USER MANUAL

ZKBioSecurity

Version : 2.1

Date : August, 2017

Software Version : ZKBioSecurity 3.0.5.0 or above version

Important Claims

Firstly, thank you for purchasing this product, before use, please read this manual carefully to avoid the unnecessary damage! The company reminds you that the proper user will improve the use effect and authentication speed.

Without the consent by our company, any unit or individual is not allowed to excerpt and copy the content of this manual partially or thoroughly and spread the content in any formats.

The product being described in the manual perhaps includes the software whose copyrights are shared by the licensors including our company. Except for the permission from the relevant holder, any person cannot copy, distribute, revise, modify, extract, decompile, disassemble, decrypt, reverse the engineering, lease, transfer, sub-license the software, or perform other acts of copyright infringement, but the limitations applied to the law is excluded.

Due to the constant renewal of products, the company cannot undertake the actual product in consistence with the information in the document, or any dispute caused by the difference between the actual technical parameters and the information in this document. Please forgive any change without notice.

Contents

Important Claims i

1 System Instruction 1

1.1 Brief Introduction of Personnel 1
1.2 Brief Introduction of Access Control 2
1.3 Brief Introduction of Elevator 2
1.4 Brief Introduction of Hotel Management System 2
1.5 Brief Introduction of Visitor 2
1.6 Brief introduction of Patrol 2
1.7 Brief introduction of Video 2
1.8 Brief Introduction of System Management 2

2 System Operations 4

2.1 Log into the System 4
2.2 Personal Self-Login 5
2.3 Dashboard 5
2.4 Activate the System 6
2.5 Modify Password 6
2.6 Customer Service 7
2.7 Exit the system 7

3 Personnel System 8

3.1 Personnel 8
3.1.1 Department Management 8
3.1.2 Personnel 9
3.1.3 Custom Attributes 20
3.1.4 Parameters 22
3.2 Card Manage 23
3.2.1 Card 23
3.2.2 Wiegand Format 24
3.2.3 Issue Card Record 26
3.3 AD Management 26

4 Access 27

4.1 Device 27
4.1.1 Device 27
4.1.2 Device Operation 31
4.1.3 Doors 38
4.1.4 Reader 41
4.1.5 Auxiliary Input 42
4.1.6 Auxiliary Output 43
4.1.7 Event Type 44
4.1.8 Daylight Saving Time 45

4.1.9 Device Monitoring....47
4.1.10 Real-Time Monitoring....47
4.1.11 Alarm Monitoring....51
4.1.12 Map....51
4.2 Access Control Management....52
4.2.1 Access Control Time Zones....52
4.2.2 Access Control Holidays....54
4.2.3 Access Levels....55
4.2.4 Interlock Settings....56
4.2.5 Linkage Setting....57
4.2.6 Anti-Passback Settings....61
4.2.7 First-Person Normally Open....62
4.2.8 Multi-Person Group....62
4.2.9 Multi-Person Opening Door....63
4.2.10 Verification Mode....64
4.2.11 Parameters....64
4.3 Advanced Functions....65
4.3.1 Zone....65
4.3.2 Reader Define....66
4.3.3 Who is Inside....67
4.3.4 Global Anti-passback....68
4.3.5 Global Linkage....69
4.3.6 Global Interlock Group....70
4.3.7 Global Interlock....71
4.3.8 LED Data....72
4.4 Access Reports....73
4.4.1 All Transactions....73
4.4.2 Events from Today....73
4.4.3 Last Known Position....74
4.4.4 All Exception Events....74
4.4.5 Access Rights....75
4.4.6 Charts....76
4.5 Video Integrated....76
5 Elevator....77
5.1 Elevator Device....77
5.1.1 Add an Elevator Device....77
5.1.2 Reader....79
5.1.3 Floor....80
5.1.4 Auxiliary Input....81
5.1.5 Event Type....82
5.1.6 Device Monitoring....83
5.1.7 Real-Time Monitoring....84
5.2 Elevator Rules....88
5.2.1 Time Zones....88

5.2.2 Holidays 90
5.2.3 Elevator Levels 90
5.2.4 Global Linkage 92
5.2.5 Parameters 94
5.3 Elevator Reports 94
5.3.1 All Transactions 94
5.3.2 All Exception Events 95
5.3.3 Access Rights 95
6 Hotel Management System 97
6.1 Hotel Settings 97
6.2 Room Management 98
6.2.1 Room Types 98
6.2.2 Building 99
6.2.3 Floor 99
6.2.4 Room 99
6.2.5 Room Areas 101
6.2.6 Booking Methods 102
6.2.7 Access/Elevator Control Levels★ 102
6.3 Card Service Center 105
6.3.1 Lock Management Cards 105
6.3.2 Personnel Cards 109
6.3.3 Maintenance Card 112
6.4 Hotel Management 114
6.4.1 Reception Center 114
6.4.2 Reservation Center 127
6.4.3 Reservation Management 129
6.5 Report Management 131
6.5.1 Guest Check-In Details Report 131
6.5.2 Room Check-In Details Report 131
6.5.3 Room Expenses Details Report 132
6.5.4 Card Writing Record Report 133
6.5.5 Lock Opening Record Report 133
7 Visitor System 135
7.1 Registration 135
7.1.1 Entry Registration 135
7.1.2 Visitor Information 139
7.2 Reservation 139
7.3 Basic Management 140
7.3.1 Parameters 140
7.3.2 Device Debugging 142
7.3.3 Print Settings 143
7.3.4 Visitor Levels 144
7.3.5 Entry Place 145

7.3.6 Visit Reason 146
7.4 Visitor Reports 146
7.4.1 Last Visited Location 146
7.4.2 Visitor History Record 146
7.4.3 Charts 146
8 Patrol System 147
8.1 Operation Wizard 147
8.2 Route Monitoring 147
8.3 Basic Management 148
8.3.1 Device 148
8.3.2 Checkpoint 149
8.3.3 Parameters 150
8.4 Patrol Management 150
8.4.1 Plan 150
8.4.2 Patrol Group 151
8.4.3 Route 152
8.5 Reports 154
8.5.1 All transactions 154
8.5.2 Patrol Records Today 154
8.5.3 Patrol Route Statistics 154
8.5.4 Patrol Personnel Statistics 154
9 Video 155
9.1 Video Device 155
9.2 Video Channel 156
9.3 Video Preview 157
9.4 Video Event Record 159
9.5 Parameters 159
9.6 Solutions of Exceptions 160
10 System Management 162
10.1 Basic Management 162
10.1.1 Operation Logs 162
10.1.2 Database Management 162
10.1.3 Area Setting 164
10.1.4 System Parameters 165
10.1.5 E-mail Management 166
10.1.6 Data Cleaning 166
10.1.7 Audio File 167
10.1.8 Certificate Type 167
10.1.9 Parameters 168
10.2 Authority Management 168
10.2.1 User 168
10.2.2 Role 170
10.2.3 Role Group 170

10.2.4 API Authorization 171
10.2.5 Client Register 172
10.3 Communication 173
10.4 Extended Management 174
10.4.1 LED Device 174
11 Appendices 178
11.1 Common Operations 178
11.2 Access Event Type 181
11.3 Elevator Event Type 184
11.4 FAQs 186
11.5 END-USER LICENSE AGREEMENT 187

1 System Instruction

Security Management has increasing concerns for modern enterprises. This management system helps customers to integrate operation of safety procedures on one platform. The system is divided into eight modules, namely: Personnel, Access, Elevator, Hotel Systems, Visitor Systems, Patrol Systems, Video Systems, Systems Management. Personnel System, Video System and System Management modules are in the public section, respectively, while the access control and elevator systems are in use.

- System Features
  - Powerful data processing capacity, allows management of data for 30,000 people.
  - Multilevel management role-based level management secures user data confidentiality.
  - Real-time data acquisition system ensures prompt feedbacks of data to the manager.
- Configuration Requirements
  - CPU: Dual core processor with speeds of 2.4GHz or more .
  - Memory: 4G or above.
  - Hardware: Available space of 30G or above. We recommend using NTFS hard disk partition as the software installation directory.
  - Monitor Resolution: 1024*768px or above.
- Operating System
  - Supported Operating Systems: Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows Server 2008(32/64).
  - Supported Databases: PostgreSQL(Default), SQL Server & Oracle（Optional）
  - Recommended browser version: IE 11+/Firefox 27+/Chrome 33+

Note: You must use IE 8.0 or newer version for fingerprint registration and matching.

1.1 Brief Introduction of Personnel

Personnel primarily consists of two parts: first, Department Management settings, used to set the Company's organizational chart; second, Personnel Management settings, used to input personnel information, assign departments, maintain and manage personnel.

1.2 Brief Introduction of Access Control

Access Control is a WEB-based management system which enables normal access control functions, management of networked access control panel via computer, and unified personnel access management. The access control system sets door opening time and levels for registered users.

1.3 Brief Introduction of Elevator

Elevator Control is mainly used to set device parameters (such as the swiping interval for taking elevators and elevator key drive duration), manage personnel's rights to floors and elevator control time, and supervise elevator control events. You may set registered users' rights to floors. Only authorized users can reach certain floors within a period of time after being authenticated.

1.4 Brief Introduction of Hotel Management System

It provides hotel service management functions covering check-in, overstay, check-out, rate settlement, and lock setup and management.

1.5 Brief Introduction of Visitor

Visitor is a web-based management system that implements entry registration, exit registration, snapshot capturing, visitor quantity statistics, and reservation management, as well as shares information among registration sites. It is highly integrated with the access control system and elevator control system and generally used at reception desks and gates of enterprises, to understand and manage visitors.

1.6 Brief introduction of Patrol

The online patrol system in the access control devices can help enterprise management personnel to effectively supervise and manage the patrol personnel, plans and routes. In addition, periodic statistics and analysis can be performed on the patrol routes and results.

1.7 Brief introduction of Video

Video provides video linkage function to manage the Video Server, view the Real-Rime Video, and query the Video Record, popup the Real-Time Video when linkage events happen.

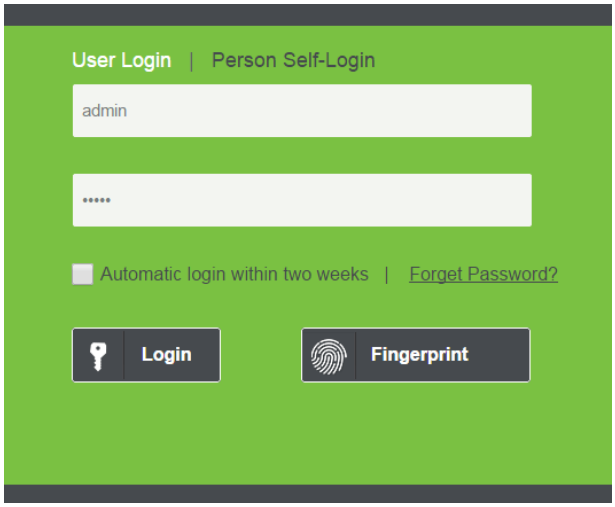
1.8 Brief Introduction of System Management

System Management is primarily used to assign system users and configure the roles of corresponding modules, manage database such as backup, initialization and recovery, and set system parameters and manage system

operation logs.

2 System Operations

2.1 Log into the System



After the software is installed, you may double-click the ZKBioSecurity icon to enter the system. You may also open the recommended browser, and input the IP address and server port in the address bar. Input http://127.0.0.1:8088 by default.

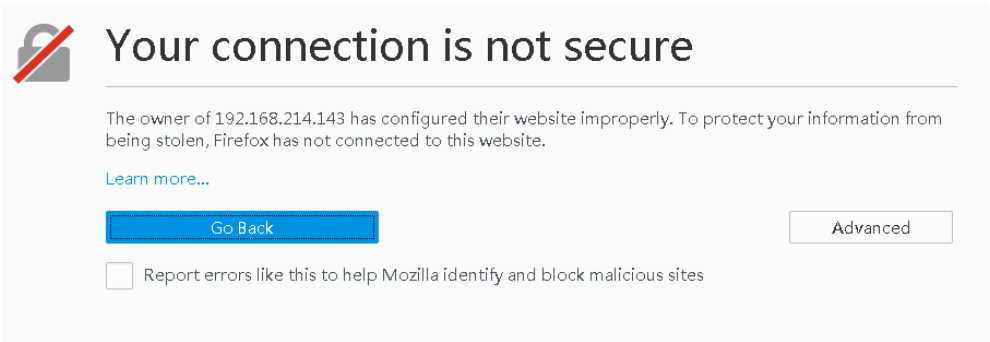
If the software is not installed in your server, you may input the IP address and server port in the address bar.

Enter user name and password, click [login], or click [Fingerprint] and then press the administrator fingerprint to enter the system.

Note:

1. The user name of the super user is [admin], and the password is [admin]. After the first login to the system, please reset the password in [Personnel Information].

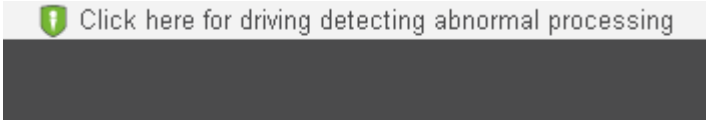
2. If you select the HTTPS port during software installation, input the server IP address and port number (for example, https://127.0.0.1:8448) in the address bar and press Enter. The following page may be displayed:



Here, you need to add a site exception following the exception adding prompts after you press **Advance**. Different

operations may be performed in different browsers.

3. If you select the HTTPS port during software installation, the following message may be displayed on the login page:



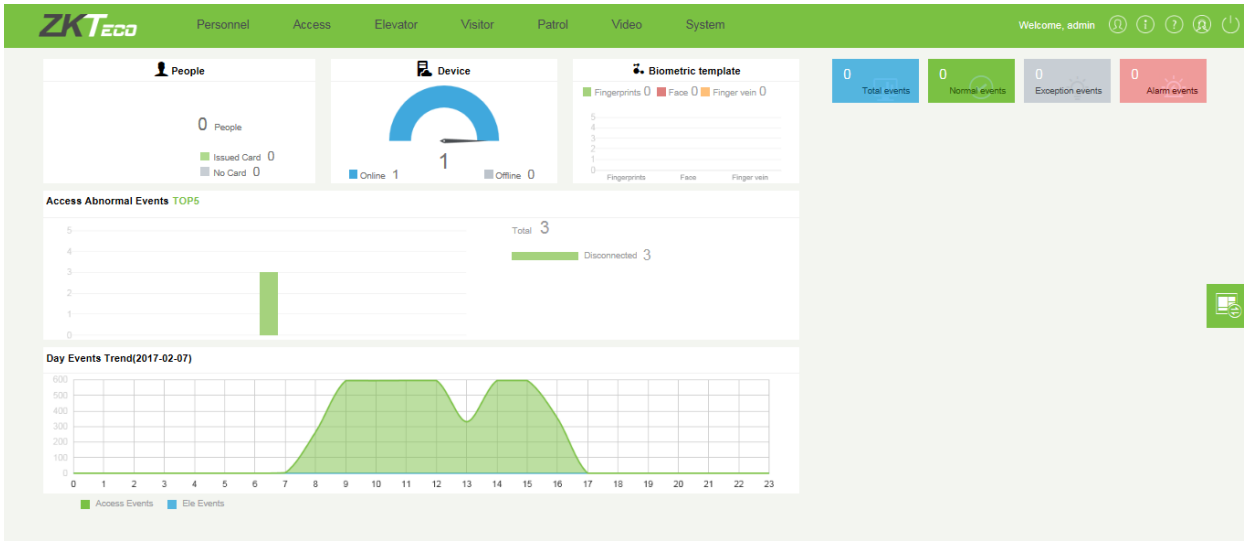
Click **Connect**. On the page that is displayed, download issonline.exe and corresponding certificates before using functions such as fingerprint and external devices.

2.2 Personal Self-Login

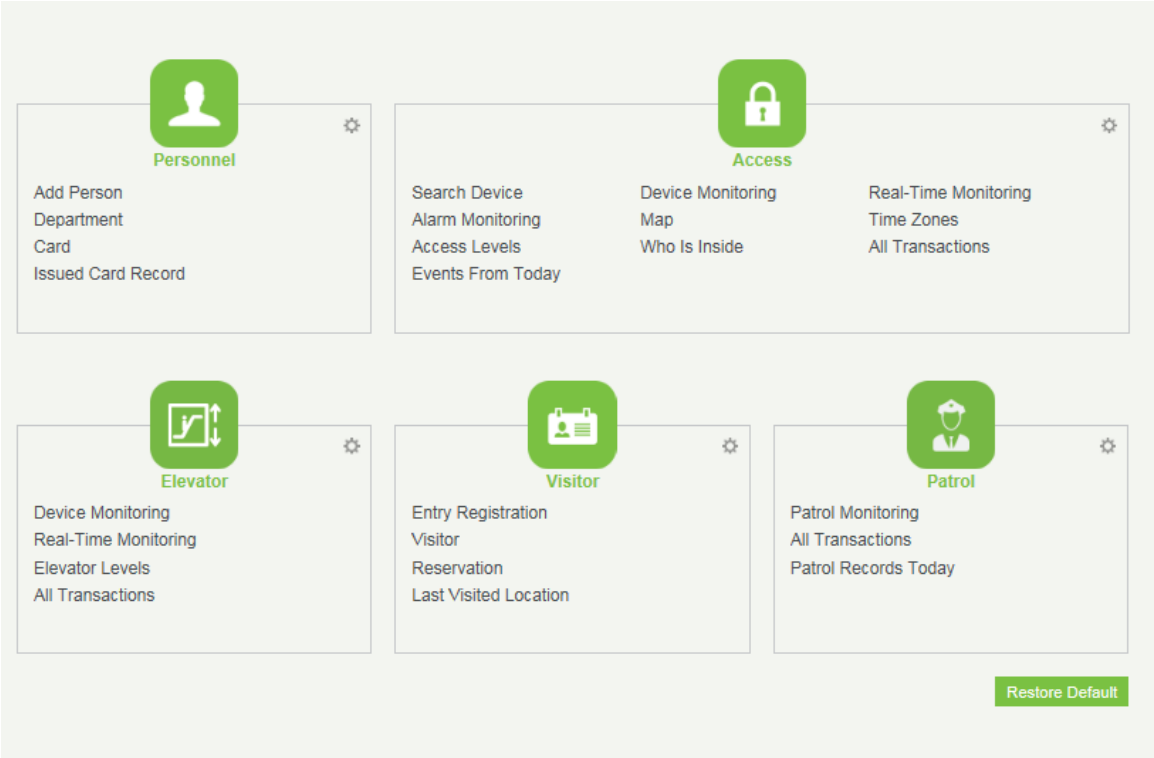
Click [Personal Self-Login], the personnel can reserve visitor for themselves. The personnel must be registered in the system. The login account and password is the personnel number and password registered in the system. The default password is 123456. For more details about the Reservation of visitors, please refer to Reservation.

2.3 Dashboard

After logging in, the main page is displayed as follows. You can click on the upper left corner of the interface to return to the main page while in other page.



This panel allows you to view statistics of each module and monitor real-time system events. Click to switch to the module quick connection page.



You may quickly access to desired pages through modules in the menu.

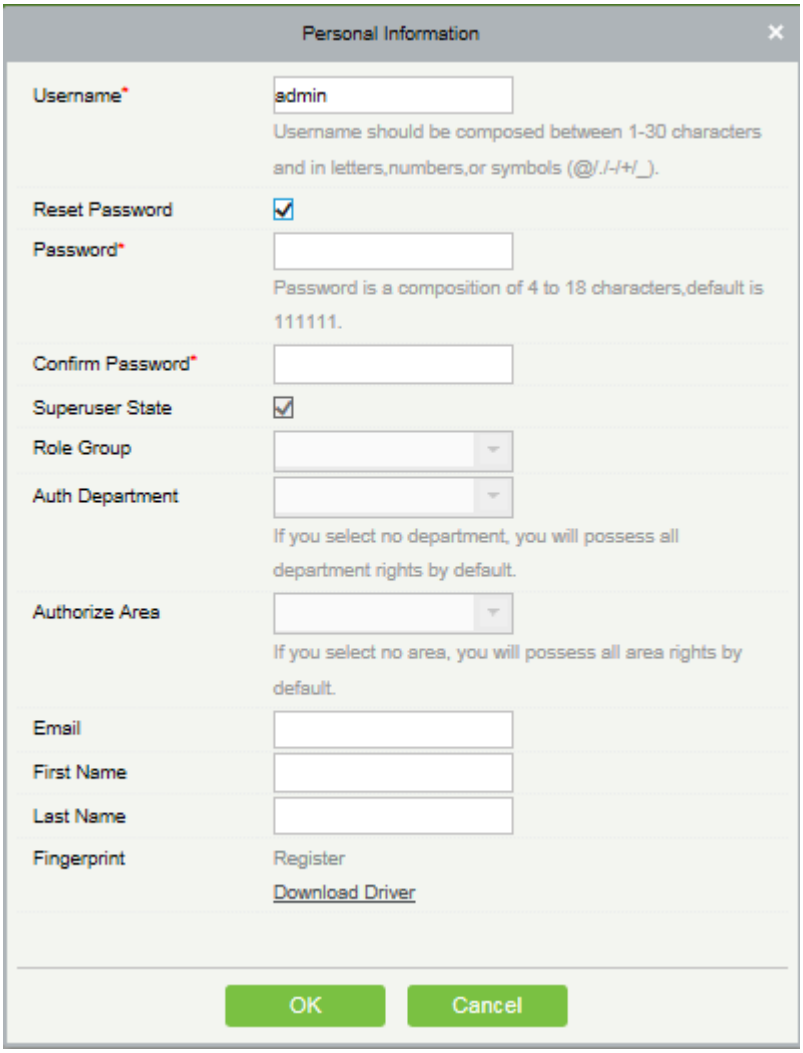
Click ⚙ to edit the function lists in the top right corner of every module.

2.4 Activate the System

Please refer to the corresponding license document.

2.5 Modify Password

You may modify the login password in [Personal Information]:



Check [Reset Password] box to modify the password.

Note: The super user and the new user are created by the super user (the default password for the new user is 111111). The user name is case-insensitive, but the password is case-sensitive.

2.6 Customer Service

Click the [Customer Service] button on the top right corner of the interface to submit your problems and obtain help.

2.7 Exit the system

Click the [Logout] button on the upper right corner of the interface to exit the system.

3 Personnel System

Before using the other functions, please configure the personnel system: Personnel and Card Management.

3.1 Personnel

Personnel system includes these modules: Department, Personnel, Custom Attributes and Parameters.

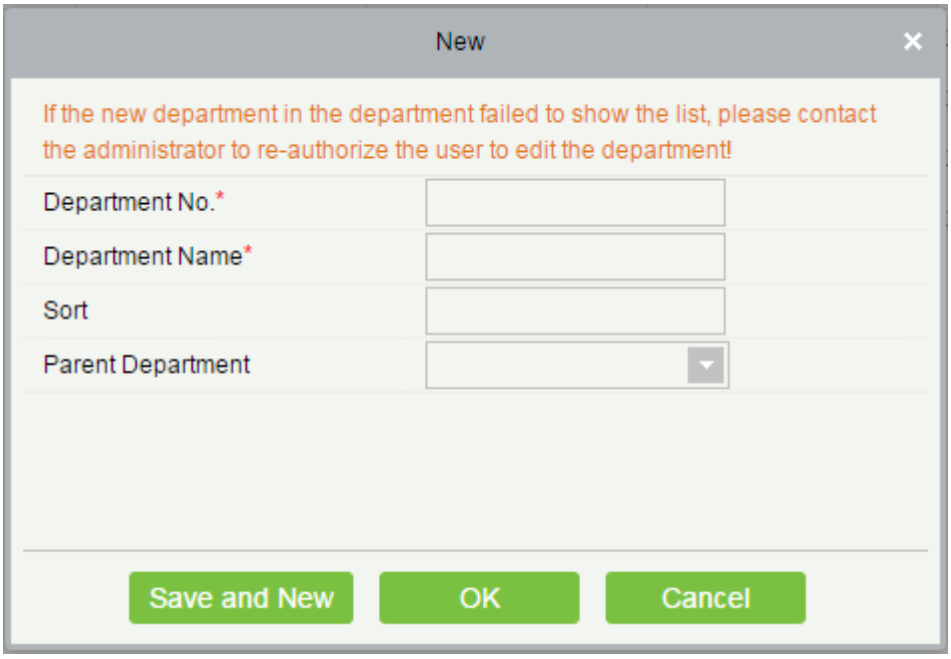
3.1.1 Department Management

Before managing company personnel, it is required to set company departmental organization chart. Upon first use of the system, by default it has a primary department named [General] and numbered [1]. This department can be modified but can't be deleted.

Main functions of Department Management include Add, Edit, Delete Department.

- Add a Department

1. Click [Personnel] > [Personnel] > [Department] > [Add]:



Fields are as follows:

Department No.: Letters and numbers are available. It cannot be identical to another department. Length shall not exceed 30 digits.

Department Name: Any character, at most a combination of 100 characters. The department name must be unique.

Sort: Supports only numbers. The valid range is 1-999999999. The smaller the number of department sort in a same

level, the higher ranking a department has. If not filled in, it will be arranged in accordance with the added order.

Parent department: Select parent department from the pull-down list. Parent Department is an important parameter to determine the Company's organizational chart. On the left of the interface, the Company's organizational chart will be shown in the form of a department tree.

2. After editing, click [OK] to complete adding, click [Cancel] to cancel it, click [Save and new] to save the edit and continue to add news.

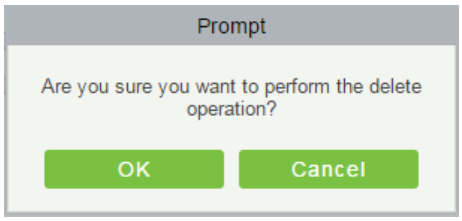
To add a department, you may also use [Import] to import department information from other software or other document into this system. For details, see Common Operations.

- Edit a Department

Click [Personnel] > [Personnel] > [Department] > [Edit].

- Delete a Department

1. Click [Personnel] > [Personnel] > [Department] > [Delete]:



2. Click [OK] to delete.

Note: If the department has sub-departments or personnel, the department cannot be deleted.

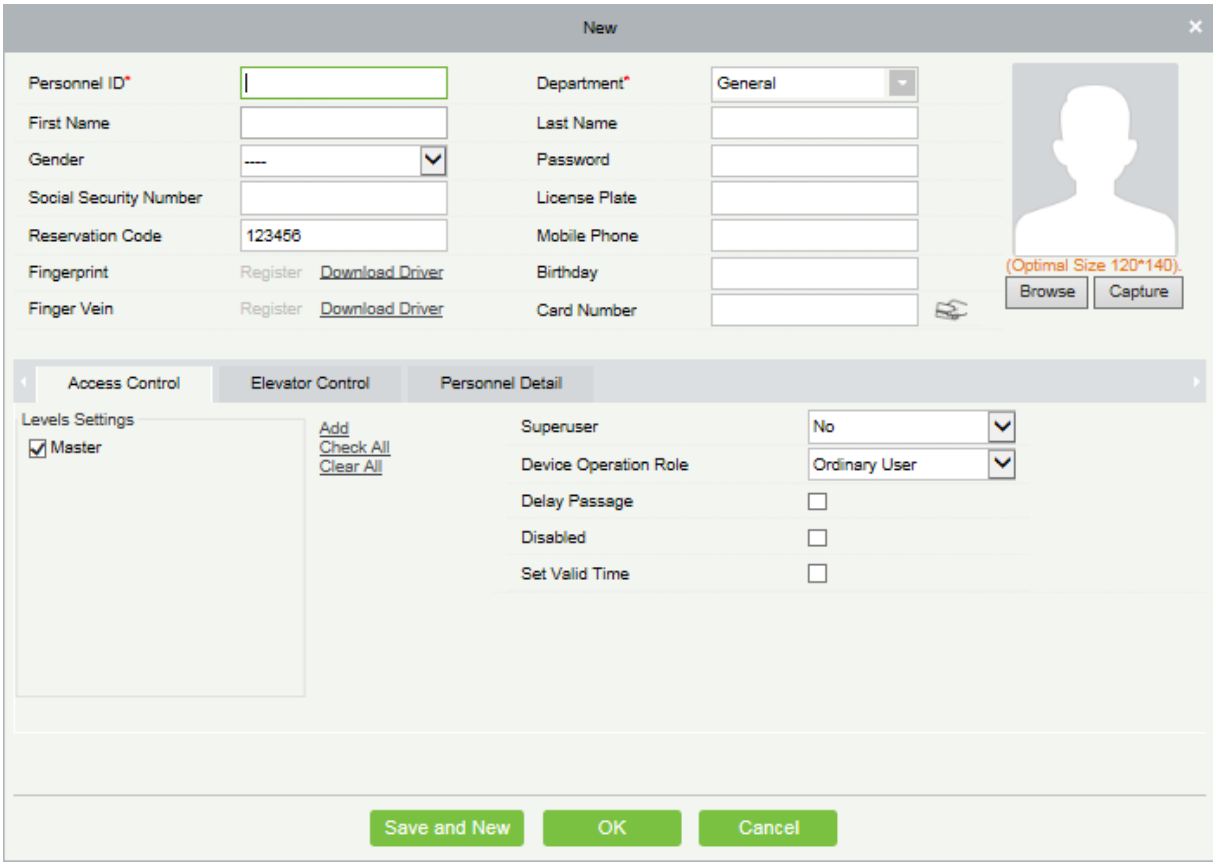
3.1.2 Personnel

When using this management program, the user shall register personnel in the system, or import personnel information from other software or document into this system. For details, see Common Operations.

Main functions of Personnel Management include Add, Edit, Delete personnel and Adjust Department.

- Add Personnel

1. Click [Personnel] > [Person] > [New]:



Fields are as follows:

Personnel ID: It must be unique. 9 characters at max, length, the valid range is 1-79999999, it can be configured based on actual conditions. The Personnel No. contains only numbers by default but may also include letters.

Notes:

(1) When configuring a personnel number, check whether the current device supports the maximum length and letter inclusion of the personnel number.

(2) When modifying the maximum length or letter inclusion of a personnel number, please enter into Personnel > Parameters to set.

Department: Select from the pull-down menu and click [OK]. If the department was not set previously, you can only select the default [Company Name] department.

First Name/Last Name: The max length is 50.

Gender: Set personnel gender.

Password: Set personnel password. Only supports 6-digit passwords. If password exceeds the specified length, the system will truncate it automatically. It can't be same with others and duress password.

Social Security Number: Set personnel social security number. The max length is 20.

License Plate/Mobile Phone**:** The max length is 20, and it may not fill in.

Card number: The max length is 10, and it can't be duplicated.

Employment Date: Input the actual date of employee begin to work.

Reservation Code: The max length is 6, the initial password is 123456.

Personal Photo: The picture preview function is provided, supporting common picture formats, such as jpg, jpeg, bmp, png, gif etc. The best size is 120×140 pixels.

- Browse: Click [Browse] to select a local photo to upload.
- Capture: Taking photo by camera is allowed when the server is connected with a camera.

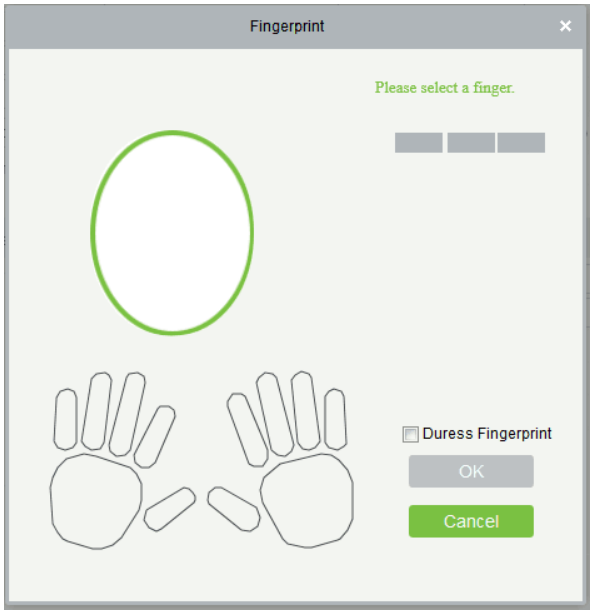
Register Fingerprint / Finger Vein: Enroll the Personnel Fingerprint, Finger Vein or Duress Fingerprint. To trigger the alarm and send the signal to the system, press the Duress Fingerprint.

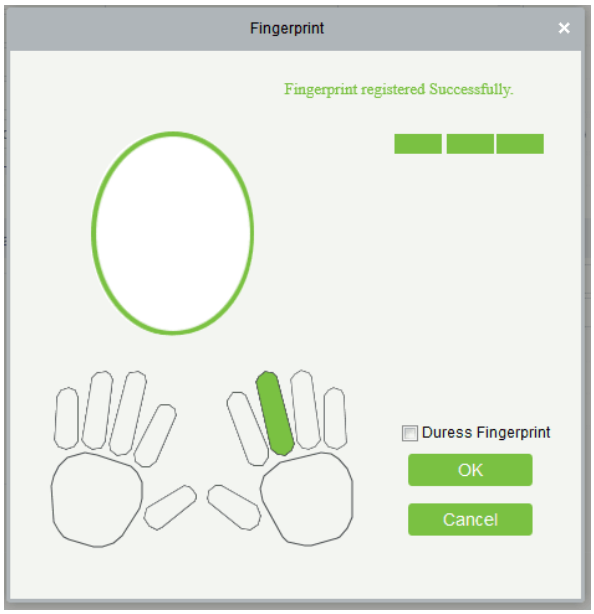
How to register fingerprint:

1) Click [Register].

2) Select a fingerprint, press in the sensor by three times, "Fingerprint registered Successfully" will be prompted.

3) Click [OK] to finish registration.





Click a fingerprint to delete. If you need to register a duress fingerprint, check the Duress Fingerprint box.

Notes:

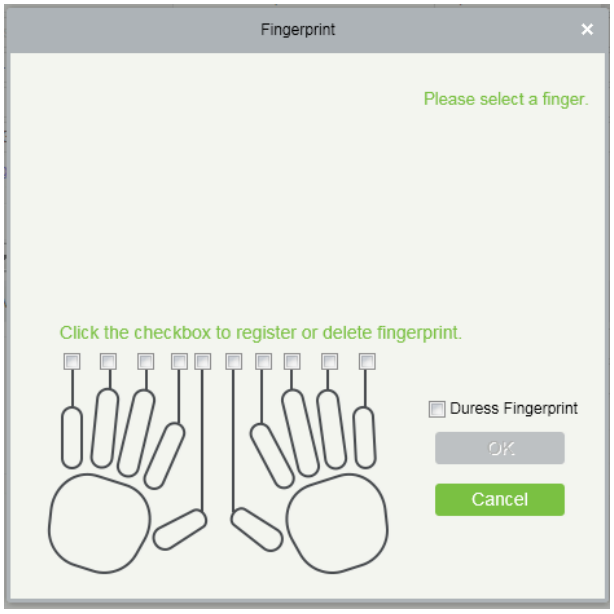
- If fingerprints are duplicated, "Don't repeat the fingerprint entry" will be prompted.
- If the fingerprint sensor driver is not installed, click "Install drive" and the system will prompt to download and install driver.
- After the fingerprint sensor driver is installed, if fingerprint register button is grey in IE browser while it is normal in other browsers (such as Firefox, Google), you may change the settings of IE browser, as follows:

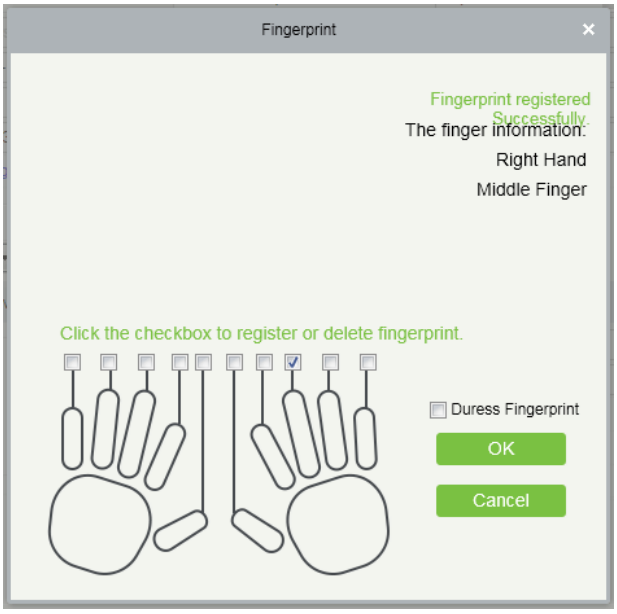
  1) In IE browser, click [Tools] → [Internet Options] →[Security] →[Credible Sites], add http://localhost to the credible sites, then restart the IE browser.

2) In IE browser, click [Tools] → [Internet Options] →[Advanced] →[Reset] to pop up a dialog of Reset Internet Explorer Settings, click [Reset] to confirm; then restart the IE browser (this step can be used when step1 has no effect).

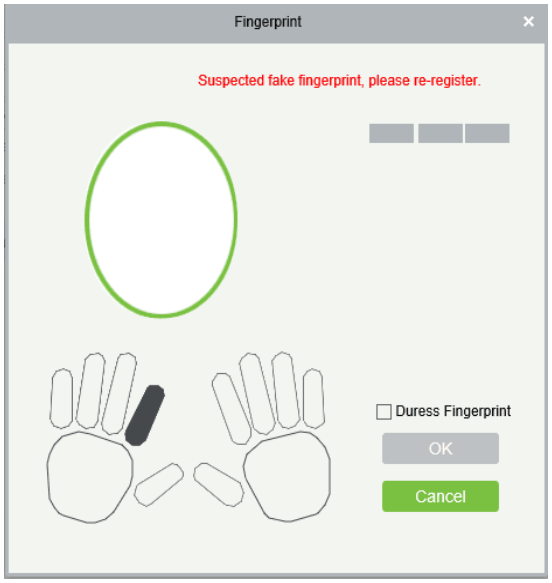
3) If above settings are all invalid, please execute following operations (take IE11 browser as an example): click [Tools] → [Internet Options] →[Advanced] →[Security], check the option of [Allow software to run or install even if the signature is ...], and remove the tick before [Check for server certificate revocation], then restart IE.

4) If the browser is below IE8, the fingerprint registration page will be different:





（5）The system supports the access from the Live20R fingerprint device and the fake fingerprint prevention function.



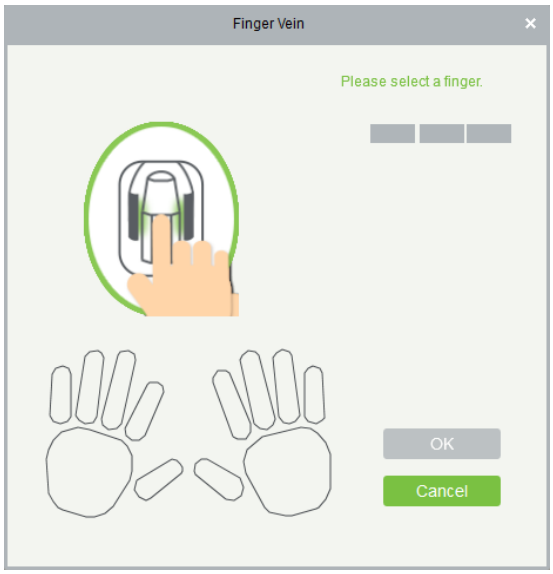
The finger vein registration process is as follows:

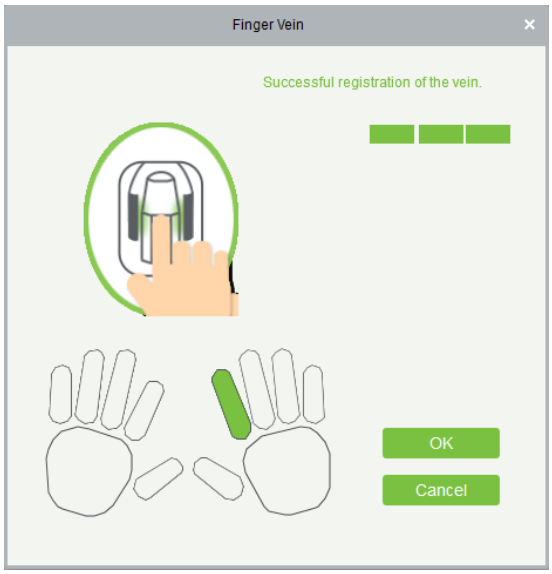
1) Click [Register]. The register page is displayed.

2) Select a finger and press the finger vein device for three consecutive times. The system prompts "Finger vein

successfully registered".

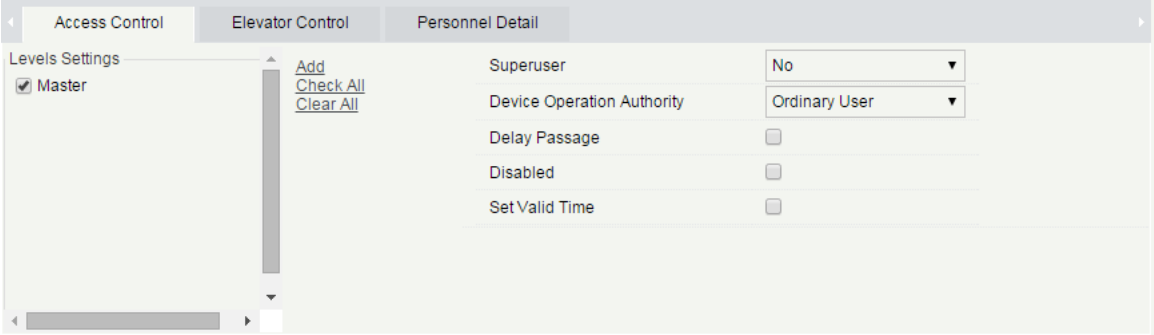
3) Click [OK] to save the setting and close the finger vein registration page.





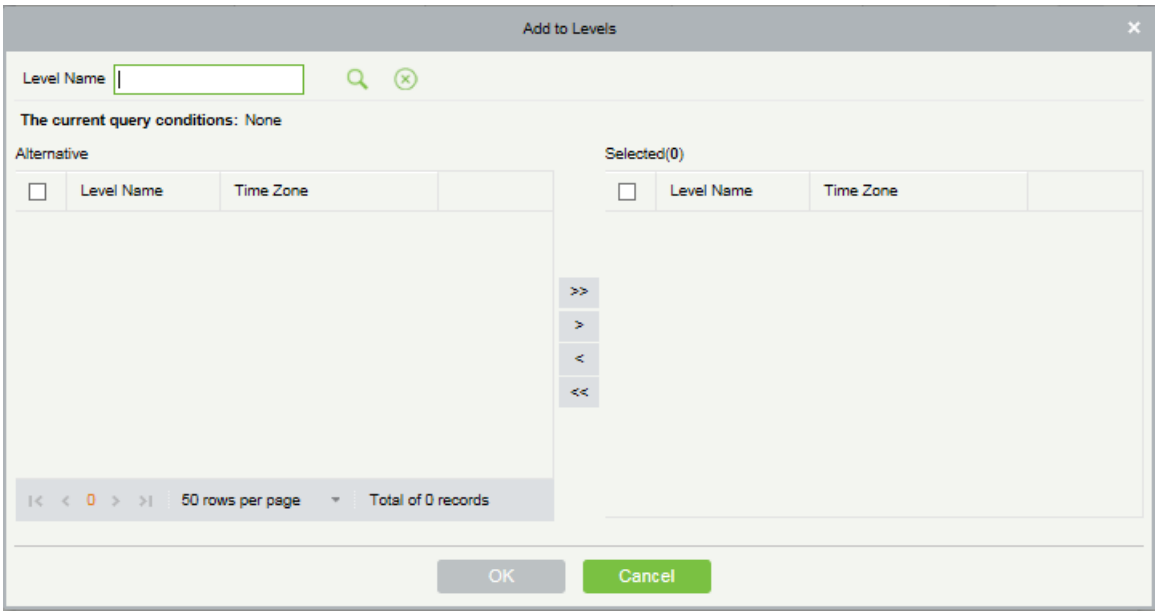
To delete a registered finger vein, click the finger vein and then click [OK].

2. Set the Access Control parameters for the personnel. Click [Access Control]:



Fields are as follows:

Level Settings: Click [Add], set passage rules of special positions at different times.



Superuser: In access controller operation, a super user is not restricted by the regulations on time zones, anti-passback and interlock and has extremely high door-opening priority.

Device Operation Authority: Select administrator to get its levels.

Delay Passage: Extend the waiting time when the movement of persons. Suitable for people with disabilities or other special needs populations.

Disabled: Temporarily disable the personnel's access level.

Set Valid Time: Set Temporary access level. Doors can be set to open only within certain effective period of time. If not checked, the time to open the door is always active.

Note: The number of a person, whether departed or in service, must be unique. The system, when verifying, will automatically search the number in the departure library.

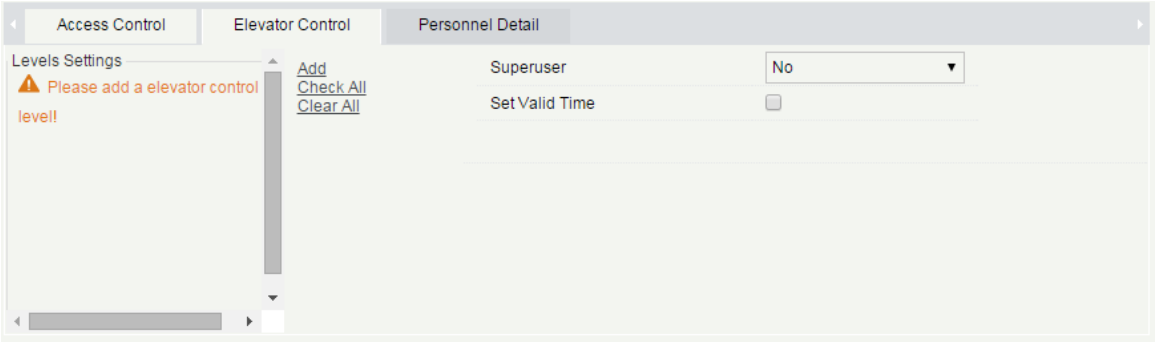
The Personnel Information List, by default, is displayed as a table. If Graphic Display is selected, photos and numbers will be shown. Put the cursor on a photo, details about the personnel will be shown.

Notes:

(1) Not all the devices support the "Disabled" function. When a user adds a device, the system will notify the user whether the current device support this function. If the user needs to use this function, upgrade the device that originally does not support the function.

(2) Not all the devices support the "Set Valid Time" function of setting the hour, minute, and second. Some devices only allow users to set the year, month, and day of the active time. When a user adds a device, the system will notify the user whether the current device support this function. If the user needs to use this function, upgrade the device that originally does not support the function.

3. Set the Elevator Control parameters for the personnel. Click [Elevator Control]:



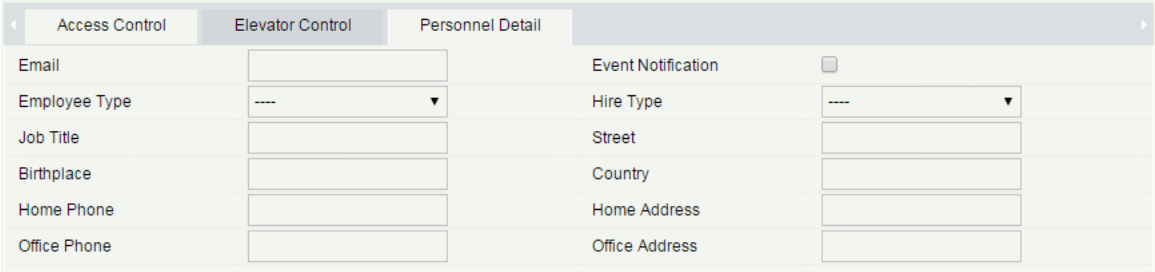
Fields are as follows:

Superuser: In elevator controller operation, a super user is not restricted by the regulations on time zones, holidays and has extremely high door-opening priority.

Set Valid Time**:** Set Temporary elevator level. Floor buttons can be set to be pressed only within the effective period of time. If not checked, the time to press the floor button is always active.

Note: The Elevator level must be set in advance.

4. Click [Personnel Detail] to enter the detail information and edit interface, complete personnel detail info.



Fields are as follows:

Email: Set the available email address of the personnel, the max length is 30. The "-","_" and"." are supported. If the Event Notification is checked, the Email is required.

Event Notification: After checking this menu, the system will send email to this person once an access or an elevator event occurs. If there is no setting to email sending server, the Email Parameter Settings window will pop up. Please refer to E-mail Management for the setting information.

5. After filling in the information, click [OK] to save and exit, the person will be displayed in the added list.

- Edit Personnel

Click [Personnel] > [Personnel], select a person, click [Edit].

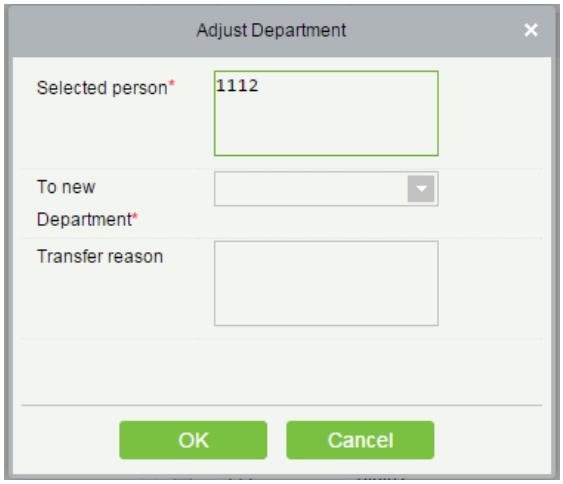
- Delete Personnel

Click [Personnel] > [Person], select a person, click [Delete] > [OK] to delete.

Note: Delete a person, all information about the person will be deleted.

Adjust Department

1) Click [Personnel] > [Person], select a person, click [Adjust Department]:

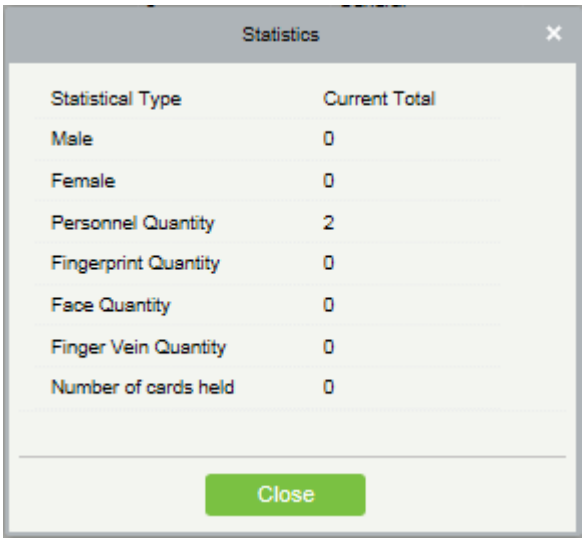


2) Select "To new Department".

3) Click "OK" to save and exit.

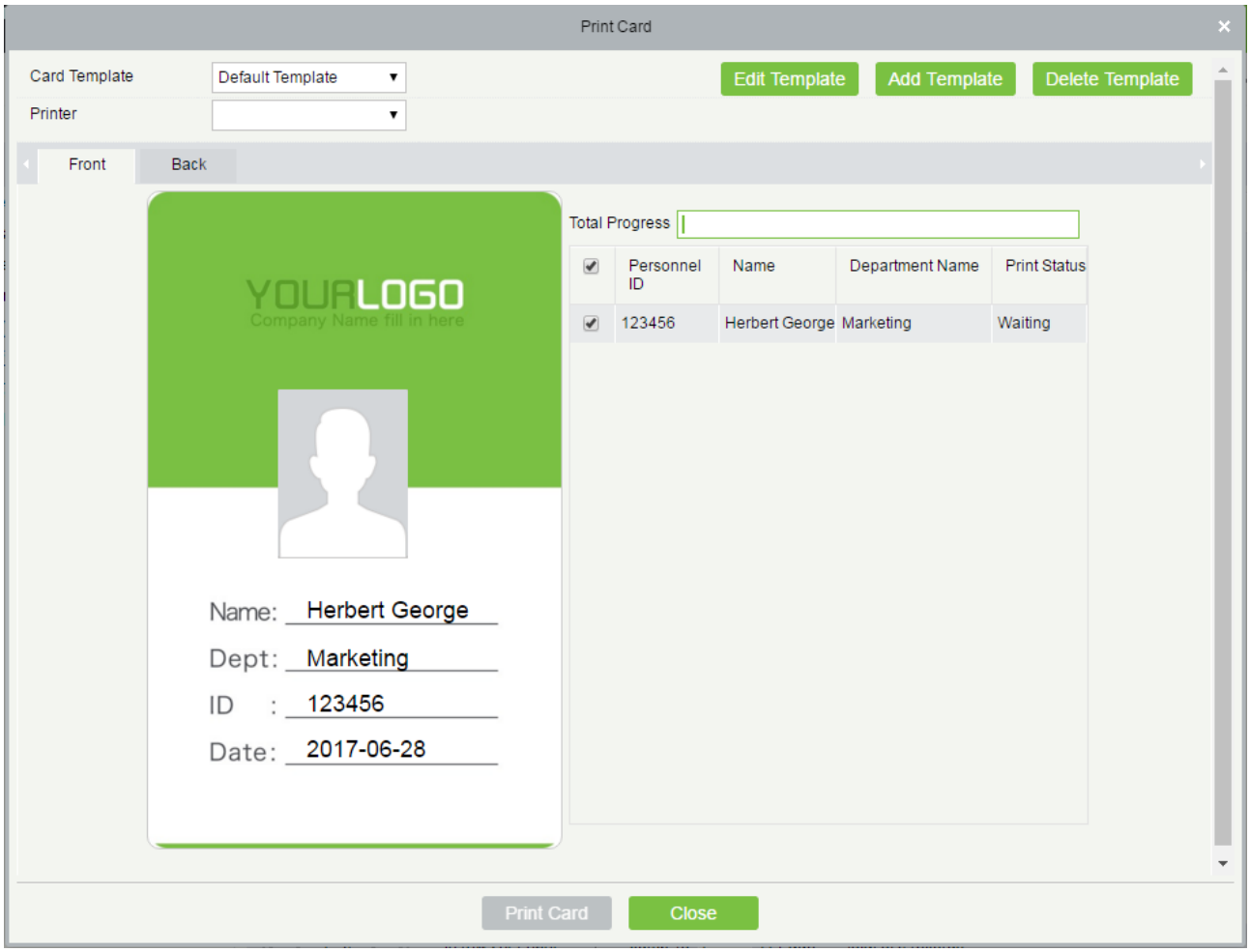
Statistics

Click [Personnel] > [Person] > [Statistics]. View the number of personnel, the number of fingerprints, facial number, finger vein number, card number, gender and other statistical information.



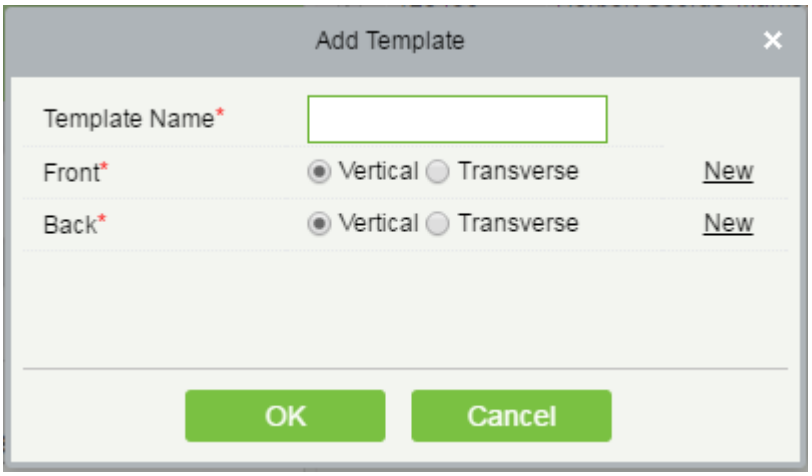
Card Printing

Click [Personnel] > [Person], select a person, and click [Print Card].

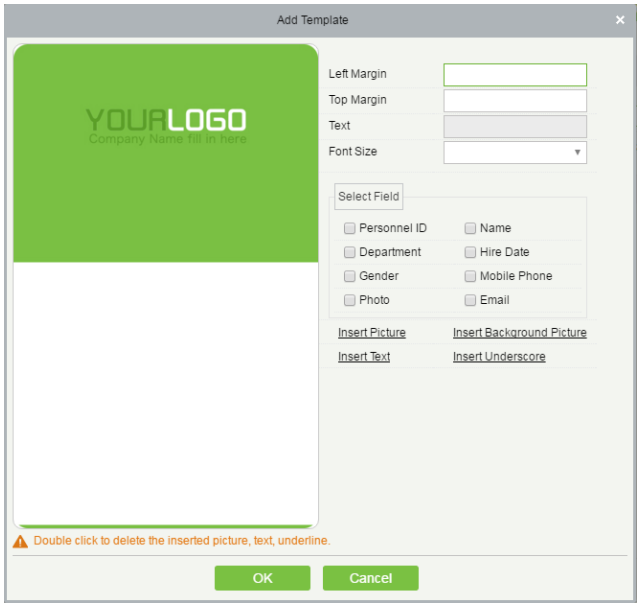


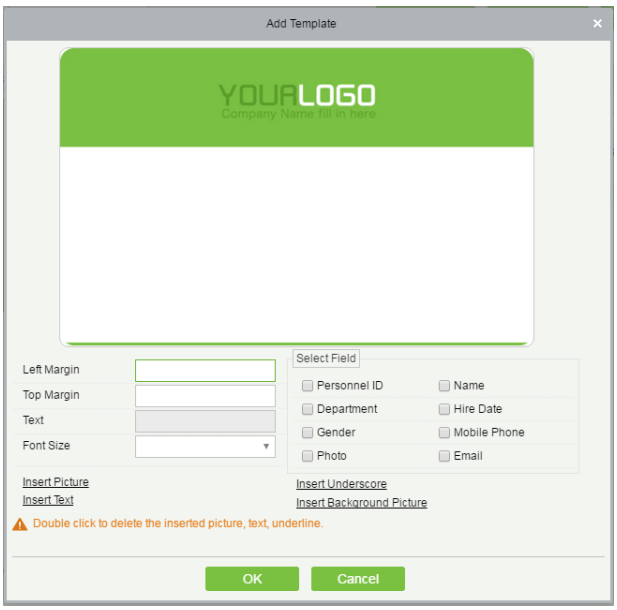
Select a card template and a printer and click [Print Card].

1. To add a template, click [Add Template].

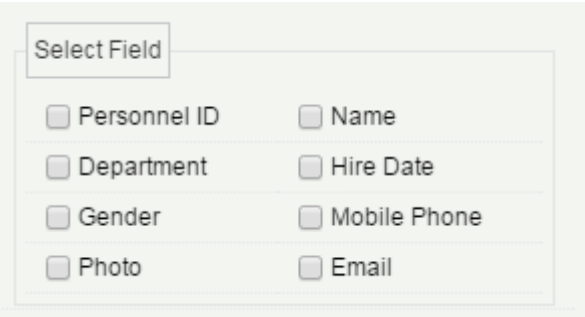


Enter [Template Name], select the template direction, and click [OK]. The left figure below is a vertical template and the right one is a transverse template.

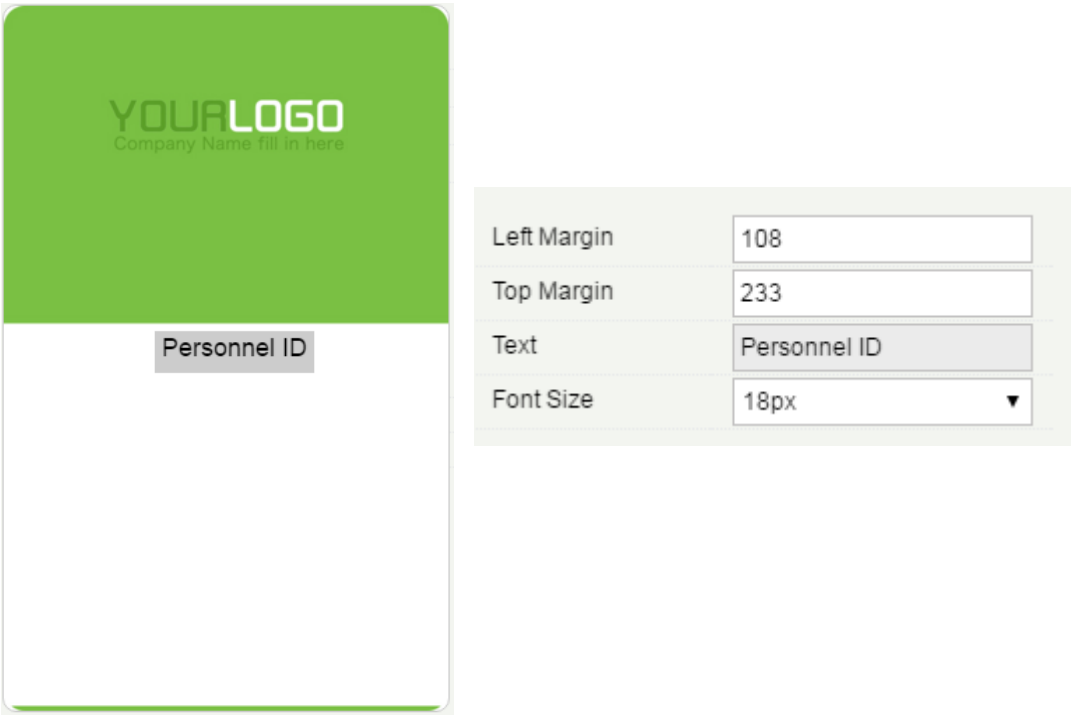




(1) Select fields.



Select corresponding fields. The fields will be displayed in the template. You can drag the fields to change the field coordinate.



(2) You can insert pictures, background images, texts and underlines into the template.

Enter the text to be inserted in [Text] to insert texts to the template.

Notes:

1) Click to delete inserted fields.

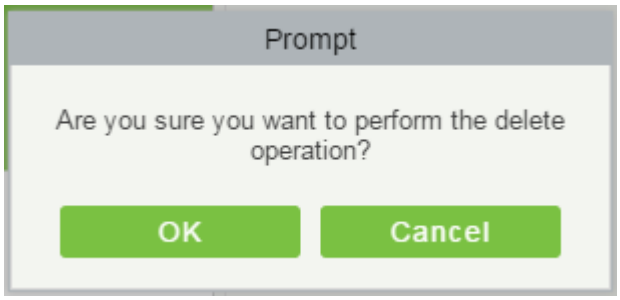
2) Double-click inserted pictures, texts or underlines to delete them.

3) Upload a background image of 635 x 1010 pixels for a vertical template and a background image of 1010 x 635 pixels for a transverse template.

2. To edit a template, click [Edit Template]. The procedures for editing a template are the same as those for adding a template and will not be mentioned here.

Note: By default, neither of the vertical template nor the transverse template can be edited. Only user-defined templates can be edited.

3. To delete a template, click [Delete Template].



Click [OK] to delete the template.

Note:

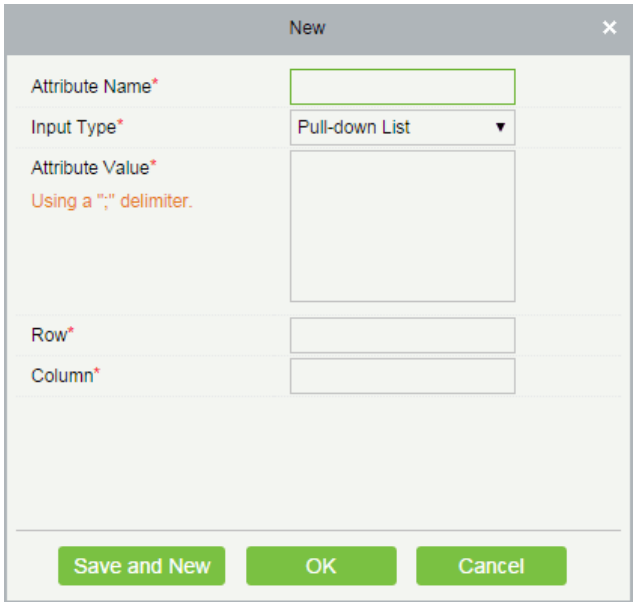
By default, neither of the vertical template nor the transverse template can be deleted. Only user-defined templates can be deleted.

3.1.3 Custom Attributes

Some personal attributes can be customized or deleted to meet different customers' requirements. When the system is used for the first time, the system will initialize some personal attributes by default. Customized personal attributes can be set for different projects according to requirements.

- New a Custom Attribute

1) Click [Personnel] > [Personnel] > [Custom Attributes] > [New], edit the parameters and click [OK] to save and exit.



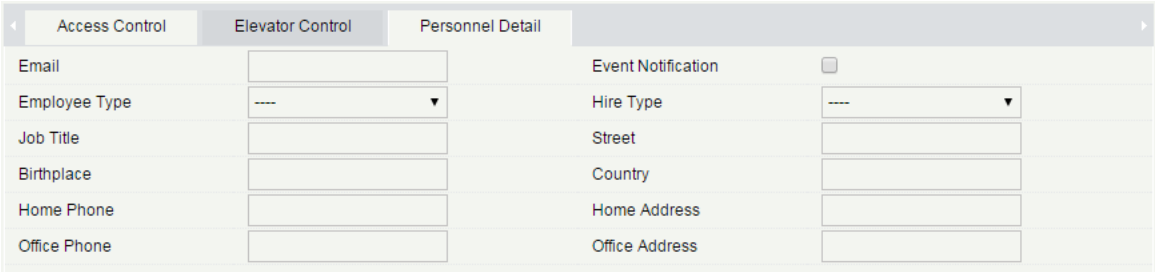
Fields are as follows:

Attribute Name: Must be filled in and not be duplicated. Max length is 30.

Input Type: Select the display type, includes "Pull-down List", "Multiple Choice", "Single Choice" and " Text".

Attribute Value: Suitable for the Pull-down List, Multiple Choice and Single Choice of input type. Use a ";" to distinguish the multiple values. If the input type is Text, the attribute value is not suitable.

Row/Colum: The column and row of a field are used together to control the display position of the field. Numerals are supported. The column number cannot exceed 99, and the row number can only be 1 or 2. The combination of the column and row must not be duplicated. As shown in the following figure, starting from Employee Type, it is in the first column and first row, and Hire Type is in the first column and second row.



- Edit a Custom Attribute

Click [Edit] below operations to modify the corresponding attribute.

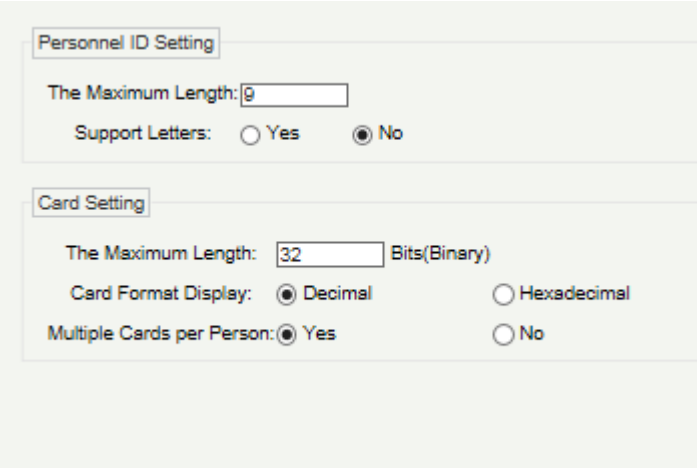
- Delete a Custom Attribute

Click [Delete] below operations to delete an unneeded attribute. If the attribute is in use, the system will prompt before confirming to delete.

Note: The custom attribute will not recovery once deleted.

3.1.4 Parameters

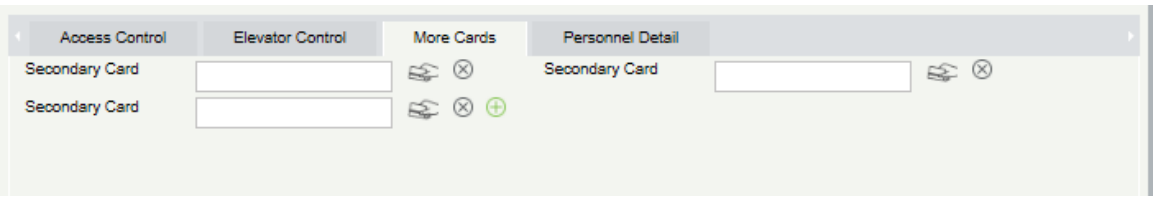
1) Click [Personnel] > [Personnel] > [Parameters]:



2) Set the maximum length of pesonnel number and whether it supports letters.
3) Set the maximum length (binary number) of the card number that the current system supports.
4) Set the card format currently used in the system. The card format cannot be switched when the system has a card.
5) Set whether the Multiple Cards per Person function is enabled in the system.
6) Click [OK] to save the setting and exit.

- More Cards

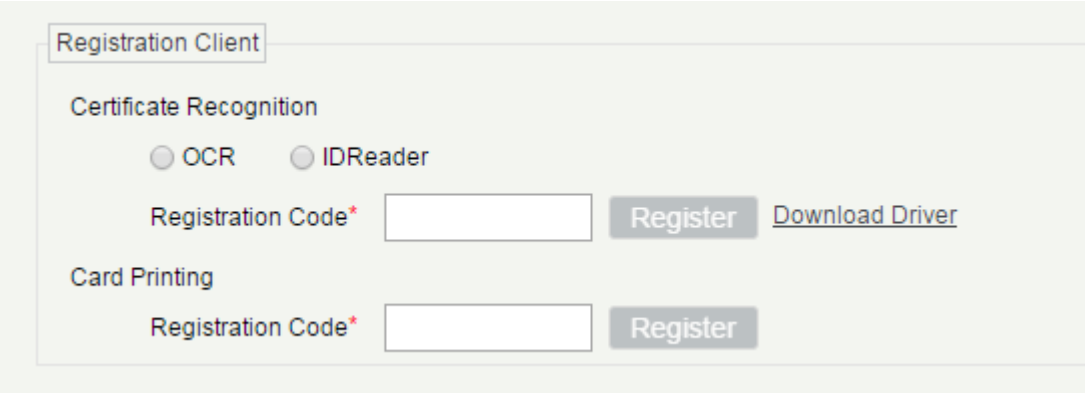
After the multiple cards per person function are enabled, you can set multiple cards on the Personnel page.



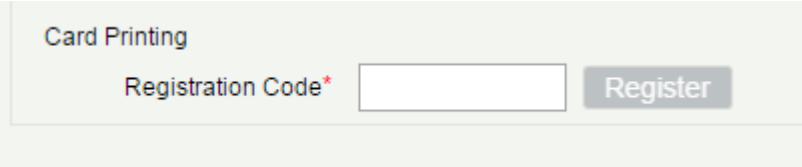
Note: Not all devices support the Multiple Cards per Person function. For details, please consult the technical personnel.

- Registration Client

1) If no driver has been installed, the [Download Driver] link is displayed. Click the link to download and install the driver.



2) Enter the corresponding registration code and click [Register].



Note: Click [System] > [Authority Management] > [Client Register] to view the registration code.

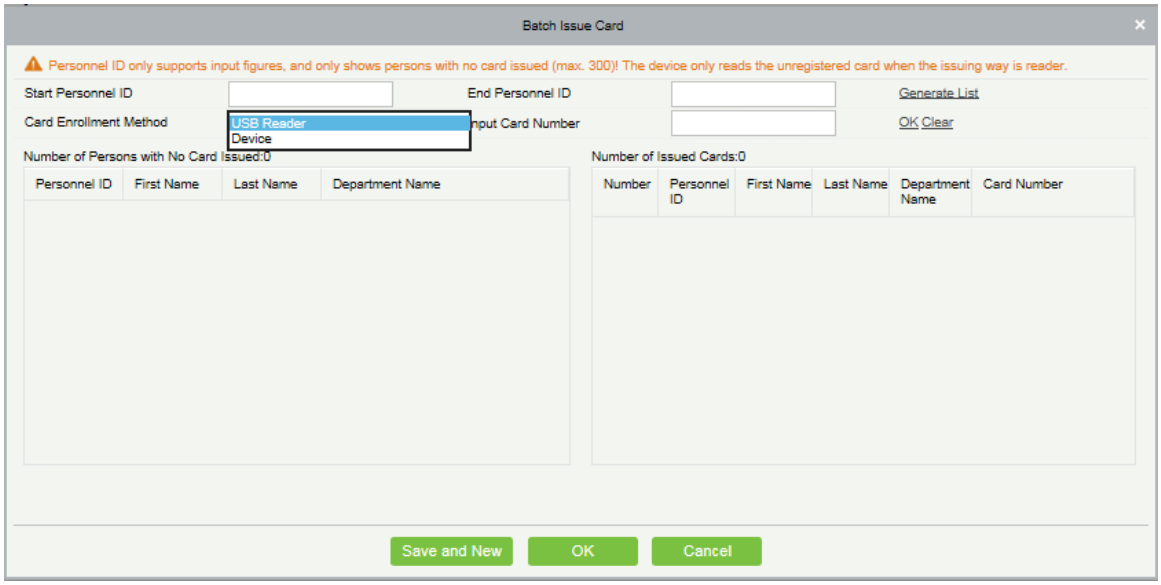
3.2 Card Manage

There are three modules in card management: Card, Wiegand Format and Issue Card Record.

3.2.1 Card

- Batch Issue Card

1) Click [Personnel] > [Card Manage] > [Batch Issue Card]:



2) Enter Start and End Personnel No. and click [Generate List] to generate personnel list and show all personnel without cards within this number series.

Note: The Enter Start and End Personnel No. only support numbers.

3) Select Card Enrollment Method: USB Reader or device.

For the use of USB reader, punching on the Issue machine directly. The System will get the card number and issue it to the user in the left list.

For the use of device, you need to select the position of punching, click [Start to read], the system will read the card number automatically, and issue it to the user in the left list one by one. After that, click [Stop to read].

Note: During Batch Issue Card, System will check whether the card number issues card or not, if card has been issued before, the system will prompt "The Card Number has already been issued".

4) Click [OK] to complete card issue and return.

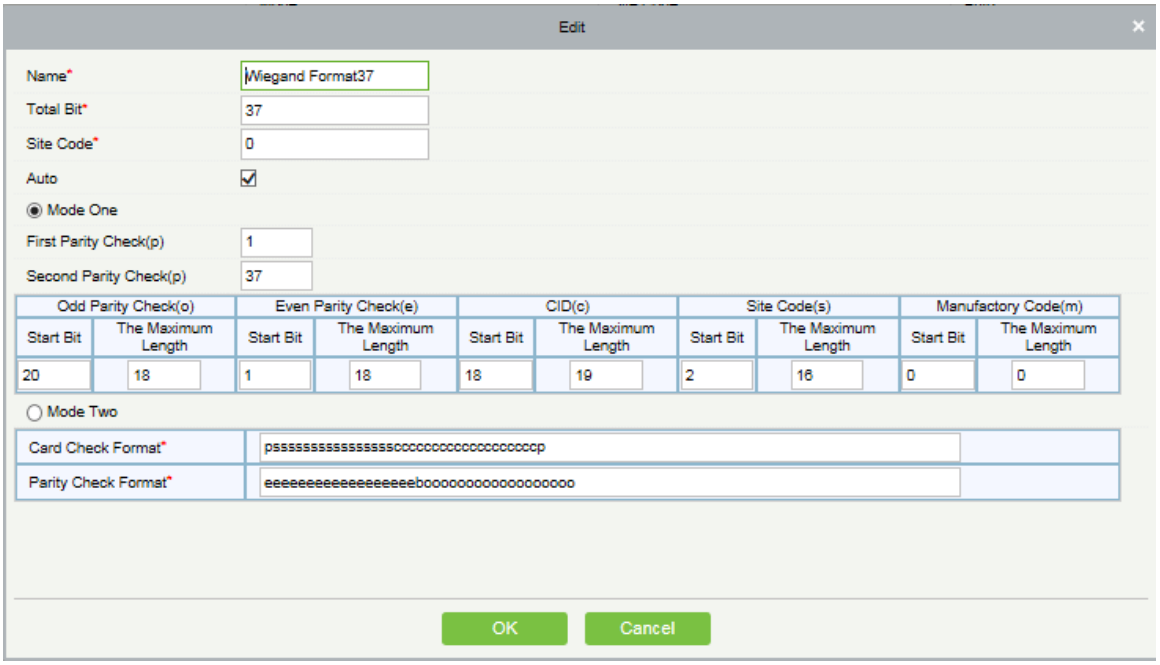
3.2.2 Wiegand Format

Wiegand Format is the card format that can be identified by Wiegand reader. The software is embedded with 9 Wiegand formats. You may set the Wiegand card format as required.

Refresh New Delete Card Formats

Name	Mode	Site Code	Auto	Operations
Wiegand Format26	Mode One	0	Yes	Edit
Wiegand Format26a	Mode One	0	No	Edit
Wiegand Format34	Mode One	0	Yes	Edit
Wiegand Format34a	Mode One	0	No	Edit
Wiegand Format36	Mode One	0	Yes	Edit
Wiegand Format37	Mode One	0	Yes	Edit
Wiegand Format37a	Mode One	0	No	Edit
Wiegand Format50	Mode One	0	Yes	Edit
Wiegand Format66	Mode One	0	Yes	Edit

This software supports two modes for adding Wiegand Format, if mode 1 does not meet your setting requirement, switch to mode 2. Take Wiegand Format 37 as an example:



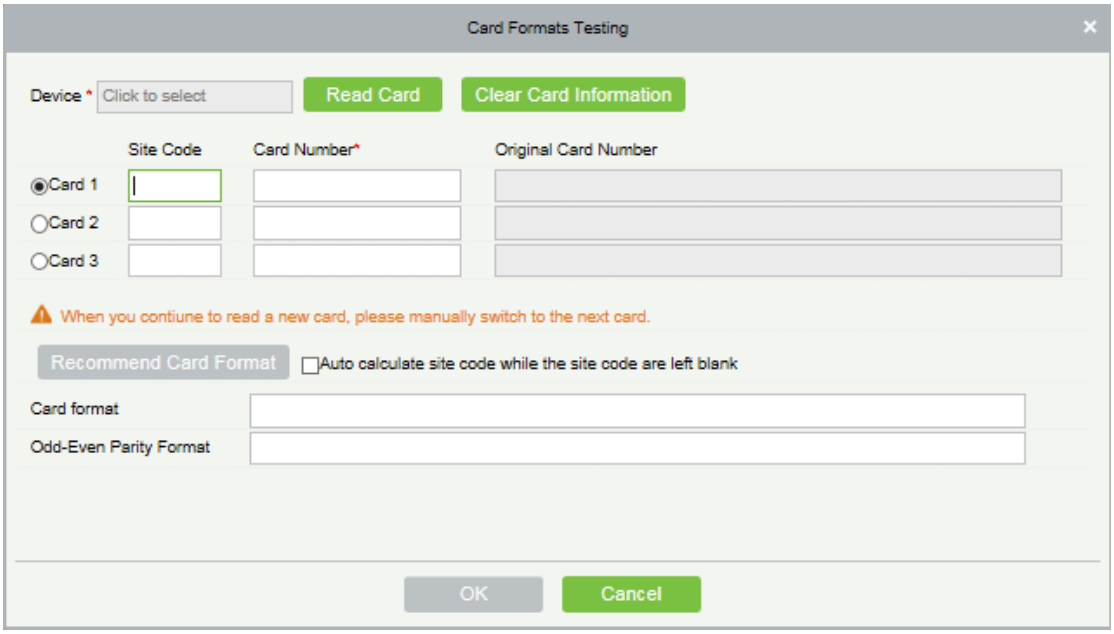
Format Specifying:

P indicates Parity Position, s indicates Site Code, c indicates Cardholder ID, m indicates Manufactory Code, e indicates Even Parity, O indicates Odd Parity, b indicates both odd check and even check, x indicates parity bits no check.

The previous Wiegand Format 37: the first parity bits (p) check "eeeeeeeeeeeeeeeeee", the second parity bits check "ooooooooooooooooooo". Card Check Format only can be set "p, x, m, c, s", Parity Check Format only can be set " x, b, o, e".

- ## Card Formats Testing

If the number on the card is different from the number that is displayed after you swipe the card, you can use this function to calibrate the Wiegand format. The page is displayed as follows:



Select a device that supports the card formats testing function and input the number and site code (optional) on the card.

1) Click [Read Card] and swipe the card on the device reader. The original card number read by the device is displayed in the input box on the right.

2) Click [Recommend Card Format]. The Wiegand card format recommended for the input card number is displayed below.

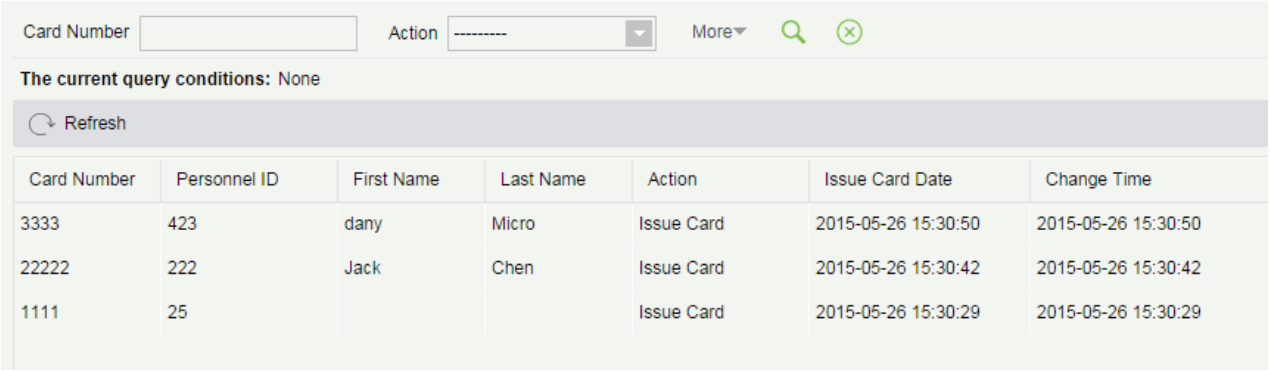
3) If [Auto calculate site code while the site code are left blank] is selected, the software calculates the site code based on the card format and card number.

4) Click [OK]. The page skips to the Wiegand Format Adding page to save the recommended Wiegand format.

Note: The card formats testing function is supported only by certain devices.

3.2.3 Issue Card Record

Used to record the life cycle of a card and display the operations performed on the card.



Card Number	Personnel ID	First Name	Last Name	Action	Issue Card Date	Change Time
3333	423	dany	Micro	Issue Card	2015-05-26 15:30:50	2015-05-26 15:30:50
22222	222	Jack	Chen	Issue Card	2015-05-26 15:30:42	2015-05-26 15:30:42
1111	25			Issue Card	2015-05-26 15:30:29	2015-05-26 15:30:29

Note: The cards and card issuing records of an employee will be deleted altogether when the employee is deleted completely.

3.3 AD Management

For details about this function, please refer to its user manual.

4 Access

The system needs to be connected to access controller to provide access control functions. To use these functions, user must install devices and connect them to the network first, then set corresponding parameters, so you can manage devices, upload access control data, download configuration information, output reports and achieve digital management of the enterprise.

4.1 Device

Add access device, set the communication parameters of connected devices, including system settings and device settings. When communication is successful, you can view the information of connected devices, and perform remote monitoring, uploading and downloading etc.

4.1.1 Device

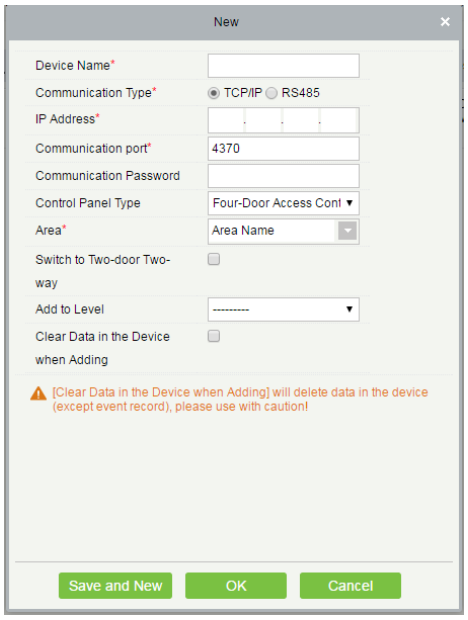
- Add Device

There are three ways to add Access Devices.

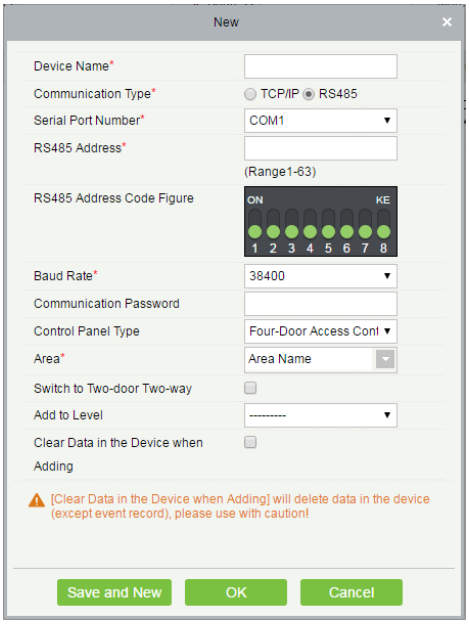
1. Add Device by manually

(1) Click [Access Device] > [Device] > [New] on the Action Menu, the following interface will be shown:

TCP/ IP communication mode



RS485 communication mode



Fields are as follows:

IP Address: Enter the IP Address of the access controller.

Communication port: The default value is 4370.

Serial Port No.: COM1~COM254.

RS485 Address: The machine number, the range is 1-255. When Serial Port No. is same, it is not allowed to set repeated RS485 addresses.

Baud Rate: Same as the baud rate of the device. The default is 38400.

RS485 Address Code Figure: display the code figure of RS485 address.

Common options:

Device Name: Any character, up to a combination of 20 characters.

Communication Password: The max length is 6 with numbers or letters.

Notes:

1) You do not need to input this field when it is a new factory device or just after the initialization.

2) When setting the standalone device's communication password and communication password to 0, it means no password; however for access control panel, it means the password is 0.

3) You need to restart the device after setting the door sensor of the standalone device.

Control Panel Type: One-door access control panel, two-door access control panel, four-door access control panel, Standalone Device.

TimeZone: You need to set this option if the device supports setting the time zone and the device time zone is not in the same time zone as the server. This option does not appear for devices that do not support setting the time zone. The newly added device defaults to synchronize server's time zone.

Area: Specify areas of devices. After Area Setting, devices (doors) can be filtered by area upon Real-Time Monitoring.

Switch to Two-door Two-way:: When the control panel type is set to the four-door access control panel, the four-door access control panel can be switched to the two-door two-way access control panel in the system.

Add to Level: Automatically add the device to the selected level. The device cannot be automatically added to the selected level if the number of personnel exceeds 5000. You can add personnel after the device is successfully added.

Clear Data in the Device when Adding: Tick this option, after adding device, the system will clear all data in the device (except the event logs). If you add the device just for demonstration or testing, there is no need to tick it.

(2) After editing, click [OK], and the system will try to connect the current device.

If successful connect, it will read the corresponding extended parameters of the device.

Extended Device Parameters: includes serial number, device type, firmware version number, auxiliary input quantity, auxiliary output quantity, door quantity, device fingerprint version, and reader quantity etc.

Note: When deleting a new device, the software will clear all user information, time zones, holidays, and access control levels settings (including access levels, anti-pass back, interlock settings, linkage settings etc.) from the device, except the events record (unless the information in the device is unusable, or it is recommended not to

delete the device in used to avoid the loss of information).

Access Controller Settings:

✧ TCP/ IP Communication Requirements

Support and enable TCP/ IP communication, directly connect device to the PC or connect to the local network, query IP address and other information of the device;

✧ RS485 Communication Requirements

Support and enable RS485 communication, connect device to PC by RS485, query the serial port number, RS485 machine number, band rate and other information of the device.

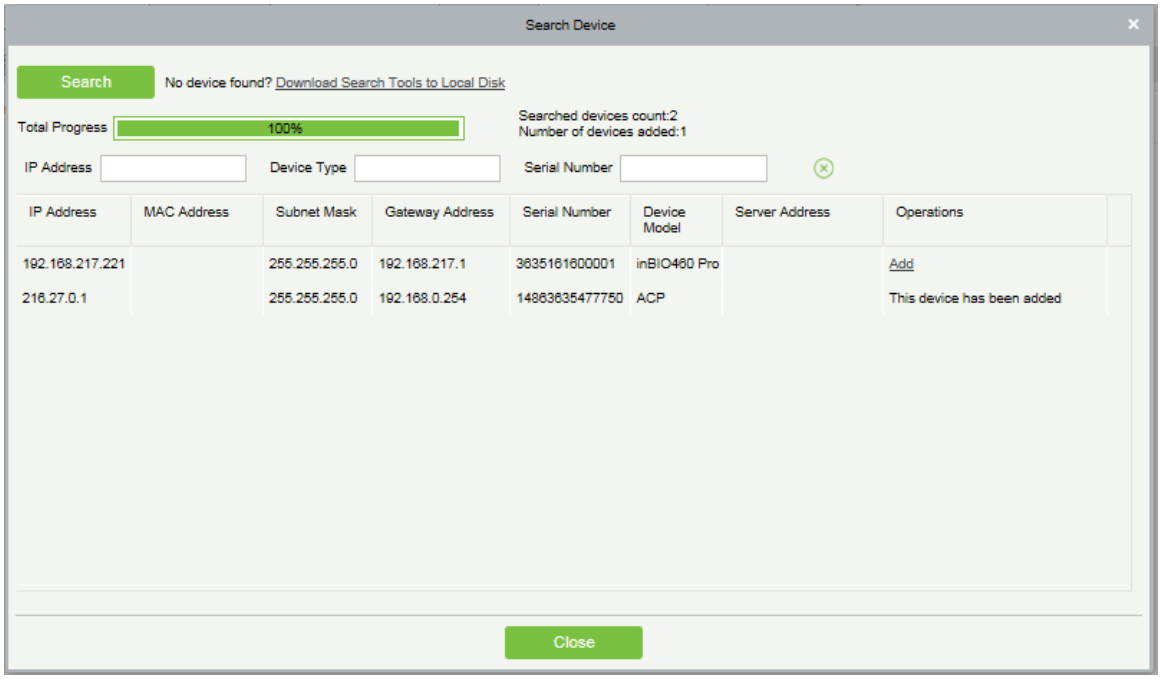
2. Add Device by Searching Access Controllers

Search the access controllers in the Ethernet.

(1) Click [Access Device] > [Device] > [Search Device], to show the Search interface.

(2) Click [Search], and it will prompt [Searching……].

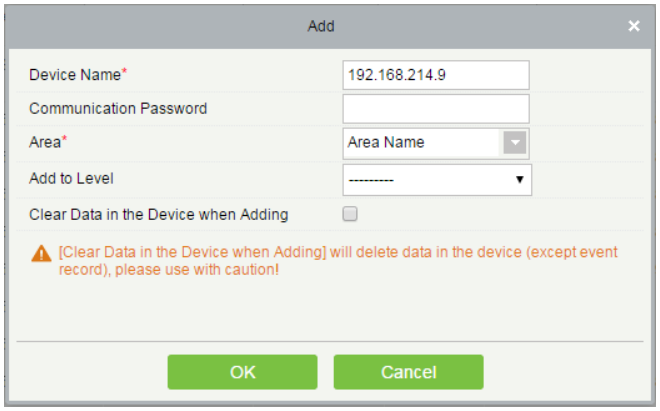
(3) After searching, the list and total number of access controllers will be displayed.



Note: UDP broadcast mode will be used to search access device, this mode cannot perform cross-Router function. IP address can provide cross-net segment, but must be in the same subnet, and needs to be configured the gateway and IP address in the same net segment.

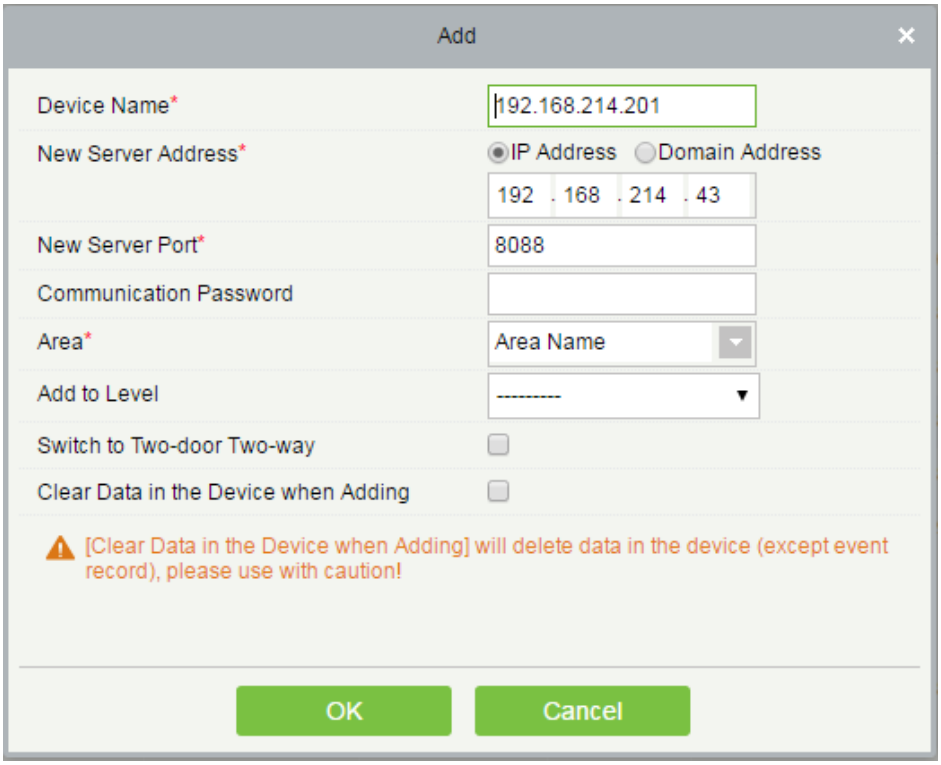
(4) Click [Add Device] behind the device.

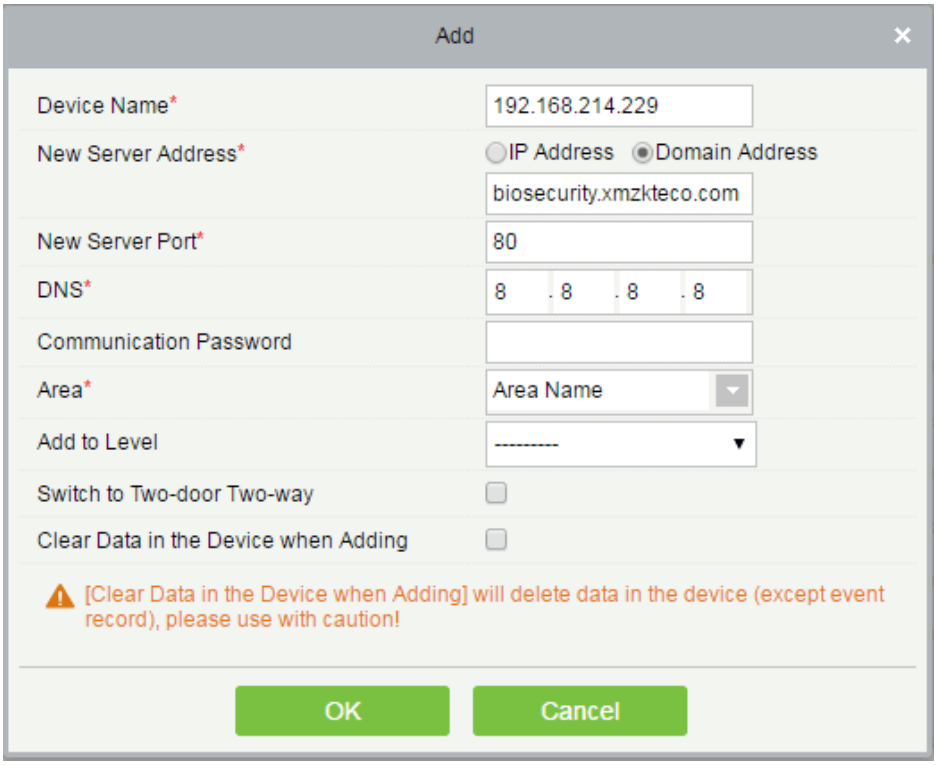
If the device is a pull device, enter a device name, and click [OK] to complete device adding.



Clear Data in the device when adding: Tick this option, after adding device, the system will clear all data in the device (except the event logs).

If the device is with a push firmware, the following windows will pop-up after clicking [Add]. After configure IP address and port number when tick IP Address in [New Server Address] option, or configure domain address, port number and DNS when tick Domain Address in [New Server Address] option, device will be added to the software automatically.





New Server Address: To add device by IP Address or Domain Address, part devices can be added to the software by entering domain address.

New Server Port: Set the access point of system.

DNS: Set DNS address of the server

Clear Data in the Device when Adding: Check this option, after adding device, the system will clear all data in the device (except the event logs). If you add the device just for demonstration or testing, there is no need to tick it.

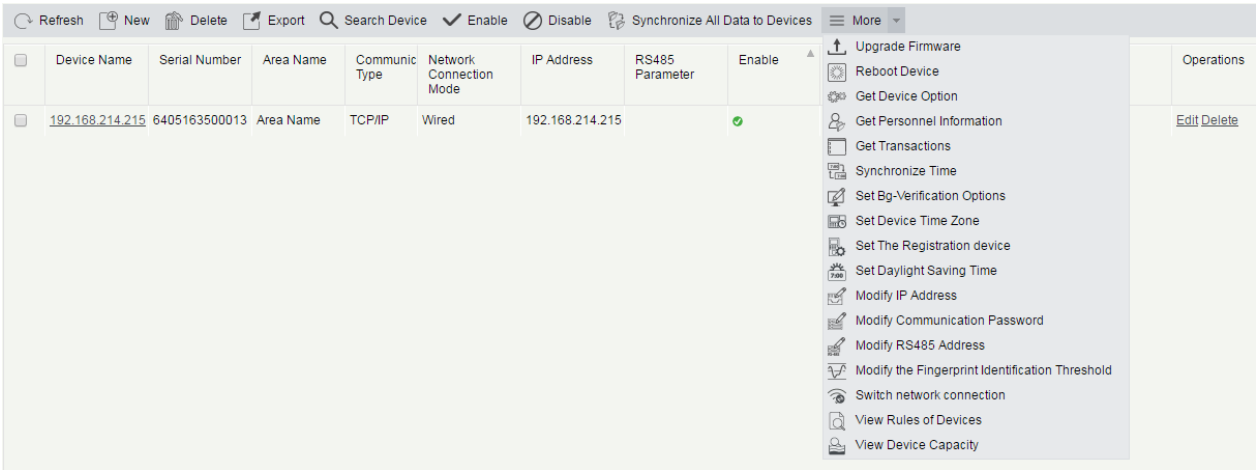
Note: When using one of the three add device methods above, if there exist residual data in original device, after a new device added to the software, please sync original data to it by clicking [Device] > [Synchronize All Data to Devices], otherwise these original data may conflict with normal usage.

(5) The default IP address of the access device may conflict with the IP of a device on the Local network. You can modify its IP address: Click [Modify IP Address] behind the device and a dialog box will open. Enter the new IP address and other parameters (Note: Configure the gateway and IP address in the same net segment).

Note: Some PUSH devices support SSL. To use this function, select the HTTPS port during software installation and ensure that the device firmware supports SSL.

4.1.2 Device Operation

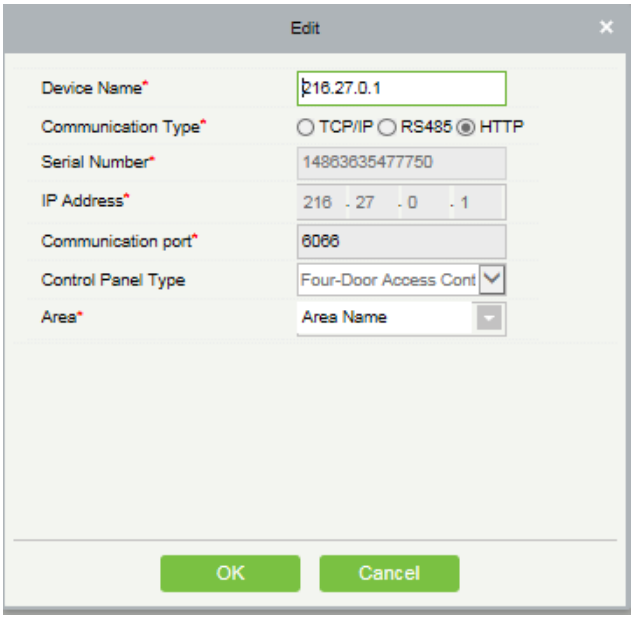
For communication between the system and device, data uploading, configuration downloading, device and system parameters shall be set. User can edit access controller within its levels in the current system, and only can add or delete devices in Device Management if needed.



- Edit or Delete a Device

Edit: Click Device Name, or click [Edit] below operations to open the edit interface.

Delete: Select device, click [Delete], and click [OK] to delete the device.



For the meanings and settings of the above parameters, see the relevant chapters for details. Items displayed in grey are not editable. Device Name must not be identical to the name of another device.

Access Control Panel Type cannot be modified, if the type is wrong, user need to manually delete the device and add it again.

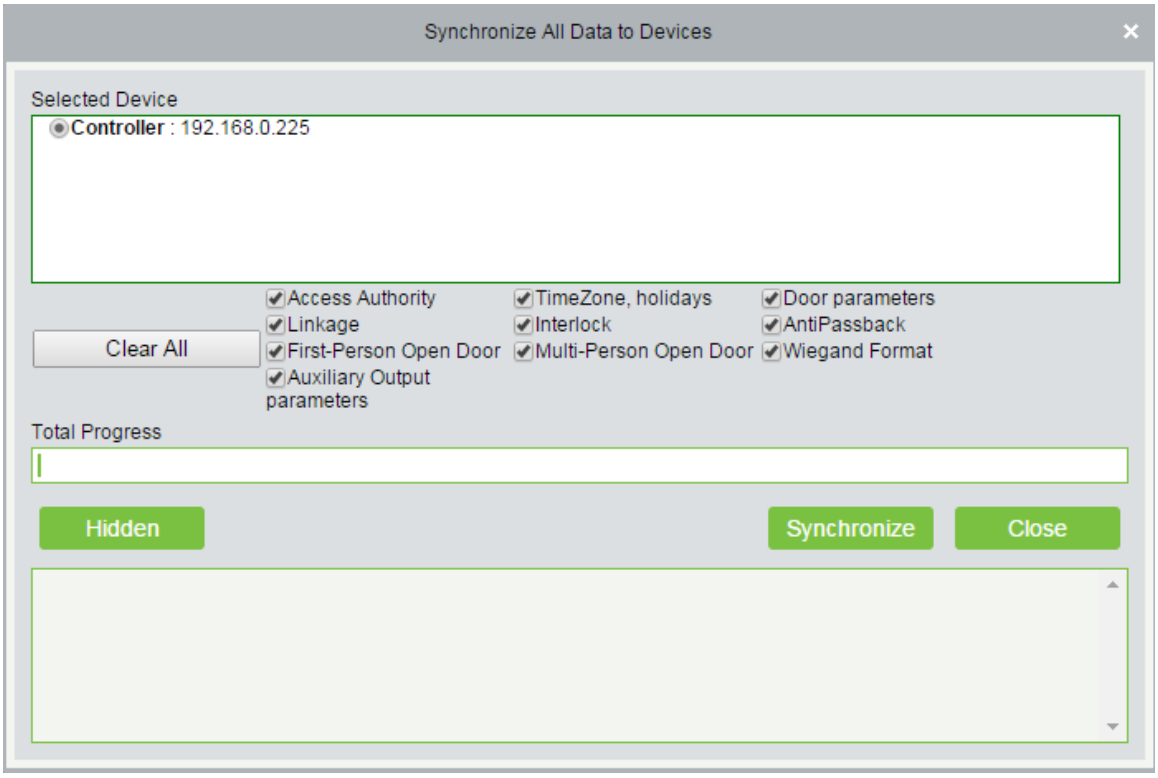
- Disable/Enable

Select device, click [Disable/ Enable] to stop/ start using the device. When communication between device and the system is interrupted or device fails, the device may automatically appear in disabled status. After adjusting local network or device, click [Enable] to reconnect the device and restore device communication.

- Synchronize All Data to Devices

Synchronize data in the system to the device, Select device, click [Synchronize All Data to Devices] and click [OK] to

complete synchronization.



Note: [Synchronize All Data to Devices] will delete all data in the device first (except transactions), and thus download all settings again. Please keep the net connection stable and avoid power down situations, etc. If the device is working normally, please use this function with caution. Execute it in rare user situations to avoid impact on normal use of the device.

- Upgrade Firmware

Tick the device that needs to upgrade firmware, click [Upgrade firmware] to enter edit interface, then click [Browse] to select firmware upgrade file (named emfw.cfg) provided by Access software, and click [OK] to start upgrading.

Note: The user shall not upgrade firmware without authorization. Contact the distributor before upgrading firmware, or upgrade it with instruction by the distributor. Unauthorized upgrade may bring problems that affect your normal use.

- Reboot Device

Reboot the selected device.

- Get Device Option

Get the common parameters in the device. For example, get the firmware version after the device is updated.

- Get Personnel Information

Renew the current number of personnel, fingerprints, finger vein and face in the device. The final value will be displayed in the device list.

- Get Transactions

Get transactions from the device into the system. Two options are provided for this operation: Get New Transactions and Get All Transactions.

Get New Transactions: The system only gets the new transactions since the last time transactions were collected and recorded into the database. Repeated transactions will not be rewritten.

Get All Transactions: The system will get all of the transactions again. Repeated Entries will not be rewritten.

When the network status is operating well and the communication between system and device is normal, the system will acquire transactions of the device in real-time and save them into the system database. However, when the network is interrupted or communication is interrupted for any reasons, and the transactions of the device have not been uploaded into the system in real-time, [Get Transactions] operation can be used to manually acquire transactions of the device. In addition, the system, by default, will automatically acquire transactions of the device at 00:00 each day.

Note: Access controller can store up to 100 thousands of transactions. When transactions exceed this number, the device will automatically delete the oldest stored transactions (delete 10 thousands transactions by default).

- Synchronize Time

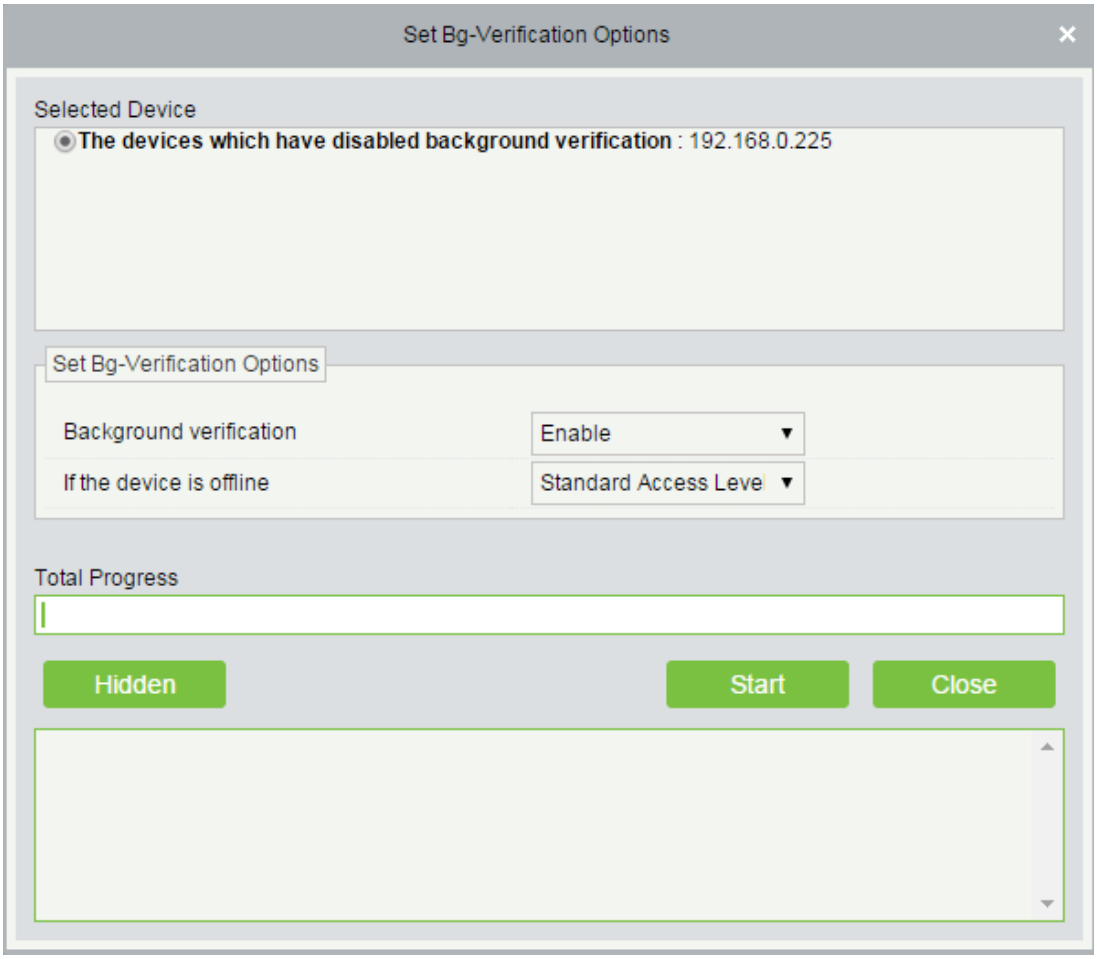
Synchronize device time with current server time.

- Set Server

Setting parameters of the device connected to the server.

- Set Background Verification Parameters

(1) Select the device which shall be on line, click [More] > [Set Bg verification parameters]:



Background verification: Enable or Disable Background verification function.

If the device is offline: If the controller is offline, device has levels of Standard Access Level or Access Denied.

(2) After setting, click [Start] button to issuing the Background verification parameters Settings.

Note: If you need advanced access control functions, please enable [Background verification], and issue the background verification parameters to the device.

- Set Device Time Zone

If the device supports the time zone settings and is not in the same time zone with the server, you need to set the time zone of the device. After setting, the device will automatically synchronize the time according to the time zone and server time

- Set Daylight Saving Time

According to the requirements of different regions, set Daylight Saving Time rules.

- Modify IP Address

Select device and click [Modify IP address] to show the modification interface. It will obtain real-time network gateway and subnet mask from the device (If obtaining fails, IP address cannot be modified). Enter new IP address, gateway, and subnet mask. Click [OK] to save settings and quit. This function is the same as [Modify IP Address Function] in Device. The difference is when searching control panels, the devices has not been added into the

system, while the current Modify Device IP Address is regarding added devices.

- Modify Communication Password

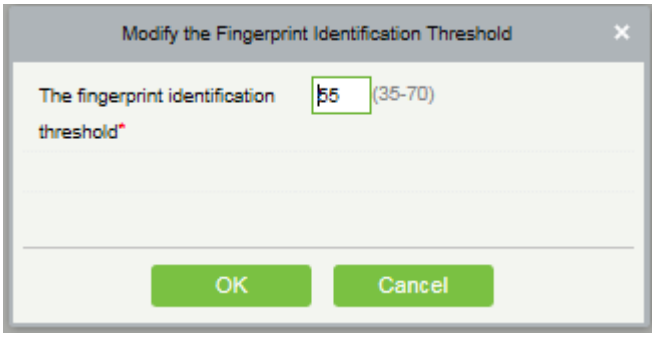
Enter the old communication password before modification. After verification, input the same new password twice, and click [OK] to modify the communication password.

Note: Communication password cannot contain space; it is recommended that a combination of numbers and letters be used. Communication password setting can improve the device security. It is recommended to set communication password for each device.

- Modify RS485 Address

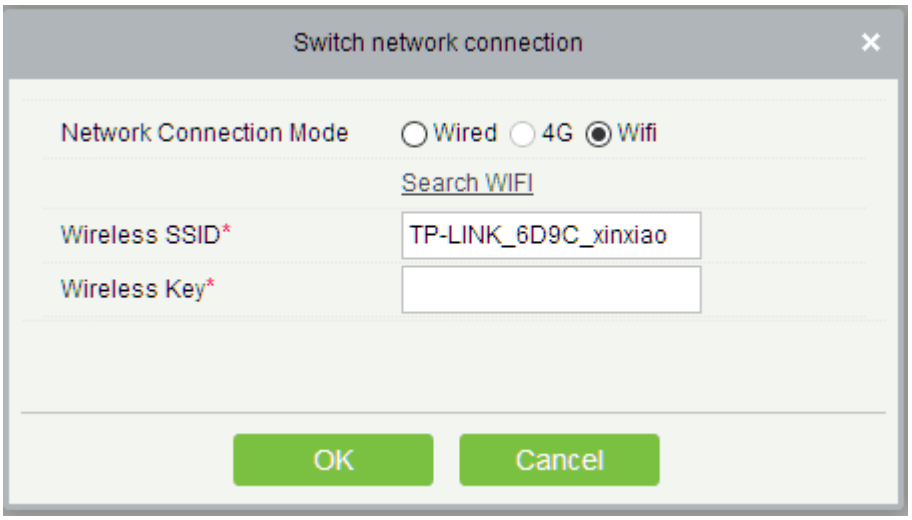
Only the devices that use RS485 communication and with no DIP Switch can modify RS485 address.

- Modify the fingerprint identification threshold (Ensure that the access controller supports fingerprint function)



User can modify the fingerprint identification threshold in the device; scale is 35-70 and 55 by default. When add device, the system will read the threshold from the device. User can view the threshold in devices list. Batch operation is permitted.

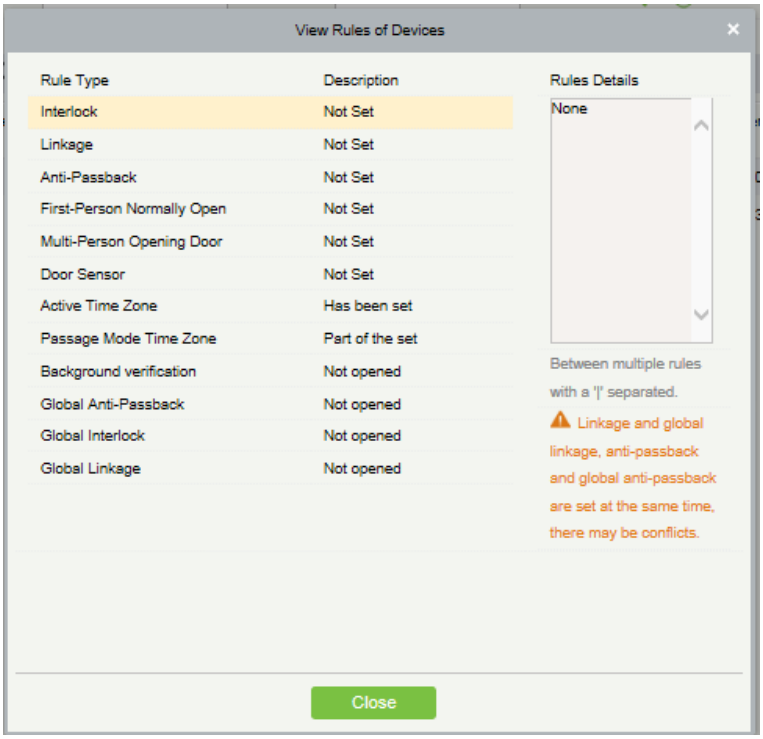
- Switch network connection



This function is applicable to InBio5 series access control panels, which is used to switch currently network connection mode of control panel.

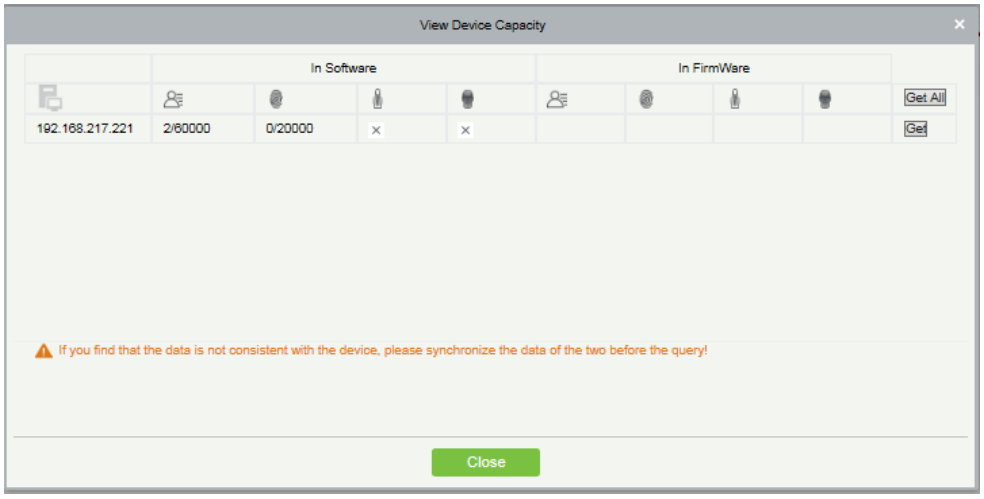
View Rules of Devices

View the Access rules in the device.



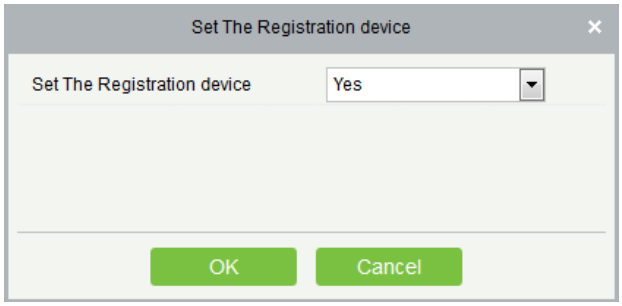
View Device Capacity

Check the capacity of personnel's fingerprint in the device.



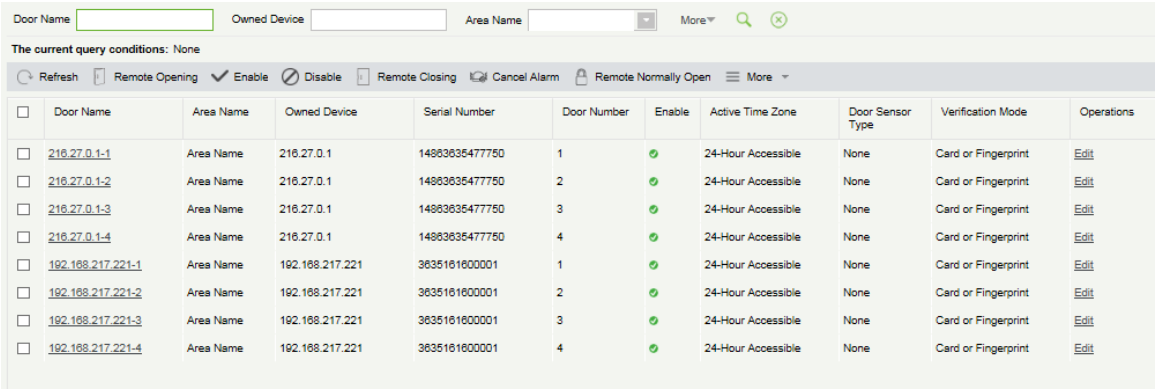
Set The Registration device

Only when set the registration device, standalone device's data such as personnel can automatically upload.



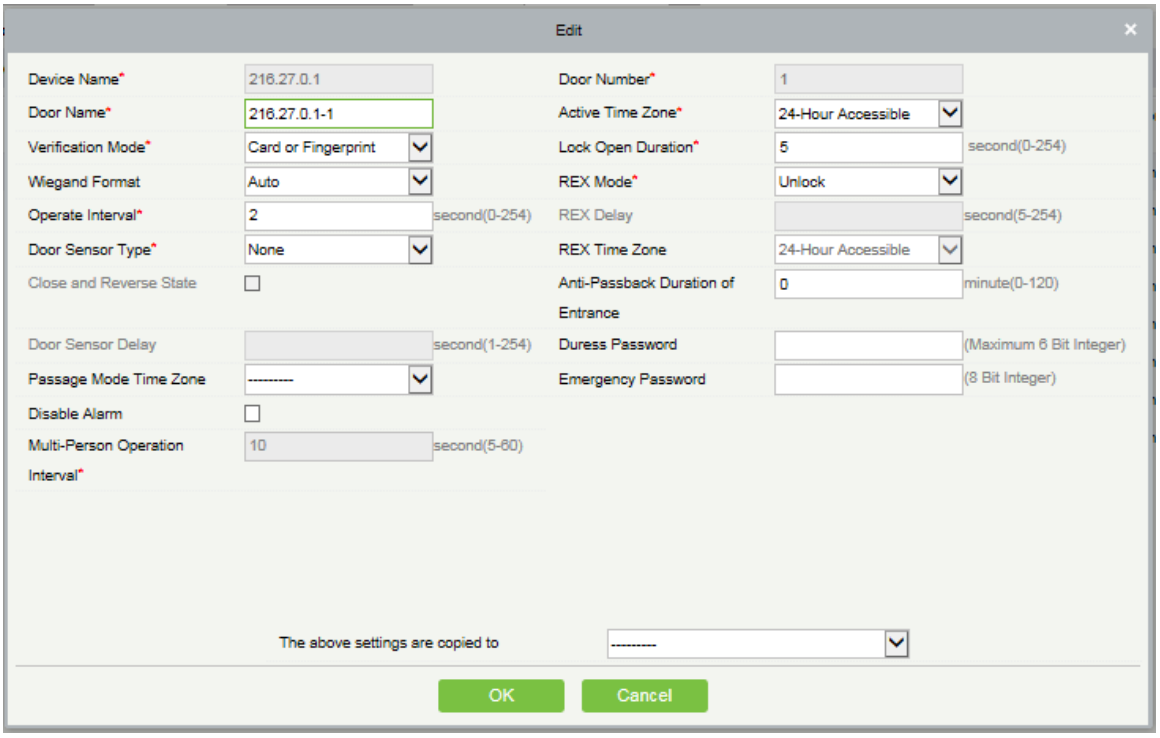
4.1.3 Doors

1. Click [Access Device] > [Device] > [Door] to enter Door Management interface (click "Area Name" in the left, system will automatically filter and display all access devices in this area).



- Door parameter modification:

Select the door to be modified, and click Door Name or [Edit] button below operations to show the Edit interface:



Fields are as follows:

Device Name: It is not editable.

Door Number: System automatically names it according to doors quantity of the device. This number will be consistent with the door number on the device.

Note: By default the number following the underline in the Door Name is consistent with the Door Number, but 1/2/3/4 in anti-passback and interlock refer to Door Number rather than the number following the Door Name, and they are not necessarily related.

Door Name: The default is "device name _door number". The field allows user to modify as required. Up to 30 characters can be entered.

Active Time Zone: By default both are null. Active Time Zone must be input, so that the door can be opened and closed normally. Passage Mode Time Zone must be set within the Active Time Zone.

Note: For a door currently in Normal Open state, consecutive verification of a person having access level for the door for 5 times (verification interval should be within 5 second.) can release the current Normal Open status and close the door. The next verification will be a normal verification. This function is only effective at the Active Time Zone of specified door. And within the same day, other Normal Open intervals set for the door and First-Person Normally Open settings will not take effect anymore.

Lock Open Duration: Used to control the delay for unlocking after punching. The unit is second (range: 0~254 seconds), and the default is 5 seconds.

Operate Interval: Interval between two punches, the unit is second (range: 0~254 seconds), and the default is 2 seconds.

Anti-passback Duration of Entrance: Only one entry is allowed with a reader in this duration. The unit is minute (range: 0~120 minutes), and the default is 0 minute.

Door Sensor Type: None (no detect door sensor), Normal Open, Normal Close. The default is NO. When select Normal Open or Normal Close, you need to set Door Sensor Delay and decide whether or not Close and Reverse-lock is required. When door sensor type is set as Normal Open or Normal Close, The default door sensor delay is 15 seconds, and enable close and reverse state.

Door Sensor Delay: The duration for delayed detection of the door sensor after the door is opened. When the door is not in the Normally Open period, and the door is opened, the device will start timing. It will trigger an alarm when the delay duration expired, and stop alarm when you close the door. The default door sensor delay is 15s (range: 1~254 seconds). Door Sensor Delay should be longer than Lock Open Duration.

Close and Reverse State: Set locking or not after door closing. Tick it for lock after door closing.

Verification Mode: Identification modes include Only Card, Card plus Password, Only Password, Card plus Fingerprint, Card or Fingerprint. The default is Card or Fingerprint. When Card plus Password mode is selected, make sure the door is equipped with a reader with keyboard.

Wiegand Format**:** Select the Wiegand card format that can be identified by the Wiegand reader of the door. If the punched card format is different with the setting format, the door cannot be opened. The software is embedded with 9 formats, and the default is automatic matching to Wiegand card format. (except for the card format name with a, b or c).

Request to Exit（REX Mode）: Locking indicates that the door is locked after the exit button is pressed. Unlocking indicates that the door is unlocked after the exit button is pressed. The default is unlocking.

Request to Exit Delay（REX Delay）: Indicates the alarm delay time for door detection after the exit button is locked. When the door is unlocked forcibly, the system detects the door status after a period of time. The default is 10s (range: 1~254 seconds). The exit button has to be locked before setting this option.

REX Time Zone: The button is available only in the specified time segment.

Duration of Entrance: Based on the lock open duration, the door sensor delay and exit delay, the duration of entrance is the extra time limit. To function this feature, you need to check [Delay passage] option to extend when add or edit staff. For example, you may set the duration of entrance for people with disabilities.

Open Door Delay: The time period from the completion of verification to opening door (range: 1~60 seconds).

Multi-Person Operation Interval: The time period during two people verify with card or fingerprint (range: 1~60 seconds).

Duress Password, Emergency Password: Upon duress, use Duress Password (used with legal card) to open the door, when opening with Duress Password, it will alarm. Upon emergency, user can use Emergency Password (named Super Password) to open door. Emergency Password allows normal opening, and it is effective in any time zone and any type of verify mode, usually used for the administrator.

- ✧ Duress Password Opening (used with legal card): Password is a number not exceeding 6 digits. When Only Card verification mode is used, you need to press [ESC] first, and then press the password plus [OK] button. Finally punch legal card. The door opens and triggers the alarm. When Card + Password verify mode is used, please punch legal card first, then press the password plus [OK] button (same to normal opening in card plus password verification mode), the door open and trigger the alarm.

- Emergency Password Opening: Password must be 8 digits. The door can be opened only by entering the password. Please press [ESC] every time before entering password, and then press [OK] to execute.

When using Duress Password or Emergency Password, the interval for entering each number shall not exceed 10 seconds, and the two passwords should not be the same.

Disable Alarm: check the box to disable the alarm voice in real-time monitoring page.

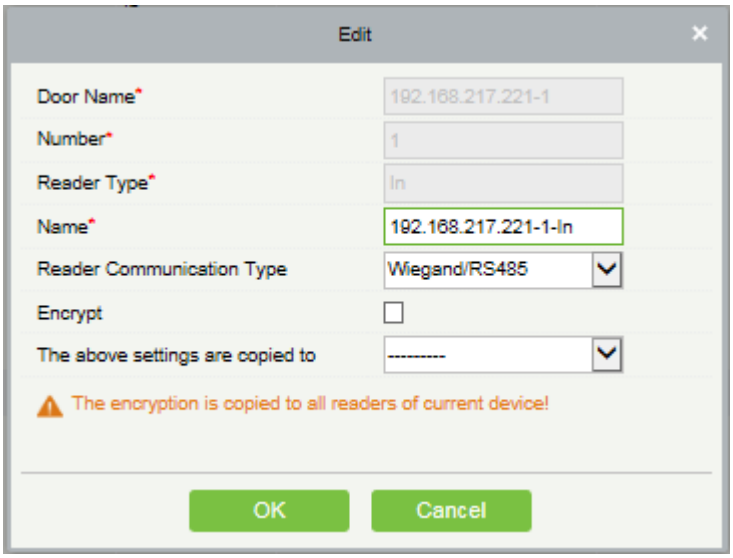
The above Settings are Copied to: Including below two options.

- All doors of current device: Click to apply to all doors of the current access device.
- All doors of all devices: Click to apply to all doors of all access devices within the current user's level.

2. After parameter editing, click [OK] to save and quit.

4.1.4 Reader

1. Click [Access Device] > [Reader] on the Action Menu, select a reader and click [Edit]:

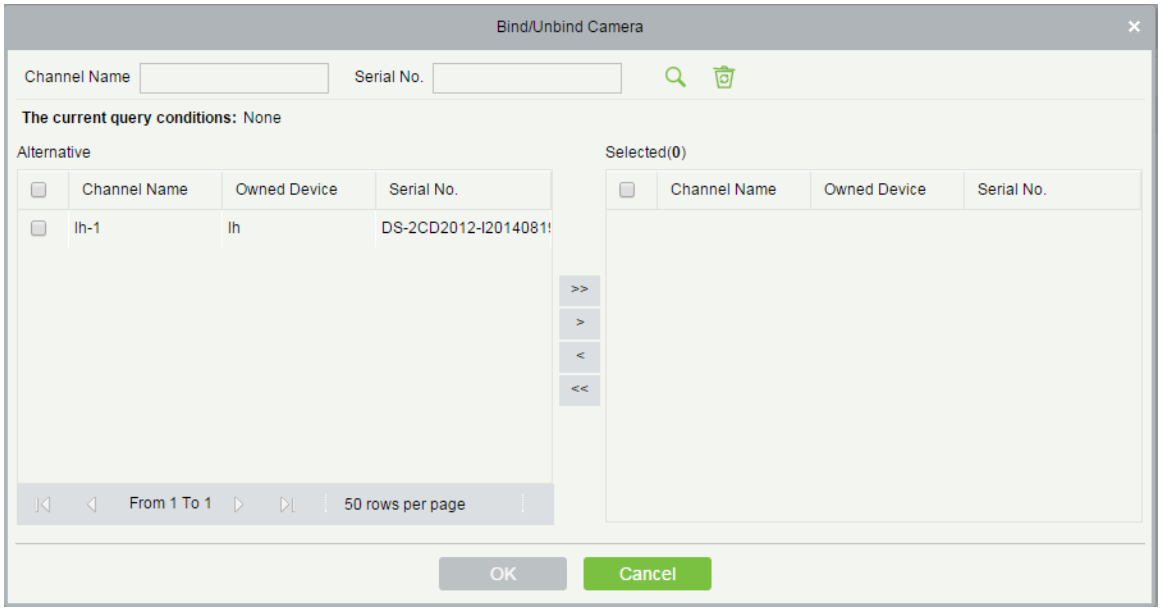


Name: Name of the reader displayed on the list page.

Reader Communication Type: Wiegand/RS485, Wiegand, RS485, and Disabled are available. When a communication type is selected, the reader interface on the device receives data (including card and fingerprint data) only of the specified type.
Encrypt: If this option is selected, the device can use only encrypted readers, such as SF10 and FR1300.
Bind/Unbind Camera

Bind camera, if carried out the interaction setting in Linkage or in Global Linkage, it will make a video linkage (pops up video, video or capture) once there is a corresponding event occurs.

Click [Bind/Unbind Camera] to select a channel or channels:



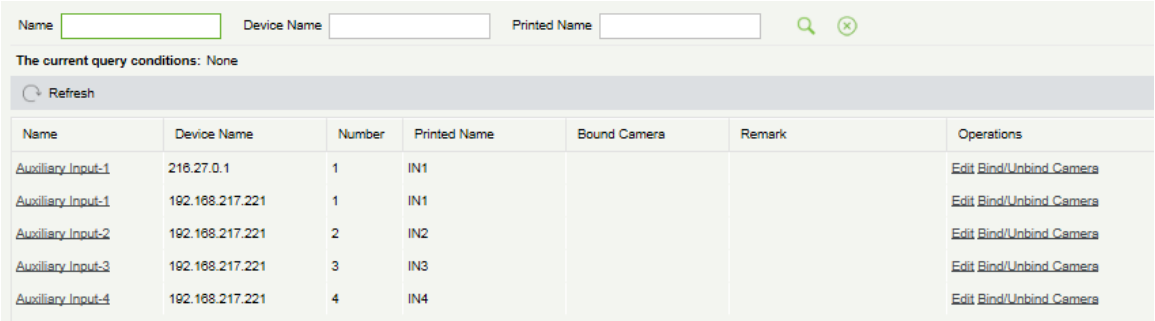
Click [OK] to finish.

Note: A reader can bind more than one channel.

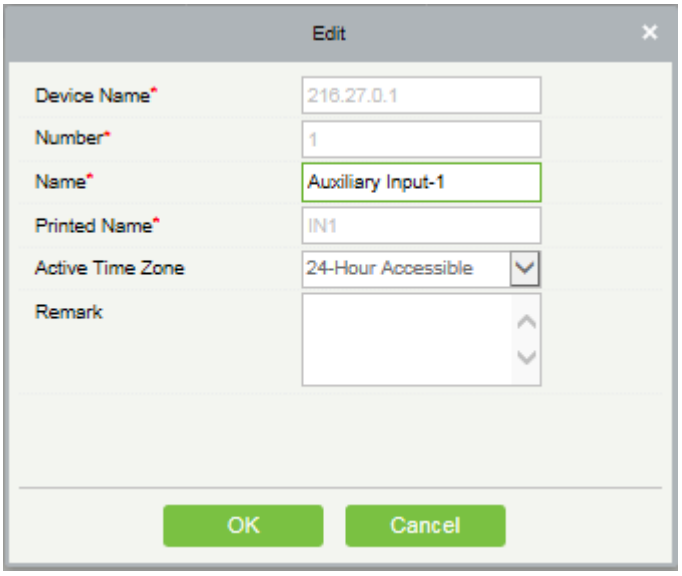
4.1.5 Auxiliary Input

It is mainly used to connect to devices, such as the infrared sensor or smog sensor.

1. Click [Access Device] > [Auxiliary Input] on the Action Menu, enter into the following page:



2. Click [Edit] to modifiy the parameters:



Fields are as follows:

Name: You can customize the name according to your preference.

Printed Name: The printing name in the hardware, for example IN5.

Active Time Zone: Auxiliary input is available only in the specified time segment.

Note: Only Name, Active Time Zone and Remarks can be modified.

3. Click [Edit] to modify the name and remark. Others are not allowed to edit here.

- Bind/Unbind Camera

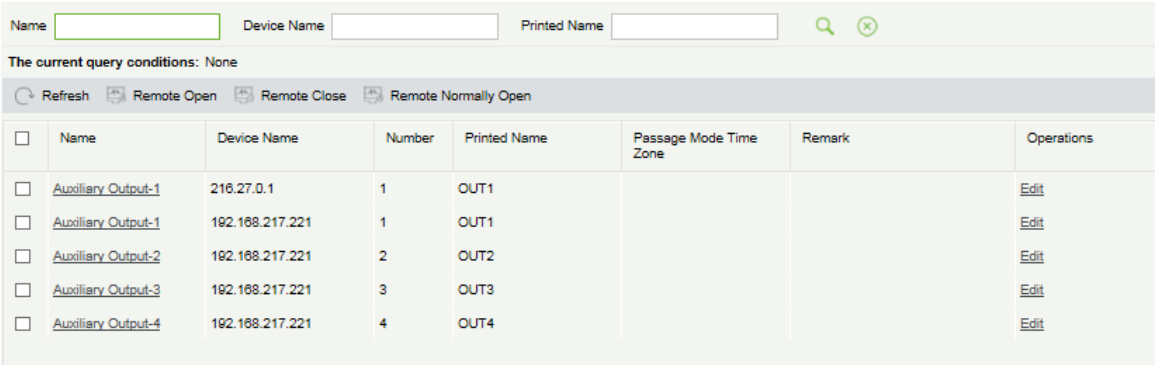
Bind camera, if carried out the interaction setting in Linkage or in Global Linkage, it will make a video linkage (pops up video, video or capture) once a corresponding event occurs. For more steps, please refer to Reader: Bind/Unbind Camera.

Note: An input point can bind more than one channel.

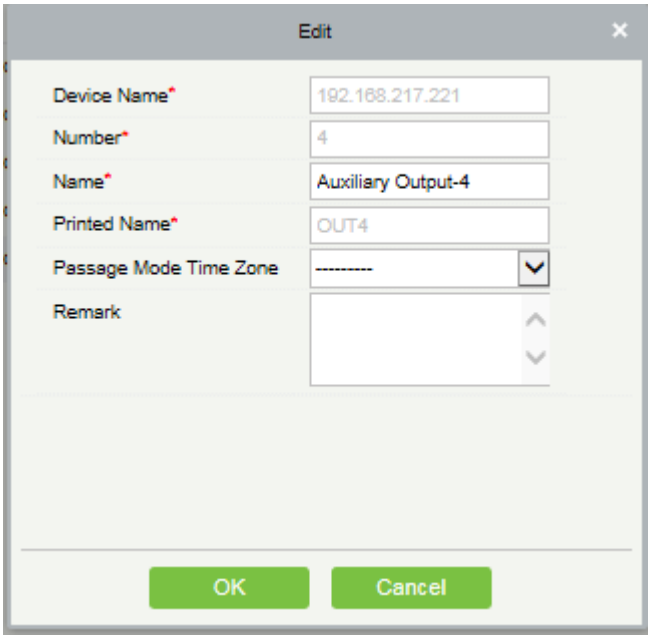
4.1.6 Auxiliary Output

Mainly connected to alarm, it is used when linkage is working.

1. Click [Access Device] > [Auxiliary Output] on the Action Menu, enter into the following page:



2. Click [Edit] to modifiy the parameters:



Fields are as follows:

Name: You can customize the name according to your preference.

Printed Name: The printing name in the hardware, for example OUT2.

Passage Mode Time Zone: The auxiliary output is in normal open or normal close in this time zone.

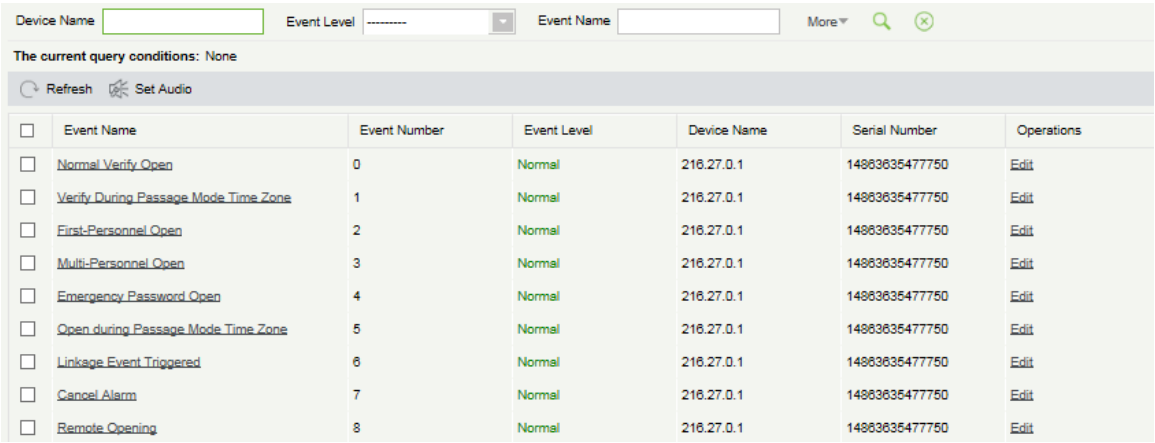
Note: Only Name, Passage Mode Time Zone and Remarks can be modified.

3. Click [Edit] to modify the name and remark.

4.1.7 Event Type

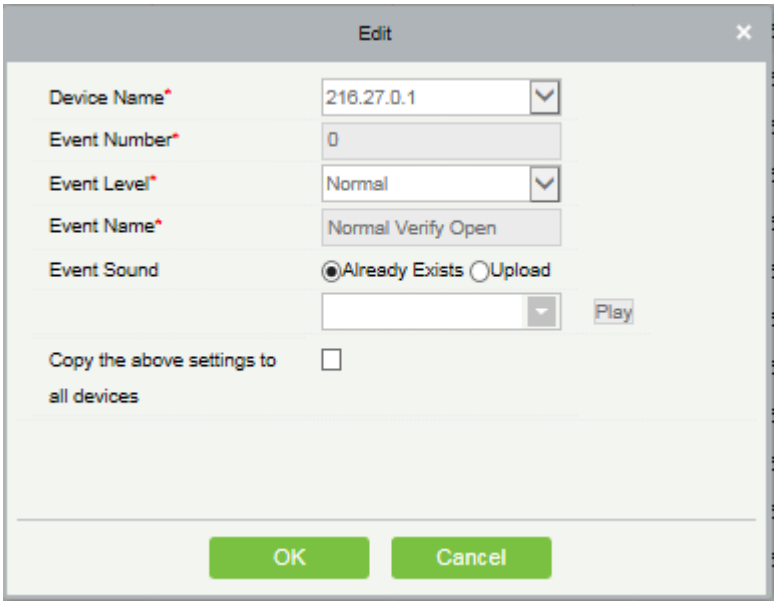
Display the event types of the access devices.

1. Click [Access Device] > [Event], the following page is displayed:



Event Name	Event Number	Event Level	Device Name	Serial Number	Operations
Normal Verify Open	0	Normal	216.27.0.1	14863635477750	Edit
Verify During Passage Mode Time Zone	1	Normal	216.27.0.1	14863635477750	Edit
First-Personnel Open	2	Normal	216.27.0.1	14863635477750	Edit
Multi-Personnel Open	3	Normal	216.27.0.1	14863635477750	Edit
Emergency Password Open	4	Normal	216.27.0.1	14863635477750	Edit
Open during Passage Mode Time Zone	5	Normal	216.27.0.1	14863635477750	Edit
Linkage Event Triggered	6	Normal	216.27.0.1	14863635477750	Edit
Cancel Alarm	7	Normal	216.27.0.1	14863635477750	Edit
Remote Opening	8	Normal	216.27.0.1	14863635477750	Edit

2. Click [Edit] or click the event type name to edit:



Fields are as follows:

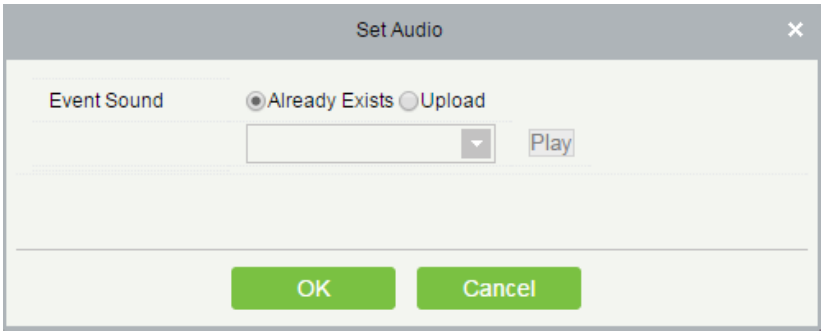
Event Level: Normal, Exception, and Alarm are available.

Event Name: It can't be modified.

Event Sound: Custom a sound being played when the event occurred in real-time monitoring.

Copy the above settings to all devices: This event is applied to all current devices within the purview of the same user event number.

Set Audio: Same as the event sound. Click [Set Audio] :



You may upload a sound from the local. The file must be in wav or mp3 format, and it must not exceed 10M.

More details about Event Type, please refer to Access Event Type.

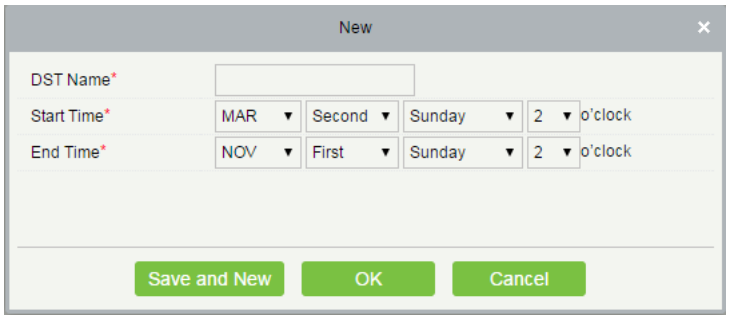
4.1.8 Daylight Saving Time

DST, also called Daylight Saving Time, is a system to prescribe local time in order to save energy. The unified time adopted during the system date is called "DST". Usually, the time will be one hour forward in summer. It can make people sleep early and get up early. It can also reduce lighting to save power. In autumn, the time will be recovered. The regulations are different in different countries. At present, nearly 110 countries adopt DLST.

To meet the demand of DLST, a special option can be customized. Make the time one hour forward at XX (hour) XX (day) XX (month), and make the time one hour backward at XX (hour) XX (day) XX (month) if necessary.

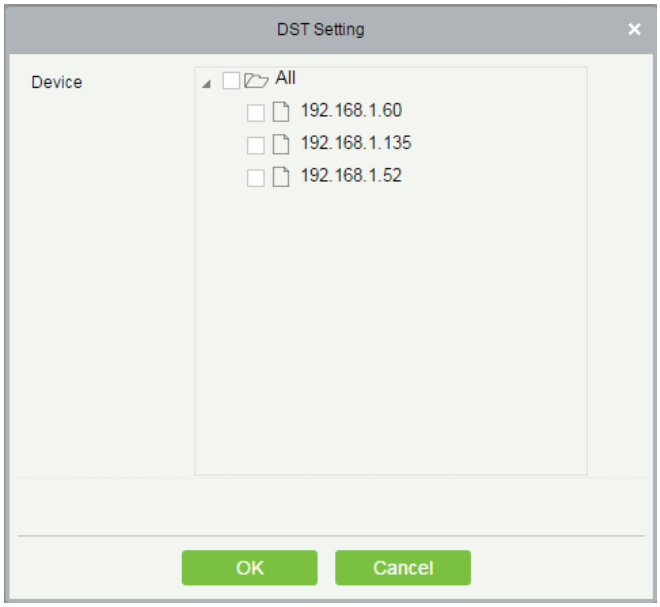
- Add DST

1. Click [Access Device] > [Daylight Saving Time] > [New]:



Set as "Month-Weeks-week hour: minute" format. The start time and end time is in need. For example, the start time can be set “second Monday in March, 00:00” When the start time arrives, the system will be advanced one hour. When the end time arrives, the system will turn back to the original time.

- Use a DST



The user can enable the DST setting on a device: In the DST interface, select a DST setting, and click [DST Setting], select the device to apply the DST setting to and click [OK] to confirm.

Notes:

1) If a DST setting is in use, it cannot be deleted. Stop the DST before deleting.

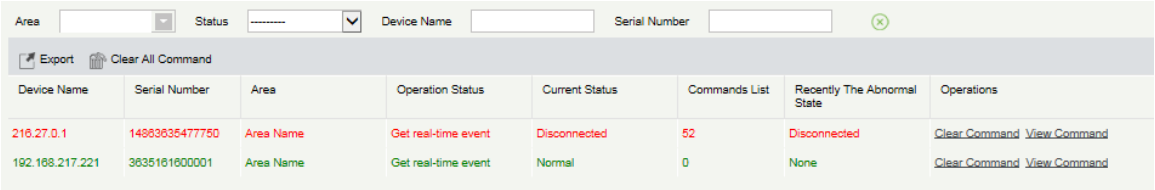
2) If a DST setting is in use, the latest modification will be sent to the device. The device disconnection will lead to transmission failure, and it will continue transmission at the next connection.

3) In the Door Management module of the access control system, you can enable or disable DST function. If you

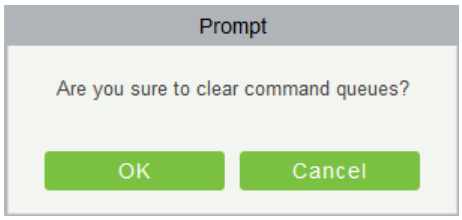
enable DST setting, when the start time arrives, the system will be advanced one hour. When the end time arrives, the system will turn back to the original time. If you have not set a DST in the device, when you disable DST, the system will prompt "The Daylight Saving Time hasn't been set in this device".

4.1.9 Device Monitoring

By default it monitors all devices within the current user's level, click [Access Device] > [Device Monitoring], and lists the operation information of devices: Device Name, Serial No., Area, Operation Status, current status, commands List, and Related Operation.



You may clear command as required. Click [Clear Command] behind the corresponding device:



Click [OK] to clear.

Notes:

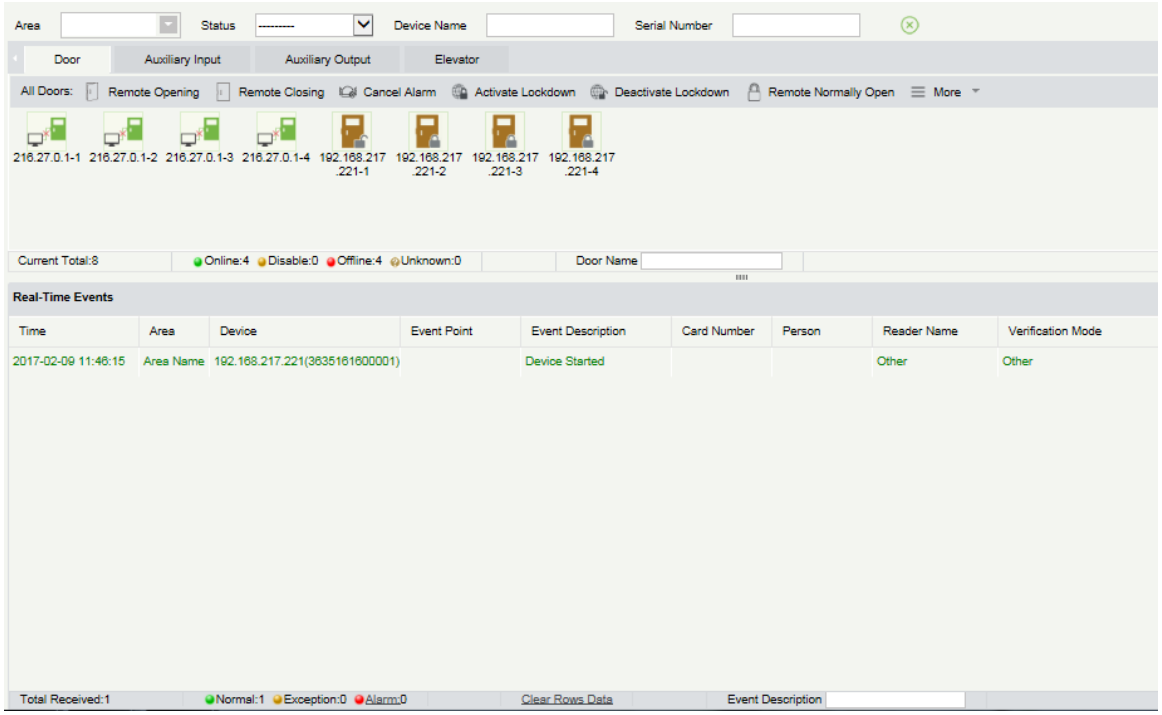
(1 After the Clear Command is executed, you can perform the Synchronize All Data to Devices operation on the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once the capacity is insufficient, you may replace the current device with a large-capacity one, or delete the right of some personnel to access this device, and then perform the Synchronize All Data to Devices operation.

(2) Operate State is the content of communications equipment of current device, mainly used for debugging.

(3) The number of commands to be performed is greater than 0, indicating that data is not synchronized to the device, just wait.

4.1.10 Real-Time Monitoring

Click [Access Device] > [Real-Time Monitoring], monitor the statuses and real-time events of doors under the access control panels in the system in real-time, including normal events and abnormal events (including alarm events). Real-Time Monitoring interface is shown as follows:



Different Icons represent statuses as follows:

Icons	Status	Icons	Status
	Device banned		Door Offline
/	Door sensor unset, Relay closed /Without relay status	/	Door sensor unset, Relay opened/Without relay status
/	Online status Door closed, Relay closed/Without relay status	/	Online status Door closed, Relay opened/Without relay status
/	Online status Door opened, Relay closed/Without relay status	/	Online status Door opened, Relay opened/Without relay status
	Door opened alarming, Relay closed		Door opened alarming, Relay opened
/	Door opening timeout, Relay closed /Without relay status, Door Sensor Opened	/	Door opening timeout, Relay opened/Without relay status
	Door opening timeout, Relay closed/ Door Sensor Closed		Door opening timeout, Relay opened/ Door Sensor Closed
/	Door closed alarming, Relay closed/Without relay status	/	Door closed alarming, Relay opened/Without relay status

	Door sensor unset, Door alarming, Relay closed		Door sensor unset, Door alarming, Relay opened
	Door opening timeout, Without relay status/Door Sensor Closed		Door locking

Note: Without relay status, indicates that the current firmware does not support detect relay status function.

1. Door

- Monitoring All

By default the home page displays all doors of the panels within the user's level. User may monitor one (or several) door by setting the Area, Access Control or Door.

Remote Opening/Closing: controls one door or all doors.

To control a single door, right click mouse, and click [Remote Opening/ Closing] in the pop-up dialog box. To control all doors, directly click [Remote Opening/ Closing] behind Current All.

In remote opening, User can define the duration of a door being open (The default is 15s).You can select [Enable Intraday Passage Mode Time Zone] to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door is not limited by any time zones (open for 24 hours).

To close a door, select [Disable Intraday Passage Mode Time Zone] first to avoid enabling other normal open time zones to open the door, and then select [Remote Closing].

Note: If [Remote Opening /Closing] always fails, check whether many devices are disconnected. If any, check the network.

Cancel the alarm: Once an alarming door is displayed on the interface, the alarm sound will ring. Alarm cancellation is involved in control on single door and all doors. To control a single door, put the mouse on the door icon, a menu will come out, then click [Remote Opening/ Closing] which in the menu. To control all doors, directly click [Remote Opening/ Closing] behind Current All.

Note: If [Cancel the alarm] fails, check whether many devices are disconnected. If any, check the network.

Remote Normally Open: Set the device as normal open by remote.

Activate Lockdown: Remotely sets the door status to locked status. At this time, the door cannot receive any operations, such as card reading and remote operations. This function is supported only by certain devices.
Deactivate Lockdown: Unlocks a locked door. This function is supported only by certain devices.

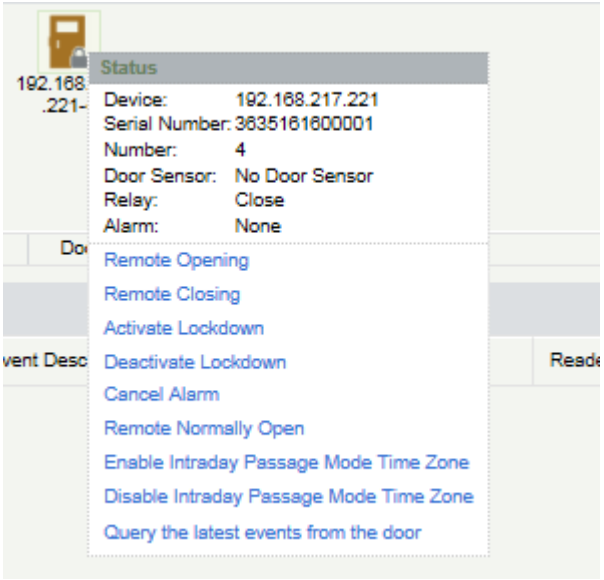
Personnel photo display: If Real-Time Monitoring is involved in a person, the monitor displays the personal photo (if no photo is registered, display default photo). The event name, time and name are displayed.

Play Audio: After checking this option, it plays a sound once the current page occurs an alarming even.

- Quick Management of Doors

Move the cursor to a door's icon; you can also do the above operations. In addition, you can query the latest events

from the door.



Query the latest events from the door: Click to quickly view latest events happened on the door.

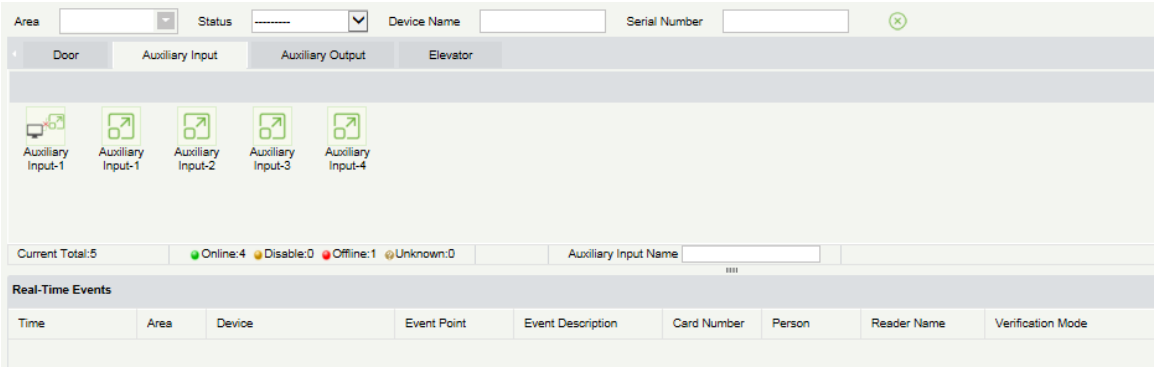
Issue card to person: If you swap an unregistered card, in real-time monitoring interface, will turn up a record wi th a card number. Right click that card number will show you a menu, click "Issue card to person", you can assign that card to one person.

- Event monitoring

System automatically acquires monitored device event records (by default, display 200 records), including normal and abnormal access control events (including alarm events). Normal events appear in green, alarm events appear in red, other abnormal events appear in orange.

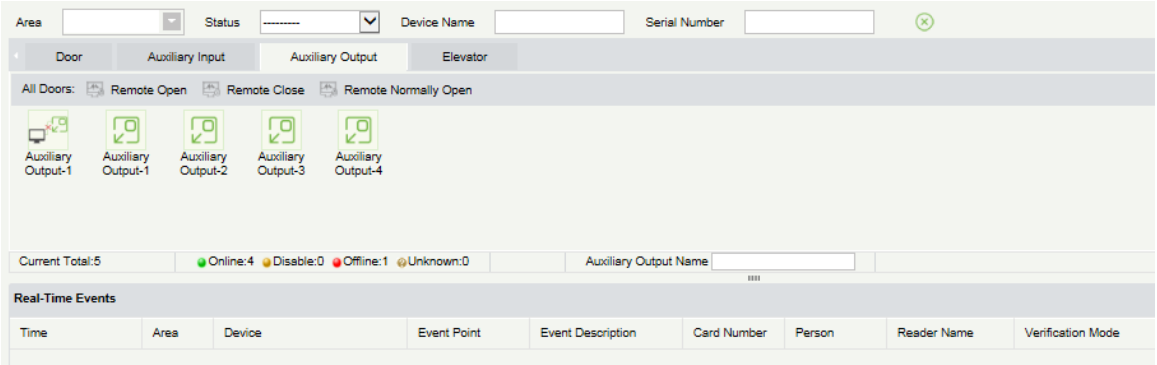
2. Auxiliary Input

Real-time monitor the current auxiliary input events.



3. Auxiliary Output

You can perform Remote open, Remote Close, Remote Normally Open.

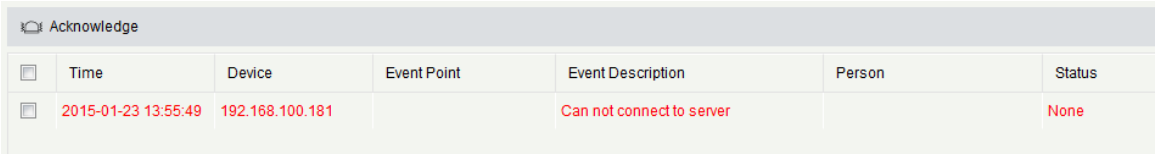


4. Elevator

About the real-time monitoring of elevator, please refer to Real-Time Monitoring.

4.1.11 Alarm Monitoring

Monitor alarm events of doors. If a door sends an alarm and is not confirmed, the page will always display the alarm events.



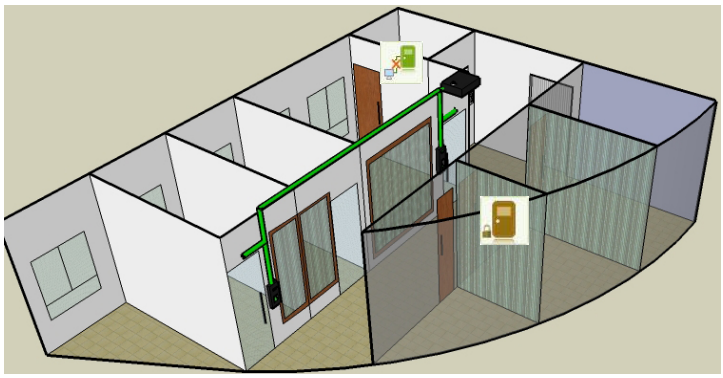
Note: The alarm type description will display only when the firmware version of the device supports, or Event Description will only display "alarm", detail types will not distinguish.

Cancel alarm: Select the door in alarm status, and click [Cancel alarm], the system will send email to alarm monitoring recipient's mailbox (The mailbox must be set in the Parameters)

Note: When a door has multiple alarm states, It will display just one alarm type description in the descending severity order, the order as follows: tamper-resistant alarm > duress alarm (password + fingerprint) > duress password or fingerprint alarm > unexpected opening alarm > opening timeout alarm > device disconnects alarm.

4.1.12 Map

Before using map, click [Access Device] > [Map] > [Add] to add a map first. After successful adding, user can add door, zoom-in, zoom-out map (and the door on the map), etc. If users need to change position of icon or the map, click [Save Positions] to save the current change, then the user can view the setting at next visit.



Add / Delete Map: User can add or delete map as needed.

Edit Map: User can edit map name, change map or the area it belongs to.

Adjust map (includes door): User can add a door on the map, or delete an exist one (right click the door icon, and select [Delete Door]), or adjust the map or position of the door or camera icon (by drag the door or camera icon), adjust size of the map (click [Zoom in] or [Zoom out] or click [Full Screen]).

Door operation: Move the mouse to a door, the system will automatically filter and display the operation according to the door status. User can remote opening / closing, cancel alarm, etc.

Levels control:

(1) In adding process, users need to select the belonging area for map. The area is relevant to the user access levels, user can only view or manage the map within levels. If the belonging area of a map is modified, all doors on the map will be cleared, user need to add manually again.

(2) When administrator adds a new user, he can manage the user operation rights by role setting, such as Save positions, Add Door, Add Camera, etc.

Notes:

(1) In map modification, user can select to modify the map name but not the path, only need to cancel the tick before Modify Path.

(2) The system supports to add multi doors at the same time. After door has been added, user needs to set the door position on the map, and click [Save].

(3) In door icon modifying, especially zoom out the map, the margin of upward and leftward shall not be smaller than 5 pixels. Or system will prompt error.

(4) Recommend adding map size under 1120 * 380 pixels. If the multi clients access the same server, the display effect will be differed according to resolution of screen and the setting of browser.

4.2 Access Control Management

4.2.1 Access Control Time Zones

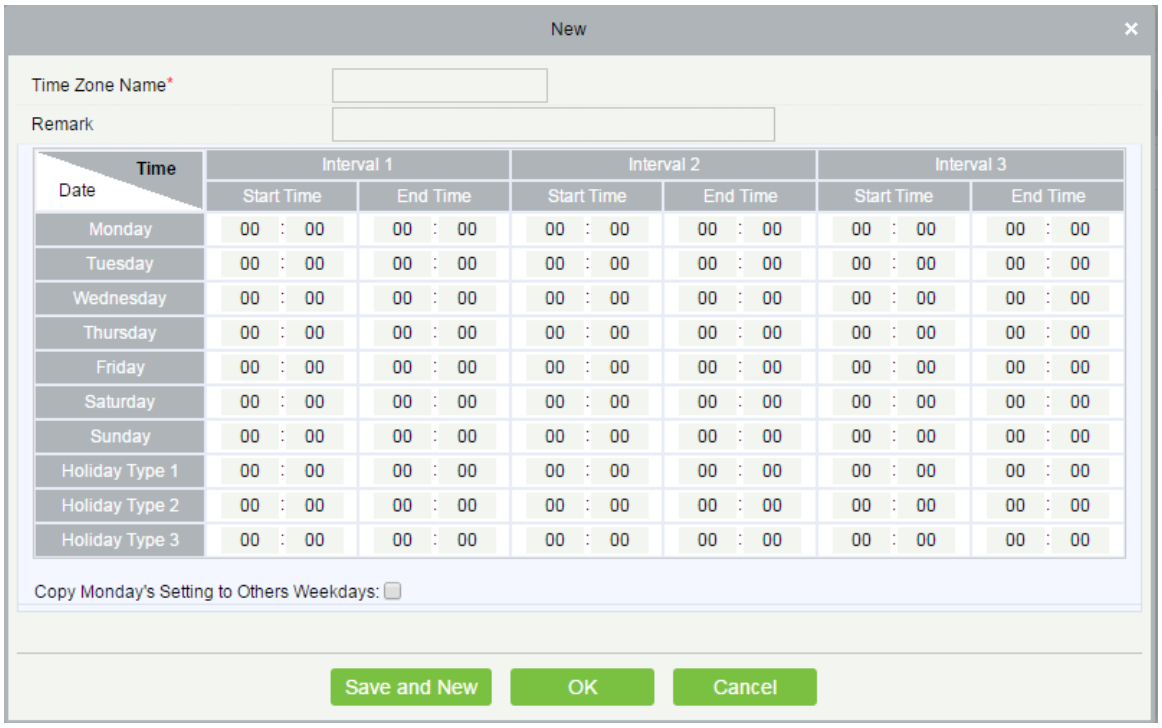
It set usage time of a door; the reader is usable during valid time periods of certain doors and unusable during

other time periods. Time Zone can also be used to set Normal Open time periods, or set access level so that specified users can only access specified doors during specified time periods (including access levels and First-Person Normally Open).

The system controls access according to Time Zones (up to 255 time zones). The format of each interval for a time zone: HH: MM-HH: MM, Initially, by default the system has an access control time zone named [24 hours Accessible]. This time period cannot be modified and deleted. The user can add new Access Control Time Zones that can be modified or delete.

1. Add Access Control Time Zone

(1) Click [Access Control] > [Time zones] > [New] to enter the time zone setting interface:



The parameters are as follows:

Time Zone Name: Any character, up to a combination of 30 characters.

✍Remarks: Detailed description of the current time zone, including explanation of current time zone and primary applications. The field is up to 50 characters.

Interval and Start/ End Time: One Access Control Time Zone includes 3 intervals for each day in a week, and 3 intervals for each of the three Holidays. Set the Start and End Time of each interval.

Setting: If the interval is Normal Open, just enter 00:00-23:59 as the interval 1, and 00:00-00:00 as the interval 2/3. If the interval is Normal Close: All are 00:00-00:00. If only using one interval, user just needs to fill out the interval 1, and the interval 2/3 will use the default value. Similarly, when only using the first two intervals, the third interval will use the default value. When using two or three intervals, user needs to ensure two or three intervals have no time intersection, and the time shall not span days. Or the system will prompt error.

Holiday Type: Three holiday types are unrelated to the day of a week. If a date is set to a holiday type, the three intervals of the holiday type will be used for access. The holiday type is optional. If the user does not enter one, system will use the

default value.

Copy on Monday: You can quickly copy the settings of Monday from Tuesday to Sunday.

(2) After setting, click [OK] to save, and it will display in the list.

2. Maintenance of Access Control Time Zones

Edit: Click the [Edit] button under Operation to enter the edit interface. After editing, click [OK] to save.

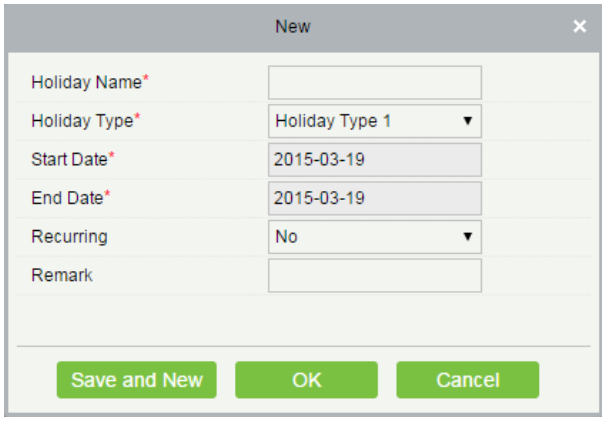
Delete: Click the [Delete] button under Related Operation, then click [OK] to delete, or click [Cancel] to cancel the operation. A time zone in use cannot be deleted. Or tick the check boxes before one or more time zones in the list, and click the [Delete] button over the list, then click [OK] to delete, click [Cancel] to cancel the operation.

4.2.2 Access Control Holidays

Access Control Time of a holiday may differ from that of a weekday. The system provides access control time setting for holidays. Access Control Holiday Management includes Add, Modify and Delete.

- Add

(1) Click [Access Control] > [Holidays] > [Add] to enter edit interface:



Fields are as follows:

Holiday Name: Any character, up to a combination of 30 characters.

Holiday Type: Holiday Type 1/2/3, namely, a current holiday record belongs to the three holiday types and each holiday type includes up to 32 holidays.

Start/ End Date: The date format: 2010-1-1. Start Date cannot be later than End Date otherwise the system will prompt an error. The year of Start Date cannot be earlier than the current year, and the holiday cannot span years.

Recurring: It refers a holiday whether to require modification in different years. The default is No. For example, the Near Year's Day is on January 1 each year, and can be set as Yes. The Mother's Day is on the second Sunday of each May; this date is not fixed and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2010, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Friday, but the Access Control Time of Holiday Type 1.

(2) After editing, click [OK] button to save, and it will display in holiday list.

- Modify

Click Holiday Name or [Edit] button under Operations to enter the edit interface. After modification, click [OK] to save and quit.

- Delete

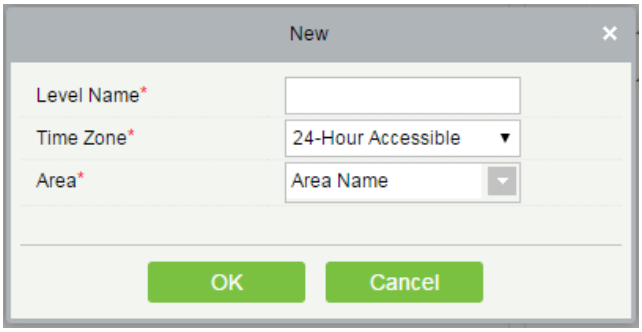
In the access control holiday list, click [Delete] button under Operations. Click [OK] to delete, click [Cancel] to cancel the operation. An Access Control Holiday in use cannot be deleted.

4.2.3 Access Levels

Access levels indicate that one or several selected doors can be opened by verification of a combination of multi person within certain time zone. The combination of multi person set in Personnel Access Level option.

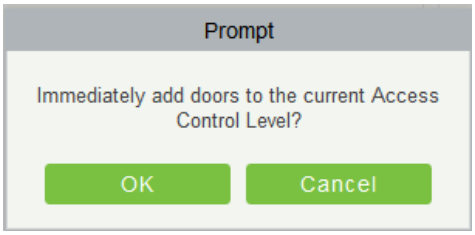
- Add

1. Click [Access Control] > [Access Levels] > [Add] to enter the Add Levels editing interface:



2. Set each parameter: Level Name (unrepeatable), Time Zone.

3. Click [OK], the system prompts "Immediately add doors to the current Access Control Level", click [OK] to add doors, click [Cancel] to return the access levels list. The added access level is displayed in the list.



Note: Different doors of different panels can be selected and added to an access level.

- Set Access By Levels

Add/Delete Personnel for Selected Levels:

(1) Click [Access Control] > [Access Levels] > [Set Access By Levels] to enter the edit interface, Click an Access level in left list, personnel having right of opening door in this access level will be displayed on right list.

(2) In the left list, click [Add Personnel] under Operations to pop-up the Add Personnel box; select personnel (multiple) and click > to move to the right selected list, then click [OK] to save and exit.

(3) Click the level to view the personnel in the right list. Select personnel and click [Delete Personnel] above the right list, then Click [OK] to delete.

- Set Access By Person

Add selected personnel to selected access levels, or delete selected personnel from the access levels.

Add/Delete levels for Selected Personnel:

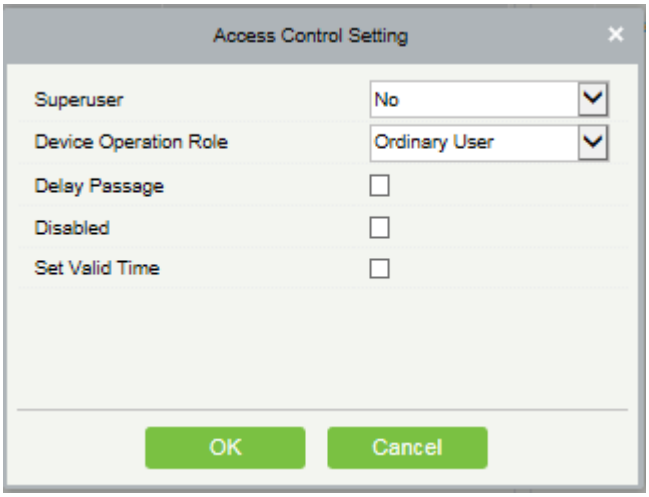
(1) Click [Access Control] > [Access Levels] > [Set Access By Person], click Employee to view the levels in the right list.

(2) Click [Add to Levels] under Related Operations to pop-up the Add to Levels box, select Level (multiple) and click > to move it to the right selected list; click [OK] to save and complete.

(3) Select Level (multiple) in the right list, and click [Delete from levels] above the list, then click [OK] to delete the selected levels.

Setting Access Control for Selected Personnel:

（1）Select a person in the list on the left and click [Access Control Setting].



（2）Set access control parameters and click [OK] to save the setting.

- Set Access By Department

Add selected department to selected access levels, or delete selected department from the access levels. The access of the staff in the department will be changed.

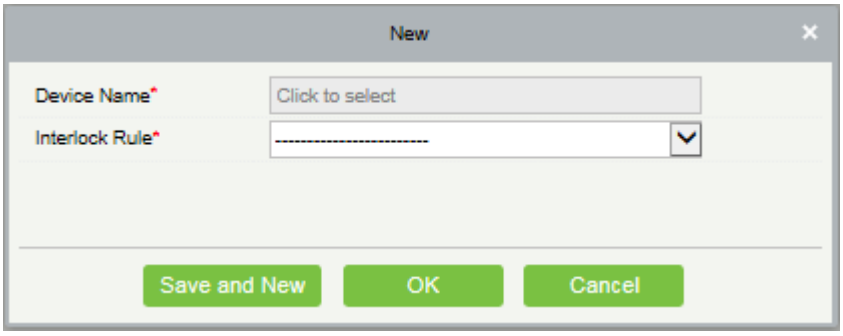
4.2.4 Interlock Settings

Interlock can be set for two or more lock belong to one access controller, when one door is opened, the others will be closed, or you cannot open the door.

Before interlock setting, please ensure that the access controller is connected with door sensor, which has been set as NC or NO state.

- Add Interlock

1. Click [Access Control] > [Interlock] > [New] to enter the edit interface:



2. Select Device Name. When adding, interlocked devices cannot be seen in the dropdown list, after deleting established interlock information, the corresponding device will return to the dropdown list. Interlock setting will vary with the number of doors controlled by selected device:

- A one-door control panel has no interlock settings.
- A two-door control panel: 1-2 two-door interlock settings.
- A four-door control panel: 1-2 two-door interlock, 3-4 two-door interlock, 1-2-3 three-door interlock, 1-2-3-4 four-door interlock.

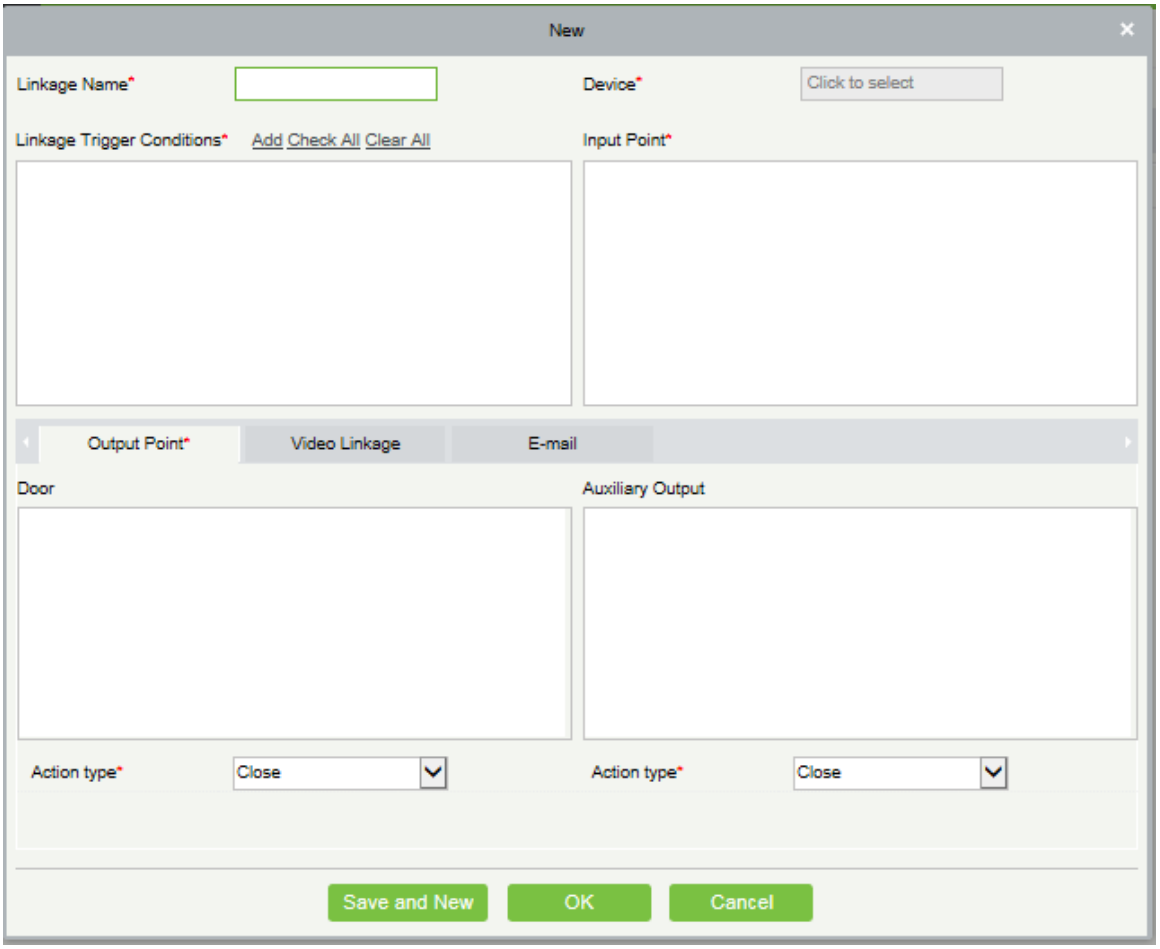
3. Select Interlock Rule, tick an item, click [OK] to complete, the new added interlock settings will be shown in the list.

Note: When editing, the device cannot be modified, but the interlock setting can be modified. If interlock setting is not required for the device any more, the interlock setting record can be deleted. When deleting a device record, its interlock setting record, if exists, will be deleted.

4.2.5 Linkage Setting

Linkage setting means when an event is triggered at an input point of the access control system, a linkage action will occur at the specified output point to control such events as verification, opening, alarm and abnormal of system and list them in the corresponding monitored report for view.

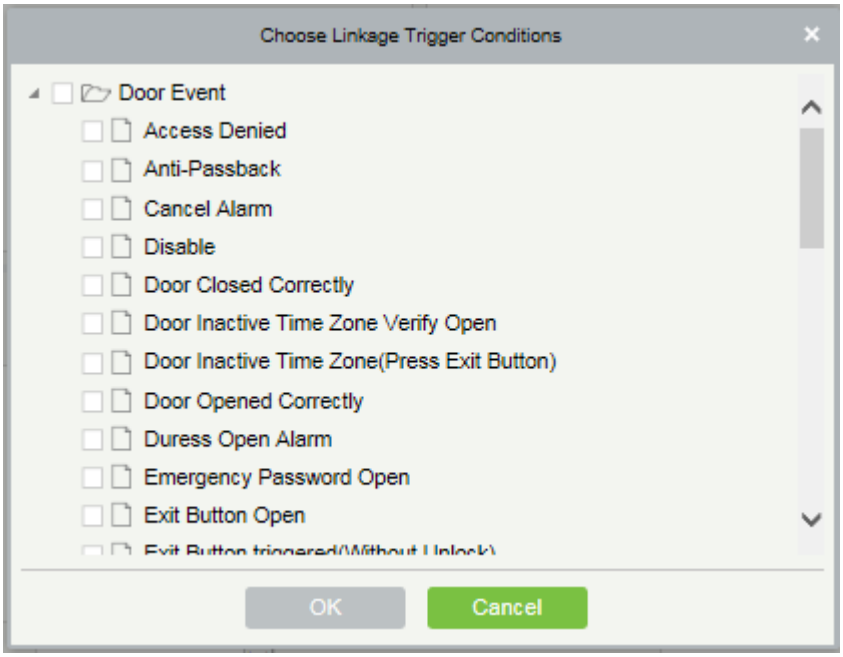
Add Linkage setting:



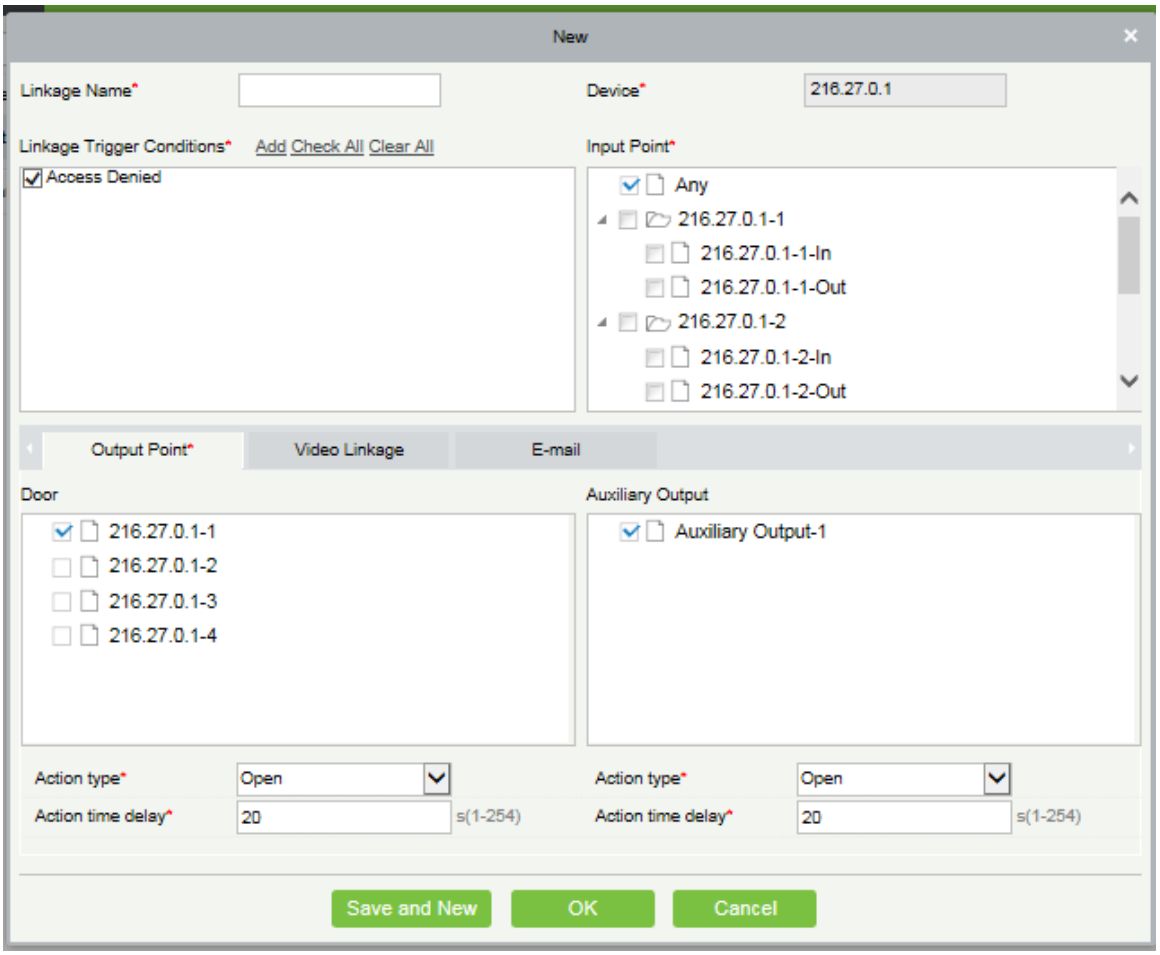
1. Click [Access Control] > [Linkage] > [Add]:

2. Enter linkage name, select linkage device, select linkage trigger conditions, select input point, select output point, set linkage action, video linkage and other parameters.

3. After selecting device, corresponding linkage setting will display (System will first judge whether or not the device is successfully connected and has read extended parameters. If no available extended parameters, system cannot set linkage. Otherwise, it will show linkage setting according to the door quantity, auxiliary input and output quantity of currently selected device):



Note: Linkage trigger conditions contain Door Event and Auxiliary Input Event. And "Fail to connect server", "Recover connection", "Device connection off" will be filtered from Door Event.



4. Select the Input point and output point, Linkage action, Video Linkage and Email Address.

The fields are as follows:

Linkage Name: Set a linkage name.

Linkage Trigger Condition: Linkage Trigger Condition is the event type of selected device. Except Linkage Event Triggered, Enable/Disable Auxiliary Output, and Device Start, all events could be trigger condition.

Input Point: Any, Door 1, Door 2, Door 3, Door 4, Auxiliary Input 1, Auxiliary Input 2, Auxiliary Input 3, Auxiliary Input 4, Auxiliary Input 9, Auxiliary Input 10, Auxiliary Input 11, Auxiliary Input 12 (the specific input point please refers to specific device parameters).

Output Point: Lock 1, Lock 2, Lock 3, Lock 4, Auxiliary Output 1, Auxiliary Output 2, Auxiliary Output 3, Auxiliary Output 4, Auxiliary Output 6, Auxiliary Output 8, Auxiliary Output 9, and Auxiliary Output 10 (the specific output point please refers to specific device parameters).

Linkage Action: Close, Open, Normal Open, Lock, Unlock. The default is close. To open, delay time shall be set, or select Normal Close.

Video Linkage:

- Pop up video: Whether to set the pop-up preview page in real-time monitoring, and set the pop-long.
- Video: Enable or disable background video recording, and set the duration of background video recording.
- Photograph: Enable or disable background snapshot

Delay: Ranges from 1~254s (This item is valid when Action type is Open).

5. After editing, click [OK] to save and quit, the added linkage setting will be shown in the list.

For example: If select Normal Punching Open Door as trigger condition, input point is Door 1, output point is Lock 1, action type is Open, delay is 60s, then when Normal Punching Open Door occurs at Door 1, the linkage action of Open will occur at Lock 1, and door will be open for 60s.

Note: When editing, you cannot modify the device, but can modify linkage setting name and configuration.

When deleting a device, its linkage setting record, if exist, will be deleted.

If the device and trigger condition are the same, and system has linkage setting record where the input point is a specific door or auxiliary input, it will not allow user to add (or edit) a linkage setting record where the input point is Any.

On the contrary, if the device and trigger condition are the same, and the system has linkage setting record where the input point is 'Any', it will not permit user to add (or edit) a linkage setting record where the input point is a specific door or auxiliary input.

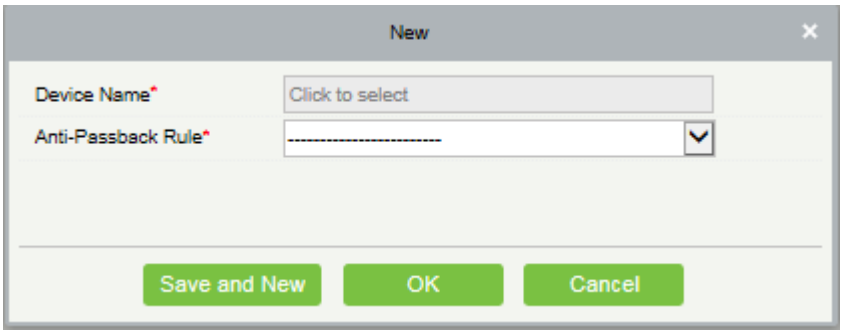
In addition, same linkage setting at input point and output point is not allowed. The same device permits consecutive logical linkage settings. The system allows to set several trigger conditions for a linkage setting one time.

4.2.6 Anti-Passback Settings

Currently anti-passback settings support in and out anti-passback. In some special occasions, it is required that the card holder who entered from a door by punching must exit from a door by punching, with the entry and exit records strictly consistent. The user can use this function just by enabling it in the settings. This function is normally used in prisons, the army, national defense, scientific research, bank vaults, etc.

Add Anti-Passback Settings:

1. Click [Access Control] > [Anti-Passback] > [Add] to show the edit interface:



2. Select device, when adding, devices with anti-passback settings cannot be seen in the dropdown list. When deleting established anti-passback information, the corresponding device will appear in the dropdown list again. The settings vary with the number of doors controlled by the device.

- Anti-passback settings of a one-door control panel: Anti-passback between door readers.
- Anti-passback settings of a two-door control panel: Anti-passback between readers of door 1, anti-passback between readers of door 2, anti-passback between door 1 and door 2.
- Anti-passback settings of a four-door control panel: Anti-passback of door 1 and door 2, anti-passback of door 3 and door 4, anti-passback of door 1/2 and door 3/4, anti-passback of door 1 and door 2/3, anti-passback of door 1and door 2/3/4, Anti-passback between readers of door 1/2/ 3/ 4.

Note: Door reader mentioned above includes Wiegand reader that connected with access controller and inBIO reader. The single and two door controller with Wiegand reader include out and in reader. There is only in reader for four door control panel. The reader number of 1, 2 (that is RS485 address or device number, the same below) is for door 1, the reader number of 3, 4 is for door 2, etc. No need to consider if it is Wiegand reader or inBIO reader in setting of anti-passback between doors or between readers, just make sure in or out reader and set according to the actual requirement. For the reader number, odd number is for in reader, and even number is for out reader.

3. Select Anti-Passback Rule, and tick one item, Click [OK] to complete, and the added anti-passback settings will be shown in the list.

Note: When editing, you cannot modify the device, but can modify anti-passback settings. If anti-passback setting is not required for the device any more, the anti-passback setting record can be deleted. When deleting a device, its anti-passback setting record, if exists, will be deleted.

4.2.7 First-Person Normally Open

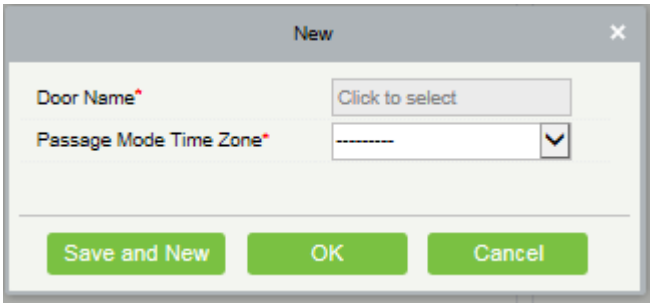
First-Person Normally Open: During a specified interval, after the first verification by the person having First-Person Normally Open level, the door will be Normal Open, and will automatically restore closing after the valid interval has expired.

User can set First-Person Normally Open for a specific door (the settings include door, door opening time zone and personnel with First-Person Normally Open level). A door can set First-Person Normally Open for multiple time zones. The interface of each door will show the number of existing First-Person Normally Open.

When adding or editing First-Person Normally Open setting, only select door and time zone. After successful adding, then add personnel that can open the door. You can browse and delete the personnel on the right of the interface

Operation steps are as follows:

1. Click [Access Control] > [First-Person Normally Open] > [New], select Door Name and Passage Mode Time, and click [OK] to save the settings.

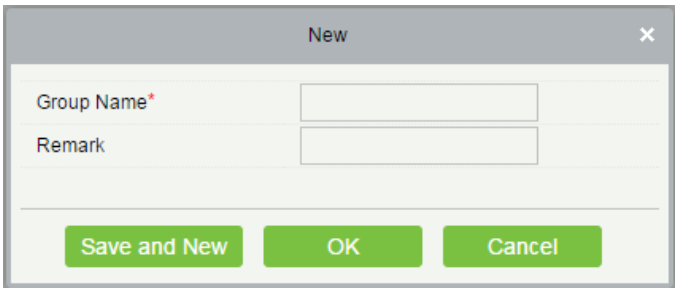


2. Click [Add Personnel] under Related operation to add personnel having First-Person Normally Open level (this personnel must have access control level), then click [OK] to save.

4.2.8 Multi-Person Group

The door will open only after the consecutive verification of multiple people. Any person verifying outside of this combination (even if the person belongs to other valid combination) will interrupt the procedure and you need to wait 10 seconds to restart verification. It will not open by verification by only one of the combination.

(1) Click [Access Control] > [Multi-Person Group] > [New] to show the following edit interface:



Group name: Any combination of up to 30 characters that cannot be identical to an existing group name.

After editing, click [OK] to save and return, the added Multi-Person Personnel Group will appear in the list.

(2) Click [Add personnel] under Related Operations to add personnel to the group.

(3) After selecting and adding personnel, click [OK] to save and return.

Note: A person can only belong to one group, and cannot be grouped repeatedly.

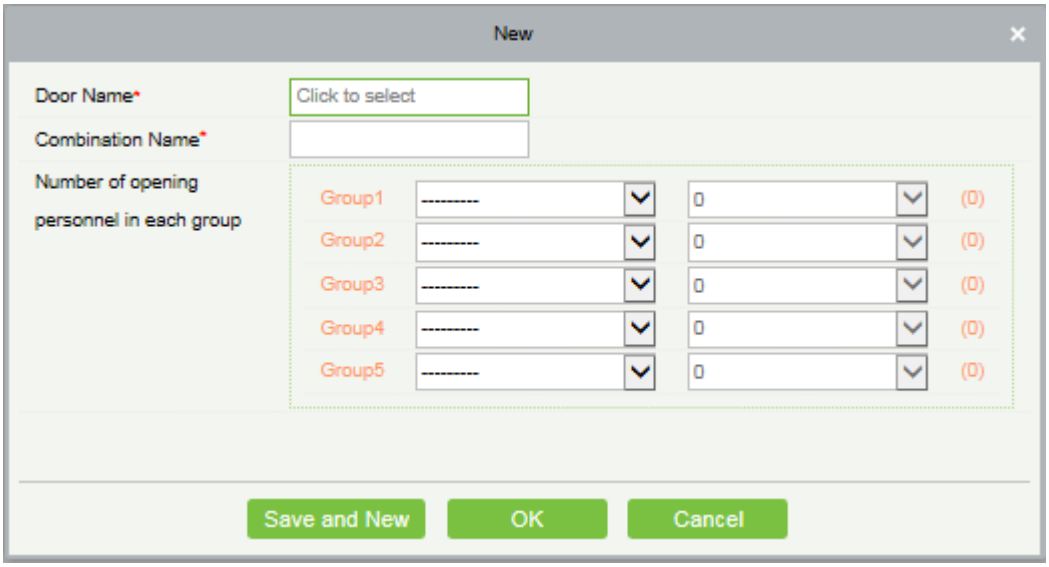
4.2.9 Multi-Person Opening Door

Set levels for personnel in Multi-Person Personnel Group.

It is a combination of the personnel in one or more Multi-Person Personnel Groups. When setting the number of people in each group, you can configure one group (such as combined door opening by two people in one group) or multiple groups (such as combined door opening by four people, including 2 people in group 1 and 2 people in group 2), and at least one group shall be entered a number of door opening people not being 0, and the total number shall not be greater than 5. In addition, if the number of people entered is greater than that in the current group, Multi-Person Opening Door will be disabled.

Multi-Person Opening Door Settings:

(1) Click [Access Control] > [Multi-Person Opening Door] > [New]:



(2) The number of Multi-Person Opening Door people for combined door opening is up to 5. That in the brackets is the current actual number of people in a group. Select the number of people for combined door opening in a group, and click [OK] to complete.

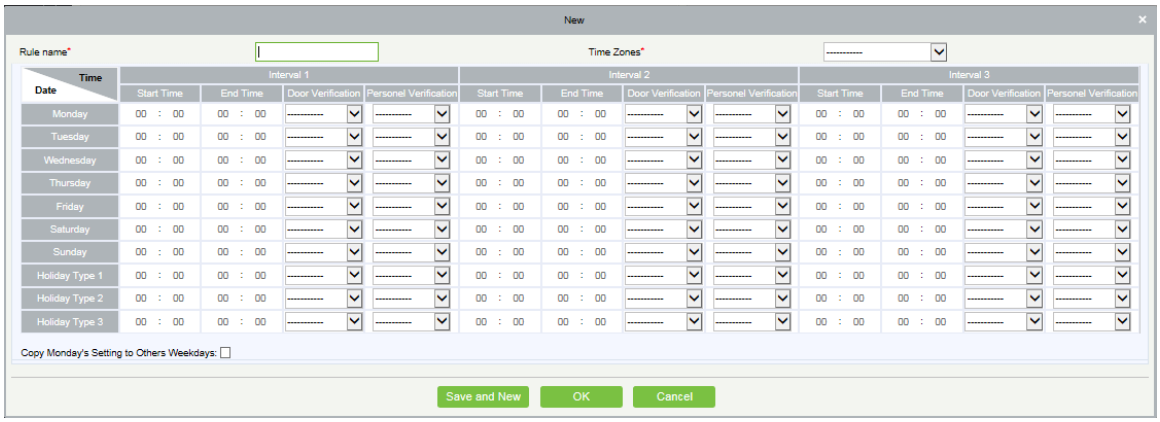
Note: The default Credit Card Interval is 10 seconds, it means that the interval of two personnel's verification must not exceed 10 seconds. You can modify the interval while the device supports.

4.2.10 Verification Mode

Verification Mode: You can set verification modes for doors and personnel separately in a specified time segment.

- Add

1. Click [Access Control] > [Verification Mode] > [New] to go to the page for adding a verification mode rule.



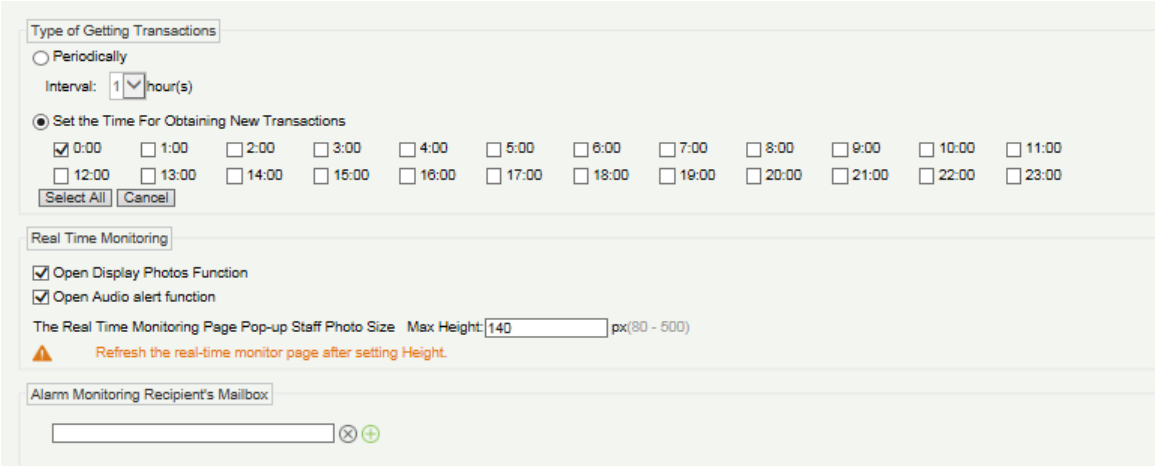
2. Set the following parameters: Select a rule name (not repeatable), the time segment, and verification mode for a door or person in each time segment.
3. Click [OK] to finish the setting.
4. On the list page, you can add or delete doors in the verification mode rule.

Note: If a rule includes the verification mode for personnel, you cannot select doors with the RS485 readers when adding doors. You can modify only the configuration on the reader setting page before adding doors.

Verification Mode Group: Set appropriate personnel for configured verification mode rule.

4.2.11 Parameters

Click [Access Control] > [Parameters] to enter the parameter setting interface:



Type of Getting Transactions

- Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

- Set the Time For Obtaining New Transactions

The selected Time is up, the system will attempt to download new transactions automatically.

The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up, set the size of the pop-up photos, the range is 80-500px.

Alarm Monitoring Recipient Mailbox: The system will send email to alarm monitoring recipient's mailbox when there is an alarming event occurs.

4.3 Advanced Functions

Advanced Access control is optional function. If needed, please contact business representative or pre-sales engineer, you can use these functions after obtaining license and activating.

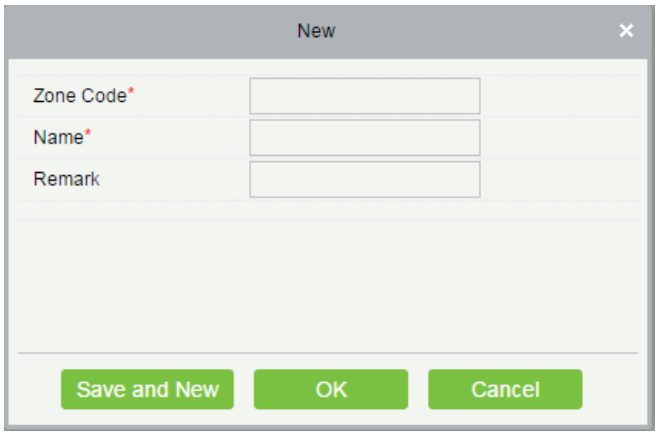
Note: Except Global Linkage, to use other advanced functions you need to enable Background Verification. For detail, please see Device Operation.

4.3.1 Zone

It mainly used partition Zones in advanced access control. When using such advanced functions as Global Zone APB, you must define Access Zones.

- Add

1. Click [Access Control] > [Advanced Functions] > [Zone] > [New] to enter the Add Zone interface:



2. Set Zone Code, Name, Parent Zone and Remark as required.

3. Click [OK] to save and quit. The added Zone will appear in the list.

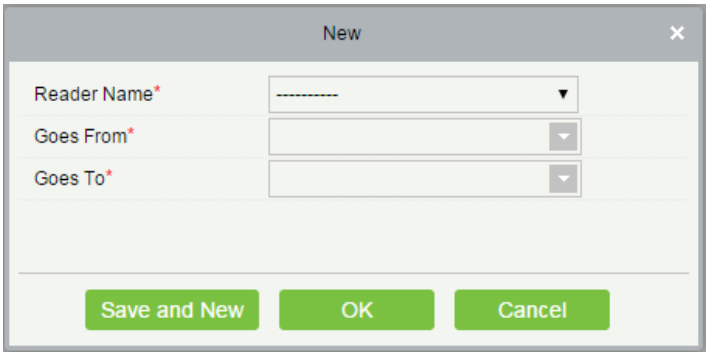
What rules inside:

4.3.2 Reader Define

Reader Define indicates that Reader control from one access zone to another one, it is based on access zone. If advanced functions are needed, you shall set the Reader Define.

- Add

1. Click [Access Control] > [Advanced Functions] > [Reader Define] > [New] to enter the add interface:

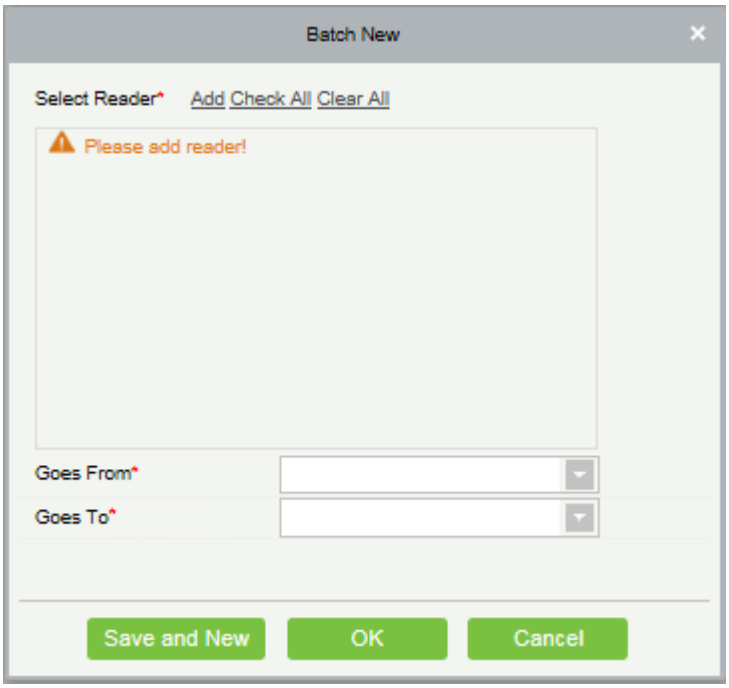


2. Set Reader Name, Goes from and Goes to as required.

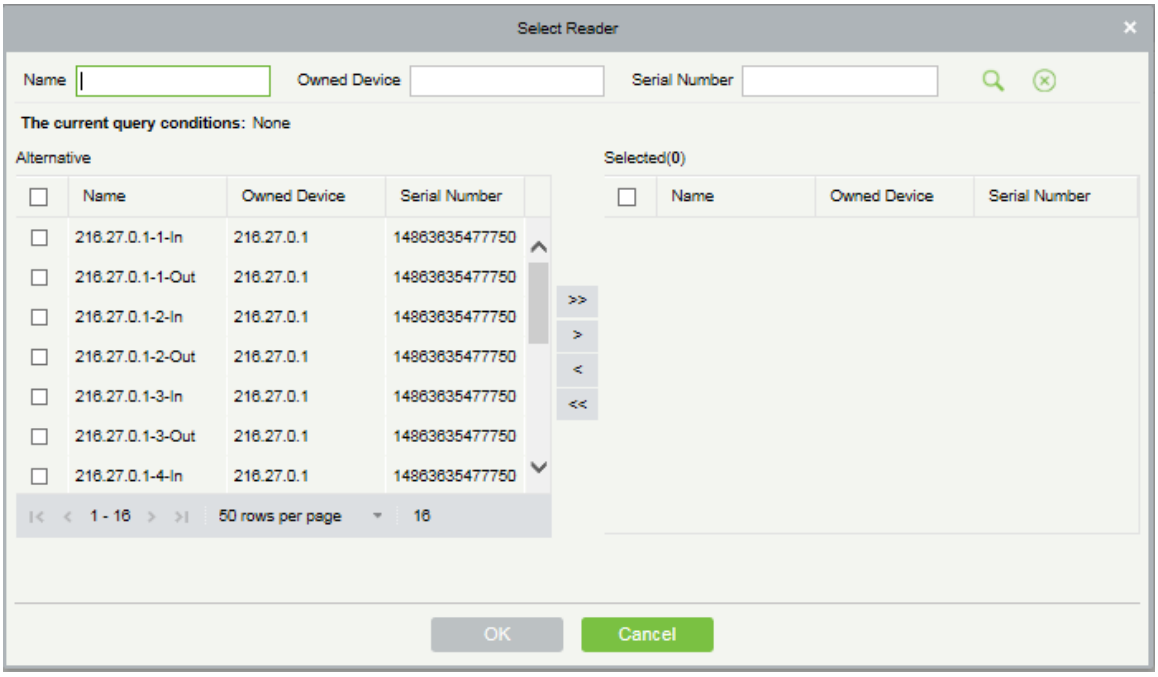
3. Click [OK] to save and quit. The added Reader Define will appear in the list.

- Batch New

1. Click [Access Control] > [Advanced Functions] > [Reader Define] > [Batch New] to enter the batch add interface:



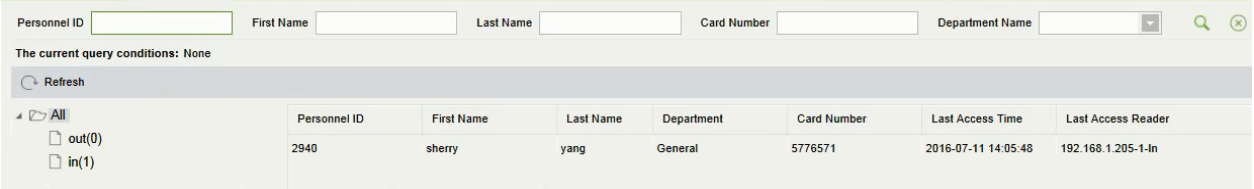
2. Click [Add], select Reader and Click [OK]



3. Set Goes from and Goes to as required.

4.3.3 Who is Inside

After enter the zone, you can view all personnel status in the zone by zone tree.



- **Delete Personnel**

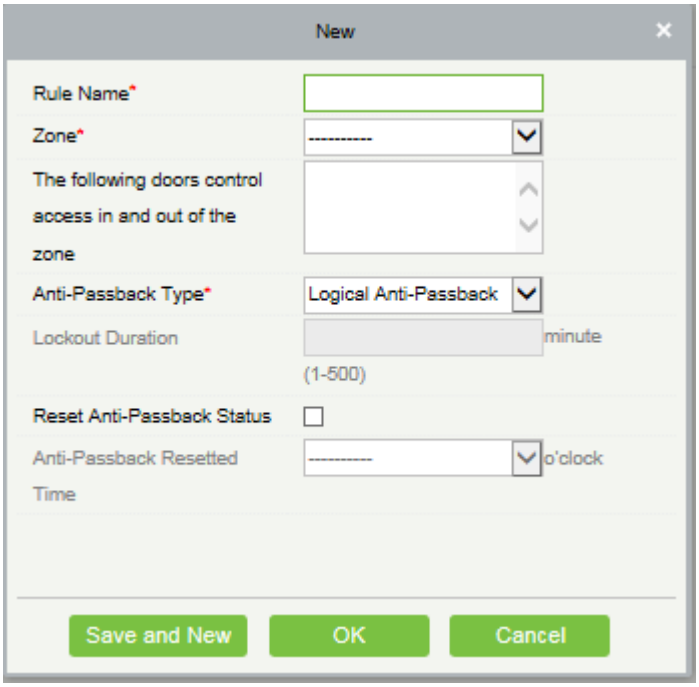
Deleting personnel in the selected area will clear the global anti-passback status of the personnel.

4.3.4 Global Anti-passback

Global Zone APB can set Anti-Passback across devices; you can use this function after setting Global Anti-passback. You must set Access Zone and Reader Define before using, and also the device that has set Anti-Passback shall issue background verification parameters.

- Add

1. Click [Access Control] > [Advanced Functions] > [Global Anti-passback] > [New] to enter the add interface:



2. Set Rule Name (Unrepeatable), Zone, Anti-passback Type, Lockout Duration, Reset Anti-passback Status and When to Reset the Anti-passback as required.

Zone: Select an option from the dropdown list, Corresponding doors will display in the text box of " The following doors control access in and out of the zone". At the same time, the doors obey the rule of one door cannot set as the boundary of two independent Anti-Passback.

Anti-passback Type: Logical Anti-passback, Timed Anti-passback or Timed Logic Anti-passback.

- Logical Anti-passback: With the entry and exit records strictly consistent in Anti-passback zone, or door will not open.
- Timed Anti-passback: In Specified time period, user can enter Anti-passback zone for only once. Time period expired, user state will be cleared, and allow user to enter this zone again.
- Timed Logic Anti-passback: In Specified time period, Users who enter Anti-passback zone must obey the rule of Logical Anti-passback. If exceeds timed period, system will time again.

Lockout Duration: Only select Timed Anti-passback and Timed Logic Anti-passback in Anti-passback Type, Lockout Duration can be set.

Reset Anti-passback Status: Tick it to clear Anti-passback status of personnel in the system, and recover initial state. Only tick this option. When to Reset the Anti-passback can be select. Time of reset the Anti-passback expired, system will clear all the Anti-passback status of personnel in zone.

When to Reset the Anti-passback: Select time to reset Anti-passback.

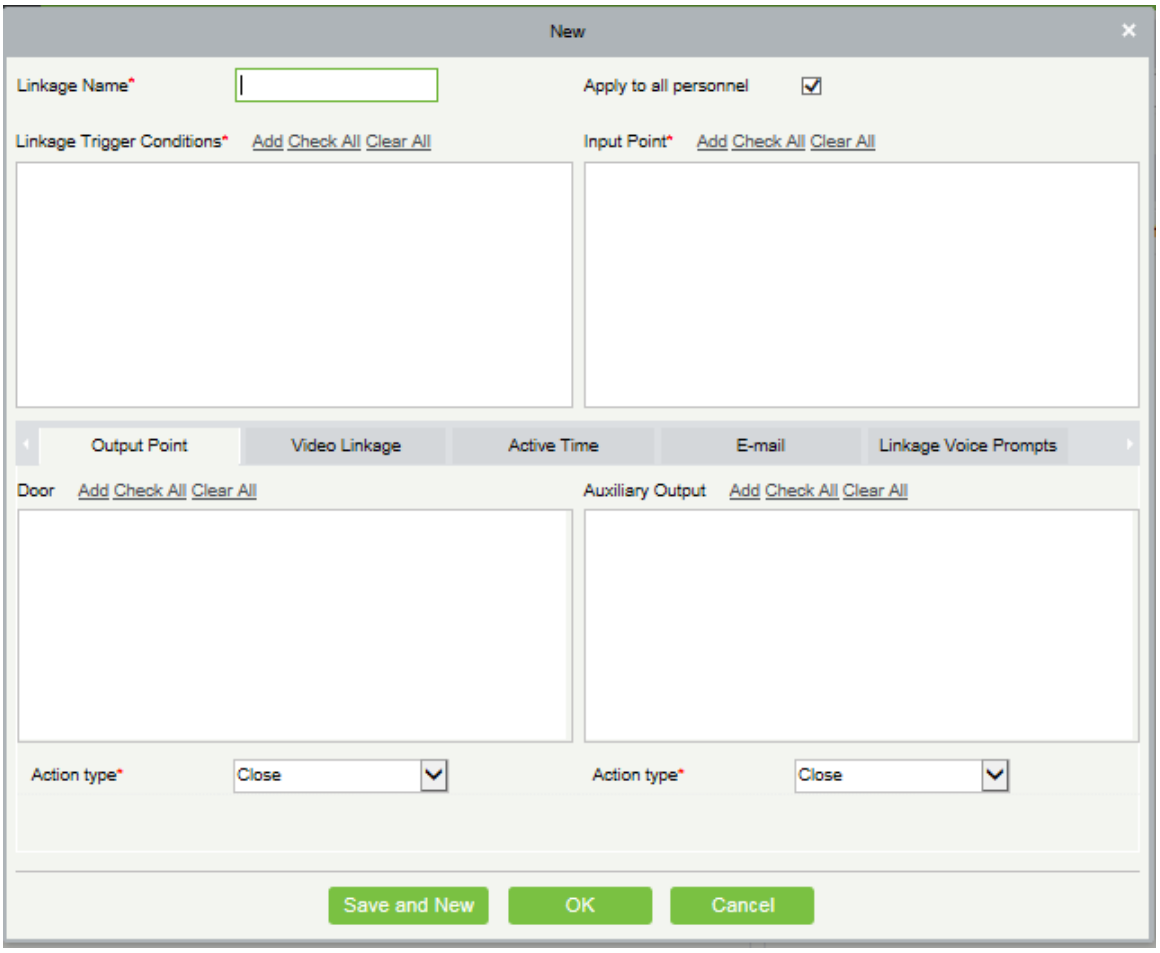
3. Click [OK] to save and quit. The added Global Zone APB will display in the list.

4.3.5 Global Linkage

The global linkage function allows you to configure data across devices. Only push devices support this function.

- Add

1. Click [Access Control] > [Access Rule]> [Advanced Functions] > [Global Linkage] > [New]:



Apply to all personnel: If this option is selected, this linkage setting is effective for all personnel.
Active Time: Set the active time of the linkage setting.

2. Choose Global Linkage trigger conditions, the input point (System will filter devices according to the choice in first step) and the output point, Set up linkage action. For more details about these parameters, please refer to Linkage Setting.

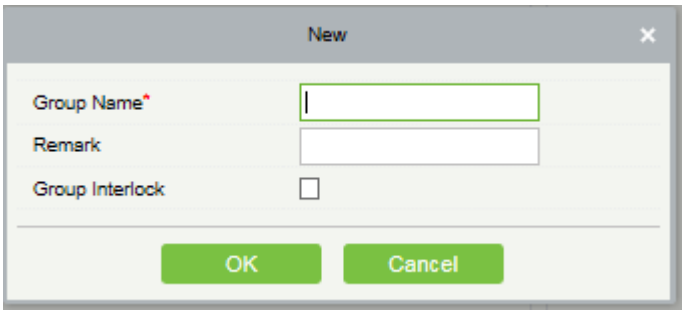
Note: You can select multiple Door Events, but "Fail to connect server", "Recover connection" and "Device connection off" will be filtered automatically from Door Event.

3. Click [OK] to save and quit. The added Global Linkage will display in the list.

4.3.6 Global Interlock Group

The global interlock group groups the doors in the global interlock, but to use the global interlock function, the device must be enabled with background authentication.

1. Click [Access Control] > [Global Interlock Group]> [New]:



Group Name:

(1) Any combination of up to 30 characters that cannot be identical to an existing group name.

(2) After editing, click [OK] to save. After confirming that add the door immediately, the information of added door will appear in the list.

(3) Click [Add Door] under Related Operations to add door to the group.

(4) After selecting and adding personnel, click [OK] to save and return.

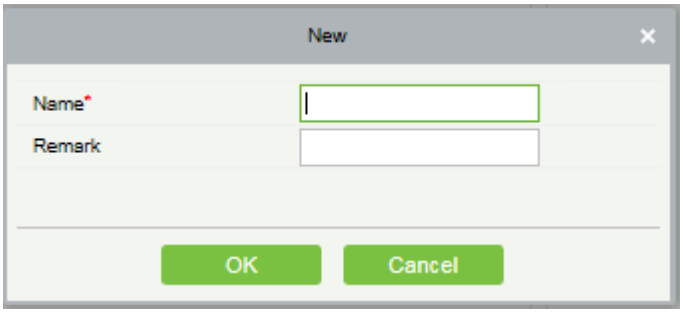
Group Interlock: If the option is selected, set global interlock rule for the interlocking group.

4.3.7 Global Interlock

The global interlock function allows you to configure data across devices. Only push devices support this function.

Multi-Person Opening Door Setting:

1. Click [Access Control] > [Global Interlock]> [New]:



Name:

(1) Any combination of up to 30 characters that cannot be identical to an existing name.

(2) After editing, click [OK] to save. After confirming that add the group immediately, the information of add group will appear in the list.

(3) Click [Add Group] under Related Operations to add door to the group.

(4) After selecting and adding group, click [OK] to save and return.

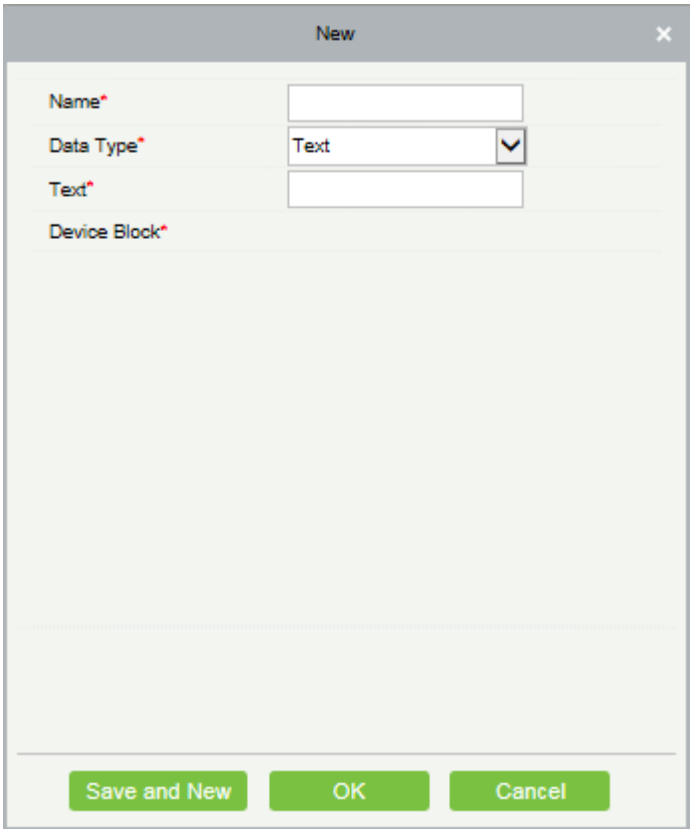
Group Interlock: If the option is selected, set global interlock rule for the interlocking group.

Notes:

1. In the same interlock, all the doors in the group cannot be duplicated.
2. When the interlock group exists in the interlock function, it cannot be deleted directly.

4.3.8 LED Data

- Add



Name: LED data name.

Data Type:

Text: Send self-defined texts to blocks.

Zone data: Total number of personnel in the zone to be sent and statistical number of personnel in the departments in the zone.

Notes:

1. The access control zone is that in the advanced access control.
2. If the content to be sent is department, please select the department whose statistics are to be collected.

Changed data: Real-time information about personnel going in and out. The content to be sent can be selected.

4.4 Access Reports

Includes “All transactions”, “Events from Today”, “All Exception Events” and so on. You can export after query.

You can generate statistics of relevant device data from reports, including card verification information, door operation information, and normal punching information, etc.

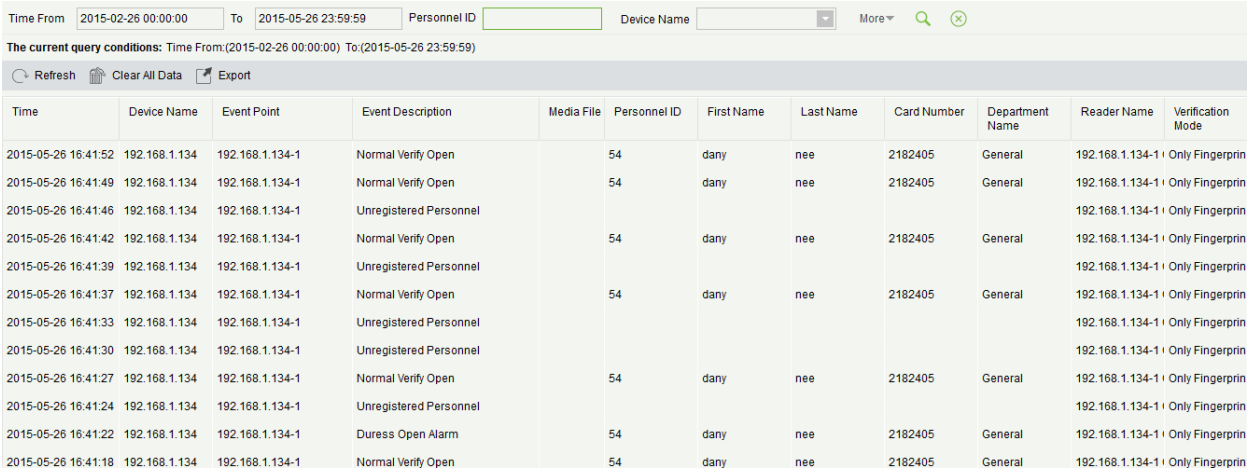
About the Normal and abnormal event please refer to Real-Time Monitoring for details.

Verify mode: Only Card, Only Fingerprint, Only Password, Card plus Password, Card plus Fingerprint, Card or Fingerprint and etc.

Note: Only event records generated when the user uses emergency password to open doors will include only password verification mode.

4.4.1 All Transactions

Because the data size of access control event records is large, you can view access control events as specified condition when querying. By default, the system display latest three months transactions. Click [Reports] > [All Transactions] to view all transactions:



Time	Device Name	Event Point	Event Description	Media File	Personnel ID	First Name	Last Name	Card Number	Department Name	Reader Name	Verification Mode
2015-05-26 16:41:52	192.168.1.134	192.168.1.134-1	Normal Verify Open		54	dany	nee	2182405	General	192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:49	192.168.1.134	192.168.1.134-1	Normal Verify Open		54	dany	nee	2182405	General	192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:46	192.168.1.134	192.168.1.134-1	Unregistered Personnel							192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:42	192.168.1.134	192.168.1.134-1	Normal Verify Open		54	dany	nee	2182405	General	192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:39	192.168.1.134	192.168.1.134-1	Unregistered Personnel							192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:37	192.168.1.134	192.168.1.134-1	Normal Verify Open		54	dany	nee	2182405	General	192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:33	192.168.1.134	192.168.1.134-1	Unregistered Personnel							192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:30	192.168.1.134	192.168.1.134-1	Unregistered Personnel							192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:27	192.168.1.134	192.168.1.134-1	Normal Verify Open		54	dany	nee	2182405	General	192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:24	192.168.1.134	192.168.1.134-1	Unregistered Personnel							192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:22	192.168.1.134	192.168.1.134-1	Duress Open Alarm		54	dany	nee	2182405	General	192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:18	192.168.1.134	192.168.1.134-1	Normal Verify Open		54	dany	nee	2182405	General	192.168.1.134-1	Only Fingerprin

Media File: You can view or download the photos and videos created in the video system.

Clear All Data: Click [Clear All Data] to pop up prompt, and click [OK] to clear all transactions.

4.4.2 Events from Today

Check out the system record today.

Click [Access] > [Reports] > [Events from Today] to view today’s records.

Personnel ID Device Name More

The current query conditions: None

Refresh Clear All Data Export

Time	Card Number	Personnel ID	First Name	Last Name	Department Name	Device Name	Event Point	Event Description	Media File	Reader Name	Verification Mode
2015-05-26 16:41:56	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:54	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:52	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:49	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:42	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:37	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:27	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:22	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Duress Open Alarm		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:18	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:14	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:03	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-2	Normal Verify Open		192.168.1.134-2-	Only Card

4.4.3 Last Known Position

Check out the final position of personnel who has access privileges to access. It is convenient to locate a personnel.

Click [Access] > [Reports] > [Last Know Position] to check out.

Time From To Personnel ID Device Name More

The current query conditions: None

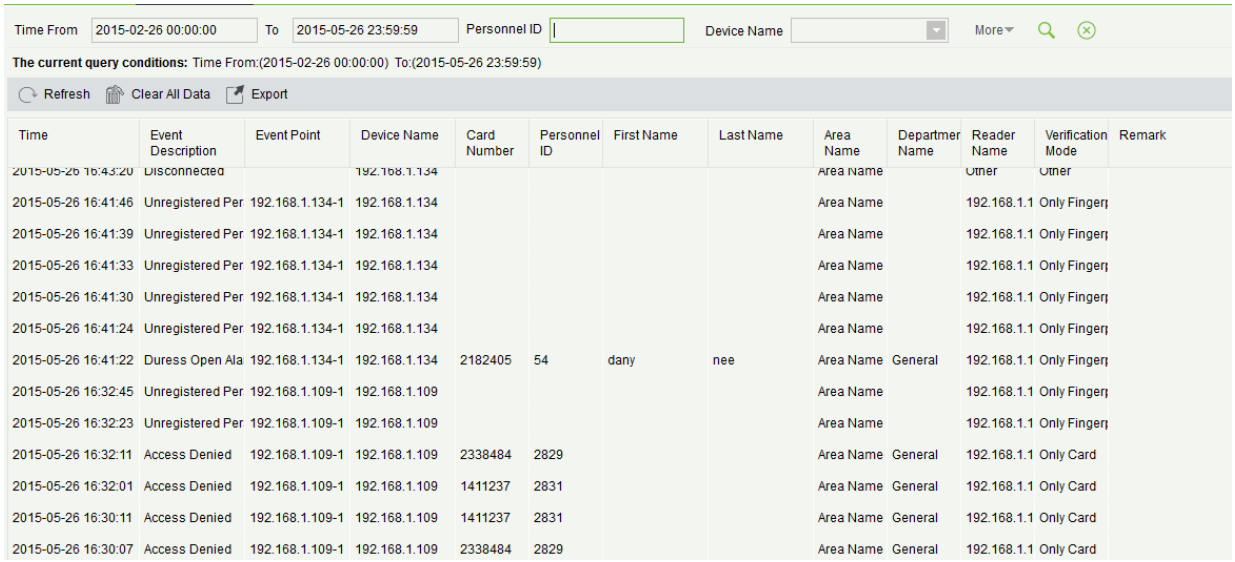
Refresh Clear All Data Export

Personnel ID	First Name	Last Name	Card Number	Time	Department Name	Device Name	Event Point	Event Description	Reader Name	Verification Mode	Area Name
22201	BF1	BL1	3401273	2015-05-22 20:36:02	General	192.168.1.109	192.168.1.109-1	Unregistered Personnel	192.168.1.109-1-	Only Card	Area Nam
56	anne	lee	2182405	2015-05-22 18:07:14	General	192.168.1.134	192.168.1.134-1	Global Anti-passback(logical)	192.168.1.134-1	Only Card	Area Nam
47	liu	xiaomei	5764784	2015-05-22 17:57:37	General	192.168.1.47	192.168.1.47-1	Unregistered Personnel	192.168.1.47-1-In	Only Card	Area Nam
800000002	F2	L2	3419842	2015-05-22 17:08:38	Visitor	192.168.1.109	192.168.1.109-1	Normal Verify Open	192.168.1.109-1-	Only Card	Area Nam
1011	123	1	2826316	2015-05-22 16:26:23	General	192.168.1.134	192.168.1.134-1	Normal Verify Open	192.168.1.134-1	Only Card	Area Nam
800000001	F1	B1	3419842	2015-05-22 16:15:59	Visitor	192.168.1.109	192.168.1.109-1	Normal Verify Open	192.168.1.109-1-	Only Card	Area Nam
7698711			7698711	2015-05-22 14:38:32		1.46.0.40	1.46.0.40-1	Emergency Password Open	1.46.0.40-1-In	Only Card	Area Nam
7139145			7139145	2015-05-22 14:38:32		1.46.0.9	1.46.0.9-1	Remote Closing	1.46.0.9-1-In	Only Card	Area Nam
6723011			6723011	2015-05-22 14:38:32		1.46.0.11	1.46.0.11-1	Verify During Passage Mode Time Z	1.46.0.11-1-In	Only Card	Area Nam
[illegible]			[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Locate the location of personnel: Personnel with electronic map authority, click on the corresponding [Personnel ID], you can locate the specific location of the personnel in the electronic map by the way of flashing the door.

4.4.4 All Exception Events

Click [Reports] > [All Exception Events] to view exception events in specified condition. The options are same as those of [All Transactions].



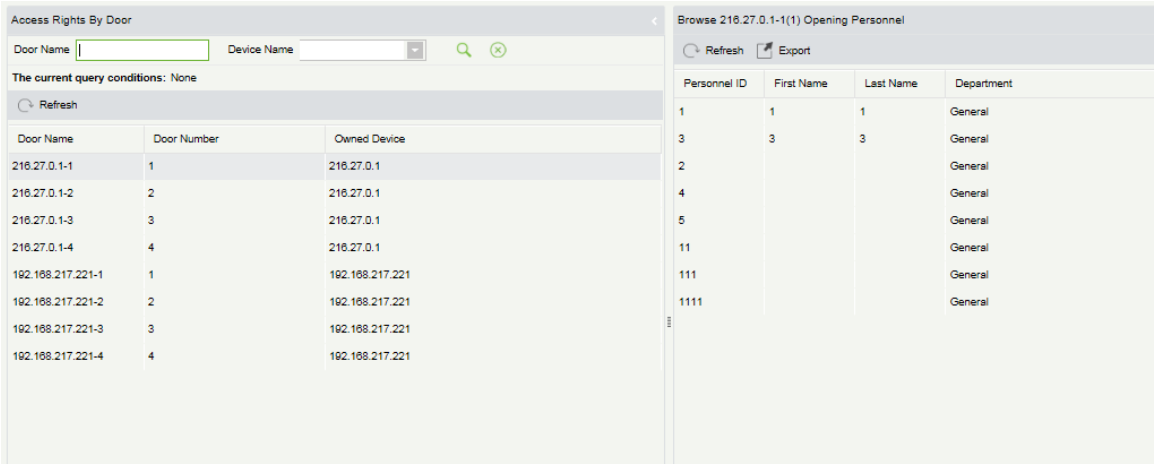
Time	Event Description	Event Point	Device Name	Card Number	Personnel ID	First Name	Last Name	Area Name	Departmer Name	Reader Name	Verification Mode	Remark
2015-05-26 16:43:20	Disconnected		192.168.1.134					Area Name		Other	Other	
2015-05-26 16:41:46	Unregistered Per	192.168.1.134-1	192.168.1.134					Area Name		192.168.1.1	Only Finger	
2015-05-26 16:41:39	Unregistered Per	192.168.1.134-1	192.168.1.134					Area Name		192.168.1.1	Only Finger	
2015-05-26 16:41:33	Unregistered Per	192.168.1.134-1	192.168.1.134					Area Name		192.168.1.1	Only Finger	
2015-05-26 16:41:30	Unregistered Per	192.168.1.134-1	192.168.1.134					Area Name		192.168.1.1	Only Finger	
2015-05-26 16:41:24	Unregistered Per	192.168.1.134-1	192.168.1.134					Area Name		192.168.1.1	Only Finger	
2015-05-26 16:41:22	Duress Open Ala	192.168.1.134-1	192.168.1.134	2182405	54	dany	nee	Area Name	General	192.168.1.1	Only Finger	
2015-05-26 16:32:45	Unregistered Per	192.168.1.109-1	192.168.1.109					Area Name		192.168.1.1	Only Finger	
2015-05-26 16:32:23	Unregistered Per	192.168.1.109-1	192.168.1.109					Area Name		192.168.1.1	Only Finger	
2015-05-26 16:32:11	Access Denied	192.168.1.109-1	192.168.1.109	2338484	2829			Area Name	General	192.168.1.1	Only Card	
2015-05-26 16:32:01	Access Denied	192.168.1.109-1	192.168.1.109	1411237	2831			Area Name	General	192.168.1.1	Only Card	
2015-05-26 16:30:11	Access Denied	192.168.1.109-1	192.168.1.109	1411237	2831			Area Name	General	192.168.1.1	Only Card	
2015-05-26 16:30:07	Access Denied	192.168.1.109-1	192.168.1.109	2338484	2829			Area Name	General	192.168.1.1	Only Card	

Clear All Data: Click [Clear All Data] to pop up prompt, and then click [OK] to clear all exception events.

4.4.5 Access Rights

- By Door

View related access levels by door. Click [Reports] > [Access Rights By Door], the data list in the left side show all doors in the system, select a door, the personnel having access levels to the door will display on the right data list.



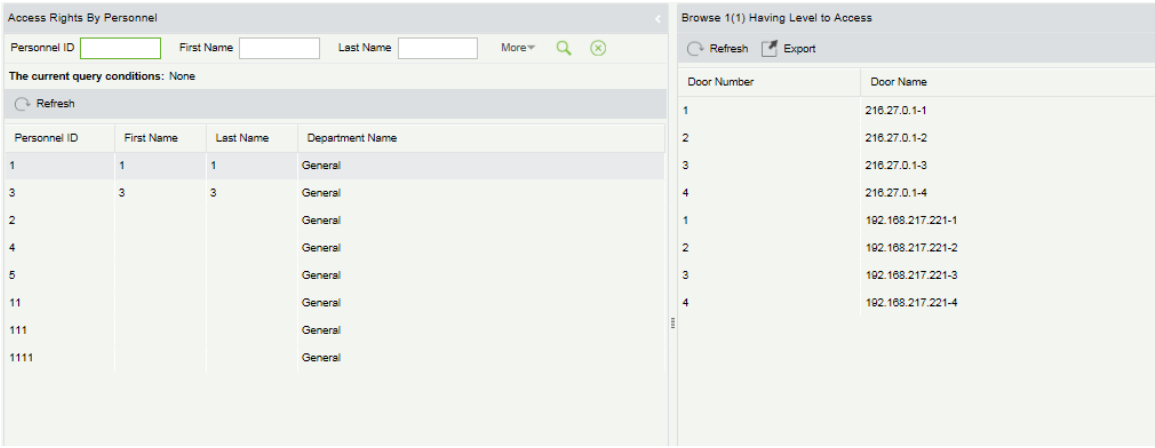
Door Name	Door Number	Owned Device
216.27.0.1-1	1	216.27.0.1
216.27.0.1-2	2	216.27.0.1
216.27.0.1-3	3	216.27.0.1
216.27.0.1-4	4	216.27.0.1
192.168.217.221-1	1	192.168.217.221
192.168.217.221-2	2	192.168.217.221
192.168.217.221-3	3	192.168.217.221
192.168.217.221-4	4	192.168.217.221

Personnel ID	First Name	Last Name	Department
1	1	1	General
3	3	3	General
2			General
4			General
5			General
11			General
111			General
1111			General

- By Personnel

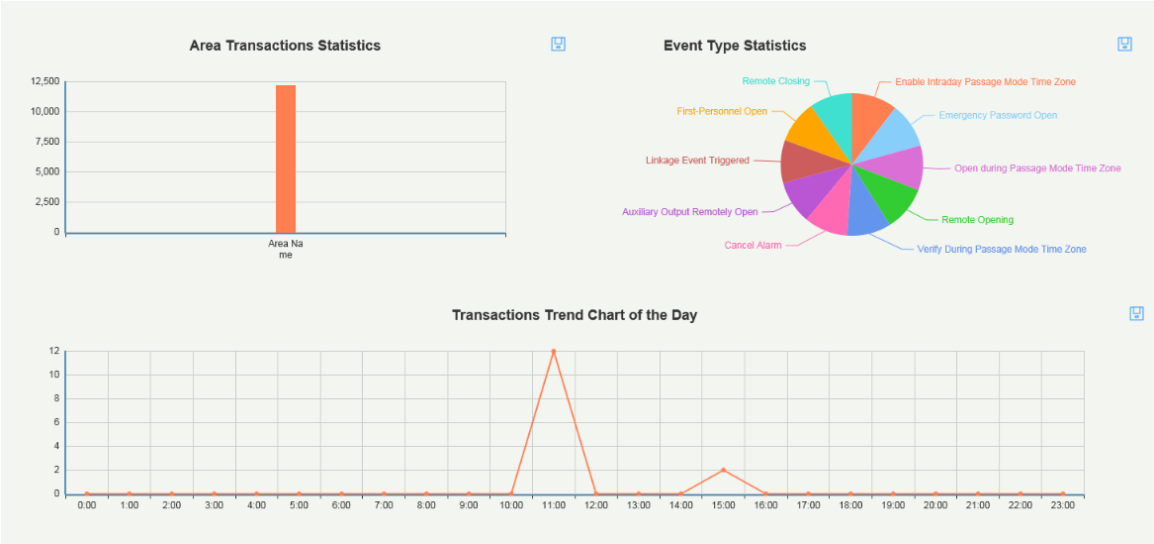
View related access levels by door or personnel.

Click [Reports] > [Access Rights By Personnel], the data list in the left side show all doors in the system, select a personnel, the personnel having access levels to the door will display on the right data list.



4.4.6 Charts

You can view the charts of statistics about access control events.



4.5 Video Integrated

For details about this function, please refer to its user manual.

5 Elevator

The Elevator Control System is mainly used to set device parameters (such as the swiping interval for taking elevators and elevator key drive duration), manage personnel's rights to floors and elevator control time, and supervise elevator control events. You can set registered users' rights to floors. Only authorized users can reach certain floors within a period of time after being authenticated.

5.1 Elevator Device

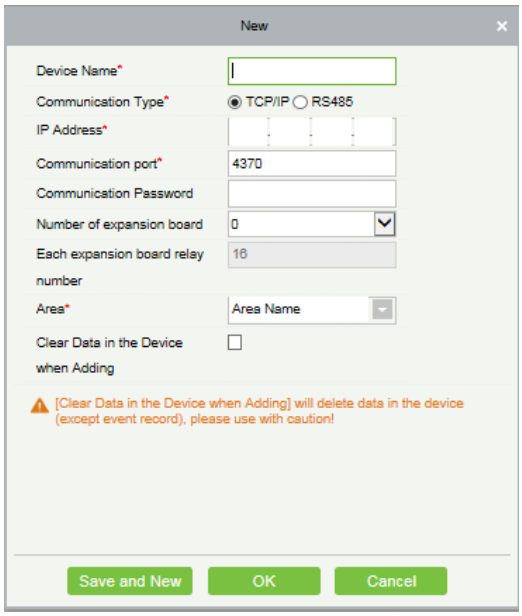
5.1.1 Add an Elevator Device

There are two ways to add Elevator Devices.

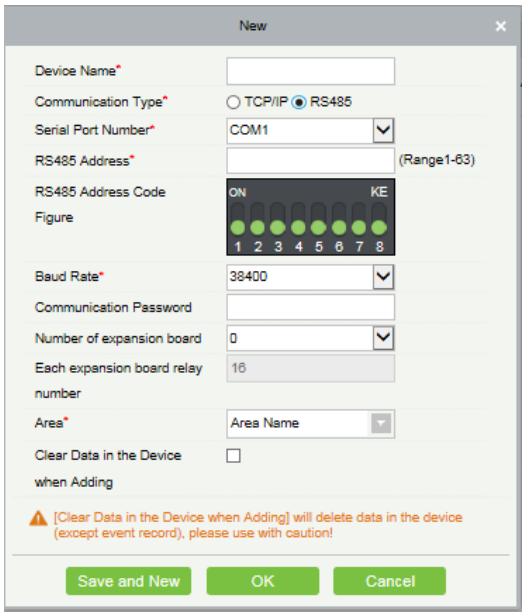
- Add Device by manually

(1) Click [Elevator Device] > [Device] > [New] on the Action Menu, the following interface will be shown:

TCP/ IP communication mode



RS485 communication mode



IP Address: Enter the IP Address of the access controller.

Communication port: The default is 4370.

Serial Port No.: COM1~COM254.

RS485 Address: The machine number, range 1-255. When Serial Port No. is same, it is not allowed to set repeated RS485 addresses.

Baud Rate: Same as the baud rate of the device. The default is 38400.

RS485 Address Code Figure: display the code figure of RS485 address.

Common options:

Device Name: Any character, up to a combination of 20 characters.

Communication Password: The max length is 6 with numbers or letters. The initialized device's communication password is blank.

Note: You do not need to input this field if it is a new factory device or just after the initialization.

Number of expansion board: The expansion board number of elevator device controlling.

Each expansion board relay number: Each expansion board has 16 relays.

Access Control Panel Type: One-door panel, two-door panel, four-door panel, Access Device.

Area: Specify areas of devices. After Area Setting, devices (doors) can be filtered by area upon Real-Time Monitoring.

Clear Data in the Device when Adding: Tick this option, after adding device, the system will clear all data in the device (except the event logs). If you add the device just for demonstration or testing, there is no need to tick it.

(2) After editing, click [OK], and the system will try to connect the current device.

If successful connect, it will read the corresponding extended parameters of the device. At this time, if the selected access controller type does not meet the corresponding parameters of the actual device, the system will remind user. If clicks [OK] to save, it will save the actual access controller type of the device.

Extended Device Parameters: includes serial number, device type, firmware version number, auxiliary input quantity, auxiliary output quantity, door quantity, device fingerprint version, and reader quantity etc.

Note: When deleting a new device, the software will clear all user information, time zones, holidays, and access control levels settings (including access levels, anti-pass back, interlock settings, linkage settings etc.) from the device, except the events record (unless the information in the device is unusable, or it is recommended not to delete the device in used to avoid the loss of information).

Elevator Controller Settings:

✧ TCP/ IP Communication Requirements

Support and enable TCP/ IP communication, directly connect device to the PC or connect to the local network, query IP address and other information of the device;

✧ RS485 Communication Requirements

Support and enable RS485 communication, connect device to PC by RS485, query the serial port number, RS485 machine number, baud rate and other information of the device.

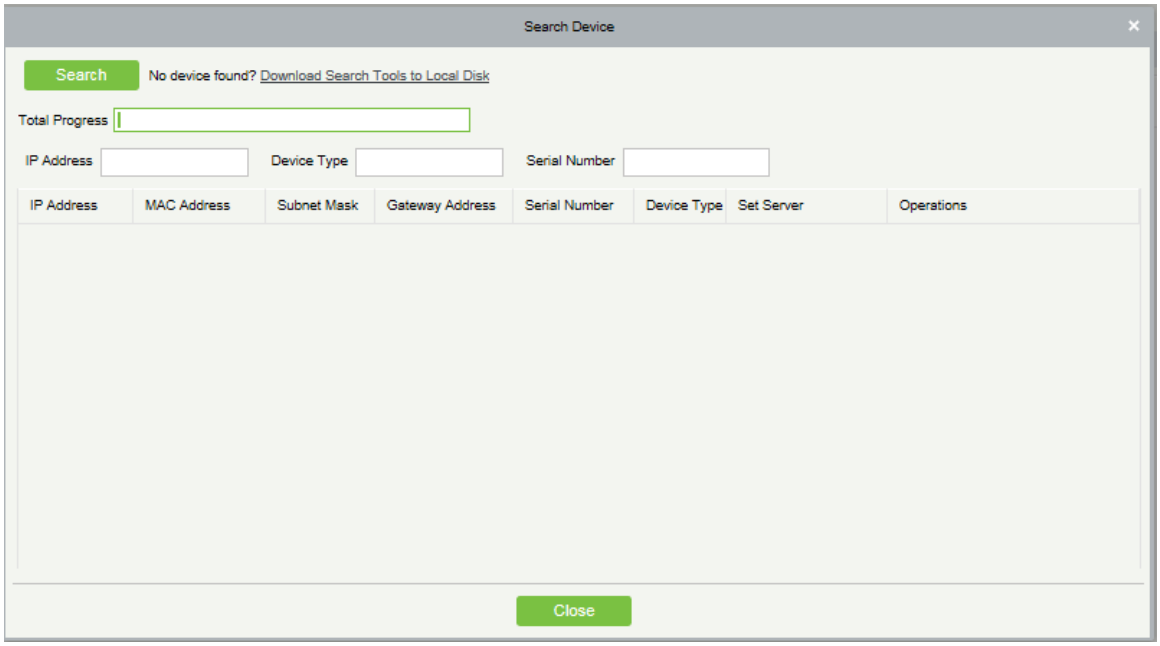
2. Add Device by Searching Elevator Controllers

Search the access controllers in the Ethernet.

(1) Click [Elevator Device] > [Device] > [Search Device], to show the Search interface.

(2) Click [Search], and it will prompt [searching……].

(3) After searching, the list and total number of access controllers will be displayed.



Note: Here we use UDP broadcast mode to search elevator devices, this mode cannot perform cross-Router function. IP address can be cross-net segment, but must belong to the same subnet, and needs to be configured the gateway and IP address in the same net segment.

(4) Click [Add Device] behind the device, and a dialog box will pop up. Enter self-defined device name, and click [OK] to complete device adding.

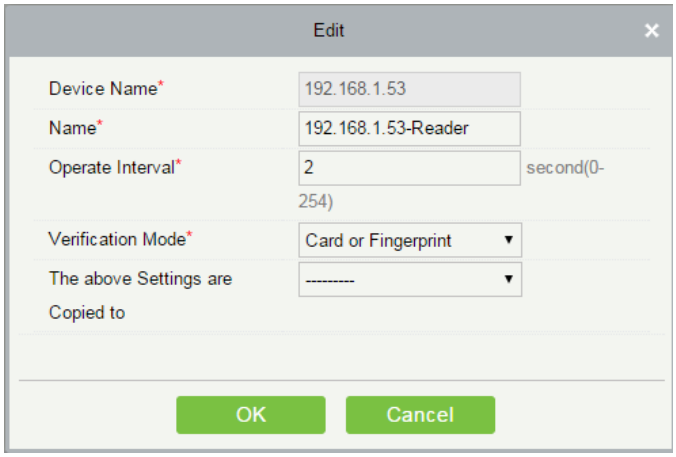
(5) The default IP address of the access controller may conflict with the IP of a device on the Local network. You can modify its IP address: Click [Modify IP Address] behind the device and a dialog box will open. Enter the new IP address and other parameters (**Note:** Configure the gateway and IP address in the same net segment).

Note: The system cannot add Elevator Devices automatically.

5.1.2 Reader

Each elevator device has a reader, the reader information can be set.

Click [Elevator Device] > [Reader], select a reader name in the reader list:



Fields are as follows:

Device Name: It is not editable.

Name: The default format is "Device Name - Reader", it is editable within 30 characters.

Operate Interval: The interval between two verifications. The default value is 2 seconds, the range is 0~254 seconds.

Verification Mode: The default setting is "Card or Fingerprint". The Wiegand reader supports "Only Card", "Only Password", "Card or Password", "Card and Password", "Card or Fingerprint". The RS485 reader supports "Card or Fingerprint". Make sure the reader has a keyboard when the verification mode is "Card and Password".

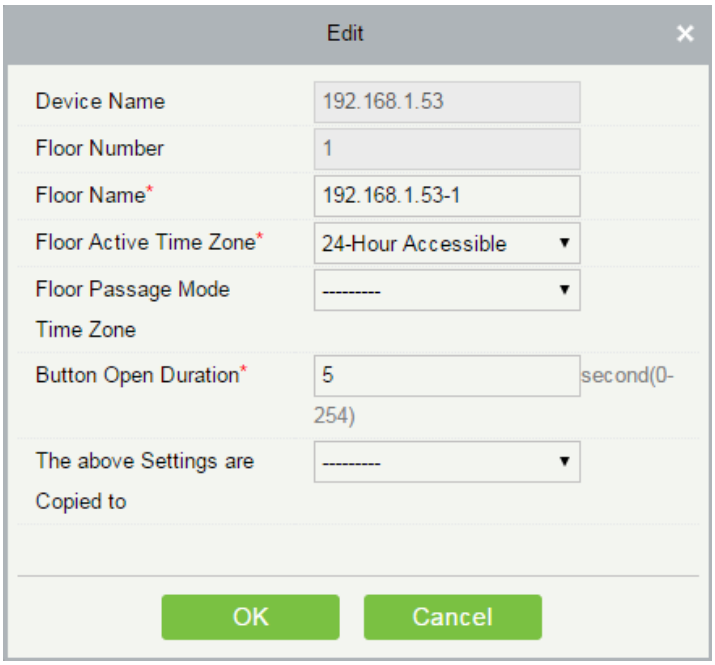
The above Settings are Copied to:

All Readers of All Devices: Apply the above settings to all readers within the current user's level.

Click [OK] to save and exit.

5.1.3 Floor

Click [Elevator Device] > [Floor], select a floor name in the list to click [Edit]:



Fields are as follows:

Device Name: It is not editable.

Floor Number: The system automatically numbered according to the number of relays.

Floor Name: The default setting is "Device Name- Floor Number", it is editable within 30 characters.

Floor Active Time Zone, Floor Passage Mode Time Zone: The default setting is Null. The Floor Active Time Zones that are initialized or newly added by users will be displayed here so that users can select a period. When editing a floor, the Floor Active Time Zone must be specified. The key for closing the related floor can be released continuously only after the effective periods of this floor are specified. Floor Passage Mode Time Zone takes effect only within the floor effective period. It is recommended that the floor continuous release period be included in the floor effective period.

Button Open Duration: It is used to control the time period to press floor button after verification. The default value is 5 seconds; the range is 0~254 seconds.

The above Settings are Copied to: Including below two options.

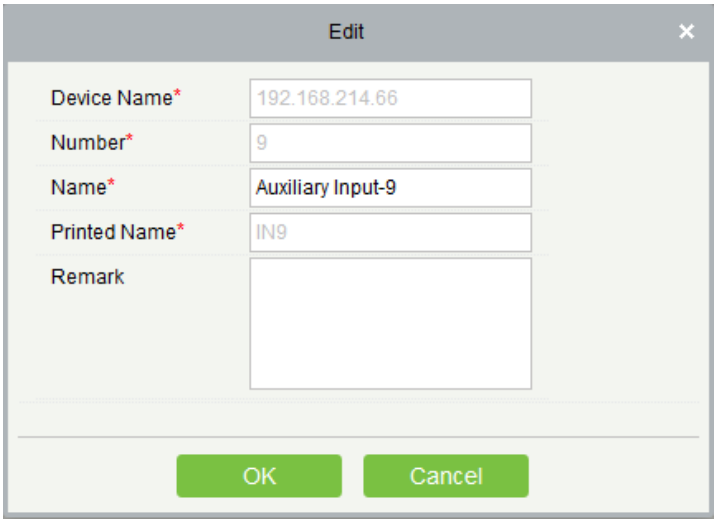
- ✧ All Floors of Current Device: To apply the above settings to all floors of the current elevator device.
- ✧ All floors of all Devices: To apply the above settings to all floors within the current user's level.

5.1.4 Auxiliary Input

It is mainly used to connect to devices, such as the infrared sensor or smog sensor.

1. Click [Elevator Device] > [Auxiliary Input] on the Action Menu, enter into the following page:

2. Click [Edit] to modifiy the parameters:



Fields are as follows:

Name: You can customize the name according to your preference.

Printed Name: The printing name in the hardware, for example IN9。

3. Click [Edit] to modify the name and remark. Others are not allowed to edit here.

5.1.5 Event Type

Display the event types of the elevator devices. Click [Elevator Device] > [Event], the following page is displayed:

Refresh

Event Name	Event No.	Event Level	Device Name	Serial No.
Normal Punch Open	0	Normal	192.168.90.235	0013130700074
Punch during Passage Mode Time Zone	1	Normal	192.168.90.235	0013130700074
Open during Passage Mode Time Zone	5	Normal	192.168.90.235	0013130700074
Remote Release	8	Normal	192.168.90.235	0013130700074
Remote Locking	9	Normal	192.168.90.235	0013130700074
Disable Intraday Passage Mode Time Zone	10	Normal	192.168.90.235	0013130700074
Enable Intraday Passage Mode Time Zone	11	Normal	192.168.90.235	0013130700074
Normal Fingerprint Open	14	Normal	192.168.90.235	0013130700074
Press Fingerprint during Passage Mode Time Zc	16	Normal	192.168.90.235	0013130700074
Operate Interval too Short	20	Exception	192.168.90.235	0013130700074
Button Inactive Time Zone(Punch Card)	21	Exception	192.168.90.235	0013130700074
Illegal Time Zone	22	Exception	192.168.90.235	0013130700074
Access Denied	23	Exception	192.168.90.235	0013130700074
Disabled Card	27	Exception	192.168.90.235	0013130700074
Card Expired	29	Exception	192.168.90.235	0013130700074
Password Error	30	Exception	192.168.90.235	0013130700074
Press Fingerprint Interval too Short	31	Exception	192.168.90.235	0013130700074

More details about Event Type, please refer to Elevator Event Type.

5.1.6 Device Monitoring

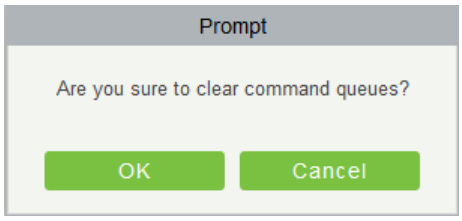
By default it monitors all devices within the current user's level, click [Elevator Device] > [Device Monitoring], and lists the operation information of devices: Device Name, Serial No., Area, Operation Status, current status, commands List, and Related Operation.

Area Status -------- Device Name Serial Number

Export

Device Name	Serial Number	Area	Operation Status	Current Status	Commands List	Recently The Abnormal State	Operations
192.168.214.66	0013130700074	Area Nameaa	Get real-time event	Normal	0	None	Clear Command View Command

You can clear command as required. Click [Clear Command] behind the corresponding device:



Click [OK] to clear.

Notes:

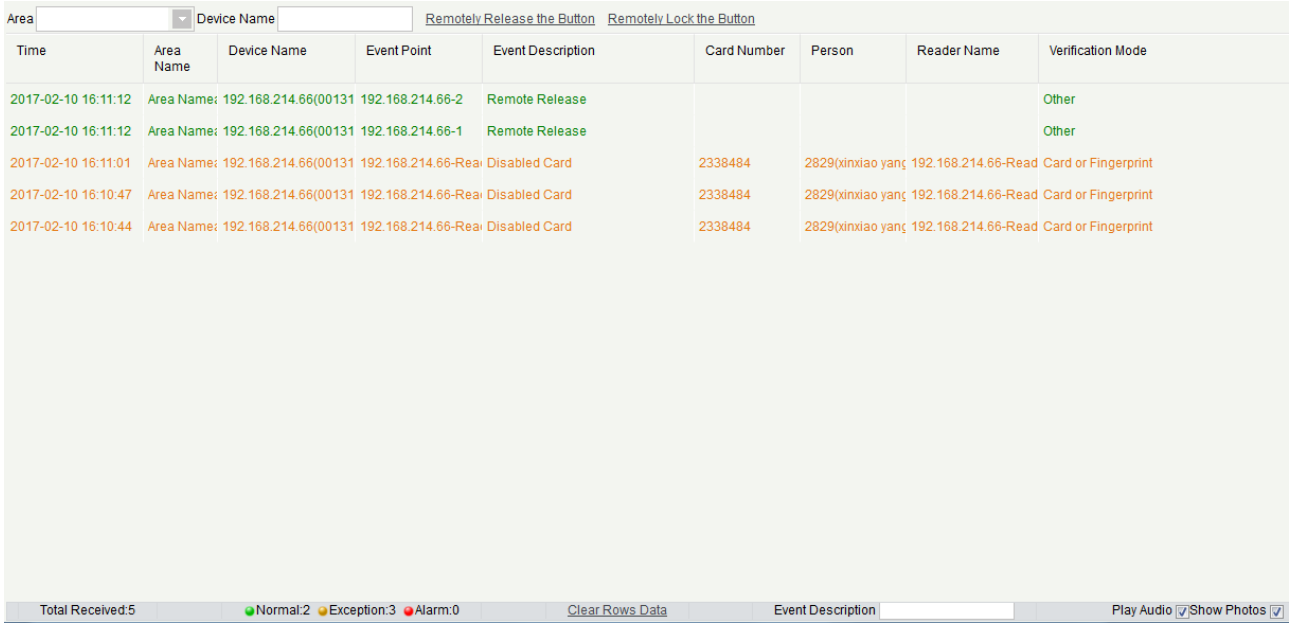
(1) After the Clear Command is executed, you can perform the Synchronize All Data to Devices operation on the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once the capacity is insufficient, you can replace the current device with a large-capacity one, or delete the right of some personnel to access this device, and then perform the Synchronize All Data to Devices operation.

(2) Operate State is the content of communications equipment of current device, mainly used for debugging.

(3) The number of commands to be performed is greater than 0, indicating that data is not synchronized to the device, just wait.

5.1.7 Real-Time Monitoring

Click [Elevator Device] > [Real-Time Monitoring], real-time monitor the status and real-time events of elevator controllers in the system, including normal events and abnormal events (including alarm events). Real-Time Monitoring interface is shown as follows:



1. Event Monitoring

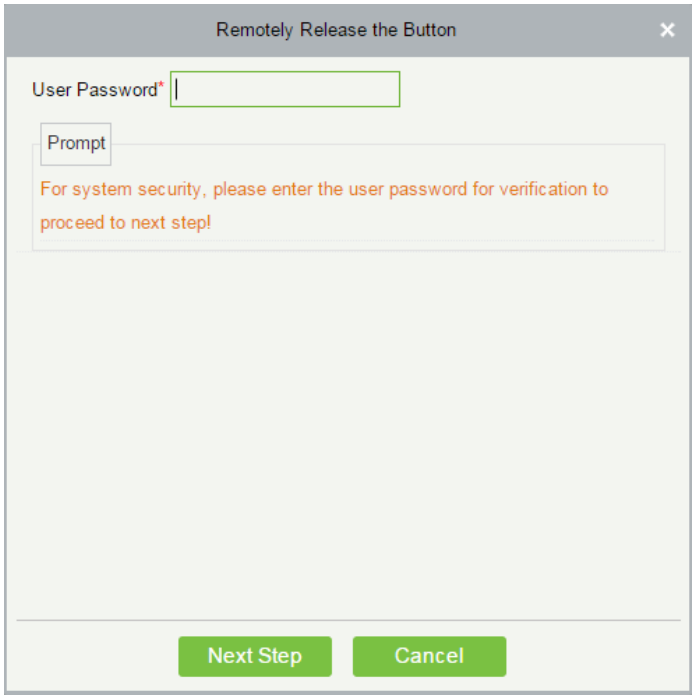
System automatically acquires monitored device event records (by default, display 200 records), including normal and abnormal elevator control events (including alarm events). Normal events appear in green, alarm events appear in red, other abnormal events appear in orange.

Monitor Area: All floors with elevator controller in the system is monitored by default, you can target to monitor one or more floors by Area, Status, Device Name and Serial NO.

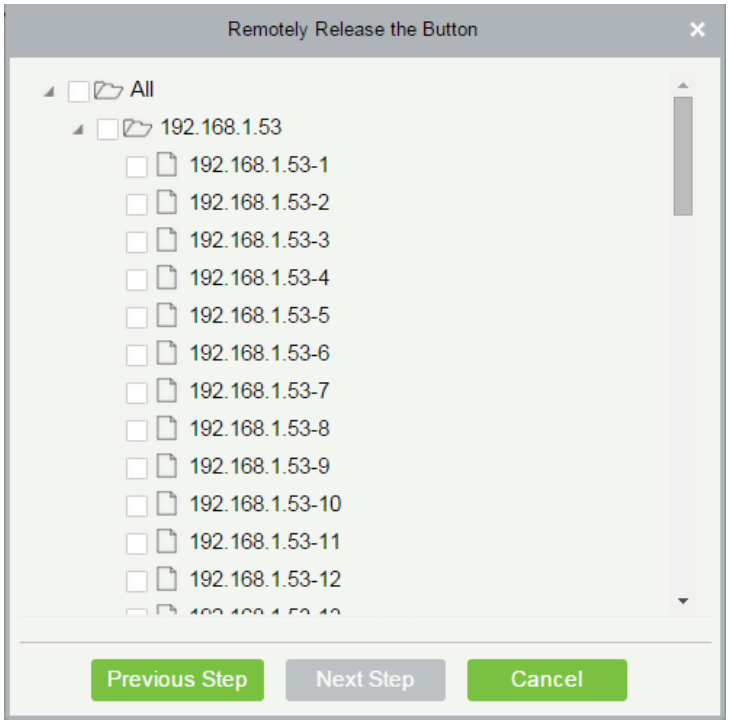
Show Photos: If Real-Time Monitoring is involved in a person, the monitor displays the personal photo (if no photo is registered, display default photo). The event name, time and name are displayed.

2. Remotely Release Button

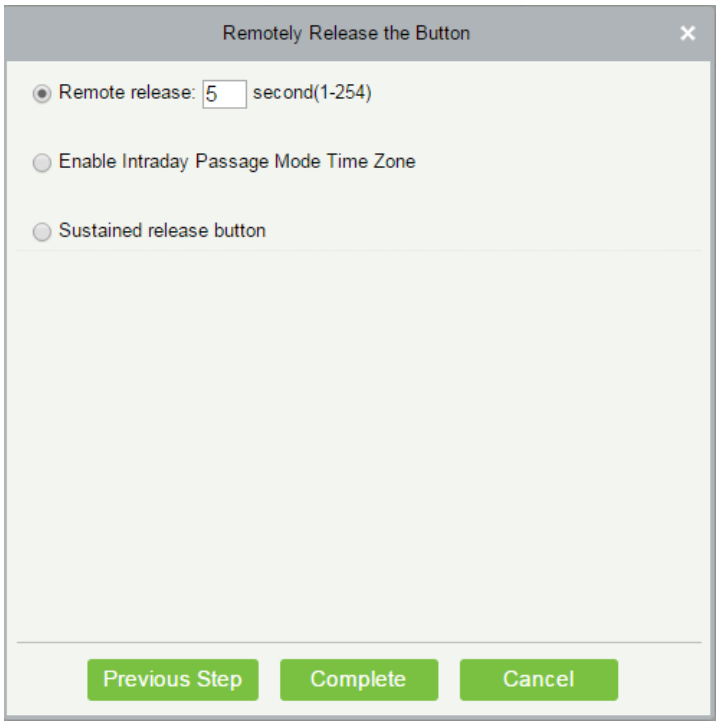
Click [Remotely Release Button]:



Input the user password (the system logging password), click [Next Step]:



Select the floor, and click [Next Step]:



Fields are as follows:

Remote Release: It determines whether the key corresponding to the selected floor can be pressed. You can customize the key release duration (15s by default), or select Enable Intraday Passage Mode Time Zone. You can also directly set the current status of the floor to continuously release. In this case, the floor is not subject to restrictions of any periods, including Floor Active Time Zone, Floor Passage Mode Time Zone, and Button Open Duration. That is, the floor will be continuously released in 24 hours every day.

Enable Intraday Passage Mode Time Zone: To close a floor, you must first set Disable Intraday Passage Mode Time Zone to prevent the case that the floor is opened because other continuous open periods take effect. Then, you need to set to close the Remote Lock Button.

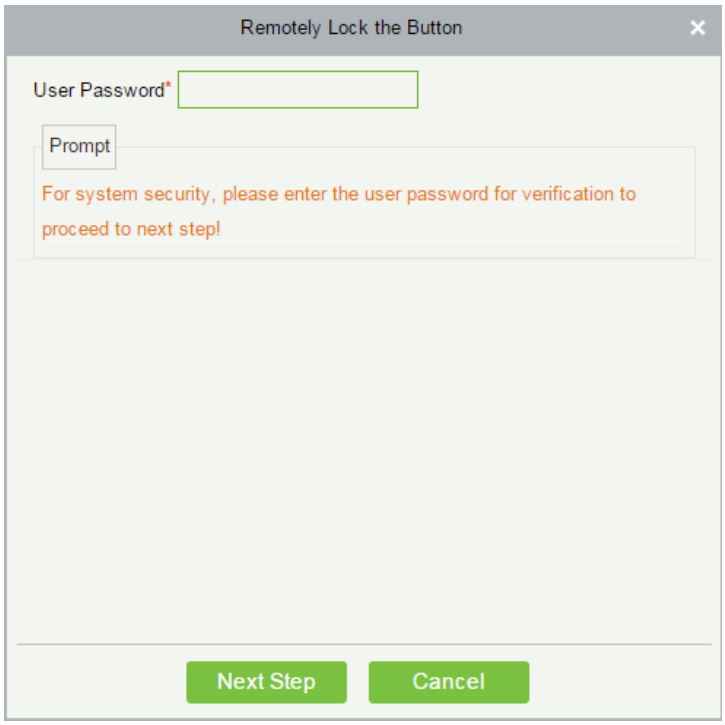
Sustained Release Button: The floor that is set to the continuously release state is not subject to restrictions of any periods, that is, the floor will be continuously released in 24 hours every day. To close the floor, you must select Disable Intraday Passage Mode Time Zone.

Note: If a failure message is always returned for the remote release key, check whether there are too many currently disconnected devices on the device list. If yes, check the network connection.

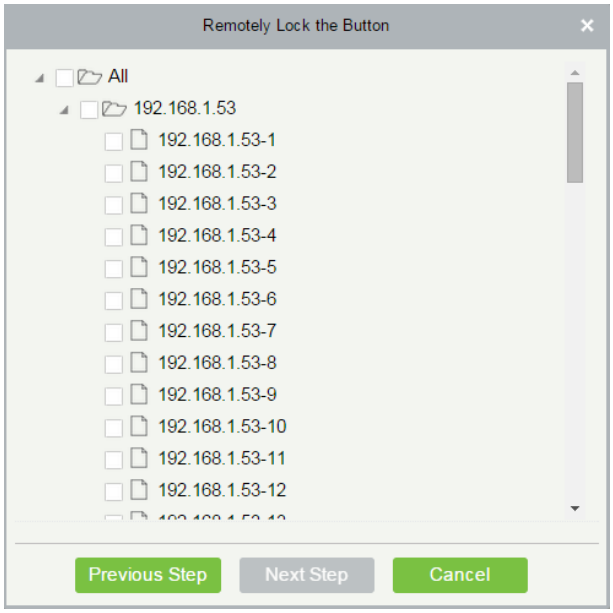
Select the options, click [Complete] to finish enabling the button.

2. Remotely Lock Button

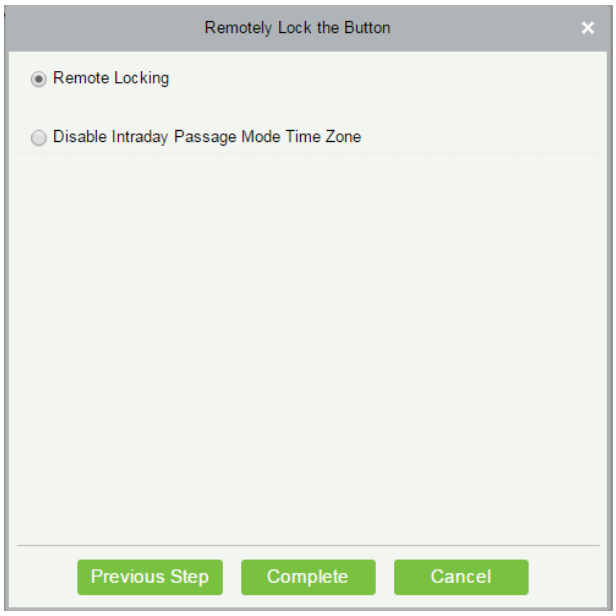
Click [Remotely Lock Button]:



Input the user password (the system logging password), click [Next Step]:



Select the floor, and click [Next Step]:



Fields are as follows:

Remote Locking: Lock the remotely released button.

Note: If a failure message is always returned for the remote lock key, check whether there are too many currently disconnected devices on the device list. If yes, check the network connection.

Select the options, click [Complete] to finish enabling the button.

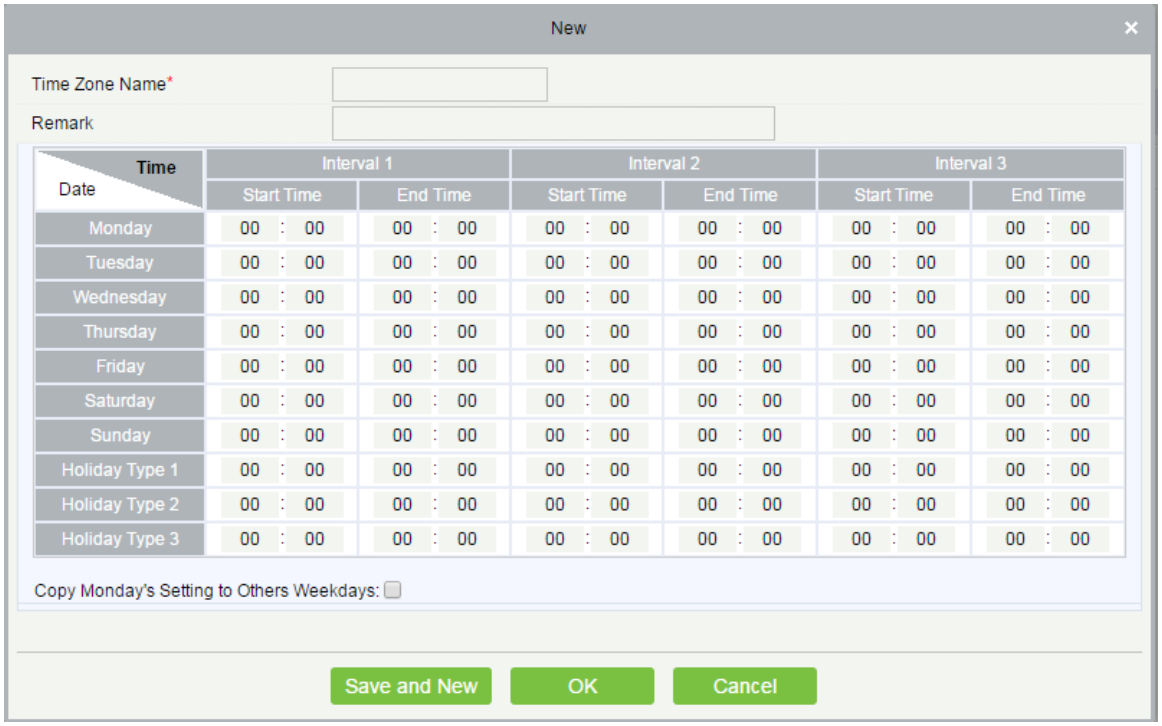
5.2 Elevator Rules

It can control buttons of a common elevator and implement unified management on people going in or coming out of each floor through the elevator controller on the computer management network. You can set the rights of registered personnel for operating floor buttons on the elevator.

5.2.1 Time Zones

1. Add Elevator Control Time Zone

(1) Click [Elevator] > [Time Zones] > [New] to enter the time zone setting interface:



The parameters are as follows:

Time Zone Name: Any character, up to a combination of 30 characters.

Remarks: Detailed description of the current time zone, including explanation of current time zone and primary applications. The field is up to 50 characters.

Interval and Start/ End Time: One Elevator Control Time Zone includes 3 intervals for each day in a week, and 3 intervals for each of the three Holidays. Set the Start and End Time of each interval.

Setting: If the interval is Normal Open, just enter 00:00-23:59 as the interval 1, and 00:00-00:00 as the interval 2/3. If the interval is Normal Close: All are 00:00-00:00. If only using one interval, user just needs to fill out the interval 1, and the interval 2/3 will use the default value. Similarly, when only using the first two intervals, the third interval will use the default value. When using two or three intervals, user needs to ensure two or three intervals have no time intersection, and the time shall not span days. Or the system will prompt error.

Holiday Type: Three holiday types are unrelated to the day of a week. If a date is set to a holiday type, the three intervals of the holiday type will be used for access. The holiday type is optional. If the user does not enter one, system will use the default value.

Copy on Monday: You can quickly copy the settings of Monday from Tuesday to Sunday.

(2) After setting, click [OK] to save, and it will display in the list.

2. Maintenance of Elevator Time Zones

Edit: Click the [Edit] button under operation to enter the edit interface. After editing, click [OK] to save.

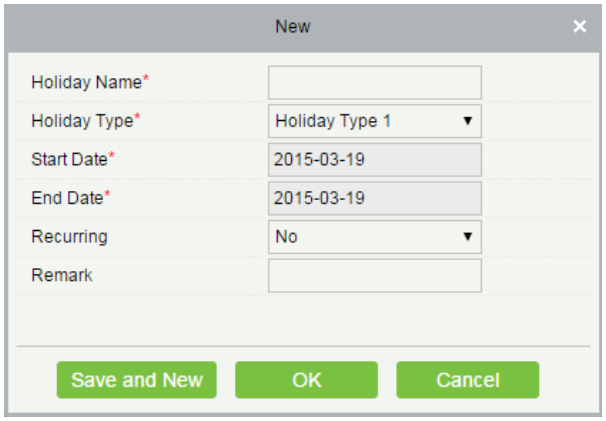
Delete: Click the [Delete] button under Related Operation, then click [OK] to delete, or click [Cancel] to cancel the operation. A time zone in use cannot be deleted. Or tick the check boxes before one or more time zones in the list, and click the [Delete] button over the list, then click [OK] to delete, click [Cancel] to cancel the operation.

5.2.2 Holidays

Elevator Control Time of a holiday may differ from that of a weekday. The system provides elevator control time setting for holidays. Elevator Holiday Management includes Add, Modify and Delete.

- Add

(1) Click [Elevator] > [Holidays] > [Add] to enter edit interface:



Fields are as follows:

Holiday Name: Any character, up to a combination of 30 characters.

Holiday Type: Holiday Type 1/2/3, namely, a current holiday record belongs to the three holiday types and each holiday type includes up to 32 holidays.

Start/ End Date: The date format: 2010-1-1. Start Date cannot be later than End Date otherwise the system will prompt an error. The year of Start Date cannot be earlier than the current year, and the holiday cannot span years.

Recurring: It means that a holiday whether to require modification in different years. The default is No. For example, the Near Year's Day is on January 1 each year, and can be set as Yes. The Mother's Day is on the second Sunday of each May; this date is not fixed and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2010, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Friday, but the Access Control Time of Holiday Type 1.

(2) After editing, click [OK] button to save, and it will display in holiday list.

- Modify

Click Holiday Name or [Edit] button under Operations to enter the edit interface. After modification, click [OK] to save and quit.

- Delete

In the access control holiday list, click [Delete] button under Operations. Click [OK] to delete, click [Cancel] to cancel the operation. An Elevator Holiday in use cannot be deleted.

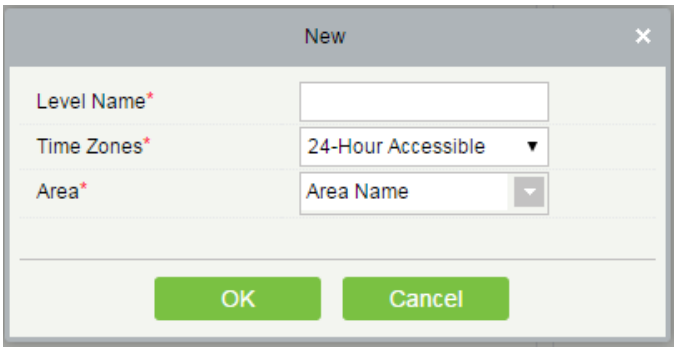
5.2.3 Elevator Levels

Elevator levels indicate that one or several selected doors can be opened by verification of a combination of multi

person within certain time zone. The combination of multi person set in Personnel Access Level option.

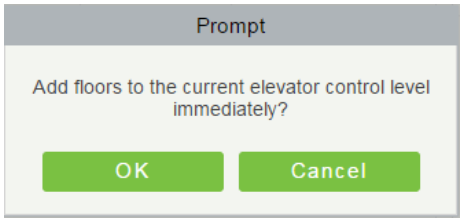
- Add

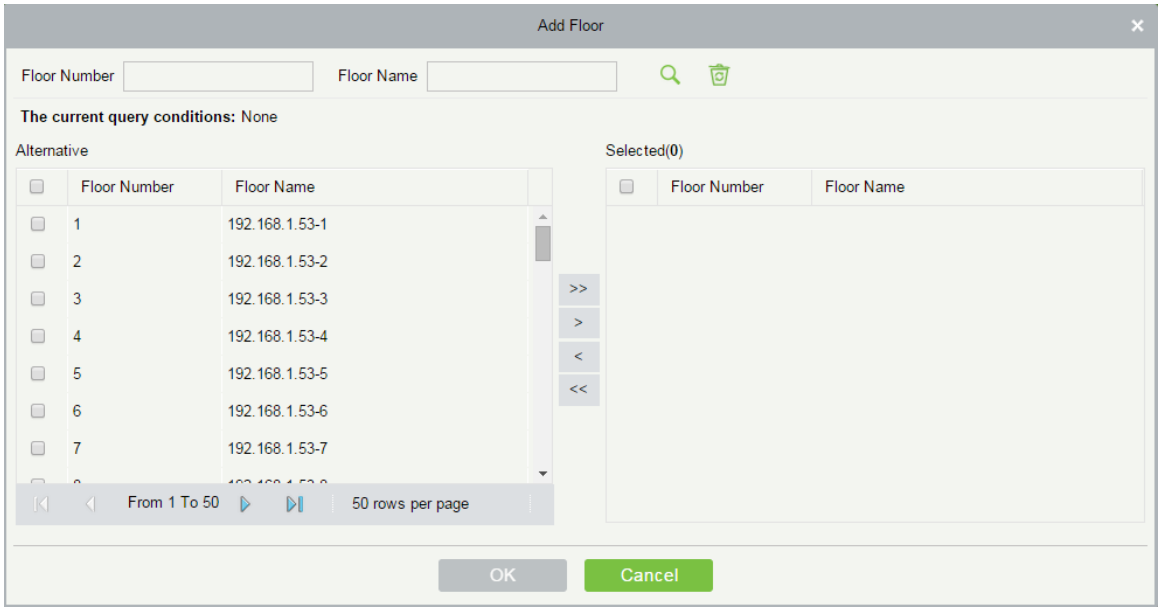
1. Click [Elevator] > [Access Levels] > [Add] to enter the Add Levels editing interface:



2. Set each parameter: Level Name (unrepeatable), Time Zone and Area.

3. Click [OK], the system prompts "Add floors to the current elevator control level immediately", click [OK] to add floors, click [Cancel] to return the elevator levels list. The added level is displayed in the list.





Note: Different floors of different elevator controllers can be selected and added to an elevator level.

- Set Access By Levels

Add/Delete Personnel for Selected Levels:

1. Click [Elevator] > [Set By Levels] to enter the edit interface, Click an Elevator level in left list, personnel having right of opening door in this access level will display on right list.

2. In the left list, click [Add Personnel] under Operations to pop-up the Add Personnel box; select personnel (multiple) and click > to move it to the right selected list, then click [OK] to save and complete.

3. Click the level to view the personnel in the right list. Select personnel and click [Delete Personnel] above the right list, then Click [OK] to delete.

- Set Access By Employee

Add selected personnel to selected elevator levels, or delete selected personnel from the elevator levels.

Add/Delete levels for Selected Personnel:

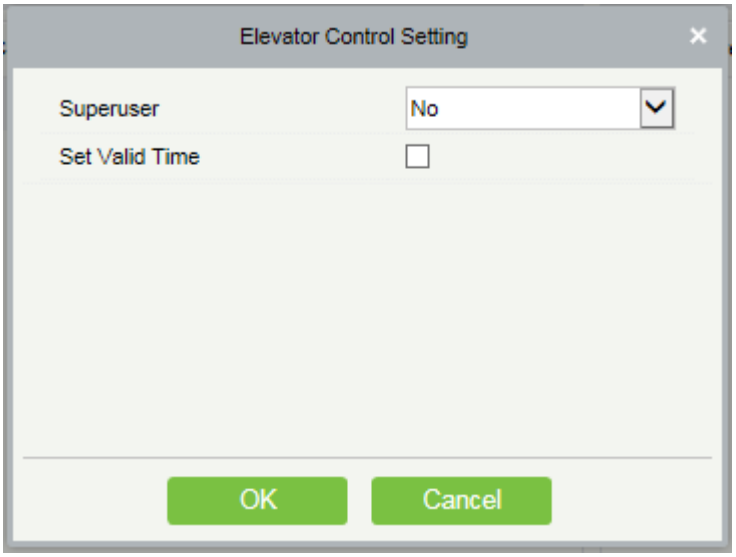
(1) Click [Elevator] > [Elevator Levels] > [Set By Person], click employee to view the levels in the right list.

(2) Click [Add to Levels] under Operations to pop-up the Add to Levels box, select Level (multiple) and click > to move it to the right selected list; click [OK] to save and complete.

(3) Select Level (multiple) in the right list, and click [Delete from levels] above the list, then click [OK] to delete the selected levels.

Setting levels for Selected Personnel:

(1) Select a person in the list on the left and click [Elevator Control Setting]. The following page is displayed:



(2) Set access control parameters and click [OK] to save the setting.

- Set Access By Department

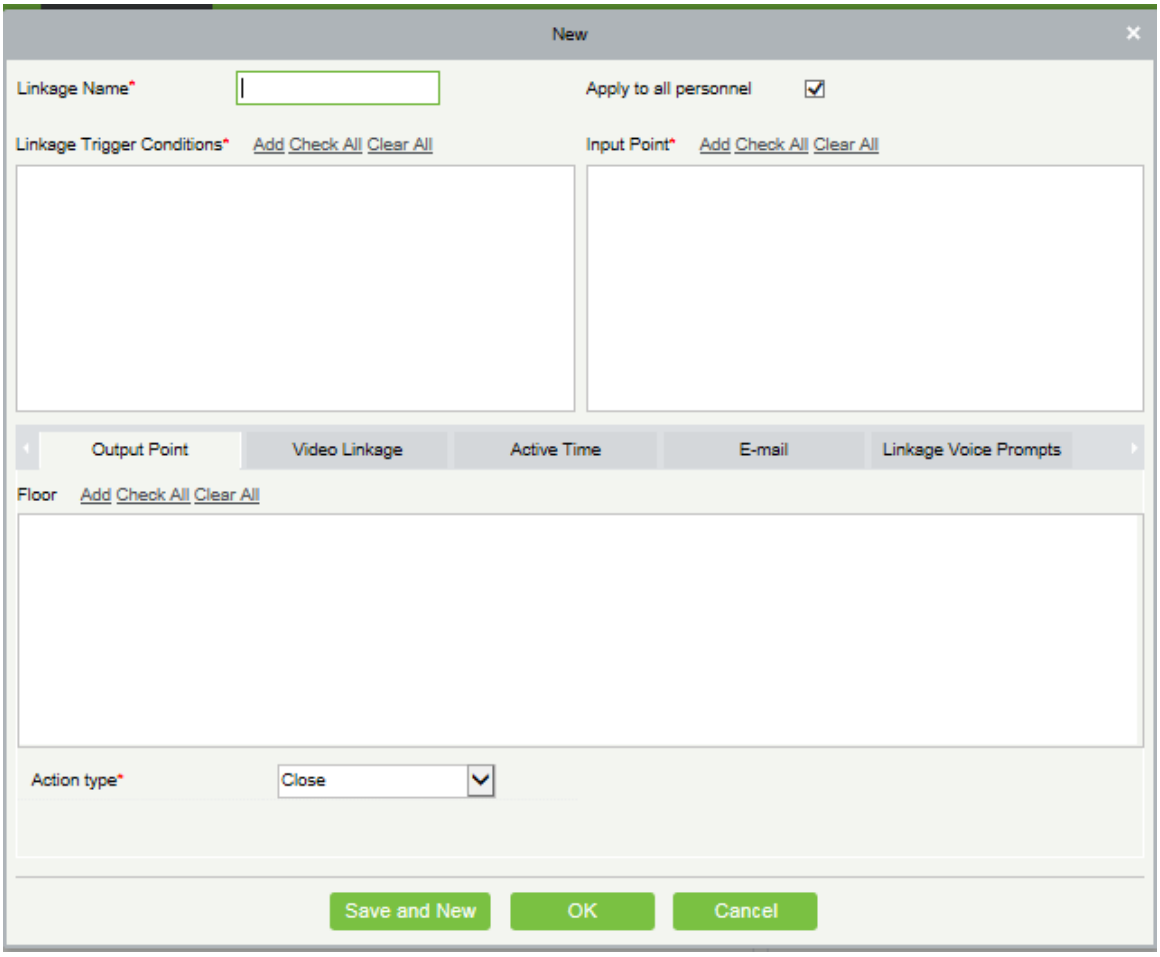
Add selected department to selected elevator levels, or delete selected department from the elevator levels. The access of the staff in the department will be changed.

5.2.4 Global Linkage

The global linkage function allows you to configure data across devices. Only push devices support this function.

- Add

1. Click [Elevator] > [Elevator] > [Global Linkage] > [New]:



The fields are as follows:

Linkage Name: Set a linkage name.

Linkage Trigger Condition: Linkage Trigger Condition is the event type of selected device. Except Linkage Event Triggered, Cancel Alarm, Enable/Disable Auxiliary Output, and Device Start, all events could be trigger condition.

Input Point: Any, Door 1, Door 2, Door 3, Door 4, Auxiliary Input 1, Auxiliary Input 2, Auxiliary Input 3, Auxiliary Input 4, Auxiliary Input 9, Auxiliary Input 10, Auxiliary Input 11, Auxiliary Input 12 (the specific input point please refers to specific device parameters).

Output Point: Lock 1, Lock 2, Lock 3, Lock 4, Auxiliary Output 1, Auxiliary Output 2, Auxiliary Output 3, Auxiliary Output 4, Auxiliary Output 6, Auxiliary Output 8, Auxiliary Output 9, and Auxiliary Output 10 (the specific output point please refers to specific device parameters).

Linkage Action: Close, Open, Normal Open. The default is closed. To open, delay time shall be set, or select Normal Close.

Video Linkage:

- Pop up video: Whether to set the pop-up preview page in real-time monitoring, and set the pop-long.
- Video: Enable or disable background video recording, and set the duration of background video recording.

✧ Capture: Enable or disable background snapshot

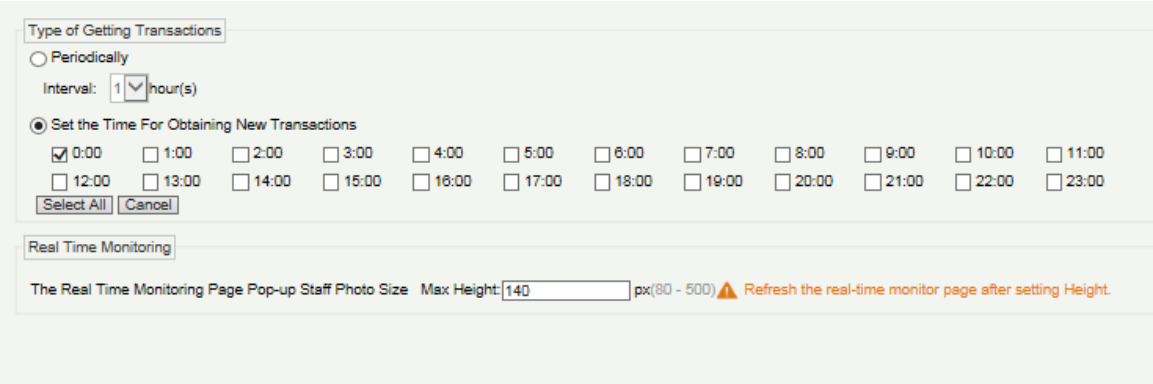
Delay: Ranges from 1~254s (This item is valid when Action type is Open).

2. Click [OK] to save and quit. The added Global Linkage will display in the list.

Note: It is not allowed to set the same linkage setting at input point and output point. The same device permits consecutive logical linkage settings. The system allows you to set several trigger conditions for a linkage setting one time.

5.2.5 Parameters

1. Click [Elevator] > [Elevator] > [Parameters]:



Type of Getting Transactions

- Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

- Set the Time For Obtaining New Transactions

The selected Time is up, the system will attempt to download new transactions automatically.

The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up, set the size of the pop-up photos, the range is 80-500px.

5.3 Elevator Reports

Includes “All transactions” and “All Exception Events”. You can export after querying.

5.3.1 All Transactions

Because the data size of access control event records is large, you can view access control events as specified condition when querying. By default, the system displays latest three months transactions.

Click [Reports] > [All Transactions] to view all transactions:

Time From 2015-02-26 00:00:00 To 2015-05-26 23:59:59 Personnel ID Device Name More

The current query conditions: Time From:(2015-02-26 00:00:00) To:(2015-05-26 23:59:59)

Refresh Clear All Data Export

Time	Device	Event Point	Event Description	Media File	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-1	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-1	Trigger global linkage		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-2	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-2	Trigger global linkage		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-1	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-1	Trigger global linkage		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-2	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-2	Trigger global linkage		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 16:58:26	192.168.60.53	192.168.60.53-2	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw

Clear All Data:

Click [Clear All Data] to pop up prompt, and click [OK] to clear all transactions.

5.3.2 All Exception Events

Click [Reports] > [All Exception Events] to view exception events in specified condition. The options are same as those of [All Transactions].

Time From 2015-02-26 00:00:00 To 2015-05-26 23:59:59 Personnel ID Device Name More

The current query conditions: Time From:(2015-02-26 00:00:00) To:(2015-05-26 23:59:59)

Refresh Clear All Data Export

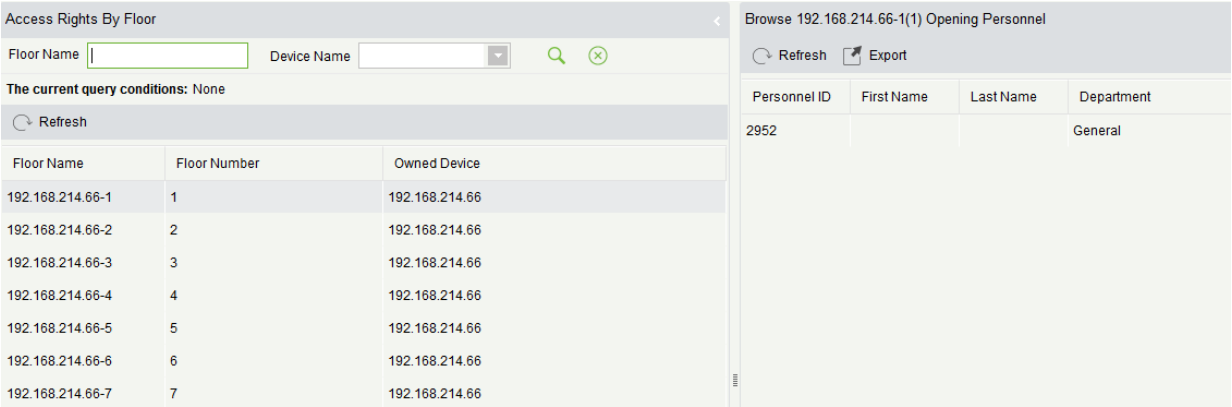
Time	Area	Device	Event Point	Event Description	Card Number	Personnel ID	First Name	Last Name	Departmer	Reader Name	Verification Mode	Remark
2015-05-20 10:41:31	Area Name	192.168.60.53	192.168.60.53-R	Disabled Card	3406918		jolly2	wei	General	192.168.60.	Card or Fing	
2015-05-20 10:41:23	Area Name	192.168.60.53	192.168.60.53-R	Disabled Card	3406916		jolly1	wei	General	192.168.60.	Card or Fing	
2015-05-19 14:59:46	Area Name	192.168.60.53	192.168.60.53-R	Disabled Card	3406916		jolly1	wei	General	192.168.60.	Card or Fing	
2015-05-19 13:57:12	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Fing	
2015-05-19 13:54:46	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Fing	
2015-05-19 11:53:35	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Fing	
2015-05-19 11:50:51	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Fing	
2015-05-19 11:42:57	Area Name	192.168.60.53	192.168.60.53-R	Disabled Card	8651633					192.168.60.	Card or Fing	
2015-05-18 14:36:23	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Fing	

Clear All Data: Click [Clear All Data] to pop up prompt, click [OK] to clear all exception events.

5.3.3 Access Rights

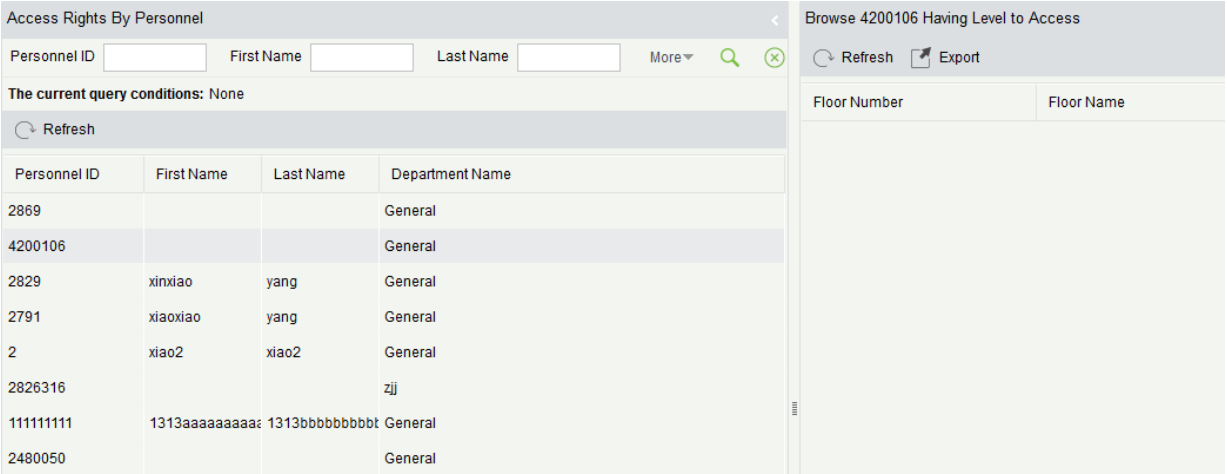
- Access Rights By Floor

View related access levels by door. Click [Reports] > [Access Rights By Floor], the data list in the left side show all floors in the system, select a floor, the personnel having access levels to the floor will display on the right data list.



Access Rights By Personnel

Click [Reports] > [Access Rights By Personnel], the data list in the left side show all doors in the system, select a personnel, the personnel having access levels to the door will display on the right data list.



6 Hotel Management System

It provides hotel service management functions covering check-in, overstay, check-out, rate settlement, and lock setup and management.

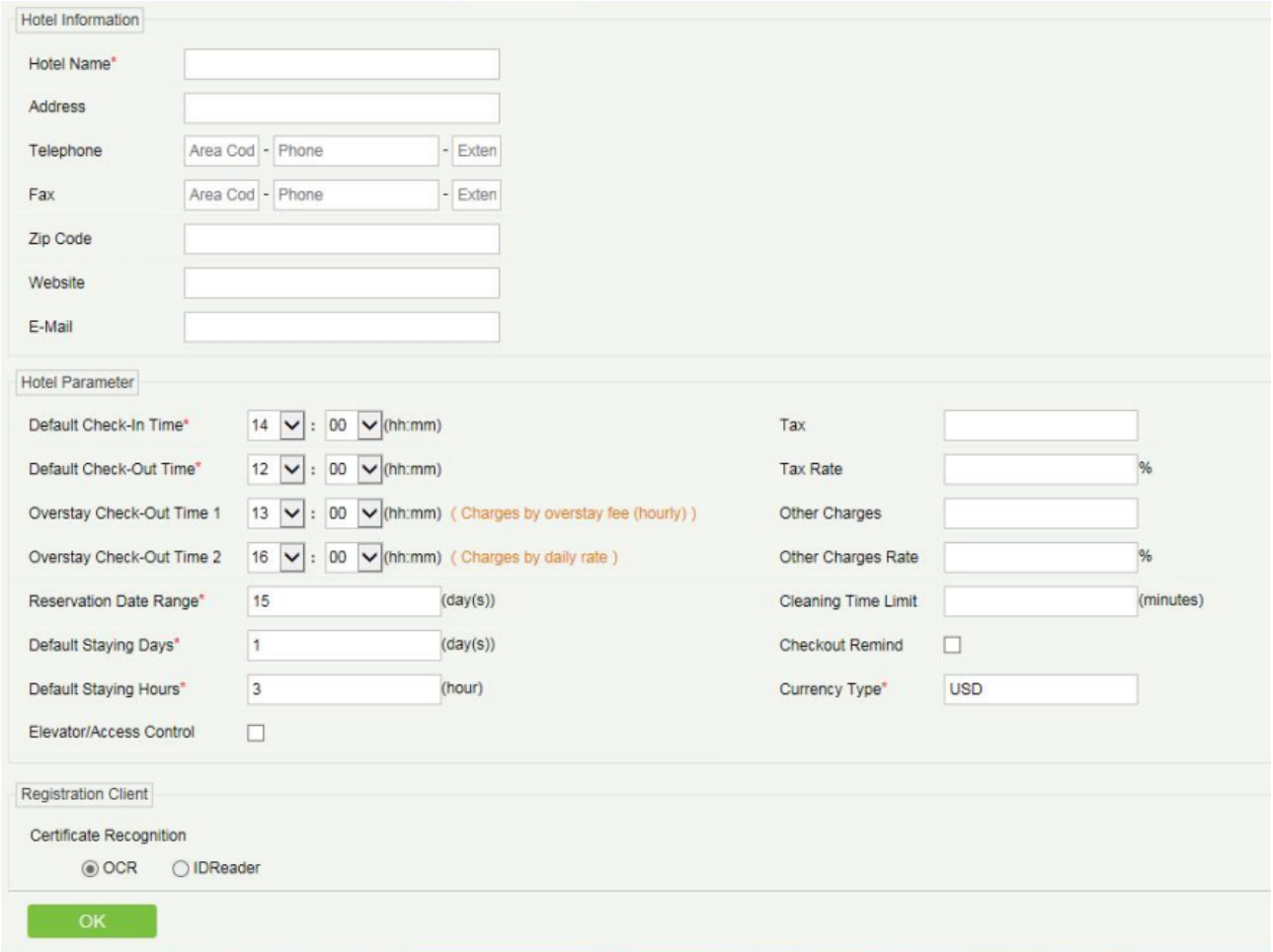
- Operation Guide

It helps you quickly understand how to quickly navigate to specific function pages and configure and use the hotel management software.

6.1 Hotel Settings

You can set the basic information about a hotel, including its name, address, phone number, fax number, zip code, website address, and email address. You can also set the function parameters regarding the check-in time, check-out time, check-out reminder, and access/elevator control permissions.

Choose **Room Management** > **Hotel Settings**. The page shown in the following figure appears.



The fields are described as follows:

Default Staying Days: It specifies the default number of days a guest stays. Generally, a guest stays for 1 day.

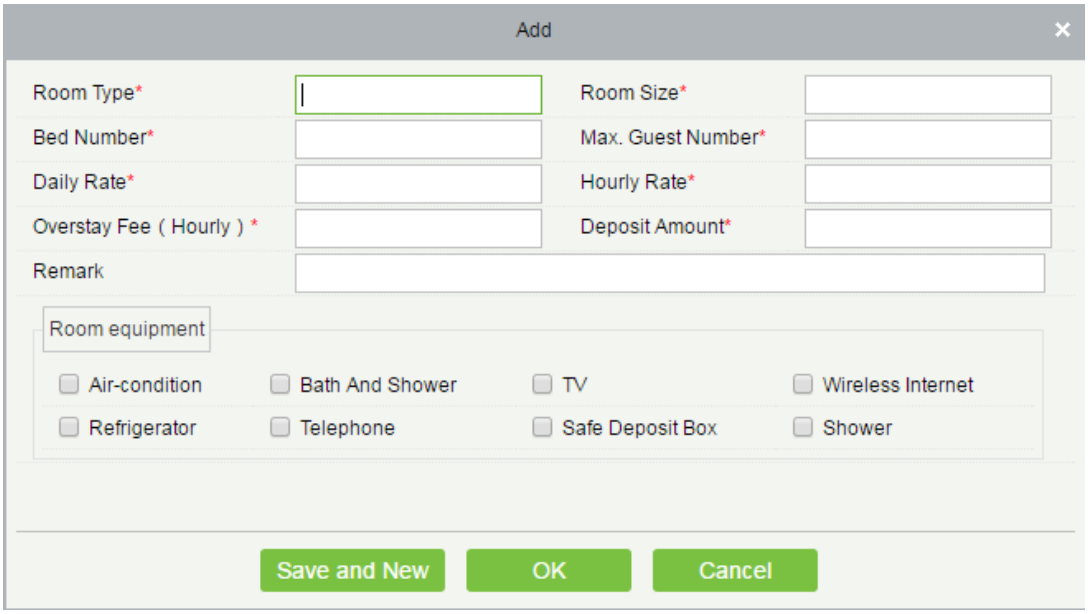
Default Staying Hours: It specifies the user-defined minimum number of hours a guest may stay. If a guest stays for a period less than this limit, the guest is charged the rate corresponding to this limit.
Default Check-In Time: You can set this time yourself. If a guest checks in before this time, the check-out date is the current day if the guest stays for one day. Otherwise, the check-out date is the next day.
Default Check-Out Time: It specifies the end time of a day use room.
Overstay Check-Out Time 1/2: You can set this time yourself. If a guest checks out at a time between **Overstay Check-Out Time 1** and **Overstay Check-Out Time 2**, the guest must pay an overstay charge. If a guest checks out at a time after **Overstay Check-Out Time 2**, the guest must pay for an extra day.
Cleaning Time Limit: It specifies the time available for cleaning a room after a guest checks out.
Checkout Remind: It specifies whether to display a reminder one hour before checkout.
Currency Type: It specifies the currency.
Elevator/Access Control: After selecting this check box, you can select an access/elevator control level on the card issuing UI, so that an issued card can be used not only as a hotel card, but also used to access the devices corresponding to the selected level. (**Note:** This check box is available on the **Hotel Settings** page only after you use the access control module and/or elevator control module and obtain and activate a license.)

Note: The hotel management system can be used to define buildings, floors, and rooms as well as handle check-in requests only after you set these parameters.

6.2 Room Management

6.2.1 Room Types

You can design information about various types of room, such as the number of beds and number of guest allowed. You can lock and unlock vacant rooms.
Choose **Room Management** > **Room Type** > **Add**. The page shown in the following figure appears.



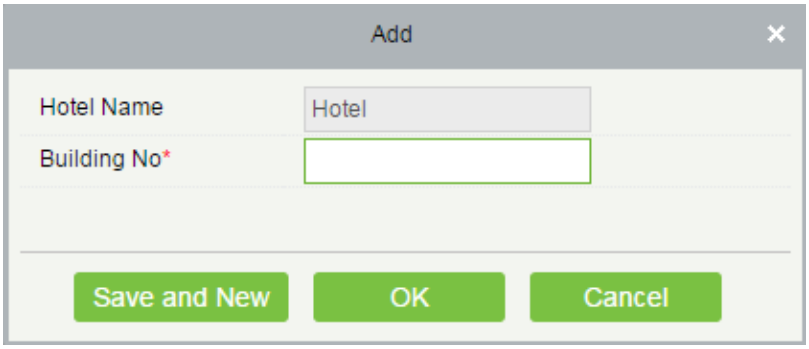
Note: When you add a room type, the system checks whether hotel settings are configured. If no, you are

redirected to the hotel settings page. All room types must be unique.

6.2.2 Building

You can define buildings of a hotel. When the rooms in a building are not booked or guests have not checked into the rooms, you can lock or unlock the building.

Choose **Room Management** > **Building** > **Add**. The page shown in the following figure appears.

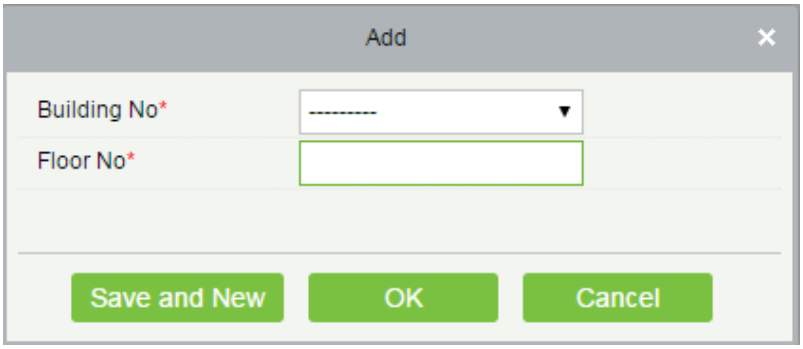


Note: When you add a building, the system checks for hotel settings and room types in order. If they have not been configured, configure the settings and types first. All building names must be unique.

6.2.3 Floor

You can define floors of a hotel. When the rooms on a floor are not booked or guests have not checked into the rooms, you can lock or unlock the floor.

Choose **Room Management** > **Floor** > **Add**. The page shown in the following figure appears.

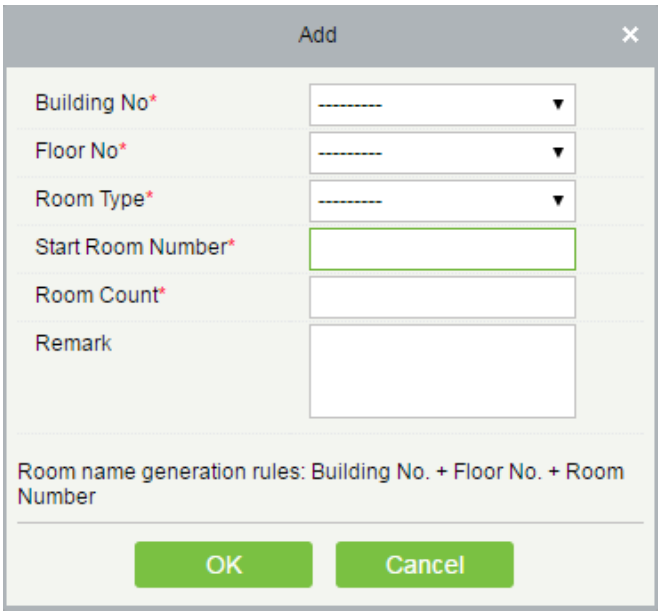


Note: When you add a floor, the system checks for hotel settings, room types, and buildings in order. If they have not been configured, configure the settings, types, and buildings first. All floor names must be unique.

6.2.4 Room

- **Adding guest rooms**

Choose **Room Management** > **Room** > **Add**. The page shown in the following figure appears.



Start Room Number: It specifies the start number of rooms.

Room Count: It specifies the number of rooms to add. The value **1** indicates only one room is added. A value greater than **1** indicates that a batch of rooms is added.

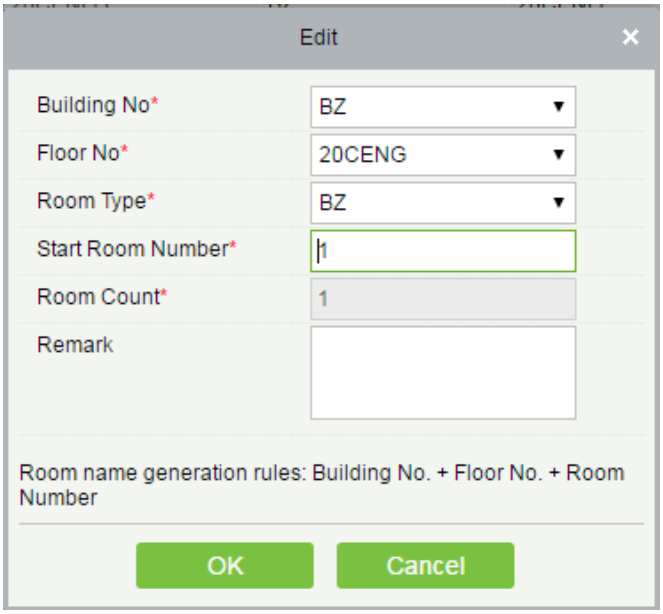
Remark: It describes the rooms added.

Note: All room names must be unique.

- **Editing guest room**

1) Editing one guest room

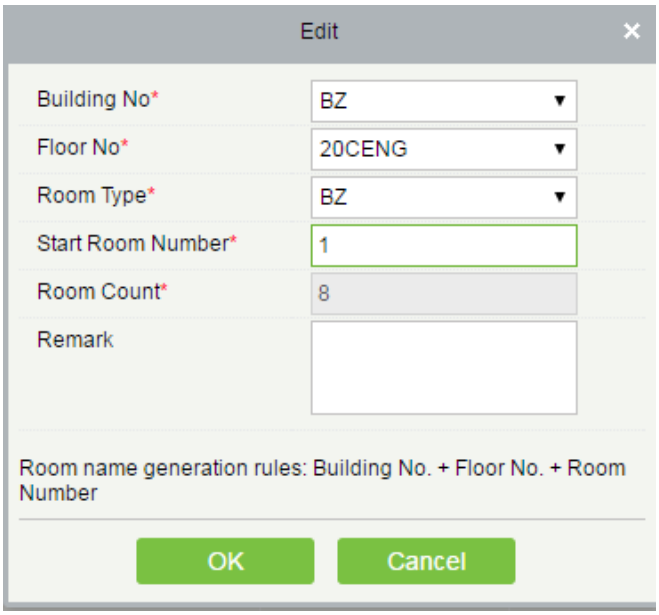
Select one guest room and edit the guest room. Duplicate guest room names are not allowed. Guest rooms that has been checked in or booked cannot be edited. See the following figure.



2) Editing guest rooms in batches

Select the check boxes of multiple guest rooms and edit them in batches. Duplicate guest room names are not allowed.

Only the rooms of the same type and belonging to the same building and same floor can be edited in batches. See the following figure.



- **Deleting guest rooms**

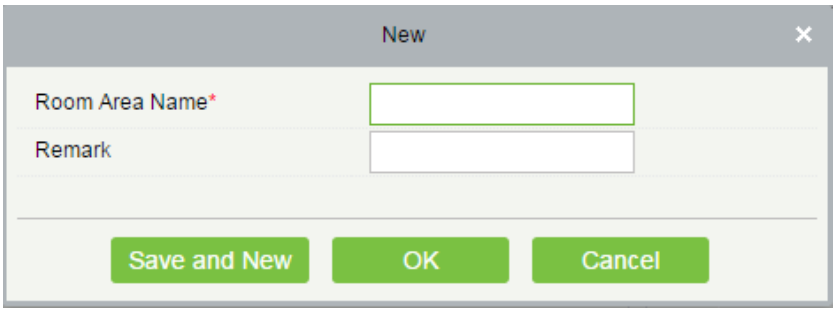
Select one or more guest rooms and delete them.
Only the guest rooms that has not been checked in or booked can be deleted.

- **Exporting guest room information**

Refer to Common Operations in Appendix.

6.2.5 Room Areas

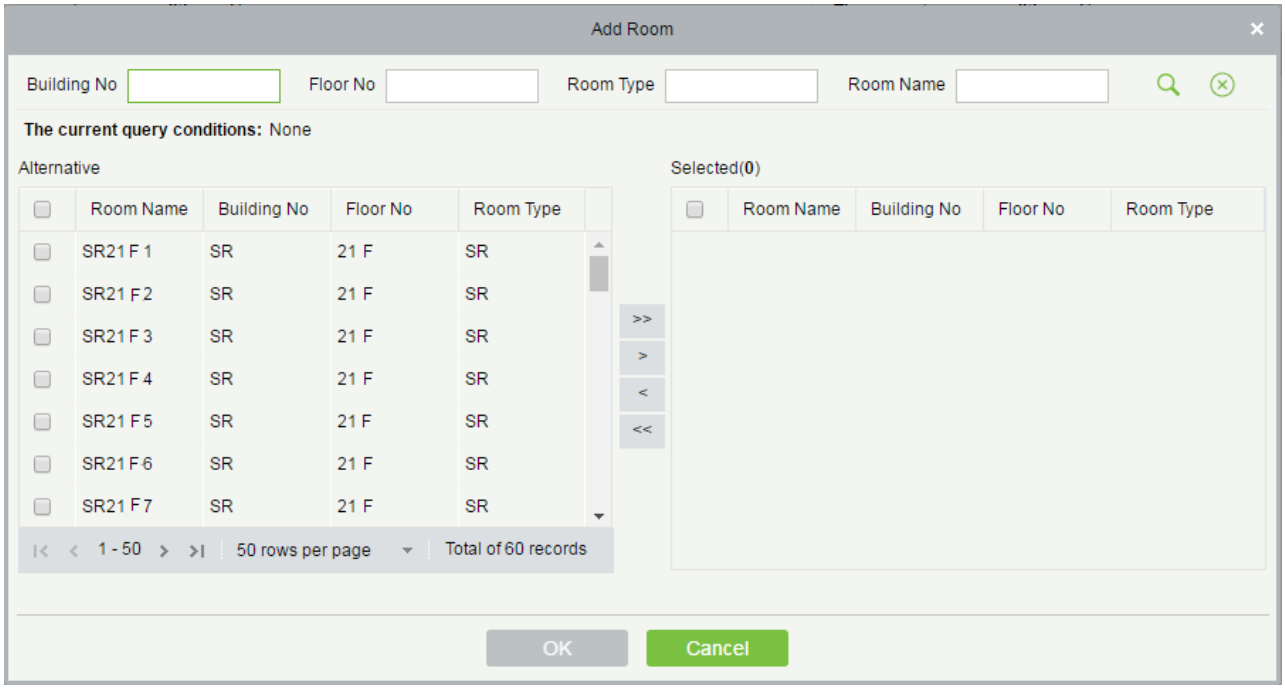
You can define a room area, issue a card for the room area, and associate the locks of the rooms in the area with the area, so that a hotel manager can use the card to manage all the guest rooms in the area.
Choose **Room Management** > **Room Area** > **New**. The page shown in the following figure appears.



Note:

Duplicate room area names are not allowed.

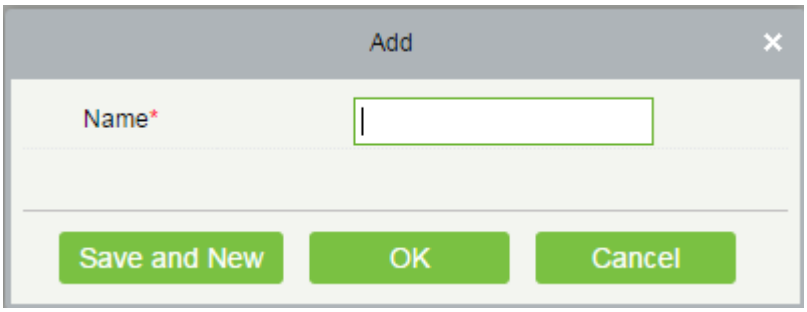
Click **Add Room** and then you can add rooms to the area. See the following figure.



6.2.6 Booking Methods

You can define methods for booking hotel rooms. During system installation, the basic booking methods are initialized by default and cannot be edited or deleted.

Choose **Room Management** > **Booking Method** > **Add**. The page shown in the following figure appears.



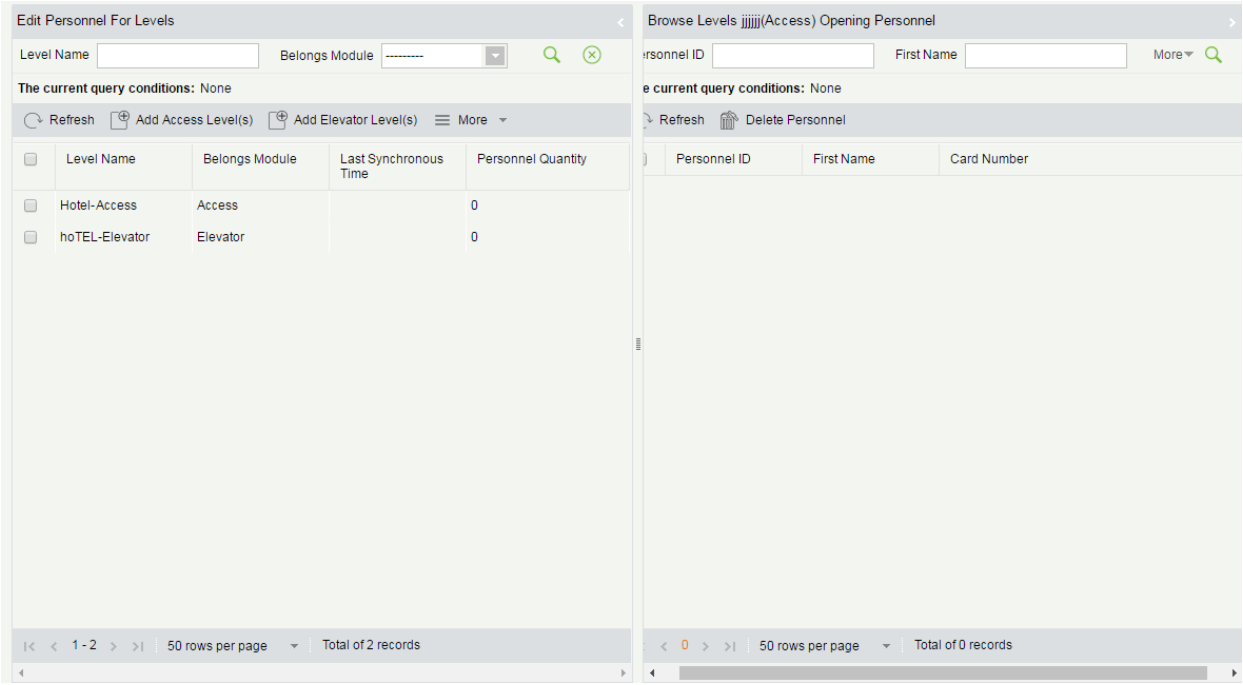
Note: Duplicate booking method names are not allowed. Unused booking methods can be deleted.

6.2.7 Access/Elevator Control Levels★

You can assign access/elevator control levels to cards issued using the hotel module. This allows a user to use the same card for the hotel module and the access/elevator control module. That is, a card for the hotel module can also be used to access all the devices covered by the specified access/elevator control level.

Note: This function and the **Edit Personnel For Levels** page are available only after you use the access control module and/or the elevator control module and obtain and activate a license.

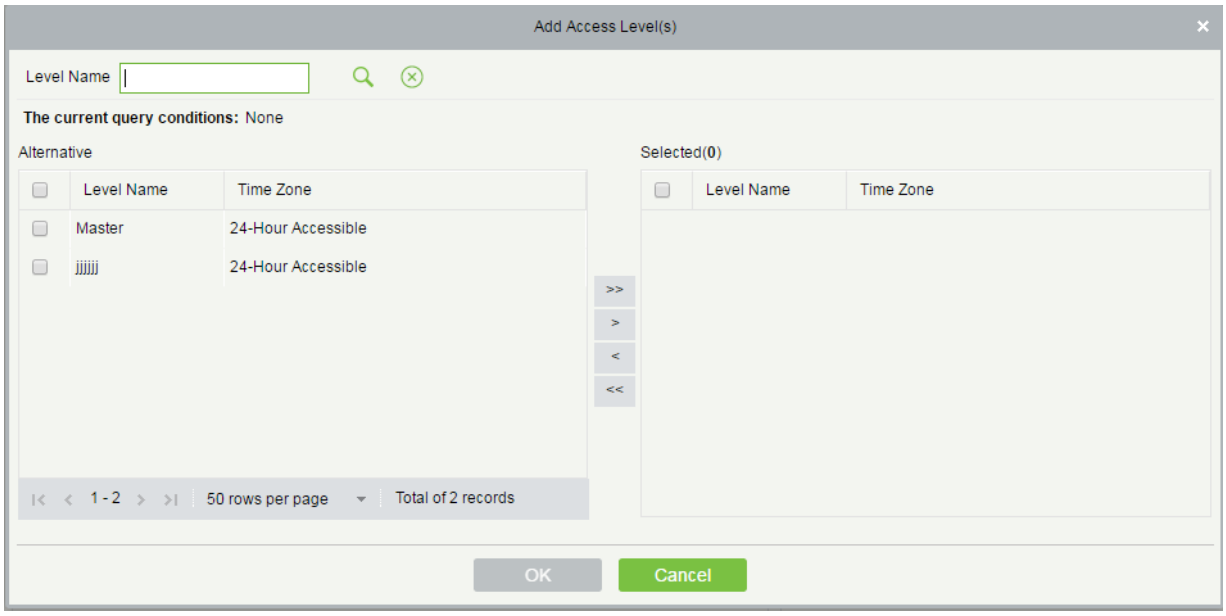
Choose **Room Management** > **Edit Personnel For Levels**. The page shown in the following figure appears.



You can add and delete access/elevator control levels, synchronize levels, browse personnel of levels, and delete personnel of levels. To delete personnel of a level, you need to deregister their cards instead of directly deleting them on this page, unless their cards are lost or another emergency occurs.

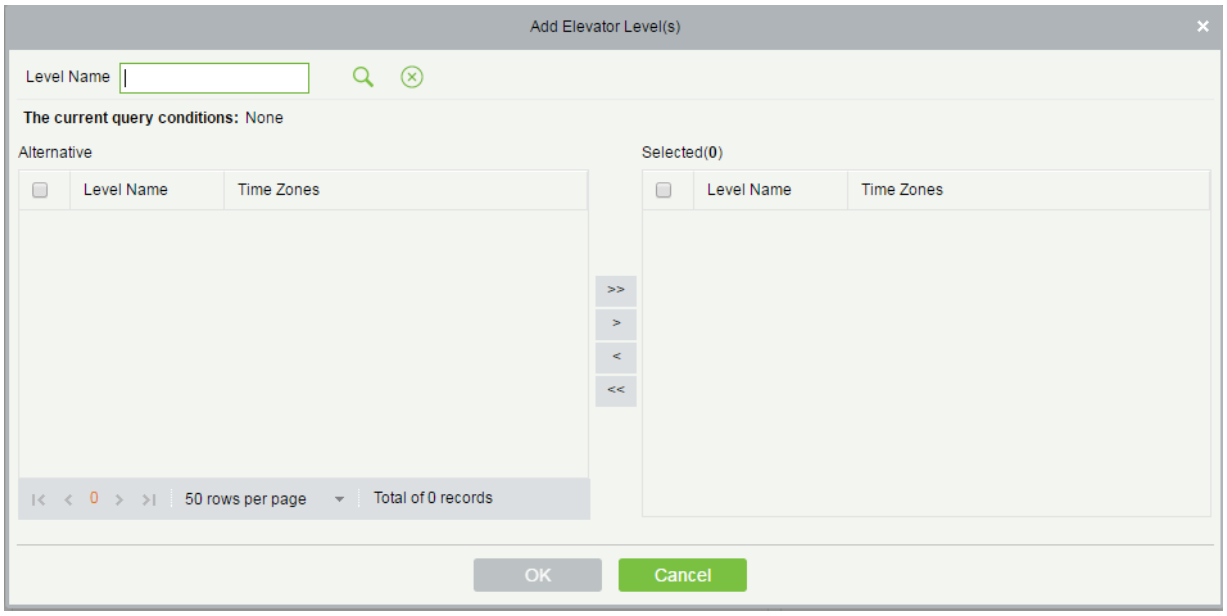
- **Adding a level**

Click **Add Access Level(s)**. The page shown in the following figure appears.



Select the access control level to be added and click **OK**. Add access control level **Floor 1 of Building A** to the hotel management level list. See the preceding figure. If you select this access control level in the **Access/Elevator Control** field when issuing a card, the card can get authenticated by all the access control devices on floor 1 of building A and unlock hotel rooms.

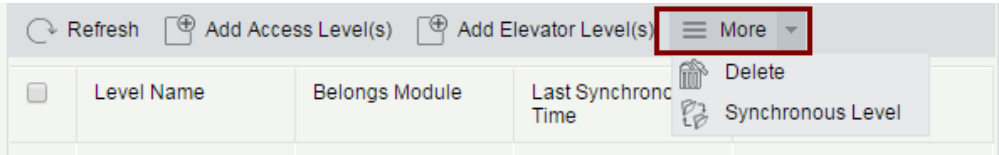
Click **Add Elevator Level(s)**. The page shown in the following figure appears.



Select the elevator control level to be added and click **OK**. Add elevator control level **Floor 6 of Elevator 1** to the hotel management level list. See the preceding figure. If you select this elevator control level in the **Access/Elevator Control** field when issuing a card, the card can get you to floor 6 by elevator 1 and unlock hotel rooms.

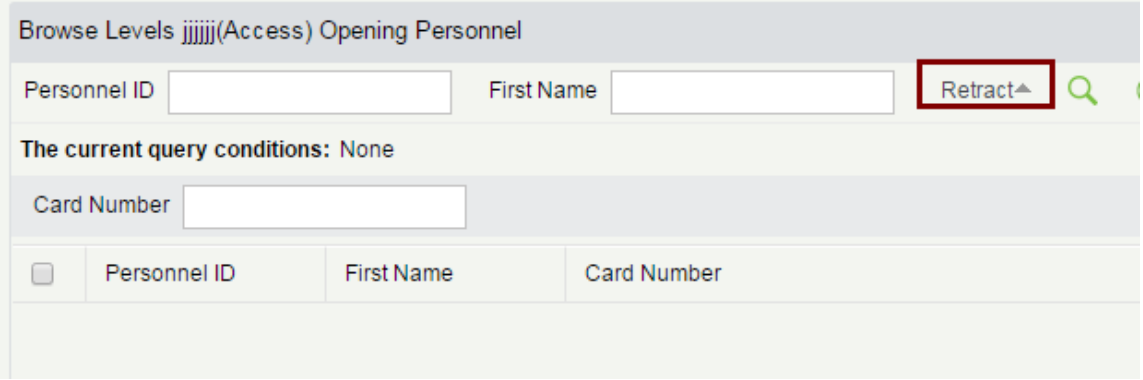
- **Deleting/synchronizing levels**

On the **Edit Personnel For Levels** page, select a level, click **More**, and choose to delete or synchronize the selected level.



- **Browsing/deleting personnel corresponding to levels**

When you select a level on the **Edit Personnel For Levels** page, information about the personnel corresponding to the level is displayed on the right. You can select the personnel to be deleted by clicking **More**, and delete the selected personnel. After being deleted, the personnel cannot access the devices covered by the level.



6.3 Card Service Center

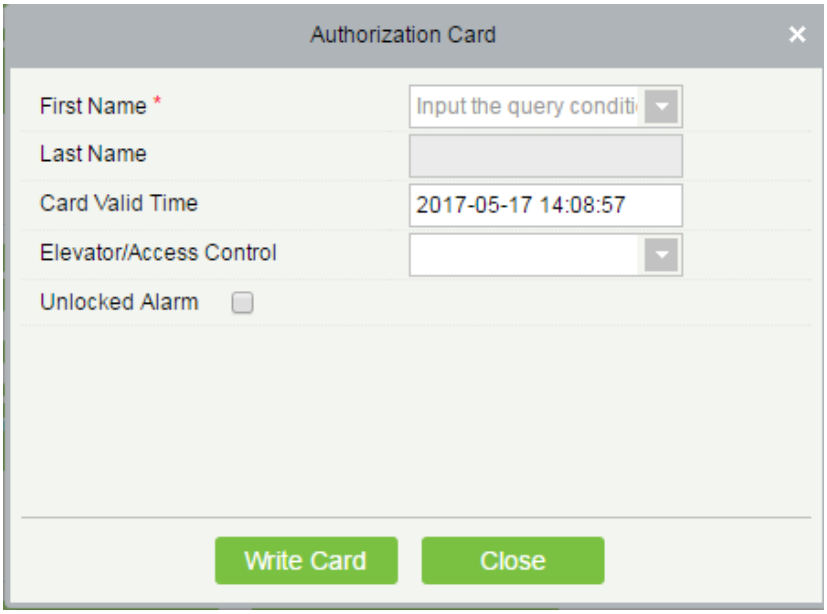
You can create different types of card for setting and managing room locks based on daily hotel business management requirements. Holders of the cards are employees of the hotel. You need to add the holders using the HR module and specify their departments using the hotel module, so that you can select the holders when issuing management cards.

6.3.1 Lock Management Cards

You can set the basic information, including authorization, time, room number, and area information about locks of the hotel.

1. Authorization card

You can authorize cards for hotel locks by binding cards with related hotel information to ensure card security. After authorization, the locks can be unlocked only by the authorized cards. They will emit alarms if other cards are used to unlock them.



Field description:

First Name: You can enter one or more characters contained in the surname or ID of a card holder to fuzzily find the card holder. A card holder must be a person who has been added using the HR module.

Card Valid Time: It specifies the expiration time of the card. Select a time as required. The default time is one day later than the current system time.

Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

Notes:

1. The **Elevator/Access Control** field is available only after the **Room management** field on the **Hotel Settings** page is selected. It is used to deliver the card ID to access/elevator control devices. For details about hotel settings, see section Hotel Settings.
2. For the access control devices and all elevator control devices that do not allow one person to hold multiple cards, bind only one card with one person. That is, you can select only one card for one **Elevator/Access Control** option when issuing cards to card holders. As shown in the preceding figure, if **Elevator/Access Control** is set to **Floor 1 of Building A** (all the access control devices on floor 1 of building A do not allow one person to hold multiple cards) when an authorization card is issued to a card holder, only the first card can be assigned the permission to access floor 1 of building A. You cannot set **Elevator/Access Control** to **Floor 1 of Building A** when issuing any other card to the card holder.
3. If an access control device allows one card holder to hold multiple cards, you can assign one access/elevator control level to multiple cards for the same card holder. You can select that level again when issuing any other types of card or continuous cards to the card holder.
4. The preceding three points regarding access/elevator control are applicable to all the cards of the hotel module described in this document.
5. The models and firmware version numbers of the access control devices that allow one person to hold multiple cards include:

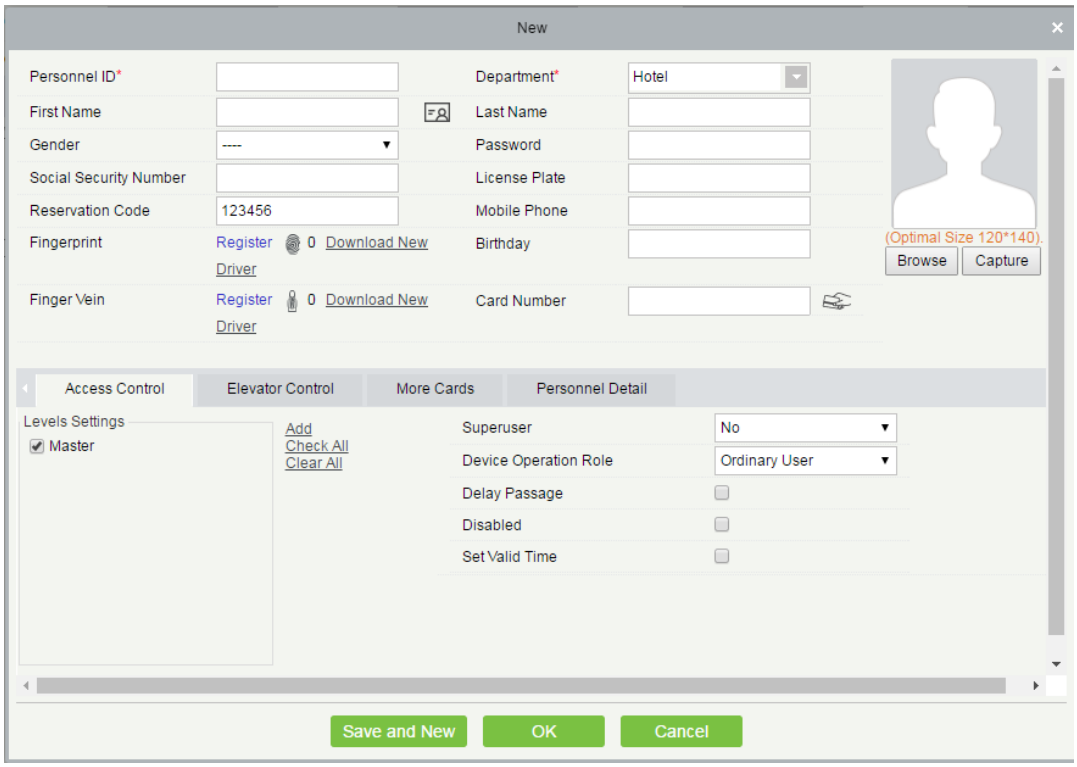
   InBio Pro Series: AC Ver 5.7.7.3030 Mar 23 2017 and above version.

Unlocked Alarm: After selecting this check box, you can specify the number of times to emit an alarm.

After the configuration, put a card to be written in the card writing area of the card writer and click **Write Card**.

- **Adding hotel personnel**

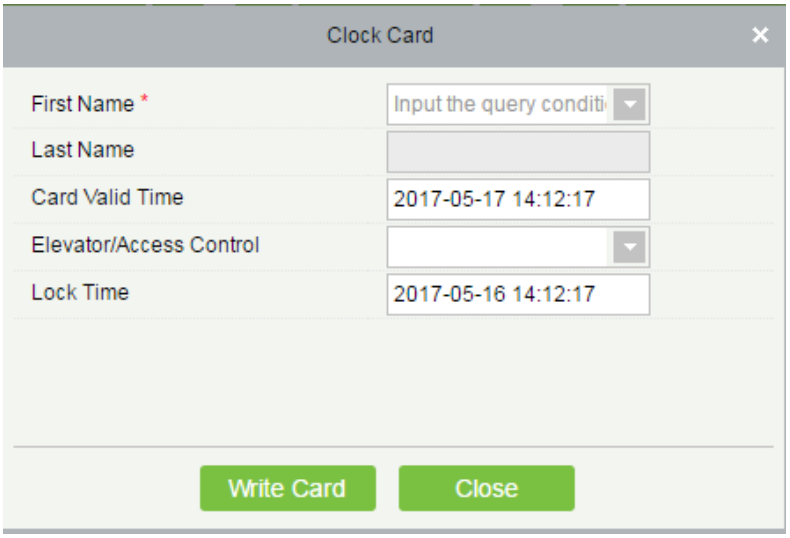
Choose **HR** > **Personnel Management** > **Personnel** > **Add**. The page shown in the following figure appears.



Enter personnel information, select a hotel department, and click **OK**. You can select added personnel in the card issuing module.

2. Clock card

A clock card can be used to unlock rooms within its validity period. After configuration, synchronize the time of room locks with the time of the computer system. Otherwise, an alarm of card expiration may be triggered when you punch the card.

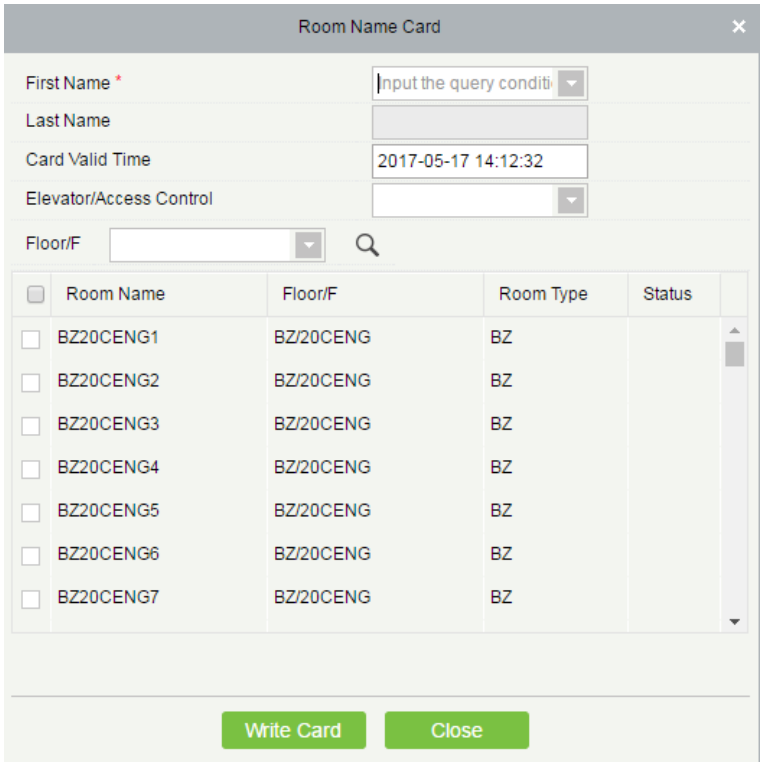


Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

After the configuration, put a card to be written in the card writing area of the card writer and click **Write Card**.

3. Room name card

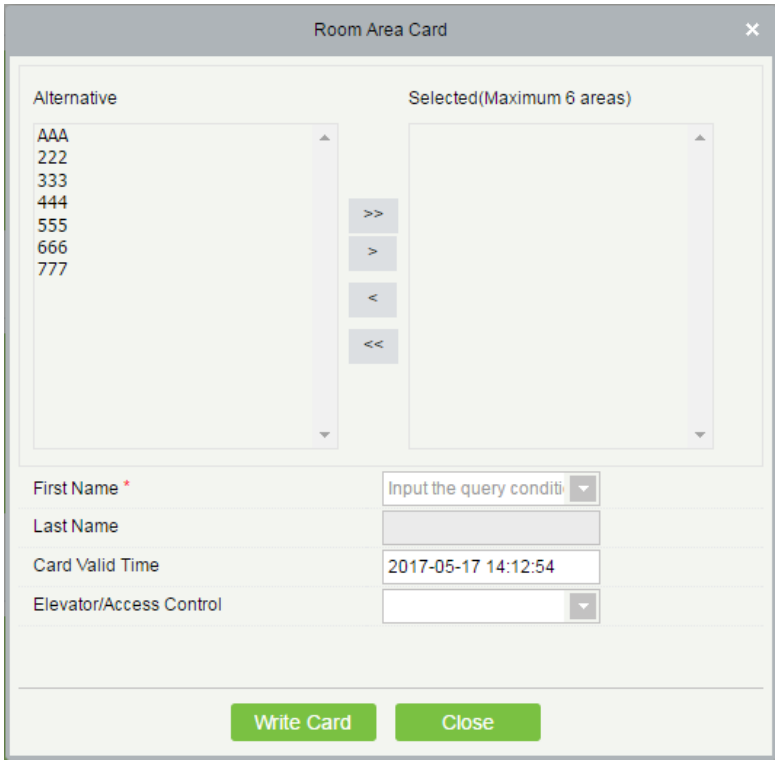
A room name card is used to unlock rooms with specified room names. You can select multiple rooms to issue room name cards in batches.



Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

4. Room area card

A room area card is used to unlock rooms in a specified area. If a room is within the specified area, the card can unlock the room.



Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

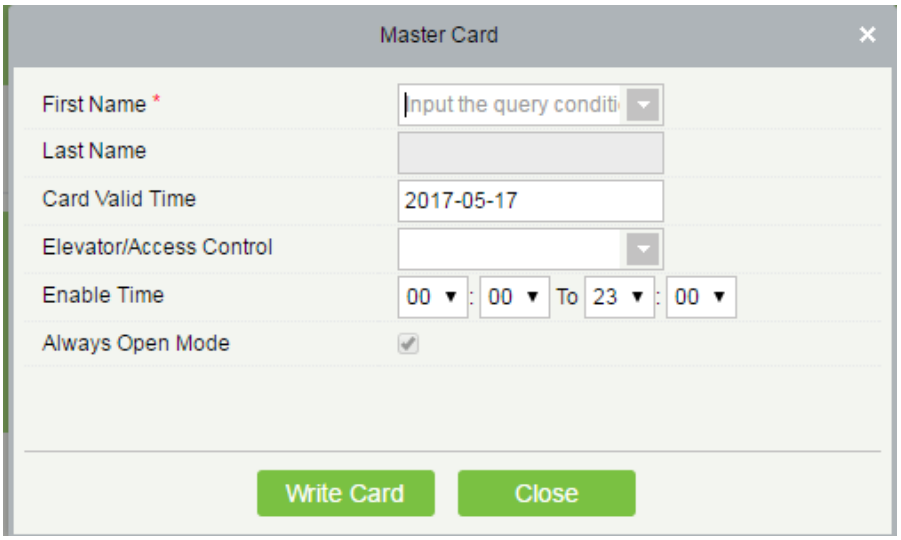
Note: A maximum of 6 areas can be selected for one room area card.

6.3.2 Personnel Cards

You can create various access/elevator control cards, such as master cards and emergency cards for hotel personnel to manage hotel services.

1. Master card

A master card can be used to unlock all the rooms of the hotel within its validity period. By default, it is in Always Open mode.



Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

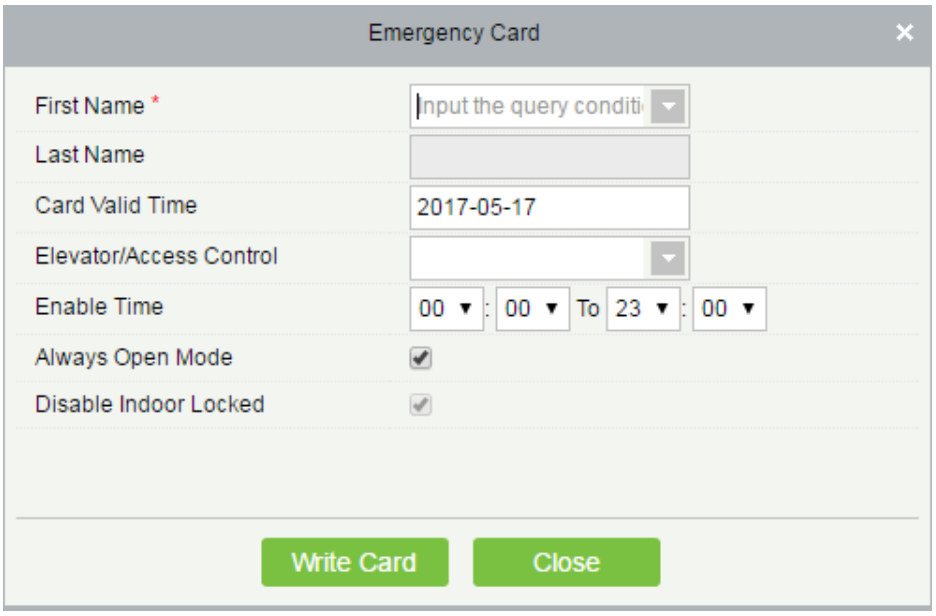
If you select Always Open Mode, the unlocked rooms are kept unlocked.

Set **Card Valid Time** and **Enable Time** as well. The card can unlock rooms only within the specified periods.

After the configuration, put a card to be written in the card writing area of the card writer and click **Write Card**.

2. Emergency card

A master card can be used to unlock all the rooms of the hotel within its validity period. By default, **Disable Indoor Locked** is selected. You can specify whether to enable the Always Open mode.



Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

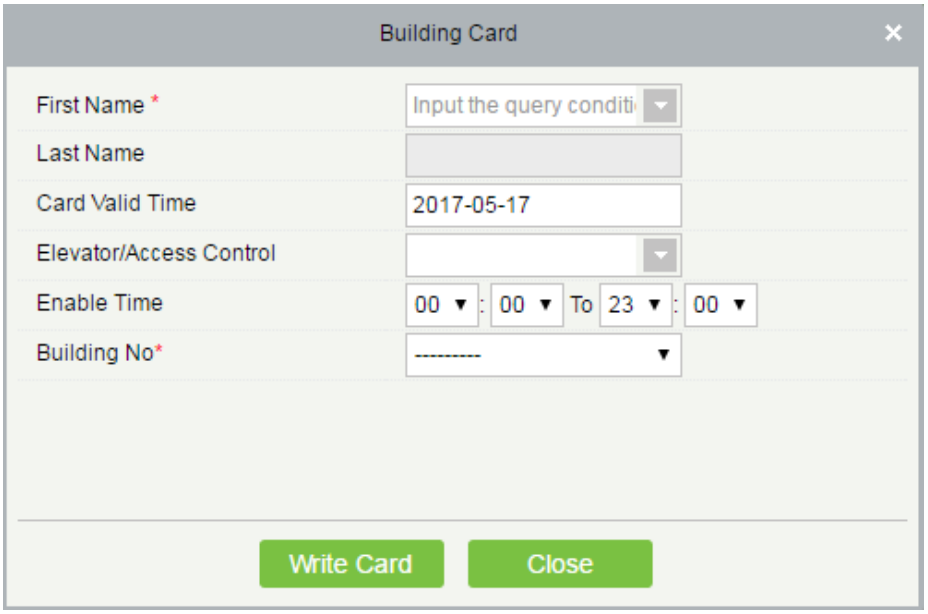
If you select **Always Open Mode**, the unlocked rooms are kept unlocked.

To disable **Always Open Mode**, you need to use a card that can unlock rooms, such as a building card or floor card.

Disable Indoor Locked is selected, which means that the card can open rooms even though the rooms are locked from inside.

3. Building card

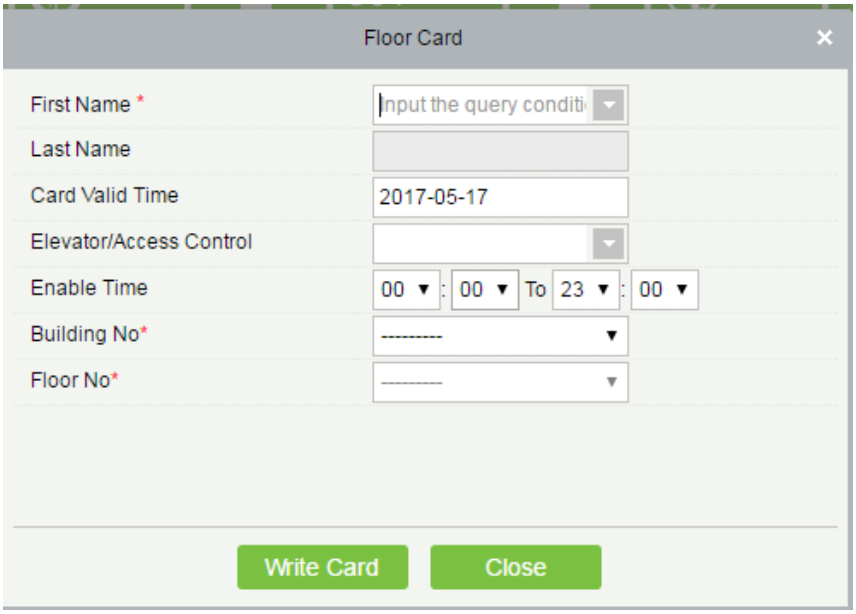
A building card can be used to unlock rooms in a specified building in common unlocking mode within its validity period.



Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

4. Floor card

A floor card can be used to unlock rooms on a specified floor in common unlocking mode within its validity period.

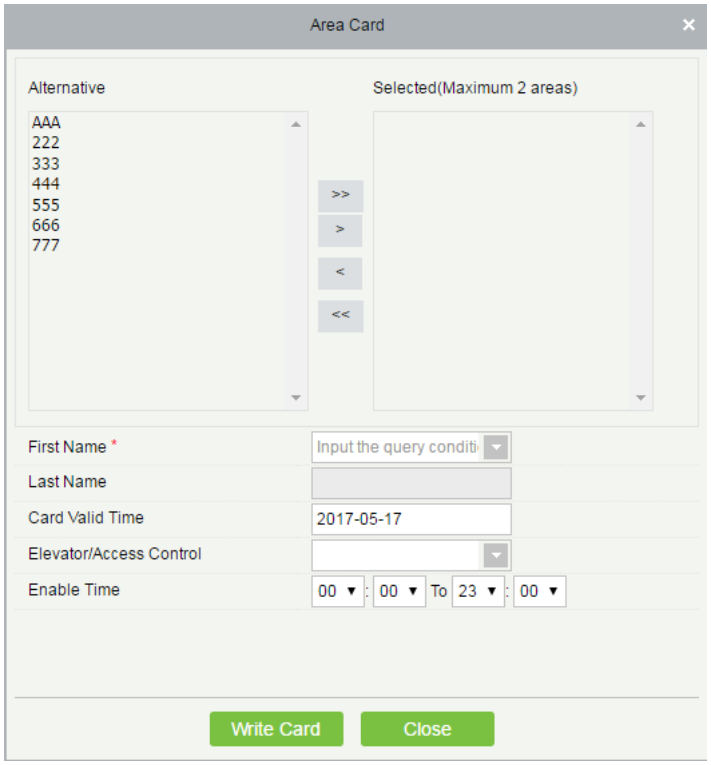


Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding

to the elevator/access control level.

5. Area card

A floor card can be used to unlock rooms in a specified area in common unlocking mode within its validity period.



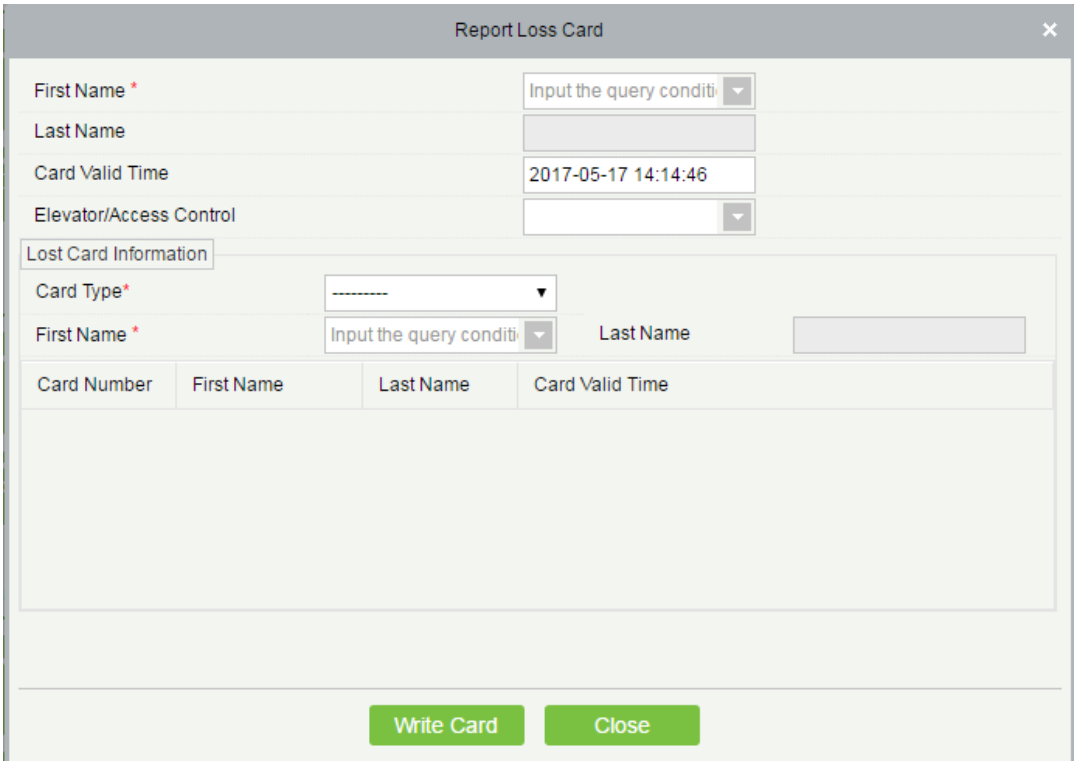
Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

6.3.3 Maintenance Card

A maintenance card can be used to maintain and manage room locks of the hotel.

1. Report loss card

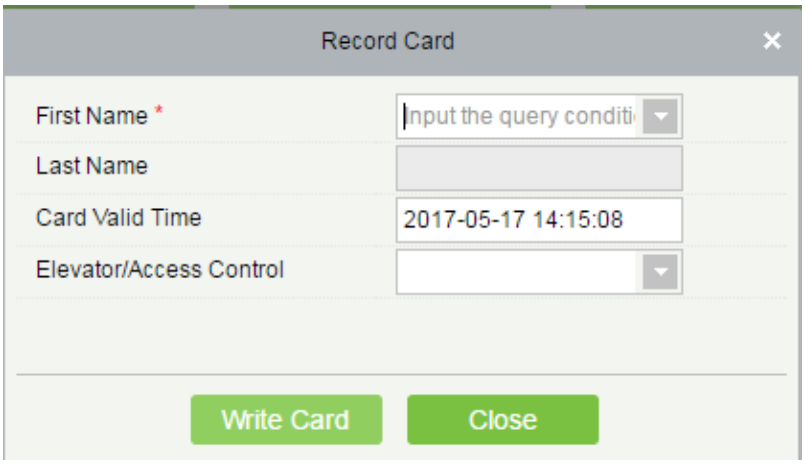
A report loss card is a card that is invalidated and obsolete (usually due to loss or damage of the card) during its validity period.



Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

2. Record card

A record card can be used to read unlocking records from locks within its validity period. Only S70 Mifare cards can be used as record cards.

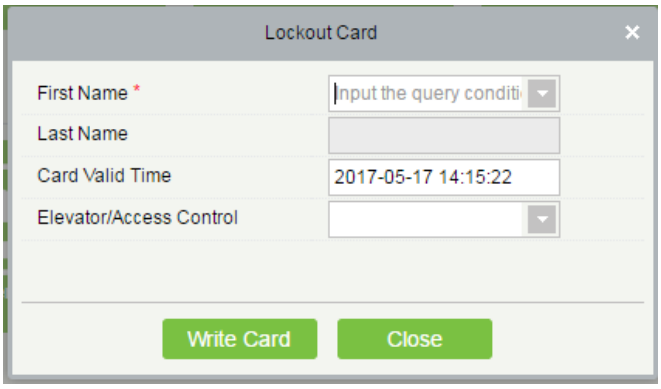


Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

3. Lockout card

A lockout card is a special card used to lock and protect a scene in a room in case of an emergency. Once lockout is implemented, the room can no longer be unlocked by all the cards that can originally unlock it before the cards are

re-authorized.



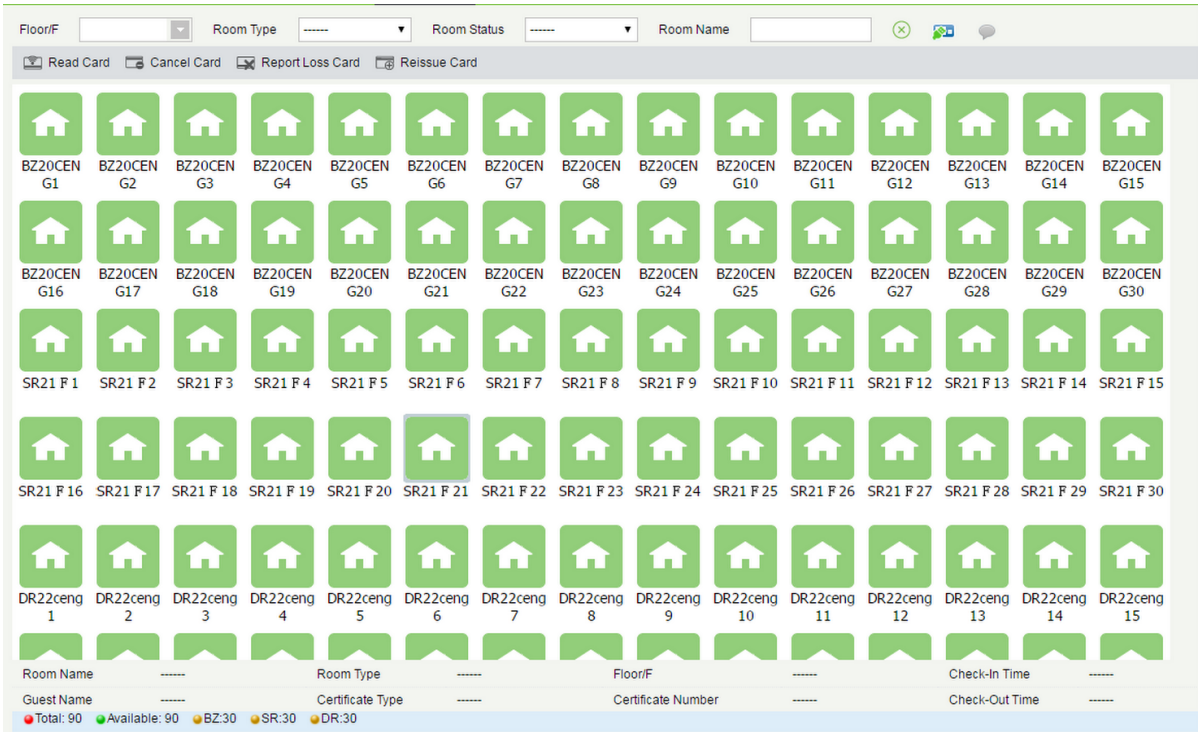
Elevator/Access Control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the card can not only unlock the specified room, but also access the devices corresponding to the elevator/access control level.

6.4 Hotel Management

6.4.1 Reception Center

The function allows users to handle room services and check the hotel room occupancy, such as the total number of rooms, number of available rooms, and number of available rooms of a specific room type.

See the figure below.



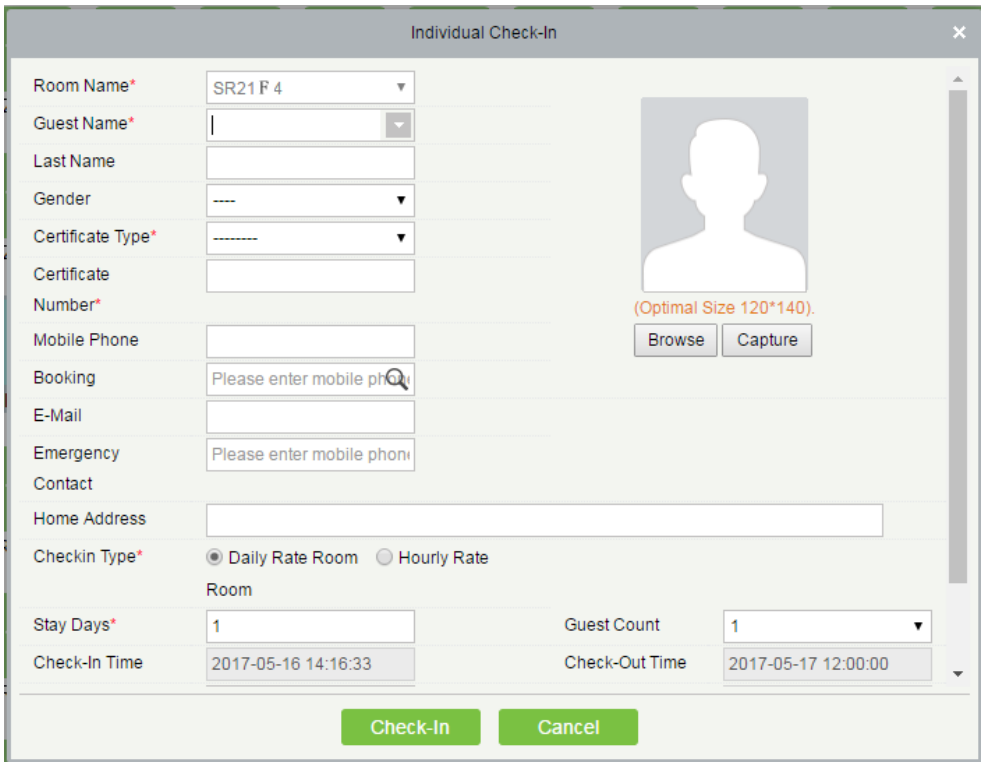
Description of room icons

	Vacant		**Extended**		**Individual check-in**		**Group check-in**
	Out of service		**Under maintenance**		**To be cleaned**		

1. Individual management

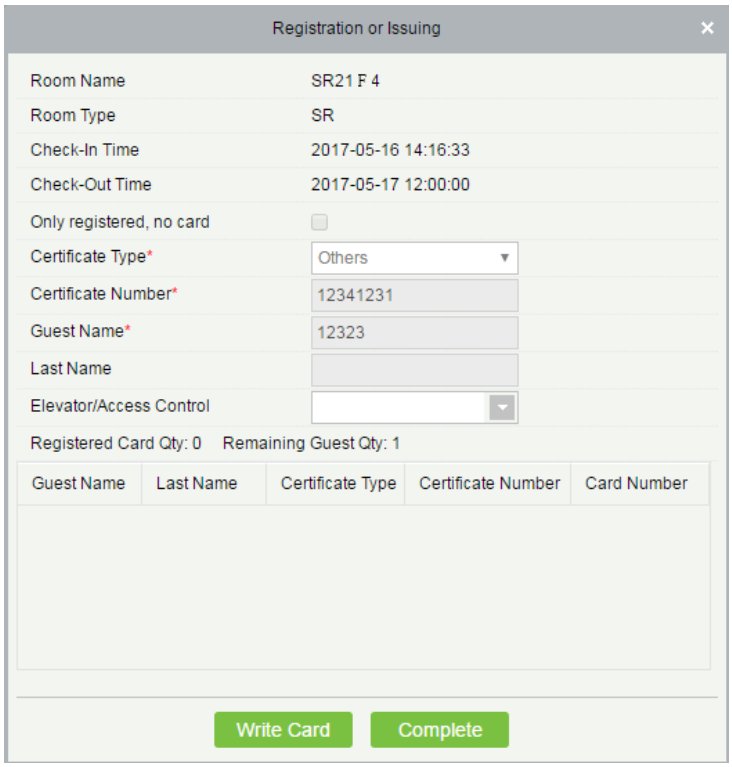
- **Individual check-in**

1) Double-click or right-click a vacant icon and choose **Individual Management** > **Individual Check-In**. A page as shown in the following figure appears.



Reservation query: Enter the mobile phone number used for reservation to query the reservation information.
Stay days: Enter the number of days that the guest wish to stay.
Discount: Discount on the room cost, for example, at a 10% discount, the room cost will be 1*120*0.9 + 150=258 in the example in the previous figure.
Amount due: Amount to be paid at check-in, including the room cost and the deposit.

2) After the information in the **Individual Check-In** page is filled in, the **Registration or Issuing** page appears

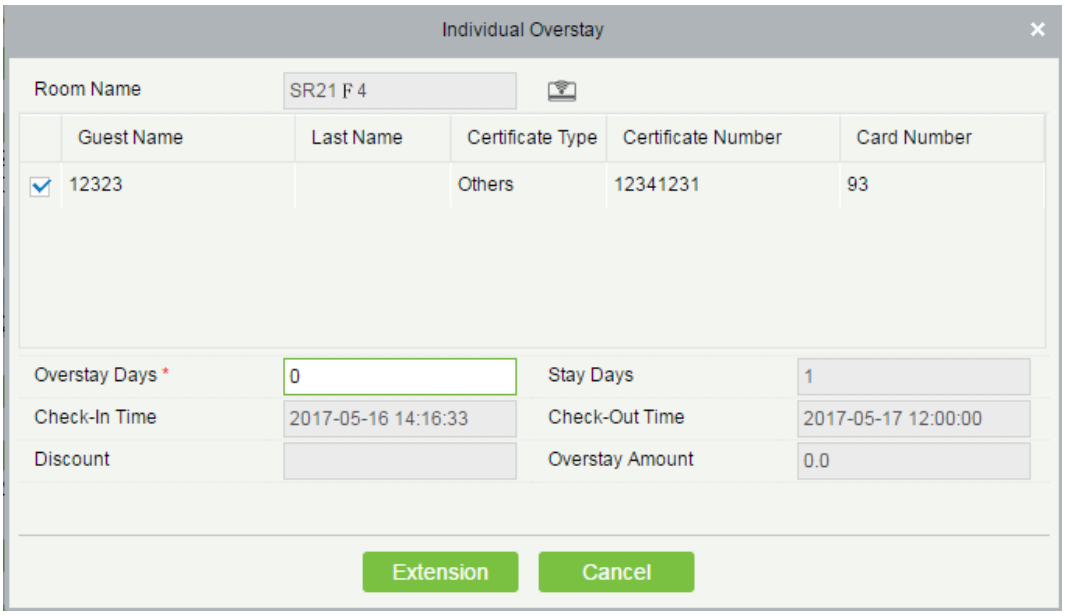


Elevator/access control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the room card can open not only the specified room, but also the devices corresponding to the elevator/access control level.

Note: Issue at least one card for each room. The card must be issued for the registered guest. When issuing the first guest card, the **Only registered, no card** option is not available. After the first guest card is issued, you can select **Only registered, no card** as required. The option indicates that the guest is registered only and does not hold a guest card.

- **Individual overstay**

1) Right-click a checked-in room icon and choose **Individual Management** > **Individual Overstay**. The page as shown in the following figure appears.



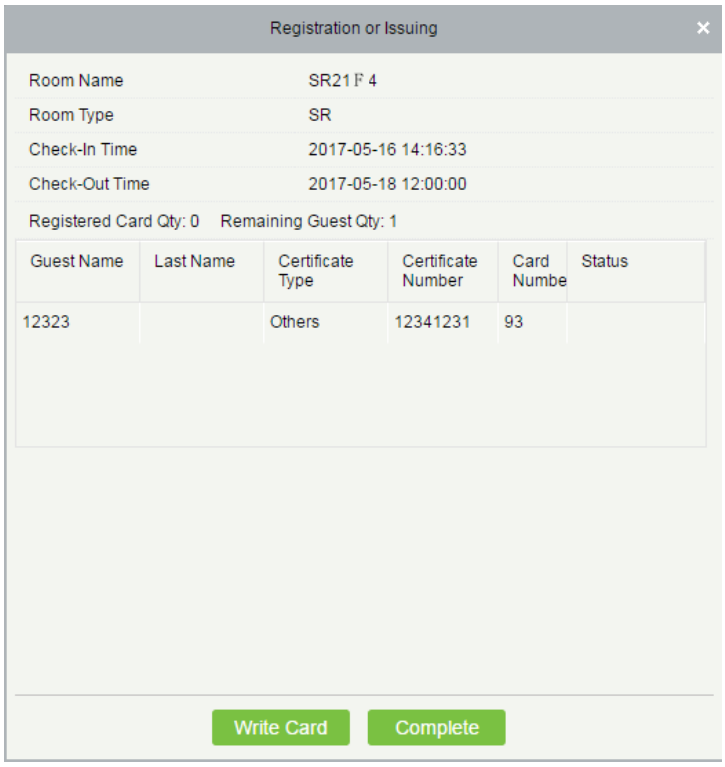
Notes: a. If the number of overstay days conflicts with the room reservation, extension is not allowed.

b. Choose the guest that needs extension for service processing.

c. The discount rate cannot be modified for overstay.

d. **Overstay amount** shows the amount to be paid for overstay.

2) After the information in the **Individual Overstay** page is filled in, the **Registration or Issuing** page appears, as shown below.

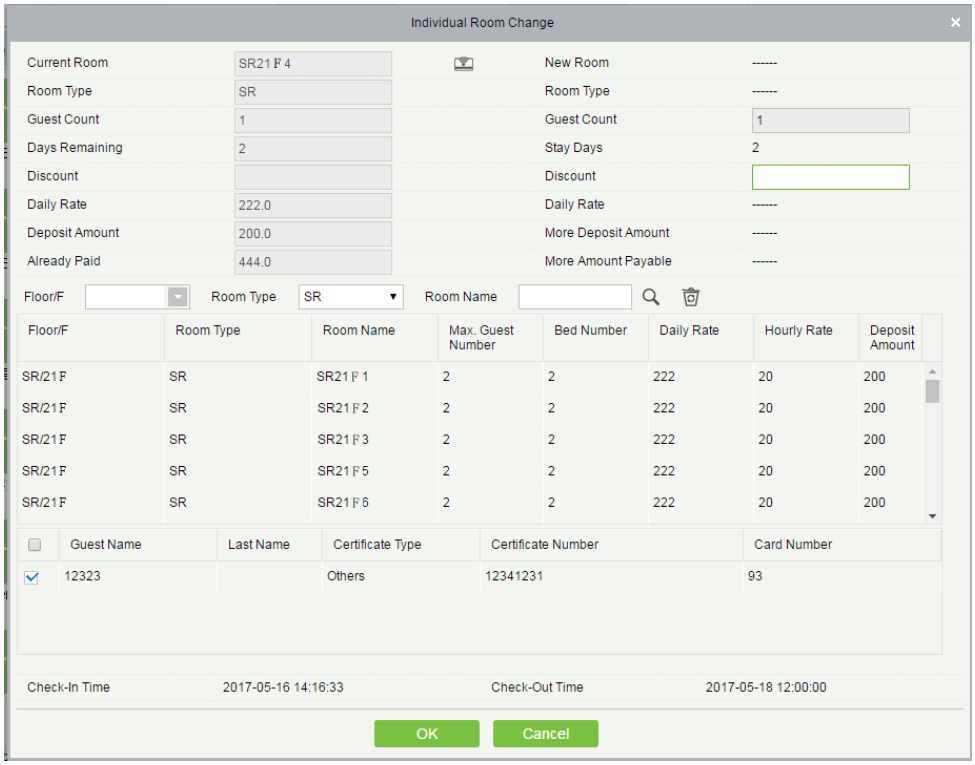


Notes: a. Re-issue the guest card for the overstay guest. The card must be the exact guest card issued during check-in; otherwise, card issuance fails.

b. You can click Write Card to automatically write cards for overstay in circulation until all overstay cards are written in an interval of 3 seconds.

- **Individual room change**

1) Right-click a room checked-in icon and choose **Individual Management** > **Individual Room Change**. The page as shown in the following figure appears.



Guest Count: Number of guests that require room change.

Notes: a. You can check the room information by reading the card.

b. The maximum number of guests of the selected guest room must not be smaller than the maximum number of guests of the original guest room.

c. Guests without a card are not allowed to change the room alone.

d. If the original guest room is left with a guest without a card during room change, the system asks whether to change the room for the guest without a card as well. If you choose **No**, the room change service fails to proceed.

e. If the new guest room is reserved, the conflict information is displayed. You can choose whether to proceed the service.

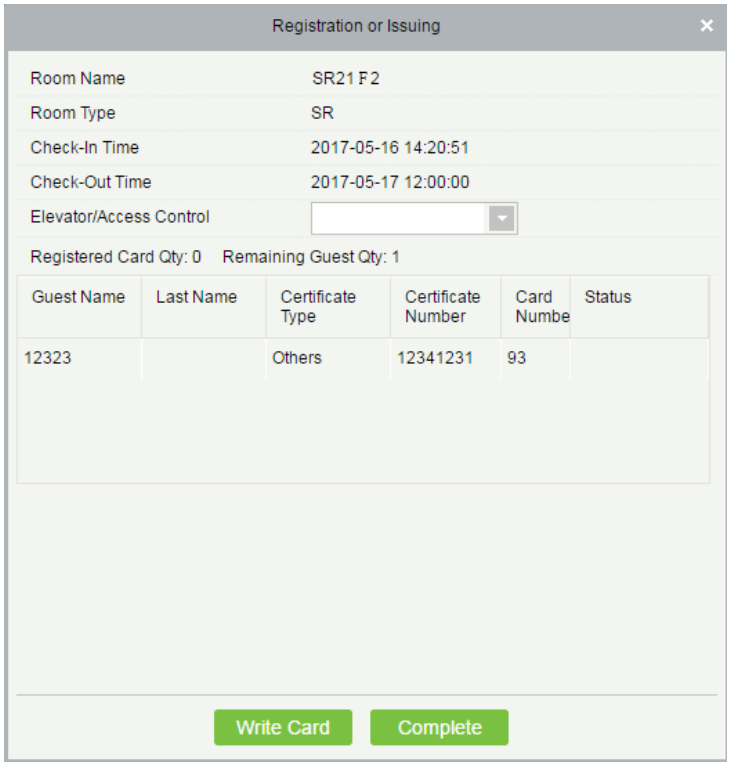
f. The discount can be set for room change.

g. If the deposit required for the new guest room is greater than that of the original guest room, the guest needs to make up the deposit. If the deposit required for the new guest room is smaller than that of the original guest room, all of the deposit is returned at check-out.

h. If the rate of the new guest room is greater than that of the original guest room, the guest needs to make up the room cost. If the rate of the new guest room is smaller than that of the original guest room, the overpaid amount is returned at check-out.

2) After the information is filled in for room change, click **OK**, and the **Registration or Issuing** page appears, as

shown below.

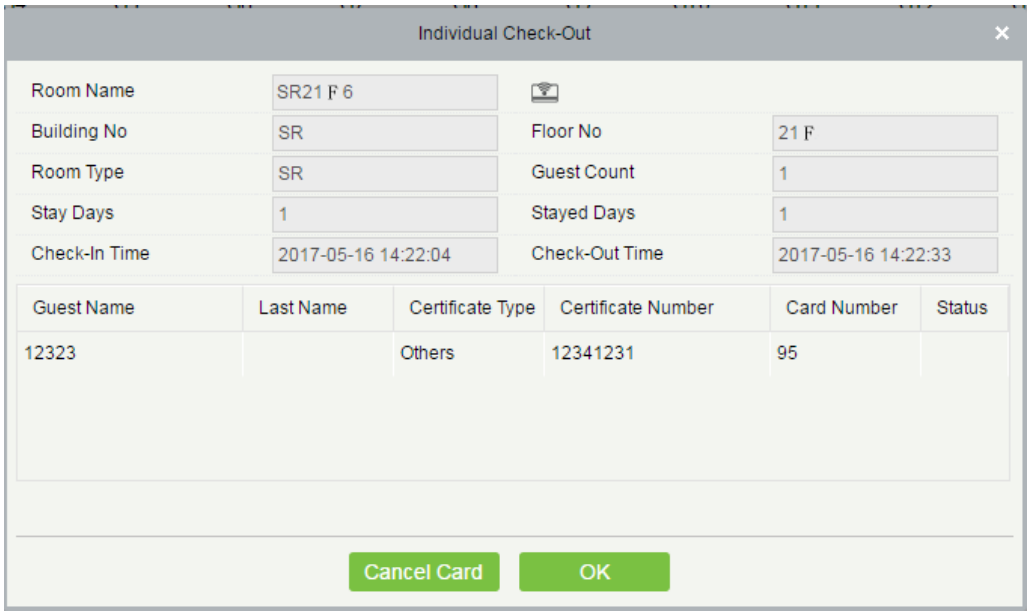


Elevator/access control: Click the drop-down list box to select an elevator/access control level. After the parameter is specified, the room card can open not only the specified room, but also the devices corresponding to the elevator/access control level.

Note: You can click **Write Card** to automatically write cards for all room changes in circulation until all room change cards are written.

- **Individual check-out**

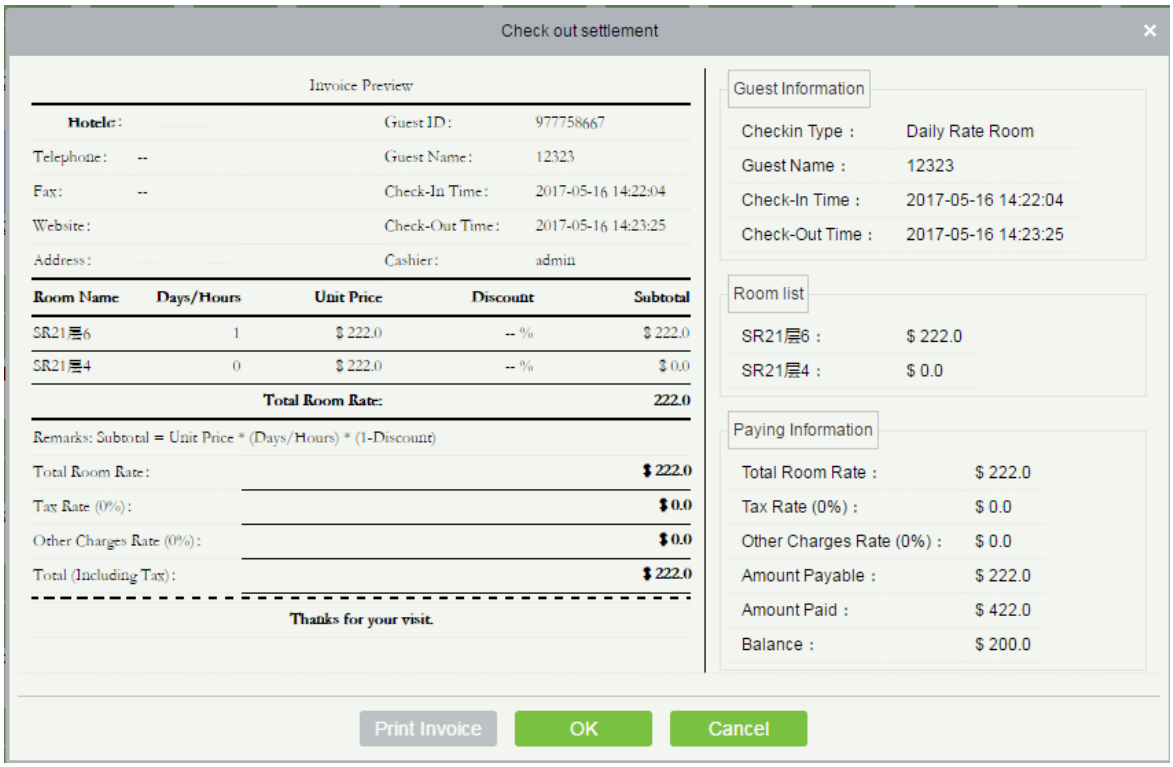
Right-click a checked-in room icon and choose **Individual Management** > **Individual Check-Out**. The page as shown in the following figure appears.



Cancel Card: Check whether the card to be cancelled is the guest card matches the current guest room, cancel the card if it matches the guest room, and display the notification if it does not match.

Note: When cards are cancelled one by one, the number of guests checked in is reduced. When there is no card holder, the **Cancel Card** button is unavailable.

Click **OK**, and the C**heck out settlement** page appears, as shown below.

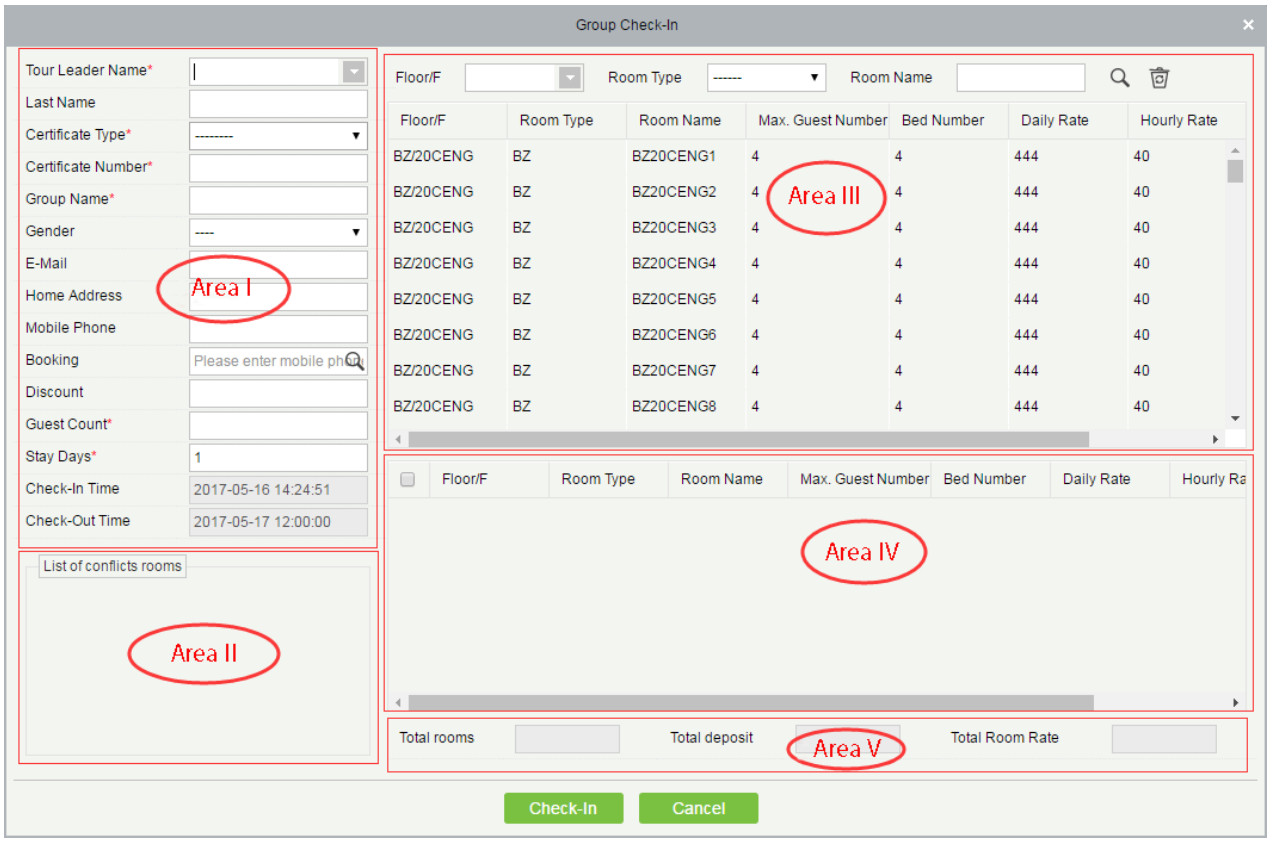


2. Group Management

- **Group check-in**

1) Right-click a checked-in room icon and choose **Group Management** > **Group Check-In**. The page as shown

in the following figure appears.



Reservation query: Enter the mobile phone number used for reservation and click to query for all guest rooms reserved with the mobile phone number.

Page description:

Area I: Allows you to enter the group check-in information.

Area II: Shows the reservation information of the current room. If the room has been reserved, the reservation information is displayed in the list in Area II. If the reservation conflicts with the check-in time, check-in cannot be processed.

Area III: Displays the list of available guest rooms (and you can double-click a room to add it to Area IV).

Area IV: Displays the reservation and the guest rooms selected in Area III.

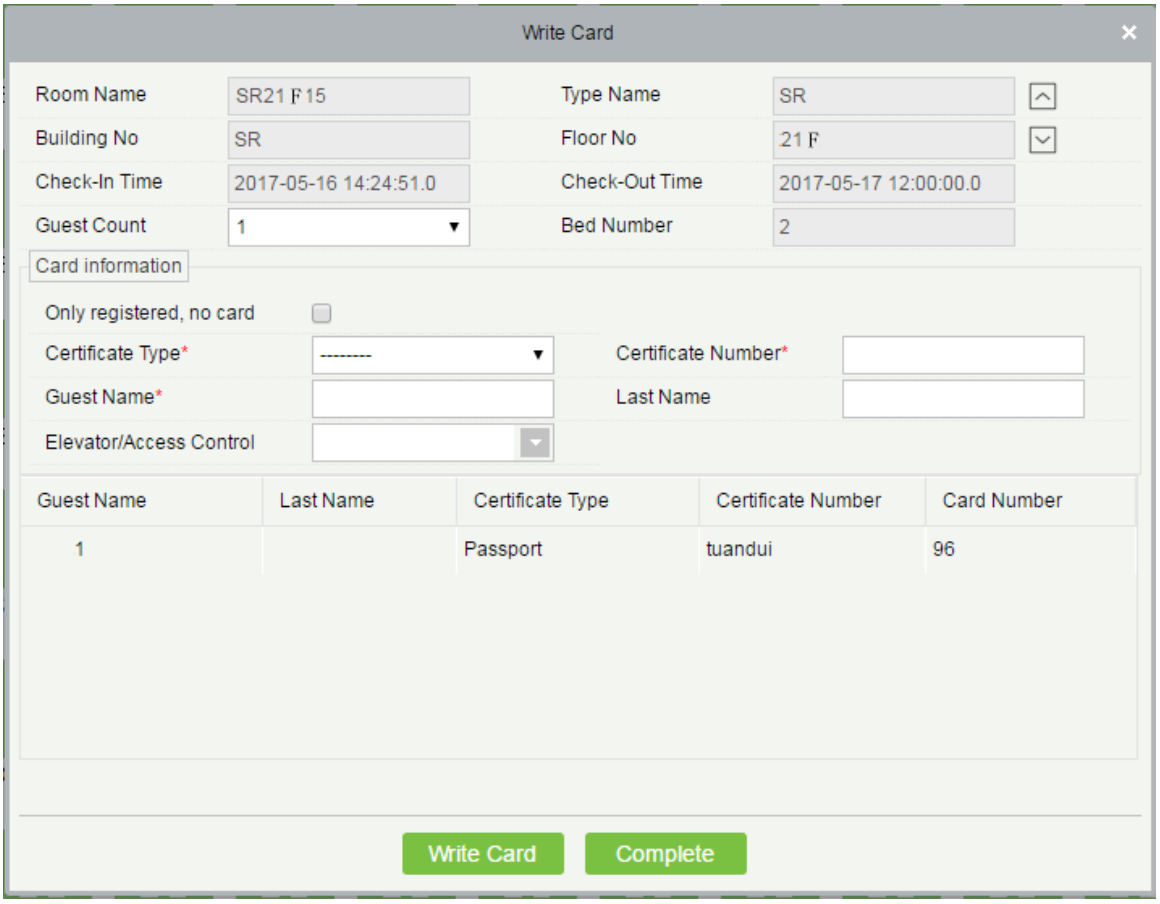
Area V: Shows the deposit amount and room cost for the group check-in.

Notes:

a. If the stay period overlaps with the reservation period, the **Check-In** button is unavailable and check-in is not allowed.

b. If the number of check-in guests is greater than maximum number of guests for all guest rooms in total, the **Check-In** button is unavailable and check-in is not allowed.

2) Click **Check-In**, and the **Write Card** page for group check-in appears, as shown below.



Guest Count: Number of guests checked in for the room. The number must not exceed the maximum number of guests allowed for the room.

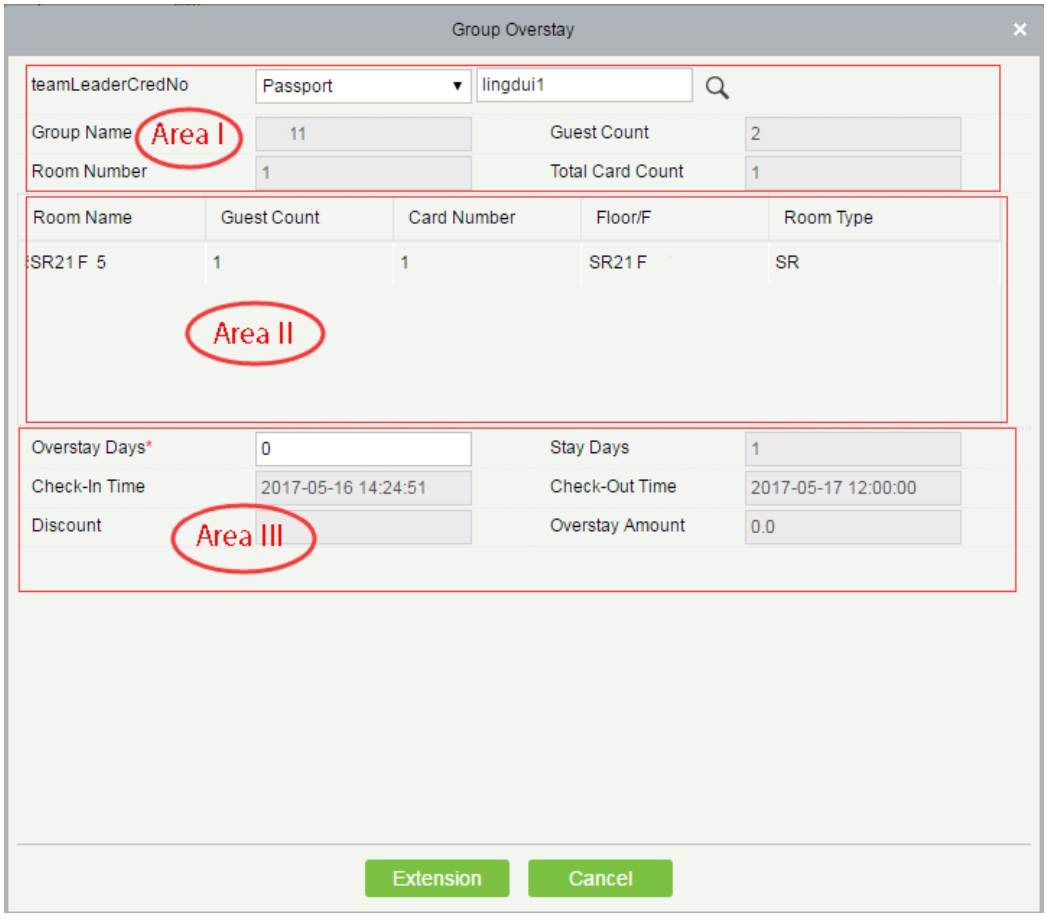
Only registered, no card: If this option is selected, only the guest information is registered and no card is issued for the guest.

Elevator/Access Control: If the access control or elevator control module exists, and the **Elevator/Access Control** checkbox is selected in **Hotel Settings**, the option will be available and you can assign access control or elevator control level to a card. For details about hotel settings, see section Hotel Settings.

Note: You can click ⌃ or ⌄ to go to the previous or next room.

- **Group Overstay**

1) Right-click a checked-in room icon and choose **Group Management** > **Group Overstay**. The page as shown in the following figure appears.



Page description:

Area I: Information about the rooms checked in by the group and the guest information.

Area II: List of reserved guest rooms.

Area III: Check-in information of the group.

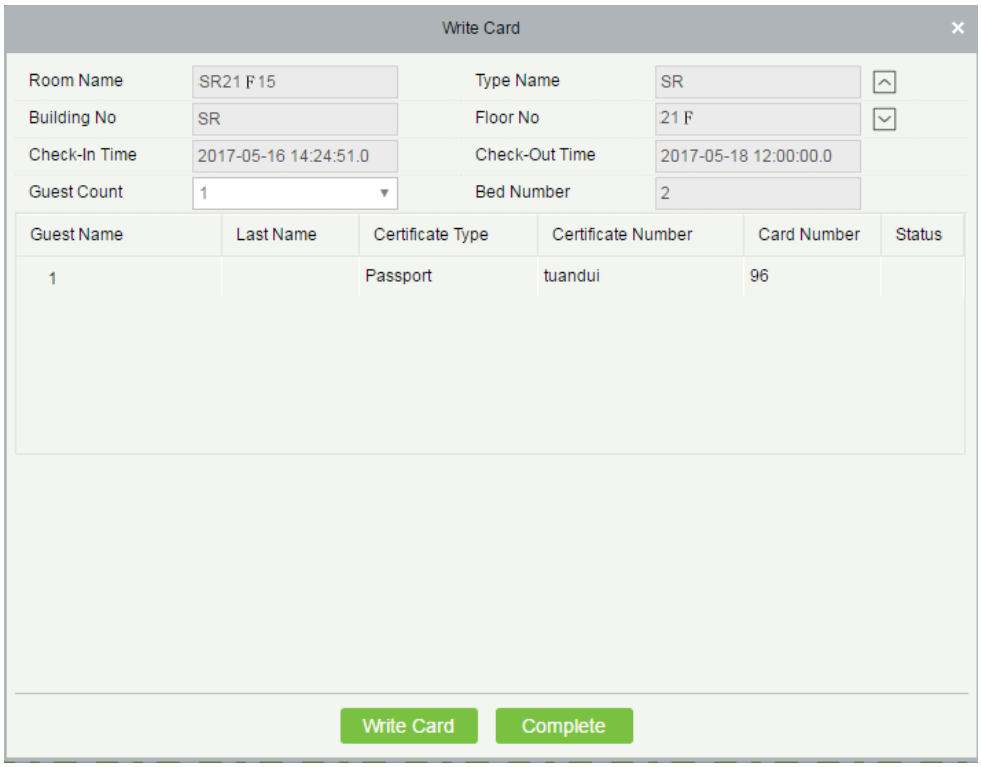
Notes:

a. The overstay period cannot overlap with the reservation period; otherwise, the **Extension** button is unavailable.

b. By default, the stay period is extended for the whole group.

c. The overstay period is one day in the minimum. For a special condition, the overstay days can be set to **0**.

2) Click **Extension**, and the **Write Card** page for group overstay appears, as shown below.



Notes:

Re-write all cards issued to the group members for overstay.

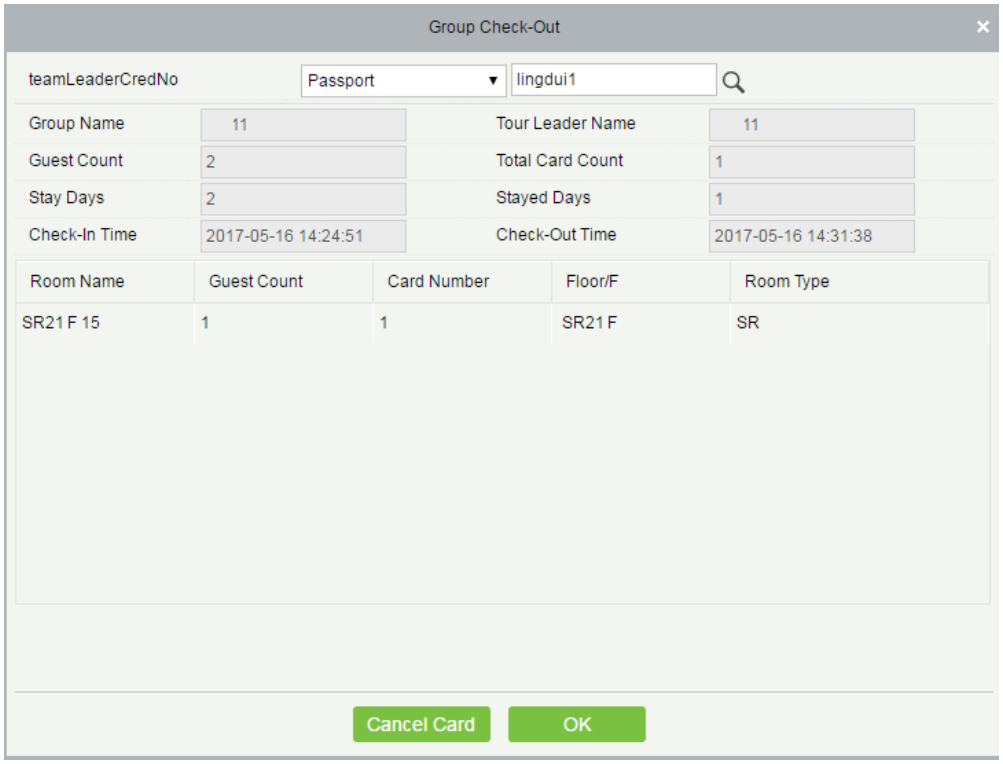
When you click **Write Card**, all cards are written for the rooms one by one in a cycle at an interval of 3 seconds.

The card issued during guest check-in is required for re-writing. In the case of card damage or missing, report of loss and make-up must be carried out for the card before reissuance.

You can click ⌃ or ⌄ to switch to the previous or next room.

- **Group check-out**

Right-click a checked-in room icon and choose **Group Management** > **Group Check-Out**. The page as shown in the following figure appears.



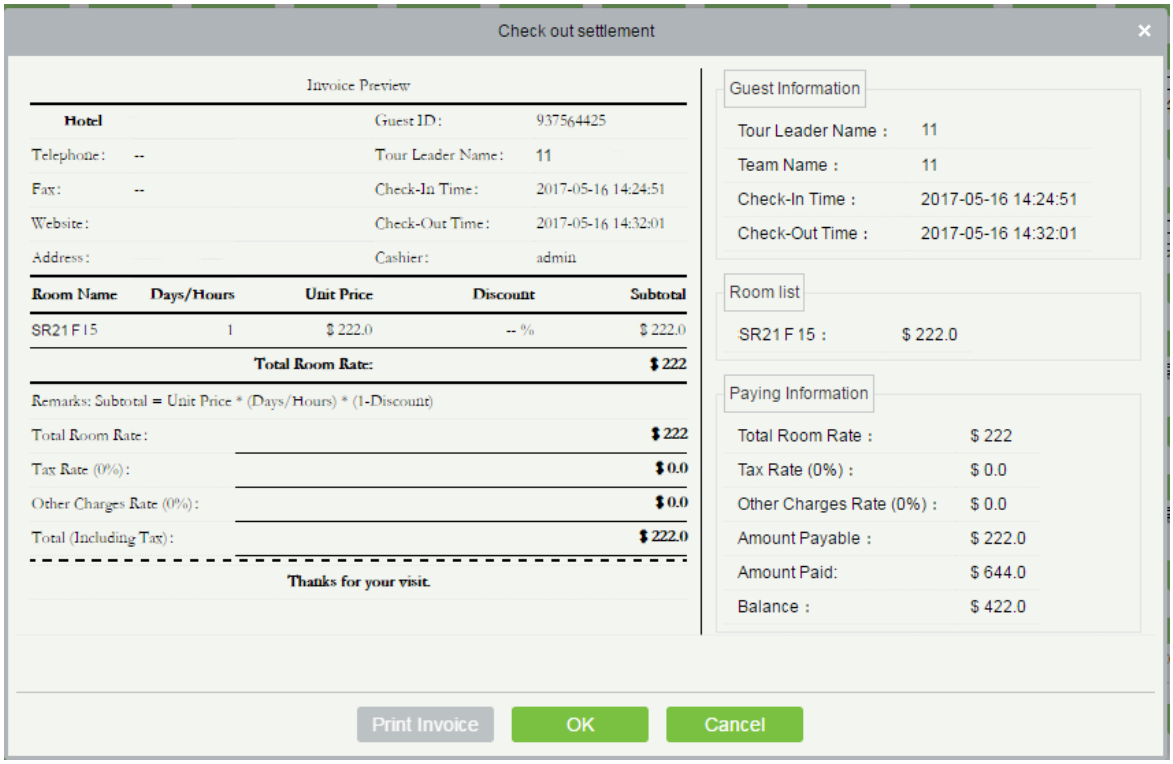
Notes:

a) You can choose to check out only some of the rooms for the group. By default, all rooms are checked out for one group.

b) The cards of the selected room are cancelled.

c) You can check out a room before cancelling its cards (and cancel the cards after they are collected).

Click **Check Out,** the check out settlement page appears, as shown below.



3. Reading a card

You can view the issuance information of all module cards in the hotel, except for the record cards. The content is displayed based on the card type (for example, guest cards and authorization cards). When a record card is read, only the card type is provided.

4. Canceling a card

You can clear all the card (IC) information. For a guest card, the system checks whether the card is the last card of the room checked in by the guest. If it is, the card cannot be cancelled (as the system does not support free-of-card check-in). For other types of cards, no verification is performed.

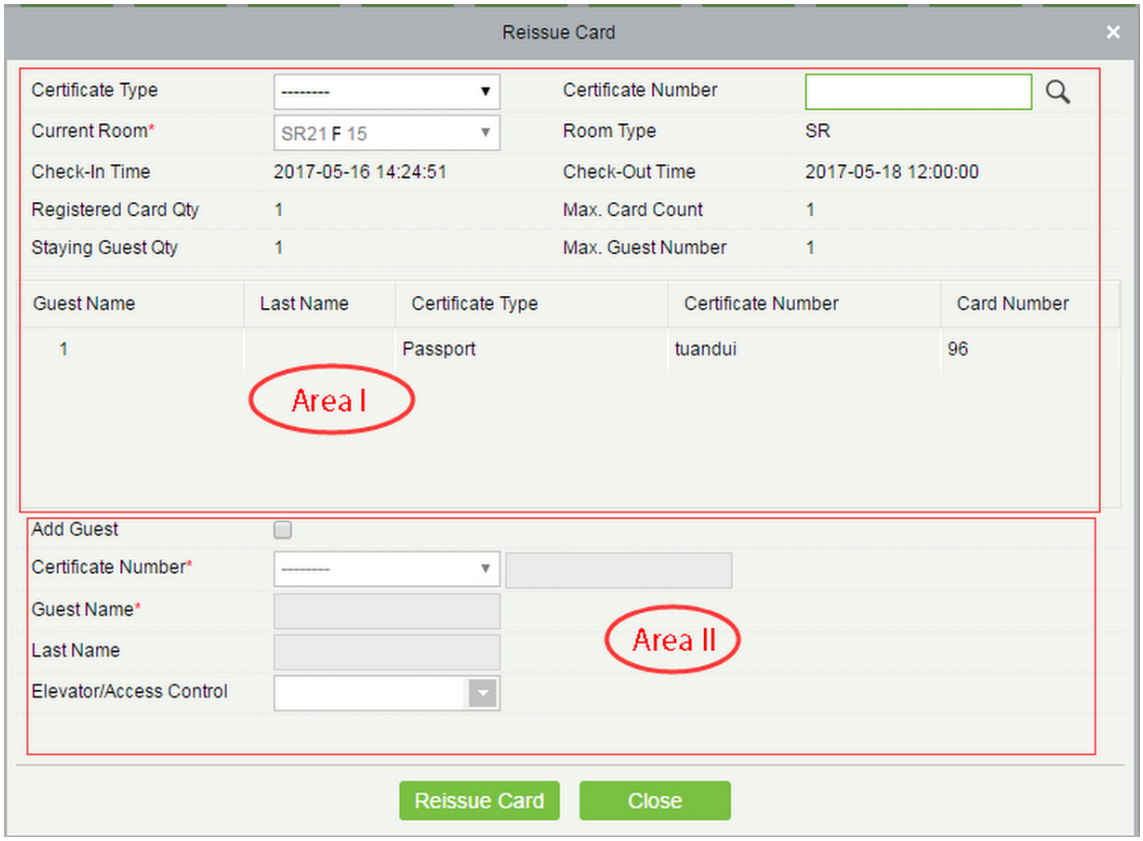
5. Report of loss

You can set a damaged or lost card to an invalid state. For details, see Report card loss in section Maintenance Card.

6. Re-issuing a card

You can re-issue a card for a registered guest or a guest that reports card loss and an additional card for a checked-in room. If the number of guests checked in a room has reached the maximum, no additional card is allowed.

Choose **Hotel Management** > **Reception Center** > **Reissue Card**. Select a room for card re-issuance, or locate the room by querying the certificate information (by clicking 🔍) on the **Reissue Card** page, as shown bellow.



Page description:

Area I: Displays the guest information and check-in information of the room.
Area II: Allows you to input the guest information for the card to be issued.

6.4.2 Reservation Center

You can check the check-in and reservation status of all rooms in a specified period and process room reservation. Choose **Hotel Management** > **Reservation Center**. The page shown in the following figure appears.

Page description:

Area I (available dates): By default, a 15-day period (starting from the current system date) is displayed. You can change the displayed period with the **Reservation Date Range** parameter on the **Hotel Information** page. For details, see section Hotel Settings.

The room reservation time ranges from 12:00 on the reservation start date to 12:00 on the reservation due date. You can change the time point with the **Default Check-Out Time** parameter on the **Hotel Information** page. For details, see section Hotel Settings.

Area II (available rooms): All rooms in the hotel are displayed. You can specify the start and end time and room type to query for a required room.

Room status indicates that the room can be reserved for the time period.

Room status indicates that the room is occupied in the time period and cannot be reserved.

Room status indicates that the room has been reserved for the time period.

Note: If a room is occupied by guests, and will be checked out in the reservation period, the room will be displayed among the available rooms, but cannot be reserved before it is checked out.

Area III: Guest information of the reservation.

Area IV: Information about the rooms selected for reservation.

- **Reservation process**

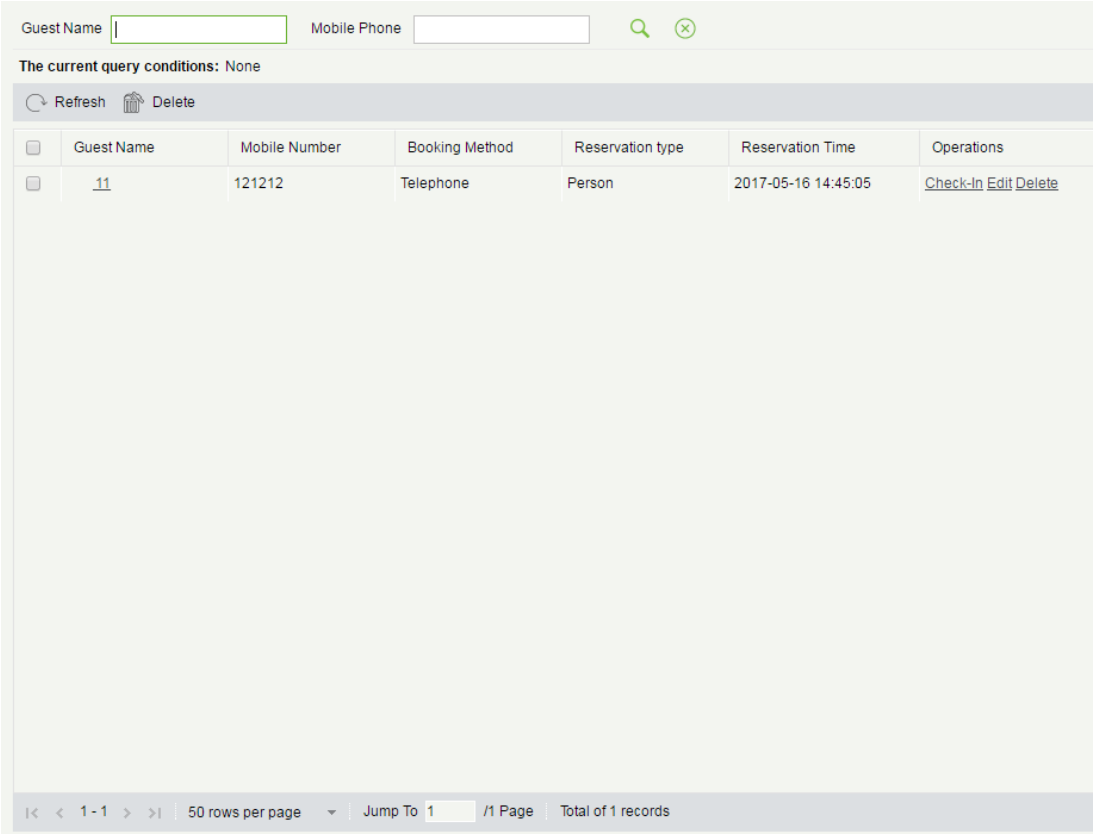
Step 1: Click the room and date for reservation. The selected date of a room turns into red as . You can click the room and date again to cancel the selection. You can select multiple rooms of the same date, multiple dates (continuous only) of one room, or multiple dates (continuous only) of multiple rooms.
After selection, the information about the selected rooms are listed in Area IV in the right part of the **Reservation Center** page.
Step 2: Fill in the guest information, including the name, mobile phone, certificate number, and the booking method (telephone or reception desk).
Step 3: Click **Save**.

6.4.3 Reservation Management

You can query, edit, delete, and handle check-in for a reservation.

- **Querying a reservation**

Choose **Hotel Management** > **Reservation Management**. The page shown in the following figure appears.
You can also enter the guest name and mobile phone number to query for a required reservation.

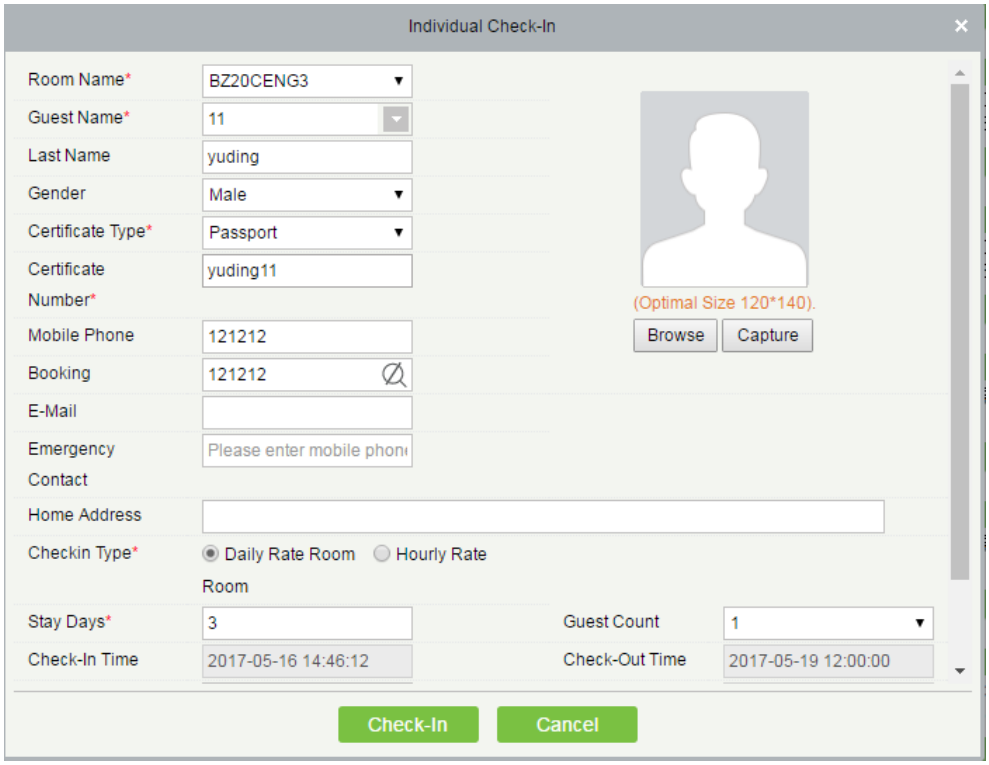


- **Editing/deleting a reservation**

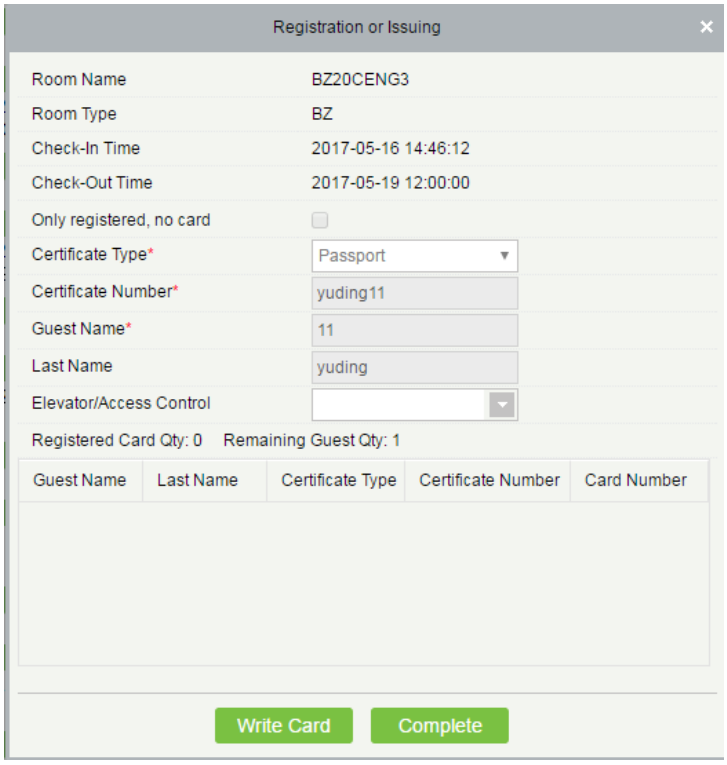
Select the guest name of a reservation, click **Edit** under **Operations**. On the displayed **Reservation Center** page, you can change a room or modify the guest information for the reservation.
Select the guest name of a reservation, click **Delete** under **Operations** or the **delete** button on the top of the list to delete the reservation.

- **Handling check-in**

Select the guest name of a reservation, click **Check-In** under **Operations**. The **Individual Check-In** page appears.



The system automatically loads the reservation information of the room. Modify and complete the guest information and click **Check-In**. The **Registration or Issuing** page appears, as shown below.



Place the guest card on the card writer and click **Write Card** and **Complete** to complete check-in.

Notes:

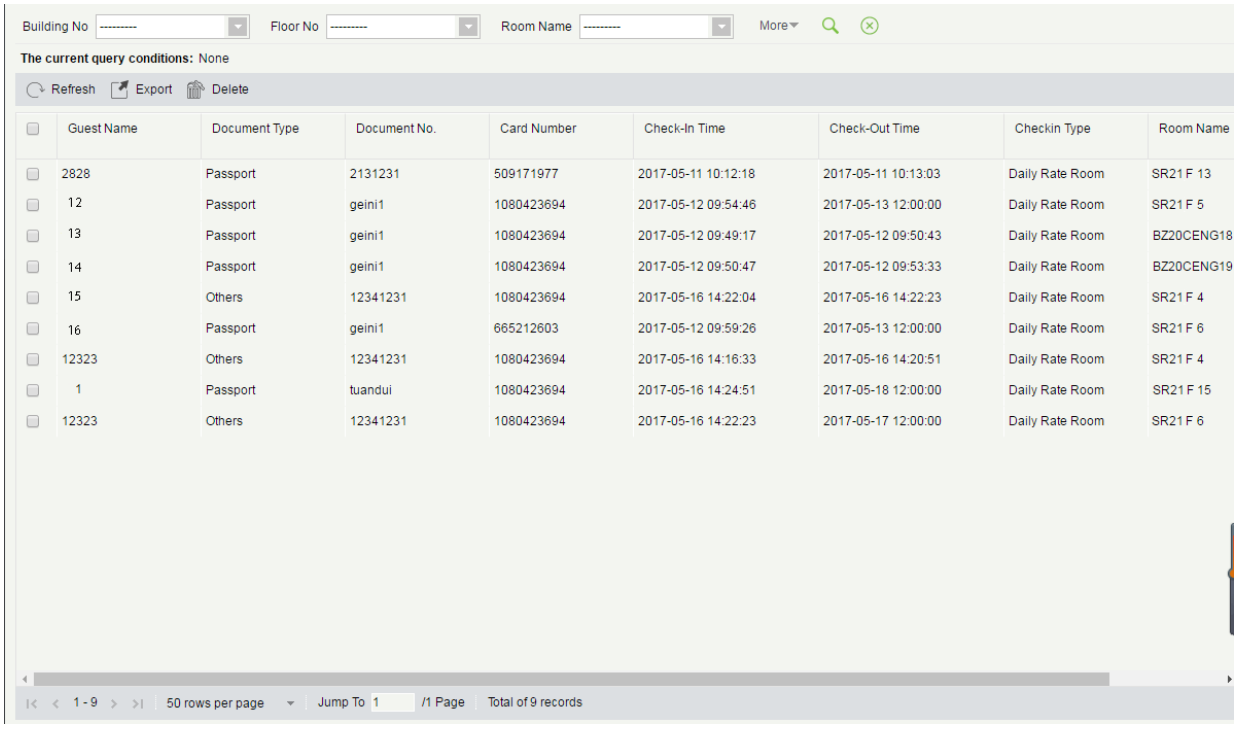
(1) You cannot process check-in for an expired reservation. Check-in can only be processed on site. For details, see Individual check-in in section Reception Center.

(2) The guest can check in before the reserved time.

6.5 Report Management

6.5.1 Guest Check-In Details Report

To view the guest check-in details report, enter the search conditions and view the records. You can export the records into an Excel, PDF, or CSV file. See the following figure.



Guest Name	Document Type	Document No.	Card Number	Check-In Time	Check-Out Time	Checkin Type	Room Name
2828	Passport	2131231	509171977	2017-05-11 10:12:18	2017-05-11 10:13:03	Daily Rate Room	SR21 F 13
12	Passport	geini1	1080423694	2017-05-12 09:54:46	2017-05-13 12:00:00	Daily Rate Room	SR21 F 5
13	Passport	geini1	1080423694	2017-05-12 09:49:17	2017-05-12 09:50:43	Daily Rate Room	BZ20CENG18
14	Passport	geini1	1080423694	2017-05-12 09:50:47	2017-05-12 09:53:33	Daily Rate Room	BZ20CENG19
15	Others	12341231	1080423694	2017-05-16 14:22:04	2017-05-16 14:22:23	Daily Rate Room	SR21 F 4
16	Passport	geini1	665212603	2017-05-12 09:59:26	2017-05-13 12:00:00	Daily Rate Room	SR21 F 6
12323	Others	12341231	1080423694	2017-05-16 14:16:33	2017-05-16 14:20:51	Daily Rate Room	SR21 F 4
1	Passport	tuandui	1080423694	2017-05-16 14:24:51	2017-05-18 12:00:00	Daily Rate Room	SR21 F 15
12323	Others	12341231	1080423694	2017-05-16 14:22:23	2017-05-17 12:00:00	Daily Rate Room	SR21 F 6

6.5.2 Room Check-In Details Report

To check the room occupancy information (including the room name, type, check-in type, check-in time, and check-out time), enter the search conditions and view the records. You can export the records into an Excel, PDF, or CSV file. See the following figure.

Building No --------- Floor No --------- Room Name --------- More

The current query conditions: None

Refresh Export

Room Name	Room Type	Checkin Type	Check-In Time	Check-Out Time
SR21 F 4	SR	Daily Rate Room	2017-05-16 14:22:04	2017-05-16 14:22:23
SR21 F 5	SR	Daily Rate Room	2017-05-12 09:54:46	2017-05-13 12:00:00
SR21 F 13	SR	Daily Rate Room	2017-05-11 10:12:18	2017-05-11 10:13:03
BZ20CENG19	BZ	Daily Rate Room	2017-05-12 09:50:47	2017-05-12 09:53:33
SR21 F 4	SR	Daily Rate Room	2017-05-16 14:16:33	2017-05-16 14:20:51
BZ20CENG18	BZ	Daily Rate Room	2017-05-12 09:49:17	2017-05-12 09:50:43
SR21 F 6	SR	Daily Rate Room	2017-05-12 09:59:26	2017-05-13 12:00:00
SR21 F 6	SR	Daily Rate Room	2017-05-16 14:22:23	2017-05-17 12:00:00
SR21 F 15	SR	Daily Rate Room	2017-05-16 14:24:51	2017-05-18 12:00:00

1 - 9 50 rows per page Jump To 1 /1 Page Total of 9 records

6.5.3 Room Expenses Details Report

To check the room expenses record, enter the search conditions (including time, guest name, room name, and room type) and view the records. See the following figure.

Time From 2017-02-16 00:00:00 To 2017-05-16 23:59:59 Guest Name More

The current query conditions: Time From:(2017-02-16 00:00:00) To:(2017-05-16 23:59:59)

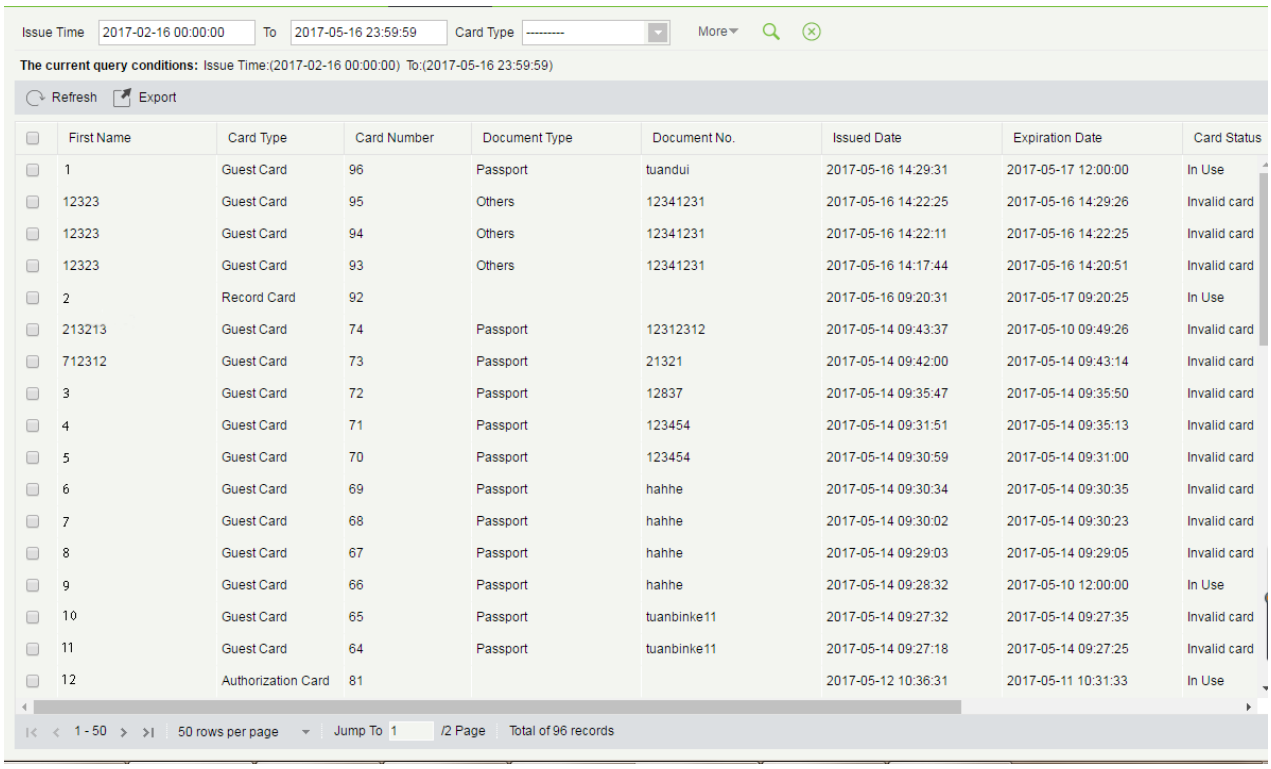
Refresh

Room Name	Room Type	Guest Name	Check-In Time	Check-Out Time	Checkin Type	Stay Times	Room Rate	Overtime Fees	Tax Rate	Othe
BZ20CENG16	BZ	11	2017-05-05 17:45:46	2017-05-05 17:51:10	Daily Rate Room	1	444.0	0.0	0.0	0.0
BZ20CENG3	BZ	22	2017-05-09 10:42:21	2017-05-09 10:55:45	Hourly Rate Room	3	40.0	0.0	0.0	0.0
BZ20CENG12	BZ	21	2017-05-05 17:45:46	2017-05-09 10:58:28	Daily Rate Room	1	444.0	0.0	0.0	0.0
BZ20CENG10	BZ	20	2017-05-09 10:59:25	2017-05-09 14:05:18	Daily Rate Room	1	444.0	0.0	0.0	0.0
SR21 F 5	SR	19	2017-05-09 14:06:02	2017-05-09 14:38:03	Daily Rate Room	1	222.0	0.0	0.0	0.0
BZ20CENG5	BZ	18	2017-05-09 14:06:02	2017-05-09 14:38:03	Daily Rate Room	1	444.0	0.0	0.0	0.0
BZ20CENG5	BZ	17	2017-05-09 14:39:46	2017-05-09 14:40:44	Daily Rate Room	1	444.0	0.0	0.0	0.0
BZ20CENG19	BZ	16	2017-05-09 15:21:27	2017-05-09 15:25:04	Daily Rate Room	1	444.0	0.0	0.0	0.0
SR21 F 4	SR	15	2017-05-09 15:25:40	2017-05-09 15:27:07	Daily Rate Room	1	222.0	0.0	0.0	0.0
SR21 F 4	SR	14	2017-05-09 15:25:40	2017-05-09 15:31:59	Daily Rate Room	1	222.0	0.0	0.0	0.0
BZ20CENG20	BZ	tfy	2017-05-10 09:48:31	2017-05-10 09:49:08	Daily Rate Room	1	444.0	0.0	0.0	0.0
DR22ceng26	DR	213	2017-05-10 09:49:38	2017-05-10 09:50:00	Daily Rate Room	1	111.0	0.0	0.0	0.0
SR21 F 13	SR	2828	2017-05-11 10:12:18	2017-05-11 10:13:01	Daily Rate Room	1	222.0	0.0	0.0	0.0
BZ20CENG18	BZ	12	2017-05-12 09:49:17	2017-05-12 09:50:41	Daily Rate Room	1	444.0	0.0	0.0	0.0
BZ20CENG19	BZ	13	2017-05-12 09:50:47	2017-05-12 09:53:32	Daily Rate Room	1	444.0	0.0	0.0	0.0
SR21 F 4	SR	12323	2017-05-16 14:21:41	2017-05-16 14:21:57	Daily Rate Room	1	222.0	0.0	0.0	0.0
SR21 F 6	SR	12323	2017-05-16 14:22:04	2017-05-16 14:22:47	Daily Rate Room	1	222.0	0.0	0.0	0.0

1 - 19 50 rows per page Jump To 1 /1 Page Total of 19 records

6.5.4 Card Writing Record Report

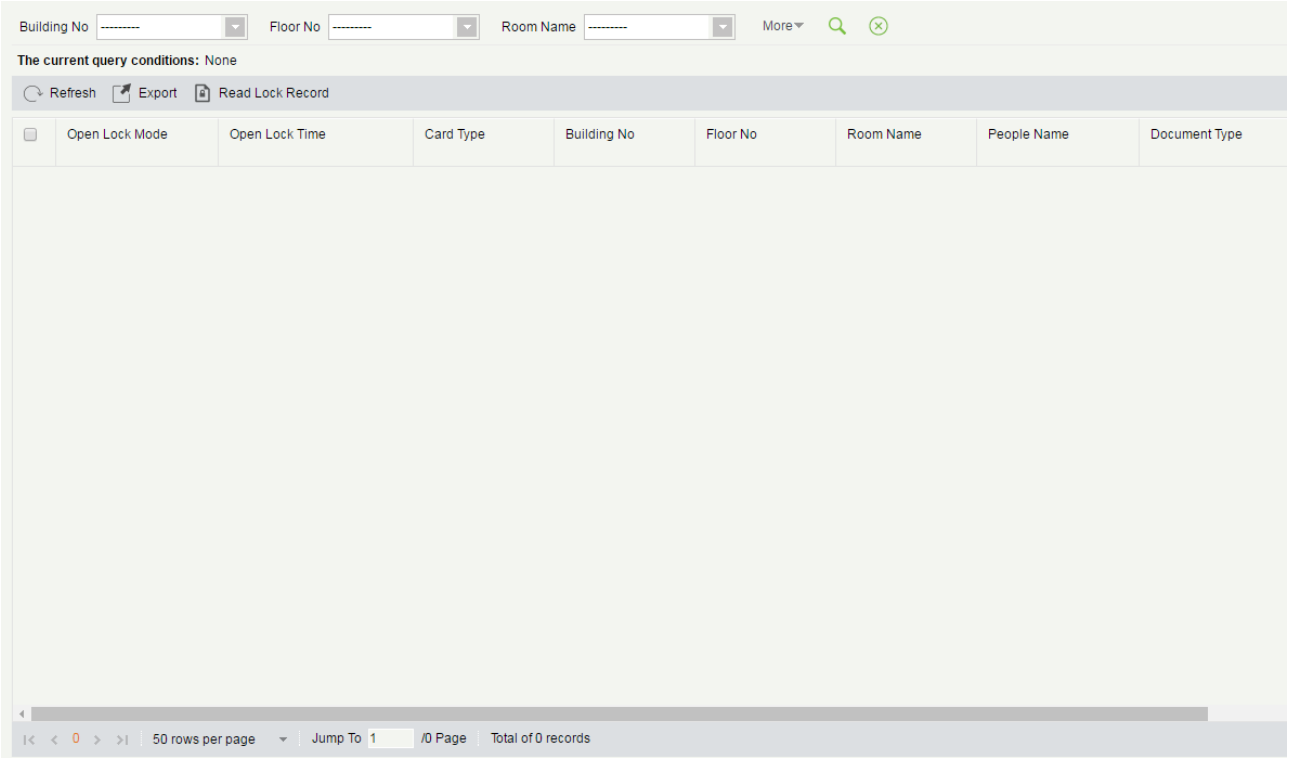
You can also view all card writing records or search required card writing records with multiple search conditions. Enter the search conditions (including time, card type, card No., issuing date, and expiration date) and check the associated card writing records.



First Name	Card Type	Card Number	Document Type	Document No.	Issued Date	Expiration Date	Card Status
1	Guest Card	96	Passport	tuandui	2017-05-16 14:29:31	2017-05-17 12:00:00	In Use
12323	Guest Card	95	Others	12341231	2017-05-16 14:22:25	2017-05-16 14:29:26	Invalid card
12323	Guest Card	94	Others	12341231	2017-05-16 14:22:11	2017-05-16 14:22:25	Invalid card
12323	Guest Card	93	Others	12341231	2017-05-16 14:17:44	2017-05-16 14:20:51	Invalid card
2	Record Card	92			2017-05-16 09:20:31	2017-05-17 09:20:25	In Use
213213	Guest Card	74	Passport	12312312	2017-05-14 09:43:37	2017-05-10 09:49:26	Invalid card
712312	Guest Card	73	Passport	21321	2017-05-14 09:42:00	2017-05-14 09:43:14	Invalid card
3	Guest Card	72	Passport	12837	2017-05-14 09:35:47	2017-05-14 09:35:50	Invalid card
4	Guest Card	71	Passport	123454	2017-05-14 09:31:51	2017-05-14 09:35:13	Invalid card
5	Guest Card	70	Passport	123454	2017-05-14 09:30:59	2017-05-14 09:31:00	Invalid card
6	Guest Card	69	Passport	hahhe	2017-05-14 09:30:34	2017-05-14 09:30:35	Invalid card
7	Guest Card	68	Passport	hahhe	2017-05-14 09:30:02	2017-05-14 09:30:23	Invalid card
8	Guest Card	67	Passport	hahhe	2017-05-14 09:29:03	2017-05-14 09:29:05	Invalid card
9	Guest Card	66	Passport	hahhe	2017-05-14 09:28:32	2017-05-10 12:00:00	In Use
10	Guest Card	65	Passport	tuanbinke11	2017-05-14 09:27:32	2017-05-14 09:27:35	Invalid card
11	Guest Card	64	Passport	tuanbinke11	2017-05-14 09:27:18	2017-05-14 09:27:25	Invalid card
12	Authorization Card	81			2017-05-12 10:36:31	2017-05-11 10:31:33	In Use

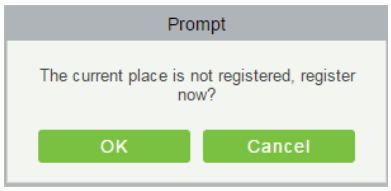
6.5.5 Lock Opening Record Report

You can read a record card to check the lock opening record. Place the record card on a card writer and click **Read Lock Opening Record** to obtain all lock opening records of the record card. You can enter search conditions (including the building/floor/room name, start time, and end time) and view the associated records. You can export the records into an Excel, PDF, or CSV file.


Building No
Floor No
Room Name
More
The current query conditions: None
Refresh
Export
Read Lock Record
Open Lock Mode
Open Lock Time
Card Type
Building No
Floor No
Room Name
People Name
Document Type
50 rows per page
Jump To 1
/0 Page
Total of 0 records

7 Visitor System

After clicking [Visitor], the following window will pop up. Click [OK] to register the clients accessing the server to the Entry Place lists. More detail about registering an entry place, please refer to Entry Place.

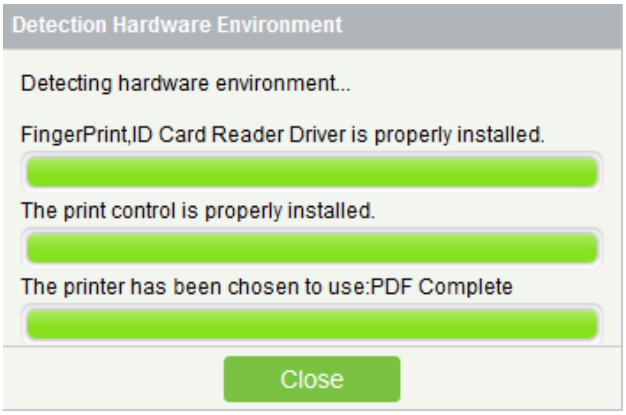


7.1 Registration

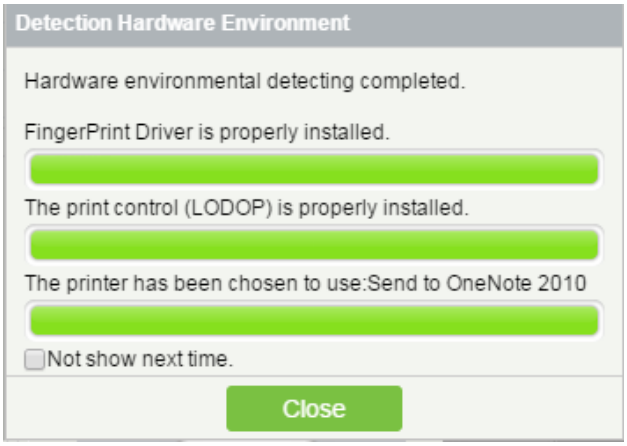
7.1.1 Entry Registration

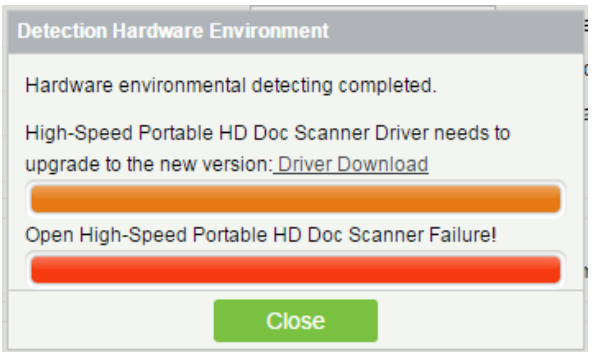
- Entry Registration

1. Click [Register] > [Entry Register] > [Entry Register], the system will detect the hardware environment based on the parameters of [Parameters] in [Basic Management] before entering the registration page:



If the detecting is completed, click [Close] to continue registering, shown as the left figure below. If the detecting failed, the system will prompt to download driver, click [Close] to close the registration window, shown as the right figure below.



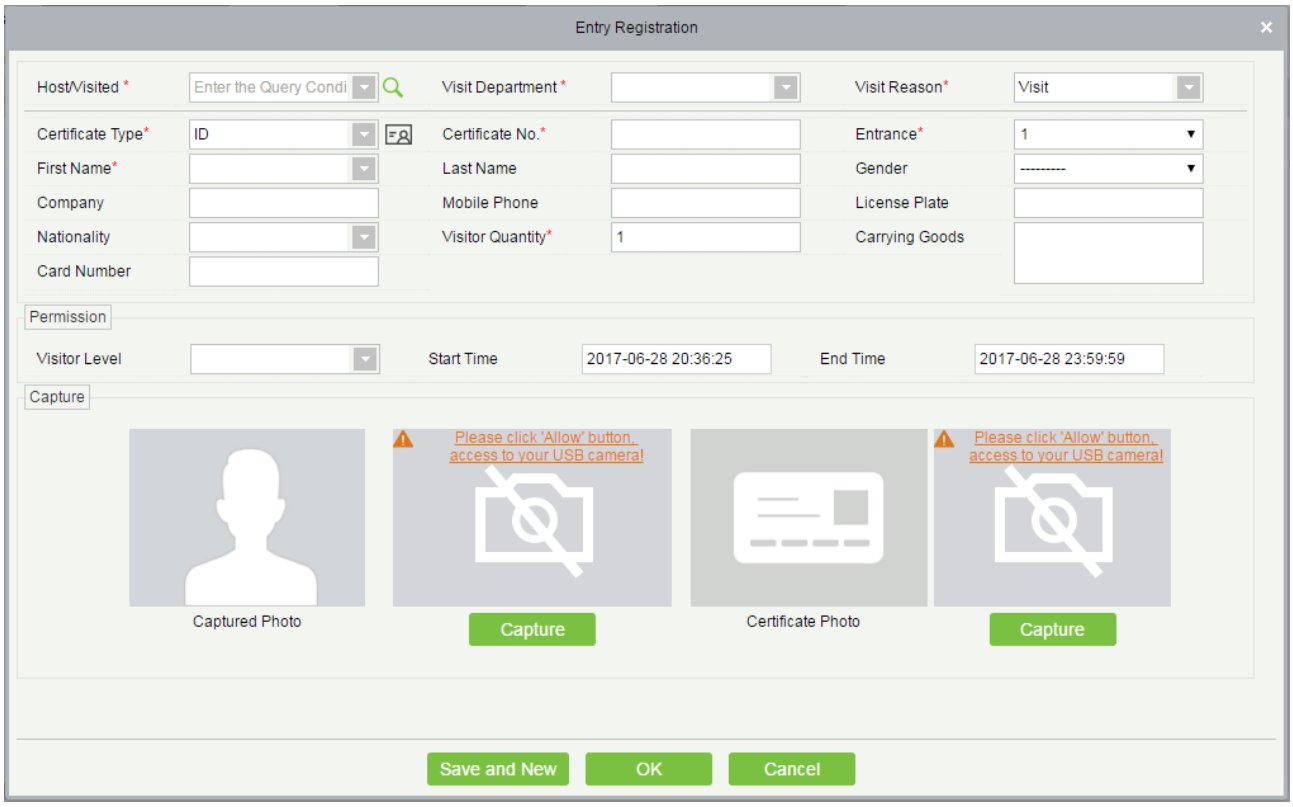


Notes:

1) In the [Parameters] of [Basic Management], if you checked the" Type of Photo Printed on the Receipt Catch Photo", "Fingerprint Registration is Required" and "Use High-Speed Portable HD Doc Scanner", the related controls or drives will be detected. More details about [Parameters], please refer to Parameters.

2) Upon detection of a driver is not installed or installed an older version of the driver, the system will be prompted to download the latest drivers.

2. The registration page is shown as below:



Fields are as follows:

Host/Visited: Select the visited personnel.

Visit Department: Select the department the visitor will visit.

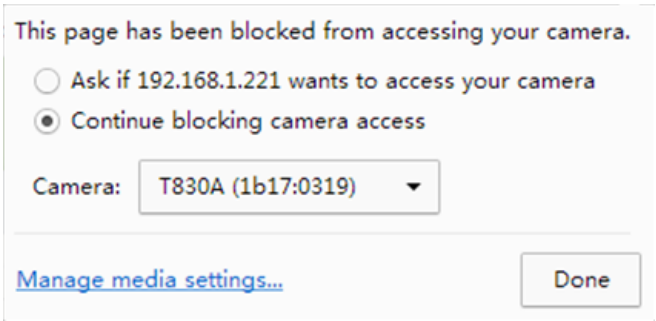
Visit Reason: Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the [Visit Reason] of [Basic Management].

Certificate Type: Passport, Driver's License, ID Card and Others are available to choose. If ID Scan OCR function is activated, visitor information will display automatically after clicking icon.

Entrance: Select the entry place for the visitor. You can add an entry place in the [Entry Place] of [Basic Management].

ID Number: The numbers and letters are legal, the max length is 20.

Head Potrait: The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings).If there is a camera (High-Speed Portable HD Doc Scanner) connected with the server, you can click [Capture] to take the visitor's photo. The browser may block the camera to access, please click in the IP address bar to select the camera and set it allowed to access this page.



Notes:

1) For different browsers, the contents of tips are different, the actual browser display prevail, just choose the shared camera, and allows the system to access the camera.

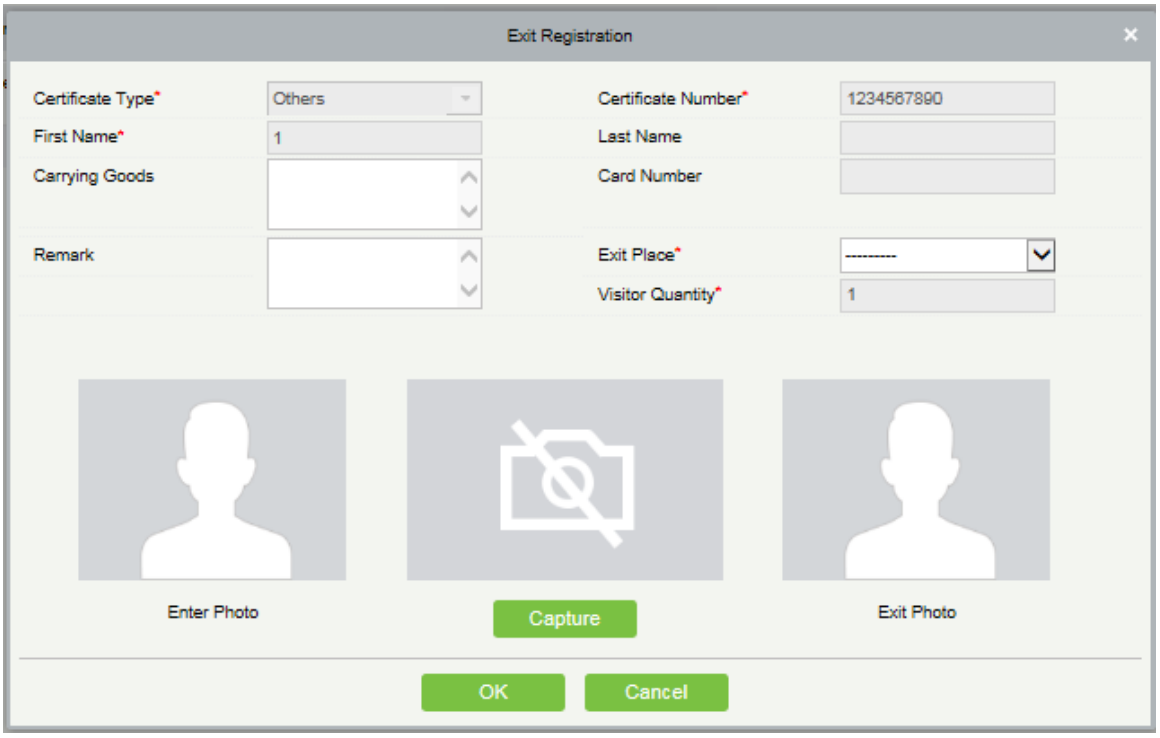
2) If the entry place supports network camera, scanner, high camera, it will not pop up this tip.

3) You can select card number, fingerprint, password or code scanning for registration (set in the parameter setting).

- Exit Registration

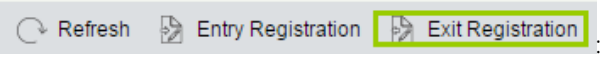
There are 2 ways:

1. Click [Exit Registration] below Operations as a visitor is ready to leave.

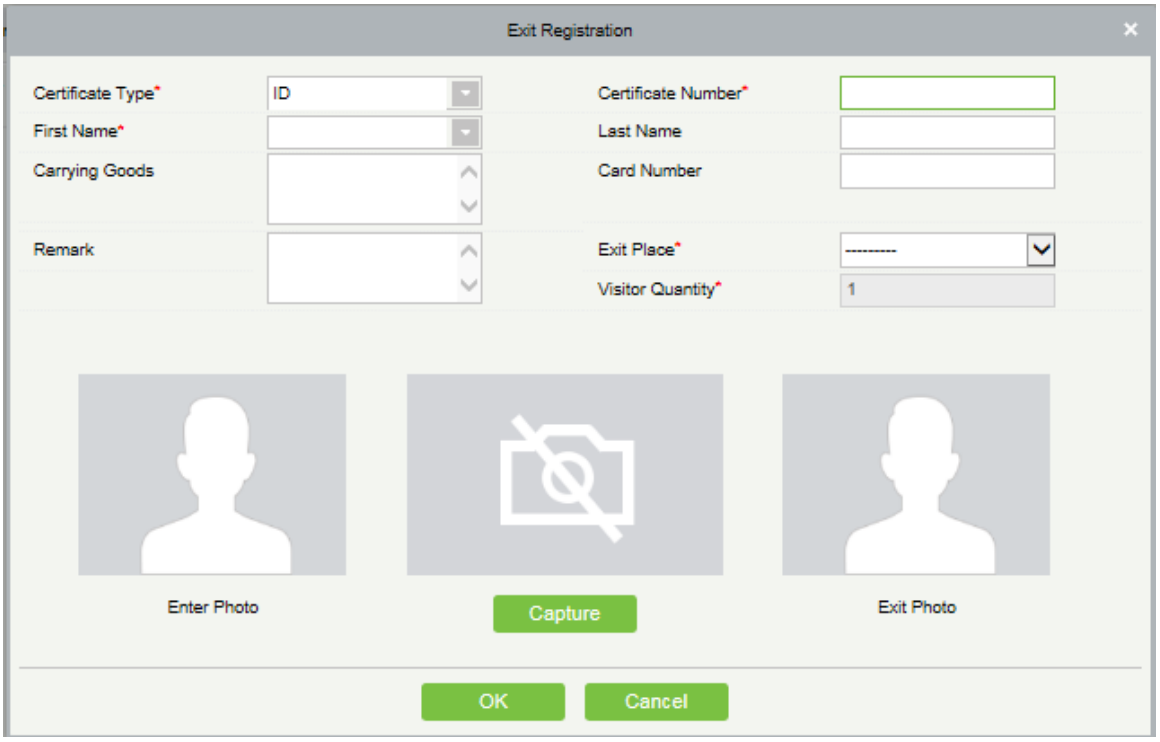


Select the Exit Place and click [OK].

2. You can also click [Exit Registration] in the menu bar when there is too much information in the list:



:



Input the ID Number to get the other information of this visitor quickly. Select the Exit Place and click [OK].

7.1.2 Visitor Information

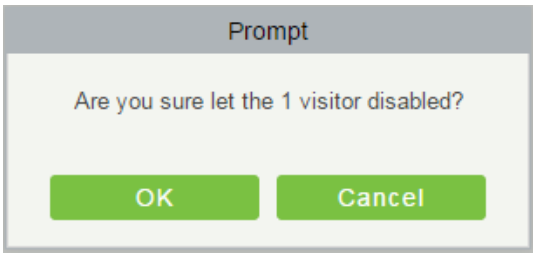
You can delete a visitor, disable or enable a visitor.

- Delete a Visitor

Click [Registration] > [Visitor], select a visitor, click [Delete].

- Disable a Visitor

Click [Registration] > [Visitor], select a visitor, click [Disable]:



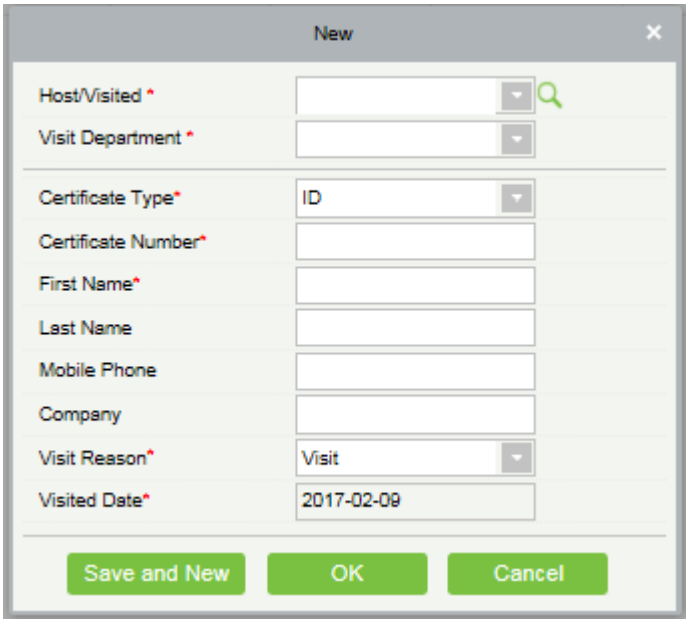
Click [OK] to block the visitor. The below Disable indicates the visitor is blocked.

- Enable a Visitor

Click [Registration] > [Visitor], select a blocked visitor, click [Enable].

7.2 Reservation

1. Click [Reservation] > [Reservation] > [New]:



Host/Visited: Select the visited personnel. Click the input box to filter the query according to the input characters, or click the query button to pop up the list of the visited personnel to select the visited personnel.

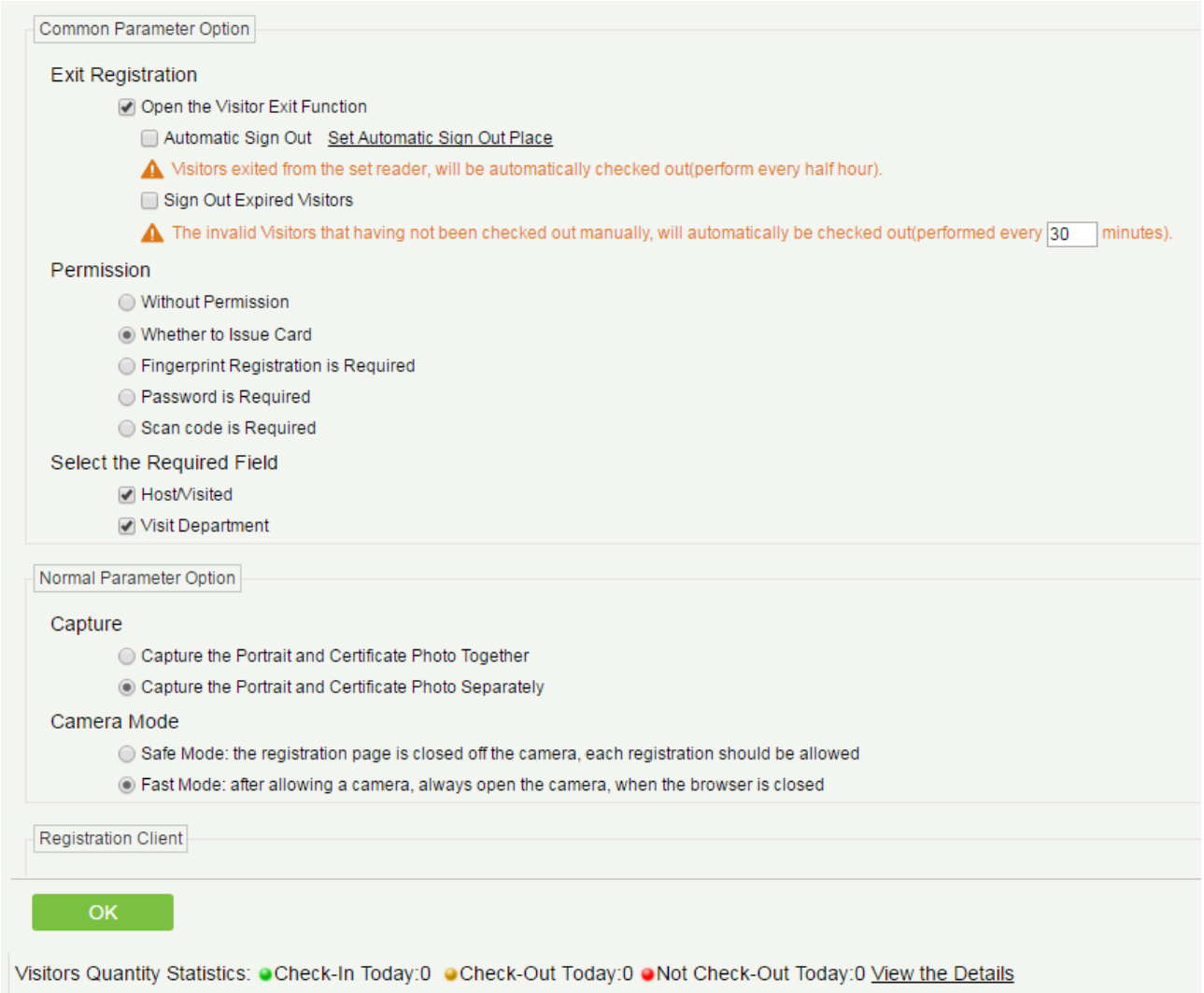
2. Complete the reservation information, click [OK].

The personnel can reserve visitor for themselves by “Personal Self-Login”. The method is same with above descriptions. About how to login to the personal-self system, please refer to Personal Self-Login.

7.3 Basic Management

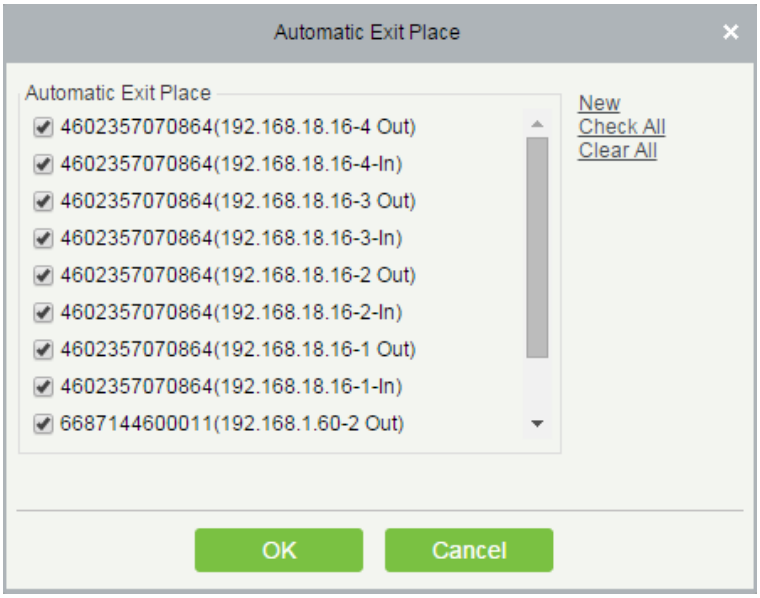
7.3.1 Parameters

Click [Basic Management] > [Parameters]:



Common Parameter Option

- Exit Registration: Enable or disable the auto sign-off function. Auto sign-out means a visitor leaves by directly punching a card or using his/her fingerprint at the preset auto sign-out place, without performing the Exit Registration operation in the software. Setting automatic sign-out place means specifying some readers as the auto sign-out place. Click [Set Automatic Sign Out Place]:



Click [OK] to finish.

Sign Out Expired Visitors: Expired visitors who have not been manually signed out will be automatically signed out after a specified interval.

Visitor Detail Information Today Remind Time: Set the remind time of unsigned-out visitor lists every day.

- Permission

Whether to Issue Card: Whether to issue card for the visitor.

Fingerprint Registration is Required: Whether to register the fingerprint for the visitor.

- Select the Required Field: You can set whether the interviewed and visited departments are required in the registration page and the reservation page.

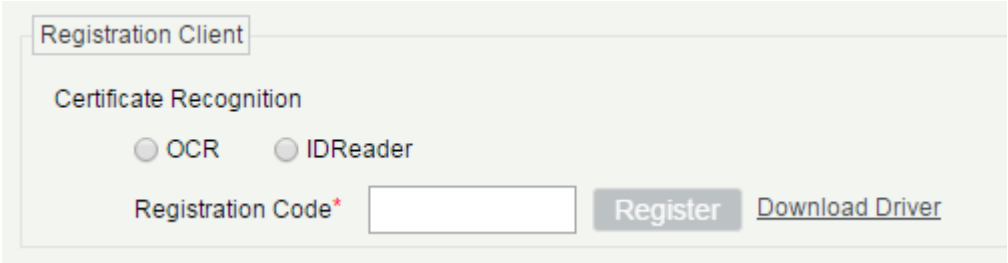
Normal Parameter Option

Device: Whether to use Certificate Identification Equipment and High-Speed Portable HD Doc Scanner.

- Capture: Whether to capture the portrait and certificate photo together.
- Camera Mode: Can set the USB camera only authorized once when not refresh the page.
- ID Scan OCR Setting: To set Certificate Capture and Recognize Together or Separately.

Registration Client:

1) If no driver has been installed, the [Download Driver] link is displayed. Click the link to download and install the driver.

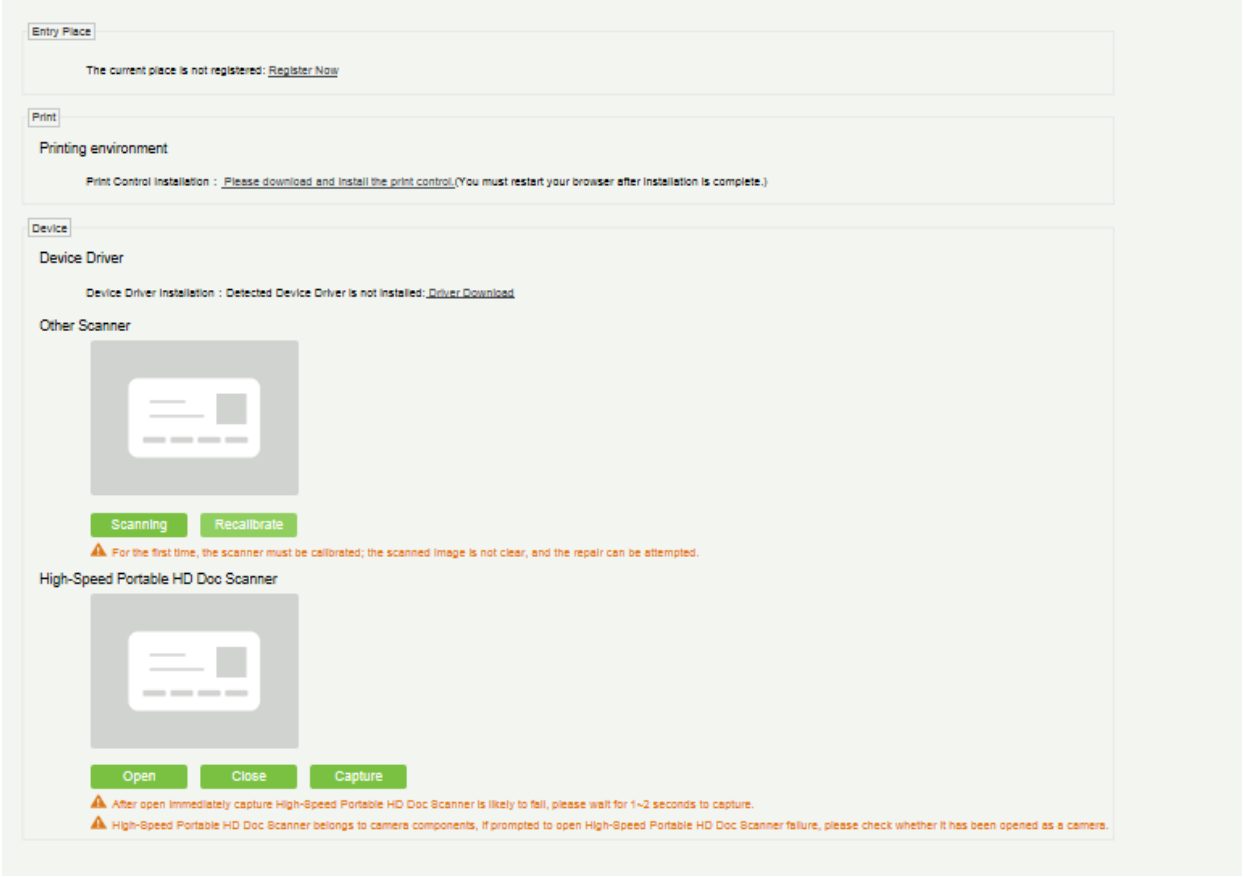


2) Enter the corresponding registration code and click [Register].

Note: Click [System] > [Authority Management] > [Client Register] to view the registration code.

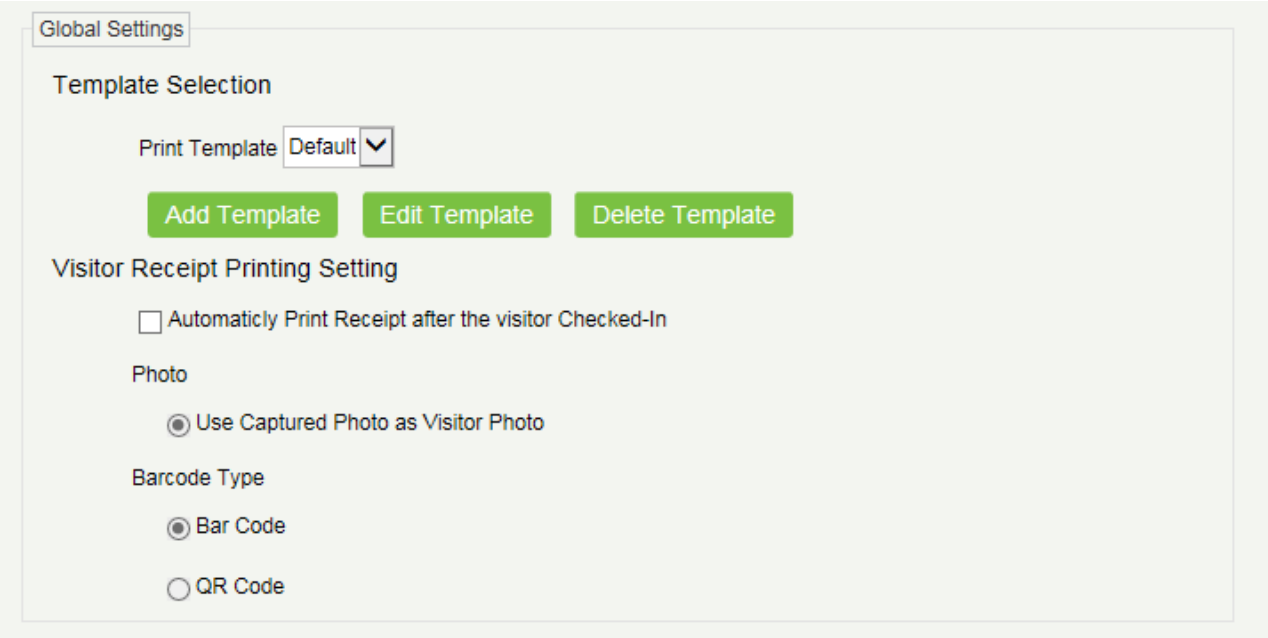
- The Visitor List the Recipient Mailbox: Configure the recipient's mailbox and the time for system to send the list of visitors today.

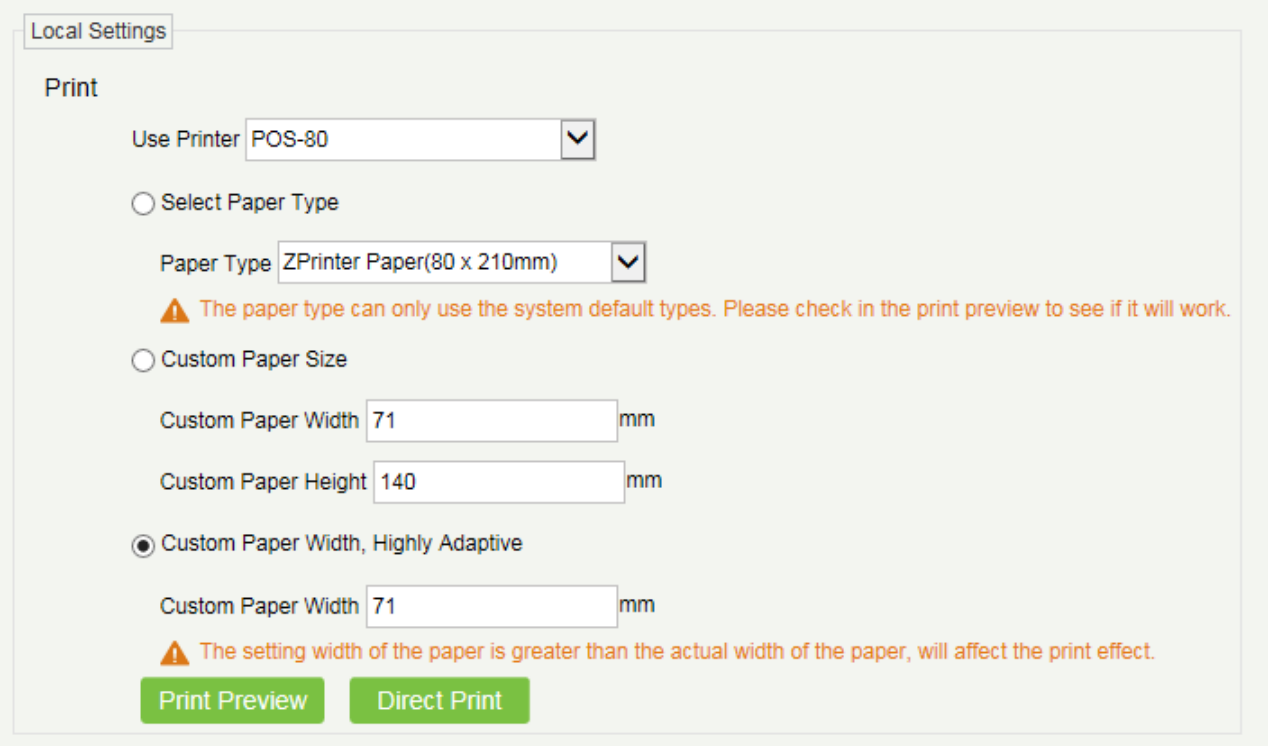
7.3.2 Device Debugging



Entry Place: Displays the information of the current entry place, such as the name of the entry place, IP, equipment usage.
Print: Print-driven installation.
Device: Display device driver installation, you can debug the scanner, the high camera, USB camera when correctly install the display driver (IE browser does not display USB device debugging).

7.3.3 Print Settings





- Global Settings（Valid at each Entry Place）

Template Selection: Select a template to print the template, if the template does not meet the print content, you can add or edit the template (the default template cannot be edited, deleted).

Print Photos: Select whether to print receipt when the server connected with a printer, select whether to use the catch photo in the receipt (Visitor Photo or Capture Photo).

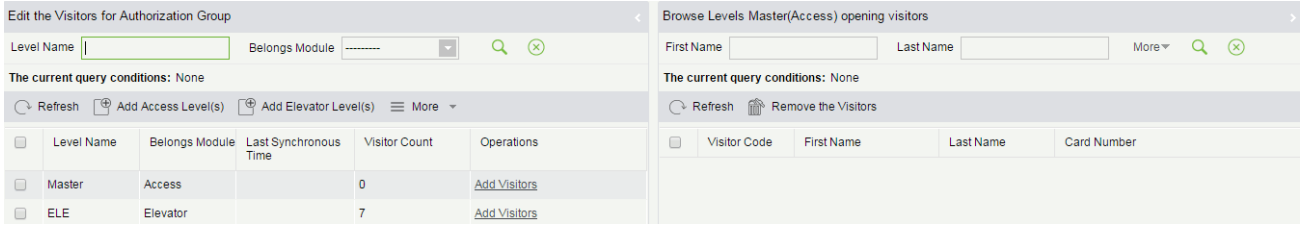
- Local Settings（Valid at the current Entry Place）

Print: You can set the options for the printer, the type of paper to be printed, or the custom paper size, and view the effect by clicking Print Preview / Direct Print. Finally, you can save at the current registration location to print out the effect of setting the print.

7.3.4 Visitor Levels

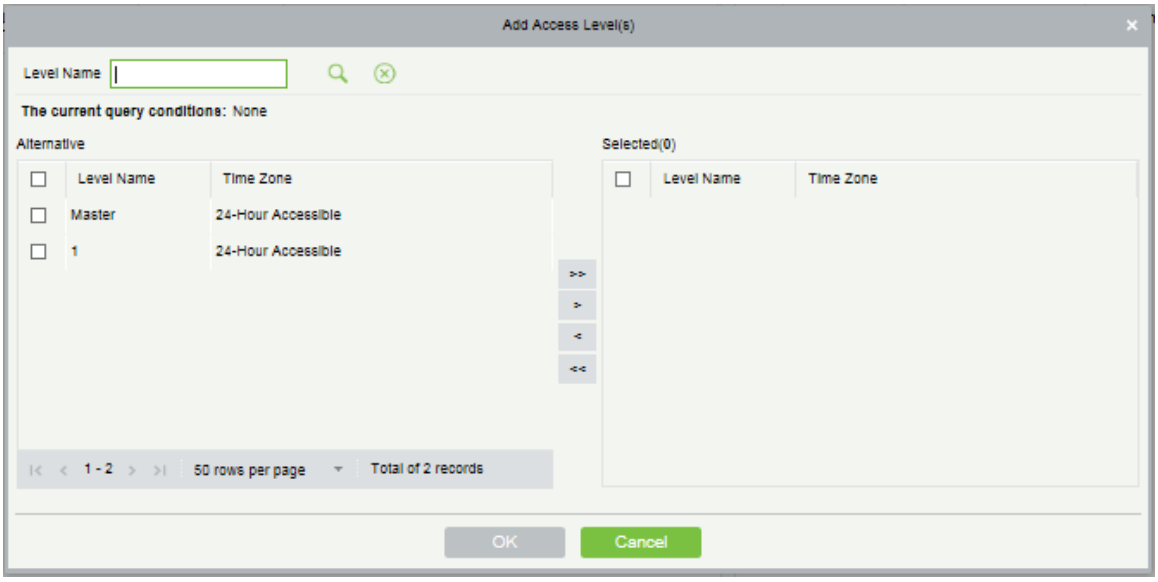
The visitor can be allocated Access or Elevator levels with in registration after the visitor level has been set.

Click [Basic Management] > [Visitor Levels]:



- Add Access Levels

Click [Basic Management] > [Visitor Levels] > [Add Access Levels]:



Set a visitor level name, select one or more access levels, click > or >> to move into the Selected menu. Clcik [OK].

Allocate the Access levels for the visitor when registering.

- Add Elevator Levels

The same way with Add Access Levels.

- Delete Levels

Select a visitor level, click [Delete] in the drop-down list of [More].

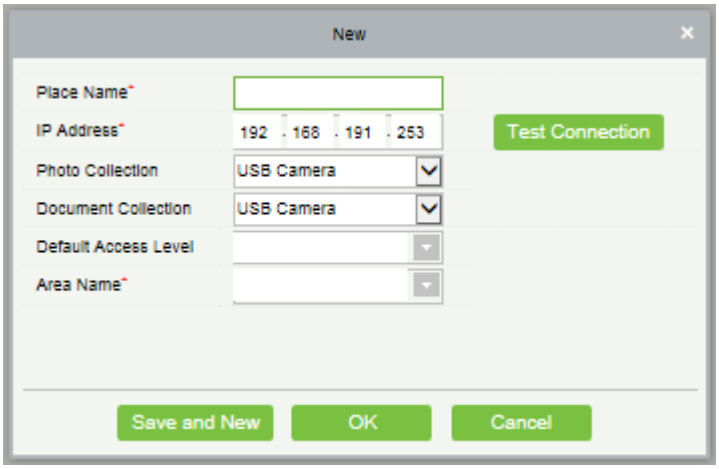
- Synchronous Level

When the Access or Elevator levels are modified, click [Synchronous Level] in the drop-down list of [More] to update the modification in time.

7.3.5 Entry Place

- Add an Entry Place

Click [Basic Management] > [Entry Place] > [New]:



Fields are as follows:

Place Name: It must be unique. Any character with a length of 50 is ok.

IP Address: The IP address of the server.

Photo Collection: USB Camera, IP Camera and Dual Camera High-Speed Portable HD Doc Scanner are available. The IP Camera must be added in the "Video Device" before.

Document Collection: USB Camera, High-Speed portable HD Doc Scanner, Scanner and Dual Camera High-Speed Portable HD Doc Scanner are available.

Default Access Level: Set the default levels in this entry place.

Area Name: The name of the area the entry place belongs, and the registration record for each entry place is filtered according to the area of the entry place.

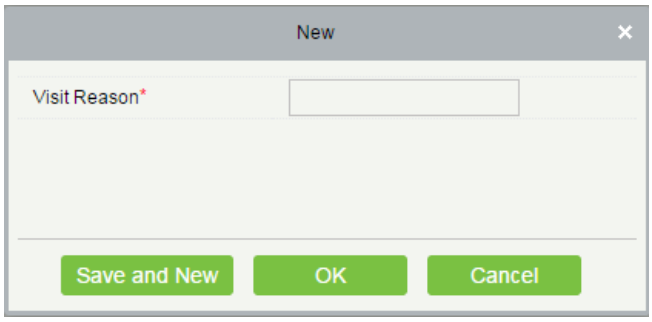
2. Click [Edit] or [Delete] as required.

- Automatic Exit Place

Please refer to Parameters

7.3.6 Visit Reason

1. Click [Basic Management] > [Visit Reason] > [New]:



2. Click [OK] to finish. You can also click [Edit] or [Delete] as required.

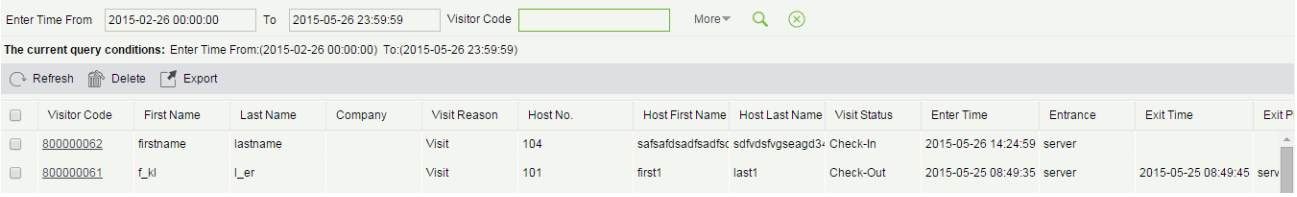
7.4 Visitor Reports

7.4.1 Last Visited Location

Click [Reports] > [Last Visited Location] to view the reports. The reports can be filtered by different conditions.

7.4.2 Visitor History Record

Click [Reports] > [Visitor History Record] to view the reports. The reports can be filtered by different conditions.



7.4.3 Charts

Click [Visitor] > [Reports] > [Charts]. The charts showing visitor records are displayed.

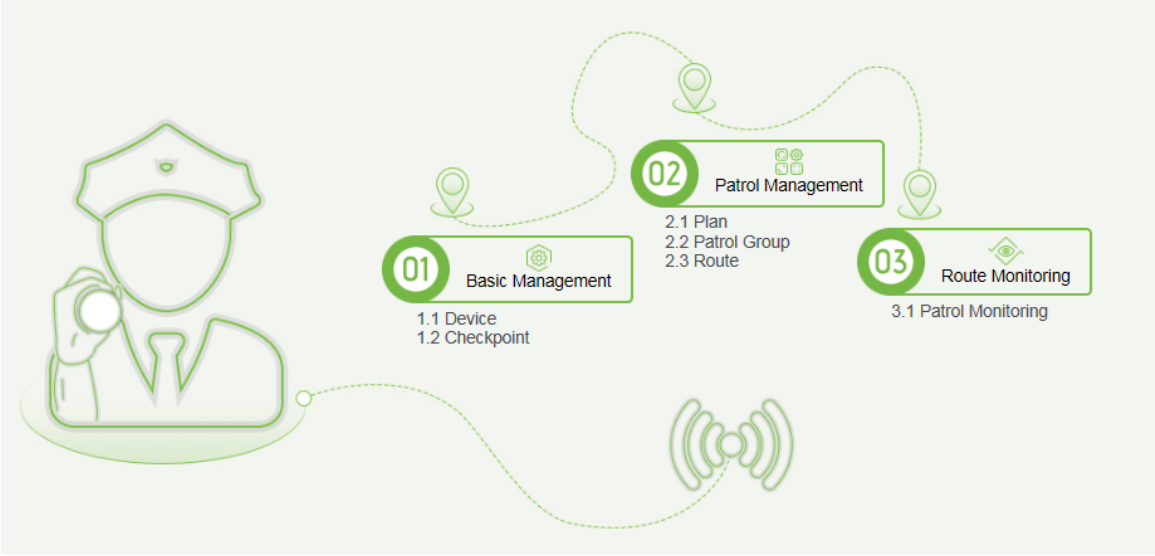
8 Patrol System

The patrol system can help enterprise management personnel to effectively supervise and manage the patrol personnel, plans and routes. In addition, periodic statistics and analysis can be performed on the patrol routes and results.

Note: Before patrol operations, you need to add patrol devices in the [Access] module and add patrol personnel in the [Personnel] module.

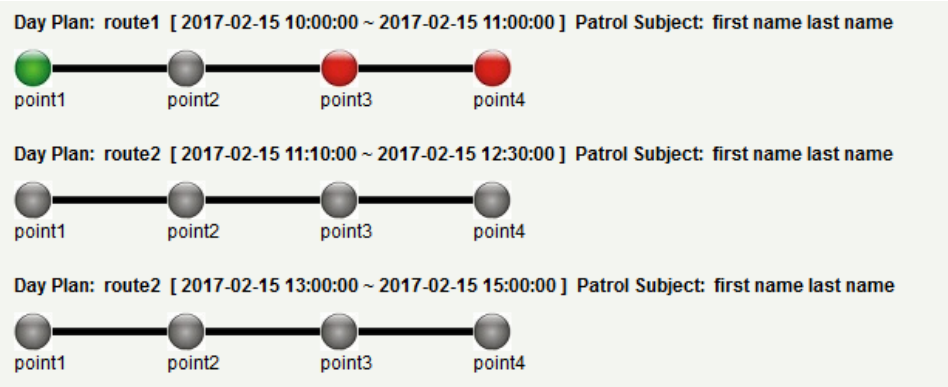
8.1 Operation Wizard

After logging into the system, click [Patrol] to go to [Operation Wizard]. Click on the page as prompted to go to different functional modules and perform operations. The page is displayed as follows:

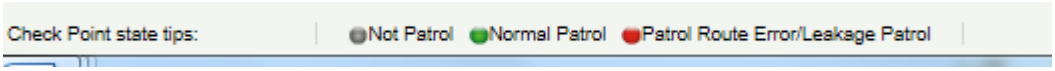


8.2 Route Monitoring

This function displays all the scheduled routes of the current day in the patrol plan. When the patrol personnel patrol based on the plan, the corresponding checkpoints in the patrol route will turn green. If the personnel do not patrol based on the plan, the checkpoints will turn red. The page is displayed as follows:



Checkpoint status:



Normal Patrol: The patrol personnel finished the patrol in the normal time segment in normal sequence.

Patrol Route Error: The patrol personnel finished the patrol in the normal time segment but didn't follow the route.

Leakage Patrol: The patrol personnel didn't finish the patrol in the normal time segment, that is, one or more checkpoints are not patrolled.

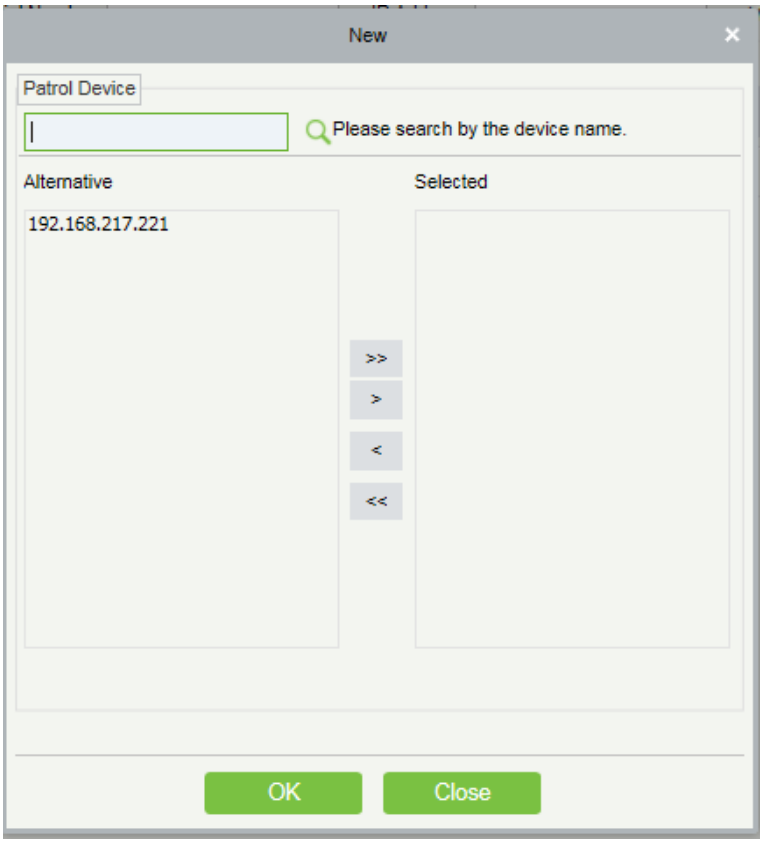
Not Patrol: The patrol personnel didn't finish the patrol in the normal time segment, that is, the entire patrol route is not patrolled.

8.3 Basic Management

8.3.1 Device

- Add

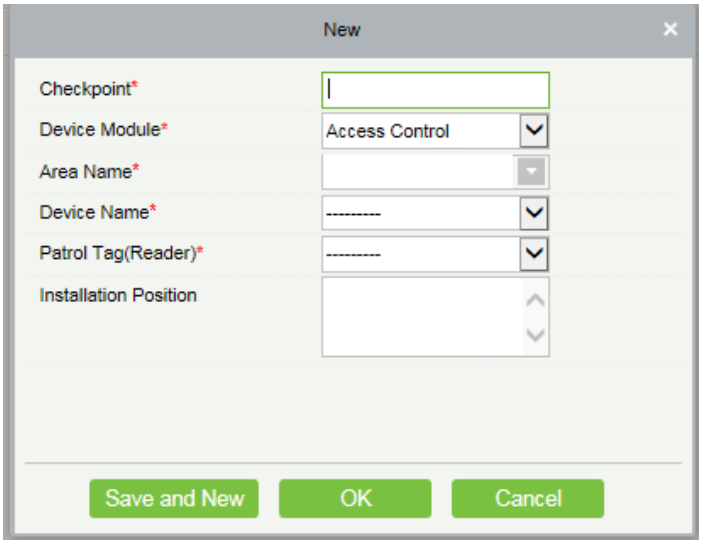
Select a device to be used as the patrol device from the access control devices. Click [Basic Management] > [Device] > [New]. In the [Alternative] box, add available devices and click [OK] to save the setting. The page is displayed as follows:



8.3.2 Checkpoint

- Add

(1)Click [Basic Management] > [Checkpoint] > [New]. The page is displayed as follows:



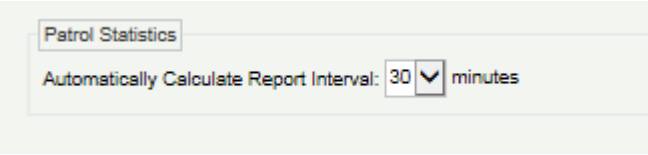
Patrol Tag: Currently, only access control device readers are supported.

(2) After the setting (parameters with * are mandatory), click [OK] to save the setting. You can also click [Save and New] to save the current setting and add another checkpoint. Click [Cancel] to cancel the setting and return to the

upper-level menu.

✍ **Note:** Patrol tags that have been used by checkpoints cannot be used again when you add another checkpoint.

8.3.3 Parameters



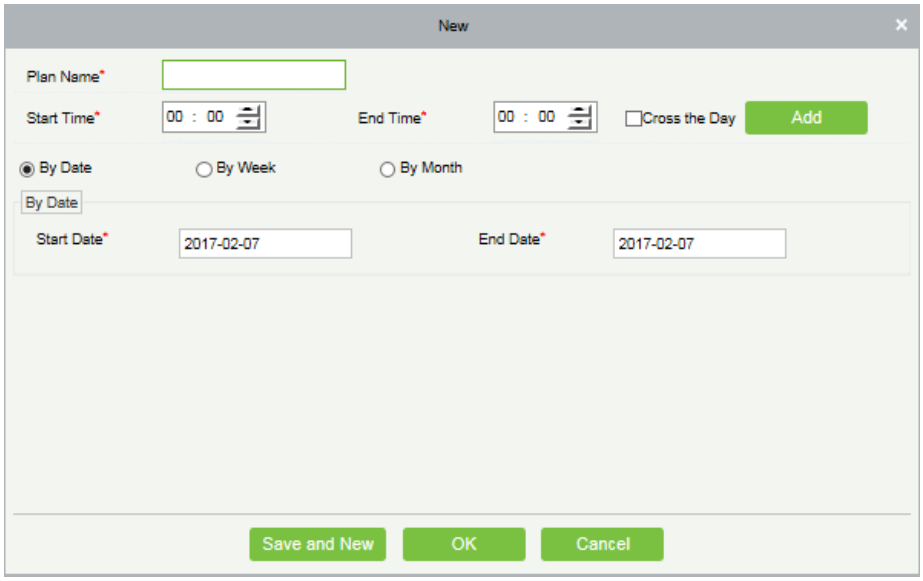
1) Click [Patrol] > [Basic Management] > [Parameters].
2) Set the interval for patrol statistics collection.
3) Click [OK] to save the setting.

8.4 Patrol Management

8.4.1 Plan

- Add

Click [Patrol Management] > [Plan] > [New]. Plans by date, week and month are displayed as follows:



Time Segment: You can set the start and end time of the patrol. The time segment can be across different days.
By Date: The patrol plan is scheduled by day. Select [By Date] and set the start and end date for the patrol plan.
By Week: The patrol plan is scheduled by week.
By Month: The patrol plan is scheduled by month.

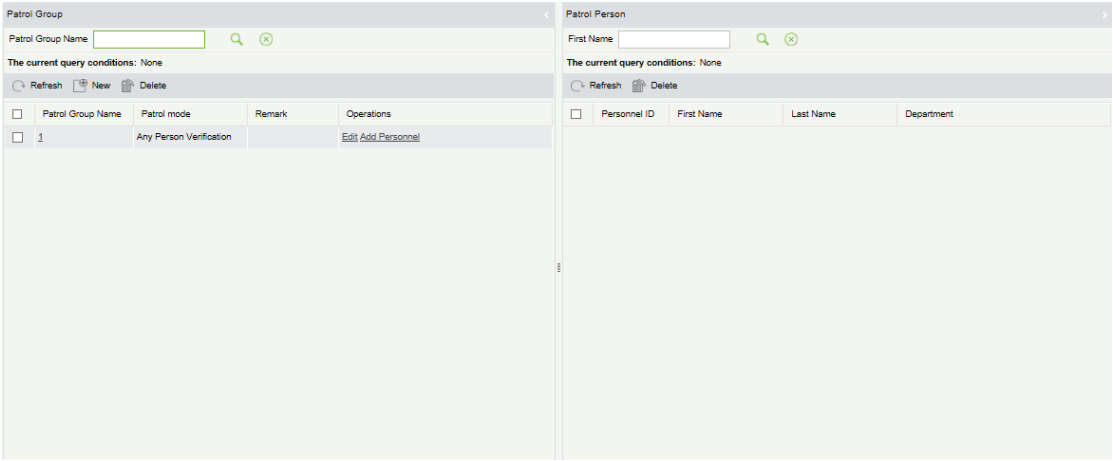
A patrol plan by month can be executed every day or periodically. If you choose to execute the patrol plan every day, the patrol task is performed every day in the specified month. If you choose to periodically execute

the patrol plan, the patrol task is performed on the specified date in the month.

Note: A maximum of three patrol shifts can be added for a patrol plan.

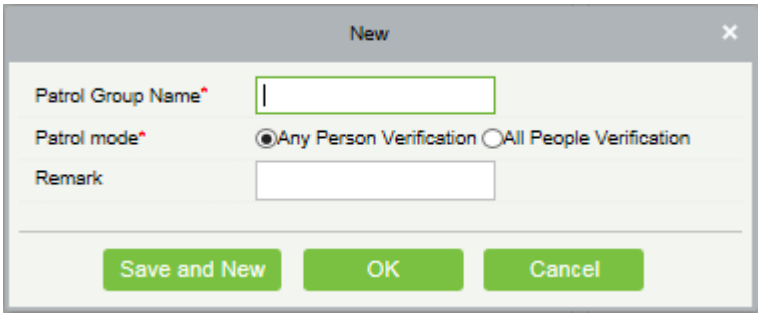
8.4.2 Patrol Group

A patrol group consists of multiple patrol personnel. Personnel in the patrol group work together to finish the corresponding patrol task. Click [Patrol Management] > [Patrol Group].



- Add

1. Click [Patrol Management] > [Patrol Group] > [New] to go to the patrol group adding page as follows:



2. Set the following parameters: Select a patrol group name (not repeatable), patrol mode and remarks.
3. Click [Save and New] to add another patrol group and click [OK] to finish the setting.
4. Add/Delete personnel for a specified patrol group. (The following operations cannot be performed if the patrol group is used by a patrol route).
(1) Click [Patrol Management] > [Patrol Group]. Click a patrol group from the list on the left. Personnel in the patrol group are displayed in the list on the right.
(2) Click [Add Personnel] under Operation in the list on the left. The page for adding personnel is displayed (or adding by department). Add personnel to the list on the right and click [OK] to finish the setting.
(3) Select personnel in the list on the right and click [Delete] above the list to delete the personnel from the patrol group.

Note: In [Patrol Mode], Any Person Verification means that the patrol task is finished as long as one person in the patrol group swipes the card at the checkpoint in the plan, while All People Verification means that the patrol

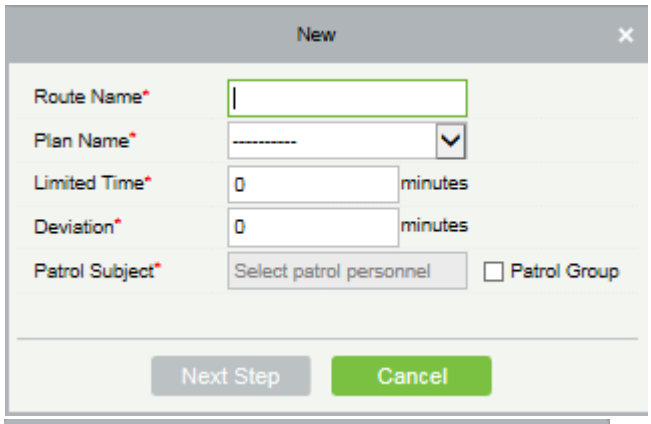
task is finished only after all people in the patrol group swipe their cards at the checkpoint in the plan. A patrol group cannot be edited or deleted when it is used by a patrol route.

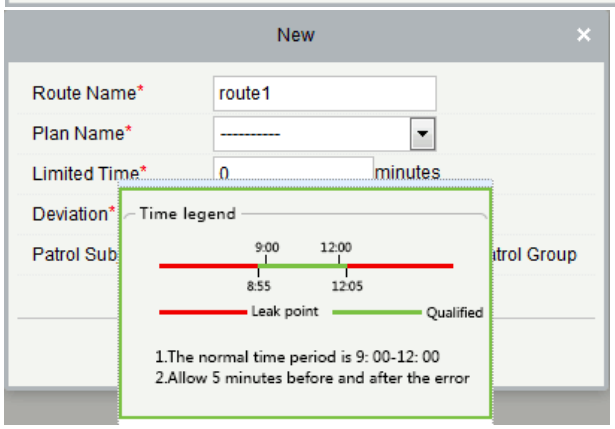
8.4.3 Route

A patrol route consists of a series of checkpoints in a specified sequence.

- Add

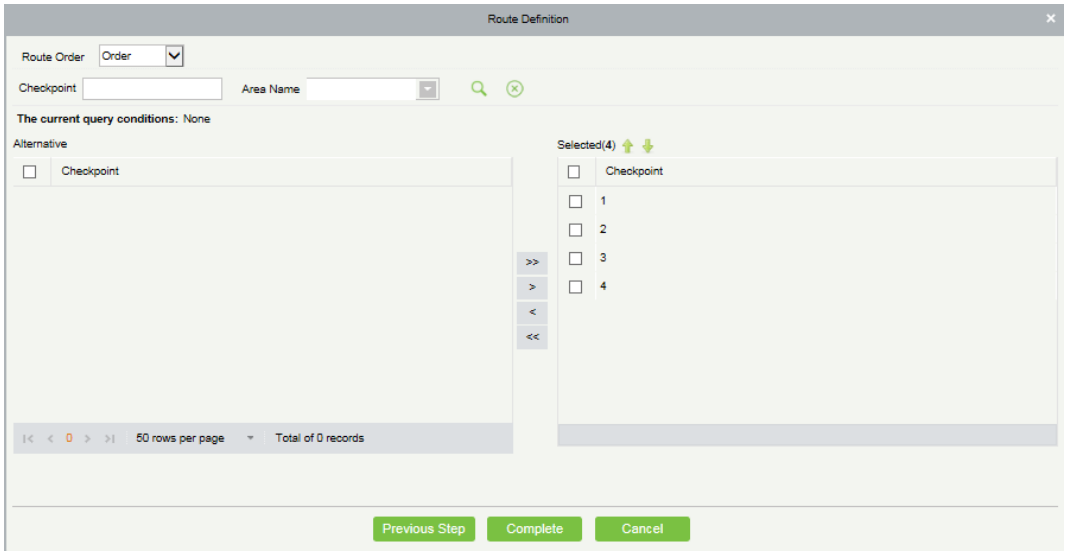
Click [Patrol Management] > [Route] > [New]. The page is displayed as follows:
1. Set basic information for a route in the following box. The Limited Time parameter refers to the time limit for finishing the entire route.





Description of the time segment legends: It is set according to the allowed error time during the patrol. Suppose that the patrol plan is scheduled between 9:00 and 12:00 (which can be set in the patrol plan), and the allowed error time is 5 minutes. This means records between 8:55 and 12:05 are valid and those out of this time segment are invalid.

2. After the setting, click [Next] to go to the [Route Definition] dialog box. Routes can be classified to Order routes and Disorder routes (two categories and five situations are available). The ⬆ and ⬇ buttons are used to move the checkpoint up and down.
Order: During patrol plan execution, there is no time limit between checkpoints. Patrol personnel can patrol checkpoints in a specified sequence according to their habits within the time limit.



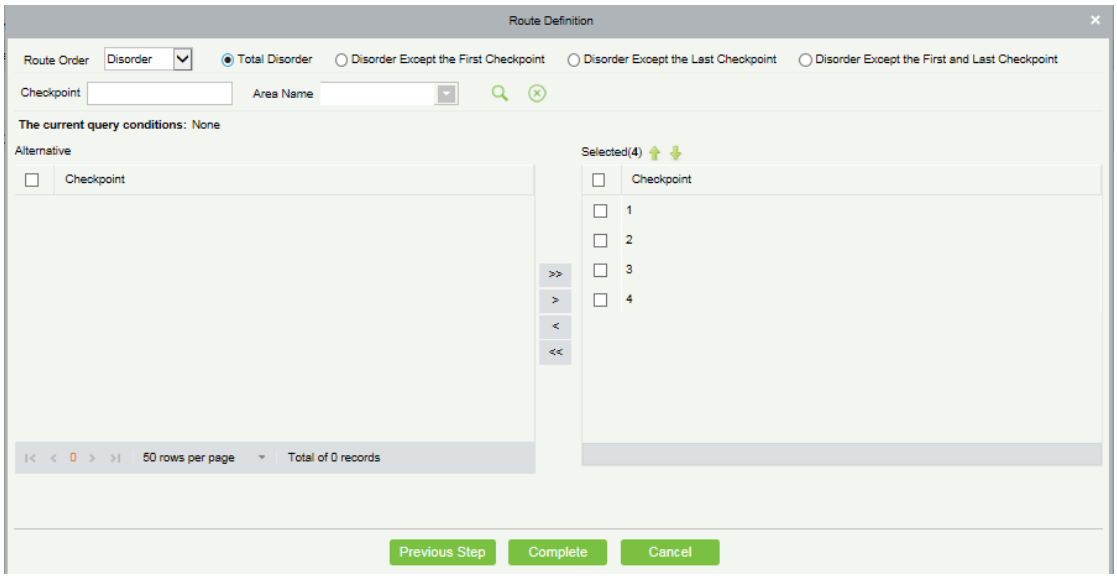
Disorder: Disorder routes are divided into the following:

Total Disorder: All checkpoints in the patrol route are disordered. Patrol personnel can patrol checkpoints according to their habits within the time limit.

Disorder Except the First Checkpoint: In the patrol route, all checkpoints except the first checkpoint are disordered.

Disorder Except the Last Checkpoint: In the patrol route, all checkpoints except the last checkpoint are disordered.

Disorder Except the First and Last Checkpoint: In the patrol route, all checkpoints except the first and last checkpoints are disordered.



3. Click [OK] to save the setting.

Note:

Before patrol operations, you need to add patrol devices in the [Access] module and add patrol personnel in the [Personnel] module. Note that if the patrol personnel are required to patrol according to the card number but do not have the right for opening the door, you cannot select any rights group in the access control setting when adding personnel, or add a rights group that cannot pass the door in any time segment, and then select the rights group in the access control setting when adding personnel.

8.5 Reports

There are four modules: All transactions, Patrol Records Today, Patrol Route Statistics, and Patrol Personnel Statistics. You can analyze and collect statistics on the patrol data to gain an overall control on the patrol process.

8.5.1 All transactions

Click [Reports] > [All transactions] to view all transactions, that is, all event records generated by the patrol device.

8.5.2 Patrol Records Today

Click [Reports] > [Patrol Records Today] to view event records generated by the patrol device today.

8.5.3 Patrol Route Statistics

Click [Reports] > [Patrol Route Statistics] to view all normal and abnormal situations collected during the patrol process.

8.5.4 Patrol Personnel Statistics

Click [Reports] > [Patrol Personnel Statistics] to view patrol statistics of patrol personnel.

Supposed Patrol Times: Number of times that the patrol personnel should normally patrol.

Real Patrol Times: Number of times that the patrol personnel actually patrol.

Wrong Patrol Times: Number of times that the patrol personnel do not patrol based on the patrol route.

Missed Patrol Times: Number of times that the patrol personnel miss one or more checkpoints in the patrol route within the patrol time.

Absence Times: Number of times that the patrol personnel do not patrol.

9 Video

The system supports video linkage of access elevator control. You can achieve the management of DVR / NVR / IPC, real-time video preview, video records query and automatically popping up of linkage events.

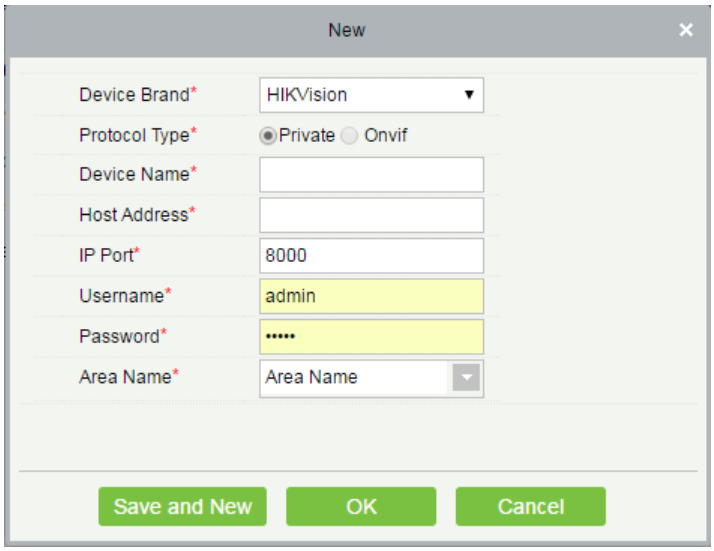
You need to add video device, set linkage function in Linkage Setting and Global Linkage in advanced.

Note: The current software only supports HIKVision, ZKIVision and Dahua devices. For more details about the devices models, please contact technical support personnel to confirm.

9.1 Video Device

- Add a Video device

Click [Video] > [Video Device] > [Video Device] > [New]:



Fields are as follows:

Device Brand: The current software version supports only ZKTeco, HIKVISION, Dahua, Axis, Panasonic and Geovision brands. For each brand supporting models, please refer to the Hardware Support List for Video Module.

Protocol Type: The Private or Onvif protocol is automatically selected after Device Brand is specified.

Device Name: Any characters within a length of 30.

Host Address: Input the device's IP address.

IP Port: The default corresponding IP Port will display after select Device Brand.

User Name: Any characters within a length of 15(no blanks).

Password: Any characters within a length of 32(no blanks).

Area Name: Divide area for the device.

Note: After adding device, only the device name and area name can be modified again, other options cannot be modified.

- Enable/Disable a Video Device

Select a video device in the list, and click [Enable] or [Disable].

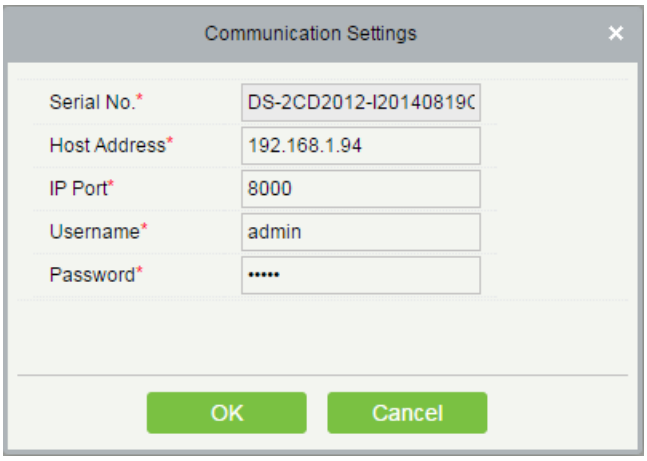
- Edit/Delete Video a Device

Select a video device in the list, and click [Edit] or [Delete].

- Communication Settings

When the communication parameters are modified in the device, the modification must be synchronize to the software to keep the consistency, otherwise all the channels of the video device will not work normally.

Select a device, click [Communication Settings]:



- Video Linkage Operation Guide

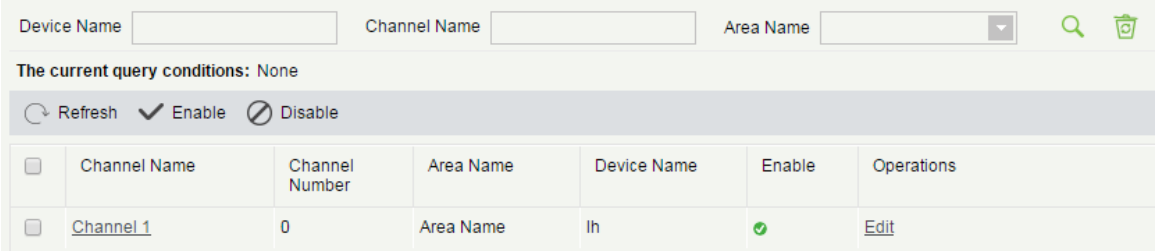
Click [Video Linkage Operation Guide], guide users to add video equipment, binding cameras for access control equipment and set the linkage.

9.2 Video Channel

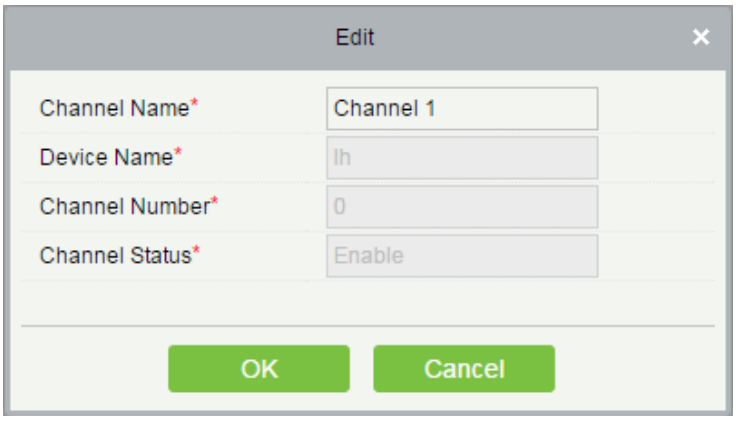
When adding a video device, the system will automatically detect the number of cameras on this device, that is, the number of channels, and generate a number of channels accordingly. For example, a video device has 16 cameras. After adding this device, the system will generate 16 channels, and name the channels by default using the format "Device name-channel No.".

- Enable/Disable Video Device

Click [Video] > [Video Device] > [Channel]:



Click [Edit] below Operations in the list:



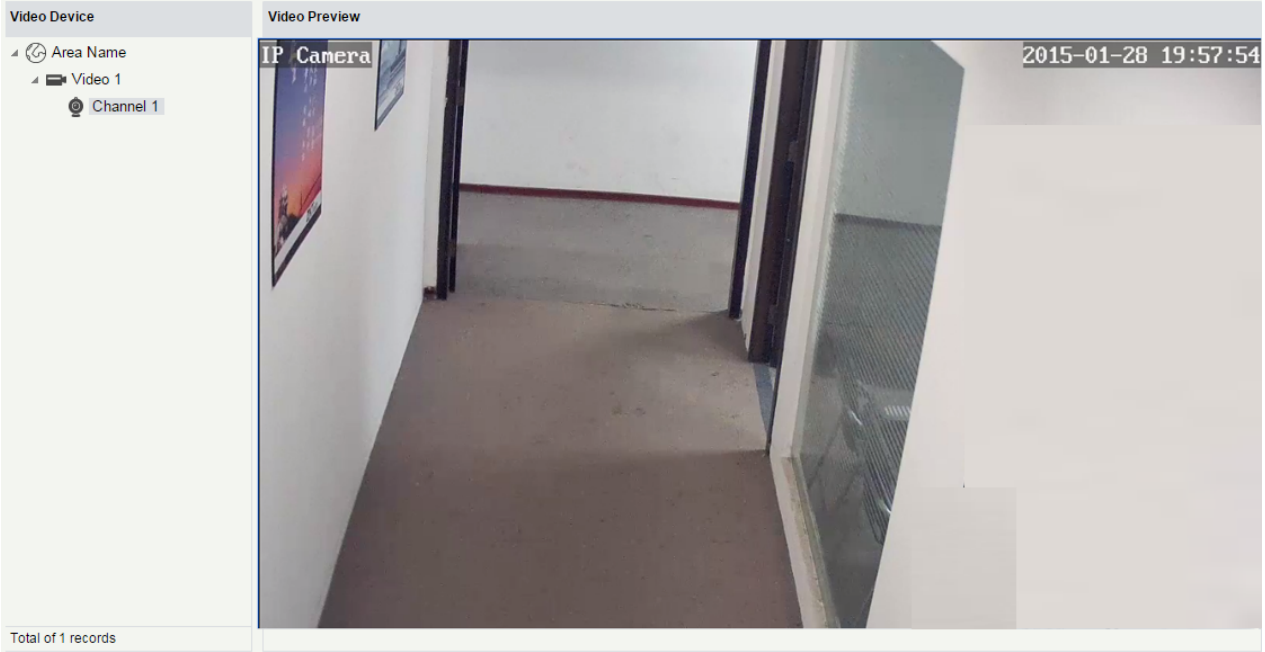
Fields are as follows:

Channel Name: Any characters within a length of 30.

Device Name, Channel Number and Channel Status are not editable in this page. You can modify them in Video Device. The channel number is the channel number in video device.

9.3 Video Preview

Click [Video] > [Video Device] > [Video Preview], the left side is the device and channel lists, click a channel to view the monitor screen.

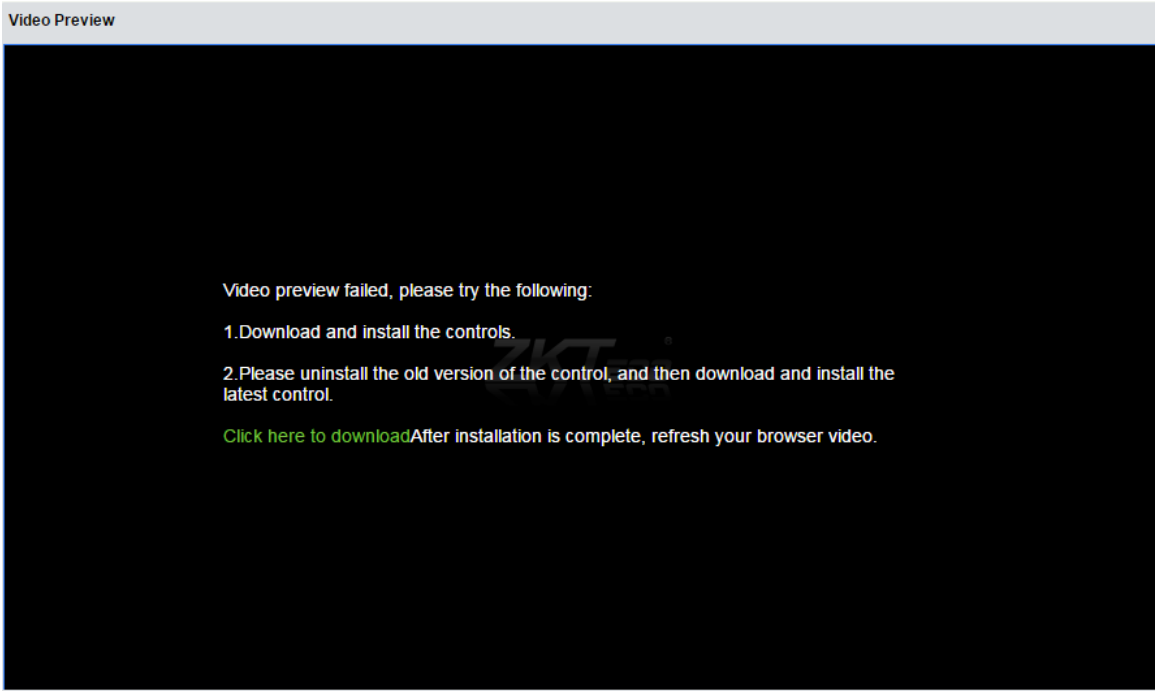


Re-click the channel to shut down the screen.

Notes:

1) A video can allow five users to preview at the same time. In chronological order, the exceeded users can not preview the video normally, and the page will be grey.

2) If there are no video controls in the system, the prompts will be displayed:

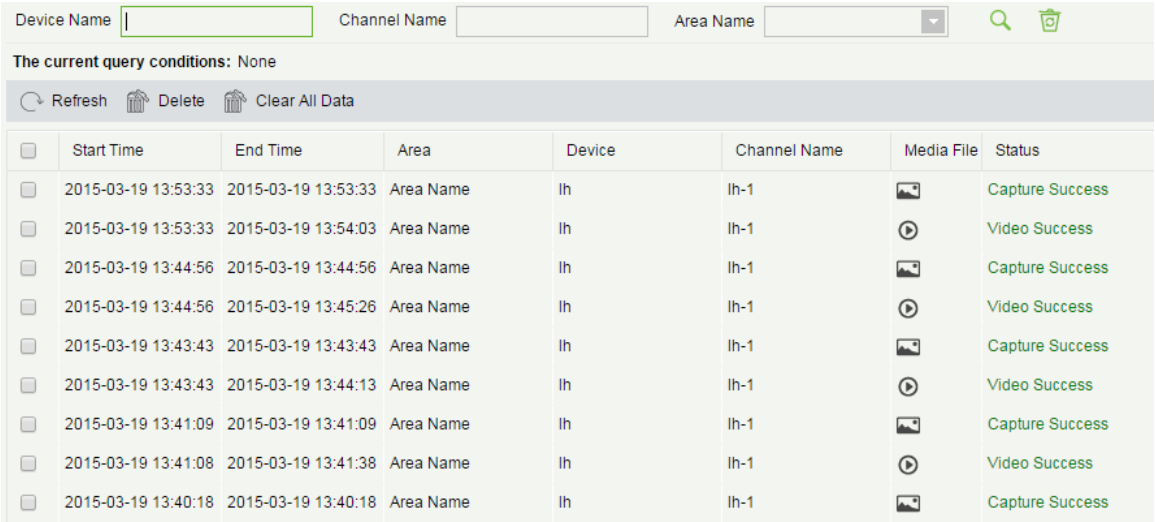


Click "Click here to download", the controls will be downloaded. Install the controls, and refresh the page, you can view the monitor screen normally. To prevent the video displayed abnormally, please install the controls that ZKBioSecurity offered.

9.4 Video Event Record

View the records of catching pictures and videos.

Click [Video] > [Video Device] > [Video Event Record]:



Start Time	End Time	Area	Device	Channel Name	Media File	Status
2015-03-19 13:53:33	2015-03-19 13:53:33	Area Name	Ih	Ih-1		Capture Success
2015-03-19 13:53:33	2015-03-19 13:54:03	Area Name	Ih	Ih-1		Video Success
2015-03-19 13:44:56	2015-03-19 13:44:56	Area Name	Ih	Ih-1		Capture Success
2015-03-19 13:44:56	2015-03-19 13:45:26	Area Name	Ih	Ih-1		Video Success
2015-03-19 13:43:43	2015-03-19 13:43:43	Area Name	Ih	Ih-1		Capture Success
2015-03-19 13:43:43	2015-03-19 13:44:13	Area Name	Ih	Ih-1		Video Success
2015-03-19 13:41:09	2015-03-19 13:41:09	Area Name	Ih	Ih-1		Capture Success
2015-03-19 13:41:08	2015-03-19 13:41:38	Area Name	Ih	Ih-1		Video Success
2015-03-19 13:40:18	2015-03-19 13:40:18	Area Name	Ih	Ih-1		Capture Success

The media file is:

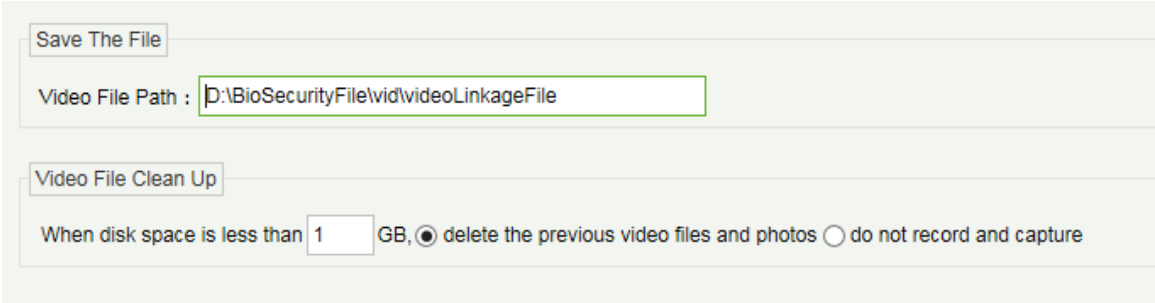
: Indicates that the linkage type is "Video", you can click to download this file. Please choose a third part of video player to play the file, or else it cannot be played normally.

: Indicates that the linkage type is "Capture", you can click to view this file.

Note: If the "Video" and "Capture" are both selected, there will be 2 records. For more details about the way to set the linkage type, please refer to Linkage Setting

9.5 Parameters

Click [Video] > [Video Device] > [Parameters]:



Video File Path: Path for storing files when the server records videos or capture images.

Video File Clean Up: When the disk space for storing video files is smaller than the pre-set value, you can choose to

delete the old video files or not to record videos or capture images. If you choose Delete, the software will delete the video files that are generated in the earliest day and continue to record videos; otherwise, the software does not record videos.

9.6 Solutions of Exceptions

1. Client browser cannot playback video, preview, or Real-Time Monitoring page has no video pops-up:

Firstly, Ensure IE11 and above version browser is available, client and Video Server are on the same network segment and the video ActiveX installation is successful. If the ActiveX installation fails, above all, uninstall the video ActiveX that were originally installed, run the "regsvr32-u NetVideoActiveX23.ocx"command, and then in the browser, set all the options in "Tools -> Internet Options -> Security -> Custom Level" on the ActiveX to "Enable or Prompt", re-open the browser, re-login screen and open the video preview page, run the button "all add items of the site".

2. The network or power of video device is shut off while previewing the video screen.

Check whether the network or power is connected normally. Refresh the page after ensuring that the connection is normal, refresh the page, and re-open the video preview.

3. In the E-Map, no video pops-up after clicking the camera icon:

Make sure to use IE11 and above version browser, client and Video Server on the same network segment and the video ActiveX installation is successful. Also, view whether the browser is preventing the temporary window pops up, if it is, change to allow window pops up to the site.

4. .Video linkage is triggered, the video server does not have video or size of the video file that the client downloads from the Video Server is 0kb:

First, ensure that the software server has set Time Server (keep the Windows time service and has set the NTP function of the video server), it is recommended to set the time interval of the video server smaller to ensure accurate synchronization software server and video server time, so as to keep the time consistent between software server and controllers. It is recommended set Linkage Recording Time more than 5 seconds, to avoid executing video linkage commands delay, which may lead to the downloaded 0kb video file.

5. The Video system is not normal to use in windows server 2008:

Desktop Experience feature needs to be added in windows server2008 before the normal use of the video.

Step 1: Run" services.msc" to open the "Service Manager".

Step2: Set the start type of "Windows Audio" and "Themes" as Automatically Start.

Step3: Run the service manager, click [Add functions], check the "Desktop Experience" box and click [Install]. Reboot the server after the installation is done.

6. The video downloaded to local cannot be played:

Please choose a third part of video player to play the file, or else it can't be played normally.

7. When the browser is chrom42 or above version, the system will prompt you to install video controls though

you have already installed.

The old NPAPI controls are disabled in chrom42 or above version. You should open the browser, and enter "chrome://flags/#enable-npapi" in address bar to enable the controls.

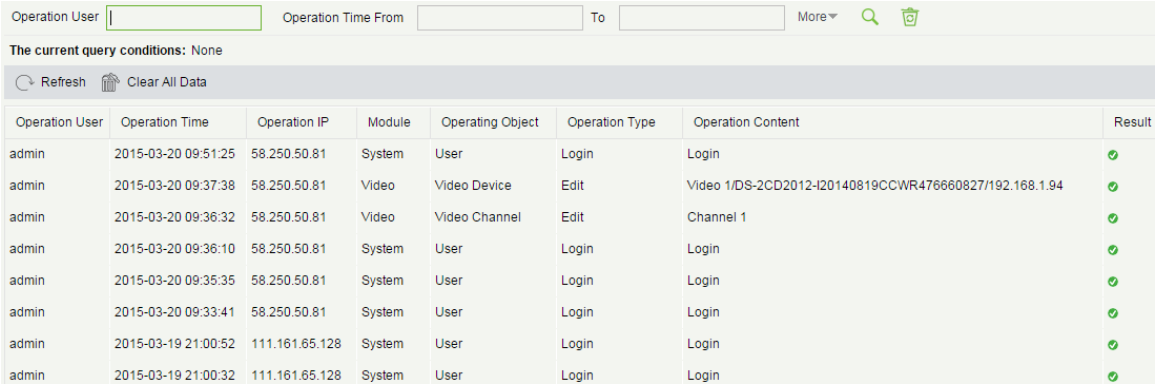
10 System Management

System settings primarily include assigning system users (such as company management user, registrar, access control administrator) and configuring the roles of corresponding modules, managing database, setting system parameters and view operation logs, etc.

10.1 Basic Management

10.1.1 Operation Logs

Click [System] > [Basic Management] > [Operation Log]:



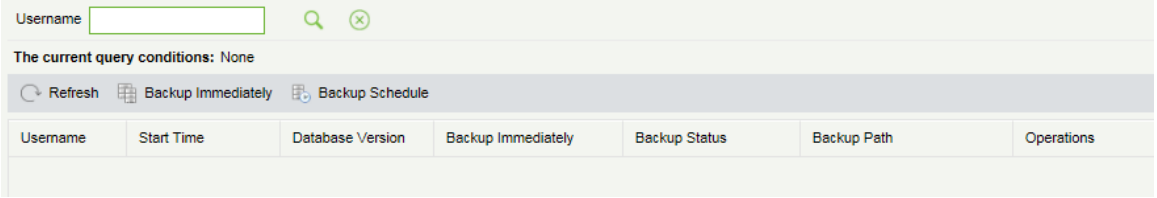
Operation User	Operation Time	Operation IP	Module	Operating Object	Operation Type	Operation Content	Result
admin	2015-03-20 09:51:25	58.250.50.81	System	User	Login	Login	
admin	2015-03-20 09:37:38	58.250.50.81	Video	Video Device	Edit	Video 1/DS-2CD2012-I20140819CCWR476660827/192.168.1.94	
admin	2015-03-20 09:36:32	58.250.50.81	Video	Video Channel	Edit	Channel 1	
admin	2015-03-20 09:36:10	58.250.50.81	System	User	Login	Login	
admin	2015-03-20 09:35:35	58.250.50.81	System	User	Login	Login	
admin	2015-03-20 09:33:41	58.250.50.81	System	User	Login	Login	
admin	2015-03-19 21:00:52	111.161.65.128	System	User	Login	Login	
admin	2015-03-19 21:00:32	111.161.65.128	System	User	Login	Login	

All operation logs are displayed in this page. You can query specific logs by conditions.

Clear All Data: Delete all logs in the system.

10.1.2 Database Management

Click [System] > [Basic Management] > [Database Management]:



Username	Start Time	Database Version	Backup Immediately	Backup Status	Backup Path	Operations

All history operation logs about database backup are displayed in this page. You can delete, backup and schedule backup database as required.

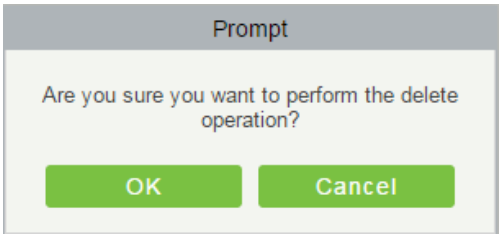
- Backup Immediately

Backup database to the path set in installation right now.

Note: The default backup path for the system is the path selected during the software installation. For details, refer to 《Software Installation Guide》.

- Delete

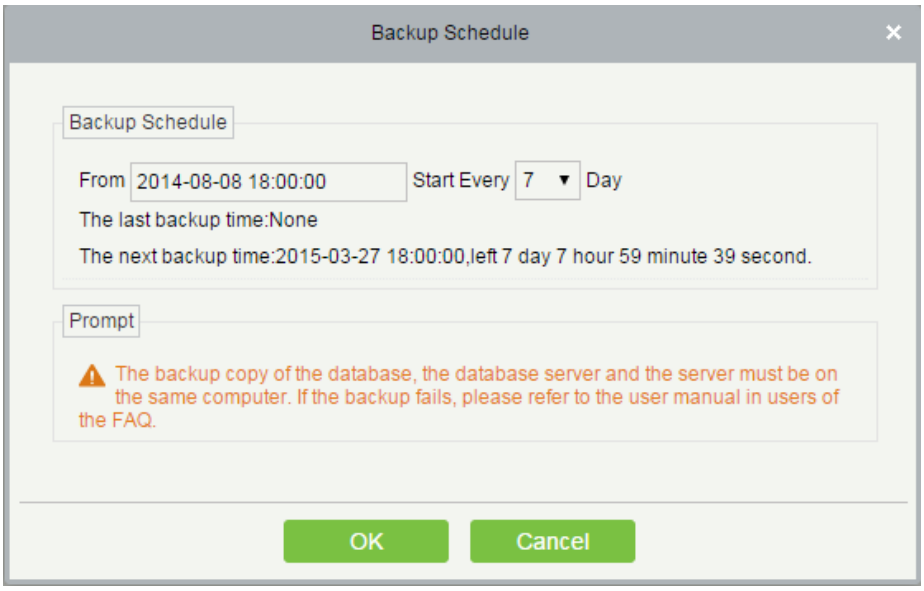
Select one or backup records to delete, click [Delete]:



Clcik [OK] to finish deleting.

- Backup Schedule

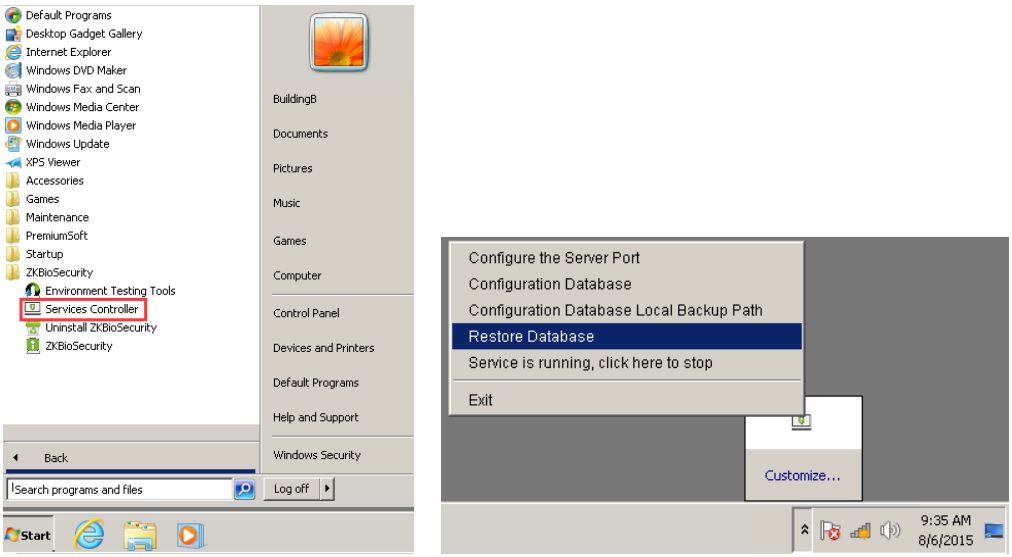
Click [Backup Schedule]:



Set the start time, set interval between two automatic backups, click [OK].

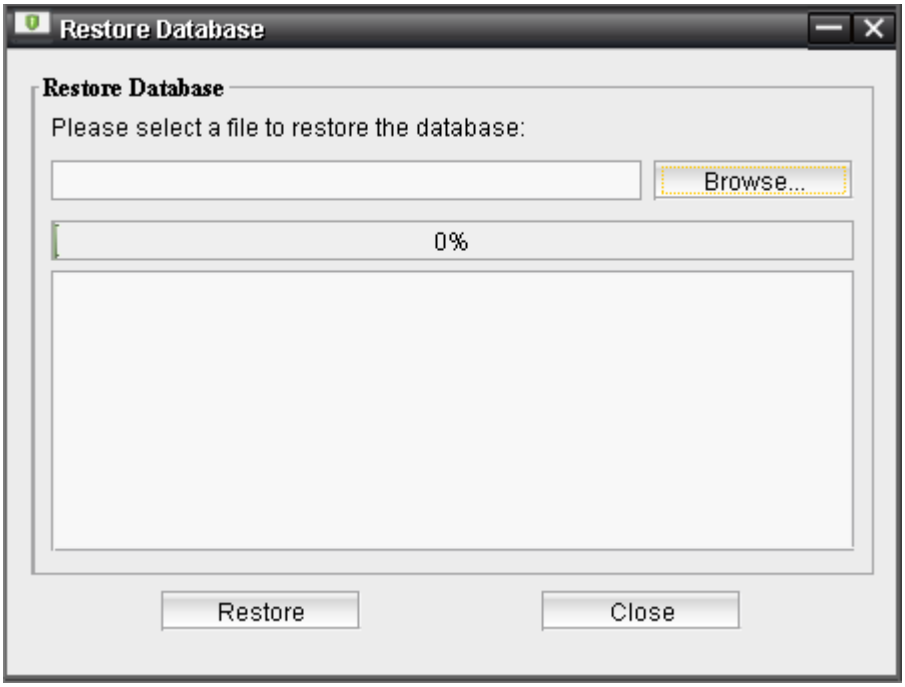
- Restore DataBase

1. Click the start menu of the PC→[All programs]→[ZKBioSecurity]→Then run "Services Controller", and you can find out the icon of "Services Controller" in Taskbar as follow, right click that icon, then left click "Restore Database".



2. In the popup window, click "Browse" to choose the backup file to restore the database.

Note: Before restoring a database, it is recommended that you back up the current database to avoid data loss.



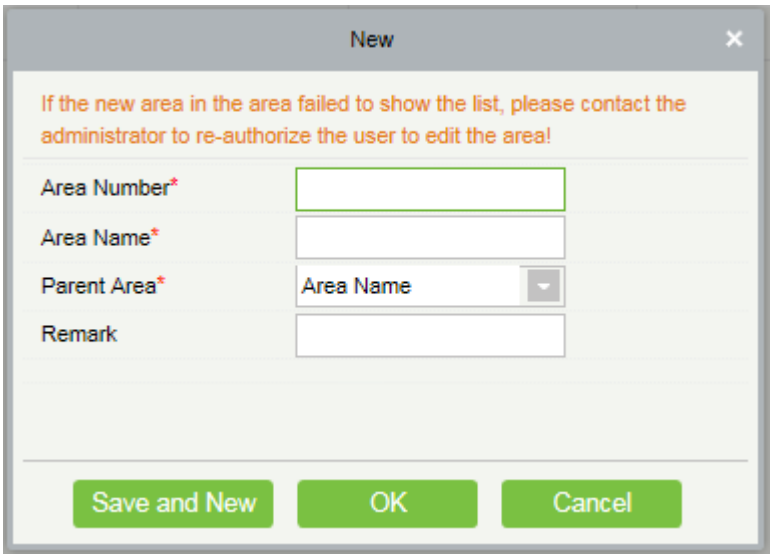
10.1.3 Area Setting

Area is a spatial concept which enables the user to manage devices in a specific area. After area setting, devices (doors) can be filtered by area upon real-time monitoring.

The system, by default, has an area named [Headquarters] and numbered [1].

- Add an Area

Click [System] > [Basic Management] > [Area] > [New]:



Fields are as follows:

Area Number: It must be unique.

Area Name: Any characters with a length less than 30.

Parent Area: Determine the area structure of system.

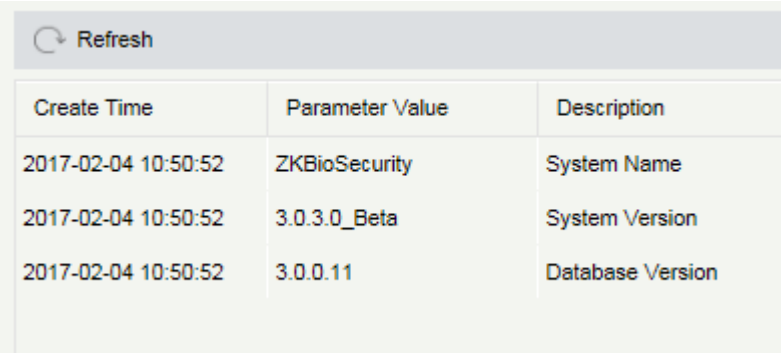
Click [OK] to finish adding.

- Edit/Delete an Area

Click [Edit] or [Delete] as required.

10.1.4 System Parameters

Click [System] > [System Parameter]:

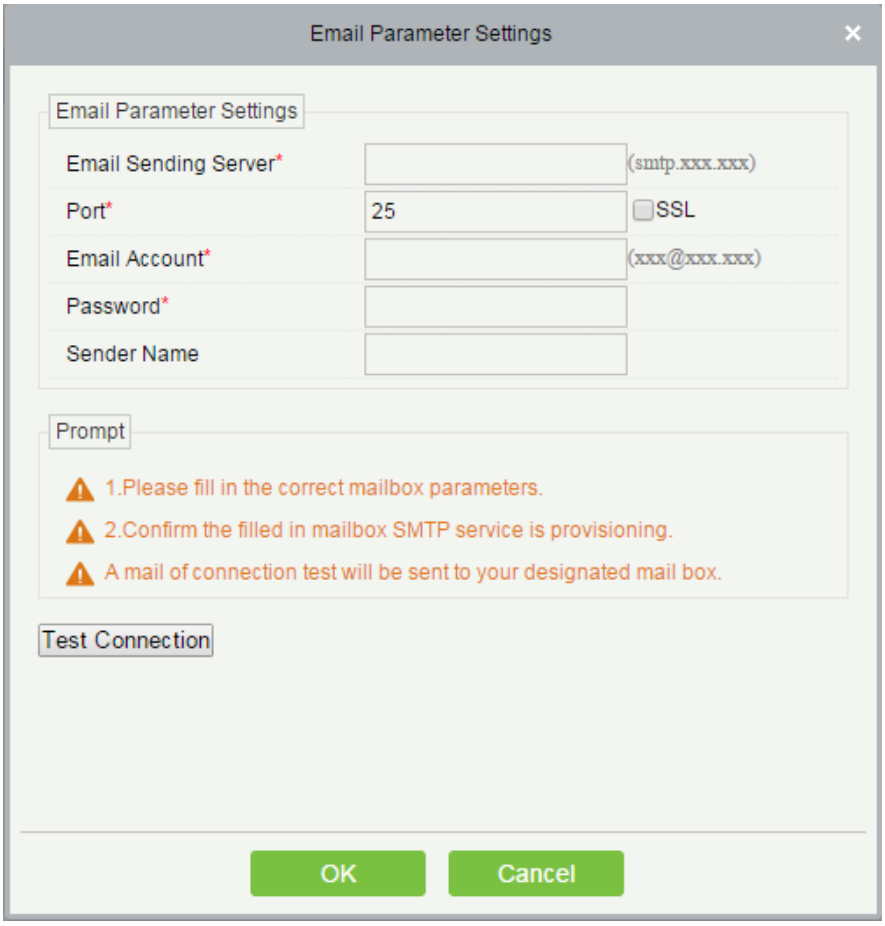


Click [Edit] to modify the system name.

10.1.5 E-mail Management

Set the email sending server information. The recipient e mail should be set in Linkage Setting.

Click [Basic Management] > [Email Management] > [Email Parameter Settings]:

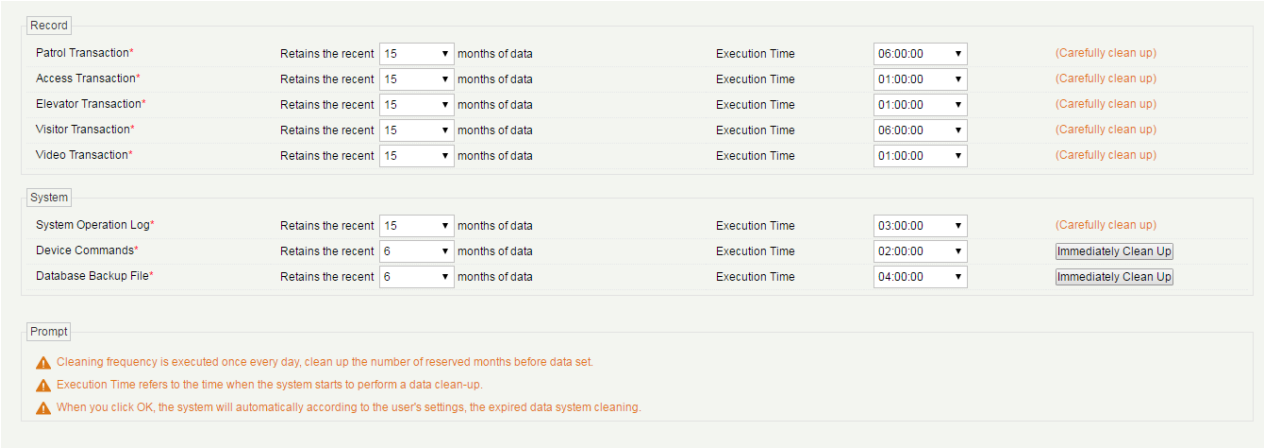


Note: The domain name of E-mail address and E-mail sending sever must be identical. For example, the Email address is: test@gmail.com, and the E-mail sending sever must be: smtp.gmail.com.

10.1.6 Data Cleaning

The data cleaning time settings are available to set. The data volume will increase with the use of the system. To save the storage space on the disks, you need to periodically clean expired data generated by the system.

Click [Basic Management] > [Email Management] > [Email Parameter Settings]:

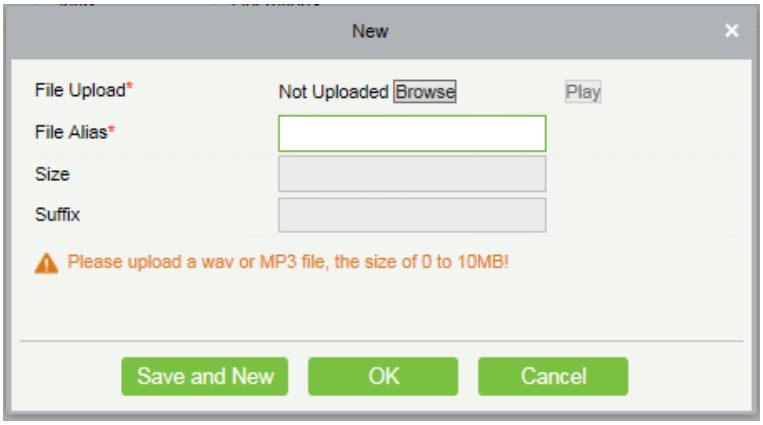


The system executes Immediately Clean Up operation after it is clicked and [OK] is clicked. Without clicking [OK], the system will not clean data.

Note: In order to reduce the load of the system and not to affect the normal running, the cleaning time should be set in the 1 o'clock am.

10.1.7 Audio File

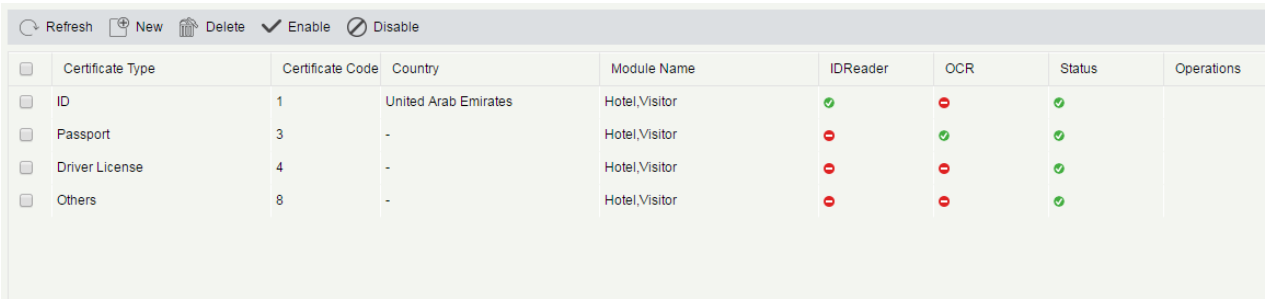
Click [Basic Management] > [Audio File] > [New]:



You can upload a sound from the local. The file must be in wav or mp3 format, and it must not exceed 10M.

10.1.8 Certificate Type

The types of certificates available for registration in the system, where you can add, delete, enable, disable these document types as follows:



Certificate Type	Certificate Code	Country	Module Name	IDReader	OCR	Status	Operations
ID	1	United Arab Emirates	Hotel,Visitor	✓	⊖	✓	
Passport	3	-	Hotel,Visitor	⊖	✓	✓	
Driver License	4	-	Hotel,Visitor	⊖	⊖	✓	
Others	8	-	Hotel,Visitor	⊖	⊖	✓	

- Add

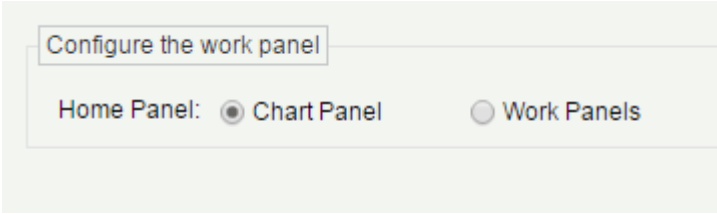
Click New to input the Certificate Type Name, click [OK].

- Delete/Enable/Disable

Select the Certificate Type, click [Delete]/ [Enable]/ [Disable]], perform the appropriate action. "√"means to enable the certificate, "—"means to disable the certificate.

10.1.9 Parameters

Configure the system-related settings parameters, as shown below:



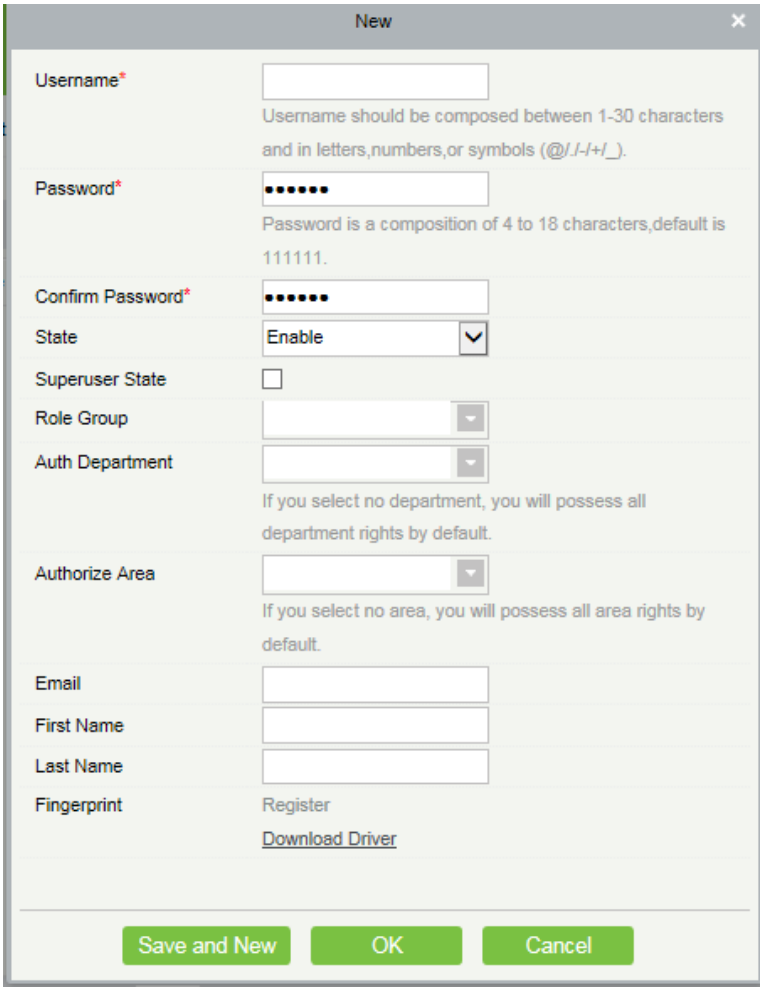
Configure the work panel: You can choose chart panel or work panels as the home panel style.

10.2 Authority Management

10.2.1 User

Add new user and implement levels for the user in the system.

1. Click [System Management] > [Authority Management] > [User] > [New]:



Fields are as follows:

Username: Any characters within a length of 30.

Password: The length must be more than 4 digits and less than 18 digits. The default password is 111111.

State: Enable or disable the user to operate the system.

Super User State: Enable or disable the user to have the superuser's levels.

Role Group: Non-super user needs to choose a role group to get the leves of the group. The role group must be set in advanced in Role Group.

Authorize Department: No department means the user possesses all department rights by default.

Authorize Area: No area means the user possesses all area rights by default.

Fingerprint: Enroll the user fingerprint or duress fingerprint. The user can login the system by pressing the enrolled fingerprint. If the user presses the duress fingerprint, it will trigger the alarm and send the signal to the system.

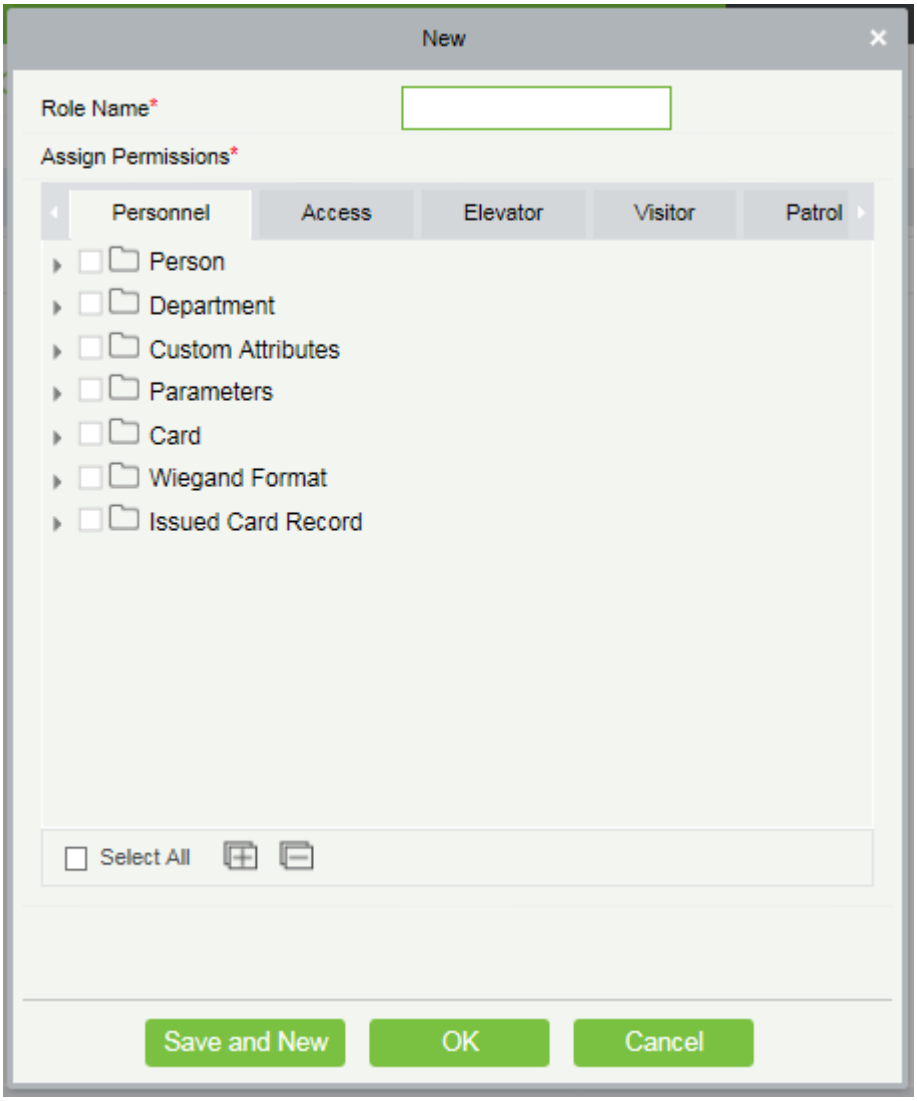
2. After editing, click [OK] to complete user adding, and the user will be shown in the list.

Click [Edit] or [Delete] as required.

10.2.2 Role

When using the system, the super user needs to assign different levels to new users. To avoid setting users one by one, you can set roles with specific levels in role management, and assign appropriate roles to users when adding users. A super user has all the levels, can assign rights to new users and set corresponding roles (levels) according to requirements.

1. Click [System Management] > [Authority Management] > [Role] > [New]:



2. Set the name and assign permissions for the role.

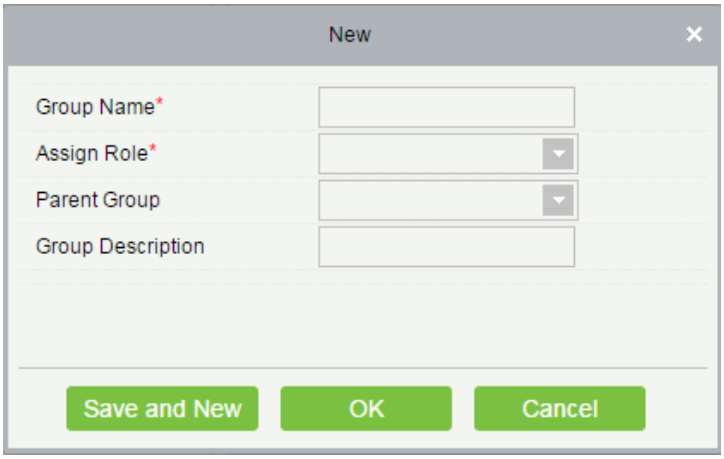
3. Click [OK] to save.

10.2.3 Role Group

You can add role groups to the system. A role group has all the levels assigned to roles within the group. An appropriate role group can be directly assigned to a newly-added user. Include all the levels for using all the service

modules of the system and the system setup module. The default super user of the system has all the levels, can assign rights to new users and set corresponding role groups (levels) according to requirements.

1. Click [System Management] > [Authority Management] > [Role Group] > [New]:

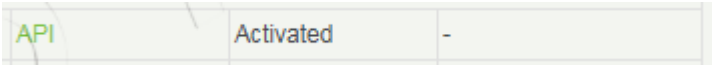


2. Set the name and parent group, assign role for the group.

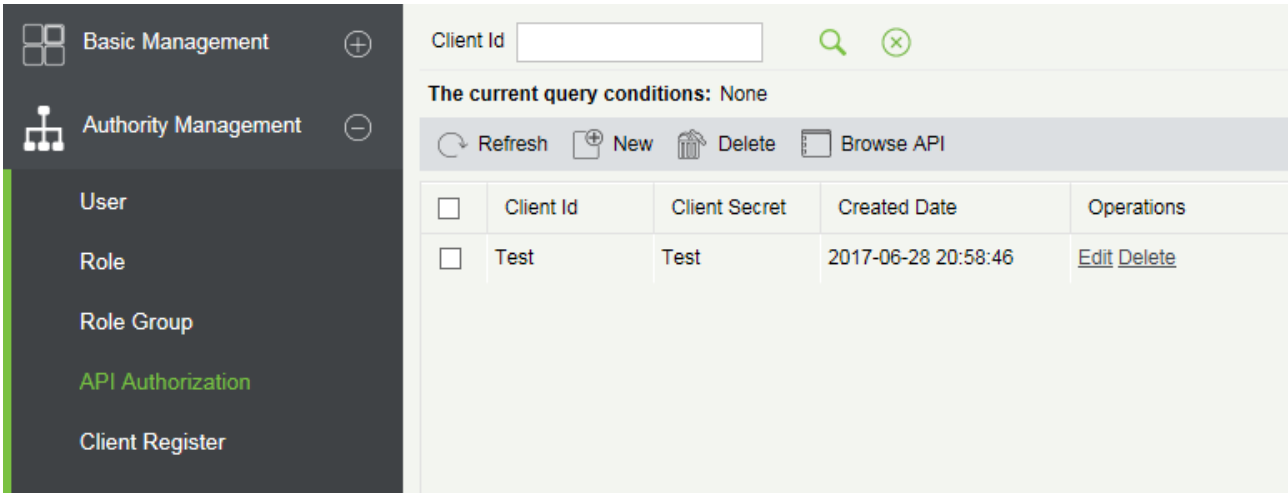
3. Click [OK] to save.

10.2.4 API Authorization

1. Activate the API through authorization. You can check whether the API has been activated on the About page (The API Authorization menu is displayed in System Management only when the API is activated), as shown in the following figure:

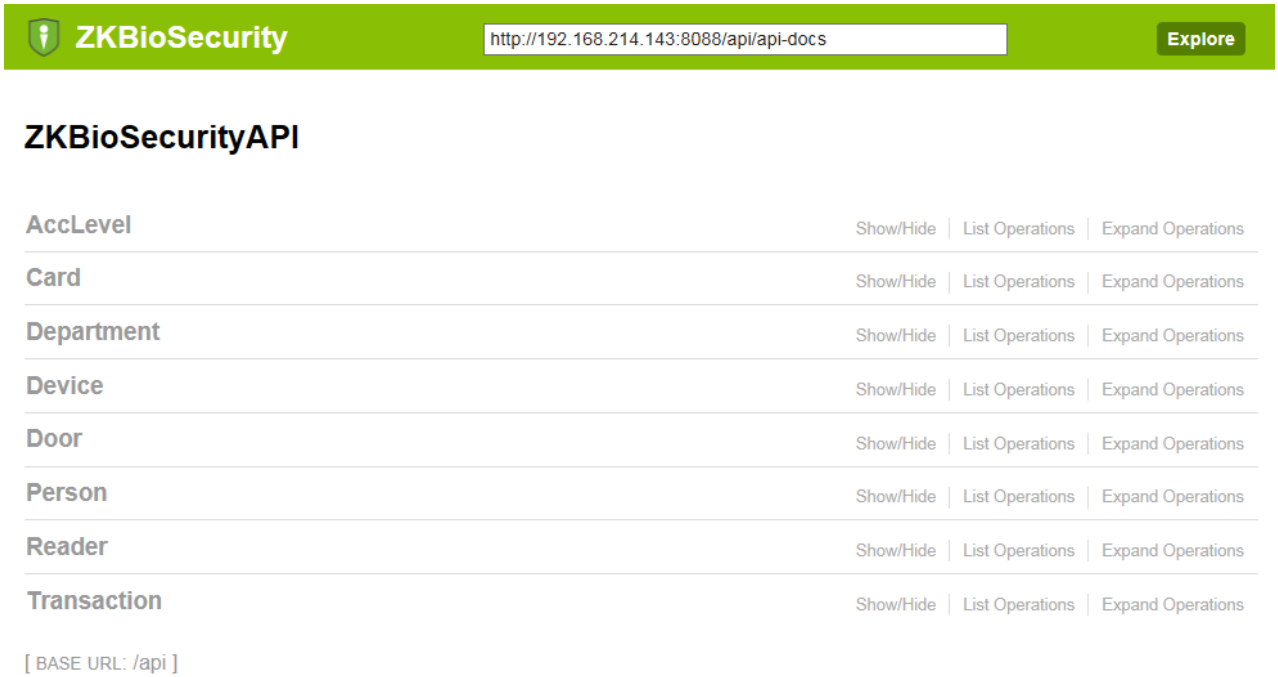


2. Log in to the system (as the super user, for example, admin) to enter the software. Click [System Management] > [Authority Management] > [API Authorization]. Add a client ID, which must be unique, and a client secret, which will be used when the API is invoked (only when the client ID and secret are added can the next API operation page be displayed normally. Otherwise, the access is abnormal):

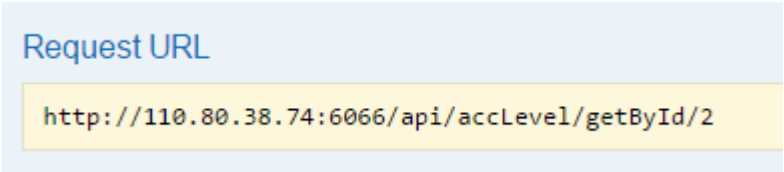


3. After the client ID and secret are added, click Browse API on the API Authorization page to skip to the API operation page (The page of the ZKBioSecurity system must be open for normal access of the API operation page).

This page provides multiple APIs:



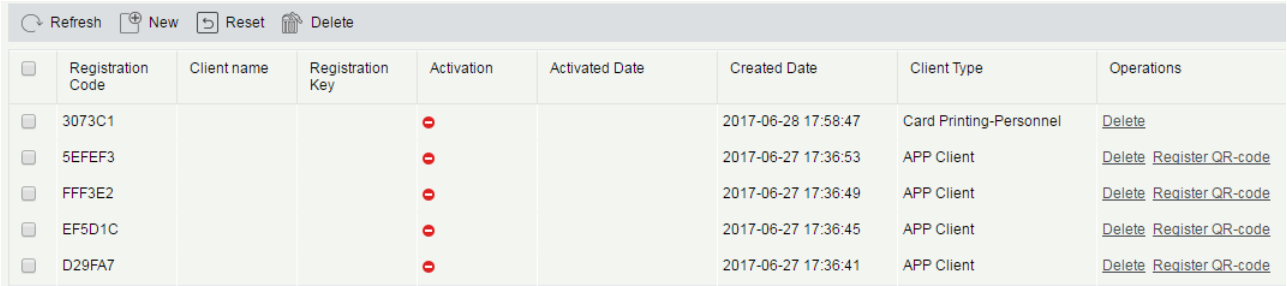
When APIs are invoked, URLs of all request APIs must contain the access_token parameter, whose value is determined by the client key configured on the background (if there are multiple keys, only one is selected), for example:



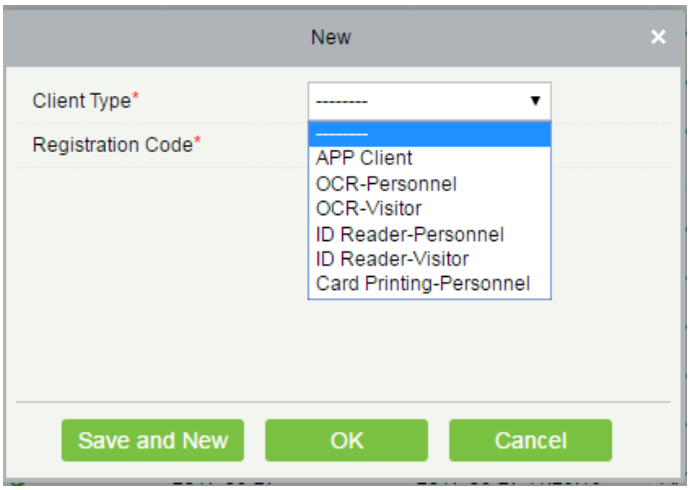
The access_token parameter must be added when the API is invoked (one request URL can be invoked): http://110.80.38.74:6066/api/accLevel/getById/2.

10.2.5 Client Register

You can add client types for the system and generate registration codes for client registrations of each module function. The number of allowed clients is controlled by the number of allowed points.



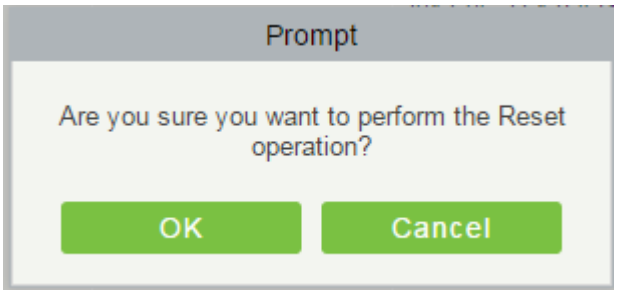
1. Click [System Management] > [Authority Management] > [Client Authorization] > [New] to go to the [New] page:



Client Type: The value can be APP Client, OCR-Personnel, OCR-Visitor, ID Reader-Personnel, ID Reader-Visitor or Card Printing- Personnel.

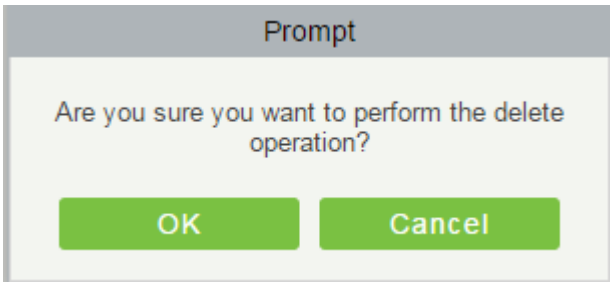
Registration Code: The registration code for [APP Client] is used under [Network Settings] on the APP login page and that for [Print Card-Personnel] is used under [Parameter Settings] > [Client Registration]. Only new registration codes added on the server are authorized and one registration code can be used by only one client.

2. To reset a client, select the client and click [Reset].



Click [OK] to reset the client.

3. To delete a client, select the client and click [Delete].



Click [OK] to delete the client.

10.3 Communication

Click [System Management] > [Communication] > [Device Commands], the commands lists will displayed.

Serial No. Back To Results ---------

The current query conditions: None

Refresh Clear Commands Export

ID	Serial No.	Content	Submit Time	Return Time	Returned Value
108	4602357070864	DATA QUERY tablename=transaction,fielddesc=*,filter=NewRecord	2015-03-20 00:00:00		
107	6564150400091	DATA QUERY tablename=transaction,fielddesc=*,filter=NewRecord	2015-03-20 00:00:00		
106	6564150400091	DATA QUERY tablename=transaction,fielddesc=*,filter=NewRecord	2015-03-19 20:42:02	2015-03-19 20:42:06	0
105	6564150400091	SET OPTIONS DateTime=489098522	2015-03-19 20:42:02	2015-03-19 20:42:06	0
104	6564150400091	DATA UPDATE userauthorize Pin=33 AuthorizeTimezoneId=1 Authorizet	2015-03-19 20:42:02	2015-03-19 20:42:12	-10053
103	6564150400091	DATA UPDATE user CardNo=2483386 Pin=33 Password= Group=0 Star	2015-03-19 20:42:02	2015-03-19 20:42:12	0
102	6564150400091	SET OPTIONS Door1Drivertime=5,Door1KeepOpenTimeZone=0,Door1V	2015-03-19 20:42:02	2015-03-19 20:42:09	0
101	6564150400091	DATA UPDATE timezone TimezoneId=1 SunTime1=2359 SunTime2=0 S	2015-03-19 20:42:02	2015-03-19 20:42:06	0
100	6564150400091	SET OPTIONS DateTime=489098522	2015-03-19 20:42:02	2015-03-19 20:42:03	0

If the returned value is more than or equal to 0, the command is successfully issued. If the returned value is less than 0, the command is failed to be issued.

Clear Commands: Clear the command lists.

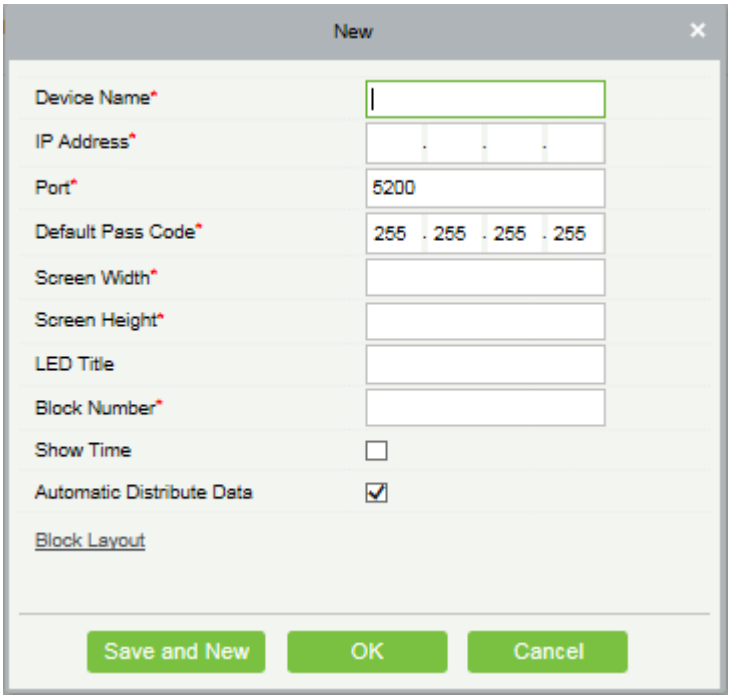
Export: Export the command lists to local host.

10.4 Extended Management

10.4.1 LED Device

- Add

Click [System]> [Extended Management]> [LED Device]> [New]. The page is displayed as follows:



Device Name: Name of the LED device.

IP Address: IP address of the LED device.

Communication Port: The default port is 5200.

Default Pass Code: The default value is 255.255.255.255.

Screen Width: Width of the dot matrix (resolution).

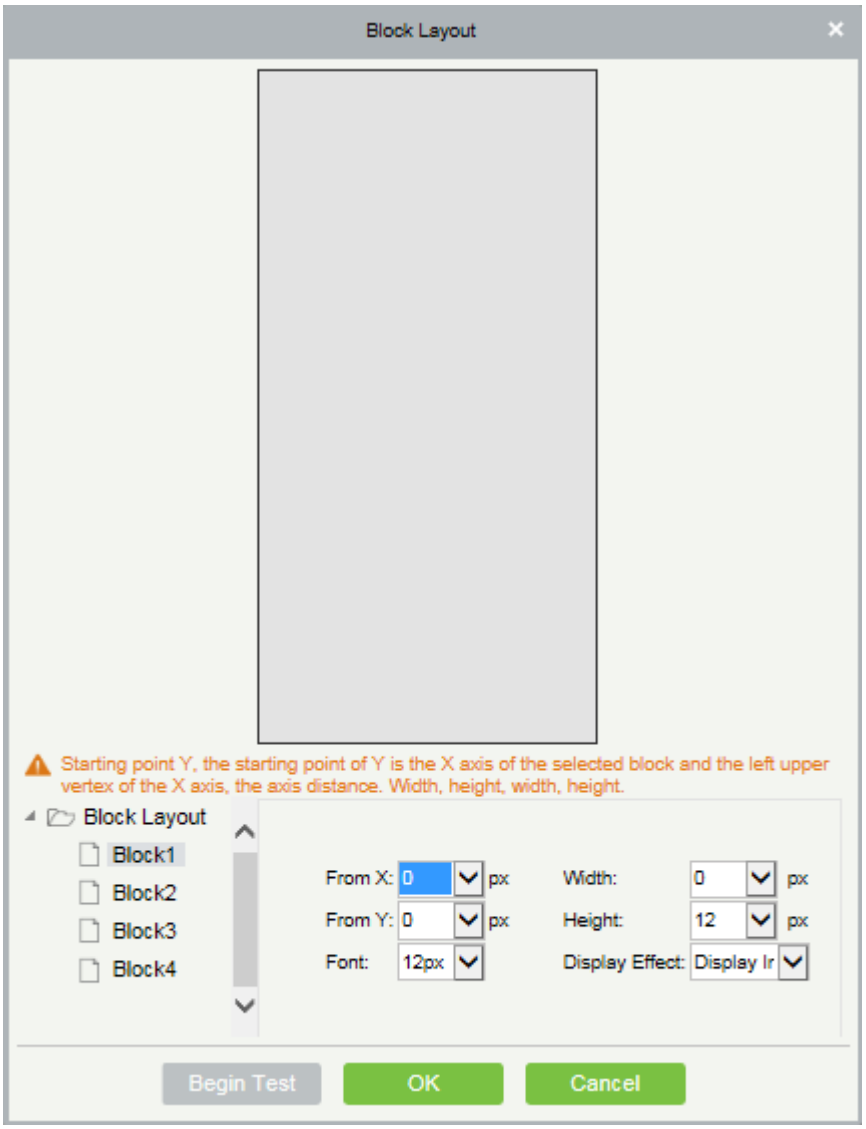
Screen Height: Height of the dot matrix (resolution).

LED Title: Select whether to display the title. If the parameter is left blank, the title is not displayed.

Block Number: Number of blocks that the LED is divided into (Note that the blocks do not contain the title and system time blocks).

Automatic Distribute Data: By default, this parameter is selected. You send data to the LED in the access control module only when you select this parameter. Otherwise, the content to be sent needs to be manually defined.

Block Layout: After you click the block coordinate, the following box is displayed:



Notes:

1. Parameters must be set for each block.
2. The height of each block must be equal to or larger than 12. Otherwise, the letters cannot be completely displayed.
3. The total height of all blocks cannot be larger than the screen height.

- Edit

Click a device name or [Edit] under [Operation] to go to the edit page. After editing the device, click [OK] to save the setting.

- Delete

Click a device name or [Delete] under [Operation] in the device list and click [OK] to delete the device or click [Cancel] to cancel the operation. Select one or more devices and click [Delete] above the list and click [OK] to delete the selected device(s) or click [Cancel] to cancel the operation.

- Enable and Disable

Select a device and click [Enable/Disable] to start/stop using the device. If the device is enabled, data is transmitted to the device. Otherwise, no data is transmitted to the device.

- Synchronize All Data To Devices

Synchronize the LED block layout and LED data setting in the system to the device. Select a device, click [Synchronize All Data To Devices], and then click [Synchronize] to synchronize the data.

- Restart

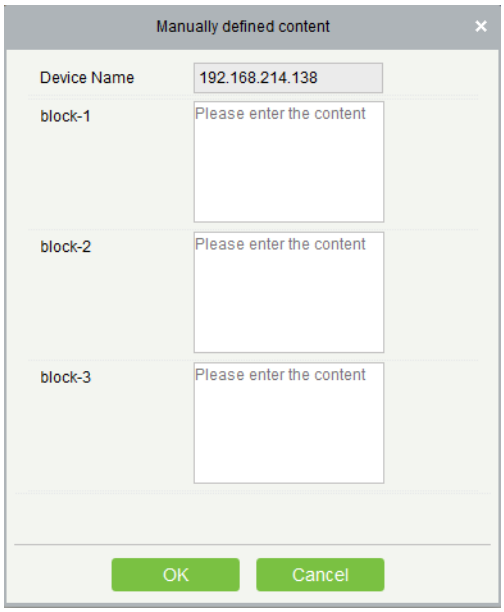
After you restart the device, the LED control card system will be restarted, data on the screen is cleared and data saved in the system is restored. After the device is successfully restarted, click [Synchronize All Data To Devices] to display all distributed content on the LED screen.

- Modify IP address

Modify the IP address of the device. The default IP address of the control card is 192.168.1.222.

- Manually defined content

Select a device and click [Manually defined content]. The page is displayed as follows:



Notes:

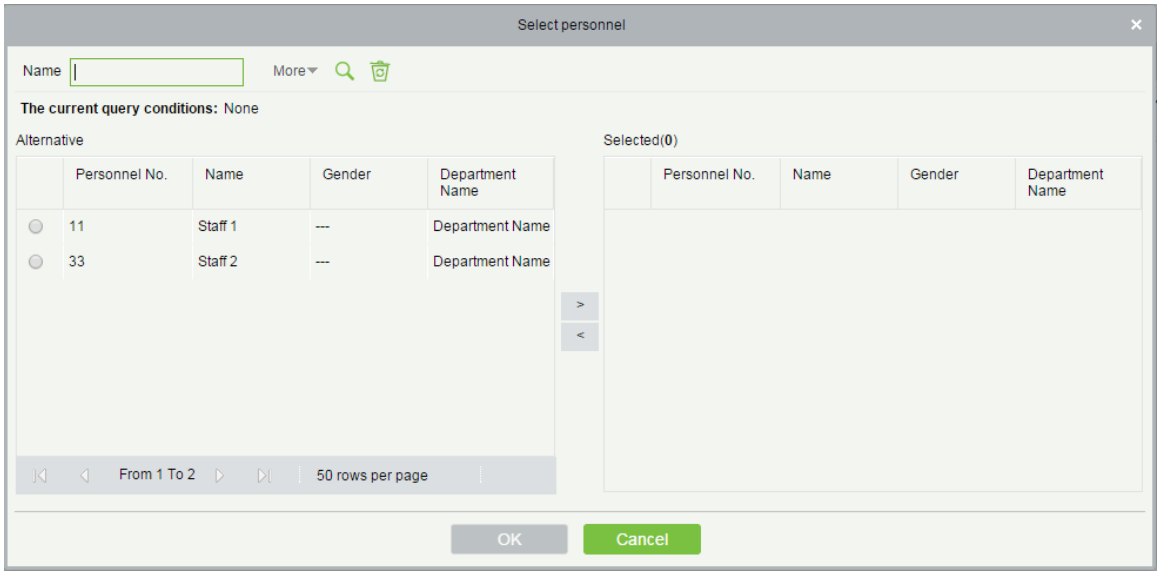
1. At least one block must be selected for distribution of manually defined content.
2. After the manually defined content is selected, the access control module cannot send data to the LED device.

11 Appendices

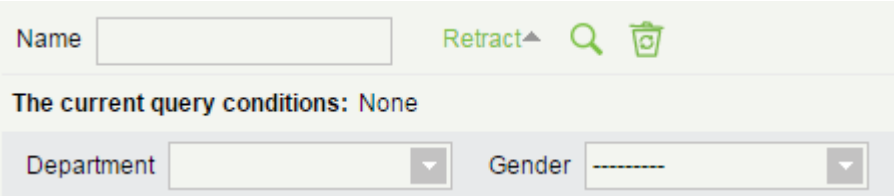
11.1 Common Operations

- Select Personnel

The selected personnel page in the system is always as below:



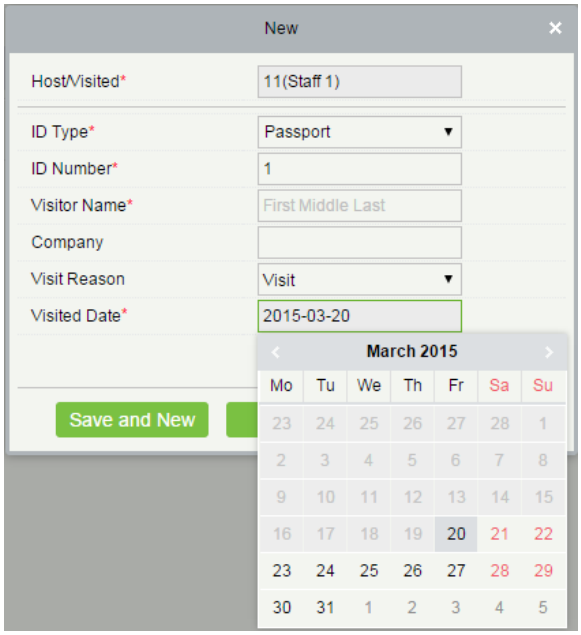
You can select the personnel in the Alternative list, or you can also click [More] to filter by gender or department.



Click > to move the selelcted personnel in to the selected lists. If you want to cancel the movement, click <.

- Set Date and Time

Click the date and time box:

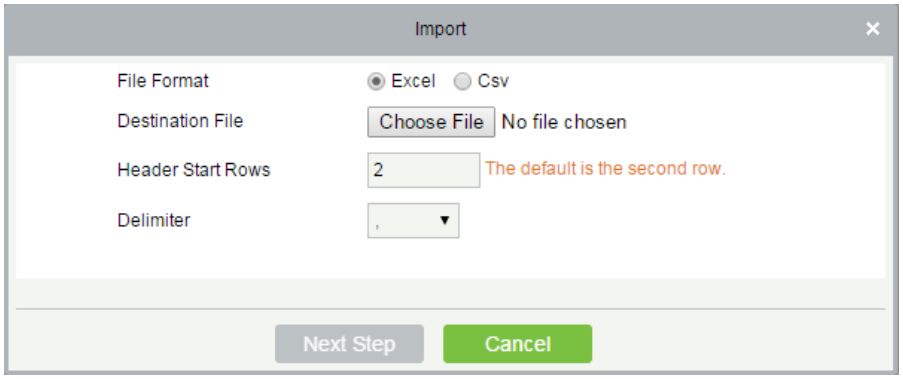


Click the Year to select by rolling click ◁ or ▷. Clcik the Month and Date to select directly.

- Import (take the personnel list importing as an example)

If there is a personnel file in your computer, you can Import it into the system.

1. Click [Import]:



Fields are as follows:

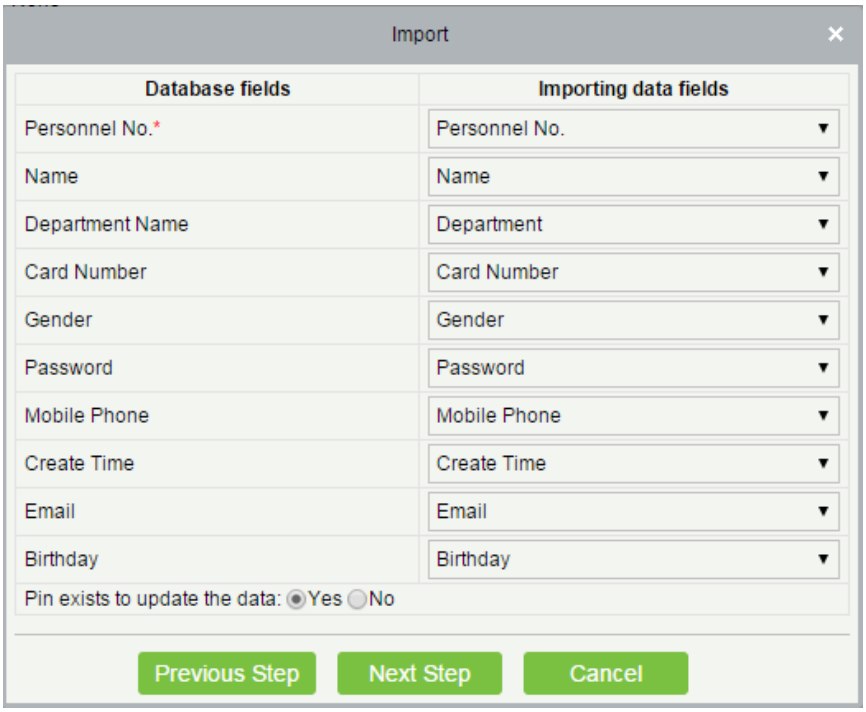
File Format: Select the file format to be imported.

Destination File: Choose file to be imported.

Head Start Rows: which row is the first row to be imported.

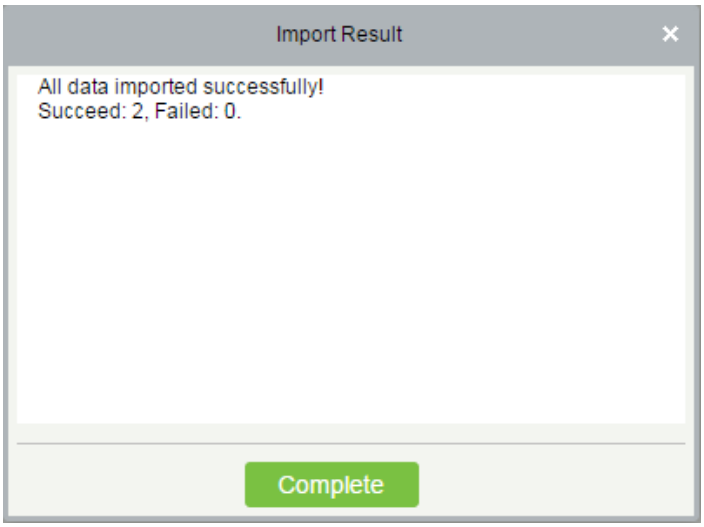
Delimiter: The delimiter of CSV format file, only "." and "-" are available.

2. Click [Next Step]:



3. Seletct the fieds to be imported to the system. "----------" indicates the fileds will not be imported.

4. Click [Next Step]:



The data is imported successfully.

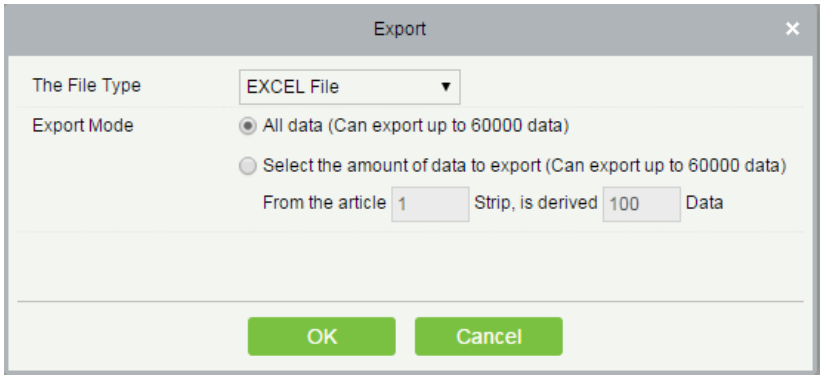
Notes:

1) When importing department table, department name and department number must not be empty, the parent department can be empty. Duplicated number does not affect the operation, it can be modified manually.

2) When importing personnel table, personnel number is required. If the personnel number already exists in the database, it will not be imported.

- Export (take the personnel list exporting as an example)

1. Click [Export]:



2. Select the file format and export mode to be exported. Click [OK].

3. You can view the file in your local drive.

Note: 10000 records are allowed to export by default, you can manually input as required.

11.2 Access Event Type

- Normal Events

Normal Punch Opening: In [Only Card] verification mode, the person having open door levels punch card at valid time period, open the door, and trigger the normal event.

Normal Press Fingerprint Opening: In [Only Fingerprint] or [Card or Fingerprint] verification mode, the person having open door levels press fingerprint at valid time period, the door is opened, and trigger the normal event.

Card and Fingerprint Opening: In [Card and Fingerprint] verification mode, the person having the open permission, punch the card and press the fingerprint at the valid time period, and the door is opened, and trigger the normal event.

Exit button Open: press the exit button to open the door within the door valid time zone, and trigger this normal event.

Trigger the exit button (locked): indicates the normal event triggered by pressing the exit button when the exit button is locked

Punch during Normal Open Time Zone: At the normal open period (set normal open period for a single door or for first-person normally open), or through the remote normal open operation, the person having open door permission punch effective card at the opened door to trigger this normal events.

Press Fingerprint during Normal Open Time Zone: At the normal open period (set normal open period for a single door or for first-person normally open), or through the remote normal open operation, the person having open door permission press the effective fingerprint at the opened door to trigger this normal events.

First-Person Normally Open (Punch Card): In [Only Card] verification mode, the person having first-person normally open permission, punch at the setting first-person normally open time period (the door is closed), and trigger the normal event.

First-Person Normally Open (Press Fingerprint): In [Only Fingerprint] or [Card plus Fingerprint] verification mode,

the person having first-person normally open permission, press the fingerprint at the setting first-person normally open period (the door is closed), and trigger the normal event.

First-Person Normally Open (Card plus Fingerprint): In [Card plus Fingerprint] verification mode, the person having first-person normally open permission, punch the card and press the fingerprint at the setting first-person normally open period (the door is closed), and trigger the normal event.

Normal Open Time Zone Over: After the normal open time zone over, the door will close automatically.

Remote Normal Opening: When set the door state to normal open in the remote opening operation, this normal event is triggered.

Cancel Normal Open: When Punch the valid card or use remote opening function to cancel the current door normal open state, this normal event is triggered.

Disable Intraday Passage Mode Time Zone: In door normal open state, punch effective card for five times (must be the same user), or select [Disable Intraday Passage Mode Time Zone] in remote closing operation, and this normal event is triggered.

Enable Intraday Passage Mode Time Zone: If the intraday passage mode time zone is disabled, punch effective card for five times (must be the same user), or select [Enable Intraday Passage Mode Time Zone] in remote opening operation, and this normal event is triggered.

Multi-Person Opening Door (Punching): In [Only Card] verification mode, Multi-Person combination can be used to open the door. After the last card is verified, the system trigger this normal event.

Multi-Person Opening Door (Press Fingerprint): In [Only Fingerprint] or [Card plus Fingerprint] verification mode, Multi-Person combination can be used to open the door. After the last fingerprint is verified, the system trigger this normal event.

Multi-Person Opening Door (Card plus Fingerprint): In [Card plus Fingerprint] verification mode, Multi-Person combination can be used to open the door. After the last card plus fingerprint is verified, the system trigger this normal event.

Emergency Password Opening Door: Emergency password (also known as super password) set for the current door can be used for door open. This normal event will be triggered after the emergency password is verified.

Opening Door during Normal Open Time Zone: If the current door is set a normally open period, the door will open automatically after the setting start time has expired, and this normal event will be triggered.

Linkage Event Triggered: After linkage configuration takes effect, this normal event will be triggered.

Cancel Alarm: When the user cancels the alarm of corresponding door successful, this normal event will be triggered.

Remote Opening: When the user opens a door by [Remote Opening] successful, this normal event will be triggered.

Remote Closing: When the user closes a door by [Remote Closing] successful, this normal event will be triggered.

Open Auxiliary Output: In linkage setting, if the user selects Auxiliary Output for Output Point, selects Open for Action Type, this normal event will be triggered when the linkage setting takes effect.

Close Auxiliary Output: In linkage setting, if the user selects Auxiliary Output for Output Point, selects Close for Action Type, or closes the opened auxiliary output by [Door Setting] > [Close Auxiliary Output], this normal event

will be triggered.

Door Opened Correctly: When the door sensor detects the door has been properly opened, triggering this normal event.

Door Closed Correctly: When the door sensor detects the door has been properly closed, triggering this normal event.

Auxiliary Input Point Disconnected: Will be triggered auxiliary input point is disconnected.

Auxiliary Input Point Shorted: When the auxiliary input point short circuit, trigger this normal event.

Device Start: Will be triggered if device starts (This event of PULL devices will not appear in real-time monitoring and can be viewed only in event records of reports).

- Abnormal Events

Too Short Punch Interval: When the interval between two punching is less than the set time interval, this abnormal event will be triggered.

Too Short Fingerprint Pressing Interval: When the interval between two fingerprints pressing is less than the set time interval, this abnormal event will be triggered.

Door Inactive Time Zone (Punch Card): In [Only Card] verification mode, if the user having the door open permission punch but not at door effective period of time, this abnormal event will be triggered.

Door Inactive Time Zone (Press Fingerprint): If the user having the door open permission, press the fingerprint but not at the door effective time period, this abnormal event will be triggered.

Door Inactive Time Zone (Exit Button): If the user having the door open permission, press exit button but not at the effective period of time, this abnormal event will be triggered.

Illegal Time Zone: If the user with the permission of opening the door, punches during the invalid time zone, this abnormal event will be triggered.

Illegal Access: If the registered card without the permission of current door is punched to open the door, this abnormal event will be triggered.

Anti-Passback: When the anti-pass back takes effect, this abnormal event will be triggered.

Interlock: When the interlocking rules take effect, this abnormal event will be triggered.

Multi-Person Verification (Punching): When Multi-Person combination opens the door, the card verification before the last one (whether verified or not), this abnormal event will be triggered.

Multi-Person Verification (Press Fingerprint): In [Only Fingerprint] or [Card or Fingerprint] verification mode, When Multi-Person combination opens the door, the fingerprint verification before the last one (whether verified or not), this abnormal event will be triggered.

Unregistered Card: If the current card is not registered in the system, this abnormal event will be triggered.

Unregistered Fingerprint: If the current fingerprint is not registered or it is registered but not synchronized with the system, this abnormal event will be triggered.

Opening Door Timeout: If the door sensor detects that it is expired the delay time after opened, if not close the door, this abnormal event will be triggered.

Card Expired: If the person with the door access level, punches after the effective time of the access control and cannot be verified, this abnormal event will be triggered.

Fingerprint Expired: If the person with the door access permission, presses fingerprint after the effective time of the access control and cannot be verified, this abnormal event will be triggered.

Password Error: If using [Card plus Password] verification mode, duress password or emergency password to open door, this abnormal event will be triggered.

Failed to Close door during Normal Open Time Zone: If the current door is in normal open state, but the user can not close it by [Remote Closing], this abnormal event will be triggered.

Verification Mode Error: If the user opening door mode is inconsistent with that set for current door, this abnormal event will be triggered.

Background Verification Failed: If the background verification fails, this abnormal event will be triggered.

Background Verification Success: If the background verification succeeds, this abnormal event will be triggered.

Background Verification Timeout: If no background verification result is returned in the specified period, this abnormal event will be triggered.

Multi-Person Verification Failed: When Multi-Person combination opens the door, the verification is failed, and triggers this abnormal event.

- Alarm Events

Duress Password Opening Door: Use the duress password of current door for verifying successfully and trigger this alarm event.

Duress Fingerprint Opening Door: Use the duress fingerprint of current door for verifying successfully and trigger this alarm event.

Duress Opening Door Alarm: Use the duress password or duress fingerprint set for current door for verifying successfully and trigger this alarm event.

Opened Accidentally: Except all normal events, if the door sensor detects that the door is opened, and this alarm event will be triggered.

Door-open timeout: This alarm event is triggered when the opened door is not locked at closing door time.

Tamper-Resistant Alarm: This alarm event will be triggered when AIO device is tampered.

Server Connection Failed: This alarm event will be triggered when the device is disconnected from the server.

11.3 Elevator Event Type

- Normal Events

Normal Punch Open: This normal event is triggered if the verification mode is associated with cards, and a user with the floor opening right punches his/her card and passed the verification.

Punch during passage mode time zone: This normal event is triggered if a valid card is punched after a user with the floor opening right sets the Normally Open periods for a specific floor, or sets the floor to the Normally Open state through the remote opening floor operation.

Open during passage mode time zone: This normal event is triggered if a fingerprint is pressed after a user with the floor opening right sets the Normally Open periods for a specific floor, or sets the floor to the Normally Open state through the remote opening floor operation.

Remote release: This normal event is triggered if a user remotely releases a button successfully.

Remote locking: This normal event is triggered if a user remotely locks a button successfully.

Disable intraday passage mode time zone: This normal event is triggered if a user performs this operation on the Remotely Release Button page when a floor is in Normally Open state.

Enable intraday passage mode time zone: This normal event is triggered if the user performs this operation on the Remotely Lock Button page when the Normally Open periods of the floor are prohibited on the day.

Normal fingerprint open: This normal event is triggered if a user with the button releasing right presses his/her fingerprint in the "Card or fingerprint" verification mode and the verification is passed.

Press fingerprint during passage mode time zone: This normal event is triggered if a fingerprint is pressed after a user with the floor opening right sets the Normally Open periods for a specific door, or sets the door to the Normally Open state through the remote opening door operation.

Passage mode time zone over: When the preset Normally Open period arrives, the button is automatically locked.

Remote normal opening: This normal event is triggered if a user selects the continuously releasing button to set the button in continuously released state on the page for remotely opening the floor.

Device started: This normal event is trigger upon startup of the device. (This event will not appear in the real-time monitoring, and can only be viewed through the event records in the report.)

Password open: This normal event is triggered if a user with the button releasing right presses the password in the "Password only" or "Card or fingerprint" verification mode and the verification is passed.

Superuser open buttons: This normal event is triggered if the super user remotely releases a button successfully.

Start the fire floor: Release all buttons in the case of emergency so that users can select floors.

Superuser close buttons: This normal event is triggered if the super user remotely closes floors (locks the buttons) successfully.

Enable elevator control button: Restart the elevator control function.

Disable elevator control button: Temporarily disable the elevator control function.

Auxiliary input disconnected: This normal event is triggered if the auxiliary input point is disconnected.

Auxiliary input shorted: This normal event is triggered if the auxiliary input point is short circuited.

- Abnormal Events

Operate interval too short: This abnormal event is triggered if the actual interval between two times of card punching is smaller than the interval that is set for this floor.

Press fingerprint interval too short: This abnormal event is triggered if the actual interval between two times of fingerprint pressing is smaller than the interval that is set for this floor.

Button inactive time zone (punch card): This abnormal event is triggered if the verification mode is associated with cards, and a user with the floor opening right punches his/her card beyond the effective periods.

Illegal time zone: This abnormal event is triggered if a user with the floor opening right punches his/her card beyond the effective periods.

Access denied: This abnormal event is triggered if a registered card is punched before the elevator control right of the current floor is set for this card.

Disabled card: This event is triggered if the current card number is not registered in the system yet.

Card expired: This event is triggered if a person, for whom the elevator control effective time is set, punches his/her card beyond the elevator control effective periods and verification fails.

Fingerprint expired: This event is triggered if a person, for whom the elevator control effective time is set, presses his/her fingerprint beyond the elevator control effective periods and verification fails.

Password error: This event is triggered if the verification mode is associated with the password and the password verification fails.

Disabled fingerprint: This event is triggered if the current fingerprint is not registered in the system or has been registered but not synchronized to the device.

Button inactive time zone (press fingerprint): This abnormal event is triggered if a user with the floor opening right presses his/her fingerprint beyond the effective periods of the floor.

Failed to close during passage mode time zone: This abnormal event is triggered if the current floor is in Normally Open state and the button cannot be locked by performing the Remotely locking Button operation.

Wiegand format error: This abnormal event is triggered if a card is punched and the Wiegand format of this card is incorrectly set.

Note: User can self-define the level of each event (normal, abnormal or alarm).

11.4 FAQs

Q: How to use a card issuer?

A: Connect the card issuer to PC through USB port, and then select individual personnel card issue or batch card issue. Move the cursor to the card number input box, and punch the card on the card issuer, then the card number will be automatically shown in the input box.

Q: What is the use of role setting?

A: Role setting has the following uses: 1. To set unified level for the same type of users newly added, just directly select this role when adding users; 2. When setting system reminder, and determine which roles can be viewed.

Q: How to operate if I want to set accounts for all personnel of the Company's Financial Department?

A: First, create a new role in system setting and configure the functions to be used for this role. Then add a user, set user information, and select the user's role, thus adding a new account. For other accounts, do the same.

Q: In Windows Server 2003, why the IE browser displayed error when access the system, how to solve it?

A: This problem occurs because that Server 2003 has [Security Configuration Option] settings. If you want to access the system, please configure it as follows: click Start – Control Panel – Add or Remove Program, select [Add and

remove Windows components] in the interface and click [Internet Explorer Enhanced Security Configuration] option, cancel the tick before it. Then click [Next] to remove it from the system. Open the system again the browser will access the system properly.

Q: If backing up or restoring the database fails, the possible reason?

A:

Backup fails: Please check the system environment variables, please go to Properties > Advanced to set the environment variables as "C:\Program Files\ZKBioSecurity3.0\MainResource\postgresql\bin:". "C:\Program Files" is the system installation path, you can modify by your actual situation.

Restore fails: There are several reasons: The system version is too high or too low, or the database has been damaged, you need to follow the prompts to change the system version or repair the system, re-install the database.

11.5 END-USER LICENSE AGREEMENT

Important - read carefully:

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the mentioned author of this Software for the software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This EULA grants you the following rights: Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Limitations on Reverse Engineering, Recompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Separation of Components.

The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on

more than one computer.

Software Transfer.

You may permanently transfer all of your rights under this EULA, provided the recipient agrees to the terms of this EULA.

Termination.

Without prejudice to any other rights, the Author of this Software may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.
Distribution.

The SOFTWARE PRODUCT may not be sold or be included in a product or package which intends to receive benefits through the inclusion of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT may be included in any free or non-profit packages or products.

3. COPYRIGHT.

All title and copyrights in and to the SOFTWARE PRODUCT(including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by the Author of this Software. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes.

LIMITED WARRANTY

NO WARRANTIES.

The Author of this Software expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or no infringement. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

NO LIABILITY FOR DAMAGES.

In no event shall the author of this Software be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if the Author of this Software has been advised of the possibility of such damages.

Acknowledgment of Agreement.

I have carefully read and understand this Agreement, ZKTeco, Inc.'s Privacy Policy Statement.

If YOU ACCEPT the terms of this Agreement:

I acknowledge and understand that by ACCEPTING the terms of this Agreement.

IF YOU DO NOT ACCEPT the terms of this Agreement.

I acknowledge and understand that by refusing to accept these terms, I have rejected this license agreement and therefore have no legal right to install, use, or copy this Product or the Licensed Software that it incorporates.

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com

© Copyright 2014. ZKTeco CO., LTD. ZKTeco Logo is a registered trademark of ZKTeco or a related company. All other product and company names mentioned are used for.