/alarm name in the drop-down list.
8. Click **Search**.

   The matched event or alarm logs display on the list.
9. **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.

## 13.6 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 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

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

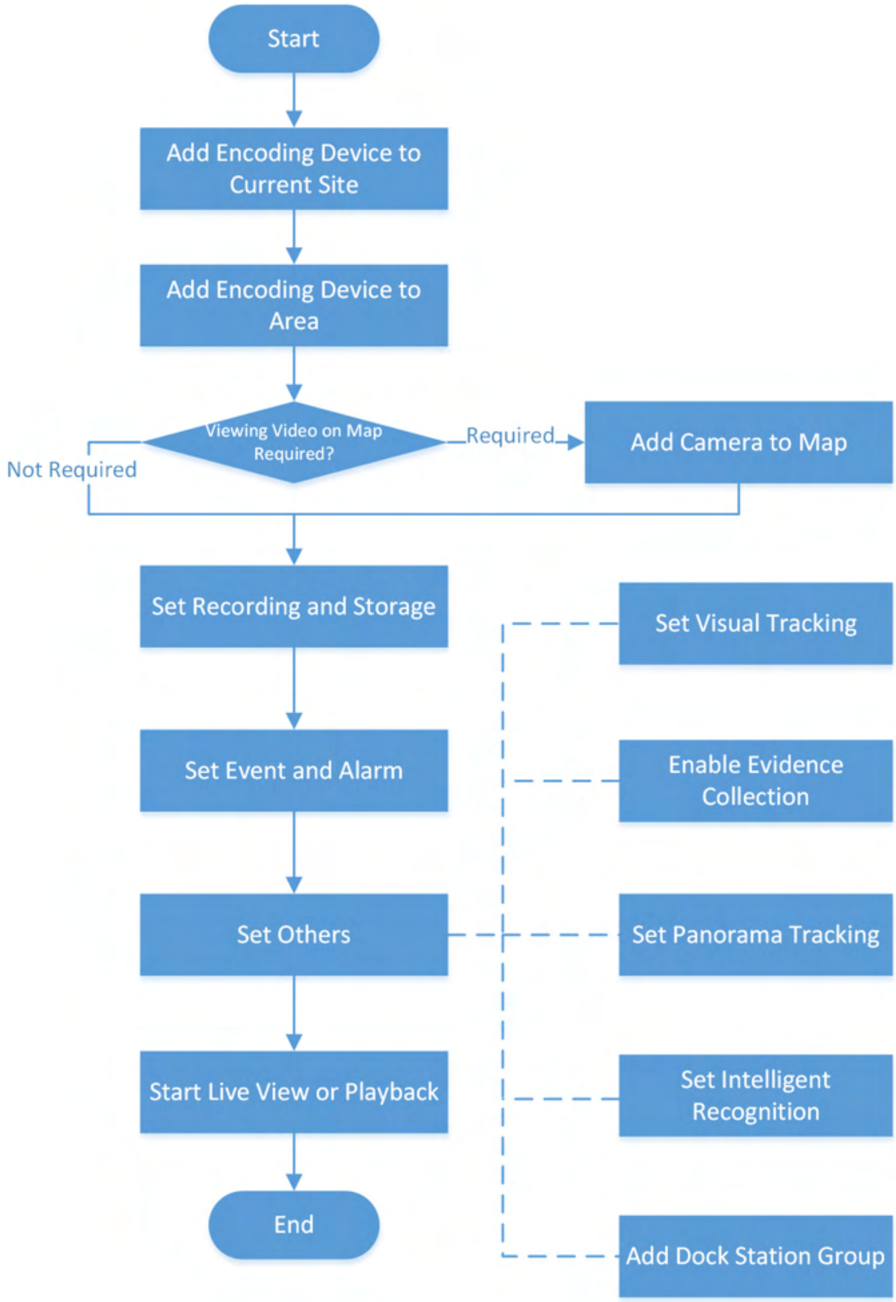



**Table 14-1 Flow Chart Description**

| 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.<br>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.<br>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).<br>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.<br>For details, see ***Event and Alarm Configuration*** . |
| Configure Others | You can configure other video related functions including visual tracking, evidence collection, smart linkage, intelligent recognition, and dock station group.<br>• Configure Video Tracking: Video 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*** .<br>• Configure Evidence Collection: Only when evidence collection is enabled on the Web Client, can operators save specific video footage as evidence and search the saved evidence on the Control Client. For details about enabling this function, see ***Enable Evidence Collection*** .<br>• Configure Smart Linkage: Smart linkage 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.<br>For details about configuring this function, see ***Configure Panorama Tracking*** . |

| Procedure | Description |
|---|---|
| | • Configure Intelligent Recognition: Intelligent recognition refers to the recognition of faces, body features, or behaviors, etc., by intelligent analysis devices added to the platform. For details configuring this function, see ***Intelligent Recognition*** .<br>• 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.<br>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. For details, see ***Video Application*** . |

## View Videos of Encoding Devices on Remote Site

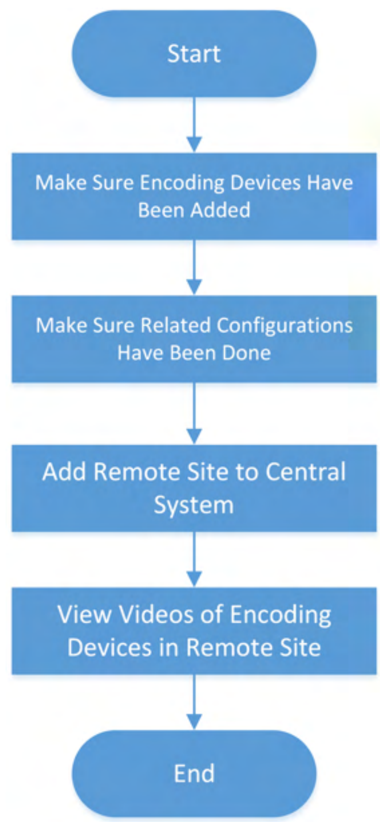


**Table 14-2 Flow Chart Description**

| 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.<br>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.<br>For details, see ***Video Application*** . |

## 14.2 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.

### 14.2.1 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 14-1 Add Remote Site

**3.** Select **IP/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.

**Alias**

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.

**Figure 14-2 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.

### 14.2.2 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 ientering 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.

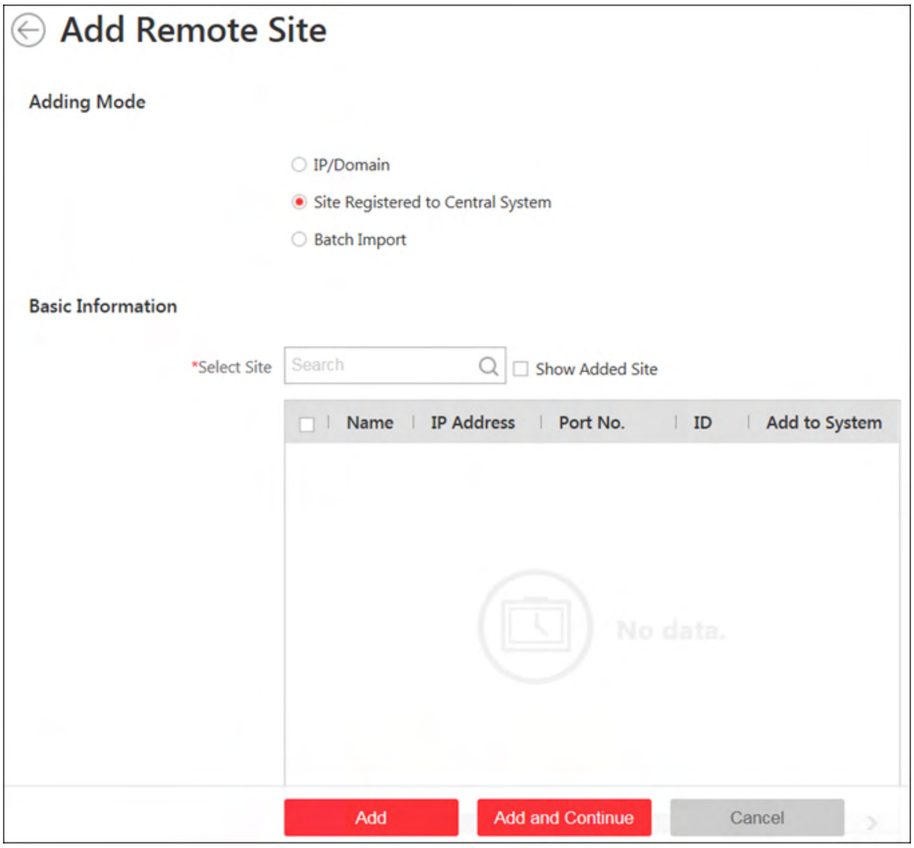



**Figure 14-3 Add Remote Site Page**

**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. Finish adding Remote Site.
   - Click **Add** to add the Remote Site and back to the Remote Site list page.
   - Click **Add and Continue** to save the settings and continue to add other Remote Sites.

### 14.2.3 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.

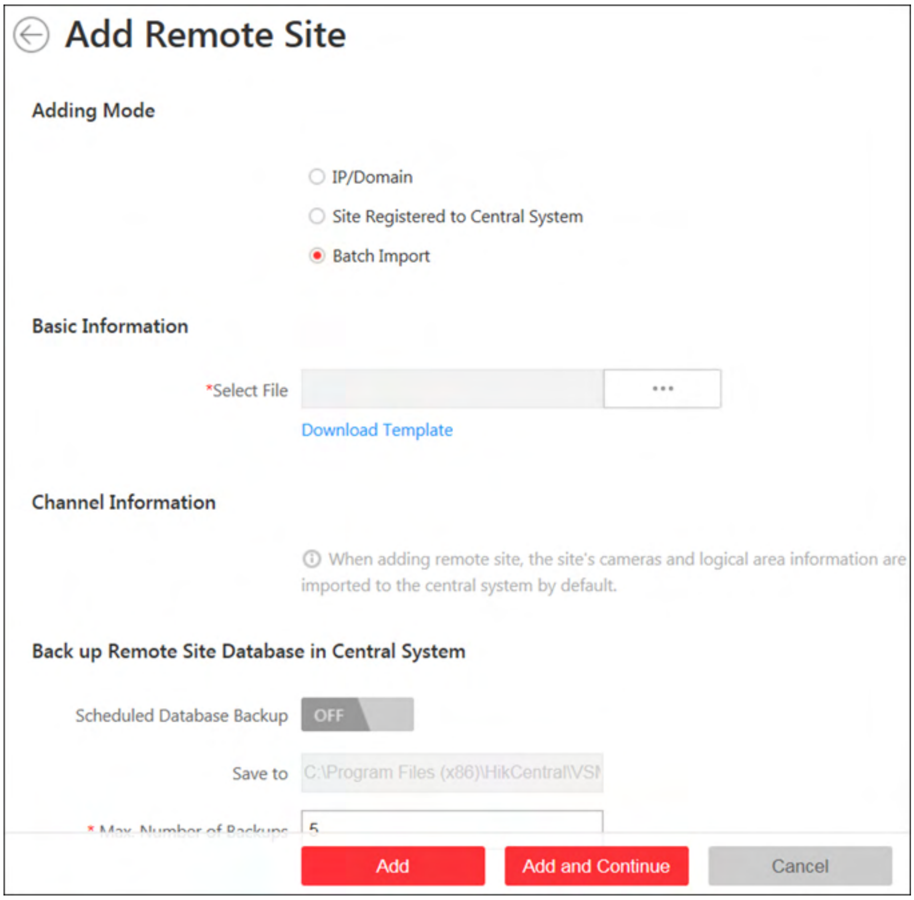



**Figure 14-4 Add Remote Site**

**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.** Finish adding Remote Site.

- Click **Add** to add the Remote Site and back to the Remote Site list page.

- Click **Add and Continue** to save the settings and continue to add other Remote Sites.

### 14.2.4 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.

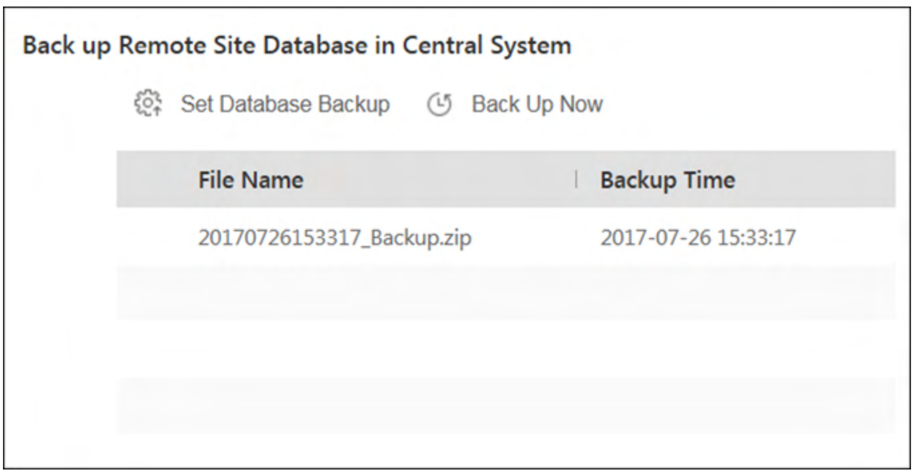



**Figure 14-5 Back up Remote Site Database in Central System**

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.

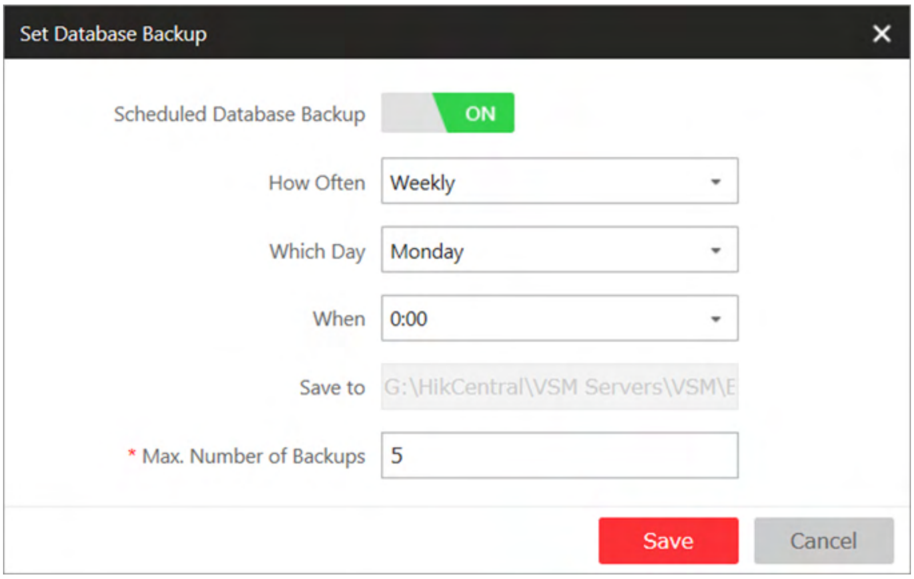



**Figure 14-6 Set Database Backup**

2) Set the **Scheduled Database Backup** switch as **ON** 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 **Maximum 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.

### 14.2.5 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**.

### 14.2.6 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.

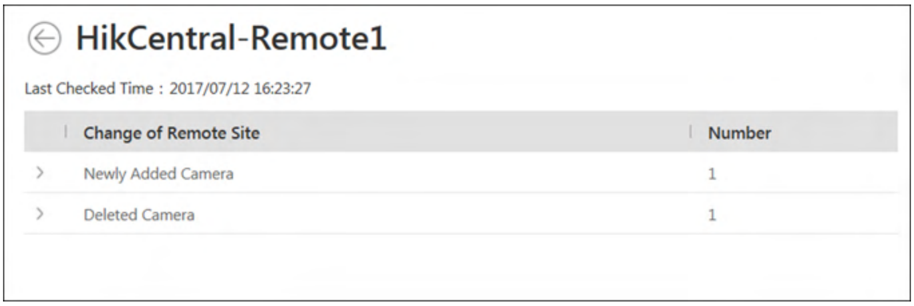



**Figure 14-7 Remote Site Management**

**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.

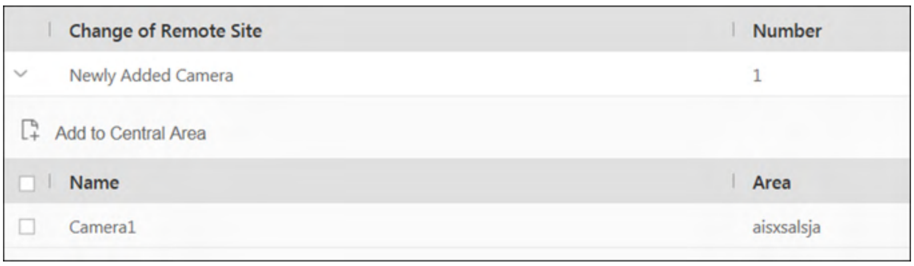



**Figure 14-8 Changes of Remote Site**

   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.

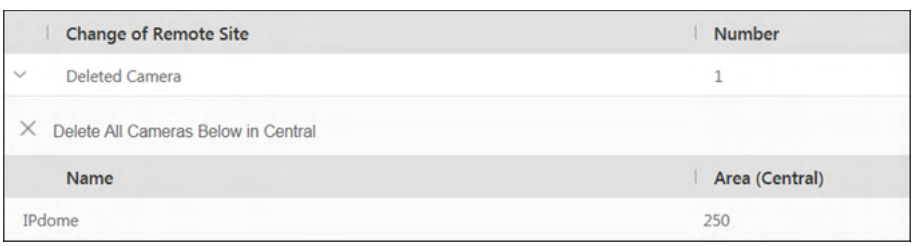



**Figure 14-9 Change of Remote Site**

   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.

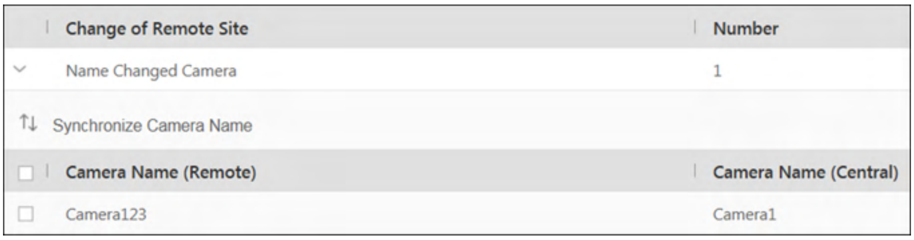



**Figure 14-10 Name Changed Camera**

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.

## 14.3 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. And 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, or 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** → **Device Management** → **Encoding Device** → ), and then click **Storage** → **General** , and then select the HDD, Net HDD or SD/SDHC card, and finally click **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*** .

## 14.3.1 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.

**Note**

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.

**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.

**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.

**Recording Server Gets Video from Camera**

If you select **Hybrid Storage Area Network**, **Cloud Storage Server**, **pStor** or **pStor Cluster Service** as the storage location, set the **Recording Server Gets Video from Camera** switch to on. And then configure the camera IP address, camera port, user name and password.

**Note**

- After the function is enabled, the recording server gets videos from the camera directly, avoiding the risk that if the NVR camera connected is offline, the recording server can not get video from the offline NVR.
- By default, the camera IP address is the IP address of current camera, you can also edit the IP address as the other camera's.

- 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 to**

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.

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**.

## 14.3.2 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.

   **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.
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.

     **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**.

## 14.3.3 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 **Restrict Quota for Pictures** and set the storage quota for the pictures.
4. Configure the related parameters for storing files.
   1) Select the disk to store the files.

      **Note**

      The disk should have at least 9 GB of free space for file storage.
   2) **Optional:** Switch on **Restrict Quota for Files** and set the storage quota for the files.
   3) 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 **Save**.

### 14.3.4 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.

### 14.3.5 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.

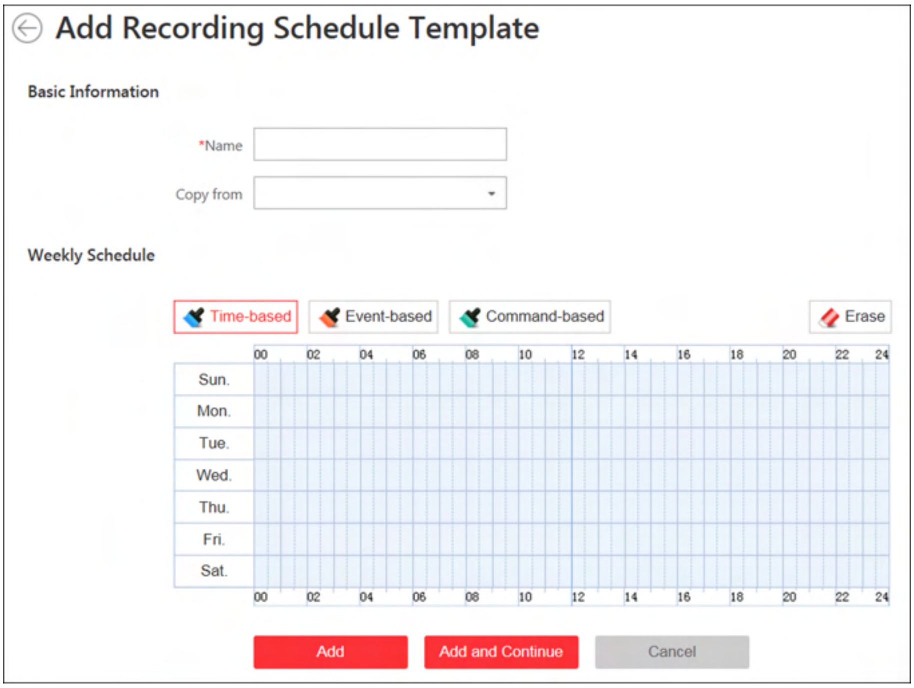



**Figure 14-11 Adding Recording Schedule Template Page**

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. Finish adding the template.
   - Click **Add** to add the template and back to the recording schedule template list page.
   - Click **Add and Continue** to save the settings and continue to add other template.
7. **Optional:** Perform the following operations on the recording schedule template list page.

| | |
|---|---|
| **View Template Details** | Click the template to check the detailed settings. |
| **Edit Template** | Click in the Operation column to edit template details (except the template(s) in use). |
| **Delete Template** | Click in the Operation column to delete the template. |
| **Delete All Templates** | Click **Delete All** to delete all the schedule templates (except the default templates and the template(s) in use). |

## 14.4 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 14-12 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 14-13 Surveillance Image of Camera A**

## 14.5 Enable Evidence Collection

Only when evidence collection is enabled, can the operators save specific video footage as evidence and search the saved evidence on the Control Client. Evidence collection is helpful for settling issues such as traffic disputes and criminal cases.

**Before You Start**

Make sure you have configured a SFTP (Secure File Transfer Protocol) server.

**Steps**

**Note**

Operator is the role that has all the permission for operating the Control Client and the permission for operating the Applications (Live View, Playback, and Local Configuration) on the Web Client. For details about configuring users and roles, see ***Role and User Management*** .

1. In the top left corner of the Home page, select → **All Modules** → **Video** → **Video Settings** → **Event Collection** .
2. Turn on **Evidence Collection**.

   The required information for enabling evidence collection will be displayed.
3. Set the required SFTP parameters.

   **SFTP Address**

   Enter the IP address of the SFTP server.

   **Port**

   Enter the port number of the SFTP server.

   **User Name**

   Enter the user name of the SFTP server.

   **Password**

   Enter the password of the SFTP server.
4. Set other required parameters for the evidence.

   **Evidence Type**

   Define the evidence types that the operators can select when they edit evidence information on the Control Client.

   **Organization on Site**

   Define the type(s) of organization on site that the operators can select when they edit the evidence information on the Control Client.

   Organization on site refers to the organization or personnel (e.g., police, fire department) on the site of the accident or criminal incident.

   **Result/Conclusion**

Define the evidence-related incidents' results or conclusions that the operators can select when they edit evidence information on the Control Client.

5. Click **Save** to enable evidence collection.

## 14.6 Set Network Parameters

You can set parameters for registering the platform without Remote Site Management module (or Remote Site) to the Central System, set access mode for encoding and decoding devices, and set the waiting time for the configurations.

**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 **HikCentral Professional 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.

**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.

**Note**

The two parameters **Register to Central System** and **Receive Site Registration** are not available at the same time.

3. Click **Save**.

## 14.7 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 → Panorama Tracking Settings** .
2. Select one area on the area list.
3. In the Basic Information, click **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 14-14 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.

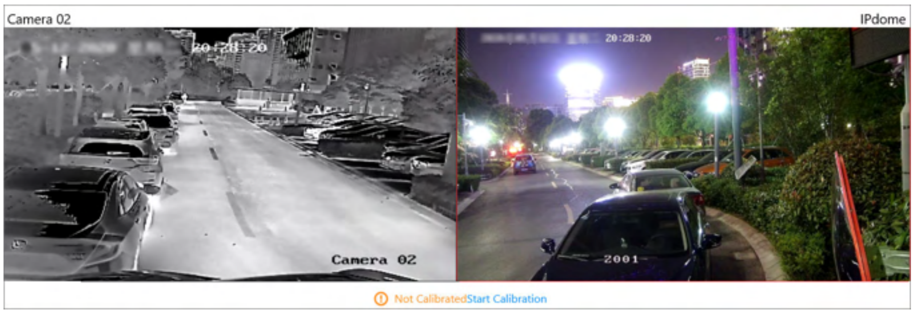



**Figure 14-15 Auto Calibrating**

**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. |

## 14.8 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.

### 14.8.1 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 Face Comparison Group

You need to add a face comparison group and add person(s) 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 panel.
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:** Select a group from the group list and then click to delete the group.

**7.** Click **Add → Add New Person** or **Add → Add Existing Person** to add person(s) to the group.

| | |
|---|---|
| **Add New Person** | Select the group from the group list, and then click **Add → Add New Person** to enter the Add New Person page, and then 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 the group from the group list, and then click **Add → Add Existing Person** to open the person list window, and then search for person(s) or select person(s) from the person list, and then click **Add**. |

**Note**

You can check **Include Sub-Group** to include the persons in sub-groups to the persons available for your selection.

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

**8.** Enter the required person information such as ID, first name, and last name.

**9.** Add 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.

**10. Optional:** Delete person(s) added to a group.

| | |
|---|---|
| **Delete Specific Person(s)** | Select a group from the group list, and then select specific added person(s), and then click **Delete** to delete them. |
| **Delete All Persons** | Select a group from the group list, and then hover the cursor over and click **Delete All** to delete all persons from the group. |

**11. Optional:** Perform one or more of the following operations.

| | |
|---|---|
| **Manage Persons in Face Comparison Group** | Click the added face comparison group and the persons in this group will be displayed on the right.<br>You can add more persons into this group, or perform other operations such as importing and exporting persons. For details, refer to ***Person Management*** . |
| **Edit Face Comparison Group** | Click in the Operation column to edit its details and edit the cameras that it is applied to. |
| **Export All Face Information in a Group** | a. Click **Export** to open the password settings window.<br>b. Create a password for decompressing the exported file, and then confirm it. |
| **Delete Face Comparison Group** | Select one face comparison group and click to delete it. |

| | |
|---|---|
| **Delete All Face Comparison Groups** | Click **Delete All** to delete all the added face comparison groups. |

## 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 panel.
3. Select **Encoding Device** or **Facial Recognition Server** from the Device Type field.

   The available device(s) will be displayed.


**Figure 14-16 Import Face Comparison Group from Device Panel**

**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.

## Import Zipped Profile Pictures

You can batch import profile pictures zipped in an archive 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 panel.
4. Click to select a ZIP file from the local PC.
5. Click **Import**.

## 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 panel.
4. Click **Download Template** in the panel to download the template.
5. Fill required information in to 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 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 open the Import from Enrollment Station panel.

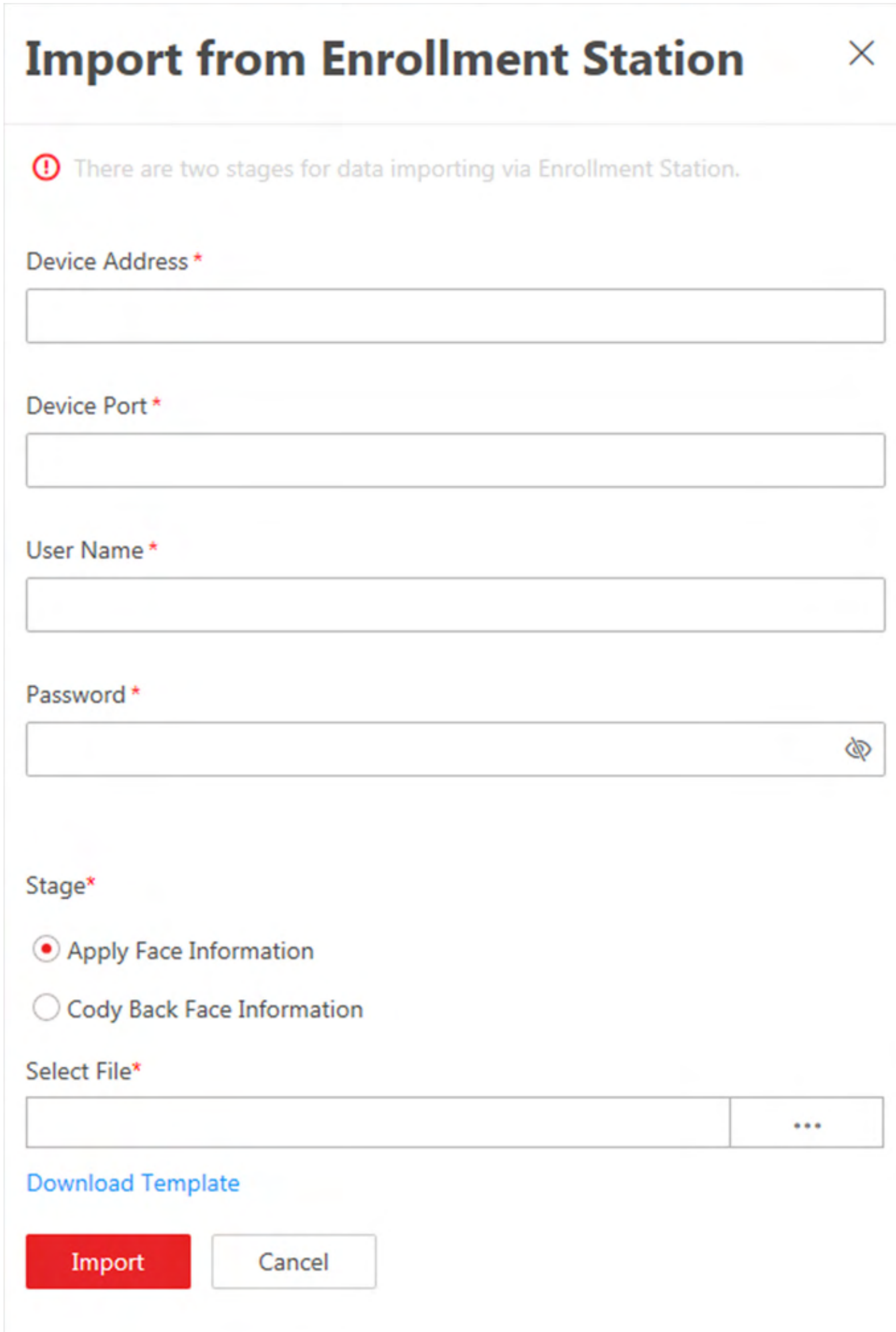



**Figure 14-17 Import from Enrollment Station**

**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**.

## 14.8.2 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. |

## 14.8.3 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.

## 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** .
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.

## 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 person group from the person 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 person group from the person 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 Failed to Be Applied**, select a person group from the person group list in the left side, 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 **Faces to Be Applied**, select a person group from the person group list in the left side, 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.

## 14.8.4 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 04 : 00 – 04 : 30 . |
| **Erase Task Time** | Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period. |

**6.** Click **Add**.
**7. Optional:** Select a task from the task list, and then click to delete it.

## 14.9 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 dock station, see the user manual of the device.
- For details about searching video footage of the dock stations, see the *User Manual of HikCentral Professional Control Client*.

### 14.9.1 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.

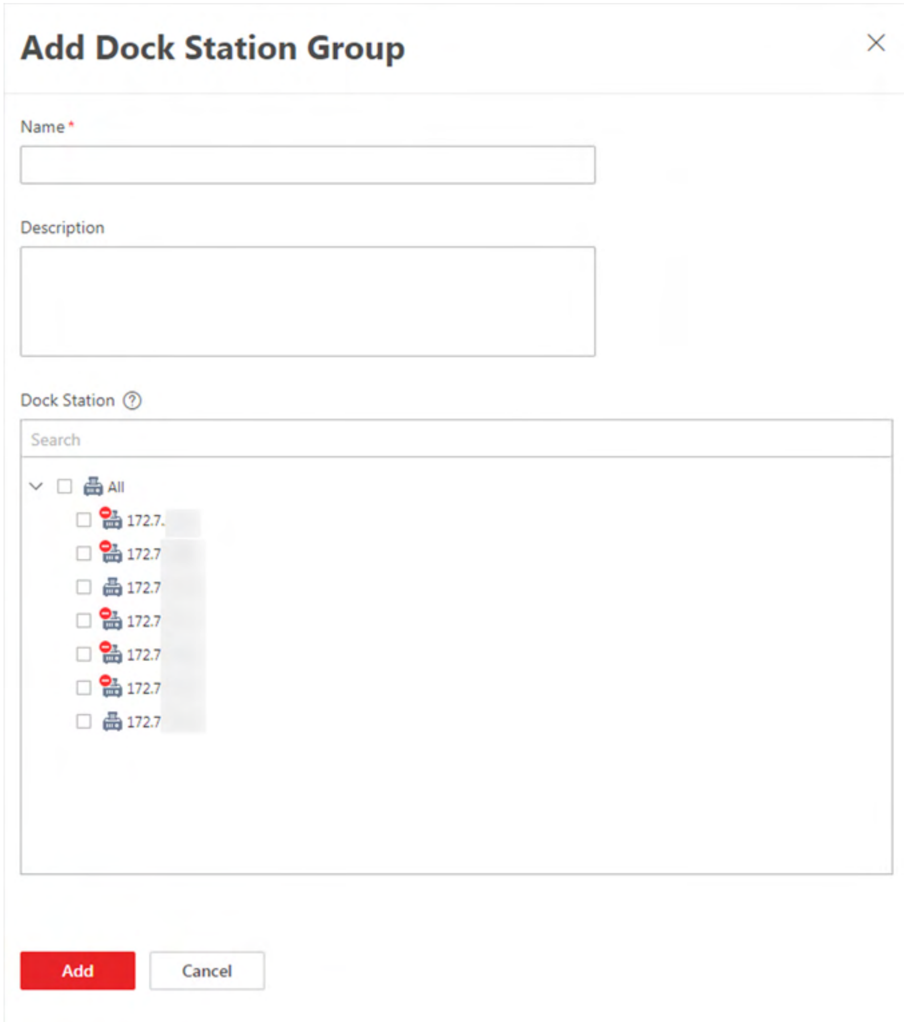



**Figure 14-18 Add Dock Station Group**

**3.** Set 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 will be displayed in the dock station list.

**5. Optional:** Click to edit the dock station group.

**6.** Add person(s) to the dock station group.

**Note**

Up to 20 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.
5) **Optional:** 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 the pop-up **Delete All** to delete all persons in the group.

## 14.10 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.

### 14.10.1 Live View

In the Live View module of Web Client, you can view the live video of the added cameras and do some basic operations, including picture capturing, recording, PTZ control, and so on.

### Start Live View

After adding cameras into areas, you can use live view to play the live footage of cameras and perform basic operations via the Web Client.

**Before You Start**

- Make sure you have added cameras to areas. For details, refer to ***Add Camera to Area for Current Site*** .
- If the system is Central System with Remote Site Management module, you can also view the live image of the cameras imported from remote sites. For managing remote site's cameras, refer to ***Add Camera to Area for Remote Site*** .

**Steps**

1. In the top left corner of Home page, select  → **All Modules** → **Video** → **Video Application** .
2. Click **Live View** on the left.
3. **Optional:** If you have added remote site to the platform, select a site from the drop-down list to show the area and cameras in the site.
4. **Optional:** Move the cursor to a camera to see the live view thumbnail.

**Note**

To search a camera or area, enter a keyword of camera name or area name in the search field and search.

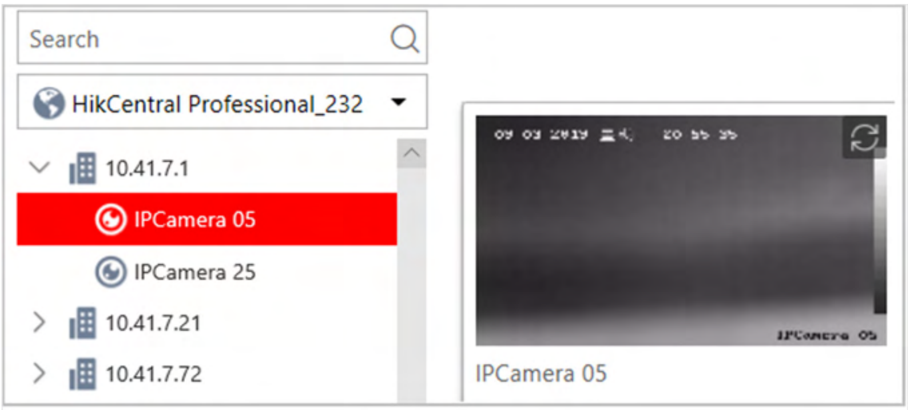



**Figure 14-19 Thumbnail**

5. Do one of the following to start live view.
   - To start the live view of a camera, drag the camera to a display window or select a display window and then double-click the camera.
   - To start the live view of all cameras in an area, drag the area to any display window or double-click the area. Window division will automatically adapt to the number of cameras in the area.
6. **Optional:** To change window division mode, click  on the live view toolbar at the bottom and select a mode.
7. **Optional:** Move the cursor over the display window during live view to show the camera toolbar. You can perform basic operations to cameras, such as digital zoom, instant playback, two-way audio, fisheye dewarping, and PTZ control, etc.

## PTZ Control

Cameras with the pan/tilt/zoom functionality can be controlled through the web browser. You can also set the preset, patrol, and pattern for the cameras.

**Note**

The PTZ control function should be supported by the camera.

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 camera position which contains configurations 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 Home page, select → **All Modules** → **Video** → **Video Application** .
2. Click **Live View** on the left.
3. Start live view.

   **Note**

   For details, see ***Start Live View*** .
4. Click **PTZ Control** on the navigation bar to open the PTZ control panel.

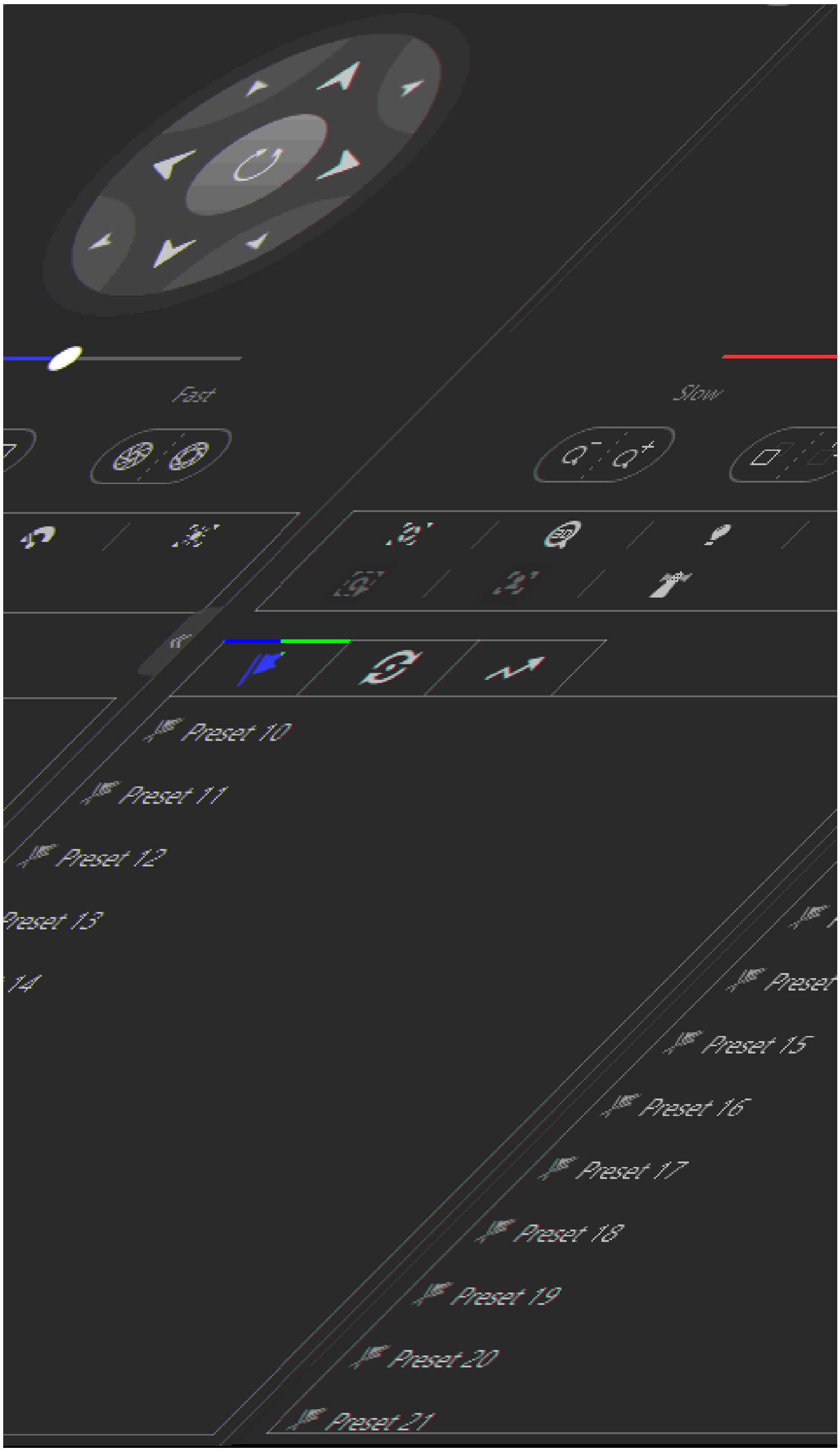



**Figure 14-20 PTZ Control Panel**

5. Use PTZ control to adjust the camera image to the desired direction and adjust other parameters such as zoom, focus, and iris to optimize the image.
6. Click to show the preset list.
7. Select an unconfigured PTZ preset ( ) in the preset list.
8. Click to create a name for the preset.
9. Click **OK** to save the settings.

**Note**

Up to 256 presets can be configured.

10. **Optional:** Perform further operations.

| | |
|---|---|
| **Call Preset** | Double-click a configured preset, or select a preset and click to call the preset. |
| **Edit Preset** | Select a configured preset and click to edit it.<br>**Note**<br>Some presets cannot be edited. |
| **Delete Preset** | Select a configured preset and click to delete it.<br>**Note**<br>Some presets cannot be deleted. |

### Configure Patrol

A patrol is a scanning track specified by a group of user-defined presets (including virtual presets) with programmable scanning speed between adjacent presets and dwell time of each preset.

**Before You Start**

Add at least two presets for a PTZ camera. For instructions, see ***Configure Preset*** .

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **Video** → **Video Application** .
2. Click **Live View** on the left.
3. Start live view. For details, see ***Start Live View*** .
4. Click in the live view toolbar to open the PTZ control panel.
5. Click to show the patrol list.

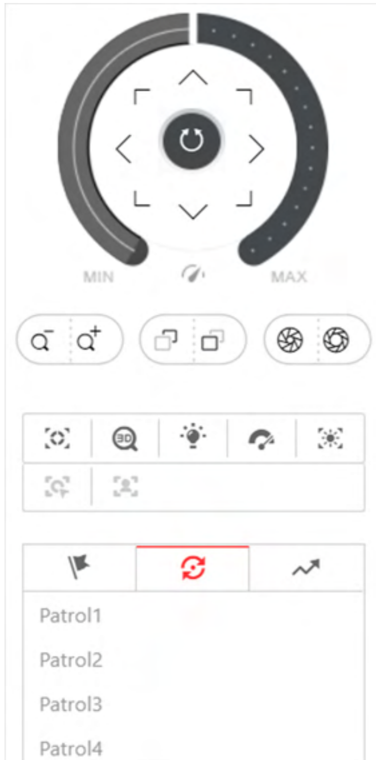



**Figure 14-21 Configure Patrol**

**6.** Select a unconfigured patrol (gray) and click .

**7.** Click to add a preset, and set the dwell time and the patrol speed.

**Note**

- Patrol speed ranges from 1 to 40.
- Preset dwell time ranges from 15 to 30s.


**Figure 14-22 Add Preset to Patrol**

**8.** Repeat the previous step to add other presets to the patrol.

**9. Optional:** Perform further operations after adding presets.

| | |
|---|---|
| **Remove Preset from Patrol** | Select an added preset and click ✕ to remove the preset from the patrol. |
| **Adjust Preset Sequence** | Select an added preset and click ↑ ↓ to adjust the preset sequence. |

**10.** Click **OK** to save the patrol settings.

**Note**

Up to 8 patrols can be stored.

**11. Optional:** Perform further operations after configuring patrols.

| | |
|---|---|
| **Call Patrol** | Click to start the patrol. |
| **Stop Calling Patrol** | Click to stop the patrol. |

## Configure Pattern

A pattern is a record of manual manipulation of PTZ movement. You can configure a pattern to record the movement of a camera.

**Steps**

**1.** In the top left corner of Home page, select → **All Modules** → **Video** → **Video Application** .
**2.** Click **Live View** on the left.
**3.** Start live view. For details, see ***Start Live View*** .
**4.** Click in the live view toolbar to open the PTZ control panel.
**5.** Click to show the pattern list.


**Figure 14-23 Configure Pattern**

**6.** Click to start recording the pattern path.
**7.** Control the PTZ movement.
**8.** Click to stop and save the pattern recording.

**Note**

Only one pattern can be stored. Newly-defined pattern will overwrite the previous pattern.

**9. Optional:** Perform further operations after configuring the pattern.

| | |
|---|---|
| **Call Pattern** | Click to start the pattern. |
| **Stop Calling Pattern** | Click to stop the pattern. |
| **Delete Pattern** | Click to delete the pattern. |

## 14.10.2 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.

## Search Video File

You can search for the video footage of cameras and filter the video footage by video type, tag type, storage location, etc.

**Before You Start**

If the system is central system with Remote Site Management module, you can also play back the recorded video of the cameras imported from remote site. For managing remote site's cameras in areas, refer to ***Area Management*** .

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **Video** → **Video Application** .
2. Click **Playback** on the left.
3. In the area and camera list, find the camera that you want to search playback video files.

   **Note**

   - You can enter the keyword of camera name or area name in the search field to search for the target camera or area.
   - You can hover the cursor to the camera and view its live view thumbnail. You can also click → **Add to Favorites** on the right side of camera name to add the current camera to Favorites.
4. Drag the camera to the display window, or double-click the camera to start playback.
5. **Optional:** Click the date and time on the playback toolbar to specify the date and time for searching.

   **Note**

   - In the calendar panel, the date that has video files is marked with a green triangle.

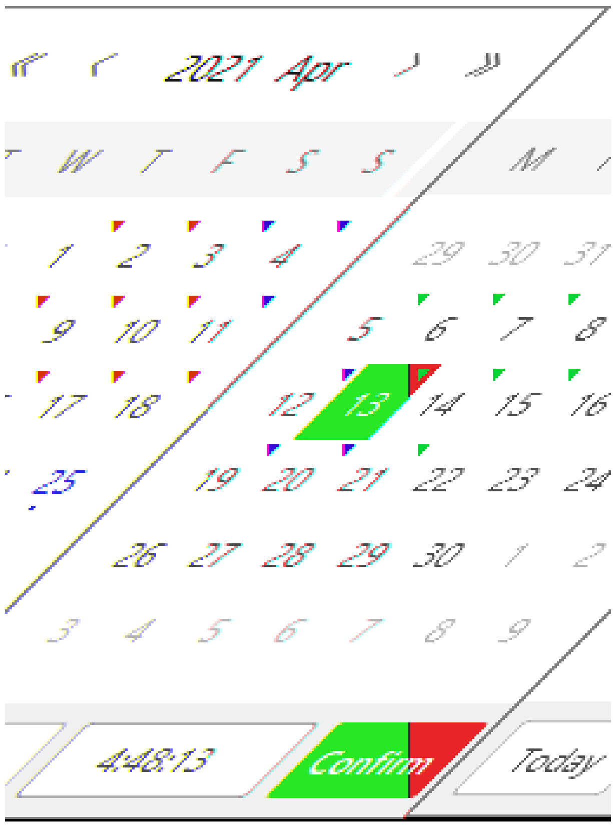


**Figure 14-24 Calender Panel**

- The calendar panel is not available to cameras in the remote sites.

**6. Optional:** Click on the playback toolbar to filter video files by recording types, tag types, target types, etc.

**Note**

- Filtering video files by target types (All, Vehicle, People) should be supported by device.
- When you check the target types as **Vehicle** and/or **People**, the corresponding icons representing vehicle and/or people will be displayed on the playback timeline if the targets are detected on the video. The icon of single vehicle/person is different from that of multiple vehicles/people.

**Figure 14-25 Icons of Single And Multiple Vehicles**

**7.** Play and control the playback video file. For details, see ***Play Video File*** .

## Play Video File

After searching video footage, the playback starts. You can control the video playback via timeline. The timeline indicates the duration time of the video footage.

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **Video** → **Video Application** .
2. Click **Playback** on the left.
3. Search the video file of a camera. For details, see ***Search Video File*** .

   Playback starts.
4. To control the playback, click the icons on the playback toolbar.

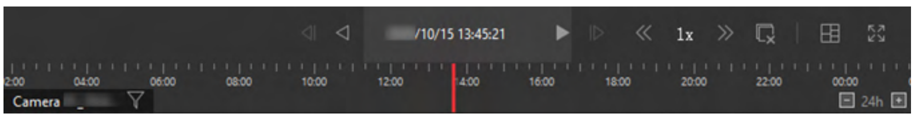



**Figure 14-26 Playback Toolbar**

5. Click or drag the timeline to play the video footage from a specific time.

   **Note**

   You can click  or  , or use the mouse wheel to scale up or scale down the timeline.
6. **Optional:** Move the cursor to the display window of a camera to show the camera toolbar. Perform further operations via the camera toolbar.

**Control Digital Zoom**

Click  to enable digital zoom and draw a rectangle on the video to zoom in. Click again to disable digital zoom.

**Note**

When the playback is in software decoding mode, you can also capture the zoomed-in picture after using digital zoom.

**Check Camera Status**

Click  to show the camera's recording status, signal status, connection number, etc.

**Switch Stream**

Click  ,  , or  (if supported) to switch the live view stream to main stream, sub-stream, or smooth stream (if supported).

**Note**

The smooth stream is available if the device supports the feature. You can switch to smooth stream in low-bandwidth network environment to make the playback more fluent.

**Control Audio**

Click  or  to turn off/on the sound.

**Note**

You can adjust the volume by moving the cursor to  .

### 14.10.3 Local Configuration

HikCentral Professional provides live view and playback for cameras via the Web Client. You can set network transmission parameters (hardware decoding, stream type, etc.) to optimize the performance of live view and playback for your current Web Client. You can also check the current saving path of video files and captured pictures on your PC.

**Steps**

**Note**

The parameters in Local Configuration only affect the current Web Client.

1. In the top left corner of Home page, select  → **All Modules** → **Video** → **Video Application** .
2. Click **Local Configuration** on the left.
3. Click **Network Transmission** to configure network transmission parameters.

**GPU Hardware Decoding**

Enable GPU decoding for live view and playback to save CPU resources.

**Note**

- To enable GPU hardware decoding, your PC must support the feature.
- After enabling GPU hardware decoding, restart live view or playback to take effect.
- If the client displays a blurred screen after enabling GPU hardware decoding, disable it.

**Global Stream**

If a device does not support smooth stream, it will use sub-stream. If a device does not support sub-stream, it will use main stream.

If the network connection is good, select main stream or sub-stream for better image quality. If the network connection is poor, select smooth stream for speed.

**Threshold for Main/Sub-Stream**

If the window division of display window is larger than the configured threshold, the stream type will automatically switch to main stream. If not, the stream type will switch to sub-stream.

For example, if you set the threshold to ¼ and you set window division to 9-window mode, the cameras' stream type will switch to sub-stream.

**Note**

This parameter is only available when **Main Stream** is set as **Global Stream**.

**Network Timeout**

The default waiting time for the operations in Applications on the current Web Client. The operations will be regarded as failure if no response within the configured time.

The minimum default waiting time of the interactions between the Applications and SYS server is 60s. The minimum waiting time between SYS server and devices is 5s. The minimum waiting time between the Applications and devices is 5s.

**Video Caching**

Video caching should be determined based on network performance, computer performance, and bit rate. You can set it to **Small (1 Frame)**, **Medium (6 Frames)**, or **Large (15 Frame)**. Larger frame caching results in better video performance but requires more network and computer resources.

**Time Zone**

Set the time reference for live view and playback to client time or device time.

**Picture Format**

Set the file format for the captured pictures during live view or playback.

**Device Access Mode**

**Default Configuration**

Restore the device access mode.

**Automatically Judge**

Judge the device access mode according to the network.

**Directly Access**

Access the device directly, not via HikCentral Professional Streaming Service.

**Proxy**

Access the device via HikCentral Professional Streaming Gateway and HikCentral Professional Management Service.

**Note**

By default, the platform will judge the device access mode according to the network. If you change to other modes, it only affects the client you currently logged in.

4. **Optional:** Click **Default Value** to restore to default settings.
5. Click **Save** to save the settings.
6. **Optional:** Click **Saving Path** on the left to view the saving path of the video files and captured pictures during live view or playback on your local PC.

# Chapter 15 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.

## 15.1 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.

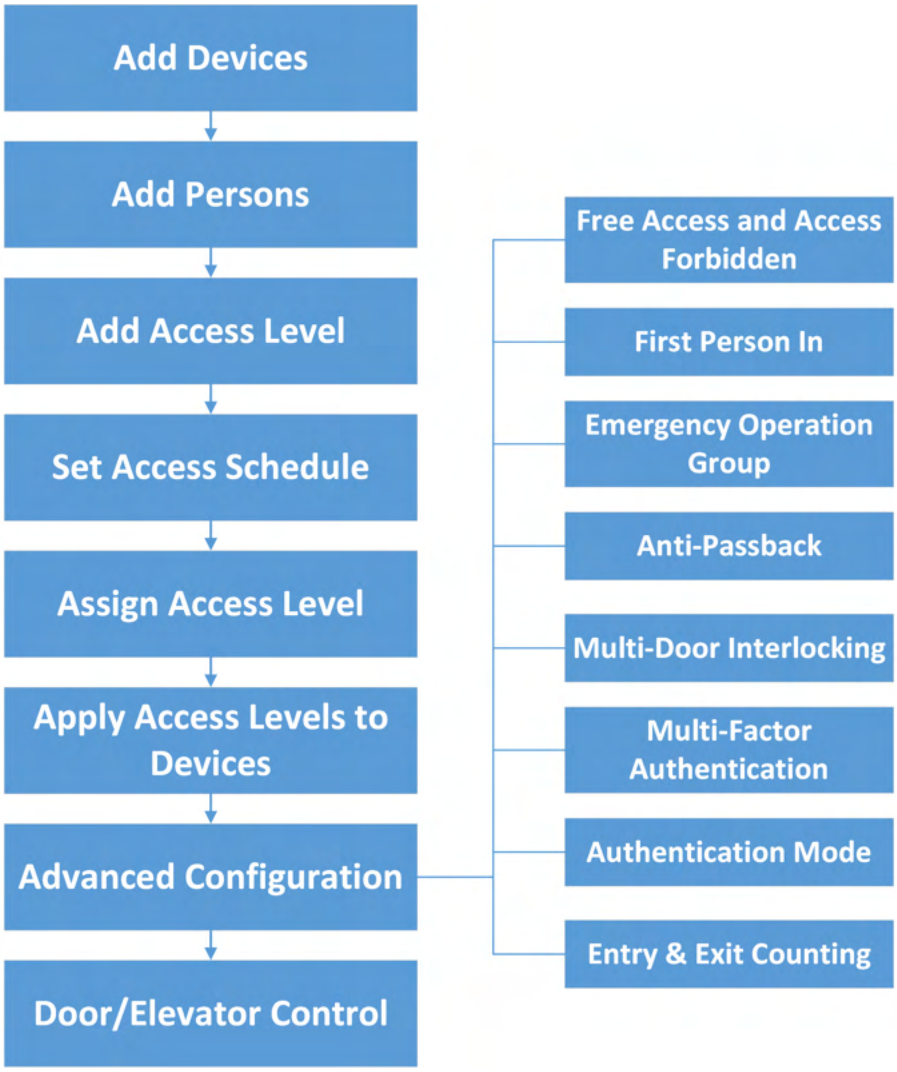



**Figure 15-1 Flow Chart of Access Control and Elevator Control**

- **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.

## 15.2 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.

### 15.2.1 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.

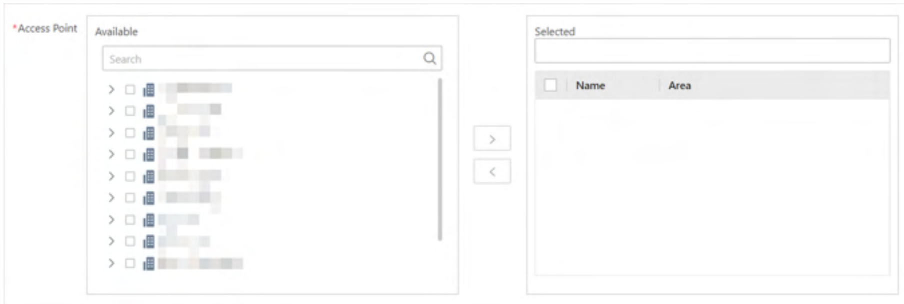



**Figure 15-2 Select Access Points**

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*** .

## 15.2.2 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.

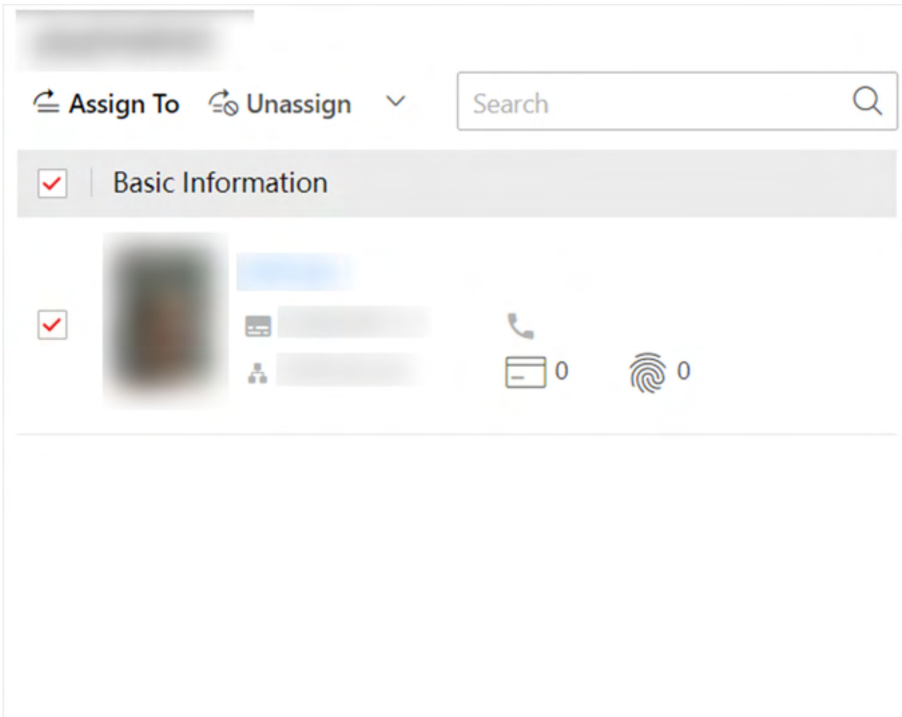



**Figure 15-3 Assignee Panel**

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.

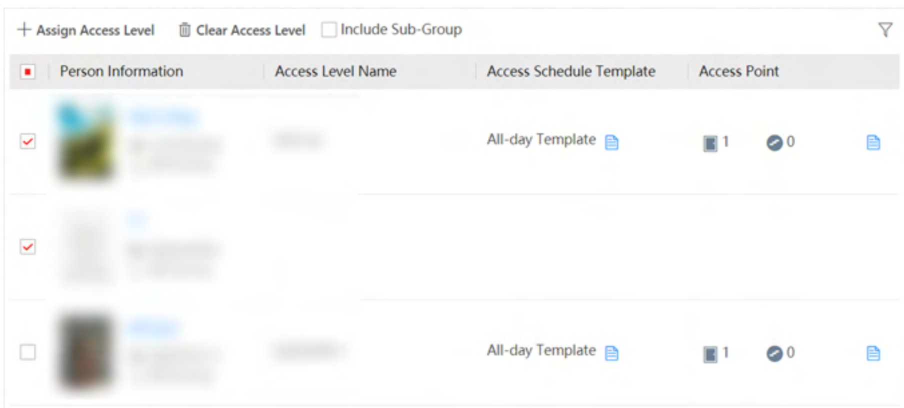



**Figure 15-4 Person Information Panel**

> **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.

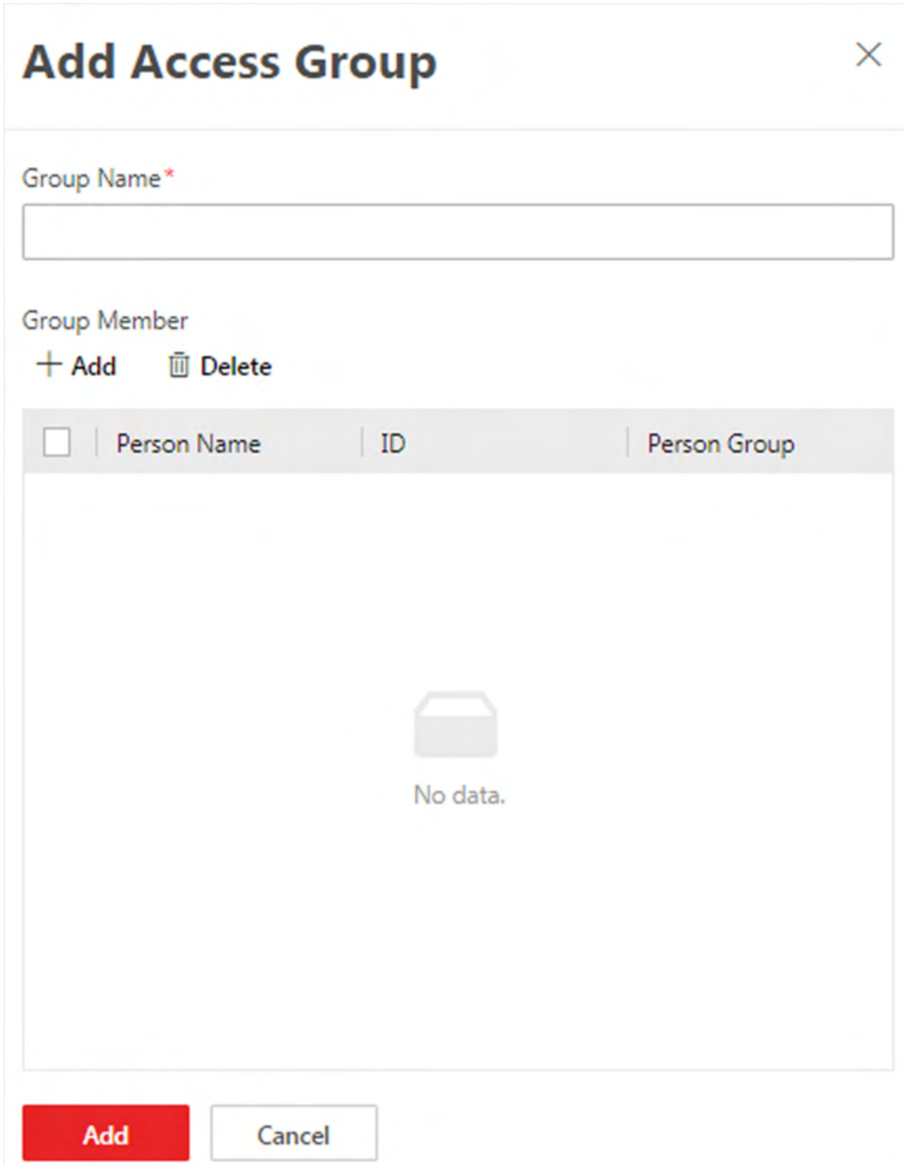



**Figure 15-5 Add Access Group Page**

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*** .

### 15.2.3 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**.

## 15.2.4 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.

### 15.2.5 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*** .

### 15.2.6 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**.

## 15.3 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.

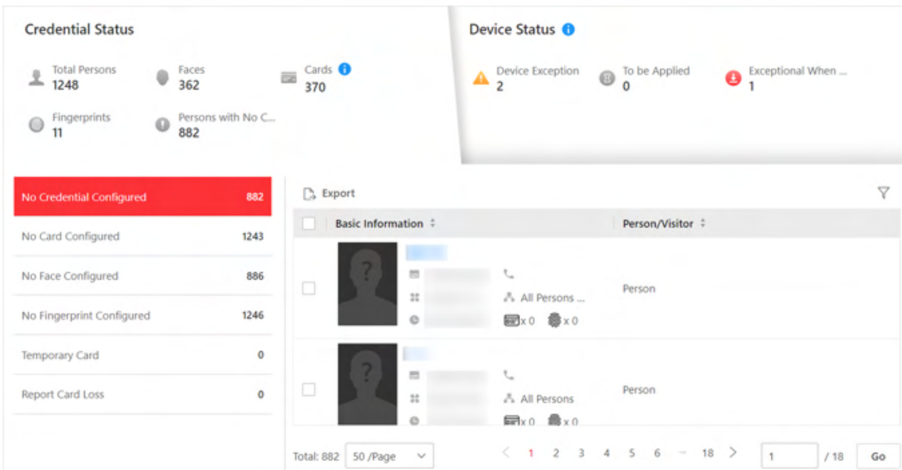



**Figure 15-6 Credential Status**

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.

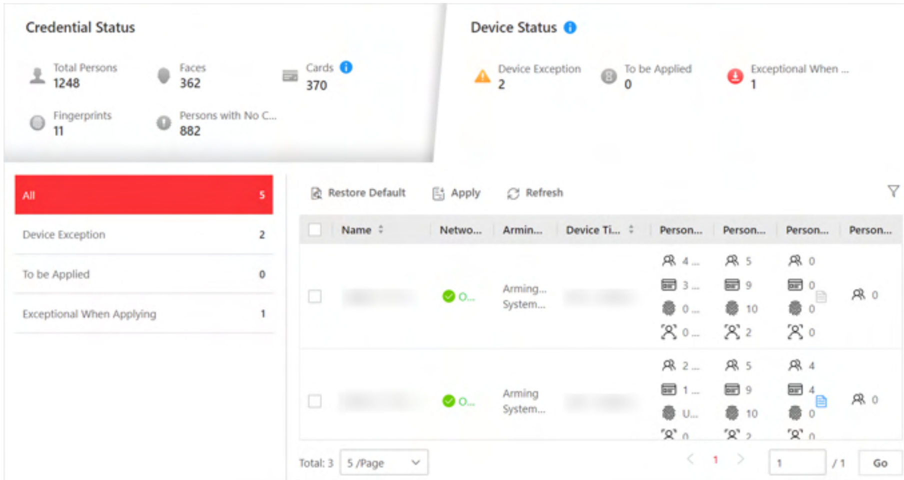



**Figure 15-7 Device Status**

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.

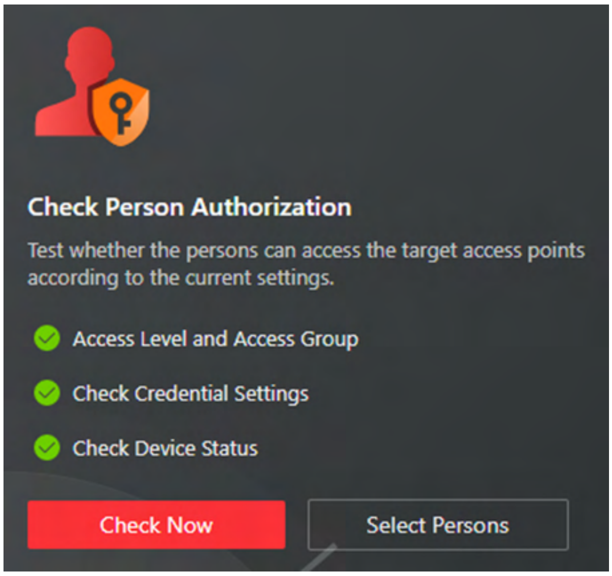



**Figure 15-8 Check Authorization Settings**

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.

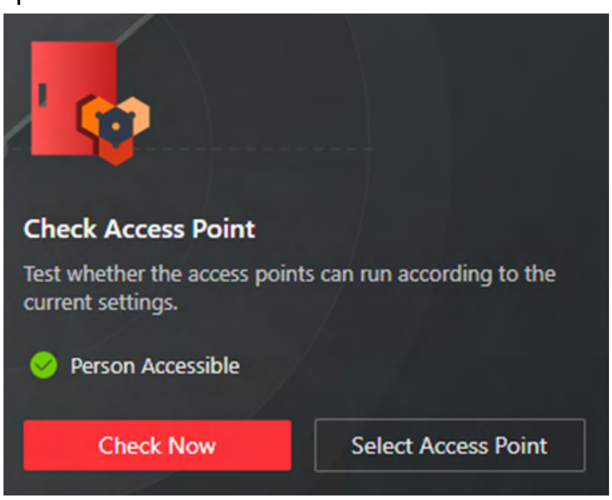



**Figure 15-9 Check Access Point Settings**

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.

## 15.4 Advanced Functions

### 15.4.1 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.

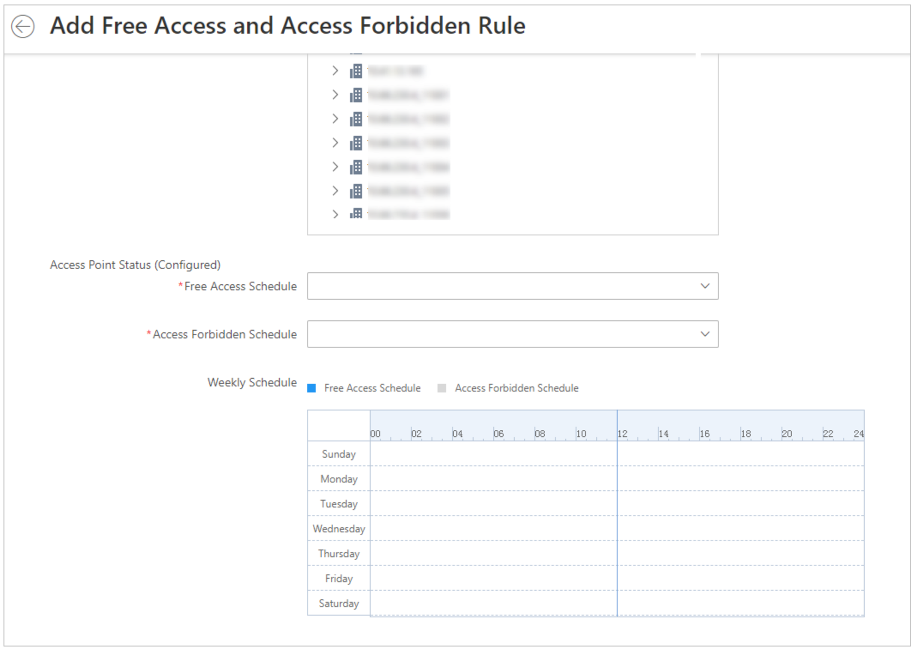



**Figure 15-10 Add Free Access and Access Forbidden Rule Page**

**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. |

## 15.4.2 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**.

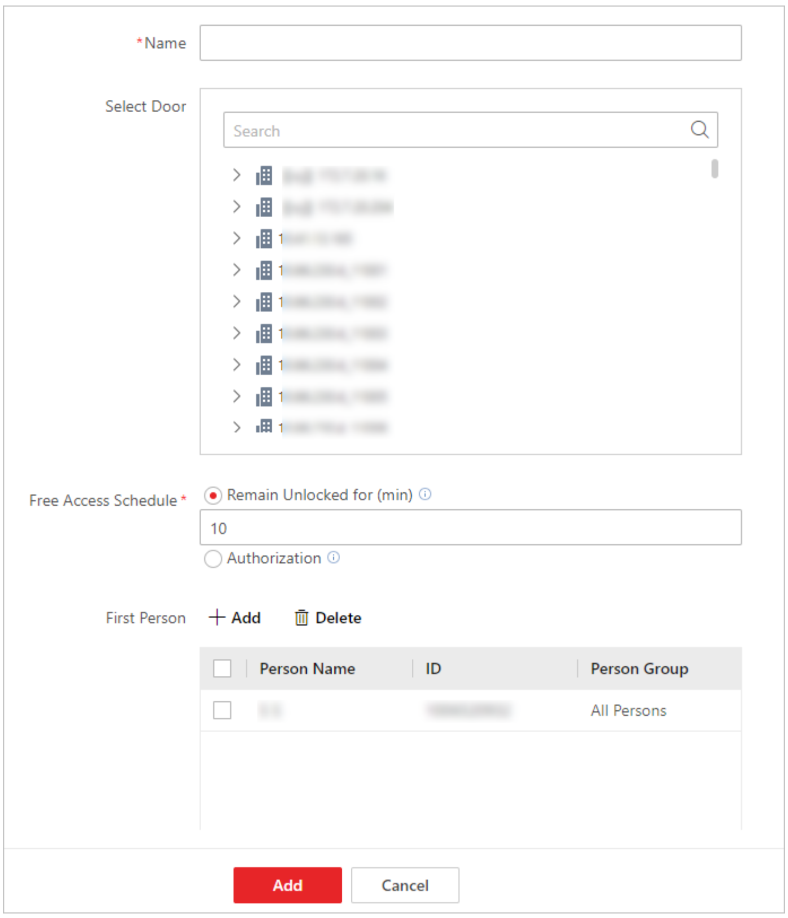



**Figure 15-11 Add First Person In Rule Page**

**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.

### 15.4.3 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**.

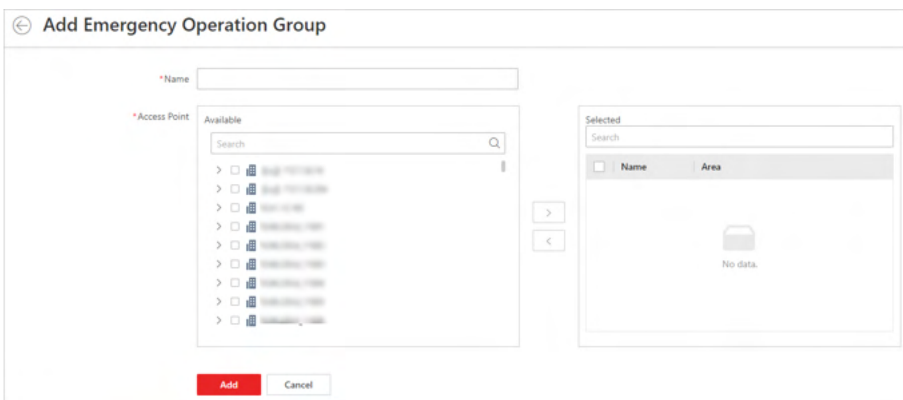



**Figure 15-12 Add Emergency Operation Group Page**

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.

### 15.4.4 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.

   **Note**

   You cannot set forgiving anti-passback violations regularly when there is only one door in the anti-passback group.
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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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). |

## 15.4.5 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**.

## 15.4.6 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**.

## 15.4.7 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.

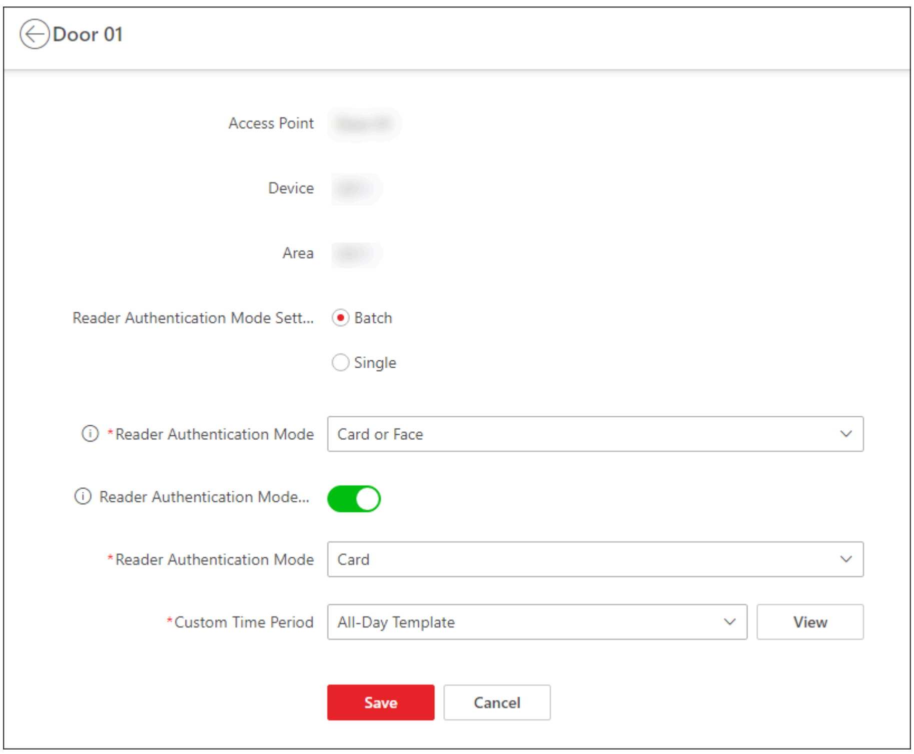



**Figure 15-13 Set Reader Authentication Mode Page**

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.

### 15.4.8 Add Entry and Exit Counting Group

The entry and exit counting group is used to group the doors in certain region. You can set some doors as the region border. Only the persons accessing these doors are counted, and other doors inside the region are ignored. By grouping these doors, the system provides counting functions based on the entry and exit records on these doors. 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 **Identity Access Search → 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 doors from the area list.
6. Set the entering or exiting direction of the card readers of the selected doors.

   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 doors in the group.

## 15.5 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.

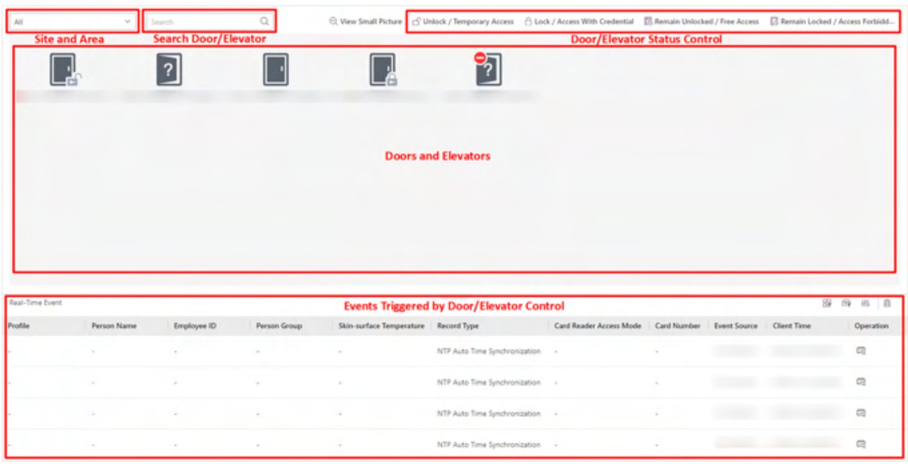



**Figure 15-14 Access Control Real-time Monitoring**

### 15.5.1 View Real-Time Access Event

In **Access Control** module, you can view events of 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. |

### 15.5.2 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*** .

### 15.5.3 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*** .

## 15.6 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.

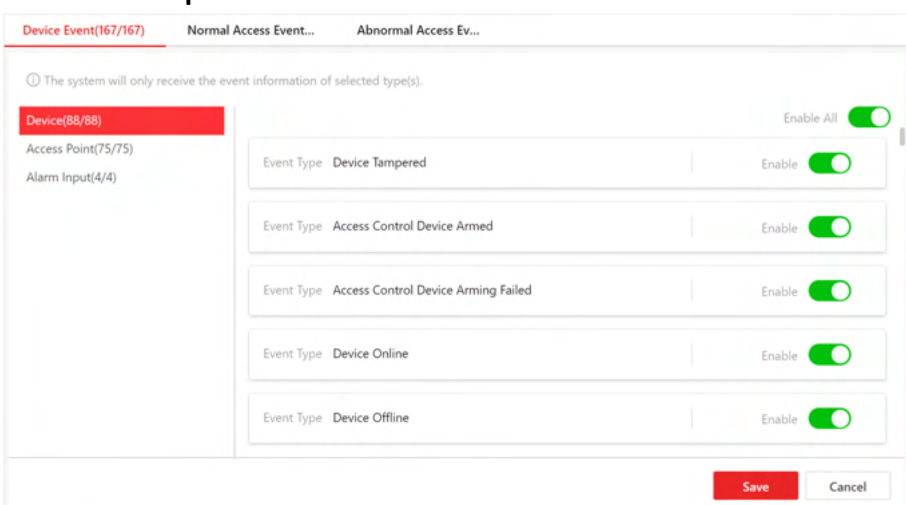



**Figure 15-15 Device and Access Event Subscription**

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*** .

## 15.7 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.

## 15.8 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.

## 15.9 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 visitee information, including name, person profile, visit reason, 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.<br>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.<br>**Note**<br>Up to 500 records can be exported each time. |

## 15.10 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**.

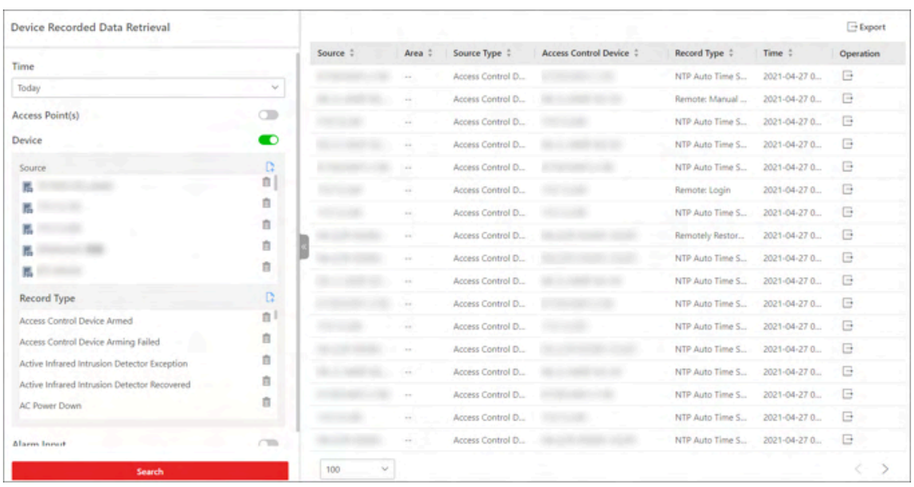



**Figure 15-16 Device Recorded Data Retrieval**

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 16 Parking Management

HikCentral Professional provides 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. On the Vehicle Overview page, you can view the health status of parking lot, parking space statistics, traffic flow statistics, and vehicle passing event. Besides, you can go to different pages according to your need.

## 16.1 Flow Chart

The following flow chart shows the process of configuring and operating the parking lot.

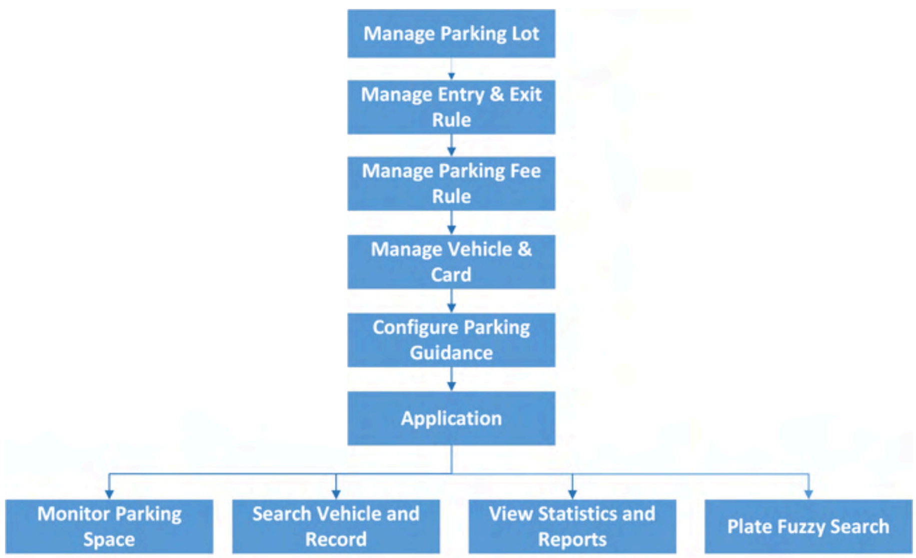



**Figure 16-1 Flow Chart of Parking Lot Management**

- **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.

## 16.2 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 & exit should contain at least one lane. The lane can be linked with a capture unit, an access control device, or a video intercom device, which can be used for capturing and recognition, identity verification, video intercom, as well as controlling barrier to open or close. You can also mount one LED screen at the lane and link it with the lane to display information such as entering/exiting time, number of available parking spaces, etc.

The two pictures below shows the typical relation of parking lot, entrances & exits, and lanes.

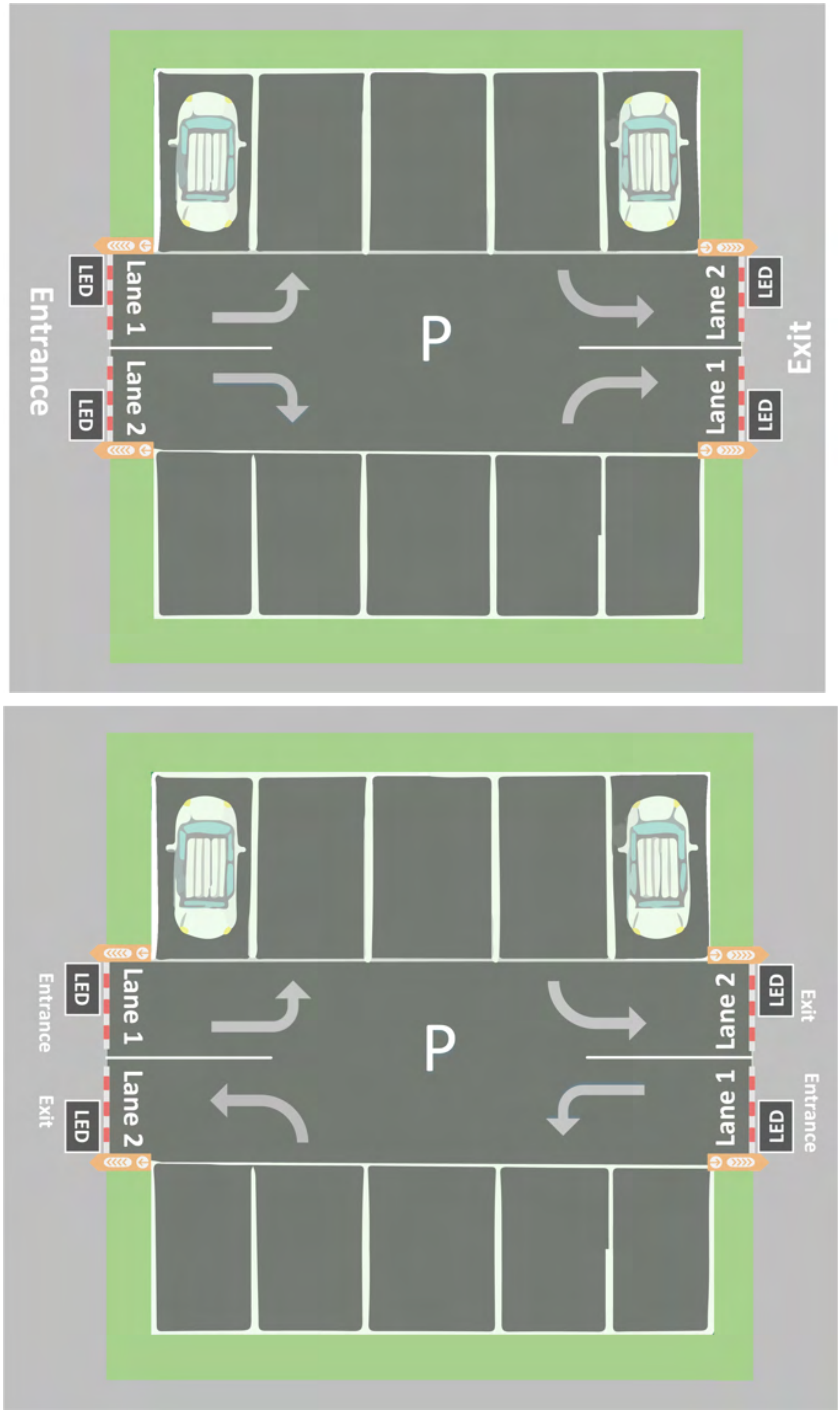



**Figure 16-2 Parking Lot**

### 16.2.1 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.

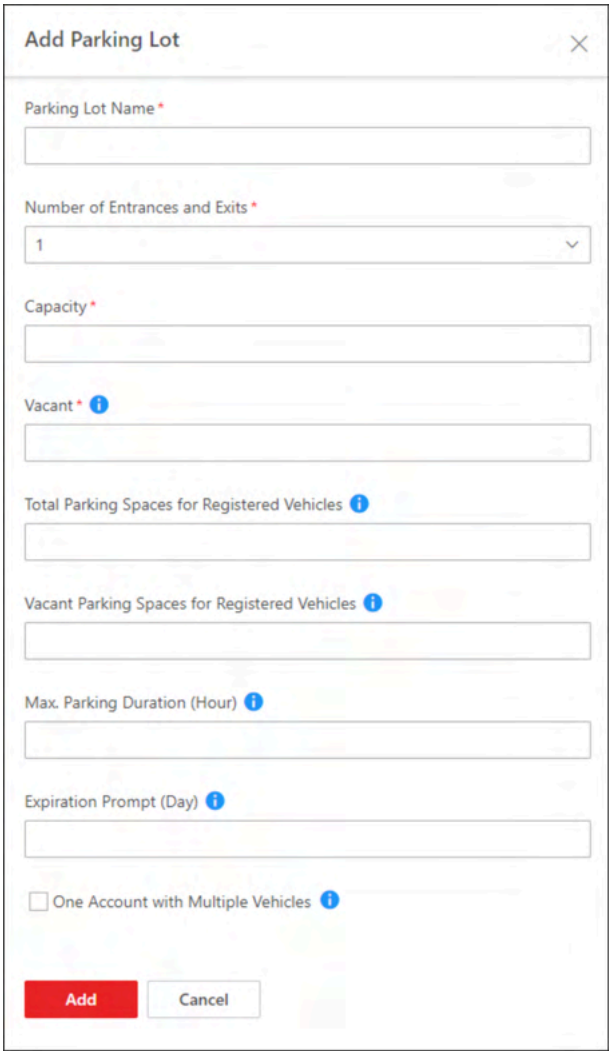



**Figure 16-3 Create Parking Lot Window**

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. 6$^{th}$, 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. 1$^{st}$, 2020 to Jan. 5$^{th}$, 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.<br>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.

## 16.2.2 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.

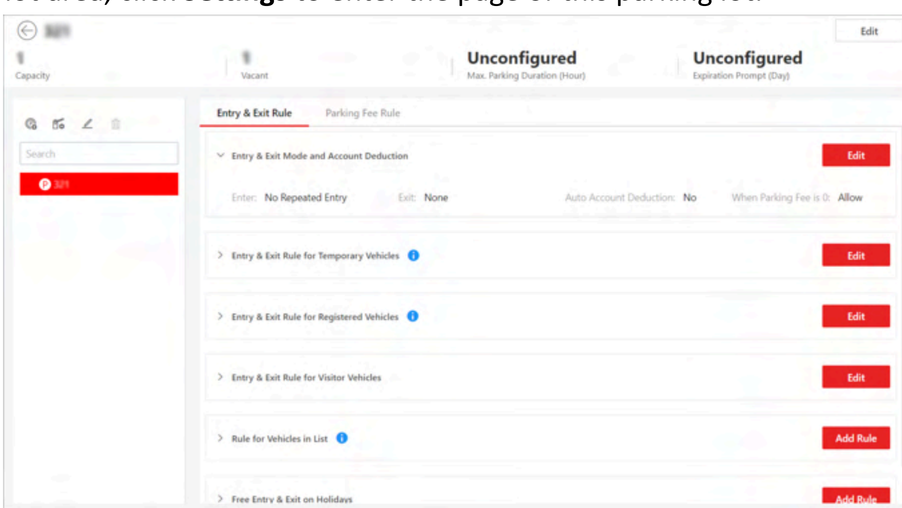



**Figure 16-4 Parking Lot Page**

**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.

### 16.2.3 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 and exit in the left list.
**4.** Click  to enter the Add Lane page.
**5.** Set the lane.

**Basic Information**

Create a name for the lane, and set the lane type as **Entrance** or **Exit**.

**Enable Time Range**

Set the entry & exit time range for the lane. If you select **All-Day**, the lane will be available for vehicles to pass throughout the day; if you select **Custom**, you need to set a period that allows the vehicles to enter and exit the parking lot through the lane.

**Entry & Exit Rule for Temporary/Registered/Visitor Vehicles**

The entry & exit rule for a specific type of vehicles. If you switch on **Same Rule as Parking Lot**, the entry & exit rule of this parking lot will be applied to the lane; if you switch off it, you can configure the method to open the barrier gate, and the entry & exit time range of the lane by yourself.

**Entry & Exit Rule for Vehicles in List**

You can switch on **Same Rule as Parking Lot** to apply the entry & exit rule of this parking lot to the lane. You can also switch off it and click **Add Rule** to create a rule.

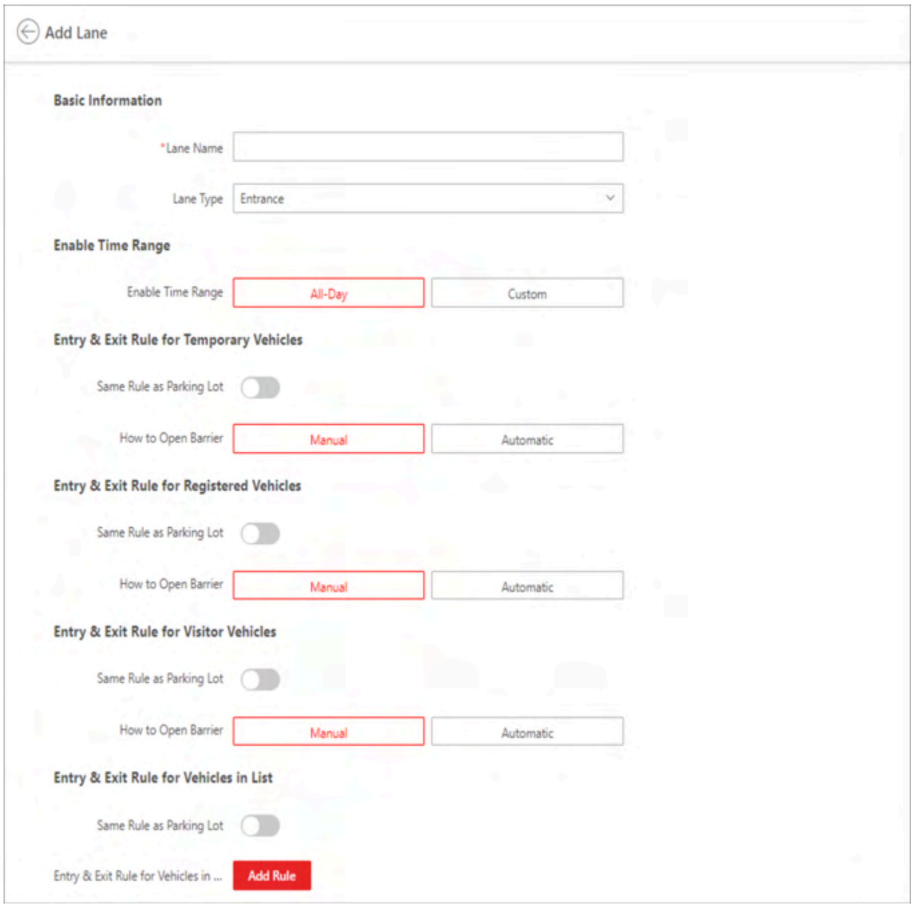



**Figure 16-5 Add Lane Page**

6. **Optional:** Configure linkage devices for the lane.
   1) Select a capture unit in the drop-down list.

**Note**

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.

2) Select **Access Control Device** or **Video Intercom Device** as the **Device Type**.
3) Select a device for swiping card or video intercom from the **Select Device** drop-down list.

**Access Control**

If you selected a card (already issued to the owner for card authentication) for the owner when adding a vehicle, you actually bind the card with the vehicle license plate number. So the barrier will open when you swipe the card at the lane with an access control/video intercom device. In this circumstance, a capture unit is not needed.

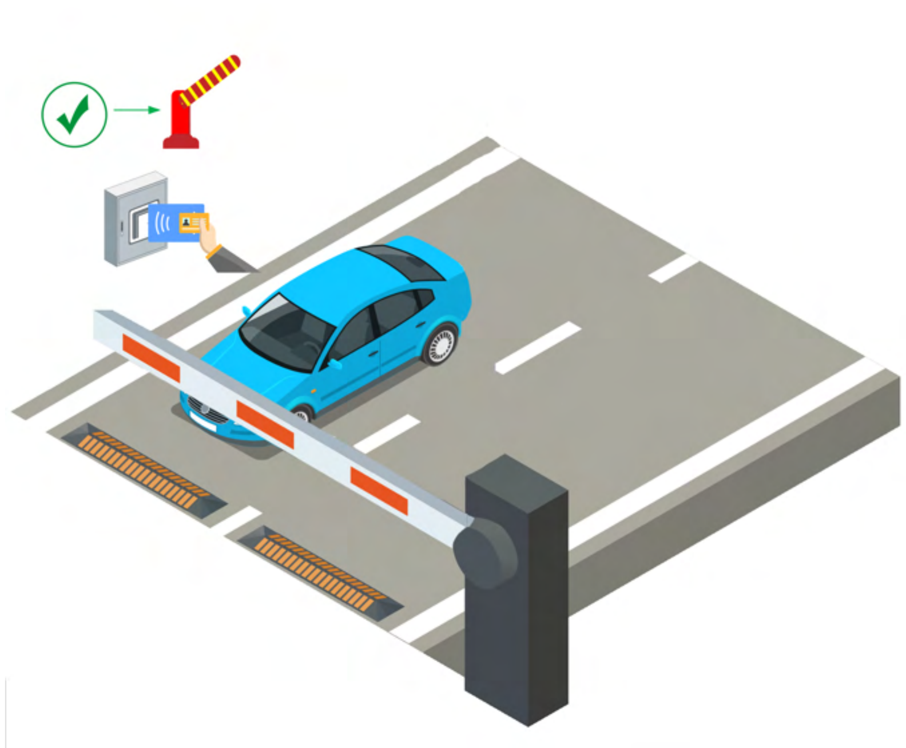


**Figure 16-6 Opening Barrier by Card Swiping**

**Video Intercom**

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 license plate number captured by a capture unit.
c. The security guard opens the barrier manually if the vehicle owner is authenticated.

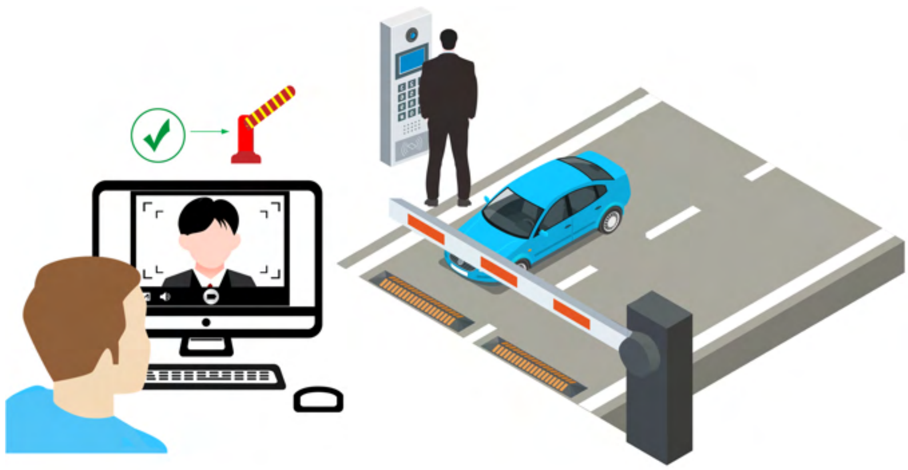


**Figure 16-7 Opening Barrier by Video Intercom**

4) Select a guidance screen for the lane.

**Note**

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.

5) Select either **Capture Unit** or **Access Control /Video Intercom Device** selected by the above step as the device for barrier control.

**7.** Relate the lane with camera(s).

**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 with the lane.
- One camera can be related with multiple lanes.
- You can view the pictures captured by the related camera in the passing vehicle information on the Control Client.

1) Click **Add** to open the resource list.
2) Select a camera from the resource list.
3) Click **Add**.

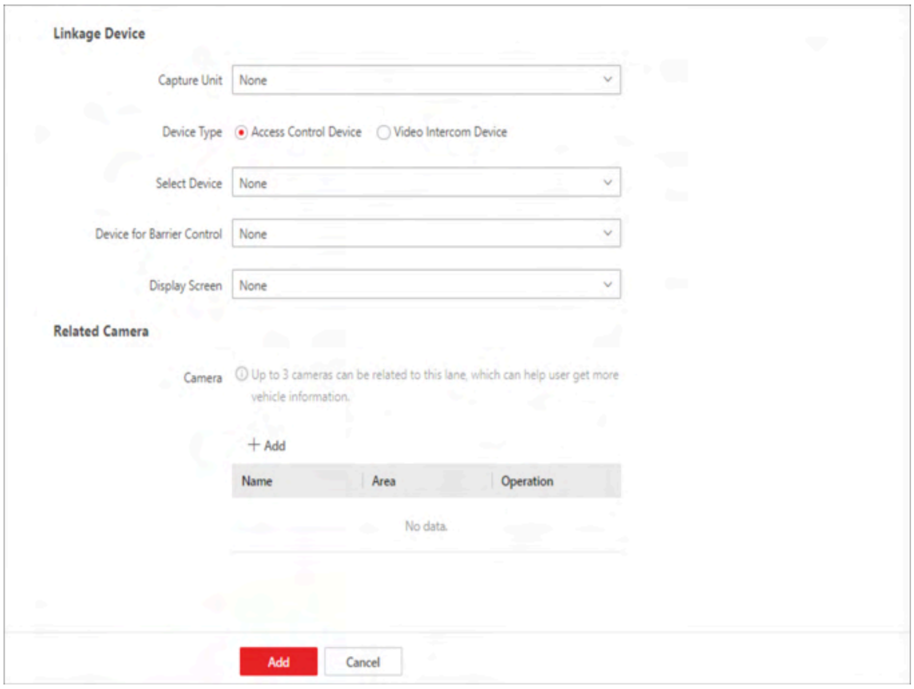



**Figure 16-8 Link Device and Relate Camera**

**8.** Click **Add**.

## 16.2.4 Set Contents Displayed on Guidance Screen

A guidance screen related to a lane can be used for displaying date and time, parking duration, plate number, and expiration prompt.

**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.

The guidance screen related to the entrance/exit is displayed in the entrance/exit area.

**4.** Click the name of the guidance screen to open the Screen Configuration panel.

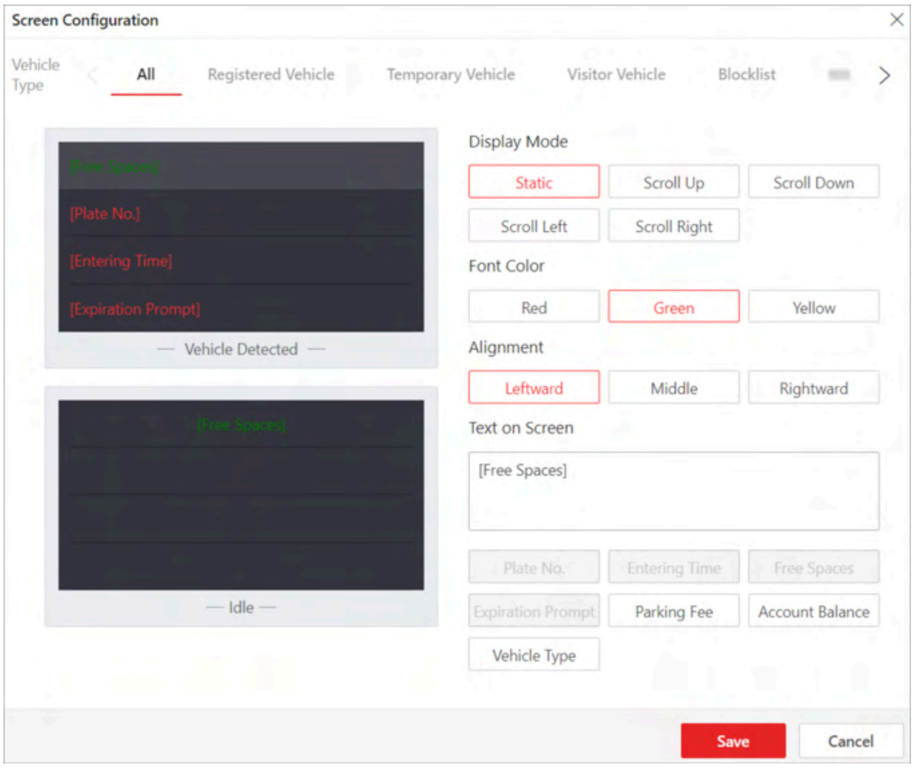



**Figure 16-9 Screen Configuration Window**

5. Select a vehicle type or **All**.
6. Click the four different lines in the**Vehicle Detected** screen and select information type under the **Text on Screen** frame. You can select **Plate No.** / **Entering Time** / **Free Spaces** / **Expiration Prompt** / **Parking Fee** / **Account Balance** / **Vehicle Type** to be displayed on the 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 parking lot.

   **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.
7. Click each line in the **Vehicle Detected** screen and select a display mode, font color, and alignment for the information displayed in each line.

8. Click a line in the **Idle** screen and click **Free Spaces**, and the number of vacant parking spaces will be displayed in the selected line when there is no vehicle detected at the lane.
9. Click the line displaying the number of vacant spaces and select a display mode, font color, and alignment for it.
10. Click **Save** to save the screen settings.

### 16.2.5 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** .

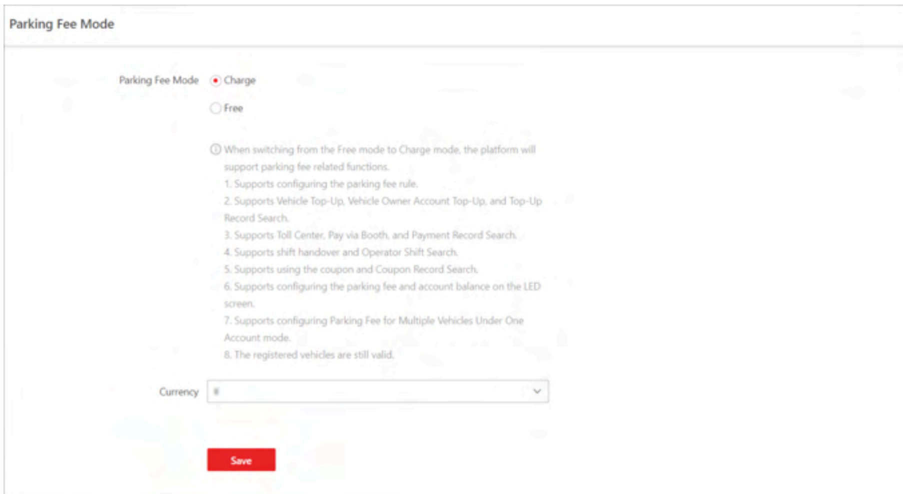



**Figure 16-10 Parking Fee Mode Settings Page**

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**.

## 16.3 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.

### 16.3.1 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.

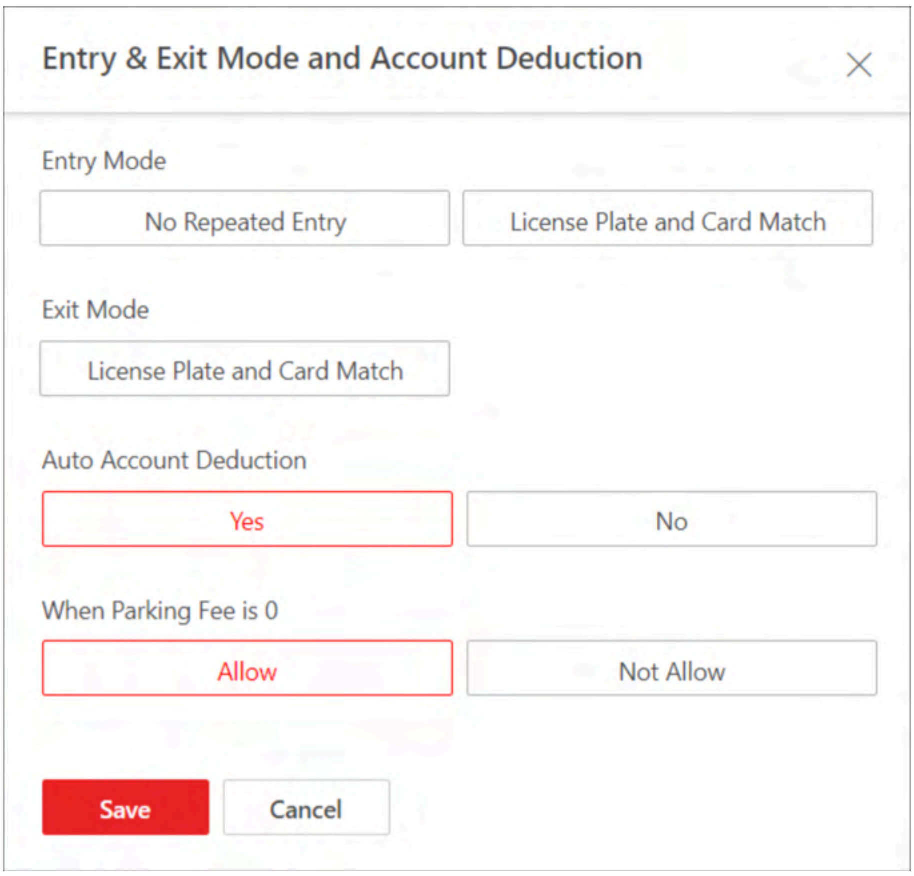



**Figure 16-11 Entry & Exit Mode and Account Deduction**

**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**.

### 16.3.2 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.

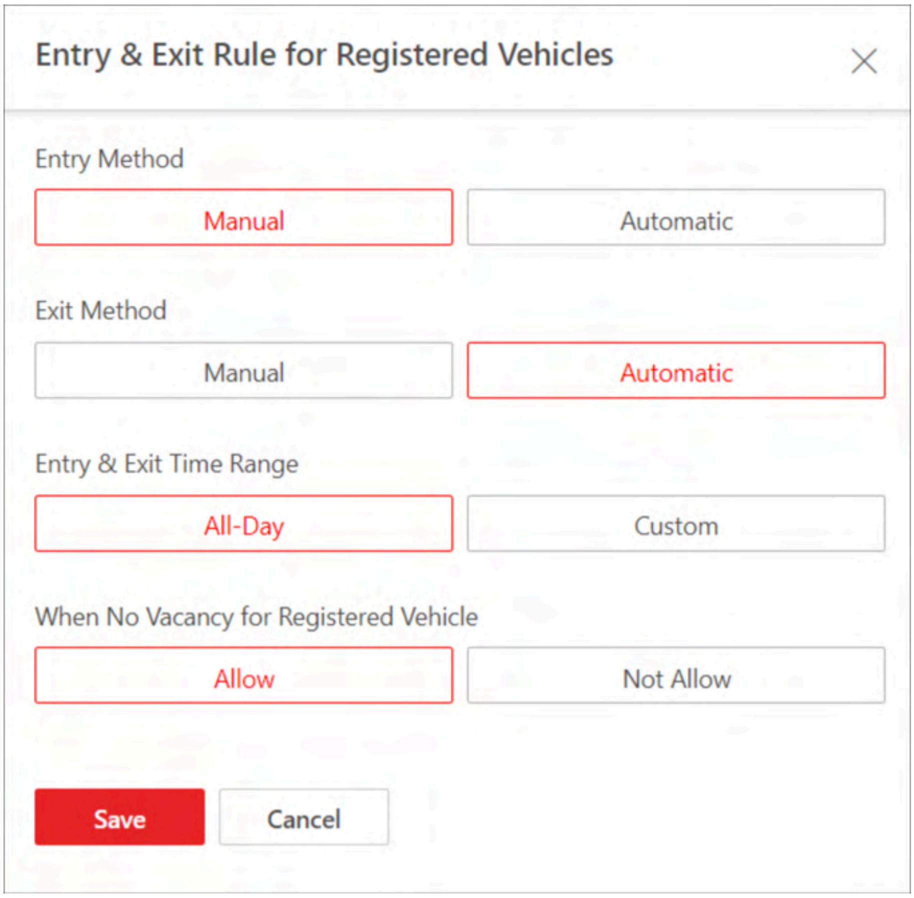



**Figure 16-12 Entry & Exit Rule for Registered Vehicles**

**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**.

### 16.3.3 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.

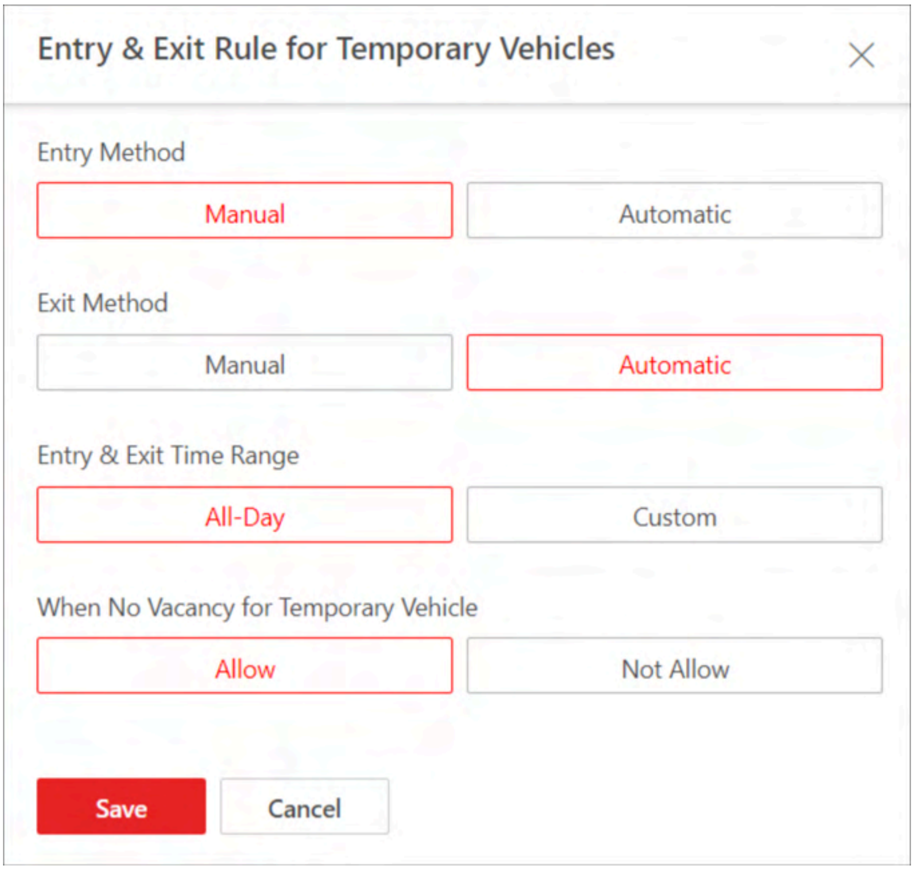



**Figure 16-13 Entry & Exit Rule for Temporary Vehicles**

**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**.

### 16.3.4 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.

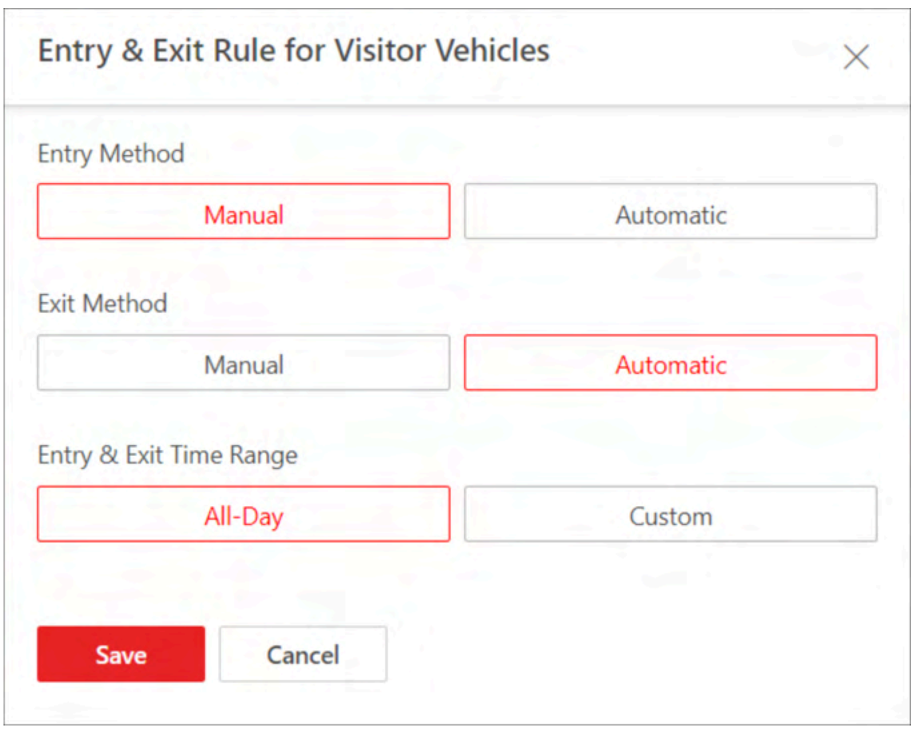



**Figure 16-14 Entry & Exit Rule for Visitor Vehicles**

**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**.

### 16.3.5 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.

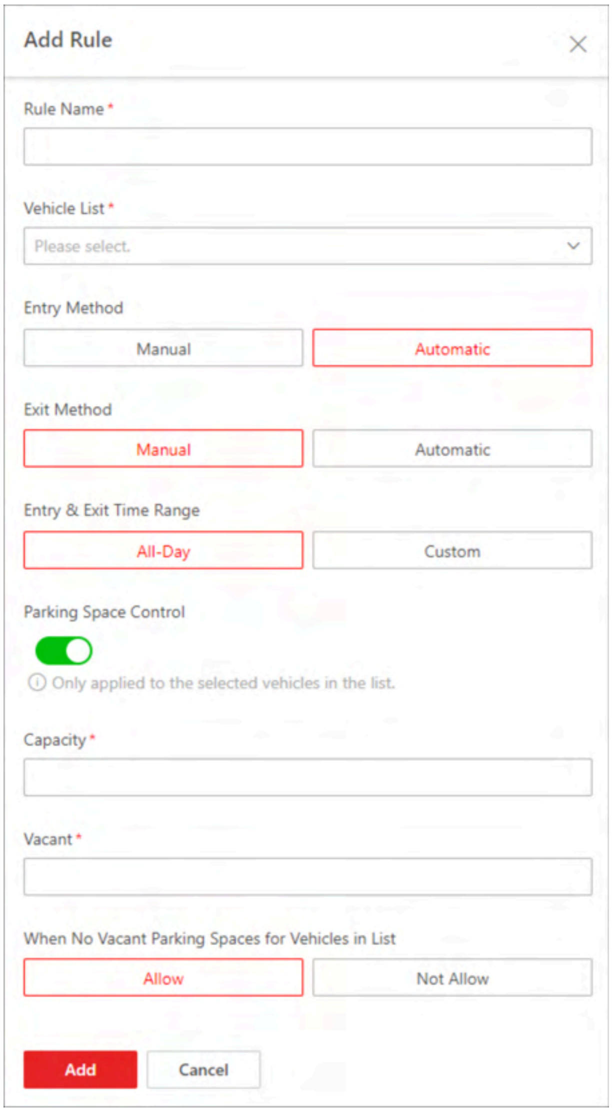



**Figure 16-15 Add Rule**

**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. |

## 16.3.6 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.<br>b. (Optional) Enter remarks in the Description field if needed.<br>c. Click **Add**. |
| **Day of Week** | a. Create a name for the holiday.<br>b. Click to set a time range for the holiday.<br>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**.

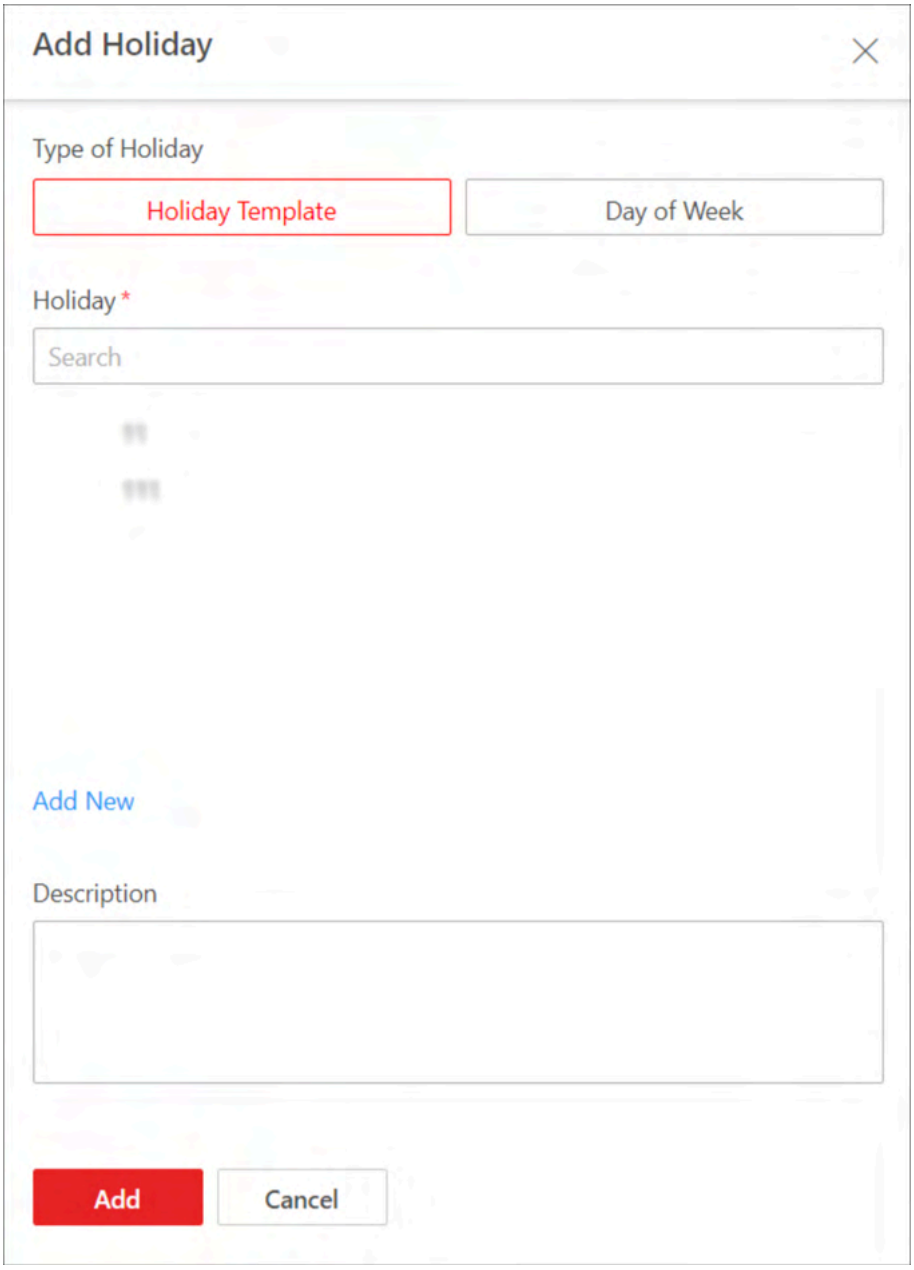



**Figure 16-16 Holiday Template**

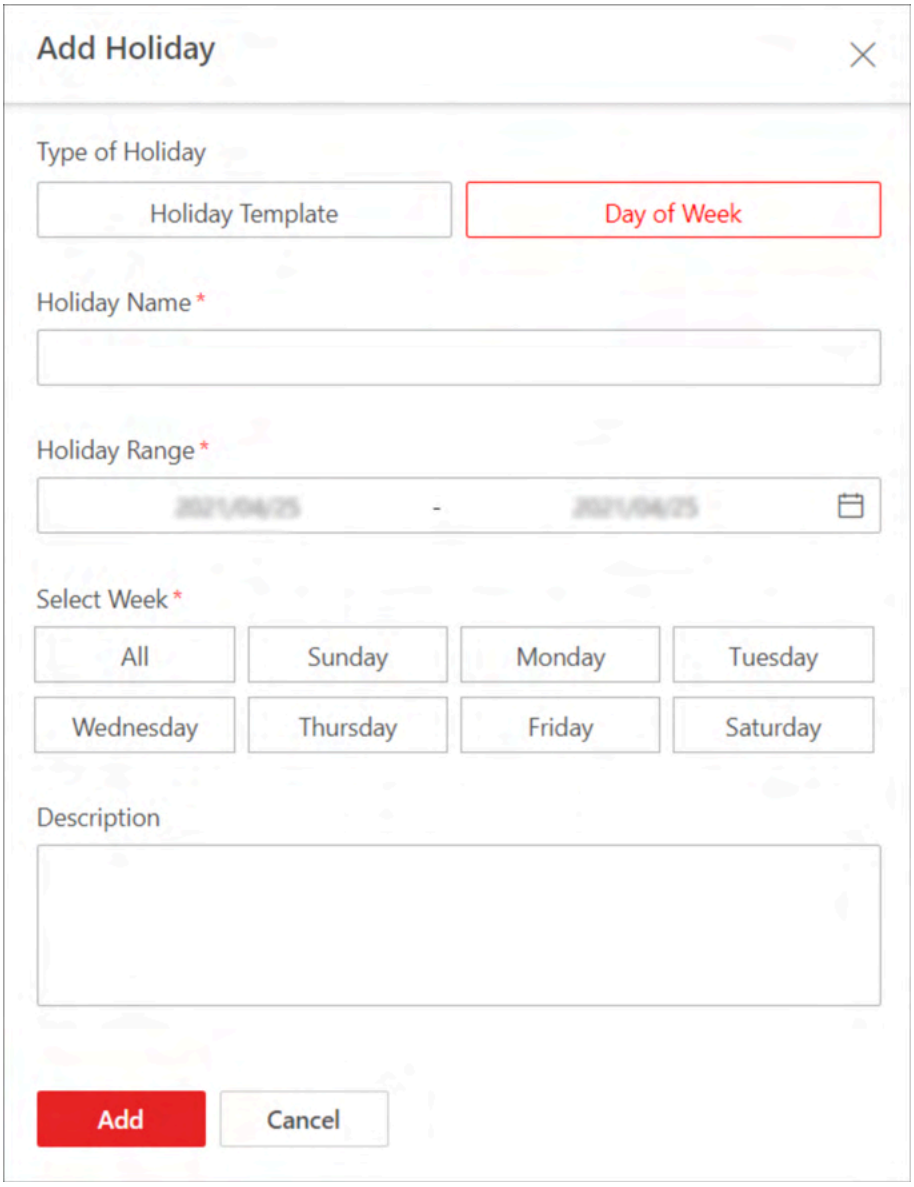



**Figure 16-17 Day of Week**

**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. |

## 16.4 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.

## 16.4.1 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. |

## 16.4.2 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.<br>a. Enter the parking duration that is free of charge.<br>b. Enter the fee for the initial parking duration.<br>c. Enter the fee for subsequent parking duration.<br>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.<br>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. |

### 16.4.3 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.

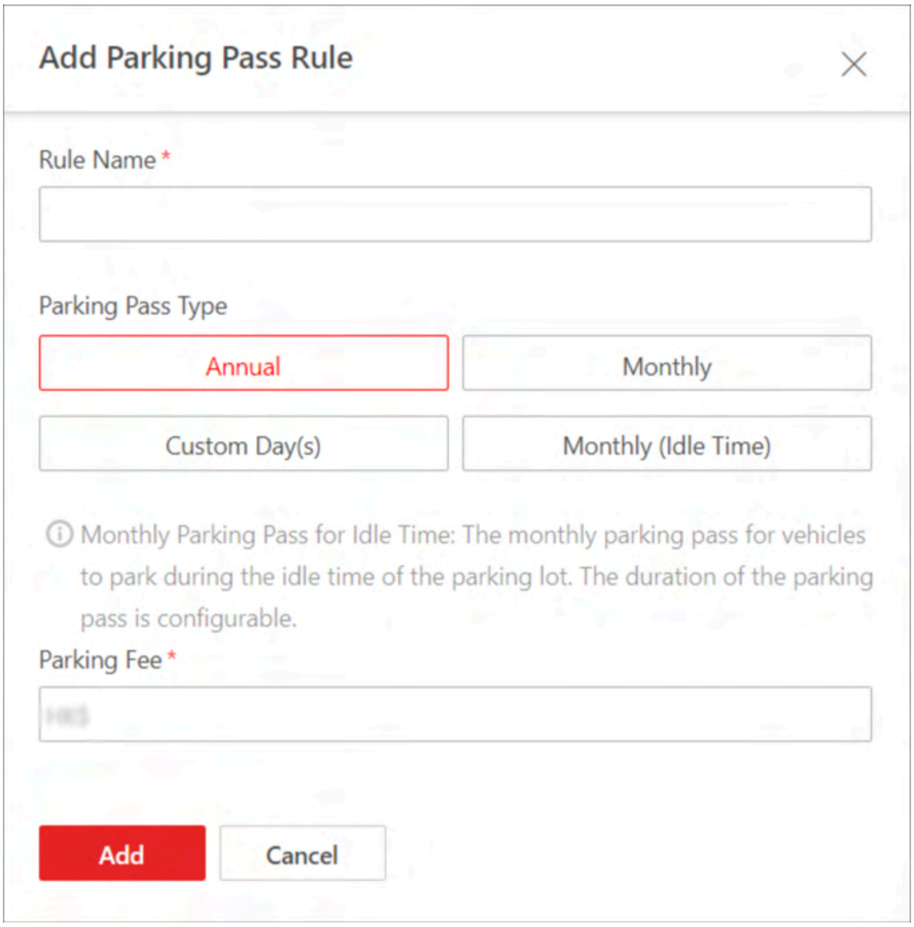



**Figure 16-18 Add Parking Pass Rule Panel**

**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. |

### 16.4.4 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. |

### 16.4.5 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. |

### 16.4.6 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**.

## 16.5 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.

### 16.5.1 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.

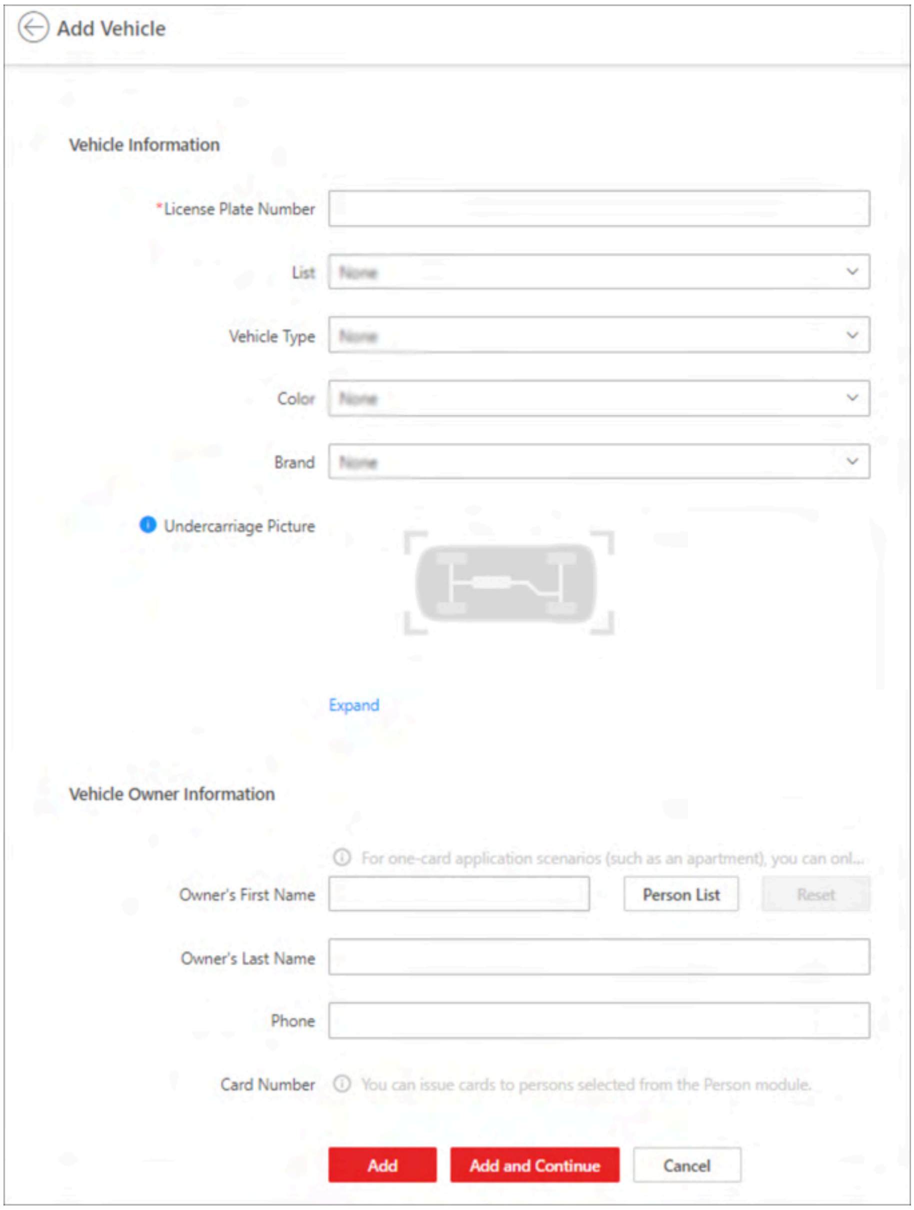



**Figure 16-21 Add Vehicle Page**

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.

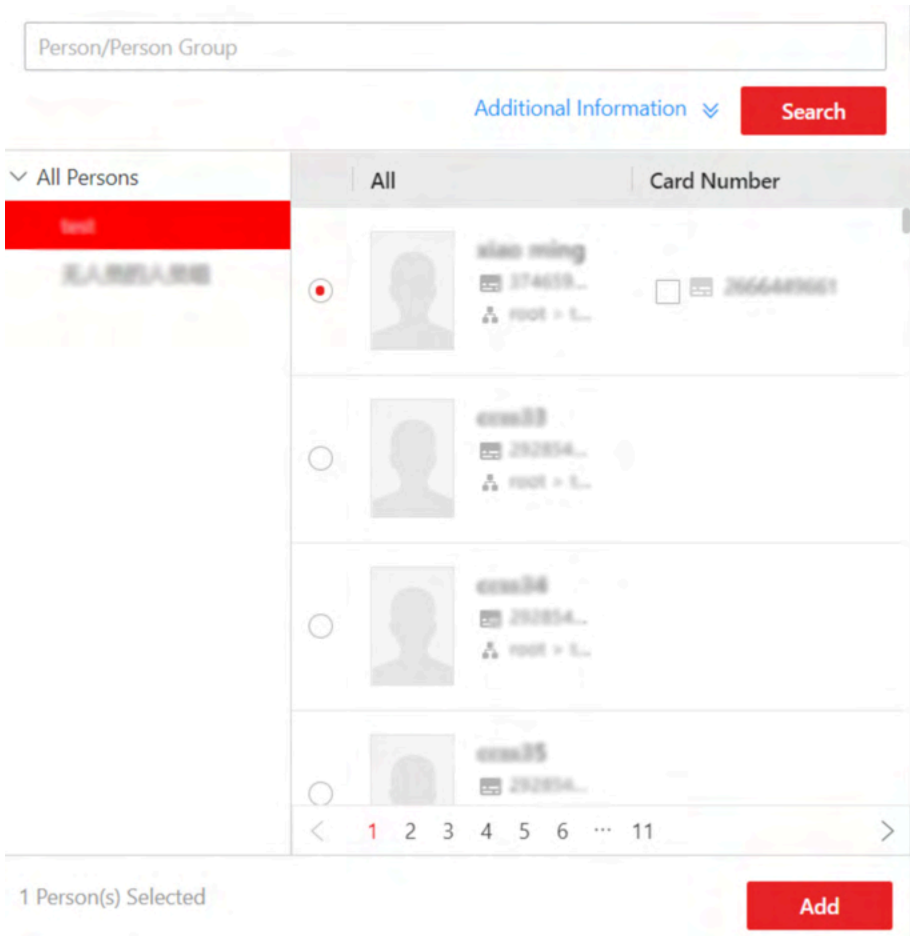



**Figure 16-22 Add Person in Person List as Vehicle Owner**

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. |
| **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**.

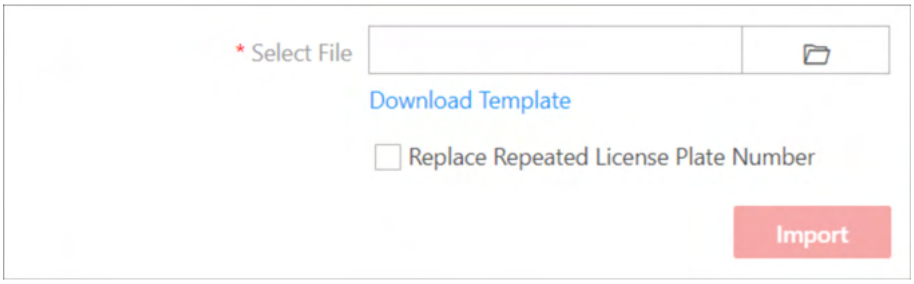



**Figure 16-23 Import File**

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. |
| **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.

### 16.5.2 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.

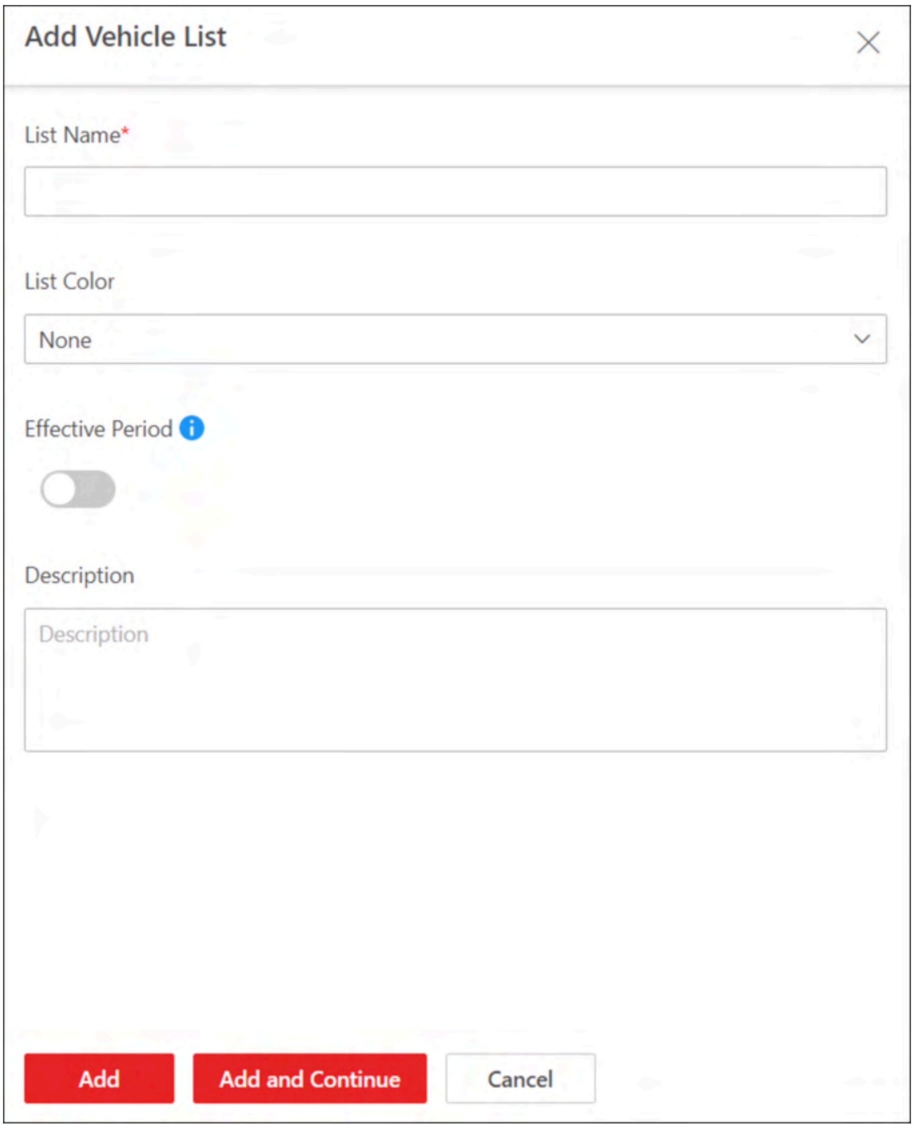



**Figure 16-24 Add Vehicle List Page**

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.

| | |
|---|---|
| **Edit a Vehicle List** | Select a vehicle list and click to edit it. |
| **Delete a Vehicle List** | Select a vehicle list and click to delete it. |
| **Add Vehicle(s) to a Vehicle List** | Select a vehicle list and click **Add** to add vehicle(s) to it.<br>**Note**<br>You can search for vehicles by entering the custom vehicle information. See ***Customize Vehicle Information*** for more details. |
| **Remove Vehicle(s) from a Vehicle List** | Select a vehicle list, check vehicle(s), and click **Delete** to remove them from the current list. |

## 16.5.3 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.

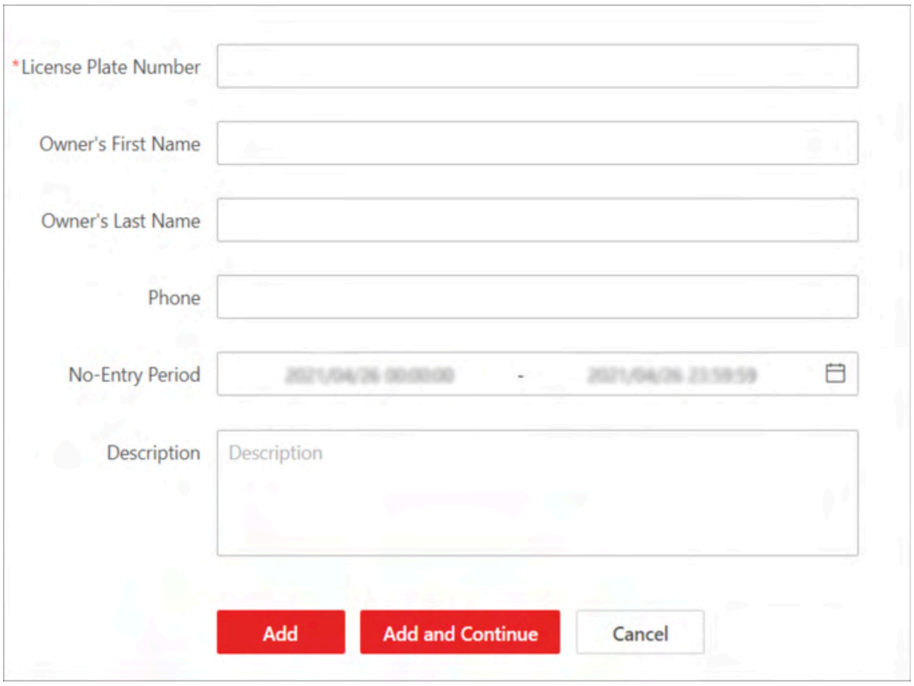



**Figure 16-25 Add Vehicle to Blocklist**

**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**.

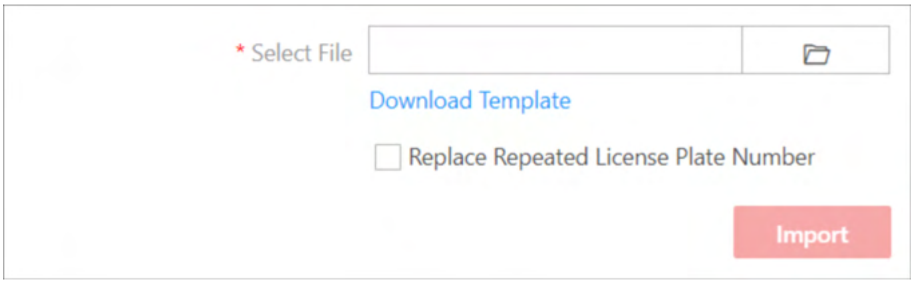



**Figure 16-26 Import File**

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. |

### 16.5.4 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** .

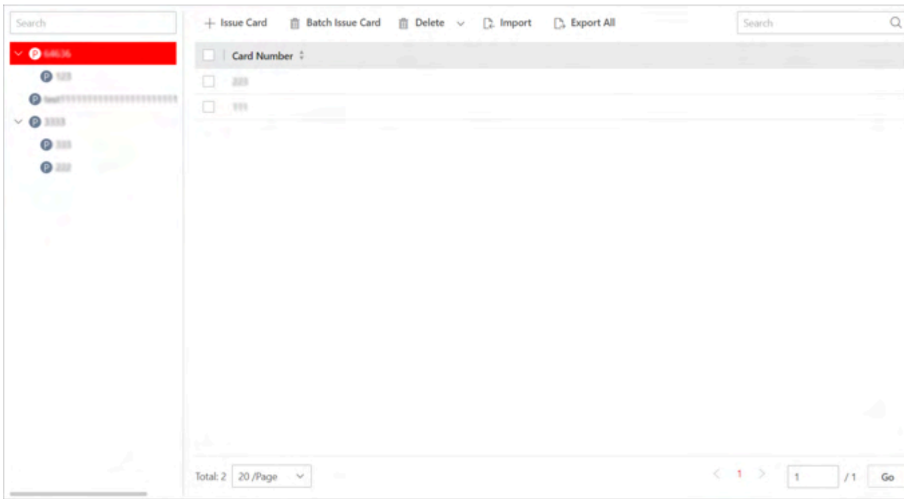



**Figure 16-27 Issue Temporary Card Page**

**2.** Select a parking lot from the left list.

**3.** Click **Issue Card** to open the Issue Card panel.

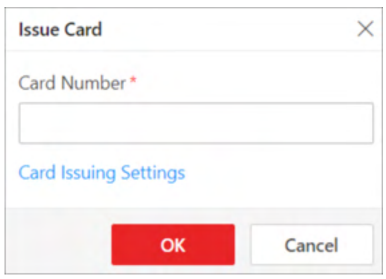



**Figure 16-28 Issue Card Panel**

**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. |

## 16.5.5 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.

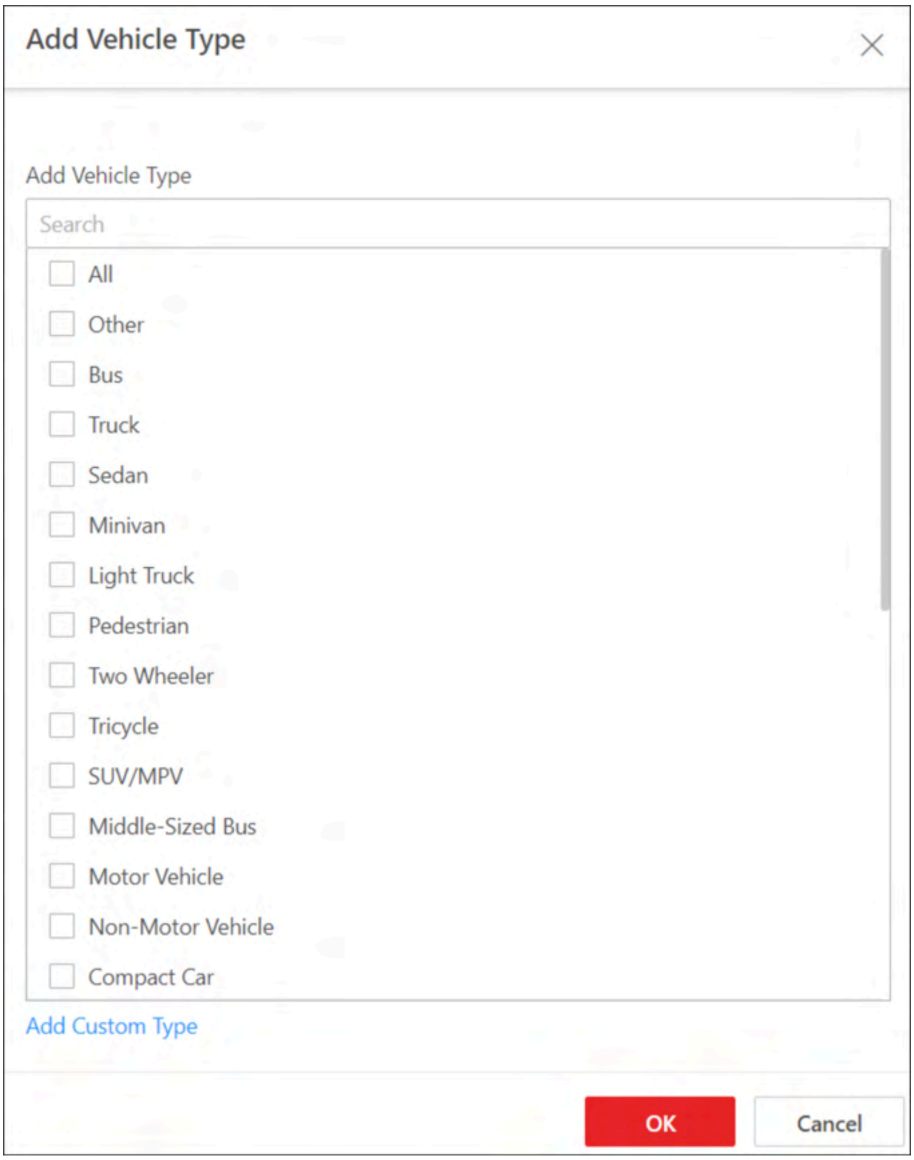



**Figure 16-29 Add Vehicle Type Panel**

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.

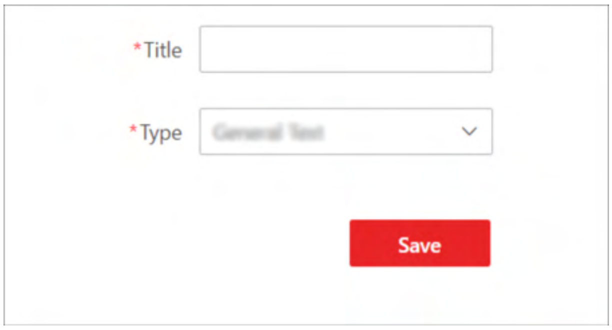



**Figure 16-30 Customize Information Panel**

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. |

## 16.6 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**.

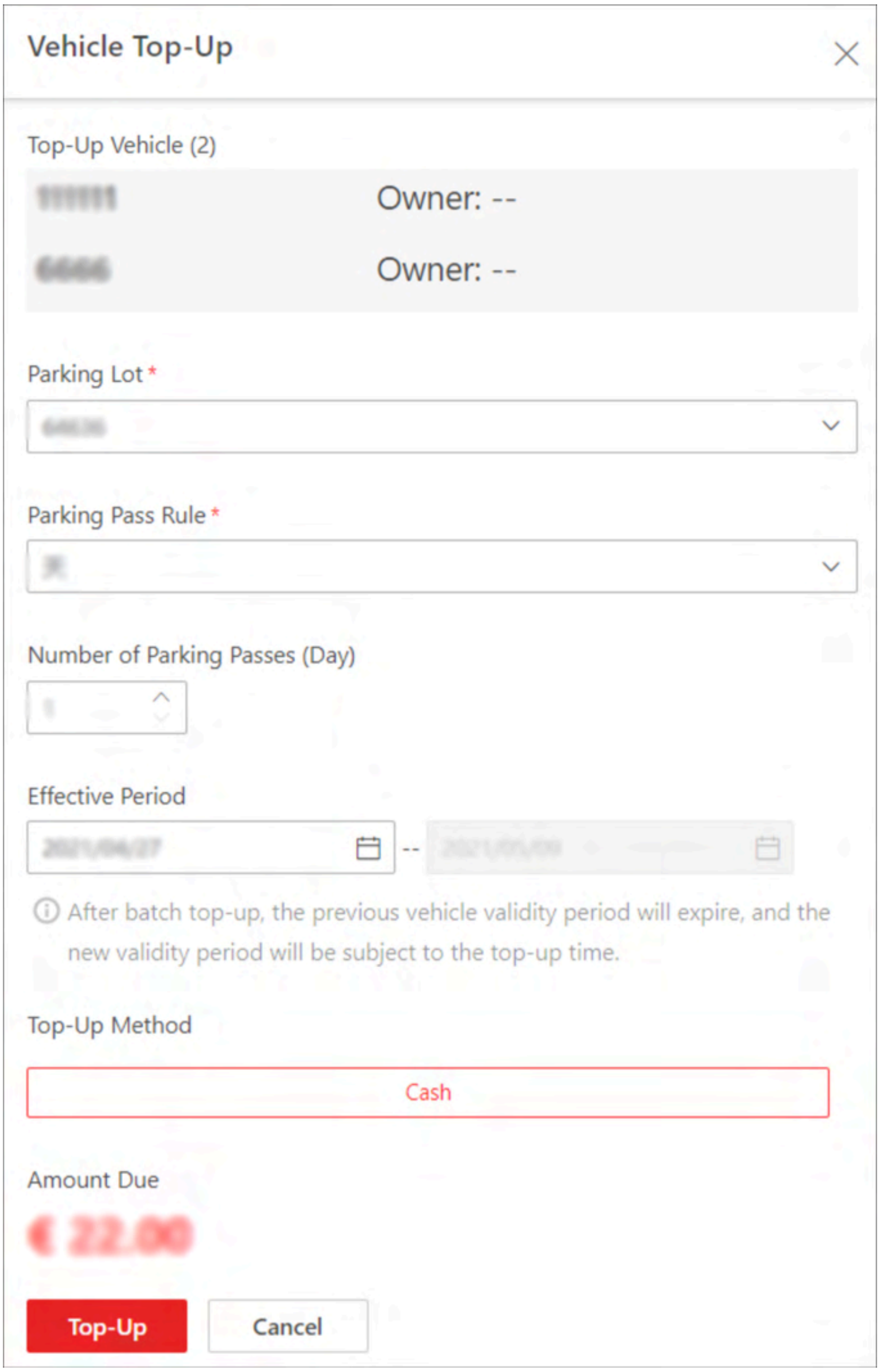



**Figure 16-31 Vehicle Top-Up Window**

**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**.

## 16.7 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** .

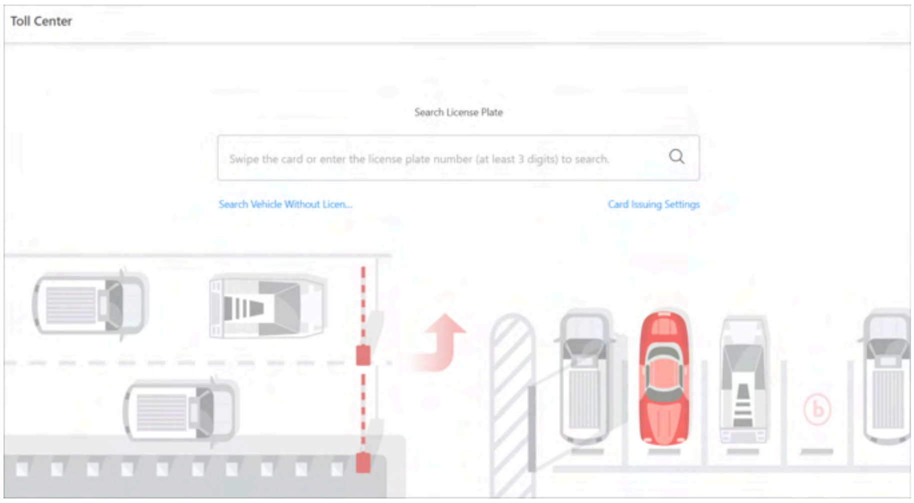



**Figure 16-32 Toll Center Page**

**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.

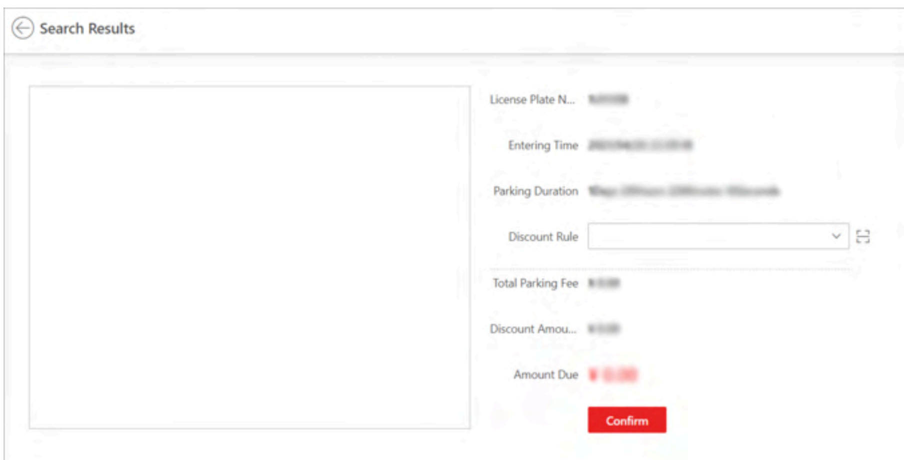



**Figure 16-33 Search Result Page**

**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.

## 16.8 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.

### 16.8.1 Add a Floor to the Parking Lot

In the Parking Guidance Configuration module, you can 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** .

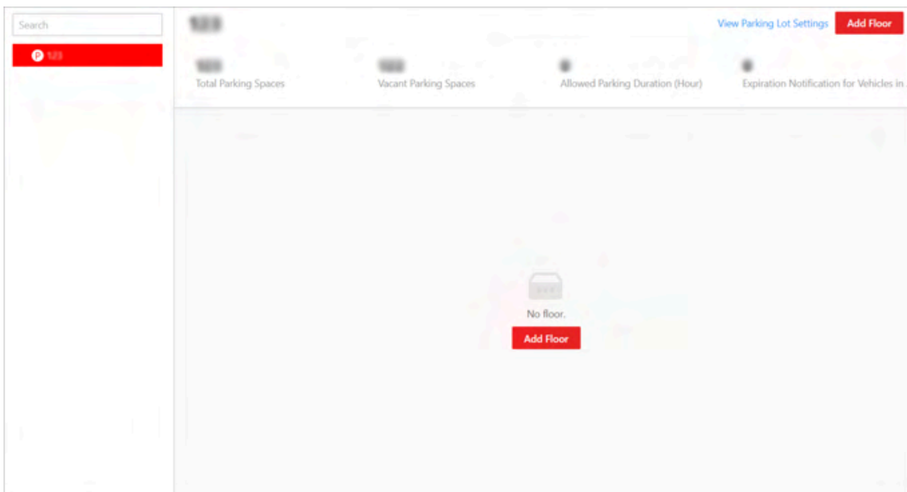



**Figure 16-34 Add Floor Page**

2. Select a parking lot from the left list.
3. In the right area or the upper-right corner, click **Add Floor**.

   The Add Floor panel pops up.
4. Create a name for the floor.
5. Click **OK**.

   You will enter the page for relating devices, configuring a map, marking guidance screen, and configuring types of parking spaces.

**What to do next**

Relate devices to the floor. See ***Relate Devices to the Floor*** .

## 16.8.2 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 and guidance screen) to the floor. The guidance terminal can relate multiple parking cameras for management, such as playing the live video, playing back the recorded video. The 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.

**Before You Start**

Make sure that at least one guidance terminal and one guidance screen have been added to the platform.

**Steps**

**1.** After adding a floor, you will enter the following page.

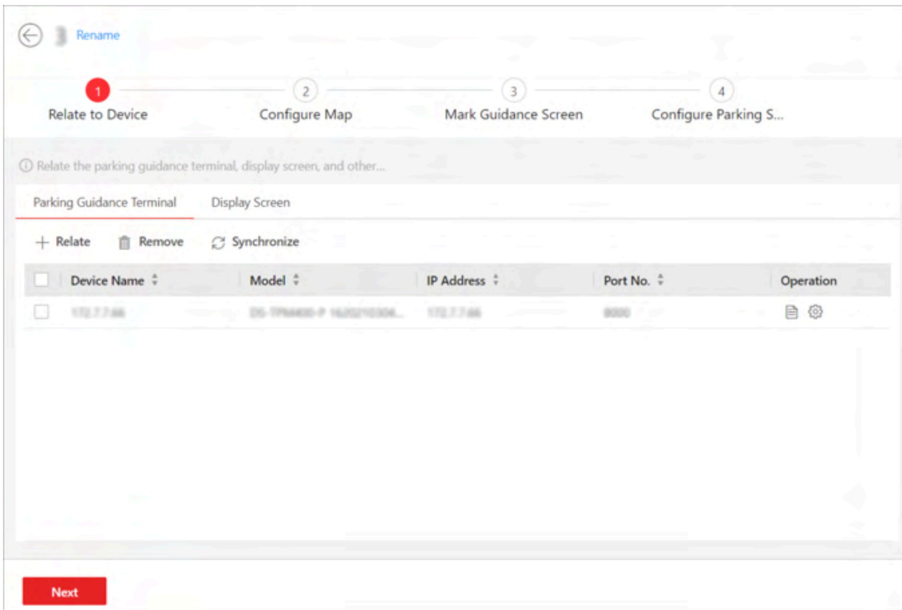



**Figure 16-35 Relate Device Page**

**2.** Click **Relate Device**.

**3.** Relate guidance terminal(s).

1) Click **Guidance Terminal**.
2) Click **Relate** to open the Relate Guidance Terminal panel.
3) Select one or multiple terminals from the list.
4) Click **OK**.
5) **Optional:** Perform the following operations if needed.

- Select one or multiple guidance terminals and click **Remove** to remove the device(s) from the floor.
- 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 the guidance terminal, and the parking spaces monitored by the parking camera(s).
- Click to edit the settings of the guidance terminal.

**Note**

On the pop-up page, you need to log in with the account and password of the terminal.

**4.** Relate guidance screen(s).

**Entrance Guidance Screen**

Displays the welcome message and the number of vacant parking spaces in the parking lot.

**Indoor Guidance Screen**

Displays the number of vacant parking spaces and guides vehicles to the area where there are vacant parking spaces.

1) Click **Guidance Screen**.
2) Click **Relate** to open the Relate Guidance Screen panel.
3) Select one or multiple guidance screens from the list.
4) Click **OK**.
5) **Optional:** Select one or multiple guidance screens and click **Remove** to delete the device(s).

**What to do next**

Click **Next** to configure a map for the floor. See ***Configure a Map for the Floor*** .

## 16.8.3 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.

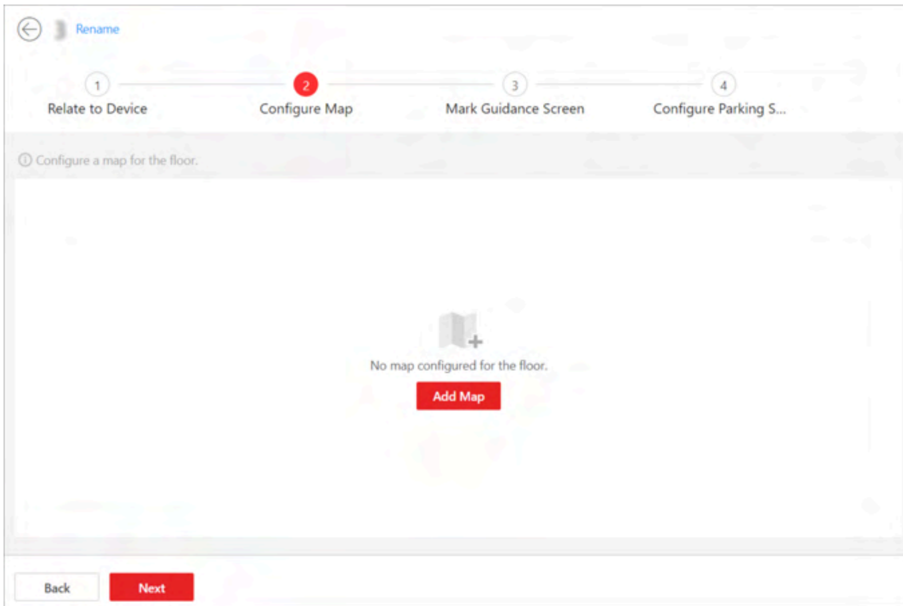



**Figure 16-36 Add a Map**

**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.

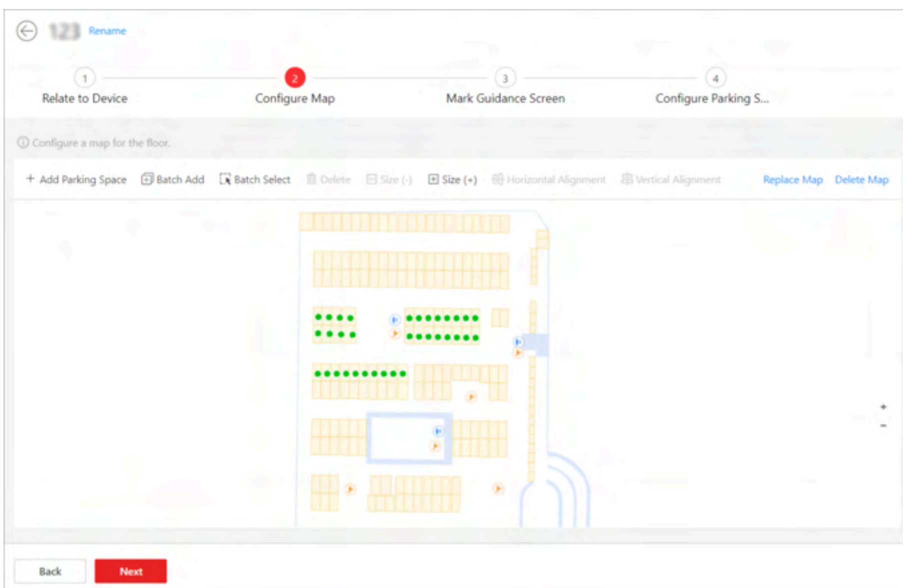



**Figure 16-37 Configure the Map**

**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.<br>• 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.<br>• 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*** .

## 16.8.4 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.

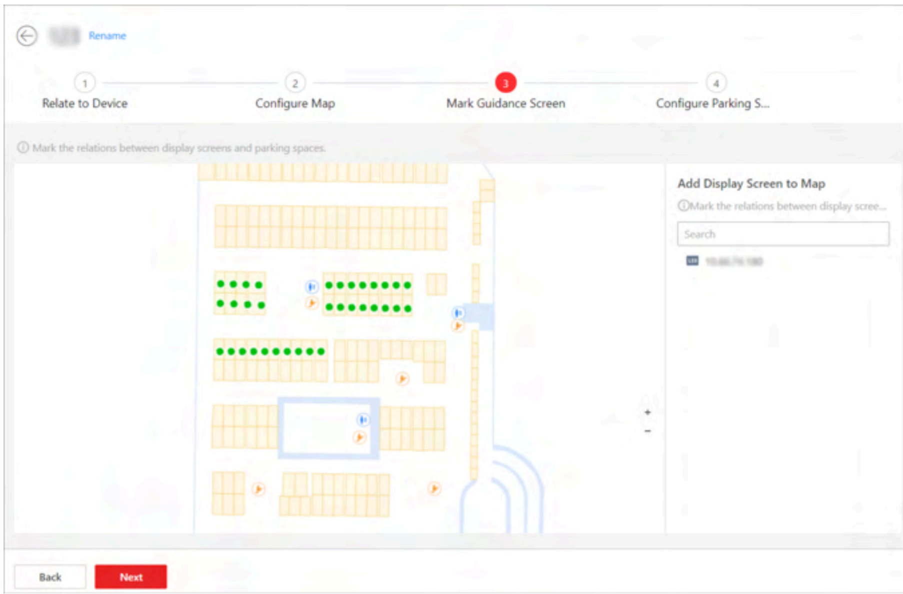



**Figure 16-38 Mark Guidance Screen**

**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 select it, or click **Batch Select** and drag to select multiple parking spaces.

The color of selected parking space(s) will turn into red.

3) Click **OK**.

**Note**

You can also mark the parking space(s) at right or in the middle via the same steps.

**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.<br>a. Click .<br>b. Click anywhere on the map.<br>**Note**<br>The color of the related parking space(s) turns into green.<br>c. Click **OK**. |
| **Add a Related Floor** | Click **Add a Related Floor** and select a floor to add it. |

| | |
|---|---|
| **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 a related map to display it. |

**What to do next**

Click **Next** to configure the types of parking spaces. See ***Set Types for Parking Spaces on the Map*** .

## 16.8.5 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.

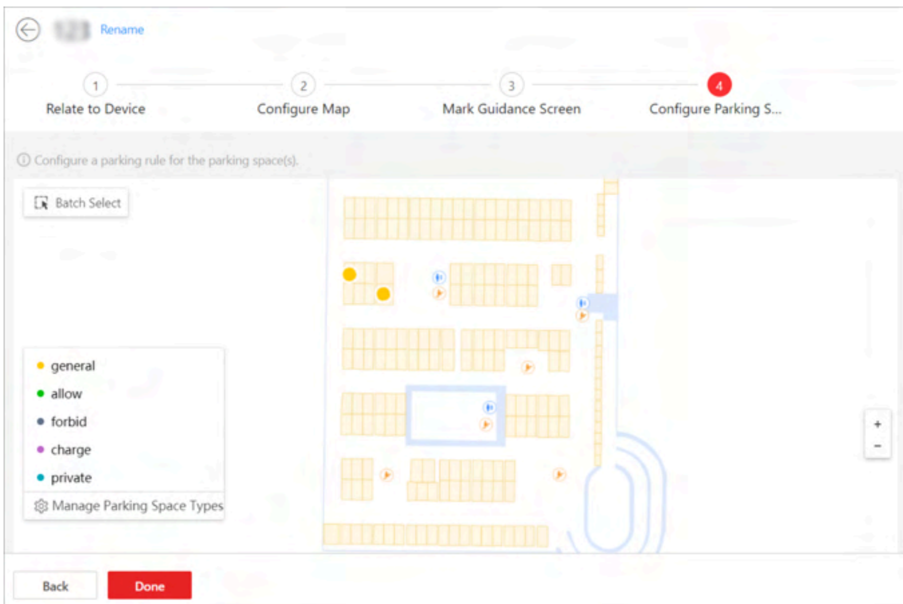



**Figure 16-39 Set Types for Parking Spaces**

**2.** Click a parking space.

The following panel pops up.

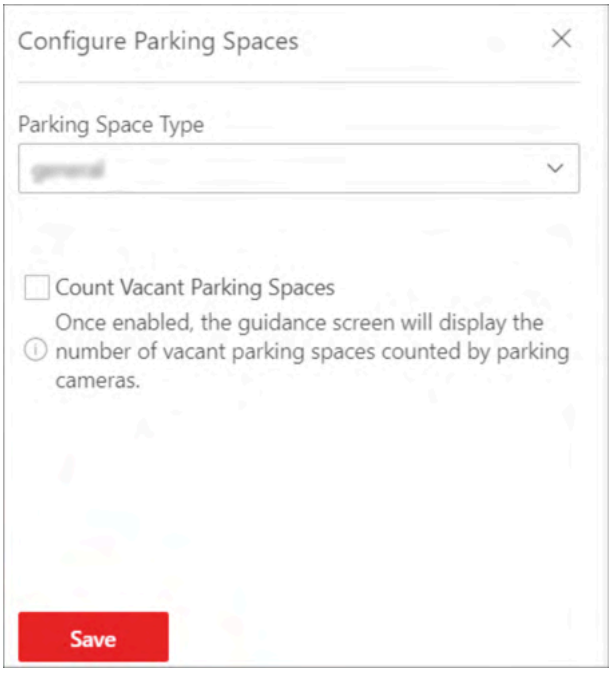



**Figure 16-40 Select a Type for the Parking Space**

**3.** Select a type from the drop-down list.

**4. Optional:** Check **Count Vacant Parking Spaces** to display the number of vacant parking spaces on the guidance screen.

**5. Optional:** Click **Manage Parking Space Types** and perform the following operations if needed.

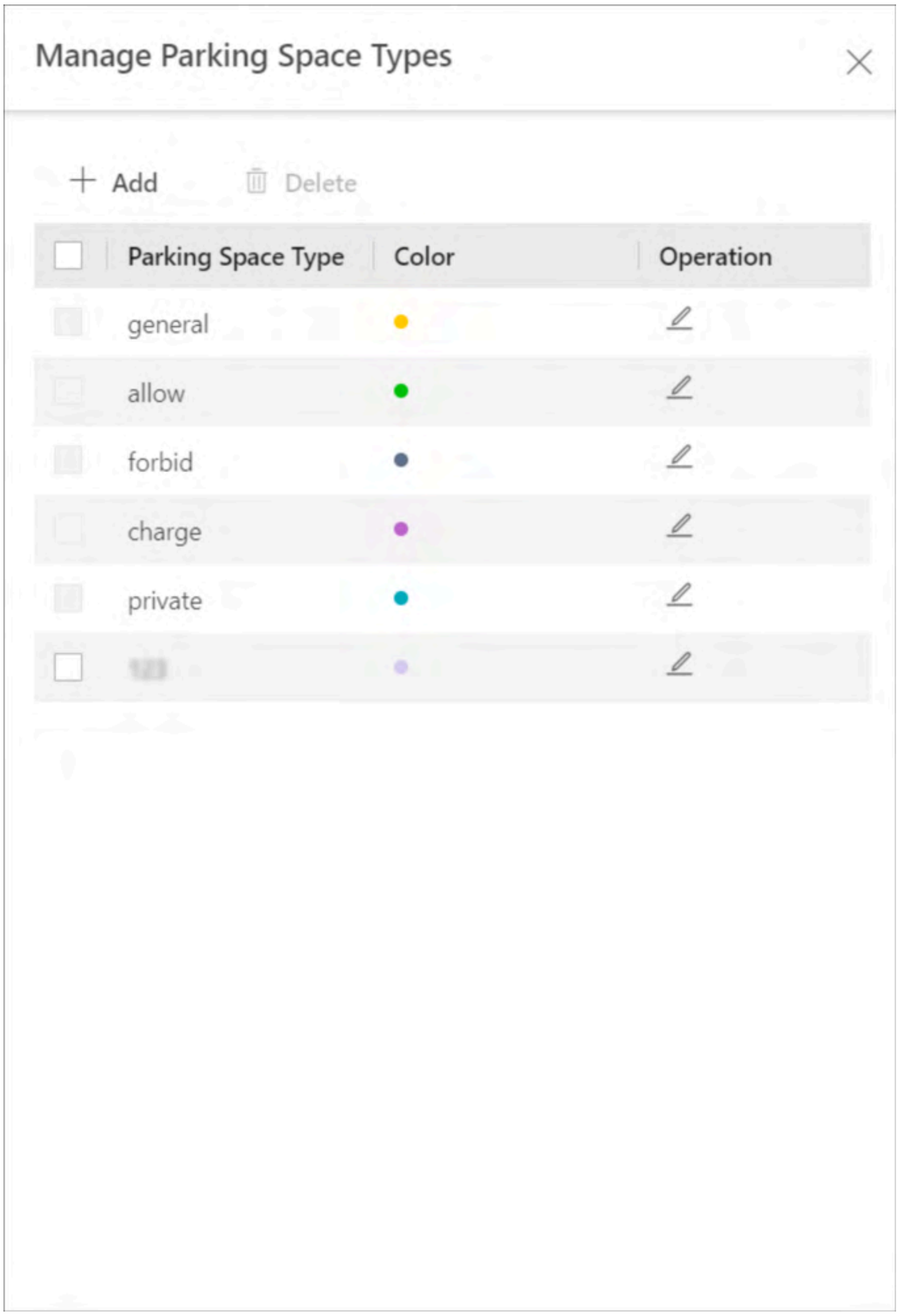



**Figure 16-41 Manage Parking Space Types**

| | |
|---|---|
| **Add a Parking Space Type** | a. Click **Add**.<br>b. Create a name for the type.<br>c. Set a color for the type.<br>d. Click**Save**. |
| **Edit a Parking Space Type** | Click ✎ to edit the name and color of a type. |

| | |
|---|---|
| | **Note**<br>The name of the default types (general, allow, forbid, charge, private) cannot be edited. |
| **Delete Parking Space Type(s)** | Select one or multiple types and click **Delete** to delete them.<br>**Note**<br>The default types cannot be deleted. |

**6.** Click **Done**.

**7. Optional:** Click **Back** to edit former configuration.

## 16.9 Parking Space Monitoring

With this function, you can view the statistics about 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 as well as the number of overtime parking and parking violations. You can also click one parking space on the map to view its detailed information, such as its status and type. In addition, you can enter the parking space No., license plate No., or parking time to search for specific information.

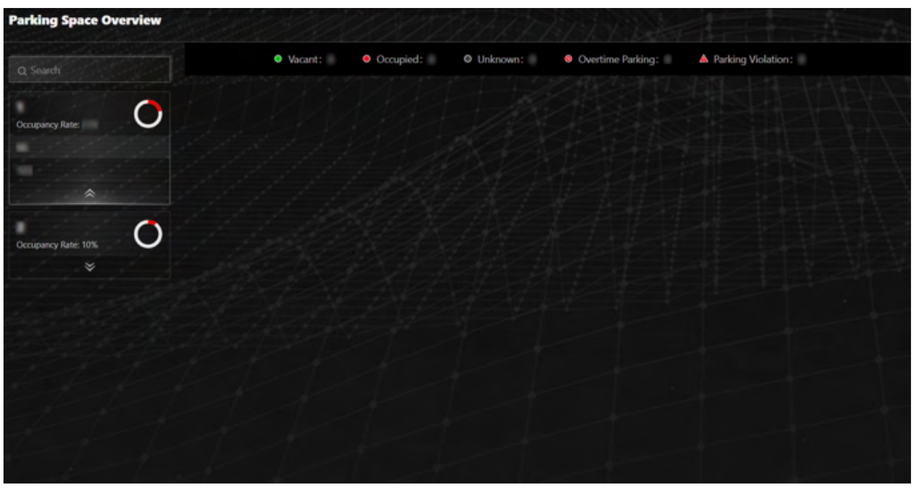



**Figure 16-42 Parking Space Overview Page**

## 16.10 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.

### 16.10.1 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**.


**Figure 16-43 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. |

## 16.10.2 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.

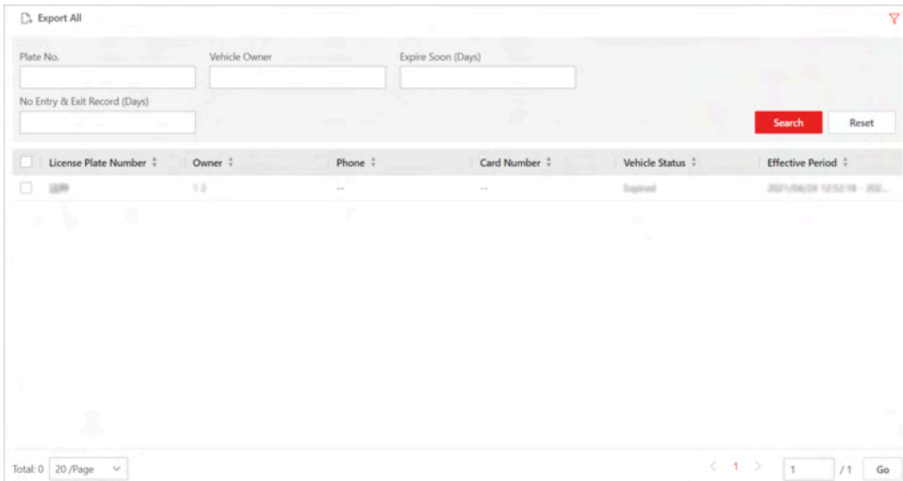



**Figure 16-44 Search Visitor Vehicle Page**

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.

## 16.10.3 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 Home page, select → **All Modules** → **Vehicle** → **Search** → **Vehicle Passing Record Search** .

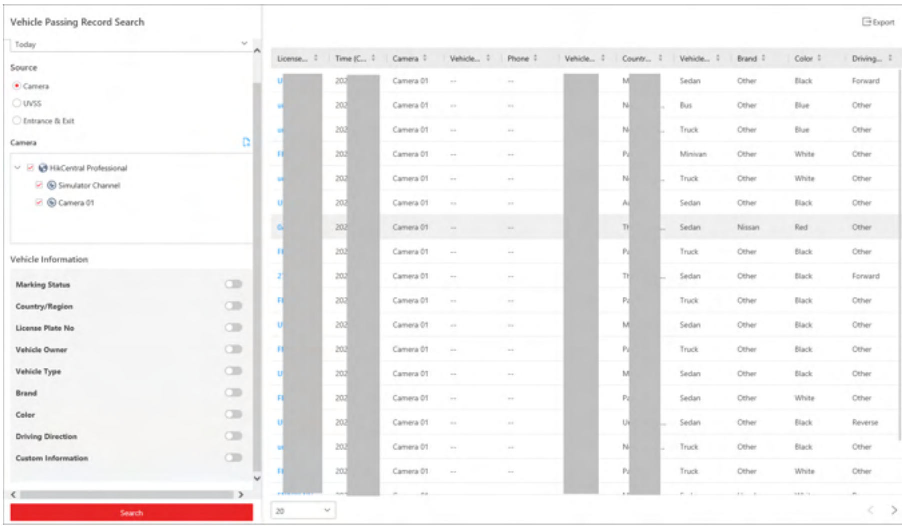


**Figure 16-45 Vehicle Passing Record Search Page**

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.

**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. |
| **Export All Vehicle Passing Records** | a. Click **Export** in the upper-right corner to open the Export panel.<br>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.<br>c. Click **Browse** to select a saving path.<br>d. Click **Save**.<br>**Note**<br>Up to 500 vehicle passing records with captured pictures can be exported at one time. Up to 100,000 vehicle passing records without pictures can be exported at one time. |

### 16.10.4 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 Home page, select → **All Modules** → **Vehicle** → **Search** → **Parking Record Search** .
2. Set search conditions according to actual needs.

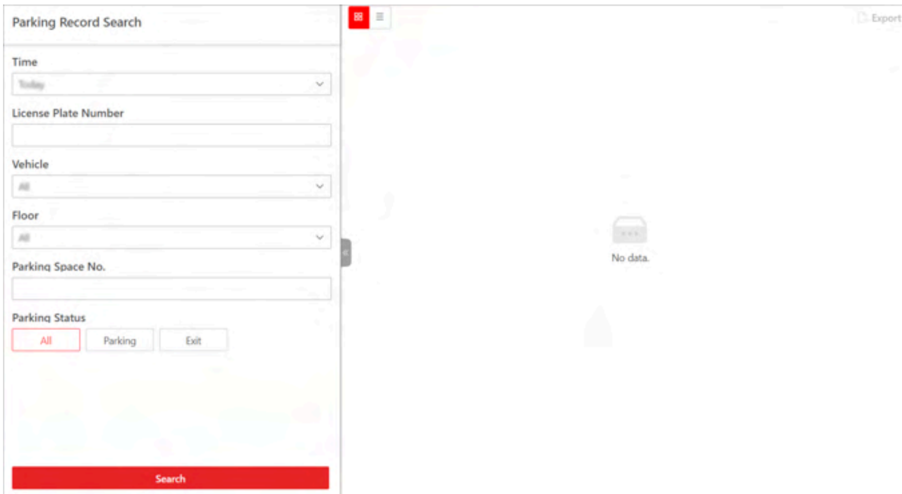



**Figure 16-46 Parking Record Search Page**

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.

## 16.10.5 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 Home page, select → **All Modules** → **Vehicle** → **Search** → **Parked Vehicle Search** .
2. Set searching conditions according to actual needs.

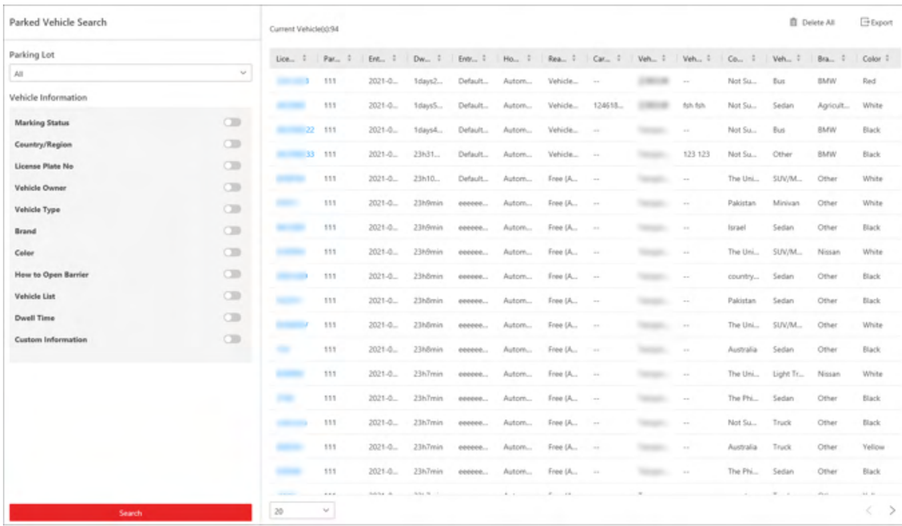



**Figure 16-47 Search Vehicles in Parking Lot**

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.

<table>
<tr><td>Delete Vehicles from Parking Lot</td><td>• Click Delete All to delete all searched vehicles from the parking lot.<br><br>Note<br>After deleting a vehicle in the list, there will be one more vacant parking space in the parking lot.</td></tr>
<tr><td>Export Vehicle Information to PC</td><td>• Save information of all searched vehicles as a file in PC.<br>a. In the top right corner, click Export to open the Export panel.<br>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.<br>c. Click Browse to select a saving path.<br>d. Click Save.<br><br>Note<br>Up to 500 vehicle passing records with captured pictures can be exported at one time. Up to 100,000 vehicle passing records without pictures can be exported at one time.</td></tr>
<tr><td>View Vehicle Information</td><td>Click a license plate number in the list to view the detailed information of the vehicle.</td></tr>
</table>

## 16.10.6 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** .

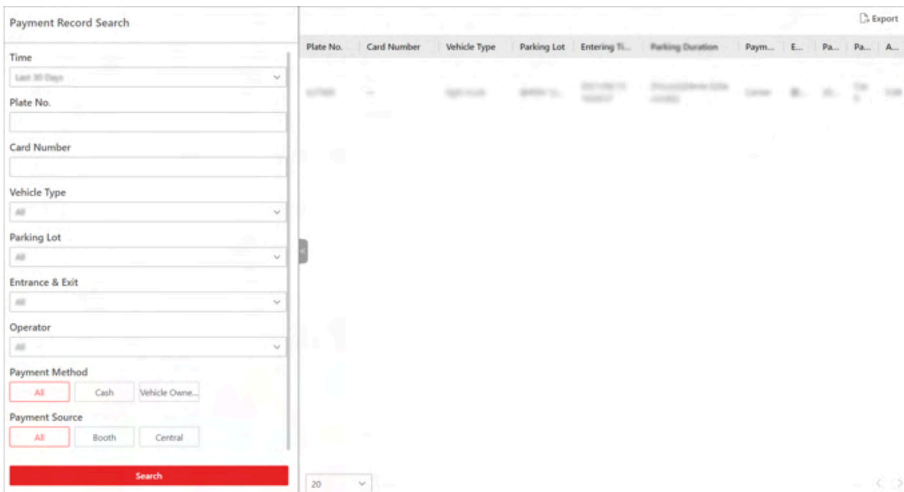



**Figure 16-48 Payment Record Search Page**

**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.

## 16.10.7 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** .

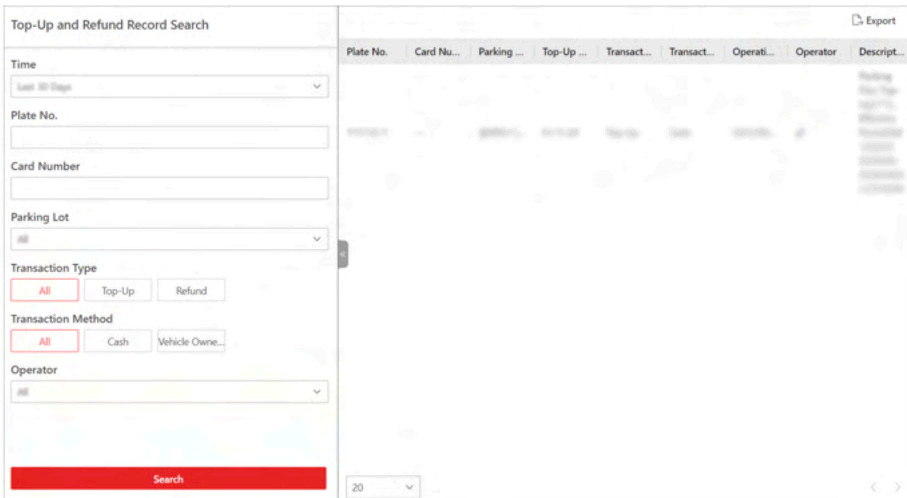



**Figure 16-49 Top-Up and Refund Record Search Page**

**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.

## 16.10.8 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.

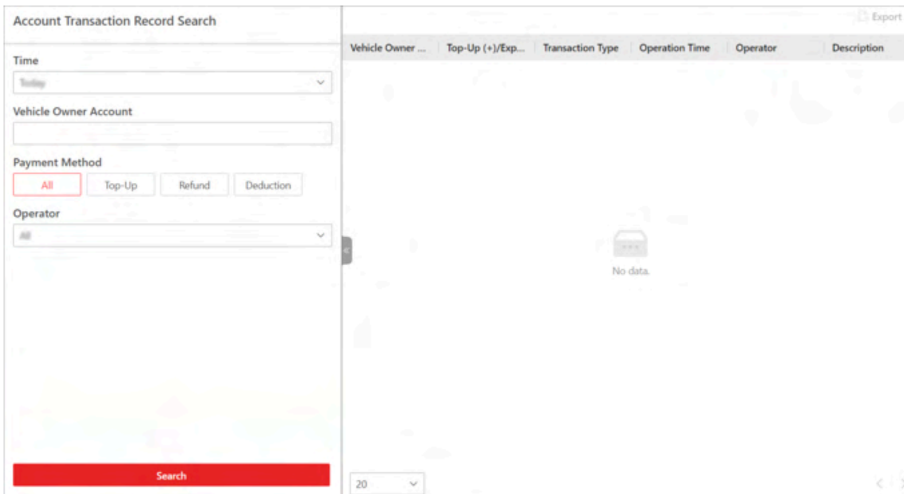



**Figure 16-50 Account Transaction Record Search Page**

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.

## 16.10.9 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 offduty 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.

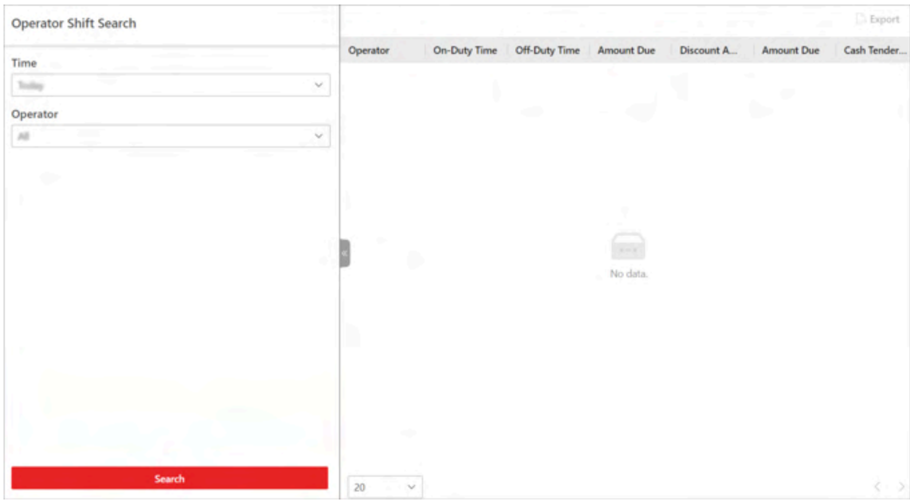



**Figure 16-51 Operator Shift Search Page**

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.

## 16.10.10 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.

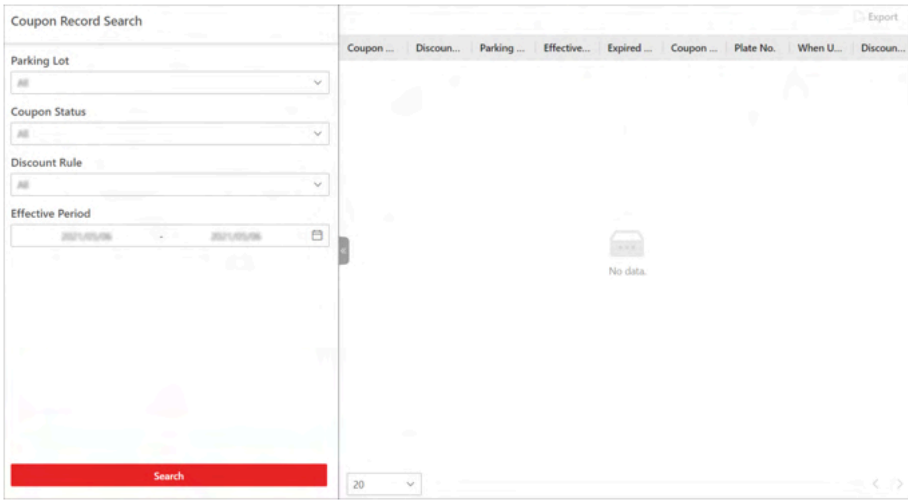



**Figure 16-52 Coupon Record Search Page**

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.

## 16.11 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.

## 16.12 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** .

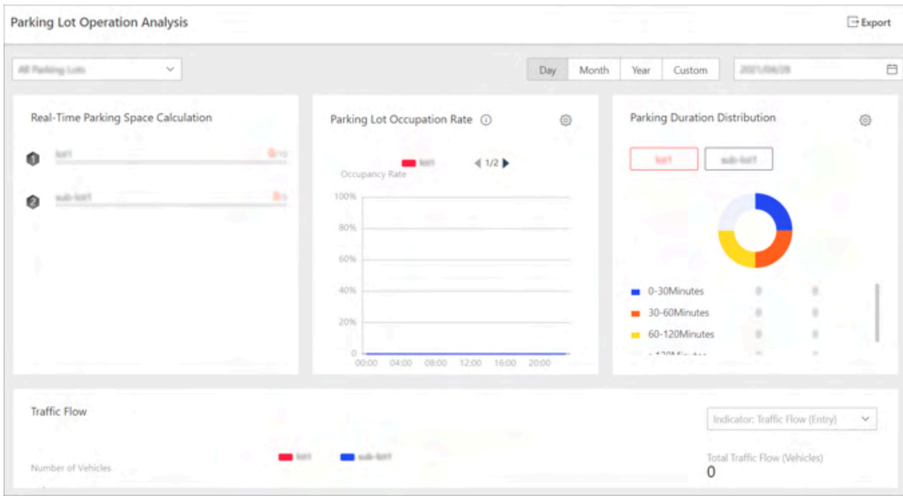



**Figure 16-53 Parking Lot Operation Analysis Page**

**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.

## 16.13 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** .

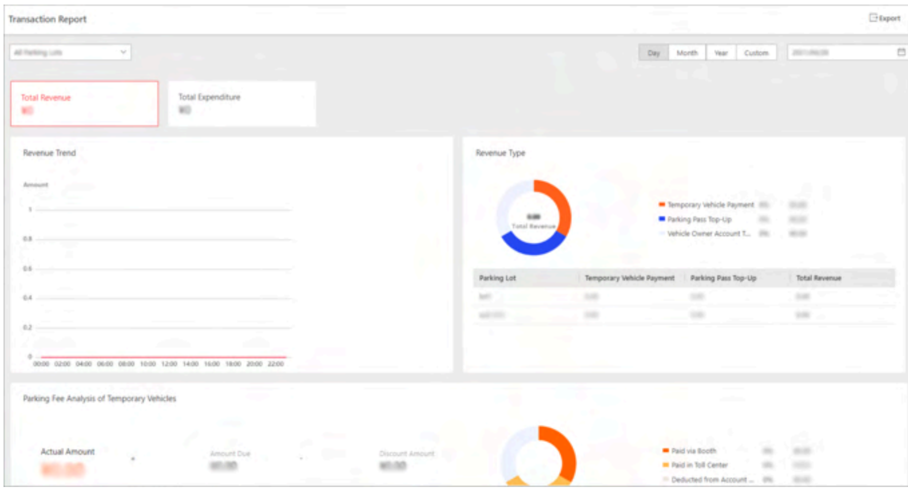



**Figure 16-54 Transaction Analysis Page**

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.

## 16.14 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.

# Chapter 17 Visitor Management

The system provides an entire process for visitors tour from registration to check-out. You can group visitors with different visiting reason to different access groups for effective management; customize the accessible area of the visitors, and the visitors can access the areas by various ways like face picture, and ID card.

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.

## 17.1 Flow Chart

The flow chart below shows the process of visitor settings management.

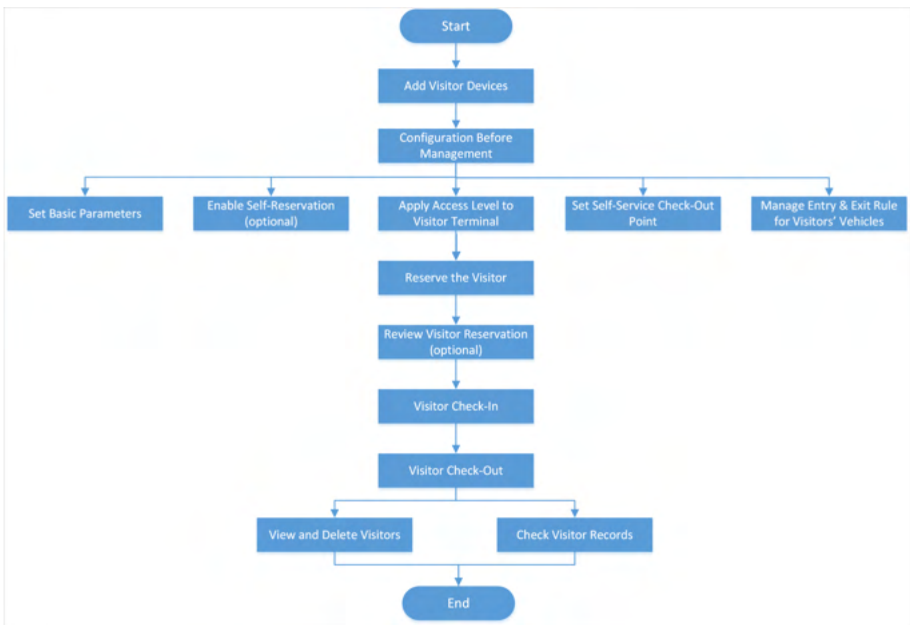



**Figure 17-1 Flow Chart**

**Table 17-1 Flow Chart Description**

| Procedure | Description |
|---|---|
| Add Visitor Devices | Add devices used for visitor reservation, check-in, check-out, authentication, etc. See ***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 |

| Procedure | Description |
| --- | --- |
| | 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 visitee 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. 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 and Delete Visitors in Visitor List*** for details. |
| Check Visitor Records | Filter and check visitor records. See ***Check Visitor Records*** . |

## 17.2 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.

### 17.2.1 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, Visitor 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.

**Take Photo of Visitor's Belongings**

If you enable this function, you can take a picture for the visitor's belongings and upload to the platform when checking in/out for the visitor.

**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 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 Frequency** will be disabled if you enable **Auto Checkout for Visitor After Effective Period**.

**Alarm Detection Frequency**

With the **Alarm Detection Frequency** enabled, if the 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 Frequency**. By default, the **Alarm Detection Frequency** should range from 3 to 10 minutes.

**Visit Purpose**

You define visit purpose 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.

**Visitor Email Template**

You can select the email templates sent to visitors when they successfully reserve or check in. You can customize the templates according to your need. See ***Add Visitor Email Template*** for details.

**Visitor 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 mobile phones. When checking in, the visitor should provides the reservation code.

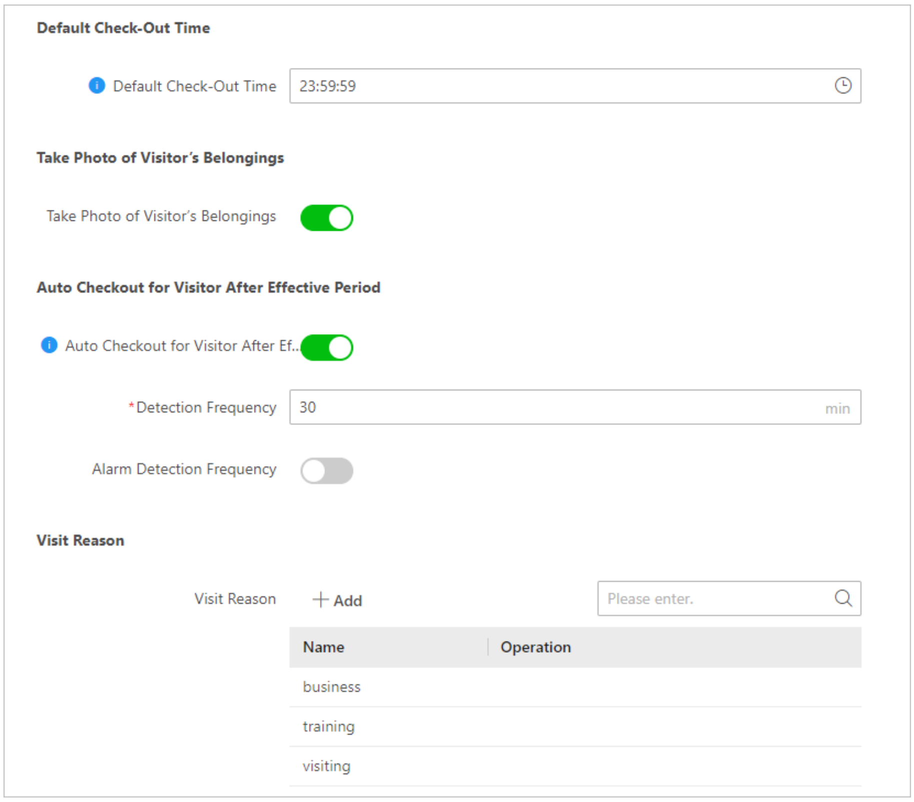



**Figure 17-2 Basic Parameters**

**3.** Click **Save**.

## 17.2.2 Add a Visitor Type

You can add visitor types 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.

**Steps**

**1.** In the top left of the Home page, select  → **All Modules** → **Visitor** → **Visitor Settings** → **Visitor and Registration** → **Visitor Information** .

**2.** Click + to open the Visitor Type Name window.

**3.** Create a visitor type name, and then click **Add**.

**4. Optional:** Perform the following operations after adding a visitor type.

| | |
|---|---|
| **Edit Visitor Type** | Click  to change the visitor type's information. |
| **Delete Visitor Type** | Select a visitor type and click  to delete it. |

### 17.2.3 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.

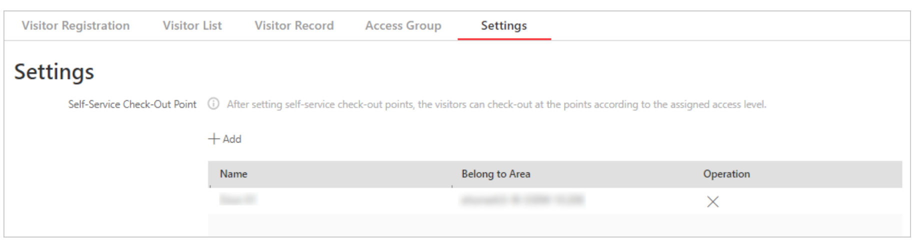



**Figure 17-3 Set Self-Service Check-Out Point Page**

4. **Optional:** Select a self-service check-out point and click to cancel setting the door as a self-service check-out point.

### 17.2.4 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.<br>The default access level will be automatically selected for the visitor when registering a visitor. |
| **Delete Access Levels for Visitors** | Select access levels and click **Delete** to delete the selected access group.<br>Or click → **Delete All** to delete all the access levels. |

**What to do next**

Apply visitor's access levels to device. See ***Manually Apply Visitors' Access Level Settings to Device*** for details.

## 17.2.5 Manually Apply Visitors' Access Level Settings to Device

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. You should apply the changes to the devices to make the changes take effect.

**Steps**

1. In the top left of the Home page, select → **All Modules** → **Visitor** → **Visitor Settings** → **Basic Settings** → **Access Level** .
2. Click to open the Apply Access Level Settings window.
3. There are two modes of applying access level settings available. Select the applying mode according to your actual needs.

   **Apply**

Apply the visitors' changed (newly added, edited, deleted) access levels to the devices. It will keep the configured and applied access levels on the devices. This mode is frequently used when the visitor information, access group information, or access level settings are changed, such as added, edited, and deleted.

In this mode, select the visitors to apply their access level settings to the selected access points.

**All Visitors**

The access level settings of all the visitors in the visitor list will be applied to the selected access points.

**Specified Visitor**

The access level settings of the target visitors will be applied to the selected access points.

**Apply (Initial)**

First, clear all the access levels configured on the devices. Then, apply all the visitors' access levels configured in the system to the devices. This mode is mainly used for first time deployment.

**Note**

During this initial applying process, the devices will be offline for a while, and visitors cannot access via these access points.

4. Select the access point(s) to apply the visitors' access level settings to.

**Note**

You can select doors of access control devices or video intercom devices to apply the access level settings to.

5. **Optional:** If the visitors' access level settings are changed (such as changes of linked access level, credentials, etc.) or the applying process failed, the icon will display near the icon, indicating that these new access level settings should be applied to the device. You can hover the cursor to it to view how many visitors' access levels should be applied to the device.

## 17.2.6 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 designate 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 of top left corner of Home page, select → **All Modules** → **Visitor** → **Visitor Settings** → **Basic Settings** → **Visitor Email Template** .

2. Click **Add**.
3. Select the email type.
4. Enter the required parameters.

   **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 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.
5. 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.
6. **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**

In the email template list page, there are two default templates. You can view or edit default templates but not delete them.

## 17.3 Visitor Reservation

Before visiting, visitors can make a reservation. The Administrator can make a reservation for the visitors by entering the visitor and visitee 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.

### 17.3.1 Reserve a Visitor

You can make a reservation for one visitor by entering the visitor and visitee information on the platform

**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, 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, visitee, 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, including license plate number, gender, email, etc.

**Note**

- The license plate number can be added to the parking lot so that the visitor's vehicle will be recognized as visitor vehicle and be allowed to enter or exit from the parking lot.
- The email is used to receive the reservation code.

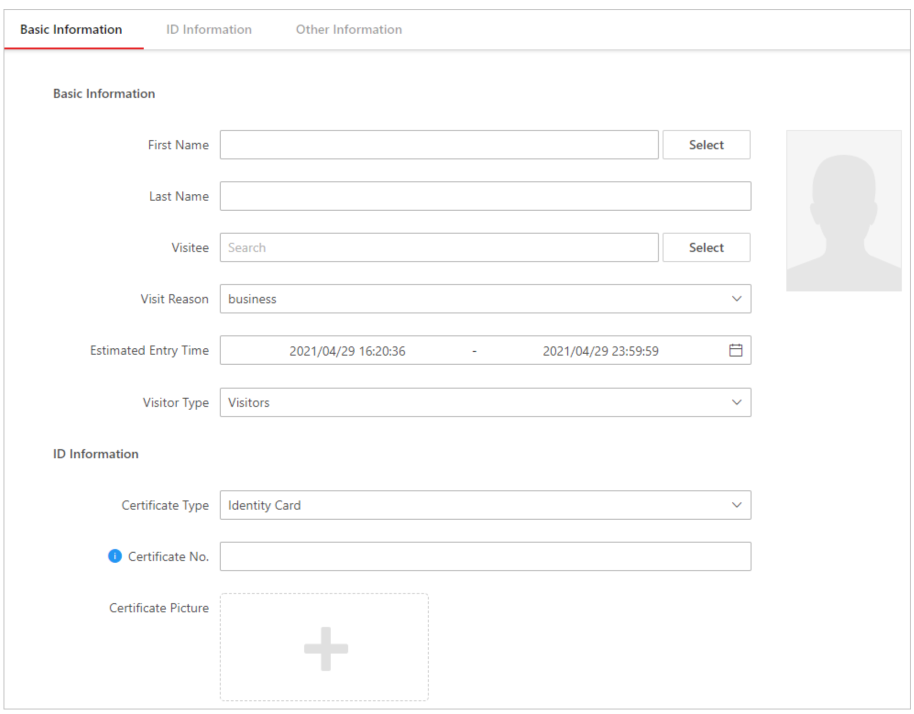



**Figure 17-4 Reserve Page**

6. Click **Reserve** to finish the reservation, or click **Reserve and Continue** to finish the reservation and continue to reserve for other visitors.

7. **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.

## 17.3.2 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.

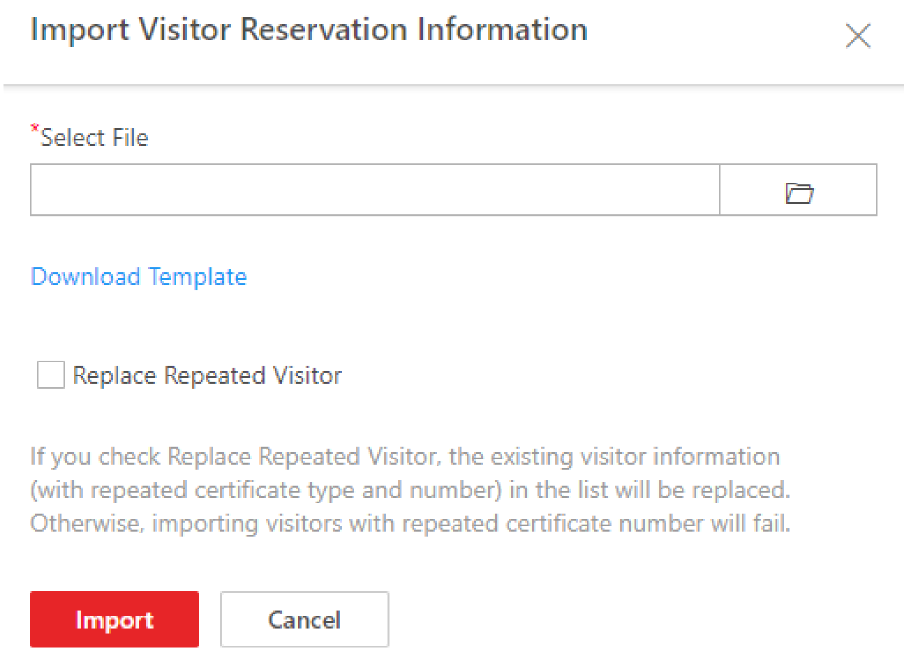



**Figure 17-5 Import Visitor Reservation Information**

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.

### 17.3.3 Set Self-Service Reservation Parameters

Before the visitors starts self-registration, you need to enable self-service registration and set self-service registration parameters. A QR code is necessary for registering visitor information. Besides, you can configure face quality verification and visitor information review.

**Steps**

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 visitees or visitors who are going to reserve. The visitee 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 photo 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 system beforehand.

**Visitor Group**

Set a default visitor group. After reserving successfully, the visitors will be added to this group. If you do not select a visitor group, the visitors 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. If you do not enable this, all self-reservations will take effect.

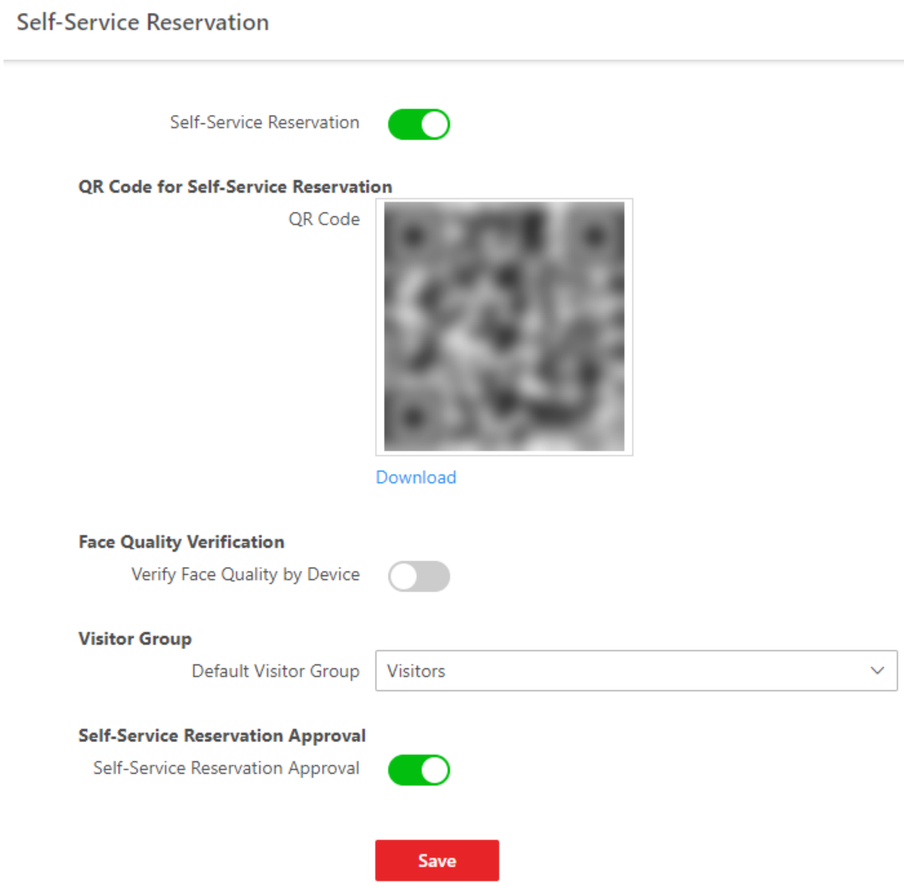



**Figure 17-6 Self-Service Reservation**

**4.** Click **Save**.

### 17.3.4 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**

**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.

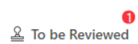



**Figure 17-7 The Number of The To-Be-Approved Visitors**

**2.** Click **To Be Reviewed** on the top.

**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 is correct, 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 there is something wrong or missing with the self-service reserved visitor information, 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.

## 17.4 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.

### 17.4.1 Check in a Visitor Without Reservation

Prior to 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, visitee, 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 **Visitee** to select an existing person as the visitee.
- You can set the visitor profile picture by 3 ways: collecting a face picture from device, take a picture by the camera of the running computer, or upload a picture saved in the running computer.
- Hover the cursor on the uploaded profile picture and click **×** to delete it.

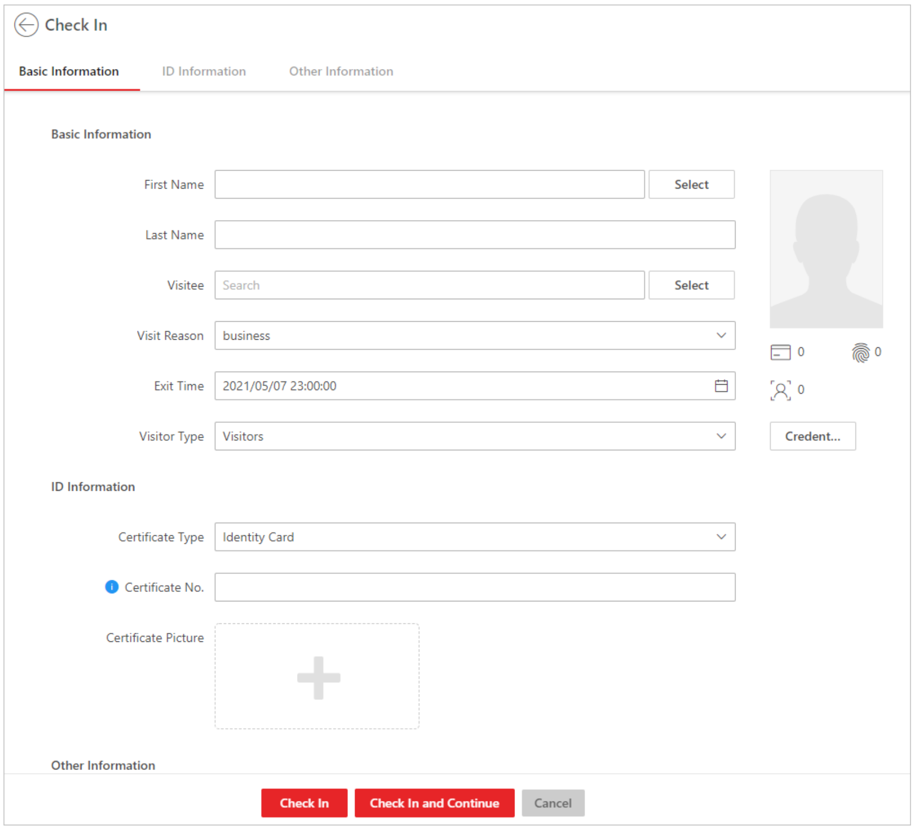



**Figure 17-8 Check-In Page**

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 17-9 Read Card**

**Note**

Only one card can be issued to a visitor.

**Fingerprint**

Platform provides three ways to collect fingerprint: 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 scenario that 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 scenario that 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.

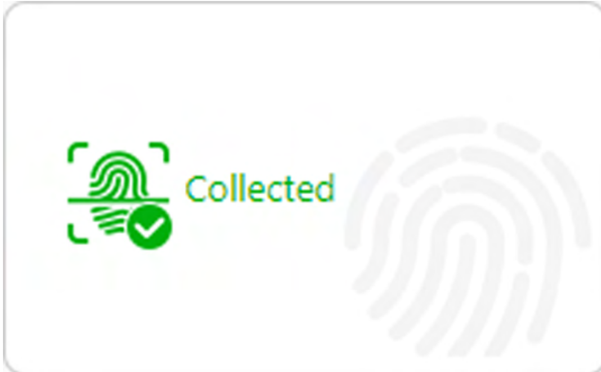



**Figure 17-10 Fingerprint Recorded**

**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. Edit other information, including license plate number, gender, skin-surface temperature, etc.

**Valid Times for Visit**

The maximum times a visitor can access certain doors or floors by QR code authentication. For example, if you set 4 for the visitor, the visitor can access the authorized doors and floors for 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.

8. Click **Check In** to check in the visitor and return to the previous page; click **Check In and Continue** to save the settings and continue to check in another visitor.
9. **Optional:** Perform the following operations after adding a visitor.

| | |
|---|---|
| **Filter Visitors** | Click to filter visitors by certificate No., name, phone, company, visitee, visit reason, visit time, status, and skin-surface temperature. |

| | |
|---|---|
| **Export Visitors** | Select visitors and click **Export** to export registered visitors to the computer as a file.<br>**Note**<br>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. |
| **Check Out Visitors** | Select visitors and click **Check Out** to check out for the visitor. |
| **Edit Visitor Information** | Click on a visitor's name to edit the information.<br>**Note**<br>If the visitor is checked out, you cannot edit the information. |
| **Download 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. |

**What to do next**

You can view the added visitors in the Visitor List. For details, see ***View and Delete Visitors in Visitor List*** .

## 17.4.2 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**.

## 17.5 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.

## 17.6 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.

### Manually Check-Out A Visitor

In the top left of the Home page, select → **All Modules** → **Visitor** → **Visitor Check-In** → **Visitor Check-In** , and then select a visitor and click **Check-Out** to open the Check-Out window. The visitor's information will show. You can click to take a picture of the visitor's belongings or upload the picture of the visitor's belongings to the platform.

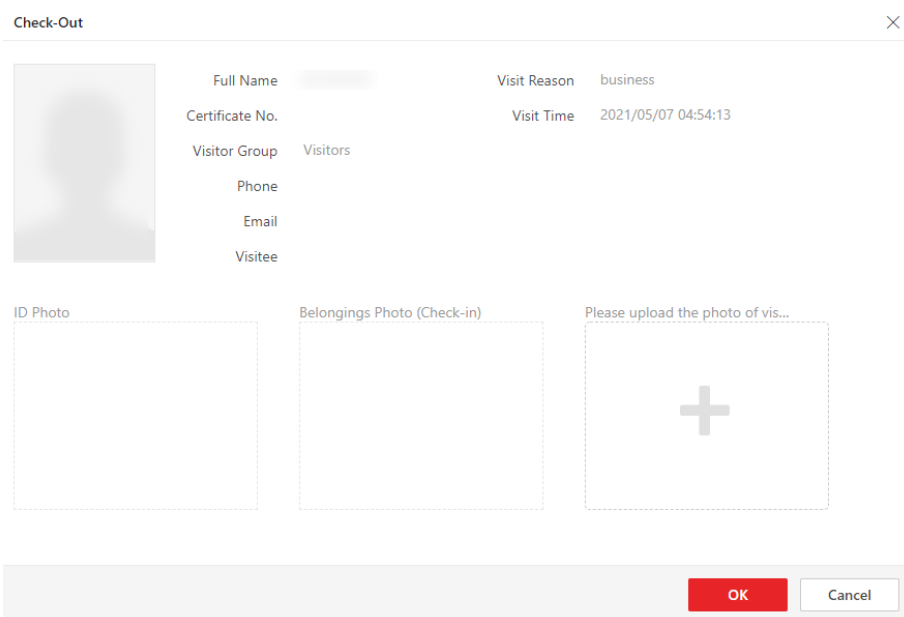



**Figure 17-11 Manually Check Out for A Visitor**

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 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.

### Manually Check-Out for Multiple Visitor

In the top left of the Home page, select → **All Modules** → **Visitor** → **Visitor Check-In** → **Visitor Check-In** , and then select multiple visitors and click **Check-Out**.

### Automatically Check-Out

The visitor will be checked out by the system automatically when the visiting duration ends if you do not manually check out for him/her.

**Note**

You can still view the checked-out visitor's information in Visitor List. See ***View and Delete Visitors in Visitor List*** for details.

## 17.7 View and Delete Visitors in Visitor List

You can view all registered visitors (including those who have checked out) in the visitor list and perform related operations if you need.

In the top left of the Home page, select → **All Modules → Visitor → Visitor Check-In → Visitor Information** , and information of all the registered visitors will appear, including basic information, credential information, and access information. You can perform the following operations.

- 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.
- **Delete Visitor:** Check one or more visitor 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:** Check one or more visitor and click **Move** to move the selected visitor(s) into a different visitor group.
- **Register Again:** For regular visitors that have checked out, you can find them and click to register again quickly. In the opened Register Again window, set the visiting information. The visitors' existing basic information (including personal information, profile, and fingerprint) are not needed to recollect.

  **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 any more.

## 17.8 Check Visitor Records

Visitor records refer to the visitors who have checked in. By filtering visitors who have checked in, you can quickly get the information of wanted visitors. For example, by filtering records of visitor who have checked in but not checked out, you will know who still stays at the visiting place, and call the visitor or find the visitor at the place of last access to remind her/him to check out.

In the top left corner of Home page, select → **All Modules → Visitor → Visitor Access Record** to display the visitor records. On the top of the visitor records, total visitor amount and unchecked-out visitor amount are displayed. Click on the top right to filter visitors by certificate No., name, phone, company, visitee, visit reason, visit time, status, and skin-surface temperature.

With the visitor records, you can learn the visitors' visitee, visit reason, location of last access, entering time, entering location, exiting time, exiting location, and status. Click **Export** to save the visitor records as an excel file to your PC.

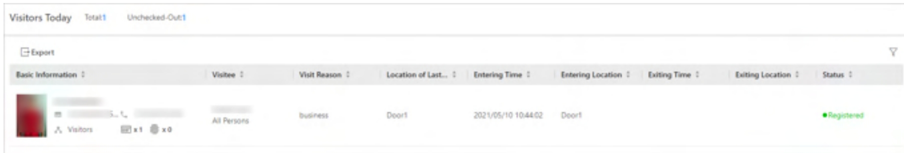



**Figure 17-12 Visitor Records Page**

**Location of Last Access**

The place of a visitor's last authentication. By this location, you can quickly find the visitor.

**Entering Time**

The time when a visitor checks in.

**Entering Location**

The location where a visitor checks in by authentication on access points. The names of the access point and card reader of the location are displayed.

**Exiting Time**

The time when a visitor checks out by swiping card on a self-service check-out point. If the visitor check-out in other way, no information will be displayed here.

**Exiting Location**

The location where a visitor checks out by swiping card/fingerprint authentication/face authentication at a self-service check-out point. The names of the door and card reader of the location are displayed. If the visitor checks out in other way, no information will be displayed here.

**Note**

See ***Set Self-Service Check-Out Point*** for details about how to set a self-service check-out point.

# Chapter 18 Time & Attendance

In the Attendance module, you can easily manage the time & attendance system of your organization and track your employees' attendance.

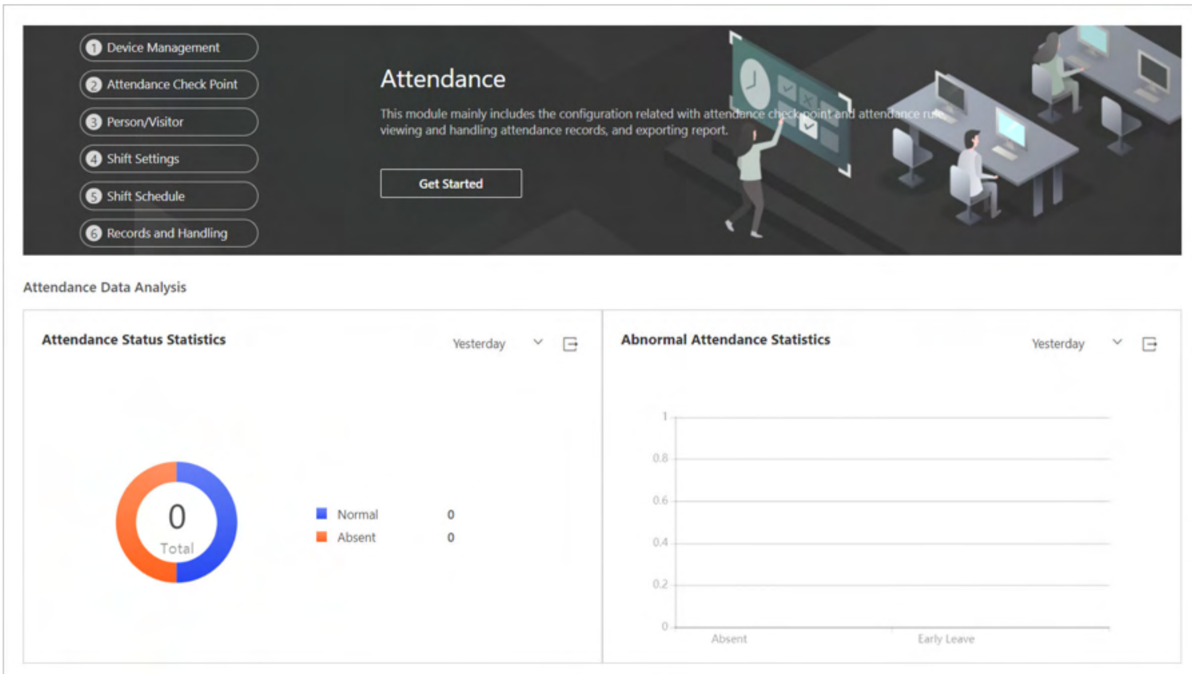



**Figure 18-1 Time & Attendance Overview**

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 **Getting 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*** .

## 18.1 Flow Chart

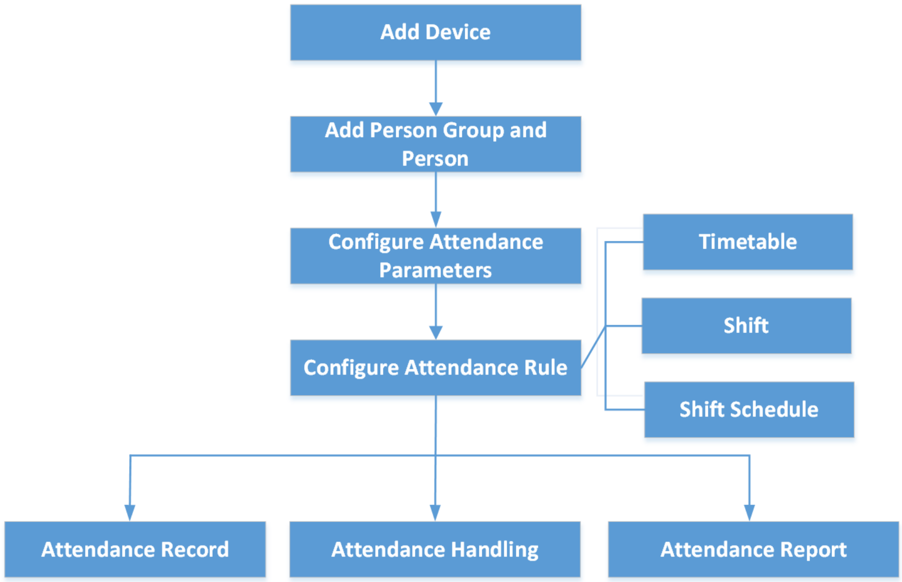



**Figure 18-2 Flow Chart for Time & Attendance**

- **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*** .

## 18.2 Configure Attendance Parameters

You can configure the attendance parameters, including the weekends, absence rule, overtime parameters, attendance check point, leave type, etc.

### 18.2.1 Add Attendance Check Point

You can set the doors, cameras which support facial recognition (such as DeepinView series camera, and the camera connected with DeepinMind series NVR), or terminals, so that the check-in/out by credentials (such as swiping card on the door'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.

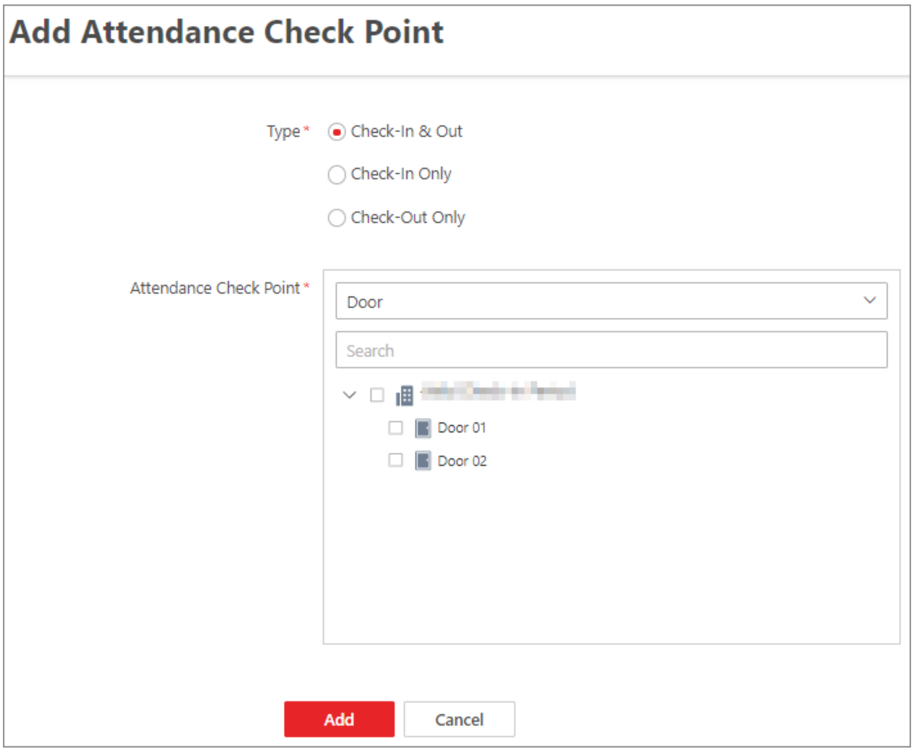



**Figure 18-3 Add Attendance Check Point**

All the resources which have not been set as attendance check point will be displayed.

6. Select the resources to be added.
7. Click **Add**.

   The selected resource(s) 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.

### 18.2.2 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.

### 18.2.3 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.

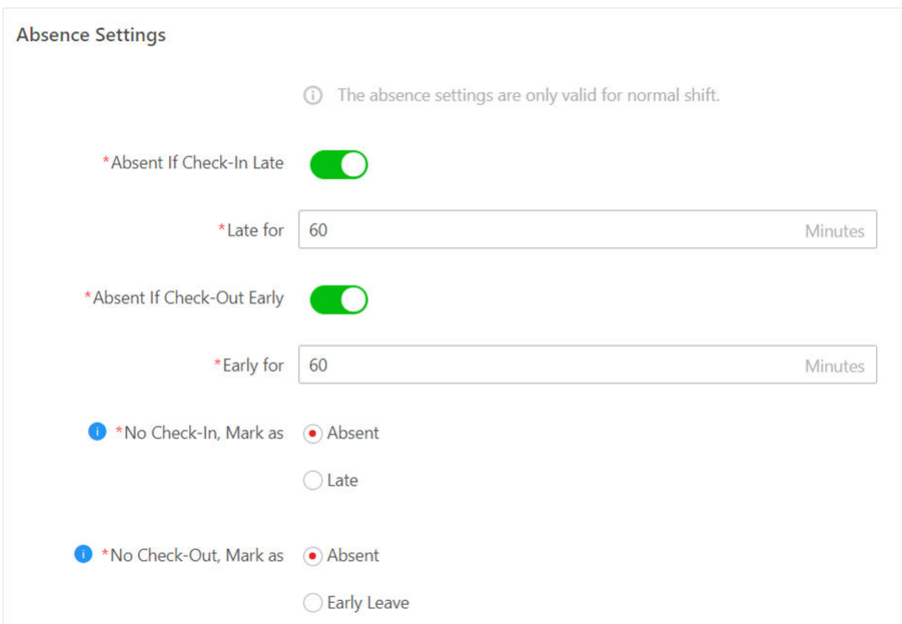



**Figure 18-4 Absence Settings**

### 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*** .

## 18.2.4 Configure Authentication Mode

You can configure authentication modes, including card 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.

### 18.2.5 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**.

### 18.2.6 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.

### 18.2.7 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, so the work hours will be calculated as 2 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.

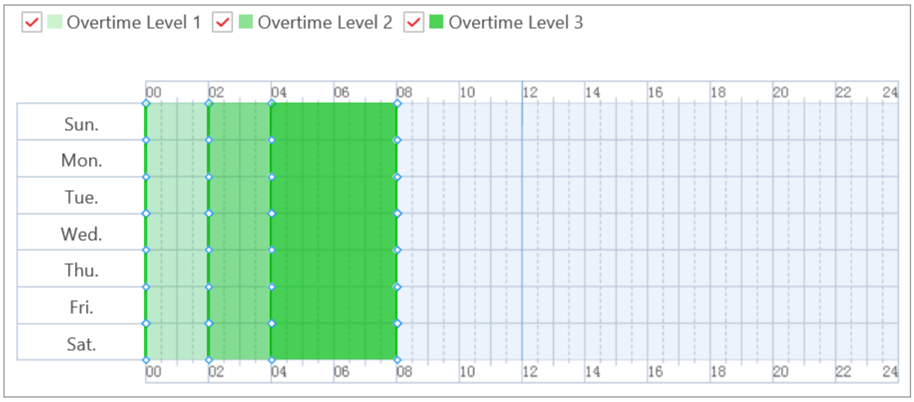



**Figure 18-5 Overtime Level Settings**

**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**.

## 18.2.8 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.

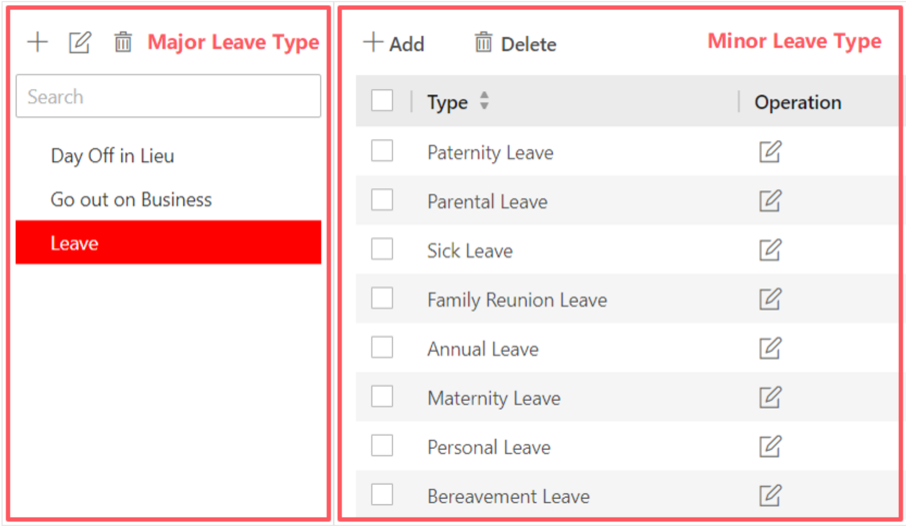



**Figure 18-6 Leave Type Management Page**

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 Single Person*** or ***Apply for Leave for Multiple Persons*** .

## 18.2.9 Customize T&A Status on Device

You can enable T&A Status on Device and customize the rule. After setting up T&A 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 T&A Status on Device** on the left.
3. Switch on **Enable T&A Status on Device** to set up the rule of T&A 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.

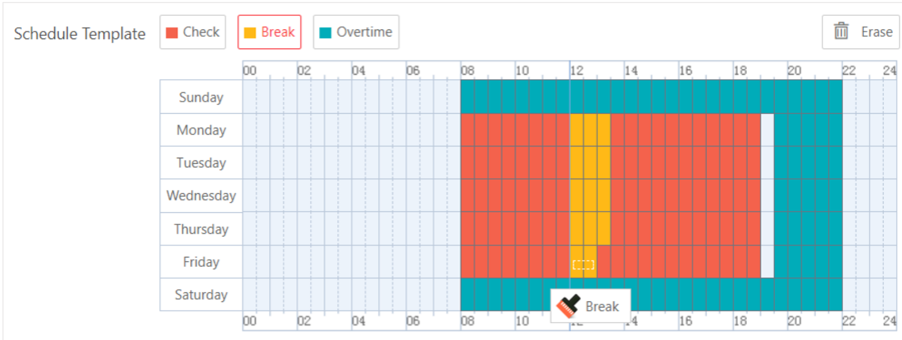



**Figure 18-7 Schedule Template**

**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.

## 18.3 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.

### 18.3.1 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.

**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.

**Mark Early Return As**

Choose to count the remaining time of a early return as overtime.

**Mark Late Return As**

Choose to count the exceeded time of a late return as late, early leave, or absent.

**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 T&A 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*** .

## 18.3.2 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.

**Timetable 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 T&A 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, and the late allowable duration is 30 minutes, and the employee checks in at 09:15, 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 to 18:00, and the flexible duration is 30 minutes, and the employee checks in at 09:15, and checks out at 18:15, 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.

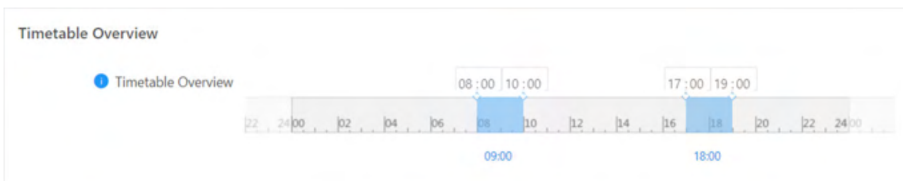



**Figure 18-8 Timetable Overview**

**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*** .

### 18.3.3 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.

**Timetable 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 T&A 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.

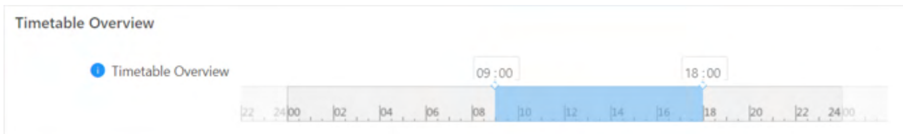



**Figure 18-9 Timetable Overview**

**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*** .

## 18.4 Add Shift

Shift is time arrangement for employment practice, which is designed to make use of all 24 hours of the clock each day, and usually assigned to employees to perform their duties according to the rule. Based on the actual requirements, you can add shift and apply one or multiple timetables in one shift for employees, which requires them to check in and check out for each timetable.

**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 7/14 days based on the week. If you select 2-4 weeks, you need to set the start week.

**Day**

You can customize the number of days (1-31) in one period. You should set a start date of one period for reference which can define how the shift repeats.

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 the added timetable and click on the time bar to apply the timetable.

   **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.
9. Select a general calculation mode for the shift.

   **First In & Last Out**

   The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

   **Each Check-In/Out**

   Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid work hours. You need to set Min. Interval for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the period is not be calculated.
10. Set **Enable T&A Status on Device** switch to on to calculate according to attendance status on the device.

    **Note**

    The function should be supported by the device.
11. **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.
12. Select the holidays. On holidays, the shift will not be effective.

    **Note**

    For setting the holiday, refer to ***Set Holiday*** .
13. Click **Add** to finish adding the shift.

## 18.5 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.

### 18.5.1 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.

### 18.5.2 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 Shift Schedule 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**.

### 18.5.3 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**

You should 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 Shift Schedule 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. Check the person(s) you want to assign the shift to.
5. Click **Set Shift Schedule** to enter setting person 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**.

### 18.5.4 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**.

## 18.6 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.

### 18.6.1 Search Attendance Record

You can search attendance records to view the person's attendance status by setting the search conditions such as attendance group, person name, status, and skin-surface temperature status.

**Before You Start**

Make sure the person information is not expired.

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance Records** on the left.
3. In the filter area, set the search conditions.

   **Time Period / Time**

   Set the time range of the attendance records you want to search. You can set one year's time range at most and search the persons' attendance records recorded within three years.

   **Name**

   Enter the person name to view the attendance records.

   **Person Group**

   Select the person group to view the attendance records.

   **Status**

   You can search the attendance records of certain status. For example, if you want to view the late arrival record, you can select **Late** to search.

   **Skin-Surface Temperature Status**

   You can search the attendance records by setting skin-surface temperature status, including All, Normal, Abnormal, and Unknown.

   **Select Additional Information**

You can search the attendance record by more custom condition(s). Click **Select Additional Information** to select the additional search condition(s).

**Note**

For more details about adding additional condition, refer to ***Customize Additional Information*** .

4. Click **Filter** to show all matched attendance records.
5. **Optional:** Perform further operations.

| | |
|---|---|
| **Sort Records** | Click ⇅ and select a sorting rule to sort the matched records in order. |
| **Select Display Items** | Click and select the items displayed in the search result. |
| **View Person's Attendance Records** | Click the person name to view the person's attendance records.<br>**Note**<br>Hover the cursor on the date to view the detailed work time, including scheduled work time and actual work time. |
| **Export Attendance Records** | Click **Export** to export the filtered attendance records and save in your PC.<br>**Note**<br>For more details, refer to ***Export Attendance Records*** . |
| **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 Attendance Record for Single Person*** / ***Correct Check-In/Out for Multiple Persons*** , ***Apply for Leave for Single Person*** / ***Apply for Leave for Multiple Persons*** , and ***View Attendance Handling Records*** . |

## 18.6.2 Correct Attendance Record for Single Person

After searching the person's attendance records, 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 Records** on the left.
3. Search the attendance records.

**Note**

For details, refer to ***Search Attendance Record*** .

4. If you set **Daily** as time period, perform one of the followings to enter the correcting check-in/out time page. If you select other time periods, you can only perform the second choice to enter the correcting check-in/out time page.
   - Click in the Operation column.
   - Click the name in the list of attendance records, hover the cursor over the date and click **Handle**.
5. Select **Correct Check-in/out**.
6. Set the correction type and time.
7. **Optional:** Enter the remarks, such as correction reason.
8. Click **Save**.

### 18.6.3 Correct Check-In/Out for Multiple Persons

You can correct multiple persons' check-in/out time in a batch 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 **Attendance Records** on the left.
3. Click **Batch Handle**.
4. Select **Correct Check-in/out**.
5. 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 corrected type and time.
   - Select Person(s): Select one or multiple persons in person group(s), and set corrected type and time.

     **Note**

     Up to 10,000 persons can be selected at a time.
   - 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 wrong information, and import the edited information again.
6. Click **Save**.

**Note**

The system will recalculate the attendance results according to the imported attendance records.

### 18.6.4 Apply for Leave for Single Person

After searching the person's attendance record, 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 Records** on the left.
3. Search the attendance records.

**Note**

For details, refer to ***Search Attendance Record*** .

4. If you set **Daily** as time period, perform one of the followings to enter the applying for leave page. If you select other time periods, you can only perform the second choice to enter the applying for leave page.
   - Click in the Operation column.
   - Click the name in the list of attendance records, hover the cursor over the date and click **Handle**.
5. Select **Apply for Leave**.
6. Set the leave type and time.
7. **Optional:** Enter the remarks, such as leave reason.
8. Click **Save**.

### 18.6.5 Apply for Leave for Multiple Persons

You can apply for leave for multiple persons when they want to 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 Records** on the left.
3. Click **Batch Handle**.
4. Select **Apply for Leave**.
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 records. You need to set leave type and time.
   - Select Person(s): Select one or multiple persons in person group(s), and set leave type and time.

**Note**

Up to 10,000 persons can be selected at a time.

6. **Optional:** Enter some words as remark, such as leave reason.
7. Click **Save**.

**Note**

The system will recalculate the attendance results according to the imported attendance records.

### 18.6.6 Manually Calculate Attendance Results

If person group or shift schedule changes, abnormal attendance is handled, etc. you can calculate the attendance data manually according to the latest settings. After calculating, the original data will be replaced by new attendance data.

**Steps**

**Note**

HikCentral Professional can calculate the attendance data automatically at the fixed time (4 o'clock by default) every day. You can edit the time point in → **All Modules** → **Attendance** → **Attendance Settings** → **General Rule** .

1. In the top left corner of Home page, select → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance Records** on the left.
3. Click **Calculate Again** to open the calculation settings window.
4. Set the start time and end time as the **Time Period** for attendance data.
5. Select **All Persons** or **Specified Persons** for attendance calculation.
6. Click **OK**.

**Note**

It can only calculate the attendance data within three months.

### 18.6.7 Export Attendance Records

The attendance records can be exported in Excel, PDF, or CSV format and be saved in the local PC. You can select the items to display in the exported file.

**Before You Start**

Make sure the person information is not expired.

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **Attendance** → **Records and Handling** .
2. Click **Attendance 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 Record*** .

4. Click **Export** in the left top corner.
5. Select the format as the file format of the exported file.

**Note**

The exported file is in Excel, PDF, or CSV format. If the file is larger than 50 MB, the file will be compressed to a ZIP package.

6. Select the items to be exported.
7. **Optional:** Click ↑ or ↓ to adjust the display order in the exported file.
8. Click **Export** to export the attendance records and save in your PC.

## 18.6.8 Get Attendance Records from Device

Some causes (such as abnormal running status and offline devices) may lead to asynchronous attendance data between HikCentral Professional and the devices. You can use this function to get the latest attendance records from the devices.

In the top left corner of Home page, select → **All Modules** → **Attendance** → **Records and Handling** → **Attendance Records** .

Click **Get from Device** and select resource(s) to get attendance data from the device(s).

## 18.6.9 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, cancel the handling operation or export the record 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 Record: Click and set conditions (e.g., Name, ID, Time, etc.) to filter the handling records.
- Undo Handing 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 Record: Click **Export** to save the handling records in CSV or Excel format in the local PC.

## 18.7 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.

### 18.7.1 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.

### 18.7.2 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 Settings** .
2. Select **Set Regular 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 Target**, select the person group(s) and click > to include the persons in the person group(s) in this report.
6. 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 ***Customize Attendance Report*** .

7. Set the report frequency to **Daily**, **Weekly**, or **Monthly** and set the sending time in **Send At**.

   **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 detected 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 records 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 records of the last 7 days or last month before 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 records detected between the Monday and Sunday of the last week.

**Note**

- Daily or weekly report is not available when you set report type to Monthly Overview, Monthly OT Overview, or Monthly OT Overview.
- To ensure the accuracy of the report time, 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*** .

8. 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*** .

9. Select **CSV**, **Excel**, or **PDF** as the format.

**Note**

You can select **TXT** as the format if the report type is **Access Records**.

10. Select a report language.
11. Click **Add** to add the report schedule.

    The report will be generated and sent to the recipient at the specified sending time.

### 18.7.3 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. Click and select the 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 Report (Monthly Overview, Monthly OT Details, or Monthly OT Overview)** | • **By Calendar Month**: Select a calendar month as the report time range.<br>• **Custom Time Period**: Report time range is 30 days from the start date you specify. |
| **Other Report Type** | 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.

## 18.7.4 Customize Attendance Report

You can create a customized attendance report based on the predefined report type in the platform. After creating a custom report, you can export the report manually or set a schedule to send the custom report to your email regularly.

**Steps**

1. Select → **All Modules** → **Attendance** → **Export Report** .
2. Select **Custom Report** on the left.
3. Click **Add**.
4. Create a descriptive name for the report in the **Report Name** field.
5. 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.

6. In the **Report Field** area, select the data items (table headers of the report) to be included in the report.

**Note**

You can click ↑ or ↓ on the Operation column to adjust the order of the table header.

7. Select a sorting rule for records from the **Table Display Rule** drop-down list.
8. Click **Add** to save the custom report, or click **Add and Continue** to add another one.
9. **Optional:** Perform further operations.

| | |
|---|---|
| **Edit Custom Report** | Click on report name to edit it. |
| **Delete Custom Report** | Select the report(s) and click **Delete** to delete the selected report(s). |
| **Export Custom Report** | Click and specify the target persons, time range, and report format to export the report to the PC. |

| | |
|---|---|
| **Send Custom Report Regularly** | You can set a schedule to send the custom report regularly. See details in ***Send Attendance Report Regularly*** . |

# Chapter 19 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.

## 19.1 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 Home page, select → **All Modules** → **Intelligent Analysis** → **Analysis Report** .
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 expanded 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**.

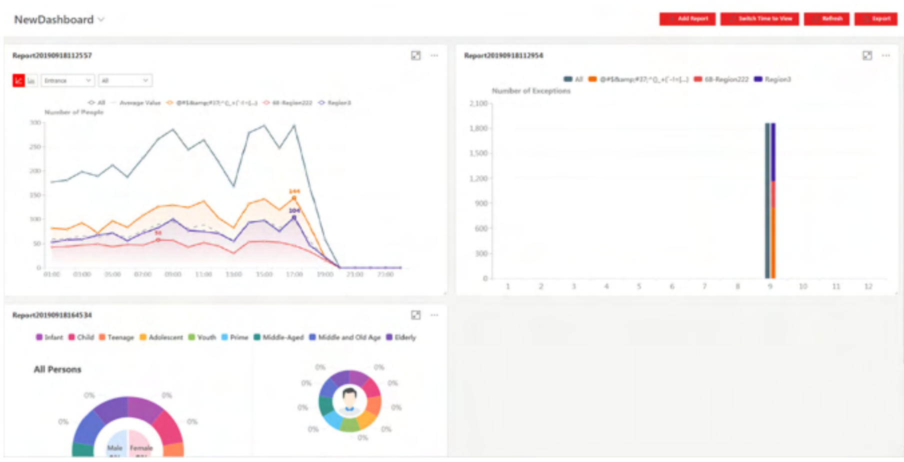


**Figure 19-1 Report Dashboard**

**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** or **CSV** as the format of the exported report(s).
4) Click **Export**.

## 19.2 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*** .

## 19.2.1 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. 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".

4. Create a name for the group.
5. Select a site.
6. 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.
7. 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.

8. **Optional:** Set the **Regularly Clear All** switch to ON and set a time for clearing all data regularly.
9. **Optional:** Switch on the **Maximum Capacity** and enter the maximum number of persons that can enter the area monitored by this group.
10. Click **Add**.

The people counting group is added in the table and you can view the resources in the group.

11. **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 19-2 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.

## 19.2.2 Generate People Counting Report

You can manually generate a 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 statistics type as **Entry & Exit**.
3. 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.

4. 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.

     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.
5. 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.
6. 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.

7. Click **Generate Report**.

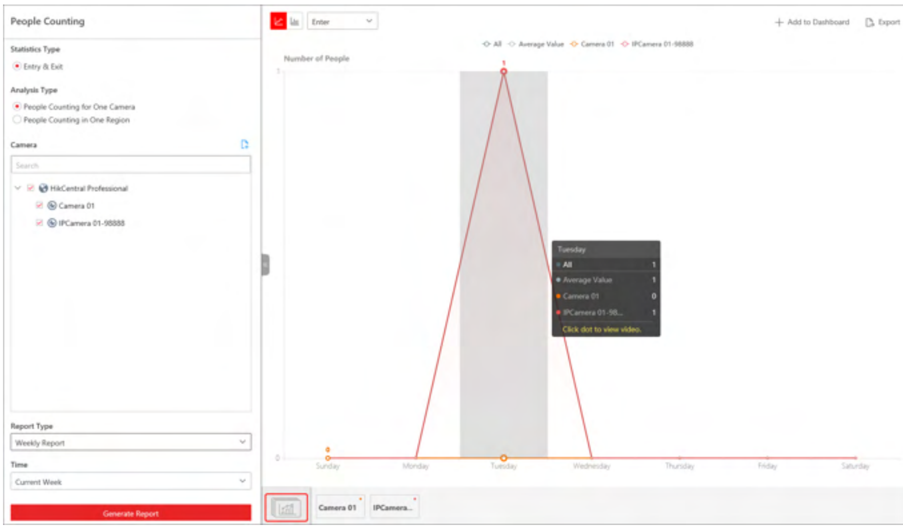



**Figure 19-3 People Counting Report (Entry & Exit)**

The statistics of all the selected item(s) are displayed in the right panel.

8. **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.<br>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). |

9. **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 or CSV.
5) Click **Export**.

### 19.2.3 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, etc. 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 sending time according to the report type.
11. 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. Select the **Report Language**.
13. Click **Add**.

## 19.3 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.

### 19.3.1 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 Home page, 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**

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**.

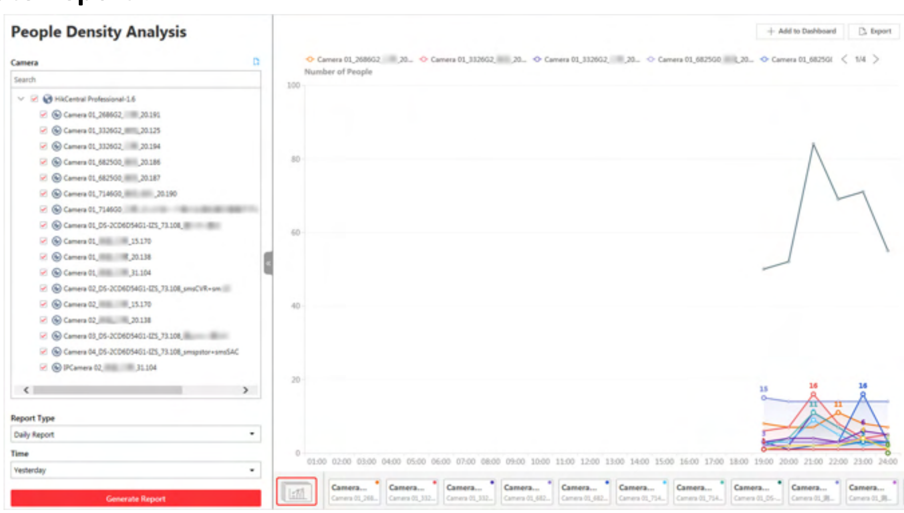



**Figure 19-4 People Density Analysis Report**

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.<br>b. Create a report name. |

| | |
|---|---|
| | c. Select a dashboard. Or click **New** to create a new board and then select it.<br>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.<br>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.<br>**Note**<br>Viewing linked videos is not supported by annual report. |
| **View Detailed Data in Each Minute** | **Note**<br>Viewing detailed data in each minute is only supported by daily report.<br>a. Generate a daily report.<br>b. Select a camera at the bottom of the line chart to display its statistics only.<br>c. Hover the cursor onto the line chart and then click **Details** on the pop-up floating window.<br>The line chart that shows statistics in each minute will be displayed.<br>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 19-5 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 or CSV.

5) Click **Export**.

### 19.3.2 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, etc. 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 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. After setting the report type, 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 sending time according to the report type.
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 ***Add Email Template for Sending Report Regularly*** .
10. Select the **Report Language**.
11. Click **Add**.

## 19.4 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.

### 19.4.1 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 Home page, 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 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. Optional:** 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**.

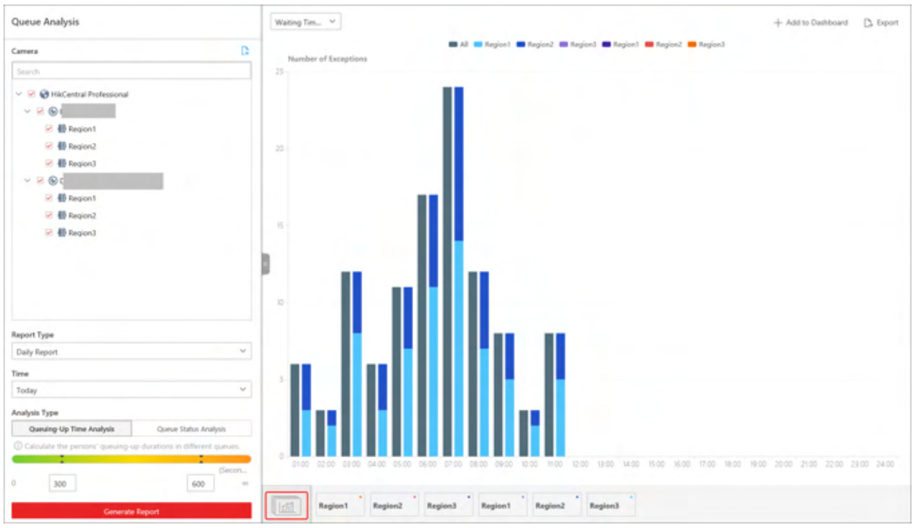



**Figure 19-6 Queue Analysis Report**

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.<br>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.<br>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.<br>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.<br>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 or CSV.
7) Click **Export**.

### 19.4.2 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, etc. 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 sending time according to the report type.
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 ***Add Email Template for Sending Report Regularly***

10. Select the **Report Language**.
11. Click **Add**.

## 19.5 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*** .

### 19.5.1 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.

## 19.5.2 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 Home page, 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 heat analysis camera or heat analysis group will be displayed here.

2) Check the heat analysis camera(s) or heat analysis group(s) for statistics.

**4.** Select camera(s) for the report in the camera list.

**Note**

Up to 20 heat analysis cameras can be selected for statistics at the same time.

**5.** 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.

**6. 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.

**7.** 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.

**8.** Click **Generate Report**.

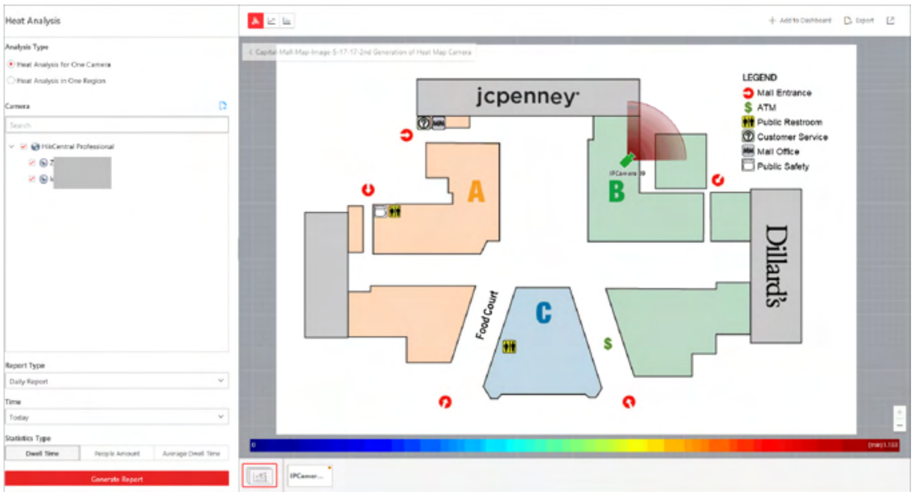



Figure 19-7 Static Map of Selected Cameras

The static maps of the selected cameras will appear.

9. 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.

10. **Optional:** Click the camera icon on the page below to view heat analysis of a camera.

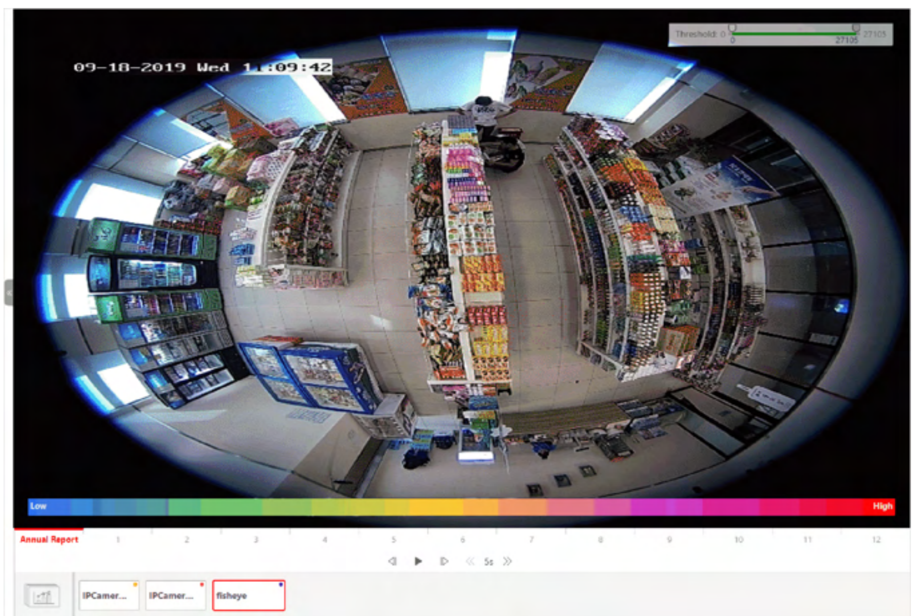



Figure 19-8 Heat Map of a Camera

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.

**11. Optional:** Click to switch among heat map, histogram, line chart to view the details.


**Figure 19-9 Line Chart of Heat Analysis**

**12. 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 or CSV.

5) Click **Export**.

### 19.5.3 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, etc. 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 sending time according to the report type.
11. 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. Select the **Report Language**.
13. Click **Add**.

## 19.6 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*** .

### 19.6.1 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.

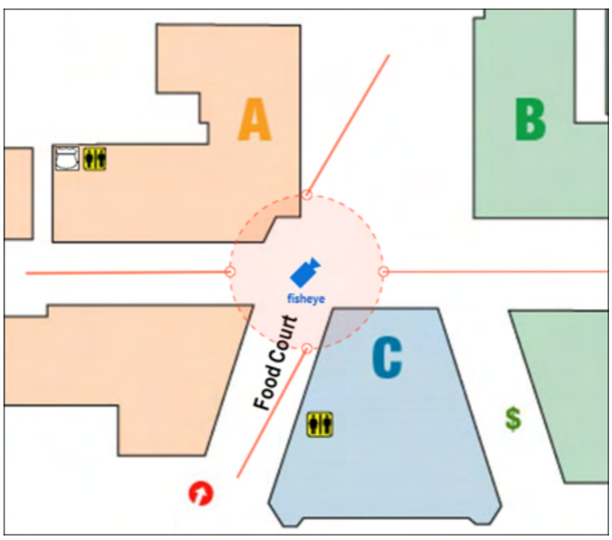



**Figure 19-10 Add Pathway Analysis Group**

   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.

### 19.6.2 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 Home page, 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**.

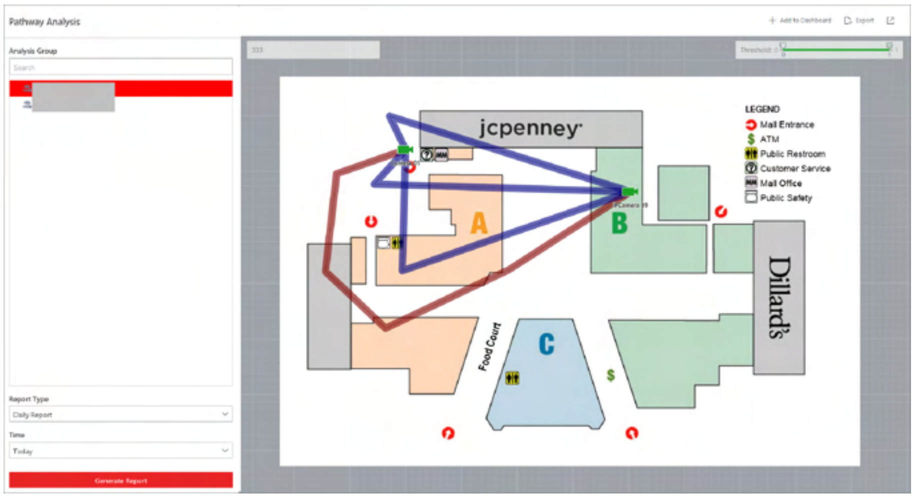



**Figure 19-11 Pathway Analysis Report**

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.

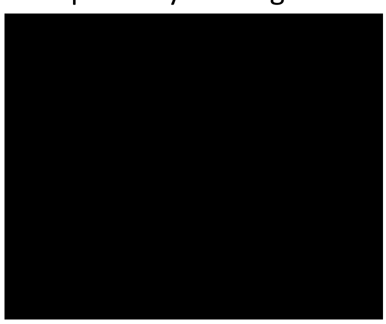


**Figure 19-12 View Heat Map or Line Chart**

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 or CSV.
5) Click **Export**.

### 19.6.3 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, etc. 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 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 **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. 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 analysis results on each day or each hour for one camera.

8. Set the sending time according to the report type.
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 ***Add Email Template for Sending Report Regularly*** .

---

10. Select the **Report Language**.
11. Click **Add**.

## 19.7 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*** .

### 19.7.1 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.

## 19.7.2 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 Home page, 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**

- 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**.

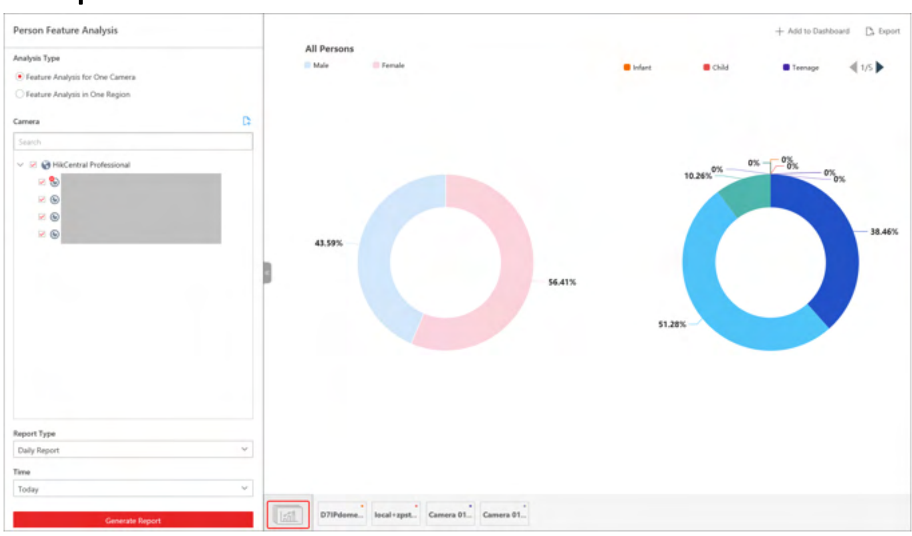



**Figure 19-13 Person Feature Analysis**

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 or CSV.
5) Click **Export**.

### 19.7.3 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, etc. 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. 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 percentage and number of people of different gender and age groups detected on each day or each hour for one camera.
9. Set the sending time according to the report type.
10. 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*** .
11. Select the **Report Language**.
12. Click **Add**.

## 19.8 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.

### 19.8.1 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 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**.

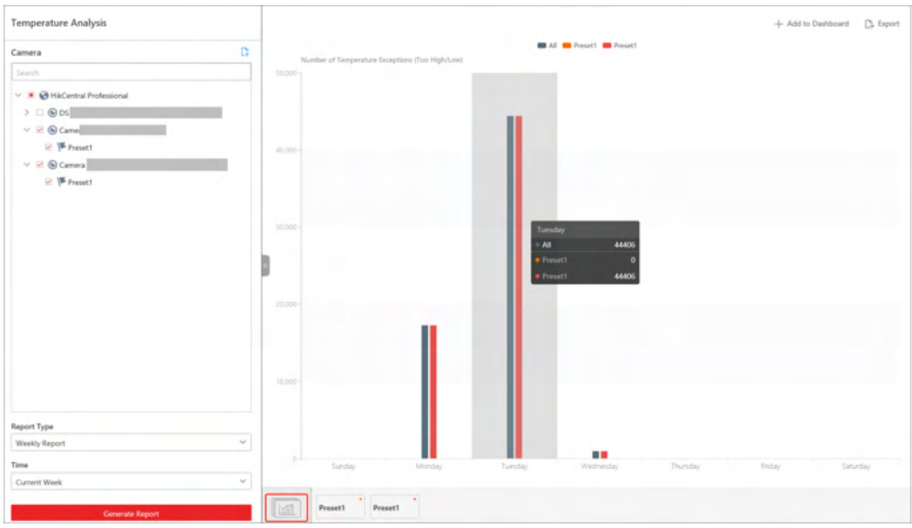



**Figure 19-14 Temperature Analysis Report**

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 or CSV.
   6) Click **Export**.

## 19.8.2 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, etc. 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. After setting the report time, 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. 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*** .

10. Select the **Report Language**.
11. Click **Add**.

## 19.9 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.

### 19.9.1 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 Home page, select → **All Modules → Intelligent Analysis → Analysis Report → Vehicle Analysis** .
2. 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 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.
3. 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.

**4.** 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.

---

**5.** Click **Generate Report**.

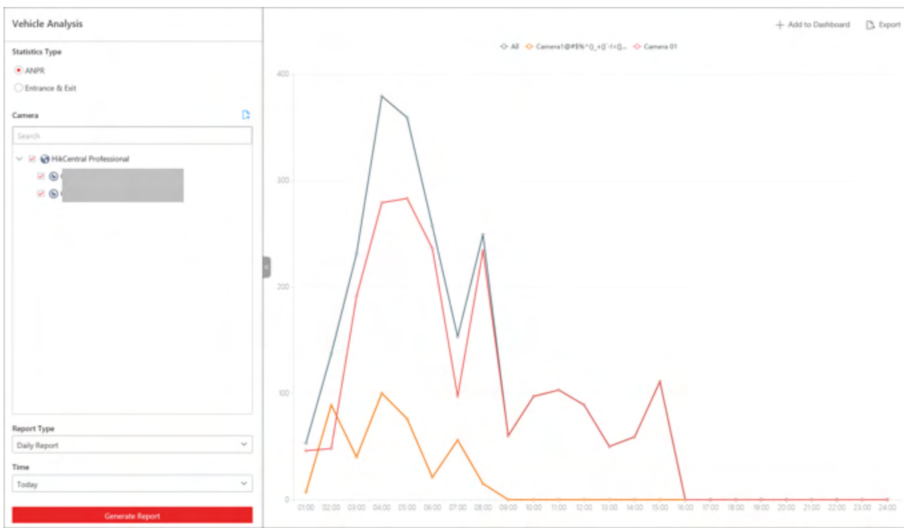



**Figure 19-15 Vehicle Analysis Report**

The passing vehicles statistics detected by all the selected cameras are displayed in the right panel.

**6. 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 or CSV.
5) Click **Export**.

## 19.9.2 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, etc. 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. After setting the report time, 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. 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*** .
9. Select the **Report Language**.
10. Click **Add**.

## 19.10 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.

### 19.10.1 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) 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.
     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**.

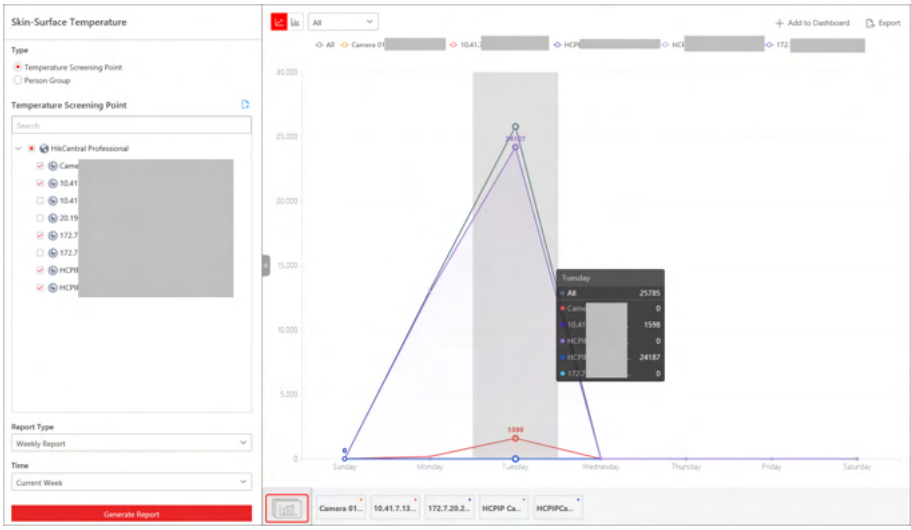



**Figure 19-16 Skin-Surface Temperature Analysis Report**

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 or CSV.
5) Click **Export**.

### 19.10.2 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, etc. 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 sending time according to the report type.
10. 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*** .

11. Select the **Report Language**.
12. Click **Add**.

# Chapter 20 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.

## 20.1 Flow Chart

For the first time, you can follow the flow chart below.

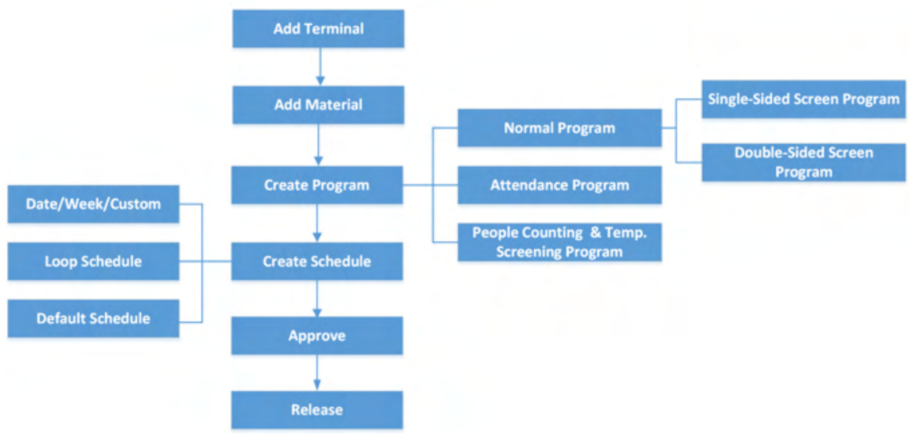



**Figure 20-1 Flow Chart**

- **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 normal program (including single-sided screen program and double-sided screen program), attendance program, and people counting & temperature screening 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*** .

## 20.2 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 creating dynamic materials in the platform. After uploading the materials, you can mange them including editing, searching, replacing, etc.

### 20.2.1 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** → **Digital Signage Management** .
2. Click **Upload Local Material** and select one or more materials to be uploaded from the local PC.

**Table 20-1 Supported Material Types and Formats**

| Material Types | Formats |
| --- | --- |
| Picture | BMP, JPG, PNG, GIF<br>**Note**<br>The largest resolution for a picture material is 3840 × 2160. |
| 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 |

**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**.

Uploading of the selected local materials will start automatically. 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 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.<br>**Note**<br>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.<br>• Fuzzy Search: Enter a keyword on the upper right corner of the page, and click to quickly find the target materials.<br>• Accurate Search: Click , and filter the added materials according to the uploaded time, material type, check status, and property.<br>• Status Search: 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. |

### 20.2.2 Upload Dynamic Material

You can upload dynamic materials used for creating programs to the platform. The material types supported to be uploaded 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** → **Digital Signage Management** .
2. Click **Upload 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**

   The material can be seen and used by all users in the platform.

   **Private**

   The material can be seen and used by all users in the organization where the user who creates the material belongs to.

   **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.<br>**Note**<br>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.<br>• Fuzzy Search: Enter a keyword on the upper right corner of the page, and click to quickly find the target materials.<br>• Accurate Search: Click , and filter the added materials according to the uploaded time, material type, check status, and property.<br>• Status Search: 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. |

## 20.3 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 normal program, attendance program, and people counting & temperature screening 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, cutting in, and adding to favorites.

### 20.3.1 Create Normal Program

You can create normal programs in the platform. The platform provides multiple program templates for different application scenarios such as chain retail and financial bank. You can select a program template according to the actual scene and edit the predefined template with the added materials as needed. After creating the program, you can preview the program, cut in the program, etc.

According to the different screen types of the terminals, the platform supports creating two types of normal programs, including single-sided screen program and double-sided screen program.

#### Create Single-Sided Screen Program

For the terminal with single-sided screen, you should configure a single-sided program in the platform. This 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 → Digital Signage Management → Programs → Normal** .
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 Type**

   Select **Single-Sided Screen** from the drop-down list.

   **Screen Size**

   Select the screen size as Landscape Mode, Portrait Mode, or Custom.

   **Sharing Property**

   **Public**

   The program can be seen and used by all users on the platform.

   **Private**

   The program can be seen and used by all users in the organization where the user who creates the material belongs to.

   **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** tab in the lower-left corner to select the template that have been added to Favorites.

**6.** Click **OK**.

**7.** Edit page properties, including page name, background, and play time.

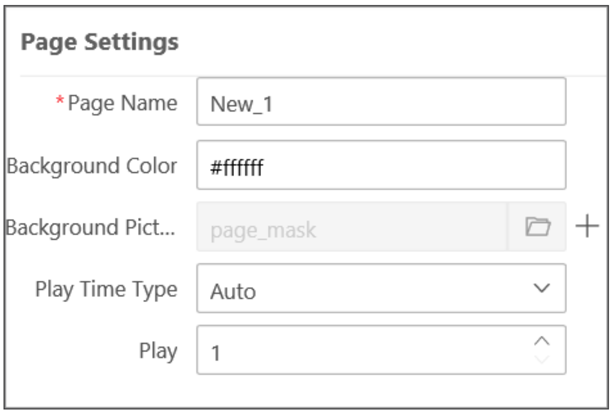



**Figure 20-2 Page Settings**

**8. Optional:** Add 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.

**9.** Select a material from the left list and drag it to the corresponding window in the template to add the selected material.

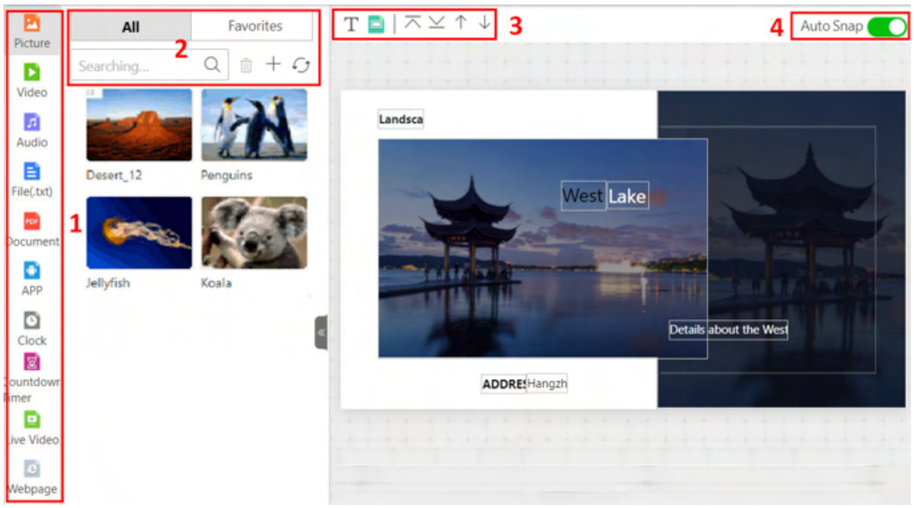



**Figure 20-3 Add Materials**

**Table 20-2 Page Description**

| Number | Description |
|---|---|
| 1 | There are 10 types of windows. Audio window cannot be added with video window or live video window at the same time. Up to 16 windows can be added for single page. |
| 2 | You can select materials from **All** or **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 move the window layer up/down/stick on top/stick at bottom. |
| 4 | You can enable **Auto Snap**, and two windows will be connected when they are near enough. |

**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 window jump link and page jump link for such 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 move the window layer up/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 view the current program on the terminal. |
| **Cut-In** | Click **Cut-in** to cut in the current program.<br>**Note**<br>For details, refer to ***Cut in Program*** . |
| **Create Schedule** | Click **Next** to enter the managing schedules page and create a schedule for the program.<br>**Note**<br>For details, refer to ***Schedule Management*** . |

**12.** Click **Save** to save the current program.

**13. Optional:** In 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. |
| **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.<br>**Note**<br>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:<br>• 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.<br>• Enter a keyword in the search field on the upper right corner, and click to quickly search for the target programs.<br>• Click , and filter programs by conditions such as uploading date, check status, sharing property and resolution. |
| **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. |

## Create Double-Sided Screen Program

For the terminal with double-sided screens (i.e., main screen and auxiliary screen), you should configure a main screen program and an auxiliary screen program respectively in the platform. This is called double-sided screen program, which can be used in places such as airport lobby to display flight information, so that passengers of different directions in the airport can view the information they need.

**Before You Start**

You have added materials to the platform and the materials have been approved. For details, refer to ***Material Management*** and ***Approve*** .

To create a double-sided screen program, you should configure a main screen program and an auxiliary screen program respectively. The method of configuring these two programs is the same. The following shows the steps of configuring the main screen program first and then the auxiliary screen program.

**Steps**

1. In the top left corner of Home page, select → **All Modules → Digital Signage → Digital Signage Management → Programs → Normal** .
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 Type**

   Select **double-sided Screen** from the drop-down list.

   **Screen Size**

   It is **Portrait Mode** by default.

   **Sharing Property**

   **Public**

   The program can be seen and used by all users on the platform.

   **Private**

   The program can be seen and used by all users in the organization where the user who creates the material belongs to.

   **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. In the pop-up window, select the templates for main screen program and auxiliary screen program respectively.

**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** tab in the lower-left corner to select the template that have been added to Favorites.

6. Click **OK** to enter the editing program page.

**Note**

If you need to configure the auxiliary screen program first, click **Auxiliary Screen** on the lower side of the page.

7. Edit page properties, including page name, background, and play time.

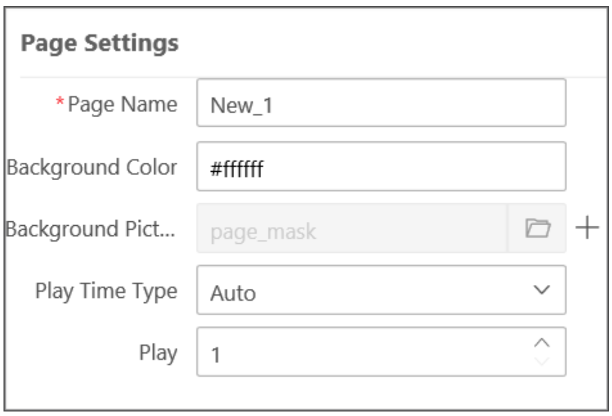



**Figure 20-4 Page Settings**

8. **Optional:** Add 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. |

9. Select a material from the left list and drag it to the corresponding window in the template to add the selected material.

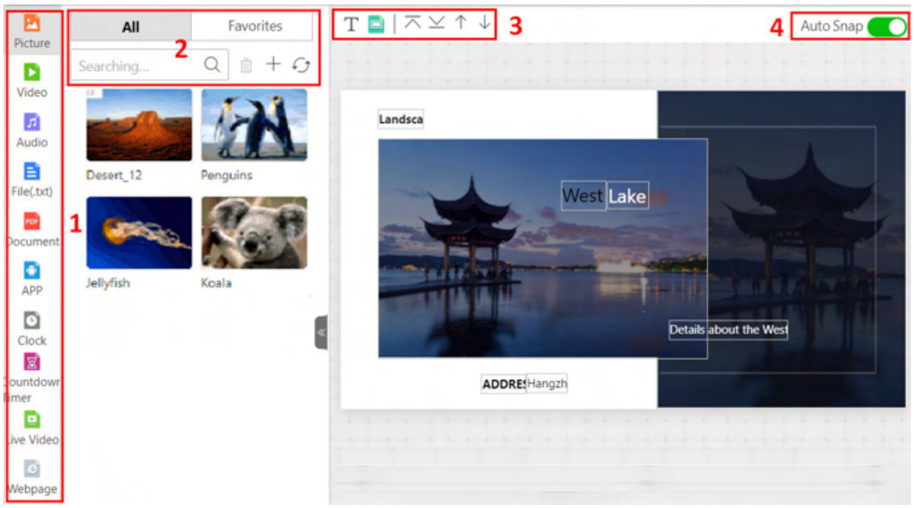



**Figure 20-5 Add Materials**

**Table 20-3 Page Description**

| Number | Description |
|---|---|
| 1 | There are 10 types of windows. Audio window cannot be added with video window or live video window at the same time. Up to 16 windows can be added for single page. |
| 2 | You can select materials from **All** or **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 move the window layer up/down/stick on top/stick at bottom. |
| 4 | You can enable **Auto Snap**, and two windows will be connected when they are near enough. |

**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 window jump link and page jump link for such 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 move the window layer up/down/stick on top/stick at bottom.

**Switching Effect**

Select the switching effect from the drop-down list for the current window. There are 8 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. Repeat the Step 5 to Step 11 to configure the auxiliary screen program.

**Note**

Having configured both main screen program and auxiliary screen program, you can click **Switch Program on Main/Auxiliary Screen** to switch the programs on the main screen and auxiliary screen.

12. **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 view the current program on the terminal. |
| **Cut-In** | Click **Cut-in** to cut in the current program.<br>**Note**<br>For details, refer to ***Cut in Program*** . |

| | |
|---|---|
| **Create Schedule** | Click **Next** to enter the managing schedules page and create a schedule for the program.<br><br>**Note**<br><br>For details, refer to ***Schedule Management*** . |

13. Click **Save** to save the current double-sided screen program.
14. **Optional:** In 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. |
| **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.<br><br>**Note**<br><br>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.<br><br>**Note**<br><br>By default, the page of the main screen program is enlarged and displayed. You can click to view the enlarged page of the auxiliary screen program. |
| **Filter Program** | You can filter programs via the following three methods:<br>• 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.<br>• Enter a keyword in the search field on the upper right corner, and click to quickly search for the target programs.<br>• Click , and filter programs by conditions such as uploading date, check status, sharing property and resolution. |
| **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. |

## 20.3.2 Create Attendance Program

You can create attendance programs in 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. Click **Digital Signage Management → Programs → Attendance** .
2. In the top left corner of Home page, select → **All Modules → Digital Signage → Digital Signage Management → Programs → Attendance** .
3. Click **Add**.
4. 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**

The program can be seen and used by all users in the platform.

**Private**

The program can be seen and used by all users in the organization where the user who creates the program belongs to.

**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.

5. Click **Next**.
6. 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** tab in the lower-left corner to select the template that have been added to Favorites.

7. Click **OK** to enter the creating program page.

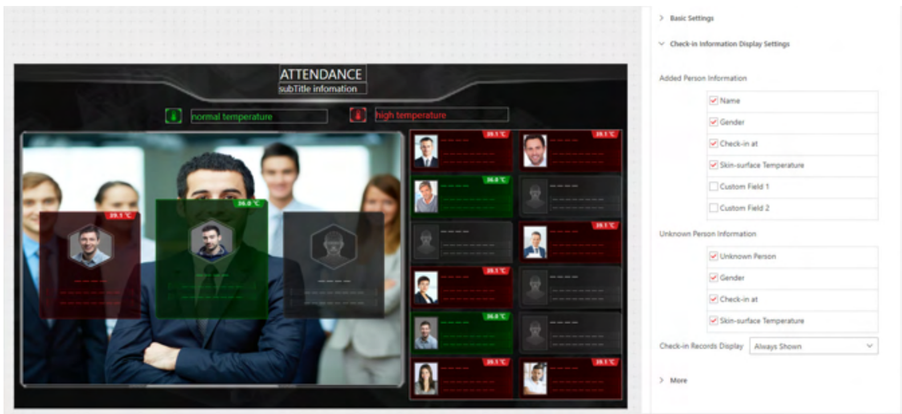



**Figure 20-6 Create Program**

**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.

**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 or videos) to the program, and configure switching effect and playing time for the advertisements.

**8. 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 view the current program on the terminal.

**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*** .

**9.** Click **Save** to save the current program.

**10. 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.

**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:<br>• 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.<br>• Enter a keyword in the search field on the upper right corner, and click to quickly search for the target programs.<br>• Click , and filter programs by conditions such as uploading date, check status, sharing property and resolution. |
| **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. |

### 20.3.3 Create People Counting & Temp. Screening Program

You can create people counting and temperature screening program in 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** → **Digital Signage Management** → **Programs** → **People Counting & Temp. Screening** .

**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**

The program can be seen and used by all users in the platform.

**Private**

The program can be seen and used by all users in the organization where the user who creates the material belongs to.

**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** tab in the lower-left corner to select the template that have been added to Favorites.

**6.** Click **OK** to enter the creating program page.

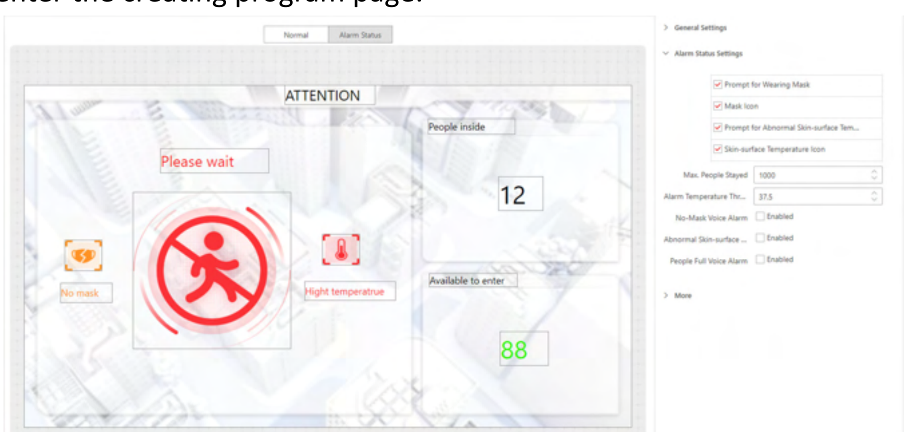



**Figure 20-7 Create Program**

**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. The configuration in this area will be applied to **Normal** and **Alarm Status** simultaneously.

You can enable audio prompt for the normal temperature.

**Alarm Status Settings**

You can check whether to display alarm status related information, such as prompt for abnormal temperature; set max. people stayed; enable voice alarm for no mask, abnormal temperature and people full, and configure corresponding audio file for them.

**Advertisement Settings**

You can add advertisements (pictures or videos) to the program, and configure switching effect and playing time for the advertisements.

**Note**

Only when selecting **Temperature Screening Template**, you can configure advertisement.

**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 view the current program on the terminal. |
| **Cut-In** | Click **Cut-in** to cut in the current program.<br>**Note**<br>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. |
| **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.<br>**Note**<br>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:<br>• 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.<br>• Enter a keyword in the search field on the upper right corner, and click to quickly search for the target programs.<br>• Click , and filter programs by conditions such as uploading date, check status, sharing property and resolution. |
| **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. |

## 20.4 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.

### 20.4.1 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**.
   - Select → **All Modules** → **Digital Signage Management** → **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.

   **Sharing Property**

   **Public**

   The schedule can be seen and used by all users in the platform.

   **Private**

   The schedule can be seen and used by all users in the organization where the user who creates the schedule belongs to.

   **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 a program from the program list.

**Note**

- You can click **All** or **Added to 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.
- You can select programs from the lists of normal programs, attendance programs, or people counting & temperature screening programs.

5. Move the cursor to the timeline on the right side, and drag the cursor on the timeline to specify the play time 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** | • Click to delete a single schedule.<br>• Check one or multiple schedules, and click **Delete** to delete the selected schedule(s). |
| **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.<br>**Note**<br>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. |

- Fuzzy Search: Enter a keyword on the upper right corner of the page, and click to quickly find the target schedules.
- Accurate Search: Click on the upper right corner of the page, and set the search conditions such as check status, sharing property, and play mode, to quickly filter the target schedules.
- Status Search: 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.

## 20.4.2 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 in the platform. For details, refer to ***Program Management*** .

**Steps**

**1.** Enter the Create Schedules page.
- After creating a program, click **Next**.
- Select → **All Modules** → **Digital Signage Management** → **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.

**Sharing Property**

**Public**

The schedule can be seen and used by all users in the platform.

**Private**

The schedule can be seen and used by all users in the organization where the user who creates the schedule belongs to.

**Area**

Set the area which the schedule belongs to.

**Description**

Enter the schedule description.

**3.** Select the play mode as **Loop**.

**4.** Select a program in the program list and drag the program to the playlist.

**Note**

- You can click **All** or **Added to 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.
- You can select programs from the lists of normal programs, attendance programs, or people counting & temperature screening 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** | • Click to delete a single schedule.<br>• Check one or multiple schedules, and click **Delete** to delete the selected schedule(s). |
| **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.<br><br>**Note**<br>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.<br>• Fuzzy Search: Enter a keyword on the upper right corner of the page, and click to quickly find the target schedules.<br>• Accurate Search: Click on the upper right corner of the page, and set the search conditions such as check status, sharing property, and play mode, to quickly filter the target schedules.<br>• Status Search: 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. |

### 20.4.3 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**.
- Select → **All Modules** → **Digital Signage Management** → **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.

**Sharing Property**

**Public**

The schedule can be seen and used by all users in the platform.

**Private**

The schedule can be seen and used by all users in the organization where the user who creates the schedule belongs to.

**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 **Added to 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.
- You can select programs from the lists of normal programs, attendance programs, or people counting & temperature screening 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** | • Click to delete a single schedule.<br>• Check one or multiple schedules, and click **Delete** to delete the selected schedule(s). |
| **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.<br>**Note**<br>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. |

- Fuzzy Search: Enter a keyword on the upper right corner of the page, and click to quickly find the target schedules.
- Accurate Search: Click on the upper right corner of the page, and set the search conditions such as check status, sharing property, and play mode, to quickly filter the target schedules.
- Status Search: 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.

## 20.5 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** → **Digital Signage Management** → **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 64 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.

## 20.6 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.

## 20.6.1 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.

In the top left corner of Home page, select → **All Modules → Digital Signage → Digital Signage Management → Release** .

You can view the 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.

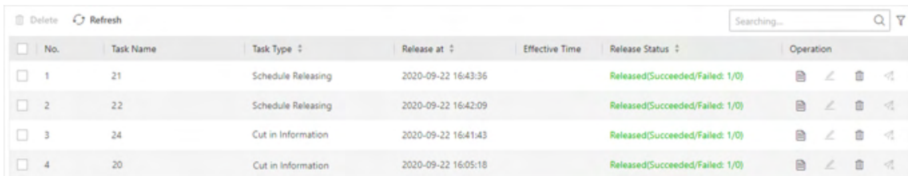



**Figure 20-8 View Release Records**

- **View Release Details:** Click to view release details of single task, including the terminal name, release progress, and current release 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.

## 20.6.2 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, refer to ***Add Terminal*** .
- The program schedules to be released should have been approved. For details, refer to ***Approve*** .

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **Digital Signage** → **Digital Signage Management** .
2. Enter the releasing schedule page.
   - After creating the program, click **Next**. For details about creating programs, refer to ***Program Management*** .
   - Click **Manage Programs** , move the cursor to a program, click to enter the adding schedules page, and click **Release** on the upper right corner.
   - Click **Manage Schedules** to enter managing schedules page, and click .
3. Enter the task name.
4. Select the release mode as **Release Later** or **Release Now**.

**Note**

When selecting **Release Later**, you should set the release time, and the program schedule will be released at the configured time period.

5. Select the effective mode as **Take Effect Later** or **Take Effect Now**.

**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.

6. 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.

7. Click **OK** to confirm the above settings.

### 20.6.3 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** .
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.

### 20.6.4 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**

- You have added terminal(s) to the platform. For details, refer to ***Add Terminal*** .
- The cut-in program should have been approved. For details, refer to ***Approve*** .

**Steps**

1. In the top left corner of Home page, select → **All Modules** → **Digital Signage** → **Device Control** .
2. Enter Cut in Program page.
   - Click **Manage Programs** , move the cursor to a program, and click .
   - After creating a program, click **Cut-in** on the upper right corner of the page.
3. Enter the task name.
4. Select the cut-in mode as **Play Duration(h/m/s)** or **End Time**.
5. Select one or more terminals for the cut-in program.

**Note**

You can enter a keyword in the search box to quickly find the target device(s).

6. Click **OK** to confirm the above operations.

## 20.7 Resource Overview

You can have an overall view about the resources added in the platform.

In the top left corner of Home page, select → **All Modules** → **Digital Signage** → **Digital Signage Overview** .

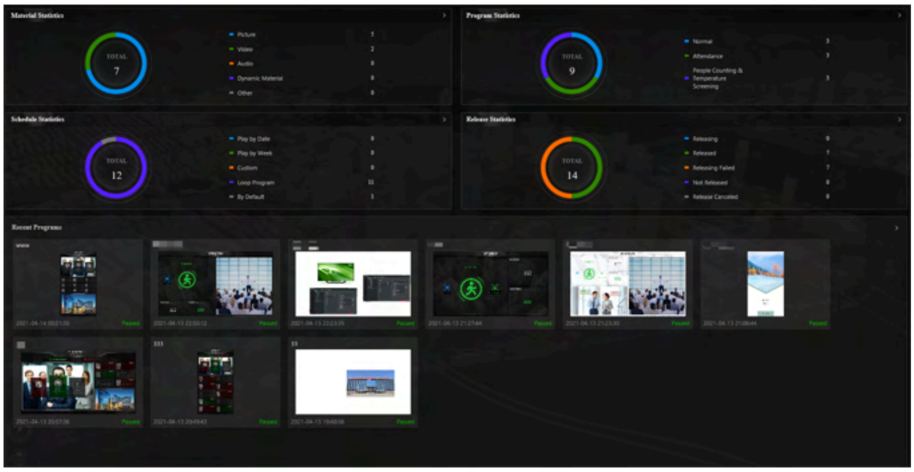


**Figure 20-9 Resource Overview**

- **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**: Mainly displays different releasing status such as Releasing, Released and Releasing Failed, and their corresponding number and proportion.
- **Recent Programs**: Displays the recently played programs. Supports editing, deleting and releasing these programs.

**Note**

Up to 15 latest programs can be displayed.

## 20.8 Control Terminal

After adding terminals (called devices in the following page) to the platform, you can control the terminals on the platform, such as start up/shut down/reboot, play/stop programs, customize cut-in message, volume settings and export report, etc.

In the top left corner of Home page, select → **All Modules** → **Digital Signage** → **Device Control** .

Perform the following operations according to you requirements:

**Switch Thumbnail/List**: Click / to display the added devices by thumbnail/list.

**Refresh Device Status**: Click **Refresh** to get the latest status(online/offline) of the devices.

**View Device Details**: Click in the Operation column to view the details of the device, such as software version, system version, IP address, MAC address, CPU usage, HDD usage, etc.

**Search Devices**: Click to set the search conditions (such as network status, cut-in status, release status, playback status) and click **Search** to search the devices accorded with the conditions.

Select one or multiple devices, perform the following operations according to your requirements:

**Start UP/Shut Down/Reboot**

Remotely start up/shut down/reboot the terminal(s).

**Play/Stop**

Play/stop the programs or cut-in messages on the screen of the terminal(s).

**Cut-in Message**

Go to the Gut in Message page to custom the cut-in messages displayed in the screen of the terminal(s).

**Stop Cut-in/Stop Message**

Stop playing cut-in messages/Stop program messages.

**Clear Content on Terminal**

Clear all the contents to be played on the terminal(s), including programs, cut-in 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*** .

**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.

**Restore Default**

Restore the parameters of the terminal(s) to the default settings.

**Volume Settings**

Manually adjust the volume of the terminal(s).

**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.

## 20.9 Migrate Data

You can migrate data (of materials, programs, schedules, and devices) from platform of the previous version to platform of the current version (e.g., from V1.0.0 to V1.1.0).

You can perform the following operations to migrate data.

1. On the top left corner of Home page, select → **All Modules** → **Digital Signage** → **Basic Settings** → **Data Migration** .
2. Click **Migrate** to start migrating data. You can view the migration progress and failure details (if there is data that fails to be migrated).

After migration, you can click **Migration Records** to view the migration time and migration results.

## 20.10 Set Material Storage Location

The materials uploaded can be saved to the pStor server.

**Before You Start**

Make sure you have added pStor servers to the platform. For details, refer to ***Add pStor*** .

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

# Chapter 21 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.

## 21.1 Set Storage Location for Broadcast

You can set storage location (local PC or pStor) for the broadcasted audio and the uploaded media files.

**Steps**

1. In the top left corner of the Home page, select → **All Modules** → **Speaker Unit** → **Basic Settings** .
2. Select **Local Storage** or **Storage on pStor** as the storage location.

**Note**

To select pStor as the storage location, make sure you have added pStor to the platform. For details, refer to ***Add pStor*** .

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

## 21.2 Group Speaker Units

You can group multiple speaker units for convenient management. Take the school scenario for example, if there are 4 classes in grade one, then you can group all the speaker units of grade one 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 ones. |
| **Adjust Volume** | Check one or more speaker units, and click **Volume** to adjust the volume of the selected ones. |

## 21.3 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 MP4 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. |

## 21.4 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 speaker unit(s) for live broadcast.

   **Note**

   You should select the online speaker unit(s).

   - 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 Broadcast**.

**What to do next**

Speak to the PC microphone or play the audio file.

## 21.5 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 **Live Broadcast Recording** in → **All Modules** → **Speaker Unit** → **Basic Settings** .

**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.** Enter the keyword(s) of the broadcaster.
**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 receiver (i.e., speaker unit), the start time, and the file size.

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

| | |
|---|---|
| **Download** | Click  on the Operation column to download the broadcasted audio. |
| **View Receiver** | Click  to view the receiver. |

## 21.6 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.<br>**Note**<br>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.<br>• Click **Stop** to stop playing the audio. |
| **Apply** | • Click **Apply All** to apply all the tasks to the speaker units.<br>• Select the tasks to be applied, click **Apply All** to apply the selected tasks to the speaker units.<br>**Note**<br>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 22 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.

## 22.1 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**.

   **GPU Hardware Decoding**

   Enable or disable GPU hardware decoding.

   **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.

   **Match Detected Metal with Face(s) Captured Within (sec)**

   This parameter is for walk-through metal detectors. When the metal 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 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.

## 22.2 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**.

## 22.3 View Videos of Security Inspection

After adding security inspection channels and linking security inspection devices to them, you can view the videos of live view and playback.

**Note**

Make sure you have added security inspection channels to the area. 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 channel, click **Live View** or **Playback** to view the videos of security inspection.

**Note**

To configure the network transmission parameters to optimize the performance of live view and playback for the current Web Client, you can view ***Local Configuration*** for details.

## 22.4 Historical Data Search

You can search for the historical data of security inspection, including package detection records, metal detection records, and inspector absence records.

### 22.4.1 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** .

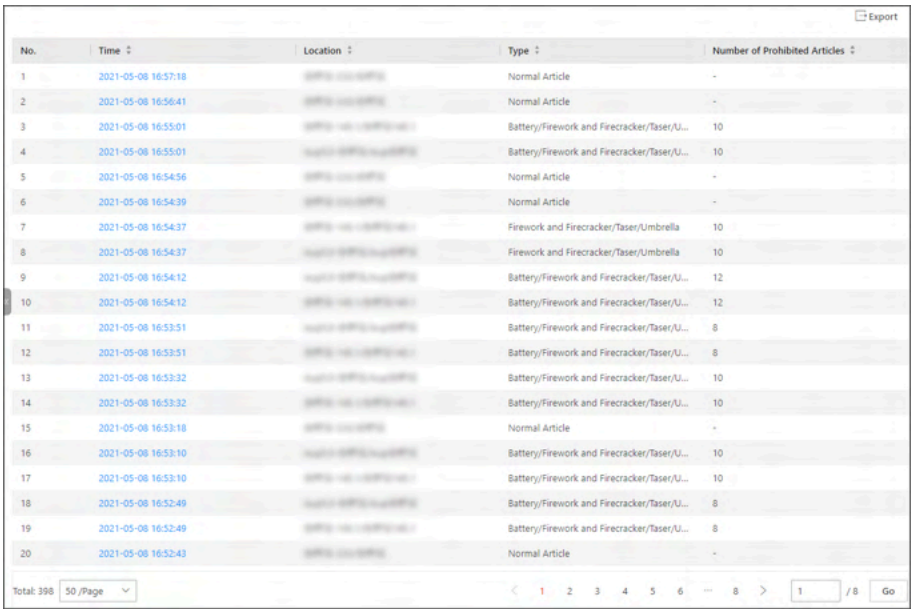
**2.** Select a period of time from the drop-down list.

**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.



Export

| No. | Time | Location | Type | Number of Prohibited Articles |
|---|---|---|---|---|
| 1 | 2021-05-08 16:57:18 | [illegible] | Normal Article | - |
| 2 | 2021-05-08 16:56:41 | [illegible] | Normal Article | - |
| 3 | 2021-05-08 16:55:01 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 4 | 2021-05-08 16:55:01 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 5 | 2021-05-08 16:54:56 | [illegible] | Normal Article | - |
| 6 | 2021-05-08 16:54:39 | [illegible] | Normal Article | - |
| 7 | 2021-05-08 16:54:37 | [illegible] | Firework and Firecracker/Taser/Umbrella | 10 |
| 8 | 2021-05-08 16:54:37 | [illegible] | Firework and Firecracker/Taser/Umbrella | 10 |
| 9 | 2021-05-08 16:54:12 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 12 |
| 10 | 2021-05-08 16:54:12 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 12 |
| 11 | 2021-05-08 16:53:51 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 8 |
| 12 | 2021-05-08 16:53:51 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 8 |
| 13 | 2021-05-08 16:53:32 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 14 | 2021-05-08 16:53:32 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 15 | 2021-05-08 16:53:18 | [illegible] | Normal Article | - |
| 16 | 2021-05-08 16:53:10 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 17 | 2021-05-08 16:53:10 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 10 |
| 18 | 2021-05-08 16:52:49 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 8 |
| 19 | 2021-05-08 16:52:49 | [illegible] | Battery/Firework and Firecracker/Taser/U... | 8 |
| 20 | 2021-05-08 16:52:43 | [illegible] | Normal Article | - |

Total: 398 50 /Page < 1 2 3 4 5 6 ··· 8 > 1 / 8 Go

**Figure 22-1 Search for Package Detection Records**

**6. Optional:** Click **Export** to export the records to the local PC.

### 22.4.2 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.

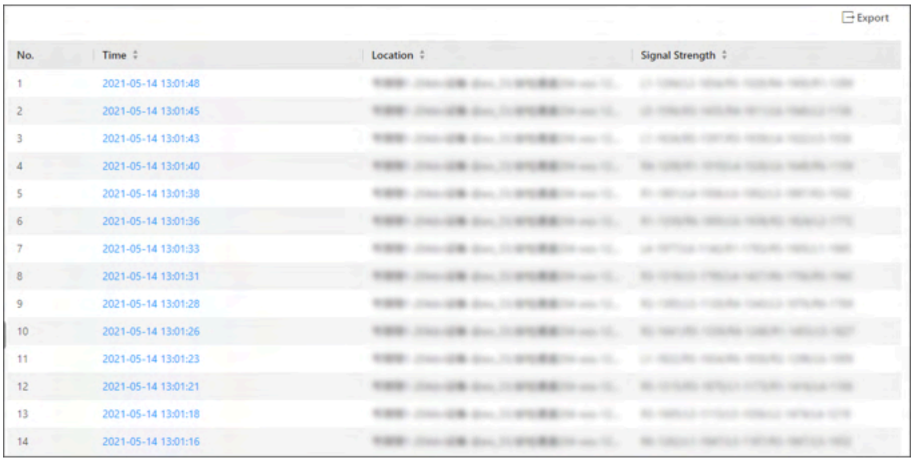



**Figure 22-2 Search for Metal Detection Records**

**5. Optional:** Click **Export** to export the records to the local PC.

### 22.4.3 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.


**Figure 22-3 Search for Absence Records**

**5. Optional:** Click **Export** to export the records to the local PC.

## 22.5 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.

## 22.6 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 23 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 defense 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 a defense schedule to these security control partitions. After that, the zones can be armed according to the schedules respectively.

## 23.1 Flow Chart

The following flow chart shows the process of the configurations and operations of alarm detection.

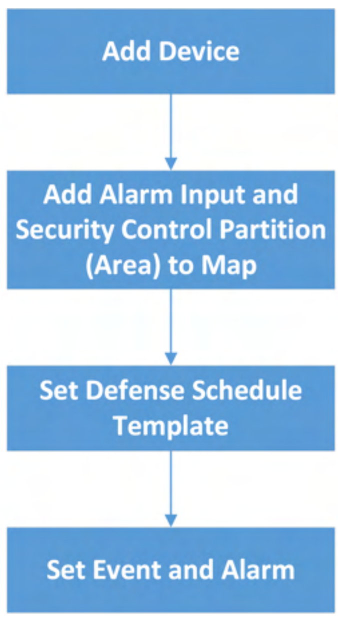



**Figure 23-1 Flow Chart of Alarm Detection**

- **Add Device**: Add security control device to detect persons, vehicles, or other emergency events in the detection region to trigger alarms, and then notifies security personnel of alarm information. And then, add alarm input and partition (area) to area 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 input and partition (area) on map to view their geographic locations, arm or disarm, bypass, and clear alarms. Refer to ***Add Hot Spot on Map*** for details.
- **Set Defense Schedule Template**: Set defense schedule template for a specified partition (area) to specify arming schedule and alarm linkage of alarm inputs in this partition (area). Refer to ***Configure Defense Schedule Template*** for details.
- **Event and Alarm**: Set event and alarm parameters and linkage actions to view event and alarm details on client or mobile client, timely remind the security personnel to handle, or search history events and alarms when some emergency situations occurred. Refer to ***Event and Alarm Configuration*** for details.

## 23.2 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. In the Security Control Partition (Area) field, click + .

   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 this area.

   **Note**

   After adding the alarm inputs to this 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:** Set a defense schedule for this partition, which defines how and when to arm the alarm inputs in the security control partition (area). See details in ***Configure Defense Schedule Template*** .
7. **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 defense schedule for it. |

| | |
|---|---|
| **Partition (Area)** | **Note**<br>For the partition (area) of AX security control panel, you cannot edit the defense schedule via the platform. Only editing on the device is supported. |
| **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.<br>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).<br>There are three arming modes available.<br>• **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.<br>• **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.<br>• **Instant Arming**: It is used after people leave the detection area. The zone will be armed immediately without delay.<br>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. |
| **Delete Security Control Partitions (Areas)** | Select one or multiple partitions (areas) and click **Delete**. |

## 23.3 Configure Defense Schedule Template

The defense 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 defense 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 → Defense Schedule Template** .
2. Click + to enter the Add Defense 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 defense schedule template will be displayed on the defense schedule template list.

# Chapter 24 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, and link person with indoor station. After settings related parameters, the person can view the live video of the camera, call indoor station, answer call via Control Client, etc.

## 24.1 Flow Chart

For the first time, you can follow the flow chart to perform configurations and operations.

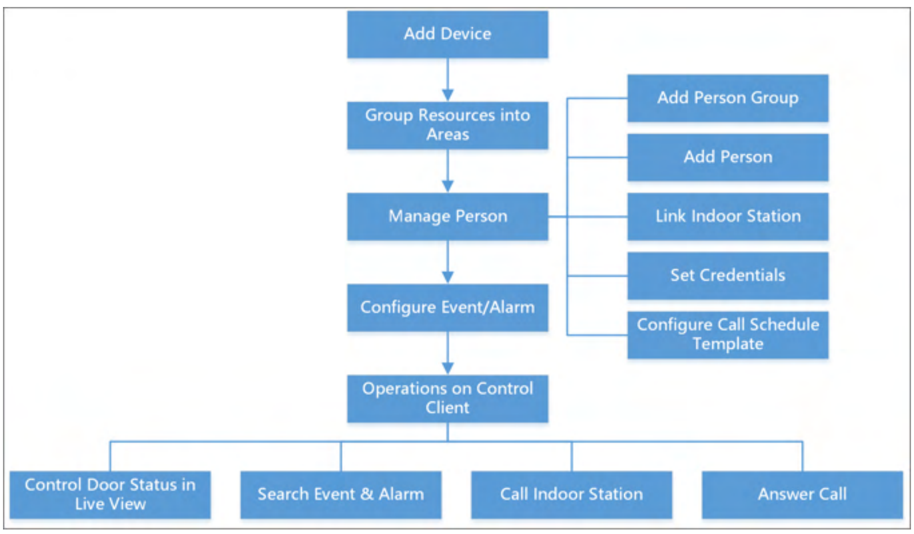



**Figure 24-1 Flow Chart of Video Intercom**

- **Add Device**: Add video intercom devices (such as master 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, link person with indoor station, set credential information, and configure call schedule template. For more detail, refer to ***Person Management*** .

- **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*** .

## 24.2 Relate Camera with 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 Indoor Station by IP Address*** .

Make sure the camera(s) to be related are correctly installed and are added to the system by Hikvision Private Protocol/ONVIF Protocol.

**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. Select an indoor station in the video intercom device list.
4. Click .

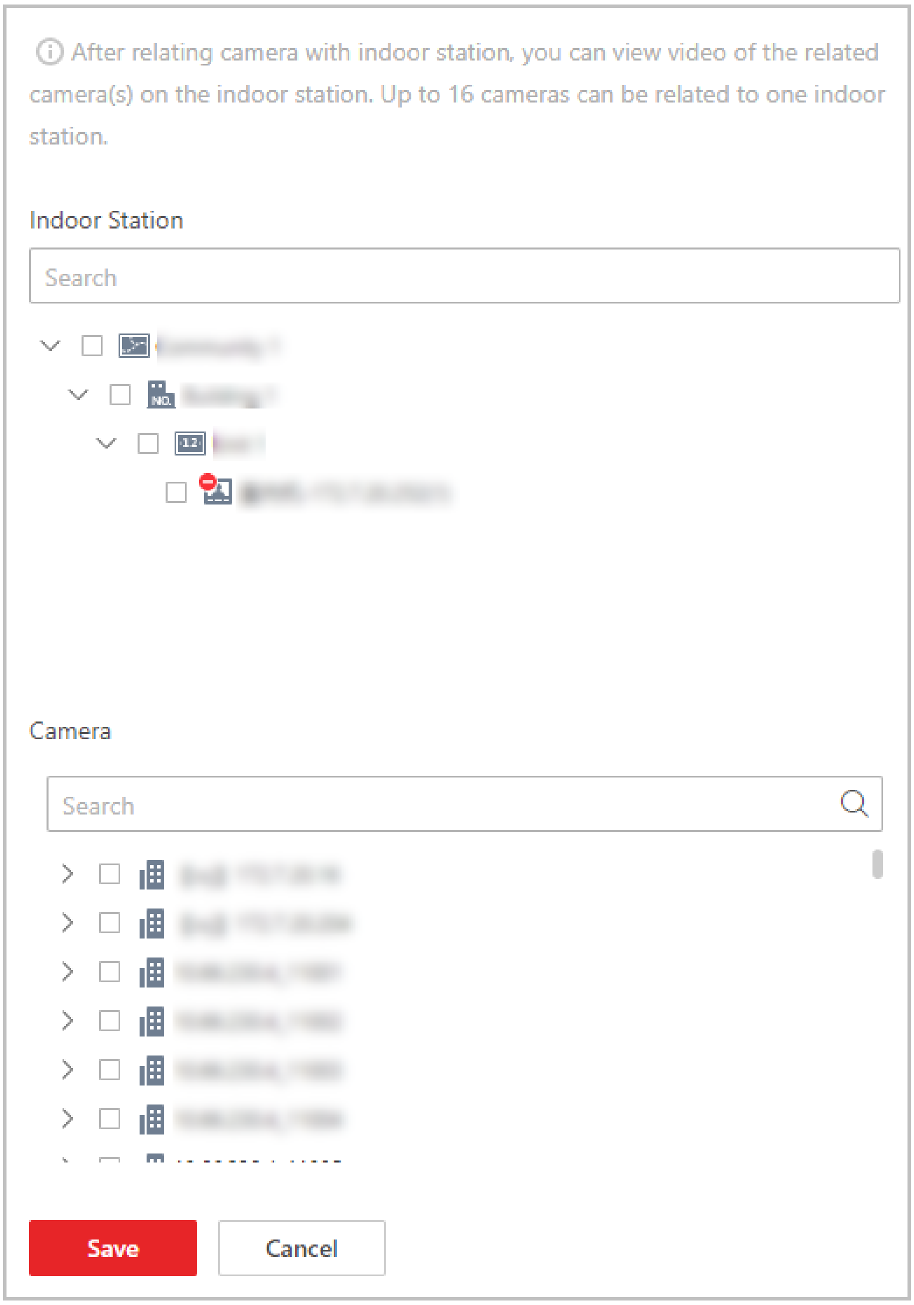



**Figure 24-2 Add Related Camera**

---

**Note**

You can also relate camera with indoor station in the configuration page of the indoor station. For details, refer to ***Configure Device Parameters*** .

---

**5.** In the Indoor Station list, check one or more indoor station(s).

**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.

6. In the Camera list, check one or more cameras.

**Note**

You can enter a keyword to search for the target camera(s). And the keyword of corresponding camera(s) will be displayed in red.

7. Click **Save**.

**Note**

You can also delete the related camera(s) in the configuration page of the indoor station.

## 24.3 Batch Link Persons with 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) conveniently.

**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** → **General** → **Person** .
2. Select person group on the left to filter the persons.
3. Select the person(s) for linking with indoor station.
4. Click .
5. Select desired indoor station on Indoor Station column for each person.

**Note**

Up to 10 persons can be linked with one indoor station and the person cannot be linked with multiple indoor stations.


**Figure 24-3 Batch Link Persons with Indoor Station(s)**

**6.** Click **Save**.

The linked person information will be applied to the indoor station(s).

## 24.4 Relate Doorbell with 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** → **General** → **Resource Management** .

**2.** Click **Device and Server** → **Video Intercom Device** on the left.

**3.** Click to enter Link Doorbell with Indoor Station.

The added doorbells are displayed in the list.

**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.

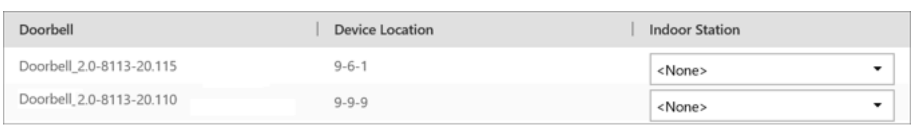



**Figure 24-4 Relate Doorbell with Indoor Station**

**5.** Click **Save**.

**Result**

The doorbell will be related with the selected indoor station.

## 24.5 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.

## 24.6 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.

### 24.6.1 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 call center during workdays and call the indoor station during weekends and holidays.

**Steps**

1. On the Home page, click → **All Modules → Access Control → Video Intercom Applications → Call Schedule Template** .
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 nor deleted.
3. Create a name for the template.
4. **Optional:** Select an existing template from the **Copy to** drop-down list.
5. Select **Indoor Station** or **Call Center**.

   **Note**

   Select **Indoor Station** if there is someone indoor who can answer the call from door station while select **Call 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 sations 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*** .

## 24.6.2 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. On the Home page, click → **All Modules** → **Access Control** → **Video Intercom Applications** → **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.<br>• 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*** .

## 24.6.3 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. On the Home page, click → **All Modules** → **Access Control** → **Video Intercom Applications** → **Door Station Call Schedule Settings** .
2. Click **Apply Settings** on top of the device list page.
3. Select **All Door Station(s)** 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.

# Chapter 25 Skin-Surface Temperature Screening

After adding the temperature screening cameras and access control devices with temperature screening function to the system, you can view the temperature of the detected persons in the Skin-Surface Temperature module. The system also shows whether the detected person is wearing a mask or not. With skin-surface temperature screening and mask detection functions, the system provides an alert if an individual is running a fever or not wearing a mask.

In the Skin-Surface Temperature module, you can view the real-time and history temperature screening records and face mask detection records. You can also generate a report about these records to view the overall information.

**Note**

The mask detection function will show when the mask related function is turned on in the **System → Normal → User Preference** page. For details, refer to ***Set User Preference*** .

## 25.1 Temperature Screening Configuration

Before temperature screening, you should set temperature screening point groups and add related temperature screening points to the added groups. Also, for the temperature screening points, you can configure their parameters including temperature screening threshold and alarm threshold.

### 25.1.1 Group Temperature Screening Points

You can group multiple temperature screening points for convenient management. For example, you can group all the temperature screening points on the same floor into a group.

**Steps**

1. 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 the delete icon to delete single temperature screening point.<br>• 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).<br>**Note**<br>For details, refer to ***Configure Temperature Screening Parameters*** . |
| **Export** | Click **Export** to export detailed information of temperature screening point(s) such as device type, serial No., and temperature screening threshold to the local PC. |

## 25.1.2 Configure Temperature Screening Parameters

For the added temperature screening point(s), you can configure the related parameters including temperature screening threshold and alarm threshold.

Check one or more added temperature screening point(s), and click **Configuration** to configure temperature screening parameters.

**Temperature Screening Threshold**

Set the threshold for temperature screening. When the detected skin-surface temperature is higher than the threshold, a temperature screening event will be triggered.

**Alarm Threshold**

Set the threshold for alarm. When the detected skin-surface temperature is higher than the threshold, an alarm will be triggered.

**Note**

- The temperature screening threshold should be smaller than alarm threshold.
- For temperature screening points which are access control points, you should configure their temperature screening parameters on the device parameters configuration page. For details, refer to ***Configure Other Parameters*** .

## 25.2 Real-Time Skin-Surface Temperature Monitoring

You can view the latest skin-surface temperature information detected by screening points. If there are persons whose skin-surface temperatures are abnormal, you will know at the first time. Besides, you will be able to quickly locate the persons according to the displayed screening point name and screening group. For unregistered persons, you can quickly register for them.

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 and the person wears no mask; green means the captured person's skin-surface temperature is normal and the person is wearing a mask. Click **More** to jump to the History page to view more captured pictures.

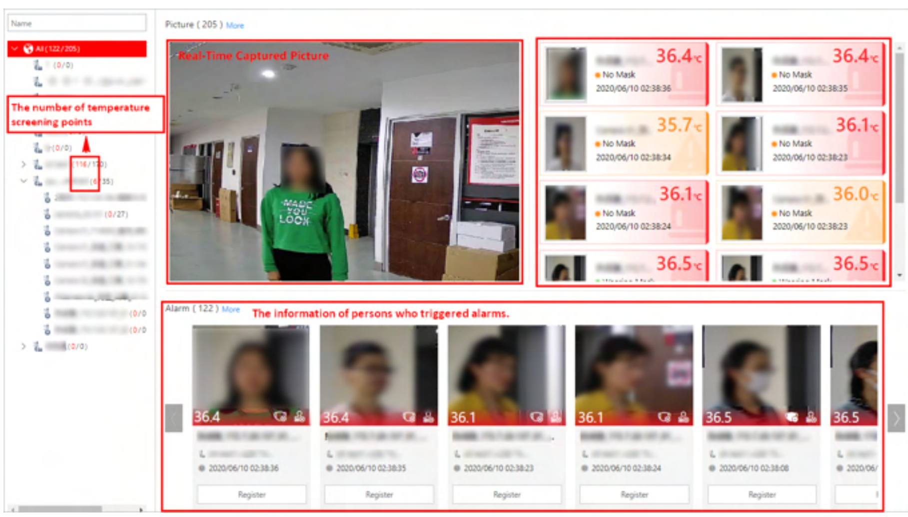



**Figure 25-1 Real-Time Skin-Surface Temperature**

When a person's skin-surface temperature exceeds the threshold you set, or the person is not wearing a mask, an alarm will be triggered. In the Alarm area, the pictures and information of persons who have triggered alarms are displayed. Following the title Alarm, the alarm amount is displayed. See *The User Manual of HikCentral Professional Web Client* for details about how to set a temperature threshold.

The person information includes skin-surface temperature, wearing mask or not, registered or unregistered, temperature screening point name, temperature screening point group name, and detecting time. You can click **Register** to register for the person, or click **More** to go to the History page to view more alarm information.

## 25.3 Search History Temperature Screening Data

You can set search conditions such as start time, end time, and skin-surface temperature to search for history temperature screening data.

**Before You Start**

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.<br>**Note**<br>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.<br>• : The person is registered. For the registered person, click **Edit** to edit the person information.<br>• : The person is unregistered. For the unregistered person, click **Register** to enter person's registration information. For details, refer to ***Register Person Information*** . |
| **Export** | Click **Export** to export temperature screening data including temperature screening point, temperature screening point group, temperature status, etc., in excel file. |

## 25.4 Registration

To manage the people who have been screened skin-surface temperature conveniently, you can register for them by entering their personal information. After registration, you can view and filter the registered persons' information.

### 25.4.1 Register Person Information

For unregistered persons displayed on real-time skin-surface temperature page or history page of skin-surface temperature, you can register for them.

**Steps**

1. 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.

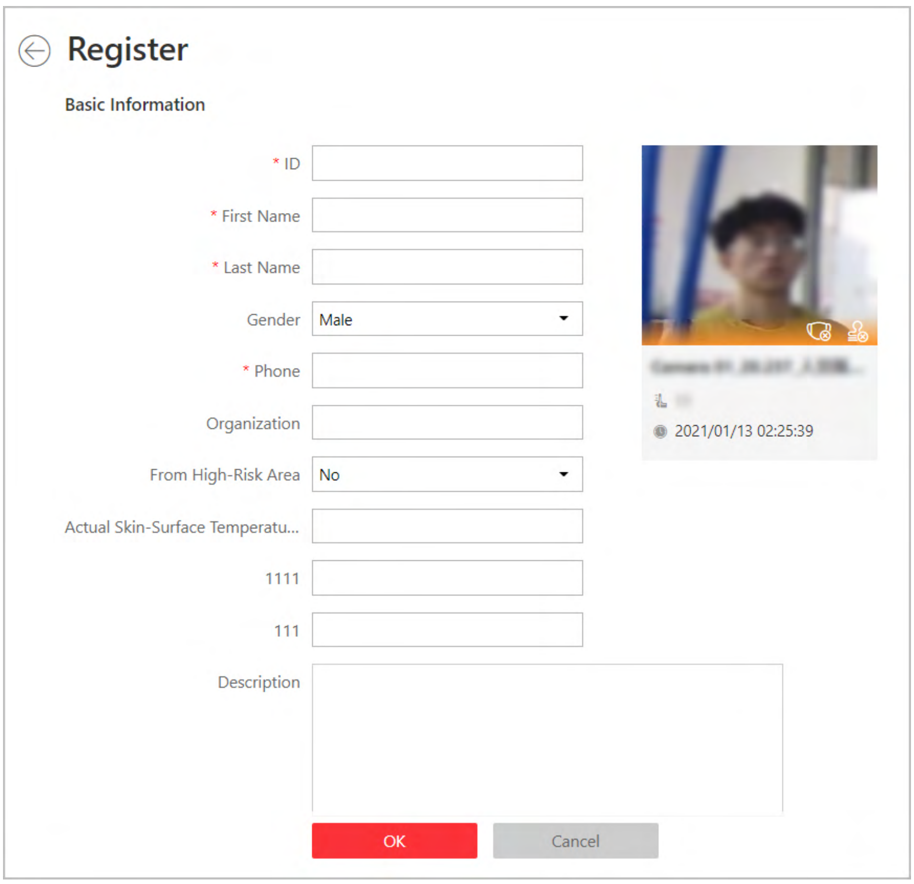



**Figure 25-2 Register Page**

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.

### 25.4.2 Customize Registration Template

You can set customized person information for registration which are not predefined in the system according to your actual needs.

**Steps**

**Note**

Up to 5 additional items can be added.

1. 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. |

### 25.4.3 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.

## 25.5 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**.

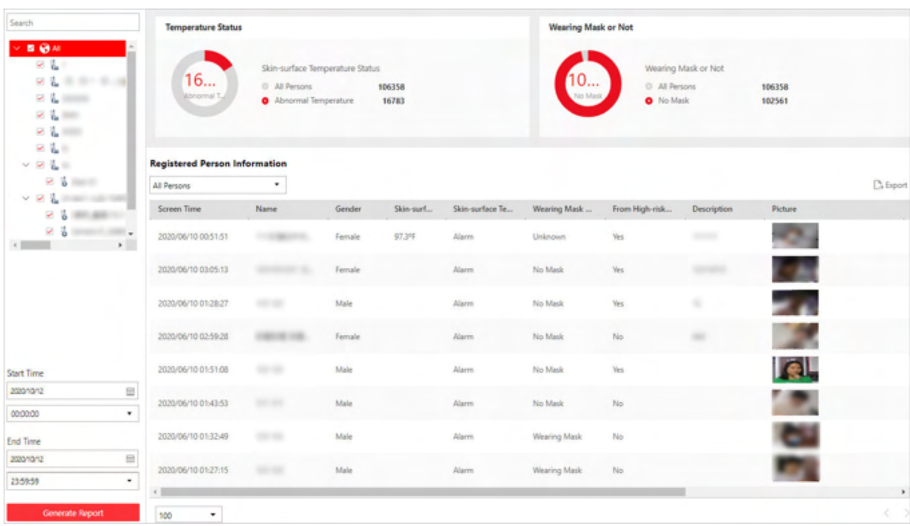



**Figure 25-3 Skin-Surface Temperature Report**

### 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 26 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.

## 26.1 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. |

## 26.2 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. |

## 26.3 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.

## 26.4 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. |

## 26.5 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. |

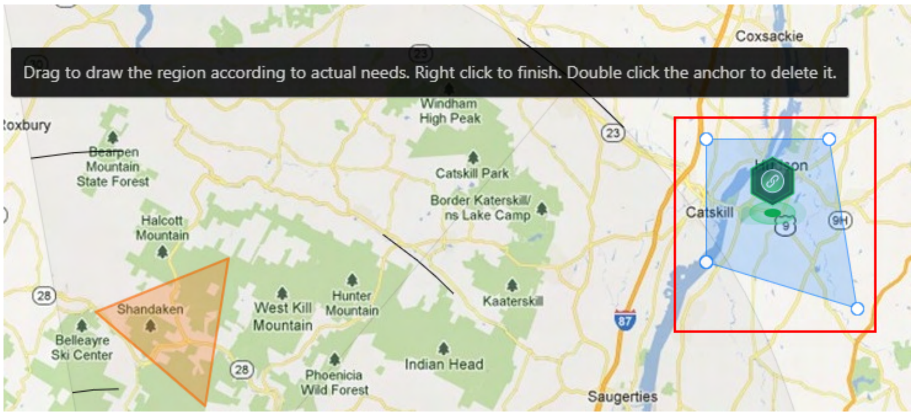



Figure 26-1 Edit Hot Region Area

## 26.6 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. |

## 26.7 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 a defense 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*** .

## 26.8 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. |

## 26.9 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. |

## 26.10 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.

## 26.11 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.

### 26.11.1 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.<br>**2D/3D**: Switch the displaying dimension of the map.<br>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.

## 26.11.2 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.

## 26.11.3 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**

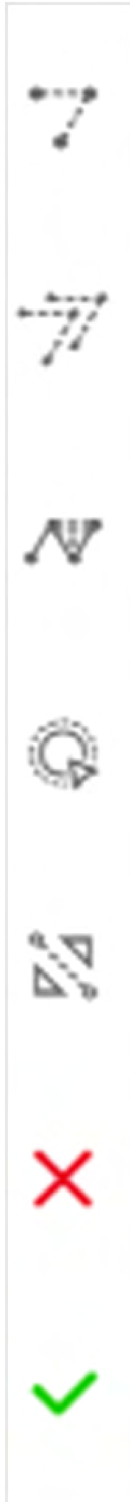
A radar has been added to the area and map. Refer to ***Add Radar to Area for Current Site*** and ***Add Hot Spot on Map*** for details.

**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.

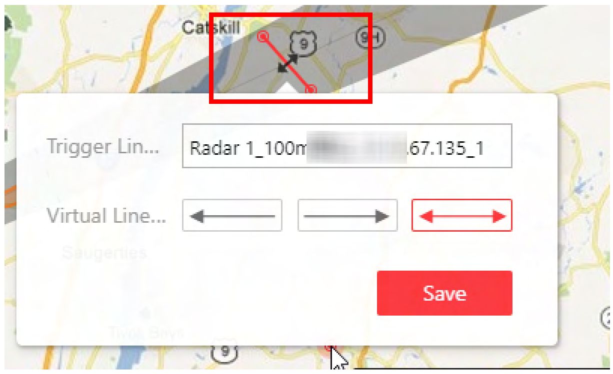



**Figure 26-3 Trigger Line in the Detection Area**

### 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.

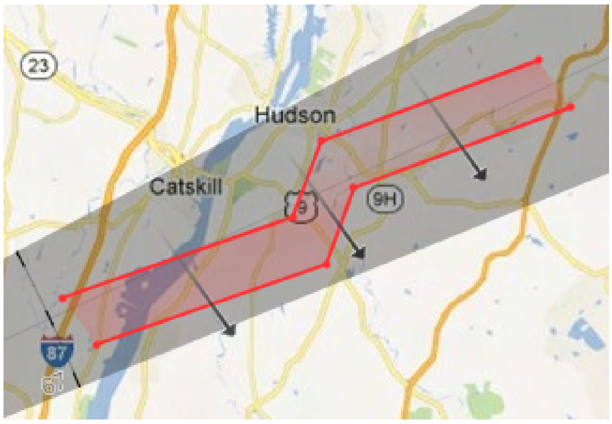



**Figure 26-4 Dual-Trigger Line in the Detection Area**

**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.

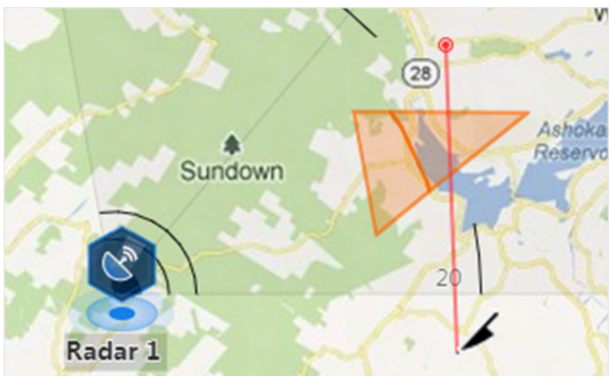



**Figure 26-5 Zone Segmentation**

**Distance Segmentation**

Split a zone into two smaller zone by an arc.

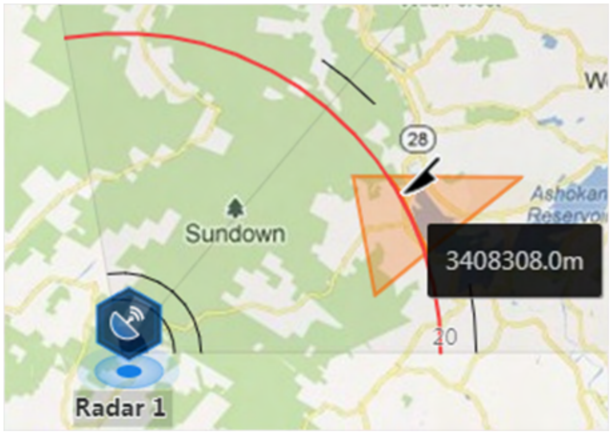



**Figure 26-6 Distance Segmentation**

**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.

## 26.11.4 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.

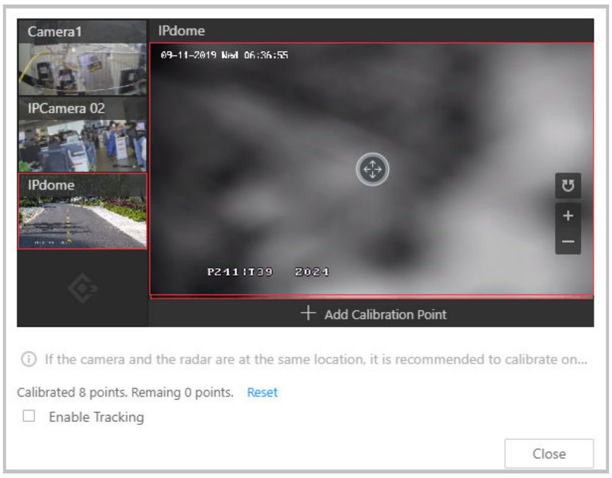



**Figure 26-7 Add Calibration Point**

   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.

## 26.11.5 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.

### 26.11.6 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.

## 26.12 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.

## 26.13 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.

## 26.14 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.

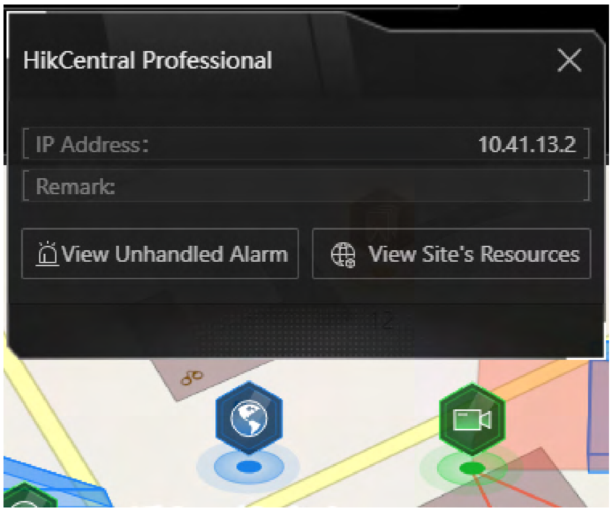



**Figure 26-8 Site Details**

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. |

## 26.15 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 27 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.

## 27.1 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.

### 27.1.1 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 27-1 Real-Time Health Status Overview**

**Table 27-1 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.<br><br>**Note**<br><br>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 |
| --- | --- |
| | <br>**Figure 27-2 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.<br><br>If the icon  appears at the top of device picture, it indicates that the device firmware should be upgraded. For upgrading the firmware, refer to ***Upgrade Device Firmware*** . |
| Refresh | • Manually Refresh: Click **Refresh** in the upper right corner of Real-Time Overview page to manually refresh the resource status on the page.<br>• 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 Exception Data** to export the exception data in Excel/CSV format. |

| Section | Description |
| --- | --- |
| | <br>**Figure 27-3 Export Overview Page or Exception Data** |

### 27.1.2 Real-Time Health Status Overview (Topology)

In the Health Monitoring module, you can view the real-time health 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.

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.

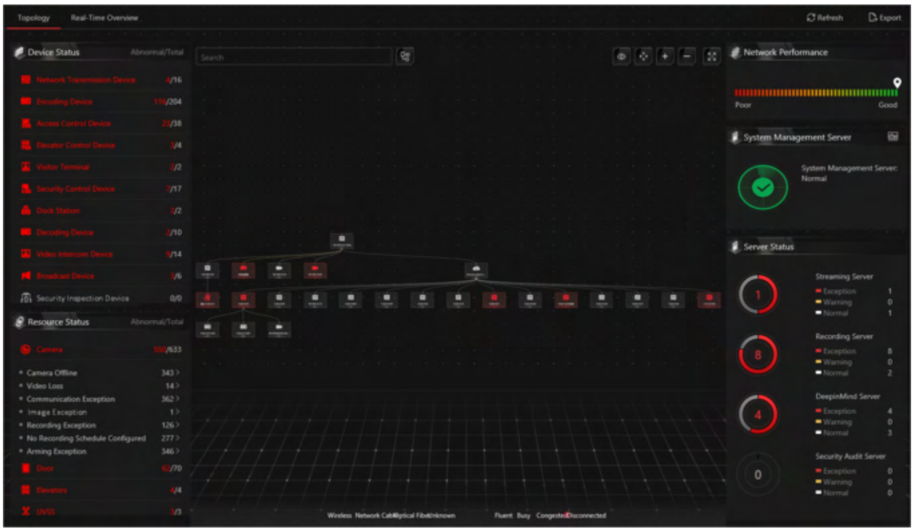
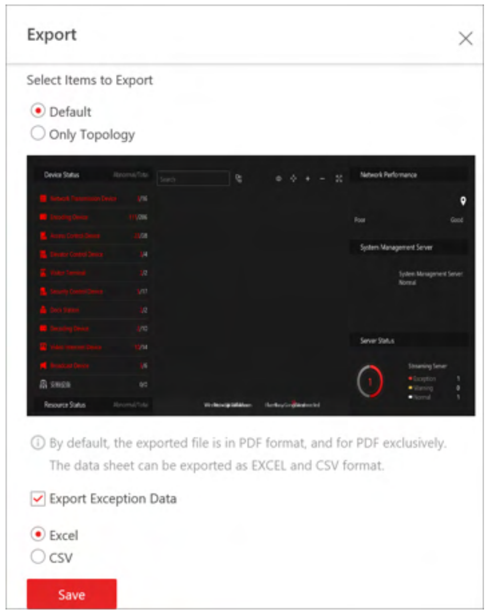



**Figure 27-4 Topology Overview**

**Table 27-2 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.<br>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.<br>**Note**<br>The Remote Site status is only available for the Central System with the Remote Site Management module (based on the License you purchased). |
| 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. |

| Section | Description |
|---|---|
| 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.<br><br>**Figure 27-5 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.<br>• 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 topology in PDF format or the exception data in Excel/CSV format.<br>**Note**<br>• If the export type is selected as **Default**, the whole displayed information (topology and exception data) on the Health Monitoring page will be exported.<br>• If the export type is selected as **Only Topology**, only the topology will be exported in PDF format. |

| Section | Description |
| --- | --- |
| | <br><br>**Figure 27-6 Export Topology** |

## Topology Details

The topology of devices will display the hierarchical relationships among the devices, device information, link status, alarm information, etc.

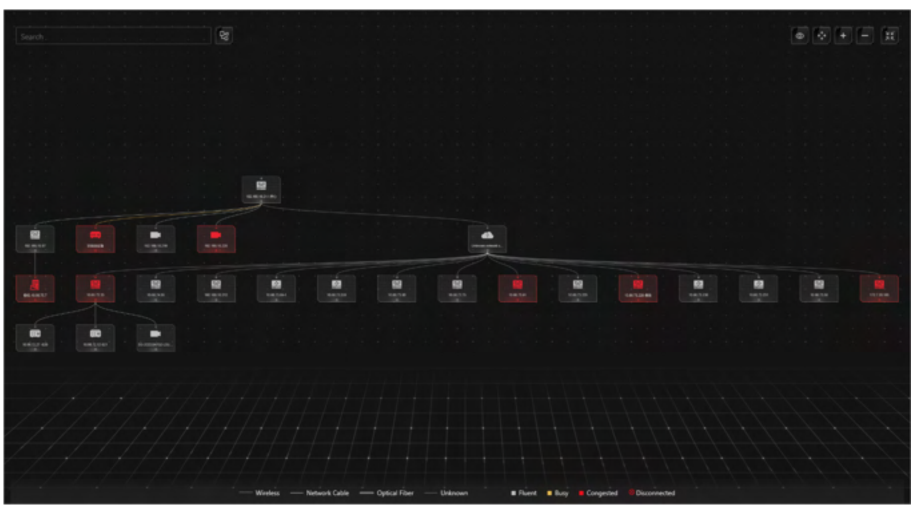


**Figure 27-7 Topology Details**

**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).

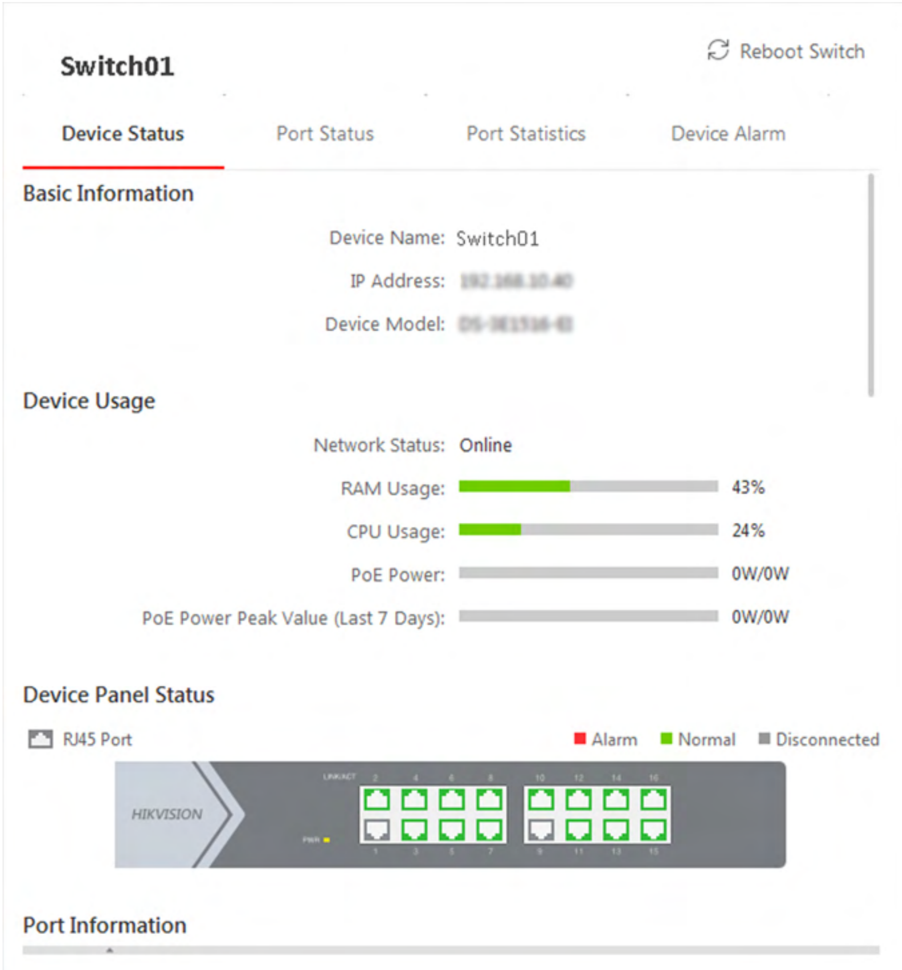



**Figure 27-8 View Device Details**

---

**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.

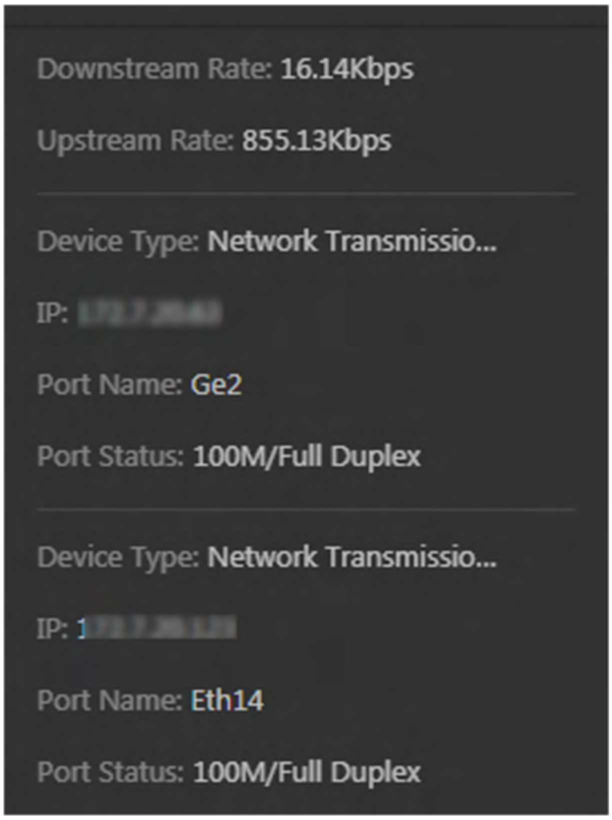



**Figure 27-9 View Link Details**

**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.

## 27.1.3 Historical Health Data Overview

You can view the historical online rate of resources and devices, or the recording integrity rate.

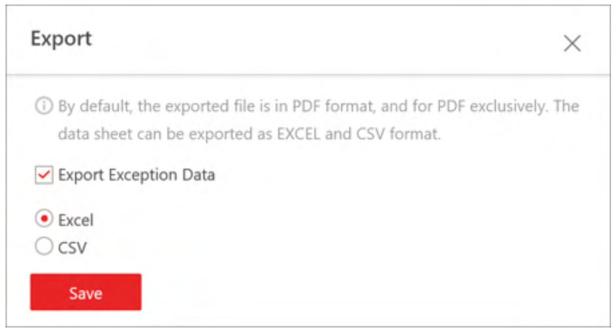
In the top left corner of Home page, select → **All Modules** → **Maintenance** → **Health Monitoring** → **History Overview** .


**Figure 27-10 Historical Health Data Overview**

**Table 27-3 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:<br>◦ Move the cursor on the line chart to view the camera online rate and the number of offline cameras at specific time points.<br>◦ 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.<br>• On the doughnut chart, you can perform the following operations:<br>◦ 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.<br>◦ 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.<br>• On the table, you can do one of the followings:<br>◦ Click **Total Offline Duration** to rank the cameras in terms of total offline duration within the time period you select.<br>◦ 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. |

| Section | Description |
|---|---|
| | ◦ Move the cursor on the line chart to view the device online rate and the number of offline devices at specific time points.<br>◦ 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.<br>• On the doughnut chart, you can perform the following operations.<br>◦ 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.<br>◦ 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.<br>• On the table, you can do one of the followings.<br>◦ Click **Total Offline Duration** to rank the devices in terms of total offline duration within the time period you select.<br>◦ 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. |
| Refresh | • Manually Refresh: Click **Refresh** in the upper right corner of History Overview page to manually refresh the data on the page.<br>• 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. |

| Section | Description |
| --- | --- |
| | <br><br>**Figure 27-11 Export Overview Page or Exception Data** |

## 27.2 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.

### 27.2.1 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 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, 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 past 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. The report contains logs recorded between last Monday and Sunday.

**Report Content**

Select the log content to be included in the report.

**Send At**

Set a report sending time.

**Email Template**

Select an email template to define the recipient information and content.

**Note**

You can click **Add New** to add a new email template. For setting email template, refer to ***Set Email Template*** .

**Report Language**

Select a report language.

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 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 system 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, the system 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 system will send a report at the sending time every week or every month, which contains logs recorded during the past 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. The report contains logs recorded between last Monday and Sunday.

**Report Content**

Select the log content to be included in the report.

**Send At**

Set a report sending time.

**Email Template**

Select an email template to define the recipient information and content.

**Note**

You can click **Add New** to add a new email template. For setting email template, refer to ***Set Email Template*** .

**Report Language**

Select a report language.

**6.** Click **Add** to save the report rule.

## 27.2.2 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** .

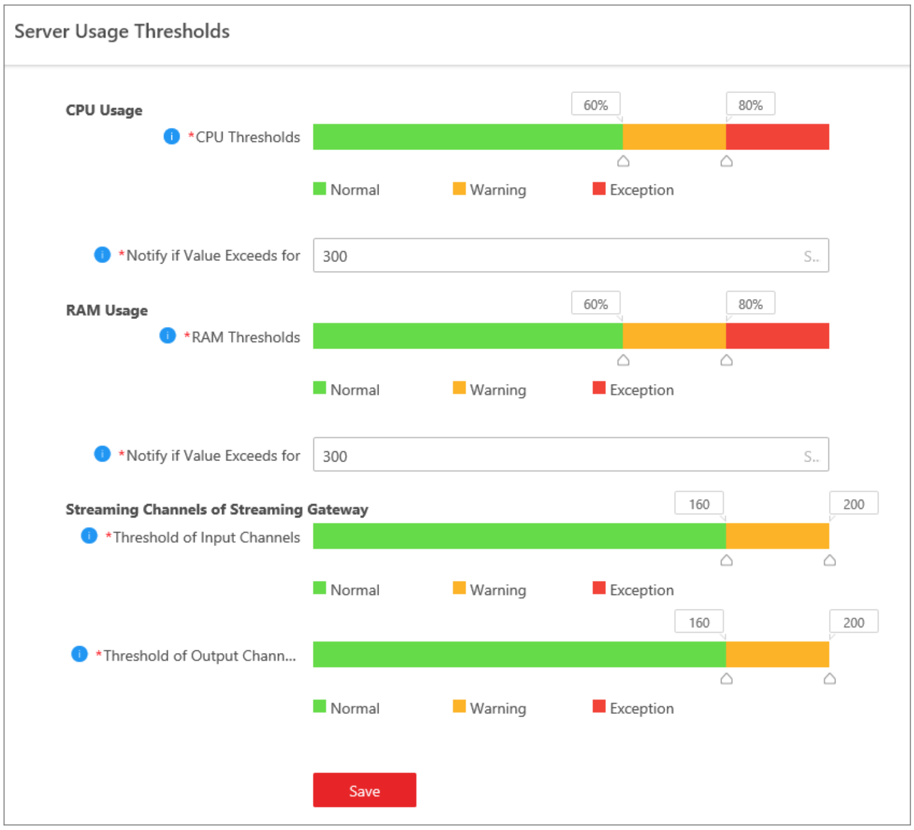



**Figure 27-12 Set Server Usage Threshold**

## 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.

### 27.2.3 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 27-4 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.

### 27.2.4 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 encoding devices, access control devices, elevator control devices, video intercom devices, security control devices, dock stations, network transmission devices, IP speakers, and security inspection devices, managed on the platform. It controls how often the platform pings these devices to determine whether they are online.
After disabled, the platform will not update the status of the managed devices. You need to refresh manually to get the latest status.

**Note**

You should adjust the check frequency according to the number of devices. The greater the number of devices, the lower the frequency of health checks..

### 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.

## 27.2.5 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**


**Figure 27-13 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.

## 27.3 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.

**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.

## 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*** .

## 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.
- Click beside the **Alarm Input Type** and select a device type from the drop-down list to filter the alarm input status by device 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.

## 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*** .

## Third-Party Integrated Resource Status

In the third-party integrated resource status page, you can view the status and information of third-party integrated resources, such as the resource type, manufacturer, network status, and resource status.
You can also perform the following operations.

- Click the name to view the status details and basic information.
- Click in the Operation column to go to the Area page to configure the parameters of the specified third-party integrated resource. See details in ***Edit Third-Party Integrated Resource for Current Site*** .

## 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.
- Select a Remote Site from the drop-down list at the top to display the status of Streaming Servers on the Remote Site.

## 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.

## 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.

## 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.

## 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*** .

### 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.

### Elevator Control Device

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.

### 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.

### Security Control Panel 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.
- 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, 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.

## 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.
- 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.
- 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*** ).

## 27.4 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.

### 27.4.1 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** → **Audit Trail** → **Server Logs** .

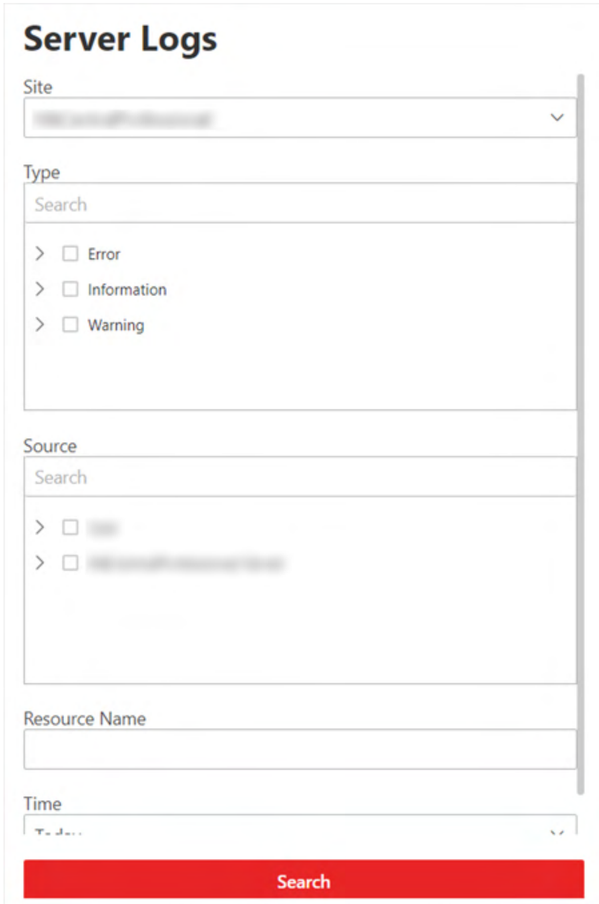



**Figure 27-14 Search for Server Logs**

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:** 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.

## 27.4.2 Search for Online/Offline Logs of Device

You can search for the online/offline logs of encoding devices and security inspection 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** → **Audit Trail** → **Device Logs** .

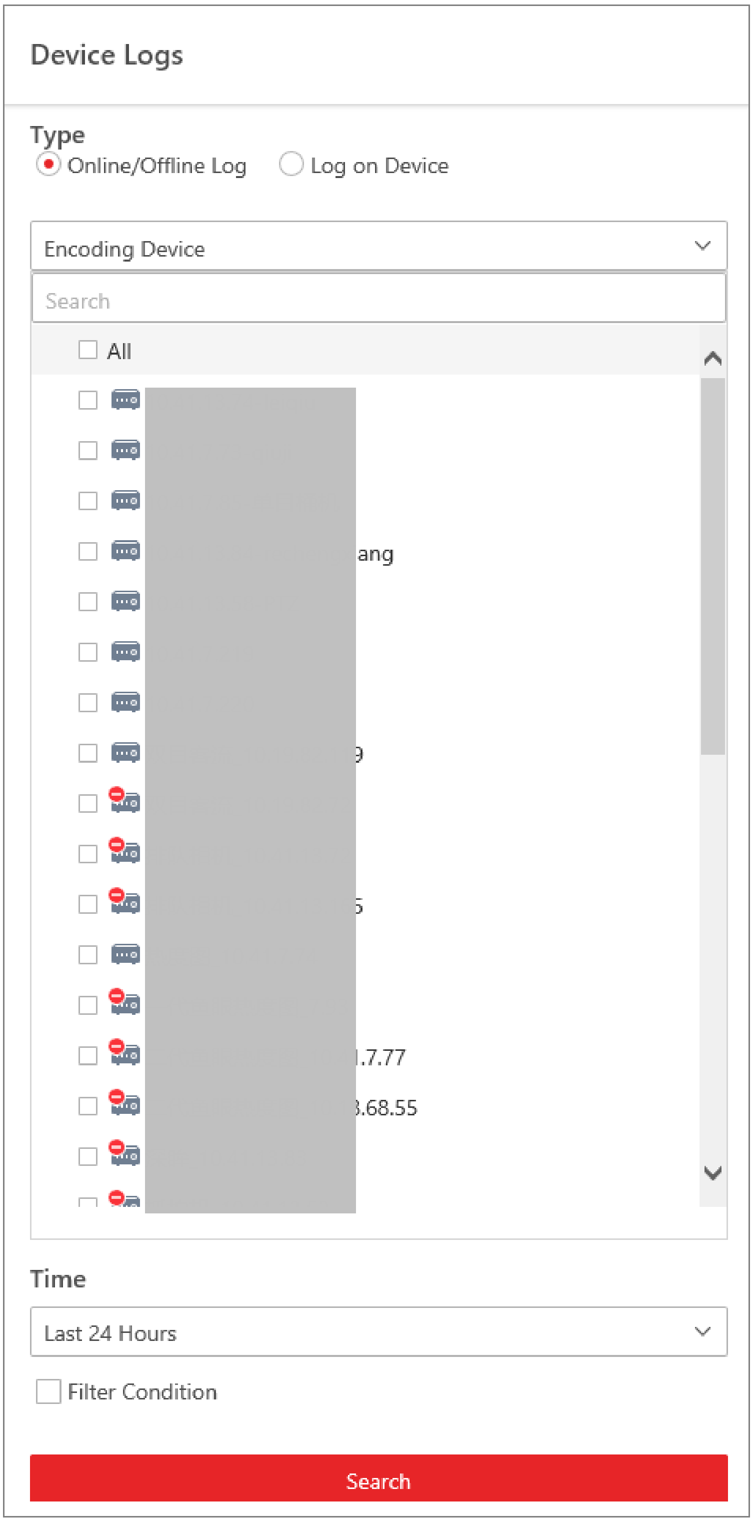



**Figure 27-15 Search for Device Online/Offline Logs**

**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.

**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.<br>You can perform the following operations.<br>• Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter the data.<br>• 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. |

## 27.4.3 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** → **Audit Trail** → **Device Logs** .

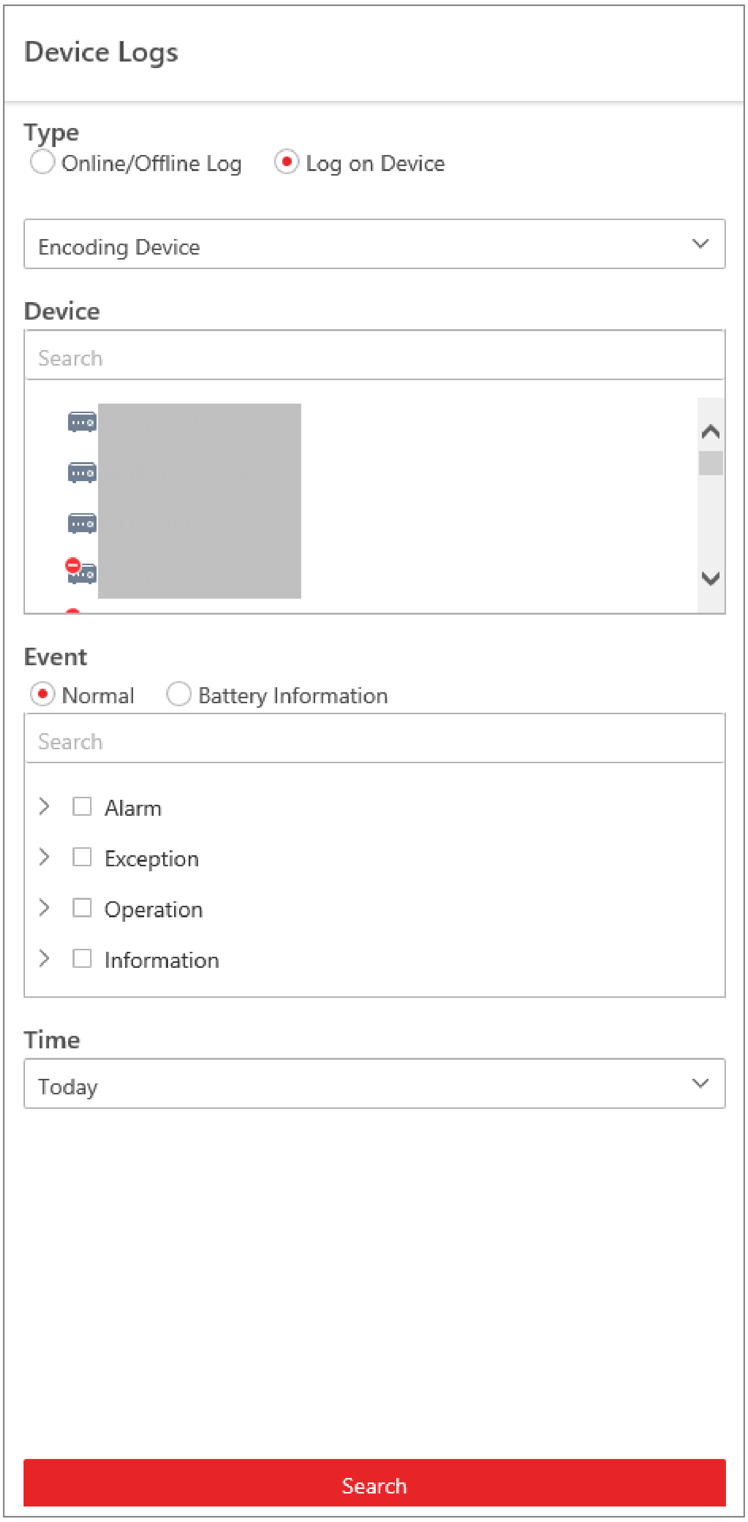



**Figure 27-16 Search for Logs Stored on Device**

**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.

### 27.4.4 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** → **Audit Trail** → **Resource Logs** .

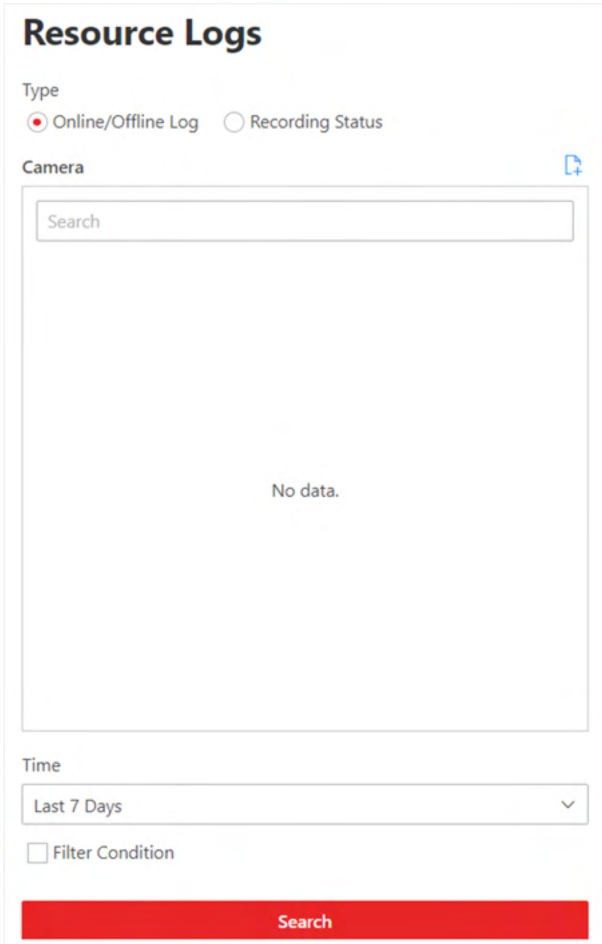



**Figure 27-17 Search for Resource Online/Offline Logs**

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.<br>You can perform the following operations.<br>• Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter data.<br>• 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. |

## 27.4.5 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 → Audit Trail → Resource Logs** .

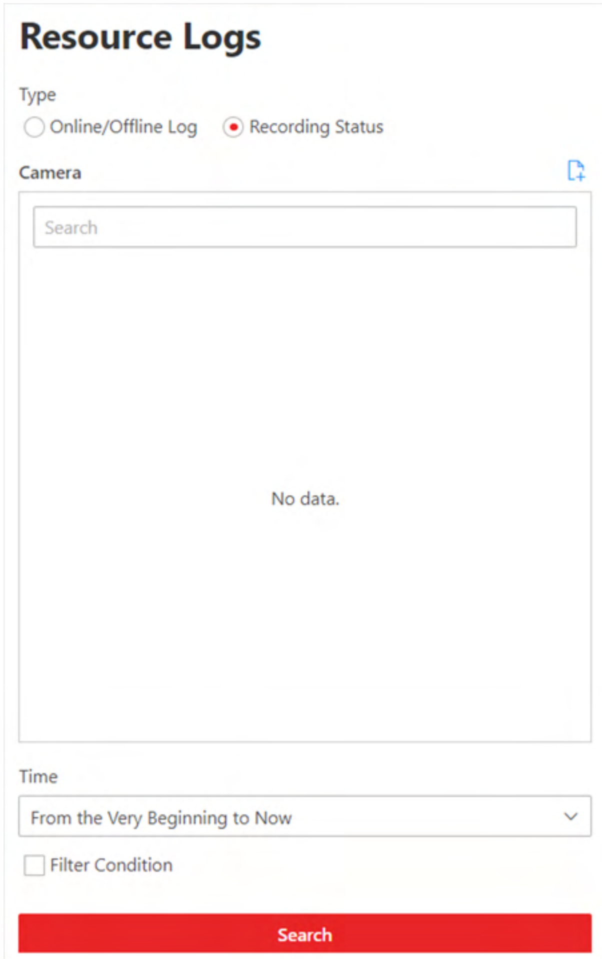



**Figure 27-18 Search for Resource Recording Status**

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**

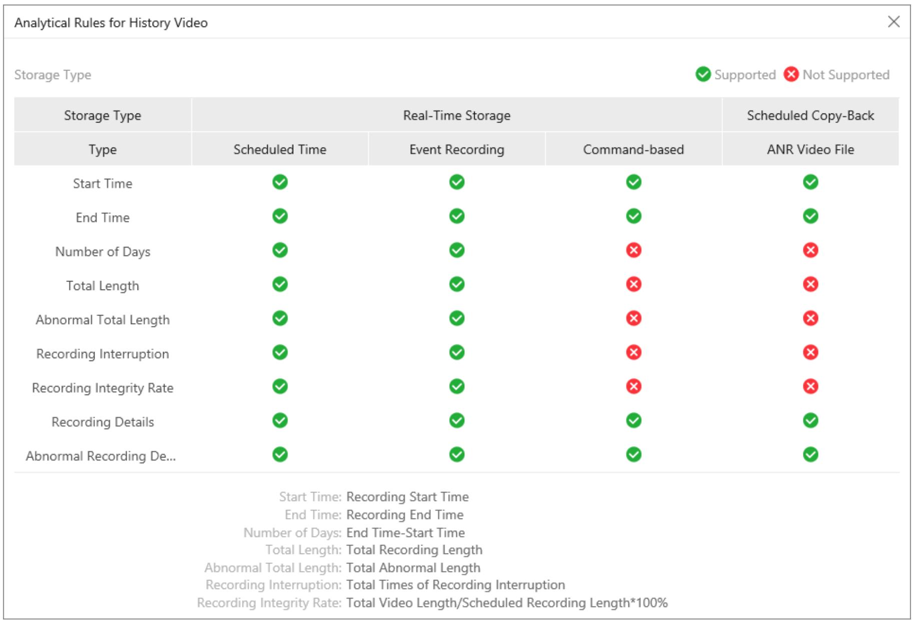
The total time length of the video loss within the scheduled time.

**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 27-19 Analytical Rules for History Video**

2) Click a camera name to open the History Recording Status panel.

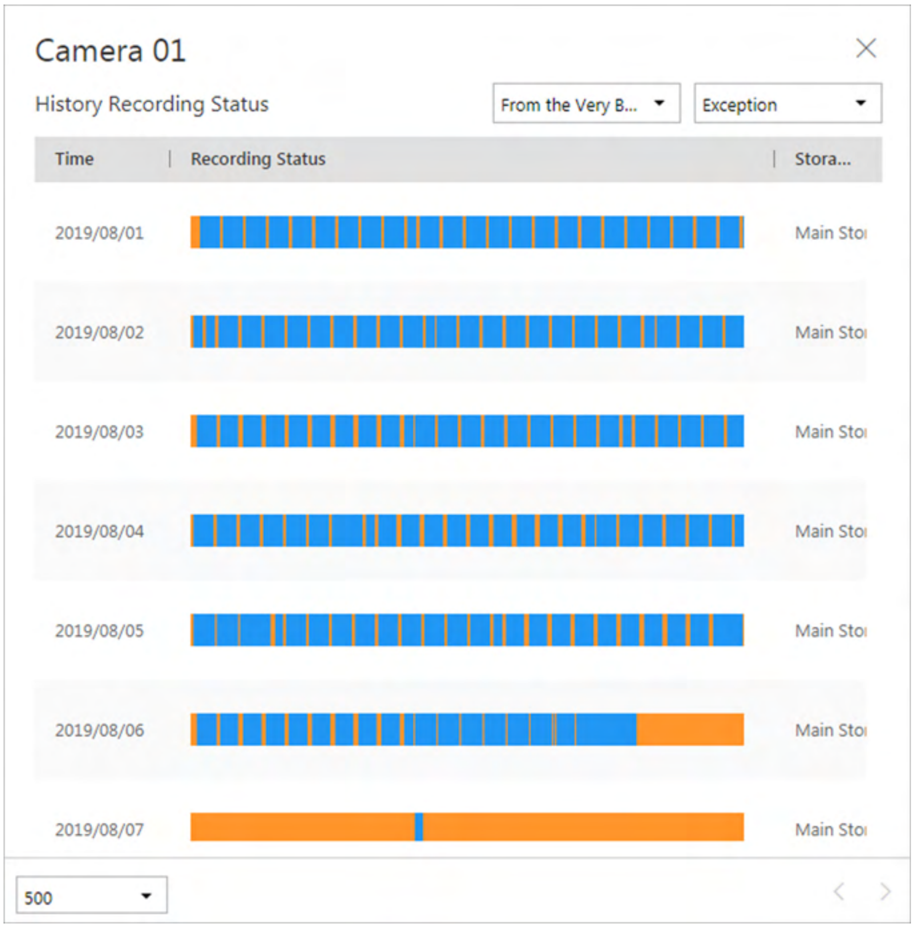



**Figure 27-20 History Recording Status**

**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.

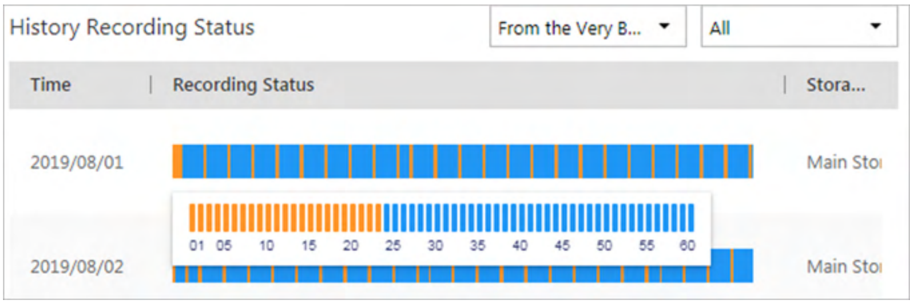



**Figure 27-21 Recording Status Details within One Hour**

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.

## 27.5 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.

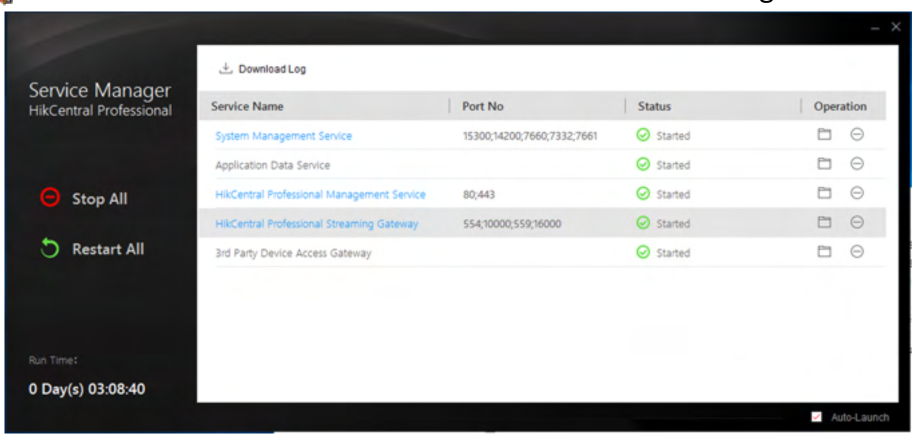



**Figure 27-22 Service Manager Main Page**

**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.

## 27.6 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.

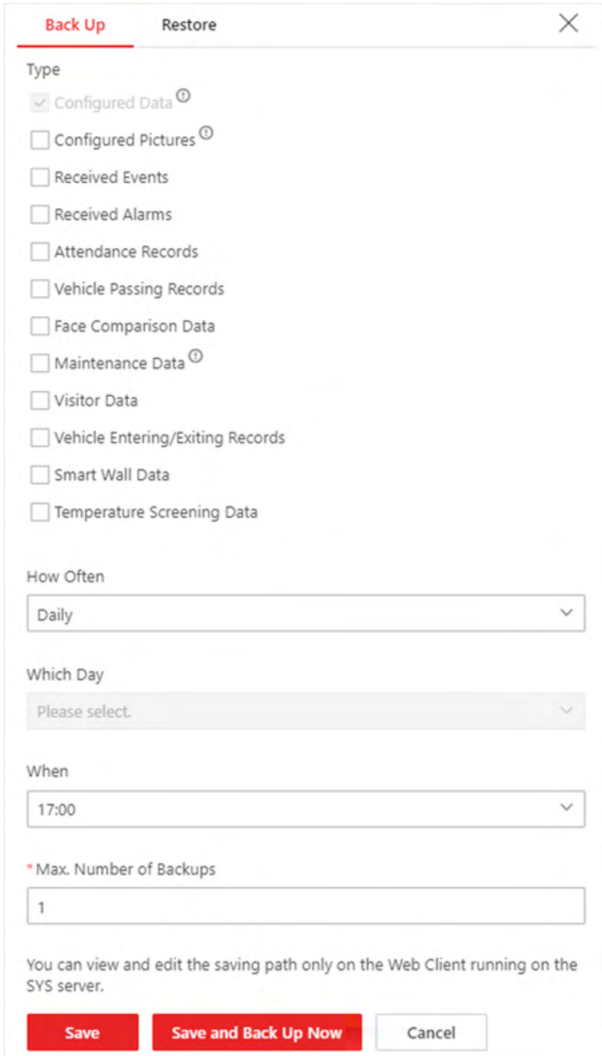



**Figure 27-23 Set System Data Backup**

**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.

## 27.7 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.

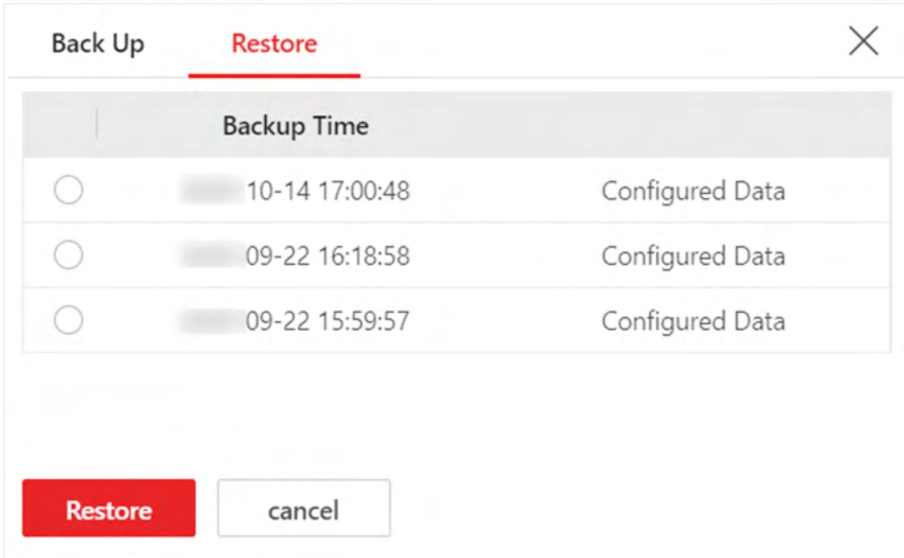



**Figure 27-24 Restore System Data**

**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.

## 27.8 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 28 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.

## 28.1 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.

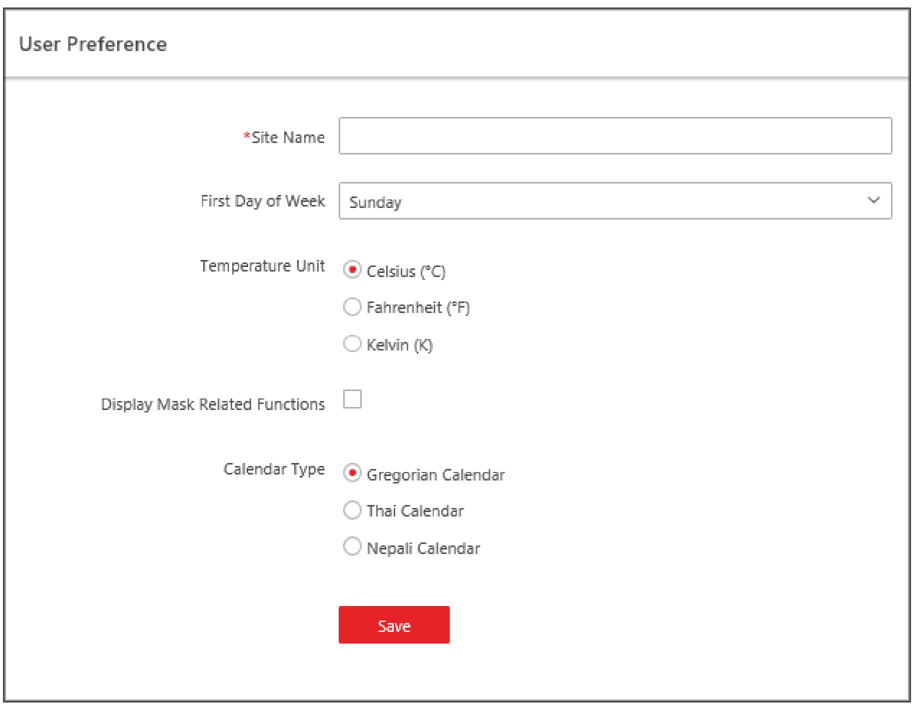



**Figure 28-1 User Preference**

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 Nepail Calendar according to the custom of the actual scene.

## 28.2 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.

## 28.3 Set NTP

You can set the NTP server for synchronizing the time between the SYS and the NTP server.

**Steps**

**Note**

For devices added via ONVIF protocol, time synchronization will fail. Please configure the time on the device locally and make sure the device's NTP settings are the same with the platform's.

1. In the top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Network** → **NTP** .
2. Set the **Time Synchronization** switch to ON to enable the NTP function.
3. Set the NTP server address and NTP port.
4. Enter the interval for the auto time synchronization.
5. **Optional:** Click **Test** to test the communication between the SYS and NTP server.
6. Click **Save**.

## 28.4 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.

Perform this task when you need to set active directory.

**Steps**

1. In the top left corner of 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 and not 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.

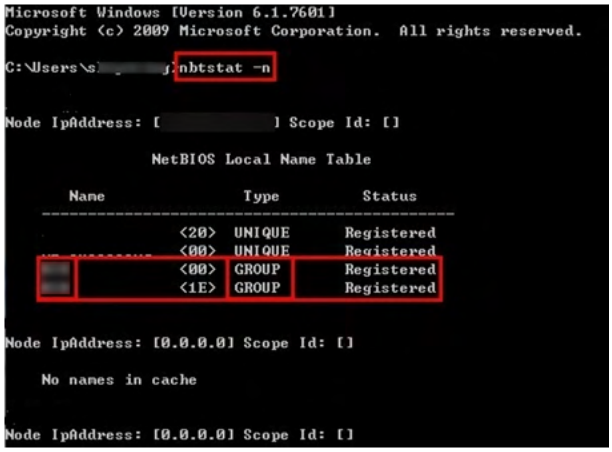



**Figure 28-2 How to Get NetBIOS Domain Name**

**Host Name**

The DNS server's IP address. You can get it in Network Connection Details.

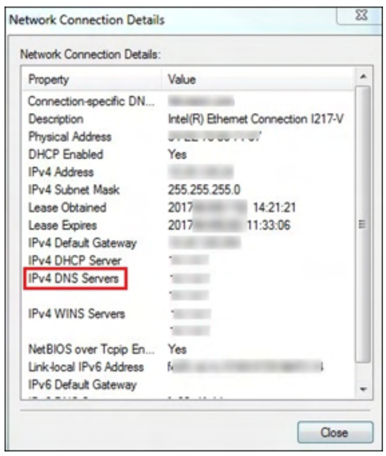



**Figure 28-3 How to Get Host Name**

**Port No.**

The port No. of the AD domain controller. By default, it is 389.

**Enable SSL (Optional)**

Enable SSL if required by the AD domain controller.

**User Name**

The user name of the AD domain controller. This needs to be the domain administrator.

**Password**

The password of the AD domain controller.

**Base DN (Distinguished Name)**

Enter the filter condition in the text filed 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 Organizational Unit (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 on the AD domain controller will be obtained.

**3. Optional:** Link the person information you concerned stored in the domain to the person information in the system.

1) Set the **Link Person Information** switch to ON.

The default and custom additional information items ( see ***Customize Additional Information*** ) are displayed in the Person Information area by default. You can set the link relationship for those or add new person information items as you desired.

2) **Optional:** Click **Add New** to add a person information item you concerned.

**Note**

- You needn't add the basic person information items, including ID, First Name, Last Name, Phone, and Remark) manually, which has the default link relationship with the domain.
- The new person information item is also displayed on 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 items when importing the domain persons.

5) **Optional:** Hover over the linked person information in domain and click × to remove the relationship. You can also change the link relationship among each other by clicking and dragging the one item to anther.

**4.** Click **Save**.

After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on User Management page.

If the Link 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.

## 28.5 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 ONVIF Protocol** when accessing the device via ONVIF protocol.

Switch on **Allow ISUP Registration**.

Check **Allow ISUP of Earlier Version**.

**Note**

The device may be attacked when accessing the system by ISUP of earlier versions.

Click **Save**.

## 28.6 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 domain name and ports for HikCentral Professional.

**Steps**

1. In the upper-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 domain name of the server for WAN access.
4. Set the following ports.

   **Client Communication Port**

   Used for Web Client and Control Client to access the platform via HTTP. By default, it is 80.

   **Client SSL Communication Port**

   Used for Web Client and Control Client to access the platform via HTTPS. By default, it is 443.

   **Real Time Streaming Port**

   Used for getting stream for live view via Control Client. By default, it is 554.

   **Video File Streaming Port**

   Used for getting stream for playback via Control Client. By default, it is 10000.

   **Web Client Streaming Port**

   Used for getting stream via Web Client (for 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 stream via 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.

5. **Optional:** If you adopts generic events to integrate HikCentral Professional with external sources, you need to set the TCP port and UDP port for receiving the TCP and/or UDP data packages.

**Note**

For setting the generic event, refer to ***Configure Generic Event*** .

6. **Optional:** For the platform with Remote Site Management module, set the port to receive the registration from a 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 accessing via ISUP, you can set the ports for these ISUP devices, such as registration port, alarm receiving port, and so on.

**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 stream from ISUP devices via VAG server. By default, it is 7661.

**ISUP Streaming Port (via Plugin)**

Used for getting stream from ISUP devices via Plugin. By default, it is 16000.

**Note**

If the ISUP ports are disabled on the SYS, the ISUP related ports will not be displayed in the WAN Access page.

8. Click **Save**.

## 28.7 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**.

## 28.8 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, face comparison data, vehicle entering/exiting records, etc.

**Steps**

1. In the upper-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.

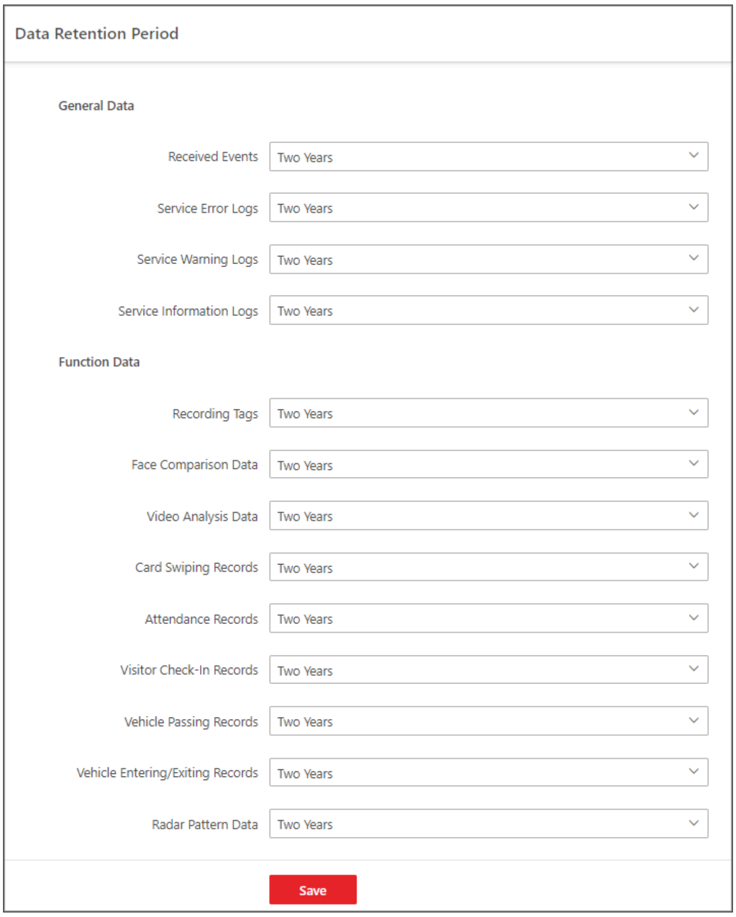



**Figure 28-4 Set Data Retention Period**

**Note**

The data recorded by devices 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.

**3.** Click **Save**.

## 28.9 Set Holiday

You can add the holiday to define the special days that can adopt different shifts schedule or access schedule. You can set regular holiday and irregular holiday according to the actual scene.

### Add Regular Holiday

Regular holiday is suitable for the holiday that has fixed date. For example, the Christmas is in December 25th of each year.

In the top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Normal** → **Holiday Settings** → **Add** to open the adding holiday dialog. Select the Holiday Type as **Regular Holiday**.

Set the parameters as the following instructions:

**Start Date**

The start date of the holiday.

**Number of Days**

The lasting days of the holiday.

**Repeat Annually**

If selected, the system will generate date of holiday according to the date of the VSM server.

### Add Irregular Holiday

Irregular holiday is suitable for the holiday that is calculated by the weekdays, and specified date might be different in different year. For example, the Mother's Day is in the second Sunday of each May.

In the top of top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Normal** → **Holiday Settings** → **Add** to open the adding holiday dialog. Select the Holiday Type as **Irregular Holiday**..

Set the parameters as 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 selected, the system will generate date of holiday according to the date of the SYS server.

**Note**

If you select **Repeat Annually**, the specified date of this holiday will be generated automatically according to the current year of the SYS server.

For example, the Mother's Day in 2019 and 2020 is on 12th, May, 2019 and on 10th, May, 2020. The the system will automatically set these two days as holidays for Mother's Day if you have selected **Repeat Annually**.

## 28.10 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 of top left corner of 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 of the template. |

6. **Optional:** Set the back style of the template.

**Note**

You can set the back style according to the 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**

In the card template list page, there are two default templates. You can view default templates but not edit or delete them.

## 28.11 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.

### 28.11.1 Configure Email Account

You should configure the parameters of sender's email account before the system can send the message to the designate email account(s) as email linkage.

**Steps**

1. In the top of top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Email** → **Email Settings** .

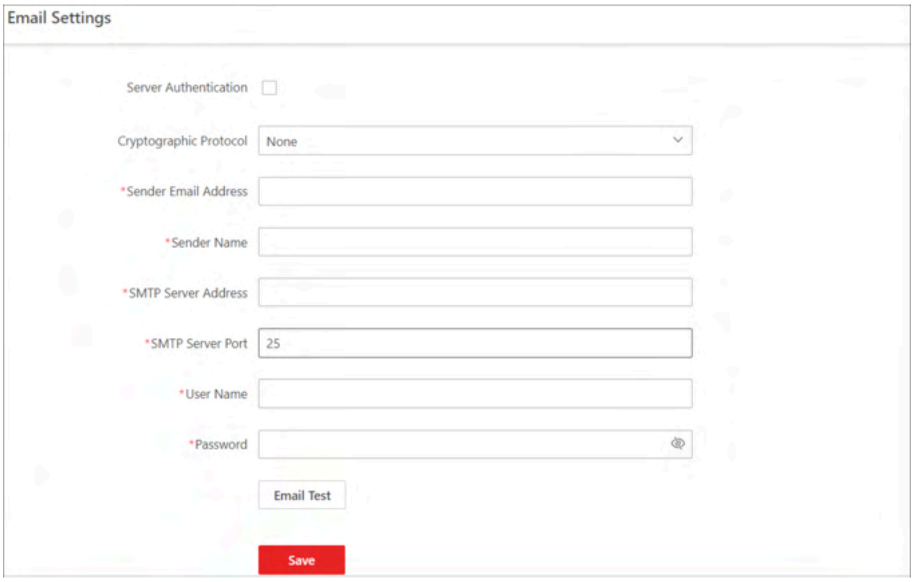



**Figure 28-5 Email Settings**

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.

   **SMTP Server Address**

   The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

   **SMTP Server Port**

   The default TCP/IP port used for SMTP is 25.

3. Click **Email Test** to test whether the email settings work or not.

   The corresponding attention message box will pop up.

4. Click **Save**.

### 28.11.2 Add Email Template for Sending Report Regularly

You can set email templates (including specifying the recipient, email subject, and content) for sending report regularly, so that the platform can send report as email attachment 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 → Scheduled 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(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.

   **Content**

   Define the report content to be sent. You can also click buttons below the **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 on 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. |

## 28.11.3 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.

   **Content**

   Define the event or alarm information to be sent. You can also click buttons below the **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. |

## 28.12 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**

**Note**

Setting transfer protocol is only available when accessing the Web Client on the SYS server locally.

**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.

**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 logout during reboot. The reboot takes about one minute and after that, the users can login again.

## 28.13 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**

**Note**

Exporting SYS server's service component certificate is only available when you access the Web Client on the SYS server locally.

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*** .

## 28.14 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.

## 28.15 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**.

## 28.16 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.

## 28.17 Data Interchange

The card swiping data recorded in HikCentral Professional can be used by the third-party system for pay calculation or other applications. You can apply the card swiping records or dump the records as CSV files for data synchronization with the third-party system.

### 28.17.1 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. Set the required parameters of the third-party database, including server IP address, server port, database name, user name and password.
8. Click **Test Connection** to test whether database can be connected.
9. 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.
10. Click **Save**.

    The data will be written to the third-party database.

### 28.17.2 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 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 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 **Access Record Dump**.
7. In Dump Rule area, click **Add** and set the required parameters.

   **File Name**

   The name of 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 and saved in local disk of 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 into the Web Client running on 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 SFTP server as the storage location for saving dumped file by setting SFTP address, port, user name, and password. And you can enter the path to save the dumped file in the folder on SFTP server or leave it empty to save that in 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 certain fixed length.

You can switch it on and set the value of **Length**. If the length of 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 number need to be dumped as 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.

**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 Dump Rule area.

**Note**

You can click × on Operation column to delete the rule or click **Delete All** to delete all added rules.

9. Click **Save**.

## 28.18 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.

## 28.19 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.

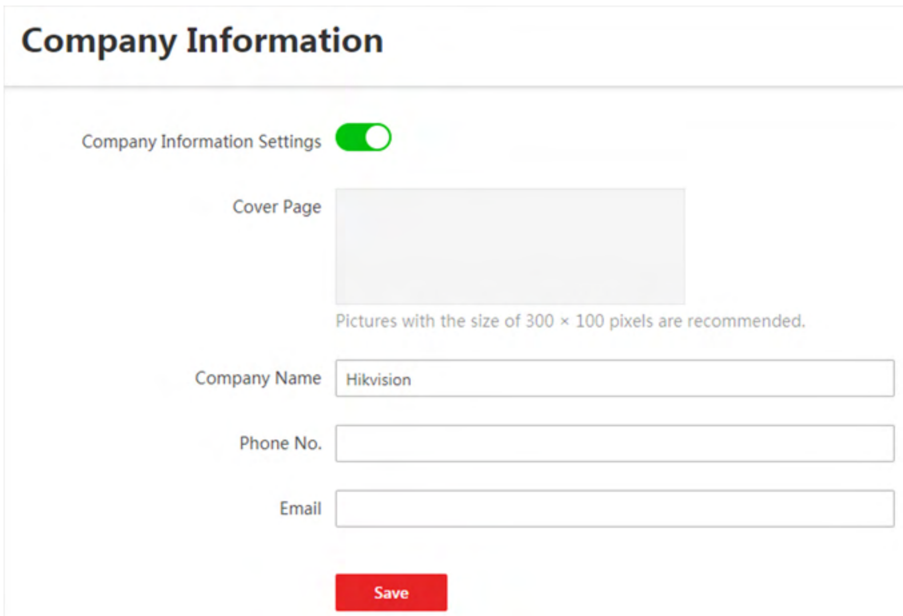



**Figure 28-6 Company Information Settings**

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.

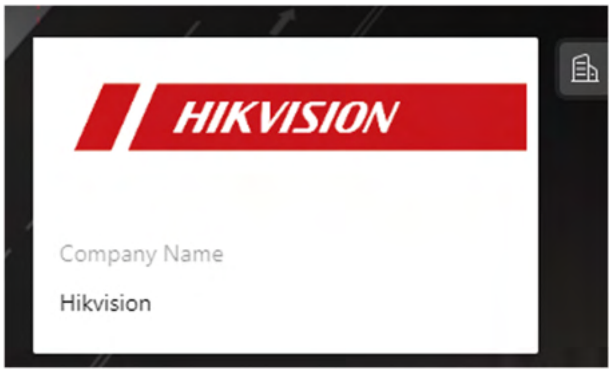



**Figure 28-7 Company Information Displayed on Web Client**

# Chapter 29 Important Ports

HikCentral Professional uses particular ports when communicating with other servers, devices, and so on.

Make sure that the following ports are not occupied for data traffic on your network and you should forward these ports on router for WAN access or open these ports in the firewall in case you may need to access the system via other networks.

| Destination | Port No. | Description |
|---|---|---|
| System Management Service (SYS) Port | | |
| SYS | 80 (HTTP/WebSocket) | Used for web browser access in HTTP protocol. |
| SYS | 443 (HTTPS/ WebSocket over TLS) | Used for web browser access in HTTPS protocol. |
| SYS | 14200 (HTTP/HTTPS) | Used for Remote Site registration to central system. |
| SYS | 15300 (TCP and UDP) | Used for receiving generic event. |
| SYS | 7332 (TCP) | Used for receiving alarms from ISUP device. |
| SYS | 7334 (UDP) | Used for receiving alarms from ISUP device. |
| SYS | 7660 (TCP) | Used for receiving registration from ISUP device. |
| SYS | 7661 (TCP) | Used for getting stream from ISUP device via Streaming Server |
| SYS | 8686 (TCP) | Listener port for listening the alarms of guidance terminal. |
| SYS | 6123 (HTTP) | Used for the picture storage of ISUP devices. |
| SYS | 6203 (HTTP) | Used for the object storage of digital signage terminals. |
| SYS | 7662 (TCP) | Signaling port for getting information of IP speakers. |
| SYS | 8877 (TCP) | Listener port for the registration of IP speakers accessing via Hikvision private speaker protocol. |
| SYS | 10015 (TCP) | Used for transmitting the audio data of IP speakers accessing via Hikvision private speaker protocol. |
| SYS | 27661 (HTTP) | Used for calling back the ISUP signaling. |
| SYS | 6470 (TCP) | Used for upgrading digital signage terminals in version 3.1 or below. |

| Destination | Port No. | Description |
|---|---|---|
| SYS | 6471 (TCP) | Used for releasing programs to digital signage terminals in version 3.1 or below. |
| SYS | 9980 (HTTP) | Used for uploading materials to the server. |
| Streaming Gateway (SG) Port | | |
| Streaming Gateway | 554 (RTSP) | Used for getting stream (real time streaming port). |
| Streaming Gateway | 559 (WebSocket) | Used for getting stream for Google Chrome or Firefox (WebSocket port). |
| Streaming Gateway | 10000 (TCP) | Used for getting stream for playback (video file streaming port). |
| Streaming Gateway | 16000 (TCP) | Used for getting stream from ISUP device via plugin. |
| Streaming Gateway | 6001 (SNMP) | Used for getting the status of Streaming Gateway. |
| Streaming Gateway | 6678 (HTTPS) | Used for setting the certificate. |
| Streaming Gateway | 16001 (TCP) | Used for uploading audio files by device. |
| Streaming Server Port | | |
| Streaming Service | 554 (RTSP) | Used for Streaming Service to get stream (real time streaming port). |
| Streaming Service | 559 (WebSocket) | Used for getting stream for Google Chrome or Firefox (WebSocket port). |
| Streaming Service | 10000 (TCP) | Used for Streaming Service to get stream for playback (video file streaming port). |
| Streaming Service | 6001 (TCP) | Used for getting the status of Streaming Service. |
| Streaming Service | 16000 (TCP) | Used for getting stream from ISUP device via plugin. |
| Streaming Service | 8208 (WebSocket over TLS) | Used for security certificate authentication. |
| Streaming Service | 6678 (HTTPS) | Used for setting the certificate. |
| pStor Cluster Service Port | | |
| pStor Cluster Service | 9012 (HHTP) | Used for accessing the pStor Cluster Service via Web Browser. |

| Destination | Port No. | Description | |
|---|---|---|---|
| pStor Cluster Service | 6300 (HTTP) | Used for signaling gateway. | |
| OpenAPI Service Port | | | |
| OpenAPI Service | 443 (HTTPS) | Used for third-party system accessing OpenAPI service. | |
| OpenAPI Service | 8208 (WebSocket over TLS) | Listener port for Service Manager after encrypted transmission enabled. | |

See Far, Go Further

UD24078B