



**HikCentral Enterprise**  
**Web Client**

**User Manual**

## **User Manual**

COPYRIGHT ©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

### **ALL RIGHTS RESERVED.**

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be “Hikvision”). This user manual (hereinafter referred to be “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

## **About this Manual**

This Manual is applicable to HikCentral Enterprise Web Client.

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 in the company website (<http://overseas.hikvision.com/en/>).

Please use this user manual under the guidance of professionals.

## **Trademarks Acknowledgement**

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

## **Legal Disclaimer**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. 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.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

# Contents

Chapter 1	Overview.....	9
1.1	About This Document.....	9
1.2	Introduction.....	9
Chapter 2	System Requirement .....	10
2.1	Service Requirement .....	10
2.2	Web Browser Requirement .....	10
Chapter 3	Login .....	11
Chapter 4	Getting Started .....	12
4.1	Person Management .....	12
4.1.1	Manage Organization .....	12
4.1.2	Set Fields of Basic Person Information .....	14
4.1.3	Set Parameters for Biometric Features Collection Device .....	14
4.1.4	Add Single Person.....	15
4.1.5	Import Multiple Persons .....	15
4.1.6	Export Added Persons .....	16
4.1.7	Restore Deleted Persons .....	16
4.2	Role and User Management .....	17
4.2.1	Add Role .....	17
4.2.2	Manage User Group .....	18
4.2.3	Add Single User .....	19
4.2.4	Import Multiple Users .....	20
4.2.5	Synchronize Users from Windows Domain .....	20
4.2.6	Export Users .....	21
4.3	Manage Registered Vehicles.....	21
4.3.1	Register a Vehicle to HikCentral Enterprise.....	21
4.3.2	Import Vehicles in a Batch.....	22
4.3.3	Export Registered Vehicles .....	22
4.4	Area Management.....	22
4.4.1	Add Single Area .....	23
4.4.2	Import Areas .....	23
4.4.3	Export Areas .....	24
4.5	Device Management.....	24
4.5.1	Manage Encoding Device .....	24
4.5.2	Manage Access Control Device .....	36
4.5.3	Manage Elevator Control Device .....	44
4.5.4	Manage Parking Devices .....	48
4.6	Event Configuration .....	54
4.6.1	Configure Arming Schedule Template .....	55
4.6.2	Configure Event Rule .....	56
4.6.3	Configure Event Parameters.....	60
4.7	Map Configuration.....	60
4.7.1	Configure GIS Map .....	60

4.7.2	Add Static Map .....	61
4.7.3	Add Hot Spot .....	62
4.7.4	Add Hot Region .....	63
4.8	Video Surveillance Settings .....	63
4.8.1	Recording Settings.....	63
4.8.2	Capture Settings .....	67
4.8.3	Configure Media Server .....	69
4.8.4	Device Arming Settings .....	73
4.8.5	Set Parameters .....	74
4.9	Access Control Configuration .....	75
4.9.1	Set Device Parameters.....	75
4.9.2	Set Permission Parameters.....	76
4.9.3	Set Event Parameters .....	77
4.9.4	Control Client Secondary Permission Authentication .....	78
4.10	Visitor Configuration.....	78
4.10.1	Basic Parameters .....	78
4.10.2	Set Picture Storage Location .....	79
4.10.3	Set Visitor Permissions .....	79
4.10.4	Pre-Define Visit Purpose .....	80
4.10.5	Set Template for Visitor Pass.....	80
4.10.6	Set Message Notification Content.....	81
4.10.7	Set Access Control Point for Self-Service Check-Out.....	81
4.10.8	Group Visitors.....	81
4.10.9	Set Retention Time of Visitor Records.....	82
4.11	Elevator Control Configuration .....	82
4.11.1	Configure Floor.....	82
4.11.2	Set Permission Parameters.....	83
4.11.3	Set Event Parameters .....	84
4.12	Time and Attendance Configuration.....	85
4.13	Parking Configuration .....	86
4.13.1	Manage Parking Lot.....	86
4.13.2	Manage Floors.....	87
4.13.3	Add Entrance and Exit to Parking Lot .....	89
4.13.4	Manage Lanes .....	89
4.13.5	Set Parameters .....	91
4.14	Maintenance Configuration.....	93
4.14.1	Configure Health Monitoring Schedule.....	93
4.14.2	Add Custom Schedule Template.....	95
4.14.3	Configure Alarm for Resource Health Status.....	95
4.14.4	Monitor Health Status of Subordinate System.....	103
4.15	Advanced Parameters Settings .....	104
4.15.1	Synchronize Device Time.....	104
4.15.2	Set User Security .....	104
4.15.3	Join User Experience Program.....	105

---

4.16	Menu Customization .....	105
Chapter 5	Monitoring.....	106
5.1	Live View.....	106
5.1.1	Start Live View.....	106
5.1.2	Manual Capture .....	106
5.1.3	Manage View.....	107
5.1.4	PTZ Control.....	108
5.1.5	Auto-Switch Live View.....	110
5.1.6	Auxiliary Screen Preview .....	110
5.1.7	Broadcast to Connected Devices.....	110
5.1.8	Customize Icons on Live View Toolbar.....	111
5.2	Playback.....	112
5.2.1	Play Video File .....	113
5.2.2	Add Tag for Video File .....	115
5.2.3	Download Video File .....	116
5.2.4	Customize Icons on Playback Toolbar.....	116
5.3	Live View and Playback Settings .....	118
Chapter 6	Map Application .....	121
6.1	Manage Hot Spot.....	121
6.2	Operate Map .....	122
6.3	View Alarm on Map .....	123
6.3.1	View Real-Time Alarm .....	123
6.3.2	Search History Event .....	124
6.4	Play Driving Pattern .....	124
Chapter 7	One-Card .....	125
7.1	Issue Cards.....	125
7.1.1	Set Card Issuing Parameters.....	125
7.1.2	Write to Card.....	125
7.1.3	Issue Card to Person.....	126
7.1.4	Operate Card .....	127
7.2	Access Control .....	128
7.2.1	Add Access Control Group.....	129
7.2.2	Add Person Group .....	129
7.2.3	Configure Access Control Schedule Template .....	130
7.2.4	Configure Access Control Permission .....	132
7.2.5	Configure Card Holder of Special Card .....	136
7.2.6	Configure Multiple Authentication .....	137
7.2.7	Configure First Card Opening Door .....	138
7.2.8	Configure Anti-passback.....	138
7.2.9	Configure Multi-Door Interlocking .....	139
7.2.10	Configure Reader Authentication Mode .....	140
7.2.11	Configure Access Control Status.....	141
7.2.12	Configure Capture Linkage .....	142
7.2.13	Search Access Control Event .....	143

7.3	Visitor .....	144
7.3.1	Visitor Reservation .....	144
7.3.2	Group Permissions .....	145
7.3.3	Search Visit Records .....	146
7.3.4	View Unauthorized Visit Records .....	146
7.3.5	View Permissions Applied to Visitors .....	147
7.4	Elevator Control .....	147
7.4.1	Add Floor Group .....	147
7.4.2	Configure Elevator Control Permission .....	148
7.4.3	Configure Elevator Control Status .....	149
7.4.4	Search Elevator Control Event .....	150
7.5	Time and Attendance .....	151
7.5.1	Manage Shift Group .....	151
7.5.2	Manage Shift .....	152
7.5.3	Configure Holiday .....	155
7.5.4	Configure Shift Schedule .....	155
7.5.5	Configure Attendance Check Point .....	157
7.5.6	Manage Attendance Adjustment .....	158
7.5.7	Recalculate Attendance Data .....	158
7.5.8	Search Attendance Information .....	159
7.5.9	Generate Attendance Report .....	160
Chapter 8	Parking System .....	162
8.1	Manage Vehicles .....	162
8.1.1	Group Registered Vehicles .....	162
8.1.2	Manage Vehicles in Blacklist .....	163
8.1.3	Manage Temporary Card .....	164
8.2	Manage Entry & Exit Rules .....	165
8.2.1	Set Entry & Exit Rule for Vehicles in Group .....	165
8.2.2	Set Free Entry & Exit on Holidays .....	166
8.3	Make a Parking Reservation .....	166
8.4	Manage Parking Spaces .....	167
8.4.1	Correct Number of Vacant Parking Spaces .....	167
8.4.2	View and Search Parked Vehicles .....	168
8.4.3	Set Parking Spaces .....	169
8.5	Search .....	170
8.5.1	Search Vehicle Passing Records .....	170
8.5.2	Search Vehicles in Parking Lot .....	171
8.5.3	Search Parking Records in Parking Spaces .....	171
8.5.4	Search Reservation Records .....	171
8.6	Generate Traffic Flow Report .....	171
8.7	Manage Advertisements .....	172
8.7.1	Uploading a Poster .....	172
8.7.2	Release Poster to Self-Service Device .....	172
Chapter 9	Search Event .....	174

Chapter 10	Search Pictures .....	175
Chapter 11	Maintenance.....	176
11.1	Status Overview.....	176
11.1.1	Doughnut Chart.....	176
11.1.2	View Resource Status in Area.....	177
11.1.3	Camera Status Tendency Chart .....	178
11.1.4	Video Exceptions .....	178
11.1.5	Quick Check of Overall Health Status.....	179
11.2	Status Monitoring (Video) .....	180
11.2.1	Camera Online Detection .....	180
11.2.2	Video Quality Diagnosis .....	181
11.2.3	Recording Check .....	182
11.2.4	Device Status .....	183
11.2.5	Topology .....	184
11.3	Alarm Search .....	186
11.4	Report.....	187
11.4.1	Area Overview Report .....	187
11.4.2	Video Quality Report.....	188
11.4.3	Recording Status Report.....	189
11.4.4	Streaming Status Report .....	189
11.4.5	Camera Status Report .....	190
11.4.6	Video Retention Status Report.....	191



# Chapter 1 Overview

## 1.1 About This Document

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

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 is developed for central management of video monitoring system, parking system, access control system, visitor management system, elevator control system, and time and attendance system. 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, 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 System Requirement

### 2.1 Service Requirement

The requirements of the service's running environment are shown as follows:

- **Operating System:** Microsoft® Server 2016 (64-bit), Microsoft® Server2012 R2 (64-bit), Microsoft® Server 2008 R2 (64-bit).
- **CPU:** 8 Core Processor or above.
- **Memory:** 32 GB and above for all the modules installation.
- **HDD:** 1 TB, SATA or SAS Hard Drive
- **NIC:** 1GbE Intel® Ethernet Network Adapters
- **Database:** PostgreSQL 9.6.9
- **JDK:** Oracle JDK 8u (1.8.0\_181)
- **Web Container:** Apache Tomcat 8.5.33

**Note:** For high stability and good performance, these above system requirements must be met.

### 2.2 Web Browser Requirement

The web browser to access the HikCentral Enterprise Web Client should be:

- Internet Explorer 10/11 and above (32 or 64-bit)
- Google Chrome 63.0.3239.108 and above (32 or 64-bit)

## Chapter 3 Login

**Purpose:**

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 CMS (Central Management Service) and press Enter key.  
**For 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 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.



- 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.

# Chapter 4 Getting Started

## 4.1 Person Management

### **Purpose:**

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.

### 4.1.1 Manage Organization

#### **Purpose:**







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.


### Add Single Organization

#### **Purpose:**

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 *4.1.7 Restore Deleted Persons*.
  - **Move Organization:** Select the organization name on the left panel, and then click  or




- ↓ to move the organization up or down in the same parent organization.
- **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.

## Import Organizations in a Batch

### **Purpose:**

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.

## Export Added Organizations

### **Purpose:**

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.

## 4.1.2 Set Fields of Basic Person Information

### **Purpose:**

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.




## 4.1.3 Set Parameters for Biometric Features Collection

### Device

### **Purpose:**

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.

## 4.1.4 Add Single Person

### Purpose:


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.
 




**Note:** For details about customizing the fields of basic person information, refer to *4.1.2 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 Plugin 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 *4.1.3 Set Parameters for Biometric Features Collection Device*.
6. Click **Save** to save the settings and add the person to the person list.
7. (Optional) 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 *4.1.7 Restore Deleted Persons*.
  - **Change Organization:** Select the person(s), and then click **Change Organization** to move the person(s) to another organization.

## 4.1.5 Import Multiple Persons

### Purpose:

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.

**Note:** 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.

## 4.1.6 Export Added Persons

**Purpose:**

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.

## 4.1.7 Restore Deleted Persons

**Purpose:**

Similar like the recycle bin of the computer, HikCentral Enterprise 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. (Optional) 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.

## 4.2 Role and User Management

### **Purpose:**

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.



### 4.2.1 Add Role




#### **Purpose:**

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.

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

#### **Steps:**

1. Click  -> **System Configuration** ->  **Person, User, and Role** -> **Role** to enter the Role Management page.
2. Click **Add** in the role list to enter the Add Role page.
3. Set the role name and descriptions for this role.
5. 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.
6. Click **Save** to save the settings and add the role to the role list.
  7. (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.



## 4.2.2 Manage User Group

### **Purpose:**

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.



## 4.2.3 Add Single User


### **Purpose:**





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.

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


### **Steps:**

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.

## 4.2.4 Import Multiple Users

### **Purpose:**

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:** 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.

## 4.2.5 Synchronize Users from Windows Domain

### **Purpose:**

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 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.

## 4.2.6 Export Users

### **Purpose:**

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.

## 4.3 Manage Registered Vehicles

### **Purpose:**

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.

### 4.3.1 Register a Vehicle to HikCentral Enterprise

#### **Purpose:**

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 *4.1 Person Management*.
4. Click **Save** to save the settings.

## 4.3.2 Import Vehicles in a Batch

### **Purpose:**

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.

## 4.3.3 Export Registered Vehicles

### **Purpose:**

If you need to back up the vehicle information registered on the system, you need to export them and save them in a CSV file and store it in the current PC.

### **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.

## 4.4 Area Management

### **Purpose:**

HikCentral Enterprise 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.

## 4.4.1 Add Single Area



### **Purpose:**

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.

## 4.4.2 Import Areas

### **Purpose:**

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.
5. **Note:** For one file, up to 50,000 records can be imported. The file should be within 50 MB.
6. Fill the area information in the template.
 




**Note:** Click **Field Description** to view the rules of filling the fields of the template.
7. Click **Select** to select the template of area information from the local disk.
8. Click **Import** to import the areas to the system.

### 4.4.3 Export Areas

**Purpose:**

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.

## 4.5 Device Management

**Purpose:**

HikCentral Enterprise supports multiple resource types, such as encoding device, access control device, elevator control device, and parking device. After adding them to the system, you can manage them, configure required settings, and perform further operations. For example, you can add encoding devices for live view, playback, recording settings, etc., add access control devices for access control, access group management, etc., add elevator control device for elevator permission configuration, floor group management, etc., and add parking device for entrance and exit management, vehicle search, parking space management, etc.

### 4.5.1 Manage Encoding Device

**Purpose:**

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

## Add an Encoding Device by IP Address

### **Purpose:**



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.

**Note:** Encoding devices connected via Hikvision EHome 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*.

### **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 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 device.
3. Click **Encoding Device** to enter the encoding device page, and click **Add** to enter the Add Encoding Device page.

\* Access Protocol  ▼  
 Select the protocol for device to access the system. [Protocol Definition](#)

\* IP Address  Single  IP Segment

When adding encoding devices by IP segment, the start IP address and the end IP address should be in the same C class address.

\* Port No.

\* User Name

\* Password

\* Domain  ▼  
 Indicates device's network.

Intelligent Capability  ▼

Panoramic Capability  ▼

Description

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., user name, password, network, intelligent capability, panoramic capability, and description.
  - **IP Address:** Enter the IP address of the encoding device.
  - **Port No.:** Enter the device port No.
  - **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.



*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:** For details about network domain configuration, refer to the *User Manual of Operation and Management Center*.
- **Intelligent Capability:** Select one or more intelligent capabilities from the drop-down list for

the encoding device if needed.

- ✧ **GPS:** For devices such as MNVR, PVR, etc., the GPS capability will show the accurate location of the devices on the GIS map in real-time.

**Note:** For details about operating the devices on the map, refer to *6.1 Manage Hot Spot*.

- ✧ **Temperature:** For thermal cameras, the Temperature capability will enable temperature detection, fire and smoke detection, temperature difference, etc.
- ✧ **Behavior Analysis:** For VCA cameras, the Behavior Analysis capability will detect a series of behaviors, such as intrusion, absence, climbing, etc.


- **Panoramic Capability:** Select the panoramic capability from the drop-down list for the encoding device if needed. HikCentral Enterprise supports PanoVu camera and panoramic camera.
- **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 click **Test** to start online test again.

8. Click **Save** to add the encoding device.



9. (Optional) 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 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 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.

## Add Encoding Devices by IP Segment

### Purpose:



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.

**Note:** Encoding devices connected via Hikvision EHome Protocol cannot be added to the system by IP segment. For details about adding encoding devices by EHome Protocol, refer to *Add Encoding Devices by EHome Protocol*.

### 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 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.




*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.*

- **Intelligent Capability:** Select one or more intelligent capabilities from the drop-down list for the encoding device if needed.
    - ✧ **GPS:** For devices such as MNVR, PVR, etc., the GPS capability will show the accurate location of the devices on the GIS map in real-time.
 

**Note:** For details about operating the devices on the map, refer to *6.1 Manage Hot Spot*.
    - ✧ **Temperature:** For thermal cameras, the Temperature capability will enable temperature detection, fire and smoke detection, temperature difference, etc.
    - ✧ **Behavior Analysis:** For VCA cameras, the Behavior Analysis capability will detect a series of behaviors, such as intrusion, absence, climbing, etc.
  - **Panoramic Capability:** Select the panoramic capability from the drop-down list for the encoding devices if needed. HikCentral Enterprise supports PanoVu camera and panoramic camera.
  - **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 click **Test** to start online test again.
  7. Click **Save** to add the encoding devices.
  8. (Optionally) You can perform the following operation(s) after adding the encoding devices.
    - **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 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.

## Add Encoding Devices by EHome Protocol



### Purpose:

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 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. Set the parameters for the encoding devices, including device No., network, intelligent capability, panoramic capability, and description.
  - **Device No.:** Enter the unique device No. of the encoding device. The device No. should be the same with that entered in the device. You can also click **Add No.** to add multiple encoding devices at a time.
  - **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*.
  - **Intelligent Capability:** Select one or more intelligent capabilities from the drop-down list for the encoding device if needed.
    - ◇ **GPS:** For devices such as MNVR, PVR, etc., the GPS capability will show the accurate location of the devices on the GIS map in real-time.
 


**Note:** For details about operating the devices on the map, refer to *6.1 Manage Hot Spot*.
    - ◇ **Temperature:** For thermal cameras, the Temperature capability will enable temperature detection, fire and smoke detection, temperature difference, etc.
    - ◇ **Behavior Analysis:** For VCA cameras, the Behavior Analysis capability will detect a series of behaviors, such as intrusion, absence, climbing, etc.
  - **Panoramic Capability:** Select the panoramic capability from the drop-down list for the

encoding devices if needed. HikCentral Enterprise supports PanoVu camera and panoramic camera.

- **Description:** Enter the custom description.
6. Click **Save** to add the encoding device(s).
  7. (Optional) 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 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.



*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 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.

## Add Online Encoding Devices



### **Purpose:**

The active online encoding devices in the same local subnet with the HikCentral Enterprise 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 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 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 device.
3. Click **Encoding Device** to enter the encoding device page.
4. Click **Online Devices** to start detecting online encoding devices.

The detected online devices are listed on the Online Encoding Devices page.


Result(0/3)					
<input type="checkbox"/>	Device Name	Access Protocol	IP Address and Port No.	Device No.	Device Serial No.
<input type="checkbox"/>	Ehome_182.86_1	HTTP (Device Protocol)	-	182.86.1	182.86.1
<input type="checkbox"/>	3402000001320000009	HTTP	-	3402000001320000009	3402000001320000009
<input type="checkbox"/>	3408000001320000001	HTTP	-	3408000001320000001	3408000001320000001

Total 3 item(s)    20 items/page    1 / 1Page    Go

5. Select one or more devices you want to add to the system from the list, or click  to filter the online encoding devices by specific conditions.
6. Click **Save** to add selected online encoding devices.
7. (Optional) 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 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.





*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 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.

## Import Encoding Devices in a Batch



### Purposes:

When there are multiple devices to be added to HikCentral Enterprise, 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 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 **Select** 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. (Optional) 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 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.



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 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.



## Manage Cameras


### **Purpose:**

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. (Optional) Perform the following operation(s) after adding the cameras.
  - **Search Device:** Check **Include Child Area** to filter the cameras, or click  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.
- **Export Cameras:** Click **Export Camera** to export information of all the added cameras in a

CSV file.






## Manage Alarm Devices

### **Purpose:**

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.

**Note:** This user manual only introduces configurations and operations on HikCentral Enterprise 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.

### **Steps:**

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. (Optional) Perform the following operation(s) after adding the alarm devices.
  - **Search Device:** Check **Include Child Area** to filter the alarm devices, or click  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.

## 4.5.2 Manage Access Control Device

### **Purpose:**

You can add the access control devices to HikCentral Enterprise 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.

## Add an Access Control Device by IP Address

### **Purpose:**



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.

**Note:** Access control devices connected via Hikvision EHome Protocol cannot be added to the system by IP address. For details about adding access control devices by EHome Protocol, refer to *Add an Access Control Device by EHome Protocol*.

### **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 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:**

1. Click  -> **System Configuration** ->  **Devices** -> **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, and 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 *4.9.1 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.





*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 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 Child Area** to filter the devices, or click  to filter access control devices by specific conditions.
  - **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 *Manage Access Control Points*

#### **Purpose:**



After the access control devices are added to the system and configured properly, the access control point linked to the access control device should be added to an area for management.

#### **Steps:**

1. Click  -> **System Configuration** ->  **Devices** -> **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 linked access control points in the area will be listed in the Door Channel to be Selected list.
5. Select the access control points(s) you want to add in the Door Channel to be Selected list, and click > to add to the Selected Door Channel list.
6. Click **Save**.
7. (Optional) Perform the following operation(s) after adding the access control points.
  - **Search Device:** Check **Include Child Area** to filter the access control points, or click  to filter access control points by specific conditions.
  - **Edit Device:** Click  to edit the device information, including access control point name, position description, and description.
  - **Delete Device:** Click  to delete the access control point, or select multiple access control points and click **Delete** to delete access control points in a batch.

**Note:** Deleting the access control point will delete all configurations for the access control point.

Set Parameters for Doors 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.

## Add an Access Control Device by EHome Protocol



### **Purpose:**


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 network.


### **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 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:**

1. Click  -> **System Configuration** ->  **Devices** -> **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, 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 *4.9.1 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. (Optional) Perform the following operation(s) after adding the access control device.
  - **Search Device:** Check **Include Child Area** to filter the devices, or click  to filter access control devices by specific conditions.








- **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 *Manage Access Control Points*

**Purpose:**

After the access control devices are added to the system and configured properly, the access control point linked to the access control device should be added to an area for management.

**Steps:**

8. Click  -> **System Configuration** ->  **Devices** -> **Access Control** to enter the Access Control page.
9. Select an area in the area list, and click **Access Control Point** to enter the access control point page.
10. Click **Add** to enter the Add Access Control Point page.
11. Select the area in the Current Area list.  
All linked access control points in the area will be listed in the Door Channel to be Selected list.
12. Select the access control point(s) you want to add in the Door Channel to be Selected list, and click > to add to the Selected Door Channel list.
13. Click **Save**.
14. (Optional) Perform the following operation(s) after adding the access control points.
  - **Search Device:** Check **Include Child Area** to filter the access control points, or click  to filter access control points by specific conditions.
  - **Edit Device:** Click  to edit the device information, including access control point name, position description, and description.
  - **Delete Device:** Click  to delete the access control point, or select multiple access control points and click **Delete** to delete access control points in a batch.  
**Note:** Deleting the access control point will delete all configurations for the access control point.  
*Set Parameters for Doors 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.

## Add Online Access Control Devices

**Purpose:**

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.





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



**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 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:**





1. Click  -> **System Configuration** ->  **Devices** -> **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. (Optional) Perform the following operation(s) after adding the access control device.
  - **Search Device:** Check **Include Child Area** to filter the devices, or click  to filter access control devices by specific conditions.
  - **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 *Manage Access Control Points*


**Purpose:**

After the access control devices are added to the system and configured properly, the access control point linked to the access control device should be added to an area for management.

**Steps:**



15. Click  -> **System Configuration** ->  **Devices** -> **Access Control** to enter the Access Control page.
16. Select an area in the area list, and click **Access Control Point** to enter the access control point page.
17. Click **Add** to enter the Add Access Control Point page.
18. Select the area in the Current Area list.  
All linked access control points in the area will be listed in the Door Channel to be Selected list.
19. Select the access control points(s) you want to add in the Door Channel to be Selected list, and click > to add to the Selected Door Channel list.
20. Click **Save**.
21. (Optional) Perform the following operation(s) after adding the access control points.
  - **Search Device:** Check **Include Child Area** to filter the access control points, or click  to filter access control points by specific conditions.
  - **Edit Device:** Click  to edit the device information, including access control point name,

position description, and description.

- **Delete Device:** Click  to delete the access control point, or select multiple access control points and click **Delete** to delete access control points in a batch.

**Note:** Deleting the access control point will delete all configurations for the access control point.

Set Parameters for Doors 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.

## Manage Access Control Points

### **Purpose:**

After the access control devices are added to the system and configured properly, the access control point linked to the access control device should be added to an area for management.

### **Steps:**

22. Click  -> **System Configuration** ->  **Devices** -> **Access Control** to enter the Access Control page.
23. Select an area in the area list, and click **Access Control Point** to enter the access control point page.
24. Click **Add** to enter the Add Access Control Point page.
25. Select the area in the Current Area list.  
All linked access control points in the area will be listed in the Door Channel to be Selected list.
26. Select the access control points(s) you want to add in the Door Channel to be Selected list, and click > to add to the Selected Door Channel list.
27. Click **Save**.
28. (Optional) Perform the following operation(s) after adding the access control points.
  - **Search Device:** Check **Include Child Area** to filter the access control points, or click  to filter access control points by specific conditions.
  - **Edit Device:** Click  to edit the device information, including access control point name, position description, and description.
  - **Delete Device:** Click  to delete the access control point, or select multiple access control points and click **Delete** to delete access control points in a batch.

**Note:** Deleting the access control point will delete all configurations for the access control point.




## Set Parameters for Doors

### **Purpose:**

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** -> **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. (Optional) 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.

## Set Parameters for Card Readers


**Purpose:**

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** -> **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**
    - ◇ **Communication Method:** Select the communication method between the access 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 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 *4.9.3 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 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. (Optional) 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.

### 4.5.3 Manage Elevator Control Device

**Purpose:**

You can add the elevator control devices to HikCentral Enterprise 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.

## Add an Elevator Control Device by IP Address



### Purpose:

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** -> **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.



*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.*



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.
7. (Optional) Perform the following operation(s) after adding the elevator control device.




- **Search Device:** Check **Include Child Area** to filter the devices, or click  to filter elevator control devices by specific conditions.
  - **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 *Manage Access Control Points*



**Purpose:**

After the access control devices are added to the system and configured properly, the access control point linked to the access control device should be added to an area for management.

**Steps:**

29. Click  -> **System Configuration** ->  **Devices** -> **Access Control** to enter the Access Control page.
30. Select an area in the area list, and click **Access Control Point** to enter the access control point page.
31. Click **Add** to enter the Add Access Control Point page.
32. Select the area in the Current Area list.
 

All linked access control points in the area will be listed in the Door Channel to be Selected list.
33. Select the access control point(s) you want to add in the Door Channel to be Selected list, and click > to add to the Selected Door Channel list.
34. Click **Save**.
35. (Optional) Perform the following operation(s) after adding the access control points.
  - **Search Device:** Check **Include Child Area** to filter the access control points, or click  to filter access control points by specific conditions.
  - **Edit Device:** Click  to edit the device information, including access control point name, position description, and description.
  - **Delete Device:** Click  to delete the access control point, or select multiple access control points and click **Delete** to delete access control points in a batch.
 

**Note:** Deleting the access control point will delete all configurations for the access control point.
  - 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.

## Set Parameters for Elevator Control Devices

**Purpose:**

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** -> **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. (Optional) 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.

## Set Parameters for Card Readers

### **Purpose:**

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** -> **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 *4.11.3 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. (Optional) 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.

## 4.5.4 Manage Parking Devices

### **Purpose:**

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.

**Before You Start:**



- 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.

## Add a Booth Client Terminal

**Purpose:**

Booth client terminal is the PC running the booth client. The booth client terminal usually mounts at the booth of the entrance or exit. The parking lot manager view the passing vehicle details and control the vehicles to pass or not by controlling the connected barrier gate.

**Steps:**



1. Click  -> **System Configuration** ->  **Devices** -> **Parking** -> **Entrance and Exit Device** -> **Booth Client Terminal**.
2. Click **Add**.
3. Enter the required information.
  - **IP Address:** The IP address of the PC running the booth client.
  - **Port No.:** The port of the terminal. By default, it is 8500.
4. (Optional) 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**.

## Add a Capture Unit

**Purpose:**

Capture units are ANPR cameras which can recognize the license plate numbers of the passing vehicles.

**Steps:**

1. Click  -> **System Configuration** ->  **Devices** -> **Parking** -> **Entrance and Exit Device** -> **Capture Unit**.
2. Click **Add**.
3. 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:** If the barrier gate is connected to the capture unit via serial port, you can

enable the capture unit's barrier control function. After enabled, if the capture unit recognize the plate number of registered vehicle, the barrier gate arm will open.



4. (Optional) 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**.

## Add a Display Screen

### *Purpose:*

A display screen mounted at the entrance or exit is used to show the vacant parking spaces information in the parking lot in real-time.

### *Steps:*



1. Click  -> **System Configuration** ->  **Devices** -> **Parking** -> **Entrance and Exit Device** -> **Display Screen**.
2. Click **Add**.
3. 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.
  - **Port No.:** The port of the device. By default, it is 8000.
  - **Screen Dimension:** The height and width of the screen, which you can get from the device label.
  - **Display Content:** Set the display mode such as font color, position, etc. You can preview in the example areas below.
4. (Optional) 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**.

## Add an Entrance & Exit Station

### *Purpose:*

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** -> **Parking** -> **Entrance and Exit Device** -> **Entrance & Exit Station**.
2. Click **Add**.
3. 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:** If the barrier gate is connected to the station via serial port, you can enable

the station's barrier control function. After enabled, if the plate number of registered vehicle is detected, the barrier gate arm will open.



- **Display Content:** Set the content display on the LED screen of the station. You can preview in the example areas below.
4. (Optional) 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**.

## Add a Barrier Gate

### **Purpose:**

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 entering or leaving a parking area. The barrier gate connected to the booth client terminal should be added to the system.

### **Steps:**

1. Click  -> **System Configuration** ->  **Devices** -> **Parking** -> **Entrance and Exit Device** -> **Barrier Gate**.
2. Click **Add**.
3. 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.
4. Click **Save**.

## Add a Bluetooth Card Reader

### **Purpose:**

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** -> **Parking** -> **Entrance and Exit Device** -> **Bluetooth Card Reader**.
2. Click **Add**.
3. 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.




4. Click **Save**.

## Add a Guidance Server

### **Purpose:**

Guidance server is a server running the guidance service. It is used to manage the parking spaces in the parking lot and provide parking space guidance and query. You need to deploy the guidance server in the Operation and Management Center.

### **Steps:**



1. Install the guidance service on the guidance server.  
For details, refer to *User Manual of Operation and Management Center*
2. Click  -> **System Configuration** ->  **Devices** -> **Parking** -> **Guidance Device** -> **Guidance Server**.
3. Click **Add**.  
All the guidance servers deployed will display in the To Be Added list.
4. Select one server you want to add to the parking system.
5. Click  to add the server to the Added Guidance Server list.
6. Click **Save**.

## Add a Guidance Terminal

### **Purpose:**

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** -> **Parking** -> **Guidance Device** -> **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. (Optional) 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. (Optional) 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.



- 5) **Note:** Up to 300 records can be imported. The file size should be within 1 MB.
- 6) Click **Select** and select the template file filled with terminal information.
- 7) Click **Import** to start.

## Add a Guidance Screen

### **Purpose:**

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** -> **Parking** -> **Guidance Device** -> **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.
4. Click **Save**.
5. (Optional) 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.
  - 5) **Note:** Up to 300 records can be imported. The file size should be within 1 MB.
  - 6) Click **Select** and select the template file filled with screen information.
  - 7) Click **Import** to start.

## Add an Entrance Guidance Screen

### **Purpose:**

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** -> **Parking** -> **Guidance Device** -> **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**.

## Add a Query Terminal

**Purpose:**

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** -> **Parking** -> **Guidance Device** -> **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. (Optional) 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**.

## 4.6 Event Configuration

**Purpose:**

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.

## 4.6.1 Configure Arming Schedule Template




### **Purpose:**

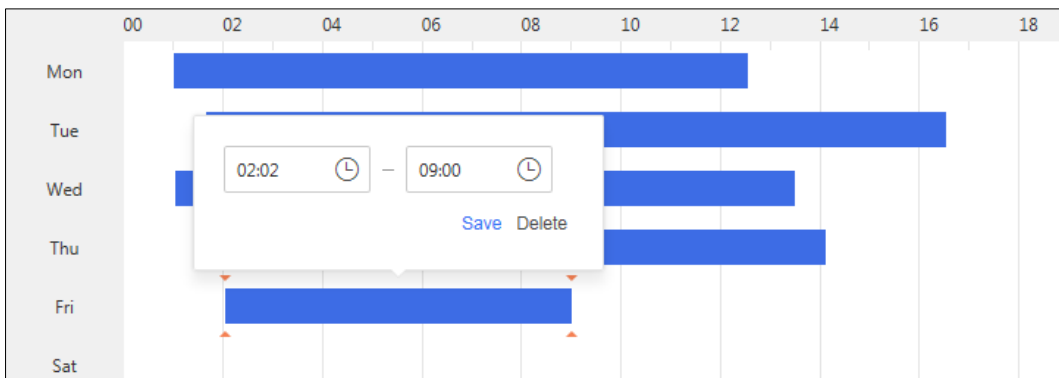
When setting event rule, you can select the predefined arming schedule template to define when the event will be triggered. The system predefines three default arming schedule templates: all-day template, weekday template, and weekend template. You can also add a custom template according to actual needs.




- **All-Day Template:** Events can be triggered at any time.
- **Weekday Template:** Events can only be triggered on weekday.
- **Weekend Template:** Events can only be triggered on weekend.

Perform the following task if you need to add a customized template.

### **Steps:**

1. Click  -> **System Management** ->  **Integrated Control**-> **Event Linkage** to enter the Event Configuration page.
2. Click **Set Schedule Template** on the upper-left of the Event Configuration page to enter the Schedule Template Settings page.
3. Click  to enter the adding custom template page.
4. Create a name for the template.
5. Set the time periods in which event can be triggered.
  - 1) Click **Arming Schedule**.
  - 2) Drag on the time bar to set the time periods.



6. (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 then 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 a time period and then tap **Delete** on the pop-up dialog to delete the time period.
  - Click **Clear** to clear all the time periods.

7. Click **Save**.

## 4.6.2 Configure Event Rule

### **Purpose:**



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.

## Configure Event Rule by Template

### **Purpose:**

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.

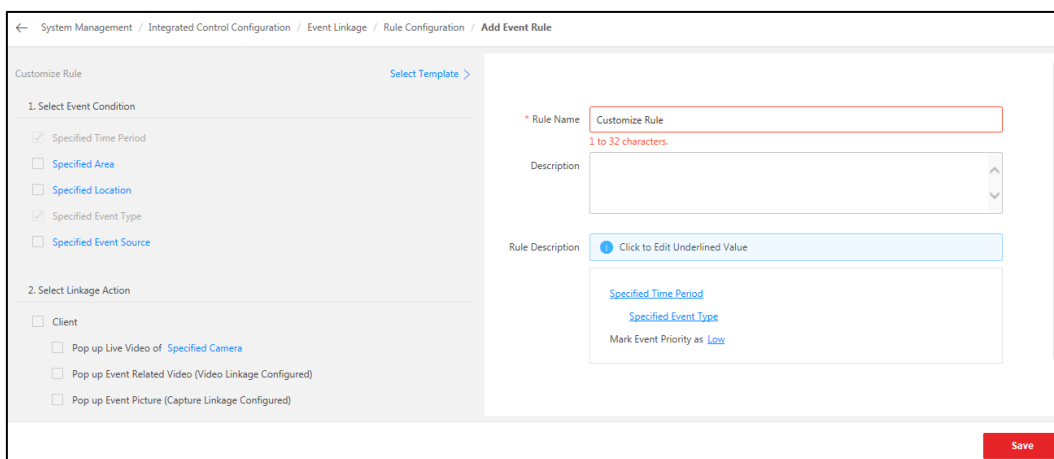
## Configure Custom Event Rule

### Purpose:

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. (Optional) Enter the description of the rule in the Description field.
6. Select event conditions on the left of the page and then configure the selected conditions in Rule Description section on the right.

### Notes:

- 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: <ul style="list-style-type: none"> <li>● <b>Event Source Camera:</b> The specified camera will be camera which detects the event.</li> </ul>

Linkage Action	Description
	<ul style="list-style-type: none"> <li>● <b>Specified Resource:</b> Click  -&gt;  to select camera(s) from the resource tree.</li> </ul>
Pop up Event-Related Video	<p>When the event you defined occurs, the video footage recorded by the specified camera will pop up on the Control Client and Mobile Client.</p> <p><b>Note:</b> 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.</p>
Pop up Event-Related Picture	<p>When the event you defined occurs, the event-related picture will pop up on the Control Client and Mobile Client.</p> <p><b>Note:</b> You should have configured the linkage of capturing picture (Specified Camera Captures Pictures at an Interval of Specified Seconds for Specified Times).</p>
Control Specified Two-Way Audio Channel's Two-Way Audio	<p>You can specify a two-way audio channel for this linkage action.</p> <p>When the event you defined occurs, the specified two-way audio channel will pop up on the Control Client and Mobile Client.</p>
Audio Warning	<p>When the event you defined occurs, there will be audio warning on the Control Client and Mobile Client.</p>
Voice Prompt	<p>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.</p>
Pop-up Window Overlay Event Information	<p>Overlay the information of event source and event rule on the pop-up live view window.</p>
Display Video of Specified Camera on Specified Video Wall	<p>When the event you defined occurs, the live video of a specified camera will be displayed on a specified video wall.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● You should have set alarm window on the video wall. For details, refer to the <i>User Manual of the HikCentral Enterprise Control Client</i>.</li> <li>● The alarm priority of the alarm window on the video wall should not be higher than the event priority. For details, refer to the <i>User Manual of the HikCentral Enterprise Control Client</i>.</li> </ul>
Record Video Footage	<ul style="list-style-type: none"> <li>● <b>Specified Camera Records Video:</b> You can specify a camera to record video footage if the event you defined occurs. <b>Note:</b> You should have configured at least one type of recording schedule (device storage or central storage) for the specified camera.</li> <li>● <b>Add Video Tag Type and Description to Specified Camera:</b> 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. <b>Note:</b> Line breaks are not allowed when entering the</li> </ul>

Linkage Action	Description
	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. <b>Note:</b> You should have configured picture storage server. See the <i>User Manual of Operation and Management Center</i> 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	<ul style="list-style-type: none"> <li>● Call Specified Camera's Preset <ul style="list-style-type: none"> <li>◇ 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.</li> <li>◇ 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.</li> </ul> </li> <li>● 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.</li> <li>● 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.</li> </ul>
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. <b>Note:</b> You should have set the user's mobile phone number. See 4.2 <i>Role and User Management</i> 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. <b>Note:</b> You should have set the user's email. See 4.2 <i>Role and User Management</i> 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.

## 4.6.3 Configure Event Parameters

### **Purpose:**

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.

## 4.7 Map Configuration

### **Purpose:**

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.

### 4.7.1 Configure GIS Map

#### **Purpose:**



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:**

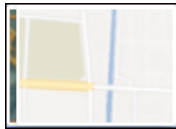
Make sure you have got Google map API URL.

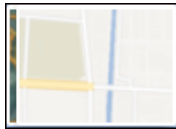

**Steps:**

1. Click  ->  **Integrated Control** -> **Map** -> **Parameters**.
2. Enter the Google map API URL and click **Save**.

**Notes:**

- 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. (Optional) 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 [4.7.3 Add Hot Spot](#).
  - Add hot region(s). For details, refer to [4.7.4 Add Hot Region](#).
7. Click **Save**.

## 4.7.2 Add Static Map


**Purpose:**

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. (Optional) 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.
 

**Note:** 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. (Optional) Add hot spots. For details, refer to [4.7.3 Add Hot Spot](#).
6. (Optional) Add hot regions. For details, refer to [4.7.4 Add Hot Region](#).
7. (Optional) Perform the following operation(s) to manage the maps.
  - Click **Edit** -> **Upload** to add more static maps.
  - 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**.
- 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**.
- Click **Clear** to clear map configuration.

### 4.7.3 Add Hot Spot

**Purpose:**

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 4.7.1 *Configure GIS Map* and 4.7.2 *Add Static Map*.

Resource(s) (e.g., camera, alarm output, access control point, parking lot, etc.) should be added. For details about adding resources, refer to 4.5 *Device Management*.


Perform this task when you need to get the live view or playback of events via the hot spot on the 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. (Optional) Perform the following operation(s).
  - Drag a hot spot to move it.
  - Select a hot spot on the map and click  to delete resource.
  - Adjust hot spot locations in a batch.
    - 1) Click **Select**.
    - 2) (Optional) Press **ESC** to stop selecting resources.
    - 3) Drag to select the resources on the map.
    - 4) Click **Align**.
    - 5) Select a desired align mode.
  - **Copy Configuration to Other Areas:** Click **Copy**, then select areas to copy the map to and click **OK**.
  - Click **Clear** to clear map configuration.

## 4.7.4 Add Hot Region



### **Purpose:**

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 4.7.1 *Configure GIS Map* and 4.7.2 *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**.

 will be displayed on the map.

## 4.8 Video Surveillance Settings

### 4.8.1 Recording Settings

#### **Purpose:**

Recording schedule settings are for defining when, how the recording starts and where the video is recorded with the pre-defined parameters.

HikCentral Enterprise provides two storage locations to record the video files of the cameras: storage on the encoding devices (including DVR, NVR, cameras' SD card, cameras' disk) and central storage (including Hybrid SAN and cloud storage).

### Configure Encoding Device Storage

#### **Purpose:**

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 setting recording schedule for the devices on the HikCentral Enterprise, 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.

## Configure Central Storage

### **Purpose:**

The video files can be stored on the Hybrid SAN and cloud storage device added to the system. For adding Hybrid SAN and cloud storage, you need to login into the Operation and Management Center to add and configure the storage devices.

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




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

## Configure Recording Schedule Template

### **Purpose:**


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 **Set Recording 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. (Optional) Perform the following operations to customize the template.
  - Click the time period to manually enter the start time and end time or delete it.
  - Click **Clear** to clear all the time periods in the time bar.






- Click  in the last column to copy the time period(s) to other weekdays.
8. Click **Save** to save the settings.

## Configure Recording Schedule

### Purpose:

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. (Optional) 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.
  - **Recording Schedule Template:** It defines when the recording starts and ends, and the recording type. You can select the template from 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. (Optional) 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 from the default templates or the customized template. For details about configuring schedule template, refer to *Configure Recording Schedule Template*.
6. Click **Save** to save the settings.
  7. (Optional) After configuring the recording schedule, you can perform the following operations for verification.
    - 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.
    - 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.
    - Click **View Details** to view the details of the recording schedule applying result of the system.
  8. (Optional) Perform the following operations according to your requirements.
    - Click  in the Operation column to re-apply the recording schedule for this camera.
    - Select the camera(s) and click **Apply Again** to apply the recording schedule(s) for the camera(s) again.
    - Click  in the Operation column to copy the recording schedule of this camera to other camera.
    - Click  in the Operation column to delete the recording schedule of this camera.
    - Select the camera(s) and click **Clear Configuration** to delete the recording schedule(s) of the camera(s).
    - Click **Export Recording Schedule Report** to export the recording schedule report file of the in CSV format to the local disk of the PC running 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.

**Notes:**

- HikCentral Enterprise 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 are consistent.

**Warning:**

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

## 4.8.2 Capture Settings

**Purpose:**

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.

### Configure Picture Storage Server

**Purpose:**

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.

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



**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:**

1. Click  -> **System Configuration** ->  **Video Surveillance** -> **Parameter Configuration** to enter the Parameter Configuration page.
2. Select the storage resource pool in the drop-down list of **Picture Storage Location**.
3. Click **Save** to save the settings.

### Configure Capture Schedule Template

**Purpose:**

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 provides two capture schedule template modes: time segment template and time point template.

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.

The configuration of time segment template is as follows:

**Steps:**


1. Click  -> **System Configuration** ->  **Video Surveillance** -> **Capture Schedule**.
2. Click **Set Schedule Template** -> **Time Segment Template**.


**Note:** HikCentral Enterprise provides three default templates, which are not allowed to be edited. All-Day Template can be used to capture pictures all-day with the capture interval set by manual when you set capture schedule for cameras. Weekdays Template can be used to capture pictures all the weekdays with the capture interval set by manual. Weekends Template can be used to capture pictures all the weekends with the capture interval set by manual.

3. The configuration of Time Segment Template is similar with configuring recording schedule template. For details, refer to *Configure Recording Schedule Template*.

The configuration of time point template is as follows:

**Steps:**

1. Select **Time Point Template**.
2. Click  to add new template.
 




**Note:** HikCentral Enterprise 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.
3. Enter the template name in the input field.
4. Move the mouse to the week form to draw the time point for capturing pictures.
5. (Optional) Perform the following operations to custom the template.
  - Click the time point in the week form to manually select the time of capturing pictures (The system only supports 5 mins interval for capturing).
  - Click **Clear** to clear all time points in the week form.
  - Click  in the last column to copy the time point(s) to the other weekdays.
6. Click **Save** to save the settings.



## Configure Capture Schedule

**Purpose:**

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 Capture 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. (Optional) Perform the following operations according to your requirements.
  - Click  in the Operation column to edit the capture schedule for this camera.
  - Click  in the Operation column to delete the capture schedule of this camera.
  - 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.

### 4.8.3 Configure Media Server

**Purpose:**

You can add media servers to HikCentral Enterprise to get the video data stream or transcoding stream from the media servers, thus to lower the load of the device.

**Steps:**

Click  -> **System Configuration** ->  **Video Surveillance** -> **Media Server**. The page is shown as follows:

**Note:** In the condition that cameras are few or the operation of live view and playback is few, you don't need to manually configure media servers on the Web Client, and keep the default configuration of the system.

### Live View and Playback on the Same System

**Purpose:**

DAS (Device Access Stream Media) service is used to get stream from devices when the clients request the live video of the cameras in the current system or play back videos stored in the encoding devices. In the page of Live View and Playback on the Same System, by default, the DAS service(s) added to the Operation and Management Center is are) displayed in the group.

The connection paths of streaming stream in different conditions is as follows:

Conditions of DAS Service	The Streaming Connection Path
DAS service(s) in the group	The clients get the video stream via this DAS service.

You don't need to configure manually, and keep the default configurations unchanged.

**Note:** Make sure you have configured the DAS services on the Operation and Management Center. For

details, refer to *User Manual of Operation and Management Center*.

## Live View or Playback in Cascading Mode

### **Purpose:**

Cascading Stream Media service is used to forward stream when the clients of the upper-level system (HikCentral Enterprise support system cascading, and the upper-level system can view the videos from the subordinate system, which helps you to expand to monitoring scope and manage the systems uniquely.) get stream for live view, playback and transcoded video from the subordinate system.

In the page of Live View or Playback in Cascading Mode, HikCentral Enterprise provides two groups: Stream forwarding group is used to forward the video stream for live view and playback in cascading mode. Transcoding group is used to forward the transcoding stream in cascading mode.

In the page of Live View or Playback in Cascading Mode, by default, the Cascading Stream Media service(s) added on the Operation and Management Center is(are) displayed in the Stream Forwarding Group.

The connection paths of streaming and transcoding stream in different conditions are as follows:

Conditions of Cascading Stream Media Service	The Streaming Connection Path	The Transcoding Streaming Connection Path
Cascading Stream Media service(s) in the stream forwarding group	The clients get the video stream via the Cascading Stream Media service(s) in the stream forwarding group.	The clients get the transcoding stream via this Cascading Stream Media service(s) in the stream forwarding group.



Manually configuring Cascading Stream Media service for transcoding usage uniquely is also supported.

Perform the following the operations if you want to add Cascading Stream Media service to Transcoding Group.

### **Before you start:**

Make sure there are 2 or more Cascading Stream Media services in the stream forwarding group.

### **Steps:**

1. Click  -> **System Configuration** ->  **Video Surveillance Configuration** -> **Media Server** -> **Live View and Playback in Cascading Mode**.
2. In the stream forwarding group, click **Switch Group** in the Operation column of to switch the services to the transcoding group.

**Note:** The stream forwarding group requires one Cascading Media Service at least.

### **Step Result:**

The connection paths of streaming and transcoding streaming are as follows:

Conditions of Cascading Stream Media Service	The Streaming Connection Path	The Transcoding Streaming Connection Path
1 Cascading Stream Media service in the stream forwarding group p and 1 Cascading Stream Media service in the transcoding	The clients get the video stream via the Cascading Stream Media service in the stream forwarding group.	The clients get the transcoding stream via this Cascading Stream Media service in the transcoding group.

group		
-------	--	--

## Playback for Central Storage

### **Purpose:**

VOD service is used to get stream for playback from the central storage devices (Hybrid SAN, cloud storage, or pStor).

In the page of Playback for Central Storage, by default, the VOD service(s) added to the Operation and Management Center is(are) displayed in the default group.

The connection paths of streaming in different conditions are as follows:



Conditions of VOD Service	The Streaming Connection Path
Media service(s) in the default group	The clients get the video stream via this VOD service(s) in the default group.

Manually configuring the connection between VOD services and cameras is also supported by adding new group. Perform the following operations to add a new group.

### **Before You Start:**

Make sure there are 2 or more VOD services in the default group.

### **Steps:**

1. Click  -> **System Configuration** ->  **Video Surveillance** -> **Media Server** -> **Playback for Central Storage**.
2. (Optional) Click **Add Group** and enter the group name for the new group.
3. (Optional) Click **Switch Group** in the Operation column of the default group to switch the service(s) to the newly added group.
4. Click **Link Camera** to connect cameras with the newly added group.

### **Notes:**

- The default group requires at least one VOD services.

### **Step Result:**

The streaming connection paths of different cameras are as follows:

Conditions of VOD Service	The Streaming Connection Path for Cameras Linked with Newly Added Group	The Streaming Connection Path for Cameras not Linked with Newly Added Group
1 VOD service in the default group and 1 VOD service in the newly added VOD group	The clients get the video stream via this VOD service in the default group.	The clients get the video stream via the VOD service in the newly added VOD group.

## Stream Forwarding

### **Purpose:**

When the clients which tries to get stream and the video sources are not in the same LAN (RTSP protocol, WebSocket protocol, HLS protocol and RTMP protocol are supported), and when the clients get transcoded video stream (e.g. The stream format can be transformed into the format compatible

with the clients, or the video resolution and bitrate is reduced), the video is forwarded via the Media Gateway service.



In the page of Stream Forwarding, the Media Gateway service(s) added to the Operation and Management Center is(are) displayed in the default group with the transcoding function disabled by default.

The connection paths of streaming stream in different conditions are as follows:

Conditions of Media Gateway Service	The Streaming Connection Path
Media Gateway service(s) in the default group with transcoding function disabled	The clients get the video stream via the Media Gateway service(s) in the default group.

Manually configuring the connection between Media Gateway services in the default group and cameras is also supported. Perform the following operations.

**Steps:**

1. Click  -> **System Configuration** ->  **Video Surveillance** -> **Media Server**-> **Stream Forwarding**.
2. Click **Link Camera** above the default group to link cameras with the group. After that, the clients get the linked cameras' video stream via the group preferentially.
3. (Optional) Click **Edit Group** above the default group to enable the transcoding function for this group. After that, both the transcoding streaming connection and normal streaming connection use the Media Gateway service(s) in the default group.

**Step Result:**

Conditions of Transcode Function	The Streaming Connection Path	The Transcoded Streaming Connection Path
The transcoding function of the default group is enabled.	The clients get the video stream via this Media Gateway service(s) in the default group in secondly priority.	The clients preferentially get the transcoded video stream via this Media Gateway service(s) in the default group.

In some conditions, you need more groups to bind different cameras to different group, you can add new group and configure the connection between Media Gateway services in the newly added group and cameras. Perform the following operations.

**Before You Start:**

Make sure there are 2 or more Media Gateway services in the default group.

**Steps:**

1. Click **Add Group**.
2. Enter the group name in the pop-up window.
3. In the default group, select one service and click **Switch Group** in the Operation column to switch the service to the newly added group.
4. Click **Link Camera** above the newly added group to link cameras with the group. After that, the clients get the linked cameras' video stream via the group preferentially.
5. (Optional) Click **Edit Group** above the newly added group to enable transcoding. After that, the services in the newly added group are only for transcoding usage.

**Step Result:**

Conditions of Transcode Function	The Streaming Connection Path	The Transcoded Streaming Connection Path
The transcoding function of	The clients get the video stream of	The clients get the transcoded



the newly added group is disabled.	the cameras linked with the newly added group via this Media Gateway service(s) in the newly added group.	video stream of the cameras linked with the newly added group via this Media Gateway service in the default group.
The transcoding function of the newly added group is enabled.	The clients get the video stream of the cameras linked with the newly added group via this Media Gateway service(s) in the default group.	The clients get the transcoded video stream of the cameras linked with the newly added group via this Media Gateway service in the newly added group.

## 4.8.4 Device Arming Settings

### **Purpose:**

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.





## Configure Arming Schedule Template

### **Purpose:**

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.

Perform the following operations to customize new templates.

### **Steps:**

1. Click  -> **System Configuration** ->  **Video Surveillance** -> **Device Event 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.
  - Click the time period to manually enter the start time and end time, or delete it.
  - Click **Clear** to clear all time periods in the time bar.
  - Click  in the last column to copy the time period(s) to the other weekdays.
7. Click **Save** to save the settings.

## Event Arming Control




### Purpose:



You can arm/disarm the added devices for the following events:

- **Motion Detection:** With motion detection feature, motion can be detected in any part of a camera's view. Users can configure full screen or a number of zones in a camera's view where motion is to be detected. Using motion detection helps to prioritize recordings, decrease the amount of recorded video and make searching for events easier.
- **Video Tampering Detection:** Trigger alarm when the lens is covered and take alarm response actions.
- **Video Loss Detection:** IP camera can automatically detect picture frame loss when the video is transmitting, and can resend the lost frame.
- **Alarm Input:** The alarm is triggered when the encoding devices' connected alarm detector detects the alarm signal.
- **Alarm Output:** Alarm output is the node signal or other signal sent from the alarm controller to the peripheral devices when the alarm is triggered.

The operations of configuring arming or disarming are as follows:

### 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 on 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. (Optional) Select devices in a batch, and then click **Batch Configure Schedule** to select an arming schedule template for the selected devices.
10. (Optional) Select devices in a batch, and then click **Batch Arm** to arm the devices by the arming schedule template selected in step 8.
11. (Optional) Select devices in a batch, and then click **Batch Disarm** to disarm the devices by the arming schedule template selected in step 8.

## 4.8.5 Set Parameters

### Purpose:

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

### Steps:

1. Click  -> **System Configuration** ->  **Video Surveillance** -> **Parameter Configuration** 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.
  - **Picture Storage Location:** The storage location of the pictures captured by capture schedule and the pictures of vehicle passing records captured in the parking lot subsystem. You need to configure the storage server in the operation and management center. For details about configuring the storage server, refer to *User Manual of Operation and Management Center*.

## 4.9 Access Control Configuration

### **Purpose:**



After adding access control devices and access control points to the system, you can configure parameters for them, including device parameters, parameters of permission auto-applying, and parameters of access control event.

### 4.9.1 Set Device Parameters

#### **Purpose:**

You can configure the types of access control devices available for adding, the timeout period of authentication interval, capture settings of the access control terminal, and the storage location for the pictures captured by the access control terminal.

#### **Steps:**

1. Click  -> **System Configuration** ->  **One-Card** -> **Access Control** -> **Device Parameters** to enter the Device Parameters page.
2. Configure the parameters.
  - **Select Device Type:** Click  /  to select or unselect types of access control devices available for adding to the system. When adding access control devices, you can select the device types configured here.
 

**Note:** For details about adding access control device, see *4.5.2 Manage Access Control Device*.
  - **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 *7.2.6 Configure Multiple Authentication*.
  - **Capture Settings:** Enable or disable the access control terminal to capture a picture when an

access control event occurs.

- **Picture Storage Location:** Select a picture storage server to store the pictures captured by the access control terminal.

**Note:** For details about adding picture storage server, refer to the *User Manual of Operation and Management Center*.

## 4.9.2 Set Permission Parameters

### **Purpose:**

In the Permission Parameters module, you can configure the permission-related parameters such as auto-applying permissions.

### **Apply Permission Automatically**





#### **Purpose:**

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

#### **Before You Start:**

You should have configured card permissions, registered fingerprint information, and uploaded face pictures. See *Chapter 7 One-Card* for details.

#### **Steps:**

1. Go to  -> **System Configuration** ->  **One Card** -> **Access Control** -> **Permission Parameters** -> **Auto Apply Permission**.
2. Select **Card Permission**, **Fingerprint**, or **Face Picture**.
3. Switch  to  to enable the system to automatically apply the selected item.
4. Select a method for automatically applying the access control permission.
  - **Apply at Fixed Time of Each Day:** Set a start time for auto-applying, and then set the interval for auto-applying. 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-applying time in non-peak hours of system usage, such as the wee hours, thus avoiding system exceptions.
  - **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-applying.
 



**Note:** Over-frequent auto-applying may take excessive service resources. Take your service resource into account when setting the auto-applying times.
5. Click **Save**.

## Configure Retention Period of Permission-Applying Record

### **Purpose:**

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.

### **Steps:**





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

## Copy Permission Settings from Parent Organization

### **Purpose:**

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

### **Steps:**

1. Go to  -> **System Configuration** ->  **One-Card** -> **Access Control** -> **Permission Parameters** -> **Copy Permission Settings from Upper-Level Organization**.
2. Switch  to  to enable the function.
3. Click **Save**.

## 4.9.3 Set Event Parameters

### **Purpose:**



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

### **Purpose:**

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** -> **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

### **Purpose:**

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 Configuratioo** ->  **One-Card** -> **Access Control** -> **Event Parameters** -> **Event Record Retention Period**.
2. Select a period from the drop-down list.
3. Click **Save**.

## 4.9.4 Control Client Secondary Permission Authentication

### **Purpose:**

You can enable Control Client Secondary Permission Authentication to allow the doors to be opened via the Control Client even if the access control permissions configured on the Web Client has not been applied to the access control devices, thus avoiding the inconvenience that the doors cannot be opened when the permissions are lost on the device end.

Go to  -> **System Configuratioo** ->  **One-Card** -> **Access Control** -> **Event Parameters** -> **Control Client Secondary Permission Authentication** and then enable the function.

## 4.10 Visitor Configuration

### **Purpose:**

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.

### 4.10.1 Basic Parameters

#### **Purpose:**

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.

## 4.10.2 Set Picture Storage Location

### **Purpose:**

In this section, you need to set the storage location of the captured visitor pictures.

Click  -> **System Configuration** ->  **One-Card System** -> **Visitor** -> **Picture Saving Path**.

Select a picture storage server to store the pictures captures when visitors check-in.



**Note:** For adding the picture storage server, refer to the *User Manual of Operation and Management Center*.


## 4.10.3 Set Visitor Permissions

### **Purpose:**

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 *7.3.2 Group Permissions*.

## 4.10.4 Pre-Define Visit Purpose

**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**.

## 4.10.5 Set Template for Visitor Pass

**Purpose:**

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.
  - 1) Click **Upload Background Picture** to select a picture as the background on the pass.  
You can click **Restore Default Picture** to reset it.
  - 2) 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**.



## 4.10.6 Set Message Notification Content

### **Purpose:**

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.




## 4.10.7 Set Access Control Point for Self-Service Check-Out

### **Purpose:**

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

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

### **Steps:**




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**.


## 4.10.8 Group Visitors

### **Purpose:**



You can pre-define 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.

## 4.10.9 Set Retention Time of Visitor Records

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.

## 4.11 Elevator Control Configuration

### **Purpose:**



You can configure the related parameters for the elevator control devices, such as floor parameters, permission parameters, and received elevator control events.

### 4.11.1 Configure Floor

#### **Purpose:**

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.

Elevator Name	Total Floor Number	Start Floor	Edit
Build A-1	26	-2	<input type="button" value="Edit"/>

Floor (F)	Floor Name	No.
-2	-2F	1
-1	-1F	2
1	1F	3
2	2F	4
3	3F	5
4	4F	6
5	5F	7
6	6F	8
7	7F	9
8	8F	10

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.

## 4.11.2 Set Permission Parameters

### **Purpose:**



The elevator control permissions configured in the system need to be applied to the device automatically or manually. Here you can set permission parameters for applying automatically, including permission applying time and retention period of permission applying record.

### **Automatically Apply Permission**

### **Purpose:**

When you want to apply all elevator control permission settings (e.g., issuing card and returning card) to the devices automatically, you can enable this function to apply permission at the fixed time or for fixed times.

**Steps**



1. Click  -> **System Configuration** ->  **One-Card System** -> **Elevator Control** -> **Permission Parameters** -> **Auto Apply Permission** to enter Auto Apply Permission page.
  2. Set **Auto Apply Permission** switch to on.
  3. Select **Method of Auto Applying**.
    - **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.
- Notes:**
- 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.
4. Click **Save** to save the settings.

## Set Retention Period of Permission Applying Record

**Purpose:**

The permission applying records are saved in the system. You can search the records within the valid period. If expired, the records will be deleted.

**Steps:**

1. Click  -> **System Configuration** ->  **One-Card System** -> **Elevator Control** -> **Permission Parameters** -> **Retention Period of Permission Applying Record** to enter retention period setting page.
2. Select the retention period from drop-down list.
3. Click **Save** to save the settings.

### 4.11.3 Set Event Parameters

**Purpose:**



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

**Purpose:**

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

**Purpose:**

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.



## 4.12 Time and Attendance Configuration

**Purpose:**

You can configure the retention periods of the attendance record, which contains the attendance details and the card swiping record.

**Note:** For details about time and attendance, refer to *7.5 Time and Attendance*.

**Steps:**

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**.

## 4.13 Parking Configuration

### **Purpose:**

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.

### 4.13.1 Manage Parking Lot

#### **Purpose:**




First of all, you need to add the parking lot to the system and set its parameters.

### Add Parking Lot

#### **Purpose:**

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. Click  to add a parking lot.
3. 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.
  - **Reservable Parking Spaces:** Enter the number of parking spaces that can be reserved in this parking lot.
4. Click **Save**.

### Link Device with Parking Lot




#### **Purpose:**

After adding a parking lot, you need to link a guidance server and booth client terminals to the parking lot.

**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.

**Steps:**

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 from the area list.  
All the devices added to this area will display.
5. Select one guidance server and several booth client terminals and click  to add to the selected device list.
6. Click **Save**.

## 4.13.2 Manage Floors

**Purpose:**

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

**Purpose:**

In this section, we introduce how to add a floor to the parking lot.

**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 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

**Purpose:**

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** -> **Parking** -> **Parking Lot**.
2. Select a floor on the parking lot list.
3. Click **Link Device** tab.  
There five types of devices that can be linked to one floor.
4. Click the device tab and click **Link Device**.
5. Select an area from the area list.  
All the guidance devices added to this area will display.
6. Select the device(s) and click  to add to the selected device list.
7. Click **Save**.

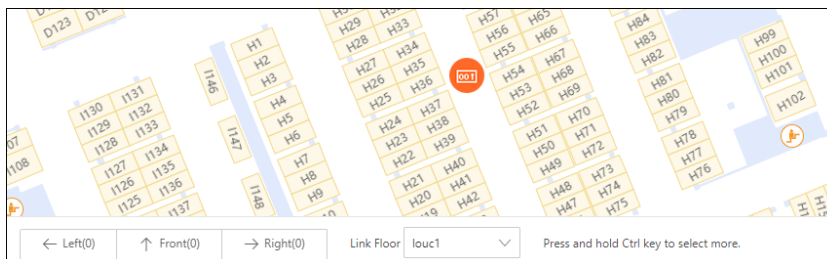
## Locate Device on Floor Map

### Purpose:

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** -> **Parking** -> **Parking Lot**.
2. Select a floor on the parking lot list.
3. Click **Map Configuration**.  
The map of the floor will show.
4. Locate the guidance screens on the map.
  - 1) Click **Guidance Screen** on the upper-left corner.  
The guidance screen which has been linked with the floor will show.
  - 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) Click  and click **Left**, **Right**, or **Front** icon shown below.



- 5) Drag to select the parking spaces that the guidance screen will monitor in these three directions respectively.
- 6) Click **Link** to link these selected parking spaces with the guidance screen.
5. Locate the self-service devices on the map.
  - 1) Click **Self-Service Device** on the upper-left corner.



The query terminal which has been linked with the floor will show.




- 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.

### 4.13.3 Add Entrance and Exit to Parking Lot

**Purpose:**

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 from the dropdown 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 4.5.4 *Manage Parking Devices*.

6. Click **Save**.

### 4.13.4 Manage Lanes

**Purpose:**

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

**Purpose:**

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 entering or lane for exiting.
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 with No 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.
  - **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.
  - **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.
  - **Voice Prompt Mode:** Voice prompts are pre-recorded message which will be played at the entrances and exits when vehicles entering and exiting. You can set the prompt content in System Configuration. For details, refer to *Set Voice Prompt Content*.
    - ◇ **System Prompt:** The message is played by the PC running the booth client linked with the lane.
    - ◇ **Device Prompt:** The message is played by the Entrance and Exit Station linked with the lane.
  - **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.




7. Click **Save**.

## Link Device with Lane

### *Purpose:*

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 gate, 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 from the area list.  
All the lane devices added to this area will display.
6. Select the device(s) and click  to add to the selected device list.
7. Click **Save**.

## 4.13.5 Set Parameters

### *Purpose:*

After setting the parking system, you should set parameters about vehicle entry & exit, card enrollment, voice prompt, data storage, etc.

## Set Entry & Exit Parameters

Click  -> **System Configuration** ->  **Vehicle Control** -> **Parking** -> **Parameters** -> **Entry & Exit Parameters**.

- **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.

## Set Card Enrollment Parameters

Click  -> **System Configuration** ->  **Vehicle Control** -> **Parking** -> **Parameters** -> **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.

## Set Voice Prompt Content

Click  -> **System Configuration** ->  **Vehicle Control** -> **Parking** -> **Parameters** -> **Voice Prompt Parameters**.

When vehicles entering or exiting the parking lot, the booth client terminal or Entrance & Exit Station can play a message to notify the driver parking details such as license plate number, entering time, parking duration, etc.

## Set Data Storage Parameters

Click  -> **System Configuration** ->  **Vehicle Control** -> **Parking** -> **Parameters** -> **Data Storage Parameters**.

Set the retention time of the data such as passing vehicle records and parking records.

Set the storage location of the pictures such as vehicle pictures captured when entering and exiting.

**Note:** For deploying a picture storage server, refer to the *User Manual of Operation and Management Center*.

## Other Parameters

Click  -> **System Configuration** ->  **Vehicle Control** -> **Parking** -> **Parameters** -> **Other Parameters**.

- **Including Registered Spaces (Guidance):** The system can calculate the vacant parking spaces in the parking lot in real-time. After enabled, the number of vacancy displayed on the Guidance Screen will include the vacant parking spaces for registered vehicles.
- **Including Registered Spaces (Entrance & Exit):** The system can calculate the vacant parking spaces in the parking lot in real-time. After enabled, the number of vacancy displayed on the Entrance & Exit Screen will include the vacant parking spaces for registered vehicles.
- **Reservation Valid for:** Set how long the parking reservation is valid after reservation.
- **Max. Reservable Parking Spaces per Contact:** Set how many parking spaces can be reserved at most for one contact phone number.
- **Map Type:** Set the type of the floor map according to the type of your map.
- **Parking Lot Manager Phone Number:** Set the phone number of the manager which will be displayed on the query terminal.

## 4.14 Maintenance Configuration

### **Purpose:**

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 *Chapter 11 Maintenance*.

### 4.14.1 Configure Health Monitoring Schedule

#### **Purpose:**

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 resource 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, including 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 camera.
 

**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 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 video 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 noise.
- **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 *4.14.2 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**.

**Result:**

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.

## 4.14.2 Add Custom Schedule Template

### *Purpose:*

You can add custom schedule template for health monitoring.

### *Steps:*

1. Click  -> **System Configuraiton** ->  **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 ttime period.
  - Click **Clear** to clear all the time periods.
6. Click **OK**.

*Result:* The added template will be displayed on the Schedule Template drop-down list on the Add Schedule page.

## 4.14.3 Configure Alarm for Resource Health Status

### *Purpose:*

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).

**Notes:**

- For details about searching alarm information related to resource health status, refer to *11.3 Alarm Search*.
- Performance alarm is only supported by camera and access control device.

**Before You Start:**



You should have configured health monitoring schedule. See *4.14.1 Configure Health Monitoring Schedule* for details.

## Configure Alarm for Encoding Device

**Purpose:**

Perform the following task to configure health status alarm for the encoding device such as NVR.

**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.

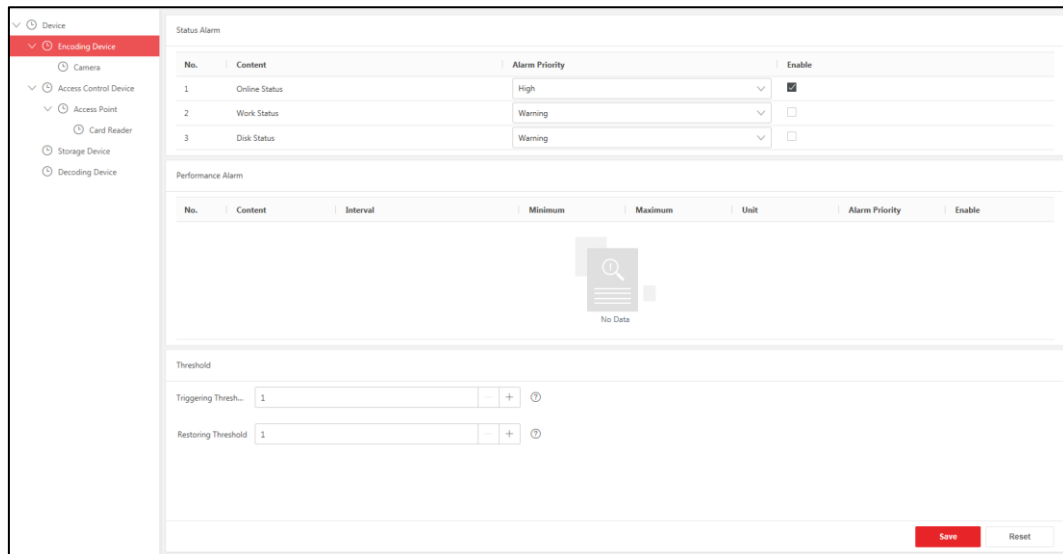
**Note:** The alarm priority defines the alert level of the alarm. The alert level ascends from Prompt all the way to High.



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.





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

### Purpose:

Perform the following task to configure health monitoring alarm for camera.

### 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 encoding device.

- **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 *4.14.1 Configure Health Monitoring Schedule*.

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

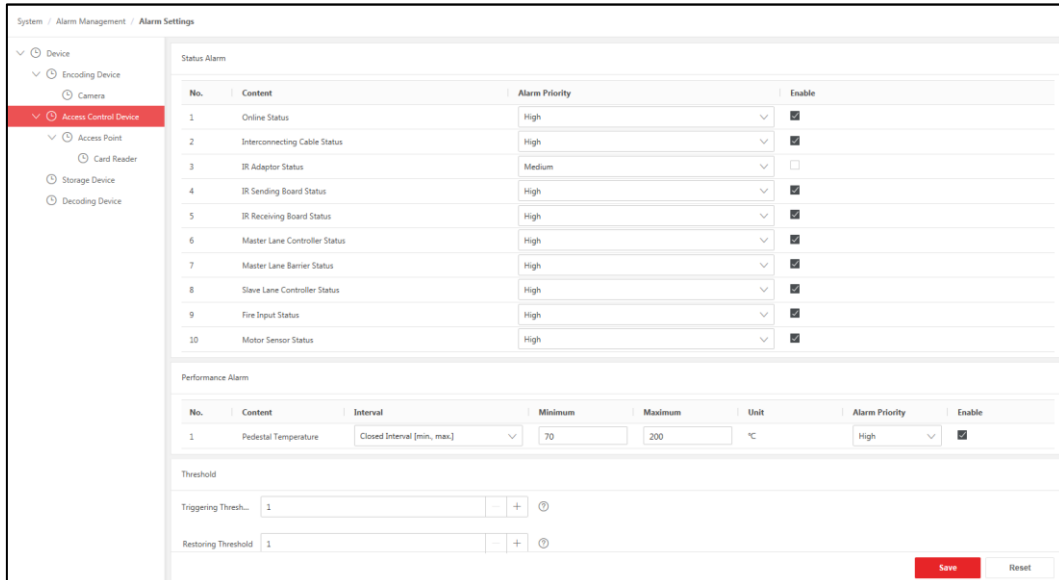
### **Purpose:**

Perform the following task to configure health monitoring alarm for access control device.

**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.



No.	Content	Alarm Priority	Enable
1	Online Status	High	<input checked="" type="checkbox"/>
2	Interconnecting Cable Status	High	<input checked="" type="checkbox"/>
3	IR Adaptor Status	Medium	<input type="checkbox"/>
4	IR Sending Board Status	High	<input checked="" type="checkbox"/>
5	IR Receiving Board Status	High	<input checked="" type="checkbox"/>
6	Master Lane Controller Status	High	<input checked="" type="checkbox"/>
7	Master Lane Barrier Status	High	<input checked="" type="checkbox"/>
8	Slave Lane Controller Status	High	<input checked="" type="checkbox"/>
9	Fire Input Status	High	<input checked="" type="checkbox"/>
10	Motor Sensor Status	High	<input checked="" type="checkbox"/>

No.	Content	Interval	Minimum	Maximum	Unit	Alarm Priority	Enable
1	Pedestal Temperature	Closed Interval [min., max.]	70	200	°C	High	<input checked="" type="checkbox"/>

Threshold

Triggering Thresh... 1

Restoring Threshold 1

Save Reset

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 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

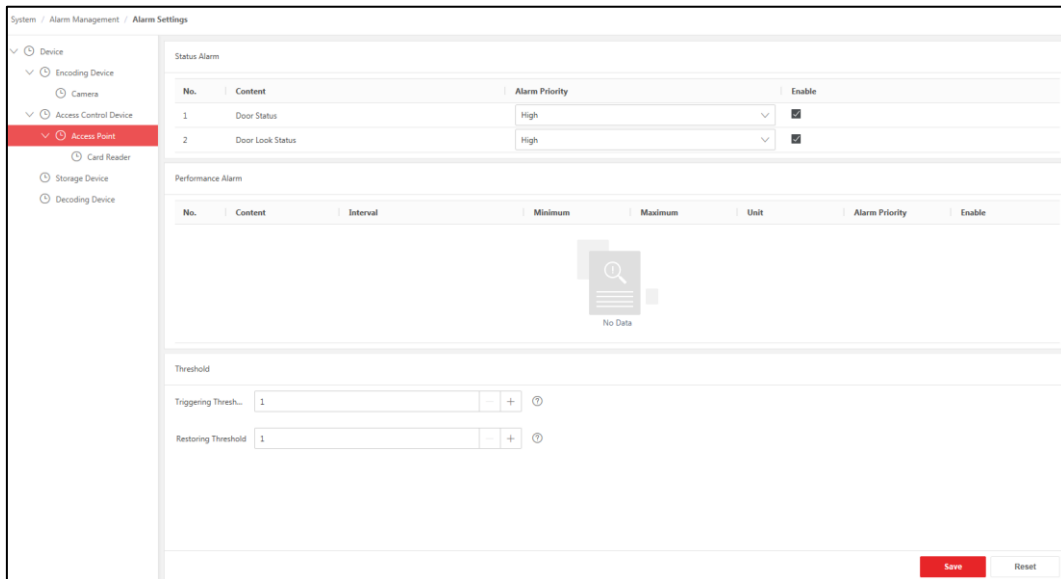
### Purpose:

Perform the following task to configure health monitoring alarm for access control point.

### 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.



No.	Content	Alarm Priority	Enable
1	Door Status	High	<input checked="" type="checkbox"/>
2	Door Lock Status	High	<input checked="" type="checkbox"/>

No.	Content	Interval	Minimum	Maximum	Unit	Alarm Priority	Enable
No Data							

Threshold

Triggering Thresh... 1  +

Restoring Threshold 1  +



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

### Purpose:

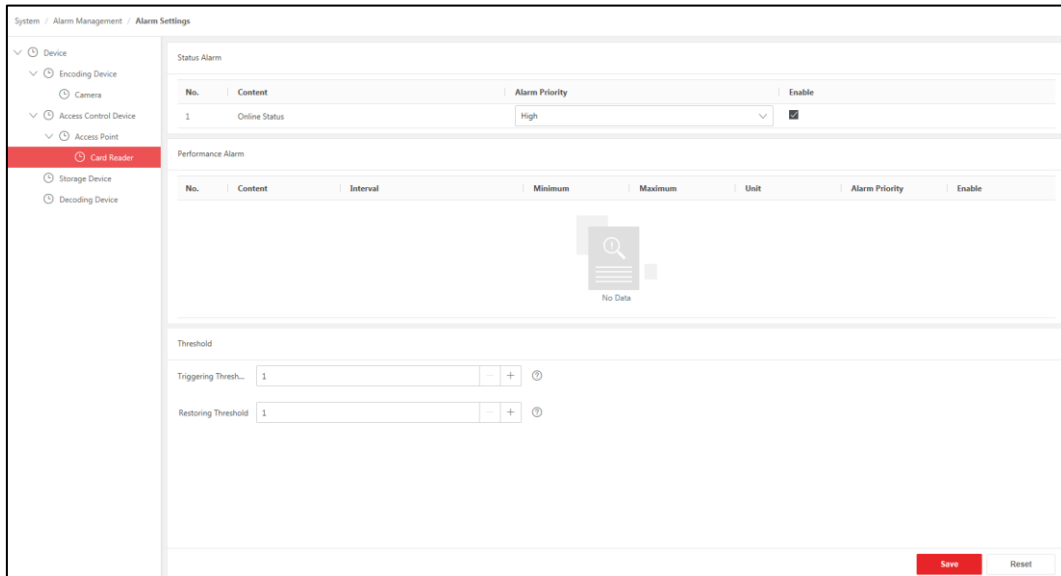
Perform the following task to configure health monitoring alarm for the card reader.

### Steps:

1. Click  -> **System Configuration** ->  **Network** -> **Alarm Configuraiton** 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.



No.	Content	Alarm Priority	Enable
1	Online Status	High	<input checked="" type="checkbox"/>

No.	Content	Interval	Minimum	Maximum	Unit	Alarm Priority	Enable
No Data							

Threshold

Triggering Thresh... 1  - +

Restoring Threshold 1  - +



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

### **Purpose:**

Perform the following task to configure health monitoring alarm for storage device.

### **Steps:**

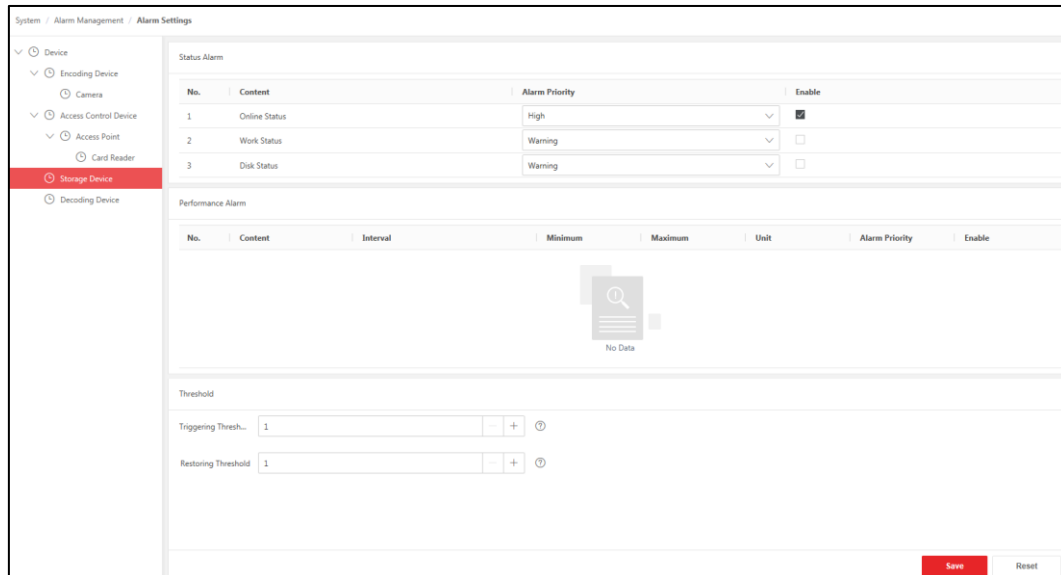
1. Click  -> **System Configuration** ->  **Network** -> **Alarm Configuraiton** to enter the Alarm Configuration page.
2. Select storage device from the device tree.
3. Enable the content(s) of the status alarm and set the alarm priority.

**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.





- 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.
- Click **Save**.

## Configure Alarm for Decoding Device

### **Purpose:**

Perform the following task to configure health status alarm for decoding device.

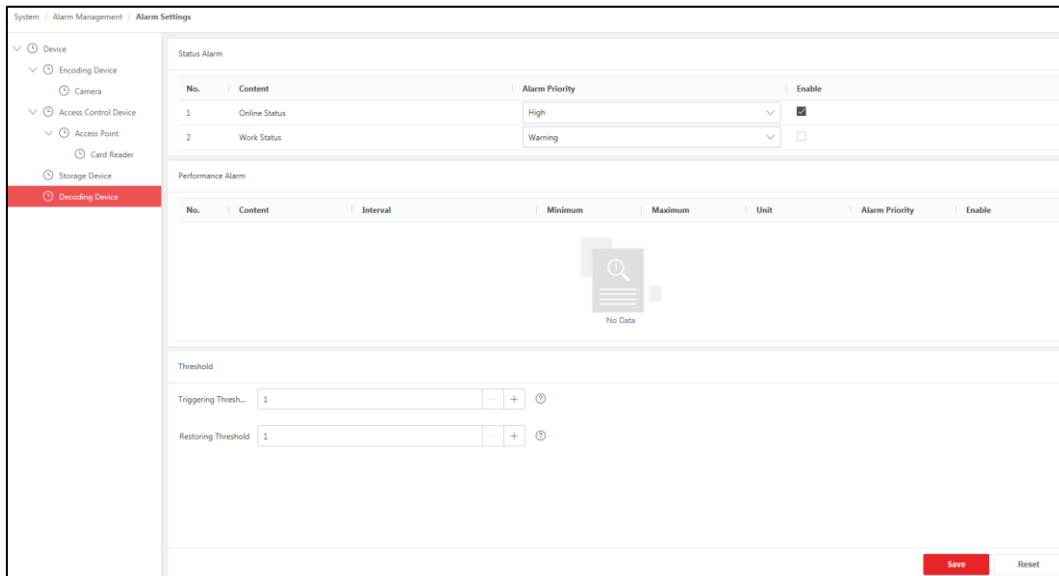
### **Steps:**

- Click  -> **System Configuration** ->  **Network** -> **Alarm Configuration** to enter the Alarm Configuration page.
- Select decoding device from the device tree.
- 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.



- 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.
- Click **Save**.



#### 4.14.4 Monitor Health Status of Subordinate System


##### **Purpose:**

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.

**Note:** For details about statistics of health monitoring data, refer to *Chapter 11 Maintenance*.

##### **Steps:**

- Click  -> **System Configuration** ->  **Maintenance** -> **Subordinate System** to enter the Subordinate System Configuration page.
- Click **Add** to enter the Add Subordinate System page.
- 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 health 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**.  
**Result:** 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.

## 4.15 Advanced Parameters Settings

### **Purpose:**



You can set the advanced parameters, including the device time synchronization, user security policy, and user experience program.

### 4.15.1 Synchronize Device Time

#### **Purpose:**

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.

### 4.15.2 Set User Security



#### **Purpose:**

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**.

### 4.15.3 Join User Experience Program

**Purpose:**

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**.

## 4.16 Menu Customization



**Purpose:**

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 5 Monitoring

## 5.1 Live View

### **Purpose:**




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.

### 5.1.1 Start Live View

#### **Purpose:**

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.

### 5.1.2 Manual Capture

#### **Purpose:**

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 *5.1.1 Start Live View*.
2. Move the cursor to the display window to show the toolbar and click  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 *5.3 Live View and Playback Settings*.










## 5.1.3 Manage View

### **Purpose:**

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 5.1.1 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.




## 5.1.4 PTZ Control

### **Purpose:**

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 <i>Add Single User</i> .
	Cancel the PTZ lock.
	Direction buttons and auto-scan.

## Configure Preset

### **Purpose:**

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** and start live view of the PTZ camera.  
The Video Surveillance client will pop up.
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 adding 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



### **Purpose:**

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** and start live view of the PTZ camera.  
The Video Surveillance client will pop up.
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.

**Notes:**

- 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

**Purpose:**

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

**Steps:**

1. Click **Live View** and start live view of the PTZ camera.  
The Video Surveillance client will pop up.
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.

## 5.1.5 Auto-Switch Live View

### **Purpose:**

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.

## 5.1.6 Auxiliary Screen Preview

### **Purpose:**

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 5.1.1 *Start Live View* and 5.1.3 *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.

## 5.1.7 Broadcast to Connected Devices

### **Purpose:**






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

### **Notes:**

- 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.

**Steps:**


1. Start live view. For details about starting live view, refer to *5.1.1 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.
    - 1) Click **Tool** -> **Broadcast**.
    - 2) 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
    - 1) Select a group and click .
    - 2) Enter group name.
    - 3) Click **OK**.
  - Edit Group.
    - 1) Select a group and click .
    - 2) Enter group name.
    - 3) Click **OK**.
  - Select a group and click  to delete the group.
  - Add Device.
    - 1) Click **Add**.
    - 2) Select an area and devices.
    - 3) Click **OK**.
  - Click  to delete a device.

## 5.1.8 Customize Icons on Live View Toolbar















**Purpose:**

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 *5.1.1 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	Turn off/on the live view sound.
	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. <b>Note:</b> 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. <b>Note:</b> 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.

## 5.2 Playback

### **Purpose:**

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.

## 5.2.1 Play Video File

### **Purpose:**

In the Playback module of HikCentral Enterprise 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 supports normal playback and synchronous playback.

### **Before You Start:**

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




## Normal Playback

### **Purpose:**

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:**










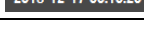








1. Click **Playback** on the Home page to open the Video Surveillance window.
 

**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 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 *5.2.4 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 <i>Synchronous Playback</i> .
	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 5.3 <i>Live View and Playback Settings</i> .
	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.
	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.
	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 <b>Esc</b> key on the keyboard to exit the full-screen mode.
	Configuration	Configure advanced video settings. For details about video settings, refer to 5.3 <i>Live View and Playback Settings</i> .



## Synchronous Playback

### **Purpose:**

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.

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

**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 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 *5.2.4 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*.


## 5.2.2 Add Tag for Video File

**Purpose:**

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 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 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.

## 5.2.3 Download Video File

### **Purpose:**


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 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 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.


## 5.2.4 Customize Icons on Playback Toolbar

### **Purpose:**



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 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. <b>Note:</b> For details about setting the saving path of the captured picture, refer to 5.3 <i>Live View and Playback Settings</i> .
	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. <b>Note:</b> For details about setting the saving path of the clipped video file, refer to 5.3 <i>Live View and Playback Settings</i> .
	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 <b>Unlock</b> 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. <b>Note:</b> 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 5.2.3 <i>Download Video File</i> .
	Show 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 5.2.2 <i>Add Tag for Video File</i> .
	Frame-Extracting Playback	Start playback frame by frame. <b>Note:</b> Frame-extracting playback should be supported by the device.
	Transcoding Playback	Enable playback in lower frame rate when the network condition is poor. <b>Note:</b> Transcoding playback should be supported by the device.




## 5.3 Live View and Playback Settings

### Purpose:

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

General Configuration	
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 will get stream from the device by default during live view instead of via media services.
PTZ Mode	HikCentral Enterprise 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.
Advanced Configuration	
Capture Configuration	<b>Picture Format:</b> Set the file format for the captured pictures during live view or playback as JPEG or BMP.
	<p><b>Capture Mode:</b> Set the capture method during live view and playback. Currently HikCentral Enterprise supports capturing single picture, and capturing pictures by time or by frame.</p> <ul style="list-style-type: none"> <li>● <b>By Time:</b> 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.</li> <li>● <b>By Frame:</b> 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.</li> </ul>
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 <b>Record Two-Way Audio</b> 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	<p>Enable GPU hardware decoding to save GPU resources during live view and playback.</p> <p><b>Note:</b> After enabling GPU decoding, restart live view or playback for GPU decoding to take effect.</p>
Live View Configuration	<ul style="list-style-type: none"> <li>● <b>Streaming Adaption:</b> 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.</li> <li>● <b>Resume Last Live View:</b> Restore the live view window last opened when you run the client next time.</li> <li>● <b>Display Online Status:</b> 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.</li> <li>● <b>Filter Offline Camera:</b> By enabling this function, offline devices will not be displayed during auto-switch.  <b>Note:</b> This button is available only when <b>Display Online Status</b> is enabled.</li> <li>● <b>VCA Information:</b> 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.</li> <li>● <b>Show Live Pictures by Default:</b> 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 <b>Download</b> in the prompt to download the captured picture.</li> </ul>
Playback Configuration	<p><b>Buffer before Decoding:</b> 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.</p>
	<p><b>Buffer after Decoding:</b> 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.</p>
	<p><b>VCA Information:</b> Display the VCA information during playback. VCA information refers to the intelligent event information on the camera,</p>

	<p>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.</p>
--	--



# Chapter 6 Map Application

## **Purpose:**

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 world. GIS map lets you view and access cameras at multiple locations around the world in a geographically correct way. If the resources locate in multiple locations (e.g., different cities, different countries), GIS map can give you a single view to show them all and help you quickly go to each location to view video 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 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.

## **Before You Start:**




Before any operations on the map, you should configure the maps and the add resources to the maps first. For details, refer to *4.7 Map Configuration*.




## 6.1 Manage Hot Spot

### **Purpose:**

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.







## 6.2 Operate Map


### **Purpose:**

You can perform some basic operations on the map, such as adding label, measuring distance, zooming in/out, etc.

**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.

## 6.3 View Alarm on Map

### *Purpose:*






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.

### 6.3.1 View Real-Time Alarm

#### *Purpose:*

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.

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 *5.1 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 *4.6 Event Configuration*.

## 6.3.2 Search History Event

### **Purpose:**

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 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 [4.6 Event Configuration](#).







## 6.4 Play Driving Pattern

### **Purpose:**

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.

**Note:** This function should be supported by the device.

### **Steps:**

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 7 One-Card

HikCentral Enterprise provides multiple functions in one card system module, including card issuing, access control management, elevator control management, visitor management, and attendance and time management.

## 7.1 Issue Cards

**Purpose:**

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

### 7.1.1 Set Card Issuing Parameters

**Purpose:**

HikCentral Enterprise 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.

### 7.1.2 Write to Card

**Purpose:**

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.

**Note:** Long range card can only be written in Windows 10.

**Before You Start:**

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

**Steps:**

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.



## 7.1.3 Issue Card to Person



**Purpose:**

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.

**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.

**Steps:**

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. (Optional) 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. (Optional) 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. (Optional) 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.

## 7.1.4 Operate Card

### **Purpose:**

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.

## Import Cards

### **Purpose:**

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**.

## Report Card Loss

### **Purpose:**

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.




## Return Card

### **Purpose:**

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.



## Replace Card

### **Purpose:**

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..

## 7.2 Access Control

### **Purpose:**

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.




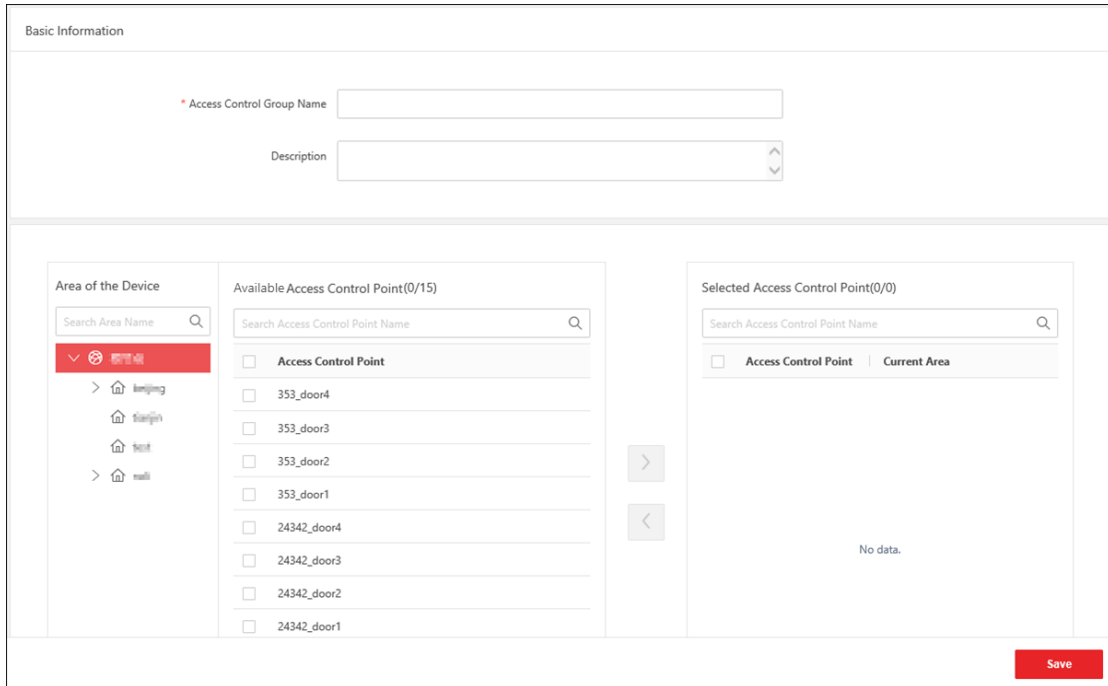
## 7.2.1 Add Access Control Group

### Purpose:

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**.
2. Click **Access Control Group** tab to enter access control group management page.
3. Click **Add** to open the adding access control group page.



Basic Information

\* Access Control Group Name

Description

Area of the Device

Search Area Name

Available Access Control Point(0/15)

Search Access Control Point Name


Selected Access Control Point(0/0)

Search Access Control Point Name

Access Control Point | Current Area

No data.

Save

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.

## 7.2.2 Add Person Group



### Purpose:

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 *4.1 Person Management*.

### Steps:

1. Click **Access Control** on the Home page and enter  **Group**.
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 textbox 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.

Basic Information

\* Person Group Name

Description

---

Organization of Person



- Home
- Home
- Home

Available Person(0/6)  Include Sub Organization

<input type="checkbox"/>	Name	Employee No.	Biometric F...
<input type="checkbox"/>	Leo	201820**	
<input type="checkbox"/>	Atex	201820**	
<input type="checkbox"/>	Jay	200120**	
<input type="checkbox"/>	Jenny	100100*	
<input type="checkbox"/>	cxz	213412	

Selected Person(0/0)

<input type="checkbox"/>	Name	Employ...	Organiz...	Biometr...
No data.				

- 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.

## 7.2.3 Configure Access Control Schedule Template

### **Purpose:**

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

### Purpose:

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:

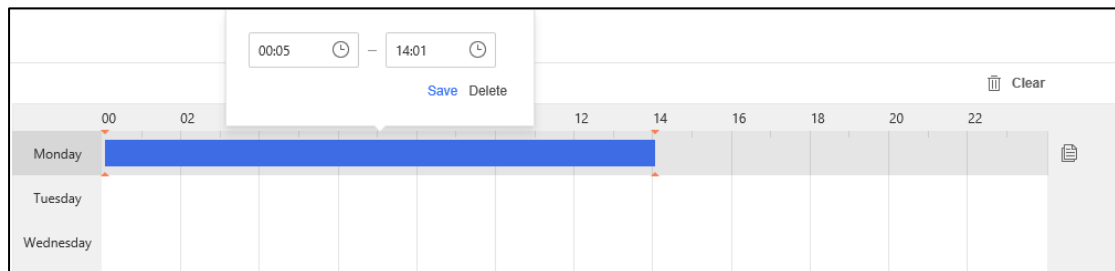
1. Click **Access Control** on the Home page and enter  **Schedule Template**.
2. Click **Holiday Group** tab to enter holiday group management page.
3. Click **Add** to open the adding holiday group page.
4. Create a name for the holiday group.
5. (Optional) Enter the remark information in the **Description** 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.



- 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

### Purpose:

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.

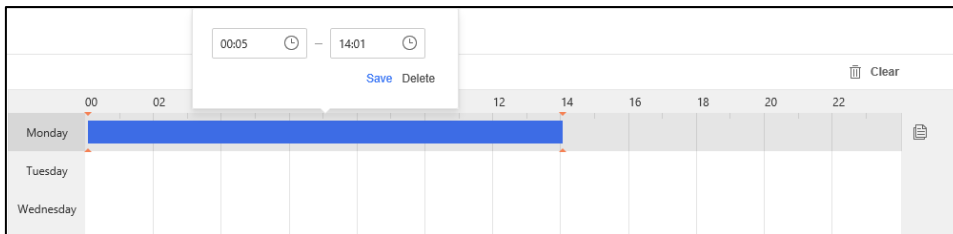
**Note:** There is a default schedule: All-Day Schedule, which cannot be edited or deleted. For All-Day schedule, card swiping is valid on each day of the week.


3. Click **Add** to open the adding 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.



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.

## 7.2.4 Configure Access Control Permission

**Purpose:**


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

### Purpose:

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:

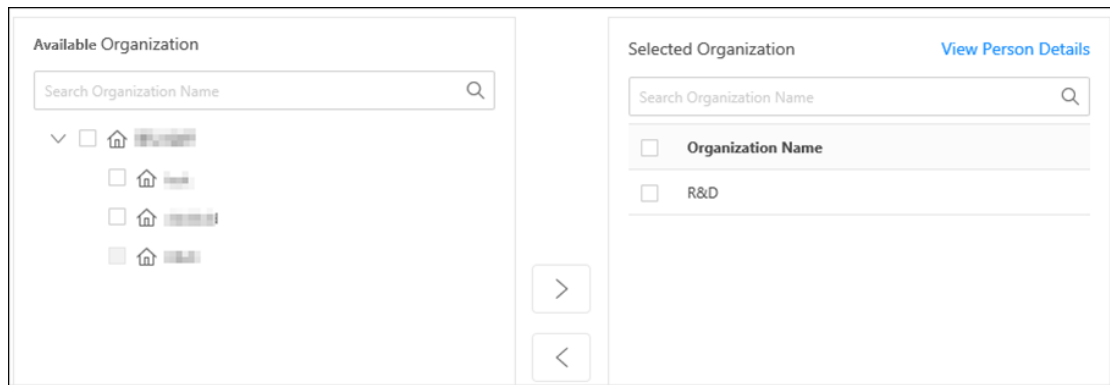
1. Click **Access Control** on the Home page and enter  **Permission Configuration**.
2. Select a tab as assigning permission mode.
  - **By Organization:** Assign access control permissions to persons in an organization to access specified access control point(s).
  - **By Person Group:** Assign access 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 adding 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 7.2.3 *Configure Access Control Schedule Template*.


5. Select organization, person group or person from the appropriate list.

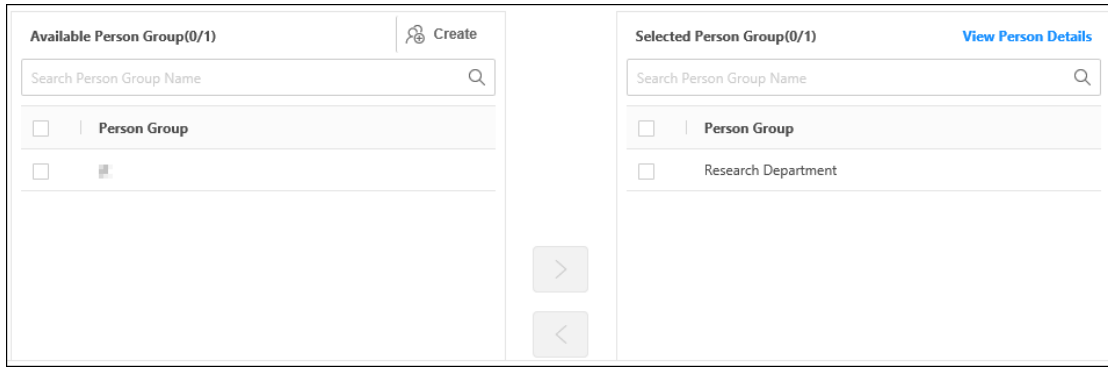
- **Assign Permission by Organization**

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



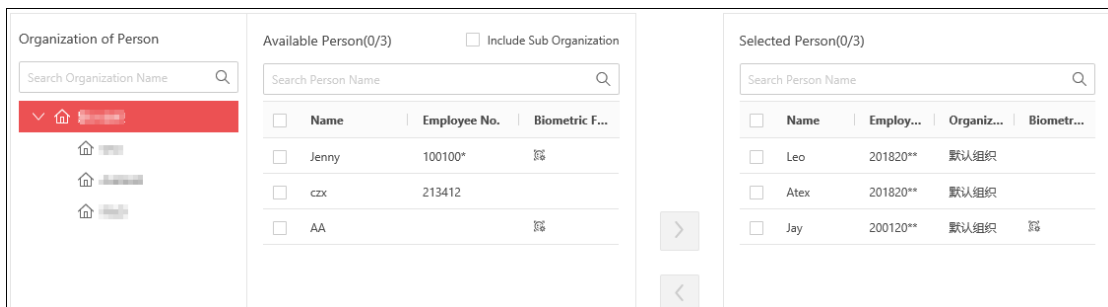
- **Assign Permission by Person Group**

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



- **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.



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



### Purpose:

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.
  - a. Enter  **Biometric Recognition**.
  - b. Select an area to filter the access control points.
  - c. Click  or .
  - d. 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.

## Search Assigned Permission

### **Purpose:**

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 **Expand** to set more conditions.
  4. Click **Search**.
- The matched search results will display.

## Check Permission Applying Record

### **Purpose:**

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.

## 7.2.5 Configure Card Holder of Special Card

### **Purpose:**

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.

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:** The door can be opened by swiping the duress card when duress occurs. At the same time, the system will report the duress event.
- **Super Card:** The card is valid for all the doors of the controller during the configured schedule.

### **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 *7.2.4 Configure Access Control Permission*.


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:**

1. Click **Access Control** on the Home page and enter  **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.

## 7.2.6 Configure Multiple Authentication



### **Purpose:**


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 *7.2.4 Configure Access Control Permission*.

### **Steps:**

1. Click **Access Control** on the Home page and enter  **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 *7.2.3 Configure Access Control 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.

## 7.2.7 Configure First Card Opening Door






### **Purpose:**

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 *7.2.4 Configure Access Control Permission*.

### **Steps:**

1. Click **Access Control** on the Home page and enter  **Remain Open with First Card**.
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 filter 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.

## 7.2.8 Configure Anti-passback

### **Purpose:**





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 7.2.4 *Configure Access Control Permission*.

**Steps:**

1. Click **Access Control** on the Home page and enter  **Anti-Passback**.
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 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.  
Example: If you select Entrance Reader 1 as the first card reader, and select Exit Reader 1, Exit Reader 2 as the linked readers, then you can only get through the access control point by swiping the card in the order as Entrance Reader 1, Exit Reader 1 and Exit Reader 2.
  - 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.

## 7.2.9 Configure Multi-Door Interlocking



**Purpose:**



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 7.2.4 *Configure Access Control Permission*.

**Steps:**

1. Click **Access Control** on the Home page and enter  **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.

## 7.2.10 Configure Reader Authentication Mode



### **Purpose:**

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


### **Before you start:**

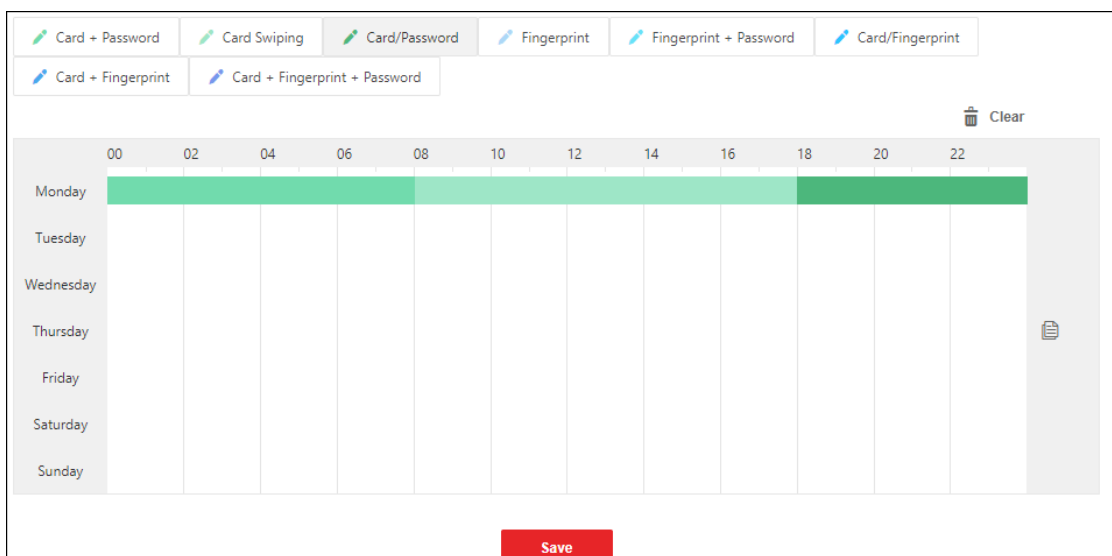
Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to [7.2.4 Configure Access Control Permission](#).



### **Steps:**

1. Click **Access Control** on the Home page and enter  **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.  
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.



- 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.

## 7.2.11 Configure Access Control Status



### **Purpose:**


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

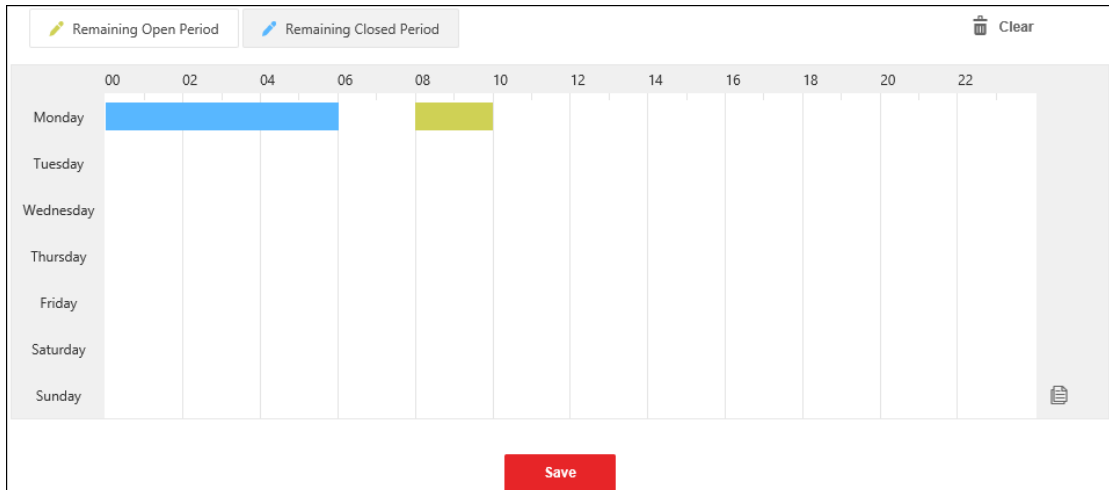
### **Before you start:**



Make sure you have assigned the access control permission and applied the permission to the access control device. For details, refer to *7.2.4 Configure Access Control Permission*.

### **Steps:**

1. Click **Access Control** on the Home page and enter  **Remaining 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.



- 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.

## 7.2.12 Configure Capture Linkage



### **Purpose:**

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 *7.2.4 Configure Access Control Permission*.

### **Steps:**

1. Click **Access Control** on the Home page and enter  **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.

## 7.2.13 Search Access Control Event

### **Purpose:**


You can search the access control history events including person access event and access control device event.

## Search Person Access Event

### **Purpose:**

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 *7.2.12 Configure Capture Linkage* 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).

## Search Access Control Device Event

### **Purpose:**

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  **Access Control 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.

## 7.3 Visitor

### **Purpose:**

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

### 7.3.1 Visitor Reservation

#### **Purpose:**


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.

### Make a Reservation for One Visit

#### **Purpose:**

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

#### **Steps:**

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.

**Note:** For pre-defining the purposes, refer to [4.10.4 Pre-Define 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**.


### Import Reservations for Visitors

#### **Purpose:**

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

#### **Steps:**



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 visatee 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.

## 7.3.2 Group Permissions







### **Purpose:**

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. For details, refer to [4.10.3 Set Visitor Permissions](#).

### **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.

### 7.3.3 Search Visit Records

**Purpose:**

The visit records are stored in the system database after the visitors' check-in, such as the visiting time, visitor detail, visatee 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, visatee, 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.



**Note:** For setting the visitor groups, refer to 4.10.8 Group Visitors.
6. (Optional) Click **Export** to export the filtering results displayed in the list and save it in the local PC.

### 7.3.4 View Unauthorized Visit Records

**Purpose:**

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. (Optional) Enter the conditions to filter the access records.
4. (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.

**Note:** For setting the visitor groups, refer to 4.10.8 Group Visitors.

## 7.3.5 View Permissions Applied to Visitors



### **Purpose:**

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

- 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. (Optional) 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.

## 7.4 Elevator Control

### **Purpose:**



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.

### 7.4.1 Add Floor Group

#### **Purpose:**

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.

## 7.4.2 Configure Elevator Control Permission

### **Purpose:**






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

#### **Purpose:**

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. 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


#### **Purpose:**

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 cursor 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. (Optional) Click  to check the progress of the applying task.

## Check Permission Applying Record

### **Purpose:**

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. (Optional) Click  in Details column to check applying result and export search result.

## 7.4.3 Configure Elevator Control Status




### **Purpose:**

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 *7.4.2 Configure Elevator Control Permission*.

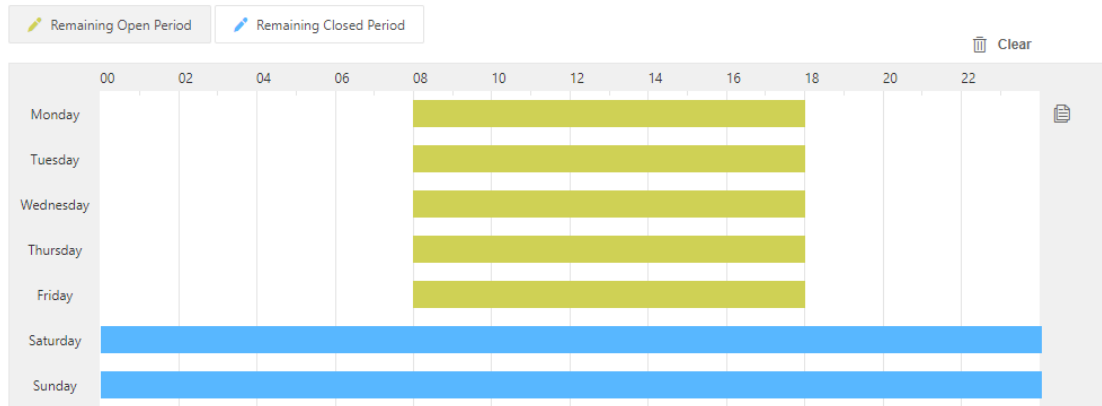
### **Steps:**



1. Click **Elevator Control** on the Home page and enter  **Remaining Open/Closed Settings**.
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.

## 7.4.4 Search Elevator Control Event

### **Purpose:**


You can search the elevator control history events including person access event and elevator control device event.

### Search Person Access Event

### **Purpose:**

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. (Optional) Click **Export** to export the search results to local PC.

## Search Elevator Control Device Event

### **Purpose:**

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. (Optional) Click **Export** to export the search results to local PC.

## 7.5 Time and Attendance

### **Purpose:**

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.

### 7.5.1 Manage Shift Group

#### **Purpose:**


The persons in one shift group are assigned with the same shift schedule. You can group persons into different attendance groups.

### Add Shift Group with Multiple Persons

#### **Purpose:**

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 **Time and 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 textbox 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.

## Add Shift Group with Single Person

### **Purpose:**

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 **Time and 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.

## 7.5.2 Manage Shift

### **Purpose:**

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.

## Configure Shift Rule for Normal Shift

### **Purpose:**

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 **Time and 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**.

## Add Normal Shift

### **Purpose:**

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 **Time and 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.
    - Note:** For details about setting the shift rule, refer to *Configure Shift Rule for Normal Shift*.
  - 3) Set the **Apply** switch to on as desired.
7. Click **Save**.


## Add Man-Hour Shift

### **Purpose:**

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 **Time and 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**.

## Add Check-in Shift

### **Purpose:**

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 **Time and 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 textbox 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**.

## 7.5.3 Configure Holiday

**Purpose:**

You can add the holiday during which the check-in or check-out function will be invalid.

**Steps:**

1. Click **Time and Attendance** on the Home page and enter  **Holiday**.
2. Click **Add** to enter adding holiday page.
3. Create a name for the holiday.
4. (Optional) 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.

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**.

## 7.5.4 Configure Shift Schedule

**Purpose:**

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.

### Configure Normal Shift Schedule

**Purpose:**


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. For details about setting the shift group, refer to 7.5.1 *Manage Shift Group*. For details about adding the shift, refer to 7.5.2 *Manage Shift*.

**Steps:**

1. Click **Time and 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.

< December 2018 >						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3 Man-Hour Shift test 08:00	4 Man-Hour Shift test 08:00	5 Man-Hour Shift test 08:00	6 Man-Hour Shift test 08:00	7 Man-Hour Shift test 08:00	8
9	10 Man-Hour Shift test 08:00	11 Man-Hour Shift test 08:00	12 Man-Hour Shift test 08:00	13 Man-Hour Shift test 08:00	14 Man-Hour Shift test 08:00	15
16	17 Man-Hour Shift test 08:00	18 Man-Hour Shift test 08:00	19 Man-Hour Shift test 08:00	20 Man-Hour Shift test 08:00	21 Man-Hour Shift test 08:00	22
23	24 Man-Hour Shift test 08:00	25 Man-Hour Shift test 08:00	26 Man-Hour Shift test 08:00	27 Man-Hour Shift test 08:00	28 Man-Hour Shift test 08:00	29
30	31 Man-Hour Shift test 08:00					

9. (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

## Configure Advanced Shift Schedule

**Purpose:**


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. For details about setting the shift group, refer to 7.5.1

*Manage Shift Group.* For details about adding the shift, refer to 7.5.2 *Manage Shift*.

**Steps:**

1. Click **Time and 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

## 7.5.5 Configure Attendance Check Point


**Purpose:**

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. For details, refer to 4.5.2 *Manage Access Control Device*.

**Steps:**

1. Click **Time and 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**.

## 7.5.6 Manage Attendance Adjustment

### **Purpose:**


You can set the attendance adjustment reason and adjust check-in/out time for the attendance records according to actual needs.

## Configure Adjustment Reason

### **Purpose:**

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 **Time and 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**.

## Correct Attendance Record

### **Purpose:**

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 **Time and 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**.



## 7.5.7 Recalculate Attendance Data

### **Purpose:**

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 **Time and 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.

## 7.5.8 Search Attendance Information

**Purpose:**


You can search the persons' card swiping records and view the attendance results based on the card swiping records.

### Search Swiping Record

**Purpose:**

You can set the search conditions and search the persons' card swiping records.

**Steps:**


1. Click **Time and 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. (Optional) Click **Export** to export the search result to the local PC.

### Search Detailed Attendance Result

**Purpose:**

You can search the attendance result details including on-work time, off-work time, late duration, early leave duration, etc.

**Steps:**

1. Click **Time and 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. (Optional) Click **Export** to export the search result to the local PC.

## 7.5.9 Generate Attendance Report

### *Purpose:*


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.

## Generate Person Attendance Report

### *Purpose:*

You can generate the person attendance report for exporting the detailed data to local storage.

### *Steps:*

1. Click **Time and 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.




## Generate Organization Attendance Report

**Purpose:**

You can generate the organization attendance report for exporting the detailed data to local storage.

**Steps:**

1. Click **Time and 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.

# Chapter 8 Parking System

## **Purpose:**

HikCentral Enterprise 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 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.

## 8.1 Manage Vehicles

In general, there are three categories of vehicles in HikCentral Enterprise:

- **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 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.

### 8.1.1 Group Registered Vehicles

#### **Purpose:**


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.


**Note:** One vehicle can only be added to one group.

#### **Before You Start:**

Add registered vehicles to the system. For details, refer to *4.3 Manage Registered Vehicles*.

#### **Steps:**

1. Click **Parking** on Home page and enter  **Vehicles and Cards -> Vehicle Group**.
2. Click **Add** to enter the Add Vehicle Group page.
3. Enter a name for the group.

4. (Optional) Enter the description for the group.
5. In the Selectable Vehicle list, all the vehicles which haven't been added to any groups will display. Select the vehicles you want to add to the group.
6. Click  to add the selected vehicles to the Selected Vehicle list.
7. Click **Save**.

## 8.1.2 Manage Vehicles in Blacklist

### **Purpose:**

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.

### **Notes:**




- For setting the blacklist alarm and configuring linkage action, refer to [4.6 Event Configuration](#).
- For setting allowing or forbidding vehicles in blacklist to pass, refer to [4.13.5 Set Parameters](#).

## Add One Vehicle to Blacklist

### **Purpose:**

You can add the vehicle to the blacklist one by one.

### **Steps:**


1. Click **Parking** on Home page and enter  **Vehicles and Cards -> Vehicle in Blacklist**.
2. Click **Add**.
3. Set the arming mode as Plate Number or Card No.
  - **Plate Number:** 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

### **Purpose:**

import multiple vehicles by uploading a file with vehicle information to the system.

### **Steps:**

1. Click **Parking** on Home page and enter  **Vehicles and Cards -> 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

### **Purpose:**

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  **Vehicles and Cards -> 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.


## 8.1.3 Manage Temporary Card

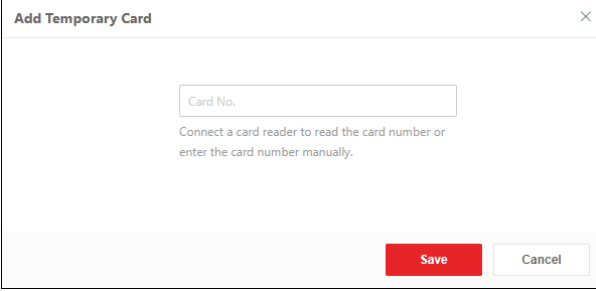
### **Purpose:**


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.

You need to add temporary cards to the system first.

### **Steps:**

1. Click **Parking** on Home page and enter  **Vehicles and Cards -> 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 card(s) and click **Delete** to delete the selected cards from the system.

## 8.2 Manage Entry & Exit Rules

### **Purpose:**

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.

### 8.2.1 Set Entry & Exit Rule for Vehicles in Group


#### **Purpose:**

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  **Entry & 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 from the dropdown 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.
7. (Optional) Enter the description information to describe the rule.
8. Click **Save**.


## 8.2.2 Set Free Entry & Exit on Holidays

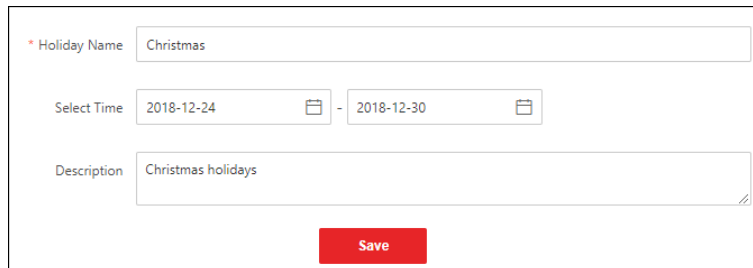
### **Purpose:**

For public parking lots, on normal days, the vehicle owners need to pay the parking fee when they exit the parking lot. On holidays, you can set free parking so that the registered and temporary vehicles can park in the parking lot without any charge.

You need to define the holidays in the system, and on the days of the holidays, the parking will be free.

### **Steps:**

1. Click **Parking** on Home page and enter  **Entry & Exit Control -> Free Entry & Exit on Holidays**. The added parking lots are displayed on the left.
2. Select a parking lot to add free parking.
3. Click **Add**.



4. Enter a name for the holiday.
5. Set the start date and end date of the holiday.
6. (Optional) Enter the description information to describe the holiday.
7. Click **Save**.

## 8.3 Make a Parking Reservation


### **Purpose:**

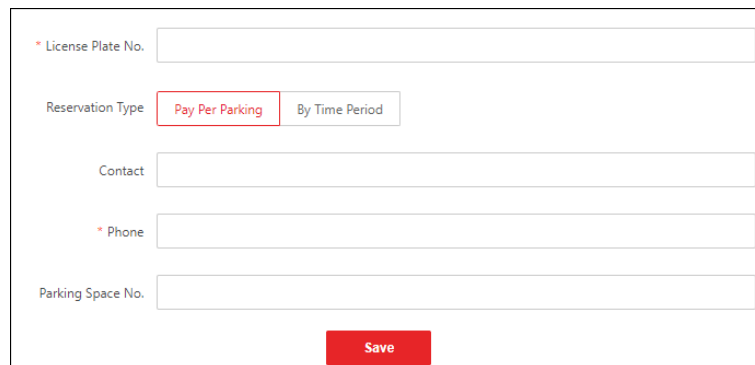
The visitors can contact the parking lot administrator if they want to park their vehicles in the parking

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.

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. Click **Parking** on Home page and enter  **Reservation**.  
The added parking lots are displayed on the left.
2. Select a parking lot to add a reservation.
3. Click **Reserve**.



4. Enter the license plate number of the visitor's vehicle.
5. Select the reservation type.
  - **By Times:** The reservation is valid for a certain duration from the time the reservation is added. For setting the duration, refer to *Other Parameters*.
  - **By Time Period:** Set the start time and end time for the reservation. During the time period, the reservation is valid.
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. (Optional) Enter the No. of the parking space which is assigned for this reservation.
9. Click **Save**.

## 8.4 Manage Parking Spaces

**Purpose:**

In this section, you can manage the parking spaces in the lot, such as setting the parking space type, link the parking space to vehicles, etc. You can also correct the number of vacant parking spaces if needed.

### 8.4.1 Correct Number of Vacant Parking Spaces

**Purpose:**

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 will 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.

You can get the current number of vacant parking spaces by searching the vehicles in parking lot. For details, refer to *8.5.2 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**.

## 8.4.2 View and Search Parked Vehicles

**Purpose:**

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. Click **Parking** on Home page and enter  **Parking Spaces -> Parking Space Settings**.

The added parking lots are displayed on the left.

2. Select a parking lot and click the button on the lower-right corner to enter the map of the whole floor.

The map of the parking lot display. You can view the status of each parking space, such as the parking space is occupied or is vacant.

3. In the search bar, select the searching mode from the dropdown list.
  - **Space No.:** 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.
4. Click **Search**.
5. (Optional) Click **Vehicle with No 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.



## 8.4.3 Set Parking Spaces

### **Purpose:**

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.





## Add Parking Space Type

### **Purpose:**

The system pre-defines five types of parking spaces. You can also customize other types according to actual needs.

**Note:** Up to 5 custom types of parking spaces can be added.

### **Steps:**


1. Click **Parking** on Home page and enter  **Parking Spaces** -> **Parking Space Settings**.  
The added parking lots are displayed on the left.
2. Select a parking lot and click the button on the lower-right corner to enter the map of the whole floor.
3. Click **Settings**.
4. Select a parking space on the map and click  in the Parking Space Type field
5. Click **Add** and enter a name for the custom type.  
The system will assign a color for the newly added type automatically.
6. (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.

## Classify Parking Spaces to Different Types

### **Purpose:**

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. Click **Parking** on Home page and enter  **Parking Spaces** -> **Parking Space Settings**.  
The added parking lots are displayed on the left.
2. Select a parking lot and click the button on the lower-right corner to enter the map of the whole floor.  
The map of the parking lot display. You can view the status of each parking space, such as the parking space is occupied or is vacant.
3. Click **Settings**.
4. Select parking space(s) on the map. You can drag to select multiple parking spaces or press and

hold *Ctrl* to select multiple spaces.


5. In the Parking Space Type field, select a type from the dropdown list.
6. Click **OK**.

## Link Parking Space with Vehicle

### **Purpose:**

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:**

1. Click **Parking** on Home page and enter  **Parking Spaces** -> **Parking Space Settings**.  
The added parking lots are displayed on the left.
2. Select a parking lot and click the button on the lower-right corner to enter the map of the whole floor.  
The map of the parking lot display. You can view the status of each parking space, such as occupied or vacant.
3. Click **Settings**.
4. Select parking space(s) on the map. You can drag to select multiple parking spaces or press and hold *Ctrl* to select multiple spaces.
5. In the Link with field, select whether the vehicle is allowed to park in or not.
6. 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).
7. Click **Link**.

## 8.5 Search

### **Purpose:**

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.

### 8.5.1 Search Vehicle Passing Records

#### **Purpose:**

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.

## 8.5.2 Search Vehicles in Parking Lot

### **Purpose:**

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.

## 8.5.3 Search Parking Records in Parking Spaces

### **Purpose:**

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.

Click **Parking** on Home page and enter  **Search -> Parking in Parking Spaces.**

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.

## 8.5.4 Search Reservation Records

### **Purpose:**

After making a reservation, the reservation will be recorded in the database. You can search the reservation records by setting filter conditions.

**Note:** For details about reservation a parking, refer to [8.3 Make a Parking Reservation](#).

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.

## 8.6 Generate Traffic Flow Report

### **Purpose:**

Reports, created for a specified period, are essential documents, which are used to check whether a business runs smoothly and effectively. In HikCentral Enterprise, 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 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 report and save in the PC running the Web Client.

## 8.7 Manage Advertisements

### **Purpose:**

There is a screen on the self-service terminals (including query terminals). You can release an advertisement to the self-service terminals as promotion.


### 8.7.1 Uploading a Poster

#### **Purpose:**

You need to upload a poster to the system first.

**Note:** The image of the poster should be in JPG, PNG, or BMP format. The recommended dimension is 1920 × 1280.

#### **Steps:**

1. Click **Parking** on Home page and enter  **Advertisement -> Upload Poster**.
2. Drag the image of the poster to the dashed area or click **Here** to upload one.  
The image will be uploaded to the system
3. (Optional) You can click **Upload** to upload other pictures.
4. (Optional) To delete the uploaded posters, select the picture(s) and click **Delete**.


### 8.7.2 Release Poster to Self-Service Device

#### **Purpose:**

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. Click **Parking** on Home page and enter  **Advertisement -> Release Poster**.  
The uploaded posters will display.

2. Select the poster(s) and self-service terminals that will display the selected posters.
3. Specify the seconds of the display interval.  
The selected posters will display on the self-service terminals in turns and each poster displays for the configured interval.
4. Click **OK**.

## Chapter 9 Search Event


### **Purpose:**

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. For details about configuring event, refer to *4.6 Event Configuration*.

### **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. (Optional) 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 10 Search Pictures





### **Purpose:**

You can search for the captured pictures stored in the server, sort the captured pictures by camera or by time, view larger pictures, download pictures, etc.

### **Before You Start:**

Configure a capture schedule. For details about configuring a capture schedule, refer to *Configure Capture Schedule*.

### **Steps:**

1. Click **Picture Search** in the Home page.
2. Select an area.
3. In the Time field, set the time period for search.
4. Click **Search**.
5. (Optional) Click **By Camera** or **By Time** to sort the founded pictures.
  - **By Camera:** The pictures will be listed in the sequence of the camera list in the left column.
  - **By Time:** The pictures will be listed in a reverse chronological order.
6. (Optional) Perform the following operation(s).
  - Click a picture to view the larger picture.
  - Click  to download the picture.
  - Click  or  to go to the next or previous picture.
  - Click  to start slideshow of the captured pictures.

# Chapter 11 Maintenance

## Purpose:

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.

## Before You Start:

You should have configured health monitoring schedule and health status alarm. For details, refer to [4.14 Maintenance Configuration](#).

## 11.1 Status Overview

### Purpose:

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. For details about configuring health monitoring schedule, refer to [4.14.1 Configure Health Monitoring Schedule](#).

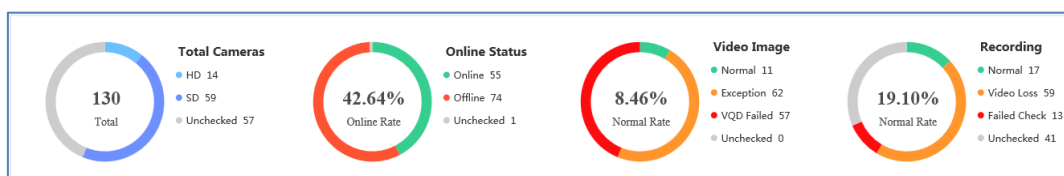
On the Home page, click **Maintenance** -> **Overview** to enter the Status Overview page, and then select an area from the drop-down box on the upper-left of the page to view the status overview of the resources in the selected area.

### 11.1.1 Doughnut Chart

#### Purpose:

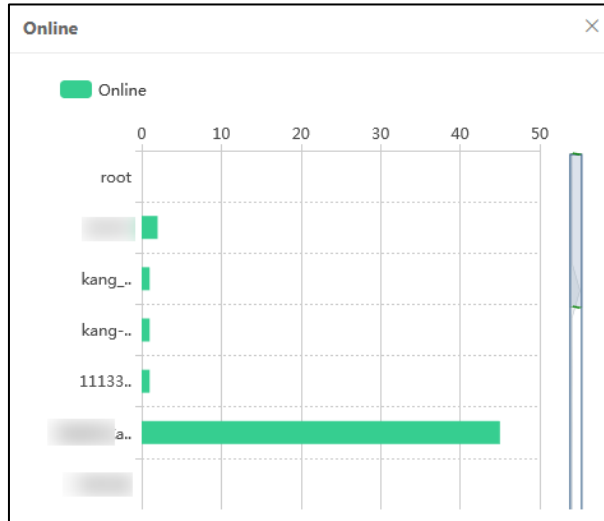
The doughnut charts on the top of the Operation and Maintenance page show total number, online rate, video image normal rate, and recording normal rate of the cameras in the selected area. You can view the details of the doughnut charts.

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.





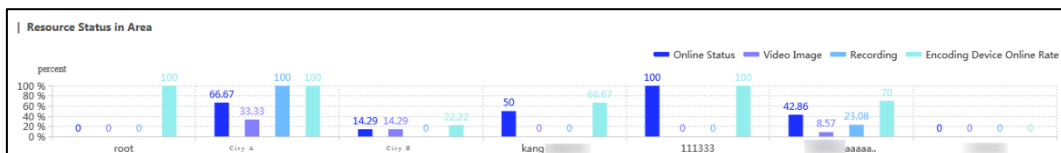
Camera Name	Area	IP Address
172.42_ SDKCa...	SDK1111111111...	10.67.172
172.42_SDK Cam...	SDK1111111111...	10.67.172
172.42_Camera 0...	SDK1111111111...	10.67.172
172.42SDKCamer...	SDK1111111111...	10.67.172
172.42_SDK Cam...	SDK1111111111...	10.67.172
172.42_SDK Cam...	SDK1111111111...	10.67.172
172.42_SDK Cam...	SDK1111111111...	10.67.172
172.42_SDK Cam...	SDK1111111111...	10.67.172
172.42_SDK C...	SDK1111111111...	10.67.172

## 11.1.2 View Resource Status in Area

**Purpose:**

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.

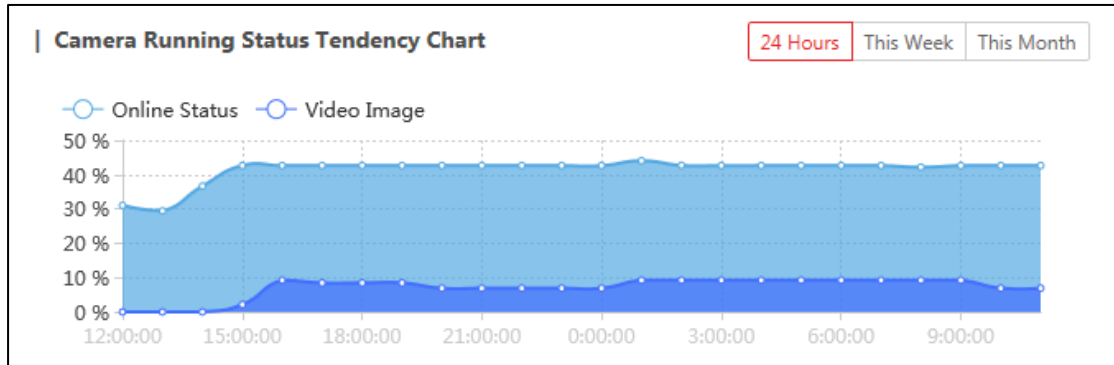
- Click the column to view the resource offline details or exception details.

### 11.1.3 Camera Status Tendency Chart

**Purpose:**

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.

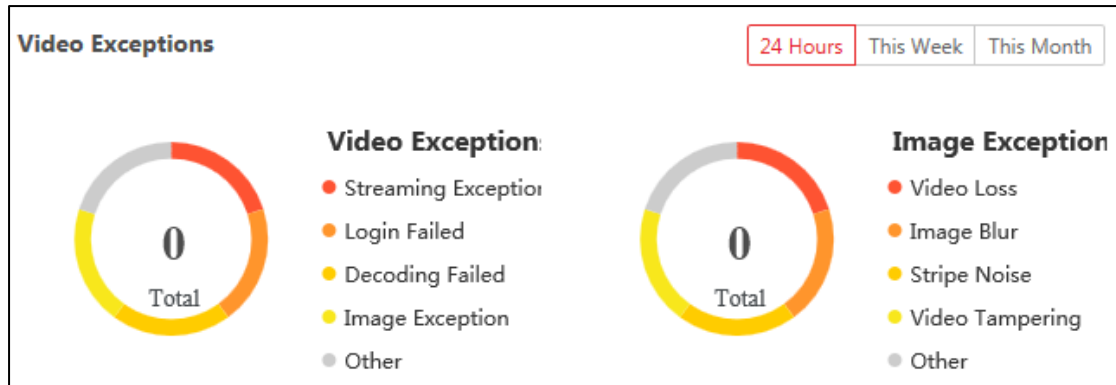
- Select a time period for the statistics.
  - 24 Hours:** Display the camera online rate and image normal rate in each time point within 24 hours.
  - This Week:** Display the camera online rate and image normal rate in each time point in the current week.
  - This Month:** Display the camera online 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.

### 11.1.4 Video Exceptions

**Purpose:**

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.

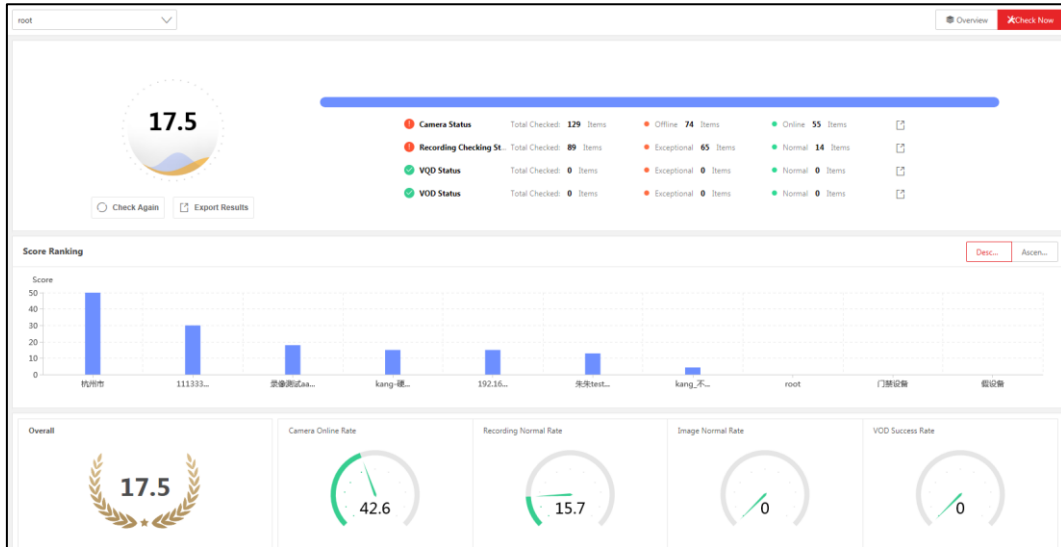
## 11.1.5 Quick Check of Overall Health Status


### **Purpose:**

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.

## 11.2 Status Monitoring (Video)

### **Purpose:**


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.

### 11.2.1 Camera Online Detection

#### **Purpose:**




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:**

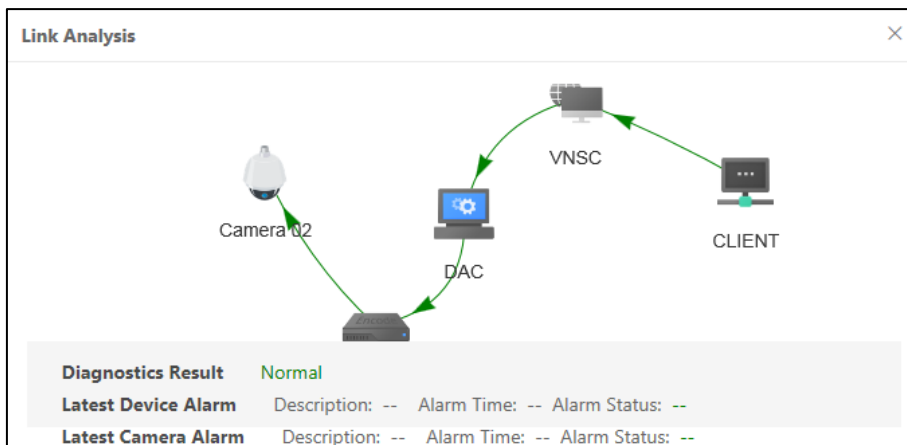
1. On the Home page, Click **Status Monitoring (Video)** in the Maintenance section and then click  **Camera -> Online Detection** to enter the Online Detection page.
2. Select an area from the area list.



**Result:**

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 **Contain Subordinate 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.

## 11.2.2 Video Quality Diagnosis

**Purpose:**

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.


**Result:**

The video quality diagnosis results of the cameras in the selected area will be displayed.

3. (Optional) Uncheck **Contain Subordinate Area** to ignore the video quality diagnosis results of the

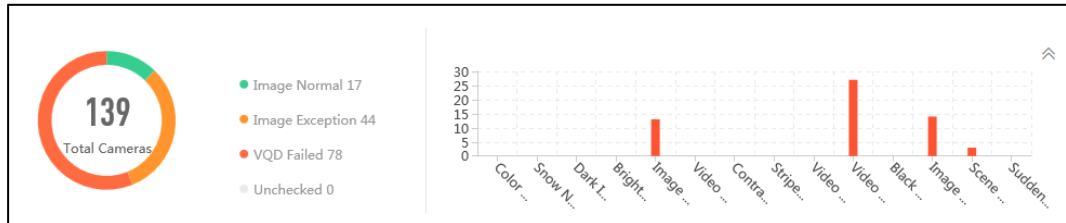
subordinate areas of the selected area.







4. (Optional) 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 details of the diagnosis result, such as basic information and history diagnosis.  
In history diagnosis, you can click  to select a month to view the history information.

## 11.2.3 Recording Check

### **Purpose:**

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 Monitoring (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.

### **Result:**

The retention status of the cameras in the selected area will be displayed.

3. (Optional) Uncheck **Contain Subordinate 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 status in a

doughnut 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.






## 11.2.4 Device Status

### **Purpose:**

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 Monitoring (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.

### **Result:**

The retention status of the devices in the selected area will be displayed.

3. (Optional) Uncheck **Contain Subordinate 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.

## 11.2.5 Topology

### **Purpose:**



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

### **Purpose:**

You can draw and edit topology according to actual needs.

### **Steps:**

1. On the Home page, Click **Status Monitoring (Video)** in the Maintenance section and then click  **Camera -> Topology** to enter the Topology page.
2. Add a view.
  - 1) Click  to open the Add View window.
  - 2) Create a view name.
  - 3) 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.
  - 4) 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.
  - 5) Click **OK**.
3. Select the view and click **Edit Topology** to enter the editing mode.
4. Add elements to the view.

### **Choose from:**

- 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.

**Node**

Element Name

\* Select Device Type  

Select Device Type

Cancel
Link Resource
Finish



- 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.

Resource Name	Area	IP Address
Camera 01	root	10.20.100.143
Camera 02	root	10.20.100.143

- 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.

**Result:**

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

**Purpose:**

After drawing the system topology, you can monitor the devices in the system via topology.

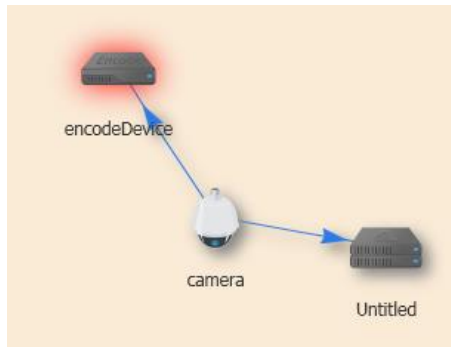
**Steps:**

1. On the Home page, Click **Status Monitoring (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. (Optional) If sub-topology exists under the element, click **Sub-Topology** on the Details window to enter the sub-topology.

## 11.3 Alarm Search

### **Purpose:**

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. See [4.14.3 Configure Alarm for Resource Health Status](#) for details.

### **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.
 

**Note:** For details about status alarm, refer to [4.14.3 Configure Alarm for Resource Health Status](#).
  - **Recording:** The number of the alarm related to recording.
3. (Optional) Check **Contain Subordinate Area**.

### **Result:**

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. For details, refer to 4.14.3 *Configure Alarm for 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

## 11.4 Report

### *Purpose:*

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.

### 11.4.1 Area Overview Report

#### *Purpose:*

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.

Score = Camera Online Rate\*  + Image Normal Rate\*  
 + Recording Normal Rate\*  + VOD Success Rate\*

**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.

## 11.4.2 Video Quality Report

### **Purpose:**

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.

### **Result:**

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.  
**Note:** For details about configuring health monitoring schedule, refer to 4.14.1 *Configure Health Monitoring Schedule*.
3. (Optional) Click **Export** to export the report details to the local PC.



## 11.4.3 Recording Status Report

### **Purpose:**

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.



## 11.4.4 Streaming Status Report

### **Purpose:**

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 streaming 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. (Optional) 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.

## 11.4.5 Camera Status Report

**Purpose:**

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 streaming status report.

**Steps:**

1. On Home page, click **Report** in the Maintenance section and then click **Camera Status** to enter the Streaming Status Report page.
2. Select an area from the area list.

**Result:**

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.

## 11.4.6 Video Retention Status Report

### **Purpose:**

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.

**Note:** You can configure the video retention days when configure health monitoring schedule. For details, refer to *4.14.1 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.

### **Result:**

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. (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.
    - 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.