HikCentral Enterprise-Commercial 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 INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

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

Symbol Conventions

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

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

Contents

Chapter 1 Overview

1.1 About This Document

This user manual is intended for the administrator of the HikCentral Enterprise-Commercial.

The manual guides you to establish and configure the surveillance system. Follow this manual to perform 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

HikCentral Enterprise-Commercial is developed for central management of video monitoring, parking (entrance and exit management), access control, visitor management, elevator control, time and attendance, patrol management, facial surveillance, and other subsystems. It 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, parking management, 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 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 live view, PTZ control, video playback and downloading, alarm receiving, video wall, and so on.
Web Client	Web Client is a B/S client for managing system. It provides multiple functionalities, including device management, area management,

Client	Introduction
	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 phone and tablet. 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

2.1 System Requirements

System requirements for accessing HikCentral Enterprise-Commercial Web Client should be as follows.

Time and Time Zone

Make sure your PC running the Web Client is in the same time and time zone as the system.

Operating System

Microsoft® Windows 7, Windows 10 (32-bit or 64-bit)

Resolution

The optimum resolution is 1440×900 and the best displaying ratio is 100%.

Web Browser

Internet Explorer 11 and above (32-bit or 64-bit)

Google Chrome 63.0.3239.132 and above

2.2 Set Internet Explorer

Before accessing the system via Internet Explorer browser for the first time, you should set the related parameters for the browser to ensure that you can operate the system smoothly.

Steps

1. Double click Internet Explorer browser icon to enter Internet Explorer browser.
2. Click **Tools → Internet Options** to enter Internet Options Page.
3. Click **Advanced**.
4. Check **Use TLS 1.1** and **Use TLS1.2**.
5. Click **Security → Trusted Sites → Sites** .
6. Enter the website of HikCentral Enterprise-Commercial Web Client, and click **Add** to add this website to the zone.
7. Click **Close**.
8. Click **OK** to finish setting Internet Explorer.

2.3 Log into HikCentral Enterprise-Commercial Web Client

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

Steps

1. In the address bar of the web browser, enter the IP address and port of the server running HikCentral Enterprise-Commercial CMS (Central Management Service) and press Enter key.

   Example

   If the IP address of the server running the CMS is 172.6.21.96, and port number is 445, you should enter ***172.6.21.96:445*** in the address bar. If the port is the default value (443), you can just enter ***172.6.21.96*** to access the CMS.

2. For the first time login, click **Download** on the upper-right corner and select **HikCentral Enterprise-Commercial Plug-in** to download and install it.

   Note

   You should run the downloaded plug-in as administrator.

3. Enter the user name and password of the CMS service.

   Caution

   - The initial password for admin user is ***Abc123++***. For the first time login, you should change the initial password.
   - 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 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 **Login** to log in to the HikCentral Enterprise-Commercial.

Chapter 3 Area Management

HikCentral Enterprise-Commercial provides areas to manage the added resources (e.g. encoding device, access control device, elevator control device, and parking device) in different groups. You can group the resources into different areas according to the resources' location. For example, on the 1st floor there mounted 64 cameras and 16 access control points. You can organize these resources into one area (named 1st Floor) for convenient management. You can view the live video, play back the video files and do some other operations of the devices after managing the resources by areas.

3.1 Select Scenario

For the first-time entering of the Security Area page, you should select a scene (general scene or community scene) for your application first before you can do further configurations.

Note

Scene cannot be changed once you select one. Please select the scene according to your applications cautiously.

Click on the Home page, and then go to **System Configuration** → **Security Area** to enter the Security Area page.

General Scene

Applicable to general surveillance scenes except the community scene.

Community Scene

Applicable to surveillance scenes for communities.

It covers functions in **General Scene**, and provides more features including:

- Quick creation of person organization tree based on building unit.
- Quick creation of security area tree based on building unit.
- Display event types that are applicable to the community by default.
- Quick match of video intercom outdoor station and house owner.

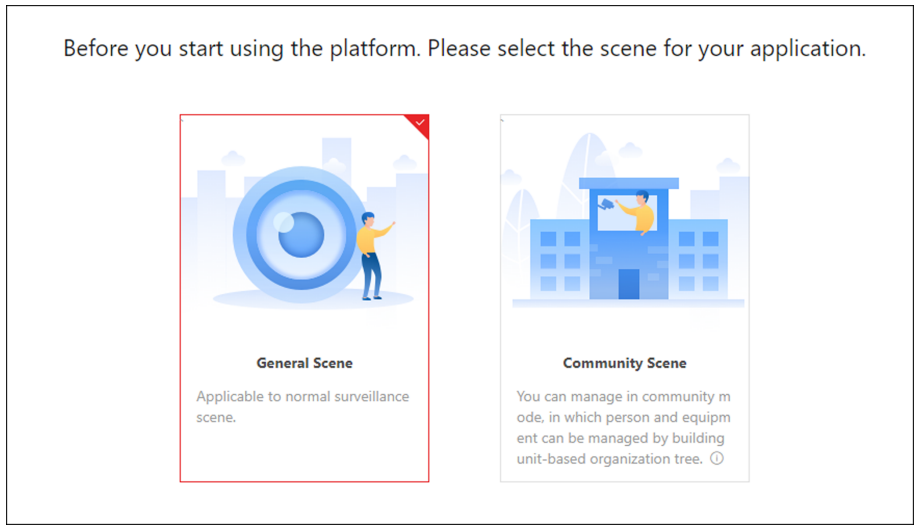


Figure 3-1 Select Scene for Your Application

3.2 Add Single Area

You should create an area in the system and add resources to the area to manage the resources by areas.

Steps

1. Click → **System Configuration** → → **Security Area Management** to enter Security Area Management page.
2. Select the upper-level area on the left panel, and then click to open the add area page.
3. Enter the area name and descriptions for the area.
4. Click **Save** to save the settings and add the area to the system.
5. **Optional:** Perform the following operations after adding areas.

Edit Area	Click the area name on the left panel, and then edit the area name and the descriptions for the area on right panel.
Delete Area	Click the area name on the left panel, and then click on the left panel to delete the area and its subordinate areas.

Note

If the area and its subordinate areas have resources inside, the area cannot be deleted.

Move Area	Select the area name on the left panel, and then click or to move the area up or down in the same parent area.

3.3 Import Areas

You can add multiple areas to the system in a batch.

Steps

1. Click → **System Configuration** → → **Security Area Management** to enter Security Area Management page.
2. Click the area name on the left panel to select it as the target area.
3. Click to enter the Import Area page.
4. Click **Download File Template** to download the template (CSV format) to the local disk of the PC running the Web Client.

   Note

   For one file, up to 50,000 records can be imported. The file should be within 50 MB.

5. Fill the area information in the template.

   Note

   Click **Field Description** to view the rules of filling the fields of the template.

6. Click Select to select the template of area information from the local disk.
7. Click **Import** to import the areas to the system.

3.4 Export Areas

You can export the areas to the local disk in CSV format in a batch. And you can view the area information on the local disk or send the area information to others.

Steps

1. Click → **System Configuration** → → **Security Area Management** to enter Security Area Management page.
2. Click the area name on the left panel to select the area to be exported.
3. Click to export the area and its subordinate areas.
4. Click **Export** in the prompt box.
5. Save the area information file.
   - Click **Save** to save the area information file to the default path: C:\Users\User Name \Downloads.
   - Click **Save as** to save the area information file to a path as your desire.

Chapter 4 Person Management

You can add person information to the system for further operations such as access control (adding the person to the person group), attendance management (setting a shift schedule for the person), parking management (setting the person as vehicle owner), visitor management (setting the person as a visitee). After adding the persons, you can edit and delete the person information if it is needed.

4.1 Organization Management

You can add organizations to manage the persons by classifications. E.g. You can add persons in the same department (e.g. human resource department) to an organization and name the organization as HR Dept. You can also export the organization information in CSV format to the local disk of the PC running the Web Client.

4.1.1 Add Single Organization

You can add organizations to the system one by one. After adding the organization, you can edit and delete the organization if needed.

Steps

1. Click → **System Configuration** → **Person, User, and Role** → **Person** to enter the Person page.
2. Select a parent organization on the left panel, and then click + to add a new organization.
3. Enter the organization name in the pop-up window.
4. **Optional:** Create an organization code in the pop-up window, which is used to identify the organization uniquely.
5. Click **OK**.
6. **Optional:** Perform the following operations after adding the organization.

Edit Organization Name	Select the organization name on the left panel, and then click on the left panel to edit the organization name.
Delete Organization	Select the organization name on the left panel, and then click on the left panel to delete the organization and its subordinate organizations.

Note

The persons added in the deleted organization(s) will be moved to the Deleted Person Information list. You can restore the deleted persons to other organizations. For details about restoring deleted persons, refer to ***Restore Deleted Persons*** .

View Person List of the Organization	Select the organization on the left panel, and then the persons of the organization are displayed in the Person List on the right panel. • Click to search the persons by different person features. • Check **Include Child Organization**, the persons of the child organization(s) are displayed in the Person List. Otherwise, only the persons of current organization are displayed.

4.1.2 Import Organizations in a Batch

You can add multiple organizations to the system in batch by filling the organizations' information to the template first.

Steps

1. Click → **System Configuration** → **Person, User, and Role** → **Person** to enter the Person page.
2. Select a parent organization on the left panel, and then click on the left panel to enter the Import Organization page.
3. Click **Download File Template** to download the template (CSV format) to the local disk of the PC running the Web Client.

   Note

   For one file, up to 50,000 records can be imported. The file should be within 50 MB.

4. Fill the organization information in the template.

   Note

   Click **Field Description** to view the rules of filling the fields of the template.

5. Click **Select** to select the template of organization information from the local disk.
6. Click **Import** to import the persons to the system.

4.1.3 Export Added Organizations

You can export the organization information to the local disk in CSV format by batch. And then you can view the organization and its subordinate organizations on the local disk or send the organization information to others.

Steps

1. Click → **System Configuration** → **Person, User, and Role** → **Person** to enter the Person page.
2. Select the organization need to be exported on the left panel, and then click on the left panel.
3. Click **OK** in the pop-up window.
4. Save the person information file.
   - Click **Save** to save the person information file to the path: C:\Users\User Name\Downloads.
   - Click **Save as** to save the person information file to a path as your desire.

Result

The organization and its subordinate organizations are exported in CSV format to the local disk of the PC running the Web Client.

4.1.4 Move Organization

If organization hierarchy changes (e.g., two departments of different hierarchy in your company become of the same hierarchy), you can drag the organizations in the organization tree to do corresponding adjustment.

Steps

1. Click on the Home page, and then go to **System Management → Person, User, and Role → Person** .
2. Click above the organization tree to open the Move Organization window.
3. Drag an organization to move it to a proper position.
4. Click **OK**.

4.2 Set Fields of Basic Person Information

By default, the system has predefined some basic person information fields (required or optional) which are displayed when adding persons. If you need to add other information fields, you can select the related fields according to actual needs.

Steps

1. Click **→ System Configuration → Person, User, and Role → Person** to enter the Person page.
2. Click on the upper-right corner of the page to enter the Basic Person Information Field Settings page.
3. **Optional:** Click **Custom Field** on the left panel to add custom fields as your desire.
4. Select the field(s) on the left panel to add the field(s) as basic person information on the right panel.
5. **Optional:** Check the field(s) on the right panel to set the field(s) as required field(s), which are required to be set when adding a person.

Note

By default, there are 6 fields on the right panel. Among them, Name, Gender, Organization and ID are required fields by default, while Employee No. and Mobile Phone No. are not required fields and can be checked to be set as required fields.

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

4.3 Set Parameters for Biometric Features Collection Device

Before adding persons, you need to set the parameters of biometric features for devices, including face recorder to collect the face picture of the persons, fingerprint recorder to collect the fingerprint information of the person, and ID card reader to read the ID card information.

Steps

1. Click → **System Configuration** → **Person** → **Basic Information** to enter the Basic Information page.
2. Click to enter the Biometric Feature Collection Device Settings page.
3. Set the parameters of face recorder.

   USB Camera

   Insert a USB camera to the USB interface of the PC running the Web Client to collect face pictures.

   Face Recognition Terminal

   Mount a face recognition terminal on a specified place to collect face pictures. You need to enter terminal's IP address, port No., user name and password to connect to the terminal.
4. Select one fingerprint recorder type from the drop-down list of Device Type.
5. Select one ID card reader type from the drop-down list of Device Type.
6. Click **Save** to save the settings.

4.4 Add Single Person

You can add person to the system one by one. After adding the persons, you can edit and delete the person information if needed.

Steps

1. Click → **System Configuration** → **Person** → **Basic Information** to enter the Basic Information page.
2. Click **Add** in the person list to enter the Add Person Information page.
3. Set the basic person information, including the default fields and the customized fields.

   For details about customizing the fields of basic person information, refer to ***Set Fields of Basic Person Information*** .
4. Perform one of the following operations to set the face picture.
   - Click **Upload** to upload the face picture from the local disk of the PC running the Web Client.

     Note

     The picture should be in JPG format, and the size should be between 10 KB and 20 KB.
   - Click **Collect** to collect the face picture by the webcam of the PC running the Web Client.

Note

Before collecting face pictures, you should download the HikCentral Enterprise-Commercial Plug-in to the local disk of the PC running the Web Client by clicking in the Home page to enter the download center.

5. Click **Add Fingerprint** to collect the person's fingerprint.

Note

Before collecting fingerprint information, make sure you have connected the fingerprint recorder to the PC running the Web Client and make sure you have set the right device type of fingerprint recorder in the system. For details about setting fingerprint recorder in the system, refer to ***Set Parameters for Biometric Features Collection Device*** .

6. Click **Save** to save the settings and add the person to the person list.
7. Perform the following operations after adding the person to the person list.

Set ID Photo	Click to set or change the ID photo for the person. **Note** The number behind represents the number of ID photos.
Set Fingerprint	Click to collect or change the fingerprint for the person. **Note** The number behind represents the number of fingerprints.
Edit Person	Click to edit the settings of the person.
Delete Person	Click in the Operation column to delete this person.
Delete Persons	Select multiple persons, and then click **Delete** to delete the selected persons in a batch. **Note** The deleted person(s) will be moved to the Deleted Person Information list. You can restore the person to the organization or delete the person thoroughly. For details, refer to ***Restore Deleted Persons*** .
Change Organization	Select the person(s), and then click **Change Organization** to move the person(s) to another organization.

4.5 Import Multiple Persons

You can import multiple persons to the system by filling the persons' information to the template first.

Steps

1. Click **System Configuration** → **Person** → **Basic Information** to enter the Basic Information page.
2. Click **Import** in the person list to enter the Import Person Information page.
3. Click **Download File Template** to download the template (CSV format) to the local disk of the PC running the Web Client.

   For one file, up to 50,000 records can be imported. The file should be within 50 MB.
4. Fill the person information in the template.

   Note

   Click **Field Description** to view the rules of filling the fields of the template.
5. Click **Select** to select the template of person information from the local disk.
6. Click **Import** to import the persons to the system.

4.6 Import Biometric Features from Collection Device

After recording biometric features (facial and fingerprint information) and registering person name by collection device (face recorder and fingerprint recorder), you can synchronize the biometric features to the system.

Steps

1. Click , and then go to **System Configuration** → **Person, User, and Role** → **Person** → **Biometric Feature Collection Device Settings** .
2. Select **Face Recorder** or **Fingerprint Recorder**.
3. Select device(s) and then click **Sync**.

   Note

   The synchronization of facial information takes a few minutes. Hence it is recommended that you synchronize facial information in batches based on different priority levels.

4.7 Export Added Persons

You can export a file with the person information to the local disk of the PC running the Web Client in CSV format, and then you can view the organization and its subordinate organizations on the local disk or send the organization information to others.

Steps

1. Click → **System Configuration** → **Person** → **Basic Information** to enter the Basic Information page.
2. Click the organization on the left panel to select the organization of the persons.
3. **Optional:** Click to filter out the persons to be exported and the persons will be displayed in the person list.
4. Click **Export** to export all the persons in the search result of the person list.
5. Click **OK** in the pop-up window.
6. Save the person information file.
   - Click **Save** to save the person information file to the default path: C:\Users\User Name \Downloads.
   - Click **Save as** to save the person information file to a path as your desire.

4.8 Restore Deleted Persons

Similar like the recycle bin of the computer, HikCentral Enterprise-Commercial provides a deleted person list to store the deleted persons and can be restored to the existing organizations, which helps you to avoid losing the deleted person information by mistake.

After you delete a person from the person list, the person is not deleted thoroughly from the system but is moved to the Deleted Person Information list. Perform the following operations to restore the deleted person.

Steps

1. Click → **System Configuration** → **Person** → **Basic Information** to enter the Basic Information page.
2. Click on the upper-right corner of the page to enter the Deleted Person Information page.
3. Perform one of the following operations to restore the deleted person(s).
   - Click in the Operation column to restore the person.
   - Select the persons to be restored, and then click **Restore** to restore the persons by batch.
4. In the Restore Person Information window, select organization for the restored person(s), and then click **OK**.
5. **Optional:** Delete the person(s) thoroughly from the system.
   - Click in the Operation column to delete the person.
   - Select the persons to be deleted, and then click **Delete** to delete the persons by batch.
6. **Optional:** Click in the Biometric Feature column to set or change the ID photo for the person.

   Note

   The number behind represents the number of ID photo of the person.

7. Click in the Biometric Feature to collect or change the fingerprint for the person.

   Note

   The number behind represents the number of fingerprint of the person.

Chapter 5 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 permissions to the user.

Note

Up to 10 roles can be assigned to one user.

5.1 Add Role

A role defines the user's access rights to the system resources. For example, the system administrator has all the configuration and management rights of the system. You can customize a role named operator to assign operation rights to it but not assign configuration rights to it. By role, you can manage the system flexibly.

Steps

Perform the following operations to add role and assign permissions to the role.

1. Click → **System Configuration** → **Person, User, and Role** → **Role** to enter the Role Management page.
2. Click **Add** in the role listto enter the Add Role page.
3. Set the role name and descriptions for this role.
4. Perform one of the following operations to set permissions for the role.
   - Click **Copy from** and select the pre-defined role to copy the permission settings of selected role to the role.
   - Assign permissions to the role.

     System Management Permission

     The management and configuration permissions of the Web Client.

     Management Menu Permission

     The Web Client's management menu permissions of different modules. The user with the role will get all the management and configuration menu permissions of the selected modules.

     Security Area Permission

     The Web Client’s management permissions of security areas. The role can view, manage, delete the selected areas, and add new areas under the selected areas

     Organization Permission

     The Web Client's management permissions of organizations. The role can view, manage, delete the selected organizations, and add new organizations under the selected organizations.

Application Permission

The application permissions of the clients.

Function Menu Permission

The client's application menu permissions of different modules. The user with the role will get all the application menu permissions of the selected modules.

Service Resource Permission

The application permissions for different resources. You need to select the area of the resources on the Resource Permission Range panel, and the operation items are displayed on the right panel.

Advanced Configuration for Every Device and Operation Item

If you want to assign specified operation items for specified devices, click **Advanced Configuration for Every Device and Operation Item** in the lower-right corner of Service Resource Permission page to configure. You need to save the role before entering the configuration page.

5. Click **Save** to save the settings and add the role to the role list.
6. **Optional:** Perform the following operations after adding the role:

Link User	Click in the Operation column to link the role with the existing users.
Edit Role	Click in the Operation column to edit the settings of this role.
Delete Role	Click in the Operation column to delete this role.
Delete Roles	Select multiple roles, and then click **Delete** to delete the roles.

5.2 Manage User Group

User group defines a group of users with the same attribute (e.g. department, operation rights), which helps you to manage the users conveniently. For example, you can create a user group named Operator Group 1 for the operators with the same permissions.

Steps

1. Click → **System Configuration** → **Person, User, and Role** → **User** to enter the User Management page.
2. Select the upper-level user group on the left panel, and then click to add a new user group.
3. Enter the user group name in the pop-up window, and then click **OK**.
4. **Optional:** Perform the following operations after adding the user group:

Edit Group Name	Select the group name on the left panel, and then click on the left panel to edit the group name.
Delete Group	Select the group name on the left panel, and then click on the left panel to delete the group and its sub-group and users.

Move Group Select the group name on the left panel, and then click ↑ or ↓ to move the organization up or down in the same parent organization.

5.3 Add Single User

User is the account that has the permission to login, configure, and operate the system. You can assign different roles to the users for granting different permissions to the users.

Steps

You can add user to system one by one and assign role to the user.

1. Click ☰ → **System Configuration** → **Person, User, and Role** → **User** to enter the User Management page.
2. Click **Add** in the user list to enter the Add User page.
3. Set the required parameters of basic information.

   User Name

   The user name.

   Password

   The password of the user.

   Confirm Password

   The same as the password.

   PTZ Control Permission

   PTZ Control Permission determines the priority of user's PTZ control requests. The user with higher permission level has the priority to control the PTZ unit. For example, when user1 and user2 control the PTZ unit at the same time, the user who has the higher PTZ control permission level will take the control of the PTZ movement.

   Description

   The descriptions about the user.
4. **Optional:** Click **Select** behind the **Person Name** to select a person as the user's linked real person.
5. **Optional:** Set the parameters of user security.

   Bind with IP Segment

   The user can only login the Web Client and Control Client on the computer whose IP address is within the specified IP address range to ensure the user security.

   Bind with MAC Address

   The user can only login the Control Client on the specified computer with the same MAC address to ensure the user security.
6. Search the existing role(s) in the search field of Role List to assign the role(s) to the user.

Note

The system provides a default role named system administrator, which has all permissions of the system.

7. Click **Save** to save the settings and add the user to the user list.
8. **Optional:** Perform the following operations after adding the normal user.

Reset Password	Click in the Operation column to reset password of this user. **Note** The admin user can reset the passwords of all the other users (except the Windows domain user). Other users with user management permission can reset the passwords of other users (except the Windows domain user and admin user).
Delete User(s)	Click in the Operation column to delete this user. Select multiple users and then click **Delete** to delete the users by batch.
Link Person	Click in the Operation column to link the user with the user's real person.
Edit User	Click to edit the settings of the user.
Disable User(s)	Click in the Operation column to disable this user. Select multiple users, and then click **Disable** to disable the users in a batch. After disabled, the user cannot log into the clients.
Enable User(s)	Click in the Operation column to enable this user. Select multiple users, and then click **Enable** to enable the users in a batch. After enabled, the user can log into the clients. The newly added users are enabled by default.

Note

The administrator user named admin was pre-defined by default. It cannot be edited, deleted and disabled.

5.4 Import Multiple Users

You can import multiple users to access the system and assign roles to the users.

Steps

1. Click → **System Configuration** → **Person, User, and Role** → **User** to enter the User Management page.
2. Click the group name on the left panel to select it as the target user group of the importing users.
3. Click **Import User** on the right panel to enter the Import User page.
4. Click **Download File Template** to download the template (CSV format) to the local disk.

Note

For one file, up to 50,000 records can be imported. The file should be within 50 MB.

5. Fill the user information in the template. Note:

Note

Click **Field Description** to view the rules of filling the fields of the template.

6. Click **Select** to select the template of user information from the local disk.
7. Enter the users' password and confirm the password.
8. Click **Import** to import the users to the system.

5.5 Synchronize Users from Windows Domain

You can synchronize users from the windows domain in a batch to the system and assign roles to the domain users. If you have the Windows domain server which contains the information (e.g., user data, computer information), you can add the users that belong to an organization unit (e.g., a department of your company) to HikCentral Enterprise-Commercial by synchronizing them from Windows domain and assign roles for the users.

Steps

1. Click → **System Configuration** → **Person, User, and Role** → **User** to enter the User Management page.
2. Click **Sync User from Windows Domain** to enter the Sync User from Windows Domain page.
3. Set the required parameters.

   Domain Server IP Address

   The IP address of domain server.

   Port No.

   The port number of account service. The default number is 389.

   Domain User Name

   A user with the permission of viewing Windows domain users.

   Domain Password

   Domain password is only used for platform connection, and will not be saved.
4. Click **Next**.
5. Select the domain users on the left panel, and then add them to the right panel as selected users.
6. Click **Save** to save the settings.

5.6 Export Users

You can export a file with user information to the local disk of the PC running the Web Client in CSV format, and then you can view the user information on the local disk or send the user information to others.

Steps

1. Click → **System Configuration** → **Person, User, and Role** → **User** to enter the User Management page.
2. Click the organization on the left panel to select the organization to be exported
3. **Optional:** Click to search the users to be exported, and then the users will be displayed in the user list.
4. Click **Export User** to export all the users in the search result of the user list.
5. Click **Export** in the prompt box.
6. Save the user information file.
   - Click **Save** to save the user information file to the default path: C:\Users\User Name \Downloads.
   - Click **Save as** to save the user information file to a path as your desire.

Chapter 6 Vehicle Management

Registered vehicles refer to the vehicles in whitelist, which are allowed to enter the parking lots and park in the parking spaces. The process of adding vehicles to the vehicle list in the system is called "registration".

The registered vehicles can park in the parking lots after buying a monthly pass or annual pass. With the parking pass, the vehicle is not required to pay parking fee when exiting or entering the parking lots.

6.1 Register a Vehicle to HikCentral Enterprise-Commercial

You can add a vehicle to the system and register its detailed information so that it will be authorized to pass when entering or exiting the parking lot if the recognized license plate number matches the one in the whitelist.

Steps

1. Click → **System Configuration** → **Vehicles** , or click **Parking** on the Home page and enter **Vehicles and Cards**.
2. Click **Add**.
3. Enter the vehicle information.

   License Plate Number

   Enter the license plate number of a vehicle, which is unique. It should contain 1 to 16 characters and special characters are not allowed.

   Vehicle Owner Name

   Click **Select** to select the vehicle owner from the added persons. For configuring persons, refer to ***Person Management*** .

6.2 Import Vehicles in a Batch

You can also register multiple vehicles to the system in a batch by importing a CSV file with vehicle information.

Steps

1. Click → **System Configuration** → **Vehicle** .
2. Click **Import**.
3. Click **Download File Template** to download a template file in CSV format.
4. Enter the vehicle information in the template.

   You can hover the cursor on **Field Description** to view the descriptions of different fields in the template.

Note

Up to 50,000 records can be imported. The file size should be within 50 MB.

5. Click **Select** and select the template file filled with vehicle information.
6. Click **Import** to start.

6.3 Export Registered Vehicles

If you need to back up the vehicle information registered on the system, you need to export them and

Steps

1. Click → **System Configuration** → **Vehicle** .
2. Click **Export**.
3. Click **OK** in the pop-up window to confirm the export and a CSV file with all the vehicle information in the system will be downloaded and stored in the PC running the Web Client.

Note

The default saving path is C:\Users\User Name\Downloads.

Chapter 7 Card Issuing

For businesses (such as access control, parking lot, and elevator control) that use cards in the system, you need issue cards to persons in the Card Issuing module.

7.1 Encrypt Mifare Card or Not

If the cards you use are Mifare cards, you should determine if encrypt the cards or not first before issuing cards.

Note

After enabling or disabling the Mifare card encryption function, this function cannot be changed.

Click **Card Issuing** on the Home page, and then determine whether to encrypt the cards according to the prompts on the pop-up window.

You can click **Ignore** on the pop-up window if no Mifare cards are used.

7.2 Set Card Issuing Parameters

HikCentral Enterprise-Commercial provides two modes for reading a card's number: reading card number by card enrollment station and entering the card number manually. If a card enrollment station is available, connect it to the PC running the Web Client, and then place the card on the card enrollment station to read the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

Steps

1. Click **Card** on the Home page and enter **Set Card Issuing Parameters**.
2. Set the card issuing parameters.

   Device Type

   The type of card enrollment station.

   Mifare Card Sector Encryption

   After enabling this function, the card will be encrypted.

   Connection Mode:

   The mode in which the enrollment station connects the PC running the Web Client.

   Reading Frequency

   The card enrollment's frequency of reading card information.

   Card Enrollment Method

   Serial number or customized card number.

Card Type

10-bit card number or 8-bit card number.

3. Click **Save** to save the settings.

7.3 Write to Card

For some scenes with high security requirements and the cards (CPU card and long range card) need to be encrypted, you can write card number to the card by encryption, and then the card is encrypted, whose card number is read as garbage characters.

Before You Start

Connect the card enrollment station to the PC running the Web Client.

Steps

Note

Long range card can only be written in Windows 10.

1. Click **Card** on the Home page and then click **Write to Card** to enter the Write to Card page.
2. Select card enrollment method.

Serial No.

Read serial number of the card and write it as card number to the card.

Custom

Write customized card number to the card.

Note

Enter start card number if you select the card enrollment method as custom, and then the card number can be written to cards incrementally by 1 on the basis, which helps you to save time for entering card number one by one. You only need to place cards on the enrollment station and click **Write to Card** one by one. For example, you entered 12345678 as the start card number, the first card put on the card enrollment station will be written as 12345678 after you click **Write to Card**, and the second card put on the card enrollment station will be written as 12345679 after you click **Write to Card** again.

3. Place the card on the card enrollment station.
4. Click **Write to Card**.

The card writing result will be displayed in the panel of Card Writing Result Details.

7.4 Issue Card to Person

You can issue one or more cards for one person. After bound, the card can be used as the access credentials of the persons for access points and parking lot, and the access records (swapping card

time) can be used for attendance record, etc. As a result, a person can use only one card to make use of multiple subsystems.

Steps

Note

For issuing cards to multiple persons simultaneously, you can only issue one card for one person. For issuing cards to one person, you can issue multiple cards for the person.

1. Click **Card** on the Home page to enter the Card Issuing page.
2. Click **Issue Card for Person**.
3. On the left panel, select the organization whose person needs to be issued card.
   The persons of the organization are all displayed on the right panel.
4. Click to search the person(s) need(s) to be issued card.
5. Select the person(s) need to be issued card.
6. Click **Issue Card** to enter the Issue Card page.
7. Enter the validity date. The card will take effect within the validity period, and be disabled after the validity date.
8. Enter the card number in the field of Card No. or place the card on the card enrollment station to read card number.
9. If the reader authentication mode includes password authentication, enter the card password in the field of Card Password.
10. Click **Save** to save the settings.
11. Perform the following operations after issuing card to the person.

    View Card Information

    Click in the Operation column to view the card information of this person.

    Issue More Cards

    Click **Issue Card** to issue more card(s) to the person.

    Edit Card

    Click in the Operation column to edit the card information.

    View Person Details

    Click to view the person details, including person basic information and fingerprint information.

7.5 Enable Virtual Card

Virtual card mode is applicable to the scenarios in which physical cards are not required by special personnel. When the virtual card mode is enabled, the system will automatically generate a virtual card (10-integer card number) by default for each person who doesn't have physical card(s). And the virtual card is linked to the facial and fingerprint information of the person by default.

Click **Card Issuing** on the Home page, and then click **Card Issuing Settings** to enter the Card Issuing Settings page.

On the page, you can set the **Virtual Card** to on to generate a virtual card(s) for each person who doesn't have physical card(s). And by clicking **Clear Virtual Card** on the upper-right, you can clear all the virtual cards of the system.

7.6 Card Operation

On the page of Operate Card, you can batch import cards and batch issue the cards. You can also report card loss, return card or replace the card.

7.6.1 Import Cards

You can import cards by batch.

Steps

1. Click **Card** on the Home page to enter the Card Issuing page.
2. Click **Card Operation**.

   All the cards of the system will be displayed in the Card List.
3. Click **Import** to enter the Import Card page.
4. Click **Download File Template** to download the template (CSV format) to the local disk.

   Note

   For one file, up to 50,000 records can be imported. The file should be within 50 MB.
5. Fill the cards information in the template.

   Note

   Click **Field Description** to view the rules about filling the fields of the template.
6. Click **Select** to select the completed template from the local disk.
7. Click **Import**.

7.6.2 Report Card Loss

If the person lost his/her card, you can report the card loss so that the related card permission will be deleted.

Steps

1. Click **Card** on the Home page to enter the Card Issuing page.
2. Click **Card Operation**.

   All the cards of the system will be displayed in the Card List.

3. Place the card on the card enrollment station or enter the card number in the search field on the upper-right corner to search the card(s) to be reported as card loss.
4. Click in the Operation column to report card loss, which will freeze the permission of this card.

Note

You can also report card loss on the Issue Card for Person page by clicking to search the person who owns the card, and then click to enter the Card Information page, and then click in the Operation column to report card loss, which will freeze the permission of this card.

7.6.3 Return Card

When the person is resigned, changes the position or some other reasons that need to cancel the permission of the card, you can return the card.

Steps

1. Click **Card** on the Home page to enter the Card Issuing page.
2. Click **Card Operation**.

   All the cards of the system will be displayed in the Card List.
3. Place the card on the card enrollment station to enter the card number in the search filed.
4. Click in the Operation column to return this card, which will unbound the card from the person and delete all the permissions of the card.

Note

You can also return card on the Issue Card for Person page by clicking to search the person who owns the card, and then click to enter the Card Information page, and then click in the Operation column to return this card, which will unbound the card from the person and delete all the permissions of the card.

7.6.4 Replace Card

When the card is broken or not applicable caused by other reasons, you can replace this card.

Steps

1. Click **Card** on the Home page to enter the Card Issuing page.
2. Click **Card Operation**.

   All the cards of the system will be displayed in the Card List.
3. Place the card on the card enrollment station to enter the card number in the search filed.
4. Click in the Operation column to replace this card, which will replace and delete the original card permission with the new card permission.

Note

You can also replace card on the Issue Card for Person page by filtering out the person who owns the card and click to enter the Card Information page, and then click in the Operation column to replace this card, which will replace and delete the original card permission with new card permission.

7.6.5 Link Fingerprint with Card

When the basic information of a person contains his/her fingerprint information, you can link the fingerprint information with one of the cards issued to him/her. After that, he/she can pass through access control devices by fingerprint identification (if supported by the access control points).

Before You Start

You should have linked the person with his/her fingerprint information.

Steps

Note

For some access control devices, the fingerprint information can only be applied to device when the fingerprint information is linked with card.

1. Click **Card Issuing** on the Home page.
2. Search persons.
   1) Set the search conditions, including name, gender, organization, biometric feature, number of cards.
   2) Click **Search**.

   The target person will be displayed.
3. Click in the Operation column to view all the card(s) issued to the person.
4. Select a card and then click in the Fingerprint column to link the fingerprint to the card.

Note

- If only one card is issued to a person, manually link fingerprint to the card is not required. The person's fingerprint will be automatically linked to the card.
- If multiple cards are issued to a person, the first issued card will be automatically linked with the person's fingerprint. You can manually link the fingerprint to another card issued to the person.
- If multiple cards are issued to a person, when the card linked with the person's fingerprint is canceled or lost, the fingerprint will be linked to next card issued to him/her.

7.6.6 Link Face Picture with Card

When the basic information of a person contains his/her face picture, you can link the face picture with the card issued to him/her. After that, the person can get through access control points by facial identification (if supported by the access control points).

Before You Start
You should have linked the person with his/her face picture.

Steps

Note
For some access control devices, the face picture information can only be applied to device when the face picture is linked with card.

1. Click **Card Issuing** on the Home page.
2. Search persons.
   1) Set the search conditions, including name, gender, organization, biometric feature, number of cards.
   2) Click **Search**.

   The target person will be displayed.
3. Click in the Operation column to view all the card(s) issued to the person.
4. Select a card and then click in the Face Picture column to link the face picture to the card.

Note
- If only one card is issued to a person, manually link face picture to the card is not required. The person's face picture will be automatically linked to the card.
- If multiple cards are issued to a person, the first issued card will be automatically linked with the person's face picture. You can manually link the face picture to another card issued to the person.
- If multiple cards are issued to a person, when the card linked with the person's face picture is canceled or lost, the face picture will be linked to next card issued to him/her.

Chapter 8 Video Surveillance

Video surveillance centers on security surveillance by video-related functions. You can perform real-time monitoring and view videos or pictures to know what happened at the monitored place by managing encoding devices, making recording schedule and capture schedule, etc.

Video surveillance covers multiple functions including live view, playback, and viewing captured pictures, which greatly helps people improve safety management.

- Live View: you can view the live video of the added network cameras and video encoders for a real-time watching of the monitored place. And some basic operations are supported, including picture capturing, manual recording, window division, PTZ control, etc. With PTZ cameras, you will be able to view live view in a 360° view for details.
- Playback: you can view what happened through recorded videos saved in devices or central storage devices when an event or alarm was triggered for analysis and judgment after recording according to a recording schedule.
- Picture Search: captured pictures helps to see details of an event and is useful for saving bandwidth and memory. The captured pictures can be saved in your computer for archiving.

8.1 Flow Chart

If this is the first time you use video surveillance, we recommend you perform configurations according to the chart below.

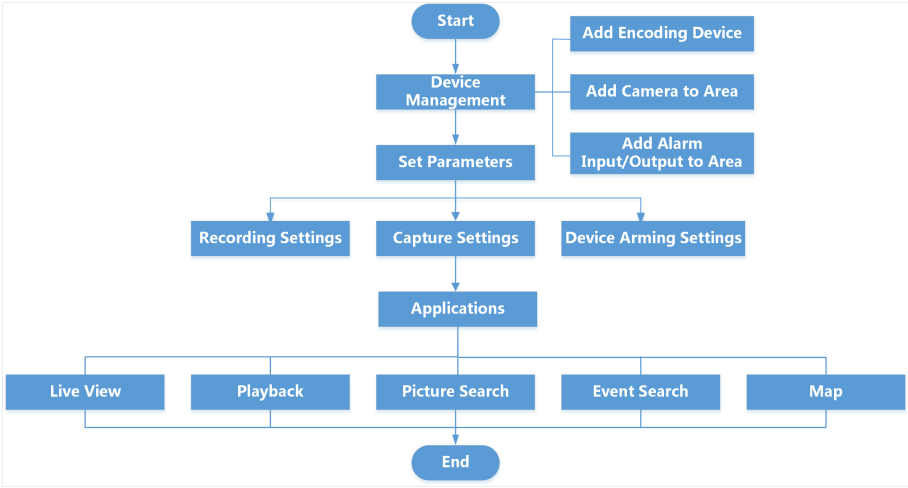


Figure 8-1 Operation Flow Chart

8.2 Encoding Device Management

For video surveillance purpose, you can add encoding devices, such as network camera (IPC), network video recorder (NVR), digital video recorder (DVR), and hybrid digital video recorder (HDVR), to the system.

Encoding devices can be added to HikCentral Enterprise-Commercial via the following protocols:

Hikvision Device Network SDK Protocol

Encoding devices using this protocol are produced by Hikvision with fixed IP address.

Dahua Device Network SDK Protocol

Encoding devices using this protocol are produced by Dahua with fixed IP address.

Hikvision EHome Protocol

Encoding devices using this protocol are produced by Hikvision. The protocol is suitable for countries or regions short of IP addresses that cannot allocate an IP address for each device. Devices with both fixed IP address and dynamic IP address can register to the system via this protocol.

ONVIF Protocol

Open industry standard established in Open Network Video Interface Forum. Encoding devices using this protocol are produced by other manufacturers.

Hikvision ISUP5.0 Protocol

Used for communication according to the Hikvision ISUP5.0 Protocol. Fixed IP, dynamic IP devices, and devices with no special requirements in terms of networking environments can use this protocol to actively register on the platform.

You can add the encoding devices to the system for live view, video recording, and event settings, etc.

8.2.1 Add an Encoding Device by IP Address

When you know the IP address of the encoding device to be added, you can add the encoding device to your system by specifying the IP address, user name, password, and other related parameters.

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 encoding devices to HikCentral Enterprise-Commercial via network.
- Make sure the time zone and time of the encoding devices are the same as those of the CMS server.

Steps

Encoding devices connected via Hikvision EHome Protocol and Hikvision ISUP5.0 Protocol cannot be added to the system by IP address. For details about adding encoding devices by EHome Protocol, refer to ***Add Encoding Devices by EHome Protocol*** .

1. Click → **System Configuration** → **Devices** → **Video Surveillance** to enter the Video Surveillance page.
2. Select an area in the area list to add the encoding device.
3. Click **Encoding Device** to enter the encoding device page, and click **Add** to enter the Add Encoding Device page.
4. Select the access protocol from the drop-down list.
5. Select **Single** from IP Address as the adding mode.
6. Set the parameters for the encoding device, including IP address, port No., device name, user name, password, domain, description, etc.

   IP Address

   Enter the IP address of the encoding device.

   Port No.

   Enter the device port No.

   Device Name

   Customize a name for the encoding device.

   User Name

   Enter the user name of the encoding device. By default, the user name is admin.

   Password

   Enter the password of the encoding device.

   Caution

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including 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.

   Domain

   Select the network domain that the encoding device belongs to from the drop-down list.

   Note

   .

Note

For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

Description

Enter the custom description.

7. Click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the encoding device and test again.

8. Click **Save** to add the encoding device.
9. Perform the following operation(s) after adding the encoding device.

Search Device	Check **Devices Never Connected**, **Include Child Area**, or set the conditions (e.g., device name, IP address, device ID, etc.) to filter the encoding devices by specific conditions.
	Note Devices Never Connected indicates that the encoding devices have never been connected to HikCentral Enterprise-Commercial since they are added to the system. This condition is used to filter encoding devices with user name or password exception.
Edit Device	Click to edit the device information, including device name, user name, password, etc.
Delete Device	Click to delete the encoding device. You can also select multiple devices and click **Delete** to delete devices in a batch.
	Note If you delete an encoding device, all the information linked to the device will be deleted, such as recording and capture schedule, alarm linkage, etc. As a result, you may lose videos, pictures, and alarms related to the device.
View Device Details	Click to view the detailed information of the device, such as device serial No., password strength, linked devices, etc.
Configure Parameters	Click to configure network parameter for the encoding device. Currently you can only configure multi-cast address for the device to forward video stream and lower the load of the device.
Change Area	Select one or more devices and click **Move** to change the area for the device(s).

Get Device Information	Select one or more devices and click **Sync** to get device information (such as device name, device serial No., etc.) from the encoding device(s) to the system.
Export All Devices	Click **Export Device** to export information of all the added encoding devices in a CSV file.

8.2.2 Add Encoding Devices by IP Segment

If the encoding devices have the same port No., user name and password, and their IP addresses are within 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 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 encoding devices to HikCentral Enterprise-Commercial via network.
- Make sure the time zone and time of the encoding devices are the same as those of the CMS server.

Steps

1. Click → **System Configuration** → **Devices** → **Video Surveillance** to enter the Video Surveillance page.
2. Select an area in the area list to add the encoding devices.
3. Click **Encoding Device** to enter the encoding device page, and click **Add** to enter the Add Encoding Device page.
4. Select the access protocol from the drop-down list, and select **IP Segment** from IP Address as the adding mode.
5. Set the parameters for the encoding devices, including IP addresses, port No., user name, password, network, intelligent capability, panoramic capability, and description.

   IP Address

   Enter the start IP address and the end IP address to add the encoding devices which have the IP addresses between them.

   Port No.

   The devices to be added should have the same port No.

   User Name

   Enter the user name of the encoding devices. By default, the user name is ***admin***.

   Password

   Enter the password of the encoding devices.

Caution

The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including 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.

Domain

Select the network domain that the encoding devices belong to from the drop-down list.

Note

For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

Description

Enter the custom description.

6. Click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the encoding device and test again.

7. Click **Save** to add the encoding devices.
8. You can perform the following operation(s) after adding the encoding devices.

Search Device	Check **Devices Never Connected** or **Include Sub-Area** to filter the devices. Set search conditions, and click **Search** to search the devices as required. **Note** Devices Never Connected indicates that the encoding devices have never been connected to HikCentral Enterprise-Commercial since they are added to the system. This condition is used to filter encoding devices with user name or password exception.
Edit Device	Click to edit the device information, including device name, user name, password, etc.
Delete Device	Click to delete the device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete an encoding device, all the information linked to the device will be deleted, such as recording and capture schedule, alarm linkage, etc. As a result, you may lose videos, pictures, and alarms related to the device.

View Device Details	Click to view the detailed information of the device, such as device serial No., password strength, linked devices, etc.
Configure Parameters	Click to configure network parameter for the encoding device. Currently you can only configure multicast address for the device. Currently you can only configure multicast address for the device to forward video stream and lower the load of the device.
Change Area	Select one or more devices and click **Move** to change the area for the device(s).
Get Device Information	Select one or more devices and click **Sync** to get device information (such as device name, device serial No., etc.) from the encoding device(s) to the system.
Export All Devices	Click **Export Device** to export information of all the added encoding devices in a CSV file.

8.2.3 Add Encoding Devices by EHome Protocol

Hikvision EHome protocol can realize the communication between the system and Hikvision mobile devices (such as body camera, MNVR, etc.) with dynamic IP addresses. The protocol is suitable for countries or regions short of IP addresses that cannot allocate an IP address for each device. You can add the encoding device connected via EHome protocol to the system by specifying device No., network and other parameters.

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 encoding devices to HikCentral Enterprise-Commercial via network.
- Make sure you have configured the platform access mode as EHome on the encoding devices to be added.
- Make sure the time zone and time of the encoding devices are the same as those of the CMS server.

Steps

1. Click → **System Configuration** → **Devices** → **Video Surveillance** to enter the Video Surveillance page.
2. Select an area in the area list to add the encoding devices.

3. Click **Encoding Device** to enter the encoding device page, and click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision EHome Protocol** from Access Protocol drop-down list as the access protocol.
5. Click **Single** to set device No. and device name for an encoding device, or click **Batch** to set device No. for each encoding device.

   Device No.

   Enter the unique device No. of the encoding device. The device No. should be the same with that entered in the device. For batch adding, you can also click **Add No.** to set device No. for multiple encoding devices.

   Device Name

   For single adding, customize a name for the encoding device.
6. Set other parameters, such as domain and description.

   Domain

   Select the network domain that the encoding devices belong to from the drop-down list.

   Note

   For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

   Description

   Enter the custom description.
7. Click **Save** to add the encoding device(s).
8. Perform the following operation(s) after adding the encoding device.

Search Device	Check **Devices Never Connected** or **Include Child Area** to filter the devices, or click to filter encoding devices by specific conditions.
	Note Devices Never Connected indicates that the encoding devices have never been connected to HikCentral Enterprise-Commercial since they are added to the system. This condition is used to filter encoding devices with user name or password exception.
Edit Device	Click to edit the device information, including device name, user name, password, etc.
	Caution The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters,

	including 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.
Delete Device	Click to delete the device. You can also select multiple devices and click **Delete** to delete devices in a batch. **Note** If you delete an encoding device, all the information linked to the device will be deleted, such as recording and capture schedule, alarm linkage, etc. As a result, you may lose videos, pictures, and alarms related to the device.
View Device Details	Click to view the detailed information of the device, such as device serial No., password strength, linked devices, etc.
Configure Parameters	Click to configure network parameter for the encoding device. Currently you can only configure multi-cast address for the device to forward video stream and lower the load of the device.
Change Area	Select one or more devices and click **Move** to change the area for the device(s).
Get Device Information	Select one or more devices and click **Sync** to get device information (such as device name, device serial No., etc.) from the encoding device(s) to the system.
Export All Devices	Click **Export Device** to export information of all the added encoding devices in a CSV file.

8.2.4 Add Encoding Devices by ISUP 5.0 Protocol

For devices that have no fixed IP addresses, you can enable ISUP 5.0 Protocol for the device and register the device to the platform by entering the platform's IP address on the device configuration page.

Before You Start

- Make sure the device is correctly installed and connected to the network.
- Make sure you have enabled ISUP5.0 protocol and registered the device to the platform on the device configuration page.

Steps

1. Click → **System Configuration** → **Devices** → **Video Surveillance** .
2. Select an area in the area list.

3. Click **Encoding Device** tab.
4. Click **Add** to enter the Add Encoding Device page.
5. Select **Hikvision ISUP5.0 Protocol** as the access protocol.
6. Enter the device parameters.

   Device Name

   You can customize a device name according to its location or features.

   Device No.

   Log into the device configuration page to get it.

   Verification Code

   Log into the device configuration page to get it.

   Domain

   Select the device's domain.
7. Click **Save** to add the device.
8. Perform the following operations.

Operation	Description
Edit Device Information	Click to edit device parameters.
Delete Device	Click to delete an added device.
View Device Details	Click to view a device's access information, version information, channels, and linked devices, and edit network parameter.

8.2.5 Add Encoding Device Registered to the System

For ISUP5.0 devices, you can enter the platform's IP address on the configuration page of the device via a web browser, and then search online ISUP5.0 devices by the platform and add the searched devices to the platform.

Before You Start

- Make sure you have configured the platform's IP address for the device on by a web browser. See the device user manual for details.
- Make sure you have enabled ISUP5.0 protocol on the device configuration page.

Steps

1. Click in the upper-right corner, and then click **System Configuration → Devices → Video Surveillance → Encoding Device** .
2. Select an area in the area list to add online device to.
3. Click **Online Devices**.

   The platform will search online ISUP5.0 devices and the searched devices with detailed information will be displayed.

4. Enter verification code and check devices to be added, and then click **Save**.

8.2.6 Import Encoding Devices in a Batch

When there are multiple devices to be added to HikCentral Enterprise-Commercial, you can enter the device details in the predefined template to add them at a time for convenience.

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 encoding devices to HikCentral Enterprise-Commercial via network.
- Make sure the time zone and time of the encoding devices are the same as those of the CMS server.

Steps

1. Click → **System Configuration** → **Devices** → **Video Surveillance** to enter the Video Surveillance page.
2. Select an area in the area list to add the encoding devices.
3. Click **Encoding Device** tab to enter the encoding device page, and click **Import Device** to enter the Import Device page.
4. Click **Download File Template** and save the predefined template (CSV file) on your computer.
5. Open the exported template file, enter the required information of the encoding devices to be added on the corresponding columns, and then save the CSV file.
6. Click to select the template file.

   The imported file will be verified automatically to check whether the device information format is correct.
7. Click **Import** to import the encoding devices.
8. Perform the following operation(s) after adding the encoding device.

Search Device	Check **Devices Never Connected** or **Include Child Area** to filter the devices, or click to filter encoding devices by specific conditions.
	Note Devices Never Connected indicates that the encoding devices have never been connected to HikCentral Enterprise-Commercial since they are added to the system. This condition is used to filter encoding devices with user name or password exception.
Edit Device	Click to edit the device information, including device name, user name, password, etc.

Caution

The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including 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.

Delete Device	Click to delete the device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete an encoding device, all the information linked to the device will be deleted, such as recording and capture schedule, alarm linkage, etc. As a result, you may lose videos, pictures, and alarms related to the device.

View Device Details	Click to view the detailed information of the device, such as device serial No., password strength, linked devices, etc.
Configure Parameters	Click to configure network parameter for the encoding device. Currently you can only configure multi-cast address for the device to forward video stream and lower the load of the device.
Change Area	Select one or more devices and click **Move** to change the area for the device(s).
Get Device Information	Select one or more devices and click **Sync** to get device information (such as device name, device serial No., etc.) from the encoding device(s) to the system.
Export All Devices	Click **Export Device** to export information of all the added encoding devices in a CSV file.

8.2.7 Add Camera to Area

After adding encoding devices to the system, the camera linked to the encoding device should be added to an area for operation and management.

Steps

1. Click → **System Configuration** → **Devices** → **Video Surveillance** to enter the Video Surveillance page.
2. Select an area in the area list, and click **Camera** to enter the camera page.

3. Click **Add** to enter the Add Camera page.
4. Select the area in the Device Area list.

   All linked cameras in the area will be listed in the Cameras to be Added list.
5. Select the camera(s) you want to add in the Cameras to be Added list, and click > to add to the Added Cameras list.
6. Click **Save**.
7. Perform the following operation(s) after adding the cameras.

Search Device Check **Include Sub-Area** to filter the cameras, or set the conditions (e.g., camera name, device name, IP address, etc.) to filter cameras by specific conditions.

Edit Device Click to edit the device information, including basic information and location information.

Camera Name

Enter the camera name. The camera name can be applied or synchronized to the camera.

Camera Type

Select the appearance type of the camera, including box camera, dome camera, speed camera, and PTZ. Different cameras will be displayed with different icons in the camera list during live view and playback.

Connection Protocol

The network protocol used for the system to get stream from the camera, including TCP and UDP. It is recommended to use TCP when the network is in good condition, and use UDP when the network is in poor condition.

Camera ID for Keyboard

Enter an integer as the camera ID for displaying its video on video wall by entering the camera ID on the connected keyboard.

Location Label

Select a label for the camera according to the actual location.

Description

Enter the custom description.

Longitude, Latitude and Altitude

Enter the actual installation location of the camera.

Delete Device Click to delete the camera, or select multiple cameras and click **Delete** to delete cameras in a batch.

Note

If you delete a camera, all the information linked to the device will be deleted, such as recording and capture schedule, alarm linkage, etc. As a result, you may lose videos, pictures, and alarms related to the device.

Configure Parameters

Click to configure video display and alarm event detections for the camera.

OSD (On-Screen Display) Settings

Set the date, time or channel information you want to display on the video. You can drag to adjust the position.

Text Overlay

Add the custom text you want to overlay on the video, and you can also drag the text to adjust the position.

Video Parameter

Set the stream type, resolution, bitrate type, and frame rate for the video.

Privacy Mask

Draw an area to protect personal privacy from displaying on the video.

Video Tampering Alarm

A video tampering alarm is triggered when the camera is covered and the monitoring area cannot be viewed. You can draw an area for the arming region, set the tampering alarm sensitivity, and reset arming time to all-day.

Motion Detection Alarm

A motion detection alarm is triggered when the camera detects motion within its defined area. You can draw an area for the arming region, set the motion detection sensitivity, and reset arming time to all-day.

Note

You cannot configure parameters for video display and event detections for cameras connected via ONVIF protocol on the Web Client. You should configure those cameras on the devices.

Change Area

Select one or more cameras and click **Move** to change the area for the camera(s).

Get Device Information:

Select one or more cameras and click **Sync** to get device information (such as device name, channel No., etc.) from the cameras to the system.

Note

Device names cannot be synchronized to cameras connected via ONVIF protocol.

Adjust Cameras' Order	Click **Adjust Order** and drag camera to desired order in the area.
Export Cameras	Click **Export Camera** to export information of all the added cameras in a CSV file.

8.2.8 Add Alarm Input/Output to Area

Video surveillance devices usually support alarm inputs and alarm outputs which are collectively called alarm devices. Alarm inputs can be connected to detectors, such as smoke detector, temperature detector, motion detector, etc., to detect various alarm events. When the alarm or event linked with the alarm outputs is triggered, the alarm devices (such as siren, alarm lamp, etc.) connected with alarm outputs will take actions. The alarm devices can be added to the system for receiving alarm inputs, and managing alarm outputs manually or automatically.

Steps

Note

This user manual only introduces configurations and operations on HikCentral Enterprise-Commercial web client. For details about connecting alarm inputs to detectors and connecting alarm outputs to alarm devices, refer to the user manual of the device.

1. Click → **System Configuration** → **Devices** → **Video Surveillance** to enter the Video Surveillance page.
2. Select an area in the area list to manage alarm devices.
3. Click **Alarm Device** to enter the alarm device page, and click **Add** to enter the Add Alarm Device page.
4. Select the area in the Device Area list.

   All linked alarm devices in the area will be listed in the Alarm Devices to be Added list.
5. Select the alarm device(s) you want to add in the Alarm Devices to be Added list, and click **>** to add to the Added Alarm Devices list.
6. Click **Save**.
7. Perform the following operation(s) after adding the alarm devices.

Search Device	Check **Include Sub-Area** to filter the alarm devices, or set conditions (e.g., alarm device name, device name, IP address, etc.) and click **Search** to filter alarm devices by specific conditions.

Edit Device	Click to edit the alarm device information, including alarm device name, location information, etc.
Delete Device	Click to delete the alarm device, or select multiple alarm devices and click **Delete** to delete alarm devices in a batch.
	Note If you delete an alarm device, all the information linked to the device will be deleted, such as alarm linkage and so on. As a result, you may lose alarms related to the device.
Change Area	Select one or more alarm devices, and click **Move** to change the area for the alarm device(s).
Export All Devices	Click **Export Alarm Device** to export information of all the added alarm devices in a CSV file.

8.3 Recording Settings

Playback helps you find what happened when an alarm or event is triggered. Playback requires the device to record after configuring a recording schedule for the device. The recorded files can be saved in devices (including DVR, NVR, SD card, and camera HDD) or central storage (including HybridSAN and cloud storage server).

8.3.1 Configure Encoding Device Storage

The video files can be stored on the local storage (e.g., SD card or disk of the camera), and can be stored on the DVR or NVR.

Before You Start

Before setting recording schedule for the devices on the HikCentral Enterprise-Commercial, you need to log into the encoding device's web configuration page to configure local storage space for the device.

Steps

1. Install SD card or disk according to the device's installation manual.
2. Log into the device's web configuration page (Usually it is ***http://device IP address.***).
3. Click **Configuration → Storage → Storage Management** .
4. Select the disk in the disk list, and then click **Format**.

Note

The newly installed disk needs to be formatted for first use to make the status become Normal. For Non-Hikvision devices' disk installation and configuration, refer to the devices' installation and configuration manual to configure the storage location on the device.

5. Click **Save** to save the settings on the device.

8.3.2 Configure Central Storage

The video files can be stored on the Hybrid SAN, cloud storage server, and ASW. You need to login into the Operation and Management Center to add and configure the storage.

Usually, the IP address of Operation and Management Center is ***http://CMS server's IP address: 8001/center***.

For details about configuring Hybrid SAN, cloud storage, and ASW (storage access component), refer to *User Manual of Operation and Management Center*.

8.3.3 Configure Recording Schedule

After setting the recording schedule template, you can use the template to define when and how the recording starts and configure where the video files are stored for different cameras.

Steps

1. Click → **System Configuration** → **Video Surveillance** → **Recording Schedule** .
2. Select the area name on the left panel, and all the devices of the area will be displayed on the right panel.
3. Click in the Operation column to open the Recording Schedule page.
4. Enable **Device Storage**, and then configure the parameters on the Device Storage page. The descriptions of the parameters are as follows.

Note

Device storage refers to storing video files on the encoding device (e.g., SD card or disk of the encoding device). Before enabling this function, configure storage space for the encoding device. For details, refer to ***Configure Encoding Device Storage*** .

Stream Type

The stream type of video recording.

Main Stream

High definition. The video file will occupy more storage resources. It is suitable for the condition that the bandwidth and storage space is enough and high quality of video is required.

Sub-Stream

Low definition. The video file will occupy less resources. It is suitable for the condition that the bandwidth and storage space is not enough and the requirement of video quality is not strict.

Schedule Template

It defines when the recording starts and ends, and the recording type. You can select the template form the default templates or the customized template. For details about configuring recording schedule template, refer to ***Configure Recording Schedule Template*** .

Video Retention Time

If you enable this function and set the time, when the recording time exceeds set time, the previous stored video will be deleted. If you don't enable this function, the stored video will only be deleted when the storage space is full.

Audio Recording

Record the audio during the video recording. The cameras should support audio recording.

5. Enable **Central Storage**, and then configure the parameters on the Central Storage page. The descriptions of the parameters are as follows.

Note

Central storage refers to storing video files on the central storage devices (Hybrid SAN device and cloud storage device). Before enabling this function, adding and configuring central storage devices in the system. For details, refer to ***Configure Central Storage*** .

Stream Type

The stream type of video recording.

Main Stream

High definition. The video file will occupy more storage resources. It is suitable for the condition that the bandwidth and storage space is enough and high quality of video is required.

Sub-Stream

Low definition. The video file will occupy less storage resources. It is suitable for the condition that the bandwidth and storage space is not enough and the requirement of video quality is not strict.

Resource Pool

The virtual storage pool composed by Hybrid SAN or cloud storage devices. You need to configure the storage resource pool on the Operation and Management Center. For details about configuring the resource pool, refer to *User Manual of Operation and Management Center*.

Streaming Method

Record the video directly from device or through the streaming server.

Directly Access

The storage devices get video stream directly from the encoding devices, which is suitable for the condition of few encoding devices.

Access via Streaming Server

The storage devices get video stream via the streaming server to reduce the streaming bandwidth of the encoding devices, which is suitable for the condition of numerous encoding devices and the network is complicated.

Schedule Template

It defines when the recording starts and ends, and the recording type. You can select the template form the default templates or the customized template. For details about configuring schedule template, refer to ***Configure Recording Schedule Template*** .

6. After configuring the recording schedule, you can perform the following operations for verification.

View Status of Device Storage/ Central Storage	View the status of **Device Storage** or **Central Storage** in the camera list to check whether the recording schedule has been applied to the cameras successfully.
View Applying Result	Move the mouse to an area name on the left panel to view the recording schedule applying result of this area. **Red** Failed to apply recording schedule(s) to the camera(s). **Blue** No recording schedule. **Green** Succeeded to apply all the recording schedule(s). **Purple** The total number of schedules.
View Details	Click **View Details** to view the details of the recording schedule applying result of the system.

7. Perform the following operations according to your requirements.

Re-Apply Recording Schedule	Click in the Operation column to re-apply the recording schedule for this camera.
Apply Again	Select the camera(s) and click **Apply Again** to apply the recording schedule(s) for the camera(s) again.
Copy Recording Schedule	Click in the Operation column to copy the recording schedule of this camera to other camera.
Delete Recording Schedule	Click in the Operation column to delete the recording schedule of this camera.
Clear Configuration	Select the camera(s) and click **Clear Configuration** to delete the recording schedule(s) of the camera(s).

Export Recording Schedule Report	Click **Export Recording Schedule Report** to export the recording schedule report file of the in CSV format to the local disk of the PC runing the Web Client. • Click **Save** to save the file to the default path: C:\Users\User Name \Downloads. • Click **Save as** to save the file to the path as your desire.

Note

- HikCentral Enterprise-Commercial does not support applying recording schedule to ONVIF devices. Refer to the ONVIF devices' user manual to configure the recording schedule on the local devices.
- Before configuring recording schedule, we recommend you to confirm the time of storage devices and HikCentral Enterprise-Commercial are consistent.

Warning

Deleting recording schedule may cause the video loss of the device(s), please operate charily.

8.3.4 Configure Video Copyback

After configuring video copyback, the videos saved in the cameras can be uploaded to the central storage devices regularly according to the predefined schedule for backup. For example, you can save videos in devices during the day, and then upload the videos to the central storage devices during the night for a high bandwidth.

Before You Start

- Make sure there are videos saved in the cameras. See ***Configure Encoding Device Storage*** for details.
- Make sure you have configured HybridSAN or cloud storage server. See ***Configure Central Storage*** for details.
- Make sure the storage device's time is the same with the time of this platform.

Steps

1. Click ☰ in the upper-right corner, and click **System Configuration → Video Surveillance → Recording Schedule** .

   Devices added to the platform will be displayed on the right panel.
2. Select an area in the area list.
3. Click ⚙ in the operation column to enter the Configure Recording Schedule page.
4. Switch **Video Copyback** on and configure parameters.

   Copyback Execution Schedule Template

   Select or customize a schedule defining when to upload videos to the central storage server.

   Copyback Recording Schedule Template

Select or customize a schedule defining when the devices to record.

Copyback Start Date

The date of the first day starting copyback.

Resource Pool

Resource pool refers to where the videos are stored. You configure it by the Operation and Manage Center. See the user manual of Operation and Manage Center for details about configuring resource pool.

Streaming Mode

Select **Direct Streaming** and the storage device will record by streaming from encoding devices when there are not so many encoding devices. Select **Streaming via Media Server** and the storage device will record by streaming from stream media server to when the bandwidth is low and there are large amount of encoding devices.

5. Click **Save** to save the settings.

   The settings will be automatically applied to the devices after the settings are saved, and you will receive a notification.

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

Operation	Description
Apply Recording Schedule Again	Click to apply recording schedule to a device again.
Copy Recording Schedule	Click to copy a device's recording schedule to other devices.
Delete Device's Settings	Click to clear a device's settings.
Export Recording Schedule Report	Click **Export Recording Schedule Report → Real-Time Stream Recording Schedule Report** to save recording schedules in the computer as CSV format. The saving path is ***C:\Users\User Name\Downloads***.

8.3.5 Configure Recording Schedule Template

Recording schedule template is time arrangement for video recording. Three default recording schedule templates are available: All-day template, Weekdays template and Weekends template. All-day template can be used for recording videos for all day continuously. Weekdays template can be used for recording videos in weekday. Weekends template can be used for recording video at weekend. You can also customize the recording schedule template to record video in a certain period. Perform this task when you need to customize the schedule to record the video files.

Steps

1. Click → **System Configuration** → **Video Surveillance** → **Recording Schedule** .

2. Click **Configure Schedule Template**.
3. Click + on the left panel to add new schedule template.

Note

The default templates (All-Day template, Weekdays template and Weekends template) provided by the system are not allowed to be edited.

4. Enter the template name in the input box.
5. Select **Time-based** or **Event-based**.

Time-based

Continuously recording according to the time you arranged. The schedule time bar is marked with blue.

Event-based

Only record when the encoding device detects motions. The schedule time bar is marked with orange.

Note

Cloud storage server V2.2.0 does not support event-based recording.

6. Drag on the time bar to draw a time period.
7. Perform the following operations to customize the template.

Configure Time Period	Click the time period to manually enter the start time and end time or delete it.
Clear Time Period	Click **Clear** to clear all the time periods in the time bar.
Copy Time Period	Click in the last column to copy the time period(s) to other weekdays.

8. Click **Save** to save the settings.

8.4 Capture Settings

Compared with video storage, capturing pictures for storage can save a lot of bandwidth and storage resources. If the project is highly sensitive to network bandwidth, you can configure capture schedule to view real-time pictures or play back the picture records.

8.4.1 Configure Picture Storage Server

Picture storage server is for storing the pictures captured by capture schedule and the pictures of vehicle passing records captured in the parking lot subsystem.

Before You Start

- Make sure the iVMS-5180-ASW has been installed and configured. For the installation and configuration of iVMS-5180-ASW, please refer to the device's user manual.
- Configure the resource pool on the Operation and Management Center. For details, refer to *User Manual of Operation and Management Center*.
- After configuring the resource pool, you should configure the resource pool as picture storage on the Web Client. The operations are as follows:

Steps

Note

HikCentral Enterprise-Commercial only supports iVMS-5180-ASW as picture storage server.

1. Click → **System Configuration** → **Advanced Parameter** → **Picture Storage Configuration** to enter picture storage settings page.
2. Select the storage resource pool in the drop-down list as default storage pool, or click **Add Storage Pool** and set the storage pool name, replace strategy, application, and storage pool to customize a specified for storing captured pictures.
3. Click **Save** to save the settings.

8.4.2 Configure Capture Schedule

After setting the capture template, you can configure capture schedule for cameras to capture pictures for storage.

Steps

1. Click → **System Configuration** → **Video Surveillance** → **Capture Schedule** .
2. Select the area on the left panel, and all the devices of this area will be displayed on the right panel.
3. Click **Add** on the right panel or click **Add to All Devices** on the upper-right corner of the page to open the Add Capture Schedule page.
4. Select the devices need to be configured capture schedule on the Available area of the left panel, and then click to add them to the Added area of the right panel.
5. Click **Next**.
6. Select **Time Segment** or **Time Point**.
7. Select the parameters on the drop-down list. The descriptions of the parameters are as follows.

   Schedule Template

   The effective time of capture schedule. For details about configuring capture schedule template, refer to ***Configure Recording Schedule Template*** .

Note

You can only select the time segment template if you have selected the schedule type as Time Segment in step 6. You can only select the time point template if you have selected the schedule type as Time Point in step 6.

Capture Interval

It defines the interval of capturing pictures. You only need to set this parameter in time segment mode.

Capture Quality

The quality of captured pictures. The higher the quality, the more storage space and bandwidth will be occupied.

8. Click **Save** to save the settings.
9. Perform the following operations according to your requirements.

Edit Capture Schedule	Click in the Operation column to edit the capture schedule for this camera.
Delete Single Capture Schedule	Click in the Operation column to delete the capture schedule of this camera.
Delete Multiple Capture Schedules	Select the camera(s) and click **Delete** to delete the capture schedule(s) of the camera(s).

Warning

Deleting capture schedule may cause the pictures loss of the device(s), please operate charily.

8.4.3 Configure Capture Schedule Template

Capture schedule template is time arrangement for picture capturing. You can customize capture schedule to define when and how the device captures pictures with the pre-defined parameters. HikCentral Enterprise-Commercial provides two capture schedule template modes: time segment template and time point template.

Steps

Note

For time segment template, you can set the capturing time period, and when you set capture schedule for cameras, you need to set the capture interval. The system will capture picture every capture interval during the time period, which is more simple to configure but lack of flexibility. For time point template, you can set each capturing time point, which is more flexible but complicated to configure.

1. Click → **System Configuration** → **Video Surveillance** → **Capture Schedule** .

2. Click **Set Schedule Template**.
3. Select the capture schedule template modes.
   - **Time Segment Template**: The configuration of Time Segment Template is similar with configuring recording schedule template. For details, refer to ***Configure Recording Schedule Template*** .
   - **Time Point Template**: The configuration of time point template is as follows:
     a. Select **Time Point Template**.
     b. Click + to add new template.

     Note

     HikCentral Enterprise-Commercial provides three default templates, which are not allowed to be edited. All-Day Hourly Template can be used to capture pictures once an hour all the days. Weekdays Hourly Template can be used to capture pictures once an hour on weekdays. Weekends Hourly Template can be used to capture pictures once an hour on the weekends.

     c. Enter the template name in the input field.
     d. Move the mouse to the week form to draw the time point for capturing pictures.
4. Click **Save** to save the settings.

8.5 Device Arming Settings

Arming Schedule template defines when and how the events or alarm will be triggered. You can arm or disarm devices by arming schedule template. During the arming period, the devices upload alarms or events to the system when the alarms or events happen. During the disarming period, the devices will not upload alarms or events to the system even if the alarms or events happen, which helps you to manage the alarms and events flexibly.

8.5.1 Configure Arming Schedule Template

Arming schedule template defines when and how the events or alarm will be triggered. The system predefines three default arming schedule templates: All-Day Template, Weekday Template and Weekend Template. All-Day Template can be used for arming or disarming devices all day. Weekday Template can be used for arming or disarming devices in weekday. Weekend Template can be used to arming or disarming devices at weekend. You can also customize new templates according to your desire.

Steps

1. Click ☰ → **System Configuration** → **Video Surveillance** → **Device Arming/Disarming** .
2. Click **Set Arming Schedule Template** to enter the Arming Schedule Template Configuration page.
3. Click + to add a new schedule template.
4. Enter the template name in the input field.
5. Drag on the time bar to draw a time period, which defines the arming period.

6. **Optional:** Perform the following operations to customize the template.

Set Start Time and End time	Click the time period to manually enter the start time and end time, or delete it.
Clear Time Periods	Click **Clear** to clear all time periods in the time bar.
Copy Time Period(s)	Click in the last column to copy the time period(s) to the other weekdays.

7. Click **Save** to save the settings.

8.5.2 Event Arming Control

You can arm/disarm the added devices for the following events: Motion Detection, Video Tampering Detection, Video Loss Detection, Alarm Input, Alarm Output.

Steps

1. Click → **System Configuration** → **Video Surveillance** → **Device Event Arming/Disarming** .
2. Select the area on the left panel, the devices in this area will be displayed in the right panel.
3. Select one event type as arming/disarming events in the drop-down list one the right panel.
4. Click in the Operation column to enter the Arming Schedule Configuration page.
5. Select one arming schedule template in drop-down list of Schedule Template.

Note

All the arming schedule templates, including the default templates and customized templates will be displayed in the drop-down list. For details about customizing arming schedule templates, refer to ***Configure Arming Schedule Template*** .

6. Click **Save** to save the settings.
7. Click in the Operation column to arm this device by the arming schedule template selected in step 5.
8. Click in the Operation column to disarm this device by the arming schedule selected in step 4.
9. Select devices in a batch, and then click **Batch Configure Schedule** to select an arming schedule template for the selected devices.
10. Select devices in a batch, and then click **Batch Arm** to arm the devices by the arming schedule template selected in step 8.
11. Select devices in a batch, and then click **Batch Disarm**to disarm the devices by the arming schedule template selected in step 8.

8.6 Set Parameters

You can set parts of the global parameters in the system.

Steps

1. Click → **System Configuration** → **Video Surveillance** → **Parameters** to enter the Parameter Configuration page.
2. Configure the parameters. The descriptions of the parameters are as follows:

   PTZ Preemption Duration

   When a user stops PTZ control, the other user with lower or the same PTZ control permission can control the PTZ after the duration.

   Display User Information in PTZ Control

   After enabling the function, the name of user who controls the PTZ will be displayed in the video.

   Time-Limited Live View

   After enabling this function, you can set live view time limit for each user, which helps to save bandwidth. The system will start countdown at 10 s before the end time and stop live view when the countdown finishes. If you continue to view, the countdown will start again.

8.7 Live View

You can view live video of the connected cameras. During live view, you can control PTZ cameras, manually record video footage, capture pictures, view instant playback, etc.

8.7.1 Start Live View

After adding the cameras into areas, you can start live view to view the camera's live video, and perform some basic operations.

Steps

1. Click **Live View** in the Home page.

   The Video Surveillance client will pop up.
2. **Optional:** Click in the bottom toolbar to customize window division.
3. Perform one of the following operations to start live view of one camera.
   - Drag a camera from camera list to a display window.
   - Double-click the camera name after selecting a display window.
4. **Optional:** Perform the following operation(s).
   - Click / to adjust the size of the display window.
   - Drag the display window to another window to change the display window for live view.
   - Right-click the camera name in the camera list to switch between direct streaming mode and indirect streaming mode.

8.7.2 Manual Capture

You can capture pictures manually during live view and store the pictures in the local PC.

Steps

1. Start live view. For details, refer to ***Start Live View*** .
2. Move the cursor to the display window to show the toolbar and click to capture a picture.

   The captured picture will be saved automatically and a dialog with the saving path will open in the upper right corner.
3. **Optional:** Click on the bottom tool bar of the live view window to capture pictures of all the display windows.
4. **Optional:** Click **Open File** or **Open Folder** on the dialog to view the captured picture(s).

Note

The saving path of the captured picture can be set on the Video Settings page. For details about configuring file saving path, refer to ***Live View and Playback Settings*** .

8.7.3 Manage View

A view is a window division with resource channels (e.g., cameras and access control points) linked to each window. View mode enables you to save the window division and the correspondence between cameras and windows as favorite so that you can quickly access these channels. For example, you can link camera 1, camera 2, and camera 3 located in your office to the certain display windows and save them as a view called office. Next time, you can access the view office and these cameras will be displayed in the linked window quickly. Two types of view modes are available: public view and private view. Public views can be viewed by other users, while private views can only be viewed by the logged-in user. For live view, the view mode can save resource type, resource ID, stream type, position and scale after digital zoom, preset No., and fisheye dewarping status, etc.

Steps

1. Click Live View in the Home page.

   The Video Surveillance client will pop up.
2. **Optional:** Add a view group.
   1) Select **Public View** or **Private View**.

      Note

      The view groups and views belonging to the private view group are hidden from the other user.
   2) Click .
   3) Create a name for the group or use the default name.
   4) Click **OK** to add this view group.

3. **Optional:** Select a view group.
4. Add a view.
   1) Click .
   2) Create a name for the view or use the default name.
   3) Click **OK**.
5. Select a view name.
6. Drag the channels to the window or double-click the channels to start live view.

Note

For detailed operations about live view, refer to ***Start Live View*** .

7. Save the view with the displayed view division and channels.
   - Click → **Save** to save the current window division mode and displayed channels as the selected view.
   - Click → **Save as** to save the current window division mode and displayed channels as a new view by creating view name (optional) and selecting the view saving path.
8. **Optional:** Perform the following operation(s) after adding the view.
   - Select a view or view group and click to edit the view (group) name.
   - Select a view or view group and click to delete the view or view group.
   - Select a view or view group and click or to change the sequence of the custom view or view group.
   - Click and enter the name of a view or view group to search a view or view group.

8.7.4 PTZ Control

The Web Client provides PTZ control for cameras with pan/tilt/zoom functionality. You can set the preset, patrol and pattern for the cameras on the PTZ control panel.

Note

The PTZ control function should be supported by the camera.

The following buttons are available on the PTZ control panel:

	Lock the PTZ. When the PTZ is locked, users with lower PTZ control permission levels cannot change the PTZ controls. For details about setting the PTZ control permission priority, refer to ***Add Single User*** .
	Cancel the PTZ lock.
	Direction buttons and auto-scan.

Configure Preset

A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. You can also set a virtual preset after enabling digital zoom.

Steps

1. Click **Live View** on the Home page and start live view of the PTZ camera.
2. Enter the PTZ Control mode in the live view page.
3. Click **Preset**.
4. Use the direction buttons and other buttons to control the PTZ movement.
5. Select a PTZ preset number from the preset list and click .
6. Create a name for the preset in the pop-up window.
7. Click **OK** to save the settings.
8. **Optional:** After setting the preset, you can do one or more of the followings.
   - Double-click a preset, or select a preset and click to call the preset.
   - Select a preset from the list and click to edit the preset.
   - Select a preset from the list and click to delete the preset.

Configure Patrol

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

Before You Start

Two or more presets for one PTZ camera need to be added. For details about adding a preset, refer to ***Configure Preset*** .

Steps

1. Click **Live View** on the Home page and start live view of the PTZ camera.
2. Enter the PTZ Control mode in the live view page.
3. Click **Patrol**.
4. Add presets to the patrol.
   1) Select a patrol number from the drop-down list and click .
   2) Click to add a configured preset, and then set the dwell time and patrol speed.

Note

- The preset dwell time ranges from 15 to 100s.
- The patrol speed ranges from 1 to 40.
- Repeat the above step to add other presets to the patrol.
- By default, the first preset is added to the patrol list. Double-click the preset, speed, and dwell time to access a drop-down configuration list.

5. **Optional:** Perform the following operation(s) after adding the preset.

- Double-click the preset to change preset in the drop-down list.
- Click to remove the preset from the patrol.
- Click or to change the sequence of presets.

6. Click OK to save the patrol settings.

Note

Up to 32 patrols can be configured.

7. **Optional:** After setting the patrol, you can do one or more of the followings.
   - Click to start the patrol.
   - Click to stop calling the patrol.

Configure Pattern

You can set patterns to record the movement of the PTZ.

Steps

1. Click **Live View** on the Home page and start live view of the PTZ camera.
2. Enter the PTZ Control mode in the live view page.
3. Click **Pattern**.
4. Click **Start Recording** to start recording the movement path of the pattern.
5. Use the direction buttons and other buttons to control the PTZ movement.
6. Click **Stop Recording** to stop and save the pattern recording.

Note

Only one pattern can be configured, and the newly-defined pattern will overwrite the previous one.

7. **Optional:** After setting the pattern, you can do one or more of the followings:
   - Click **Start Playing** to call the pattern.
   - Click **Stop Playing** to stop calling the pattern.

8.7.5 Auto-Switch Live View

You can configure auto-switch live view of key cameras in a group. The video stream of the cameras from the same group can switch automatically in a selected display window.

Steps

1. Enter the Live View page.
2. Click **Auto-Switch** in the left tool bar.
3. Select **My Group** and click to open the Auto-Switch Group window.
4. Configure auto-switch group.
   1) Enter the group name or use the default group name.
   2) Customize the switching interval and window division.

3) Click to add camera(s).
4) Click **OK**.

5. Double-click a group to start auto-switch.
6. **Optional:** Perform the following operation(s) to control the auto-switch.
   - Click / to pause/resume auto-switching custom views.
   - Click / to view the previous/next page of live view.
   - Click to stop auto-switch.
7. **Optional:** Perform the following operation(s) to edit the group.
   - Select a group and click to edit the group.
   - Select a group and click to delete the group.
   - Select a group and click or to change the sequence of the groups.
   - Click and enter a group name to search a group.

8.7.6 Auxiliary Screen Preview

Live video can be displayed on an auxiliary window to monitor multiple scenes. In an auxiliary screen, you can check live views of resources and manage views.

For details about starting live views and managing views, refer to ***Start Live View*** and ***Manage View*** .

Click **Auxiliary Screen** in the lower-left corner of the live view window to open an auxiliary screen.

Note

Only one auxiliary screen for live view can be opened.

8.7.7 Broadcast to Connected Devices

Perform the broadcast function to distribute audio content to the added device if the device has an audio output.

Before You Start

Note

- Your PC should have available microphone for broadcasting audio to the device.
- If the client is performing two-way audio with the device's camera, you cannot start broadcast with the device, and vice versa.

Enter the context of your task here (optional).

Steps

1. Start live view. For details about starting live view, refer to ***Start Live View*** .
2. Click **Broadcast** to enter the broadcast window.
3. Select a group in the left column.

4. Select the device(s) to broadcast to.
5. Click **Start Broadcast** or **Open All** to start broadcasting to the selected device(s) or all devices through the microphone.
6. **Optional:** Perform the following operation(s).
   - Stop broadcasting.
     a. Click **Tool → Broadcast** .
     b. Select the device(s) that you want to cancel broadcast and click **Stop Broadcast**. Or you can click **Close All** to stop broadcasting to all devices.
   - Add Broadcast Group
     a. Select a group and click .
     b. Enter group name.
     c. Click **OK**.
   - Edit Group.
     a. Select a group and click .
     b. Enter group name.
     c. Click **OK**.
   - Select a group and click to delete the group.
   - Add Device.
     a. Click **Add**.
     b. Select an area and devices.
     c. Click **OK**.
   - Click to delete a device.

8.7.8 Customize Icons on Live View Toolbar

You can customize the icons shown on the toolbar of the display window for live view control.

Steps

1. Start live view. For details about starting live view, refer to ***Start Live View*** .
2. Click → **Live View Tool Bar** .
3. Customize the live view toolbar.
   - Click an icon in the list to add it to the gray frame below to hide the icon. Icons in the gray frame will be hidden in the toolbar of the live view window.
   - Click the icon in the gray frame to add it back to the live view toolbar to show an icon on the toolbar.
4. Drag the icons in the icon list to adjust icon positions.

Icon	Name	Description
	Capture Picture	Take a snapshot of the current video and save in the current PC.
	Audio Control	Turn off/on the audio.
	Emergency Recording	Record the video files for current live view and save in the current PC.
	Instant Playback	Switch to instant playback to view the recorded video files.
	Two-way Audio	Start two-way audio with the camera to get the real-time audio from the device to realize voice talk with the person at the device.
	Digital Zoom	Zoom in or out the video for cameras that do not have their own optical zoom capabilities. Click again to disable the function.
	3D Positioning	Click the desired position in the video image and drag a rectangle area in the lower-right direction, then the dome system will move the position to the center and allow the rectangle area to zoom in. Use the left key of mouse to drag a

		rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out. **Note** This function needs to be supported by the device.
	Edit Transcoded Stream	Switch the live view stream to main stream or sub-stream (if supported).
	Stream Information	Click to show stream information in the lower-left corner of the display window.
	Live Pictures	Click to switch to show captured pictures according to the capture schedule from live view. **Note** A capture schedule should have been configured.
	Alarm Output	Click to turn on/off external alarm devices connected to the camera.
	PTZ Control	Click and an arrow will be displayed in the display window. Move

		the cursor and the arrow direction will change with your movement. Click different place in the window and the camera will move in the arrow direction. Click again to exit PTZ control.
	Recording Playback	Click to play the recorded video of the camera.
	Video Wall	Play the video of the camera on the video wall.

8.8 Playback

The video files stored on the local storage devices such as HDDs, Net HDDs and SD/SDHC cards or the central storage server can be searched and played back remotely through the web browser. You can also add tags for the video file for positioning playback, and download video files to your local computer for backup purpose.

8.8.1 Play Video File

In the Playback module of HikCentral Enterprise-Commercial web client, you can start playback of one or more added cameras and do some basic operations, including capturing, adding tags, downloading video files, etc. HikCentral Enterprise-Commercialsupports normal playback and synchronous playback.

Note

Make sure HikCentral Enterprise-Commercial plug-in has been installed on your computer correctly.

Normal Playback

You can search the video files of cameras and filter the found video files by video type or by storage location. After searching the video files, the playback starts. You can control the video playback via timeline. The timeline indicates the time duration of the video file.

Steps

1. Click **Playback** on the Home page to enter the playback page.

   Note

   Make sure HikCentral Enterprise-Commercial plug-in has been installed correctly.

2. **Optional:** Click on the bottom toolbar to select the window division mode for playback.
3. Select cameras from the camera list, or enter a keyword of camera name or area name in the search field and click to search the cameras or areas.

   All searched results will display in the list.
4. Perform one of the following operations to start the playback of the camera.
   - Drag the camera to a display window.
   - Double-click the camera name after selecting a display window.
5. **Optional:** Click on the timeline to filter by video type and storage location for the video files to be played back.

   Note

   For details about setting recording schedule and storage location, refer to ***Configure Recording Schedule*** .
6. **Optional:** Move the cursor to the lower-right corner in a display window. The playback toolbar will show. You can perform operation(s) using the tools during normal playback.

   Note

   For details about tools on the playback toolbar, refer to ***Customize Icons on Playback Toolbar*** .
7. **Optional:** You can perform the following operation(s) using tools on the bottom toolbar of the Video Surveillance window for all display windows during normal playback.

Icon	Name	Description
/	Hide/Show Resource Tree	Hide or show the resource tree. The larger window will be available when hiding the

		resource tree during playback.
/	Async/Sync Playback	Start or stop synchronous playback of multiple cameras. For details about synchronous playback, refer to ***Synchronous Playback*** .
/	Mute/Audio On	Turn on or turn off the audio.
	Capture	Capture pictures for all display window during playback and store on the local computer. You can customize the file format and saving path for the captured pictures. For details about setting the file format and saving path, refer to ***Live View and Playback Settings*** .
	Close Time Selection	Close the time segment selected on the timeline.
	Search by Time Segment	Select the important time segment and mark with rectangle on the timeline.
	Reverse Single Frame	Play the video file frame by frame reversely.
/	Reverse Playback/Pause	Start or pause reverse playback.

/	Play/Pause	Start or pause playback.
	Single Frame	Play the video file frame by frame.
2018-12-17 00:10:20	Accurate Positioning	Set the accurate time point to play the video file.
	Speed Down	Slow forward playback. Up to 1/16x playback speed can be supported.
1x	Restore Default Speed	Restore the playback to normal speed (1x) during fast forwarding or slow forwarding.
	Speed Up	Fast forward playback. Up to 16x playback speed can be supported.
	Close All	Close all opened playback windows.
	Window Division	Switch window-division modes during playback. Currently it supports 1-window mode, 4-window mode, 9-window mode, and 16-window mode.
/	Normal/Self-Adaptive Mode	Set the view scale of the playback window as original size or full-window mode.

	Full Screen	Show the playback video in full-screen mode. You can press **Esc** key on the keyboard to exit the full-screen mode.
	Configuration	Configure advanced video settings. For details about video settings, refer to ***Live View and Playback Settings*** .

Synchronous Playback

During synchronous playback, the video files of multiple cameras can be played back in synchronization. The synchronous playback can be used for tracking, investigation, taking evidence, and so on. For example, you can synchronously play back video files of multiple cameras at the time when a criminal case happened.

Before You Start

Note

Video files up to 16 cameras can be played back simultaneously.

Steps

1. Click **Playback** on the Home page to enter the playback page.

   Note

   Make sure HikCentral Enterprise-Commercial plug-in has been installed correctly.

2. Select a camera to start playback.

   Note

   For details about starting playback, refer to ***Normal Playback*** .

3. Click on the timeline or drag the timeline to locate the playback video to a specific time.
4. Click on the bottom toolbar to enable the synchronous playback.

   The cameras under playback will start synchronous playback.
5. Click to disable the synchronous playback.
6. **Optional:** Move the cursor to the lower-right corner in a display window. The playback toolbar will show. You can perform operation(s) using the tools during normal playback.

Note

For details about tools on the playback toolbar, refer to ***Customize Icons on Playback Toolbar*** .

7. **Optional:** You can perform operation(s) using tools on the bottom toolbar of the Video Surveillance window for all display windows during synchronous playback. For details about tools on the bottom toolbar, refer to ***Normal Playback*** .

8.8.2 Add Tag for Video File

You can add tags and descriptions for the important video points during playback to conveniently locate the video later.

Steps

1. Click **Playback** on the Home page to enter the playback page.

Note

Make sure HikCentral Enterprise-Commercial plug-in has been installed correctly.

2. Select a camera to start playback.

Note

For details about starting playback, refer to ***Normal Playback*** .

3. Click to open the Tagged Video area.
4. Click **Marked Time** to set the time point to add a tag for the video.
5. Select a tag type, and enter the description for the tag.

Note

The tag type and description will be used as the condition to search the video by tag.

6. Click Save.
7. **Optional:** Perform the following operation(s) to manage the added tag(s).
   - Search by Tag: Click to expand the Tag panel. Select the tag type, enter the keyword, and set the time period to search the video by tag. After searching the video by tag, you can double-click the video to play the video file from the marked time point.
   - Edit: You can click the tag on the timeline and click Edit to edit the time point, type, and description for the tag. You can also click after searching the video by tag to edit the tag.
   - Delete: You can click the tag on the timeline and click **Delete** to delete the tag. You can also click after searching the video by tag to delete the tag.

8.8.3 Download Video File

During playback, you can download the video files of the camera to the local computer by file for backup purpose.

Steps

1. Click **Playback** on the Home page to enter the playback page.

   Note

   Make sure HikCentral Enterprise-Commercial plug-in has been installed correctly.

2. Select a camera to start playback.

   Note

   For details about starting playback, refer to ***Normal Playback*** .

3. Click **Recording Time** to set the start time and end time of the video to be downloaded. You can also drag the cursor on the timeline to set the time period.
4. Click **Directory** to set the saving path for the downloaded video file.
5. Click **Download** to start downloading the video file.

   The Download Center will pop up automatically to display the downloading status.

6. **Optional:** Perform the following operation(s) to manage the video files being downloaded in the Download Center.
   - Search: Enter the keyword and click to search download task(s).
   - Pause: Click **Pause** to pause downloading the video file, or click **Pause All** to pause all download tasks. You can click **Continue** to continue downloading the video file, or click **Start All** to start all download tasks.
   - Delete: Click **Delete** to delete the download task, or click **Clear** to delete all download tasks.

     Note

     Deleting download task(s) will not delete downloaded video file(s).

   - Retry: If downloading video file(s) fails, click **Retry** to try to download the video file(s) again.

8.8.4 Customize Icons on Playback Toolbar

You can customize the icons displayed on the playback toolbar to conveniently operate the video during playback.

Steps

1. Click **Playback** on the Home page to open the Video Surveillance window.

Note

Video Surveillance window will pop up automatically. If video surveillance window does not pop up, please click **click here to try again** or check whether HikCentral Enterprise-Commercial plug-in has been installed correctly.

2. Click in the lower-right corner of the Video Surveillance window to open the System Settings window.
3. Click **Playback Toolbar** to expand the Playback Toolbar area.
4. Perform one of the following operations to add icon(s) to or remove icon(s) from playback toolbar.
   - Move the cursor on the icon in the grey area, and click ⊕ to add the icon to playback toolbar.
   - Move the cursor on the icon in the white area, and click ⊖ to remove the icon from playback toolbar.
5. **Optional:** You can drag the icons to adjust the order of the icons displayed on the toolbar.
6. Click **Save**.

Icon	Name	Description
	Capture	Capture picture(s) during playback. The captured picture will be stored on the local computer. **Note** For details about setting the saving path of the captured picture, refer to ***Live View and Playback Settings*** .
	Audio Control	Turn off/on the audio.
	Clip	Clip a video segment during playback. Click again to stop clipping. The clipped video file will be stored on the local computer. **Note** For details about setting the saving path of the clipped video file, refer to ***Live View and Playback Settings*** .

Icon	Name	Description
	Lock	Lock the video for a period of time to avoid being overwritten. You can set the video segment to be locked and expiry date. Click on the timeline and Click **Unlock** to unlock the video file.
	Digital Zoom	Enable the digital zoom function and draw a rectangle on the video. Click again to disable the function. **Note** When in software decoding mode, you can also capture the zoomed in picture after enabling digital zoom function.
	Download	Download the video file under playback. For details about downloading video file, refer to ***Download Video File*** .
	Stream Information	Show the stream information (such as frame rate, resolution, encoding format, etc.) in the lower-left corner of the display window. Click again to hide the stream information.
	Tag	Add tag(s) for the video to mark the important video point for quickly locating later. For details about adding tag(s), refer to ***Add Tag for Video File*** .
	Frame-Extracting Playback	Start playback frame by frame.

Icon	Name	Description
		Note Frame-extracting playback should be supported by the device.
	Transcoding Playback	Enable playback in lower frame rate when the network condition is poor. **Note** Transcoding playback should be supported by the device.
	Segmented Playback	Clip the video footage into multiple segments (e.g., 4 segments) and play all segments in the corresponding display windows asynchronously.

8.9 Live View and Playback Settings

You can configure advanced settings of the interface and functions for live view and playback, such as capture, recording, two-way audio, etc.

Click in the lower-right corner of the Video Surveillance window to open the System Configuration window for video settings. Or click on the control panel and click Video Settings tab to enter the Video Settings page.

File Saving Path	Click to select the directory to save the captured pictures and video files. Click to view the current directory for saving files.
Direct Streaming	After enabling this function, HikCentral Enterprise-Commercial will get stream from the device by default during live view instead of via media services.
PTZ Mode	HikCentral Enterprise-Commercial provides simple mode and specialist mode for PTZ control. Compared with simple mode, specialist mode provides more PTZ functions during live view, such as auxiliary focus, 3D positioning, etc.

Capture Configuration	Picture Format: Set the file format for the captured pictures during live view or playback as JPEG or BMP.
	Capture Mode: Set the capture method during live view and playback. Currently HikCentral Enterprise-Commercial supports capturing single picture, and capturing pictures by time or by frame. **By Time** Set the number of pictures and capture interval. For example, if you have set the number of pictures as 3, and set the capture interval as 200 ms, when you capture during live view or playback, the client will capture 3 pictures every 200 ms. **By Frame** Set the number of pictures. For example, if you have set the number of pictures as 3, when you capture during live view or playback, the client will capture 3 pictures frame by frame.
Record Configuration Clip Configuration	The maximum size of each video file recorded during live view and clipped during playback. You can set the size according to your storage space.
Two-way Audio Configuration	By switching **Record Two-Way Audio** on, the audio record during the two-way audio can be automatically saved when two-way audio ends. You can also set the saving path when the two-way audio ends.
Streaming Configuration	When getting stream failed, the device will try again from the device or other streaming media according to your configuration. For example, if the stream reconnection times are 3 and the reconnection interval is 10 seconds, the Video Surveillance client will get stream every 10 seconds for 3 times when getting stream failed. If getting stream failed in the third time streaming, the module will stop trying.
Decoding Configuration	Enable GPU hardware decoding to save GPU resources during live view and playback. **Note** After enabling GPU decoding, restart live view or playback for GPU decoding to take effect.
Live View Configuration	**Streaming Adaption** By setting this parameter, the live view will switch to sub-stream when live view window number is more than the configured number.

	In this way, live view fluency can be guaranteed when you open more than one live view window. 1 to 16 windows can be set. **Resume Last Live View** Restore the live view window last opened when you run the client next time. **Display Online Status** By enabling this function, device's online/offline status can be shown in the device list. will be displayed beside the online device's name; while will be displayed beside the offline device's name. **Filter Offline Camera** By enabling this function, offline devices will not be displayed during auto-switch. **Note** This button is available only when **Display Online Status** is enabled. **VCA Information** Display the VCA information during playback. VCA information refers to the intelligent event information on the camera, e.g. motion detection, line crossing and the thermal cameras' temperature displaying. For motion detection, a frame will be overlaid on the detected moving object, and the frame moves with the object's movement. **Show Live Pictures by Default** You should configure capture schedule before enable this function. Click in the live view tool bar and the captured pictures will be displayed in live view. You can click **Download** in the prompt to download the captured picture.
Playback Configuration	**Buffer before Decoding** Buffer size for video data before decoding. The buffer size should be determined based on network performance, computer performance, and bit rate. Larger buffer will result in better video performance but may cause delay. **Buffer after Decoding** Buffer size for video data after decoding. (E.g. you have set the buffer before decoding as 20 frames, you can play backward 20 frames without decoding again, which helps you to save the time of decoding.) The buffer size should be determined based on network performance, computer performance, and bit rate. Larger buffer will

	result in more video for playing backward without decoding, and more space will be occupied in the player. **VCA Information** Display the VCA information during playback. VCA information refers to the intelligent event information on the camera, e.g. motion detection, line crossing and the thermal cameras' temperature displaying. For motion detection, a frame will be overlaid on the detected moving object, and the frame moves with the object's movement.

8.10 Video Wall

With a video wall, you can display videos on the video wall screen. It supports window division and opening new windows when more display windows are needed. To realize a quick jump to image of a certain place, you can save the images of the place as a scene so that you can display the scene quickly when you want to view its image.

Video wall module supports the following functions:

- Resource management: adding decoding devices and video walls to the platform for management.
- Control Display on Video Wall: select cameras to be displayed and display mode.
- Scene Management: save frequently-viewed images and window divisions as scenes, so that you can display them on the video wall quickly.

This function is supported by the Control Client. See *User Manual of HikCentral Enterprise-Commercial Control Client* for details.

Chapter 9 Access Control

The access control module is applicable to access control devices. It provides multiple functionalities, including access control and person group management, permission configuration, and other functions. You can also search access control events and export the search result to local storage.

9.1 Flow Chart

For the first time, you can perform configurations and applications of access control according to the chart below.

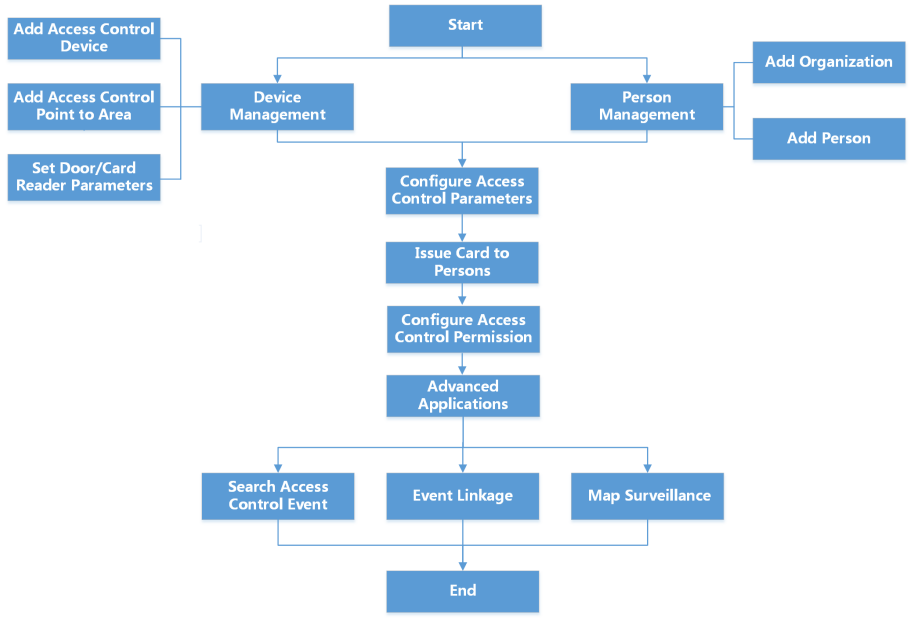


Figure 9-1 Flow Chart of Access Control

- **Device Management**: You can add the access control devices to the system for configuration and management. For details, refer to ***Access Control Device Management*** .
- **Person Management**: You can add person information to the system for further operations. For details, refer to ***Person Management*** .
- **Configure Access Control Parameters**: You can configure access control parameters in the system including device parameters, permission parameters and event parameters. For details, refer to ***Access Control Settings*** .
- **Issue Card to Person**: You can issue one or more cards for one person. For details, refer to ***Card Issuing*** .
- **Advanced Applications**: You can configure parameters in the system to realize the advanced functions including multiple authentication, anti-passback, multi-door interlocking, remaining open/closed, etc. For details, refer to ***Advanced Functions*** .

- **Search Access Control Event**: You can search the access control history events including person access event and access control device event. For details, refer to .
- **Event Linkage**: You can configure linkage actions for the access control events. When an event is detected, the system will receive the real-time information of the event and trigger linkage actions. For details, refer to ***Event Configuration*** .
- **Map Surveillance**: You can add access control resources to the map. When the alarm is triggered, you can view the live view and playback of the added resources on the map. For details, refer to ***Map*** .

9.2 Access Control Device Management

You can add the access control devices to HikCentral Enterprise-Commercial for configuration and management, such as permission configuration for people entering or exiting the door, time and attendance management, etc.

Access control devices can be added to the system via the following protocols:

Hikvision Device Network SDK Protocol

Access control devices using this protocol are produced by Hikvision with fixed IP address.

Hikvision EHome Protocol

Encoding devices using this protocol are produced by Hikvision with fixed IP address or dynamic IP address. The protocol is suitable for countries or regions short of IP addresses that cannot allocate an IP address for each device.

9.2.1 Add Online Access Control Devices

The active online access control devices in the same subnet with the computer running the Web Client will be displayed on a list. You can add one online device at a time, or add multiple online devices in a batch.

Before You Start

- Make sure the access 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 Enterprise-Commercial via network.
- Make sure the access control devices have been configured correctly according to the user manuals of the devices or the project requirements.

Steps

Only online access control devices connected via Hikvision EHome protocol can be automatically detected.

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Access Control** to enter the Access Control page.
2. Select an area in the area list to add the access control device.

3. Click **Access Control Device** to enter the access control device page.
4. Click **Online Devices** to start detecting online access control devices. The detected online access control devices are listed on the Online Access Control Devices page.
5. Select one or more devices you want to add to the system from the list, or search online access control devices by specific conditions.
6. Select device type for the online access control device(s) to be added from the Device Type drop-down list.
7. Click **Save** to add selected access control device(s).
8. Perform the following operation(s) after adding the access control device.

Search Device	Check **Include Sub-Area** to filter the devices. Set search conditions, and click **Search** to search access control devices as required.
Configure Parameters	Click to configure parameters for the access control device, including basic information, card reader information, parameters for door and card reader, etc.

Note

For details about configuring parameters for access control devices, refer to refer to ***Add Access Control Point to Area*** and ***Set Parameters for Card Readers*** .

Online Test	Click to check whether the access control device is online.
Delete Device	Click to delete the access control device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete an access control device, all the information linked to the device will be deleted, such as permission configuration and so on. As a result, you may lose alarms or fail to update access control permissions.

9.2.2 Add an Access Control Device by IP Address

When you know the IP address of the access control device to be added, you can add the access control device to your system by specifying the IP address, user name, password, and other related parameters.

Before You Start

Make sure the access 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 Enterprise-Commercial via network.

Steps

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Access Control** to enter the Access Control page.
2. Select an area in the area, and click **Access Control Device** to enter the access control device page.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Device Network SDK Protocol** as the access protocol from the drop-down list.
5. Set the parameters for the access control device, including device name, device type, IP address, port No., user name, password, and network.

Device Type

Select the device type according to the device capability.

Note

For details about the relationship between the device type and the device model, refer to ***Set Device Parameters*** .

IP Address

Enter the IP address of the access control device.

Port No.

Enter the device port No. The default value is 8000.

User Name

Enter the user name of the access control device. By default, the user name is admin.

Password

Enter the password of the access control device.

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.

Domain

Select the network domain that the access control device belongs to from the drop-down list.

Note

For details about network domain configuration, refer to *the User Manual of Operation and Management Center*.

6. Click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the access control device and click **Test** to start online test again.
7. Click **Save** to add the access control device.
8. **Optional:** Perform the following operation(s) after adding the access control device.

Search Device	Check **Include Sub-Area** to filter the devices. Set search conditions, and click **Search** to search access control devices as required.
Configure Parameters	Click to configure parameters for the access control device, including basic information, card reader information, parameters for door and card reader, etc.
	Note For details about configuring parameters for access control devices, refer to ***Add Access Control Point to Area*** and ***Set Parameters for Card Readers*** .
Online Test	Click to check whether the access control device is online.
Delete Device	Click to delete the access control device. You can also select multiple devices and click **Delete** to delete devices in a batch.
	Note If you delete an access control device, all the information linked to the device will be deleted, such as permission configuration and so on. As a result, you may lose alarms or fail to update access control permissions.

9.2.3 Add an Access Control Device by EHome Protocol

Hikvision EHome protocol can realize the communication between the system and Hikvision access control devices with dynamic IP address. The protocol is suitable for countries or regions short of IP addresses that cannot allocate an IP address for each device. You can add the access control device connected via EHome protocol to the system by specifying device name, device type, device No., and domain.

Before You Start

Make sure the access 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 Enterprise-Commercial via network.

Steps

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Access Control** to enter the Access Control Device Management page.
2. Select an area in the area list to add the access control device.
3. Click **Access Control Device** to enter the access control device page, and click Add to enter the Add Access Control Device page.
4. Select **Hikvision EHome Protocol** as the access protocol from the drop-down list.
5. Set the parameters for the access control device, including device name, device type, device No., and network.

   Device Type

   Select the device type according to the device capability. For details about the relationship between the device type and the device model, refer to ***Set Device Parameters*** .

   Device No.

   Enter the unique device No. of the access control device. The device No. should be the same with that entered in the device.

   Domain

   Select the network domain that the access control device belongs to from the drop-down list.

   Note

   For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

6. Click **Save** to add the access control device.
7. Perform the following operation(s) after adding the access control device.

Search Device	Check **Include Sub-Area** to filter the devices. Set search conditions, and click **Search** to search access control devices as required.
Configure Parameters	Click to configure parameters for the access control device, including basic information, card reader information, parameters for door and card reader, etc. **Note** For details about configuring parameters for access control devices, refer to ***Add Access Control Point to Area*** and ***Set Parameters for Card Readers*** .
Online Test	Click to check whether the access control device is online.
Delete Device	Click to delete the access control device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete an access control device, all the information linked to the device will be deleted, such as permission configuration and so on. As a result, you may lose alarms or fail to update access control permissions.

9.2.4 Add an Access Control Device by ISUP 5.0 Protocol

ISUP5.0 Protocol can realize the communication between the system and Hikvision access control devices with dynamic IP addresses. The protocol is of high security level and suitable for countries or regions short of IP addresses that cannot allocate an IP address for each device. You can add the access control device connected via ISUP 5.0 protocol to the system by specifying device No., domain, and other parameters.

Before You Start

- Make sure the access 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 Enterprise-Commercial via network.
- Edit device parameters via Hikvision Client Demo.

  Address Type

  Select **IP/IPV6** as the address type for device accessing the service.

  IP Address

  IP address for device accessing the service.

  Port

  Generally, the default port for device accessing the service is 7031.

  Protocol Type

  Select **EHome** as the protocol type for device accessing the service.

  ID

  Enter the unique ID of device.

  Enable

  Select **Enable** to enable EHome registration function.

  EHome Protocol Version

  Select **v5.0**.

  EHome Key

  Identity authentication for device accessing the system.

  Network Card Type

  Generally, select **Main Network Card**.

Steps

1. On the Home Page, click → **System Configuration** → **Devices** → **One-Card System** → **Access Control** .
2. Select an area in the area list, and click **Access Control Device** to enter the access control device page.
3. Click **Add** to enter Add Access Control Device page.
4. Set parameters for the access control device, including device name, device type, access protocol, device No., EHome key and domain.

   Device Type

   Select the device type according to the device capability.

   Note

   For details about the relationship between the device type and the device model, refer to ***Set Device Parameters*** .

   Access Protocol

   Select **Hikvision ISUP Protocol** as the access protocol from the drop-down list.

   Device No.

   Enter the unique device No. of the access control device. The device No. should be the same with that configured on the device.

   Device Verification Code

   Enter EHome Key of the device. Used for ID verification during device connection.

   Domain

   Select the network domain that the access control device belongs to from the drop-down list.
5. Click **Save** to add the access control device.
6. **Optional:** Perform the following operation(s) after adding the access control device.

Search Device	Check **Include Sub-Area** to filter the devices. Set search conditions, and click **Search** to search access control devices as required.
Edit Device	Click to configure parameters for the access control device, including basic information, card reader information, parameters for door and card reader, etc. **Note** For details about configuring parameters for card reader and door, refer to ***Set Parameters for Card Readers*** and ***Set Parameters for Doors*** .
Online Test	Click to test whether the access control device is online.

Delete Device	Click to delete the access control device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete an access control device, all the information linked to the device will be deleted, such as permission configuration and so on. As a result, you may lose alarms or fail to update access control permissions.

9.2.5 Add Access Control Point to Area

After the access control devices are added to the system, you need to add the access control points of the access control device to an area for management.

Steps

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Access Control** to enter the Access Control page.
2. Select an area in the area list, and click **Access Control Point** to enter the access control point page.
3. Click **Add** to enter the Add Access Control Point page.
4. Select the area in the Current Area list.

   All access control points in the area will be listed in the Available Access Control Point list.
5. In the Available Access Control Point list, check access control point(s) to be added to the area.

   Note

   The system supports fuzzy search of the target access control point(s).
6. Click › to add the selected access control point.

   Note

   You can click ‹ to remove the added access control point(s) from the Selected Access Control Point list.
7. Click **Save**.
8. **Optional:** Perform the following operation(s) after adding the access control point to area.

Search Access Control Point	Check **Include Sub-Area** to filter the access control points. Set search conditions, and click **Search** to search the access control points as required.
Edit Access Control Point	Select an access control point, click to edit the information of access control point, including name, position description, and description.

Delete Access Control Point	Select an access control point, click to delete it. You can also select multiple access control points and click **Delete** to delete access control points in a batch.

9.2.6 Set Parameters for Encryption

If you have enabled Mifare card encryption function and set encryption sector when issuing a card to person, you need to set encryption parameters for access controller.

Steps

1. On the Home Page, click → **System Configuration** → **Devices** → **One-Card System** → **Access Control** .
2. Select an area in the area list, and click **Access Control Device** tab to enter the access control device page.
3. Click to enter Edit Access Control Device page.
4. Select an access controller from the left list.
5. Enable **Mifare Card Encryption**.
6. Select the encryption sector.

Note

The encryption sector you select here should be the same as that has been set in issuing a card to person.

9.2.7 Set Parameters for Doors

After the access control device is added to the system, doors linked to the device should be configured properly to take effect. You can edit the basic information and access control parameters (such as contact control mode, door open duration, duress code, etc.) for the doors.

Steps

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Access Control** to enter the Access Control page.
2. Select an area in the area list, and click **Access Control Device** to enter the access control device page.
3. Click in the **Operation** column to enter the Edit Access Control Device page.
4. Select the door to be configured from the list in the left.
5. Click **Get Parameter from Device** to get parameters from the door to the system.
6. Set parameters for the door.

Door Contact

The door contact's connection mode.

Exit Button Type

The exit button connection mode.

Door Open Duration

The time interval between the door is unlocked and locked again.

Door Open Duration by Card for Person with Disabilities

The time interval between the door is unlocked and locked again. The door open duration after swiping card for disabled person is usually longer than the normal door open duration.

Door Open Timeout Alarm

After enabled, if the access control device has been 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 Operation and Management Center will receive a duress event. It should be different from the super password. You can click **Enable Password** to set the duress code for the door.

Super Password

If you enter this password on the card reader keypad, you are exempted from all the remaining locked (Credential Failed), anti-passback, and first card authorization restrictions. It should be different from the duress code. You can click **Enable Password** to set the super password for the door.

7. Click **Save**.
8. Perform the following operation(s) after setting parameters for the door.

Set time for the door	Click **Set Time** to adjust the device time for the door.
Apply parameters to the door	Click **Apply Parameter to Device** to apply configured parameters to the door.
Restore default settings	Click **Restore to Default** to restore default settings for the door.

9.2.8 Set Parameters for Card Readers

After the access control device is added to the system, card readers linked to the device should be configured properly to take effect. You can edit the basic information and parameters (such as tampering detection, offline detection time, etc.) for the card readers.

Steps

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Access Control** to enter the Access Control page.
2. Select an area in the area list, and click **Access Control Device** to enter the access control device page.
3. Click in the **Operation** column to enter the Edit Access Control Device page.

4. Select the card reader to be configured from the list in the left.
5. Click **Get Parameter from Device** to get parameters from the card reader to the system.
6. Set parameters for the card reader.

Card Reader Information

Card Reader Name

Enter the customized card reader name.

Communication Method

Select the communication method between the access control device and the card reader according to wiring configuration.

Access Symbol

Select the access symbol as **Entrance/Exit** from the drop-down list.

Card Reader Dial-Up

You should set the correct dial-up on the card reader, and the card reader dial-up will display here.

Card Reader Type

Select the card reader type from the drop-down list according to the card reader capability.

Card Reader Model

Enter the card reader model.

Card Reader Parameter

Tampering Detection

After enabled, if the access control device has been 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.

Frequent Card Reading Failure Alarm

After enabled, if the access control device has been 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. For details about event configuration for access control devices, refer to ***Set Parameters for Doors*** .

Max. Limit of Card Reader Failure

Set the maximum failure attempts of reading card. The card reading failure alarm will be triggered if the failure attempts of reading card reach the limit.

Card Reader Offline Detection Time

When the access control device cannot connect with the card reader for a time period longer than the set time, the card reader will turn offline automatically.

Valid Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

Timeout Period of Pressing Button

When you enter the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

7. Click **Save**.
8. Perform the following operation(s) after setting parameters for the card reader.

Set time for the card reader	Click **Set Time** to adjust the time for the card reader.
Apply parameters to the card reader	Click **Apply Parameter to Device** to apply configured parameters to the card reader.
Restore default settings	Click **Restore to Default** to restore default settings for the card reader.

9.3 Access Control Settings

You can configure access control parameters in the system, including device parameters, permission parameters, and event parameters. Proper parameter configuration can give you a better experience of using the system.

9.3.1 Set Device Parameters

You can configure access control device parameters in the system, including the timeout period of authentication interval and capture settings of the access control terminal.

Steps

1. Click → **System Configuration** → **One-Card System** → **Access Control** → **Device Parameters** to enter the Device Parameters page.
2. Configure the parameters.

Timeout Period of Authentication Interval

Set the interval for authentications in Multiple Authentication mode. For the access control point configured with multiple authentication, when member A in a card group completes authenticating, member B should authenticate his/her identity within the authentication interval. Or the authentication procedures will restart.

Note

For details about multiple authentication, see ***Configure Multiple Authentication*** .

Capture Settings

Enable or disable the access control terminal to capture a picture when an access control event occurs.

9.3.2 Set Permission Parameters

In the Permission Parameters module, you can configure the permission-related parameters such as auto apply permission, retention period of permission applying record, copy permission settings from parent organization, etc. to realize the corresponding functions in the system.

On the Home Page, click → **System Configuration** → **One-Card System** → **Access Control** → **Permission Parameters** to enter setting permission parameters page.

Auto Apply Permission

The system supports automatically applying the access control permission information (including card permission, fingerprint, and face picture) to devices. Two methods for auto apply permissions are available: applying at fixed time of each day, and applying for fixed times in each day.

Apply for Fixed Times in Each Day

Set how many times the system will auto-apply the access control permission information, and then set a specific time point for each auto-apply.

Note

Over-frequent auto-apply may take excessive service resources. Take your service resource into account when setting the auto-apply times.

Apply at Fixed Time of Each Day

Set a start time for auto-apply, and then set the interval for auto-apply. For example, if you set 8:00 a.m. as the start time and 30 minutes as the interval, the system will automatically apply permissions to devices starting from 8:00 a.m. at an interval of 30 minutes each day.

Note

It is recommended you set the auto-apply time in non-peak hours of using the system such as the wee hours to avoid system exceptions.

Retention Period of Permission Applying Record

You can set the retention period of the permission applying records. When the retention period of a record expires, the record will be automatically deleted.

Copy Permission Settings from Parent Organization

You can enable the newly added organization to automatically copy permission settings from its upper-level organization.

Allow Platform to Verify Permission

If you enable this function, you can open door via the Control Client even if the access control permissions configured on the Web Client has not been applied to the access control devices.

9.3.3 Set Event Parameters

You can define specific types of access control events that the system can receive, and configure the retention period of the access control events.

Event Arming Control

The access control events you selected can be received by the system, while the unselected ones will be ignored.

Steps

1. Go to → **System Configuration** → **One-Card System** → **Access Control** → **Event Parameters** → **Select Event Type** .
2. Select an event type.

   Device Event

   Events related to the access control device, such as access controller tampering alarm, opening door remotely, and card reader tampering alarm.

   Normal Access Event

   The events in which the person's identity is authenticated by the access control point. In other words, the person enters or exits an access control point by authorized credentials, such as fingerprint and card.

   Access Exception Event

   The events in which the person's identity fails to be authenticated by the access control point. In other words, the person fails to enter or exit an access control point by authorized credentials, such as fingerprint and card.
3. Select specific events.
4. Click **Save**.

Configure Event Record Retention Period

You can set the retention period for the access control events. When the retention period of a specific event expires, the event record will be deleted automatically.

Steps

1. Go to → **System Configuration** → **One-Card System** → **Access Control** → **Event Parameters** → **Event Record Retention Period** .
2. Select a period from the drop-down list.
3. Click **Save**.

9.4 Access Permission

You can configure access permission in the system to define which persons can get access to which doors during the authorized time period. To realize this function, you need to add access control group and person group, configure access schedule template, assign access control permission, and apply permission to the device. After that, you can search the assigned access permission and check permission applying record.

9.4.1 Group Management

For convenient management, you can add access control group and person group in the system. For example, you can group access control points which can be accessed by persons in the same department; group persons who have the same access control permission during the same authorized time period.

Add Access Control Group

Access control group is a group of access control point(s). To define the access control permission, you need to add an access control group first and group the access control points.

Steps

1. Click **Access Control** on the Home page and enter **Group Management**.
2. Click **Access Control Group** tab to enter access control group management page.
3. Click **Add** to open the Add Access Control Group page.

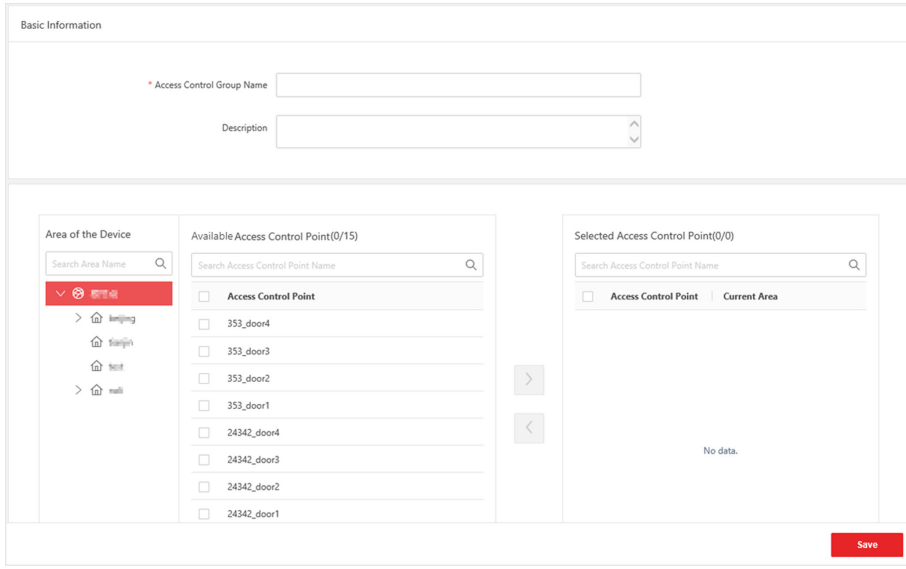


Figure 9-2 Add Access Control Group

4. Create a name for the access control group.
5. **Optional:** Enter the remark information in the Description textbox if needed.

6. Select the area to filter its access control point(s).
7. Check the access control point(s) from middle list and click › to add the access control points to the right list.
8. Click **Save** to add the selected access control point(s) to the group.

Add Person Group

Person group is a group of persons who have the same access control permission. The persons in the access control group can access the same access control points during the same authorized time period. For example, the persons in one department generally have the same permission, you can assign these persons to a group.

Before You Start

Make sure you have added the persons in the system. Refer to ***Person Management*** .

Steps

1. Click **Access Control** on the Home Page and enter **Group Management**.
2. Click **Person Group** tap to enter person group management page.
3. Click **Add by Organization** or **Add by Rule**.

   Add by Organization

   Select organization to filter person(s) and add the person(s) to the person group.

   Add by Rule

   Set rule to filter person(s), such as ID Type and gender, and add the person(s) to person group.
4. Create a name for the person group.
5. **Optional:** Enter the remark information in the Description if needed.
6. Select the persons.
   - For Add by Organization: Select the organization to filter its person(s). Check the person(s) from middle list and click › to add the persons to the right list.

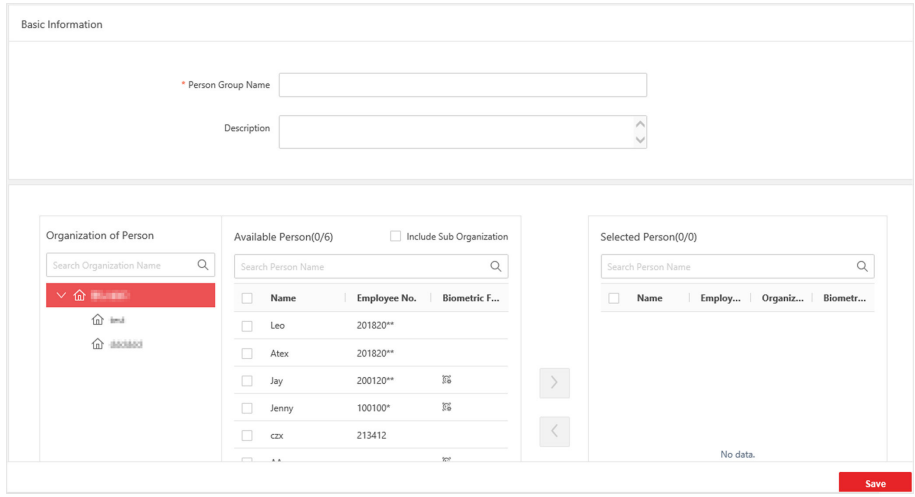


Figure 9-3 Adding by Organization

- For Add by Rule: Select the rule, relationship, and condition from drop-down list, respectively. For example, you can select: **Gender Equal to Male** to add males to person group. You can also click + or 🗑 to add another rule or delete the current rule.

7. Click **Save** to add the selected person(s) to the group.

9.4.2 Access Schedule Template

You can configure a schedule template for the permissions to define when the permission is valid to the person. After setting the templates, you can adopt the configured templates to access control permissions when setting the permission, so that the access control permission will take effect in the time durations of the template. The system provided default template or you can customize a template according to actual needs.

Add Holiday Group

Holiday group defines what time the access control permissions are valid in the holidays. During the holiday, the access control permissions' valid time period can be different with the normal days in week schedule.

Steps

1. Click **Access Control** on the Home Page and enter **Schedule Template**.
2. Click **Holiday Group** tab to enter holiday group management page.
3. Click **Add** to open the Adding Holiday Group page.
4. Create a name for the holiday group.
5. **Optional:** Enter the remark information in the **Description** textbox if needed.
6. Click **Add** on the left to add a holiday to the holiday group.
7. Set the time schedule for the holidays in the holiday group.

Note

The holidays cannot be overlapped with each other.

1) Set the start date and end date of the holiday.
2) Drag on the time bar of one holiday to draw the time schedule, which means in that period of time, the configured permission is activated.

   Note

   Up to 8 time periods can be set for each holiday.
3) **Optional:** Perform one of the following operations to edit the drawn time periods.
   - Move the cursor to the time period and drag the time period on the timeline bar to the desired position.
   - Click the time period and directly edit the start/end time in the appeared dialog. Or click **Delete** to delete the period.
   - Move the cursor to the ends of time period and drag to lengthen or shorten the time period.

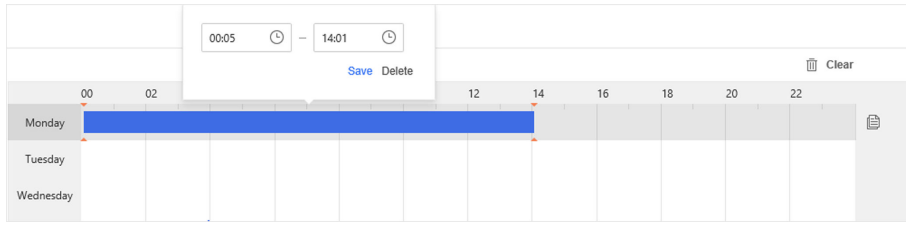


Figure 9-4 Edit Time Period

4) **Optional:** Delete the holiday
   - Click in Operation column to delete the corresponding holiday.
   - Check multiple holidays and click **Delete** on the left to delete all the selected holidays.

8. Click **Save**.

The added holiday group will be displayed in the list.

Add Schedule Template

You can add custom schedule template to make the access control permission valid or invalid in the configured schedule of the week. If you set the holiday schedule, the priority of holiday schedule is higher than the weekly schedule, which means the predefined holidays will adopt the holiday schedule rather than the weekly schedule.

Steps

1. Click **Access Control** on the Home Page and enter **Schedule Template**.

2. Click **Schedule Template** tab to enter schedule template management page.

Note

There is a default schedule: All-Day Schedule, which cannot be edited or deleted. For All-Day schedule, card swiping is valid on each day of the week.

3. Click **Add** to open the Add Schedule Template page.
4. Create a name for the schedule template.
5. **Optional:** Enter the remark information in the Description textbox if needed.
6. Add a weekly schedule.
   1) Click **Weekly Schedule** tab.
   2) Select a day of the week and draw time periods on the timeline bar.

      Note

      Up to 8 time periods can be set for each day in the weekly schedule.

   3) **Optional:** Perform one of the following operations to edit the drawn time periods.
      - Move the cursor to the time period and drag the time period on the timeline bar to the desired position.
      - Click the time period and directly edit the start/end time in the appeared dialog. Or click **Delete** to delete the period.
      - Move the cursor to the ends of time period and drag to lengthen or shorten the time period.
      - Move the cursor and click to copy the time period of this day to other day.

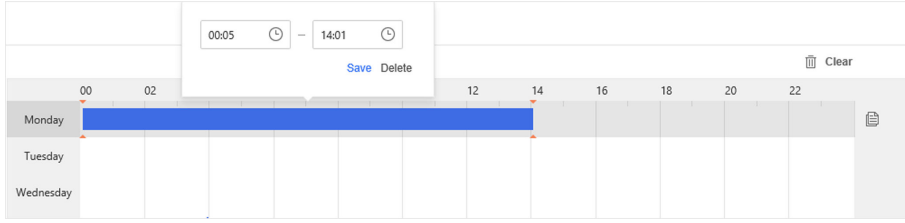


Figure 9-5 Edit Time Period

7. Add one or multiple holiday groups to schedule.
   1) Click **Holiday Schedule** tab.
   2) Click **Add**.
   3) Select a holiday group from drop-down list in Holiday Group column.
   4) **Optional:** Click to remove the holiday group or check multiple holiday groups and click **Delete** to remove them from the schedule.
8. Click **Save**.

   The added schedule template will be displayed in the list.

9.4.3 Access Permission Settings

You can assign the access control permissions to the persons so that these persons can access the access control point(s) with the assigned credentials, such as swiping the cards. You need to apply the permission settings to the device to take effect.

Assign Access Control Permission

You can assign access control permission to organization, person group or person so that persons can enter or exit specified access control point(s) during specified time period according to the assigned permission.

Steps

1. Click **Access Control** on the Home Page and enter **Permission Configuration**.
2. Select a tab as assigning permission mode.

   By Organization

   Assign access control permissions to persons in an organization to access specified access control point(s).

   By Person Group

   Assign access control permissions to persons in a person group to access the access control point(s).

   By Person

   Assign access control permissions to the specified person(s) to access the access control point(s).
3. Click **Add Permission** to enter add permission page.
4. Select a schedule template for the permission and the permission will take effect during time periods in the template.

   Note

   The schedule template should be configured before any permission settings. For details, refer to ***Access Schedule Template*** .
5. Select organization(s), person group(s) or person(s) from the appropriate list.

   Assign Permission by Organization

   Check organization(s) from left list and click › to add to the right list.

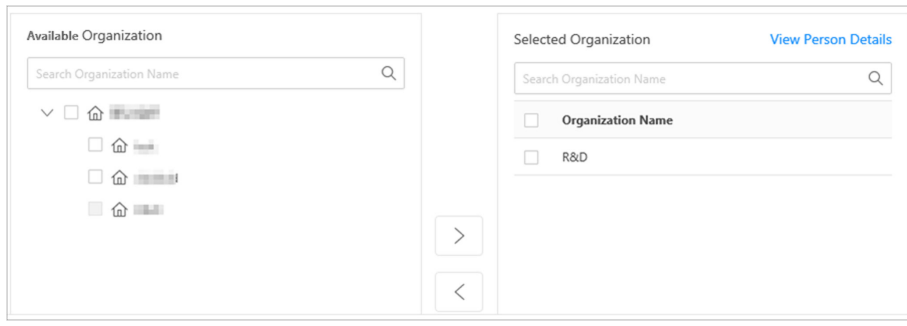


Figure 9-6 Assign by Organization

Assign Permission by Person Group

Check organization(s) from left list and click › to add to the right list.

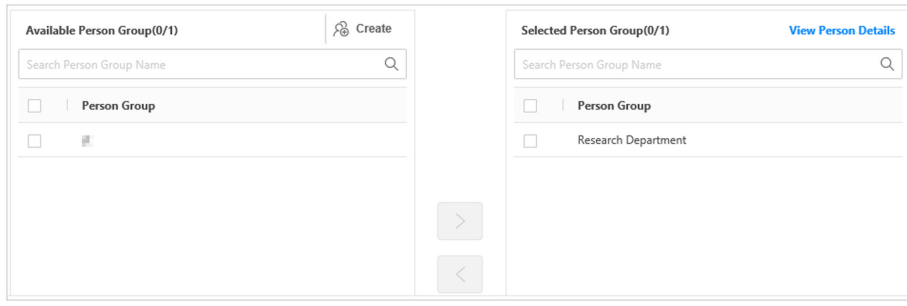


Figure 9-7 Assign by Person Group

Assign Permission by Person

Select an organization to filter the persons added in this organization. Then check person(s) from available person list and click › to add to the selected person list.

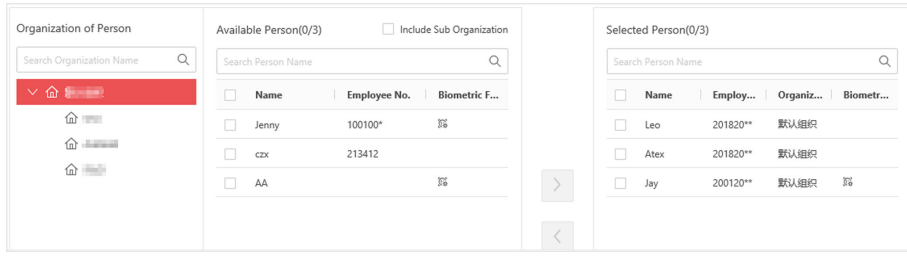


Figure 9-8 Assign by Person

6. Select Access Control Group or Access Control Point tab and select the object(s) to assign permission.

Access Control Group

Check access control group(s) from left list and click › to add to the right list. The permission of access control points in the group(s) will be assigned.

Access Control Point

Select an area to display its access control points. Check access control point(s) from middle list and click › to add to the right list. The permission of access control point(s) will be assigned.

7. Click **Save** to complete assigning permission.
8. In the pop-up window, click **OK** to save settings or click **Apply** to apply the permission to the device to take effect.

Apply Permission to Device Manually

After assigning access control permission to person, or if the person's permission is changed; you need to apply the permission to the access control device to take effect. After that, the persons can access the access control points during the authorized time period defined by the related permission.

Steps

1. Click **Access Control** on the Home Page and enter **Permission Configuration**.
2. Select permission applying mode.
   - Move the curse over near **Apply Permission** and click **Apply All** to apply all settings to the selected access control points.

     Note

     Apply All can clear previous permission of all persons, which will affect enter and exit the access control point during this period. It is recommended for the newly added devices.
   - Click **Apply Permission** to apply changes to the selected access control points.
3. Select the access control device(s).
4. Click **OK** to verify the operation.
5. Click **Apply** to start applying task.
6. **Optional:** Click to check the progress of the applying task.

Apply Fingerprint/Face Picture to Device

You can apply fingerprint or face picture to the access control device, so that the device can verifying the users' identities via the applied biometric recognition information.

Before You Start

Make sure you have collected fingerprints or face pictures for the persons and assigned access control permission to the persons.

Steps

1. Click **Access Control** on the Home Page.
2. Configure biometric identification.
   1) Enter **Biometric Recognition**.
   2) Select an area to filer the access control points.
   3) Click or .

4) Enable or disable the fingerprint or face function for the access control points.

3. Enter **Permission Configuration**.
4. Apply fingerprint or face picture.
   - Move the curse over near or button and click **Apply All** to apply all fingerprints or face pictures to the selected access control points.
   - Click **Apply Fingerprint** or **Apply Face Picture** to apply changed fingerprints or face pictures to the selected access control points.
5. Select the access control point(s) to apply to.
6. Click **OK** to verify the operation.
7. Click **Apply** to start applying task.
8. **Optional:** Click to check the progress of the applying task.

9.4.4 Search Assigned Permission

After adding the access control permissions, you can search the assigned permissions by setting the search conditions.

Steps

1. Click **Access Control** on the Home Page and enter **Permission Search**.
2. Set the search condition such as person name, employee No., organization, etc.
3. **Optional:** Click to set more conditions.
4. Click **Search**.

   The matched search results will display.

9.4.5 Check Permission Applying Record

For the failed applying tasks about access control permission, you can search them here, in order to apply them again.

Steps

1. Click **Access Control** on the Home Page and enter **Permission Applying Record**.
2. Set the search condition such as task code, controller, access control point, etc.
3. Click **Search**.

   The matched results will display.
4. **Optional:** Click in Details column to check applying result and export search result.

9.5 Advanced Functions

You can configure parameters in the system to realize the advanced functions of access control, including multiple authentication, anti-passback, multi-door interlocking, remaining open/closed, etc.

9.5.1 Configure Card Holder of Special Card

For some card holders who have special requirement or in certain scene, you can assign the added cards with different access control card types for the corresponding usage.

Before You Start

Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to ***Access Permission Settings*** . Perform this task to configure card for disabled person. The configurations about card in blacklist, duress card, and super card are similar to card for disabled person, and you can refer to this task for details.

Steps

Note

There are four card types supported.

Card for Disabled Person

The door will remain open for the configured time period for the card holder. It is usually used for people with mobility difficulty.

Card in Blacklist

The card swiping action will be reported and the door cannot be opened.

Duress Card

Duress card is used when person is under duress. The door will be unlocked when he/she swipes the card and the Control Client will receive a duress alarm (if configured) to notify the security personnel.

Super Card

The card is valid for all the doors of the controller during the configured schedule.

1. On the Home Page, click **Access Control → → Advanced Functions → Card Holder of Special Card** .
2. Click **Card for Disabled Person** tab.
3. Click **Add**.
4. Click an area to filter the access control device(s).
5. Check access control device and click › to add it to the right list.
6. Click **Save**.

   The added access control device will be displayed in the list with the status of **Not Configured**.
7. Select card as card for disabled person.
   1) Click in Operation column to enter select card page.
   2) Select the organization to filter the card holder(s).

      The persons in the selected organization and the person's card will be displayed.
   3) Select the cards and click › to add them to the right list.
   4) Click **Save** to set the cards as card for disabled person.

8. Click in Operation column to apply the new settings to the device to take effect or select multiple configured access control devices and click **Apply Parameter** to apply new settings to the selected devices to take effect.

9.5.2 Configure Multiple Authentication

The door in certain important site requires to be opened by multiple authentications from different persons for security purpose. You can manage the cards by group and set the authentication for multiple cards for one access control point.

Before You Start

Make sure you have assigned the access control permission and applied the permission to the access control device first. For details, refer to ***Access Permission Settings*** .

Steps

1. On the Home Page, click **Access Control → Advanced Functions →** **Multiple Authentication** .
2. Add a card group.
   1) Click **Card Group** tab to open card group management page.
   2) Click **Add** to set group information.
   3) Create a name for the card group as desired.
   4) Specify the effective time and expired time as the valid period.
   5) Select card(s) to add to the card group.
   6) Click **Save**.
3. Click **Authentication Method** tab.
4. Add access control point(s) for multiple authentication.
   1) Click an area to filter the access control point(s).
   2) Check access control point and click › to add it to the right list.
   3) Click **Save**.

   The added access control point will be displayed in the list with Status of **Not Configured**.
5. Set the authentication rule.
   1) Click in Operation column to show set authentication rule page.
   2) Click **Add Authentication Group**.
   3) Select schedule template. For details about setting the template, refer to ***Access Schedule Template*** .
   4) Select an authentication method.

      Local Authentication

      Authenticate via the access control device. When the persons swipe the cards in the card group, the door will be opened.

      Local Authentication + Remotely Opening Door

      Authenticate via the access control device and opening door via the system. After the persons swipe the cards in the card group, opening door operation on the Control Client is required to open the door.

Local Authentication + Super Permission

Authenticate via the access control device and inputting the super password. When the persons swipe the cards in the card group, and then input the super password, or swipe the super card, the door will be opened.

5) Set authentication group, including card group and swiping times.
6) Click **Add** to add other authentication group and set the parameters.

Note

You can drag the added authentication group up and down to change swiping order.

7) **Optional:** If **Local Authentication + Remotely Opening Door** is selected, set **Center Secondary Authentication** switch to on and set required parameters to verify the person for remote operation.
8) Click **Save**.

6. Click in Operation column to apply the new settings to the device to take effect or select multiple configured access control devices and click **Apply Parameter** to apply new settings to the selected devices to take effect.

9.5.3 Configure First Card Opening Door

You can set multiple first cards for one access control point. After the first swiping, the door remains open and allows multiple persons access the door until the end of the period. If you swipe the first card again, the door can restore the normal status. It is usually used in the scenarios such as inspection or visit, which requires the door to remain open for a period.

Before You Start

Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to ***Access Permission Settings*** .

Steps

1. On the Home Page, click **Access Control → Advanced Functions →** **First Card Opening Door** .
2. Click **Add**.
3. Click an area to filter the access control device(s).
4. Check access control device and click › to add it to the right list.
5. Click **Save**.

The added access control device will be displayed in the list with the status of **Not Configured**.

6. Set first card.
1) Click in Operation column to show set first card page.

The access control points of the access control device are displayed.

2) Enable first card opening door function for the access control point.
3) Set the time duration of remaining open.
4) Select the organization to filer the card holder(s).

The persons in the selected organization and the person's card will be displayed.

5) Select the card and click › to add to the selected first card list.

6) Click **Save** to set the card as first card.

7. Click in Operation column or click **Apply Parameter** to apply the new settings to the device to take effect.

9.5.4 Configure Anti-passback

The anti-passback feature is designed to minimize the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. The anti-passback rule establishes a specific sequence in which cards must be swiped in order to grant access. The person should exit via the access control point in the anti-passback path if he/she enter via the access control point added in the anti-passback path.

Before You Start

Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to ***Access Permission Settings*** .

Steps

1. On the Home Page, click **Access Control → Advanced Functions →** **Anti-Passback** .
2. Click **Anti-Passback (Single Device)** or **Anti-Passback (Multiple Devices)**.
3. Click an area to filter the access control device(s).
4. Check an access control device and click › to add it to the right list.
5. Click **Save**.

   The added access control device will be displayed in the list with the status of **Not Configured**.
6. Set anti-passback rule.
   1) Click in Operation column to show set anti-passback rule page.

      The access control points of the access control device are displayed.
   2) Select the card reader as the beginning of the path.
   3) In the list, click the field of **Card Reader Afterward** and select the linked card reader.
   4) Enable the anti-passback function for the card reader.
   5) Click **Save**.
7. Click in Operation column or click **Apply Parameter** to apply the new settings to the device to take effect.

9.5.5 Configure Multi-Door Interlocking

You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Before You Start

Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to ***Access Permission Settings*** .

Steps

1. On the Home Page, click **Access Control → Advanced Functions →** **Multi-Door Interlocking** .
2. Click **Add**.
3. Click an area to filter the access control device(s).
4. Check access control device and click › to add it to the right list.
5. Click **Save**.

   The added access control device will be displayed in the list with the status of **Not Configured**.
6. Set multi-door interlocking.
   1) Click in Operation column to show setting page.
   2) Select interlocking type according to the door number of device.
   3) Select the doors to add to the interlocking combination.
   4) Enable multi-door interlocking for the combination.
   5) Click **Save**.
7. Click in Operation column or click **Apply Parameter** to apply the new settings to the device to take effect.

9.5.6 Configure Reader Authentication Mode

You can set the passing rules for the card reader of the access control device according to your actual needs.

Before You Start

Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to ***Access Permission Settings*** .

Steps

1. On the Home Page, click **Access Control → Advanced Functions →** **Reader Authentication Mode** .
2. Add card reader for setting authentication mode.
   1) Click **Add**.
   2) Click an area to filter the card reader(s).
   3) Check card reader and click › to add it to the right list.
   4) Click **Save**.

      The added card reader will be displayed in the list with the status of **Not Configured**.
3. Set authentication mode.
   1) Click in Operation column to show set authentication mode page.
   2) Select a card reader authentication mode.

      Note

      The available authentication modes depend on the carder type.
   3) Drag on the time bar of one day to draw the time schedule, which means in that period of time, the card reader authentication is valid.

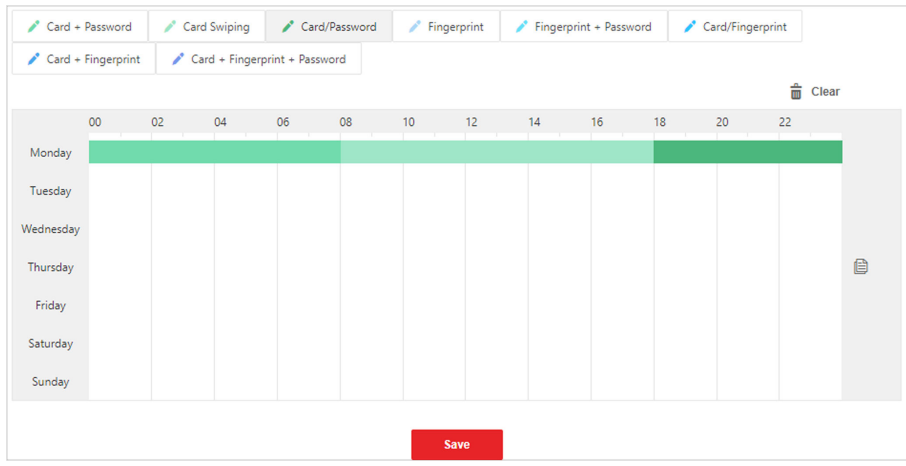


Figure 9-9 Draw Time Schedule

4) **Optional:** Perform one of the following operations to edit the drawn time periods.
   - Move the cursor to the time period and drag the time period on the timeline bar to the desired position.
   - Click the time period and directly edit the start/end time in the appeared dialog. Or click **Delete** to delete the period.
   - Move the cursor to the ends of time period and drag to lengthen or shorten the time period.
   - Move the cursor and click to copy the time period of this day to other day.
5) Click **Save**.

4. Click in Operation column or click Apply Parameter to apply the new settings to the device to take effect.

9.5.7 Configure Remaining Open/Closed

You can schedule weekly time periods for an access control point (door) to remain open or closed.

Before You Start

Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to ***Access Permission Settings*** .

Steps

1. On the Home Page, click **Access Control → Advanced Functions →** **Remain Open/Closed** .

2. Add access control point for setting access control status.
   1) Click **Add**.
   2) Click an area to filter the access control point(s).
   3) Check access control point and click › to add it to the right list.
   4) Click **Save**.

   The added access control point will be displayed in the list with the status of **Not Configured**.

3. Set schedule for remaining open or closed.
   1) Click in Operation column.

2) Select an access control status.

Remain Open Period

The door will keep open during the configured time period.

Remain Closed Period

The door will keep closed during the configured time period.

3) Drag on the time bar of one day to draw the time schedule, which means in that period of time, the access control status is valid.

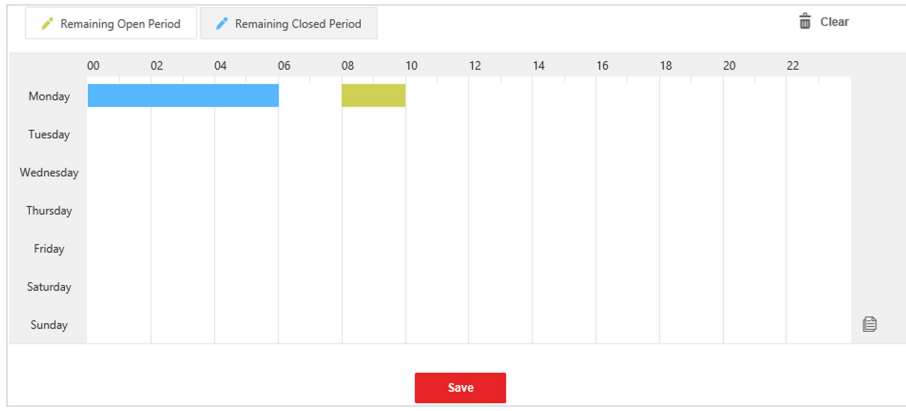


Figure 9-10 Set Schedule for Remaining Open or Closed

4) **Optional:** Perform one of the following operations to edit the drawn time periods.
   - Move the cursor to the time period and drag the time period on the timeline bar to the desired position.
   - Click the time period and directly edit the start/end time in the appeared dialog. Or click **Delete** to delete the period.
   - Move the cursor to the ends of time period and drag to lengthen or shorten the time period.
   - Move the cursor and click to copy the time period of this day to other day.

5) Click **Save**.

4. Click in Operation column or click **Apply Parameter** to apply the new settings to the device to take effect.

9.5.8 Configure Capture Linkage for Video Access Control Terminal

The access control device linked with camera, such as access control terminal and video access control terminal, can capture pictures for specific access control events. By configuring capture linkage for the devices, when the access control event (e.g., duress alarm) occurs, the camera will capture the pictures as evidence. Then you can search person access event to view the captured pictures.

Before You Start

Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to ***Access Permission Settings*** .

Steps

1. On the Home Page, click **Access Control → Advanced Functions →** **Access Control Terminal Linkage** .
2. Add access control device for setting capture linkage.
   1) Click **Add**.
   2) Click an area to filter the access control device(s).
   3) Check access control device and click › to add it to the right list.
   4) Click **Save**.

   The added access control device will be displayed in the list with the status of **Not Configured**.
3. Set event type for triggering capture action.
   1) Click in Operation column.
   2) Select event type(s).

   Note

   The displayed event types may vary for different access control devices.
   3) Click **Save**.
4. Click in Operation column or click **Apply Parameter** to apply the new settings to the device to take effect.

9.6 Search Person Access Event

When the persons go access door, the card swiping record or other authentication records will be saved in the system. You can search the relative events, such as blacklist event, no permission event and so on, and export the records to local PC.

Steps

1. Click **Access Control** on the Home page and enter **Person Access Event**.
2. Set the search conditions, such as device name, event type, event time, and so on.
3. Click **Search** to start searching the access events.

   The matched access events will be displayed.
4. **Optional:** After searching the events, you can do one or more of the followings.

   View Captured Picture

   For events contain related pictures, click the icon on Captured Picture column to view the captured picture of the relative camera when the event is triggered.

   Note

   This function should be supported by the device and the capture linkage of relative events are configured. Refer to ***Configure Capture Linkage for Video Access Control Terminal*** for details.

   Export Event Record

   Click Export to export the search results to local PC.

Synchronize Access Control Device

Click **Sync** and select the access control device(s) to synchronize access control events to the device(s).

9.7 Search Access Control Device Event

You can search the access control events stored on the access control device, which can help you to get the door status at that time.

Steps

1. Click **Access Control** on the Home Page and enter **Device Event**.
2. Set the search conditions, such as access control point, card reader, event type, event time, and so on.
3. Click **Search** to start searching the access control events.

   The matched access control events will be displayed.
4. **Optional:** Click **Export** to export the search results to local PC.

Chapter 10 Visitor Management

HikCentral Enterprise-Commercial provides visitor management system which provides visitor management and registration solution. Core features include visitor registration, message notification, visitor reservation, visitor pass, etc.

10.1 Flow Chart

If this is the first time you use Visitor, we recommend you perform configurations according to the chart below.

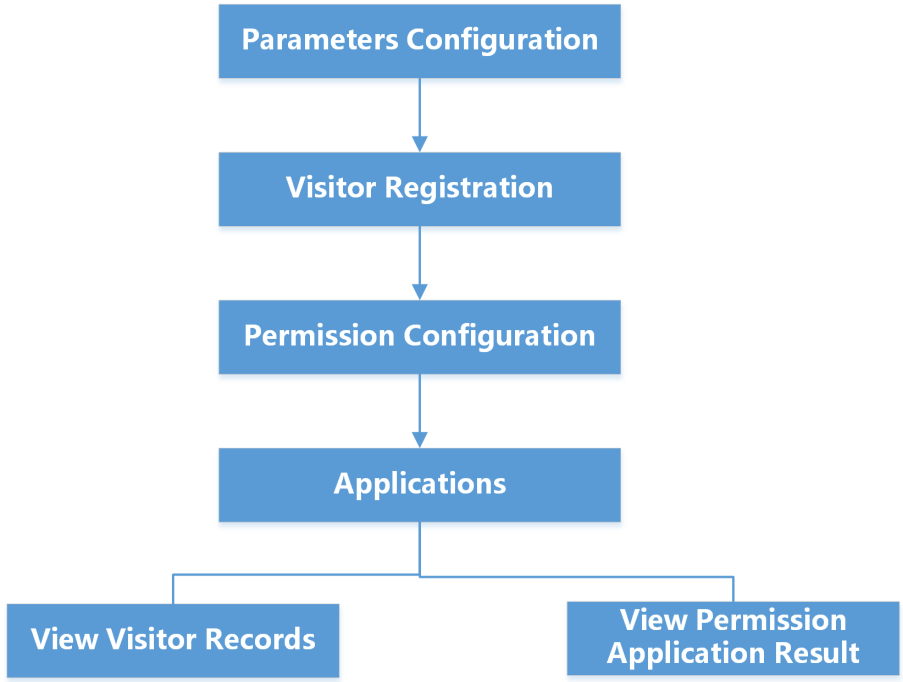


Figure 10-1 Operation Flow Chart

10.2 Visitor Parameter Settings

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, set the saving path of the pictures, etc.

10.2.1 Basic Parameters

In this section, you can set the basic parameters for the actual visiting scenario. By configuring basic parameters of different scenes, you can set different modes for reservation and visitor check-in.

Click → **System Configuration** → **One-Card System** → **Visitor** → **Basic Configuration** .

ID No.

Set whether the ID No. of the visitors are required when making a reservation and when the visitors check-in.

Check-in Not Required If Reserved

For the visitors who have made reservations in the system, whether they should check in at the reception when they arrive.

Person to Be Visited

Set whether the person to be visited is required to fill when the visitors check-in.

Visiting Mode

Set how many verification codes should be generated when reserving a visit of multiple visitors.

One Person One Code

When reserving a visit, you should enter the information of all the visitors. All the visitors will get a verification code.

Multiple Persons One Code

When reserving a visit, you should enter the information of one of the visitors, and this person will receive a verification code.

Visitor Certificate

Set what kind of certificate will be issued to the visitor after check-in.

Visitor Pass

A ticket with visitor information and a QR code which contains permissions such as access permission, parking permission, etc.

Note

Make sure the devices supports QR code scanning.

Visitor Card

A card which records the visitor information and contains permissions such as access permission, parking permission, etc.

Note

Make sure the devices supports card reading.

Auto Check-Out

If the visitor is not checked-out at 23:59, check out the visitor automatically.

Early Check-in Time

Set the minutes of early check-in before the visiting time in the reservation. For example, if you set 60 minutes, the visitor can check-in 60 minutes before the visiting time if he/she arrives early.

Default Visitor Leaving Time

The default leaving time when making a reservation.

10.2.2 Set Visitor Information Fields

You can select the information fields to enter for visitor registration, and set the fields as required or optional according to your needs.

Steps

1. Click → **System Configuration** → **One-Card System** → **Visitor** → **Visitor Information Field** .

Note

By default, visitor name is shown and required.

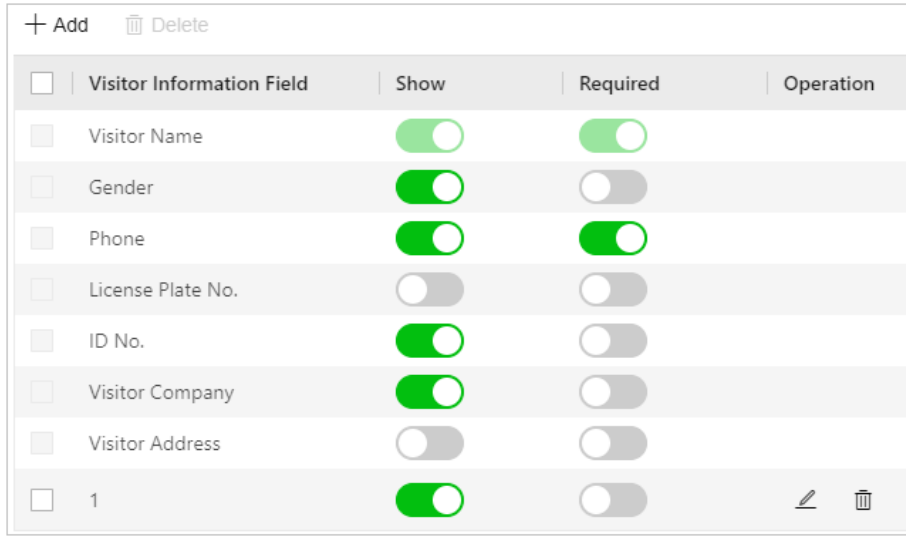


Figure 10-2 Visitor Information Fields

2. Enable a field.
   - Switch on the button in the Show column, and the field will be displayed on the visitor registration page as optional. You can complete registration without entering information in this option.
   - Switch the buttons respectively in the Show column and Required column, and the field will be displayed on the visitor registration page as required. You cannot complete registration without entering information in this option.
3. **Optional:** Add a new field.

1) Click **Add** to open the Customize Visitor Information Field window.

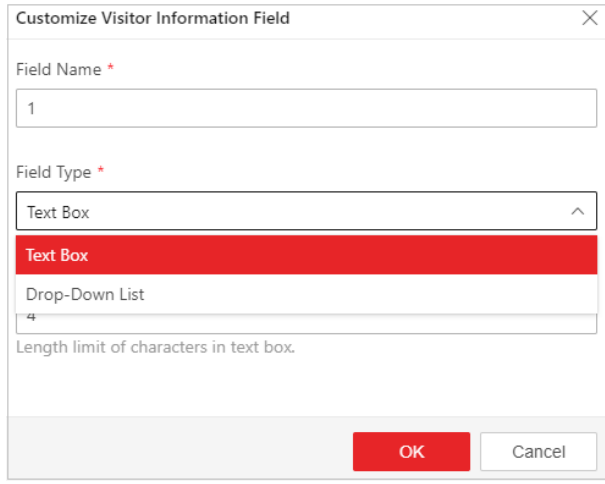


Figure 10-3 Add Visitor Information Field

2) Enter the Filed Name.
3) Select Field Type.

Text Box

If you select this, the newly added field will be displayed as a text box to enter characters as visitor information.

Drop-Down List

If you select this, you will be required to add at least one option which will be displayed on the visitor registration page. When you are registering for a visitor, you can select an option in the drop-down list.

4) Enter the Length Limit.
5) **Optional:** Perform the following operations.
   - Click in the Operation column to edit the name or length limit of a newly added field.
   - Click in the Operation column to delete a newly added field.

10.2.3 Set Visitor Permissions

You need to pre-define different permissions for the visitors, including access permissions (the visitors can access which access points), elevator control permissions (the visitors can access which floors), parking permissions (the visitors can access which parking lots), etc.

Steps

1. Click → **System Configuration** → **One-Card System** → **Visitor** → **Visitor Permission** .
2. Select a permission type, and click **Add**.
3. Select the resources that the visitors can access.

Access Control Permission

Select the access control points (doors) that the visitors can access.

Elevator Control Permission

Select the floors that the visitors can access.

Parking Lot Permission

Select the parking lots that the visitors can access.

4. Click > to add the selected resources.
5. Click **Save**.

What to do next

These permissions added here are units of permissions. You need to group them into different permission groups which can be assigned to the visitors when check-in. For grouping permissions, refer to ***Group Permissions*** .

10.2.4 Pre-Define Visit Purpose

In this section, you can pre-define several purposes for the unreserved visitors to select when they check-in their visit.

Steps

1. Click → **System Configuration** → **One-Card System** → **Visitor** → **Purpose of Visit** .
2. Click **Add**.
3. Enter the description of the purpose, e.g., training.
4. Click **OK**.

10.2.5 Set Template for Visitor Pass

The visitors need to check-in at the reception or at the terminals when they come. After check-in, they will get a pass which can be used as access credential. In this section, you can define a template for the visitor pass, including the background picture, content, etc.

Steps

1. Click → **System Configuration** → **One-Card System** → **Visitor** → **Visit Pass Template** . The system pre-defines two templates, which cannot be deleted.
2. Click **Add**.
3. Enter a name for the template.
4. Select the shape of the template as vertical or horizontal. You can preview the pass below.
5. Set the content on the pass.
   - Click **Upload Background Picture** to select a picture as the background on the pass. You can click **Restore Default Picture** to reset it.
   - Set the lines on the pass, such as title, visitor name, QR code, etc. You can drag the lines to sort them according to actual needs.
6. Click **Save**.

10.2.6 Set Message Notification Content

The system can send short messages to the visitors and persons to be visited to notify them the verification code, etc.

Click → **System Configuration** → **One-Card System** → **Visitor** → **Message Notification Content** .

Notify Visitor of Successful Reservation

If you make a reservation successfully, the system will send a message to the visitors in the reservation to notify them.

Notify Visitor of Reservation Cancellation

If you cancel a reservation, the system will send a message to the visitors in the reservation to notify them.

Notify Visitee of Successful Reservation

If you make a reservation successfully, the system will send a message to the person to be visited in the reservation to notify them.

Notify Visitee of Visitor Check-in

When the visitor(s) check in, the system will send a message to the person to be visited in the reservation to notify them.

Notify Visitee of Visitor Check-out

When the visitor(s) check out, the system will send a message to the person to be visited in the reservation to notify them.

10.2.7 Set Access Control Point for Self-Service Check-Out

Set the access control points (doors) at which the visitors can check-out by themselves by swiping the cards or scanning the QR codes.

Steps

Note

After checking out at the check-out point, all the permissions assigned to this visitor will be invalid.

1. Click → **System Configuration** → **One-Card System** → **Visitor** → **Self-Service Check-Out Point** .
2. Click **Add**.
3. Select the area and the access control point(s) belong to this area will display.
4. Select the access control point(s) and click .
5. Click **Save**.

10.2.8 Group Visitors

You can pre-defines some groups of visitors who come to visit frequently. When making a reservation, you can select a visitor group to make a reservation for them in a batch.

Steps

1. Click → **System Configuration** → **One-Card System** → **Visitor** → **Visitor Group** .
2. Add a group first.
   1) Click + to add a group.
   2) Enter a name for the group.
   3) Click **OK**.
3. Add visitors to the group.
   1) Select a group and click **Add**.
   2) Enter the person name.
   3) Select the ID type and enter the ID No. of the person.
   4) Click **OK**.
4. You can also import multiple visitor groups in a batch.
   1) Click .
   2) Click **Download File Template** to download a template file in CSV format.
   3) Enter the visitor information and group name in the template. You can hover the cursor on **Field Description** to view the descriptions of different fields in the template.

      Note

      Up to 300 records can be imported.
   4) Click **Select** and select the template file filled with visitor information.
   5) Click **Import** to start.

10.2.9 Set Retention Time of Visitor Records

Retention time of visitor records indicates how long the visitor records in the system will be saved for. When the retention time is due, the visitor records will be deleted.

Click → **System Configuration** → **One-Card System** → **Visitor** → **Visitor Records Retention** . The visitors' visiting records are saved in the system database. You can set how long these records can be saved. Once expired, the records will be deleted.

10.2.10 Enable Visitor Self-Service Reservation

After enabling visitor self-service reservation, the visitor can make a reservation by a mobile phone. You need to configure related parameters after enabling this function.

Click → **One-Card System** → **Visitor** → **Visitor Self-Service Reservation** .

Switch **Visitor Self-Service Reservation** on and set the following parameters. Select

Select a server of the platform. You can select **Customize** and configure IP address, network protocol, and port number to set a customized server.

Reservation URL

A visitor opens this reservation URL by a mobile phone browser to make a reservation.

QR Code

A visitor scans the QR code by a mobile phone to open the reservation page to make a reservation.

Click **Save** to save the settings.

10.3 Visitor Reservation

The system manager can make a reservation for the visitors by entering the visitor and visitee information in the system. After reservation, when the visitor checks in, the manager can view the reservation details and assign proper permission group to the visitor.

10.3.1 Make a Reservation for One Visit

You can make reservation for one visit one by one by entering the visitor and visitee information in the system.

Steps

1. 1. Click **Visitor** on Home page and enter **Visitor Reservation**.
2. Click **Reserve**.
3. Enter the information of the person to be visited.
4. Set the estimated time of the visit, including time for arrival and time for leave.
5. **Optional:** Select a purpose of the visit.
6. Enter the visitor(s) information.
   1) Click **Add** in the Visitor Information panel.
   2) Enter the visitor name, gender, phone number, and other information.
7. Click **Save**.

10.3.2 Import Reservations for Visitors

You can also import multiple reservations in a batch by importing a file with information of reservations to the system.

Steps

1. 1. Click **Visitor** on Home page and enter **Visitor Reservation**.
2. Click **Import**.
3. Click **Download File Template** to download a template file in CSV format.

4. Enter the reservation information in the template including visitor and visitee information. You can hover the cursor on **Field Description** to view the descriptions of different fields in the template.

   Note

   Up to 200 records can be imported.

5. Click **Select** and select the template file filled with reservation information.
6. Click **Import** to start.

10.4 Group Permissions

After adding the visitor permissions, you need to group them into different groups. After that, when the visitors check in, you can assign proper permission groups to them. For example, you can group the permission of door 1, permission of floor 1, and permission of parking lot 1 into visitor permission group 1. After assigning permission group to the visitor, the visitor can access the door 1, floor 1, and parking lot 1 with the visitor pass.

Before You Start

You should add the visitor permission to the system first.

Steps

1. Click **Visitor** on Home page and enter **Visitor Permission Group**.
2. Click **Add** to add a new permission group.
3. **Optional:** Double click the Permission Group Name and Description field to enter a name for the group and the description information.
4. Click in the Operation column to set the permission(s) in the group.
   1) Select a permission type.
   2) Select the area and all the resources in this area which have been added as visitor permissions will display.
   3) Select the resource(s) and click .
   4) Click **Save**.
5. **Optional:** Perform the following operations after adding the permission group.
   - Click in the Operation column to edit the permissions in the group.
   - Click in the Operation column to delete this group from the system.
   - Select the vehicle(s) and click **Delete** to delete the selected ones.
   - Click in the Operation column to set this permission group as the default one. When the visitor(s) check in, the default permission group will be stuck on top when assigning the permission group to the visitor(s) on the Visitor Client.

Note

Only one permission group can be set as default. For example, if you set group B as default group on the premise that group A has already been set as default, group B will replace group A as the default group.

10.5 Search Visit Records

The visit records are stored in the system database after the visitors' check-in, such as the visiting time, visitor detail, visitee details, and you can view the access records such as the card swiping records at floors, QR code recognition records at doors, license plate recognition at parking lots, etc.

Steps

1. Click **Visitor** on Home page and enter **Visit Records**.
   All the visit records are displayed in the list sorted by time.
2. **Optional:** Click in the Operation column to view the visit details including the visitors, visitee, visit time, captured pictures, etc.
3. **Optional:** Enter the conditions to filter the records.
4. Click in the Operation column to view the visitors' access records such as the card swiping records at floors, QR code recognition records at doors, license plate recognition at parking lots, etc.
5. **Optional:** Add the visitor(s) to the visitor group.
   - Click in the Operation column and select a visitor group to add the visitor to the group.
   - Select the visit records and click **Add to Visitor Group** and select a group to add the selected visitors to the group.
6. **Optional:** Click **Export** to export the filtering results displayed in the list and save it in the local PC.

10.6 View Unauthorized Visit Records

When the visitors check in, the manager should assign specified visitor permission group to the visitors, so that the visitors can access some floors, doors, parking lots, with the issued credentials (cards or passes). If they access the location with the credential (such as swiping the cards, or scanning QR code, scanning fingerprints, recognizing face) on the card readers or scanners of the floors, doors, parking lots which are not authorized, the access will be denied and these access records will be recorded in the system database.

Steps

1. Click **Visitor** on Home page and enter **Unauthorized Access Records**.
   All the access records (access denied) are displayed in the list sorted by time.
2. View the access details such as visitor name, credential type, recorded time, etc.

3. Enter the conditions to filter the access records.
4. Add the visitor(s) to the visitor group.
   - Click in the Operation column and select a visitor group to add the visitor to the group.
   - Select the visit records and click **Add to Visitor Group** and select a group to add the selected visitors to the group.

10.7 View Permissions Applied to Visitors

The system should apply the permission request to the devices in the following situations:

Before You Start

- When the visitors check in, the manager should assign specified visitor permission group to the visitors. After assignment, the system will apply these permission settings in the group to the devices related so that the visitor permissions can take effect..
- When the visitors check out, the system will apply the check-out request to the devices again to delete the related permissions on the devices.
- You can change the permissions via the Visitor Client, and the system will apply the changed permissions to the devices so that the changes can take effect.

The above processes are recorded in the system database.

Steps

1. Click **Visitor** on Home page and enter **Permission Applying Records**.
2. View the visitor permission applying details such as visitor credential details, applying status, device applied to, etc.
3. Enter the conditions to filter the records.
4. If the process of applying permission is failed, you can process again.
   - Click in the Operation column to process the permission again, such as applying the permission again, checking out again, etc.
   - Select the records and click **Process Again** to process the selected permissions again.

Chapter 11 Video Intercom

Video intercom is an audiovisual communication and security technique used in a building or a small collection of buildings. With microphones and video camera devices 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.

Be sure to add video intercom devices and persons to HikCentral Enterprise-Commercial beforehand. You can issue card to the persons, set the access authorization for the persons and apply to the devices. The authorized persons can access the doors using the credentials. You can also check person access events and device events to locate the persons' information and the device's status at that time.

11.1 Flow Chart

For the first time, you can follow the flow chart to perform configurations and operations.

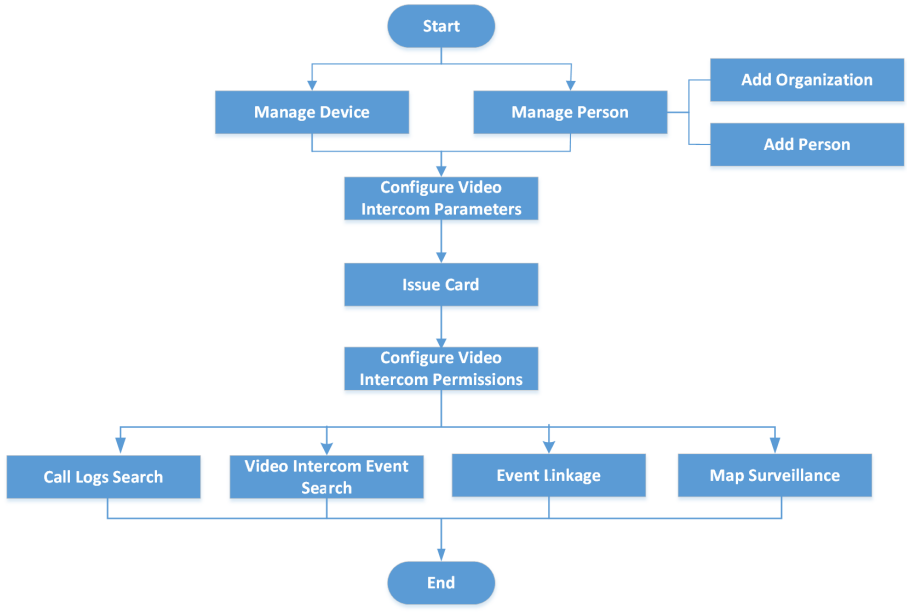


Figure 11-1 Flow Chart of Video Intercom

- **Manage Device**: Add video intercom devices (such as master station, outer door station, indoor station, and door station) to the platform. For more details, refer to ***Video Intercom Device Management*** .
- **Manage Person**: Add organization and person to the platform.
- **Configure Video Intercom Parameters**: Configure device parameters, permission parameters, and event parameters. For more details, refer to ***Video Intercom Configuration*** .
- **Issue Card**: Issue cards to persons.

- **Configure Video Intercom Permissions**: Assign video intercom permissions to organization and persons. For more details, refer to ***Video Intercom Permission Configuration*** .
- **Call Logs Search**: Search call logs of video intercom devices. For more details, refer to ***Call Log Search*** .
- **Video Intercom Event Search**: Search person entering/exiting events and device events. For more details, refer to ***Event Search*** .
- **Event Linkage**: Configure linkage actions for the video intercom events. When an event is detected, the system will receive the real-time information of the event and linkage actions will be triggered.
- **Map Surveillance**: Add video intercom resources to the map. When the alarm is triggered, you can view the live view and playback of the added resources on the map, and get a notification message from the map.

11.2 Video Intercom Device Management

You can add the video intercom devices (e.g., master station, outer door station, door station, and indoor station) to HikCentral Enterprise-Commercial for management and configuration.

Note

Make sure the video intercom 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 Enterprise-Commercial via network.

11.2.1 Add Master Station

The master station is a intelligent terminal used for responding and sending residents call, unlocking door remotely, etc. It is normally installed on the management center, and can be operated with a capacitive touch screen, touch buttons and mechanical buttons. You can add master station to HikCentral Enterprise-Commercial by specifying IP address and related parameters for management and further video intercom applications.

Steps

1. Click → **System Configuration** → **Devices** → **One Card System** → **Video Intercom** to enter the video intercom device management page.
2. Select an area in the area list to add the video intercom device.
3. Click **Master Station** tab.

   The added master stations will be displayed in the list. You can search the desired master station by set conditions, such as device name, device type, IP address, and password strength.
4. Click **Add** to enter the Add Master Station page.
5. Set required parameters.

   Device Name

   Customize a name for the video intercom device.

Set as Main Master Station

Set the switch to on to set the added device as main master station.

Device Type

Select the device type according to the device capability. The default one is embedded master station.

Access Protocol

Hikvision Device Network SDK Protocol is selected by default for realizing communication according to the Hikvision Device Network SDK.

IP Address

Enter the IP address of the video intercom device.

Port No.

Enter the device port No. The default value is 8000.

User Name

Enter the user name of the video intercom device. By default, the user name is admin.

Password

Enter the password of the video intercom device.

Caution

The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including 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.

Domain

The network domain that the video intercom device belongs to, which is used for multi-domain network scenario.

Note

For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

Management Partition

If the community is divided into multiple management areas, enter the correct value. If not, enter 1.

Installation Position Description

Information for describing device installation position or device code. For example, Area 1 Property Management Center 01.

6. Click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the video intercom device and click **Online Test** to start online test again.
7. Click **Save** to add the video intercom device.
8. **Optional:** Perform the following operation(s) after adding the video intercom device.

Filter Device	Check **Include Sub-Area** to display the added devices in this area and its lower-level areas, or click **Search** to filter devices by specific conditions.
Edit Device Information	Click on Operation column to edit information for the video intercom device.
Delete Device	Click on Operation column to delete the video intercom device. You can also select multiple devices and click **Delete** to delete devices in a batch.
	Note If you delete a video intercom device, all the information linked to the device will be deleted, such as permission configuration and so on.
Online Test	Click to check whether the video intercom device is online.

11.2.2 Add Outer Door Station

The outer door station is mainly applied in the villa and community, and provides reliable security assurance and convenient visit calling service. You can add outer door station to HikCentral Enterprise-Commercial for management and further video intercom applications.

Steps

1. Click → **System Configuration** → **Devices** → **One Card System** → **Video Intercom** to enter the video intercom device management page.
2. Select an area in the area list to add the video intercom device.
3. Click **Outer Door Station** tab.

   The added outer door stations will be displayed in the list. You can search the desired outer door station by set conditions, such as device name, device type, IP address, and password strength.
4. Click **Add** to enter the Add Outer Door Station page.
5. Set required parameters.

   Device Name

   Customize a descriptive name for the video intercom device.

   Device Type

   Select the device type according to the device capability. The default one is outer door station.

Access Protocol (Hikvision Device Network SDK Protocol)

Select **Hikvision Device Network SDK Protocol** as access protocol for realizing communication according to the Hikvision Device Network SDK.

IP Address

Enter the IP address of the video intercom device.

Port No.

Enter the device port No. The default value is 8000.

User Name

Enter the user name of the video intercom device. By default, the user name is admin.

Password

Enter the password of the video intercom device.

Caution

The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including 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.

EZVIZ supported

You can set **EZVIZ supported** switch to on for the outer door station which supports EZVIZ. If enabled, you need to set serial No. and verification code for the device.

Access Protocol (EZVIZ Protocol)

Select **EZVIZ Protocol** as access protocol for realizing communication according to the EZVIZ Open Service SDK.

Device Serial No.

The serial No. of the device.

Device Verification Code

The verification code of the device.

Domain

The network domain that the video intercom device belongs to, which is used for multi-domain network scenario.

Note

For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

Management Partition

If the community is divided into multiple management areas, enter the correct value. If not, enter 1.

Installation Position Description

Information for describing device installation position or device code. For example, Area 1 Property Management Center 01.

6. **Optional:** For Hikvision Device Network SDK Protocol, click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the video intercom device and click **Online Test** to start online test again.
7. Click **Save** to add the video intercom device.
8. **Optional:** Perform the following operation(s) after adding the video intercom device.

Filter Device	Check **Include Sub-Area** to display the added devices in this area and its lower-level areas, or click **Search** to filter devices by specific conditions.
Edit Device Information	Click on Operation column to edit information for the video intercom device.
Delete Device	Click on Operation column to delete the video intercom device. You can also select multiple devices and click **Delete** to delete devices in a batch.
	Note If you delete a video intercom device, all the information linked to the device will be deleted, such as permission configuration and so on.
Online Test	For the device added by Hikvision Device Network SDK Protocol, click to check whether the video intercom device is online.

11.2.3 Add Door Station

The door station is mainly applied in the villa, community and office building, and provides reliable security assurance and convenient visit calling service. You can add door station to HikCentral Enterprise-Commercial for management and further video intercom applications.

Steps

1. Click → **System Configuration** → **Devices** → **One Card System** → **Video Intercom** to enter the video intercom device management page.
2. Select an area in the area list to add the video intercom device.
3. Click **Door Station** tab.

   The added door stations will be displayed in the list. You can search the desired door station by set conditions, such as device name, device type, IP address, and password strength.
4. Click **Add** to enter the Add Door Station page.

Note

You can also click **Import** and edit the template to add multiple door stations in a bath at the same time.

5. Set required parameters.

Device Name

Customize a descriptive name for the video intercom device.

Device Type

Select the device type according to the device capability, such as unit door station and villa door station.

Access Protocol (Hikvision Device Network SDK Protocol)

Select **Hikvision Device Network SDK Protocol** as access protocol for realizing communication according to the Hikvision Device Network SDK.

IP Address

Enter the IP address of the video intercom device.

Port No.

Enter the device port No. The default value is 8000.

User Name

Enter the user name of the video intercom device. By default, the user name is admin.

Password

Enter the password of the video intercom device.

Caution

The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including 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.

EZVIZ supported

You can set **EZVIZ supported** switch to on for the door station which supports EZVIZ. If enabled, you need to set serial No. and verification code for the device.

Access Protocol (EZVIZ Protocol)

Select **EZVIZ Protocol** as access protocol for realizing communication according to the EZVIZ Open Service SDK.

Device Serial No.

The serial No. of the device.

Device Verification Code

The verification code of the device.

Domain

The network domain that the video intercom device belongs to, which is used for multi-domain network scenario.

Note

For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

Management Partition

If the community is divided into multiple management areas, enter the correct value. If not, enter 1.

Building No.

The actual building number which indicates each building.

Building Unit No.

A building may include some units. If it is a separate house without being in a building unit. Please enter 1.

Installation Position Description

Information for describing device installation position or device code. For example, Area 1 Property Management Center 01.

6. **Optional:** For Hikvision Device Network SDK Protocol, click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the video intercom device and click **Online Test** to start online test again.
7. Click **Save** to add the video intercom device.
8. **Optional:** Perform the following operation(s) after adding the video intercom device.

Filter Device	Check **Include Sub-Area** to display the added devices in this area and its lower-level areas, or click **Search** to filter devices by specific conditions.
Edit Device Information	Click on Operation column to edit information for the video intercom device.
Delete Device	Click on Operation column to delete the video intercom device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete a video intercom device, all the information linked to the device will be deleted, such as permission configuration and so on.

Online Test For the device added by Hikvision Device Network SDK Protocol, click to check whether the video intercom device is online.

11.2.4 Add Single Indoor Station

The indoor station is the intelligent terminal, which provides two-way audio, network transmission, data storage, unlocking door remotely, alarm handling, capturing picture, etc., and is mainly applied in intelligent building, large community, etc. You can add single indoor station to HikCentral Enterprise-Commercial by specifying IP address and related parameters for management and further video intercom applications.

Steps

1. Click → **System Configuration** → **Devices** → **One Card System** → **Video Intercom** to enter the video intercom device management page.
2. Select an area in the area list to add the video intercom device.
3. Click **Indoor Station** tab.

   The added indoor stations will be displayed in the list. You can search the desired indoor station by set conditions, such as device name, device type, IP address, room No., and password strength.
4. Click **Add** to enter the Add Indoor Station page.
5. Set required parameters.

   Device Name

   Customize a descriptive name for the video intercom device.

   Device Type

   Select the device type according to the device capability, such as unit indoor station and villa indoor station.

   Access Protocol

   Hikvision Device Network SDK Protocol is selected by default for realizing communication according to the Hikvision Device Network SDK.

   IP Address

   Enter the IP address of the video intercom device.

   Port No.

   Enter the device port No. The default value is 8000.

   User Name

   Enter the user name of the video intercom device. By default, the user name is admin.

   Password

   Enter the password of the video intercom device.

Caution

The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including 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.

Domain

The network domain that the video intercom device belongs to, which is used for multi-domain network scenario.

Note

For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

Management Partition

If the community is divided into multiple management areas, enter the correct value. If not, enter 1.

Building No.

The actual building number which indicates each building.

Building Unit No.

A building may include some units. If it is a separate house without being in a building unit. Please enter 1.

Room No.

The actual room number which indicates each room. It is recommended to name the room No. using floor No. + room No. For example, 1702 (Room 2, 17th Floor).

Installation Position Description

Information for describing device installation position or device code. For example, Area 1 Property Management Center 01.

6. **Optional:** For Hikvision Device Network SDK Protocol, click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the video intercom device and click **Online Test** to start online test again.
7. Click **Save** to add the video intercom device.
8. **Optional:** Perform the following operation(s) after adding the video intercom device.

Filter Device	Check **Include Sub-Area** to display the added devices in this area and its lower-level areas, or click **Search** to filter devices by specific conditions.

Edit Device Information	Click on Operation column to edit information for the video intercom device.
Delete Device	Click on Operation column to delete the video intercom device. You can also select multiple devices and click **Delete** to delete devices in a batch.
	Note If you delete a video intercom device, all the information linked to the device will be deleted, such as permission configuration and so on.
Online Test	For the device added by Hikvision Device Network SDK Protocol, click to check whether the video intercom device is online.

11.2.5 Import Indoor Stations

When there are a large number of indoor stations needed to add to HikCentral Enterprise-Commercial, you can edit the template file which contains the device parameters, and add the devices in a batch at the same time.

Steps

1. Click → **System Configuration** → **Devices** → **One Card System** → **Video Intercom** to enter the video intercom device management page.
2. Select an area in the area list to add the video intercom device.
3. Click **Indoor Station** tab.

   The added indoor stations will be displayed in the list. You can search the desired indoor station by set conditions, such as device name, device type, IP address, room No., and password strength.
4. **Optional:** Set parameters for multiple indoor stations quickly and export the file as template.
   1) Click **Batch Add** to enter the Batch Add Indoor Station page.
   2) Set required parameters.

      Device Type

      Select the device type according to the device capability, such as digital indoor station and analog indoor station.

      Access Protocol

      Hikvision Device Network SDK Protocol is selected by default for realizing communication according to the Hikvision Device Network SDK.

      Port No.

      Enter the device port No. The default value is 8000.

      Domain

The network domain that the video intercom device belongs to, which is used for multi-domain network scenario.

Note

For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

Management Partition

If the community is divided into multiple management areas, enter the correct value. If not, enter 1.

Building No.

The actual building number which indicates each building.

Building Unit No.

A building may include some units. If it is a separate house without being in a building unit. Please enter 1.

Room No.

Enter the room No. range for all devices. It is recommended to name the room No. using floor No. + room No. For example, 1702 (Room 2, 17th Floor).

Installation Position Description

Information for describing device installation position or device code. For example, Area 1 Property Management Center 01.

3) Click **Next**.
4) Select devices to generate the parameters for them.
5) In added device list, select the devices and click **Export** to export the template file with indoor station parameters.

5. Click **Import** to enter Import Indoor Station page.
6. Edit the exported template in step 4, or click **Download File Template** to download and edit the new template file.
7. Select the edited template and click **Import** to import devices.
8. **Optional:** Perform the following operation(s) after adding the video intercom device.

Filter Device	Check **Lower-Level Area Included** to display the added devices in this area and its lower-level areas, or click **Search** to filter devices by specific conditions.
Edit Device Information	Click on Operation column to edit information for the video intercom device.
Delete Device	Click on Operation column to delete the video intercom device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete a video intercom device, all the information linked to the device will be deleted, such as permission configuration and so on.

Online Test For the device added by Hikvision Device Network SDK Protocol, click to check whether the video intercom device is online.

11.3 Video Intercom Configuration

You can configure the related parameters for the video intercom devices, such as device parameters, permission parameters, and received video intercom events.

11.3.1 Set Device Parameters

You can set the calling priority for master station and set picture storage for captured pictures by video intercom devices.

Calling Priority of Master Station

You can configure calling priority for master station. The smaller the master station No. is, the higher the calling priority will be. The default priority is based on the sequence of adding devices. The first added device has the highest priority.

Click → **System Configuration** → **One-Card System** → **Video Intercom** → **Device Parameters** to enter device parameter settings page. Click one master and drag up or down to the desired location.

Picture Storage Location

You can select picture storage pool for storing the captured pictures by video intercom devices.

Click → **System Configuration** → **Advanced Parameter** → **Picture Storage Configuration** to enter picture storage settings page. You can select a storage from drop-down list as default storage. You can also click **Add Storage Pool** and set the storage pool name, replace strategy, application, and storage pool to customize a specified for video intercom devices.

11.3.2 Set Permission Parameters

The permissions configured in HikCentral Enterprise-Commercial need to be applied to the device automatically or manually. Here you can set permission parameters for applying automatically.

When you want to apply all permission settings to the devices automatically, you can enable this function to perform permission application at the fixed time or for fixed times.

Click → **System Configuration** → **One-Card System** → **Video Intercom** → **Permission Parameters** to enter permission parameter settings page. Select the one of the methods and set required parameters as follows.

Apply at Fixed Time of Each Day:

Set what time the system will start applying permissions automatically each day and how long to apply once repeatedly. For example, if you set 00:00 and 12 hours for the two, the system will start applying permissions at 00:00 and 12:00, and perform applying twice each day.

Apply for Fixed Times Each Day:

Set how many times the system will apply permission automatically each day and the start applying time for each time. For example, if you set 3 times, and set 1:00, 04:00, and 22:00 as each applying time, then the system will apply permissions at the above three time points each day.

Note

- You'd better select the night time or wee hours for applying permission, to avoid affecting normal use of the system.
- To many applying times every day may take up much system recourse. You should set reasonable parameters for that.

11.3.3 Set Event Parameters

The system can receive and record the video intercom events including entering/exiting event and device event. You can select which events to receive and set the retention period for saving the events, which means only the received events during the valid period can be searched in the system.

Event Arming Control

For the video intercom events you concerned, you can enable receiving these event types as you desired. When the events occur, the system can only receive and record the selected events and ignore the unselected events.

Steps

1. Click → **System Configuration** → **One-Card System** → **Video Intercom** → **Event Parameters** → **Select Event Type** to enter Select Event Type page.
2. Select **Device Event** or **Entering/Exiting Event** tab.
3. Check the event types for receiving event.

Note

You can uncheck the event types to ignore the corresponding events.

4. Click **Save**.

Event Retention Period

When the specified video intercom events occur, the system can receive the events and save the event records for a period, which can be set as 1 month, 2 mouths, 6months, etc. If expired, the event record will be deleted and you cannot search the events in the system.

Click → **System Configuration** → **One-Card System** → **Video Intercom** → **Event Parameters** → **Event Retention Period** to enter Event Retention Time Setting page. Select the retention period from drop-down list for each items and click **Save** to save the settings.

11.4 Video Intercom Permission Configuration

The video intercom permission can be used to control person entering and exiting, in order to strengthen safety. You can assign access control permission, apply permission to device to take effect, configure video permission of indoor station, etc.

11.4.1 Access Control Permission

Access control permission is used for persons who need to access specified outer door station and door station. You need to assign the access control permission to the persons in a group or specified persons and apply the permission settings to the device to take effect.

Assign Access Control Permission by Person

You can assign access control permission to the persons so that persons can access specified door station(s) or outer door station(s) according to the assigned permission.

Steps

1. Click **Video Intercom** on the Home page and enter **Access Control Permission Configuration**.
2. Select **Configure Permission by Person** as assigning permission mode.
3. Click **Add Permission** to enter adding permission page.
4. Select an organization to filter the persons added in this organization, check person(s) from available person list and click › to add to the selected person list.
5. Select **Door Station** or **Outer Door Station** tab.
6. Select an area to display its devices, check device(s) from middle list and click › to add to the right list.
7. Click **Save** to complete assigning permission.

8. In the pop-up window, click **OK** to save settings or click **Apply** to apply the permission to the device to take effect.

Assign Access Control Permission by Organization

You can assign access control permission to organization so that persons in the organization can access specified door station(s) or outer door station(s) according to the assigned permission.

Steps

1. Click **Video Intercom** on the Home page and enter **Access Control Permission Configuration**.
2. Select **Configure Permission by Organization** as assigning permission mode.
3. Click **Add Permission** to enter adding permission page.
4. Check organization(s) from left list and click › to add to the right list.
5. Select **Door Station** or **Outer Door Station** tab.
6. Select an area to display its devices, check device(s) from middle list and click › to add to the right list.
7. Click **Save** to complete assigning permission.
8. In the pop-up window, click **OK** to save settings or click **Apply** to apply the permission to the device to take effect.

Apply Access Control Permission

After access control permission is assigned to person, or if the person's permission is changed, you need to apply the permission to the video intercom device to take effect. After that, the persons can access door station or outer station defined by the related permission.

Before You Start

Make sure you have assigned access control permission to the persons.

Steps

1. Click **Video Intercom** on the Home page and enter **Access Control Permission Configuration**.
2. Select permission applying mode.
   - Move the curse over ▾ near **Apply Permission** and click **Apply All** to apply all settings to the selected video intercom devices.

     Note

     Apply All can clear previous permission of all persons, which will affect accessing the door station or outer door station during this period. It is recommended for the newly added devices.
   - Click **Apply Permission** to apply changes to the selected video intercom devices.
   - Move the curse over ▾ near or button and click **Apply All** to apply all fingerprints or face pictures to the selected video intercom devices.
   - Click **Apply Fingerprint** or **Apply Face Picture** to apply changed fingerprints or face pictures to the selected video intercom devices.

3. Select the video intercom device(s) for applying.
4. Click **OK** to confirm the operation.
5. Click **Apply** to start applying task.
6. **Optional:** Click to check the progress of the applying task.

Enable/Disable Biometric Recognition on Device

You can enable biometric recognition (including fingerprint or face) so that the video intercom device can verifying the users' identities via the applied biometric recognition information. You can also disable biometric recognition for video intercom device here.

Steps

1. Click **Video Intercom** on the Home page and enter **Biometric Recognition**.
2. Select an area to filer the video intercom devices.
3. Click or .
4. Set the switch to on or off to enable or disable the fingerprint or face function for the video intercom device.

Note

You can click **Enable All** or **Disable All** to enable or disable the fingerprint or face function for all video intercom devices.

Search Assigned Permission

After configuring the access control permissions, you can search the assigned permissions by setting the search conditions, including name, organization, device, area, etc.

Steps

1. Click **Video Intercom** on the Home page and enter **Permission Search**.
2. Set the search condition such as person name, organization, door station, outer station, etc.
3. Click **Search**.

   The matched search results will display. You can click **Export** to export the search results.

Check Permission Applying Records

For the failed applying tasks about access control permission, you can search them here, in order to apply them again.

Steps

1. Click **Video Intercom** on the Home page and enter **Permission Applying Record**.
2. Set the search condition such as task code, door station, outer door station, area, etc.
3. Click **Search**.

The matched results will display.

4. **Optional:** Click on Description column to check applying result and export search result.

11.4.2 Video Permission of Indoor Station

For the purpose of higher safety, you can configure video permission for indoor station, in order to verify the visitor's identity through the authorized cameras before unlocking door.

Steps

1. Click **Video Intercom** on the Home page and enter **Indoor Station Video Permission Configuration**.
2. Click **Add** to enter adding indoor station video permission page.
3. Select an area to display indoor stations, check indoor station(s) from middle list and click › to add to the right list.
4. Select an area to display its cameras, check camera(s) from middle list and click › to add to the right list.
5. Click **Save** to complete adding permission.
6. In the pop-up window, click **OK** to save settings or click **Apply** to apply the permission to the device to take effect.

11.5 Apply Session Information

The device contacts and device information can be applied to the SIP server and video intercom devices, respectively.

11.5.1 Apply Contacts

The device contacts (the unique identifier of each device, used for communication between the devices) can be applied to SIP server, which linked with the area of the video intercom device. Via SIP server, the calling information (including caller, callee, calling time, etc.) will be uploaded to the platform automatically.

Steps

1. Click **Video Intercom** on the Home page and enter **Session Information Application**.
2. Click **Apply Contacts** tab.
3. Select an area from the left list.
4. Click **Set SIP Server** to bind SIP server to the area.

Note

The SIP server need to be added in Operation and Management Center. For more details, refer to *User Manual of Operation and Management Center*.

5. **Optional:** Set conditions to search the desired device for applying.

6. Start applying contacts.
   - Select a device and click on Operation column to apply the contact of the device.
   - Select multiple devices, and click **Apply → Apply Contacts of Selected Devices** to apply the contacts of the selected devices.
   - Click **Apply → Apply Contacts of Failed Applied Devices** to apply the contacts of the failed applied devices.
   - Click **Apply → Apply Contacts of All Devices** to apply the contacts of all devices.

11.5.2 Apply Device Information

The IP address of main master station, door station, SIP server, and video intercom drive service can be applied to the video intercom devices for calling, two-way audio, etc.

Steps

1. Click **Video Intercom** on the Home page and enter **Session Information Application**.
2. Click **Apply Device Information** tab.
3. Select an area from the left list.
4. **Optional:** Set conditions to search the desired device for applying.
5. Start applying device information.
   - Select a device and click on Operation column to apply to the device.
   - Select multiple devices, and click **Apply → Apply to Select Devices** to apply information to the selected devices.
   - Click **Apply → Apply to Failed Devices** to apply information to the failed applied devices last time.
   - Click **Apply → Apply to All Devices** to apply information to all devices.

11.6 Event Search

You can search all the events of the added video intercom devices, including device event and person entering/exiting event, and check event details (such as event time and event type). You can also export search results.

11.6.1 Search Person Entering/Exiting Event

When the persons go access door station or outer door station, the records of opening lock by the authorization method will be saved in the system. You can search the relative events, such as open lock by password, open lock by swiping card and so on, and export the records to local PC.

Steps

1. Click **Video Intercom** on the Home page and enter **Person Entering/Exiting Event**.
2. Set the search conditions, such as person name, event type, event time, and so on.
3. Click **Search** to start searching the video intercom events.

   The matched video intercom events will be displayed.

4. Click **Export** to export search results to local PC.

11.6.2 Search Device Event

You can search the video intercom events reported by the video intercom devices, which can help you to know the device status or personal operations at that time.

Steps

1. Click **Video Intercom** on the Home page and enter **Device Event**.
2. Set the search conditions, such as device name, event type, event time, and so on.
3. Click **Search** to start searching the video intercom events.

   The matched video intercom events will be displayed.
4. Click **Export** to export search results to local PC.

11.7 Call Log Search

You can search the call logs of the video intercom devices in the specified time period and export search results to local PC.

Steps

1. Click **Video Intercom** on the Home page and enter **Call Log**.
2. Set search conditions, such as caller, callee, calling time, and connected/not connected.
3. Click **Search**.

   The search results will be displayed in the list.
4. **Optional:** Click **Export** to export search results to local PC.

Chapter 12 Elevator Control

The Elevator Control module is applicable to elevator control management of the elevator controllers. It provides multiple functionalities, including floor group management, elevator control permissions configuration, searching elevator control event, etc.

12.1 Flow Chart

For the first time, you can perform configurations and applications of elevator control according to the chart below.

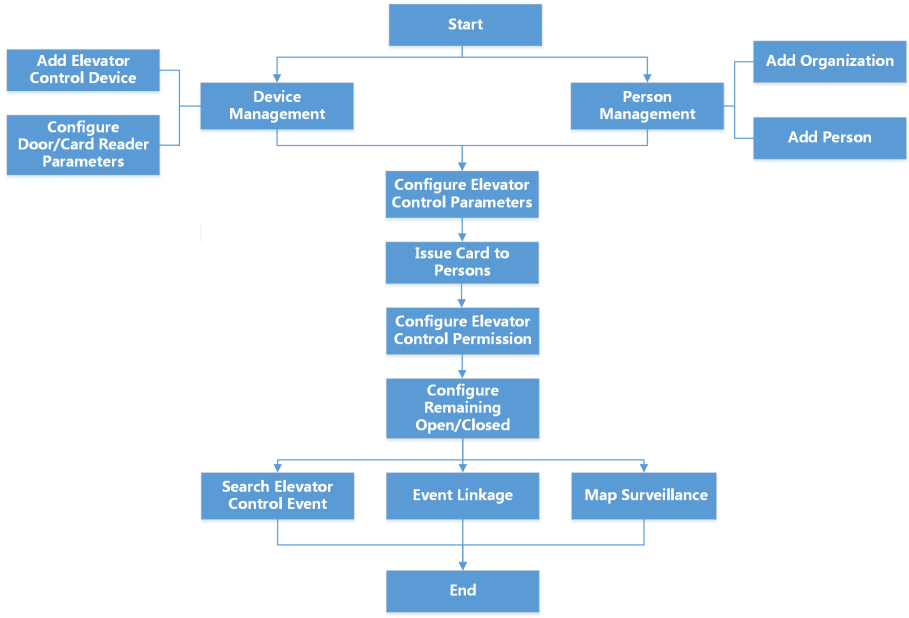


Figure 12-1 Flow Chart of Elevator Control

- **Device Management**: You can add the elevator control devices to the system for configuration and management. For details, refer to ***Elevator Control Device Management*** .
- **Person Management**: You can add person information to the system for further operations. For details, refer to ***Person Management*** .
- **Configure Elevator Control Parameters**: You can configure the related parameters for the elevator control devices, such as floor parameters, permission parameters, and received elevator control events. For details, refer to ***Elevator Control Settings*** .
- **Assign Elevator Control Permission**: You can assign elevator control permission to organization or person so that persons can access specified floor(s) during specified time period according to the assigned permission. For details, refer to ***Assign Elevator Control Permission***
- **Configure Remaining Open/Closed**: You can schedule weekly time periods for a floor to remain open or closed. For details, refer to ***Configure Remaining Open/Closed*** .

- **Search Elevator Control Event**: You can search the history elevator control events including person access event and elevator control device event. For details, refer to ***Search Elevator Control Device Event*** .
- **Event Linkage**: You can configure linkage actions for the elevator control events. When an event is detected, the system will receive the real-time information of the event and trigger linkage actions. For details, refer to ***Event Configuration*** .
- **Map Surveillance**: You can add elevator control resources to the map. When the alarm is triggered, you can view the live view and playback of the added resources on the map. For details, refer to ***Map*** .

12.2 Elevator Control Device Management

You can add the elevator control devices to HikCentral Enterprise-Commercial for configuration and management, such as the schedule template to define when the elevator control permission is valid for the person, elevator control permissions for persons to have the right to access specified floors via elevator during specified time period, etc. Elevator control devices produced by Hikvision can be added to the system via Hikvision Device Network SDK Protocol.

12.2.1 Add an Elevator Control Device by IP Address

When you know the IP address of the elevator control device to be added, you can add the elevator control device to the system by specifying the IP address, port No., user name, password, and other related parameters.

Before You Start

Make sure the elevator 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 elevator devices to HikCentral Enterprise via network.

Steps

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Elevator Control** to enter the Elevator Control page.
2. Select an area in the area list to add the elevator control device.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Set the parameters for the elevator control device, including device name, access protocol, IP address, port No., user name, and password.

   Access Protocol

   Select **Hikvision Device Network SDK Protocol** as the access protocol from the drop-down list.

   IP Address

   Enter the IP address of the elevator control device.

   Port No.

Enter the device port No. The default value is 8000.

User Name

Enter the user name of the elevator control device. By default, the user name is ***admin***.

Password

Enter the password of the elevator control device.

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 **Online Test** to check whether the device information is correct.
   The test result will show. If test failed, you should check and edit the user name or password for the elevator control device and click Test to start online test again.
6. Click **Save** to add the elevator control device.
   Enter the result of your step here (optional).
7. Perform the following operation(s) after adding the elevator control device.

Search Device	Check **Include Sub-Area** to filter the devices. Set search conditions, and click **Search** to search access control devices as required.
Configure Parameters	Click to configure parameters for the elevator control device, including basic information, card reader information, card reader parameters, etc. For details about configuring parameters for elevator control devices, refer to ***Set Parameters for Doors*** and ***Set Parameters for Card Readers*** .
Online Test	Click to check whether the elevator control device is online.
Delete Device	Click to delete the elevator control device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete an elevator control device, all the information linked to the device will be deleted, such as permission configuration and so on. As a result, you may lose alarms or fail to update elevator control permissions.

12.2.2 Set Parameters for Elevator Control Devices

After the elevator control device is added to the system, the device should be configured properly to take effect. You can edit the basic information and elevator control parameters (such as opening door button control method, valid time to light the button, duress code, etc.).

Steps

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Elevator Control** to enter the Elevator Control page.
2. Select an area in the area list.
3. Click in the **Operation** column to enter the Edit Elevator Control Device page.
4. Select the elevator control device to be configured from the list in the left.
5. Click **Get Parameter from Device** to get parameters from the device to the system.
6. Set parameters for the elevator control device.

   Exit Button Type

   The exit button connection mode.

   Valid Time to Light the Button

   The valid time to light the floor button after swiping the card.

   Duress Code

   If you enter this code on the card reader keypad, the Operation and Management Center will receive a duress event. It should be different from the super password and dismiss code.

   Super Password

   If you enter this password on the card reader keypad, you are exempted from all the remaining locked (Credential Failed), anti-passback, and first card authorization restrictions. It should be different from the duress code and dismiss code.

   Dismiss Code

   If you enter this code on the card reader keypad, the buzzer's beeping will be stopped. It should be different with the duress code and the super password.

   Delay Time of Calling Elevator

   The valid time for the visitor to press the floor button after calling the elevator.
7. Click **Save**.
8. Perform the following operation(s) after setting parameters for the elevator control device.

Set time for the device	Click **Set Time** to adjust the time for the elevator control device.
Apply parameters to the device	Click **Apply Parameter to Device** to apply configured parameters to the elevator control device. The original device configuration will be covered.
Restore default settings	Click **Restore to Default** to restore default settings for the elevator control device.

12.2.3 Set Parameters for Card Readers

After the elevator control device is added to the system, card readers linked to the device should be configured properly to take effect. You can edit the basic information and parameters (such as tampering detection, offline detection time, etc.) for the card readers.

Steps

1. Click → **System Configuration** → **Devices** → **One-Card System** → **Elevator Control** to enter the Elevator Control page.
2. Select an area in the area list.
3. Click in the **Operation** column to enter the Edit Elevator Control Device page.
4. Select the card reader to be configured from the list in the left.
5. Click **Get Parameter from Device** to get parameters from the card reader to the system.
6. Set parameters for the card reader.

Card Reader Information

Communication Method

Select the communication method between the elevator control device and the card reader according to wiring configuration.

Card Reader Dial-Up

You should set the correct dial-up on the card reader, and the card reader dial-up will display here.

Card Reader Type

Select the card reader type from the drop-down list according to the card reader capability.

Card Reader Model

Enter the card reader model.

Card Reader Parameter

Tampering Detection

After enabled, if the elevator control device has been 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.

Frequent Card Reading Failure Alarm

After enabled, if the elevator control device has been 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. For details about event configuration for elevator control devices, refer to ***Set Event Parameters*** .

Max. Limit of Card Reader Failure

Set the maximum failure attempts of reading card. The card reading failure alarm will be triggered if the failure attempts of reading card reach the limit.

Card Reader Offline Detection Time

When the elevator control device cannot connect with the card reader for a time period longer than the set time, the card reader will turn offline automatically.

Valid Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

Timeout Period of Pressing Button

When you input the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

7. Click **Save**.
8. Perform the following operation(s) after setting parameters for the card reader.

Set Time	Click **Set Time** to adjust the time for the card reader.
Apply Parameters to Card Reader	Click **Apply Parameter to Device** to apply configured parameters to the card reader.
Restore Default Settings	Click **Restore to Default** to restore default settings for the card reader.

12.3 Elevator Control Settings

You can configure the related parameters for the elevator control devices, such as floor parameters, permission parameters, and received elevator control events.

12.3.1 Configure Floor

After adding elevator control devices, you need to set elevator level and start floor for each elevator device. You can also edit device name, elevator level, start floor and floor name.

Perform this task to configure floor for the elevator control device for the first time.

Steps

1. Click → **System Configuration** → **One-Card System** → **Elevator Control** → **Floor Configuration** to enter Floor Configuration page.
2. Select the desired security area from the left panel to display the elevator control devices.
3. Select an elevator control device.

   The device information will show on the right panel.
4. Set the required information.

Elevator Name

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

Total Floor Number

Generally, the total floor number is equal to the number of managed floors, includes the upper and underground floors. It should be consistent with the actual elevator controller.

Start Floor

The actual start floor. For example, if there are two underground parking levels, enter ***-2*** as the start floor.

5. Click **Save** to save the settings.

You can view all floors listed on the page, including floor name and No.

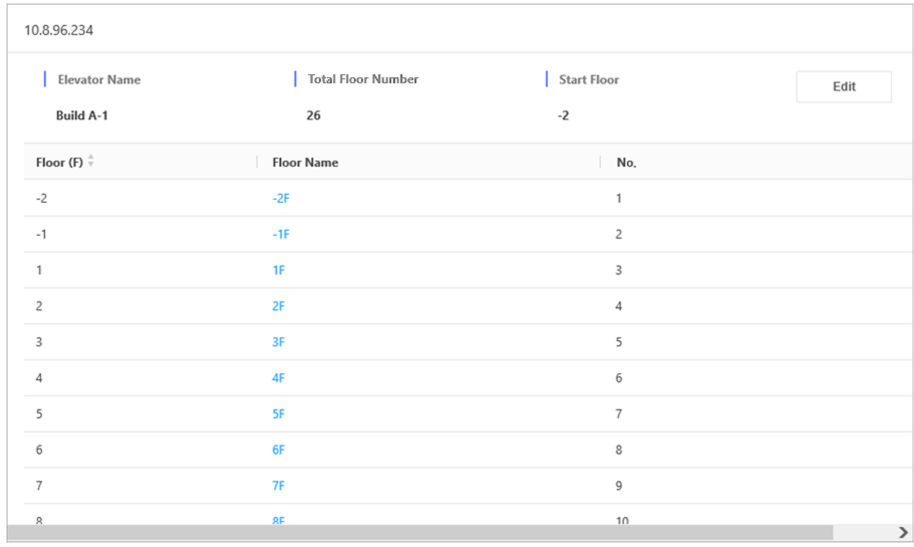


Figure 12-2 View All Floors

6. **Optional:** Perform the following operations if required.
   - Click **Edit** to edit the name, total floor number and start floor.
   - Double-click the floor name and edit it in the text filed.

12.3.2 Set Permission Parameters

You can set permission parameters in the system to apply the elevator control permission to the device automatically at the fixed time or for fixed times.

Click → **System Configuration** → **One-Card System** → **Elevator Control** → **Permission Parameters** to enter permission configuration page.

Set **Auto Apply Permission** switch to on.

Apply at Fixed Time of Each Day

Set what time the system will start applying permissions automatically each day and how long to apply once repeatedly. For example, if you set 00:00 and 12 hours for the two, the system will start applying permissions at 00:00 and 12:00, and perform applying twice each day.

Apply for Fixed Times Each Day

Set how many times the system will apply permission automatically each day and the start applying time for each time. For example, if you set 3 times, and set 1:00, 04:00, and 22:00 as each applying time, then the system will apply permissions at the above three time points each day.

Note

- You'd better select the night time or wee hours for applying permission, to avoid affecting normal use of the system.
- Too many applying times every day may take up much system recourse. You should set reasonable parameters for that.

12.3.3 Set Event Parameters

The system can receive and record the elevator control events including person access event and device event. You can select which events to receive and set the retention period for saving the events, which means only the received events during the valid period can be searched in the system.

Event Arming Control

For the elevator control events you concerned, you can enable receiving these event types as you desired. When the events occur, the system can only receive and record the selected events and ignore the unselected events.

Steps

1. Click → **System Configuration** → **One-Card System** → **Elevator Control** → **Event Parameters** → **Select Event Type** to enter Select Event Type page.
2. Select **Device Event** or **Person Access Event** tab.
3. Check the event types for receiving event.

   Note

   You can uncheck the event type to ignore the corresponding events.

4. Click **Save**.

Set Retention Period of Event Record

When the specified elevator control events occur, the system can receive the events and save the event records for a period, which can be set as 1 month, 2 mouths, 6months, etc. If expired, the event record will be deleted and you cannot search the events in the system.

Steps

1. Click → **System Configuration** → **One-Card System** → **Elevator Control** → **Event Parameters** → **Event Retention Period** to enter Event Retention Time Setting page.
2. Select the retention period from drop-down list.
3. Click **Save** to save the settings.

12.4 Elevator Control Permission

You can configure elevator control permission in the system to define which persons can get access to which floors during the authorized time period. To realize this function, you need to add floor group, assign elevator control permission and apply permission to the device. After that, you can search the assigned permission and check permission applying record.

12.4.1 Add Floor Group

Floor group is a group of floor(s). To define the elevator control permission, you need to add a floor group first used for grouping the floors.

Steps

1. Click **Elevator Control** on the Home Page and enter **Floor Group**.
2. Click **Add** to enter the adding floor group page.
3. Create a name for the floor group.
4. **Optional:** Enter the remark information in the Description textbox if needed.
5. Select the area to filter its floor(s).
6. Check the floor(s) and click to add the floors to the right list.
7. Click **Save** to add the selected floor(s) to the group.

12.4.2 Elevator Control Permission Settings

Elevator control permission is used for persons who need to be carried to the specified floor(s) via elevator. You need to assign the elevator control permission to the persons and apply the permission settings to the device to take effect.

Assign Elevator Control Permission

You can assign elevator control permission to organization or person so that persons can access specified floor(s) during specified time period according to the assigned permission.

Steps

1. Click **Elevator Control** on the Home page and enter **Permission Configuration**.
2. Select a tab as assigning permission mode.

   By Organization

   Assign elevator control permissions to persons in one organization to access specified floor(s).

   By Person

   Assign elevator control permissions to specified person(s) to access the floor(s).
3. Click **Add Permission** to show adding permission page.
4. Select organization, person group or person from the appropriate list.

   Assign Permission by Organization

   Check organization(s) from left list and click › to add to the right list.

   Assign Permission by Person

   Select an organization to display the persons added in this organization. Then check person(s) from available person list and click › to add to the selected person list.
5. 5. Select **Floor Group** or **Floor** tab and select the object(s) to assign permission.

   Floor Group

   Check floor group(s) from left list and click › to add to the right list. The permission of floors in the group(s) will be assigned.

   Floor

   Select an area to display its floors. Check floor(s) from middle list and click › to add to the right list. The permission of floor(s) will be assigned.
6. Click **Save** to complete assigning permission.
7. In the pop-up window, click **OK** to save settings or click **Apply** to apply the permission to the device now.

Apply Permission to Device Manually

After assigning elevator control permission to person, or if the person's permission is changed; you need to apply the permission to the elevator control device to take effect. After that, the persons can access the floors during the authorized time period defined by the related permission.

Steps

1. Click **Elevator Control** on the Home page and enter **Permission Configuration**.
2. Select permission applying mode.

- Move the curse over near **Download Permission** button and click **Apply All** to apply all settings to the selected floors.

  Note

  Apply All can clear previous permission of all persons, which will affect accessing the floor during this period. It is recommended for the newly added devices.

- Click **Apply Permission** to apply changes to the selected floors.

3. Select the elevator control device(s).
4. Click **OK** to verify the operation.
5. Click **Apply** to start applying task.
6. Click to check the progress of the applying task.

Search Assigned Permission

After assigning elevator control permission, you can set search conditions to search the assigned permission including floor name, permission validity, configuration time, etc.

Steps

1. Click **One-Card System → Elevator Control → Permission Configuration Search** to enter Permission Configuration Search page.
2. Set the search conditions, including name, employee No., organization, controller, etc.
3. Click **Search**.

   The corresponding search results will be displayed in the following list.
4. **Optional:** Click **Export** to export the search results to the local PC.

Check Permission Applying Record

When some applying tasks about elevator control permission failed, you can search the failed record here and apply it again.

Steps

1. Click **Elevator Control** on the Home page and enter **Permission Applying Record**.
2. Set the search condition such as task code, elevator, current area, etc.
3. Click **Search**.

   The matched results will display.
4. Click in Details column to check applying result and export search result.

12.5 Configure Remaining Open/Closed

For certain floor, you may want to set the time period during which the persons can access the floor without credentials or the persons are not allowed to access the floor. You can schedule weekly time periods for a floor to remain open or closed.

Before You Start

Make sure you have assigned the elevator control permission and applied the permission to the elevator control device. For details, refer to ***Elevator Control Permission*** .

Steps

1. Click **Elevator Control** on the Home Page and enter **Remaining Open/Closed**.
2. Add floor for setting elevator control status.
   1) Click **Add**.
   2) Click an area to filter the floor(s).
   3) Check floor and click to add it to the right list.
   4) Click **Save**.

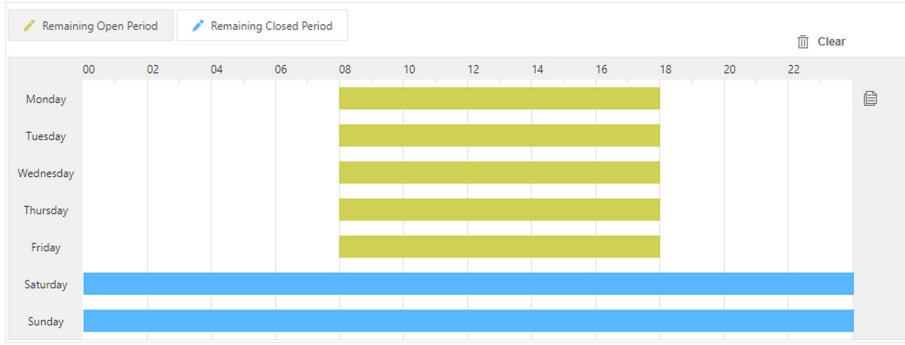
      The added floor will be displayed in the list with the status of **Not Configured**.
3. Set schedule for remaining open or closed.
   1) Click in Operation column.
   2) Select an elevator control status.

      Remain Open Period

      The persons can access the floor without certificate during the configured time period.

      Remain Closed Period

      The persons are not allowed to access the floor during the configured time period.
   3) Drag on the time bar of one day to draw the time schedule, which means in that period of time, the elevator control status is valid.



   4) **Optional:** Perform one of the following operations to edit the drawn time periods.
      - Move the cursor to the time period and drag the time period on the timeline bar to the desired position.
      - Click the time period and directly edit the start/end time in the appeared dialog. Or click **Delete** to delete the period.

- Move the cursor to the ends of time period and drag to lengthen or shorten the time period.
- Move the cursor and click to copy the time period of this day to other day.

5) Click **Save**.

4. Click in Operation column or click **Apply Parameter** to apply the new settings to the device to take effect.

12.6 Search Person Access Event

When the persons access the floor, the swiping card or other authentication records will be saved in the system. You can search the relative events, such as blacklist event, valid card event and so on, and export the records to local PC.

Steps

1. Click **Elevator Control** on the Home Page and enter **Person Access Event**.
2. Set the search conditions, such as device name, event type, event time, and so on.
3. Click **Search** to start searching the elevator control events.

   The matched elevator control events will display.
4. Click **Export** to export the search results to local PC.

12.7 Search Elevator Control Device Event

You can search the elevator control events reported by the elevator control device, which can help you to know the device status or personal operations at that time.

Steps

1. Click **Elevator Control** on the Home Page and enter **Elevator Control Device Event**.
2. Set the search conditions, such as elevator name, card reader name, event type, event time, and so on.
3. Click **Search** to start searching the elevator control events.

   The matched elevator control events will display.
4. Click **Export** to export the search results to local PC.

Chapter 13 Time and Attendance

If you want to track and monitor when the persons start/stop work and monitor their working hours and late arrivals, early departures, time taken on breaks, and absenteeism, you can add the person to the shift group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the shift group to define the attendance parameters for the persons in the shift group.

13.1 Flow Chart

For the first time, you can follow the flow chart to perform configurations and operations.

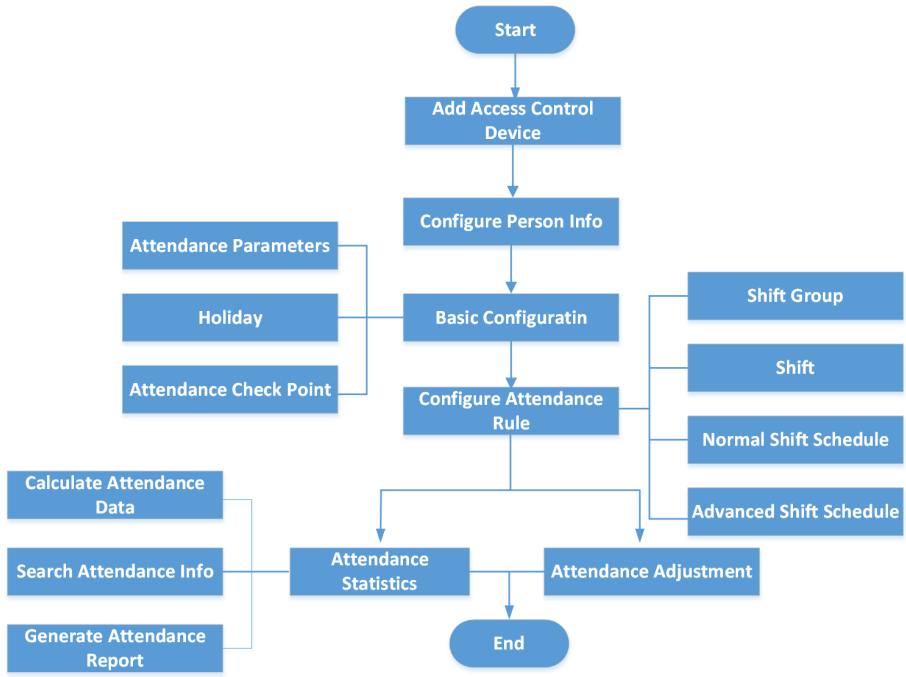


Figure 13-1 Flow Chart of Time and Attendance

- **Add Access Control Device**: Add access control devices to the platform.
- **Configure Person Info**: Add organization and person to the platform and issue cards to the persons.
- **Basic Configuration**: Configure attendance parameters, holidays, and attendance check points. For more details, refer to ***Time and Attendance Settings*** , ***Configure Holiday*** and ***Configure Attendance Check Point*** .
- **Configure Video Intercom Permissions**: Assign video intercom permissions to organization and persons. For more details, refer to ***Video Intercom Permission Configuration*** .
- **Configure Attendance Rule**: Add shift group, shift and shift schedule. For more details, refer to ***Shift Group Management*** , ***Shift Management*** , and ***Shift Schedule Management*** .

- **Attendance Statistics**: Calculate attendance data, search attendance information, and generate attendance report. For more details, refer to ***Recalculate Attendance Data*** , ***Search Attendance Information*** and ***Attendance Report*** .
- **Attendance Adjustment**: Set attendance adjustment reasons and adjust check-in/out time for attendance records. For more details, refer to ***Attendance Adjustment Management*** .

13.2 Time and Attendance Settings

You can configure the retention periods of the attendance record, which contains the attendance details and the card swiping record.

Steps

Note

For details about time and attendance, refer to ***Time and Attendance*** .

1. Click → **System Configuration** → **One Card** → **Attendance** to enter the Attendance Configuration page.
2. Set the required information.

   Retention Period of Attendance Details

   Select a period from the drop-down list. When the retention period of an item of attendance information expires, this item will be deleted automatically.

   Retention Period of Card Swiping Record

   Select a period from the drop-down list. When the retention period of a card swiping record expires, the record will be deleted automatically.
3. Click **Save**.

13.3 Shift Group Management

The persons in one shift group are assigned with the same shift schedule. You can group persons into different attendance groups.

13.3.1 Add Shift Group with Single Person

You can create multiple shift groups at a time, each of which contains one person. The person name is used as the shift group name automatically.

Steps

1. Click **Attendance** on the Home page and enter **Shift Group**.
2. Click **Add** to enter adding shift group page.
3. Select **One Persons in One Group** as Generating Method.
4. Select an organization to filter the persons.

5. Select persons and add them to the right list.
6. Click **Save**.

   The added shift groups will display in the list.

13.3.2 Add Shift Group with Multiple Persons

When you want to make the same attendance rule for the persons from different organizations or one organization, you can add multiple organizations or persons to one shift group and assign it with the same shift schedule.

Steps

1. Click **Attendance** on the Home page and enter **Shift Group**.
2. Click **Add** to enter adding shift group page.
3. Select **Multiple Persons in One Group** as Generating Method.
4. Create a name for the shift group.
5. **Optional:** Enter the remark information in the Description if needed.
6. Select **Organization List** or **Person List** tab.
   - For organization list, select the desired organization(s) to add the persons in the organization(s) to the shift group.
   - For person list, select persons to add them to the shift group.
7. Click **Save**.

   The added shift group will display in the list.

13.4 Shift Management

Shift work is an employment practice designed to make use of all 24 hours of the clock in each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shift groups perform their duties.

There are three types of shifts: normal shift, man-hour shift and check-in shift.

13.4.1 Configure Shift Rule for Normal Shift

You can set the attendance rule for the normal shift and use the normal shift when working at the fixed time period every day.

Steps

1. Click **Attendance** on the Home page and enter **Shift**.
2. Click **Normal Shift → Normal Shift Rule** to enter normal shift rule management page.
3. Click **Add** to enter adding shift rule page.
4. Create a name for the shift rule.
5. **Optional:** Enter the remark information in the Description textbox if needed.

6. Set the shift schedules.

Allowable Early Duration to Start Work

For example, if the value is 60 minutes, and the normal time to start work is 9:00 a.m. If the employee goes to work and swipes the card at the check point at 8:00 a.m., then the card swiping is valid and he will be marked as "start work normally" for the day. If he swipes the card at 7:59 a.m., then the card swiping is invalid.

Allowable Late Duration to Start Work

For example, if the value is 10 minutes, when the employee is late for 11 minutes, he will be marked as "late" for the day. when he is late for 9 minutes, he will be marked as "start work normally".

Mark as Absent After Start-Work Time

For example, the value is 60 minutes. If the employee is late for 61 minutes, he will be marked as "absent" for the day. If he is late for 59 minutes, he will be marked as "late" only.

Allowable Early Duration to End Work

For example, if the value is 30 minutes, and the normal time to get off work is 17:00 p.m. If the employee gets off work and swipes the card at the check point at 16:30 p.m., then he will be marked as "finish work normally".

Mark as Early Leave Before End-Work Time

For example, the value is 60 minutes. If the employee leaves earlier for 61 minutes, he will be marked as "absent" for the day. If he leaves earlier for 59 minutes, he will be marked as "early leave" only.

Allowable Late Duration to End Work

For example, if the value is 180 minutes, and the normal time to get off work is 17:00 p.m. If the employee gets off work at 20:01 p.m., then the checkout time is marked as 20:00 p.m.

OT Start Time: … After End-Work Time

For example, if the duration value is 60 minutes, and the normal time to get off work is 17:00 p.m. If the employee gets off work at 20:00 p.m., then the overtime starts at 18:00 p.m. and the overtime duration is two hours.

Valid Overtime Threshold Duration

For example, if the duration is 20 minutes, and the employee works in overtime for 19 minutes, then the overtime is invalid. If he works in overtime for 21 minutes, then the overtime is valid.

7. Click **Save**.

13.4.2 Add Normal Shift

Normal shift is applicable to attendance check of shifts with regular time schedule, such as nine-to-five and three-shift working mode. After setting the attendance rule, you can set the attendance shift and configure the shift's working time and attendance rule..

Steps

1. Click **Attendance** on the Home page and enter **Shift**.
2. Click **Normal Shift → Normal Shift** to enter normal shift settings page.
3. Click **Add**.
4. Create a name for the normal shift.
5. **Optional:** Enter the remark information in the Description textbox if needed.
6. Set the shift details.
   1) Click the **Start-Work Time** filed and **End-Work Time** filed to set the start-work time and end-work time.
   2) Select the attendance rule from the drop-down list.
   3) Set the **Apply** switch to on as desired.
7. Click **Save**.

13.4.3 Add Man-Hour Shift

Man-hour shift is usually used for the attendance with irregular time schedule, such as counting work time according to working hours. You can set the same time duration for work every day. Normal and sequential modes are supported.

Steps

1. Click **Attendance** on the Home page and enter **Shift**.
2. Click **Man-Hour Shift** to enter man-hour shift settings page.
3. Click **Add**.
4. Create a name for the man-hour shift.
5. Set daily working time for the man-hour shift.
6. **Optional:** Enter the remark information in the Description textbox if needed.
7. Select recording mode.

   Normal Mode

   The first card swiping record and the last card swiping record will be set as the on-duty record and the off-duty record respectively.

   Sequential Mode

   The card swiping record and the next card swiping record will be set in order as the on-duty record and the off-duty record. All periods within the working time will be accumulated.

   Min. Effective Time

If you set the attendance mode as sequential mode, set the minimum effective time duration. If one of the working duration is less than the set duration, it will not be counted in the total working hour.

8. Add invalid time period that exclude from the man-hour period. The added period will not be counted in the total working hour.
   1) Click **Add**.
   2) Set the start time and end time that do not contained in the man-hour period.
   3) **Optional:** Click in Operation column to delete this time period, or check all to delete all time periods.
9. Click **Save**.

13.4.4 Add Check-in Shift

You can use check-in shift to check for attendance, which is applicable to attendance check of shifts with unfixed working places, such as sales and patrol work. If you set only one time period for checking in a day, the employees can mark one check-in for attendance. If you set multiple time periods for checking in one day, the employees have to check in in every time period.

Steps

1. Click **Attendance** on the Home page and enter **Shift**.
2. Click **Normal Shift → Check-In Shift** to enter Check-In Shift settings page.
3. Click **Add**.
4. Create a name for the check-in shift.
5. **Optional:** Enter the remark information in the Description if needed.
6. Add check-in time period(s). You need to check in once in each time period for attendance.
   1) Click **Add**.
   2) Set the start time and end time to set the time period.
   3) **Optional:** Click in Operation column to delete this time period, or check all to delete all time periods.
7. Click **Save**.

13.5 Configure Holiday

You can add the holiday during which the check-in or check-out function will be invalid.

Steps

1. Click **Attendance** on the Home page and enter **Holiday**.
2. Click **Add** to enter adding holiday page.
3. Create a name for the holiday.
4. Enter the remark information in the Description textbox if needed.
5. Set the date for the holiday.
   1) Click **Add**.
   2) Set the date range of the holiday.

3) Select the date(s) in one week.

Example

For example, if the date range is from 2018-12-01 to 2018-12-31, and if you select Saturday and Sunday in the Week, then all the Saturdays and Sundays between 2018-12-01 to 2018-12-31 will be holidays.

6. Click **Save**.

13.6 Shift Schedule Management

A shift schedule is an attendance schedule which defines the scheduled work time and how it repeats. You can create a shift schedule to compare the employees' attendance with it so as to identify those who arrive late, leave early, or are absent, etc. .

13.6.1 Configure Normal Shift Schedule

For normal shift schedule, after assigning one shift to the shift group, during the start date and the end date, the persons in the shift group will have day off only on holidays.

Before You Start
You should set the shift group and the shift first.

Steps
1. Click **Attendance** on the Home page and enter **Shift Schedule**.
2. Select a shift group from the list on the left of the page.
3. Click **Normal Shift Schedule** to enter adding normal shift schedule page.
4. Set the shift schedule time range.
5. Select the shift in the drop-down list.
6. **Optional:** Set the holiday switch to on as desired.
7. **Optional:** Click **Copy To** and select other shift group(s) to copy the current settings to other shift group(s).
8. Click **Save**.

   The related shift will be displayed in the corresponding date filed of the calendar.

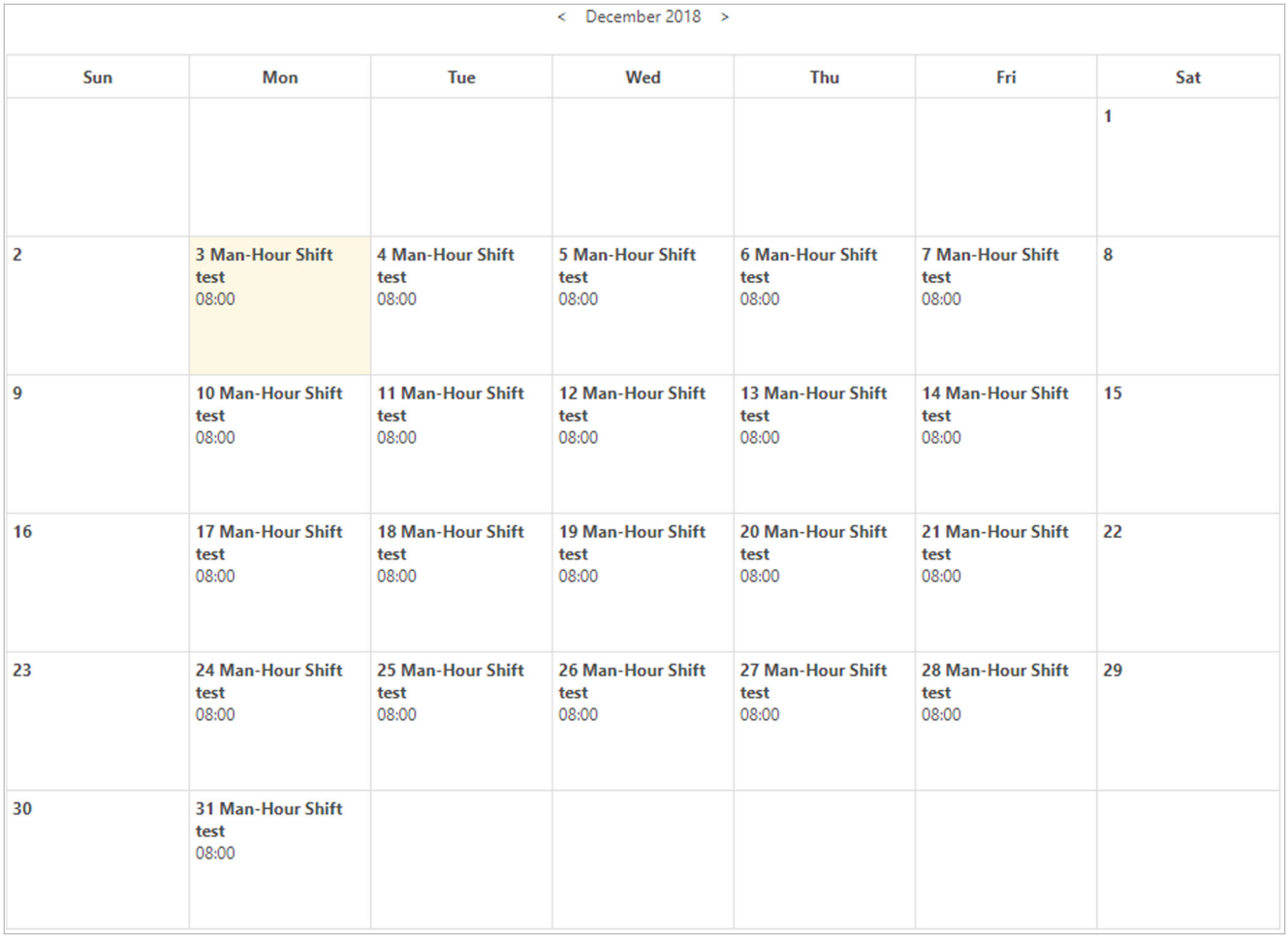


Figure 13-2 Shift Schedule

9. After adding shift schedule, perform the following operations if required.

Copy

Right-click the date and click **Copy**, then right-click another date and click **Paste** to copy the shift from that day to this day.

Delete

Right-click the date and click **Clear** to delete the shift of the date.

13.6.2 Configure Advanced Shift Schedule

For advanced shift schedule, after assigning different shifts to the shift group, during the start date and the end date, the persons in the shift group will have on duty period, shift interval, and holidays.

Before You Start

You should set the shift group and the shift first.

Steps

1. Click **Attendance** on the Home page and enter **Shift Schedule**.
2. Select a shift group from the list on the left of the page.
3. Click **Advanced Shift Schedule** to enter adding advanced shift schedule page.
4. Set the shift schedule time range.
5. Set on-duty period of the shift schedule.
6. Set the shift interval between two on-duty periods.

   Note

   The persons in the shift group will have day off during the shift interval.

7. Select the shift from the drop-down list for each day in the shift settings area.

   Note

   The item number in the shift settings area depends on the selected on-duty period.

8. **Optional:** Set the holiday switch to on as desired.
9. **Optional:** Click **Copy To** and select other shift group(s) to copy the current settings to other shift group(s).
10. Click **Save**.

    The related shift will be displayed in the corresponding date filed of the calendar.

11. **Optional:** After adding shift schedule, perform the following operations if required.

    Copy

    Right-click the date and click **Copy**, then right-click another date and click **Paste** to copy the shift from that day to this day.

    Delete

    Right-click the date and click **Clear** to delete the shift of the date.

13.7 Attendance Adjustment Management

You can set the attendance adjustment reason and adjust check-in/out time for the attendance records according to actual needs.

13.7.1 Configure Adjustment Reason

You can customize the adjustment reason according to actual needs. By default, there are four major reasons: Leave Early, Day Off in Lieu, Overtime and Reissue.

Steps

1. Click **Attendance** on the Home page and enter **Attendance Adjustment**.
2. Click **Adjustment Reason** in the top right corner to enter adjustment reason management page.
3. Select a reason type on the left panel.

4. Click **Add** to add a reason.
5. Click **OK**.

13.7.2 Correct Attendance Record

If the attendance status is abnormal (e.g., marking as absent in attendance record for normal check-in), you can manually adjust the check-in or check-out record for persons who need to apply for the attendance adjustment due to the reasons.

Steps

1. Click **Attendance** on the Home page and enter **Attendance Adjustment**.
2. Click **Add** to add a reason.
3. Select an adjustment type.
4. Select an adjustment reason.
5. Set the start date and end date as the adjustment time period.
6. Add the persons whose attendance records need to be adjusted.

   Adjust Person by Organization

   Select an organization to filter persons and add the person to the right list.

   Adjust Person by Shift Group

   Select a shift group to filter persons and add the person to the right list.
7. Click **Save**.

13.8 Configure Attendance Check Point

You should set the card reader(s) of the floor the attendance check point, so that the check-in/out by credentials (such as swiping card on the card reader) will be valid and will be recorded.

Before You Start

You should add access control device before configuring attendance check point.

Steps

1. Click **Attendance** on the Home page and enter **Attendance Check Point**.
2. Click **Add** to enter adding attendance check point page.
3. Select an area to filter the card reader(s).
4. Select card reader to add to the right list.
5. Set the related parameters.
   1) Set the validity period.
   2) Select the attendance check point type.

      Start/End-Work

      The attendance check point can be used for check-in and check-out.

      Start-Work

      The attendance check point can be used for check in.

End-Work

The attendance check point can be used for check-out.

6. Click **Save**.

13.9 Search Attendance Information

You can search the persons' card swiping records and view the attendance results based on the card swiping records.

13.9.1 Search Attendance Record

You can set the search conditions and search the persons' detailed attendance records.

Steps

1. Click **Attendance** on the Home page and enter **Search**.
2. Click **Attendance Record Search** on the left.
3. Set search conditions.

Name

Enter the keyword of person name for search.

Organization

Enter the keyword of the organization and the matched organization(s) will appear. Select an organization in the list.

Swiping Time

Set the start date and end date for search.

Search Scope

Select the first swiping record or the last card swiping during the configured time period. You can also select two in the field.

4. Click **Search** to start searching the card swiping records based on the search conditions. You can view the person name, card No., card swiping time, and other details.
5. Click **Export** to export the search result to the local PC.

13.9.2 Search Attendance Result

You can search the attendance result details including on-work time, off-work time, late duration, early leave duration, etc.

Steps

1. Click **Attendance** on the Home page and enter **Search**.
2. Click **Attendance Check Result Search** on the left.
3. Select **Normal Shift**, **Man-Hour Shift**, or **Check-In Shift** tab.

Normal Shift

Search the attendance results for the persons assigned with normal shift of the selected organization or shift group.

Man-Hour Shift

Search the attendance results for the persons assigned with man-hour shift of the selected organization or shift group.

Check-in Shift

Search the attendance results for the persons assigned with check-in shift of the selected organization or shift group.

4. Set search conditions.

Name

Enter the keyword of person name for search.

Organization

Enter the keyword of the organization and the matched organization(s) will appear. Select an organization in the list.

Parent Shift Group

Enter the keyword of the shift group for search.

Shift Name

Enter the keyword of the shift name for search.

Attendance Check Date

Set the start date and end date for search.

Start-Work Status/End-Work Status

Select the start-work status and end-work status to narrow the search result.

5. Click **Search** to start searching the attendance results based on the search conditions.
6. Click **Export** to export the search result to the local PC.

13.10 Attendance Report

Attendance statistics is to calculate the attendance record of persons in the specific organization(s) and a certain time period. The report displays the persons' attendance results such as required attendance, actual attendance, attendance rate and so on..

13.10.1 Generate Organization Attendance Report

You can generate the organization attendance report for exporting the detailed data to local storage.

Steps

1. Click **Attendance** on the Home page and enter **Statics & Reports**.
2. Click **Organization Attendance Report** on the left.
3. Enter the keyboard of the organization and in the appearing matched organization list, select an organization.
4. In the shift type field, select the shift type as normal shift, man-hour shift, or check-in shift.
5. Set the start date and end date for report.
6. Select name only or full path to display organization in the report.
7. Click **Search** to generate the report based on the search conditions.
8. **Optional:** After generating attendance report, perform the following operations if required.
   - Click **Export** to export the search result to the local PC.
   - Click **Print** to print the report.

13.10.2 Generate Person Attendance Report

You can generate the person attendance report for exporting the detailed data to local storage.

Steps

1. Click **Attendance** on the Home page and enter **Statics & Reports**.
2. Click **Person Attendance Report** on the left.
3. In the shift type field, select the shift type as normal shift, man-hour shift, or check-in shift.
4. In the organization field, select the organization(s) for the report.
5. Set the start date and end date for report.
6. Select name only or full path to display organization in the report.
7. Click **Search** to generate the report based on the search conditions.
8. **Optional:** After generating attendance report, perform the following operations if required.
   - Click **Export** to export the search result to the local PC.
   - Click **Print** to print the report.

13.11 Recalculate Attendance Data

If attendance shift group, shift, or shift schedule, changes, or attendance adjustment form is added, you can recalculate attendance result according to the newly settings. After recalculating, the original data will be replaced by new attendance data.

Steps

1. Click **Attendance** on the Home page.
2. Enter **Information Search** or **Statics & Reports**.
3. Click **Recalculate** button on the right.
4. Select the start date and end date.
5. Click **Recalculate** to start, and the attendance results during the configured time period will be recalculated.

Chapter 14 Patrol Management

Patrol refers to a security surveillance system in which patrol persons need to check in at every appointed patrol points based on certain route to make sure the monitored places are safe. The platform supports patrol function which means you can configure patrol and patrol related parameters to let patrol persons conduct patrols.

Patrol management supports the following functions:

- Supports adding multiple types of devices as patrol points including access control card reader and alarm I/O devices.
- Configuration of multiple parameters including patrol record saving time, offline patrol, and patrol SMS reminder.
- Configuration of patrol route, holidays, and patrol schedule.
- Search patrol related information including shift schedule, patrol details, and patrol reports.

14.1 Flow Chart

If this is the first time you use patrol, we recommend you perform configurations according to the chart below.

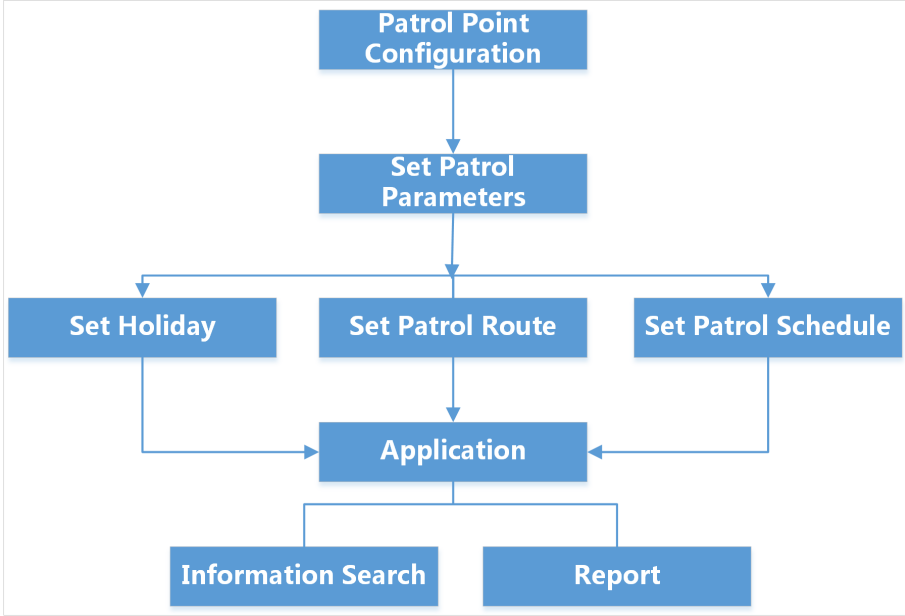


Figure 14-1 Operation Flow Chart

14.2 Patrol Configuration

Before configuring a patrol route, you need to configure patrol points (certain types of devices as patrol points) and patrol parameters to meet your diverse needs.

14.2.1 Patrol Point Configuration

A patrol point is a part of a patrol system used for guards to check in on a whole patrol route to prove he or she had arrived at the patrol point. It can be a place or device on a patrol route. You can add an access control card reader or an alarm I/O as a patrol point. So that a guard can check in at a patrol point by swiping card on the card reader or passing the alarm device.

Add Card Reader as Patrol Point

Card readers can be configured as patrol points so that the guards' card swiping on the card readers will be counted as a patrol. And then the platform will save the patrol related data.

Before You Start
Make sure you have added access control devices and card readers to the platform. See ***Access Control Device Management*** for details about adding access control devices.

Steps
1. Click ☰ on the upper-right corner, and then click **System Configuration → One-Card System → Patrol → Patrol Point** .
2. Select **Card Reader** tab.
3. Select the area where the patrol point locates.
4. Click **Add** to enter the add patrol point page.
5. In the **Available Access Control Point Card Reader** area, check card readers and click › .
   The checked card reader will be moved to the **Selected Access Control Point Card Reader** area.
6. Click **Save**.

Add Alarm I/O as Patrol Point

Alarm input/output channels (Alarm I/O) of an encoding device can be configured as patrol points for counting the guards' passing as a patrol. And then the platform will save the patrol-related data.

Before You Start
Make sure you have added alarm devices to the platform. See ***Add Alarm Input/Output to Area*** for details about adding alarm devices.

Steps

1. Click ☰ in the upper-right corner, and then click **System Configuration → One-Card System → Patrol → Patrol Point** .
2. Select **Alarm Device** tab.
3. Select the area where the patrol point locates.
4. Click **Add** to enter the add patrol point page.
5. In the **Available Alarm Device** area, check alarm devices and click > .

   The checked alarm device will be moved to the **Selected Alarm Device** area.
6. Click **Save**.

14.2.2 Set Patrol Parameters

To satisfy diverse needs of users, the platform supports configuration of multiple patrol parameters including patrol record saving time, offline patrol, and patrol reminder.

Click ☰ in the upper-right corner, and select **System Management → One-Card System → Patrol → Parameters** .

Patrol Record Retention

The retention duration of the patrol records in the platform. The patrol records will be deleted automatically when the duration expires.

Offline Patrol

When a guard tour point is not connected to the network, the patrol events generated by the point cannot be reported to the server in real time. Therefore, enabling offline patrol function means to allow a certain time period of report delay.

Patrol Reminder

Used to remind patrol person to execute guard tour patrol schedule. You need to start SMS service first to enable SMS reminder function.

14.3 Set Patrol Route

A patrol route consists of multiple patrol points. You can customize how to conduct a patrol based on a route and configure related information for the route.

Before You Start

Make sure you have configured patrol points. See ***Patrol Point Configuration*** for details.

Steps

1. Click **Patrol** on the Home page to enter the Patrol module.
2. Select **Patrol Route** on the left column.
3. Click **Add** to enter the Add Patrol Route page.
4. Set basic information for the patrol route.

Route Name

You can customize the route name.

Patrol Mode

Select a patrol mode according to actual needs.

No Order

Patrol each patrol point on the route randomly.

First Patrol Point First

Patrol the first patrol point on the patrol list at first.

First Patrol Point First and Last Patrol Point Last

Patrol the first patrol point on the list at first, and the last point on the list at last.

Patrol in Order Without Fixed Interval

Follow the order of the patrol point list to patrol, and the intervals between adjacent patrol points can be different.

Patrol in Order with Fixed Interval and Deviation

Follow the order of the patrol point list to patrol, and the intervals between adjacent patrol points are the same, so are the deviations.

Patrol in Order with Customized Interval and Deviation

Follow the order of the patrol point list to patrol, and the intervals between adjacent patrol points and the deviations can be customized.

Patrol Duration

The time duration needed for conducting patrol of an entire patrol route.

Description

You can enter some description of the route for supplementation.

5. Add patrol points.

1) Click **Add** to enter the add patrol point page.
2) Select an area on the left panel.
3) Check devices in the **Available Patrol Point** area and click ›.

   The checked devices are moved to the **Selected Patrol Point** area.
4) Click **OK**.
5) **Optional:** Drag a patrol point up or down to sort.

Note

- The sequence of the patrol points in the table indicates the patrol sequence.
- You need to customize the interval and error if you select **Patrol in Order with Fixed Interval and Deviation** or **Patrol in Order with Customized Interval and Deviation** as the patrol mode.

6. Click **Save** to save the patrol route.

14.4 Set Holiday

There may be a holiday during which you do not have to conduct the patrol during a patrol schedule. Therefore, you can set holidays by selecting time period and days so that the platform will not count patrols during the holidays.

Steps

1. Click **Patrol** on the home page.
2. Click **Holiday Configuration → Add** to enter the Add Holiday page.
3. Set basic information for the holiday including name and description.
4. Add holiday.
   1) Click **Add** to open the Add Date window.
   2) Select a start time and end time for the holiday, and the select days.

      Note

      The selected days in the selected time period will be holidays.
   3) Click **OK**.
5. Click **Save** to save the settings.

14.5 Set Patrol Schedule

A guard patrols according to the patrol schedule you make after configuring patrol points, parameters, and routes.

Before You Start

Make sure you have configured a patrol route and have added a patrol person to the platform.

Steps

1. Click **Patrol** on the home page.
2. Click **Patrol Schedule → Add** to enter the Add Patrol Schedule page.
3. Set basic information for the patrol schedule.

   Schedule Name

   You can customize the schedule name.

   Patrol Route

   Select a patrol route you had added in the drop-down list.

   Patrol Person

   Select a patrol person in the added person list.

   Start Date/End Date

   The date that the patrol starts/stops to be executed.

   Patrol Cycle

Select conducting the patrol every day/week/month. You conduct patrol every day during the patrol schedule if you select **Every Day**; you conduct patrol on selected days of every week during the patrol schedule if you select **Every Week**; you conduct patrol on selected dates of every month during the patrol schedule if you select **Every Month**.

Holiday Name

Select a holiday that you have configured according to actual needs.

4. Set patrol time period.
   - Click **Add** and select start time and end time.
   - Click **Batch Add** and set the start time, patrol times, and patrol interval, and click **OK**.
5. Click **Save** to save the patrol schedule settings.

14.6 Patrol Information Search

The platform supports searching all the patrol shift schedules and historical patrols by setting different search conditions, and save the searched results in computer.

14.6.1 Search Shift Information

The platform supports searching patrol shift schedule by multiple types of patrol information.

Steps

1. Click **Patrol** on the home page, and select **Information Search → Shift Schedule Search** .
2. Set search conditions including **Patrol Route**, **Patrol Person**, and **Patrol Time**, and click **Search**.

   Search results will be displayed below.
3. **Optional:** Perform the following operations.

Operation	Description
Export Search Result	Click **Export** to save the search results in the current computer in CSV format.
View Details of Search Result	Click to view details of searched shift schedule.

14.6.2 Search Patrol History

The platform supports searching patrol history by multiple types of patrol information.

Steps

1. Click **Patrol** on the home page, and select **Information Search → Historical Patrol Search** .
2. Set search conditions including **Patrol Route**, **Patrol Person**, **Patrol Result** and **Patrol Time**, and click **Search**.

   Search results will be displayed below.

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

Operation	Description
Export Search Result	Click **Export** to save the search results in the current computer in CSV format.
View Details of Search Result	Click to view details of searched historical patrols.

14.7 Report

Patrol points will send real-time patrol-related information to the platform, so that you can generate a patrol report to know the details of patrols during a certain time period. You can also save the report in your computer.

On the home page, click **Patrol → Report** to enter the Report page. Select patrol route/patrol person/patrol point and select a time period in the calendar and the results will be displayed below. You can click **Export** to save the reports in the current computer, or click to view detailed information.

Chapter 15 Parking System

HikCentral Enterprise-Commercial provides parking control for small lots as well as large, complex parking systems. It allows users to register vehicles to the system, set entry and exit rules, control entry & exit, etc., for parking facilities, shopping centers, airports, hotels, arenas, etc.

The parking system in HikCentral Enterprise-Commercial provides the following functions:

Entry & Exit Management

Allow the registered or temporary vehicles to enter or exit the parking lot; open the barrier gate manually or automatically.

Find My Car

Help the vehicle owners find the location where they parked their vehicles.

Parking Guidance

Guide the vehicles to the vacant parking spaces.

Information Search and Report

Search the records of passing vehicles. Show statistics of the traffic flow in the parking lots.

15.1 Flow Chart

If this is the first time you use parking, we recommend you perform configurations according to the chart below.

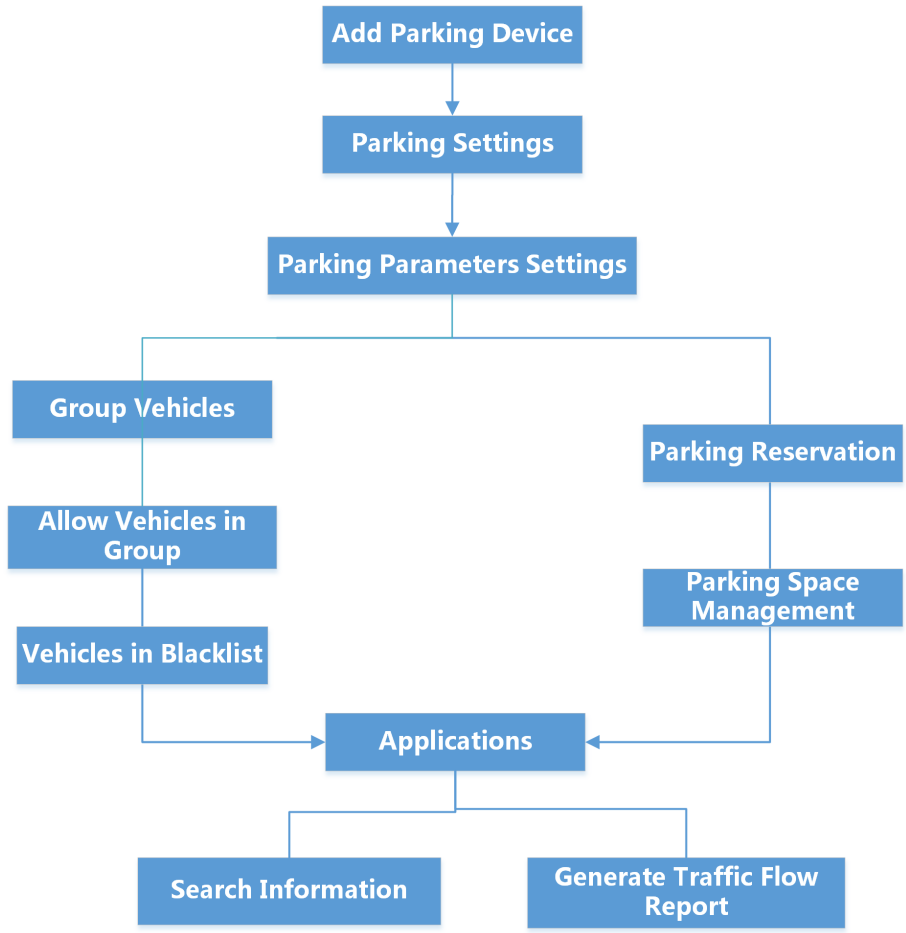


Figure 15-1 Flow Chart

15.2 Parking Device Management

Before any operations in the parking system, you need to add the parking devices (including devices used for guiding the vehicles and devices used at the entrance and exit) to the system and set the parameters respectively.

Entrance and Exit Device

Mounted at the entrances and exits to control the vehicles' entries and exits.

Guidance Device

Mounted at the entrances and in the parking lot to guide the vehicles to park in the vacant parking spaces and help vehicle owners to find where their vehicles are parked.

Note

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufactures. Such initial configuration is required in order to be able to connect the devices to the system via network.
- The devices connected by serial port are correctly connected and you can turn on or off the serial port correctly.
- The devices' working mode is correctly configured according to the device user manuals.
- The guidance server and the booth client terminal are correctly installed and started.
- Such initial configuration is required in order to be able to connect the devices to the system.

15.2.1 Add a Booth Client Terminal by IP Address

Booth client terminal is the PC running the booth client. The booth client terminal is usually mounted at the booth of an entrance or exit. The parking lot manager views passing vehicles' details and allow vehicles to pass or not by controlling the connected barrier gate.

Steps

1. Click ☰ → **System Configuration** → **Devices** → **Vehicle Control** → **Entrance and Exit** → **Booth Client Terminal** .
2. Select an area in the area list.
3. Click **Add**.
4. Enter the device name.
5. Select **By IP** as the adding mode.
6. Enter the required information.

   IP Address

   The IP address of the PC where the booth client runs.

   Port No.

   The port of the terminal. By default, it is ***8500***.
7. Click **Online Test** to check whether the device information is correct.

   The test results will show. If test failed, you should check and edit the device information and click **Test** to start online test again.
8. Click **Save**.

15.2.2 Add a Booth Client Terminal in Automatic Mode

If a booth client terminal has no fixed IP address, you can add a booth client terminal in automatic mode to generate a registration code so that you can log into a booth client by entering platform's IP address and the registration code.

Steps

1. Click ☰ in the upper-right corner, and then click **System Configuration → Devices → Vehicle Control → Entrance and Exit** .
2. Select an area in the area list and then select **Booth Client Terminal**.
3. Click **Add** to enter the Add Booth Client Terminal page.
4. Enter the device name.
5. Select **Automatic** as the Adding Mode.
6. **Optional:** Switch **Show Lane** on.

   Note

   When the function is enabled, lanes will be shown in booth client. Up to 9 lanes can be displayed.

7. Click **Registration Code** to generate a registration code.

   Note

   When you log into booth client for the first time, you will be required to enter the registration code.

15.2.3 Add a Capture Unit

Capture units are ANPR cameras that recognize license plate numbers of the passing vehicles.

Steps

1. Click ☰ **→ System Configuration → Devices → Vehicle Control → Entrance and Exit → Capture Unit** .
2. Select an area in the area list.
3. Click **Add**.
4. Enter the required information.

   Device Model

   Select the model of the capture unit you want to manage in the system.

   IP Address

   The IP address of the device.

   Port No.

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

   Barrier Control

   You can enable the capture unit's barrier control function if the barrier gate is connected to the capture unit via serial port. With this function enabled, the barrier gate will open automatically or need to be opened manually if the linked capture unit recognizes the plate number of registered vehicle.

5. Click **Online Test** to check whether the device information is correct.

Click **Online Test** to check whether the device information is correct.

6. Click **Save**.

15.2.4 Add a Display Screen

A display screen mounted at the entrance or exit is used for showing free parking spaces information in the parking lot in real-time.

Steps

1. Click ☰ → **System Configuration** → **Devices** → **Vehicle Control** → **Entrance and Exit** → **Display Screen** .
2. Select an area in the area list.
3. Click **Add**.
4. Enter the required information.

   Device Model

   Select the model of the screen you want to manage in the system.

   IP Address

   The IP address of the device.

   Screen Dimension

   The height and width of the screen, which you can get from the device label.
5. Click **Online Test** to check whether the device information is correct.

   The test results will show. If test failed, you should check and edit the device information and click **Test** to start online test again.
6. Click **Save**.

15.2.5 Add an Entrance & Exit Station

An entrance & exit station is used to control the vehicle's entering and exiting by controlling the barrier gate, enroll cards to passing vehicles, etc.

Steps

1. Click ☰ → **System Configuration** → **Devices** → **Vehicle Control** → **Entrance and Exit** → **Entrance & Exit Station** .
2. Select an area in the area list.
3. Click **Add**.
4. Enter the required information.

   Device Model

   Select the model of the device you want to manage in the system.

   IP Address

   The IP address of the device.

Port No.

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

Barrier Control

You can enable the barrier control function if the barrier gate is connected to the entrance and exit station via serial port. With this function enabled, the barrier gate will open if you swipe card at the entrance or exit.

5. Click **Online Test** to check whether the device information is correct.

   The test results will show. If test failed, you should check and edit the device information and click **Test** to start online test again.

6. Click **Save**.

15.2.6 Add a Barrier Gate

The barrier gate can be connected to the capture unit, entrance & exit station, and booth client terminal. These devices can open a parking lot gate arm when vehicles enter or leave a parking area. The barrier gate connected to the booth client terminal should be added to the system.

Steps

1. Click → **System Configuration** → **Devices** → **Vehicle Control** → **Entrance and Exit** → **Barrier Gate** .
2. Select an area in the area list.
3. Click **Add**.
4. Enter the required information.

   Connection Mode

   The terminal type the barrier gate connected to.

   Barrier Open Output

   The location where the opening barrier gate signal connects to the terminal device.

   Barrier Close Output

   The location where the closing barrier gate signal connects to the terminal device. You can leave it empty and the coil will control it.

   Note

   You can get the barrier open output and close output from ALARM OUT interface of the connected booth client terminal.

5. Click **Save**.

15.2.7 Add a Bluetooth Card Reader

The card reader which can read the card number of a Bluetooth card is called Bluetooth card reader. Connect the Bluetooth card reader with the booth client terminal by serial port.

Steps

1. Click → **System Configuration** → **Devices** → **Vehicle Control** → **Entrance and Exit** → **Bluetooth Card Reader** .
2. Select an area in the area list.
3. Click **Add**.
4. Enter the required information.

   Device Model

   Select the model of the card reader you want to manage in the system.

   Connection Mode

   The terminal type the barrier gate connected to.

   Serial Port No.

   The location where the device connects to the terminal device.

   Device No.

   Set the device number on the card reader and enter it here as what you set. If you only adopt one Bluetooth card reader, enter 1 here without setting the device ID.
5. Click **Save**.

15.3 Parking Lot Settings

Before any applications in parking system, you need to set the elements (such as lot, floor, lane, etc.) in the parking lot according to the actual situation. For example, the shopping mall owns one underground parking lot and the parking lot contains three floors. The parking lot contains two entrances and two exits, and each entrance or exit has two lanes. You need to add the above elements to the system, and link the added parking devices (such as guidance terminals, guidance screens, capture cameras, barrier gates, etc.) with these elements. After that, the system can help you build a virtual parking system based on the relations of these elements and devices just like the actual lots.

15.3.1 Parking Lot Management

First of all, you need to add the parking lot to the system and set its parameters.

Add Parking Lot

In this section, we introduce how to add a parking lot to the system.

Steps

1. Click → **System Configuration** → **Vehicle Control** → **Parking** → **Parking Lot** .
2. Select an area in the area list.
3. Click to add a parking lot.

Note

You can click to add a sub parking lot as the following steps.

4. Enter the parking lot information.

Parking Lot Name

Create a name for the parking lot.

Number of Parking Spaces

Enter the total number of parking spaces in the parking lot in **Capacity**, and enter the number of parking spaces which are not occupied currently in the **Vacant Parking Space**.

Parking Spaces for Registered Vehicles

Enter the total number of parking spaces which are for registered vehicles only, and enter the number of this type of parking spaces which are not occupied currently.

Entrance and exit permanent vehicle remaining parking space statistics

If you do not enable this function, vacant parking spaces will not include vacant free parking spaces for permanent vehicles.

Reservable Parking Spaces

Enter the number of parking spaces that can be reserved in this parking lot.

Fault-Tolerance for Registered Vehicle

In some situations, the license plate recognition may not be exactly correct. You can set the bit(s) of the plate number for fault-tolerance. If the difference between the recognized license plate number and the one registered in the system is within the configured value, it will be regarded as the same vehicle. For example, if you set the fault-tolerance as 1, the plate number registered in system is A1234B, then if the actual plate number is recognized as A12345, it will be regarded as A1234B registered in the system.

Notify in Advance before Expiration

Display notification of expiration on display screen. Take a vehicle which expires at Jan. 6th, 2020 as an example, if you enter 5, the expiration notification will be displayed on the LED screen linked to the parking lot from Jan. 1st, 2020 to Jan. 5th, 2020.

5. Click **Save**.

Link Device with Parking Lot

After adding a parking lot, you need to link a guidance server and booth client terminals to the parking lot.

Steps

Note

Up to one guidance server can be linked to one parking lot. The guidance server will manage all the guidance devices (such as guidance terminals, guidance screens, etc.) mounted in this parking lot.

1. Click → **System Configuration** → **Vehicle Control** → **Parking** → **Parking Lot** .
2. Select a parking lot and click **Link Device** tab.
3. Click **Link Device**.
4. Select an area in the area list.

   All the devices added to this area will be displayed.
5. Check a guidance server and several booth client terminals in the **To Be Linked Device** area and click to add to the selected device list.

   The checked devices will be moved to the **Linked Device** area.
6. Click **Save**.

15.3.2 Add Entrance and Exit to Parking Lot

Entrances and exits are lanes through which the vehicles can enter or exit the parking lot. One entrance and exit should link with a booth client terminal. The parking lot manager can control the barrier gate to open or close via the booth client.

Steps

1. Click → **System Configuration** → **Vehicle Control** → **Parking** → **Parking Lot** .
2. Select a parking lot on the lot list.
3. Click .
4. Enter a name for the entrance and exit.
5. Select a booth client terminal in the drop-down list to link the booth client terminal with the entrance and exit. Once linked, the manager can view the vehicles entering and exiting through this entrance and exit on the booth client and control the barrier gate to allow or forbid the vehicles to enter or exit.

   Note

   For adding the booth client terminal, refer to ***Parking Device Management*** .
6. Click **Save**.

15.3.3 Lane Management

Vehicles can enter or exit the parking lot through the lanes. You need to specify which lane is for entering and which lane is for exiting. After adding lanes to the entrance and exit, you need to set how the system can record the vehicles' entries and exists and set the entry & exit mode. Besides, you need to link the devices which are mounted in the lane with the lane, such as capture units, display screens, entrance & exit stations, card readers, etc.

Add Lane to Entrance & Exit

In this section, we introduce how to add a lane to the entrance and exit.

Steps

1. Click → **System Configuration → Vehicle Control → Parking → Parking Lot** .
2. Select an entrance and exit in the parking lot list.
3. Click .
4. Enter a name for the lane.
5. Set the lane type as lane for entrance or exit.
6. Set other parameters.

Enable Lane for Motorcycle

If the lane is for motorcycles only, enable this option. The driver should take a temperature card when entering and the lane's recognition mode will be card.

Recognition Mode

How the system distinguishes the vehicles and how the system records the vehicles' entering and exiting time.

License Plate

The ANPR camera mounted in this lane will detect the plate number of the vehicles in the lane and record the entering or exiting time based on the time recognizing the plate number. Select this mode if there is an ANPR camera mounted in the lane to recognize the license plate number of the passing vehicles.

Take a Card for Temporary Vehicle

When a vehicle enters, if the recognized license plate number is not registered in the system, the driver should take a card to record the entering time. When exiting, the driver should return the card to record the exiting time. If the card is lost when exiting, the manager can fetch its entering time according to its license plate number.

Take a Card for Vehicle Without License Plate

When a vehicle with no license plate enters, the driver should take a card to record the entering time. When exiting, the driver should return the card to record the exiting time.

Card

The driver should take a card when entering and return the card when exiting. The entering and exiting time are recorded when taking and returning the card. Select this mode if no ANPR cameras are mounted in the lane.

No Duplicate Entry or Exit

When a vehicle entering or exiting, if another vehicle with same plate number or card number already enters or exits the parking lot, the barrier gate will not open to forbid the vehicle to enter or exit.

Enabled Time Period

The time periods during which the vehicles are allowed to enter or exit through the lane. Out of these time periods, no vehicles can enter or exit.

Temporary Vehicle Entry & Exit and Registered Vehicle Entry & Exit

Set how to allow the temporary vehicles to enter or exit the parking lot, and how to allow the vehicles with no license plate enter or exit.

Manual

The manager should click the button on the booth client to open the barrier gate of the lane to allow the vehicles to enter or exit.

Auto

The system will analyze the license plate number or card number to judge whether to open the barrier gate.

Temporary Vehicle: Both Card and License Plate Match

If the lane is for exit, and you select **Take a Card for Temporary Vehicle**, when exiting, the temporary vehicle's license plate and the card number should both match with the entering record.

Registered Vehicle: Both Card and License Plate Match

If the lane is for entrance, when entering, the driver of the registered vehicle should swipe his/her card issued when adding a registered vehicle on the card reader. If the license plate number and the card number match, the vehicle can enter the lot.

If the lane is for exit, when exiting the driver of the registered vehicle should swipe his/her card issued when adding a registered vehicle on the card reader. If the license plate number and the card number match, and entering record is found, the vehicle can exit the lot.

7. Click **Save**.

Link Device with Lane

After adding a lane, you need to link the added lane devices which are mounted in the lane with the lane, such as Entrance & Exit Station, capture unit, display screen, barrier rate, etc.

Steps

1. Click → **System Configuration** → **Vehicle Control** → **Parking** → **Parking Lot** .
2. Select a lane in the parking lot list.
3. Click **Link Device** tab.
4. Click **Link Device**.
5. Select an area in the area list.

   All the lane devices added to this area will be displayed.
6. Check device(s) in the **To Be Linked Device** area and click .

   The checked devices will be moved to the **Linked Device** area.
7. Click **Save**.

15.3.4 Set Data Storage Parameters

Click → **System Configuration** → **Vehicle Control** → **Parking** → **Parameters** → **Data Storage Parameters** .

- Set the retention duration of the data such as passing vehicle records and parking records.
- Set the retention duration of parking duration of vehicles without plate.

15.4 Vehicle Management

In general, there are three categories of vehicles in HikCentral Enterprise-Commercial:

Registered Vehicle

The vehicles' information is registered in the system in advance. When they enter or exit the parking lot, the camera will recognize the plate number and record the entering or exiting time in the database.

Vehicle Group

Vehicles in one vehicle group shares the same entry & exit rule. You can set an entry & exit rule for the group after grouping vehicles into the group.

Vehicle in Blacklist

The vehicles are not allowed to enter the parking lot if the camera recognize the plate number matched with the plate number in the blacklist. Or the system can trigger blacklist alarms when these vehicle entering/exiting the lot.

Temporary Vehicle

The vehicles are not registered in the system. They can enter the parking lot for once with assigned temporary cards. When exiting, the vehicle owners need to swipe the cards on the card reader, or return the cards to the parking lot manager. With the temporary cards, these vehicles' entering and exiting time will be recorded in the database.

15.4.1 Group Registered Vehicles

In some cases, the registered vehicles need to be grouped in to different groups. The administrator can set an entry & exit rule to the vehicles in one group. For example, if the parking lot is shared by two companies, you may need to group the vehicles of these two companies into two groups respectively, since the time periods in which the vehicles are allowed to enter/exit may be different.

Before You Start

Note

One vehicle can only be added to one group.

Add registered vehicles to the system. For details, refer to *Manage Registered Vehicles.*

Steps

1. Click **Parking** on Home page and click **Vehicle and Card → Vehicle Group** .
2. Click **Add** to enter the Add Vehicle Group page.
3. Enter a name for the group.
4. Enter the description for the group.
5. In the Selectable Vehicle list, all the vehicles which haven't been added to any groups will be displayed. Check the vehicles you want to add to the group.
6. Click ❯ to add the selected vehicles to the Selected Vehicle list.
7. Click **Save**.

15.4.2 Manage Vehicles in Blacklist

For the vehicles in blacklist, when they enter/exit the parking lot, it will generate an alarm and trigger configured linkage actions.

Here are two examples for applications of vehicles in blacklist.

- If one vehicle, which is already added in the blacklist, needs to be parked in the lot, when its license plate number is detected by the ANPR cameras mounted at the entry, an alarm will be triggered to notify the surveillance center. You can set to forbid the vehicles in blacklist to enter the lot.
- For the vehicle which is already in the parking lot, if it is considered as suspicious, you can add it in the blacklist and forbid the vehicles in blacklist to exit.

Add One Vehicle to Blacklist

You can add the vehicle to the blacklist one by one.

Steps

1. Click **Parking** on Home page and enter **Vehicle and Card → Vehicle in Blacklist** .

2. Click **Add**.
3. Set the control mode as Plate Number or Card No.

   License Plate

   Arm the vehicle by license plate number. Enter the license plate number of the vehicle and when the plate number is detected, an alarm will be triggered.

   Card No

   Arm the vehicle by card number. Enter the card number and when the vehicle owner swipes the card on the card reader, an alarm will be triggered.
4. **Optional:** Enter the vehicle owner name, phone number, and remark information.
5. **Optional:** Set an end time for this vehicle. Before the end time, the vehicle will be armed. Once expired, the vehicle (license plate number or card number) will not be armed.
6. Click **Save**.
7. **Optional:** Perform the following operations after adding the vehicle to the blacklist.
   - Click in the Operation column to edit the vehicle's details.
   - Click in the Operation column to remove this vehicle from the blacklist.
   - Select the vehicle(s) and click **Delete** to remove the selected ones from the blacklist.

Import Vehicles in a Batch

Import multiple vehicles by uploading a file with vehicle information to the system.

Steps

1. Click **Parking** on Home page and enter **Vehicle and Card → Vehicle in Blacklist** .
2. Click **Import**.
3. Click **Download File Template** to download a template file in CSV format.
4. Enter the vehicle information in the template.

   You can hover the cursor on Field Description to view the descriptions of different fields in the template.

   Note

   Up to 50,000 records can be imported. The file size should be within 50 MB.
5. Click **Select** and select the template file filled with vehicle information.
6. Click **Import** to start.

Export Vehicles in Blacklist

If you need to back up the vehicle information in the blacklist, you need to export them and save them in a CSV file and store it in the current PC.

Steps

1. Click **Parking** on Home page and enter **Vehicle and Card → Vehicle in Blacklist** .

2. Click **Export**.
3. Confirm the export and a CSV file with all the vehicle information in the blacklist will be downloaded and stored in the PC running the Web Client.

15.4.3 Manage Temporary Card

The vehicles which are not registered in the system are called temporary vehicles. The vehicle owners might be visitors (for company), customers (for shopping mall), etc. When the temporary vehicle enters the parking lot, the driver should take a temporary card from the parking lot manager or from the Entrance & Exit Station, which can record the vehicle's entering time. When temporary vehicle exits the parking lot, the driver needs to return the card to the parking lot manager or Entrance & Exit Station to record the exiting time.

Before You Start

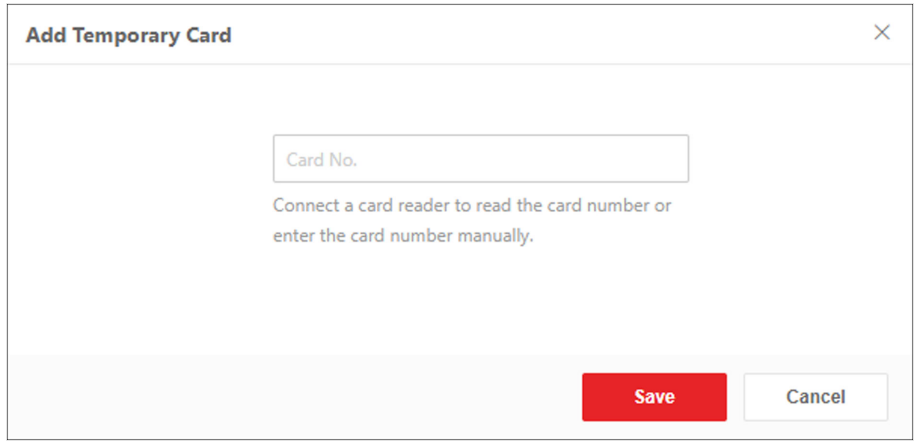
You need to add temporary cards to the system first.

Steps

1. Click **Parking** on Home page and enter **Vehicle and Card → Temporary Card** .

   The added parking lots are displayed on the left.
2. Select a parking lot to add the temporary card.

   The temporary cards added to the selected lot will display.
3. Click **Add** to open the following window.



4. Enter the card No.

   You can get the card number with a card reader connected to the PC.
5. Click **Add** to add the card.
6. **Optional:** Perform the following operations after adding the temporary cards.
   - Click in the Operation column to delete it.
   - Select the vehicle(s) and click **Delete** to delete the selected cards from the system.

15.4.4 Set Card Enrollment Parameters

On the Home Page, click **Parking → Vehicle and Card → Card Enrollment Parameters** .

Select the device model you use to read card numbers and set the parameters.

- DS-K1F100-D8E is card enrollment station. It supports issuing Mifare card, CPU card, ID card and ID serial No., and encrypting Mifare card sector and CPU card.
- DS-K1F100-D8 is card enrollment station. It supports issuing Mifare card, CPU card, and encrypting Mifare card sector and CPU card.
- DS-K1F110-I (USB)/DS-K1F1110-AB is ID card reader for reading ID card information and Mifare card number.
- DS-TRD400-4 is Bluetooth card enrollment station with battery, 433MHz, Bluetooth range: 3 to 15 cm.
- DS-TRD900-1 is card enrollment station without battery, 900 MHz, RFID range: 10cm.

15.5 Entry & Exit Rule Management

Entry & exit rules are used to define whether and when the vehicles are allowed to enter or exit the parking lot. For example, you can define that the vehicles in group A can enter the parking lot during 8:00 a.m. to 6:00 p.m., but are forbidden to exit.

15.5.1 Set Entry & Exit Parameters

On the Home Page, click **Parking → Entry & Exit Control** . Select a parking lot in the parking lot list. Click **Entry & Exit Rule** tab.

When No Vacancy for Temporary Vehicle

Allow or forbid the temporary vehicles to enter the parking lot when there are no vacant parking spaces for temporary vehicles.

When No Vacancy for Registered Vehicle

Allow or forbid the registered vehicles to enter the parking lot when there are no vacant parking spaces for registered vehicles.

When Vehicle in Blacklist

Allow or forbid the vehicles in blacklist to enter or exit the parking lot.

Fault-Tolerance for Registered Vehicle

In some situations, the license plate recognition may not be exactly correct. You can set the bit(s) of the plate number for fault-tolerance. If the difference between the recognized license plate number and the one registered in the system is within the configured value, it will be regarded as the same vehicle. For example, if you set the fault-tolerance as 1, the plate number registered in system is A1234B, then if the actual plate number is recognized as A12345, it will be regarded as A1234B registered in the system.

15.5.2 Set Entry & Exit Rule for Vehicles in Group

You can set an entry & exit rule for the vehicles in one vehicle group. The vehicles in this group share the same rule which defines whether and when they are allowed to enter or exit the parking lot.

Before You Start

Group the vehicles into vehicle groups.

Steps

1. Click **Parking** on Home page and enter **Entrance & Exit Control → Entry & Exit Rule for Vehicle Group** .

   The added parking lots are displayed on the left.
2. Select a parking lot to add the rule.
3. Click **Add**.
4. Select a vehicle group in the drop-down list.
5. Set the entry rule.
   1) Enable **Entry Permission** to allow the vehicles in the vehicle group to enter the lot.
   2) Set the time periods during which the entry permission is valid in one day.

      All-Day

      The entry permission is valid and the vehicles in the vehicle group can enter the lot during 0:00 to 24:00 every day.

      Custom

      Add time periods in one day and set the start time and end time of these time periods. The entry permission is valid and the vehicles in the vehicle group can enter the lot during these time periods every day.

      Note

      Up to 4 time periods can be added.
6. Set the exit rule.
   1) Enable **Exit Permission** to allow the vehicles in the vehicle group to exit the lot.
   2) Set the time periods during which the exit permission is valid in one day.

      All-Day

      The exit permission is valid and the vehicles in the vehicle group can exit the lot during 0:00 to 24:00 every day.

      Custom

      Add time periods in one day and set the start time and end time of these time periods. The exit permission is valid and the vehicles in the vehicle group can exit the lot during these time periods every day.

Note

Up to 4 time periods can be added.

7. **Optional:** Enter the description information to describe the rule.
8. Click **Save**.

15.6 Make a Parking Reservation

The visitors can contact the parking lot administrator if they want to park their vehicles in the parking lot. The administrator can make a reservation in advance with the visitor's license plate number. After the reservation, the visitor's vehicle can enter the parking lot before the reservation expires.

For example, if a visitor needs to park his/her vehicle in the parking lot of the company he/she will visit, the administrator should make a reservation by the license plate number of the visitor's vehicle. With this reservation, the visitor is allowed to enter the parking lot for once.

Steps

1. On the Home page, click **Parking → Vehicle and Card → Reservation Management** .
2. Select a parking lot in the parking lot list.
3. Click **Reserve** to open the Add Reservation page.
4. Enter the license plate number of the visitor's vehicle.
5. Set the following parameters for the reservation.

   Effective Time

   The time after which the vehicle can enter the parking lot. For example, you set 2020/01/09 19:17 as the effective time, and the vehicle can enter the parking lot only after this time.

   Expiry Time

   The expiry time of the reservation. For example, you set 2020/01/09 23:59 as the expiry time, and the vehicle will be prevent from entering the parking lot after this time.

   Permitted Entries

   One-time capture: the vehicle will be prevent from entering the parking lot again after exiting.

   Multiple captures: the vehicle can enter/exit the parking lot for multiple times before the expiry time.
6. Enter the contact person name. For example, the person who invites the visitors.
7. Enter the phone number of the vehicle owner or the contact.
8. Click **Save**.

15.7 Correct Number of Vacant Parking Spaces

The system will calculate the number of vacant parking spaces based on the vehicle passing data recorded by the ANPR cameras mounted at the entries and the exits. If the actual number of vacant parking spaces is different from the vacant parking spaces shown in the system, you can correct the number manually. After correction, the vacant parking spaces shown on the LED screen and on other clients (such as booth client) will be changed to the number you entered.

Before You Start

You can get the current number of vacant parking spaces by searching the vehicles in parking lot. For details, refer to ***Search Vehicles in Parking Lot*** .

Steps

1. Click **Parking** on Home page and enter **Parking Spaces → Correct Number of Vacant Parking Spaces** .

   The added parking lots are displayed on the left.
2. Select a parking lot.

   The current number of total vacant parking spaces and vacant parking spaces for registered vehicles are displayed.
3. Enter the actual number.
4. Click **Correct**.

15.8 Search

In this section, you can search the vehicles that are in the parking lot currently. You can also search the vehicle's passing records and search the parking records of different parking spaces. The reservation records can also be searched if necessary.

15.8.1 Search Vehicle Passing Records

When a vehicle entering or exiting the parking lot, the ANPR camera will capture its picture and license plate picture and record the time in the database. You can search the records of certain passing vehicle(s) by specifying the filtering conditions.

Click **Parking** on Home page and enter **Search → Passing Vehicle Records** .

Set the search conditions, such as license plate number, time, etc., and click **Search** to start.

You can click **Export** to export the search results and save in the PC running the Web Client.

15.8.2 Search Vehicles in Parking Lot

Based on the vehicle passing records recorded by the cameras mounted at the entries and exits, the system can tell the vehicles which are still in the parking lot (entering records found while exiting records not).

Click **Parking** on Home page and enter **Search → Vehicles in Parking Lot** .

Set the filter conditions, such as license plate number, card number, etc., and click **Search** to start.

Accuracy

The license plate recognition accuracy of the ANPR cameras.

Time Period

Filter the vehicles which enter the parking lot during the specified time period, or filter the vehicles which have been in the lot over the specified duration.

You can click **Export** to export the search results and save in the PC running the Web Client.

15.8.3 Search Reservation Records

After making a reservation, the reservation will be recorded in the database. You can search the reservation records by setting filter conditions.

Click **Parking** on Home page and enter **Search → Reservation** .

Set the filter conditions such as license plate number, phone number, etc., and click **Search** to start.

You can click **Export** to export the search results and save in the PC running the Web Client.

15.9 Generate Traffic Flow Report

Reports, created for a specified period, are essential documents, which are used to check whether a business runs smoothly and effectively. In HikCentral Enterprise-Commercial, reports can be generated daily, monthly, annually, and by custom time period. You can use reports as basis in creating decisions, addressing problems, checking tendency and comparison, etc.

In this section, HikCentral Enterprise-Commercial provides traffic flow reports to show how many vehicles parked in each parking lot per hour.

Click **Parking** on Home page and enter **Statistical Analysis → Traffic Flow Report** .

Set the report time and other search conditions.

Daily Report

Daily report shows data on a daily basis. The system will calculate the number of parked vehicles in each hour of one day.

Monthly Report and Annual Report

As compared to daily 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 parked vehicles in each day of one month and in each month of one year.

Custom

Users can customize the days in the report to analyze the number of parked vehicles in each day of the custom time interval.

You can click **Export** to export the search results and save in the PC running the Web Client.

Chapter 16 Query and Guidance

Query and guidance function helps you find vacant parking space or guide you to the parking space where you parked your vehicle in by query and guidance devices in a parking lot, which greatly saves your time for finding vacant parking place and locating your parking place. This function is oriented to be used in large-scaled parking lot.

16.1 Flow Chart

If this is the first time you use query and guidance function, we recommend you perform configurations according to the chart below.

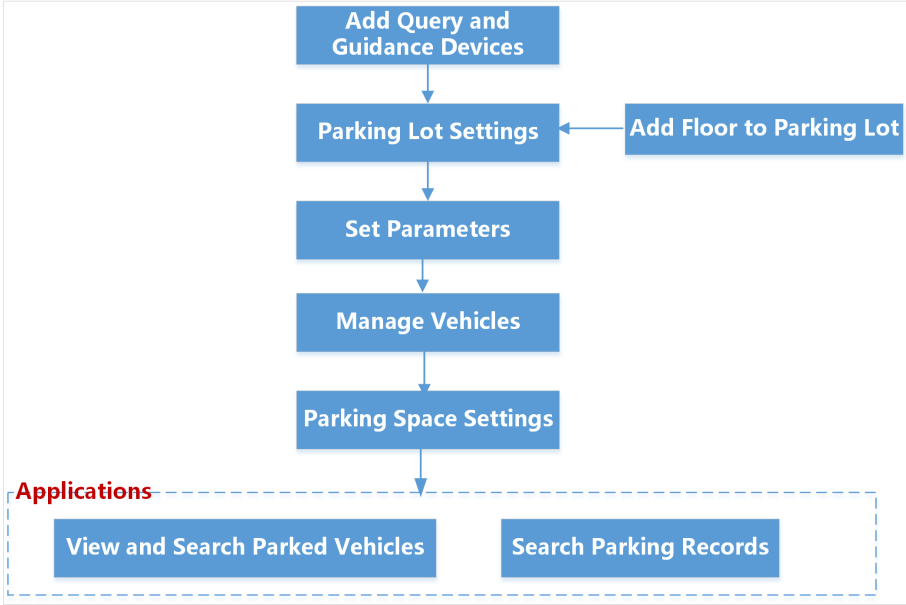


Figure 16-1 Operation Flow Chart

16.2 Query and Guidance Device Management

To perform query and guidance function, you need to add query and guidance devices to the platform beforehand. Query and guidance devices include guidance screen, entrance guidance screen, query terminal, and guidance terminal.

16.2.1 Add a Guidance Terminal

The system can manage the parking cameras and guidance screens via the guidance terminal. You can connect the parking cameras and guidance screens to the guidance terminal. For details, refer to the user manuals of the parking cameras and guidance screens.

Steps

1. Click → **System Configuration** → **Devices** → **Vehicle Control** → **Guidance** → **Guidance Terminal** .
2. Click **Add**.
3. Enter the required information.

   Device Model

   Select the model of the terminal you want to manage in the system.

   IP Address

   The IP address of the device.

   Port No.

   The port of the device. By default, it is 8000.
4. Click **Online Test** to check whether the device information is correct.

   The test results will show. If test failed, you should check and edit the device information and click Test to start online test again.
5. Click **Save**.
6. Add multiple terminals in a batch by importing a file with terminal information.
   1) Click **Import**.
   2) Click **Download File Template** to download a template file in CSV format.
   3) Enter the terminal information in the template.
   4) You can hover the cursor on **Field Description** to view the descriptions of different fields in the template.

      Note

      Up to 300 records can be imported. The file size should be within 1 MB.
   5) Click and select the template file filled with terminal information.
   6) Click **Import** to start.

16.2.2 Add a Guidance Screen

The guidance screen is mounted in the parking lot to display the vacant parking spaces in different directions, which can guide the vehicles to find the vacant parking spaces. The guidance screen can be connected to the system by network, or connected to the guidance terminal by serial port.

Steps

1. Click → **System Configuration** → **Devices** → **Vehicle Control** → **Guidance** → **Guiding Display** .

2. Click **Add**.
3. Enter the required information.

Device Model

Select the model of the screen you want to manage in the system.

Connection Mode

How the screen is connected.

Network

The screen is connected to the system via network protocol.

Serial Port

The screen is connected with the guidance terminal via RS-485 protocol.

IP Address

If you select network mode, enter the IP address of the device.

Port No.

If you select network mode, enter the port of the device. By default, it is 10000.

Guidance Terminal

If you select serial port mode, select the guidance terminal the screen connected to. You should first add this guidance terminal to the system.

Screen Address

If you select serial port mode, enter the address code configured by the guidance screen configuration tool.

4. Click **Save**.
5. You can also add multiple screens in a batch by importing a file with screen information.
   1) Click **Import**.
   2) Click **Download File Template** to download a template file in CSV format.
   3) Enter the screen information in the template.
   4) You can hover the cursor on **Field Description** to view the descriptions of different fields in the template.

Note

Up to 300 records can be imported. The file size should be within 1 MB.

   5) Click **Select** and select the template file filled with screen information.
   6) Click **Import** to start.

16.2.3 Add an Entrance Guidance Screen

The entrance guidance screen is mounted at the entrance to display the vacant parking spaces on each floor, which can guide the vehicles to park on the floor with more vacancy.

Steps

1. Click ☰ → **System Configuration** → **Devices** → **Vehicle Control** → **Guidance** → **Entrance Guidance Screen** .
2. Click **Add**.
3. Enter the required information.

   Device Model

   Select the model of the screen you want to manage in the system.

   Connection Mode

   How the screen is connected.

   Network

   The screen is connected to the system via network protocol.

   Serial Port

   The screen is connected with the guidance terminal via RS-485 protocol.

   IP Address

   If you select network mode, enter the IP address of the device.

   Port No.

   If you select network mode, enter the port of the device. By default, it is 10000.

   Guidance Terminal

   If you select serial port mode, select the guidance terminal the screen connected to. You should first add this guidance terminal to the system.

   Screen Address

   If you select serial port mode, enter the address code configured by the guidance screen configuration tool.

   Number of Lines Display

   Set how many lines can be displayed on the screen, based on which you can set the display content.
4. Click **Save**.

16.2.4 Add a Query Terminal

Query terminal is the PC running the Find My Car client, which can help the vehicle owner find the place where he/she parked her/his vehicle and generate a route to the vehicle.

Steps

1. Click ☰ → **System Configuration** → **Devices** → **Vehicle Control** → **Guidance** → **Query Terminal** .
2. Click **Add**.
3. Enter the required information.

   IP Address

The IP address of the PC that running the Find My Car client.

Port No.

The port of the terminal. By default, it is 8505.

4. Click **Online Test** to check whether the device information is correct.
5. Click **Save**.

16.3 Parking Lot Settings

After adding query and guidance devices to the platform, you need to perform operations including adding parking lot, adding floors, linking device to floors, locating device on floor map, and setting related parameters.

Note

The settings you made here will be automatically applied to the Parking module.

16.3.1 Add Parking Lot

In this section, we introduce how to add a parking lot to the system.

Steps

1. Click → **System Configuration** → **Vehicle Control** → **Parking** → **Parking Lot** .
2. Select an area in the area list.
3. Click to add a parking lot.

Note

You can click to add a sub parking lot as the following steps.

4. Enter the parking lot information.

Parking Lot Name

Create a name for the parking lot.

Number of Parking Spaces

Enter the total number of parking spaces in the parking lot in **Capacity**, and enter the number of parking spaces which are not occupied currently in the **Vacant Parking Space**.

Parking Spaces for Registered Vehicles

Enter the total number of parking spaces which are for registered vehicles only, and enter the number of this type of parking spaces which are not occupied currently.

Entrance and exit permanent vehicle remaining parking space statistics

If you do not enable this function, vacant parking spaces will not include vacant free parking spaces for permanent vehicles.

Reservable Parking Spaces

Enter the number of parking spaces that can be reserved in this parking lot.

Fault-Tolerance for Registered Vehicle

In some situations, the license plate recognition may not be exactly correct. You can set the bit(s) of the plate number for fault-tolerance. If the difference between the recognized license plate number and the one registered in the system is within the configured value, it will be regarded as the same vehicle. For example, if you set the fault-tolerance as 1, the plate number registered in system is A1234B, then if the actual plate number is recognized as A12345, it will be regarded as A1234B registered in the system.

Notify in Advance before Expiration

Display notification of expiration on display screen. Take a vehicle which expires at Jan. 6th, 2020 as an example, if you enter 5, the expiration notification will be displayed on the LED screen linked to the parking lot from Jan. 1st, 2020 to Jan. 5th, 2020.

5. Click **Save**.

16.3.2 Floor Management

In some cases, the parking lot may have more than one floors. As a result, you need to add floors to the parking lot according to actual situation. After adding a floor, you need to link the added guidance devices which are mounted on that floor with the floor. A floor map with parking spaces can help the manager manage the parking spaces which belong to specified vehicle owners. It can also be used to guide the vehicles to park in the vacant parking spaces and guide the vehicle owners to find where their vehicles are parked.

Note

If you don't need guidance function and find my car function, you can skip this section.

Add Floor to Parking Lot

In this section, we introduce how to add a floor to the parking lot.

Steps

1. Click → **System Configuration** → **Vehicle Control** → **Guidance** → **Floor** .
2. Select a parking lot in the list.
3. Click .
4. Enter a name for the floor. For example, 1st Floor.
5. **Optional:** Click **Select File** to select a pre-defined MAP file.

Note

The MAP file should be created according to the resources on the floor accurately. For how to make a MAP file, please contact our technical support.

Link Device with Floor

After adding a floor, you need to link the guidance devices mounted on this floor with it, such as guidance terminals, guidance screens, self-service terminals, etc.

Steps

1. Click → **System Configuration** → **Vehicle Control** → **Guidance** → **Floor** .
2. Select a floor in the list.
3. Click **Link Device** tab.
4. Click the device tab and click **Link Device**.
5. Select an area in the area list.

   All the guidance devices added to this area will display.
6. Check device(s) in the **Device to be Linked** and click › to add them to the **Linked Device** list.
7. Click **Save**.

Locate Device on Floor Map

After uploading a floor map to the system, you need to locate the linked guidance screens and self-service devices on the map based on their actual mounting location. For guidance screens, you also need to specify the parking spaces which will be monitored by the guidance screen. When the vehicle enters, the vacant parking spaces of the parking spaces the screen monitored will be displayed on the guidance screen.

Steps

1. Click → **System Configuration** → **Vehicle Control** → **Guidance** .
2. Select a floor in the list.
3. Click **Map Configuration**.

   The map of the floor will show.
4. Locate the guidance screens on the map.
   1) Click **Mark** → **Parking Guidance Screen** inn the upper-right corner.
   2) Click **Unmarked** tab in the Mark Guidance Screen panel to view the linked guidance screens which haven't been located on the map.
   3) Drag the guidance screen name to the map to locate it on the map according to the location where it is mounted.

      An icon will show on the location.
   4) **Optional:** Drag the screen icon to move it.
5. Locate the self-service devices on the map.
   1) Click **Mark** → **Self-Service Device** in the upper-right corner.
   2) Click **Unmarked** tab in the Mark Self-Service Device panel to view the linked query terminals which haven't been located on the map.
   3) Drag the query terminal name to the map to locate it on the map according to the location where it is mounted.

The self-service device will be displayed as .

4) **Optional:** Drag the icon to move it.

16.3.3 Set Parameters

Click → **System Configuration** → **Vehicle Control** → **Guidance** → **Parameters** to enter the parameter settings page.

Parking Record Retention Time

Select **Data Retention** tab, and then select a retention time for parking record.

Map Type

Select the map type for parking lot's floors.

Vector Map

A vetor map is often used in large-scaled parking lots with complicated internal structure. Generally speaking, it is customized by professionals.

Figure 16-2 Vector Map

Static Map

A floor plan in image format. It is often used in small-scaled parking lots with simple internal structure.

Figure 16-3 Static Map

16.4 Parking Space Settings

In most cases, the parking spaces can be classified into different types, such as parking spaces for registered vehicles only, parking spaces for disabled, etc. You can link the parking space with specified vehicle so that if it is parked by other vehicles, an alarm will be triggered to notify the manager.

16.4.1 Add Parking Space Type

The system pre-defines five types of parking spaces. You can also customize other types according to actual needs.

Before You Start

Make sure you have configured floors for the parking lot, and configured maps for the floors.

Steps

1. On Home page, click **Guidance → Parking Space Settings** .
2. Select a parking lot in the parking lot list.
3. Select a floor in the upper-left corner of the map.
4. Click **Parking Space Settings**.
5. Select one or more parking space on the map and click ⚙ to add customized parking space types.
   1) Click **Add** and enter a name for the custom type.

2) Click **Save**.

The system will assign a color for the newly added type automatically.

3) **Optional:** Perform the following operations after adding new parking space types.
   - Click in the Operation column to edit the type name.
   - Click in the Operation column to delete this type.
   - Select the custom types and click **Delete** to delete them.

6. Click **Save**.

16.4.2 Classify Parking Spaces to Different Types

After setting the types of parking spaces, you need to classify the parking spaces in the parking lots to these pre-defined types. For example, you need to specify which parking spaces are for registered vehicles.

Steps

1. On Home page, click **Guidance → Parking Space Settings** .
2. Select a parking lot in the parking lot list.
3. Select a floor in the upper-left corner of the map.
4. Click **Parking Space Settings**.
5. Select one or more parking space on the map and select a parking space type in the **Parking Space Type** drop-down list.

   Allowed Parking Space

   Parking space that allowing vehicles to park.

   Forbidden Parking Space

   Parking space that forbidding vehicles to park. An alarm will be triggered if a vehicle parks here.

   Dedicated Parking Space

   Parking spaces that are exclusively for certain vehicles.

6. **Optional:** Enable **Vacancy Statistics**. After enabling, the selected parking spaces will be counted as vacant parking spaces and displayed on the screen.
7. Click **Save**.

16.4.3 Link Parking Space with Vehicle

You can link the parking space with vehicle(s), and set to allow or forbid these linked vehicle(s) to park in. If the parking space is occupied by other vehicles, or by vehicles which are forbidden, an alarm will be triggered to notify the managers.

Steps

Note

This function is available for allowed parking space, forbidden parking space, and dedicated parking space.

1. On Home page, click **Guidance → Parking Space Settings** .
2. Select a parking lot in the parking lot list.
3. Select a floor in the upper-left corner of the map.
4. Click **Parking Space Settings**.
5. Select one or more parking space on the map.
6. In the **Parking Space Type** drop-down list, select a parking lot type.
7. Enter the license plate number(s) of the vehicle(s) or click **Select** to select the vehicle(s) which are allowed or forbidden to park in the selected parking space(s).
8. Click **Save**.

16.5 View and Search Parked Vehicles

After configuring the maps of the parking lot, if the parking space is occupied by a vehicle, its status will be changed. In this section, you can view the parking status of the parking spaces in the parking lot and view the details of the vehicles parked in.

Before You Start

This function is supported if the parking lot is deployed with devices such as parking camera, guidance servers, etc.

Steps

1. On Home page, click **Guidance → Find My Car** .
2. Select a parking lot in the parking lot list.
3. Select a floor in the upper-left corner of the map.

   The map of the floor is displayed. You can view the status of each parking space, such as the parking space is occupied or vacant.
4. In the search bar, select the searching mode in the drop-down list.

   Parking Space

   Enter the number of the parking space to search its parking status.

   Plate No.

   Enter the vehicle's license plate number to see where the vehicle is parked in.

   Parking Time

   Set a time period to see which parking spaces are occupied during this time period.
5. Click **Search**.
6. **Optional:** Click **Search Vehicle with No License Plate** to view the vehicles which are parked in the parking spaces currently, with no license plate.

You can view the search results including the parking spaces and the vehicles parked in.

Click the search result to view where the vehicle is parked.

16.6 Search Parking Records in Parking Spaces

With the deployment of parking cameras, the time that the vehicle enters or exits the parking space is recorded in the database. You can search the parking records in different parking spaces and view the vehicles pictures.

On Home page, click **Guidance → Parking Space Recod Search** .

Set the filter conditions such as parking space number, license plate number, etc., and click **Search** to start.

You can click **Export** to export the search results and save in the PC running the Web Client.

16.7 Manage Advertisements

There is a screen on the self-service terminals (including query terminals). You can release an advertisement to the self-service terminals as promotion.

16.7.1 Uploading a Poster

You can upload a poster to the system for advertisement.

Before You Start

Note

The image of the poster should be in JPG, PNG, or BMP format. The recommended dimension is 1920 × 1280.

Steps

1. On Home page, click **Guidance → Advertisement Release → Poster Management** .
2. Drag the image of the poster to the dashed area or click **Add** to upload one.

   The image will be uploaded to the system.

16.7.2 Release Poster to Self-Service Device

After uploading posters to the system, you can select the poster(s) and release them to the self-service terminals.

The posters will be displayed in turns on the screen of the self-service terminals. After releasing, the new advertisement will replace the previous one.

Steps

1. On Home page, click **Guidance → Advertisement Release → Release Poster** .
2. Select one or more poster in the **Advertisement to be Released** area.
3. In the **Self-Service Device** area, check one or more self-service terminals that will display the selected posters.
4. Enter the display interval in the lower-left corner.

   The selected posters will display on the self-service terminals in turns and each poster displays for the configured interval.
5. Click **Confirm**.

Chapter 17 Checkpoint

In the Checkpoint module, you can manage checkpoint devices and analyze checkpoint events.

The Campus Checkpoint module provides multiple functionality, such as the examples below.

- Example A: The instantaneous speed or average speed of a passing vehicles captured by the camera of checkpoint can be calculated by the speed measurement rule you specified for a specific checkpoint or a segment between two checkpoints. Based on the calculated instantaneous speed or average speed, the platform determines if the passing vehicles over-speed.
- Example B: You can set blacklist or whitelist to monitor particular vehicles with higher security level.
- Example C: You can search capture events and traffic violation events, view the amount of vehicles passing through checkpoint(s) and the amount of traffic violation events.
- Example D: You can view the driving pattern of a specific vehicle in the campus.

17.1 Flow Chart

You are recommended to follow the flowchart below to do configurations and operations in the Checkpoint module.

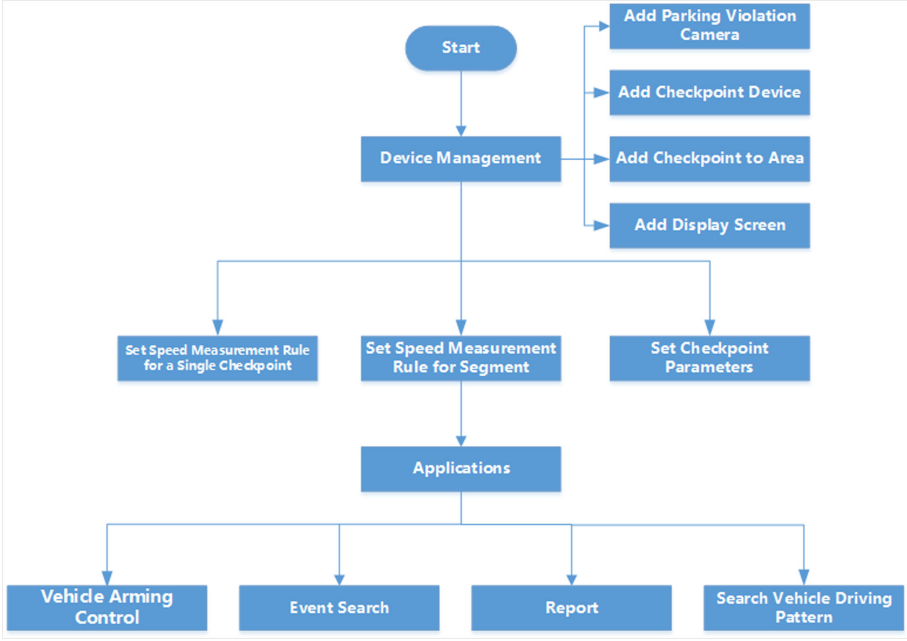


Figure 17-1 Flow Chart of Campus Checkpoint Operation

- Add Parking Violation Camera: Add parking violation cameras to the platform. For details, see ***Add Parking Violation Camera***
- Add Checkpoint Device: Add checkpoint devices to the platform. For details, see ***Add Checkpoint Device*** .
- Add Checkpoint to Area: Add checkpoints to specific areas. For details, see ***Add Checkpoint Traffic Camera to Area*** .
- Add Display Screen: Add display screen to the platform to display information such as vehicle over-speed. For details, see ***Add Display Screen*** .
- Configure Speed Measurement Rule for a Single Checkpoint: Configure speed measurement rule to a single checkpoint to calculate the instantaneous speed of a vehicle when it passing through the checkpoint. For details, see ***Set Speed Measurement Rule for a Single Checkpoint*** .
- Configure Speed Measurement Rule for Segment: Configure speed measurement rule for the segment between two checkpoints so as to calculate the average speed of a vehicle when it passing through the segment. For details, see ***Set Speed Measurement Rule for Segment*** .
- Set Checkpoint Parameters: Set parameters such as retention time of the capture events and violation records. For details, see ***Set Checkpoint Parameters*** .
- Vehicle Arming Control: Add vehicles to blacklist or white list to arm the vehicles. For details, see ***Vehicle Arming Control*** .
- Event Search: search history events of the checkpoints, including capture events and violation records. For details, see ***Event Search*** .
- Reports: Statistics of passing vehicle amounts and violation data. For details, see ***Report*** .
- Search Vehicle Driving Pattern: Search driving patterns in a specified period and then play back the driving pattern. For details, see ***Search Vehicle Driving Pattern*** .

17.2 Checkpoint Device Management

You can add devices related to checkpoints, including checkpoint devices, parking violation cameras, traffic cameras, and display screens to the system. After that, you can manage these devices and receive checkpoints events.

17.2.1 Add Parking Violation Camera

If you know the IP address of the parking violation camera, you can add it to the system for detecting parking violation.

Steps

1. Click ☰ on the Home page, and then go to **System Configuration → System Configuration →** **Devices → Vehicle Control → Checkpoint** .
2. Select the **Parking Violation Camera** tab.
3. Select an area where the device locates from the area list.
4. Click **Add** to enter the Add Parking Violation Camera page.
5. Set the device information, such as device name, IP address, and login account.

IP Address

Enter the IP address of the device.

Port No.

Enter the port No. of the device. The default value is ***8,000***.

Account

Enter the account name for logging in to the device. The default account name is ***admin***.

Login Password

Enter the device login password.

6. Finish adding the device.
   - Test and then Save (Recommended): Click **Online Test** to test the correctness of the entered device information, and then click **Save**.
   - Save Directly: Click **Save Directly**.
7. **Optional:** Select checkpoint device(s) from the device list, and then click **Synchronize** to synchronize device information from the system to devices, or vice versa.

Note

The operation is recommended if you have edited device information on the system or the device web page.

17.2.2 Add Checkpoint Device

If you know the IP address of a checkpoint device, you can add it to the platform by its IP address.

Before You Start

- You should have started the checkpoint device and connected it to a network so as to make sure the system and the device can communicate with each other.
- You should have set the time zone of the device to the same as that of the Network Time Protocol (NTP) server of the system, or vice versa.

Steps

1. Click on the Home page, and then go to **System Configuration → Devices → Vehicle Control → Checkpoint** .
2. Select **Checkpoint Device** tab.
3. Select the area where the checkpoint device locates from the area list on the left.
4. Click **Add**.
5. Set device parameters.

Device Name

Customize a name for the device to distinguish it from other devices.

Port No.

Enter the port No. of the device. The default value is ***8,000***.

Device Account

Enter the device user name. The default device user name is ***admin***.

Password

Enter the device password.

6. Finish adding the device.
   - Test and then Save (Recommended): Click **Online Test** to test the correctness of the entered device information, and then click **Save**.
   - Save Directly: Click **Save Directly**.
7. **Optional:** Select checkpoint device(s) from the device list, and then click **Synchronize** to synchronize device information from the system to devices, or vice versa.

Note

The operation is recommended if you have edited device information on the system or the device web page.

17.2.3 Add Checkpoint Traffic Camera to Area

You can add traffic cameras to specific areas and then relate it to a checkpoint. After that, you can do checkpoint applications such as setting speed measurement rules to determine if the passing vehicles overspeed.

Steps

1. Click on the Home page, and then go to **System Configuration → Devices → Vehicle Control → Checkpoint** .
2. Select the **Camera** tab.
3. Click **Add** to enter the Add Camera page.
4. Select an area from the area list.

   The available cameras in the selected area will be displayed.
5. Select camera(s) from the Available Camera list, and then click > to add the selected camera(s) to the Selected Cameras list.
6. Select camera(s) in the Selected Camera list.
7. Click **Save**.

17.2.4 Add Display Screen

If you know the IP address of a display screen, you can add it to system by its IP address for displaying vehicle overspeed information and other user-defined information.

Steps

1. Click on the Home page, and then go to **System Configuration → Devices → Vehicle Control → Checkpoint** .
2. Select the **Display Screen** tab.

3. Select an area where the display screen locates from the area list.
4. Click **Add**.
5. Set device information, such as device name and IP address.

   Board Card Model

   Select the board type.

   IP Address

   IP address of the device.

   Module Type

   Select the module type.

   Number of Modules

   The amount of modules used to form a screen.

   Note

   You can get the board card model, module type, and number of modules from the device label or user manual of the device.

6. Click **Online Test** to test if the device information you set is correct.
7. Click **Save Directly**.

17.3 Campus Checkpoint Configuration

In the Campus Checkpoint module, you can arm vehicles, search checkpoint events (capture events and violation records), view reports about passing vehicle amount and traffic violation data, as well as play back driving patterns of the passing vehicles. Before that, you should do the configurations including single-checkpoint speed measurement rule settings, segment speed measurement rule settings, and other settings such as violation records retention time.

17.3.1 Set Speed Measurement Rule for a Single Checkpoint

You can relate a camera to a checkpoint and then set a overspeed threshold for the checkpoint to make the camera capture the passing vehicles and calculate the instantaneous speed of each vehicle when it passing through the checkpoint. After that, the system will compare the calculated speed with the overspeed threshold to determine if the vehicle overspeeds.

Before You Start

You should have added checkpoint device(s), traffic camera(s), and display screen(s) to the system. For details about adding check point, traffic camera, and display screens, see ***Add Checkpoint Device*** , ***Add Checkpoint Traffic Camera to Area*** , and ***Add Display Screen*** respecitvely.

Steps

1. Click on the Home page, and then go to **System Configuration → Vehicle Control → Checkpoint → Camera Configuration** .

2. Set the required parameters, including camera name, linked channel, and overspeed threshold.

   Camera Name

   Create a name for the traffic camera.

   Linked Channel

   Select a channel and link it to the checkpoint for capturing the passing vehicles.

   Overspeed Threshold

   Set a speed (range: integer from 1 to 50, unit: km/h) as the threshold to determine if a vehicle overspeeds.

3. **Optional:** Set the optional parameters.

   Linked Display Screen

   Select a display screen and link it to the checkpoint for displaying the captured passing vehicles.

   Description

   Enter a remark about the speed measurement rule or the camera.

4. Click **Save**.

17.3.2 Set Speed Measurement Rule for Segment

When the speed measurement rule for a segment between two checkpoints is configured, the system will be able to calculate the time a vehicle spent to pass through the segment and therefore further calculate its average speed to pass through the segment. And By comparing the calculated average speed with the overspeed threshold you defined, the system will be able to determine if the vehicle overspeeds.

Before You Start

You should have added checkpoint device(s) and traffic camera(s) to the device. For details, see ***Add Checkpoint Device*** and ***Add Checkpoint Traffic Camera to Area*** to the system.

Steps

1. Click on the Home page, and then go to **System Configuration → Vehicle Control → Checkpoint → Segment Configuration** .
2. Click **Add** to enter the Add Segment page.
3. Set required parameters such as segment name, segment length, and linked camera.

   Segment Length

   Enter the length (unit: m) of the segment between two target checkpoints.

   Overspeed Threshold

   Set a speed (unit: km/h) as the threshold to determine if a vehicle overspeeds.

   Linked Camera

   Set the camera linked to the two checkpoints.

First Camera

The camera linked to the checkpoint considered as the start point of the segment.

Last Camera

The camera linked to the checkpoint considered as the end point of the segment.

4. **Optional:** Enter a description about the segment.
5. Click **Save**.

17.3.3 Set Rule for Auto Adding Vehicle to Blacklist

You can set the rule to define the upper limit of violation times for the vehicles within a certain time interval. If the violation times of a vehicle exceeds the upper limit, it will be automatically added to the blacklist.

Click on the Home page, and then go to **System Configuration → Vehicle Control → Checkpoint → Violation Configuration** to enter the Violation Configuration page, and then turn on **Violated Vehicle Management Rule** and configure the following parameters.

Allowed Violation Times

Set an upper limit for the violation times of the vehicles to keep the them staying out of the blacklist. The violation includes parking violation, wrong-way driving, overspeed, etc.

Note

You should have set violation detection for the traffic camera. For details, see the user manual of the device.

Period Interval

Set a time interval for clearing the violation times of a vehicle.

Example

Assume that you set 4 times as the **Allowed Violation Times**, and 1 month as the **Period Interval**, if vehicle A violates traffic rules and parking rules for 4 times in the month, it will be added to the blacklist, while vehicle B only violates for 2 times in the month, it will not be added to the blacklist and its violation times will be cleared at the end of the month.

17.3.4 Set Checkpoint Parameters

You can set checkpoint parameters including capture record retention duration, violation record retention duration, and default storage pool of the pictures captured by traffic cameras of checkpoints.

To configure the capture record retention duration and violation record retention duration, click on the Home page, and then go to **System Configuration → Vehicle Control → Checkpoint → Parameter Configuration** .

Capture Record Retention Duration

Set the retention duration (6 to 36 months) for the capture events. You can search for a capture event before its retention duration ends.

Note

For details about searching capture events, see ***Search Capture Event*** .

Violation Record Retention Duration

Set the retention duration (6 to 36 months) for the violation events. You can search for a violation event before its retention duration ends.

Note

For details about searching violation events, see ***Search Violation Event*** .

To configure default storage pool for the captured pictures, click on the Home page, and then go to **System Configuration → Advanced Parameter Configuration → Picture Storage Configuration** to enter the Picture Storage Configuration page.

On the page, you can select a default storage pool or customize a storage pool for the captured pictures.

Default Storage Pool - Data Overwritten

Old data in the pool will be overwritten by new data if the pool is full. This type of pool is suitable for storing pictures which only needs to be kept temporarily, such as event-related pictures and captured pictures.

Default Storage Pool - Data not Overwritten

The data in the pool will not the overwritten. This type of pool is suitable for storing pictures which should be kept permanently, such as storing person's profile picture.

Custom Configuration

You can click **Add Storage Pool** and then set the following parameters to create a storage pool for a specific type of devices.

Storage Pool Name

Create a name for the pool.

Overwritten Strategy

Select a overwritten strategy to define how the data in the pool will be overwritten.

Overwritten

The old data in the pool will be overwritten by new data if the pool is full.

Not Overwritten

The data in the pool will not overwritten.

All

All the data in the pool will be overwritten if the pool is full.

17.4 Checkpoint Application

Based on event management and speed measurement of passing vehicles at checkpoints, the checkpoint application provides functionality including vehicle arming control, event search, reports, and playback of vehicle driving pattern.

17.4.1 Vehicle Arming Control

You can arm specific vehicles by adding them to the whitelist or blacklist. After that, if these vehicles passing through checkpoints, certain linkage mechanism will be triggered. For example, if a vehicle is added to the blacklist, an event will be triggered to notify security personnel when it passing through a checkpoint.

Add Vehicle to Blacklist

You can add a vehicle which requires higher-level of monitoring effort (e.g., the stolen vehicle and the robbed vehicle) to blacklist. After that, blacklist events (the detection of vehicle in blacklist) will be triggered to notify the security personnel when the vehicle passes through the checkpoints.

Steps

1. Click **Checkpoint** in the Vehicle Control section of the Home page, and then go to **Vehicle Arming → Blacklist** .
2. Click **Add** to enter the Add Vehicle in Blacklist page.
3. Select the license plate number.
4. **Optional:** Set information such as license plate number, end time, and arming reason.

   End Time

   Specify a date and the precise time point when the vehicle will be automatically removed from the blacklist.

   Arming Reason

   Select a reason why you add the vehicle to the blacklist.
5. Click **Save**.

   The newly added vehicle will appear in the blacklist.
6. **Optional:** Perform the following operations.

Edit Vehicle in Blacklist	Click in the Operation column to edit the license plate number, vehicle owner name, mobile phone number, etc.
Remove Vehicle from Blacklist	Click in the Operation column to remove the vehicle from the whitelist.

Note

If removed from the whitelist, the vehicle will be monitored by the checkpoints. In other words, violation events will be recorded and alarms will be triggered if it overspeeds or commit other traffic violations.

Search Vehicles in Blacklist Enter the license plate number of a vehicle in the search box to search if the vehicle lists in the whitelist.

Add Vehicle to Whitelist

If a vehicle is added to the whitelist, the vehicle will be exempted from the monitoring of the checkpoints. In other words, no violation events will be recorded and no alarms will be triggered even if the vehicle overspeeds or commit other traffic violations.

Steps

1. Click **Checkpoint** in the Vehicle Control section of the Home page, and then go to **Vehicle Arming → Whitelist** .
2. Click **Add** to enter the Add Vehicle in Whitelist page.
3. Select the license plate number.
4. **Optional:** Set other information including vehicle owner name, mobile phone number, and description about the settings.
5. Click **Save**.

   The newly-added vehicle will appear in the whitelist.
6. **Optional:** Perform the following operations after adding the vehicle to whitelist.

Edit Vehicle in Whitelist Click in the Operation column to edit the license plate number, vehicle owner name, mobile phone number, etc.

Remove Vehicle from Whitelist Click in the Operation column to remove the vehicle from the whitelist.

Note

If removed from the whitelist, the vehicle will be monitored by the checkpoints. In other words, violation events will be recorded and alarms will be triggered if it overspeeds or commit other traffic violations.

Search Vehicles in Whitelist Enter the license plate number of a vehicle in the search box to search if the vehicle lists in the whitelist.

17.4.2 View Real-Time Passing Vehicle

On the Control Client of HikCentral Enterprise-Commercial, you can view the real-time passing vehicle information detected by the checkpoints.

Click **Checkpoint** on the control panel of the Control Client.

All the detected vehicle information will display.

Click the record to view the detailed vehicle information, such as captured picture, passing time, driving speed, recorded video footage, etc.

Click to lock the current list. The records displayed will not be replaced by the latest records.

17.4.3 Event Search

You can search two types events related to campus checkpoints, i.e., violation events and capture events by customizing search conditions. You can also export events and event-related pictures to the local PC.

Search Capture Event

Capture events refers to the events related to the picture capturing of the traffic camera on each checkpoint. You can search capture events by search conditions such as license plate No., event source, vehicle speed, etc.

Before You Start

You should have added checkpoint devices, set speed measurement rules, and set checkpoint parameters. For details, see ***Checkpoint Device Management*** , ***Set Speed Measurement Rule for a Single Checkpoint*** , ***Set Speed Measurement Rule for Segment*** , and ***Set Checkpoint Parameters*** for details.

Steps

1. Click **Checkpoint** in the Vehicle Control section on the Home page, and then go to **Event Search → Violation Search** .
2. Set search conditions.

   Vehicle Speed

   Specify a speed range for searching capture events.
3. Click **Search**.

   The matched capture events will appear in the event list.
4. **Optional:** Perform the following operations after search if required.

Export Matched Event and Related Picture	Click **Export**, and then check **Include Picture** to export the matched events and pictures.

Switch View Mode	Click / to switch the view mode between the list mode and thumbnail mode.
View Vehicle Picture	Click in the event list to view the picture of the vehicle in the current row.
View Driving Pattern	Click in the event list to view the driving pattern of the vehicle in the current row.

Search Violation Event

The violation events include overspeed events, wrong-way driving (driving against the direction of traffic) events, and blacklist events (the detection of vehicles in blacklist). You can search the violation events by search conditions such as license plate No., violation type, and event source.

Before You Start

You should have added checkpoint devices, set speed measurement rules, and set checkpoint parameters. For details, see ***Checkpoint Device Management*** , ***Set Speed Measurement Rule for a Single Checkpoint*** , ***Set Speed Measurement Rule for Segment*** , and ***Set Checkpoint Parameters*** for details.

Steps

1. Click **Checkpoint** in the Vehicle Control section on the Home page, and then go to **Event Search → Violation Search** .
2. Set search conditions, including license plate number, violation type, event source, speed detection type, start time, end time, and arming reason.

   Speed Detection Type

   Select the speed measurement rule which determines if the vehicles overspeed.

   Camera Speed Detection

   The instantaneous speeds of the passing vehicles calculated by the speed measurement rule for a single checkpoint.

   Segment Speed Detection

   The average speeds of the passing vehicles calculated by the speed measurement rule for segment.

   Arming Reason

   Select the reason why the vehicles are added to the blacklist.

   For example, select **Stolen vehicle** if you want to search for events related to the detection of stolen vehicles which are added to the blacklist.
3. Click **Search**.

   Matched events will appear on event list.
4. **Optional:** Perform the following operations after search if required.

Export Matched Event and Related Picture	Click **Export**, and then check **Include Picture** to export the matched events and pictures.
Switch View Mode	Click / to switch the view mode between the list mode and thumbnail mode.
View Vehicle Picture	Click in the event list to view the picture of the vehicle in the current row.
View Driving Pattern	Click in the event list to view the driving pattern of the vehicle in the current row.
View Event-related Video	Click in the event list to view the video footage of the event. **Note** To ensure the normal playing of the video footage, you should have download the required plug-in from the download center (displayed as on the Home page) and installed it.

17.4.4 Report

You can generate traffic flow report or violation report to view the traffic flow or traffic violation events of specific checkpoints within certain time period. You can also export the reports to the local PC if required.

Click **Campus Checkpoint** on the Home page, and then click **Statistics & Reports** to enter the Statistic page.

Traffic Flow Report

The traffic flow report will be generated after you specify the time period and checkpoint(s) for statistics.
The report shows the number of vehicles passed through the selected checkpoint(s) each time unit (hour, day, etc.) within the selected time period.
You can click **Export** to export the report to local PC.

Violation Report

The violation report will be generate after you specify the time period and checkpoint(s) for statistics.
The generated report is divided into two parts, i.e., the data panel and the data list. The data panel shows the total event number and the number of each type of event from all the selected checkpoint(s); The data list shows total event number and the number of each type of event from each selected checkpoint.

17.4.5 Search Vehicle Driving Pattern

You can search the driving pattern by setting the search conditions including license plate number, camera(s), and time period, and the matched driving pattern will be displayed as line segment(s) on map. The driving patterns, which can be played back to roughly simulate the driving directions and driving routes of a vehicle, are helpful in scenarios such as tracing escaped criminal and criminal case investigation.

Before You Start
You should have added checkpoint device(s) to the map.

Steps
1. Click **Campus Checkpoint** in the Vehicle Control section of the Home page, and then select **Pattern Information** to enter the Driving Pattern Information page.
2. Enter the license plate number of the target vehicle.
3. Select the area where the checkpoint(s) locate.
4. Set a time period for search.

   The matched driving pattern will appear.

Chapter 18 Intrusion Alarm

The system supports adding security control panels to detect people, vehicles, etc., entering a pre-defined region and triggers events/alarms. The system can then receive alarm information and the corresponding security personnel will take the appropriate action.

18.1 Flow Chart

For the first time, you can perform configurations and applications of intrusion alarm according to the chart below.

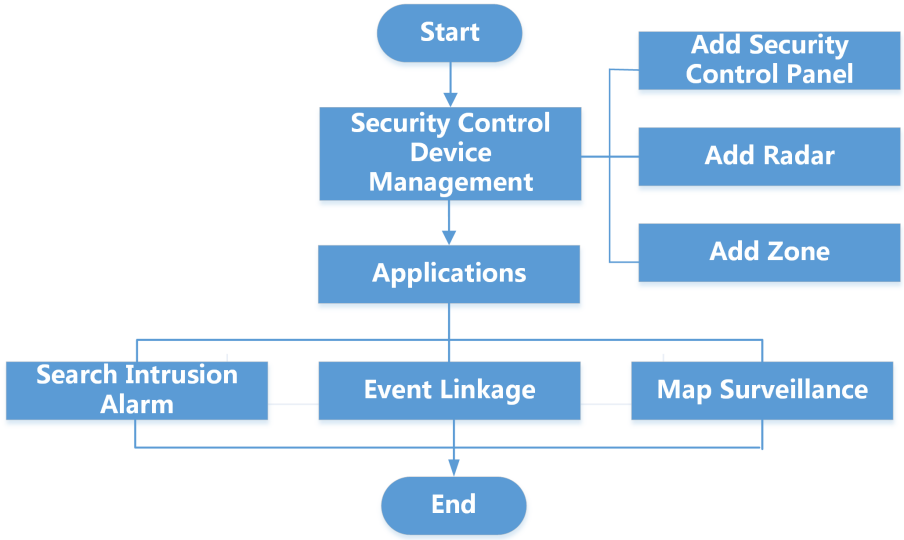


Figure 18-1 Flow Chart of Intrusion Alarm

- **Add Security Control Device**: You can add security control devices to the system. For details, refer to ***Security Control Device Management*** .
- **Event Linkage**: You can configure linkage actions for the security control events. When an event is detected, the system will receive the real-time information of the event and trigger linkage actions. For details, refer to ***Event Configuration*** .
- **Map Surveillance**: You can add security control resources to the map. When the alarm is triggered, you can view the live view and playback of the added resources on the map, and get a notification message from the map. For details, refer to ***Map*** .
- **Search Intrusion Alarm**: You can set search conditions to search the corresponding intrusion alarm event(s) as required. For details, refer to ***Search Intrusion Alarm*** .

18.2 Security Control Device Management

You can add and manage security control devices including security control panel and security radar in the system.

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 security radar is 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.

18.2.1 Add Security Control Panel

When you know the IP address of the security control panel to add, you can add device to the system by specifying the IP address, user name, password, and other related parameters.

Steps

1. On the Home Page, click → **System Configuration** → **Devices** → **Alarm Detection** → **Intrusion Alarm** .
2. Select the area in the Area List.
3. Click **Security Control Panel** tab.
4. Click **Add** to enter Add Security Control Panel Page.
5. Configure device parameters.

Access Protocol

Hikvision Device Network SDK Protocol

Security control panels using this protocol are produced by Hikvision with fixed IP address.

MTA Protocol

A protocol to fulfill the device requirements for public network penetration; supports connection of third-party security control panel and Hikvision network security control panel.

IP Address

Enter the IP address of the security control panel.

Port No.

Enter the device port No. The default value is 8000.

User Name

Enter the user name of the security control panel. By default, the user name is admin.

Password

Enter the password of the security control panel.

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.

Domain

Select the network domain that the access control device belongs to from the drop-down list.

Description

Enter the description related with the device (optional).

6. **Optional:** Click **Online Test** to check whether the device information is correct.

   The test result will show. If failed, you should check and edit the user name or password for the security control panel, and start online detection again.
7. Click **Save** to add the security control panel.
8. **Optional:** After adding device, you can perform the following operations according to your needs.

Search Device	Check **Include Sub-Area** to filter the devices. Set search conditions, and click **Search** to search the security control panel as required.
Edit Parameters	Click to edit parameters for the security control panel, including device name, port No., etc.
Delete Device	Click to delete the security control panel. You can also select multiple devices and click **Delete** to delete devices in a batch.
View Device Details	Click to view the details of the selected security control panel, including access information such as device IP and serial No., and channel information such as partition, linked zone, alarm device, etc. And you can edit the partition name, zone name, etc.
Move Device	Click **Move** to move the selected device to another area.

18.2.2 Add Security Radar

When you know the IP address of the security radar to add, you can add device to the system by specifying the IP address, user name, password, and other related parameters.

Steps

1. On the Home Page, click → **System Configuration** → **Devices** → **Alarm Detection** → **Intrusion Alarm** .
2. Select the area in the Area List.
3. Click **Security Radar**.
4. Click **Add** to enter Add Security Radar Page.
5. Configure device parameters.

   Access Protocol

   Select **Hikvision Device Network SDK Protocol** as the access protocol.

   IP Address

   Enter the IP address of the security radar.

   Port No.

   Enter the device port No. The default value is 80.

   User Name

   Enter the user name of the security radar. By default, the user name is admin.

   Password

   Enter the password of the security radar.

   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.

   Domain

   Select the network domain that the security radar belongs to from the drop-down list.

   Description

   Enter the description related with the device (optional).

6. **Optional:** Click **Online Test** to check whether the device information is correct.

   The test result will show. If failed, you should check and edit the user name or password for the security radar, and start online detection again.

7. Click **Save** to add the security radar.
8. **Optional:** After adding device, you can perform the following operations according to your needs.

   Search Device Check **Sub-Area** to filter the devices.

	Set search conditions, and click **Search** to search the security radar as required.
Edit Parameters	Click to edit parameters for the security radar, including device name, port No., etc.
Delete Device	Click to delete the security radar. You can also select multiple devices and click **Delete** to delete devices in a batch.
View Device Details	Click to view the details of the selected security radar, including access information such as device IP and serial No., and channel information such as partition, linked zone, alarm device, etc. And you can edit the partition name, zone name, etc.
Move Device	Click **Move** to move the selected device to another area.

18.2.3 Add Zone to Area

After adding the security control panel to the system, you need to add zones (channels of the security control device) to the area for management.

Steps

1. On the Home Page, click → **System Configuration** → **Devices** → **Alarm Detection** → **Intrusion Alarm** .
2. Select an area in the Area list, and click **Zone** tab.
3. Click **Add** to enter the Add Zone page.
4. Select the area in the Area list.

   All the available zones in the area will be listed in the Available Zone list.
5. In the Available Zone list, check zone(s) to be added to the area.

   Note

   The system supports fuzzy search by zone name to search the target zone(s).
6. Click to add the selected zone(s).

   Note

   You can click to remove the added zone(s) from the Selected Zone list.
7. Click **Save**.
8. **Optional:** Perform the following operation(s) after adding the zone to area.

Search Zone	Check **Include Sub-Area** to filter the zones. Set search conditions, and click **Search** to search the zone(s) as required.
Edit Zone	Select a zone, and click to edit the zone name and its description.
Move Zone	Select a zone, and click **Move** to move the zone to another area.

Delete Zone	Select a zone, and click to delete the zone. You can also select multiple zones, and click **Delete** to delete zones in a batch.

18.2.4 Add Alarm Output to Area

After adding the security control panel to the system, you need to add alarm outputs (channels of the security control device) to the area 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.

Steps

1. On the Home Page, click → **System Configuration** → **Devices** → **Alarm Detection** → **Intrusion Alarm** .
2. Select an area in the Area list, and click **Alarm Output** tab.
3. Click **Add** to enter Add Alarm Output page.
4. Select the area in the Area list.

   All the available alarm outputs in the area will be listed in the Available Output list.
5. In the Available Alarm Output list, check the alarm output(s) to be added to the area.

   Note

   The system supports fuzzy search of the target alarm output(s).
6. Click to add the selected alarm output(s).

   Note

   You can click to remove the added alarm output(s) from the Selected Alarm Output list.
7. Click **Save**.
8. **Optional:** Perform the following operation(s) after adding the alarm output to area.

Search Alarm Output	Check **Include Sub-Area** to filter the alarm outputs. Set search conditions, and click **Search** to search the alarm output(s) as required.
Edit Alarm Output	Select an alarm output, and click to edit the name of the alarm output, output duration and description.
Move Alarm Output	Select an alarm output, and click **Move** to move the alarm output to another area.
Delete Alarm Output	Select an alarm output, and click to delete the alarm output. You can also select multiple alarm outputs, and click **Delete** to delete alarm outputs in a batch.

18.3 Search Intrusion Alarm

The system supports setting search conditions to search the corresponding intrusion alarm event(s) as required. You can view the event details including event start time, area, event source, and event type. You can also export the excel file to the local PC to view the event details.

Before You Start
Make sure you have added panic alarm device(s) to the system. For details, refer to ***Add Panic Alarm Device*** .

Steps
1. Click **Intrusion Alarm** on the Home Page to enter Intrusion Alarm Module.
2. Set the search conditions, including start and end time, event source and event type.
3. Click **Search**.

   You can view the intrusion alarm events that meets the search conditions.
4. **Optional:** Click **Export** to save the searched alarm events to the local PC in CVS format.

18.4 Control Partition

You can control the partitions of the security control panels on the Control Client of HikCentral Enterprise-Commercial. You can arm or disarm the partitions of the security control devices via the Control Client. After arming the partitions, the current Control Client can receive the triggered alarms in the partitions.

Steps

Note
- If the zone of the partition is exceptional, the partition cannot be armed. You need to bypass the zone first.
- The disarming and arming control only controls the alarm receiving on the current Control Client.

1. Click **Intrusion Alarm** on the control panel of the Control Client.
2. Select an area on the left and click **Partition** tab.

   All the partitions added in the area will be displayed.
3. Select one partition and perform the following operations to control the partition.

   Arm

   Click **Arm** to arm the partition and the Control Client can receive the detected alarm information in the zones of this partition.

   Disarm

   Click **Disarm** to disarm the partition and even the zones in this partition trigger alarms, the Control Client will not receive these alarms.

Clear Alarm

Click **Clear Alarm** to clear the generated alarms in the security control partition received by the Control Client.

18.5 Control Zone

You can bypass the zones on the Control Client of HikCentral Enterprise-Commercial.

Steps

1. Click **Intrusion Alarm** on the control panel of the Control Client.
2. Select an area on the left and click **Zone** tab.

   All the zones added in the area will be displayed.
3. Select one zone and perform the following operations to control the zone.

   Bypass

   When some exception occurs for the 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 which the zone belongs to.

   Click **Bypass** to bypass the selected zone.

   Bypass Recovery

   Click **Bypass Recovery** to recover the zone that is bypassed to make it work normally.

Chapter 19 Panic Alarm

The system supports managing panic alarm devices, including pole alarm station, panic alarm station, and box panic alarm station. They are mainly installed in the areas with the crowd or high incidence of cases, such as school, square, tourist attraction, hospital, supermarket gate, market, parking lot, etc. In case of emergency, people can push the button on the panic alarm devices to send alarm to the monitoring center, and the operator in the center will take the appropriate action. The panic alarm devices help to realize alarm aid in emergency.

19.1 Flow Chart

For the first time, you can perform configurations and applications of panic alarm according to the chart below.

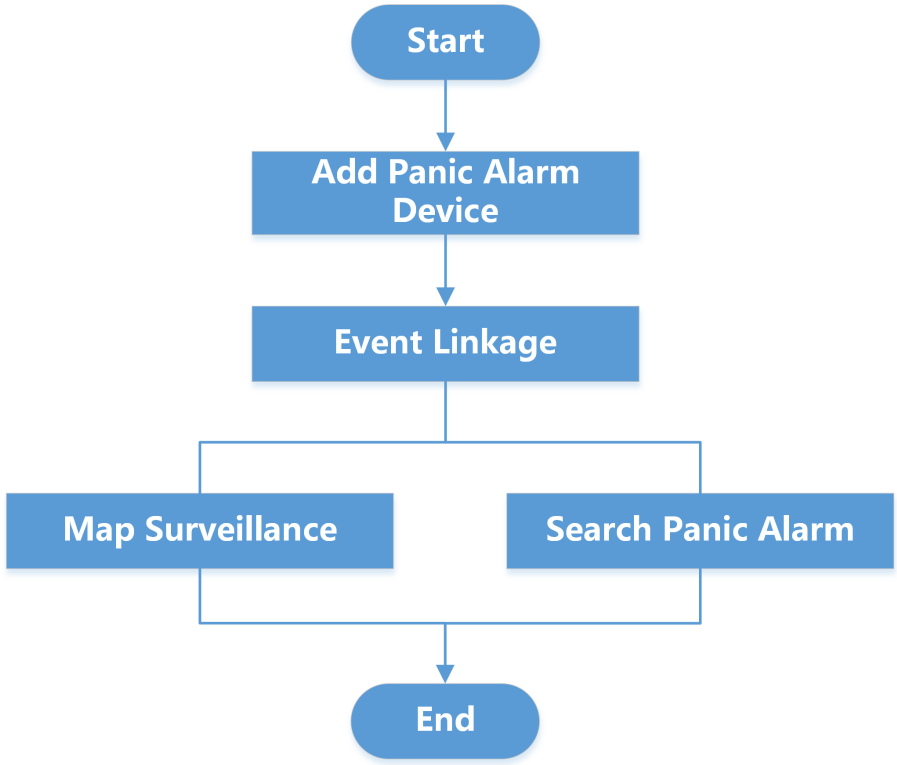


Figure 19-1 Flow Chart of Panic Alarm

- **Add Panic Alarm Device**: You can add panic alarm devices to the system by IP address. For details, see ***Add Panic Alarm Device*** .
- **Event Linkage**: You can configure linkage actions for panic alarm events. When an event is detected, the system will receive the real-time information of the event and trigger linkage actions. For details, refer to ***Event Configuration*** .

- **Map Surveillance**: You can add panic alarm resources to the map. When the alarm is triggered, you can view the live view and playback of the added resources on the map, and get a notification message from the map. For details, refer to ***Map*** .
- **Search Panic Alarm**: You can set search conditions to search the corresponding panic alarm event(s) as required. For details, refer to ***Search Panic Alarm*** .

19.2 Add Panic Alarm Device

When you know the IP address of the panic alarm device to add, you can add device to the system by specifying the IP address, user name, password, and other related parameters. Also, you can add multiple panic alarm devices with the same port No., user name and password in a batch by specifying the IP segment.

Steps

1. On the Home Page, click → **System Configuration** → **Devices** → **Alarm Detection** → **Panic Alarm** .
2. Select the area in the Area List.
3. Click **Add**.
4. Select device type according to your actual needs. The system supports the following three types: pole panic alarm station, panic alarm station, box panic alarm station.
5. Select **Hikvision Device Network SDK Protocol** as the access protocol from the drop-down list.
6. Select adding method.

   Single

   Enter the IP address of the device to add the single device.

   Segment

   If multiple devices are in the same IP segment, and they have the same port No., user name and password, you can enter the start IP address and end IP address to add these devices simultaneously.
7. Configure device parameters.

   Port No.

   Enter the port No. of panic alarm device. The default port No. is 8000.

   User Name

   Enter the user name of the panic alarm device. By default, the user name is admin.

   Password

   Enter the password of the panic alarm device.

   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.

Domain

Select the network domain that the panic alarm device belongs to from the drop-down list.

Description

Enter the description related with the device (optional).

8. **Optional:** Click **Online Test** to check whether the device information is correct.

   The test result will show. If failed, you should check and edit the user name or password for the panic alarm device, and start online detection again.
9. Click **Save** to add the panic alarm device.
10. **Optional:** After adding device, you can perform the following operations according to your needs.

Search Device	Check **Include Sub-Area** to filter the devices. Set search conditions, and click **Search** to search the panic alarm device(s) as required.
Edit Parameters	Click to edit device parameters, including device name, port number, etc.
Delete Device	Click to delete the panic alarm device. You can also select multiple devices and click **Delete** to delete devices in a batch.

19.3 Search Panic Alarm

The system supports setting search conditions to search the corresponding panic alarm event(s) as required. You can view the event details including event start time, area, event source, and event type. You can also export the excel file to the local PC to view the event details.

Before You Start

Make sure you have added panic alarm device(s) to the system. For details, refer to ***Add Panic Alarm Device*** .

Steps

1. Click **Panic Alarm** on the Home Page to enter Panic Alarm Module.
2. Set the search conditions, including start and end time, event source and event type.
3. Click **Search**.

   You can view the panic alarm events that meets the search conditions.
4. **Optional:** Click **Export** to save the searched panic alarm events to the local PC.

Chapter 20 Facial Surveillance

The facial recognition device can analyze the captured face pictures and compare with the faces in the face libraries or face groups. When detecting a matched or mismatched face, it will upload an event to the system and notify the security personnel. The security personnel can view the real-time face comparison events and monitor the key persons, frequently appeared persons, and strangers.

20.1 Flow Chart

You can perform configurations and applications of facial recognition according to the chart below.

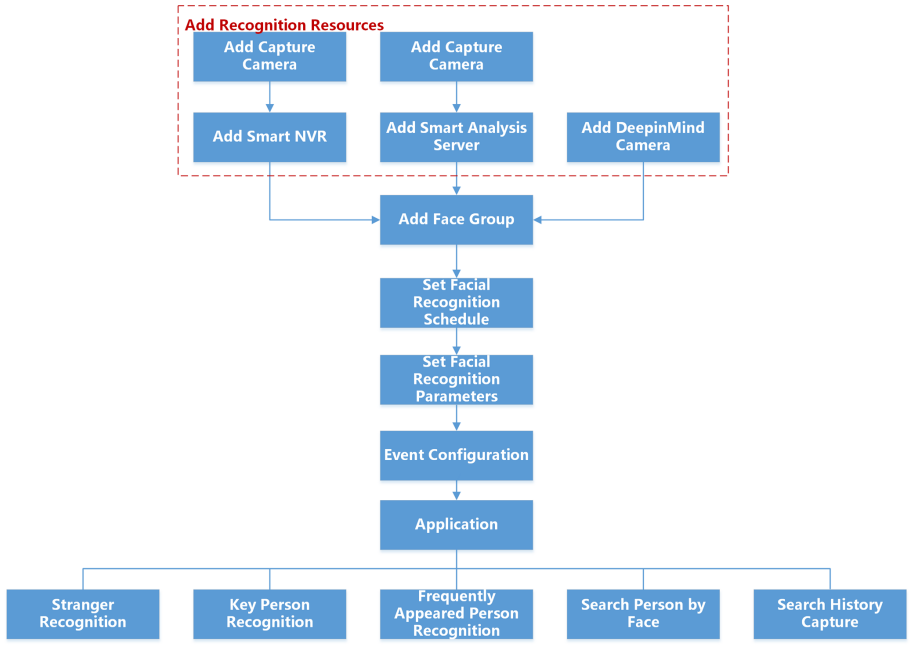


Figure 20-1 Flow Chart

20.2 Central Intelligence Device Management

After adding the central intelligence devices to the system, the system can receive the real-time face comparison records from the device and you can perform further operations such as arming the key persons and strangers.

20.2.1 Add Intelligent NVR by HIKVISION SDK Protocol

Intelligent NVR is embedded with deep learning algorithm and supports network connection, storage, management, control, and smart analysis. It provides functions including facial recognition, human body recognition, and vehicle recognition. You can add an Intelligent NVR to the system by its IP address.

Steps

1. Click → **System Configuration** → **Devices** → **Central Intelligence** to enter the Facial Recognition Device Management page.
2. Select an area in the area list to add the device.
3. Click **Intelligent NVR** tab.
4. Click **Add**.
5. Select **Hikvision Device Network SDK Protocol** as the access protocol from the drop-down list.
6. Select the adding mode.
   - **Single:** Add one Intelligent NVR to the system by entering the IP address of the device.
   - **Segment:** If the Intelligent NVRs have the same port No., user name and password, and their IP addresses are within the IP segment, you can specify the start IP address and the end IP address to add them.
7. Set the parameters for the Intelligent NVRs, including port No., user name, password, network, and description.

   Port No.

   The port number of the device. When adding multiple devices by IP segment, the devices to be added should have the same port number.

   User Name

   Enter the user name of the devices. By default, the user name is admin.

   Password

   The password of 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.

   Domain

   Select the network domain that the devices belong to from the drop-down list.

Note

For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

8. Click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the device and click **Online Test** to start online test again.

9. Click **Save** to add the Intelligent NVR.
10. **Optional:** Perform the following operation(s) after adding the device.

Search Device	Check **Devices Never Connected** or **Include Sub-Area** to filter the devices, or enter specific search conditions to filter them. **Note** Devices Never Connected indicates the devices which have never been connected to HikCentral Enterprise-Commercial since they are added to the system. This condition is used to filter devices with user name or password exception.
Edit Device	Click to edit the device information, including device name, IP address, port, user name, password, etc.
Delete Device	Click to delete the device. You can also select multiple devices and click **Delete** to delete devices in a batch. **Note** If you delete a Intelligent NVR, all the channels of the NVR will be deleted as well, including the settings of these channels such as recording and capture schedule, alarm linkage, etc. As a result, you may lose videos, pictures, and alarms related to the device.
View Device Details	Click to view the detailed information of the device, such as device IP address, password strength, linked cameras, etc.
Get Device Information	Select one or more devices and click **Sync** to get device information (such as device name, device serial No., etc.) from the device(s) to the system.

20.2.2 Add Intelligent NVR by ISUP 5.0 Protocol

Intelligent NVR is embedded with deep learning algorithm and supports network connection, storage, management, control, and smart analysis. It provides functions including facial recognition, human body recognition, and vehicle recognition. If the NVR supports ISUP 5.0

protocol, you can register the NVR to the system no matter the NVR has fixed IP address or dynamic IP addresses.

Before You Start

Register the NVR to the HikCentral Enterprise-Commercial by entering the system information on the NVR configuration page. For details, refer to the user manual of the NVR.

Steps

1. Click → **System Configuration** → **Devices** → **Central Intelligence** to enter the Facial Recognition Device Management page.
2. Select an area in the area list to add the device.
3. Click **Intelligent NVR** tab.
4. Click **Add**.
5. Select **Hikvision ISUP 5.0 Protocol** as the access protocol from the drop-down list.
6. Set the parameters for the Intelligent NVR.

   Device No.

   The device No. which you can find on the device configuration page.

   Device Verification Code

   Used for identity verification when the device connects to the system.

   Domain

   Select the network domain that the devices belong to from the drop-down list.

   Note

   For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.

7. Click **Save** to add the Intelligent NVR.
8. **Optional:** Perform the following operation(s) after adding the device.

Search Device	Check **Devices Never Connected** or **Include Sub-Area** to filter the devices, or enter specific search conditions to filter them. **Note** Devices Never Connected indicates the devices which have never been connected to HikCentral Enterprise-Commercial since they are added to the system. This condition is used to filter devices with user name or password exception.
Edit Device	Click to edit the device information, including device name, device No., etc.
Delete Device	Click to delete the device. You can also select multiple devices and click **Delete** to delete devices in a batch.

Note

If you delete a Intelligent NVR, all the channels of the NVR will be deleted as well, including the settings of these channels such as recording and capture schedule, alarm linkage, etc. As a result, you may lose videos, pictures, and alarms related to the device.

View Device Details	Click to view the detailed information of the device, such as device No.
Get Device Information	Select one or more devices and click **Sync** to get device information (such as device name, device serial No., etc.) from the device(s) to the system.

20.2.3 Add Facial Recognition Server (Pure Analysis)

The facial recognition server provides facial recognition, analysis, and comparison for the detected faces. The pure analysis facial recognition server is mainly applicable in entrance and exit, checkpoint, etc., for facial recognition. Meanwhile, the pure analysis facial recognition server provides big data analysis and cloud storage service for further operation.

Steps

1. Click → **System Configuration** → **Devices** → **Central Intelligence** to enter the Facial Recognition Device Management page.
2. Select an area in the area list to add the device.
3. Click **Smart Analysis Server** tab.
4. Click **Add**.
5. In the device type, select **Pure Face Picture Analysis Server** .
6. Set the parameters for the facial recognition server.

Cloud Analysis IP Address

The IP address of the cloud analysis module of the facial recognition server.

Cloud Analysis Port

The port number of the cloud analysis module of the facial recognition server. By default, it is 80.

Cloud Analysis User Name

The user name to log into the cloud analysis module of the facial recognition server. By default, it is admin.

Cloud Analysis Password

The password to log into the above account of the cloud analysis module.

Big Data IP Address

The IP address of the big data service of the facial recognition server.

Big Data Port

The port number of the big data service of the facial recognition server. By default, it is 8000.

Cloud Storage IP Address

The IP address of the cloud storage service of the facial recognition server.

Picture Uploading Port

The port used for uploading port. By default, it is 6011.

Picture Downloading Port

The port used for downloading port. By default, it is 6120.

Picture Storage Pool ID of Cloud Storage

The unique identification of the picture storage pool for cloud storage. You can get it from the resource pool configuration page of the cloud storage service.

Access Key of Cloud Storage

The key for downloading pictures from cloud analysis service and big data service. You can get it from the secret key management page of the cloud storage service.

Encryption Key of Cloud Storage

The key for downloading pictures from cloud analysis and big data service. You can get it from the secret key management page of the cloud storage service.

7. Click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the device and click **Online Test** to start online test again.
8. Click **Save** to add the device.
9. **Optional:** Perform the following operation(s) after adding the device.

Search Device	Enter specific search conditions to filter them.
Edit Device	Click to edit the device information, including device name, IP address, port, user name, password, etc.
Delete Device	Click to delete the device. You can also select multiple devices and click **Delete** to delete devices in a batch.

20.2.4 Add Facial Recognition Server (Stand-alone/Edge)

The facial recognition server provides facial recognition, analysis, and comparison for the detected faces. The stand-alone facial recognition server is mainly applicable in small-sized projects such as machine room, security room, security guard booth, etc.

Steps

1. Click → **System Configuration** → **Devices** → **Central Intelligence** to enter the Facial Recognition Device Management page.
2. Select an area in the area list to add the device.
3. Click **Smart Analysis Server** tab.

4. Click **Add**.
5. In the device type, select **Stand-alone/Edge Face Picture Analysis Server**.
6. Set the parameters for the facial recognition server, including custom device name, IP address, port, user name and password.
7. Click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the device and click **Online Test** to start online test again.
8. Click **Save** to add the device.
9. **Optional:** Perform the following operation(s) after adding the device.

Search Device	Enter specific search conditions to filter them.
Edit Device	Click to edit the device information, including device name, IP address, port, user name, password, etc.
Delete Device	Click to delete the device. You can also select multiple devices and click **Delete** to delete devices in a batch.

20.2.5 Add Intelligent Fusion Server

The intelligent fusion server provides facial recognition, analysis, and comparison for the detected faces. It is mainly applicable for middle and small-sized projects for facial comparison.

Steps

1. Click → **System Configuration** → **Devices** → **Central Intelligence** to enter the Facial Recognition Device Management page.
2. Select an area in the area list to add the device.
3. Click **Smart Analysis Server** tab.
4. Click **Add**.
5. In the device type, select **Intelligent Fusion Server**.
6. Set the parameters for the intelligent fusion server, including custom device name, IP address, port, user name and password.
7. Click **Online Test** to check whether the device information is correct.

   The test result will show. If test failed, you should check and edit the user name or password for the device and click **Online Test** to start online test again.
8. Click **Save** to add the device.
9. **Optional:** Perform the following operation(s) after adding the device.

Search Device	Enter specific search conditions to filter them.
Edit Device	Click to edit the device information, including device name, IP address, port, user name, password, etc.
Delete Device	Click to delete the device. You can also select multiple devices and click **Delete** to delete devices in a batch.

20.3 Face Group Management

Face group is a group of face pictures which are used for face comparison. The faces captured by the capture cameras will be compared with the faces in the face group. When the similarity between the captured face and the face in the face group is higher or lower than the threshold, an event will be triggered to notify the security personnel that a person who matched or mismatched with the faces in the face group is detected.

After adding a face group, you can add faces to the group one by one or in a batch, or you can synchronize the faces in the person list into the group.

20.3.1 Add Face Group

You can create several groups to manage the persons according to actual needs. For example, you can add a group named "VIP" and add the face pictures of VIPs into this group.

Steps

Note

Up to 16 face groups can be added.

1. Click → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Face Group** to enter the Face Group Configuration page.
2. Click **+** on the upper-left corner.
3. Enter a name for the group.

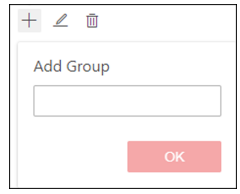


Figure 20-2 Add Face Group

4. Click **OK**.
5. **Optional:** Perform following operations after adding the face group.

Edit Group Name	Select the face group and click to edit the group name if necessary.
Delete Group	Select the face group and click to delete the group if necessary. **Note** After deleting the face group, the faces in the group will be deleted as well.

20.3.2 Add Face to Face Group

After adding a face group, you need to add face pictures into the group. You can add faces one by one.

Before You Start
Set the storage location for the face pictures in the **System Configuration → Advanced Parameters → Picture Storage** .

Steps
1. Click ☰ → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Face Group** to enter the Face Group Configuration page.
2. Select a face group and click **Add**.
3. Click **Upload** and select a face picture from your local PC.

Note
- Please upload a photo with front face.
- The face picture should be in JPG, JPEG, BMP, or PNG format.
- The size of face picture should be between 10 KB and 200 KB, and the resolution should be 480×640 and above.

4. Enter the person's information such as name, gender, and ID.
5. Click **Save**.
6. **Optional:** Perform the following operations if necessary.

Search Face	You can search the faces by person name, gender, or ID.
Copy Faces to Other Group	You can copy certain faces in one group to other groups. Select one or more faces, click **Copy to ...**, and select the target group.
View Face Details	Click • • • → in the lower-right corner of the face picture, or click in the Operation column to view the face details, including person name, gender, ID, and face picture.
Delete Face	Select the face pictures and click **Delete** to delete them from the face group.

20.3.3 Batch Import Faces into Face Group

You can also add multiple faces into one face group by importing a pre-defined ZIP file which contains multiple face photos to the system.

Before You Start
Set the storage location for the face pictures in the **System Configuration → Advanced Parameters → Picture Storage** .

Steps

1. Packet face pictures into one ZIP file.

   Note

   - It is recommended to packet less than 1,000 pictures into one file.
   - The face picture should be in JPG, JPEG, BMP, or PNG format.
   - The size of each face picture should be between 1 KB and 200 KB, and the resolution should be 480×640 and above.
   - The ZIP file should be smaller than 200 MB.
   - It is recommended to name the pictures after the person name.

2. Click → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Face Group** to enter the Face Group Configuration page.
3. Select a face group and click **Import Face Pictures**.
4. Select the ZIP file which contains face pictures.

   The system will verify the face pictures in the ZIP file automatically.
5. After verification, click **Upload**.
6. **Optional:** After importing, edit the person information if needed, such as gender and ID.
7. **Optional:** Perform the following operations if necessary.

Search Face	You can search the faces by person name, gender, or ID.
Copy Faces to Other Group	You can copy certain faces in one group to other groups. Select one or more faces, click **Copy to ...**, and select the target group.
View Face Details	Click • • • → in the lower-right corner of the face picture, or click in the Operation column to view the face details, including person name, gender, ID, and face picture.
Delete Face	Select the face pictures and click **Delete** to delete them from the face group.

20.3.4 Synchronize Faces from Person List

If you have already added face pictures for the persons in the Person list of **Person, User, and Role** module, you can synchronize face pictures from the existing faces in the person list.

Before You Start

Set the person information and face pictures in the Person List. For details, refer to ***Person Management*** .

Steps

1. Click → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Face Group** to enter the Face Group Configuration page.
2. Select a face group and click **Sync from Person List**.
3. Select the mode for synchronization.

By Organization

Synchronize all the face pictures of the persons in one or more organization(s) to the target face group.

By Person

Synchronize the face pictures of one or more persons to the target face group.

4. Select the organization(s) or person(s) and click **>** to add them to the Selected Organization or Selected Person list.
5. Click **Save**.
6. **Optional:** Perform the following operations if necessary.

Search Face	You can search the faces by person name, gender, or ID.
Copy Faces to Other Group	You can copy certain faces in one group to other groups. Select one or more faces, click **Copy to ...**, and select the target group.
View Face Details	Click • • • → in the lower-right corner of the face picture, or click in the Operation column to view the face details, including person name, gender, ID, and face picture.
Delete Face	Select the face pictures and click **Delete** to delete them from the face group.

20.4 Facial Recognition Schedule Configuration

Facial recognition schedule associates specified face group with certain recognition resource (such as DeepinView camera, DeepinMind NVR, facial recognition server, etc.), specifying the capture camera, and setting the time schedule for recognition. During the recognition time period, the recognition resource will compare the faces captured by the capture camera with the target faces in the face group and analyze the similarity. If the similarity is larger or smaller than the pre-defined threshold, the target person will be regarded as matched or mismatched with the person in the face group.

The system supports setting recognition schedule for key persons, strangers, and frequently appeared persons.

20.4.1 Set Recognition Schedule Template

The recognition schedule template defines when the facial recognition is active. The system pre-defines three default templates: All-Day Template, Weekday Template, and Weekend Template. You can customize new templates according to your actual needs.

Steps

1. Click → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Schedule** to enter the Recognition Schedule Configuration page.

2. Click **Configure Schedule Template** on the upper-right corner.
3. Click + on the upper-left corner to add a new template.
4. Create a new name for this template.
5. Select a day of the week and draw time periods on the timeline bar.

Note

Up to 8 time periods can be set for each day.

6. **Optional:** Perform one of the following operations to edit the drawn time periods.
   - Move the cursor to the time period and drag the time period on the timeline bar to the desired position.
   - Click the time period and directly edit the start/end time in the appeared dialog. Or click **Delete** to delete the period.
   - Move the cursor to the ends of time period and drag to lengthen or shorten the time period.
   - Move the cursor and click to copy the time period of this day to other day.

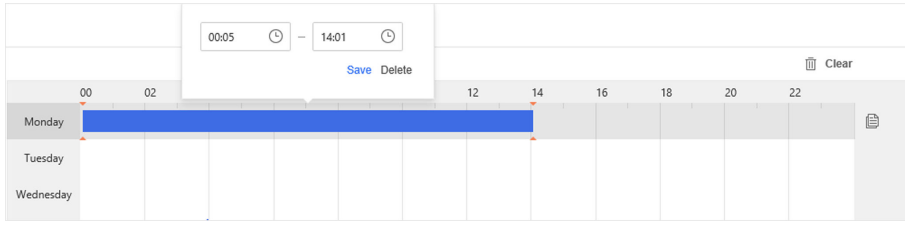


Figure 20-3 Edit Time Period

7. Click **Save**.

20.4.2 Set Recognition Schedule for Key Person

You can set a recognition schedule to define how the recognition resources compare with the face group of key persons so that when a key person is detected, an event will be triggered and the system can notify the security personnel.

Steps

1. Click → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Schedule** to enter the Recognition Schedule Configuration page.
2. Click **Key Person** tab.
3. Click **Add**.
4. Set the parameters of the recognition schedule.

   Recognition Schedule Name

   Customize a name for the schedule.

   Face Group

   The selected face group will be applied to recognition resource. When the detected person matches with the person in this group, an event will be generated to notify the security personnel.

For details about setting a face group, refer to ***Face Group Management*** .

Recognition Resource

Select a device from the drop-down list.

The selected recognition resource will compare picture captured by specified capture camera with the faces in the selected face group.

Note

If you select capture camera as the recognition resource, the camera should support facial recognition.

Capture Camera

Associate the recognition resource with a capture camera, and the recognition resource will compare picture captured by this capture camera with the faces in the selected face group.

Note

One capture camera can be associated with only one recognition resource.

Threshold

The threshold of the similarity between the captured face and the ones in the face group. When the similarity is larger than the threshold, an event will be triggered to notify the security personnel that a key person is detected.

Schedule Template

Select a schedule template from the drop-down list, which defines the time period when the face recognition is active.

5. Click **Save**.

The recognition schedule will be applied to the specified recognition resource automatically and is enabled by default.

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

Edit Schedule	Select a schedule and click to edit its details.
View Schedule Details	Select a schedule and click to view its details.
Enable/Disable Schedule	Select a schedule and check or uncheck **Enable** to enable or disable this schedule. After enabled, the schedule will be active. **Note** By default, the schedule is enabled after applying to the specified recognition resource.
Delete Schedule	Select a schedule and uncheck **Enable** to disable this schedule, and then click .

20.4.3 Set Recognition Schedule for Stranger

You can set a recognition schedule to define how the recognition resources compare with the face groups so that when a person who is NOT in any of the face groups is detected during the time period in the schedule, the system can notify the security personnel.

Steps

1. Click → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Recognition Schedule** to enter the Recognition Schedule Configuration page.
2. Click **Stranger** tab.
3. Click **Add**.
4. Set the parameters of the recognition schedule.

Recognition Schedule Name

Customize a name for the schedule.

Face Group

The selected face group(s) will be applied to recognition resource. When the detected person mismatches with any persons in the group(s), an event will be triggered to notify the security personnel.

For details about setting a face group, refer to ***Face Group Management*** .

Recognition Resource

Select a device from the drop-down list.

The selected recognition resource will compare picture captured by specified capture camera with the faces in the selected face group(s).

Note

If you select capture camera as the recognition resource, the camera should support facial recognition.

Capture Camera

Associate the recognition resource with a capture camera, and the recognition resource will compare the pictures captured by this capture camera with the faces in the selected face group(s).

Note

One capture camera can be associated with only one recognition resource.

Threshold

The threshold of the similarity between the captured face and the ones in the face group(s). When the similarity is smaller than the threshold, an event will be triggered to notify the security personnel that a stranger who is not in any of the face group(s) is detected.

Schedule Template

Select a schedule template from the drop-down list, which defines the time period when the face recognition is active.

5. Click **Save**.

   The recognition schedule will be applied to the specified recognition resource automatically and is enabled by default.

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

Edit Schedule	Select a schedule and click to edit its details.
View Schedule Details	Select a schedule and click to view its details.
Enable/Disable Schedule	Select a schedule and check or uncheck **Enable** to enable or disable this schedule. After enabled, the schedule will be active.
	Note By default, the schedule is enabled after applying to the specified recognition resource.
Delete Schedule	Select a schedule and uncheck **Enable** to disable this schedule, and then click .

20.4.4 Set Recognition Schedule for Frequently Appeared Person

You can set a recognition schedule for frequently appeared person detection. The recognition resource in the schedule will compare the faces detected by the capture camera with other captured faces. If the person is not in any of the associated face groups, and the appeared times is larger than the pre-defined value, an event will be triggered to notify the security personnel that a stranger who appeared many times is detected.

Steps

1. Click → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Schedule** to enter the Recognition Schedule Configuration page.
2. Click **Frequently Appeared Person** tab.
3. Click **Add**.
4. Set the parameters of the recognition schedule.

   Recognition Schedule Name

   Customize a name for the schedule.

   Face Group

   The selected face group(s) will be applied to recognition resource. When the detected person mismatches with any persons in the group(s), and her/his appeared times is more than the pre-defined value, an event will be triggered.

   For details about setting a face group, refer to ***Face Group Management*** .

Recognition Resource

Select a device from the drop-down list.

The selected recognition resource will compare picture captured by specified capture camera with the faces in the selected face group.

Note

If you select capture camera as the recognition resource, the camera should support facial recognition.

Capture Camera

Associate the recognition resource with a capture camera, and the recognition resource will compare picture captured by this capture camera with the faces in the selected face group.

Note

One capture camera can be associated with only one recognition resource.

Historic Days

The recognition resource will compare the detected face with the faces captured within these days. For example, if you set this value as 7 days, the recognition resource will compare the detected face with the face pictures captured in the last 7 days.

Appeared Times

During the historic days, when the appeared times of the face detected by the capture camera reaches this value, he/she will be regarded as a frequently appeared person.

Counting Interval

Within this interval, if the same person is detected for multiple times, the actual appeared time is counted as 1.

Threshold

The threshold of the similarity between the captured face and the ones in the face group. When the similarity is larger than the threshold, the detected person will not be counted as frequently appeared person.

Schedule Template

Select a schedule template from the drop-down list, which defines the time period when the face recognition is active.

5. Click **Save**.

The recognition schedule will be applied to the specified recognition resource automatically and is enabled by default.

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

Edit Schedule	Select a schedule and click to edit its details.
View Schedule Details	Select a schedule and click to view its details.

Enable/Disable Schedule	Select a schedule and check or uncheck **Enable** to enable or disable this schedule. After enabled, the schedule will be active.
	Note By default, the schedule is enabled after applying to the specified recognition resource.
Delete Schedule	Select a schedule and uncheck **Enable** to disable this schedule, and then click .

20.5 Set Facial Recognition Parameters

You can set the retention period of the facial recognition records and other parameters about facial recognition.

Click → **System Configuration** → **Integrated Control** → **Facial Surveillance** → **Parameters** .

Record Retention Period

Set how long the records (including key person recognition records, stranger recognition records, frequently appeared person recognition records, and capture records) can be saved in the database of the system. Once expired, the records will be deleted.

Capture Record Settings

You can set whether the system can receive the capture records or not. Once enabled, the system will subscribe and receive face capture records, and capture record searching page will show.

20.6 Facial Recognition Application

After setting the facial recognition schedule, when the device detects corresponding faces, the device will capture face pictures and you can search the facial recognition records and captured pictures by capture time, camera, and other search conditions. You can also search persons by uploading a face picture, and you can view the moving pattern of the matched person.

20.6.1 Real-Time Recognition

On the Control Client of HikCentral Enterprise-Commercial, the captured picture and recognized information will be displayed in real-time.

Click **Facial Surveillance** on the control panel of the Control Client, and click **Real-Time Recognition** tab to enter the real-time recognition page.

When receiving a face capture event, you can viewing the recognized person information, original picture, person's moving pattern, recorded video footage, etc.

You can filter the real-time recognition records by event type (all events, key person recognition events, stranger recognition events, and frequently appeared person events), or by different face groups.

20.6.2 Key Person Recognition

You can set search conditions including capture time and capture camera to search the capture records of the key persons. For example, you can search the capture records of the VIPs of the shopping center.

Before You Start

Set the recognition schedule for key persons first. For details, refer to ***Set Recognition Schedule for Key Person*** .

Steps

1. On the Home page, click **Key Person** in the Integrated Control section.
2. **Optional:** Select a face group on the left, or you can select **All** to search the capture records of the person in all the face groups.
3. Set the search conditions.
4. Click **Search**.

   The capture records which meet the search conditions will display.
5. **Optional:** Click to view the details of the capture record and perform the following operations.

View Details	Click **Recognition Information** to view the captured picture and person information. Click **Add to Group** to add the person to the target group.
View Original Picture	Click **Original Picture** to view the original picture of the capture record to get a clearer view.
Playback	Select one capture record and click  to view the recorded video footage at the capture time.
Pattern Playback	Click **Person Pattern** and set the time period and similarity to search the person's moving pattern on the map. Click **Pattern Playback** to start playback of the person's moving pattern according to the sequence of the capture records on the map.
Export Search Results	Click **Export** to export the search results in CSV format and you can save the file on your local PC.

20.6.3 Stranger Recognition

You can set search conditions including capture time, capture camera, and age group to search the capture records of the strangers.

Before You Start
Set the recognition schedule for strangers first. For details, refer to ***Set Recognition Schedule for Stranger*** .

Steps
1. On the Home page, click **Stranger** in the Integrated Control section.
2. Set the search conditions including capture time period, capture camera, and age group.
3. Click **Search**.

   The capture records which meet the search conditions will display.
4. **Optional:** Click to view the details of the capture record and perform the following operations.

View Details	Click **Recognition Information** to view the captured picture and person information. Click **Add to Group** to add the person to the target group.
View Original Picture	Click **Original Picture** to view the original picture of the capture record to get a clearer view.
Playback	Select one capture record and click to view the recorded video footage at the capture time.
Pattern Playback	Click **Person Pattern** and set the time period and similarity to search the person's moving pattern on the map. Click **Pattern Playback** to start playback of the person's moving pattern according to the sequence of the capture records on the map.
Export Search Results	Click **Export** to export the search results in CSV format and you can save the file on your local PC.

20.6.4 Frequently Appeared Person Recognition

You can set search conditions including capture time, capture camera, and appeared times to search the capture records of the persons who appeared frequently.

Before You Start
Set the recognition schedule for frequently appeared persons first. For details, refer to ***Set Recognition Schedule for Frequently Appeared Person*** .

Steps
1. On the Home page, click **Frequent Person** in the Integrated Control section.

2. Set the search conditions including the time period of capture, capture cameras, and minimum appeared times.
3. Click **Search**.

   The capture records which meet the search conditions will display.
4. **Optional:** Click to view the details of the capture record and perform the following operations.

View Details	Click **Recognition Information** to view the captured picture and person information. Click **Add to Group** to add the person to the target group.
View Original Picture	Click **Original Picture** to view the original picture of the capture record to get a clearer view.
Playback	Select one capture record and click to view the recorded video footage at the capture time.
Pattern Playback	Click **Person Pattern** and set the time period and similarity to search the person's moving pattern on the map. Click **Pattern Playback** to start playback of the person's moving pattern according to the sequence of the capture records on the map.
Export Search Results	Click **Export** to export the search results in CSV format and you can save the file on your local PC.

20.6.5 Search Person by Face Picture

You can upload a face photo from your local PC and set certain search conditions to search the faces from the capture records. After that, you can view the captured pictures of the person and view her/his moving pattern.

Steps

1. On the Home page, click **Search by Face** in the Integrated Control section.
2. Click **Search Face by Face** tab.
3. Click **+** to select a photo from your local PC.

   Note

   The photo should be in JPG, JPEG, BMP, or PNG format.
4. Set the search conditions such as capture time period, capture camera, and similarity.
5. Click **Search**.

   The capture records which meet the search conditions will display. You can view the moving pattern of the person if you have set the locations of the capture cameras on the map.

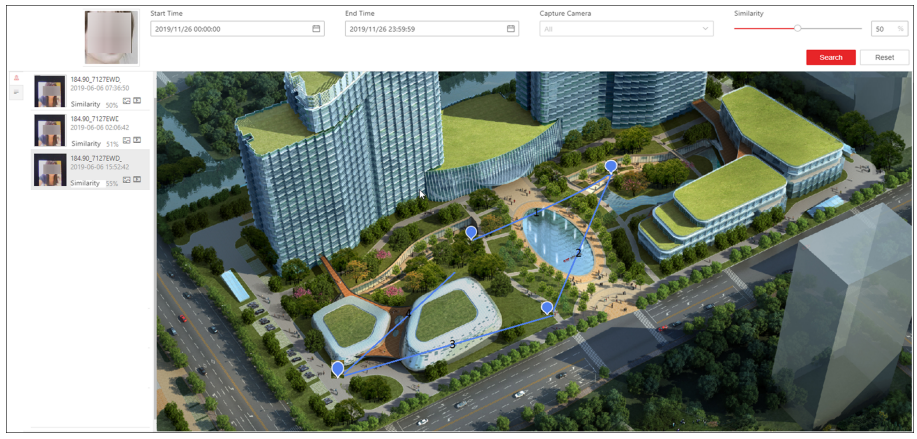


Figure 20-4 Search by Face Picture

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

Secondary Search	Select one capture record and click to search face by the face picture in the capture record.
Playback	Select one capture record and click to view the recorded video footage at the capture time.
Pattern Playback	Click **Pattern Playback** on the upper-right corner to start playback of the person's moving pattern according to the sequence of the capture records on the map.
Switch Mode	**Map Mode:** Show the map and you can view the person's moving pattern. **List Mode:** Show the captured picture of the capture record.

Note

By default, the records are displayed in map mode.

20.6.6 Search History Capture

You can search the history capture records by setting search conditions such as capture time, capture camera, person's age group, gender, wearing glasses or not, etc.

Steps

1. On the Home page, click **Search by Face** in the Integrated Control section.
2. Click **Search Capture Record** tab.
3. Set the search conditions such as capture time, capture camera, person's age group, gender, wearing glasses or not.
4. Click **Search**.

   The capture records meeting the search conditions will show.

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

View Details	Click **Recognition Information** to view the captured picture and person information.
View Original Picture	Click **Original Picture** to view the original picture of the capture record to get a clearer view.
Playback	Select one capture record and click  to view the recorded video footage at the capture time.
Pattern Playback	Click **Pattern Playback** on the upper-right corner to start playback of the person's moving pattern according to the sequence of the capture records on the map.

Chapter 21 Event Configuration

Event is the signal that resources (e.g., cameras) send when something occurs. You can configure an event rule to define an event that requires the alertness of the security personnel. The rule includes linkage actions (such as popping up event-related video on the Control Client and Mobile Client) for the detected events. After the rule being configured, when an event is detected, the system will trigger linkage actions and send the information of the event as alarm to the Control Client and the Mobile Client. The security personnel can check the alarm details via one of the two Clients and handle the particular situation of the event.

21.1 Flow Chart

It is recommended that you follow the flow chart below to do event configurations and operations.

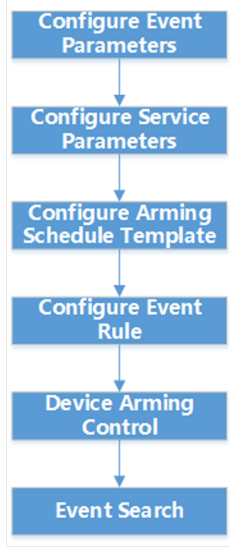


Figure 21-1 Flow Chart for Event Configurations and Operations

- Configure Event Parameters: Configure parameters such as event retention time and event level. For details, see ***Configure Event Parameters*** .
- Configure Service Parameters: If you need to configure message linkage (Sending a message to the specified user when the specified event occurs) and email linkage (Sending an email to the specified user when the specified event occurs), you should log in to the Operation and Management Center, and then go to **Maintenance → Parameter Configuration → Service Parameters** to configure message service and email service. For details, see the *User Manual of Operation and Management Center*.
- Configure Arming Schedule Template: Configure the arming schedule template which can be used in event rule configuration. For details, see ***Configure Arming Schedule Template*** .
- Configure Event Rule: Configure an event rule to define the time, source, event type, and linkage action(s) for an event. For details, see ***Configure Event Rule*** .

- Device Arming Control: After configuring events, you should arm related devices to enable the devices to upload events to the system. For details, see ***Device Arming Control*** .
- Event Search: Search history events and export events. For details, see ***Search Event*** .

21.2 Configure Event Parameters

Event parameters include retention time and event priority. Retention time defines how long the event record will be kept, and the event priority defines the event's alert level.

Steps

1. Click → **System Configuration** → **Integrated Control** → **Event Configuration** → **Parameter Configuration** to enter the Parameter Configuration page.
2. Configure the parameters.

   Keep Event for

   Enter the retention time of the events. Once the retention time expires, the events will be deleted automatically.

   Event Priority

   Define the priority for events. The priority can be used to define an event when setting event rule, as well as filter the event-related alarm information on the Control Client and Mobile Client.

   You can also click the drop-down list to select a color to represents a specific level of priority.

21.3 Configure Arming Schedule Template

Arming schedule template defines when and how the events or alarm will be triggered. The system predefines three default arming schedule templates: All-Day Template, Weekday Template and Weekend Template. All-Day Template can be used for arming or disarming devices all day. Weekday Template can be used for arming or disarming devices in weekday. Weekend Template can be used to arming or disarming devices at weekend. You can also customize new templates according to your desire.

Steps

1. Click → **System Configuration** → **Integrated Control** → **Event** → **Event Rule** to enter the Event Rule page.
2. Click **Set Arming Schedule Template** on the right corner of the page to enter the Arming Schedule Template Configuration page.
3. Click + to add a new schedule template.
4. Enter the template name in the input field.
5. Drag on the time bar to draw a time period, which defines the arming period.
6. Perform the following operations to customize the template.

Set Time Period	Click the time period to manually enter the start time and end time, or delete it.
Clear Time Periods	Click **Clear** to clear all time periods in the time bar.
Copy Time Periods	Click in the last column to copy the time period(s) to the other weekdays.

7. Click **Save**.

21.4 Configure Event Rule

The event rule includes five elements, namely, "who" (event source, i.e., the device which detects the event), "when" (specified time period), "where" (specified area), "which event" (specified event type), as well as "how to notify security personnel" (the event linkage). For example, the event can be defined as intrusion happens in the bank vault and be detected by cameras mounted in the bank vault on weekend, and notify the security personnel once happened. You can also set the event priority, which can be used for sorting event-related alarms in the alarm center of the Control Client and Mobile Client.

21.4.1 Configure Event Rule by Template

The system provides four frequently-used rule templates and other five pre-defined templates.

Steps

1. Click → **System Configuration** → **Integrated Control** → **Event Configuration** → **Rule Configuration** to enter the Rule Configuration page.
2. Click **Add** to enter the Add Event Rule page.
3. Select a template from the template list.

   The descriptions of the four frequently-used templates are as follows:

   Template for Notifying Surveillance Center of Intrusion

   An intrusion event occurs when people, vehicle or other objects enter and loiter in a pre-defined virtual region which they should not enter. When intrusion is detected by the camera added to system, the system will notify the surveillance center of the event.

   Template for Notifying Surveillance Center of Parking in No-Parking Zone

   When the camera added to the system detects a vehicle parks in no-parking zone, the system will notify the surveillance center of the event.

   Template for Notifying Surveillance Center of Fire Escape Blocked

   When the camera added to the system detects that fire escape of a building is blocked, the system will notify the surveillance center of the event.

   Template for Notifying Surveillance Center of Intrusion into Landscape Pool

When the camera added to the system detects intrusion into the landscape pool, the system will notify the surveillance center of the event.

4. Click the underlined parameter on the Rule Explanation section to set the required information.

Note

The required information varies with different templates.

5. Click **Save**.

What to do next

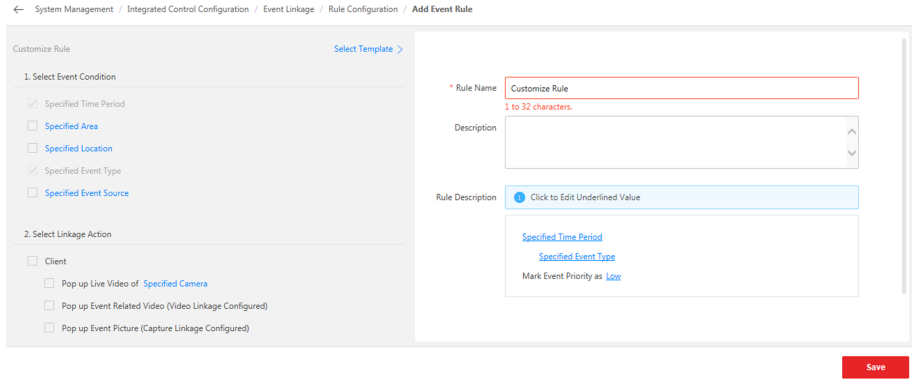
After setting the event rule, you need to arm the event so that the system can receive an event when it is triggered to notify the security personnel. You need to enter the event arming setting page of different modules respectively to arm the event. For details, refer to Event Arming Control section in this manual.

21.4.2 Configure Custom Event Rule

If the event rule template cannot properly define the rule you need, you can add a custom event rule. you can set multiple linkage actions for the event, including client linkage (such as popping up live video or specified camera), displaying live video of a specified camera on a specified video wall, PTZ control, etc.

Steps

1. Click → **System Configuration** → **Integrated Control** → **Event Configuration** → **Rule Configuration** to enter the Rule Configuration page.
2. Click **Add** to enter the Add Event Rule page.
3. Click **Add Custom Rule**.



4. Create a rule name in the Rule Name field.
5. Enter the description of the rule in the Description filed.
6. Select event conditions on the left of the page and then configure the selected conditions in Rule Description section on the right.

Note

- The selected event condition will be displayed as an underlined parameter in the Rule Description section on the right side of the page.
- Specified time period and specified event type are selected by default.

7. Configure linkage action(s).

1) Select linkage action(s) from the linkage action list on the left side of the page.
2) Click the underlined parameter(s) on the Rule Explanation section to set the required information.

Linkage Action	Description
Pop up Live Video of Specified Camera	When the event you defined occurs, the live video of the specified camera will pop up on the Control Client and the Mobile Client. You can set specified camera from the two types of resources below: **Event Source Camera** The specified camera will be camera which detects the event. **Specified Resource** Click → to select camera(s) from the resource tree.
Pop up Event-Related Picture	When the event you defined occurs, the video footage recorded by the specified camera will pop up on the Control Client and Mobile Client. **Note** You should have configured video linkage (Specified Camera Records Video or Add Video Tag Type and Description to Specified Camera) before you select this linkage action.
Pop up Event-Related Picture	When the event you defined occurs, the event-related picture will pop up on the Control Client and Mobile Client. **Note** You should have configured the linkage of capturing picture (Specified Camera Captures Pictures at an Interval of Specified Seconds for Specified Times).
Control Specified Two-Way Audio Channel's Two-Way Audio	You can specify a two-way audio channel for this linkage action. When the event you defined occurs, the specified two-way audio channel will pop up on the Control Client and Mobile Client.
Audio Warning	When the event you defined occurs, there will be audio warning on the Control Client and Mobile Client.

Voice Prompt

When the event you defined occurs, there will be a voice prompt which tells you the details of the event. You can select information for the voice prompt, including event priority, area, location, event source, time, etc.

Pop-up Window Overlay Event Information

Overlay the information of event source and event rule on the pop-up live view window.

Display Video of Specified Camera on Specified Video Wall

When the event you defined occurs, the live video of a specified camera will be displayed on a specified video wall.

Note

- You should have set alarm window on the video wall. For details, refer to the *User Manual of the HikCentral Enterprise-Commercial Control Client.*
- The alarm priority of the alarm window on the video wall should not be higher than the event priority. For details, refer to the *User Manual of the HikCentral Enterprise-Commercial Control Client.*

Record Video Footage

Specified Camera Records Video

You can specify a camera to record video footage if the event you defined occurs.

Note

You should have configured at least one type of recording schedule (device storage or central storage) for the specified camera.

Add Video Tag Type and Description to Specified Camera

You can specify a camera to record video footage if the event you defined occurs. You can also add tags and description for the event.

Note

Line breaks are not allowed when entering the description.

Specified Camera Captures Pictures at an Interval of Specified Seconds for Specified Times

For example, you can specify a camera to capture pictures for 10 times at the interval of 2 seconds.

Note

You should have configured picture storage server. See the *User Manual of Operation and Management Center* for details.

Control Specified Alarm Output

When the event you defined occurs, the specified alarm output will be activated.

	Click → to select an alarm output from the resource tree.
PTZ Control	**Call Specified Camera's Preset** **Switch to Preset when Event Occurs:** You should specify the camera and the preset. When the event you defined occurs, the camera will rotate to the position of the preset No. **Back to Preset when Event Ends** You should specify the camera and the preset. When the event you defined ends, the camera will go back to the position of preset No. **Call Specified Camera's Patrol** You should specify the camera and the patrol NO. When the event you defined occurs, the camera will travel to all the presets defined in Patrol settings in a designated sequence. **Call Specified Camera's Pattern** You should specify the camera and the pattern No. When the event you defined occurs, the camera will move along the path recorded in Pattern settings.
Open Door of Specified Access Control Point	When the event you defined occurs, the access control point you specified will be opened.
Send Message to Specified User	When the event you defined occurs, the message server will send message to the specified user. You can customize the message content. **Note** You should have set the user's mobile phone number. See ***Role and User Management*** for details.
Send Email to Specified User	When the event you defined occurs, the email server will send email to the specified user. You can customize the email content. **Note** You should have set the user's email. See ***Role and User Management*** for details.

8. Click **Save**.

What to do next

After setting the event rule, you need to arm the event so that the system can receive an event when it is triggered to notify the security personnel. You need to enter the event arming setting page of different modules respectively to arm the event. For details, refer to Event Arming Control section in this manual.

21.5 Device Arming Control

After configuring events, you should arm the configured events for the devices, or the configured events will not be triggered.

The detailed operation path are as follows:

- Arm Video Surveillance Events: Click , and then go to **Video Surveillance → Device Arming/Disarming** .
- Arm Access Control Events: Click , and then go to **One-Card System → Access Control → Event Parameters** .
- Arm Video Intercom Events: Click , and then go to **One-Card System → Video Intercom → Event Parameters** .
- Elevator Control Events: Click , and then go to **One-Card System → Elevator Control → Event Parameters** .

21.6 Search Event

You can search all the events of the added resource for checking. You can also filter events, mark events as read, view event details (including event priority, event status, start & end time, location, resource, etc.), add remarks to events, etc.

Before You Start

You should configure the event at first.

Steps

1. Click **Event Search** in the Home page.
2. Select a searching rule in the left column.

   Two rules are available: **by Event Type** & **by Event Rule Name**.
3. Select an event type or an event rule.
4. Set search conditions (including area, location, event source, start time, end time, event priority, handling status, handling suggestion) for the event.

   Event Source

   Generally, event source is the alarm device(s) of an event.
5. Set time range for searching.
6. Click **Search**.

   The matched events will be displayed on the list.

7. Perform the following operation(s) after searching alarms or events.

- Click to view details of an event.
- Click **Export** to save the found events to your PC.

Chapter 22 Map

Two types of map are available: GIS map and static map. On the GIS map, you can set and view the hot spot and element's geographic location. On the static map, you can set the view the geographic locations of the installed cameras, alarm inputs, alarm outputs, etc. After configuring the map via Web Client, you can view the live view and playback of the resources added to the map, and get a notification message from the map when the alarm is triggered.

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 area called hot spots) geographic locations in the real word. 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 form the cameras. With the hot region, you can link the static map to view the detailed monitoring scenario, for example, the monitoring scenario of a building.

The static map (It does not have to be the geographical map, although it often is. Depending on your organization's needs, photos and other kinds of image files can also be used as static maps.) gives you a visual overview of the locations and distributions of the hots 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 directions the cameras are pointing. With the function of hot region, static 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 static map via HikCentral Enterprise-Commercial Web Client, you can view the live video and playback of the elements via Web Client, and get a notification message from the map via Web Client when an alarm is triggered.

22.1 Flow Chart

It is recommended that you follow the following flow chart to do configurations and operations of monitoring resources and events on map.

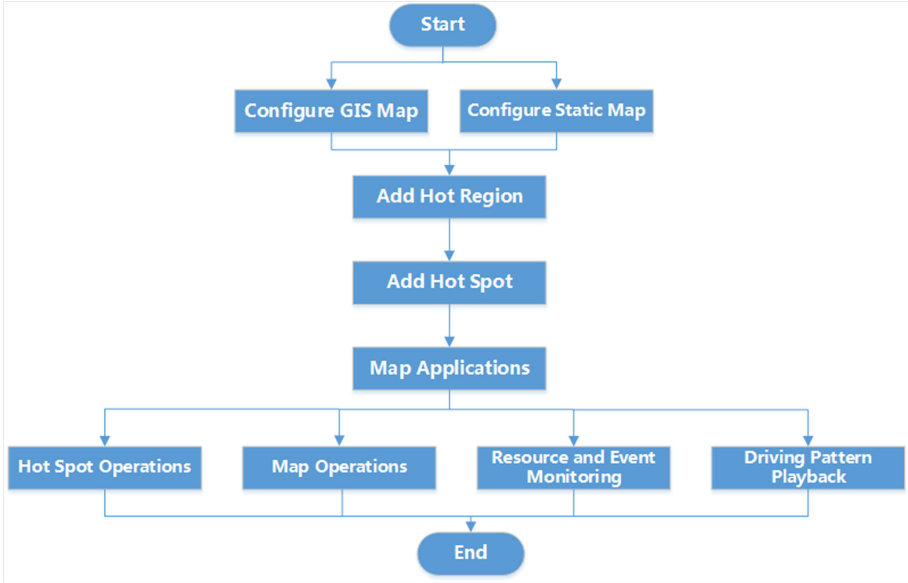


Figure 22-1 Flow Chart for Configurations and Operations in Map Module

- Configure GIS Map: Configure the online GIS map or offline GIS map. For details, see ***Configure GIS Map*** .
- Configure Static Map: Upload a picture as the static map. For details, see ***Add Static Map*** .
- Add Hot Region: Add hot regions to a map. For details, see ***Add Hot Region*** .
- Add Hot Spot: Add hot spots to a map. For details, see ***Add Hot Spot*** .
- Hot Spot Operations: Perform operations on different resources added to the map. For details, see ***Manage Hot Spot*** .
- Map Operations: Perform operations such as adding label to the map. For details, see ***Operate Map*** .
- Resource and Event Monitoring: View alarms of the resources on the map. For details, see ***View Alarm on Map*** .
- Driving Pattern Playback: View driving patterns on the map. For details, see ***Play Driving Pattern*** .

22.2 Map Configuration

By configuring base map(s), you can add resources (such as cameras, alarm inputs, and alarm outputs, etc.) to the map and view the map in E-map module. When an alarm is triggered, you will get a notification message in E-map module. Then you can view event& alarm details (including live view video, playback, captured pictures, etc.) and driving pattern playback of the added resources. With the function of hot region, base maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

Two base map types are available:

GIS Map

Online Google map. You should connect to network to use it. With GIS map, you can see the geographic locations of your surveillance system. This type of map uses 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.

Static Map

A static map does not have to be a geographical map, although it often is. Depending on your organization's needs, photos and other kinds of image files can also be used as base maps which gives you a visual overview of the locations and distributions of the hot spots. You can see the physical locations of the cameras, alarm inputs, alarm outputs, etc.

Note

Only one type of base map (either GIS map or static map) can be configured in an area.

22.2.1 Configure GIS Map

You can enter Google map API URL to display GIS map on the E-map module, showing the geographic location of the resources (such as cameras and alarm input) in the real world. You can search a desired place in the world and add resources there. Then you can view alarm information and driving pattern playback of the added resources on E-map module.

Before You Start

Make sure you have got Google map API URL.

Steps

1. Click → **Integrated Control → Map → Parameters** .
2. Enter the Google map API URL and click **Save**.

   Note

   - Apply for the API URL and the permission for using it from Google cloud platform.
   - You will not be able to search place on Google map without entering Google map API URL.

3. Click **Integrated Control → Map → Resource Operation on Map** .
4. If you have configured a static map, click **Clear** to clear the configuration.
5. Click **Switch to GIS Map** to enter the GIS map page.
6. Perform the following operation(s).
   - Drag the map to adjust the map area.
   - Scroll the mouse wheel or click **+/-** to zoom in or zoom out the map.
   - Click  or  to switch between vector map and satellite map.
   - Enter key words in the search field in the upper-left corner of the map to search a place in the world.
   - Add hot spot(s) to the map. For details, refer to .
   - Add hot region(s). For details, refer to ***Add Hot Region*** .
7. Click **Save**.

22.2.2 Add Static Map

After adding a static map, you can add hot spots and hot regions on the map. Then you can see the physical locations of the hot spots (resources (e.g., camera, alarm input)). For example, you can add a building's map as a static map and add its rooms as hot regions of the building's map.

Steps

1. Click → **Integrated Control → Map → Resource Operation on Map** .
2. If you configured GIS map in the last operation, click **Clear** to clear the former map configuration.
3. Select an area and click **Upload** to upload the static base map.

   You can add more than one static map in an area and switch maps in the lower-right corner of the map. For example, you can add maps of multiple rooms on a floor in an area.
4. Click **Save**.
5. Add hot spots. For details, refer to ***Add Hot Spot*** .
6. Add hot regions. For details, refer to ***Add Hot Region*** .
7. Perform the following operation(s) to manage the maps.

Add Static Map	Click **Edit → Upload** to add more static maps.
Zoom Map	Scroll the mouse wheel or click **+/-** to zoom in or zoom out the map.
Edit Map Name	Click **Edit**, then enter a new map name in the field under a map and click **Save**.
Set Default Map	Click **Edit → Default → Save** to set a default map.
Delete Map	Click **Edit**, then hover the mouse over the map to be deleted and click → **Save** .
Copy Configuration to Other Areas	Click **Copy**, then select areas to copy the map to and click **OK**.
Clear Map Configuration	Click **Clear** to clear map configuration.

22.2.3 Add Hot Spot

You can add hot spots such as cameras, alarm inputs, alarm outputs, access control point, and under vehicle surveillance systems, etc. into the map.

Before You Start

A map should have been added. For details about adding a GIS map or static map, refer to ***Configure GIS Map*** and ***Add Static Map*** .

Steps

1. Click → **Integrated Control → Map → Resource Operation on Map** .

2. Click **Area: Root Node** and select an area.
3. Click **Configure Resource** and select a resource type.
4. Drag a resource from the resource list to a desired location.

   For cameras, will be displayed on the map.

   Note

   Icons of different resource types vary.

5. Perform the following operation(s).

Move Hot Spot	Drag a hot spot to move it.
Delete Hot Spot	Select a hot spot on the map and click to delete resource.
Adjust Hot Spot Locations	Adjust hot spot locations in a batch. a. Click **Select**. b. Press **ESC** to stop selecting resources. c. Drag to select the resources on the map. d. Click **Align**. e. Select a desired align mode.
Copy Configuration to Other Areas	Click **Copy**, then select areas to copy the map to and click **OK**.
Clear Map Configuration	Click **Clear** to clear map configuration.

22.2.4 Add Hot Region

The hot region function links a map to another map. The added map is called child map while the map to which you add the hot region is a parent 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 parent map. With the function of hot region, base maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

Before You Start

At least 2 maps should have been added. For details, refer to ***Configure GIS Map*** and ***Add Static Map*** .

Steps

1. Click → **Integrated Control → Map → Resource Operation on Map** .
2. Click **Link** and then click a desired position on the map to open the Add Link window.
3. Select an area.
4. Enter the hot region name in the field.
5. Click **OK**.

22.3 Manage Hot Spot

After the hot spots (such as cameras, alarm inputs, alarm outputs, etc.) are added to the map, you can get the live view and playback of the cameras, control the status of the access control devices, view alarm information on the map.

Steps

1. Click **Map** on the Home page to enter the Map page.
2. Click **Resource Monitoring** to enter the resource monitoring page.
3. Click in the upper-right corner to expand the area list. Select an area from the area list to show the map.
4. **Optional:** Enter the keyword in the upper-left search field and click to search for the specified hot spots or locations.
5. **Optional:** Move the cursor on the icon of the hot spot to view the name of the hot spot. Click the icon of the hot spot to view the detailed information in the upper-left panel.
6. **Optional:** Click in the detailed information panel to add the hot spot to Favorites. The hot spots that have been added to Favorites will be marked with in the detailed information panel. You can click in the upper-left corner of the map to view all hot spots in Favorites.
7. **Optional:** You can perform further operation(s) to manage the hot spot(s). For example, you can get live view, playback, and history alarm information for the cameras, control the door status for the access control devices, view number of parking spaces for parking lot, view the vehicle passing records for entrance and exit, etc.

22.4 Operate Map

You can perform some basic operations on the map, such as adding label, measuring distance, zooming in/out, etc.

Before You Start

Note

Both GIS map and static map support all basic operations unless otherwise noted.

Steps

1. Click **Map** on the Home page to enter the Map page.
2. Click **Resource Monitoring** to enter the resource monitoring page.
3. Click in the upper-right corner to expand the area list. Select an area from the area list to show the map.
4. **Optional:** Enter the keyword in the search field and click to search for the specified hot spots or locations.
5. **Optional:** Perform the following operation(s) on the map.

   Draw to Select Cameras

Click **Drag to Select** to draw an area on the map. The number of all cameras in the area will be calculated. You can click **Live View** or **Playback** to start live view or playback of all cameras in the area.

Add Label

Click **Label** and move the cursor to the location you want to mark on the map. Click on the location again to add a label on the location. The location will be marked with .

Measure

Measure distance or area on the map.

Measure Distance

Click **Measure** and select **Measure Distance**. Click on the point to start measurement, and double-click to finish. You can click to add multiple points between the start point and the end point, and the total distance will show on the end point. Click to clear the measurement.

Measure Area

Click **Measure** and select **Measure Area**. Click on the point to start measurement, and double-click to finish. You should add at least one point between the start point and the end point, and you can also add multiple points. The area will show on the end point. Click to clear the measurement.

Note

Only GIS map supports measuring distance or area on the map.

Filter Resources

Click **Show** to check the resources you want to display on the map, and uncheck the resources you want to hide from the map.

Locate Alarm

Click **Locate Alarm** to show the source and location of the latest alarm.

Display Resource Name

Click **Display Name** to show the hot spot name on the map.

Open Hot Region

The hot region is marked with on the map. You can click the icon and click **Open Hot Region** to open the hot region linked with the map.

Switch Map

Click **Map** or **Satellite** in the lower-right corner to switch between the GIS map and the satellite map.

22.5 View Alarm on Map

You can view the triggered alarm information of the hot spot on the map in real-time, or search history alarm information, including alarm time, alarm location, captured alarm picture, etc. You can also add your suggestion on how to process the alarm event.

22.5.1 View Real-Time Alarm

You can monitor alarms on the Map module in real-time and view details about the alarm event.

Steps

1. Click **Map** on the Home page to enter the Map page.
2. Click **Resource Monitoring** to enter the resource monitoring page.
3. Click in the upper-right corner to expand the area list. Select an area from the area list to show the map.
4. **Optional:** Enter the keyword in the search field and click to search for the specified hot spots or locations, or click and select the hot spots or locations from Favorites.
5. For a hot spot on the map, if there is any alarm triggered, the icon for the hot spot will turn red and twinkle. You can perform one of the following operations to view details about the real-time alarm.
   - Click the twinkling red icon and click **View** in the upper-left panel to open the Event Details window.
   - Click in the upper-left corner of the map and select the real-time alarm from the Real-Time Alarm list to open the Event Details window.

   Note

   In the Event Details window, you can view detailed alarm information, including event priority, start time, location, etc. You can also add your suggestion on how to process the alarm.
6. **Optional:** For hot spots configured with alarm linkage, you can perform the following operations when viewing alarm event details.

   Live View Linkage

   Pop up live view window to display the alarm event when the alarm is triggered. You can also perform operations, such as capturing, zooming in, etc., during live view. For details about live view operations, refer to ***Live View*** .

   Recording Linkage

   View the video recorded by the camera when the alarm is triggered.

   Capture Linkage

   View the picture captured by the camera when the alarm is triggered.

Note

For details about event linkage configuration, refer to ***Event Configuration*** .

22.5.2 Search History Event

You can search history event information by specifying conditions, such as area, event source, time period, etc. You can also view details about the history alarm, including live view for the alarm, captured pictures, event priority, location, etc.

Steps

1. Click **Map** on the Home page to enter the Map page.
2. Click **Event Monitoring** to enter the event monitoring page.
3. Select the display mode from the drop-down list in the upper-left corner to show the alarms. HikCentral Enterprise-Commercial supports showing the history alarms by event type or by event rule name.
4. Click and set parameters, such as area, event source, start time, end time, etc., to search the history alarms.
5. **Optional:** Click **All**, **High**, **Medium** or **Low** to filter the history alarms by event priority.
6. **Optional:** Click to view details about the history alarm, such as event priority, location, event source, etc. For hot spots configured with alarm linkage, you can also view live view linkage and captured pictures.

Note

For details about alarm linkage configuration, refer to ***Event Configuration*** .

22.6 Play Driving Pattern

You can search and view the history driving pattern of the vehicle installed with mobile devices (such as mobile DVR, PVR, etc.) in the specified time period. During the driving pattern playback, you can set the playing speed, measure the distance between two points, and enable playback in the middle of the screen.

Steps

Note

This function should be supported by the device.

1. Click **Map** on the Home page to enter the Map page.
2. Click **Driving Pattern Playback** to enter the Driving Pattern Playback page.
3. Select the portable devices from the Playback Device list.
4. Set the start time and end time for the playback time period.
5. Click **Playback** to start driving pattern playback.

6. **Optional:** Perform the following operation(s) during driving pattern playback.

Pause/Continue

Click ⏸ to pause the driving pattern playback, and click ▷ to continue playback.

Stop

Click □ to stop driving pattern playback.

Set Playback Speed

Click ⏪ to slower the playback speed, or click ⏩ to speed up the playback.

Mark Interval

Select time from the drop-down list to mark the distance by time on the driving pattern.

Centered Playback

Enabling Centered Playback will fix the driving pattern being played back in the middle of the screen.

Chapter 23 Resource Maintenance

In the Maintenance module, you can set health monitoring schedules for resources. After that, the platform will monitor the running status of the resources added to the platform based on the schedules. You can also configure health monitoring alarms to ensure the maintenance personnel get notified of the resource exceptions (e.g., device faults and network exceptions) in time, so that they can locate the source of exceptions and then maintain or repair the resources without delay.

The system supports maintenance of three types of resources: video resources and access control resources.

- Video Resource Maintenance: Health monitoring for video resources added the platform, including encoding devices, decoding devices, storage servers, etc.
- Access Control Maintenance: Health monitoring for access control resources added to the platform, including access control devices, video intercom devices, and elevator control devices.

23.1 Flow Chart

You are recommended to follow the flowchart below to do configurations and operations in the Maintenance module.

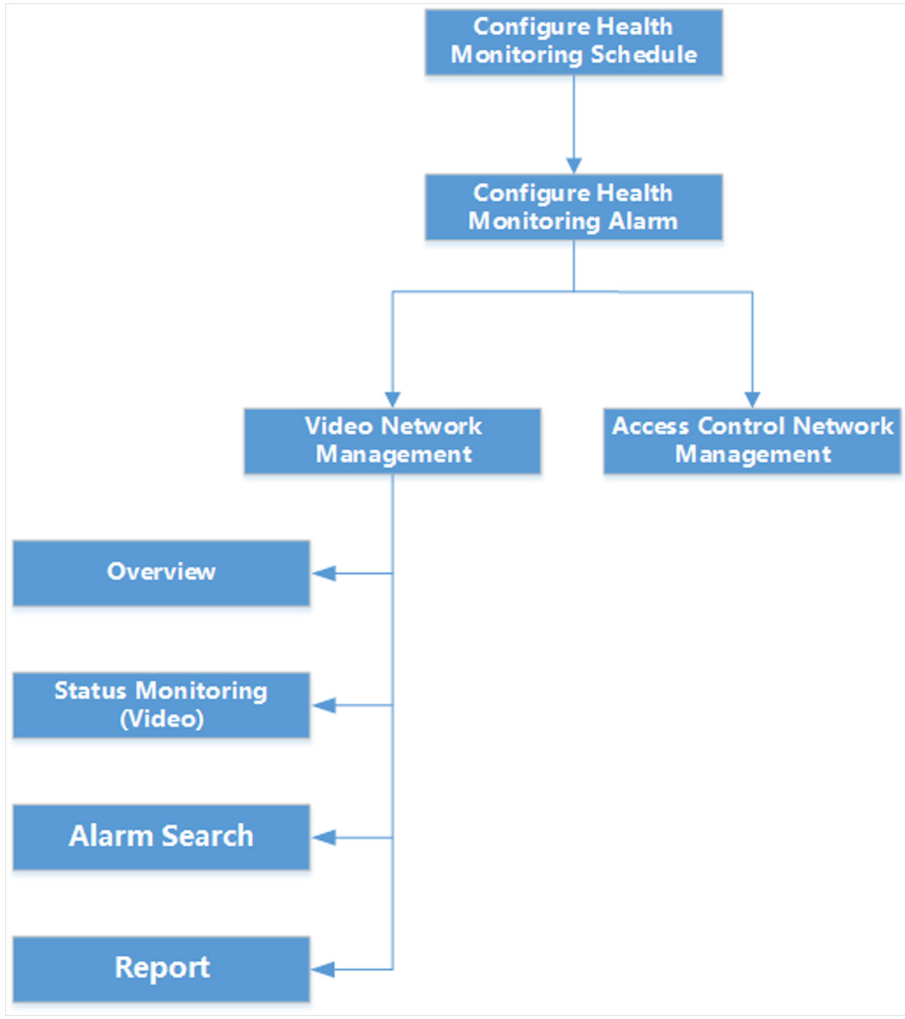


Figure 23-1 Flow Chart for Maintenance

- **Configure Health Monitoring Schedule**: Configure health monitoring schedules to specify the time schedules for monitoring different types of resources on the platform. For details, see ***Configure Health Monitoring Schedule*** .
- **Configure Health Monitoring Alarm**: Configure alarms of different priority levels for the detected exceptions. For details, see ***Configure Alarm for Access Control Device*** , ***Configure Alarm for Access Control Point*** , ***Configure Alarm for Camera*** , ***Configure Alarm for Card Reader*** , ***Configure Alarm for Decoding Device*** , ***Configure Alarm for Encoding Device*** , and ***Configure Alarm for Resource Health Status*** .
- **Alarm Search**: Search all the triggered health monitoring alarms, and handle alarms. For details, see
- **Status Monitoring (Video)**: Applications for viewing the results of health monitoring for video resources, such as video quality diagnosis and reports. For details, see ***Status Monitoring*** .
- **Access Control Network Management**: Applications for viewing the results of health monitoring for access control devices, such as health status overview and reports. For details, see ***One-Card Resource Maintenance*** .

23.2 Maintenance Configuration

To monitor the health status of the resources added to the system, you need to configure health monitoring schedules to define the time periods for the monitoring, and then configure alarms for the resource exceptions that may occur in the defined time periods. After that, alarms will be triggered if exceptions occur in the periods, and you can check the exception information and fix problems accordingly.

Note

For details about checking resource exceptions, refer to ***Video Resource Maintenance*** .

23.2.1 Configure Health Monitoring Schedule

A health monitoring schedule is a time arrangement for monitoring the health status of the resources added to the system. Besides the monitoring time periods, it defines the type of resource to be monitored (e.g., encoding device), and the type of health status to be monitored (e.g., running status). Three default templates of health monitoring schedule are available: all day template, weekday template, and weekend template. All day template is for monitoring the recourse health status at any time. Weekday template is only for monitoring in the weekday. And Weekend template is only for monitoring in the weekend. You can also customize the monitoring periods.

Steps

1. Click → **System Configuration** → **Maintenance** → **Health Monitoring Schedule** to enter the Schedule Management page.
2. Click **Add** to enter the Add Schedule page.
3. Set the required information, such as resource type and schedule name.

   Resource Type

   Select a type of resources for health monitoring.

   Checking Type

   Set the type of health status to be checked.

   Running Status

   Enable the system to check the resource running status, incuding online status, disk status, etc.

   Video Retention

   Enable the system to check the video retention status of the cameras. You should set the number of days as the qualified standard for video retention. The default value is 30 days.

   Recording

   Enable the system to check if video loss exists.

If No Recording Schedule Configured

Compare with All-Day Schedule

If no recording schedule is configured for a camera, the system will automatically generate an all-day schedule in the network management service for the camera. And then the system will check if video loss occurs in the scheduled recording time for the camra.

Note

For details about all-day schedule, refer to ***Configure Recording Schedule*** .

Compare with Latest-Day Schedule

If no recording schedule is configured for a camera, the system will automatically generate a latest-day schedule in the network management service for the camera. And then the system will check if video loss of occurs in the latest day for the camera.

Not Compare

If no recording schedule is configured for a camera, the system will NOT automatically generate any recording schedule for the camera.

Accumulated Video Loss Duration

If the accumulated vido loss duration of a camera reaches the configured value, the situation will be regarded as an exception.

Accumulated Times of Video Loss

If the accumulated times of video losses of a camera reaches the configured value, the situation will be regarded as an exception.

Single Video Loss Duration

If a video loss of a camera reaches the configured value, the situation will be regarded as an exception.

Cascade Status

Check the status of the cascading camera.

VQD (Video Quality Diagnosis)

Enable the system to perform video quality diagnosis. You should select a VQD item(s), such as stripe nosie.

Schedule Template

Select a time schedule template for health monitoring. You can select one of the three default schedule templates, or add a custom schedule template.

Note

For details about adding a custom schedule template, refer to ***Add Custom Schedule Template*** .

Checking Frequency

Set the checking frequency. For example, if you set weekend template as the time schedule, and set 15 minutes as the checking frequency, the system will check the resource health status for every 15 minutes in the weekend.

4. Click **Save**.

   The schedule will be added to the health monitoring schedule list.
5. Select the schedule from the health monitoring schedule list and then click **Enable** to enable the schedule.
6. **Optional:** Perform the following operations after adding and enabling health monitoring schedules.
   - Select a schedule from the health monitoring schedule list and then click **Disable** to disable it.
   - Select schedules and then click **Delete** to delete it.

     Note

     You should have disabled the schedule before you can delete it.
   - Click **All**, **Enabled**, or **Disabled** to filter the list by the schedule status.
   - Select a checking type to filter the list.
   - Click **View** to view the scheduled time periods.
   - Click to edit the schedule.

23.2.2 Add Custom Schedule Template

You can add custom schedule template for health monitoring.

Steps

1. Click → **System Configuration** → **Maintenance** → **Health Monitoring Schedule** to enter the Schedule Management page.
2. Select **Add Schedule Template** from the **Schedule Template** drop-down list to open the Add Template window.
3. Create a name for the template.
4. Drag on the time bar to set the time periods in which health monitoring can be performed.
5. **Optional:** Perform the following operation to manage the time periods.
   - Move the cursor to the two ends of a time period until the cursor turns to a double-end arrow shown as , and then drag to lengthen or shorten the time period.
   - Move the cursor to a time period until the cursor turns to , and then drag to move the time period.
   - Click a time period and click on the pop-up dialog to set precise start time and end time for the time period, and then click **Save** on the dialog.
   - Click and then select a day the copy the time period to the day.
   - Click a time period and then tap **Delete** on the pop-up dialog the delete the time period.
   - Click **Clear** to clear all the time periods.

6. Click **OK**.

   The added template will be displayed on the Schedule Template drop-down list on the Add Schedule page.

23.2.3 Configure Alarm for Resource Health Status

For the detected exceptions which requires alert in health monitoring, you can configure alarms of different alarm priorities (or alert levels) for them. After that, when the exceptions occur, related alarms will be triggered. And you can search all the alarm information related to resource health status and acknowledge the alarms. Two types of alarms are available: status alarm and performance alarm. The former is related to the resource status (e.g., online status and disk status), and the latter is related to the resource's functional performance (e.g., main stream frame rate).

Note

- For details about searching alarm information related to resource health status, refer to ***Alarm Search*** .
- Performance alarm is only supported by camera and access control device.

Configure Alarm for Encoding Device

Perform the following task to configure health status alarm for the encoding device such as NVR.

Before You Start

You should have configured health monitoring schedule. See ***Configure Health Monitoring Schedule*** for details.

Steps

1. Click → **System Configuration** → **Maintenance** → **Configure Alarm** to enter the Configure Alarm page.
2. Select encoding device from the device tree.
3. Enable the content(s) for the status alarm and set the alarm priority.

   Note

   The alarm priority defines the alert level of the alarm. The alert level ascends from Prompt all the way to High.

Figure 23-2 Alarm Priority

The following list describes the contents of the status alarm for encoding device.

Online Status

Detects if the device is offline.

Work Status

Detects If device exceptions, video channel exceptions, and exceptions of two-way audio channel exist.

Disk Status

Detects if disk exception exists.

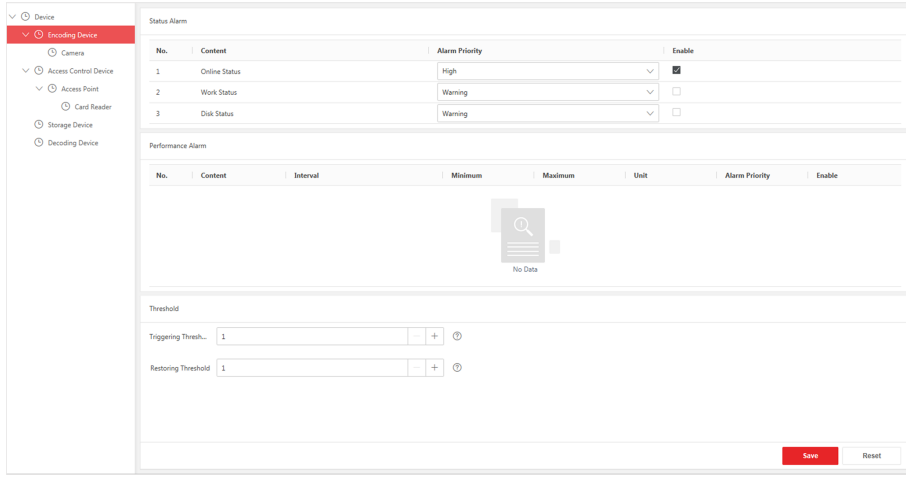


Figure 23-3 Status Alarm for Encoding Device

4. Set the thresholds for triggering alarm and restoring alarm.

Triggering Threshold

If an exception has been detected for the configured times consecutively, an alarm about the exception will be triggered.

For example, if you set the triggering threshold of Online Status to “3”, the alarm about the online status of a specific encoding device will be triggered when the system detects the device is offline for 3 times consecutively.

Restoring Threshold

If an exception has not been detected for the configured times consecutively, the alarm about the exception will be restored automatically.

For example, if you set the restoring threshold of Online Status to “2”, the alarm about online status of an encoding device will be restored when the system detects the device is online for 2 times consecutively.

5. Click **Save**.

Configure Alarm for Camera

Perform the following task to configure health monitoring alarm for camera.

Before You Start

You should have configured health monitoring schedule. See ***Configure Health Monitoring Schedule*** for details.

Steps

1. Click → **System Configuration** → **Maintenance** → **Alarm Configuration** to enter the Alarm Configuration page.
2. Select camera from the device tree.
3. Enable the content(s) of the status alarm and set the alarm priority.

Note

The alarm priority defines the alert level of the alarm. The alert level ascends from Prompt all the way to High.

The following list describes the contents of the status alarm for camera.

Online Status

Detects if the device is offline.

Video Loss

Detects If video loss exists.

VQD

Detects if video quality exception exists.

Hardware Status

Detects if hardware exception such as DSP (Digital Signal Processor) exception exists.

Video Retention Days

Detects if the resources’ video retention days meet the configured standard.

Note

For details about configuring video retention standard, refer to ***Configure Health Monitoring Schedule*** .

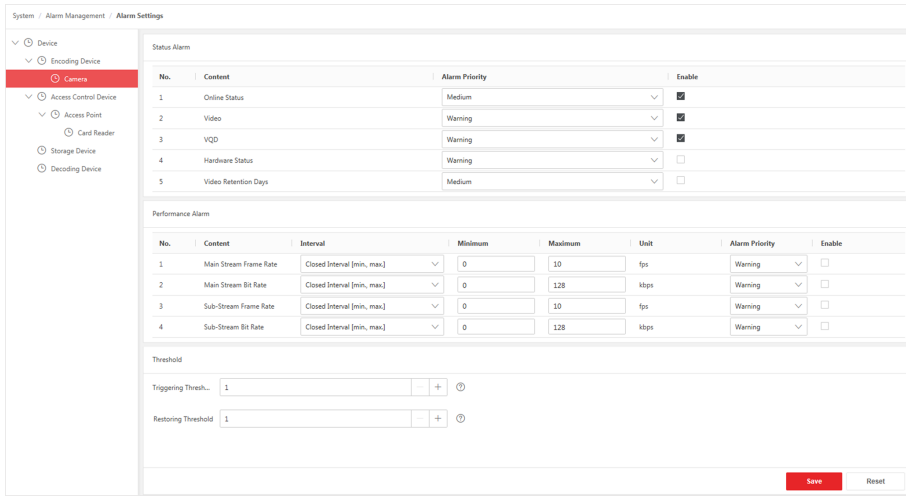


Figure 23-4 Status Alarm for Camera

4. Enable the content(s) of the performance alarm and configure the performance interval and alarm priority.

   Interval

   Select an interval type. “Interval” here refers to the interval in mathematics.

   Minimum

   Configure the minimum value of the interval.

   Maximum

   Configure the maximum value of the interval.

   Example

   If you have set the interval of main stream frame rate to Open Interval (min., max.), the minimum value to 10 fps, and the maximum value to 100 fps, when the main stream frame rate is not larger than 10 fps or not smaller than 100 fps, the system will regard this situation as an exception.

5. Set the thresholds for triggering alarm and restoring alarm.

   Triggering Threshold

   If an exception has been detected for the configured times consecutively, an alarm about the exception will be triggered.

   For example, if you set the triggering threshold of Online Status to “3”, the alarm about the online status of a camera will be triggered when the system detects the camera is offline for 3 times consecutively.

Restoring Threshold

If an exception has not been detected for the configured times consecutively, the alarm about the exception will be restored automatically.

For example, if you set the restoring threshold of Online Status to “2”, the alarm about online status of a camera will be restored when the system detects the camera is online for 2 times consecutively.

6. Click **Save**.

Configure Alarm for Access Control Device

Perform the following task to configure health monitoring alarm for access control device.

Before You Start

You should have configured health monitoring schedule. See ***Configure Health Monitoring Schedule*** for details.

Steps

1. Click → **System Configuration** → **Network** → **Configure Alarm** to enter the Configure Alarm page.
2. Select access control device from the device tree.
3. Enable the content(s) of the status alarm and set the alarm priority.

Note

The alarm priority defines the alert level of the alarm. The alert level ascends from Prompt all the way to High.

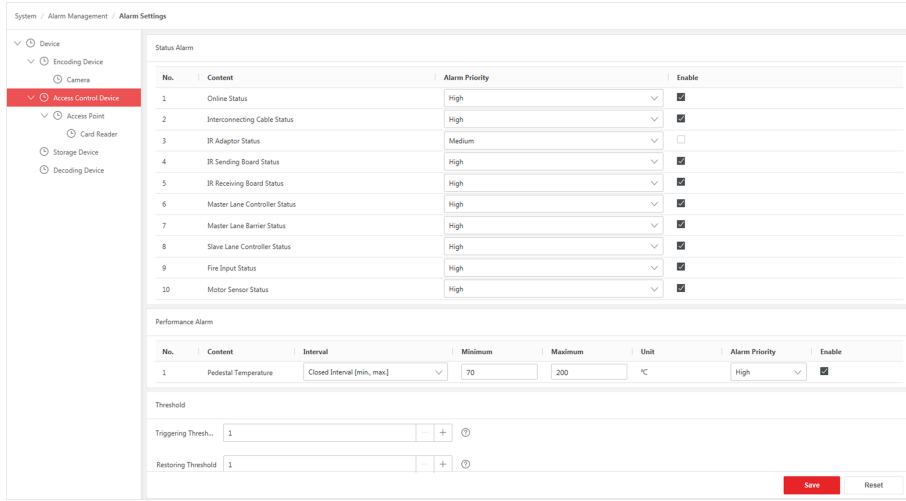


Figure 23-5 Status Alarm for Access Control Device

4. Enable the content(s) of the performance alarm and configure the performance interval and alarm priotity.

Interval

Select an interval type. “Interval” here refers to the interval in mathematics.

Minimum

Configure the minimum value of the interval.

Maximum

Configure the maximum value of the interval.

Example

If you have set the interval of the pedestal temperature to Open Interval (min., max.), the minimum value to 30 °C and the maximum value to 40 °C, when the system detects the pedestal temperature of the access control device is not higher than 30 °C or not lower than 40 °C, the system will regard this situation as an exception.

5. Set the thresholds for triggering alarm and restoring alarm.

Triggering Threshold

If an exception has been detected for the configured times consecutively, an alarm about the exception will be triggered.

For example, if you set the triggering threshold of Online Status to “3”, the alarm about the online status of an access control device will be triggered when the system detects the device is offline for 3 times consecutively.

Restoring Threshold

If an exception has not been detected for the configured times consecutively, the alarm about the exception will be restored automatically.

For example, if you set the restoring threshold of Online Status to “2”, the alarm about online status of an access control device will be restored when the system detects the device is online for 2 times consecutively.

6. Click **Save**.

Configure Alarm for Access Control Point

Perform the following task to configure health monitoring alarm for access control point.

Before You Start

You should have configured health monitoring schedule. See ***Configure Health Monitoring Schedule*** for details.

Steps

1. Click → **System Configuration** → **Network** → **Alarm Configuration** to enter the Alarm Configuration page.
2. Select access control point from the device tree.
3. Enable the content(s) of the status alarm and set the alarm priority.

Note

The alarm priority defines the alert level of the alarm. The alert level ascends from Prompt all the way to High.

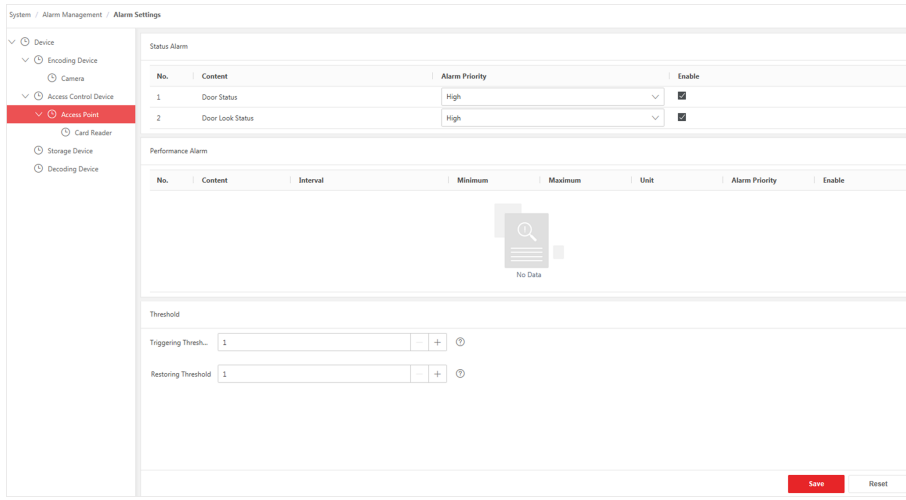


Figure 23-6 Status Alarm for Access Control Point

4. Set the thresholds for triggering alarm and restoring alarm.

   Triggering Threshold

   If an exception has been detected for the configured times consecutively, an alarm about the exception will be triggered.

   For example, if you set the triggering threshold of Online Status to “3”, the alarm about the online status of an access control point will be triggered when the system detects the access control point is offline for 3 times consecutively.

   Restoring Threshold

   If an exception has not been detected for the configured times consecutively, the alarm about the exception will be restored automatically.

   For example, if you set the restoring threshold of Online Status to “2”, the alarm about online status of an access control point will be restored when the system detects the access control point is online for 2 times consecutively.

5. Click **Save**.

Configure Alarm for Card Reader

Perform the following task to configure health monitoring alarm for the card reader.

Before You Start

You should have configured health monitoring schedule. See ***Configure Health Monitoring Schedule*** for details.

Steps

1. Click → **System Configuration** → **Network** → **Alarm Configuration** to enter the Alarm Configuration page.
2. Select card reader from the device tree.
3. Enable the content(s) of the status alarm and set the alarm priority.

   Online Status

   Detects if the card reader is offline.

   Note

   The alarm priority defines the alert level of the alarm. The alert level ascends from Prompt all the way to High.

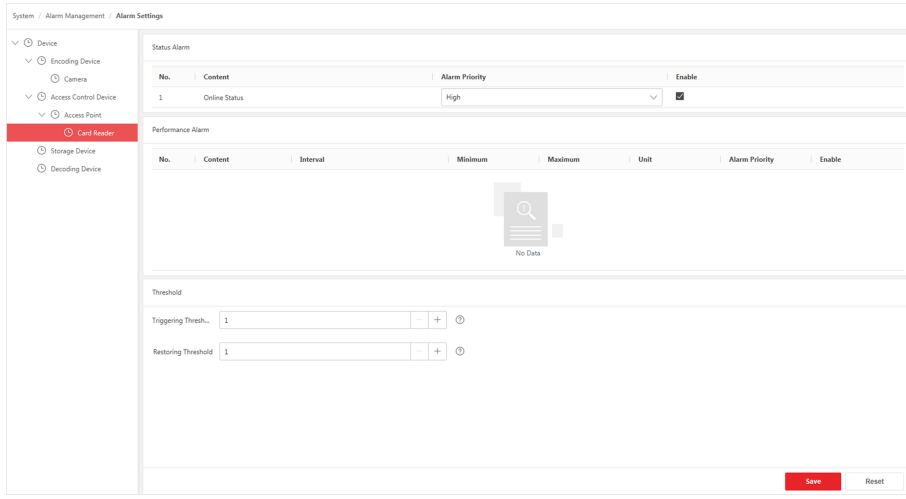


Figure 23-7 Status Alarm for Card Reader

4. Set the thresholds for triggering alarm and restoring alarm.

   Triggering Threshold

   If an exception has been detected for the configured times consecutively, an alarm about the exception will be triggered.

   For example, if you set the triggering threshold of Online Status to “3”, the alarm about the online status of a card reader will be triggered when the system detects the device is offline for 3 times consecutively.

   Restoring Threshold

   If an exception has not been detected for the configured times consecutively, the alarm about the exception will be restored automatically.

   For example, if you set the restoring threshold of Online Status to “2”, the alarm about online status of a card reader will be restored when the system detects the device is online for 2 times consecutively.

5. Click **Save**.

Configure Alarm for Storage Device

Perform the following task to configure health monitoring alarm for storage device.

Before You Start

You should have configured health monitoring schedule. See ***Configure Health Monitoring Schedule*** for details.

Steps

1. Click → **System Configuration** → **Network** → **Alarm Configuration** to enter the Alarm Configuration page.
2. Select storage device from the device tree.
3. Enable the content(s) of the status alarm and set the alarm priority.

Note

The alarm priority defines the alert level of the alarm. The alert level ascends from Prompt all the way to High.

The following list describes the contents of the status alarm for storage device.

Online Status

Detects if the device is offline.

Work Status

Detects If device exceptions, video channel exceptions, and exceptions of two-way audio channel exist.

Disk Status

Detects if disk exception exists.

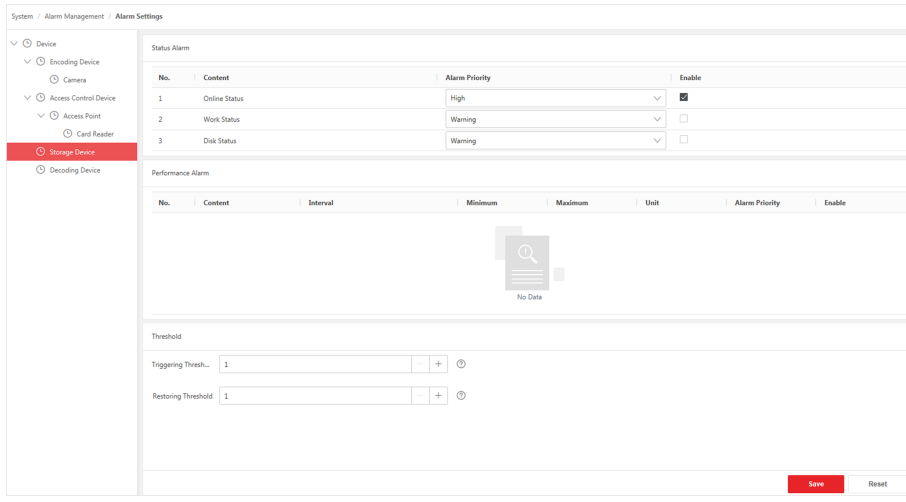


Figure 23-8 Status Alarm for Storage Device

4. Set the thresholds for triggering alarm and restoring alarm.

Triggering Threshold

If an exception has been detected for the configured times consecutively, an alarm about the exception will be triggered.

For example, if you set the triggering threshold of Online Status to “3”, the alarm about the online status of a storage device will be triggered when the system detects the device is offline for 3 times consecutively.

Restoring Threshold

If an exception has not been detected for the configured times consecutively, the alarm about the exception will be restored automatically.

For example, if you set the restoring threshold of Online Status to “2”, the alarm about online status of a storage device will be restored when the system detects the device is online for 2 times consecutively.

5. Click **Save**.

Configure Alarm for Decoding Device

Perform the following task to configure heath status alarm for decoding device.

Before You Start

You should have configured health monitoring schedule. See ***Configure Health Monitoring Schedule*** for details.

Steps

1. Click → **System Configuration** → **Network** → **Alarm Configuration** to enter the Alarm Configuration page.
2. Select decoding device from the device tree.
3. Enable the content(s) of the status alarm and set the alarm priority.

Note

The alarm priority defines the alert level of the alarm. The alert level ascends from Prompt all the way to High.

The following list describes the contents of the status alarm for decoding device.

Online Status

Detects if the device is offline.

Work Status

Detects If device exceptions, video channel exceptions, and exceptions of two-way audio channel exist.

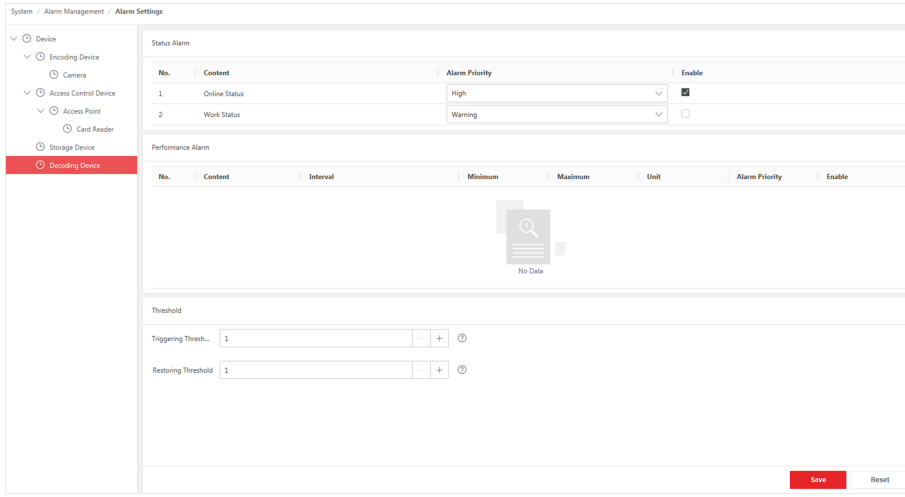


Figure 23-9 Status Alarm for Decoding Device

4. Set the thresholds for triggering alarm and restoring alarm.

   Triggering Threshold

   If an exception has been detected for the configured times consecutively, an alarm about the exception will be triggered.

   For example, if you set the triggering threshold of Online Status to “3”, the alarm about the online status of a decoding device will be triggered when the system detects the device is offline for 3 times consecutively.

   Restoring Threshold

   If an exception has not been detected for the configured times consecutively, the alarm about the exception will be restored automatically.

   For example, if you set the restoring threshold of Online Status to “2”, the alarm about online status of a decoding device will be restored when the system detects the device is online for 2 times consecutively.

5. Click **Save**.

23.2.4 Monitor Health Status of Subordinate System

You can add system A as a subordinate system to system B. You can also synchronize health monitoring data of a subordinate system to the current system so as to view the subordinate system’s data and do data statistics.

Steps

Note

For details about statistics of health monitoring data, refer to ***Video Resource Maintenance*** .

1. Click → **System Configuration** → **Maintenance** → **Subordinate System** to enter the Subordinate System Configuration page.

2. Click **Add** to enter the Add Subordinate System page.
3. Set the required information.

   System IP Address

   Enter the IP address of the subordinate system.

   System Port

   Enter the port number of the subordinate system.

   Subordinate Gateway IP Address

   Enter the IP address of the subordinate gateway.

   Cascading Type

   Select the type(s) of cascading data you required. The current system will get the selected type(s) of heath monitoring data from the subordinate system.

   Get Cascading Data

   Enable or disable the current system to get health monitoring data from the selected subordinate system.
4. **Optional:** Click **Test** to test if the subordinate system can be synchronized.
5. Click **OK**.

   The subordinate system will be displayed on the subordinate system list.
6. **Optional:** Perform the following operations.
   - Click **Get the Latest Status** to get the latest online status of the subordinate system.
   - Click to synchronize the latest data from the subordinate system.

23.2.5 Configure Resources in Whitelist

False alarms may be triggered from some resources under health monitoring because of special events such as municipal construction, power outage, and network outage. In such cases, you can add specific resources to the whitelist to prevent the occurrence of false alarms. For example, assume that your office building is deployed with the HikCentral Enterprise-Commercial system and you have configured health monitoring schedules for the devices in the building, if the power supply of the fifth floor is about to cut off next week due to certain event, you can add all the devices in the fifth floor to the whitelist and set next week as the effective period of the settings to avoid the disturbance of potential false alarms next week.

Steps

1. Click on the Home page, and then go to **System Configuration → Maintenance → Whitelist** to enter the whitelist configuration page.
2. Click **Add**.
3. Select the area where the resources locate.

   The resources in the selected area will appear in the To be Added list.
4. Select resource(s) from the To be Added list.
5. Click to add the selected resource(s) to the Added list.

6. Select resource(s) from the Added list.
7. Set the supplementary information.

   Reason for Adding

   Enter the reason why you add the resource(s) to the whitelist.

   Effective Date

   Set the date (and precise time point) when the whitelist settings of the selected resource(s) start taking effect, i.e., the start time of the effective period.

   Expiry Date

   Set the date (and precise time point) when the whitelist settings of the selected resource(s) expire, i.e., the end time of the effective period.
8. Click **Add to Whitelist**.

23.3 Video Resource Maintenance

The Maintenance module provides information about the health status of the resources added to the system. You can check overall and detailed health status of all the resources, search and acknowledge health status alarms, generate reports about resource health status, as well as monitor resource health status via topology.

23.3.1 Status Overview

You can view the status overview of the managed resources, including total number of cameras, total camera online rate, video image normal rate, and recording normal rate. It also provides charts for the resource running status of different areas, camera running status tendency, and video exceptions. You can also perform quick check of overall health status.

Note

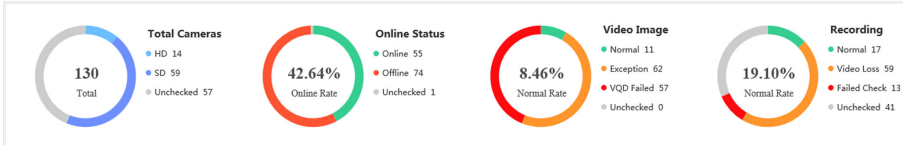
You should have configured health monitoring schedule.

On the Home page, click **Maintenance → Overview** to enter the Status Overview page, and then select an area from the drop-down box on the upper-left of the page to view the status overview of the resources in the selected area.

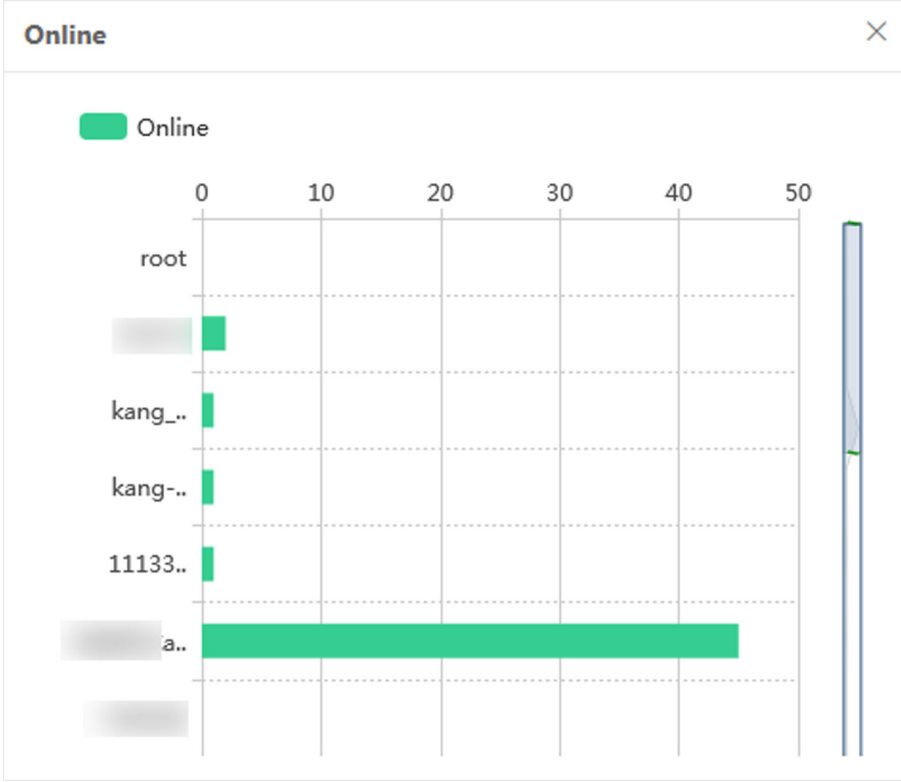
Doughnut Chart

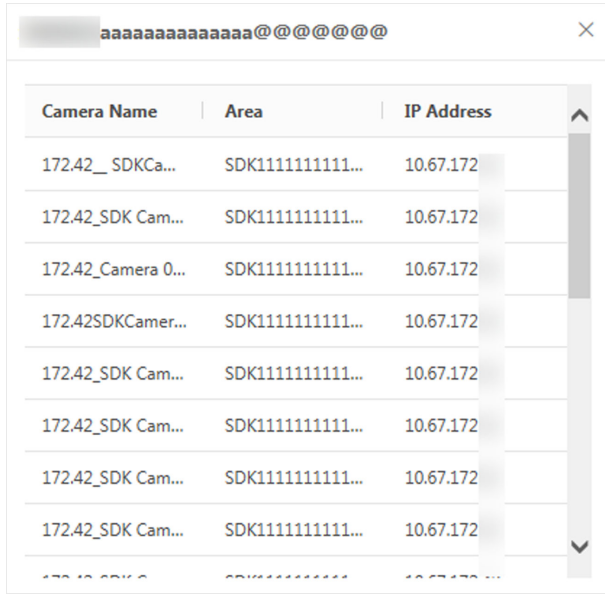
The doughnut charts on the top of the Operation and Maintenance page show total number, online rate, video image normal rate, and recording normal rate of the cameras in the selected area. You can view the details of the doughnut charts.

The doughnut charts are displayed as follows.



You can click the rings to view the statistic details displayed in a histogram chart. For example, you can click the green part in the Online Status doughnut chart, and then the histogram chart will be displayed, which shows the online camera number in each subordinate area of the selected area. You can click a column in the histogram chart to view the details of the online cameras in the selected subordinate area.

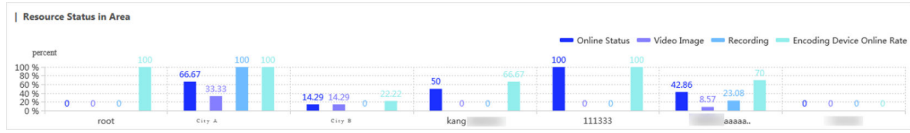




View Resource Status in Area

The resource status, including camera online rate, image normal rate, recording normal rate, and encoding device online rate of each subordinate area of the selected area are displayed in histogram chart.

The histogram chart is displayed as follows.



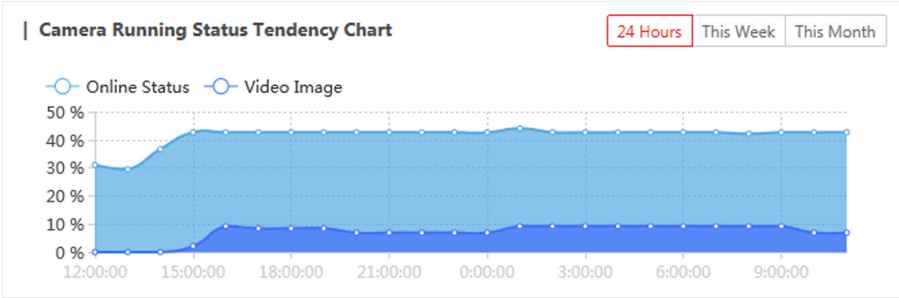
You can perform the following operations on the chart.

- Click a legend to show or hide the column.
- Move the cursor to a column to view the camera online rate, image normal rate, recording normal rate, and encoding device online rate of the selected subordinate area.
- Click the column to view the resource offline details or exception details.

Camera Status Tendency Chart

The camera status tendency chart shows the variation tendency of the camera online rate and image normal rate in a specific period.

The camera status tendency chart is displayed as follows.



You can perform the following operations on the chart.

- Select a time period for the statistics.

  24 Hours

  Display the camera online rate and image normal rate in each time point within 24 hours.

  This Week

  Display the camera online rate and image normal rate in each time point in the current week.

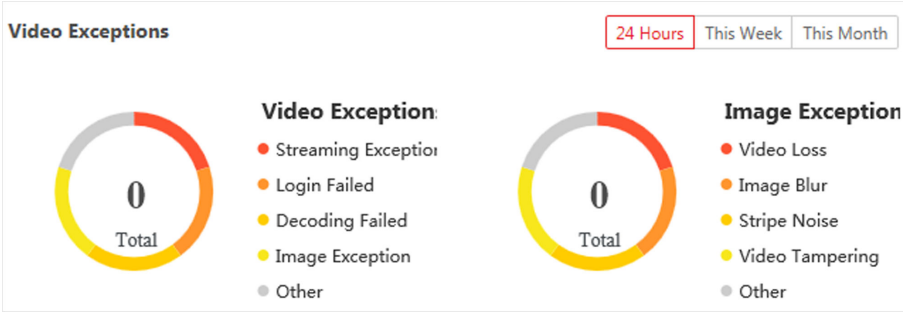
  This Month

  Display the camera online rate and image normal rate in each time point in the current month.
- Click the legend to show or hide the tendency line of the camera online status and video image normal rate.
- Move the cursor to a time point in the tendency line to view the camera online rate and video image normal rate on the time point.

Video Exceptions

The doughnut charts in the Video Exceptions section shows different types of video exceptions and images exceptions in a specific time period.

The doughnut charts are displayed as follows.



You can perform the following operations on the charts.

- Select a time period for the statistics.

  24 Hours

  Display the camera online rate and image normal rate in each time point within 24 hours.

This Week

Display the camera online rate and image normal rate in each time point in the current week.

This Month

Display the camera online rate and image normal rate in each time point in the current month.

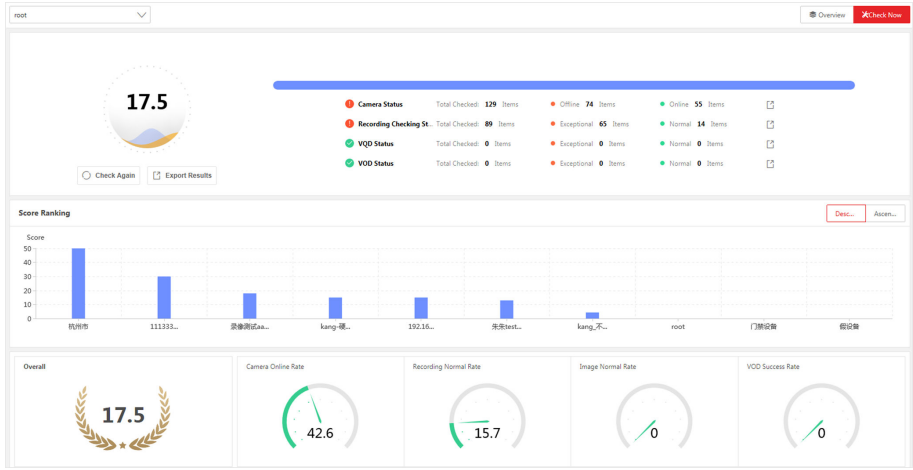
- Click the legend to show or hide the statistics of the selected type of exception in the doughnut chart.
- Move the cursor to the ring to view the statistics of the selected type of exception. For example, you can move the cursor to the Streaming Exception part in the Video Exception chart to view the number of cameras with streaming exceptions and the proportion of these cameras.
- Click the ring to view the exception details.
  For example, you can click the Video Loss part in the Image Exception chart to view the details of the cameras on which video loss occur, including camera name, area, and camera IP address.

Quick Check of Overall Health Status

You can view the latest overall health status of resources in the system by one-click.

Steps

1. Click **Check Now** on the Operation and Maintenance page to check the overall health status.
   The results will be displayed, including the overall health score, score rankings of different areas, scores of different checking items, etc.



2. **Optional:** Perform the following operations
   - Click to export the details of the selected type of exception to the local PC.
   - Click **Export Result** to export all the checking results to the local PC.
   - Click **Descending** or **Ascending** in the Score Ranking section to range the score of different areas in descending order or in ascending order respectively.

- Move the cursor to a specific column in the Score Ranking histogram chart to view the health score of resources in a specific area.
- Move the cursor to the pointers in the gauge charts at the bottom of the page to view the scores of different checking items.
  For example, you can move the cursor to the pointer of Camera Online Rate chart to view the score of camera online rate.

23.3.2 Status Monitoring

The Status Monitoring (Video) module provides detailed information about camera online status, video quality diagnosis, recording status, as well as the status of encoding device, storage device, and decoding device. System topology is also provided for monitoring resources in the topology you defined.

Camera Online Detection

You can view the online status, recording status, and VOD status of the cameras in a specific area. You can also export the status information to the local PC.

Steps

1. On the Home page, Click **Status (Video)** in the Maintenance section and then click **Camera → Online Detection** to enter the Online Detection page.
2. Select an area from the area list.

   The total camera number, online camera number, and offline camera number, HD camera number, SD camera number in the selected area, as well as a detailed list of the cameras in the area will be displayed.
3. **Optional:** Uncheck **Include Sub-Area** to ignore the camera status information of the subordinate areas of the selected area.
4. **Optional:** Perform the following operations.

   View in Doughnut Chart

   Click to view the overall status in doughnut chart.

   Filter Camera

   Set the filtering conditions, such as online status, camera IP address, and VOD status, and then click **Search**.

   Get Latest Status

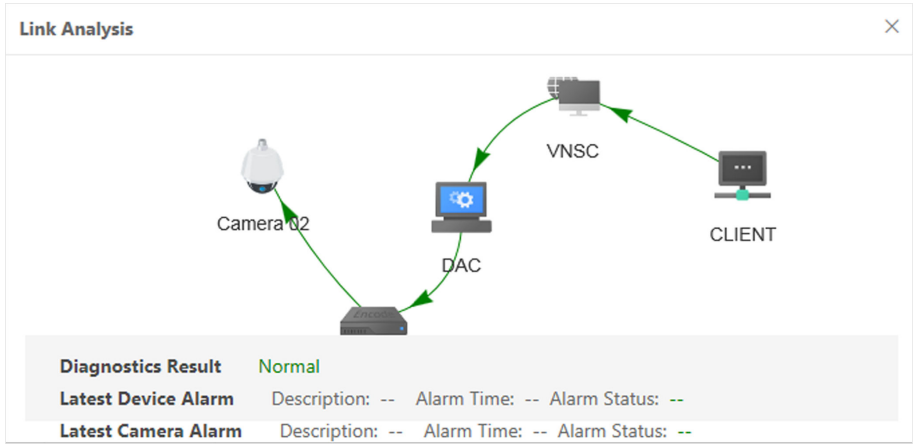
   Click to get the latest status of the selected camera.

   Link Analysis

   Click to analyze the link status of the selected camera. you can also view the latest device alarm and latest camera alarm in the pop up window shown as follow.

Note

Link here refers to the communication channel that connects two or more devices.



View Details of a Camera

Click to view the details of the selected camera, including the basic information and history status.

You can click to set a time period to filter the history status on the Details page.

Export Camera Status

Click **Export** to export the status information of all the found cameras to the local PC.

Video Quality Diagnosis

You can view the video quality diagnosis results of the cameras in a specific area. You can also export the results to the local PC.

Steps

1. On the Home page, Click **Status Monitoring (Video)** in the Maintenance section and then click **Camera → Video Quality Diagnosis** to enter the VQD page.
2. Select an area from the area list.

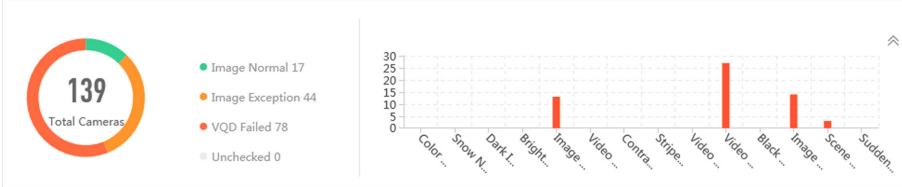
   The video quality diagnosis results of the cameras in the selected area will be displayed.
3. Uncheck **Contain Subordinate Area** to ignore the video quality diagnosis results of the subordinate areas of the selected area.
4. Perform the following operations.

   View Overall Diagnosis Results in Charts

   Click to view the overall diagnosis results in doughnut chart and histogram chart.

   The doughnut chart displays the number of cameras whose images area normal, the number of cameras with image exceptions, the number of cameras whose video quality diagnosis failed, and the number of unchecked cameras.

The histogram chart displays the camera number of each type of image exception.



Filter Cameras

Set the filtering conditions, such as diagnosis result, camera IP address, and exception reason, and then click **Search**.

Switch Between List Mode and Thumbnail Mode

Click ☰ or ⊞ to switch the camera list to list mode or thumbnail mode respectively.

Recheck video Quality of All Cameras

Click **Recheck All** to recheck video quality of all cameras in the selected area.

Recheck video Quality of a Single Camera

Click to recheck video quality of the selected camera.

View Exception Related Picture

Click to view the exception related picture of the selected camera.

View Diagnosis Result Details

Click to view the exception related picture of the selected camera.

In history diagnosis, you can click to select a month to view the history information.

Recording Check

You can view the recording status of the cameras in a specific area, such as video retention days, recording interruption, and unrecorded duration. You can also export the recording status of the cameras to the local PC.

Steps

1. On the Home page, Click**Status (Video)** in the Maintenance section and then click **Camera** → **Recording Check** to enter the Recording Check page.
2. Select an area from the area list.

   The retention status of the cameras in the selected area will be displayed.
3. **Optional:** Uncheck **Include Sub-Area** to ignore the recording status of the cameras in the subordinate areas.
4. **Optional:** Perform the following operations.

   View Overall Recording Status in Doughnut Chart

Click to view the overall diagnosis results in doughnut chart and histogram chart, which displays number of cameras whose recording status are normal, the number of cameras with video loss, the number of checking-failed camera, and the number of camera whose recording status are unknown.

Filter Cameras

Set the filtering conditions, such as recorded date (required), camera IP address, and storage type, and then click **Search**.

Export Recording Status

Click **Export** to export the recording status of the all the cameras in the area to the local PC.

View Recording Status Details

Click to view the recording status details of the selected camera, including the basic information and the timeline table shows below.

You can move the cursor on the timeline to view the detailed duration of exception.

Device Status

You can view the status of encoding devices, storage devices, and decoding devices respectively. The status information including online status, offline duration, device password strength, disk status (for encoding device and storage device), etc.

Steps

1. On the Home page, Click**Status (Video)** in the Maintenance section and then click **Device → Encoding Device** , **Device → Storage Device** or **Device → Decoding Device** to enter the status page.
2. Select an area from the area list.

   The retention status of the devices in the selected area will be displayed.
3. **Optional:** Uncheck **Include Sub-Area** to ignore the status of the cameras in the subordinate areas.
4. **Optional:** Perform the following operations.

   View Status in Chart

   Click to view the statues of the devices in chart(s).

   Filter Device

   Set the required filtering condition and then click **Search**.

View Details

Click to view the details of the device status, such as basic information and history status.

In History Status section, you can click to set a time period to filter the history information.

Export Status Information

Click **Export** to export the status information to the local PC.

23.3.3 Topology

Topology shows the links between devices added to the system, or in other words, the structure of the system. It helps you troubleshoot system faults and exceptions. You can draw system topology and check the abnormal devices in the topology.

Draw and Editing Topology

You can draw and edit topology according to actual needs.

Steps

1. On the Home page, Click **Status (Video)** in the Maintenance section and then click **Camera → Topology** to enter the Topology page.
2. Add a view.
   a. Click + to open the Add View window.
   b. Create a view name.
   c. Select topology type.

      Gravity Canvas

      The elements added to the gravity canvas will adjust their positions automatically when you save the topology.

      Static Canvas

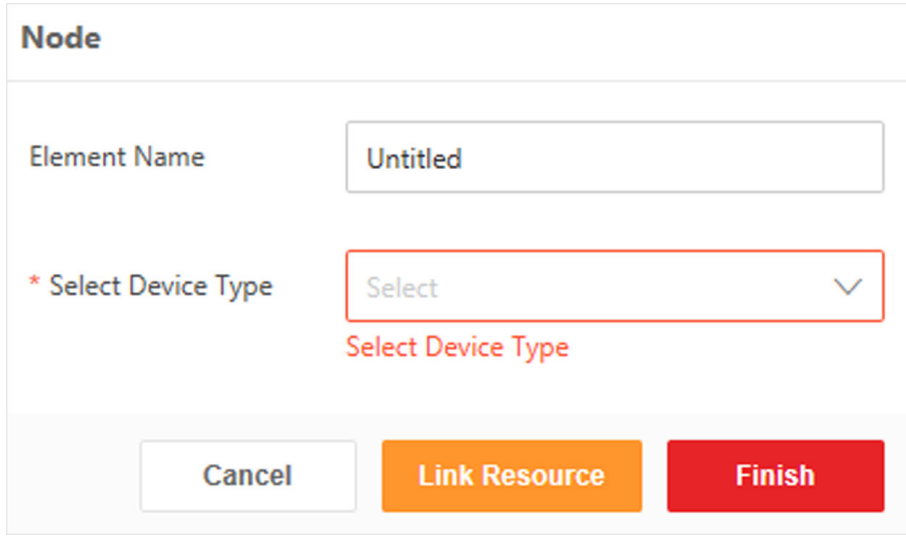
      The elements added to the gravity canvas will NOT adjust their positions automatically. You should adjust the element positions manually.

   d. Select a parent topology if a view has already been added.

      Note

      Select **Root** if you need to create a new view equal to the existed view in terms of cascading level. Select a specific type of element if you need to create a topology as the sub-topology of the element.

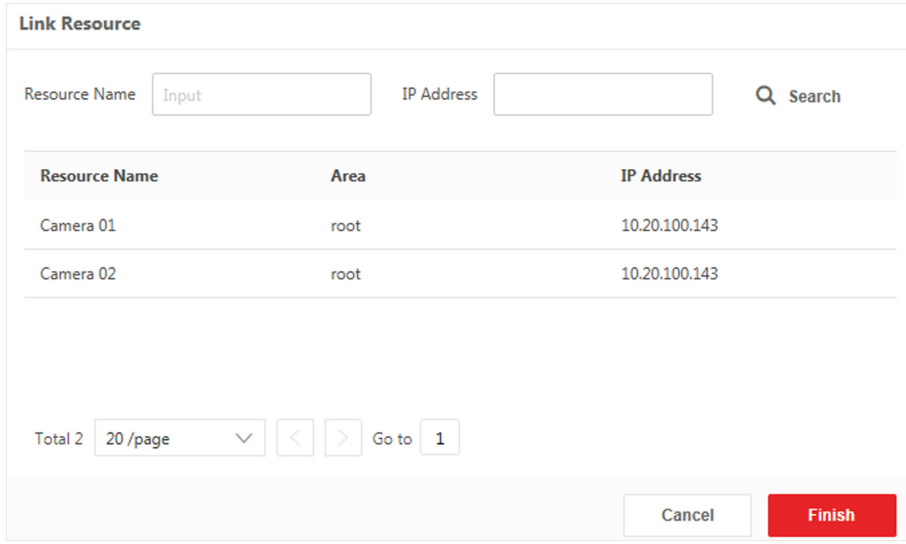
   e. Click **OK**.
3. Select the view and click **Edit Topology** to enter the editing mode.
4. Add elements to the view.
   - Click **Add Node** and click any empty place on the view, and then create a name for the node and select a device type on the pop-up Node window as follows.



- Drag an element from the element library to the view, select the element and then click **Edit** to open the Node window.

5. Link a resource to the element.

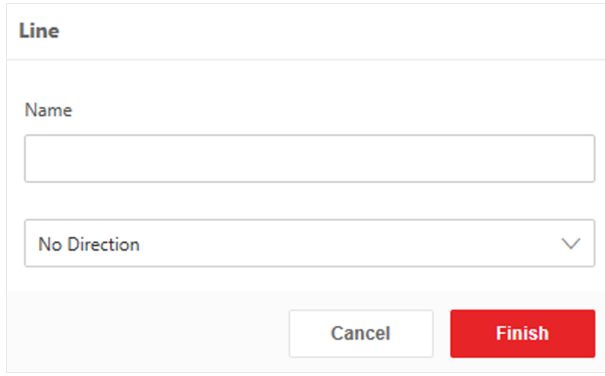
1) Click **Link Resource** on the Node window to open the Link Resource window.



2) **Optional:** Enter the name and IP address of a specific device to search for the device.
3) Double-click a device to link it with the element.
4) Click **Finish**.

6. Draw lines between elements.

1) Click **Add Edge**.
2) Select a node as the start point of the line, and then drag the line to another element. The Line window pops up.



3) **Optional:** Create a name for the line.
4) Set the direction of the line from the drop-down list.
5) Click **Finish**.

7. Click **Save Topology**.

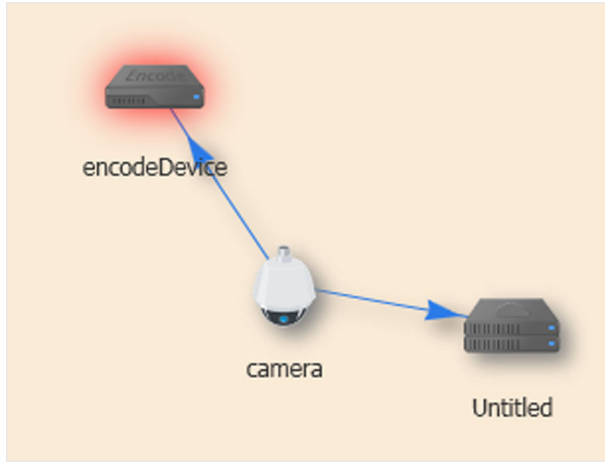
Monitoring via Topology

After drawing the system topology, you can monitor the devices in the system via topology.

Steps

1. On the Home page, Click **Status (Video)** in the Maintenance section and then click **Camera → Topology** to enter the Topology page.
2. Click a view in the View library to open the topology of the view.

   If exception occurs on the linked resource of an element, the element will flash in red.



3. Double-click the element flashing in red to open the Details window.

   You can view the alarm time and related description.
4. If sub-topology exists under the element, click **Sub-Topology** on the Details window to enter the sub-topology.

23.3.4 Report

The Report module provides different reports about the resource health status, including the report of the overall resource health status in different areas, the video quality report, the recording status report, streaming status report, etc. You can set time period to generate the reports, as well as export the report details to the local PC.

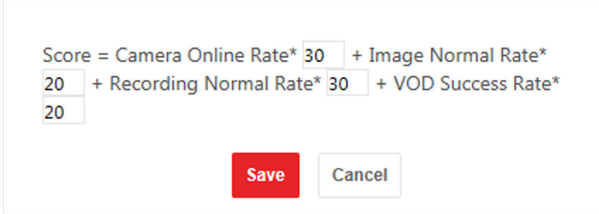
Area Overview Report

Area overview report displays the camera online rates, recording normal rates, image normal rates, VOD success rates of different areas, as well as the rankings of the areas in terms of their resources' overall health scores.

Perform the following task to generate the area overview report.

Steps

1. On Home page, click **Report** in the Maintenance section and then click **Area Overview** to enter the Area Overview Report page.
2. Select an area from the area list.
3. **Optional:** Click **Weight** and then adjust the weight coefficient values of the parameters for calculating the resource health score of a subordinate area.



Note

You can move the cursor to **Formula** to view the formulas to calculate four types of health rates respectively, including camera online rate, image normal rate, recording normal rate, and VOD success rate.

4. Select **Month** or **Custom** to set the time period mode for generating the report.
5. Set the time period for generating the report.
   - If you select **Month** in the previous step, click to select a month for generating the report.
   - If you select **Custom** in the previous step, click to customize a time period for generating the report.
6. Click **Generate** to generate the report.

   The generated report includes a histogram chart and a table.
   - The top 10 areas, as well as their camera online rate, image normal rates, recording normal rates, and VOD success rates will be displayed in the histogram chart.
   - The details of all subordinate areas are displayed in the Area Report Details table.

7. **Optional:** Perform the following operations after generating the report.
   - Move the cursor on the histogram chart to view the precise values of the above-mentioned four types of health rates.
   - Click the legend on the histogram chart to show or hide the corresponding health rate. For example, you can click  to hide the camera online rate of each area.
   - Click **Export** to export the report details to the local PC.

Video Quality Report

Video quality report displays the video quality information of different areas, as well as the rankings of the areas in terms of the image normal rate.

Perform the following task to generate the video quality report.

Steps

1. On Home page, click **Report** in the Maintenance section and then click **Video Quality** to enter the Video Quality Report page.
2. Select an area from the area list.

   The report will be generated.

   The generated report includes a histogram chart and a table.
   - The top 10 areas in terms of the image normal rates will be displayed in the histogram chart.

     Note

     You can move the cursor to **Formula** to view the formula to calculate the image normal rate.
   - The details of all subordinate areas are displayed in the Video Quality Details table.

     Not Configured

     The Not Configured column in the table displays the number of resources whose health monitoring schedules doesn't contain video quality diagnostics.
3. Click **Export** to export the report details to the local PC.

Recording Status Report

Recording status report displays the recording status of different areas, as well as the rankings of the areas in terms of the recording normal rate.

Perform the following task to generate the recording status report.

Steps

1. On Home page, click **Report** in the Maintenance section and then click **Recording Status** to enter the Recording Status Report page.
2. Select an area from the area list.
3. Select **Month** or **Custom** to set the time period mode for generating the report.

4. Set the time period for generating the report.
   - If you select **Month** in the previous step, click to select a month for generating the report.
   - If you select **Custom** in the previous step, click to customize a time period for generating the report.
5. Click **Generate** to generate the report.

   The generated report includes a histogram chart and a table.
   - The top 10 areas in terms of recording normal rate will be displayed in the histogram chart.
   - The details of all subordinate areas are displayed in the Recording Normal Rate Details table. In the table, you can view the recording normal rate of each area in the time period you set, as well as the recording normal rate of each area in each day within the time period.
6. **Optional:** Perform the following operations after generating the report.
   - Move the cursor on the histogram chart to view the precise values of the recording normal rates of the top 10 areas.
   - Click a specific area name in the table to view the recording normal rate of each camera in the area.
   - Click **Export** to export the report details to the local PC.

Streaming Status Report

Streaming status report displays the streaming status of different areas, as well as the rankings of the areas in terms of the streaming normal rate.

Perform the following task to generate the streaming status report.

Steps

1. On Home page, click **Report** in the Maintenance section and then click **Streaming Status** to enter the Streaming Status Report page.
2. Select an area from the area list.
3. Select **Month** or **Custom** to set the time period mode for generating the report.
4. Set the time period for generating the report.
   - If you select **Month** in the previous step, click to select a month for generating the report.
   - If you select **Custom** in the previous step, click to customize a time period for generating the report.
5. Click **Generate** to generate the report.

   The generated report includes a histogram chart and a table.
   - The top 10 areas in terms of recording normal rate will be displayed in the histogram chart.
   - The details of all subordinate areas are displayed in the Streaming Status Details table. In the table, you can view the duration (unit: second) of streaming exceptions (such as key frame latency), the total streaming times, the streaming-succeeded times, and the streaming success rate of each camera in the selected area.
6. Perform the following operations after generating the report.

- Move the cursor on the histogram chart to view the precise values of the streaming success rates of the top 10 areas.
- Click **Export** to export the report details to the local PC.

Camera Status Report

Camera Status report displays the camera status (online and offline) of different areas, as well as the rankings of the areas in terms of the camera online rate.

Perform the following task to generate the camera status report.

Steps

1. On Home page, click **Report** in the Maintenance section and then click **Camera Status** to enter the Camera Status Report page.
2. Select an area from the area list.

   The report will be generated, which includes a histogram chart and a table.
   - The top 10 areas in terms of camera online rate will be displayed in the histogram chart.

     Note

     You can move the cursor to **Formula** to view the formula for calculating camera online rate.
   - The details of all subordinate areas are displayed in the Camera Status Details table. In the table, you can view the number of online camera, offline camera, high definition camera, standard definition camera, and unchecked camera respectively.
3. **Optional:** Perform the following operations after generating the report.
   - Move the cursor on the histogram chart to view the precise values of the camera online rates of the top 10 areas.
   - Click **Export** to export the report details to the local PC.

Video Retention Status Report

Video retention status report displays the video retention status of different areas, as well as the rankings of the areas in terms of video retention qualified rate. "Video retention qualified" means the number of retention days of a camera's recorded videos reaches the configured standard.

Before You Start

Note

You can configure the video retention days when configure health monitoring schedule.

Perform the following task to generate the video retention status report.

Steps

1. On Home page, click **Report** in the Maintenance section and then click **Video Retention Status** to enter the Video Retention Status Report page.
2. Select an area from the area list.

   The report will be generated, which includes a histogram chart and a table.

   - The top 10 areas in terms of video retention qualified rate will be displayed in the histogram chart.

     Note

     You can move the cursor to **Formula** to view the formula for calculating video retention qualified rate.

   - The details of all subordinate areas are displayed in the Video Retention Status Details table. In the table.
3. Perform the following operations after generating the report.
   - Move the cursor on the histogram chart to view the precise values of video retention rates of the top 10 areas.
   - Click **Export** to export the report details to the local PC.
   - Click the detailed numbers (except 0) in the Retention Disqualified Cameras column to view the details of the cameras whose video retention days haven't reached the configured standard.

23.4 One-Card Resource Maintenance

You can monitor the running status of the one-card resources, including access control devices (and related card readers and access control points), video intercom devices, and elevator control devices (and related card readers). The running status information includes device online status, exception device number, offline device number, etc.

23.4.1 View Access Control Resource Running Status

You can view the running status of the access control devices and the related card reader and access control points. The running status includes offline device number, device online rate, component status, access control point's working status, etc.

Steps

Note

The operations for viewing the running status of the access control device, card reader, and access control point are similar. Hera we only introduces the operations for viewing the running status of access control point.

1. Click **Status (1-Card)** in the Maintenance section of the Home page, and then go to **Access Control → Access Control Point** .
2. Select an area from the area list.

   The access control points in the selected area will appear.
3. Perform the following operations.

View Status Overview via Charts	Click ⌄ to view the overview of the running status of the access control points in the selected area via the doughnut chart. You can click the rings on the doughnut chart to view the number of access control points in normal status, access control points remained close, access control points remained open, and unchecked devices respectively. **Note** The access control points in normal status refer to the access control points that are locked or unlocked. • Unlock: When the door is locked, unlock the door and it will be open. After the door open duration, 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). • 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.
View Status of Devices in Lower-Level Area	Check **Include Lower-Level Area** on the upper-right of the page to view status of the access control points in the lower-level areas of the selected area.
Search Devices	Set search conditions (working status, access control point name, and parent controller), and then click **Search**.
Export Search Results	Click **Export** to export the search results to the local PC.
Refresh Device List	Click **Refresh** to refresh the device list.
View Status Details of Single Device	Click ▤ to view the detailed status of the selected device.

23.4.2 View Video Intercom Resource Running Status

You can view the running status of the video intercom resources (door station, indoor station, master station, and outer door station), including offline device amount, device online rate, and online status.

Steps

Note

The operations for viewing the running status of door station, indoor station, master station, and outer door station are similar. Here we only introduces the operations for viewing the running status of indoor station.

1. Click **Status (1-Card)** in the Maintenance section of the Home page, and then select **Video Intercom → Indoor Station** .
2. Select an area from the area list.

   The indoor stations in the selected area appears.
3. **Optional:** Perform the following operations.

View Status Overview	Click to view the overview of the running status of the indoor stations of the selected area in doughnut chart. You can move cursor to the ring of the doughnut chart to view the details such as online device number and onfline device number.
View Status of Devices in Lower-Level Area	Check **Include Lower-Level Area** on the upper-right of the page to view status of indoor stations in lower-level area.
Search Devices	Set filter conditions (including online status, device name, device type, and device IP address), and then click **Search**.
Export Search Results	Click **Export** to export the search results to the local PC.
Refresh Device List	Click **Refresh** to refresh the device list.
View Status Details of Single Device	Click to view the detailed status of the selected device.

23.4.3 View Elevator Control Resource Running Status

You can view the running status of the elevator control resources (elevator control devices and related card readers), including offline device number, device online rate, and exception device number.

Steps

Note

The operations for viewing the running status of elevator control devices and card readers are similar. Here we only introduces the operations for viewing the running status of card readers.

1. Click **Status (1-Card)** in the Maintenance section of the Home page, and then select **Elevator Control → Card Reader** .
2. Select an area from the area list.

   The card readers in the selected area appears.
3. **Optional:** Perform the following operations.

View Status Overview	Click to view the overview of the running status of the indoor stations of the selected area in doughnut chart. You can move cursor to the ring of the doughnut chart to view the details such as online device number, offline device number, online rate, etc.
View Status of Devices in Lower-Level Area	Check **Include Lower-Level Area** on the upper-right of the page to view status of indoor stations in lower-level area.
Search Devices	Set filter conditions (including online status, component status, parent controller, etc), and then click **Search**.
Export Search Results	Click **Export** to export the search results to the local PC.
Refresh Device List	Click **Refresh** to refresh the device list.
View Status Details of Single Device	Click to view the detailed status of the selected device, including running status, component status, history status, etc.

23.5 Alarm Search

You can search the alarms of resource health status. You can also handle the alarms if you have handled the related exceptions.

Before You Start

You should have configured alarms for resource health status.

Steps

1. Click **Alarm Search** in the Maintenance section of the Home page to enter the Alarm Search page.
2. Select an area from the area list on the left.

   The total number of the new alarms, as well as the number of alarms of different types in the selected area will be displayed on the upper side of the Alarm Search page.

Status

The number of the status alarm.

Recording

The number of the alarm related to recording.

3. **Optional:** Check **Contain Subordinate Area**.

The alarms of subordinate areas of the selected area will be displayed.

4. Set filtering conditions for the search.

Status

Pending

The alarm is not acknowledged by the user.

Restored

The alarm is acknowledged by the user.

Alarm Source Name

The name of the resource in which the alarm is triggered.

Alarm Source Type

The type of the resource in which the alarm is triggered.

Alarm Priority

The alert level of the alarm.

Note

You can set alarm priority for the alarm related to resource health status.

Alarm Time

The date when the alarm is triggered. Click to select a date.

Restored Time

The date when the alarm is restored. Click to select a date.

5. Click **Search**.

The search results will be displayed.

6. **Optional:** Perform the following operations after search.

Acknowledge a Specific Alarm

Click in the Operation column to acknowledge the selected alarm.

Batch Acknowledge Alarms

Select alarms and then click **Acknowledge** to batch acknowledge the selected alarms.

Delete a Specific Alarm

Click in the Operation column to delete the selected alarm.

Batch Delete Alarms

Select alarms and then click **Delete** to batch delete the selected alarms.

View Alarm Details

Click  in the Operation column to view the details of the selected alarm.

You can view the basic information of the alarms, as well as the information of the alarm's history status (pending or acknowledged).

Export Search Results

Click **Export** to export the information of the found alarms.

Chapter 24 Advanced Parameters Settings

You can set the advanced parameters, including the device time synchronization, user security policy, and user experience program.

24.1 Synchronize Device Time

The asynchronous time between the system and the devices may lead to some abnormal results, such as discontinuous recording time, the time deviation for card swiping, etc. The system provides auto time synchronization function. The added devices can synchronize their time with the system via a NTP server, which needs to be configured in the Operation and Management Center.

Steps

1. Click → **System Configuration** → **Advanced Parameter** to enter Advanced Parameter Configuration page.
2. Click **Synchronize Device Time** tab.
3. Set **Synchronize Device Time** switch to on to enable this function.
4. Select the interval for auto time synchronization.
5. Click **Save**.

   NTP server will synchronize the time between the system and the devices according to the internal automatically.

24.2 Set User Security

In order to increase the security of your system, you'd better to set security policy about user password. You can set the valid password period depending on your environment, so that you must change your password within the period. This will restrict the time for Internet attackers to crack password or access network resources.

Steps

1. Click → **System Configuration** → **Advanced Parameter** to enter Advanced Parameter Configuration page.
2. Click **User Security Settings** tab.
3. Set **Enable Maximum Password Age** switch to on to force the user to change the password when password expires.
4. Select a maximum period that the password is valid.

   Note

   Before deadline of this period, you will have to change the password.

5. Click **Save**.

24.3 Join User Experience Program

User experience program is a way for users to share their information with the service provider in order to help to improve the product or service. It is recommended that you join the program, so the information of projects deployed in external networks will be collected for the purpose of pushing security patches to make sure the project is safe and steady.

Steps

1. Click → **System Configuration** → **Advanced Parameter** to enter Advanced Parameter Configuration page.
2. Click **User Experience Program** tab.
3. Set **Join Program** switch to on.
4. Click **Save**.

Chapter 25 Menu Customization

After customizing and synchronizing menu on the Operation and Management Center, you can synchronize the menu settings to the Web Client. When the menu is changed on the Operation and Management Center, you can also perform this task to synchronize the changes.

Before You Start

You should configure the menu on the Operation and Management Center first.

Steps

1. Click to enter System Configuration page.
2. Click **Interface Customization → Menu Customization** .
3. Click **Synchronize**.

Chapter 26 Get OpenAPI Document

You can visit the OpenAPI Document Center to view interface information.

Enter ***https://IP Address of Central Management Service (CMS)/artemis-portal/*** in the address bar of the browser to visit the OpenAPI Document Center.

Note

IP Address of Central Management Service (CMS) is a variable. Replace it with the IP address of the CMS of your system.


See Far, Go Further