User Manual

ZKBioSecurity 3.0

Version: 1.0

Date: April 2015

Software Version: ZKBioSecurity 3.0 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

1. System Instruction 1

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

2. System Operations 3

2.1 Log into the System 3
2.2 Personal Self-Login 3
2.3 System Panel 3
2.3 Activate the System 4
2.4 Modify Password 4
2.5 Customer Service 5
2.6 Exit the system 5

3. Personnel System 6

3.1 Personnel 6
3.1.1 Department Management 6
3.1.2 Personnel 7
3.1.3 Custom Attributes 12
3.1.4 Parameters 14
3.2 Card Manage 14
3.2.1 Card 14
3.2.2 Wiegand Format 15
3.2.3 Issue Card Record 16

4. Access 17

4.1 Device 17
4.1.1 Device 17
4.1.2 Device Operation 20
4.1.3 Doors 26
4.1.4 Reader 28
4.1.5 Auxiliary Input 29
4.1.6 Auxiliary Output 30
4.1.7 Event Type 31
4.1.8 Daylight Saving Time 32
4.1.9 Device Monitoring 34
4.1.10 Real-Time Monitoring 34
4.1.11 Alarm Monitoring 37
4.1.12 Map 38
4.2 Access Control Management 39

4.2.1 Access Control Time Zones....39
4.2.2 Access Control Holidays....40
4.2.3 Access Levels....41
4.3 Access Rule....42
4.3.1 Interlock Settings....42
4.3.2 Linkage Setting....43
4.3.3 Anti-Passback Settings....47
4.3.4 First-Person Normally Open....48
4.3.5 Multi-Person Personnel Group....48
4.3.6 Multi-Person Opening Door....49
4.3.7 Parameters....50
4.4 Advanced Functions....50
4.4.1 Zone....50
4.4.2 Reader Define....51
4.4.3 Global Anti-passback....52
4.4.4 Who is Inside....53
4.4.5 Global Linkage....53
4.5 Access Reports....55
4.5.1 All Transactions....55
4.5.2 Events from Today....55
4.5.3 Last Known Position....56
4.5.4 All Exception Events....56
5. Elevator....59
5.1 Elevator Device....59
5.1.1 Add an Elevator Device....59
5.1.2 Reader....61
5.1.3 Floor....62
5.1.4 Auxiliary Input....63
5.1.5 Event Type....64
5.1.6 Device Monitoring....64
5.1.7 Real-Time Monitoring....65
5.3 Elevator Rules....69
5.3.1 Elevator Control Time Zones....69
5.3.2 Elevator Control Holidays....71
5.3.3 Elevator Levels....71
5.3.4 Global Linkage....73
5.3.5 Parameters....74
5.4 Elevator Reports....75
5.4.1 All Transactions....75
5.4.2 All Exception Events....75
6. Visitor System....77
6.1 Registration....77
6.1.1 Entry Registration....77

6.1.2 Visitor Information 80
6.2 Reservation 81
6.3 Basic Management 81
6.3.1 Parameters 81
6.3.2 Visitor Levels 83
6.3.3 Entry Place 84
6.3.4 Visit Reason 85
6.4 Visitor Reports 85
6.4.1 Last Visited Location 85
6.4.2 Visitor History Record 85
7. Video 86
7.1 Video Device 86
7.2 Video Channel 87
7.3 Video Preview 88
7.4 Video Event Record 89
7.5 Parameters 90
7.6 Solutions of Exceptions 90
8. System Management 92
8.1 Basic Management 92
8.1.1 Operation Logs 92
8.1.2 Database Management 92
8.1.3 Area 93
8.1.4 System Parameters 94
8.1.5 E-mail Management 94
8.1.6 Data Cleaning 95
8.1.7 Audio File 96
8.2 Authority Management 96
8.2.1 User 96
8.2.2 Role 97
8.2.3 Role Group 98
8.3 Communication 99
9. Appendices 100
Appendix 1 Common Operations 100
Appendix 2 Access Event Type 104
Appendix 3 Elevator Event Type 108
Appendix 4 FAQs 110
Appendix 5 END-USER LICENSE AGREEMENT 111

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 six modules, namely: Personnel, Access, Elevator, Visitor 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: Binuclear or above.
  - Memory: 4G or above.
  - Hardware: Available space of 10G 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 Server 2008(32/64).
  - Supported Databases: PostgreSQL
  - 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 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.

1.5 Brief introduction of Visitor

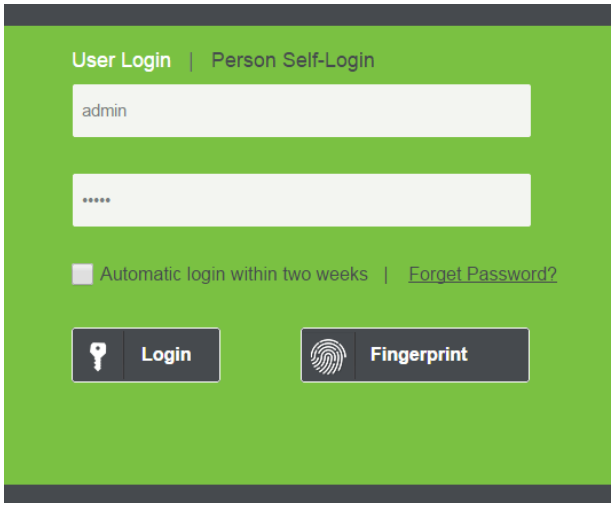
Visitor is a web-based management system that implements entry registration, exit registration, snapshot capturing, visitor quantity statistics, and reservation management, as well as shares information among registration sites. It is highly integrated with the access control system and elevator control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

1.6 Brief Introduction of 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.

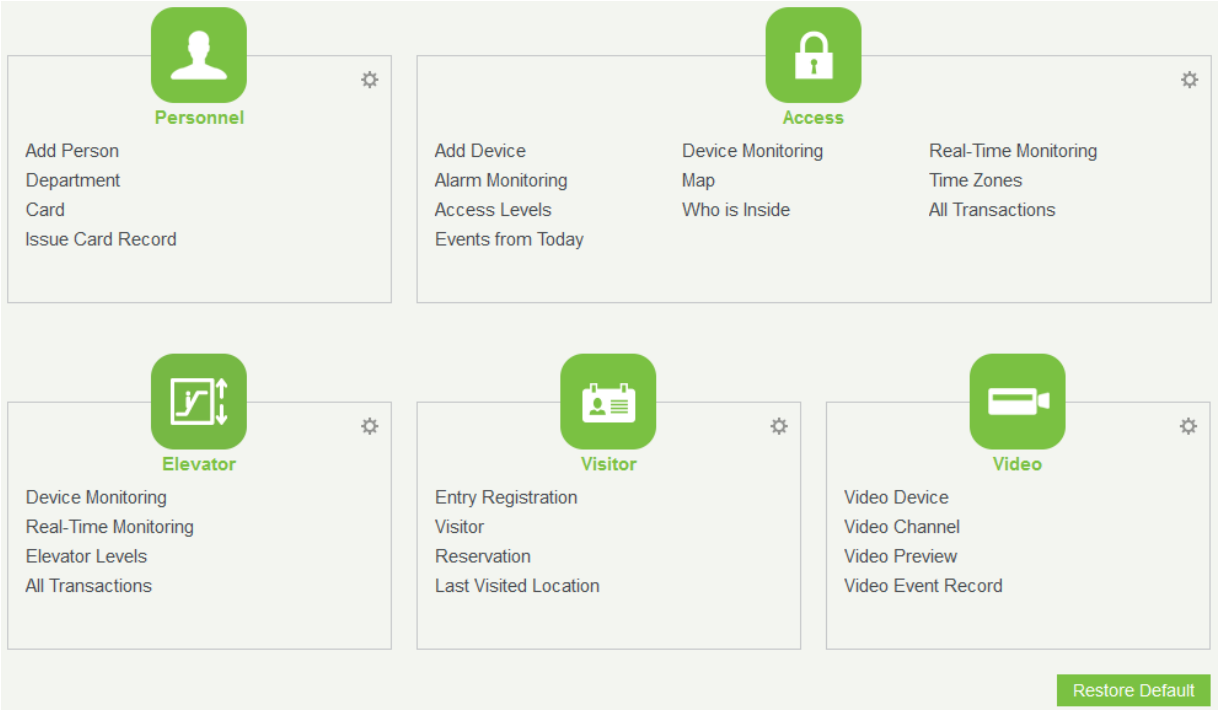
✍Note: The user name of the super user is [admin], and the password is [admin]. After the first login to the system, please reset the password in [Personnel Information].

2.2 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 6.2 Reservation.

2.3 System Panel

After logging in, the main page is displayed as follows:



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

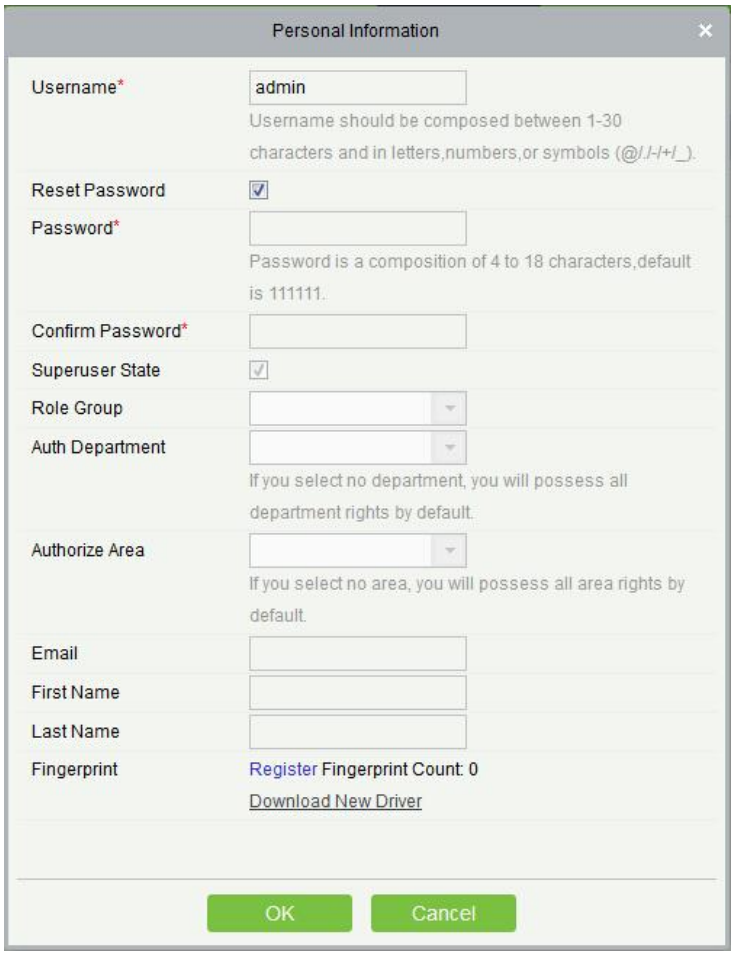
Click ⚙ to edit the function lists in the top right corner of every module.

2.3 Activate the System

Please refer to the corresponding license document.

2.4 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.

2.5 Customer Service

Click the [Customer Service] button on the top right corner of the interface to enter **http://support.zkteco.com/** to obtain help.

✍Note:

1) After you activate the software, you will get an account of After-sales service center automatically.

2) The default user name is the email which you were used to active the software, you can click [about] > [Online Activation] to check.

3. The default password is 123456.

2.6 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.

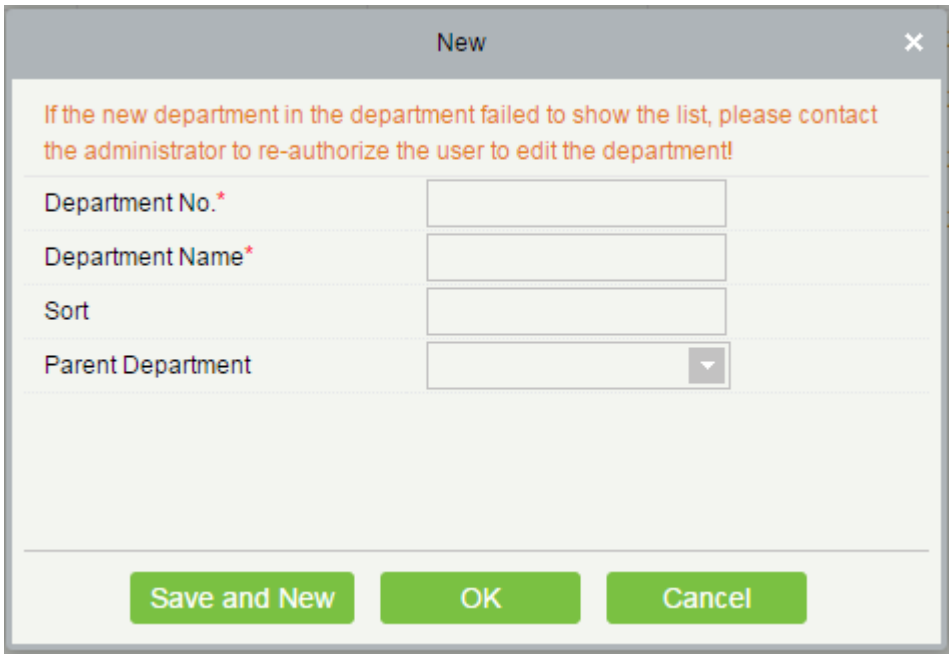
3.1.1 Department Management

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 30 characters.

Sort: Only supports numbers, the valid range is1-999999999. 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.

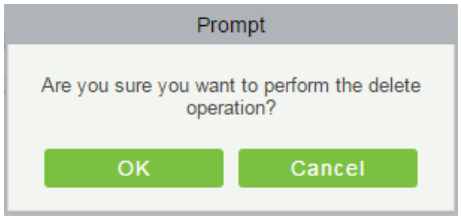
To add a department, you may also use [Import] to import department information from other software or other document into this system. For details, see Appendix 1 Common Operation.

- Edit a Department

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

- Delete a Department

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



2. Click [OK] to delete.

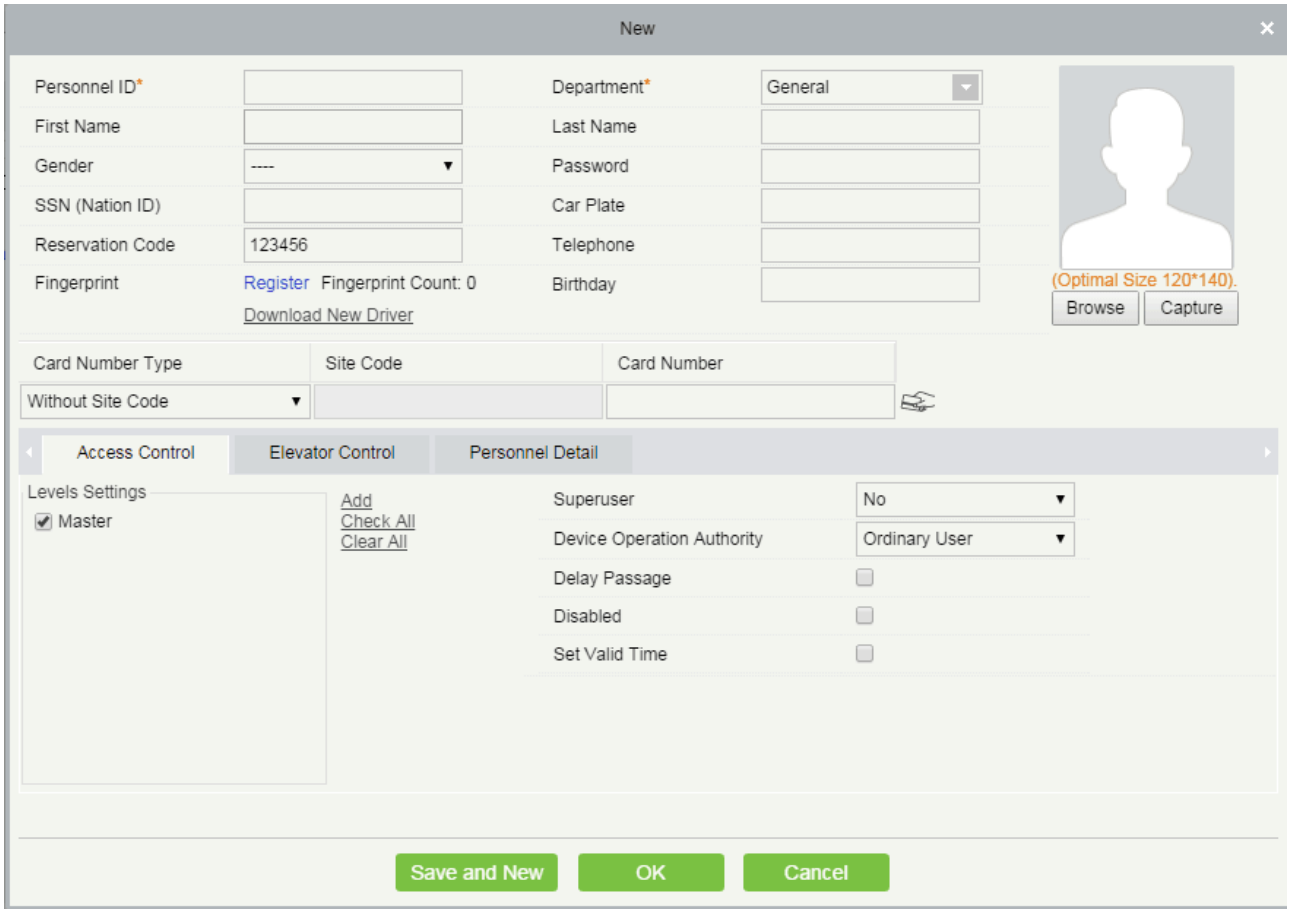
3.1.2 Personnel

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 Appendix 1 Common Operation.

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.

Name/Last Name: The max length is 9.

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.

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

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

Password: Set personnel password. Only supports 6-digit passwords. If password exceeds the specified length, the system will truncate it automatically.

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.

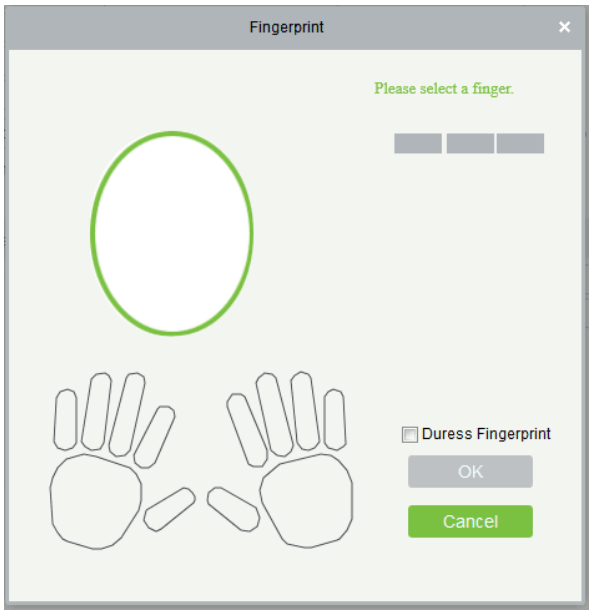
Register Fingerprint: Enroll the Personnel Fingerprint or Duress Fingerprint. To trigger the alarm and send the signal to the system, press the Duress Fingerprint,

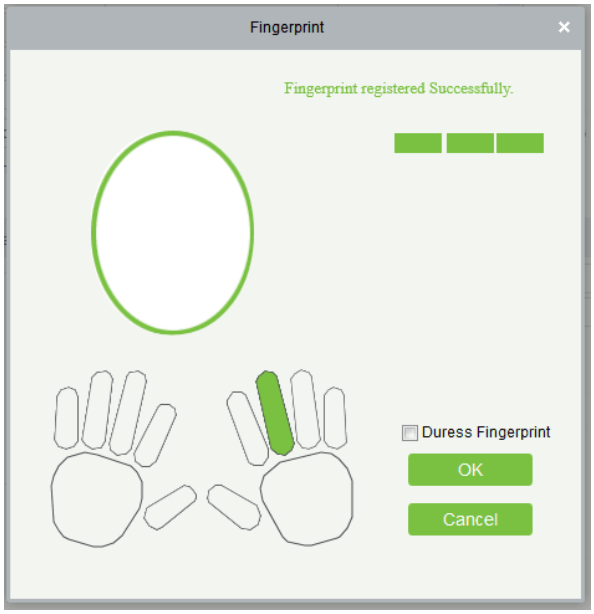
How to register fingerprint:

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.

✍Note:

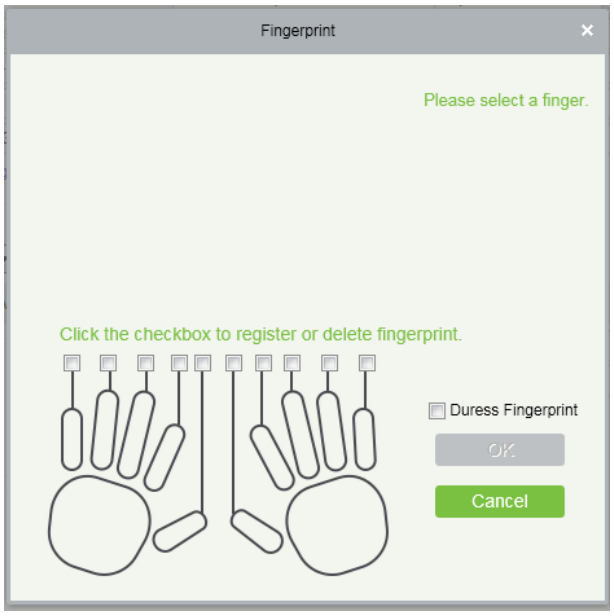
- If fingerprints are duplicated, "Don't repeat the fingerprint entry" will be prompted.
- If the fingerprint sensor driver is not installed, click "Install drive" and the system will prompt to download and install driver.
- After the fingerprint sensor driver is installed, if fingerprint register button 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:

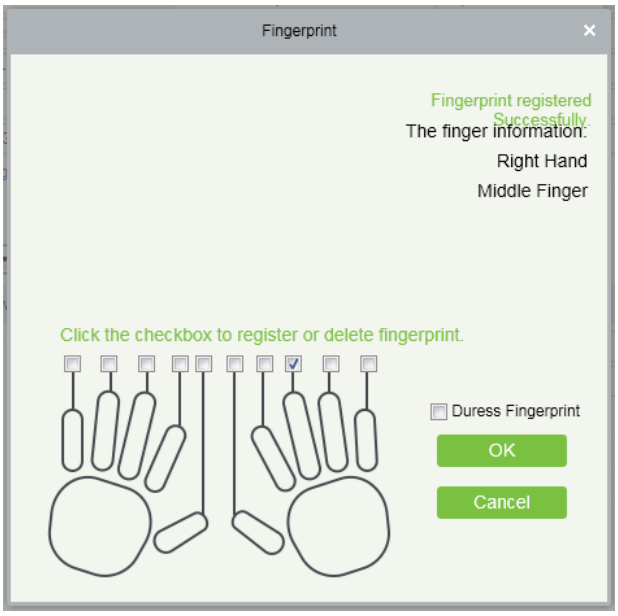
  1) In IE browser, click [Tools] → [Internet Options] →[Security] →[Credible Sites], add http://localhost to the credible sites, then restart the IE browser.

  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).

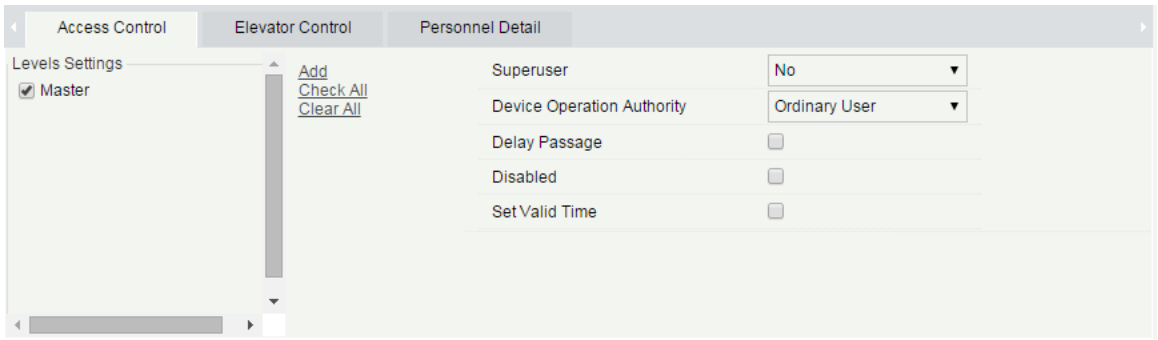
3) If above settings are all invalid, please execute following operations (take IE11 browser as an example): click [Tools] → [Internet Options] →[Advanced] →[Security], check the option of [Allow software to run or install even if the signature is ...], and remove the tick before [Check for server certificate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

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





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



Fields are as follows:

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.

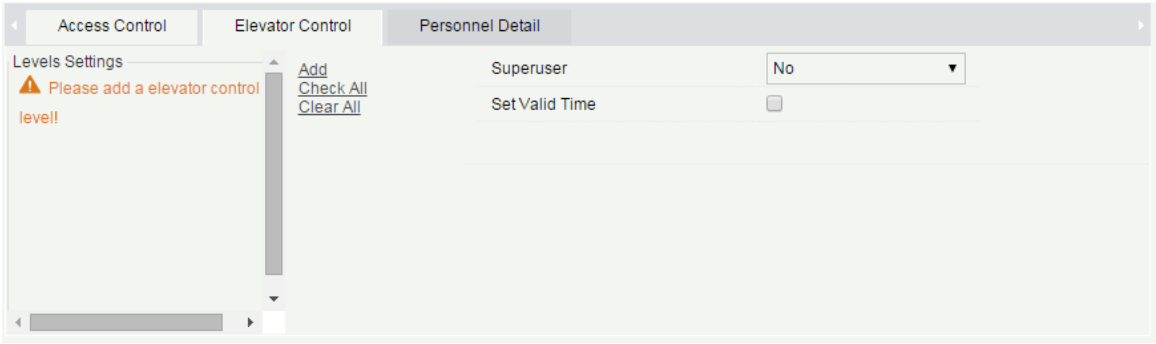
The Personnel Information List, by default, is displayed as a table. If Graphic Display is selected, photos and numbers will be shown. Put the cursor on a photo, details about the personnel will be shown.

✍Note：

(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]:



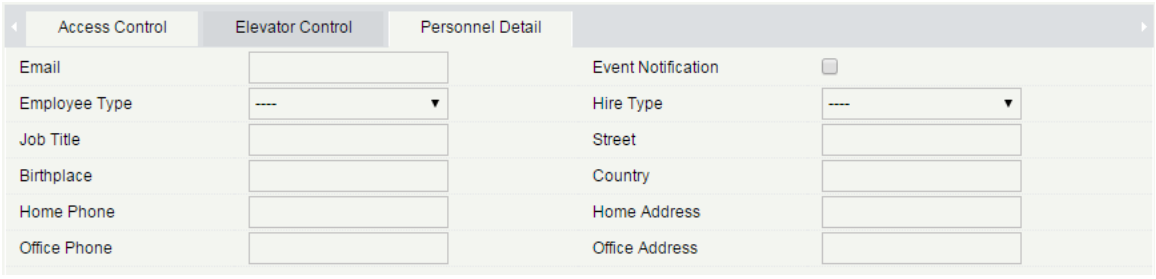
Fields are as follows:

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 8.1.5 Email Manangement 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.

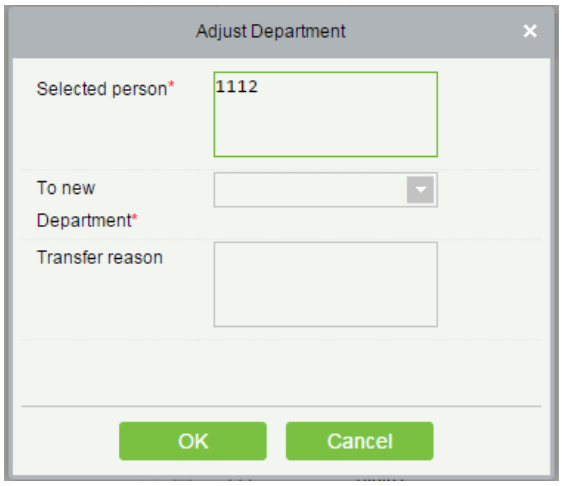
- Delete Personnel

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" .

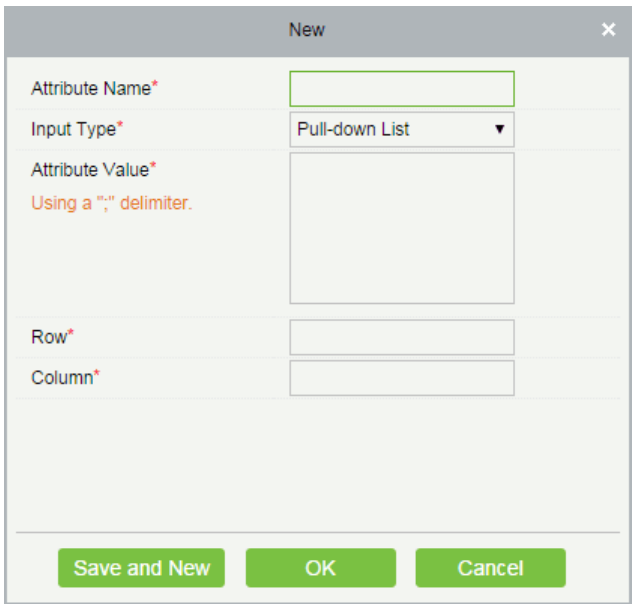
3) Click "OK" to save and exit.

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.



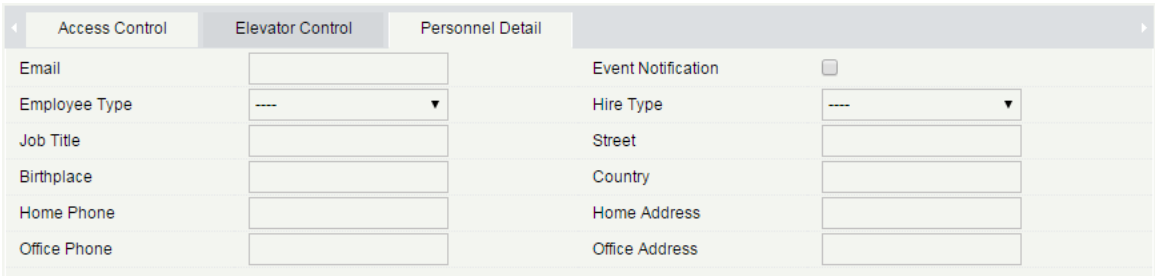
Fields are as follows:

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.

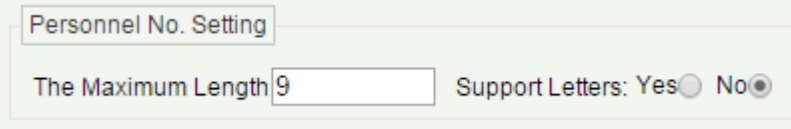
- Delete a Custom Attribute

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

Click [Personnel] > [Personnel] > [Parameters]:



Set the maximum length of pesonnel number and whether it supports letters.

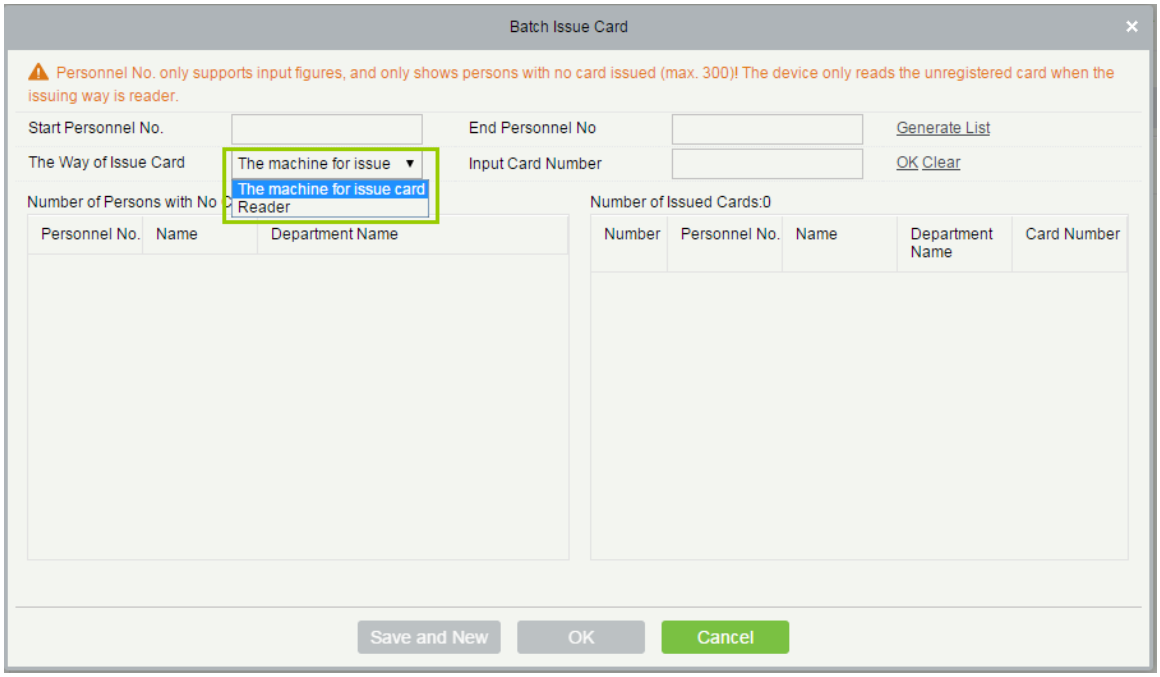
3.2 Card Manage

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 the way of Issuing card: Issue machine or Reader.

For the use of the Issue machine, 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 Read, 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].

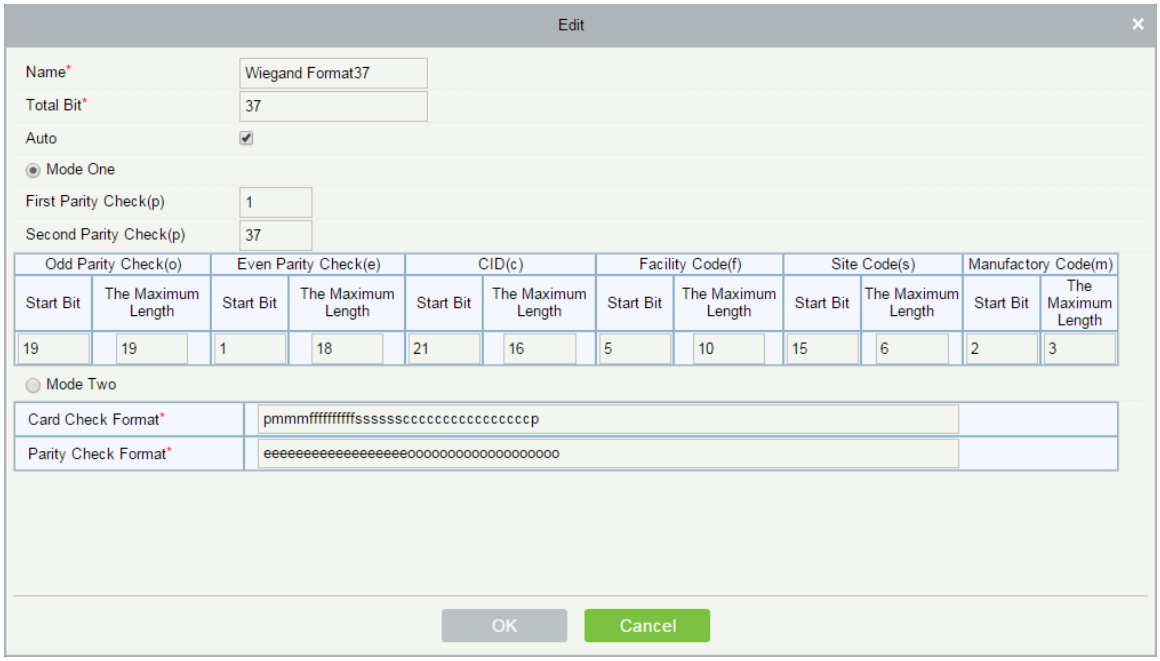
✍Note: During Batch Issue Card, System will check whether the card number issues card or not, if card has been issued before, the system will prompt "The Card Number has already been issued".

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.

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:



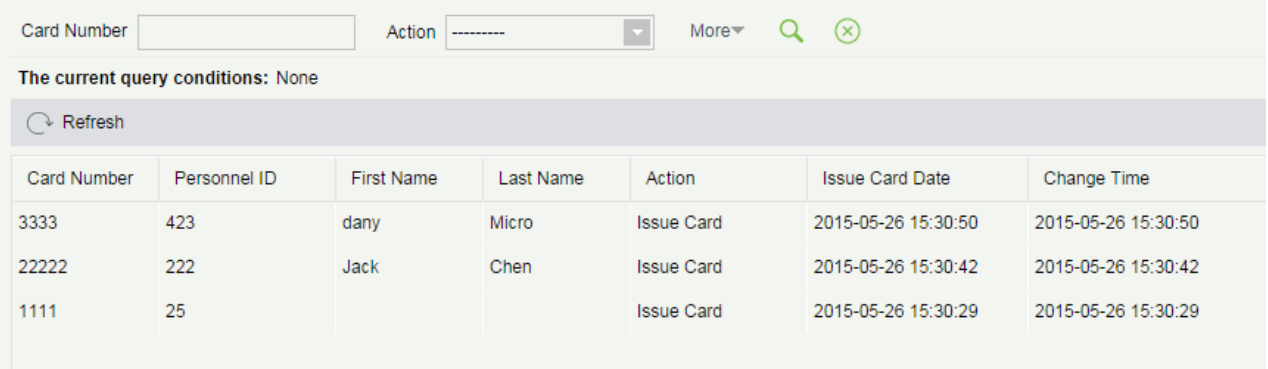
Format Specifying:

p indicates Parity Position, s indicates Site Code, c indicates Cardholder ID, f indicates Facility Code, 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 "eeeeeeeeeeeeeeeee", the second parity bits check "ooooooooooooooooo". Card Check Format only can be set " p, x, m, f, c, s", Parity Check Format only can be set " x, b, o, e".

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.

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

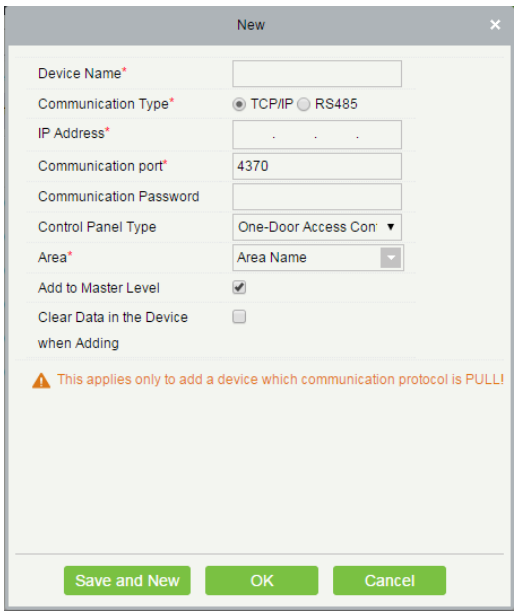
- Add Device

There are three ways to add Access Devices.

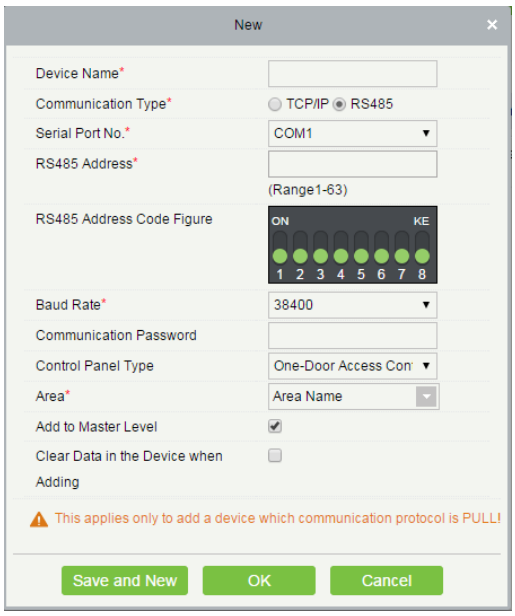
1. Add Device by manually

(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.

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

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.

Add to Master Level: The system have a default access level which named as "Master level". If ticked that option, will add this new device to the system master level by default. The new added personnel will be allocated to the system master level by default too, and there is no need to set a new level.

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.

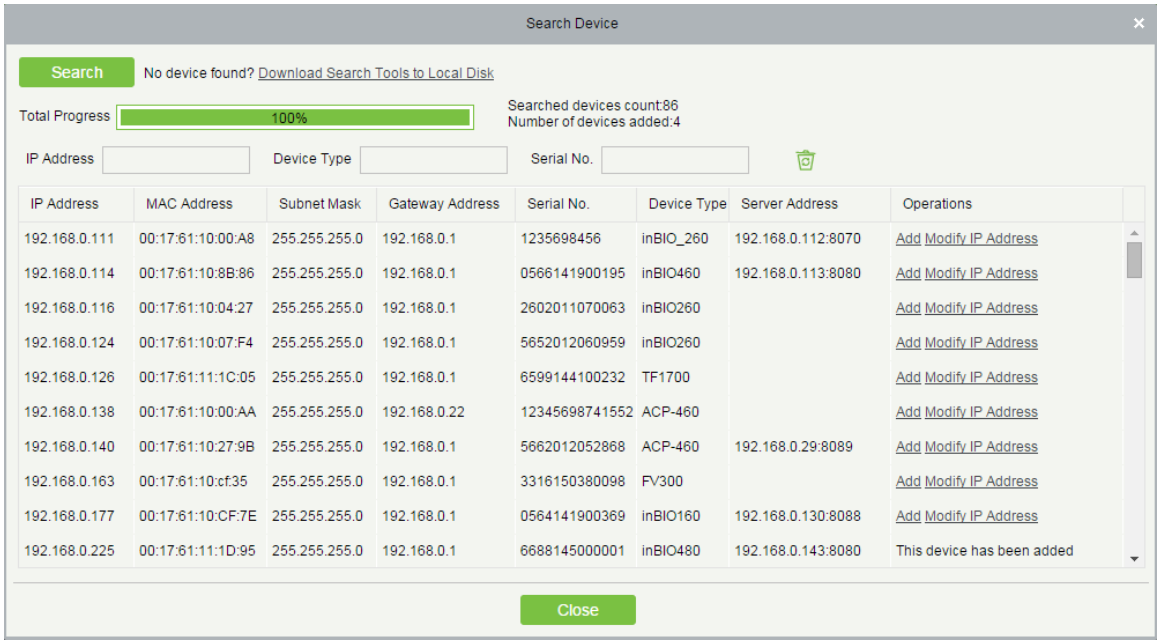
2. Add Device by Searching Access Controllers

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……].

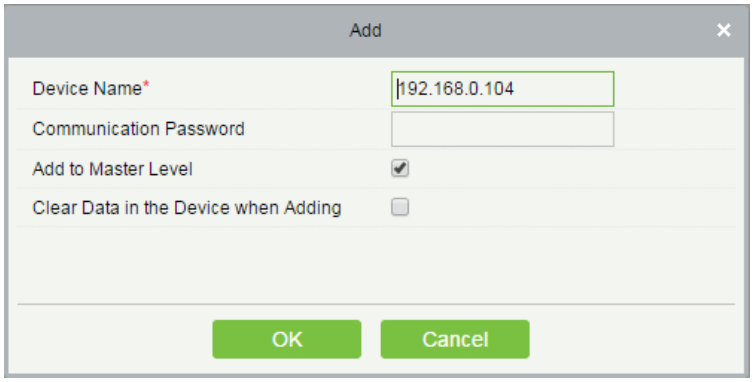
(3) After searching, the list and total number of access controllers will be displayed.



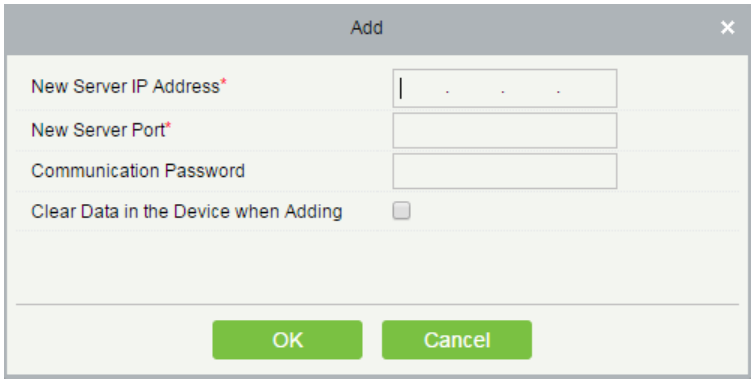
✍Note: UDP broadcast mode will be used to search access device, this mode cannot perform cross-Router function. IP address can provide cross-net segment, but must be in the same subnet, and needs to be configured the gateway and IP address in the same net segment.

(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.



If the device is with a push firmware, the following windows will pop-up after clicking [Add]. After configure IP Address and port number of the server, device will be added to the software automatically.



New Server IP Address: Set a new IP address of current system.

New Server Port: Set the access point of system.

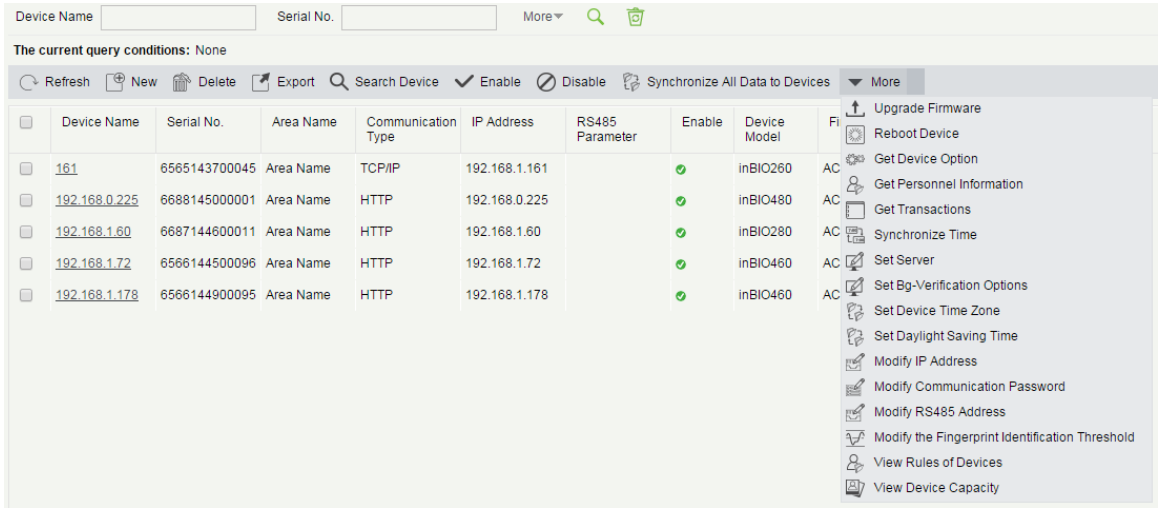
Clear Data in the Device: Check this option, after adding device, the system will clear all data in the device (except the event logs). If you add the device just for demonstration or testing, there is no need to tick it.

(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: 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], or these original data may conflict with normal usage.

4.1.2 Device Operation

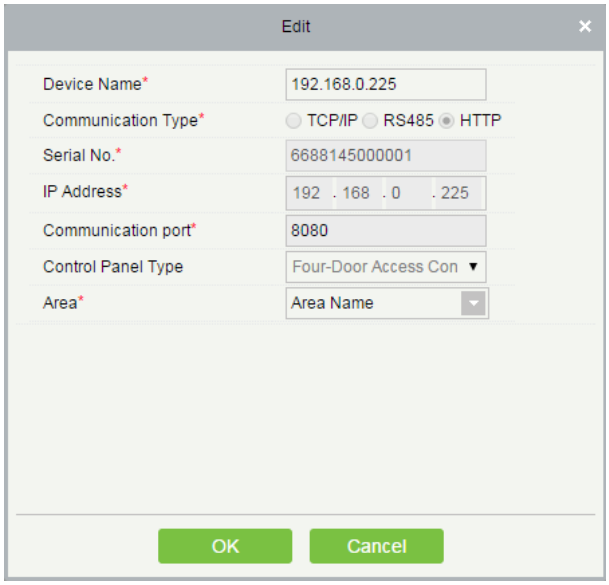
For communication between the system and device, data uploading, configuration downloading, device and system parameters shall be set. User can edit access controller within its levels in the current system, and only can add or delete devices in Device Management if needed.



- 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.

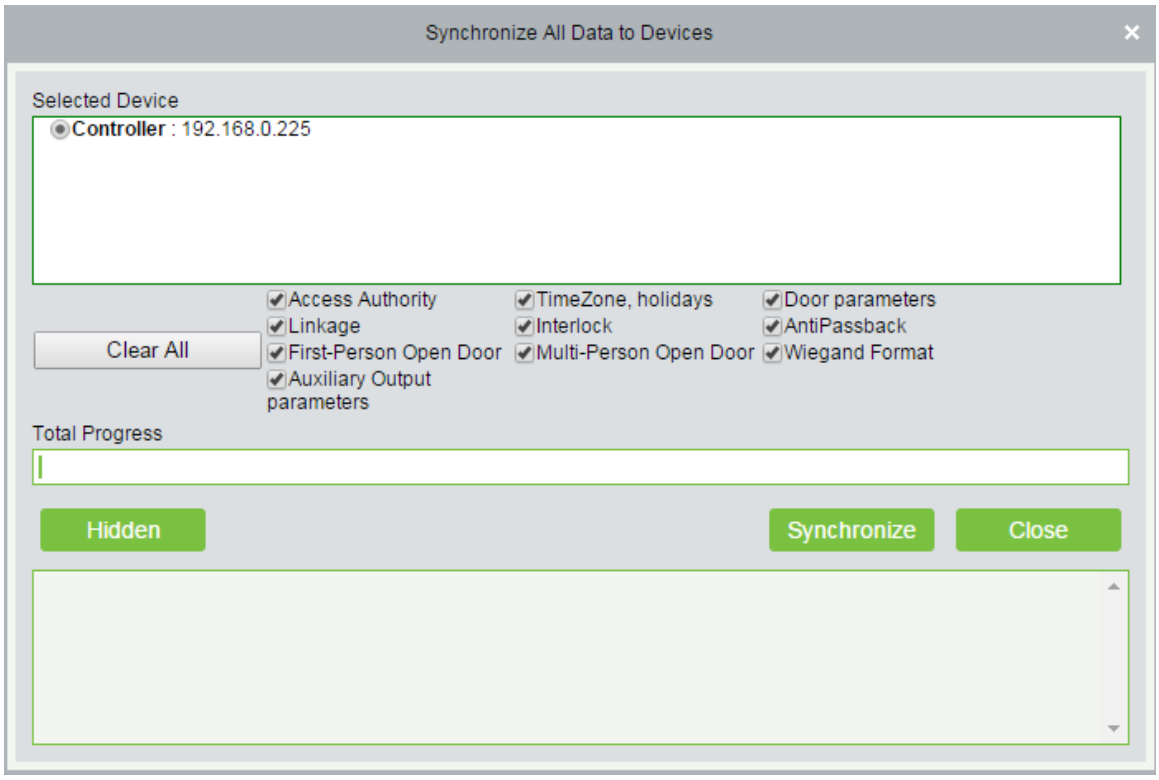
Access Control Panel Type cannot be modified, if the type is wrong, user need to manually delete the device and add it again.

- 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

To reboot the selected device.

- Get Device Option

To 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 and fingerprints 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

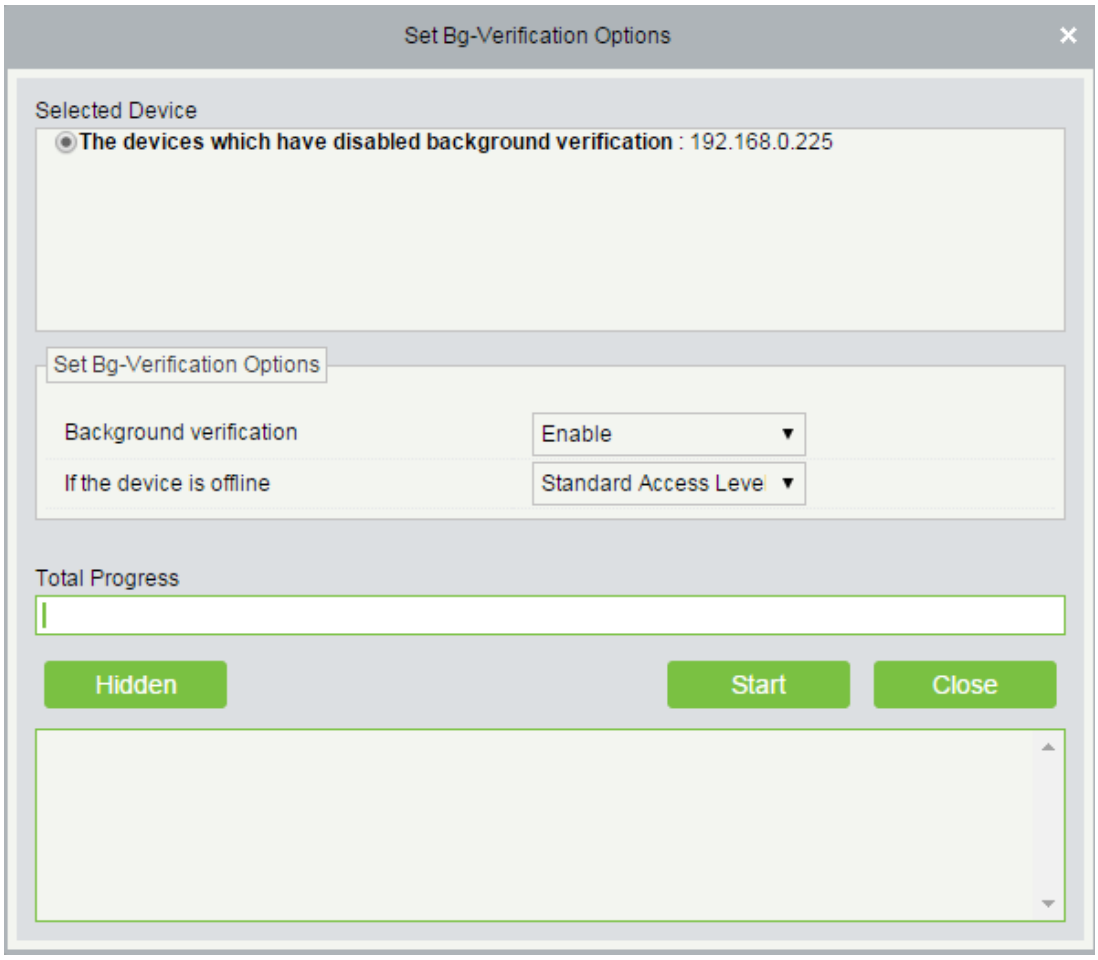
Synchronize device time with current server time.

- 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 4.1.1 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

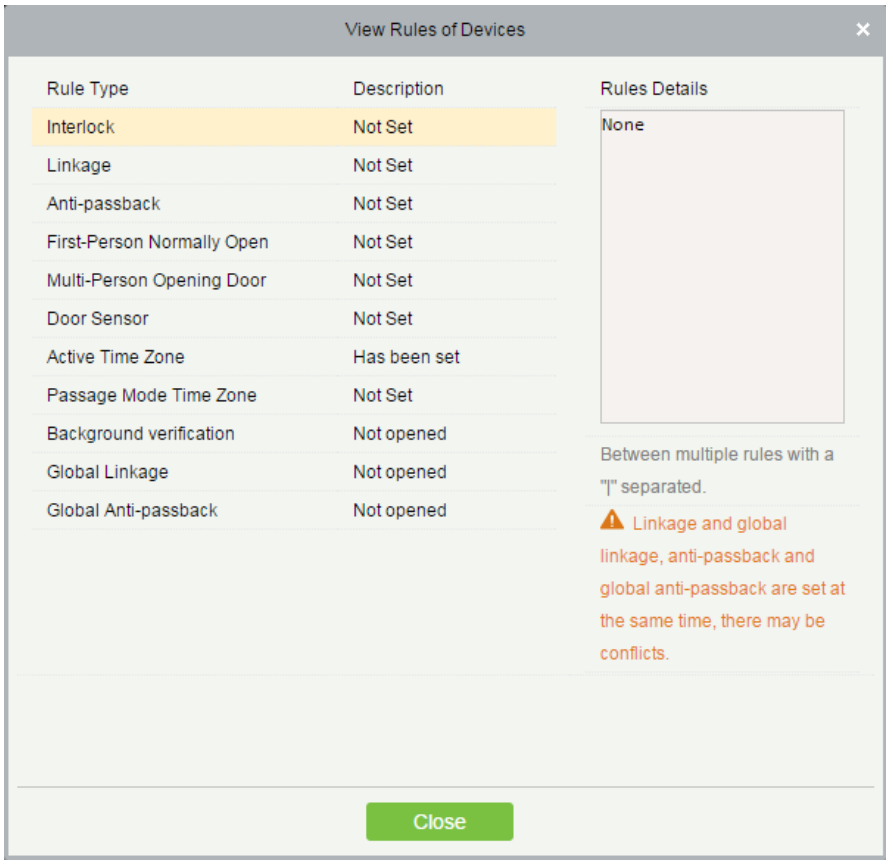
Only the devices that use RS485 communication and with no DIP Switch can modify RS485 address.

- 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.

- View Rules of Devices

View the Access rules in the device.

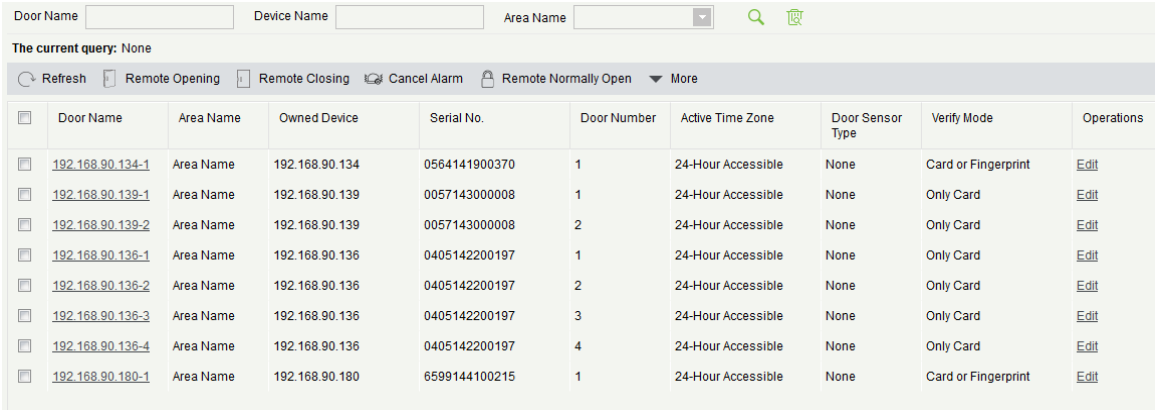


- View Device Capacity

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

4.1.3 Doors

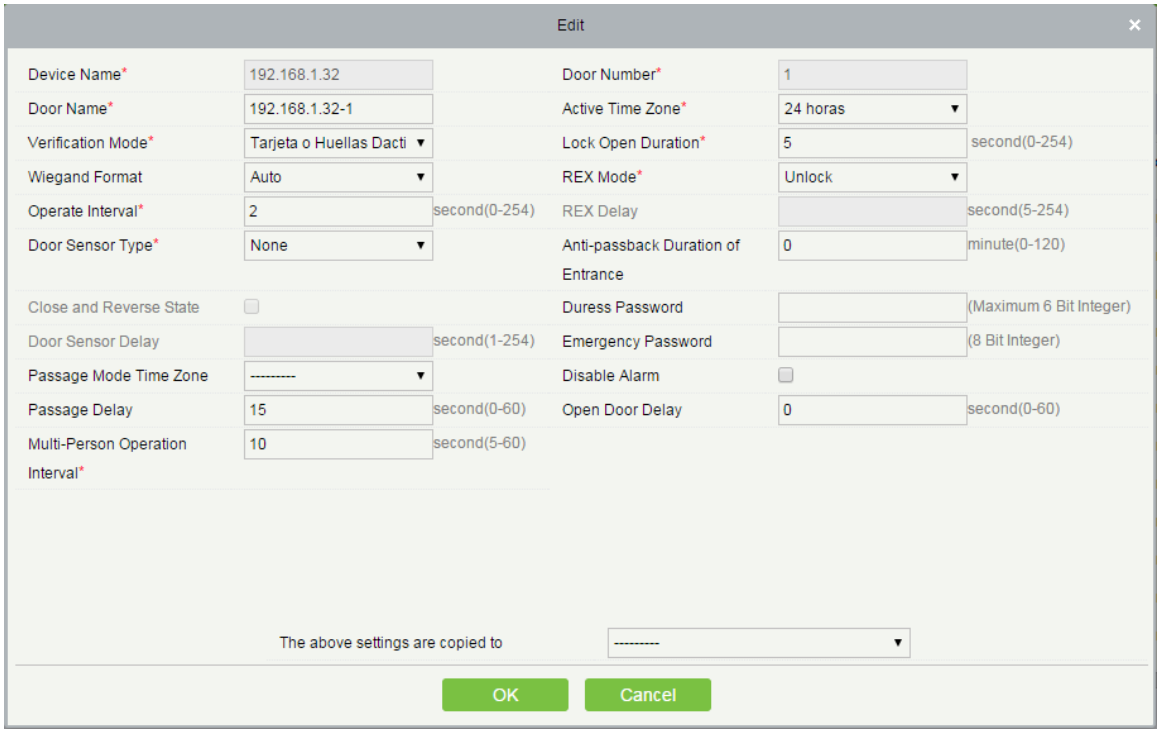
1. Click [Access Device] > [Device] > [Door] to enter Door Management interface (click "Area Name" in the left, system will automatically filter and display all access devices in this area).



Door Name	Area Name	Owned Device	Serial No.	Door Number	Active Time Zone	Door Sensor Type	Verify Mode	Operations
192.168.90.134-1	Area Name	192.168.90.134	0564141900370	1	24-Hour Accessible	None	Card or Fingerprint	Edit
192.168.90.139-1	Area Name	192.168.90.139	0057143000008	1	24-Hour Accessible	None	Only Card	Edit
192.168.90.139-2	Area Name	192.168.90.139	0057143000008	2	24-Hour Accessible	None	Only Card	Edit
192.168.90.136-1	Area Name	192.168.90.136	0405142200197	1	24-Hour Accessible	None	Only Card	Edit
192.168.90.136-2	Area Name	192.168.90.136	0405142200197	2	24-Hour Accessible	None	Only Card	Edit
192.168.90.136-3	Area Name	192.168.90.136	0405142200197	3	24-Hour Accessible	None	Only Card	Edit
192.168.90.136-4	Area Name	192.168.90.136	0405142200197	4	24-Hour Accessible	None	Only Card	Edit
192.168.90.180-1	Area Name	192.168.90.180	6599144100215	1	24-Hour Accessible	None	Card or Fingerprint	Edit

- **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, Passage Mode 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.

Punch 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.

Verify 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.

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).

Delay time interval of passage: 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.

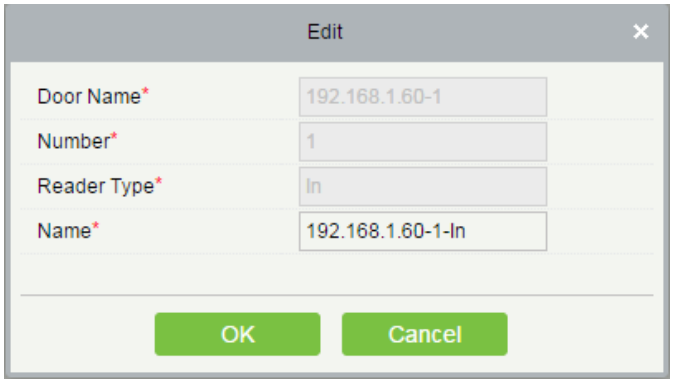
The above Settings are Copied to: Including below two options.

- 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]:

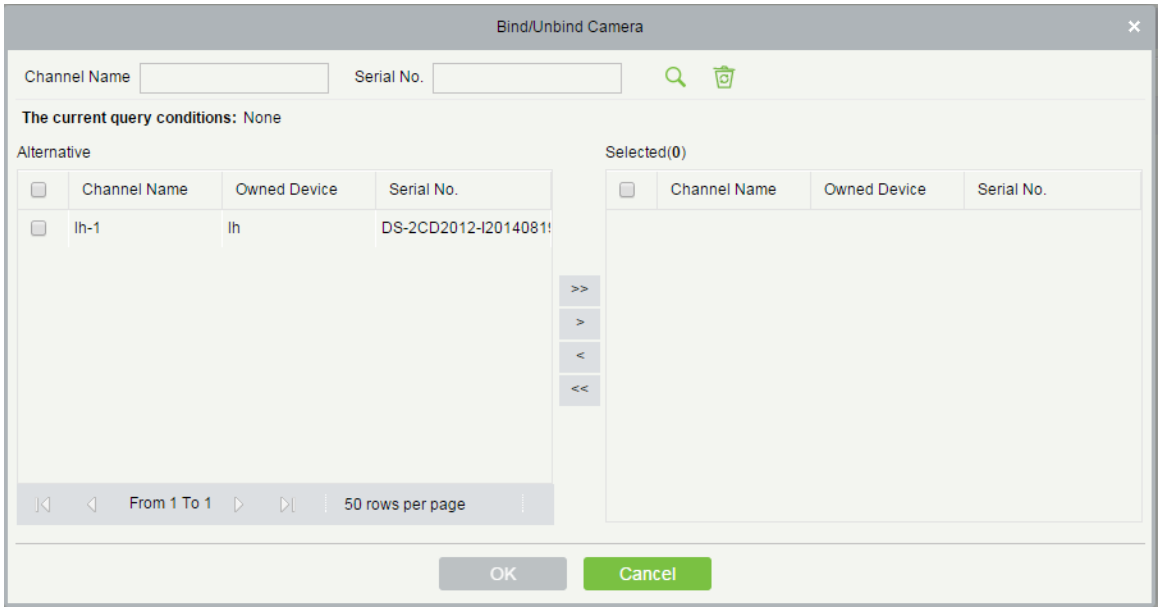


✍Note: Only the name of the reader can be modified.

- 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:



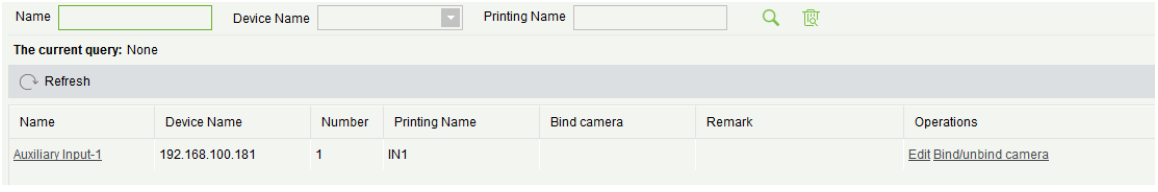
Click [OK] to finish.

✍Note: A reader can bind more than one channel.

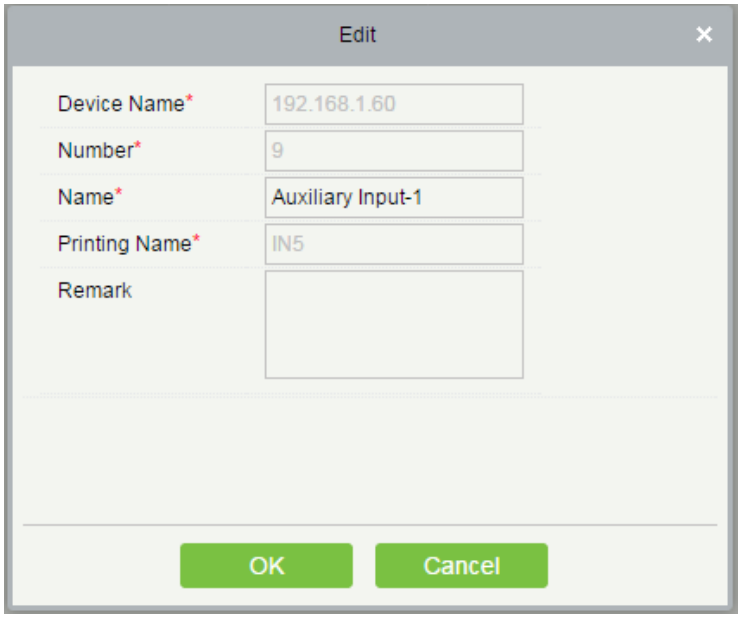
4.1.5 Auxiliary Input

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.

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

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

- Bind/Unbind Camera

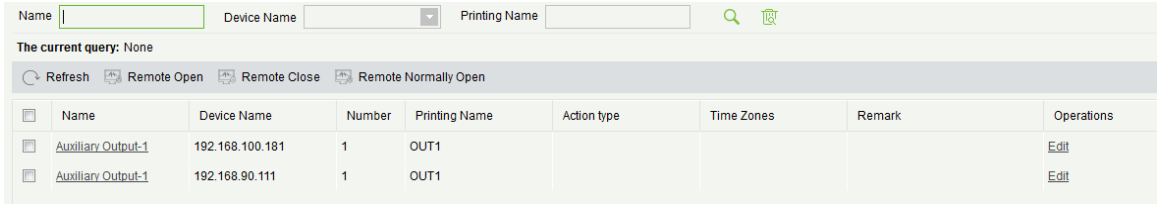
Bind camera, if carried out the interaction setting in Linkage or in Global Linkage, it will make a video linkage (pops up video, video or capture) once a corresponding event occurs. For more steps, please refer to 4.1.4 Reader: Bind/Unbind Camera.

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

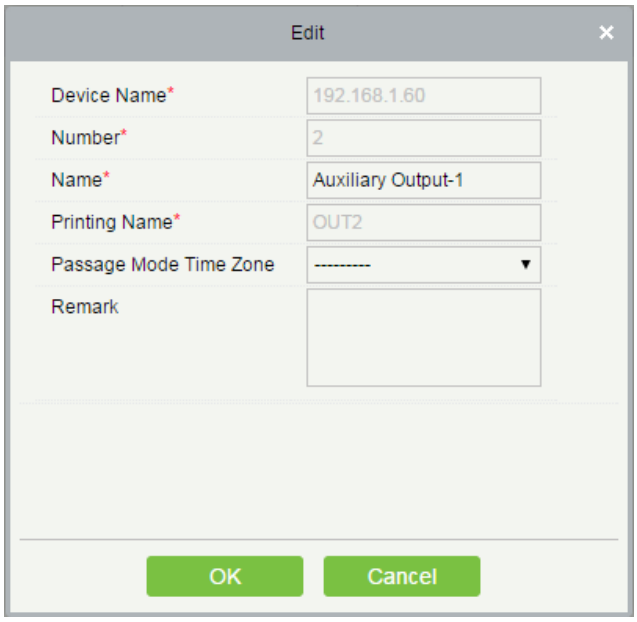
4.1.6 Auxiliary Output

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.

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

Action Type: None by default, you can set it as normal open or normal close.

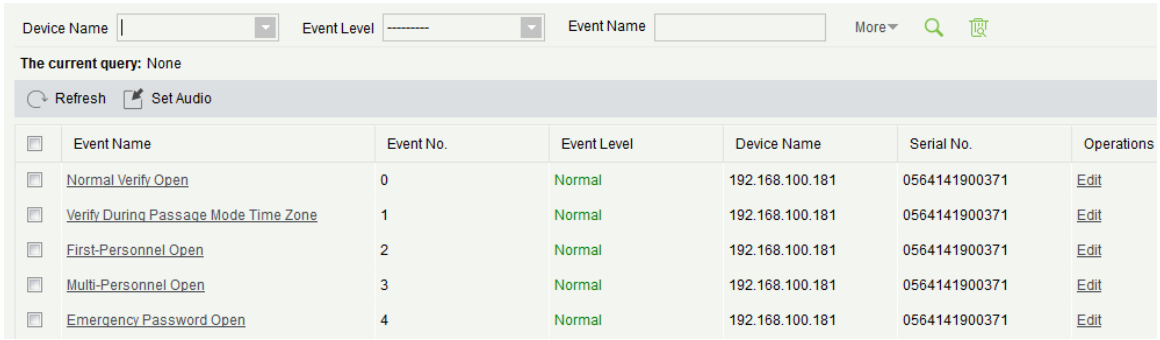
Time Zone: The auxiliary output is in normal open or normal close in this time zone.

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

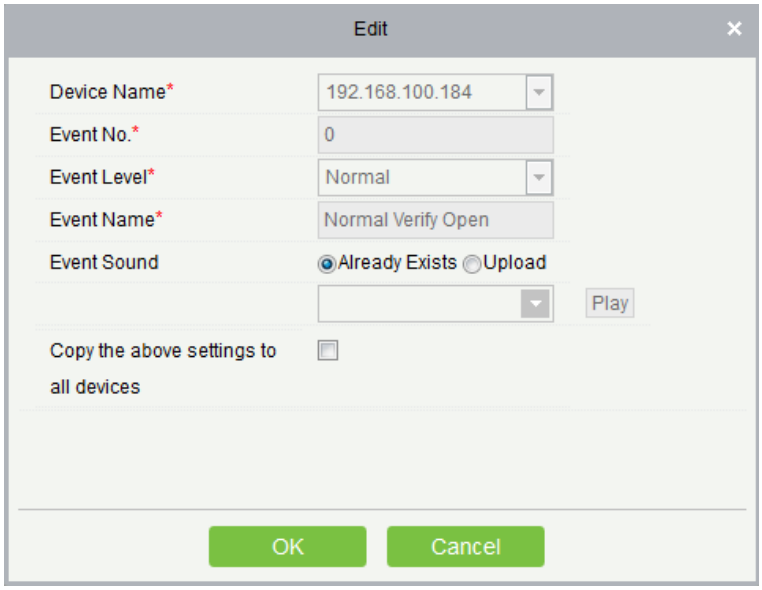
4.1.7 Event Type

Display the event types of the access devices.

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



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



Fields are as follows:

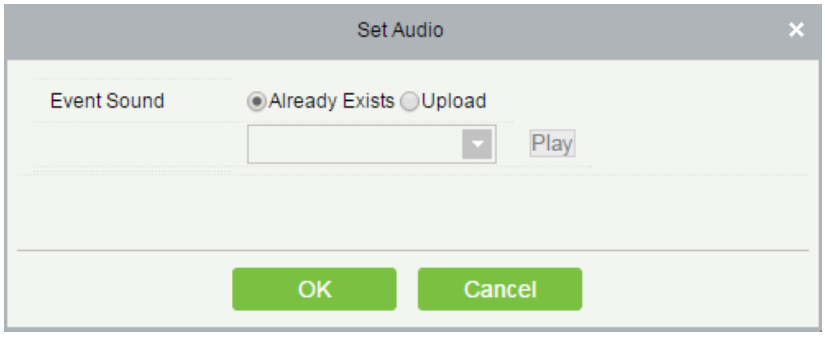
Event Level: Normal, Exception, and Alarm are available.

Event Name: It can't be modified.

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

Copies 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 Appendix 2 Access Event Type.

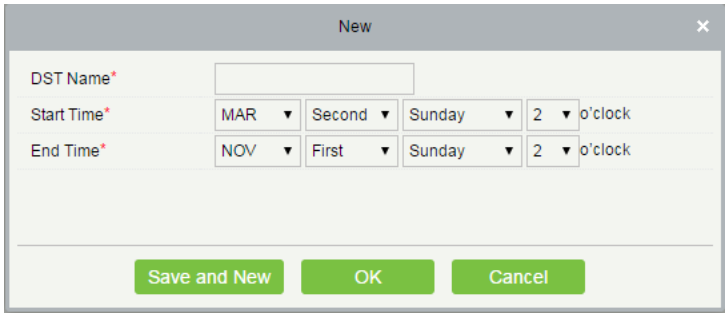
4.1.8 Daylight Saving Time

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.

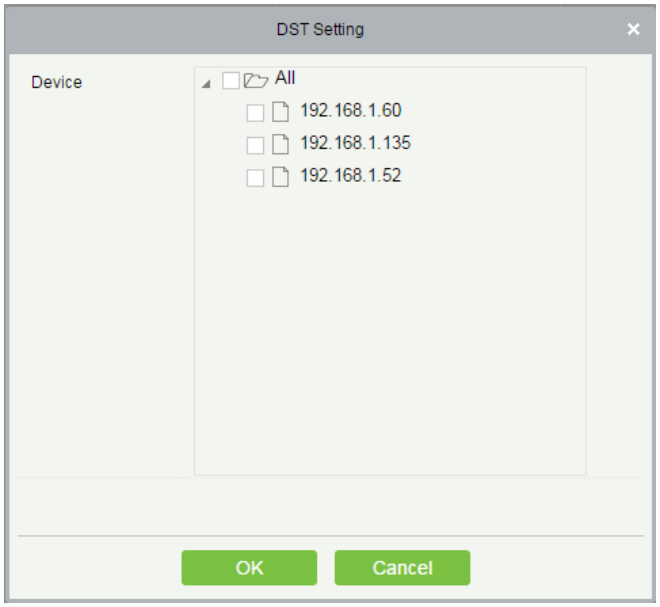
- Add DST

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.

✍ Note:

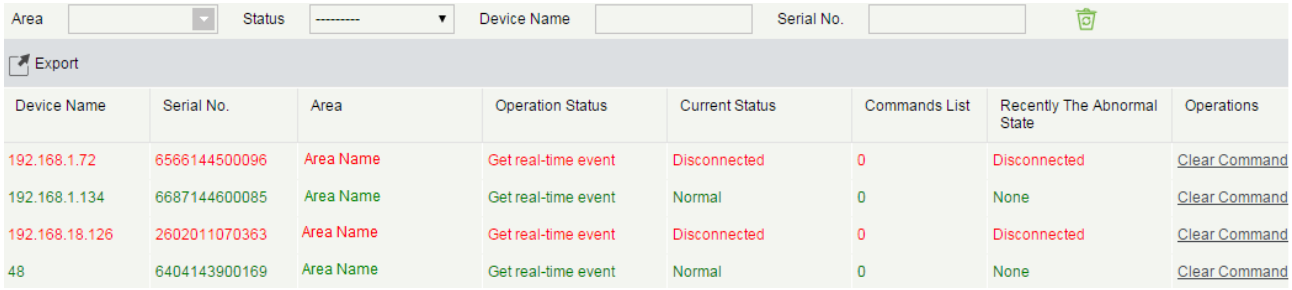
1) If a DST setting is in use, it cannot be deleted. Stop the DST before deleting.

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”.

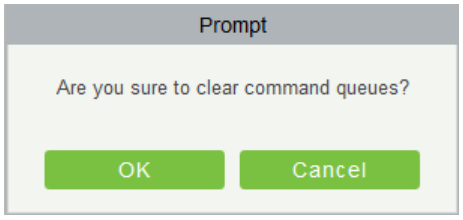
4.1.9 Device Monitoring

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.



Device Name	Serial No.	Area	Operation Status	Current Status	Commands List	Recently The Abnormal State	Operations
192.168.1.72	6566144500096	Area Name	Get real-time event	Disconnected	0	Disconnected	Clear Command
192.168.1.134	6687144600085	Area Name	Get real-time event	Normal	0	None	Clear Command
192.168.18.126	2602011070363	Area Name	Get real-time event	Disconnected	0	Disconnected	Clear Command
48	6404143900169	Area Name	Get real-time event	Normal	0	None	Clear Command

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



Click [OK] to clear.

✍Note:

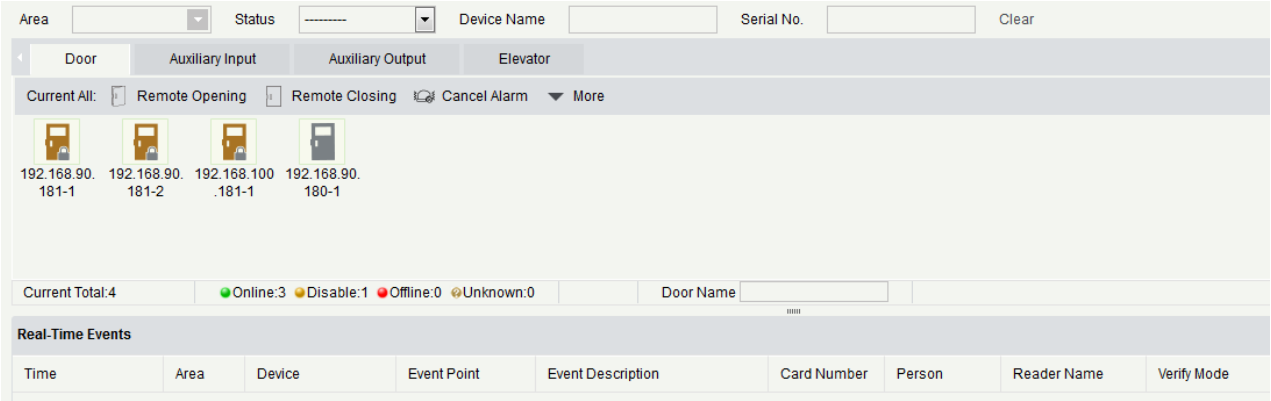
(1 After the Clear Command is executed, you can perform the Synchronize All Data to Devices operation on the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once 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

✍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, will come out a menu, 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.

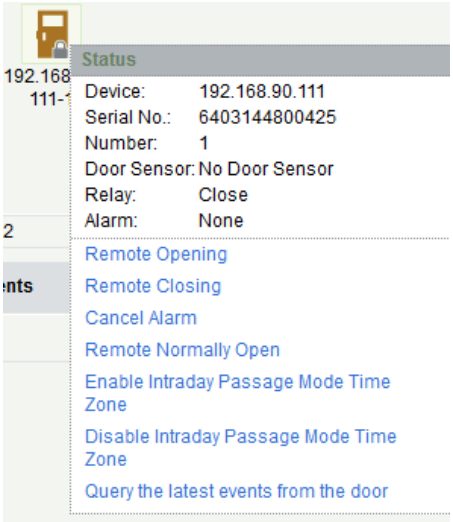
Remote Normally Open: Set the device as normal open by remote.

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.

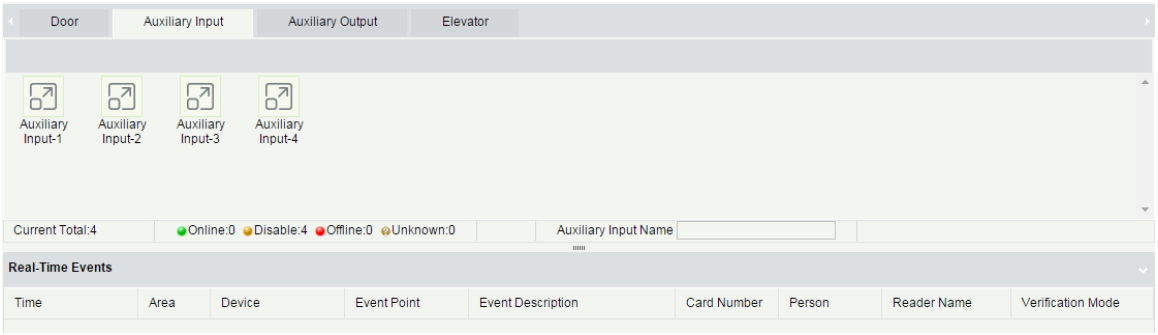
Issue card to person: If you swap an unregistered card, in real-time monitoring interface, will turn up a record with a card number. Right click that card number will show you a menu, click "Issue card to person", you can assign that card to one person.

- 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.

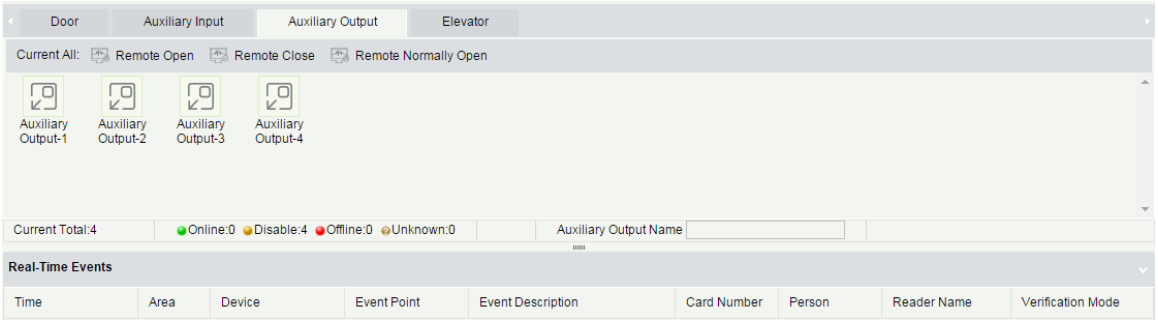
2. Auxiliary Input

Real-time monitor the current auxiliary input events.



3. Auxiliary Output

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

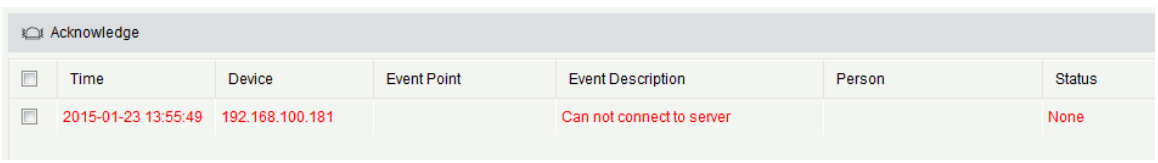


4. Elevator

About the real-time monitoring of elevator, please refer to 5.1.7 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.



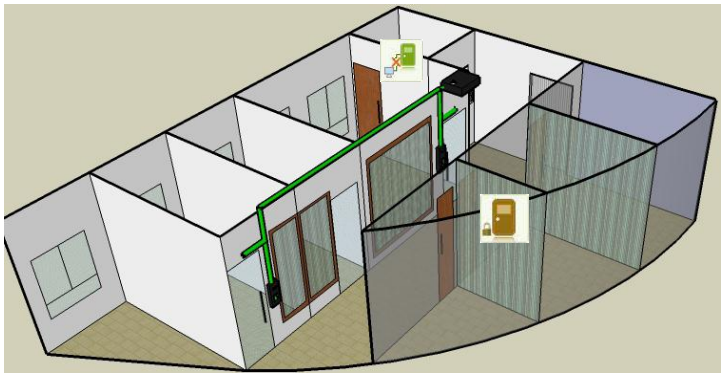
✍Note: The alarm type description will display only when the firmware version of the device supports, or Event Description will only display "alarm", detail types will not distinguish.

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 the4.3.7 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

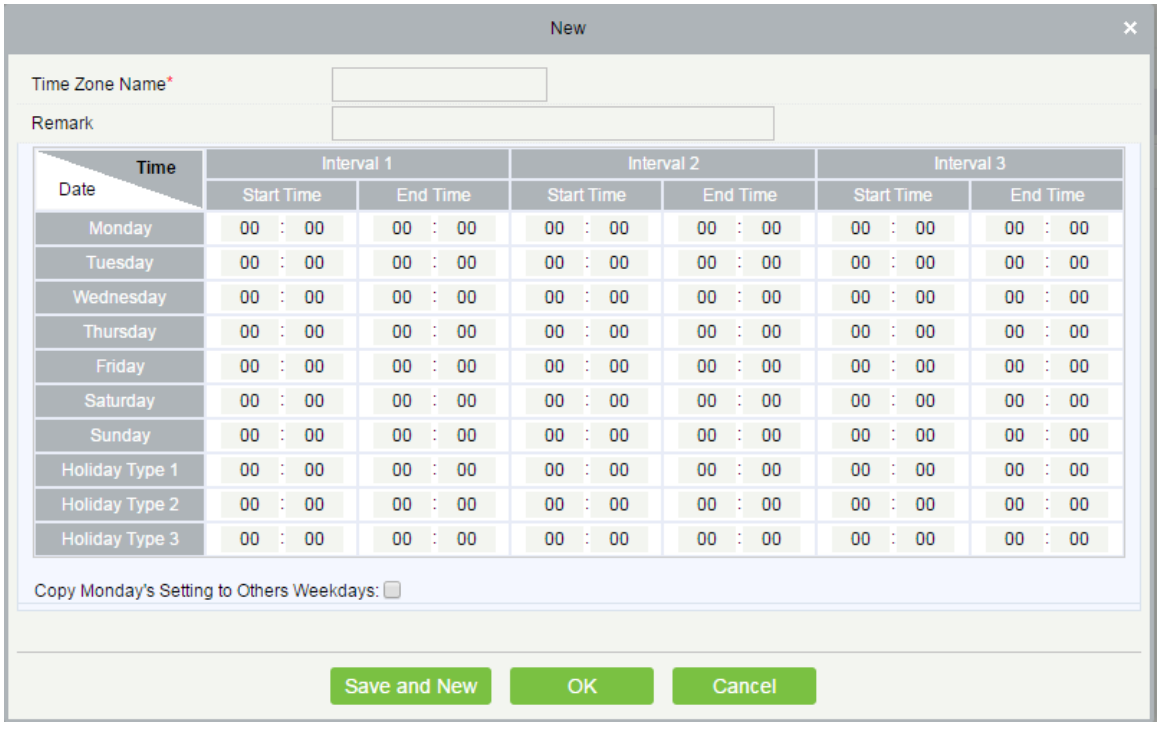
4.2.1 Access Control Time Zones

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.

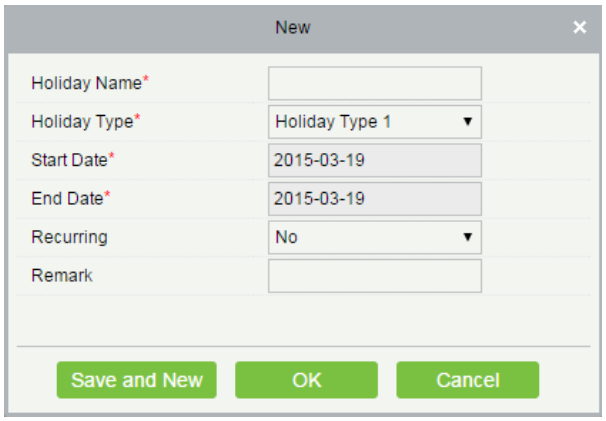
Delete: Click the [Delete] button under Related Operation, then click [OK] to delete, or click [Cancel] to cancel the operation. A time zone in use cannot be deleted. Or tick the check boxes before one or more time zones in the list, and click the [Delete] button over the list, then click [OK] to delete,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

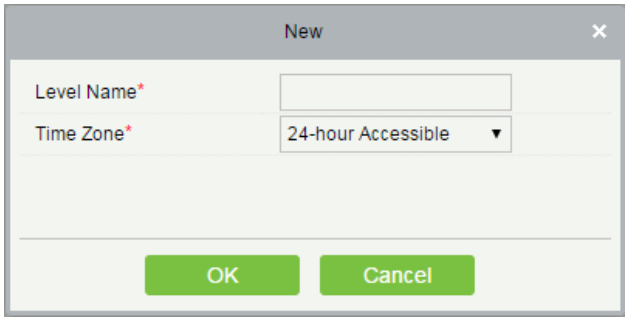
In the access control holiday list, click [Delete] button under Operations. Click [OK] to delete, click [Cancel] to cancel the operation. An Access Control Holiday in use cannot be deleted.

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.

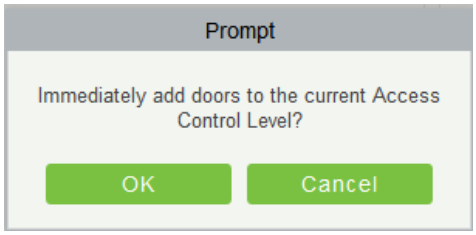
Add

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 By Levels

Add/Delete Personnel for Selected Levels:

(1) Click [Access Control] > [Access Levels] > [Set 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 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 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.

4.3 Access Rule

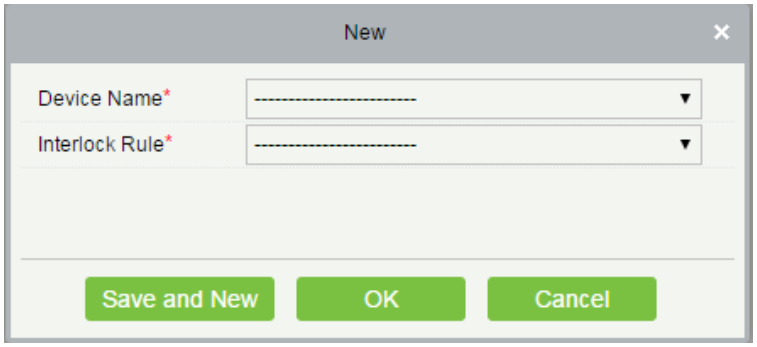
4.3.1 Interlock Settings

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.

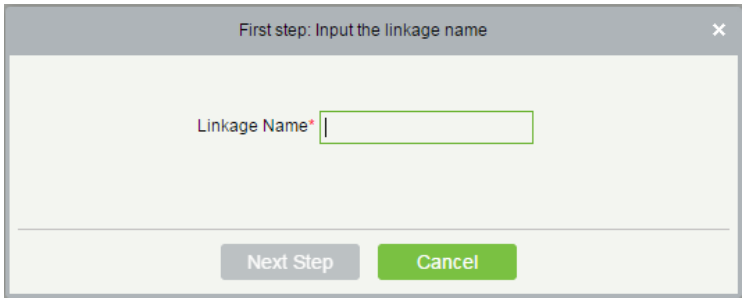
✍Note: When editing, the device cannot be modified, but the interlock setting can be modified. If interlock setting is not required for the device any more, the interlock setting record can be deleted. When deleting a device record, its interlock setting record, if exists, will be deleted.

4.3.2 Linkage Setting

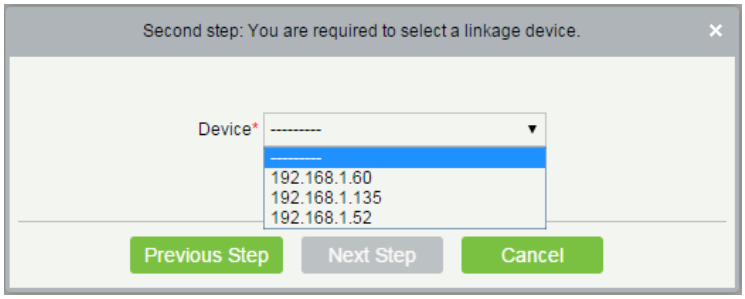
Linkage setting means when an event is triggered at an input point of the access control system, a linkage action will occur at the specified output point to control such events as verification, opening, alarm and abnormal of system and list them in the corresponding monitored report for view.

Add Linkage setting:

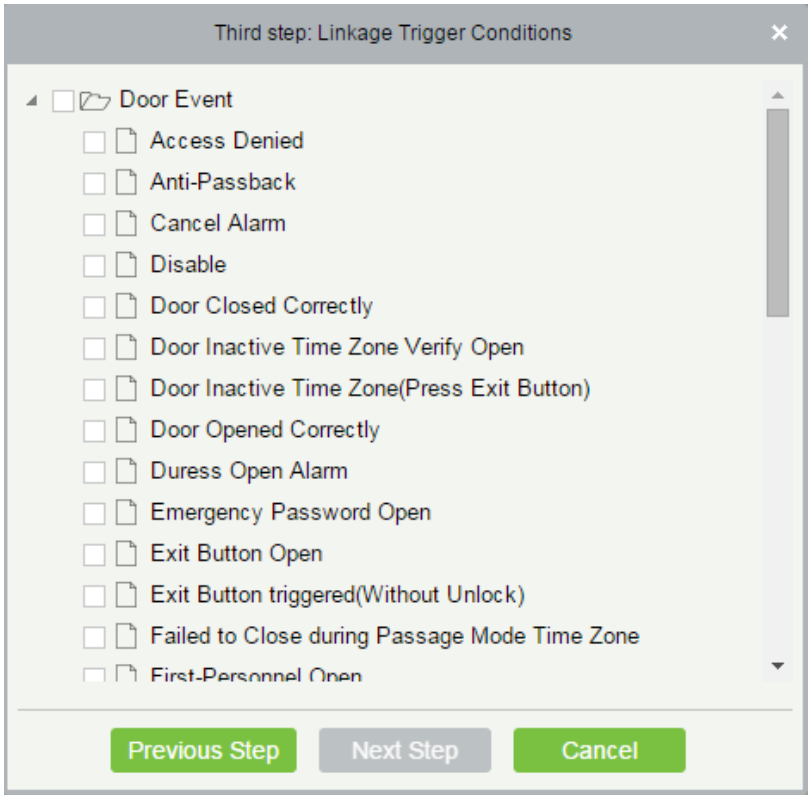
1. Click [Access Control] > [Linkage] > [Add], fill in blank with a linkage name:



2. Select a device.

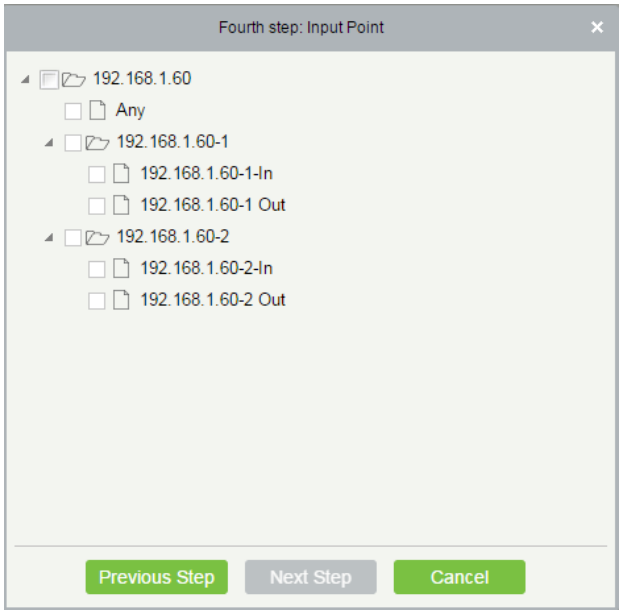


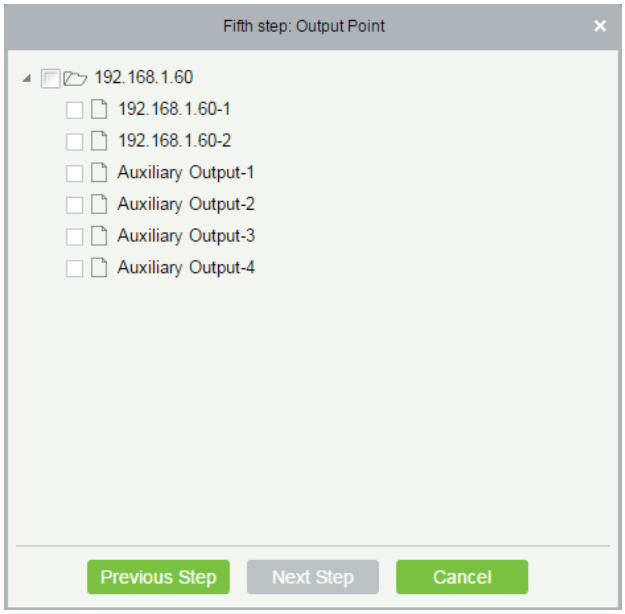
3. After selecting device, corresponding linkage setting will display (System will first judge whether or not the device is successfully connected and has read extended parameters. If no available extended parameters, system cannot set linkage. Otherwise, it will show linkage setting according to the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



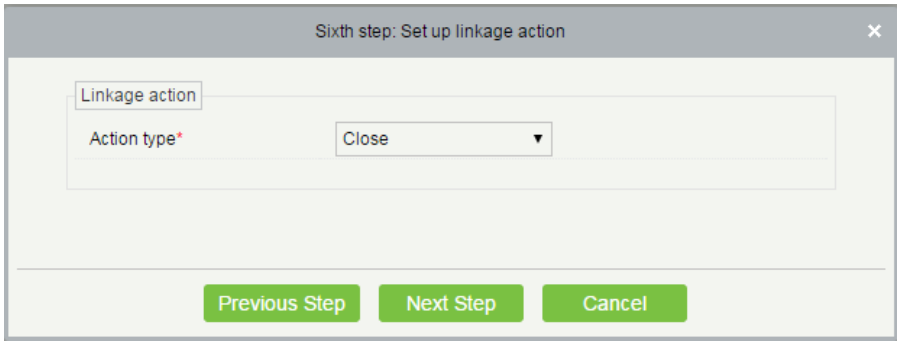
✍Note: Linkage trigger conditions contain Door Event and Auxiliary Input Event. And "Fail to connect server", "Recover connection", "Device connection off" will be filtered from Door Event.

Select the Input point and output point:

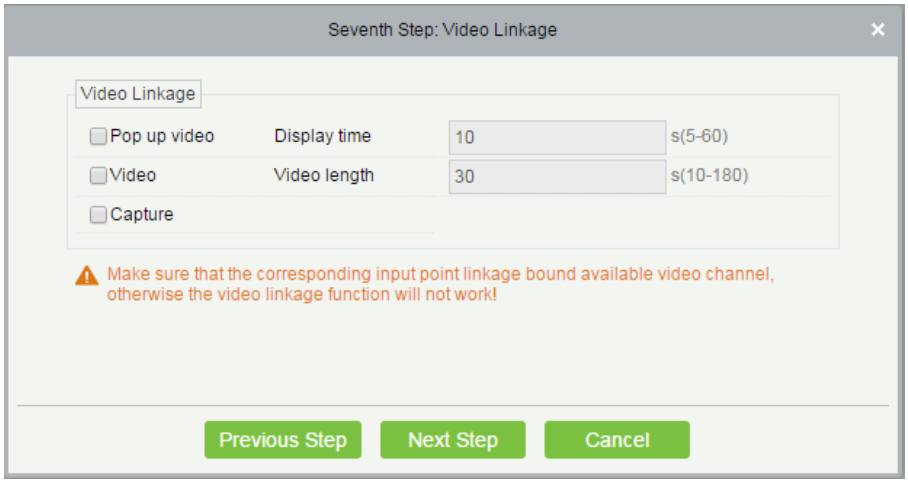




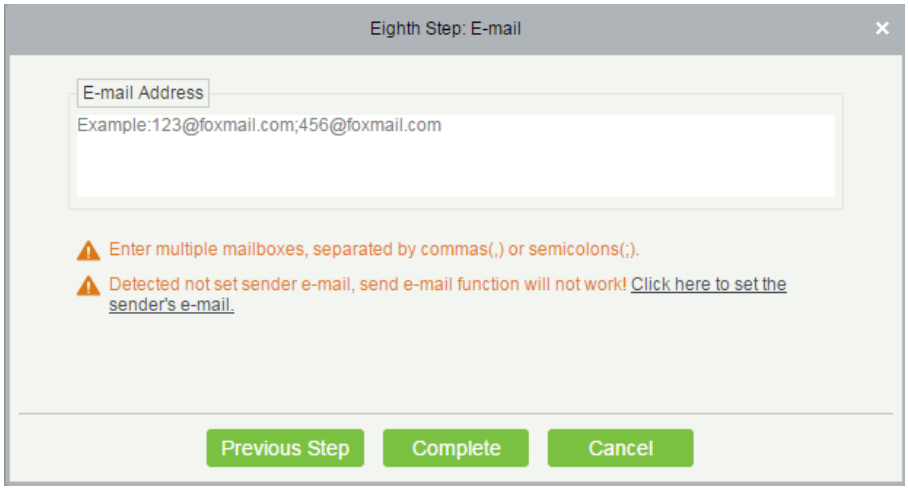
Setup Linkage action:



Setup Video Linkage:



Setup 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, 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 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).

4. 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.

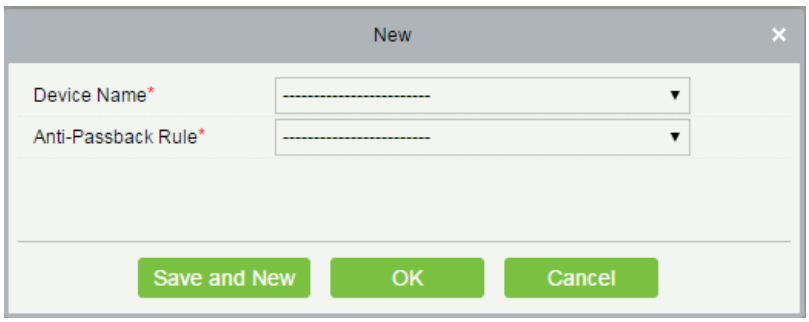
In addition, same linkage setting at input point and output point is not allowed. The same device permits consecutive logical linkage settings. The system allows to set several trigger conditions for a linkage setting one time.

4.3.3 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.

4.3.4 First-Person Normally Open

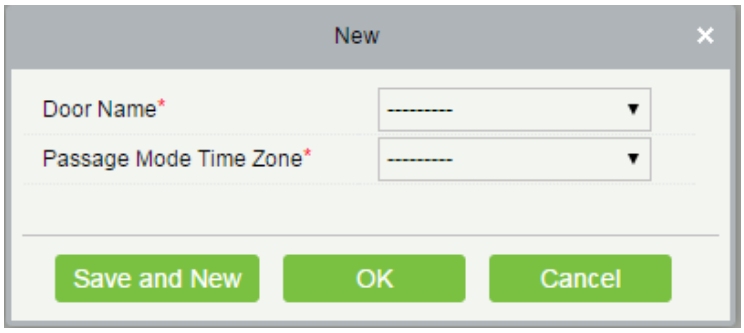
First-Person Normally Open: During a specified interval, after the first verification by the person having First-Person Normally Open level, the door will be Normal Open, and will automatically restore closing after the valid interval has expired.

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.

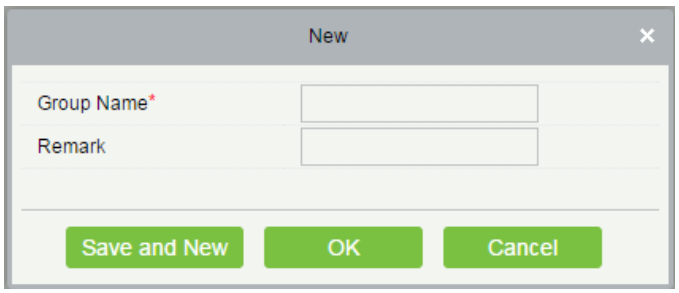


2. Click [Add Personnel] under Related operation to add personnel having First-Person Normally Open level (this personnel must have access control level), then click [OK] to save.

4.3.5 Multi-Person Personnel 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 Personnel 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.

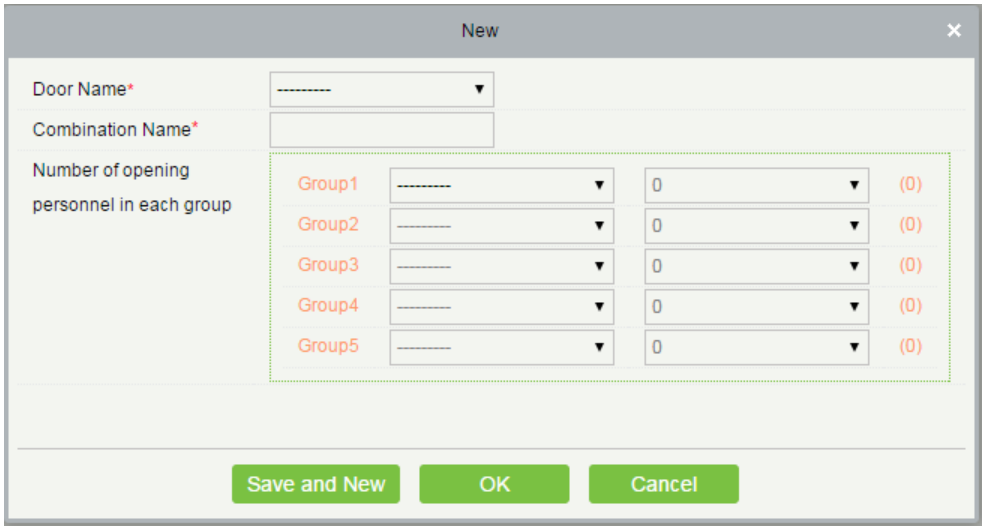
4.3.6 Multi-Person Opening Door

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 disable.

Multi-Person Opening Door Settings:

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



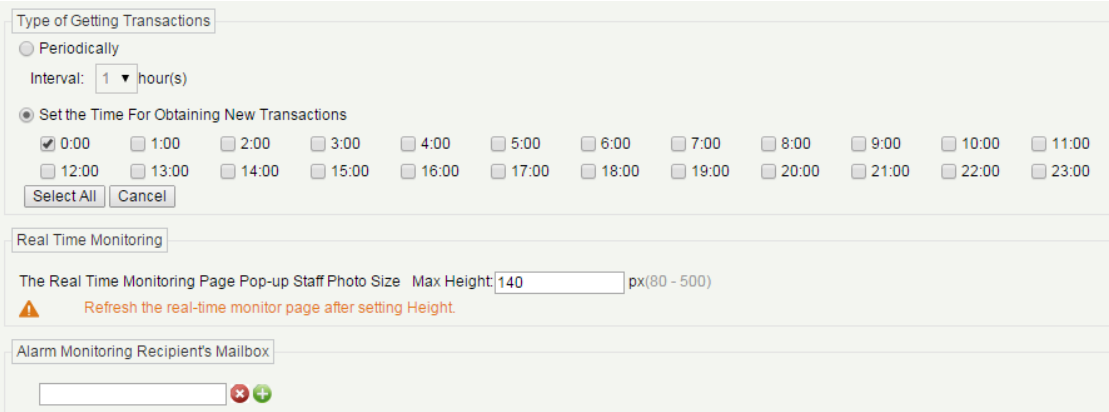
(2) The number of Multi-Person Opening Door people for combined door opening is up to 5. That in the brackets is the current actual number of people in a group. Select the number of people for combined door opening in a

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.

4.3.7 Parameters

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



Type of Getting Transactions

- Periodically

From the setting and efficient time begin, 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.

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

4.4 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.

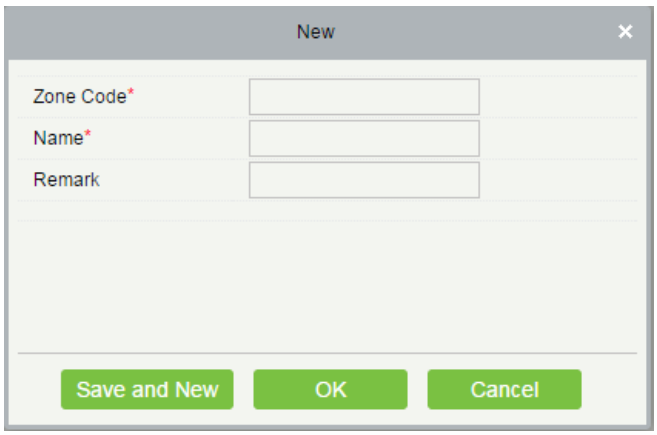
✍Note: Except Global Linkage, to use other advanced functions you need to enable Background Verification. For detail, please see 4.1.2 Device Operation.

4.4.1 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.

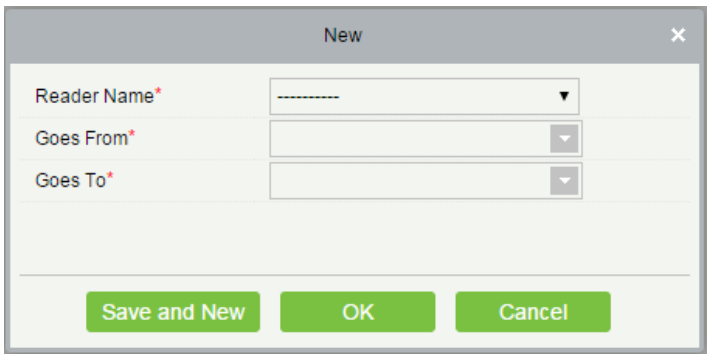
What rules inside:

4.4.2 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.

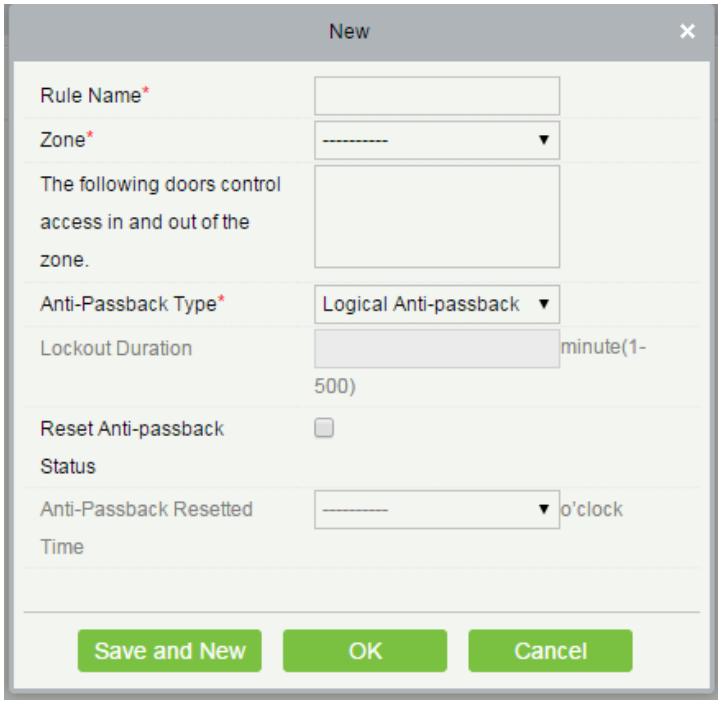
3. Click [OK] to save and quit. The added Reader Define will appear in the list.

4.4.3 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.

4.4.4 Who is Inside

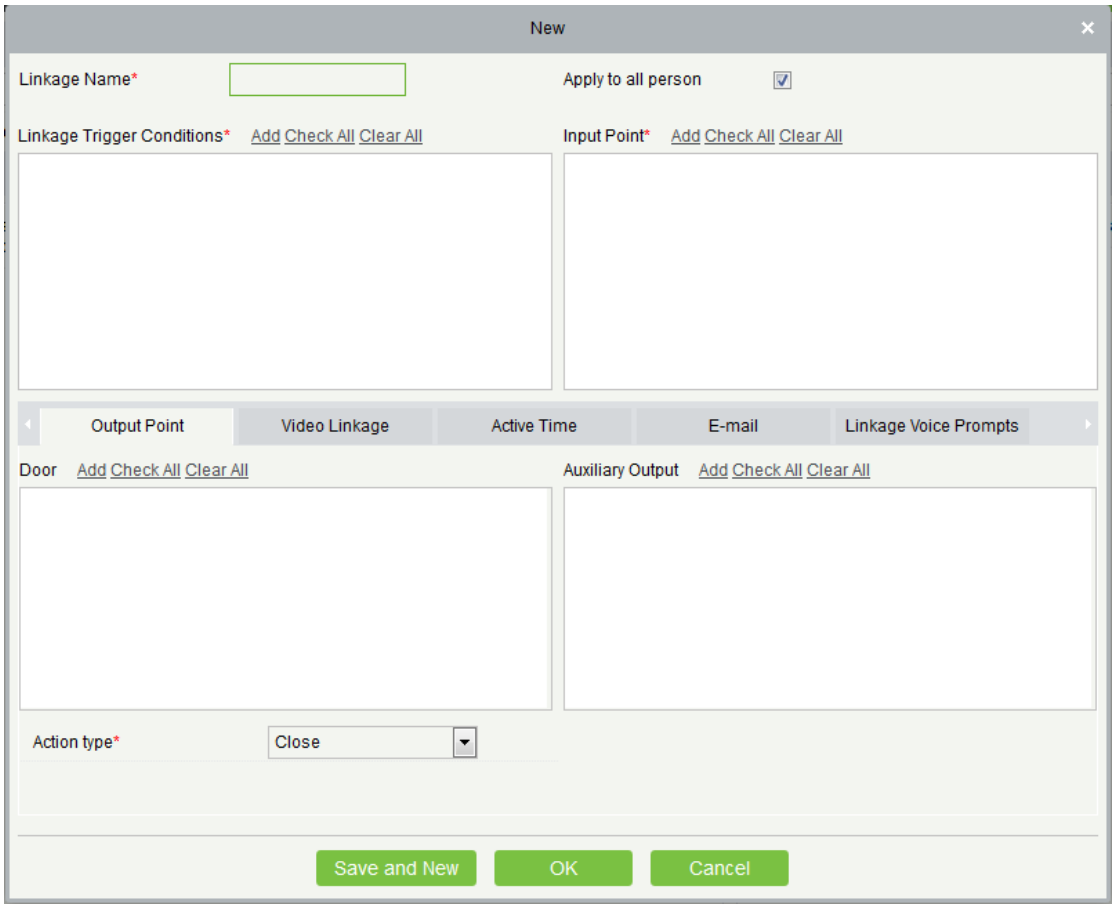
After enter the zone, you can view all personnel status in the zone by zone tree.

4.4.5 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]:



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. More details about these parameters, please refer to 4.3.2 Linkage Setting.

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

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

4.5 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.

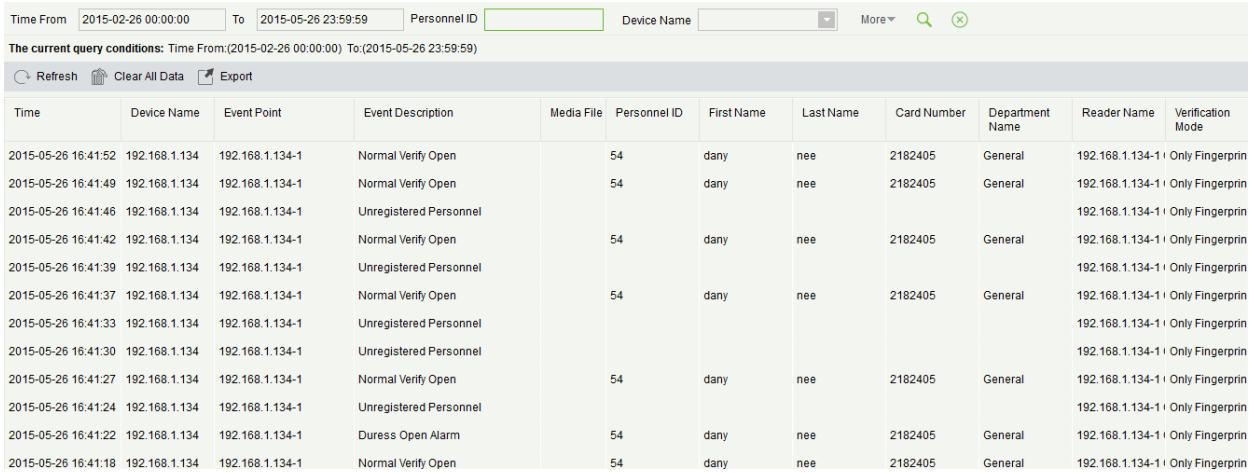
About the Normal and abnormal event please refer to 4.1.10 Real-Time Monitoring for details.

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.

4.5.1 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

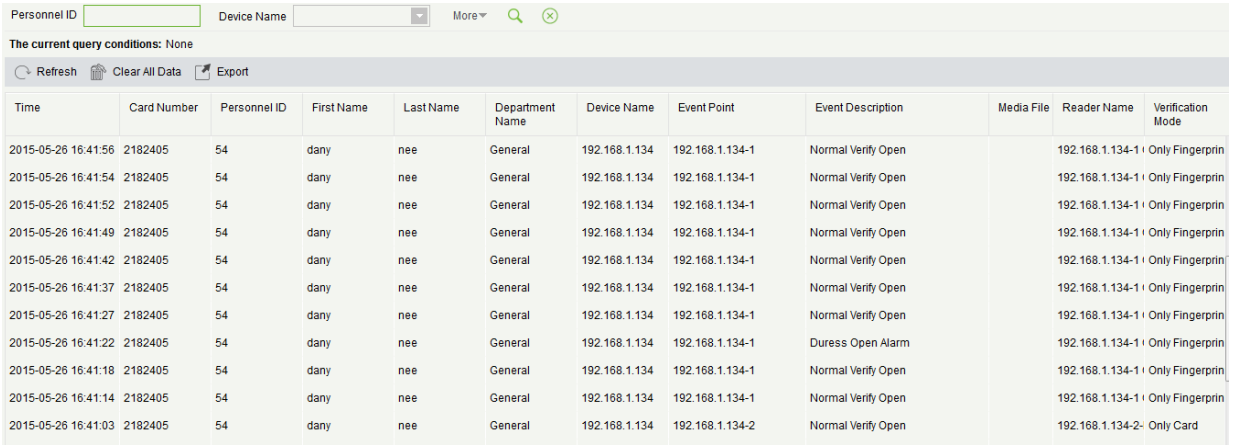
Clear All Data:

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

4.5.2 Events from Today

Check out the system record today.

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

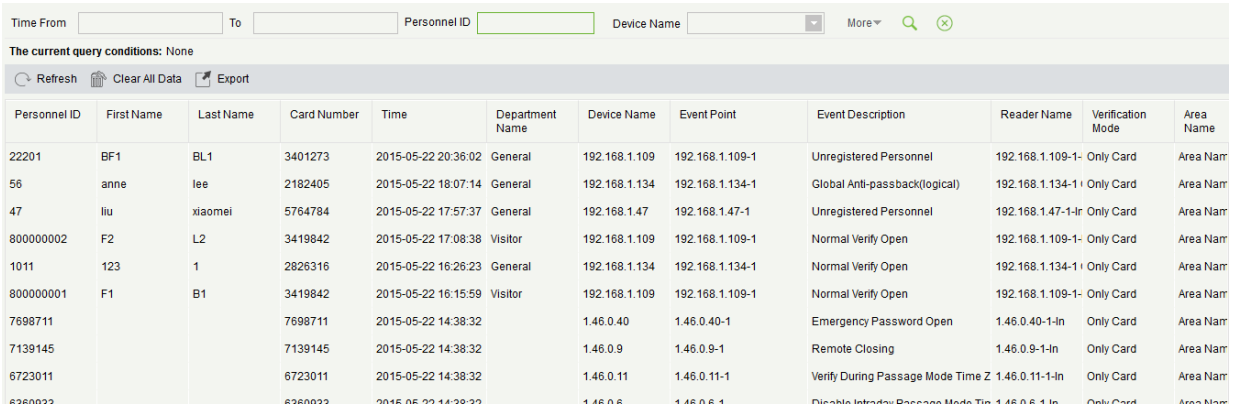


Time	Card Number	Personnel ID	First Name	Last Name	Department Name	Device Name	Event Point	Event Description	Media File	Reader Name	Verification Mode
2015-05-26 16:41:56	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:54	2182405	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

4.5.3 Last Known Position

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

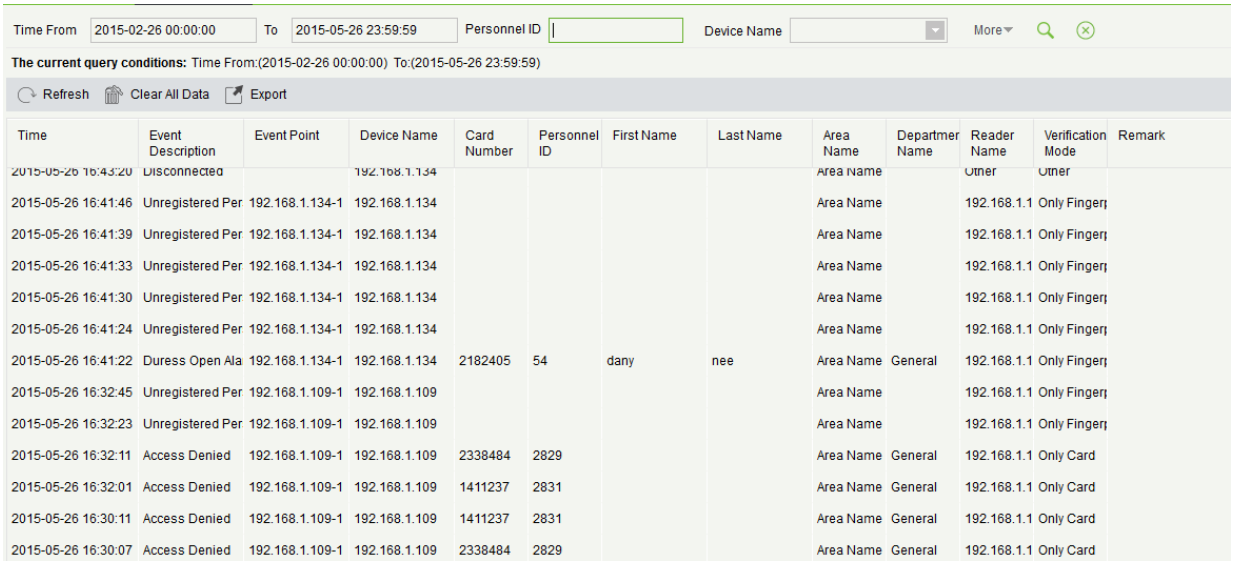
Click [Access] > [Reports] > [Last Know Position] to check out.



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
6360933			6360933	2015-05-22 14:38:32		1.46.0.6	1.46.0.6-1	Disable Intraday Passage Mode Tim	1.46.0.6-1-In	Only Card	Area Nam

4.5.4 All Exception Events

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



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

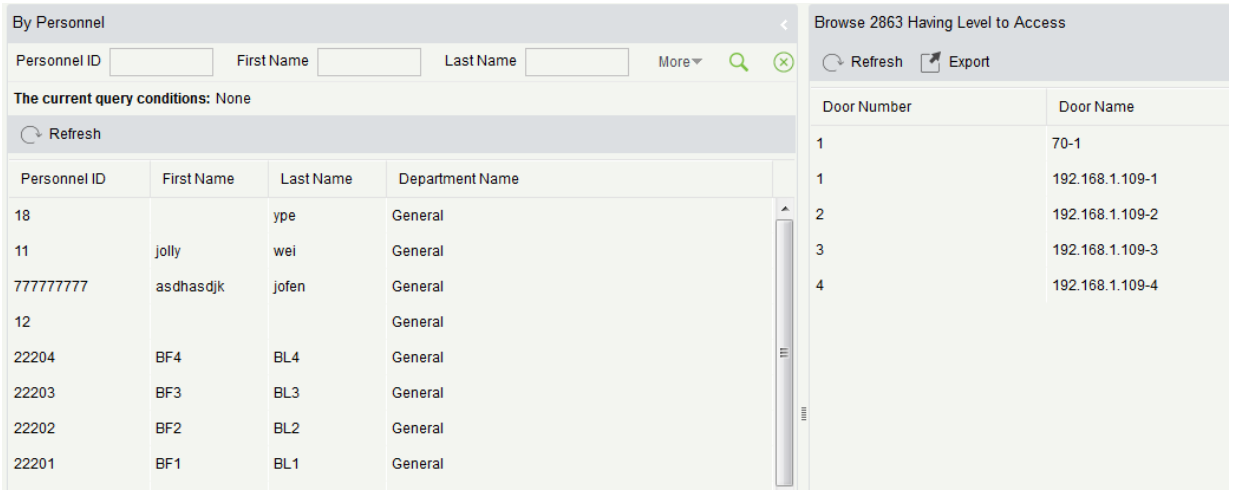
- By Door

View related access levels by door. Click [Reports] > [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.

- By Personnel

View related access levels by door or personnel.

Click [Reports] > [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.


By Personnel
Personnel ID
First Name
Last Name
More
The current query conditions: None
Refresh
Personnel ID
First Name
Last Name
Department Name
18
ype
General
11
jolly
wei
General
777777777
asdhasdjk
jofen
General
12
General
22204
BF4
BL4
General
22203
BF3
BL3
General
22202
BF2
BL2
General
22201
BF1
BL1
General
Browse 2863 Having Level to Access
Refresh
Export
Door Number
Door Name
1
70-1
1
192.168.1.109-1
2
192.168.1.109-2
3
192.168.1.109-3
4
192.168.1.109-4

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

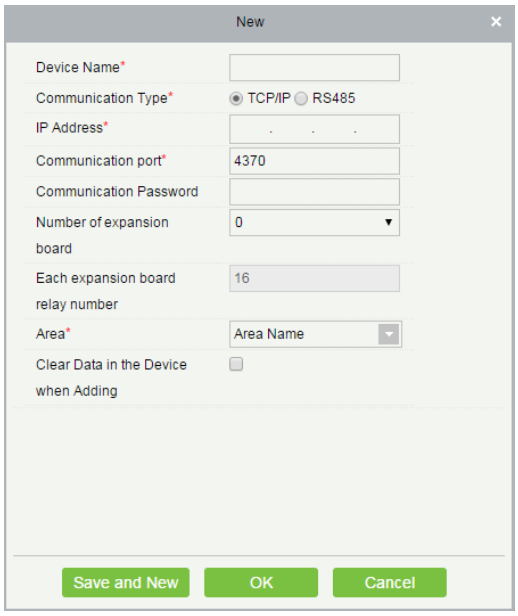
5.1.1 Add an Elevator Device

There are two ways to add Elevator Devices.

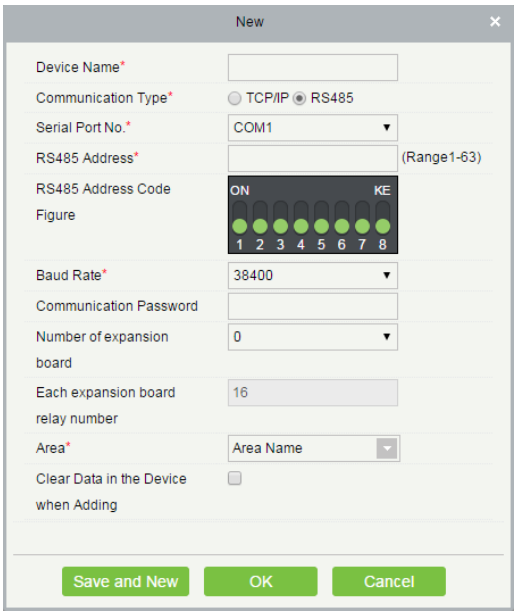
- Add Device by manually

(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.

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

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

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.

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.

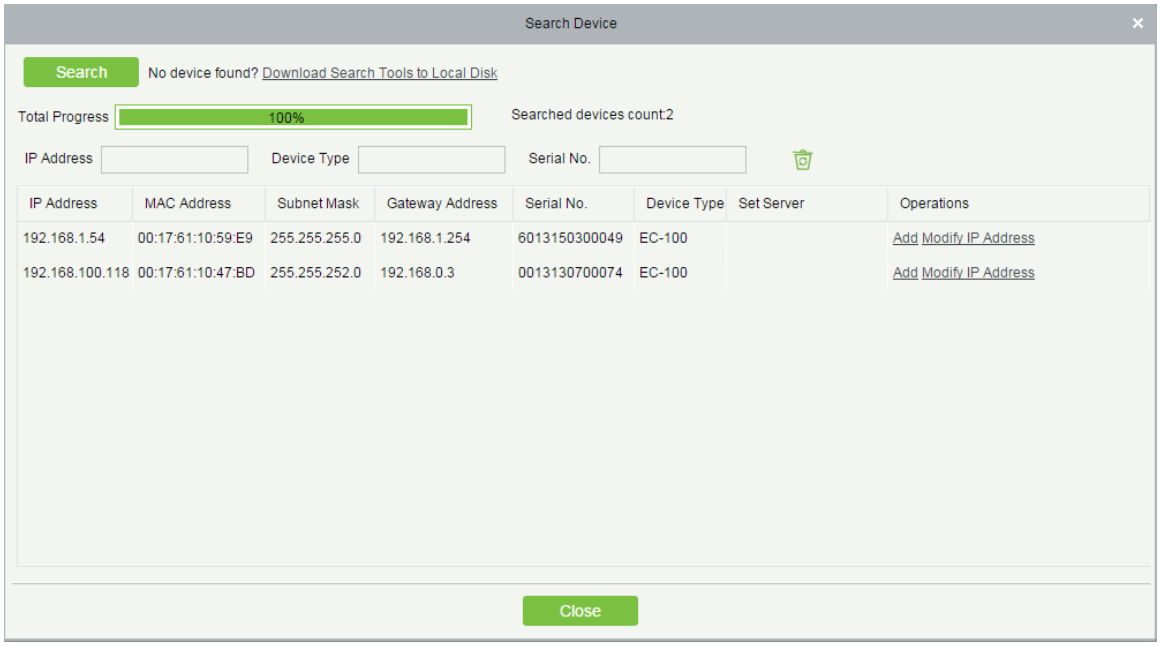
2. Add Device by Searching Elevator Controllers

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.

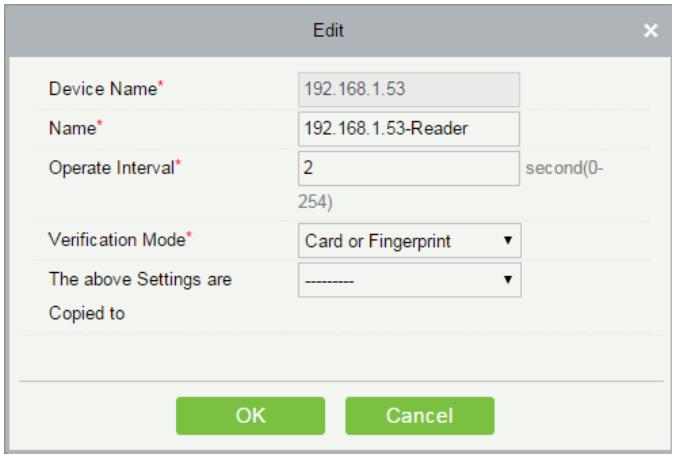
(5) The default IP address of the access controller may conflict with the IP of a device on the Local network. You can modify its IP address: Click [Modify IP Address] behind the device and a dialog box will open. Enter the new IP address and other parameters (Note: Configure the gateway and IP address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

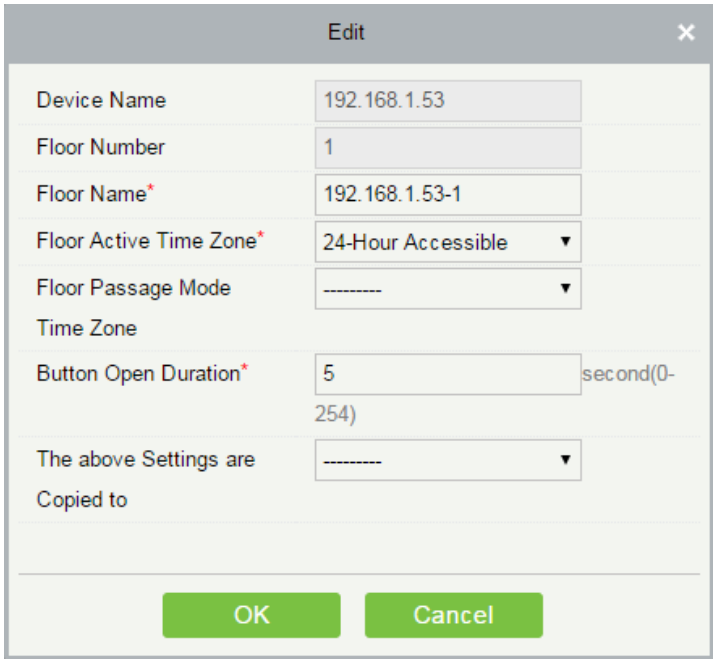
The above Settings are Copied to:

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.

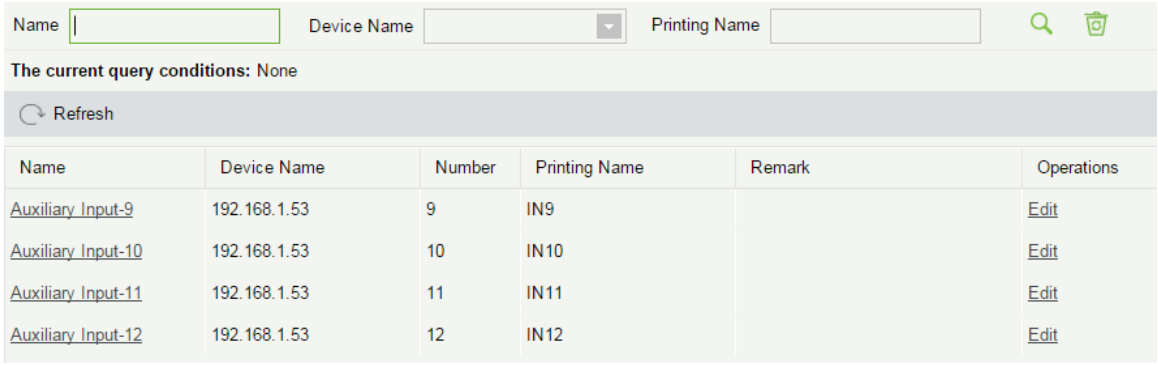
The above Settings are Copied to: Including below two options.

- 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.

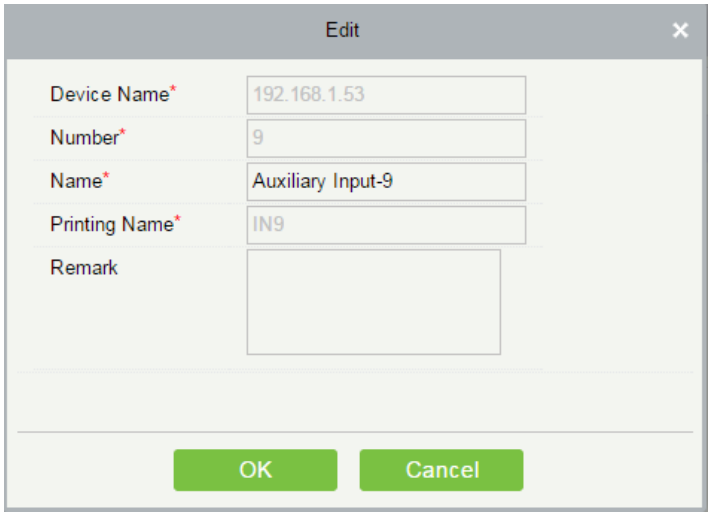
5.1.4 Auxiliary Input

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.

Printing 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 Appendix 3 Elevator Event Type.

5.1.6 Device Monitoring

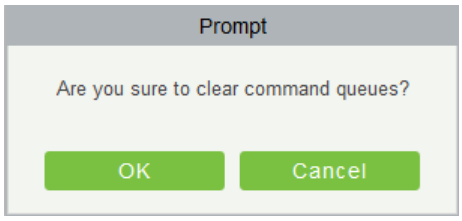
By default it monitors all devices within the current user's level, click [Elevator Device] > [Device Monitoring], and lists the operation information of devices: Device Name, Serial No., Area, Operation Status, current status, commands List, and Related Operation.

Area Status --------- Device Name Serial No. Clear

Export

Device Name	Serial No.	Area	Operate State	Current State	Commands List	Operations
192.168.100.181	0564141900371	Area Name	Get real-time event	Disconnected	0	Clear Command
192.168.90.111	6403144800425	Area Name	Get real-time event	Normal	0	Clear Command

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



Click [OK] to clear.

✍Note:

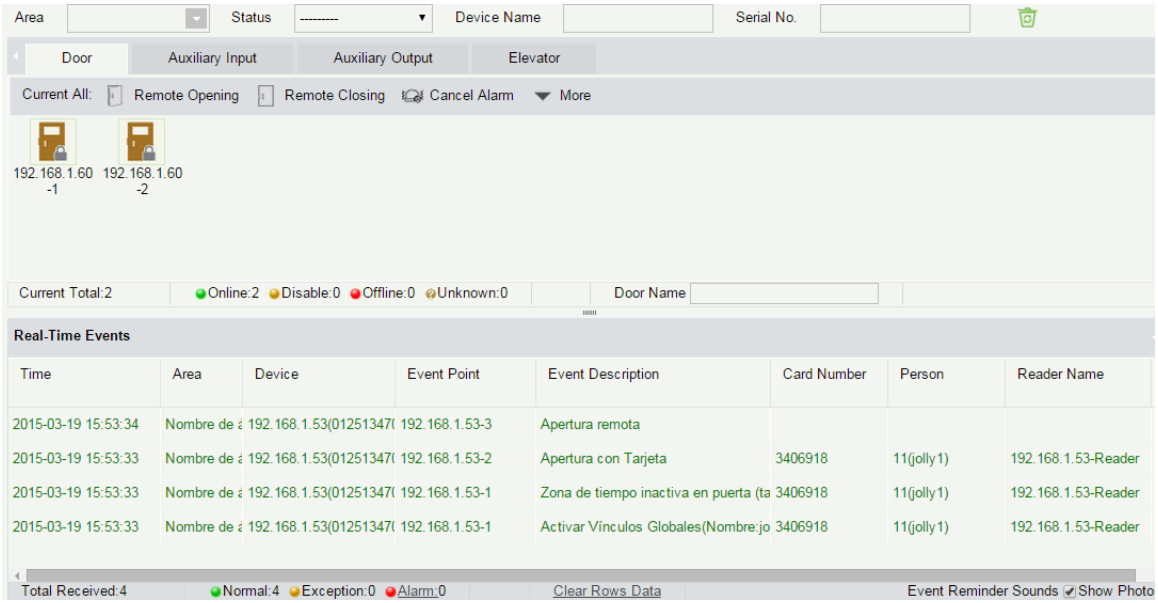
(1 After the Clear Command is executed, you can perform the Synchronize All Data to Devices operation on the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once 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 [Access 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

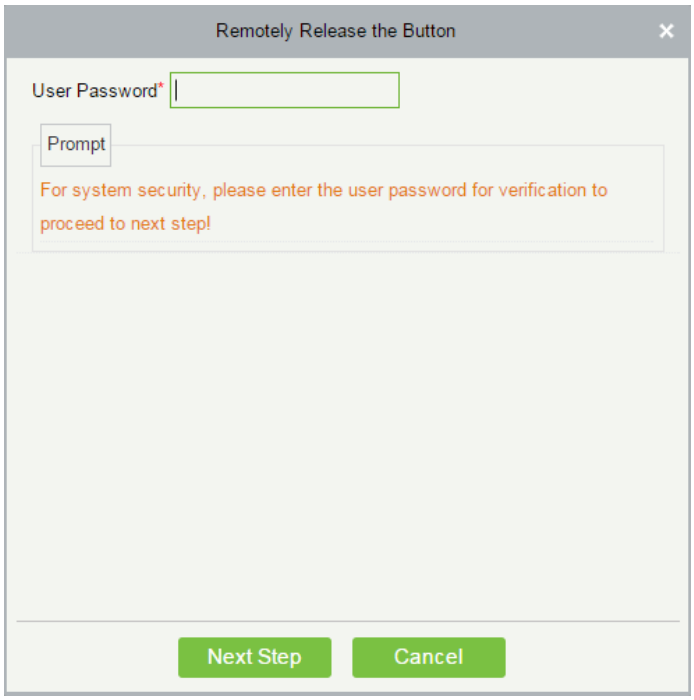
System automatically acquires monitored device event records (by default, display 200 records), including normal and abnormal elevator control events (including alarm events). Normal events appear in green, alarm events appear in red, other abnormal events appear in orange.

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

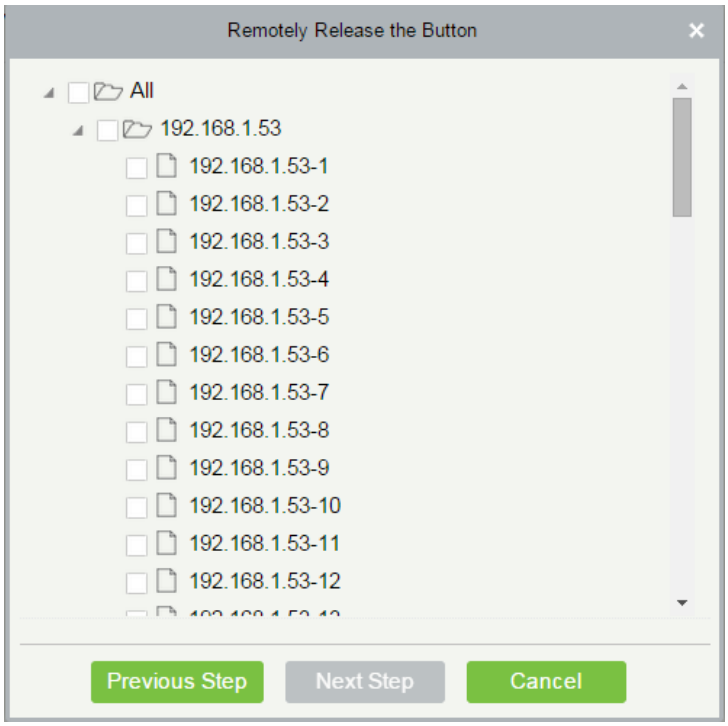
Show Photos: If Real-Time Monitoring is involved in a person, the monitor displays the personal photo (if no photo is registered, display default photo). The event name, time and name are displayed.

2. Remotely Release Button

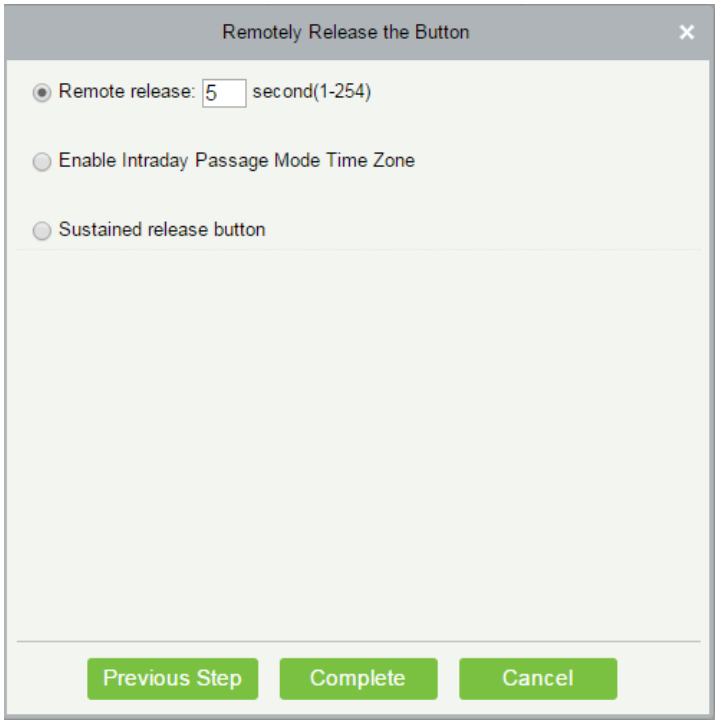
Click [Remotely Release Button]:



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.

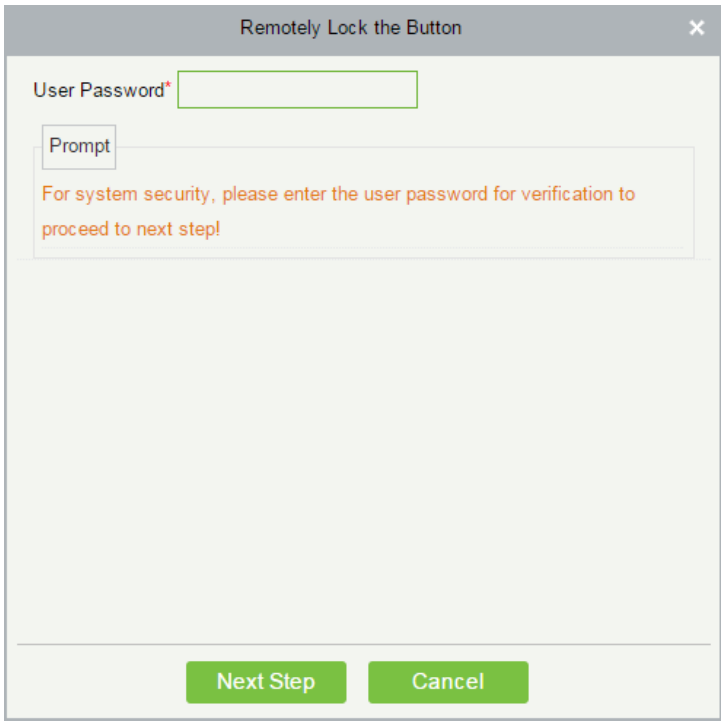
Sustained Release Button: The floor that is set to the continuously release state is not subject to restrictions of any periods, that is, the floor will be continuously released in 24 hours every day. To close the floor, you must select Disable Intraday Passage Mode Time Zone.

✍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.

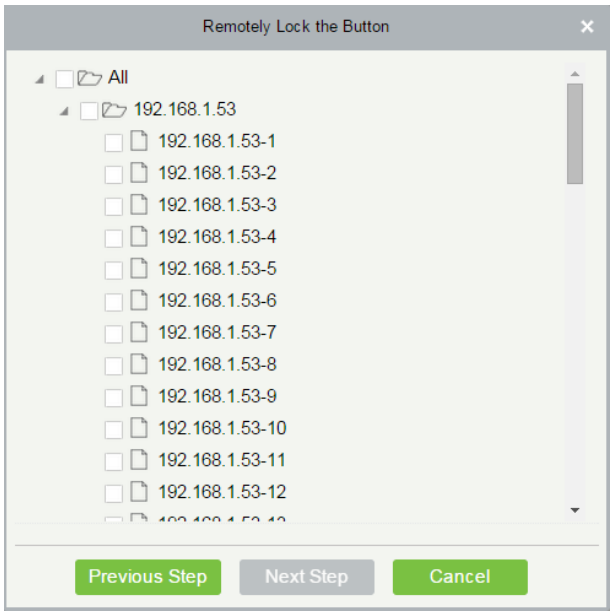
Select the options, click [Complete] to finish enabling the button.

2. Remotely Lock Button

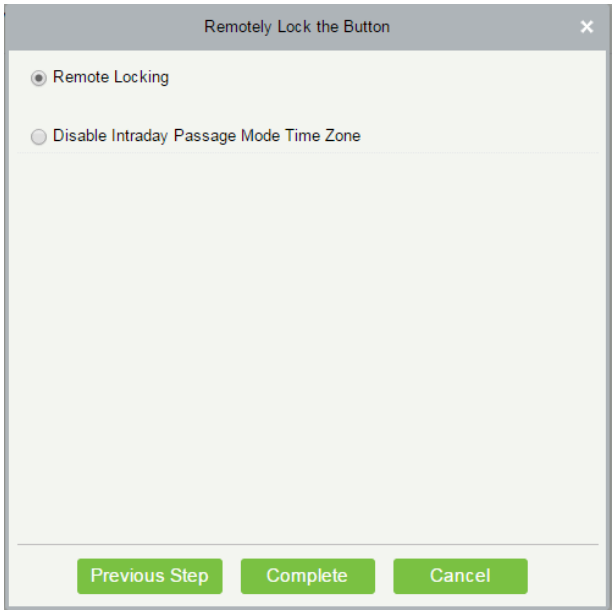
Click [Remotely Lock Button]:



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.

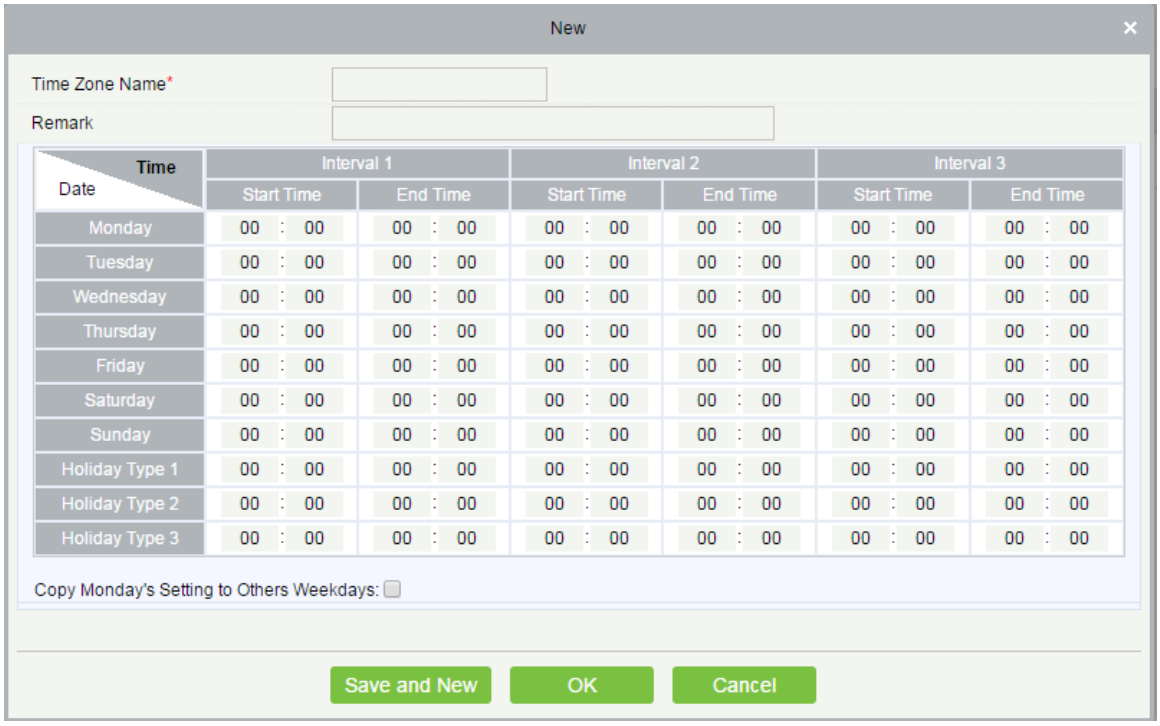
5.3 Elevator Rules

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.

5.3.1 Elevator Control 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.

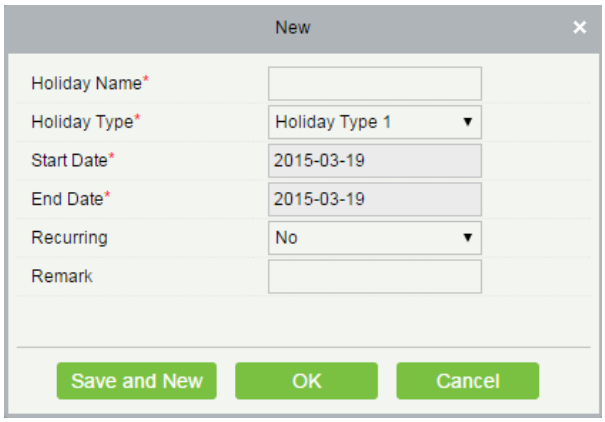
Delete: Click the [Delete] button under Related Operation, then click [OK] to delete, or click [Cancel] to cancel the operation. A time zone in use cannot be deleted. Or tick the check boxes before one or more time zones in the list, and click the [Delete] button over the list, then click [OK] to delete,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

5.3.2 Elevator Control 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.

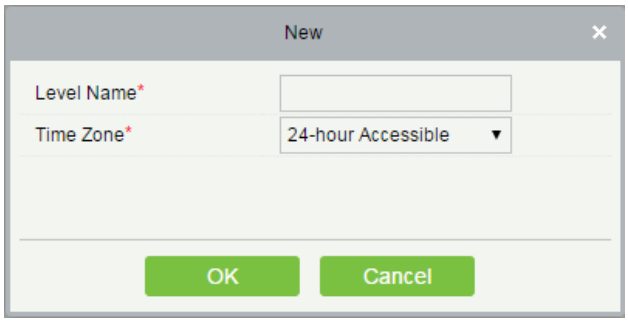
5.3.3 Elevator Levels

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.

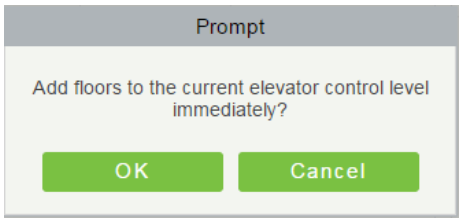
- Add

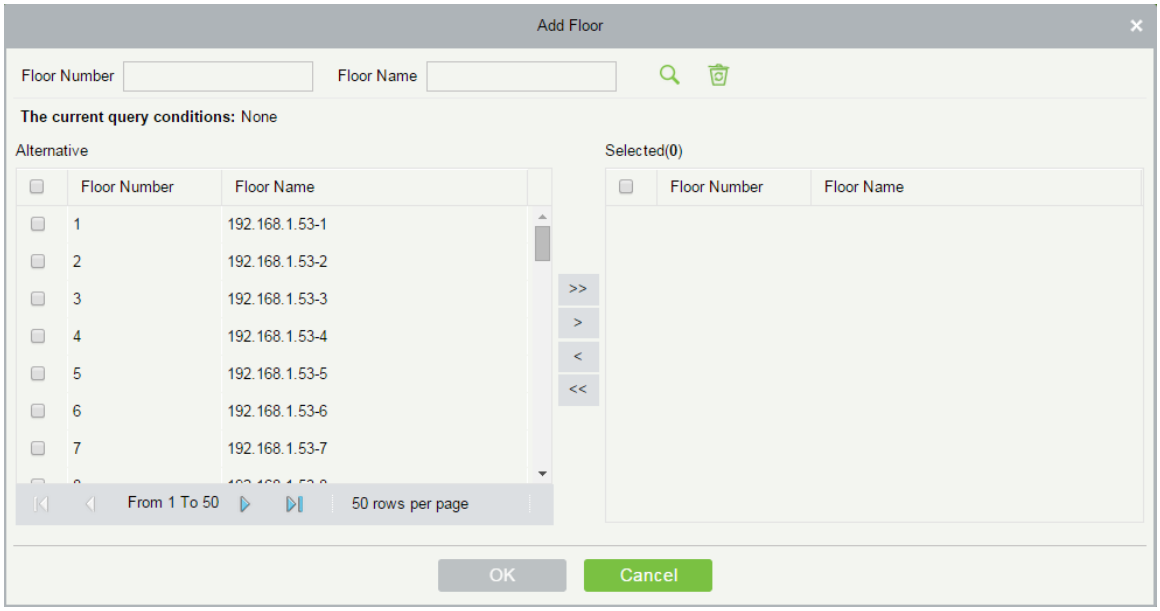
1. Click [Elevator] > [Access Levels] > [Add] to enter the Add Levels editing interface:



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

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 By Levels

Add/Delete Personnel for Selected Levels:

(4) 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.

(5) 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.

(6) 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 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.

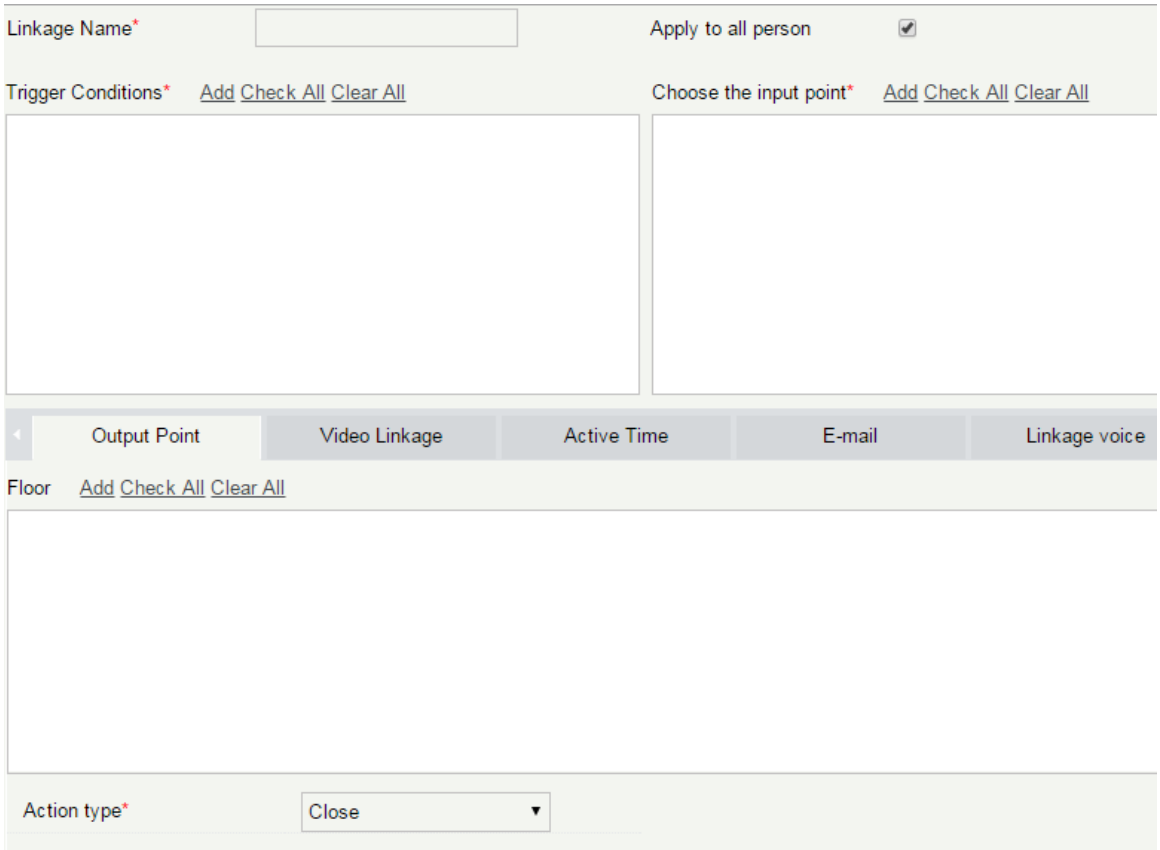
(3) Select Level (multiple) in the right list, and click [Delete from levels] above the list, then click [OK] to delete the selected levels.

5.3.4 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

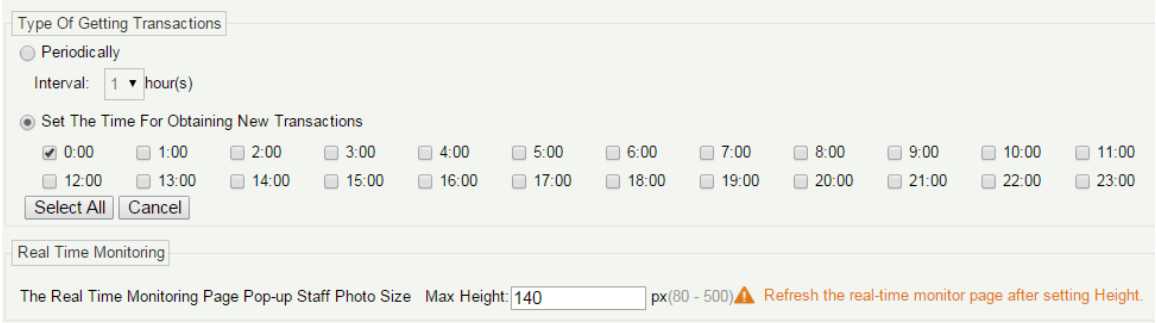
Delay: Ranges from 1~254s (This item is valid when Action type is Open).

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.

5.3.5 Parameters

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



Type of Getting Transactions

- Periodically

From the setting and efficient time begin, 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.

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

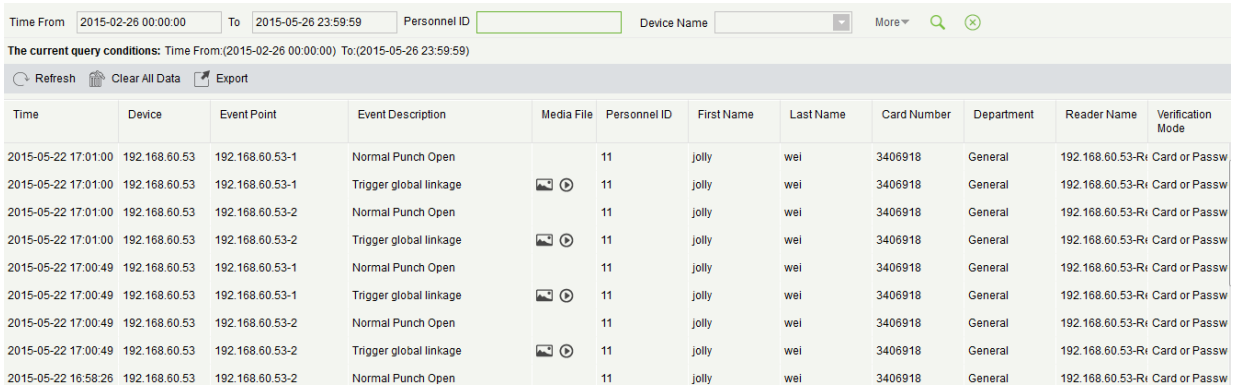
5.4 Elevator Reports

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

5.4.1 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 displays latest three months transactions.

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



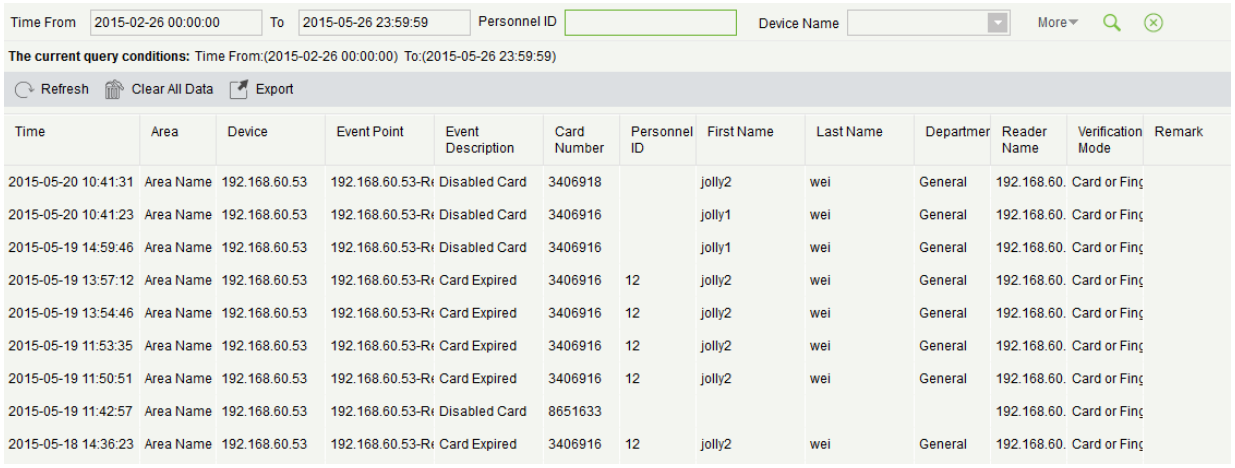
Time	Device	Event Point	Event Description	Media File	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-1	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:01:00	192.168.60.53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

5.4.2 All Exception Events

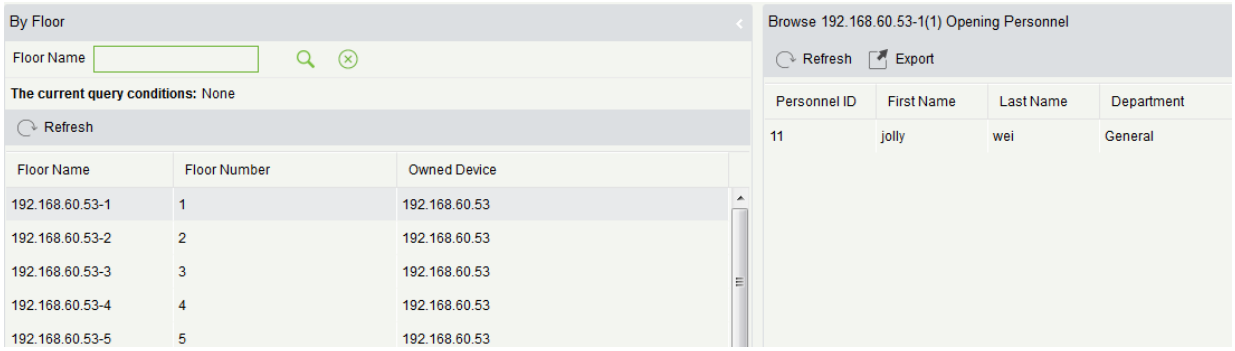
Click [Reports] > [All Exception Events] to view exception events in specified condition. The options are same as those of [All Transactions].



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

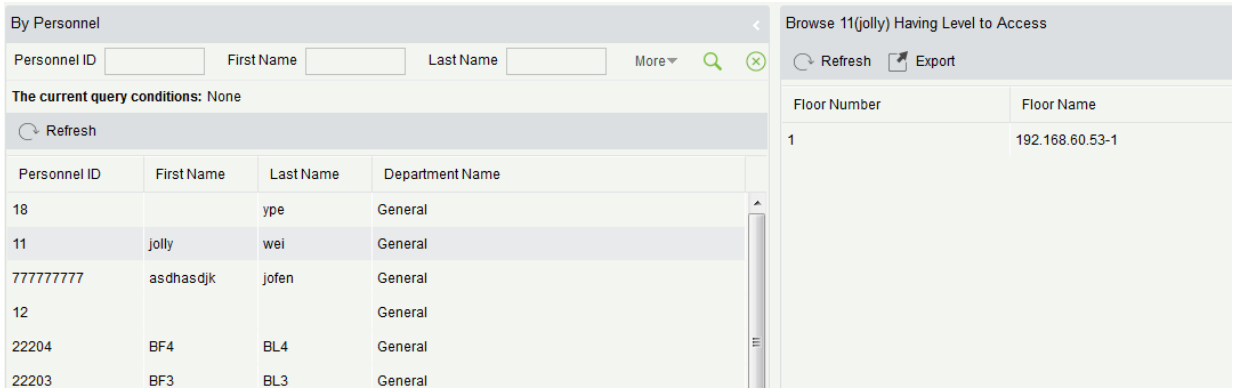
- By Floor

View related access levels by door. Click [Reports] > [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.



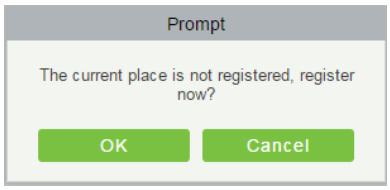
- By Personnel

Click [Reports] > [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. 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 6.3.3 Entry Place .

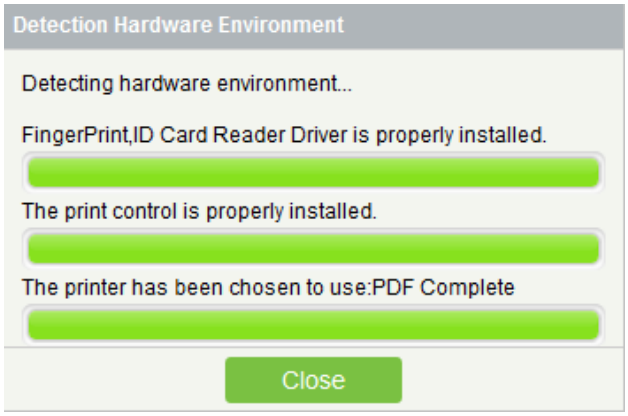


6.1 Registration

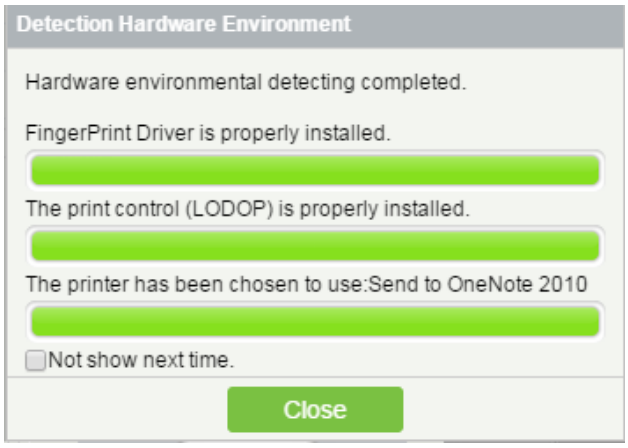
6.1.1 Entry Registration

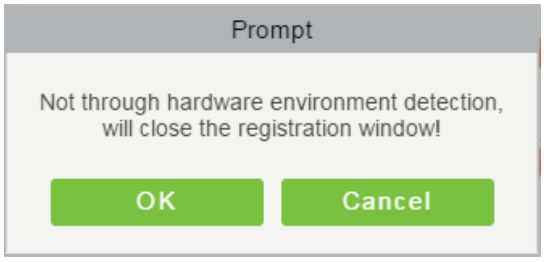
- Entry Registration

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, click [OK] to close the registration window, shown as the right figure below.



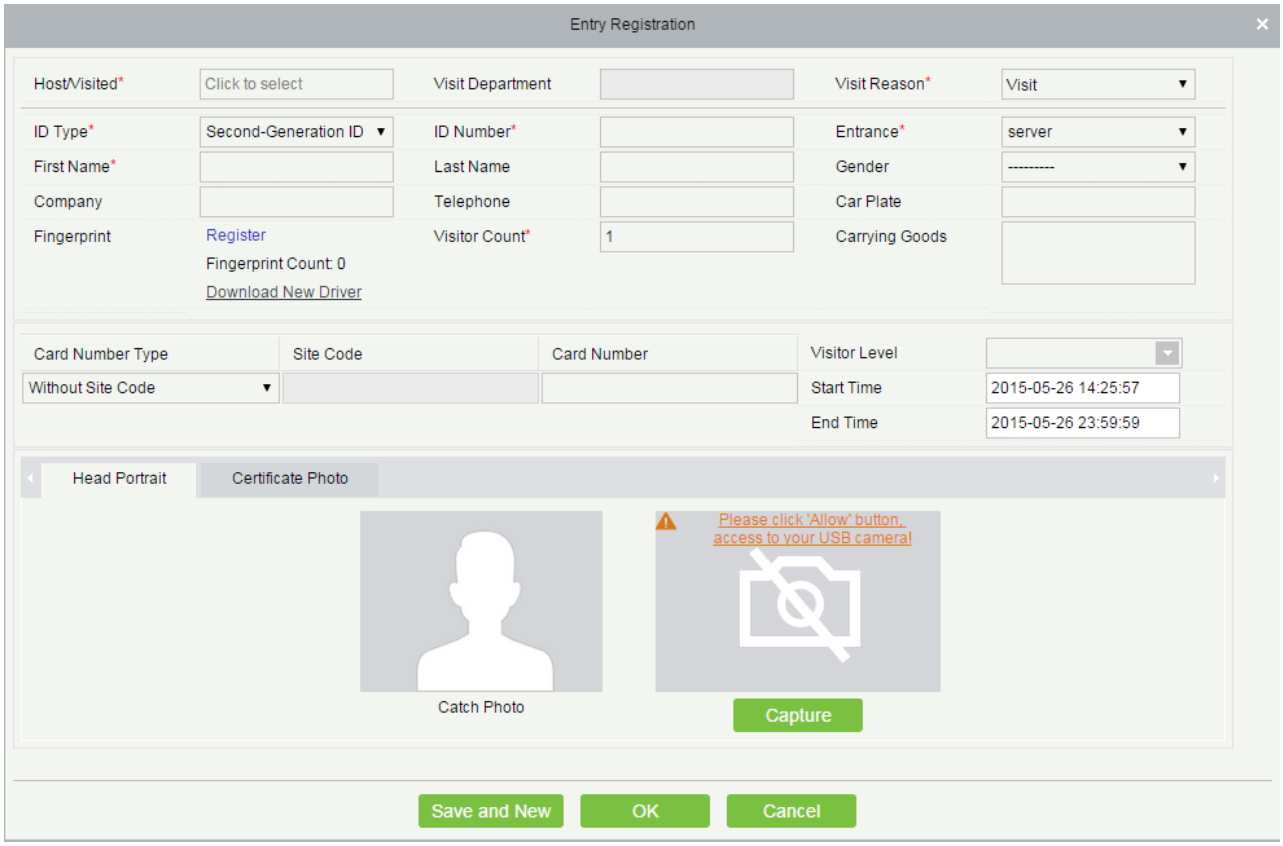


✍Note:

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 6.3.1 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.

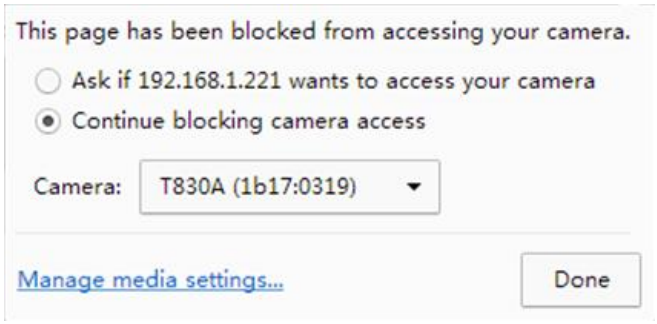
Visit Reason: Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the [Visit Reason] of [Basic Management].

ID Type: Passport, Driver's License, ID Card and Others are available to choose.

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.

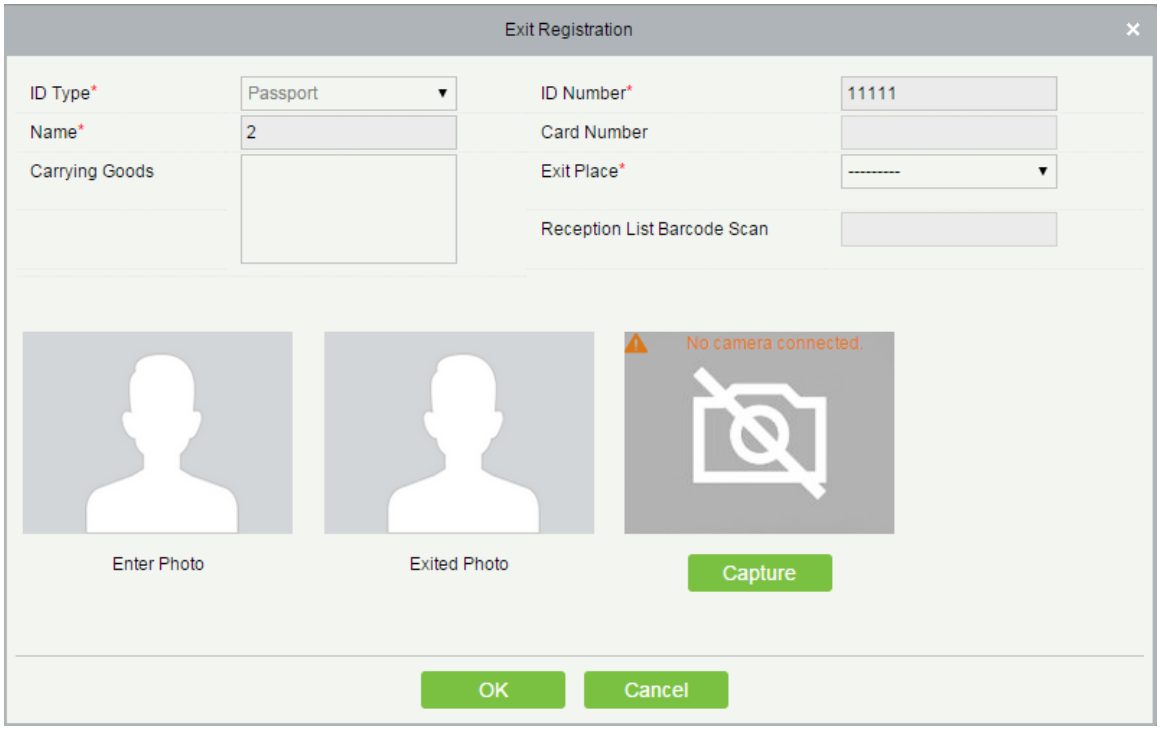
Head Potrait: If there is a camera (High-Speed Portable HD Doc Scanner) connected with the server, you can click [Capture] to take the visitor's photo. The browser may block the camera to access, please click in the IP address bar to select the camera and set it allowed to access this page.



- Exit Registration

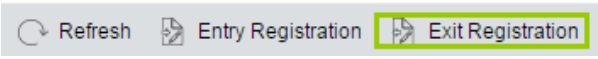
There are 2 ways:

1. Click [Exit Registration] below Operations as a visitor is ready to leave.

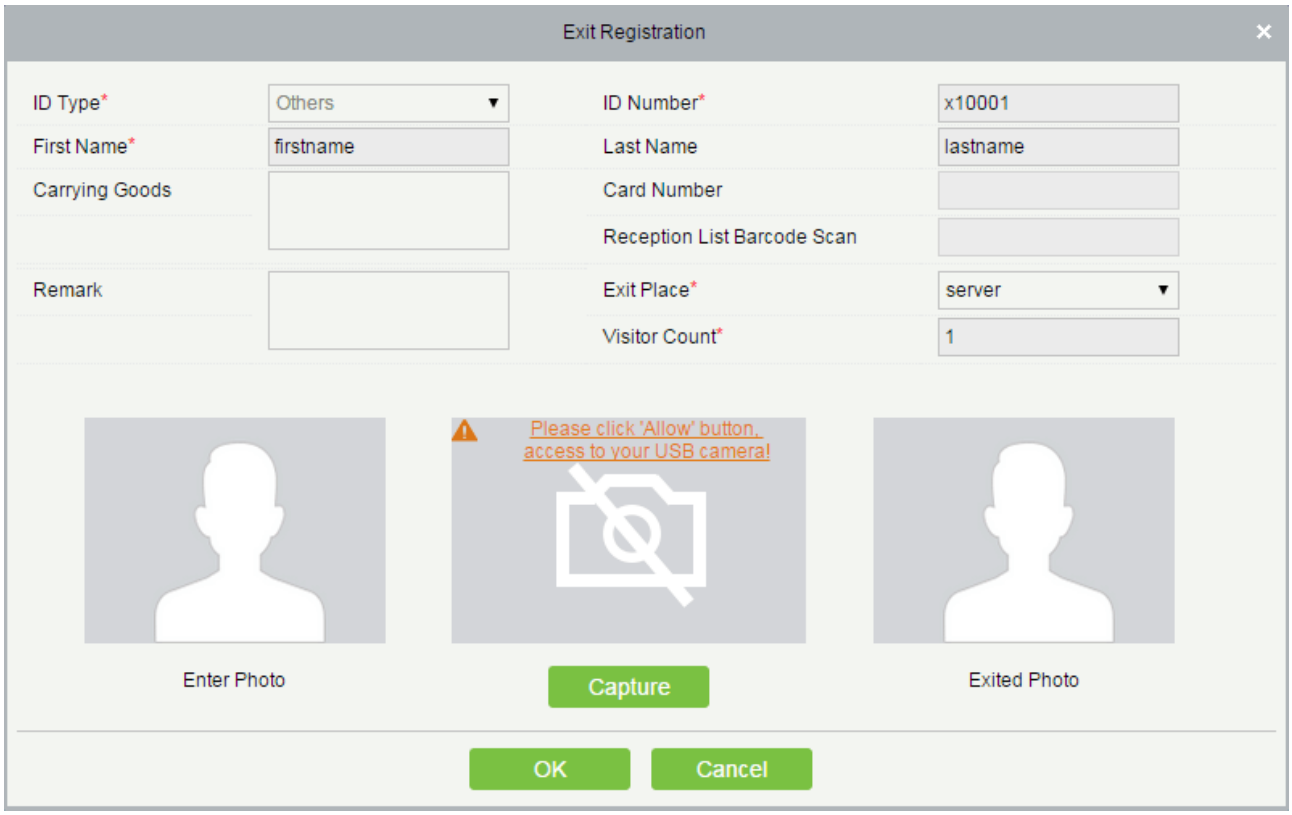


Select the Exit Place and click [OK].

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].

6.1.2 Visitor Information

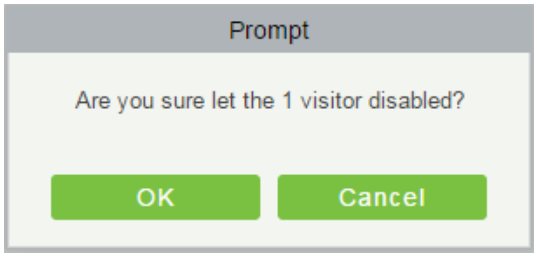
You can delete a visitor, disable or enable a visitor.

- Delete a Visitor

Click [Registration] > [Visitor], select a visitor, click [Delete].

- Disable a Visitor

Click [Registration] > [Visitor], select a visitor, click [Disable]:



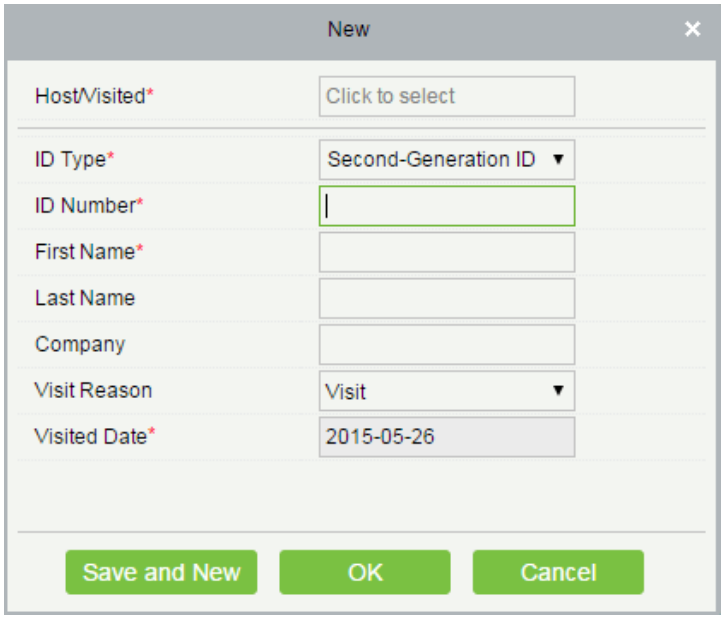
Click [OK] to block the visitor. The below Disable indicates the visitor is blocked.

- Enable a Visitor

Click [Registration] > [Visitor], select a blocked visitor, click [Enable].

6.2 Reservation

1. Click [Reservation] > [Reservation] > [New]:



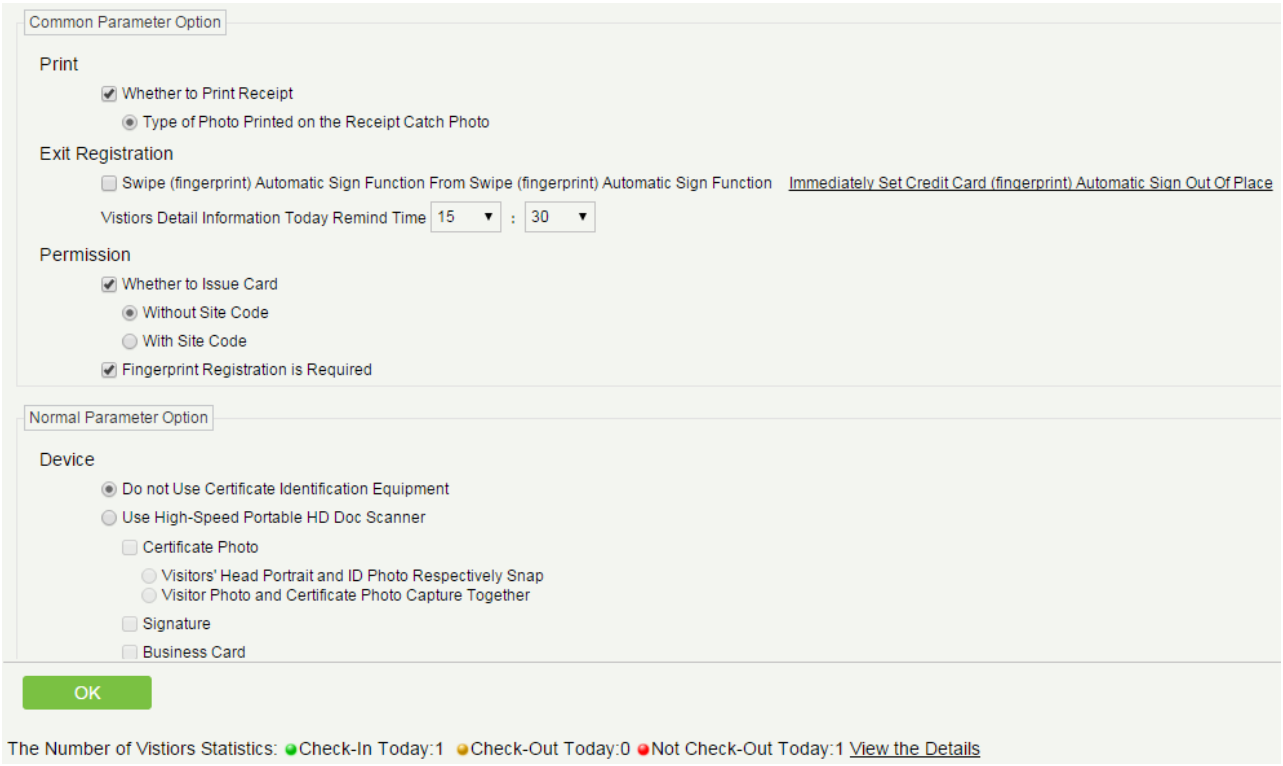
2. Complete the reservation information, click [OK].

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 2.2 Personal Self-Login.

6.3 Basic Management

6.3.1 Parameters

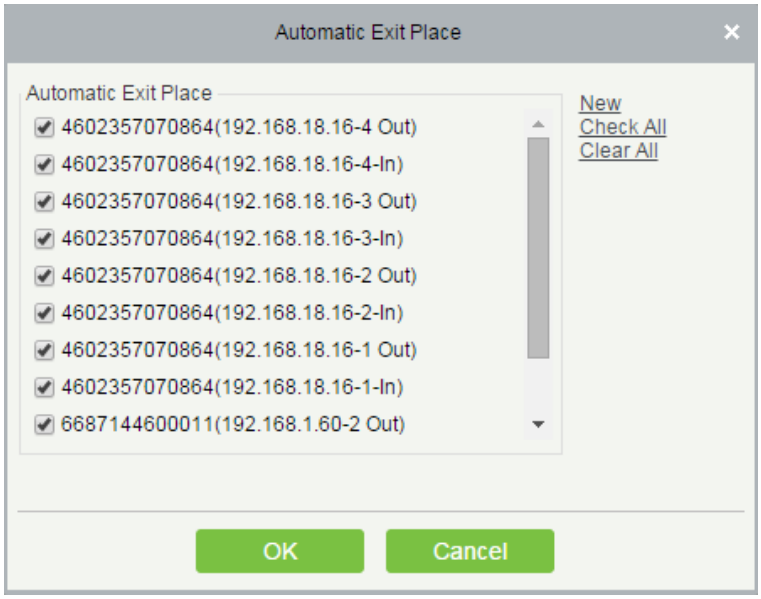
Click [Basic Management] > [Parameters]:



- Common Parameter Option

Print: Select whether to print receipt when the server connected with a printer, select whether to use the catch photo in the receipt.

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 [Immediately Set Credit Card (fingerprint) Automatic Sign-out of Place]:



Click [OK] to finish.

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.

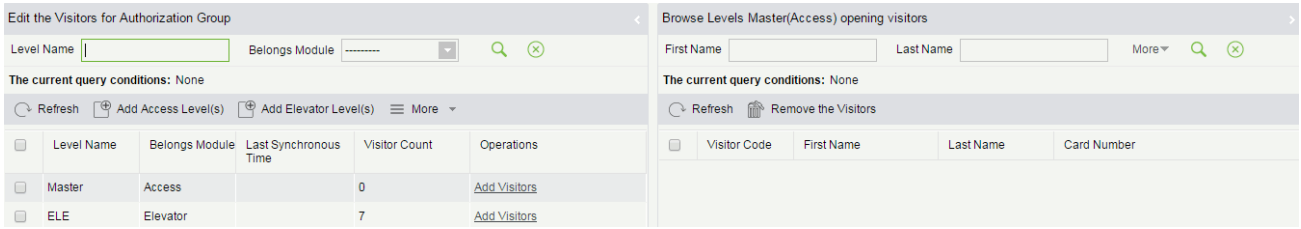
- Normal Parameter Option

Device: Whether to use Certificate Identification Equipment and High-Speed Portable HD Doc Scanner.

6.3.2 Visitor Levels

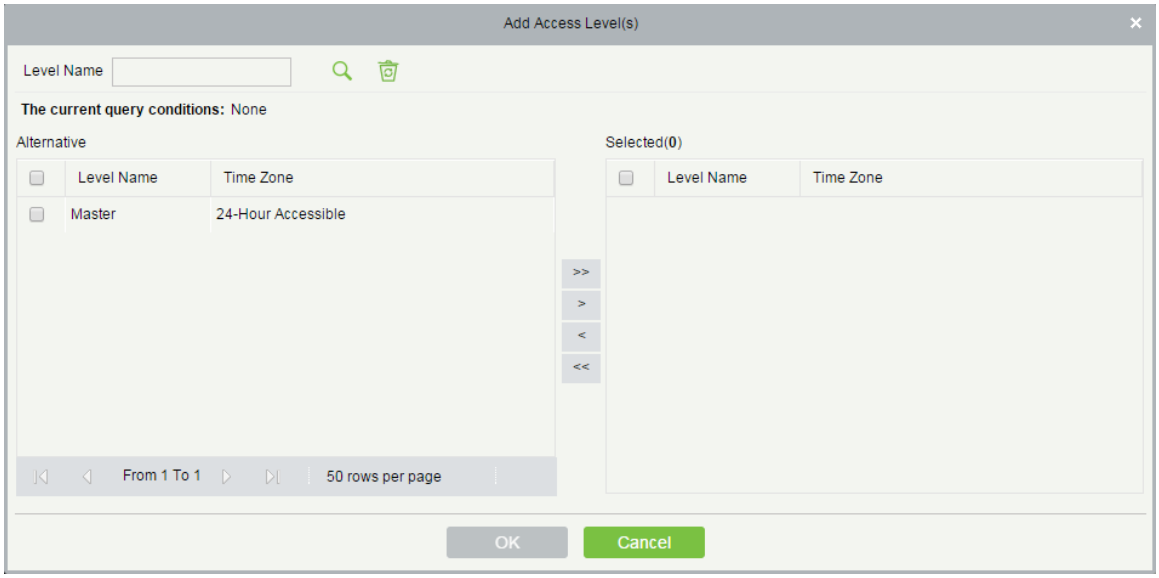
The visitor can be allocated Access or Elevator levels with in registration after the visitor level has been set.

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].

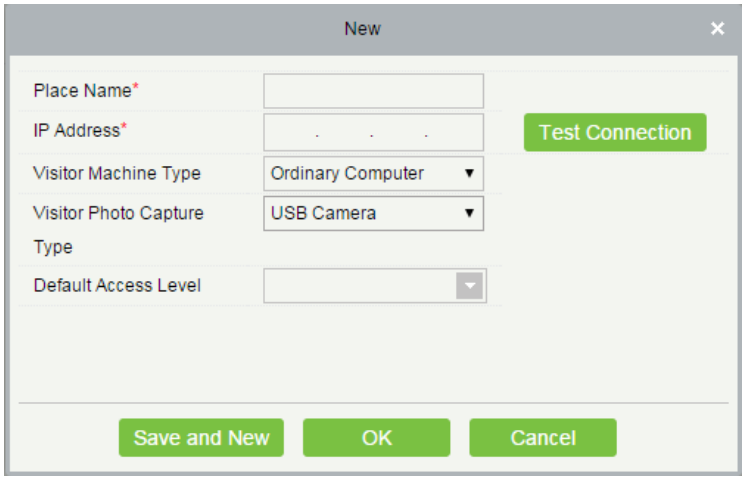
- Synchronous Level

When the Access or Elevator levels are modified, click [Synchronous Level] in the drop-down list of [More] to update the modification in time.

6.3.3 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.

Visitor Machine Type: Only Ordinary Computer is available.

Visitor Photo Capture Type: USB Camera and IP Camera are available. The IP Camera must be add in the "Video Device" before.

Default Access Level: Set the default levels in this entry place.

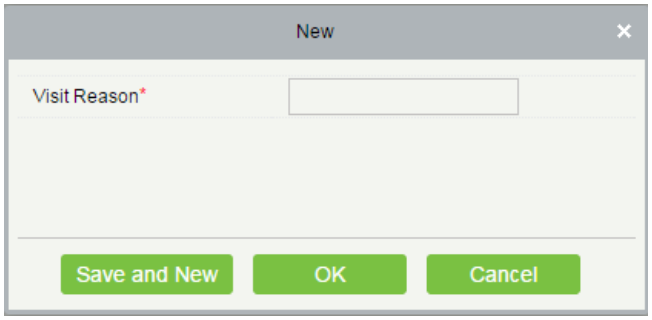
2. Click [Edit] or [Delete] as required.

- Automatic Exit Place

Please refer to 7.5 Parameters.

6.3.4 Visit Reason

1. Click [Basic Management] > [Visit Reason] > [New]:



2. Click [OK] to finish. You can also click [Edit] or [Delete] as required.

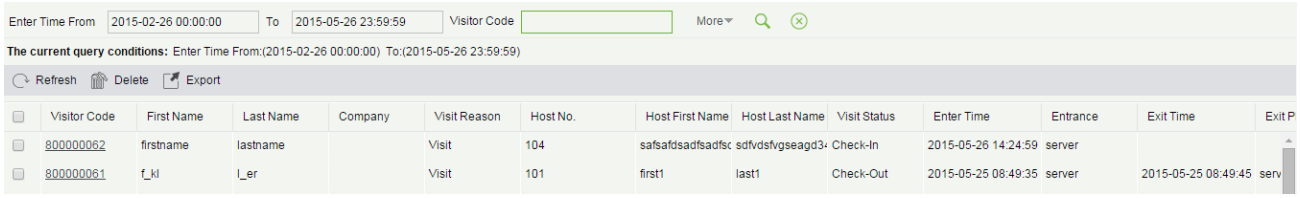
6.4 Visitor Reports

6.4.1 Last Visited Location

Click [Reports] > [Last Visited Location] to view the reports. The reports can be filtered by different conditions.

6.4.2 Visitor History Record

Click [Reports] > [Visitor History Record] to view the reports. The reports can be filtered by different conditions.



7. 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.

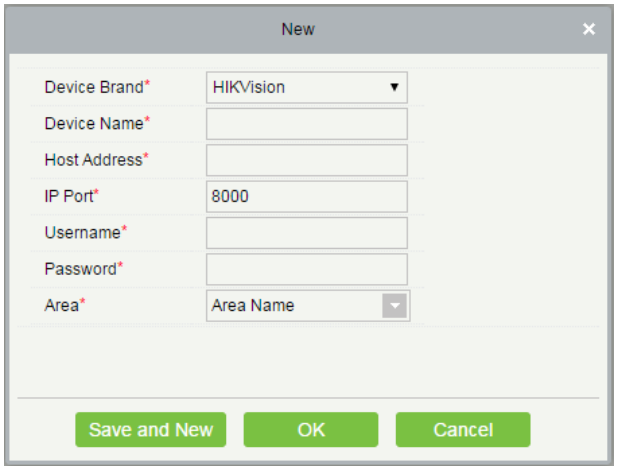
You need to add video device, set linkage function in 4.3.2 Linkage Setting and 5.3.4 Global Linkage in advanced.

Note: The current software only supports HIKVision and ZKIVision devices. For more details about the devices models, please contact technical support personnel to confirm.

7.1 Video Device

- Add a Video device

Click [Video] > [Video Device] > [Video Device] > [New]:



Fields are as follows:

Device Brand: Only HIKVision and ZKIVision are available.

Device Name: Any characters within a length of 30.

Host Address: Input the device's IP address.

IP Port: The default port is 8000.

User Name: Any characters within a length of 15(no blanks).

Password: Any characters within a length of 32(no blanks).

Area: Divide area for the device.

- Enable/Disable a Video Device

Select a video device in the list, and click [Enable] or [Disable].

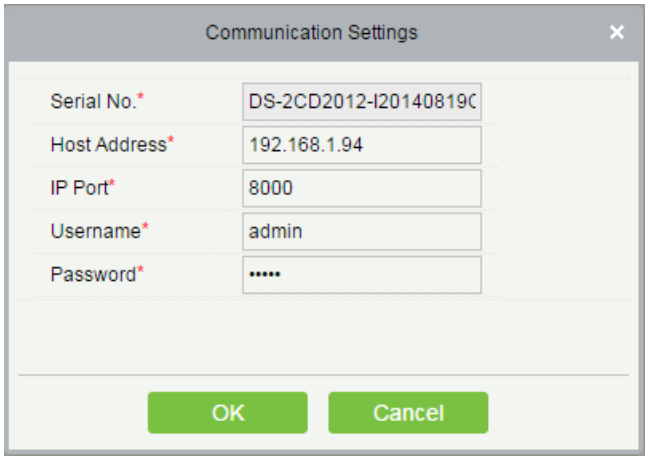
- Edit/Delete Video a Device

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]:

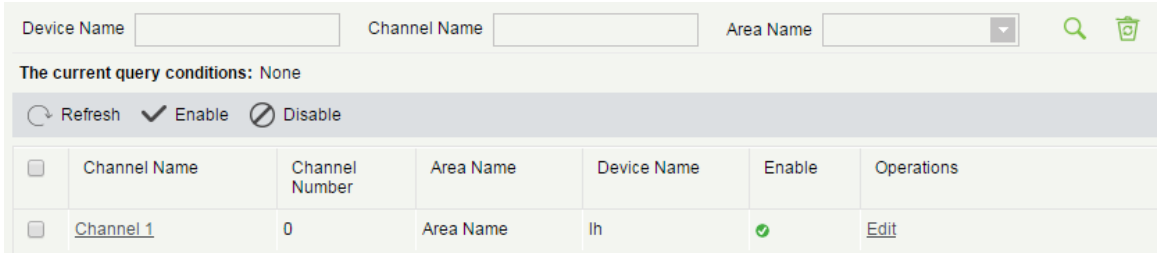


7.2 Video Channel

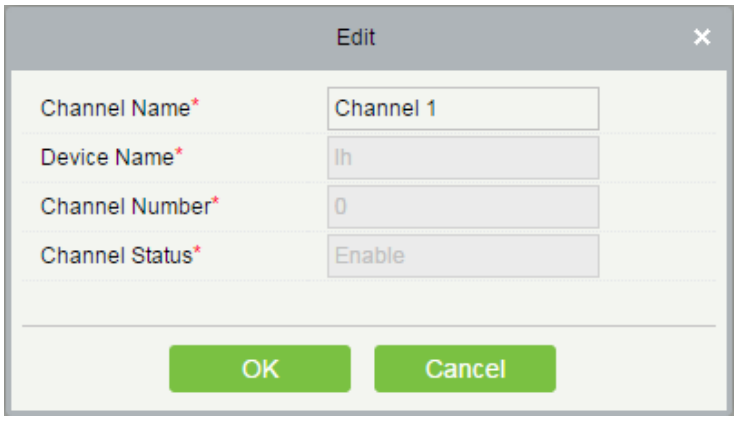
When adding a video device, the system will automatically detect the number of cameras on this device, that is, the number of channels, and generate a number of channels accordingly. For example, a video device has 16 cameras. After adding this device, the system will generate 16 channels, and name the 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 7.1 Video Device. The channel number is the channel number in video device.

7.3 Video Preview

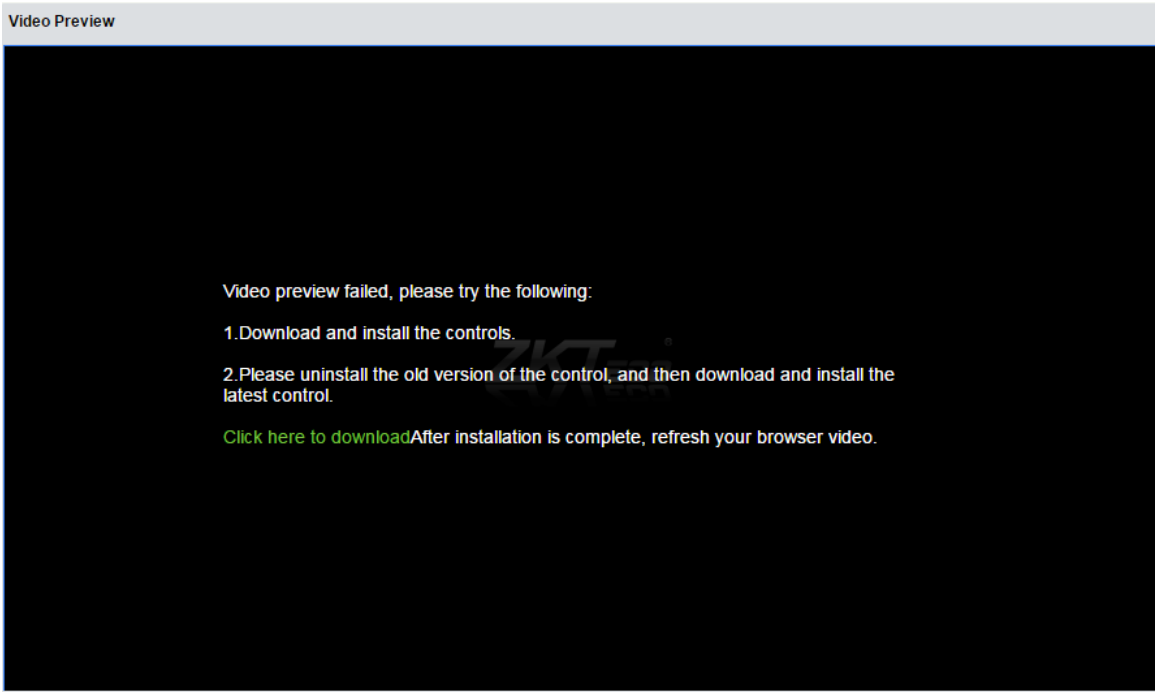
Click [Video] > [Video Device] > [Video Preview], the left side is the device and channel lists, click a channel to view the monitor screen.

Re-click the channel to shut down the screen.

✍Note:

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:

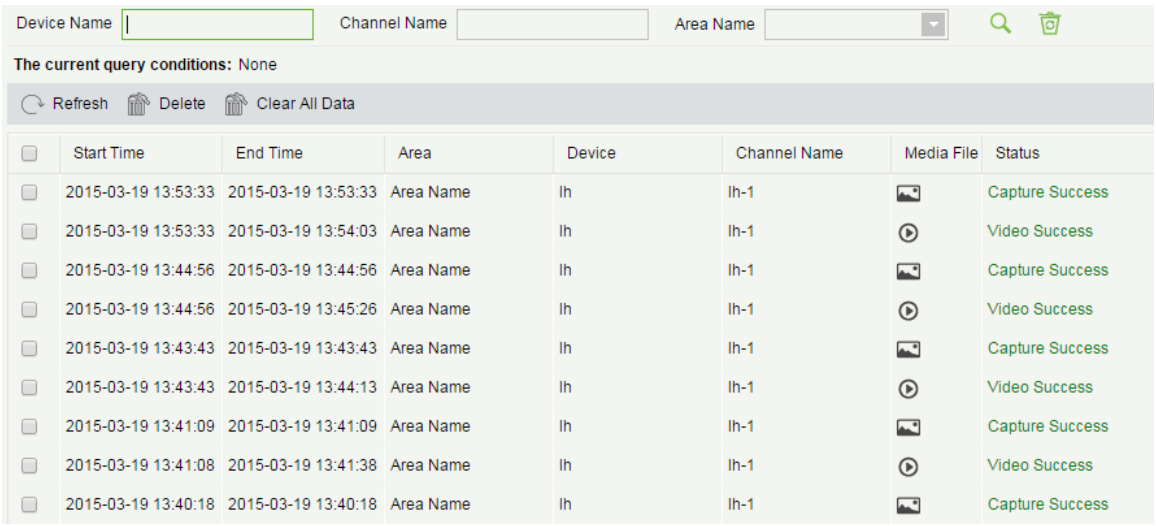


Click "Click here to download", the controls will be downloaded. Install the controls, and refresh the page, you can view the monitor screen normally. To prevent the video displayed abnormally, please install the controls that ZKBioSecurity offered.

7.4 Video Event Record

View the records of catching pictures and videos.

Click [Video] > [Video Device] > [Video Event Record]:



The media file is:

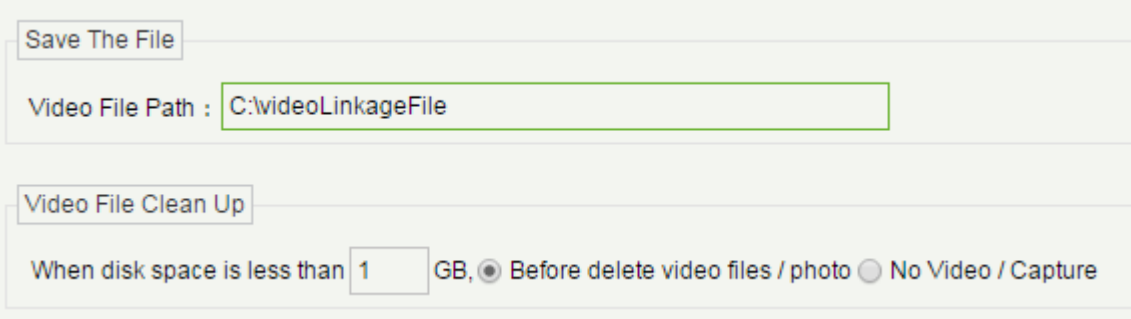
: Indicates that the linkage type is "Video", you can click to download this file. Please choose a third part of video player to play the file, or else it can not be played normally.

: 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 4.3.2 Linkage Setting.

7.5 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 preset 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.

7.6 Solutions of Exceptions

1. Client browser can not 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 can not 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.

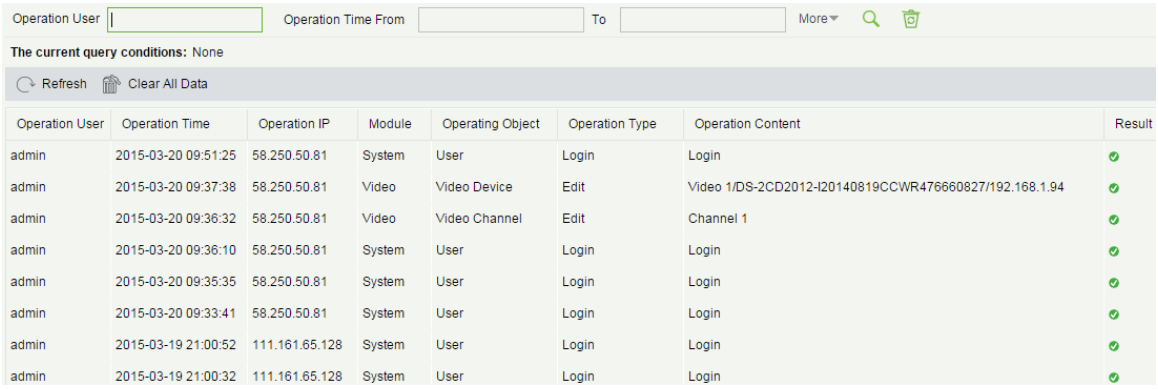
8. System Management

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.

8.1 Basic Management

8.1.1 Operation Logs

Click [System] > [Basic Management] > [Operation Log]:

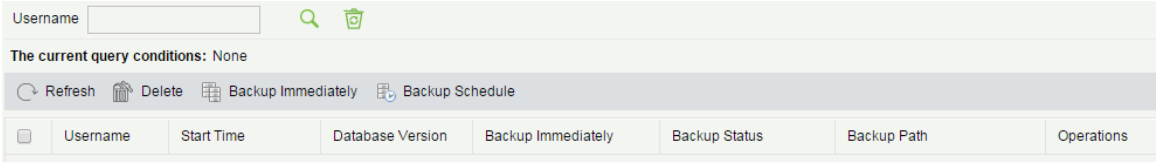


All operation logs are displayed in this page. You can query specific logs by conditions.

Clear All Data: Delete all logs in the system.

8.1.2 Database Management

Click [System] > [Basic Management] > [Database Management]:



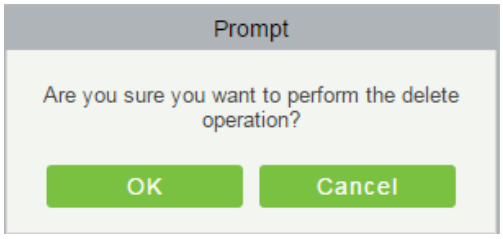
All history operation logs about database backup are displayed in this page. You can delete, backup and schedule backup database as required.

- Backup Immediately

Backup database to the path set in installation right now.

- Delete

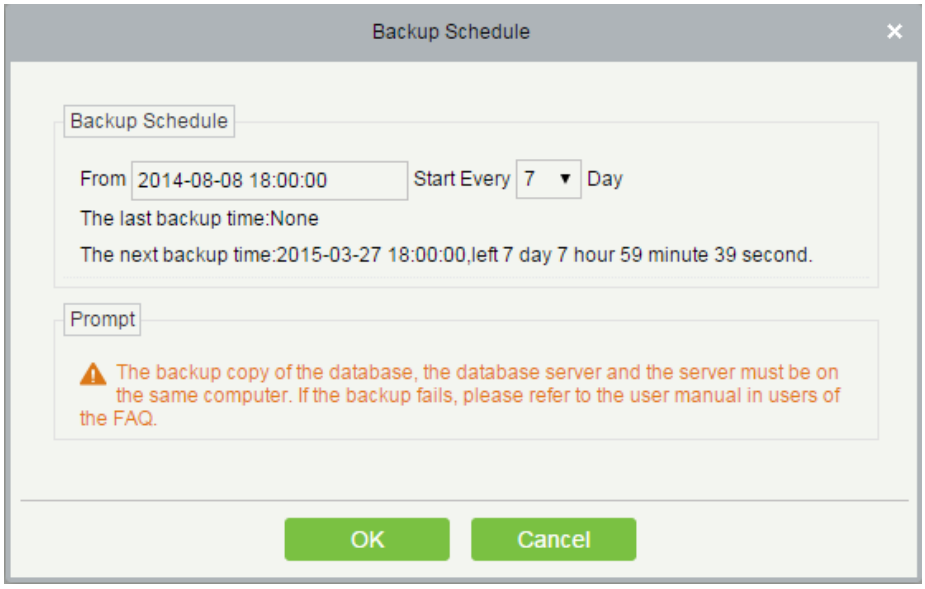
Select one or backup records to delete, click [Delete]:



Clcik [OK] to finish deleting.

- Backup Schedule

Click [Backup Schedule]:



Set the start time, set interval between two automatic backups, click [OK].

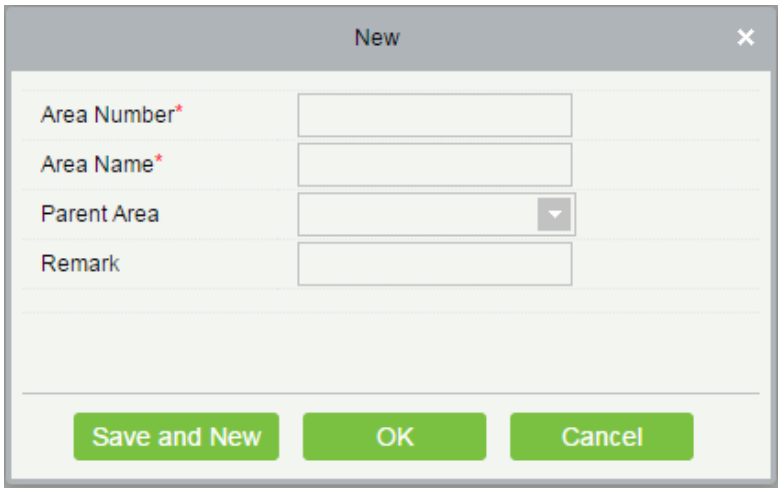
8.1.3 Area

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.

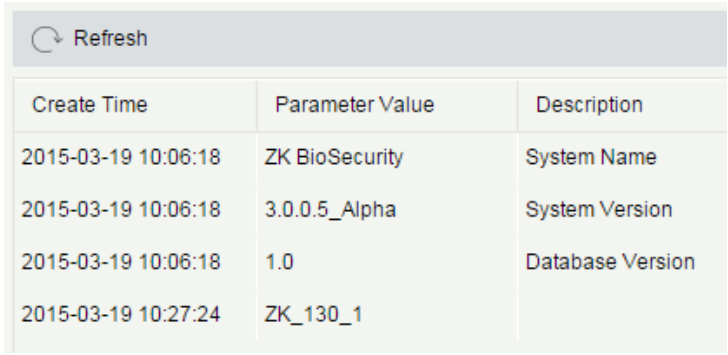
Click [OK] to finish adding.

- Edit/Delete an Area

Click [Edit] or [Delete] as required.

8.1.4 System Parameters

Click [System] > [System Parameter]:

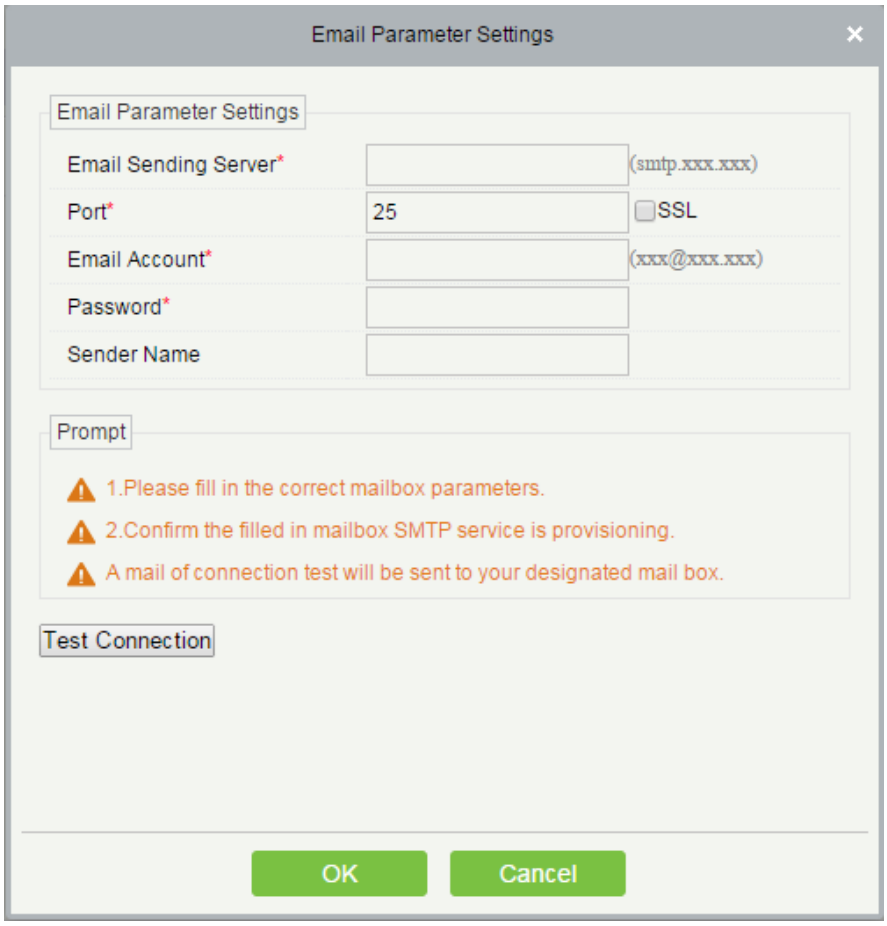


Click [Edit] to modify the system name.

8.1.5 E-mail Management

Set the email sending server information. The recipient e mail should be set in 4.3.2 Linkage Setting

Click [Basic Management] > [Email Management] > [Email Parameter Settings]:

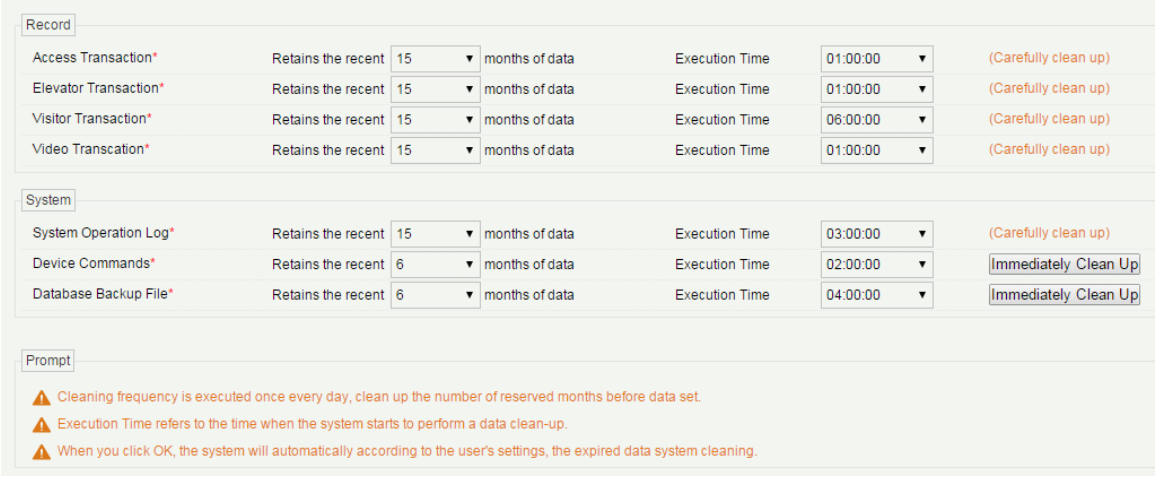


✍Note: The domain name of E-mail address and E-mail sending sever must be identical. For example, the Email address is: test@gmail.com, and the E-mail sending sever must be: smtp.gmail.com.

8.1.6 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]:

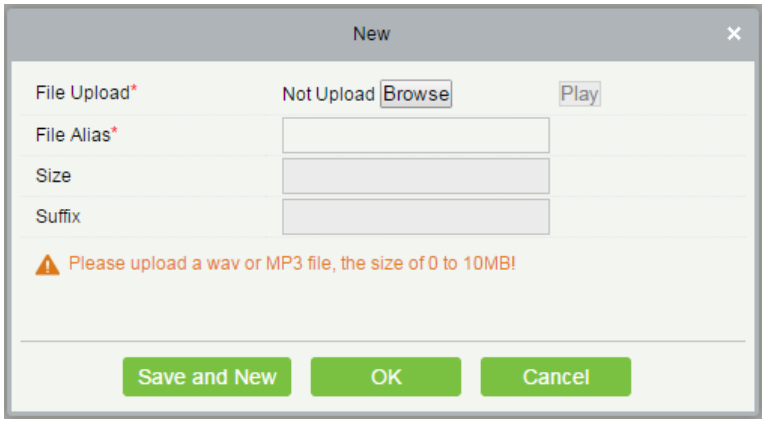


The system executes Immediately Clean Up operation after it is clicked and [OK] is clicked. Without clicking [OK], the system will not clean data.

✍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.

8.1.7 Audio File

Click [Basic Management] > [Audio File] > [New]:



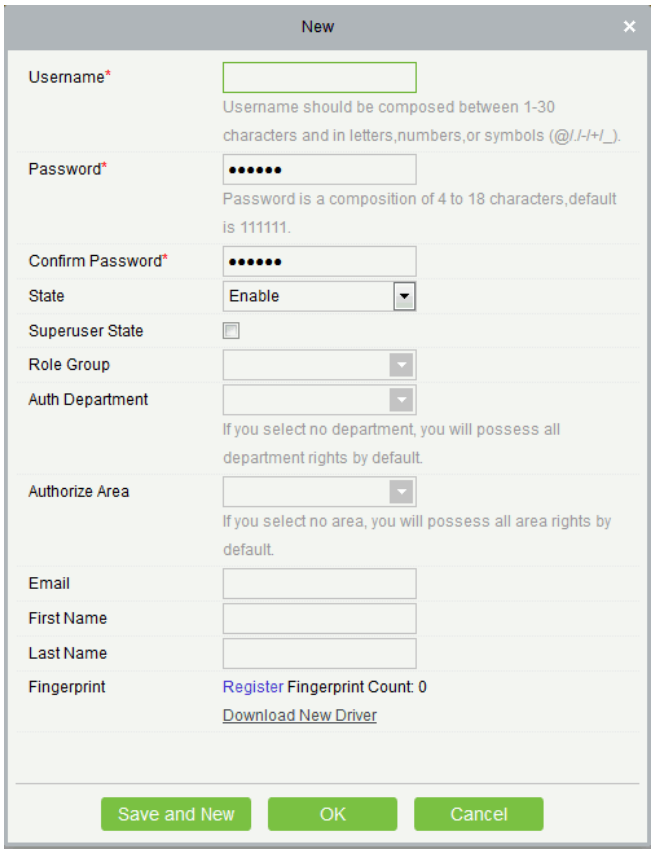
You can upload a sound from the local. The file must be in wav or mp3 format, and it must not exceed 10M.

8.2 Authority Management

8.2.1 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 8.2.3 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.

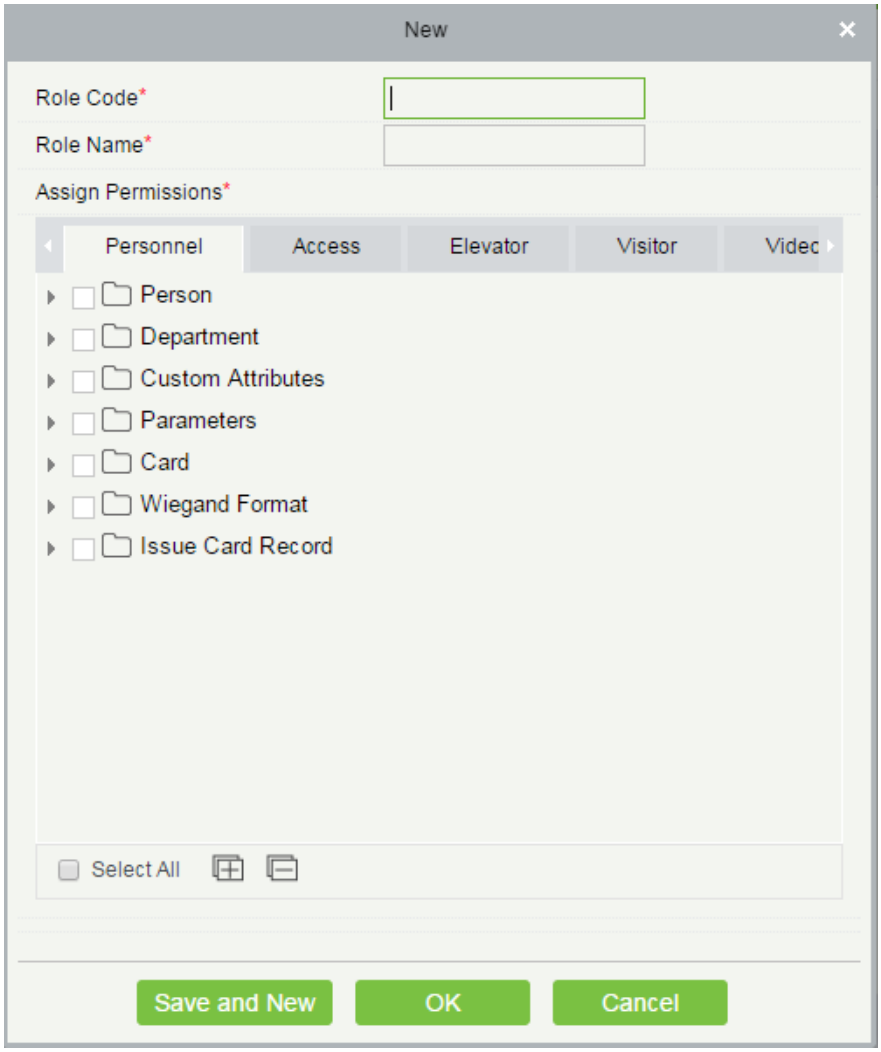
Click [Edit] or [Delete] as required.

8.2.2 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]:



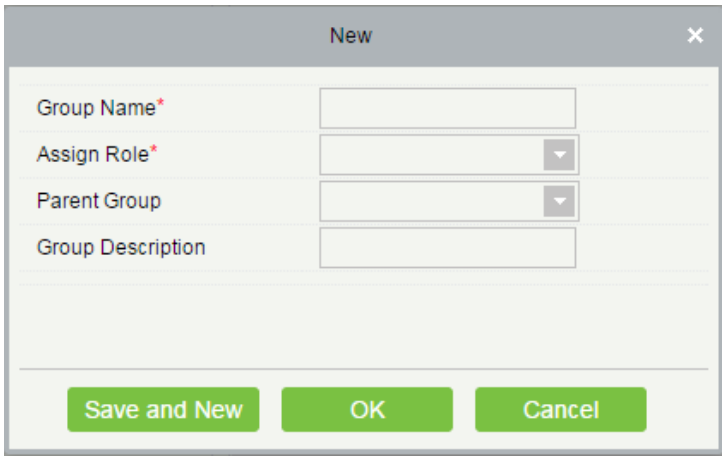
2. Set the code and name, assign permissions for the role.

3. Click [OK] to save.

8.2.3 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]:

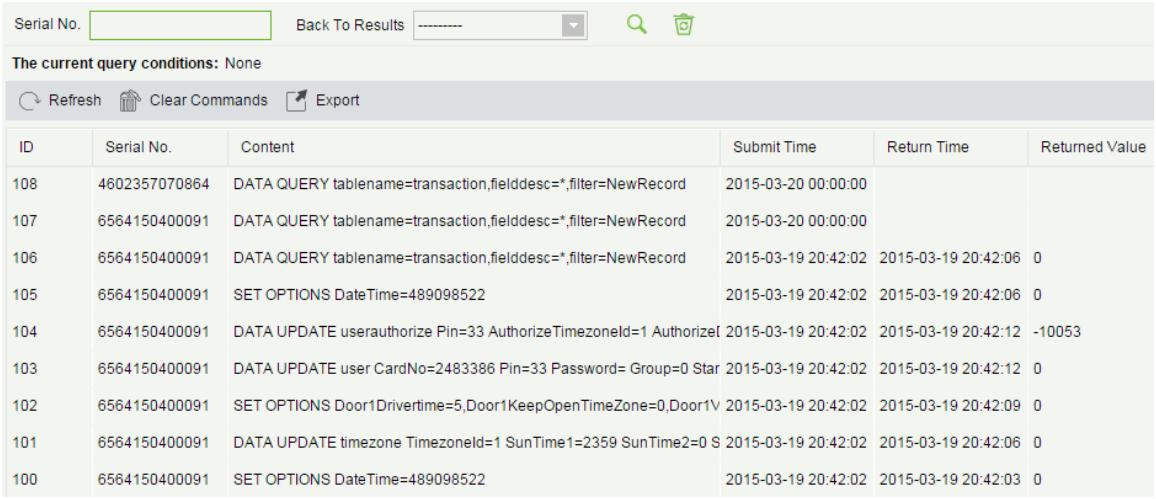


2. Set the name and parent group, assign role for the group.

3. Click [OK] to save.

8.3 Communication

Click [System Management] > [Communication] > [Device Commands], the commands lists will displayed.



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 AuthorizeI	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.

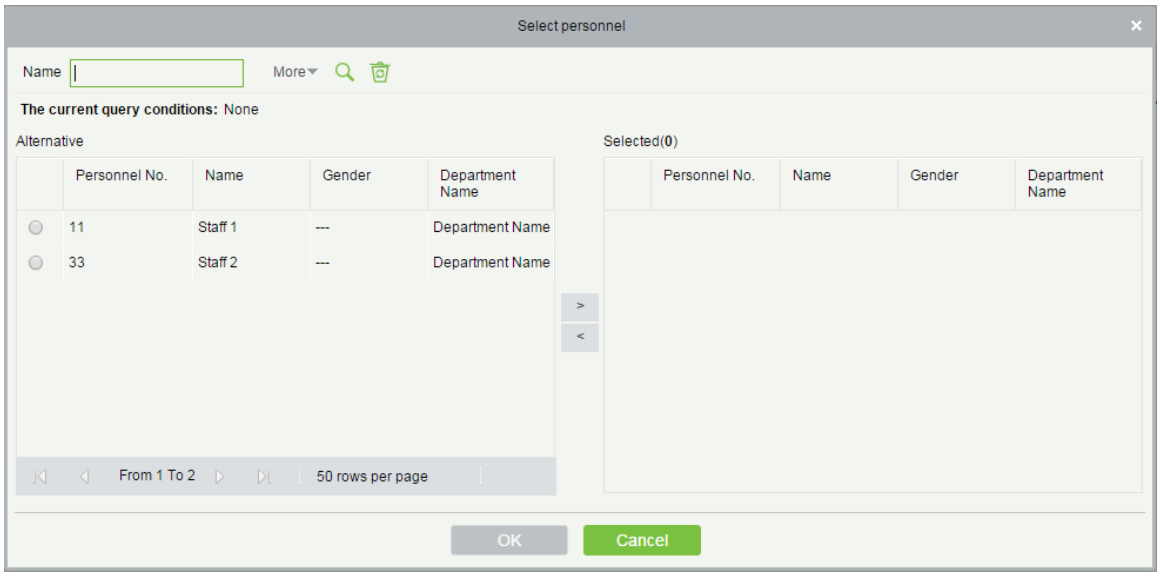
Export: Export the command lists to local host.

9. Appendices

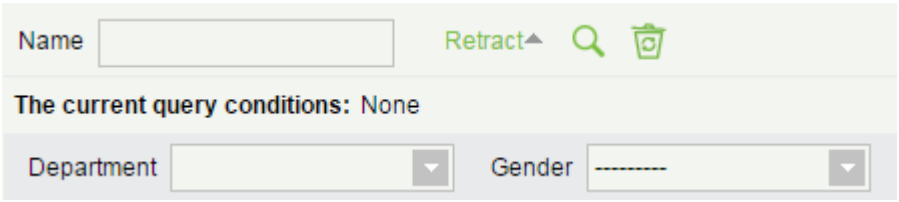
Appendix 1 Common Operations

- Select Personnel

The selected personnel page in the system is always as below:



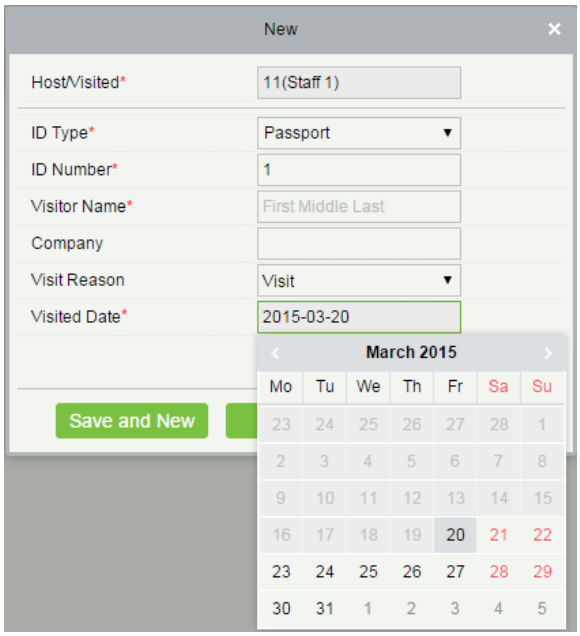
You can select the personnel in the Alternative list, or you can also click [More] to filter by gender or department.



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:

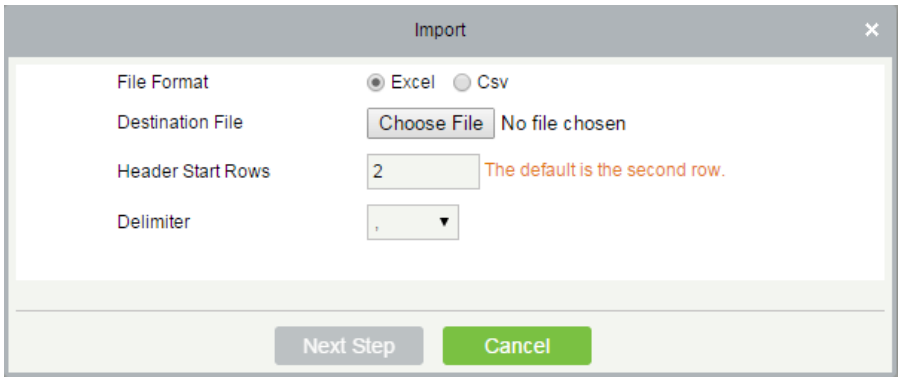


Click the Year to select by rolling click or . Clcik the Month and Date to select directly.

- 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:

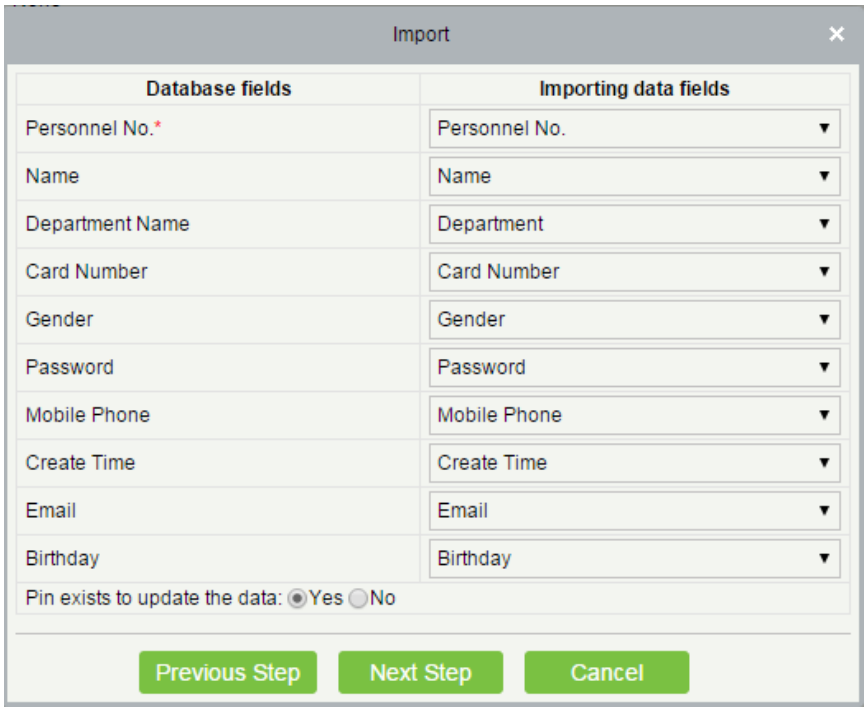
File Format: Select the file format to be imported.

Destination File: Choose file to be imported.

Head Start Rows: which row is the first row to be imported.

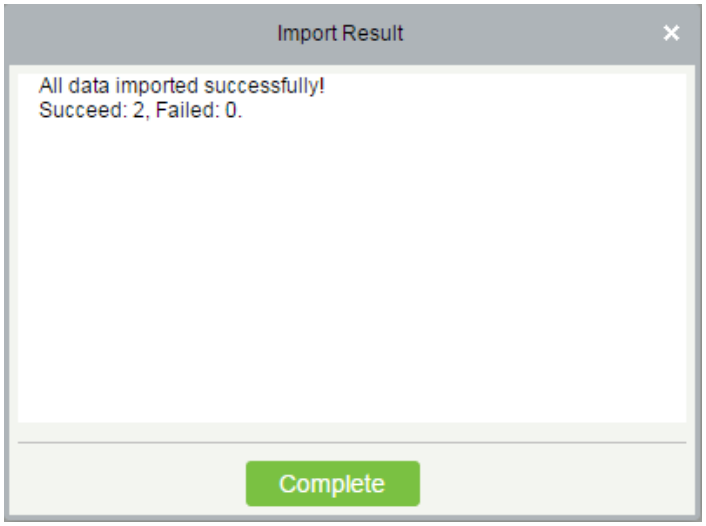
Delimiter: The delimiter of CSV format file, only "." and "-" are available.

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.

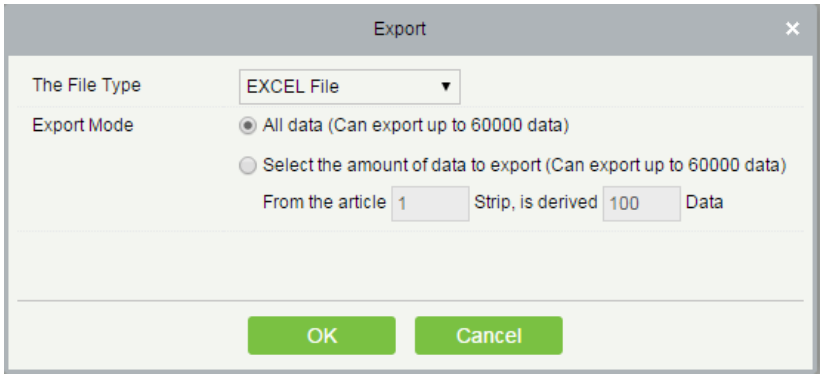
✍Note:

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.

Appendix 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 will not be displayed on the real-time monitor, but you can check it in the event report).

- 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: When Global Zone APB verification is failed, this abnormal event will be triggered.

Background Verification Success: When Global Zone APB verification is successful, this abnormal event will be triggered.

Background Verification Timeout: When the value of Global Zone APB does not return in set time, 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.

Invalid Card Punching: This alarm event will be triggered when invalid card punching for five times continuously.

✍Note: User can self-define the level of each event (normal, abnormal or alarm).

Appendix 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).

Appendix 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.

Appendix 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.