ZKAccess3.5 Software User Manual

Version: ZKAccess3.5 and above version

Supports PULLSDK version 2.2.0.169 and above version

Date: April, 2012

About This Manual

This document introduces the main functions, the user interface and operations of the system.

Table of Contents

Definitions

Super User: The user who has all operation levels of the system, who can assign new users (such as company management personnel, registrar, and access control administrator) in the system and configure the roles of corresponding users.

Role: During daily use, the super user needs to assign new users having different levels. To avoid setting individual levels for each user, roles having certain levels can be set in Role Management, and then be assigned to specified users.

Access Control Time Zone: It can be used for door timing. The reader can be made usable during valid time periods for certain doors and unusable during other time periods. Time zone can also be used to set Normal Open time periods for doors, or set access control levels so that specified users can only access specified doors during specified time periods (including access levels and First-Card Normal Open settings).

Door Status Delay: The duration for delayed detection of door sensor after the door is opened. Detection is performed only after the door is opened and the delay duration expired. When the door is not in the “Normally Open” period, and the door is opened, the device will start timing. It will trigger alarm when the delay duration expired, and stop alarm when you close the door. The door status delay should be longer than the lock drive duration.

Close and Reverse-lock: Set whether or not to lock after door closing.

Lock Drive Duration: Used to control the delay for unlocking after press fingerprint or card punching.

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

Multi-Card Opening: This function needs to be enabled in some special access occasions, where the door will open only after the consecutive verification of multiple people. Any person verifying outside of the defined combination (even if the person belongs to other combinations) will interrupt the procedure, requiring a 10 seconds wait to restart verification. It will not open by verification of only one of the combination.

Interlock: Can be set for any two or more locks belonging to one access control panel, so that when one door is opened, the others will be closed, allowing only one door to be open at a time.

Anti-pass Back: The card holder who entered from a door by card punching must

exit from the same door by card punching, with the entry and exit records strictly consistent.

Linkage Setting: 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, alarming and exception of the system and list them in the corresponding monitored report for view by the user.

1. System Instruction

1.1 Functions Instruction

Security Management has increasing concerns for modern enterprises. This management system helps customers to integrate operation of safety procedures on one platform, making access control management easier and more practical so as to improve efficiency.

❁ System Features

1. Powerful data processing capacity, allowing the management of the access control data for 30,000 people.

2. Visible and reasonable work flows come from abundant experience in access control management.

3. Automatic user name list management.

4. Multilevel management role-based level management secures user data confidentiality.

❁ Configuration Requirements:

CPU: Master frequency of 2.0G or above;

Memory: 1G or above;

Hardware: Available space of 10G or above. We recommend using NTFS hard disk partition as the software installation directory (NTFS hard disk partition has the better performance and higher security).

❁ Operating System:

Supported Operating Systems:

Windows XP/Windows 2003/Windows Vista/Windows7

Supported Databases:

MS SQL Server2005 or above/Microsoft Access

❁ System Modules:

The system includes five major functional modules:

Personnel System: Primarily 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.

Device System: Set communication parameters for device connection, including system settings and machine settings. After successful communication, the information of connected devices can be viewed and operations such as remote monitoring, uploading and downloading can be performed in the system.

Access Control System: C/S Frame-based management system, enabling 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, so that some users are permitted to unlock some doors through verification during certain intervals.

Video System (for professional version): The system provides the video linkage function, to manage the network video recorder, view the real-time video, and query the video records. It opens the Real-time Video when the linkage events happen.

System Settings: Primarily used to assign system users and configure the roles of corresponding modules; database management such as backup, initialization and recovery; and set system parameters and manage system operation logs.

1.2 Basic Operation Flow

The following are the basic steps to use the system, the user just needs to follow the steps below and skip the items which are not displayed on their interface.

Step 1: Add Device;

Step 2: Add Personnel;

Step 3: Add Access Control, includes Time Zones, Holidays, Door Setting, Access Levels;

Step 4: View Real-time Monitoring and Reports.

2. System Management

1. Log in to the System

(1) Double click the **[ZKAccess3.5 Security System]** shortcut on the desktop, the following the homepage pops up.

(2) For system security, it is required to verify identity before accessing the system. We will provide a super user (having all operation levels) for the beginner of this system. Enter user name and password, and click [OK], 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, for system security, please use the [Modify password] function to modify the password.

The super user can assign company personnel as system users to (such as company management personnel, registrar, and access control administrator) and configure the roles of corresponding modules. For details, see 8.1 User Management.

2. Quit the system:

Click the [Close] button on the upper right corner of the interface, directly to quit the system.

3. Modify Password:

The super user and the new user created by the super user (the default password for the new user is “admin”) can use the [Modify password] function to modify the login password for system security. Click [Modify password], it pops up the Edit Page. Enter the old password and the new password, confirm the new password and click [Confirm] to complete the modification.

Note: The user name is case-insensitive, but the password is case-sensitive.

3. Navigation

After the user logs in to the system, it will show the [Navigation] main interface, displaying common operations and other important information.

Click any icon on the [Navigation], it will shown corresponding interface as below:

4. Personnel System Management

Before using the system's access control management functions, first access the personnel system for configure: First, Department Management settings, used to set the company's organizational chart; Second, Personnel Management settings, used to input personnel, assign departments, and maintain and manage personnel. At last, setting the Access Control Levels.

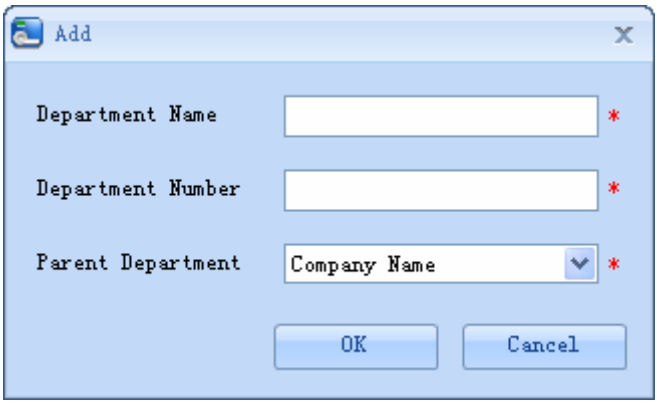
4.1 Department Management

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

Main functions of Department Management include Add Department and Department Maintenance.

1. Add Department:

Click [Personnel] - [Department] - [Add] to show the add Department edit interface.



The fields are as follows:

Department name: Any character, up to a combination of 50 characters;

Department number: If required, it shall not be identical to another department. The length shall not exceed 50 digits. Click [Verify] to see if repeated or not;

Parent department: Select from the pull-down menu and click [OK];

After editing, click [OK] to complete adding, or click [Cancel] to cancel it.

To add a department, you can also use [Import] to import department information from other software or another document into this system. For details, see Appendix 1 Common Operation. [Upper Department] is an important parameter to determine the Company's organizational chart. On the right of the interface, the Company's organizational chart will be shown in the form of a department tree.

2. Department Maintenance:

Department Maintenance includes department Edit and Delete:

Upon a change to the department or organizational structure, the user can use the [Edit] function to modify such items as Department Name, Department Number or Upper Department. Click Department Name directly or click the [Edit] button behind the department to access the edit interface for modification.

To delete a department, click the check box before the department, and click [Cancel Department], or directly click the [Delete] button behind the department.

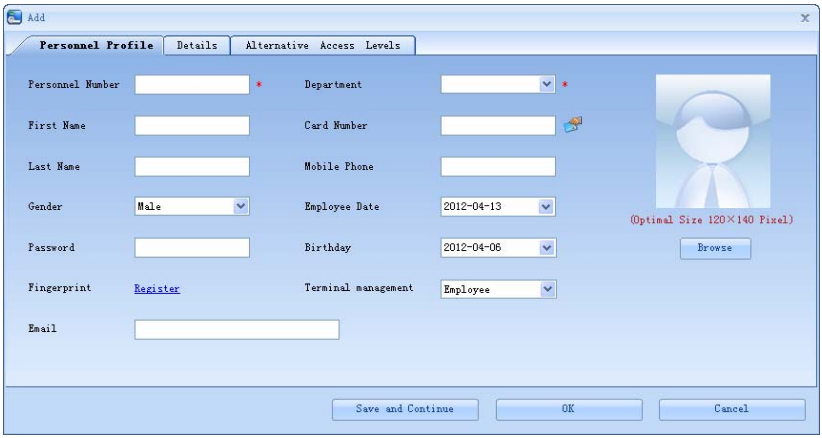
Note: A department can not be deleted freely. If so, the personnel under the department will be pending, and some historical data will not be able to be queried. If deletion is required, please first transfer the departmental personnel to another department.

4.2 Personnel Management

When starting to use 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.

4.2.1 Add Personnel

Click [Personnel] - [Personnel] - [Add] to show personnel profile edit interface:



The fields are as follows:

Personnel No.: By default, the length can not exceed 9 digits. A number with a length of less than 9 digits will be preceded with 0 automatically to complete 9 digits. Numbers can not be duplicated. Click [Verify] to see if it is duplicated or not;

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;

Social Security Number: Duplication is not allowed. Click [Verify] to check Duplication. 15-digit and 18-digit ID card numbers are supported;

Card Number: Assign a card number to the person for access control use. This can be done manually or by using card issuer. For details, see Personnel Card issue in 4.2.2 Personnel Information Maintenance;

Password: Set personnel password. An access control panel only supports 8-digit passwords. If a password exceeds the specified length, the system will truncate it automatically. If you need to modify the password, please clear the old password in the box and input the new one;

Personal Photo: The best size is 120×140 pixels, for saving space. For details, see Upload Personal Photo in 4.2.2 Personnel Information Maintenance;

Employment Date: By default it is the current date.

Register Fingerprint: Enroll the Personnel Fingerprint or Duress Fingerprint. If the person presses the Duress Fingerprint, it will trigger the alarm and send the signal to the system.

Access Control Settings: Select access levels, start and end dates of access validity time and multi-card opening personnel groups (Presetting is required. For details, see6.9 Multi-Card Opening);

Validity time is set for temporary access control, where the door can be opened only during this time period. If not ticked, the setting will be always valid.

After editing personnel information, click [OK] to save and quit. The added personnel will be shown in the personnel list.

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.

4.2.2 Personnel Information Maintenance

The operations include Personnel Card Issue, Batch Issue Card, and etc.

For such functions, you can directly click the personnel number in the personnel list to enter the edit interface for modification, or right-click the [Edit] button to enter the edit interface for modification. After modification, click [OK] to save and quit.

Personnel Card Issue:

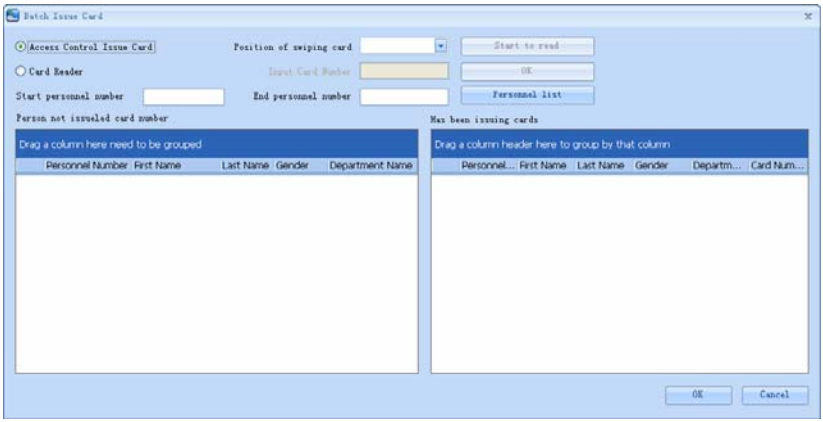
Assign card numbers to personnel, including batch card issue and individual card issue.

(1) How to use the card issuer:

The card issuer is connected to the PC through a USB port. When the cursor is on the Card Number Input box, punch the card on the card issuer, then the card number will display in the input box.

(2) Batch Card Issue:

Click [Personnel] - [Issue Card] - [Batch Issue Card] to show the Batch Issue Card edit interface;



Personnel list, show this all personnel without cards within this number series.

Select the way of “Access Control Issue Card” or “Card Reader”.

In using of the card reader, when you swipe the card near to the card reader, the System will get the card number and issue it to the user in the left list.

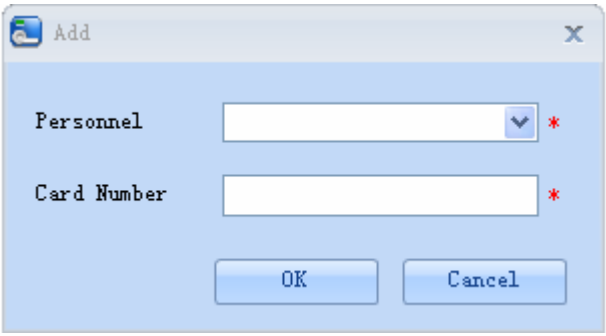
Using of the access control panel, you need to select the position of swiping card, such as a card reader connected with an access control panel. Input the Start Personnel number and End personnel number ,click Personnel list, got the personnel list, and then click [Start to read], the system will read the card number automatically, and issue it to the user in the left list one by one. After that, click [Stop to read].

Click [OK] to complete card issue and return. Personnel and corresponding card numbers will be shown in the list.

(3) Individual Card Issue:

Click [Personnel] - [Card Issue] - [Add] to show Individual Card Issue interface;

Select personnel, enter card number (or use card issuer for card issue), select card issue date, and click [OK].



✍ **Note:** The system supports card issue through card issuer and by manually inputting card numbers.

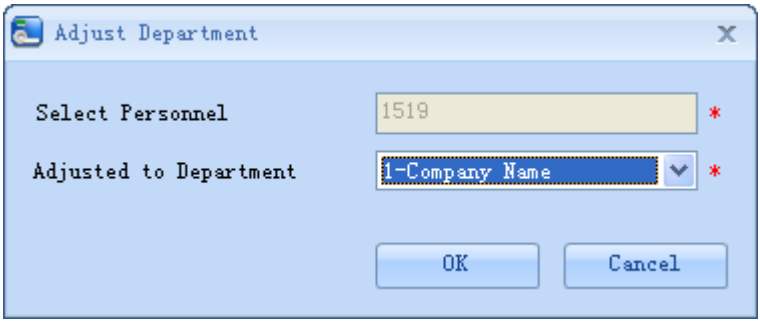
4.2.3 Personnel Adjustment

Personnel Adjustment is daily maintenance of existing personnel, primarily including: Personnel Adjust Department and Delete Personnel.

1. Personnel Adjust Department:

Operation steps are as follows:

(1) Click [Personnel] - [Personnel], and select the person subject to department adjustment from the personnel list, click the [Adjust Department] button, and the following interface appears:



(2) Select the department to be transferred to.

(3) After editing, click [OK] to save and quit.

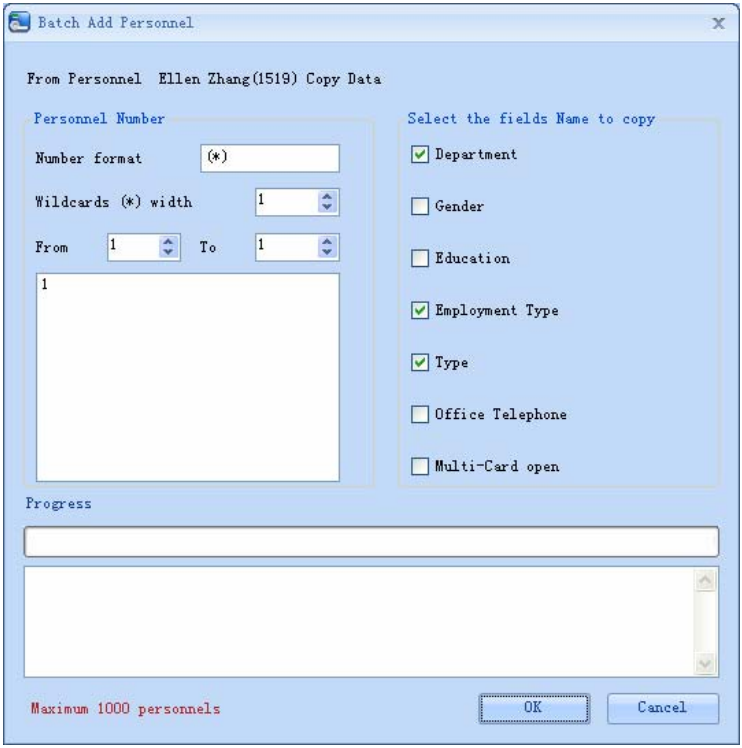
2. Delete Personnel:

Click [Personnel] - [Personnel], select personnel, click [Delete], and click [OK] to delete, or directly click [Delete] under “Related operation” of the personnel to delete.

Note: Deleting personnel also results in deleting the personnel in the database.

4.2.4 Batch Add Employees

When some departments enroll a lot of employee, you can use this function to add employees, relieve an operator work.



Batch Add Employees need select replicating object. If without personal information can not use this function.

Number length of Add Employees is less than 8 digits. A batch maximum can only add 1000 personals.

Wildcard "(*)" width: That is mean, how many figure the **Number pattern has.** After the **Wildcard "(*)" width** has been defined, by use the "**From**" box, "**To**" box to create range. Click on the "**OK**" button, add employees, and click on the "**Cancel**" button, return the interface.

Choose to copy of the fields: Select batch add personnel with the copy personnel information to the same.

5. Device Management

The access control panel to be connected to this system provides access control system functions. To use these functions, the user must first install devices and connect them to the network. Second, set corresponding parameters in the system so as to manage these devices via the system, upload user access control data, download configuration information, output reports and achieve digital management of the enterprise.

Device Management primarily includes Area Setting and Device Management.

5.1 Area Settings

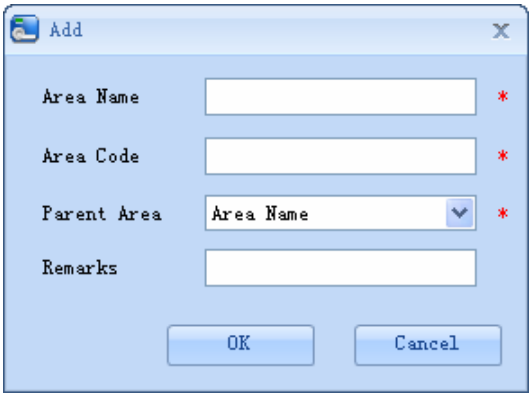
Area is a spatial concept, enabling the user to manage devices in a specific area.

In the access system, after area setting, devices (doors) can be filtered by area upon real-time monitoring.

The system, by default, has set an area named [Headquarters] and numbered [1]. Area Setting include Add Area and Delete area.

1. Add area:

Click [Device] - [Area Settings] - [Add] to activate the Add Area edit interface:



The fields are as follows:

Area Name: Any character, up to a combination of 50 characters;

Area Code: Repetition not allowed;

Parent Area: Decides the regional organization structure of the company.

After setting, click [OK].

2. Delete area:

Select area, click [Delete], or directly right click [Delete], press [OK].

5.2 Device Management

Set the communication parameters of connected devices. Only when communication parameters, including system settings and device settings, are correct, normal communication with devices will be possible. When communication is successful, you can view the information of connected devices, and perform remote monitoring, uploading and downloading data.

5.2.1 New Add Device

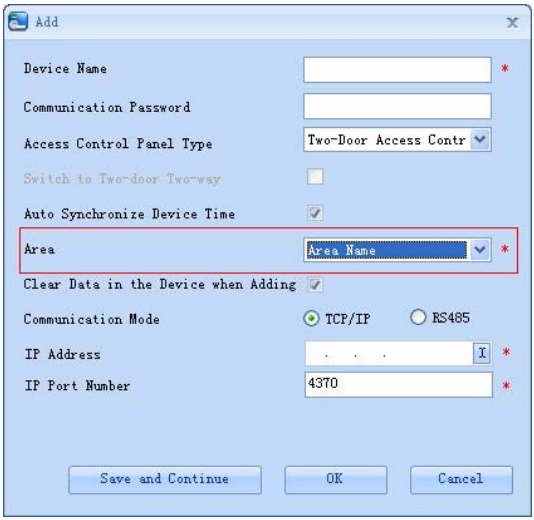
New Add Device: Click [Device] - [Device] - [Add], also through to "Search Access Control" menu and view devices connected to the network, and directly add from the searching result.

There are two ways to add Access Control Panel.

1. Add Device:

(1) In the Device Type Selection interface, select Add Access Control Panel. The communication modes are TCP/ IP or RS485. The following interface will be shown:

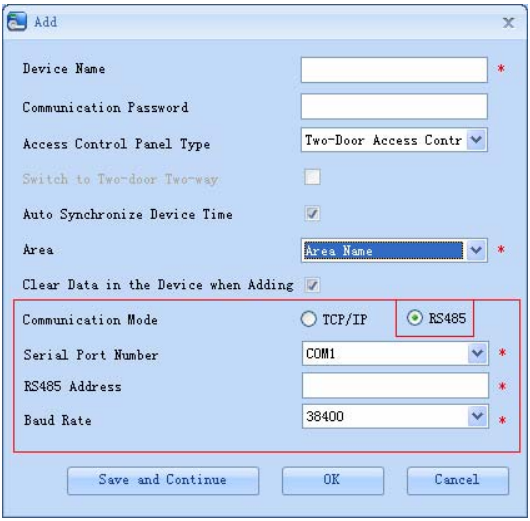
TCP/ IP:



IP Address: Please enter the IP Address of the access control panel;

IP Port No.: In Ethernet mode, the default is 4370.

RS485：



Serial Port Number: COM1-COM254;

485 Address: The machine number. When serial port numbers are the same, there will be no repeated 485 addresses;

Baud Rate: Same as the baud rate of the device (9600/19200/38400/ 57600/115200). The default is 38400;

Note: The same Serial port Number can not allow to exits many of baud rates. If RS485 address respectively for 1 and 2 of the two devices, with 38400 and 115200 baud rate respectively add in system, and use the same Serial port COM1, it will could not add.

Device Name: Any character, up to a combination of 50 characters;

Communication Password: Any character, up to a combination of 8 characters (No blank). You need to input this field only when you add a new device with the communication password. It can not be modified when you edit the device information except in [Modify communication password] operation. Please refer to6.3 Door Settings.

Note: You do not need to input this field if the device has no communication password, such as when it is a new factory device or just after the initialization.

Panel Type: One-door panel, two-door panel, four-door panel;

Switch to Two-door Two-way: When four-door panel is selected, this box will appear. By default, it is not ticked. This parameter is used to switch the four-door one-way access control panel to two-door two-way access control panel (For changes of extended device parameters before and after switching, see relevant files of access control panel).

Note: After the four door one-way access control panel is switched to two- door two-way access control panel, to switch back, you need delete the device from the system and add it again. When adding, do not tick the check box before this parameter.

Auto Synchronizes Device Time: By default it is ticked, namely, it will synchronize device time with server time each time connecting to the device. If it is not ticked, the user can manually synchronize device time;

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： If this option is being ticked, after adding device adding, the system will clear all data in the device, except the event logs. If

you add the device just for demonstration or testing of the system, there is no need to tick it.

(2) After editing, click [OK], and the system will try connecting the current device:

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

If device connection fails, while the user still needs to add the device to the system, corresponding device parameters and extended parameters, such as the serial number, will not be written into the system and settings such as anti-passback and linkage will not be impossible. These settings can be created only when the device is reconnected successfully and corresponding parameters are acquired.

Note: When you add a new device to the system, the software will clear all user information, time zones, holidays, and access control levels settings (including access control group, anti-pass back, interlock settings, linkage settings, etc.) from the device, except the events record in the device. Unless the information in the device is unusable, we recommend that you not to delete the device in used, to avoid the loss of information.

Access Control Panel Settings:

❁ TCP/ IP Communication Requirements:

To support and enable TCP/ IP communication, directly connect the device to the PC or connect to the Internet, get the device IP address and other device information of the device;

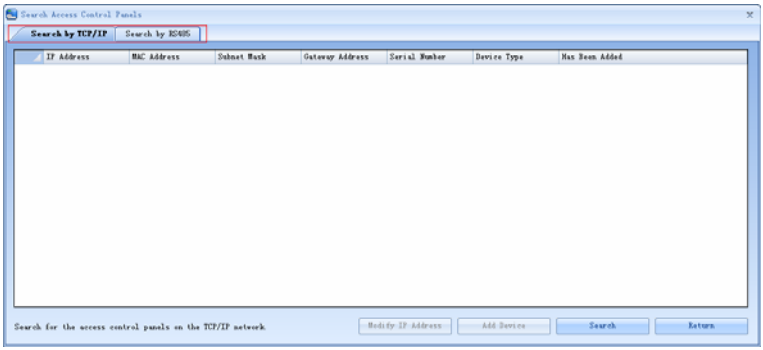
❁ RS485 Communication Requirements:

To support and enable RS485 communication, connect to PC through RS485, get the serial port number, RS485 machine number (address), baud rate and other device information of the device.

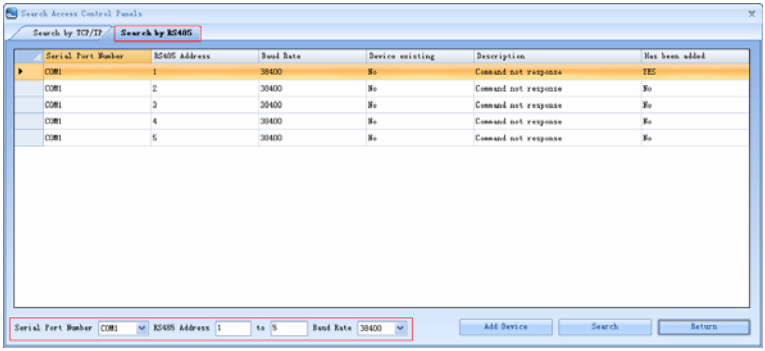
2. Add Device By Searching Access Control Panels:

Search the access control panels in the Ethernet.

(1) Click [Device] - [Search Panels], to show the Search interface, supports Ethernet and RS485 search.

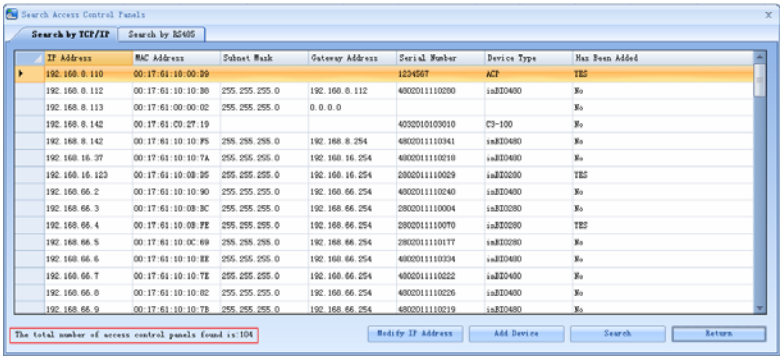


Note: If choose the way of RS485, maybe need select corresponding serial port number, baud rate, fill in RS485 address.



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

(3) After searching, the list and total number of access control panels will be displayed;



Note: Here we use UDP broadcast mode to search the access controller, this mode can not exceed the HUB scale. The IP address can exceed the net segment, but must belong to the same subnet, and needs to configure the gateway and IP address in the same network segment.

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

(5) The default IP address of the access control panel may conflict with the IP of a device on the Internet. 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: Must configure the gateway and IP address in the same network segment).

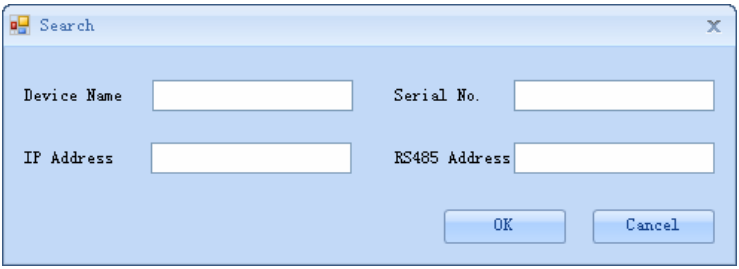
5.2.2 Device Maintenance

For communication between the system and the device, data uploading, configuration downloading, device and system parameters shall be set. The user can see access control panels within his levels in the current system, and can edit the devices here. The user can to add or delete devices in Device if needed.

Edit: Select device, tick in the box in front, then click above [Edit] menu or right click [Edit] to alter.

Delete: Select device, click [Delete], and click [OK].

Search: Click [Device]--[Device]--[Search], entry Device Name and click [OK].



Get Event Entries: Get event records from the device into the system.

Three options are provided for this operation, Get New Entries, Get All Entries, and Get Entries from SD Card. But the last one need through the "More Information" menu to operate.

Get New Entries: The system only gets the new event entries since the last time event entries were collected and records them into the database. Repeated Entries will not be rewritten.

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

When the network is interrupted or communication is interrupted for any reasons, and the event records in the device have not been uploaded into the system in real-time, the operation can be used to manually acquire event records in the device. In addition, the system also can set timing to get.

Note: The access controller can restore up to 100 thousands of event entries. When the entries exceed this number, the device will automatically delete the oldest restored entries (the default delete number is 10 thousands).

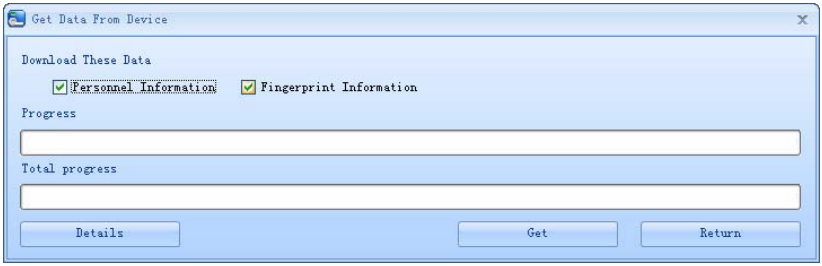
Sync Fluctuant Data to Device: new setting information in operation process

synchronization to device. Such as New Add Personnel, Access Control Setting etc., adopt incremental data synchronization.

The meaning and set mode as above parameters, please see introduction of equipment in the new add process. Gray items for cannot edit project. Device name can not repeat with others.

Equipment type of Access controller is not allowed to change, if the wrong type, should user manually delete this equipment and then again add.

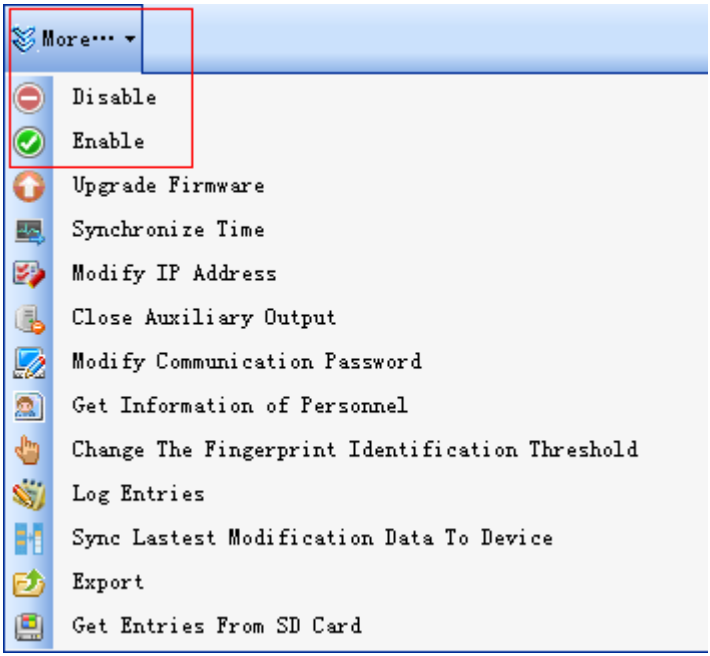
Get Personnel Data From Device: Take origin information of the device saves in the software.



More Information: Includes that Modify IP Address, Close Auxiliary Output, Disable, Enable, Modify Communication Password, Synchronize Time, Upload Event Record, Upgrade Firmware, Get Event Entries, Get Entries from SD Card and etc.

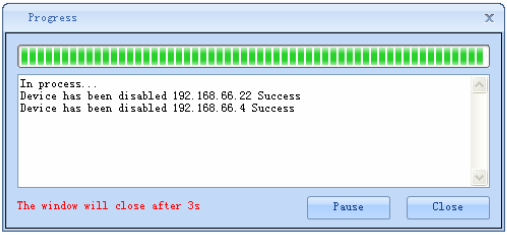
（1）Disable/Enable:

Select device, click [Disable/ Enable] from [More Information] menu to stop/ start using the device. When the device's communication with the system is interrupted or the device fails, the device may automatically appear in disabled status. At this time, after adjusting Internet or device, click [Enable Device] to reconnect the device and restore device communication.



Drag a column header here to group by that column

	Device Name	Serial Number	Communication Mode	IP Address	Serial Port Number	RS485 Address	Enable	Personnel Quantity
1	COM1-1		RS485		COM1	1	✓	0
2	192.168.66....		TCP/IP	192.168.66....			✗	0
3	192.168.66.4		TCP/IP	192.168.66.4			✗	0
4	192.168.16....		TCP/IP	192.168.16....			✓	0
5	192.168.8.1...		TCP/IP	192.168.8.1...			✓	0



Note: If the current device is in enabled status and the connection is not successful, if the user performs the enable operation, the system will immediately reconnect the device.

（2）Upgrade Firmware

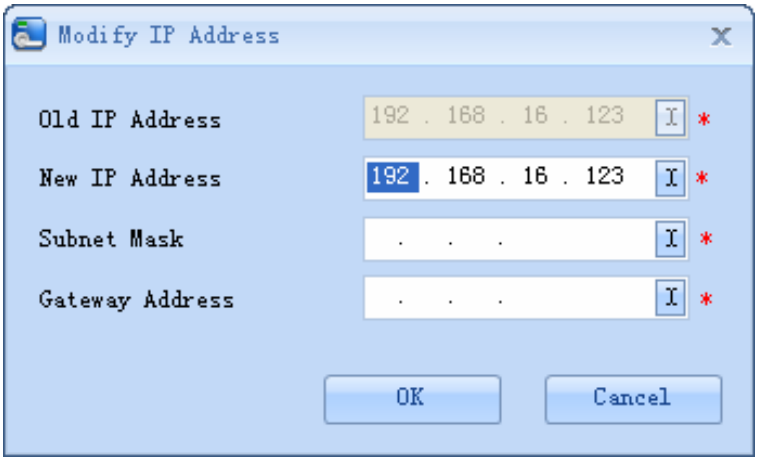
To upgrade firmware in the device, tick the device for which you want to upgrade the firmware, click [Upgrade firmware], enter edit interface, click [Browse] to select the firmware upgrade file (named emfw.cfg) provided by Access, and click [OK] to start upgrading.

（3）Synchronize Time

Synchronize device time with current server time.

（4）Modify IP Address

Select device and click [Modify IP address] to show the Modification interface. It will obtain real-time network gateway and mask from the device. If it is fails because the network is unavailable, then the IP address cannot be modified. Enter new IP address, gateway, and subnet mask. Click [OK] to save settings and quit. This function the same as [Modify IP Address Function] in 5.2.1 Add Access Control Panel. The difference is when searching control panels, the devices have not been added into the system, while the current [Modify Device IP Address] is regarding added devices.



（5）Close Auxiliary Output

Close the auxiliary device connected to the device auxiliary output interface.

（6）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: The communication password can not contain space; it is recommended that a combination of numbers and letters be used. The communication password setting can improve the device security. It is recommended to set communication password for each device.

（7）Get Information of Personnel

Renew the current number of personnel and fingerprints in the device. The final value will be displayed on the device list.

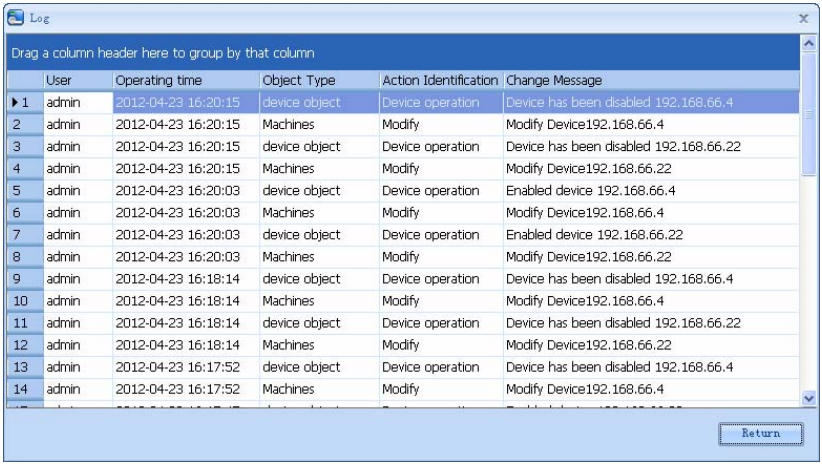
（8）Change the fingerprint identification threshold

The user can change the fingerprint identification threshold in the device. The scale is 35-70 and 55 by default. In device adding, the system will get the threshold from the device. If the operation succeeds, user can view the threshold in all of the

devices. Batch operation is permitted; the user can change multiple devices concurrently.

（9）Log Entries

Record this software history operating records, with list form to record all of the operation. At interface of Personnel, Department, Issue Card has [Log Entries] menu, click it can show the relevant record information.



	User	Operating time	Object Type	Action Identification	Change Message
▶1	admin	2012-04-23 16:20:15	device object	Device operation	Device has been disabled 192.168.66.4
2	admin	2012-04-23 16:20:15	Machines	Modify	Modify Device192.168.66.4
3	admin	2012-04-23 16:20:15	device object	Device operation	Device has been disabled 192.168.66.22
4	admin	2012-04-23 16:20:15	Machines	Modify	Modify Device192.168.66.22
5	admin	2012-04-23 16:20:03	device object	Device operation	Enabled device 192.168.66.4
6	admin	2012-04-23 16:20:03	Machines	Modify	Modify Device192.168.66.4
7	admin	2012-04-23 16:20:03	device object	Device operation	Enabled device 192.168.66.22
8	admin	2012-04-23 16:20:03	Machines	Modify	Modify Device192.168.66.22
9	admin	2012-04-23 16:18:14	device object	Device operation	Device has been disabled 192.168.66.4
10	admin	2012-04-23 16:18:14	Machines	Modify	Modify Device192.168.66.4
11	admin	2012-04-23 16:18:14	device object	Device operation	Device has been disabled 192.168.66.22
12	admin	2012-04-23 16:18:14	Machines	Modify	Modify Device192.168.66.22
13	admin	2012-04-23 16:17:52	device object	Device operation	Device has been disabled 192.168.66.4
14	admin	2012-04-23 16:17:52	Machines	Modify	Modify Device192.168.66.4

（10）Sync All Data To Device: The system will synchronize the data to the device, including door information, access control levels (personnel information, access control time zones), anti-pass back settings, interlock settings, linkage settings, first-card normal open settings, multi-card normal open settings and so on. Select device, click [Synchronize All Data] and click [OK] to complete synchronization.

Note: The operation of Synchronize All Data is mainly to delete all data in the device first (except event record). 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.

（11）Export

Click [Device]-- [Device]-- [Export], can export the relevant contents of device with

EXCEL or PDF or Txt. Format , save on your computer.

（12）Get Entries from SD Card

The system will get the event entries from the SD card in the device. Then through software analyzing, will backup records of the SD card for into the system.

6. Security System Management

1. Work principle of the access control system:

ZKAccess5.0 Security System is a C/S-based management system, providing normal access control functions, management of networked access control panel via computer, and unified personnel access management.

The access control system can set the opening levels of registered users, namely, allowing some personnel to open some doors by verification during a time period.

Otherwise, the system supports the use of data from the access control panel for attendance purpose, to save the device resource.

It facilitates the management and support of multiple databases, including Access, SQL Server. Designed based on multi-business convergence, it supports service extension, such as attendance and supports multiple languages.

2. Access control system parameters:

- 255 time zones;
- Unlimited access levels;
- Three holiday types and 96 holidays total;
- Anti-passback function;
- Interlock function;
- Linkage function;
- First-Card Normal Open function;
- Multi-Card Opening function;
- Remote door opening and closing;
- Real-time monitoring.

3. Operation functions of access control system:

Click to enter the [Access Control System] and the main interface is [Real-Time Monitoring].

Access Control System Management primarily includes Access Control Time Zones, Access Control Holiday, Door Settings, Access Levels, Personnel Access Levels, Real-Time Monitoring, and Reports, etc.

✍ **Note:** This chapter the parameters definition can refer to Definitions .

6.1 Access Control Time Zones

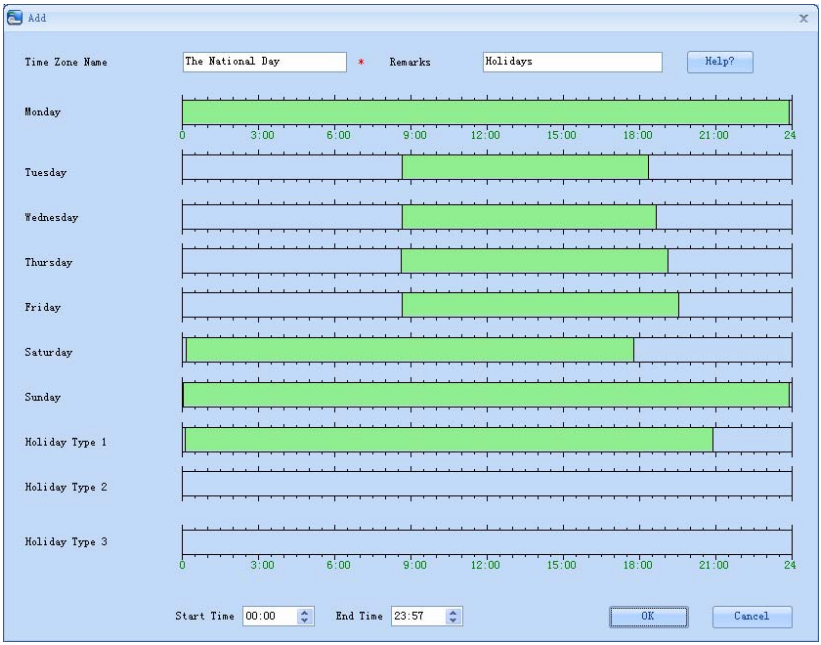
Access Control Time Zone can be used for door timing. The reader can be made usable during valid time periods of certain doors and unusable during other time periods. Time Zone can also be used to set Normal Open time periods for doors, or set access control levels so that specified users can only access specified doors during specified time periods (including access levels and First-Card Normal Open settings).

The system controls access according to Access Control Time Zones. The system can define up to 255 time zones. For each time zone, you can define, during a week, you can define up to three intervals for each day and three holiday types for each time zone. Each interval is the valid interval in 24 hours of each day. The format of each interval for a time zone: HH: MM-HH: MM, this is accurate to minutes in the 24-hour system.

Initially, by default the system has access control time zone named [Accessible 24 hours]. This time period can be modified but cannot be deleted. The user can add Access Control Time Zones that can be modified.

1. Add Access Control Time Zone:

(1) Click [Access Control System] - [Time zones] - [Add] to access the time zone setting interface;



The parameters are as follows:

Time Zone Name: Any character, up to a combination of 50 characters;

Remarks: Detailed description of the current time zone, including an explanation of the current time zone and primary applications, facilitating the user or other users with same level to view time zone information. The field is up to 70 characters;

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

Setting: If the interval is Normal Open, just fill in 00:00-23:57 as the interval, or press the mouse left key drag completely in whole time frame; Time setting is empty by default, namely the default is closed; Time Zone can sets three intervals, so press the mouse dragging three time intervals in each time frame.

Holiday Type: There are three holiday types in the time zone. They are unrelated to the day of the week. If a certain date is set to a certain holiday type, the three intervals of

the holiday type will be used for access. The holiday type in a time zone is optional. However, if the user does not enter one, the system will give the default value.

After time zone setting, click [OK] to save, and the time zone will appear in the list.

2. Maintenance of Access Control Time Zone:

Edit: In the time zone list, pitch on relevant time zone, and then right-click to select [Modify time] to access the time zone modification interface, and modify the time zone setting. After modification, click [OK], and the modified time zone will be saved and shown in the time zone list, or click [Cancel] to cancel the operation.

Delete: In the time zone list, pitch on relevant time zone, and then right-click to select [Delete time], click [OK] to delete the time zone, or click [Cancel] to cancel the operation. A time zone in use can not be deleted.

Tick the check boxes before one or more time zones in the time zone list. Click the [Delete] button over the list, and click [OK] to delete the selected time zones, or click [Cancel] to cancel the operation.

6.2 Access Control Holidays

The Access Control Time of a holiday may differ from that of a weekday. For easy operation, the system provides holiday settings to set access control time for holidays.

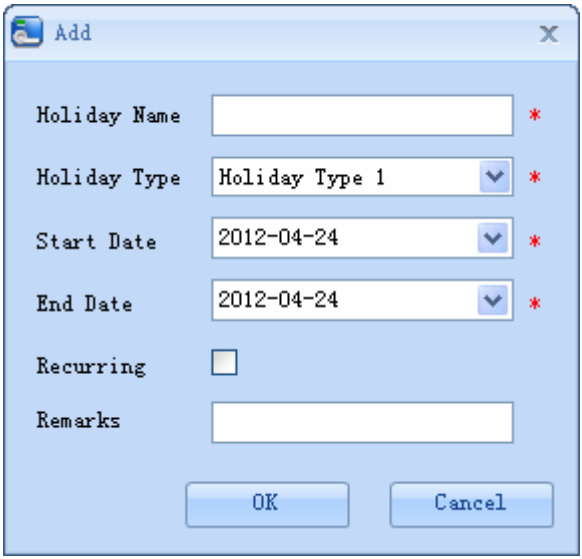
Access Control Holiday Management includes Add, Modify and Delete Access Control Holiday.

1. Add Access Control Holiday:

Three holiday types are supported, each including up to 32 holidays. To conduct special access level configuration on special dates, the user can select special holidays for setting.

The operation steps are as follows

(1) Click [Access Control System] - [Holidays] - [Add] to access Add Access Control Holiday edit interface:



The fields are as follows:

Holiday Name: Any character, up to a combination of 50 characters;

Holiday Type: Holiday Type 1/2/3, namely, A current holiday record belongs to these three holiday types and each holiday type includes up to 32 holidays;

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

Recurring: Yes or No. The default is "No". Annual cycle means that a holiday does not require modification in different years. For example, the Near Year's Day is on January 1 each year, and can be set as "Yes". For another example, the Mother's Day is on the second Sunday of each May, so its date is not fixed and should be set as "No";

For example, the date of the holiday "Near Year's Day" is set as January 1, 2012, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of "Friday" in the week, but the Access Control Time of Holiday Type 1 such as 6.1 Access Control Time Zones.

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

2. Modification of Access Control Holiday:

To modify the original Access Control Holiday, click [Edit] behind the Access Control Holiday to access the edit interface. After modification, click [OK] to save and quit.

3. Deletion of Access Control Holiday:

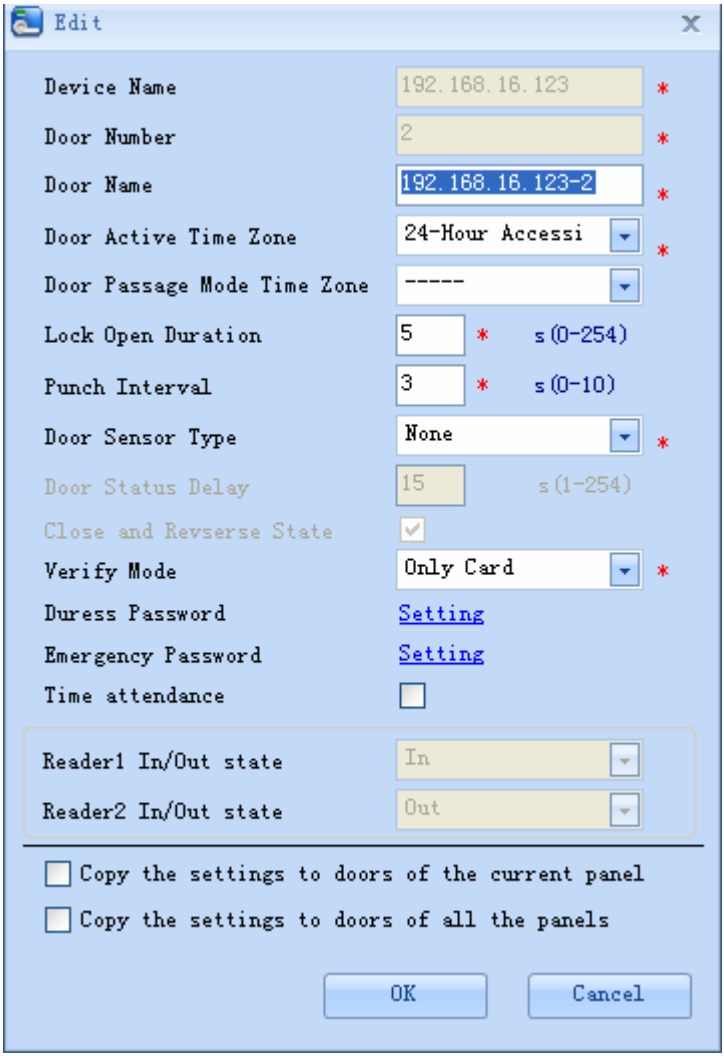
In the access control holiday list, click the [Delete] button under "Related Operation". Click [OK] to delete the holiday, or click [Cancel] to cancel the operation. An Access Control Holiday in use cannot be deleted.

Tick the check boxes before one or more holidays in the holiday list. Click the [Delete] button over the list, and click [OK] to delete the selected holiday, or click [Cancel] to cancel the operation.

6.3 Door Settings

Door parameter modification:

Click [Access Control] -- [Door Setting], Select the door to be modified, show the Edit interface as follow;



The fields are as follows:

Device Name: It is not editable (must be edited in 5.2.1 Add Access Control Panel);

Door Number: The system automatically names the numbers of doors according to how many doors of the device has (for example, the four doors of a four-door control panel are numbered 1, 2, 3 and 4). The 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 to the door number, but 1/2/3/4 in anti-passback and interlock refers to door serial number rather than the number following the door name. They are not necessarily related. The system allows the user to modify the door name, so they can not be confused;

Door Name: The default Door Name is "device name door number". The field allows the user to modify as required. Up to 50 characters can be entered;

Door Active Time Zone, Passage Mode Time Zone: By default both are null. Initialized and added access control time zones will be shown for the user to select. Upon door editing, door valid time zone is needs to be input. Only after setting the door valid time zone, the door can be opened and closed normally. We recommend to set the door Normal Open time period within the door valid time zone, only in this situation, the door normal open time zone is valid.

Note: Consecutive punching of a card having access level of the door for 5 times can release the Normal Open status for one day (including First-Card Normal Open), and close the door immediately.

Lock Drive Duration: Used to control the delay for unlocking after card punching. The unit is second, and the default is 5 seconds. The user can enter a number between 0-254;

Punch Interval: The unit is seconds (range: 0-10 seconds), and the default is 2 seconds;

Door Sensor Type: NO (door sensor not detected), Normal Open, Normal Close. The default is NO. When editing doors, the user can select the door sensor type to be Normal Open or Normal Close. If Normal Open or Normal Close is selected, it is required to select **door status delay** and whether **close and reverse-lock** is required. By default, once door sensor type is set as Normal Open or Normal Close, the default door status delay will be 15s, and by default it will enable close and reverse-lock.

Door Status Delay: The duration for delayed detection of the door sensor after the door is opened. Detection is performed only after the door is opened and the delay duration expired. 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 status delay will be 15seconds. The door status delay should be longer than **Lock Drive 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, and Only Fingerprint verify. The default is Only Card or Only Fingerprint. When Card plus Password mode is selected, make sure the door uses a reader with keyboard (the fingerprint verify modes are only available for version 5.0.8 and above version);

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

Duress Password Opening (used with legally card): When Only Card verify mode is used, you need to press [ESC] first, and then press the setting password plus [OK] button. Finally swipe your card. The door opens and triggers the alarm. When Card Plus Password verify mode is used, please swipe your card first, then press the password number plus the [OK] button (same to normal door open in card plus password verify mode), the door open and trigger the alarm.

Emergency Password Opening: The password must be a number not exceeding 8 digits (integer). The door can be opened just 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 these two numbers should not be the same.

Time attendance: If this option is checked, punch the time clock records of the door will be used for attendance.

Note: If need use in Time attendance, At least need to select a door in [Door setting]; if not select any door, so open the [TimeSheet], there will be not records.

Apply these settings to all the doors of current access control panel: Click to apply to all doors of the current access control panel;

Apply these settings to all the doors of all access control panels: Click to apply to all doors of all access control panels within the current user's level;

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

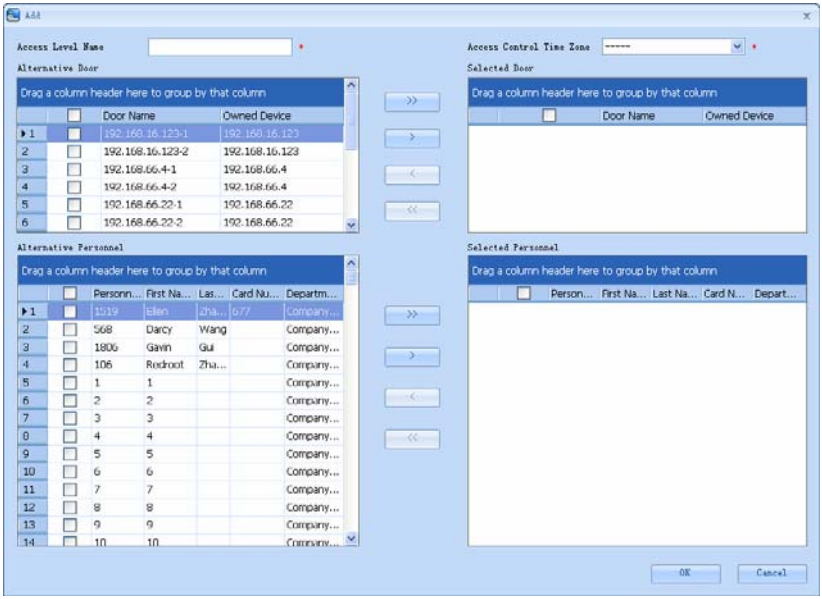
Other parameters specifications see Definitions in this user manual.

6.4 Access Levels

Access levels means in a specific time period, which door or door combination can be opened through verification.

Add access levels:

1. Click [Access Control System] - [Access levels] - [Add] to enter Add access levels edit interface:



2. Set parameters: access level name (no repetition), access control time zones, door combination, selected personnel;

3. Click [OK] to complete setting and quit, and added access levels will appear in the list.

Notes:

(1) Select the doors in the access levels as multi-choice, so you can select different doors in different control panels;

(2) When adding personnel, if selected personnel exist in the current access level, the system can not add again.

(3) Two levels with the same time zone and door combination are not allowed in the system.

Personnel Access Levels: Select personnel, click [Delete from access level] to delete the personnel from the access level.

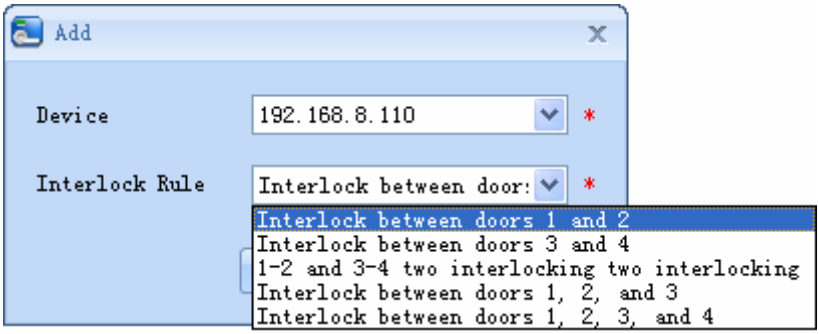
6.5 Interlock Settings

Interlock can be set for any two or more lock belong to one access control panel, so that when one door is opened, the others will be closed. And you can open one door only when others are closed.

Before interlock setting, please make sure the access controller is connected with door sensor according to the Installation Guide, and the door sensor has been set as NC or NO state.

Add interlock settings:

1. Click [Access Control] - [Interlock] - [Add] to enter the interlock setting edit interface;



2. Select device to show interlock settings. Since one device can only correspond to one interlock setting record, when adding, interlocked devices can not be seen in the dropdown list of the device. When deleting established interlock information, the corresponding device will return to the dropdown list. The setting page will vary with the number of doors controlled by the 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 settings, tick an item (multiple interlocks can be selected as long as doors are not repeated), click [OK] to complete setting, and then the added interlock settings will be shown in the list.

For example, select 1-2-3-4 four-door interlock, if you want open door 3, doors 1, 2 and 4 needs to be closed.

Note: When editing, the device can not 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 exist, will be deleted.

6.6 Anti-Passback Settings

Currently anti-passback settings support in and out anti-passback. In some special occasions, it is required that the card holder who entered from a door by card punching must exit from the same door by card punching, with the entry and exit records strictly consistent. One who followed another to enter the door without card punching will be denied when trying to exit by card punching, and one who followed another to exit without card punching will be denied when trying to enter by card punching. When a person enters by card punching, and gives the card to another to try entering, the other person will be denied. The user can use this function just by enable 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 System] - [Anti-passback settings] - [Add] to show anti-passback setting edit interface;

2. Select device (N-door control panel), because one device can only correspond to one anti-passback setting record, so 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. The settings vary with the number of doors controlled by the device:

Anti-passback can be set between readers and between doors. The card holder enter from door A, he must exit from door B, this function is used for channel or ticket management.

Anti-passback settings of 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 doors 1/2;

Anti-passback settings of a four-door control panel:

Anti-passback of doors 1-2, anti-passback of doors 3-4, anti-passback of doors 1/2-3/4, anti-passback of doors 1-2/3, anti-passback of doors 1-2/3/4, Anti-passback between readers of door 1, anti-passback between readers of door 2, Anti-passback between readers of door 3, anti-passback between readers of door 4.

Note: The reader mentioned above includes Wiegand reader that connected with access control panel and inBIO reader. The single door and two door control panel with Wiegand reader include out reader 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 the in or out state (means it is the in reader or out reader) and set according to the actual need. For the reader number, odd number is for in reader, and even number is for out reader.

3. Select anti-passback settings, and tick one item (anti-passback without repetition of doors or readers can be subject to multi-choice). Click [OK] to complete setting, and the added anti-passback settings can be shown in the list.

Note: When editing, you can not 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 record, its anti-passback setting record, if exist, will be deleted.

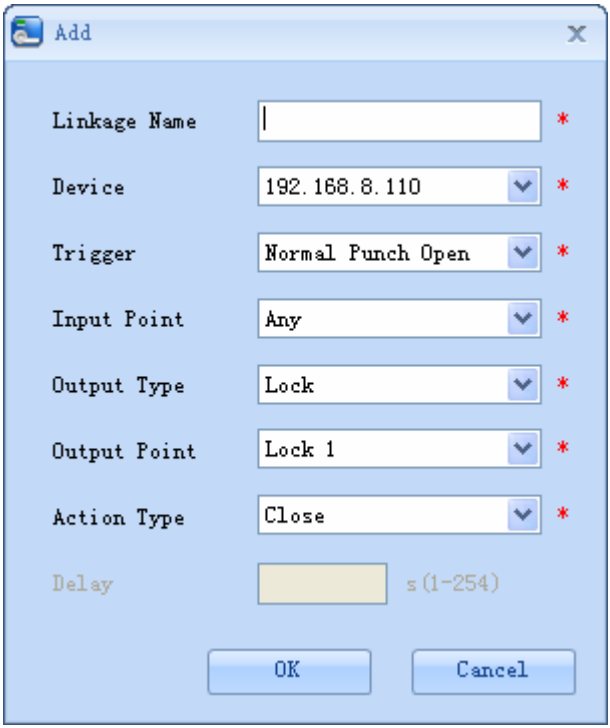
6.7 Linkage Settings

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 exception of the system and list them in the corresponding monitored report for view by the user.

Add linkage setting:

1. Click [Access Control System] - [Linkage setting] - [Add] to show the linkage setting interface;

2. Input linkage setting name (input linkage setting name before selecting device). After selecting device, corresponding linkage setting will appear (The system will first determine whether or not the device is successfully connected and has read extended device parameters such as auxiliary input quantity, auxiliary output quantity, door quantity and reader quantity. If the system has no available extended device parameters, it will remind the user of failing to set anti-passback. Otherwise, it will, shows linkage setting options according to the currently selected device, such as the door quantity, auxiliary input and output quantity):



The fields are as follows:

Trigger Condition: Please refer to 6.10 Real-time Monitoring for the Real Time Events Description. Except Linkage Event Triggered, Cancel Alarm, Open Auxiliary Output, Close Auxiliary Output, and Device Start, all events could be trigger condition.

Input Point Address: 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 refer to specific device parameters);

Output Point Address: 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, Auxiliary Output 10 (the specific output point please refer to specific device parameters);

Action Type: Close, Open, Normal Open. By default it is closed. To open, delay time shall be set, or Normal Close can be selected;

Delay: Ranges from 1-254s (This item is valid when the action type is Open)

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

For example: If select “Normal Punching Card Open” as the trigger condition, and the input point is Door 1, the output point is Lock 1, the action type is Open, the delay is 60s, then when “Normal Punching Card Open” 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 can not 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 system has set that the input point is a specific door or auxiliary input point under a trigger condition of a device, it will not allow the user to add (or edit) a linkage setting record where the device and trigger condition are the same but 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 trigger point is ‘Any’, the system will not permit the user to add (or edit) a linkage setting record where the input point is a specific door or auxiliary input.

In addition, the system does not allow the same linkage setting at input point and output point in specific trigger condition.

The same device permits consecutive logical (as mentioned above) linkage settings.

6.8 First-Card Normal

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

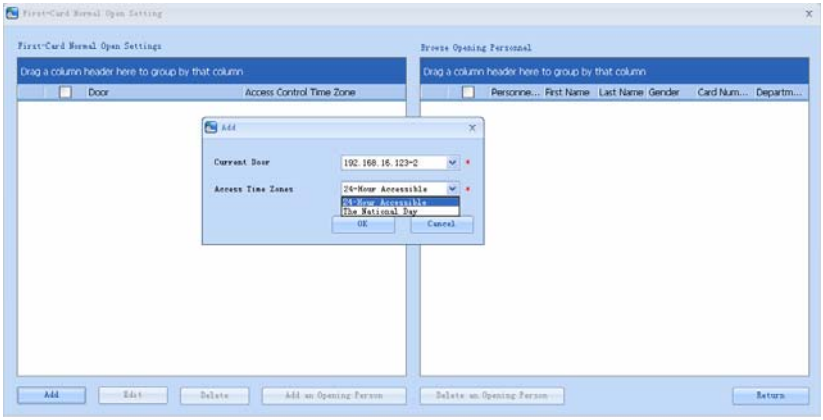
The user can set First-Card Normal Open for a specific door. The settings include door, door opening time zone and personnel with First-Card Normal Open level. A door can have First-Card Normal Open settings for multiple time zones. The interface of each door will show the number of existing First-Card Normal Open settings. For First-Card Normal Open setting, when adding or editing each record, it is not required to modify the “current door”, but to select time zone. When record

adding is successful, add personnel that can open the door for a First-Card Normal Open setting record. On the right of the interface, you can browse door opening personnel in a First-Card Normal Open setting and delete current personnel, so that some personnel will not have First-Card Normal Open level any more.

The operation steps are as follows:

1. Click [Access Control System] - [First-Card Normal] to show First-Card Normal Open setting interface;

2. Click [Setting] - [Add], select the time zone of First-Card Normal Open, and click [OK] to save the settings;



3. Select [First-Card Normal], click [Add an opening person] to set personnel having First-Card Normal Open level. Click [OK] to save and quit editing.

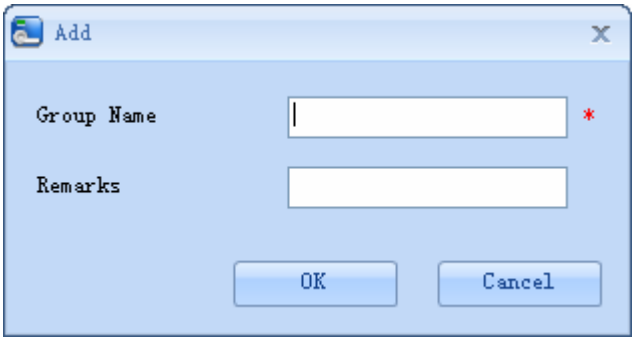
✍ **Note:** For a door currently in Normal Open time period, consecutive verification of a person having access level for the door for 5 times (the person verification interval should be within 5 second.) can release the current Normal Open status and close the door. The sixth person verification will be a normal verification. This function is only effective at the valid door valid time zone. Normal Open intervals set for other doors within the day and First-Card Normal Open settings will not take effect anymore.

6.9 Multi-Card Opening

1. Multi-Card Opening Personnel Groups:

It is personnel grouping used to set Multi-Card Opening groups.

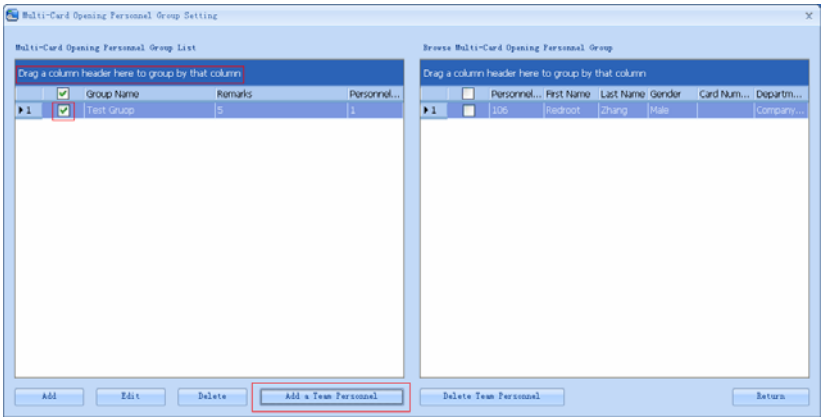
(1) Click [Access Control System] - [Multi-Card Opening] - [Multi-Card Opening Personnel Groups] - [Add] to show the following edit interface:



Group name: Any combination of up to 50 characters that cannot be identical to an existing group name;

After editing, click [OK], return and the added Multi-Card Opening Personnel Groups will appear in the list;

(2) Select a group, and click [Add a Team Personnel] 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 can not be grouped repeatedly.

2. Multi-Card Opening:

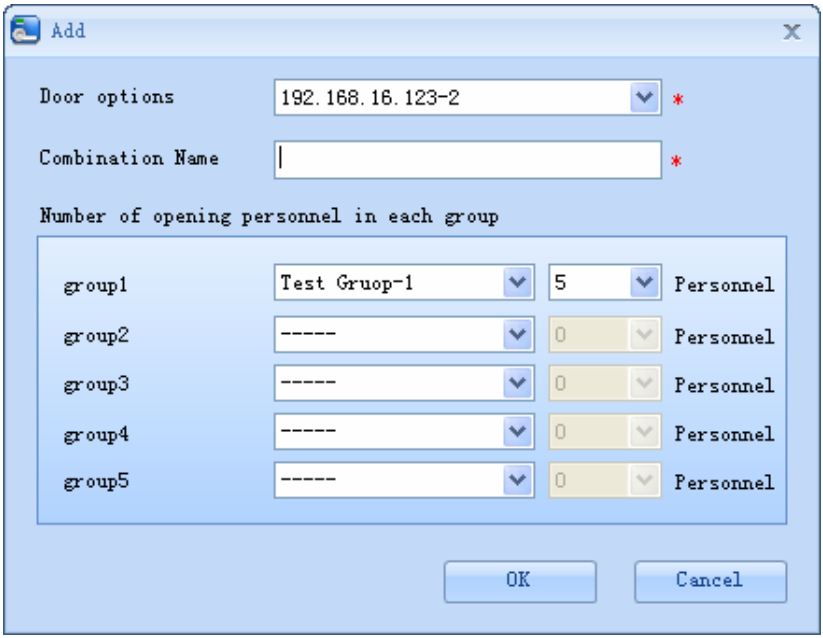
Set levels for personnel in [Multi-Card Opening Personnel Group Setting].

This function needs to be enabled in some special access occasions, where 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 combination) will interrupt the procedure, and you need to wait 10 seconds wait to restart verification. It will not open by verification by only one of the combination.

Multi-Card Opening combination is a combination of the personnel in one or more Multi-Card Opening 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 conversely the total number of door opening people shall not be greater than 5. In addition, if the number of people entered by the user is greater than the number of people in the current group, the Multi-Card Opening function will be unable to be realized normally.

Multi-Card Opening settings:

(1) Click [Access Control System] - [Multi-Card Opening] - [Add] to show the Multi-Card Opening setting interface;



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

6.10 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 exceptional events (including alarm events).

Monitoring all:

The system will, by default, show the monitoring of all doors under the control panels within the current user's access level. The user can monitor one (or more) door(s) by [Area], [Control panel] or [Door].

Remote Opening/Closing: Including the operations of single door and all current doors. In single door operation, move the cursor to the door icon, click [Remote opening/closing] in the open menu. In all current doors operation, click [Close all

current doors] in the main interface to fulfill the operation.

When you remote close the door, self-define the open time interval is enabled, 15 seconds by default. You can select [Enable Intraday Normal Open Time Zone], and the normal open time zone intraday will take effect. You can also set the door state to normal open directly, and no time zone intraday can effect the door state any more (namely normally open for 24 hours).

If you want to close the door, please select [Disable Intraday Normal Open Time Zone] first, to avoid other normal open time zones take effect and open the door. And then select [Remote Closing] to fulfill the operation.

✍ **Note:** If the operations of remote opening/closing always return failure, please check the current list of devices. If there are too many offline devices, you need to check the network to ensure the operation proceed normally.

Cancel all alarms: Once alarming doors appear on the interface, the system will alarm. Click to cancel the alarms of the control panels for alarming doors. If Cancel Alarms is successful, the system will automatically stop alarming.

✍ **Note:** If a control panel have multiple door alarms at the same time, you need only execute one cancel operation at one of these door to cancel all the alarm in this control panel.

When putting the cursor on a door, it will show relevant parameters and operations: device, door number, door name, remote opening, and remote closing. Icons in different colors represent statuses as follows:

Icon							
Status	Door alarming	Door closed when online	Door opened when online	Door sensor unset	Device banned	Door Offline	Door opening timeout

Personnel photo display:

If there is a person concerned in the real-time monitoring, and the corresponding photo is set before, then the photo will be displayed in real-time monitor. And the event name, trigger time, person name will be displayed on the photo.

Event monitoring:

The system automatically acquires monitored device event records, including normal access control events and exceptional access control events (including alarm events). Alarm events appear in red. Exceptional events excluding alarm events appear in orange. Normal events appear in green.

On the current event monitoring interface, the recent records are on the top, enabling the user to see without dragging the scrollbar. Meanwhile, the interface will show up to some 100 records.

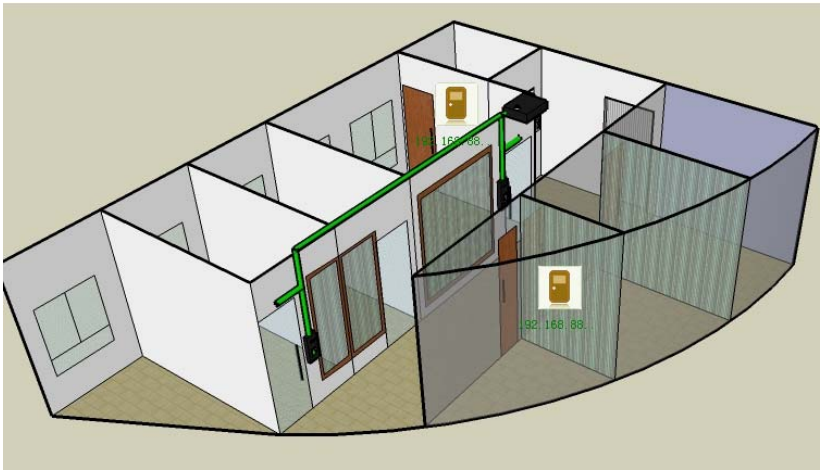
6.11 E-Map

Before using the e-map, user needs to add the map to the system first. After success adding, user can add door, zoom-in, zoom-out the map (and the door on the map), etc. If the user changes the door icon, or the map, or the position of door icon, click [Save Position] to save the current position, then the user can view the setting at the next time access.

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

Edit Map: User can change the map name, change map or change 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 [Remove Door]), or adjust the map or position of the door icon (by drag the door icon).



✍ **Note:** Add doors on the map, the system supports to add multi door at the same time. After door adding, user needs to set the door position on the map, and click [Save] after setting.

7. Access Control Reports

Includes [Events Today], [Events the latest three days], [Events This week], [Events Last week], [Exception Events] reports. You can select Export all and Export after query. The user can generate statistics of relevant device data from access control reports, including card verification information, door operation information, and normal card punching information, etc.

About the Normal event and abnormal event please refer to 6.10 Real-time Monitoringfor details.

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

7.1 Events Today

Click [Reports] - [Events Today], it will displayed following interface, then will show intraday access control events records.

Drag a column header here to group by that column

	Time	Personnel Number	First Name	Last Name	Card Number	Device	Event Point	Verify Mode	In/Out Status	Event Description
▸1	2012-04-28 16:25...	25	25		1332098	Events	Events-4	Card or Fingerp...	IN	Normal Punch Open
2	2012-04-28 16:25...	22	22		12936553	Events	Events-3	Card or Fingerp...	IN	Normal Punch Open
3	2012-04-28 16:25...	25	25		1332098	Events	Events-3	Card or Fingerp...	OUT	Normal Punch Open
4	2012-04-28 16:25...					Events	Events-1	Others	None	Linkage Event Trigge...
5	2012-04-28 16:25...	25	25		1332098	Events	Events-1	Card or Fingerp...	IN	Normal Punch Open

7.2 Events the latest three days

Click [Reports] - [Events the latest three days], it will show the latest access control events records.

7.3 Events This Week

Click [Reports] - [Events This Week], it will show the access control events records within this week.

7.4 Events Last Week

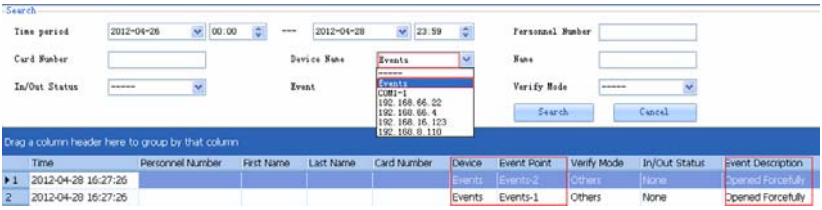
Click [Reports] - [Events Last Week], it will show the access control events records

at last week.

7.5 Exception Events

Click [Reports] - [Exception Events], it will show the access control exception events records.

You can also through put in View the specified conditions access control abnormal events, such as search "Device Name" to display the relevant exception records as below:



Clear access control exception event records: Clear the list of all access control exception events.

Real-time door status monitoring: Except to display the electro-map, the system can view the real-time event monitoring (same data source with door status monitoring, include alarm sound, etc.).

Door operation: Move the mouse icon to the door position, the system will automatically filter the operation according to the door status and display them on the popup menu. User can remote open or close the door, cancel alarm, and etc.

Appendix: Real-Time Event Description

1. Normal Events:

Normal Punch Open: In [Card Only] verification mode, the person has open door permission punch the card and trigger this normal event of open the door.

Press Fingerprint Open: In [Fingerprint Only] or [Card plus Fingerprint] verification mode, the person has the open permission, press the fingerprint at the

valid time period, and the door is opened, and triggers the normal event.

Exit button Open: User press the exit button to open the door within the door valid time zone, and trigger this normal event.

Punch during Normal Open Time Zone: At the normally open period (set to normally open period of a single door or the door open period after the first card normally open), or through the remote normal open operation, the person has open door permission punch the effective card at the opened door to trigger this normal events.

First Card Normal Open (Punch Card): In [Card Only] verification mode, the person has first card normally open permission, punch card at the setting first card normally open period but the door is not opened, and trigger the normal event.

Normal Open Time Zone Over: After the setting normal open time zone, the door will close automatically. The normal open time zone include the normal open time zone in door setting and the selected normal open time zone in first card setting.

Remote Normal Opening: Set the door state to normal open in the remote opening operation, and trigger this normal event.

Disable Intraday Normal Open Time Zone: In door normal open state, punch the effective card for five times near to the card reader (must be the same user), or select [Disable Intraday Normal Open Time Zone] in remote closing operation, and trigger this normal event.

Enable Intraday Normal Open Time Zone: If the intraday door normal open time zone is disabled, punch the effective card for five times near to the card reader (must be the same user), or select [Enable Intraday Normal Open Time Zone] in remote opening operation, and trigger this normal event.

Multi-Card Open: In [Card Only] verification mode, multi-card combination can be used to open the door. After the last card plus fingerprint verified, the system trigger this normal event.

Emergency Password Open: The password (also known as the super password) set for the current door can be used for door open. It will trigger this normal event after the emergency password verified.

Open 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, and trigger this normal event.

Linkage Event Triggered: After the system linkage configuration take effect, trigger this normal event.

Cancel Alarm: When the user cancel the alarm of the corresponding door, and the

operation is success, trigger this normal event.

Remote Opening: When the user opens a door from remote and the operation is successful, it will trigger this normal event.

Remote Closing: When the user close a door from remote and the operation is successful, it will trigger this normal event.

Open Auxiliary Output: In linkage action setting, if the user select Auxiliary Output for Output Point Address, select Open for Action Type, it will trigger this normal event when the linkage setting is take effect.

Close Auxiliary Output: In linkage action setting, if the user select Auxiliary Output for Output Point Address, select Open for Action Type, it will trigger this normal event when the linkage setting is take effect. And if the user closes the opened auxiliary output through the [Close Auxiliary Output] operation in [Door Setting], trigger this normal event too.

Door Opened Correctly: When the door sensor detects that the door has been properly opened, triggering this normal event.

Door Closed Correctly: When the door sensor detects that the door has been properly closed, triggering this normal event.

Auxiliary Input Disconnected: When the auxiliary input point disconnected, trigger this normal event.

Auxiliary Input Shorted: When the auxiliary input point short circuit, trigger this normal event.

Device Start: When the device start trigger this normal event, and this event can not display on the real-time monitor, but you can check it in the event report.

2. Abnormal Events

Too Short Punch Interval: When the interval between two card punching is less than the set time interval, trigger this abnormal event.

Door Inactive Time Zone (Punch Card): In [Card Only] verification mode, the user has the door open permission, punch card but not at the door effective period of time, and trigger this abnormal event.

Door Inactive Time Zone (Exit Button): The user has the door open permission, punch card but not at the access effective period of time, and trigger this abnormal event.

Illegal Time Zone: The user with the permission of opening the current door, punches the card during the invalid time zone, and triggers this abnormal event.

Access Denied: The registered card without the access permission of the current door, punch to open the door, trigger this abnormal event.

Anti-Passback: When the anti-pass back setting of the system takes effect, triggers this abnormal event.

Interlock: When the interlocking rules of the system take effect, trigger this abnormal event.

Multi-Card Authentication (Punching Card): Use multi-card combination to open the door, the card verification before the last one (whether verified or not), trigger this normal event.

Multi-Card Authentication (Punching Card): Use multi-card combination to open the door, the card verification before the last one (whether verified or not), trigger this normal event.

Unregistered Card: Refers to the current card is not registered in the system, trigger this abnormal event.

Opening Timeout: The door sensor detect that it is expired the delay time after opened, if not close the door, trigger this abnormal event.

Card Expired: The person with the door access permission, punch card to open the door after the effective time of the access control, can not be verified and will trigger this abnormal event.

Password Error: Use card plus password, duress password or emergency password to open the door, trigger this event if the password is wrong.

Failed to Close during Normal Open Time Zone: The current door is in normal open state, but the user can not close the door through [Remote Closing] operation, and trigger this abnormal event.

8. System Settings

System settings primarily include assigning system users (such as company management personnel, registrar, access control administrator) and configuring the roles of corresponding modules, managing database, such as backup, initialization, and setting system parameters and operation logs, etc.

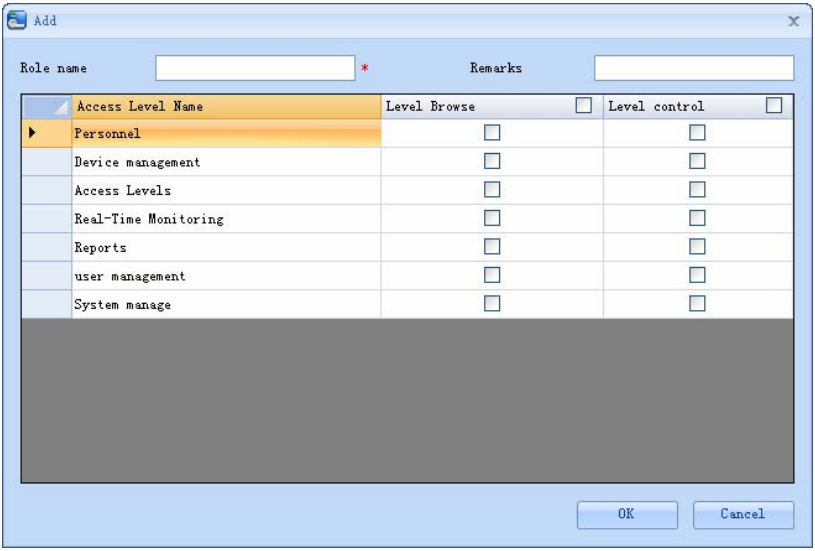
8.1 User Management

1. Role management:

During daily use, the super user needs to assign new users having different levels. To avoid individual setting for each user, roles having certain levels can be set in role management, and then be assigned to specified users, including the levels set for five major functional modules of personnel, device, access control, video system and system setting. The system's default super user has all levels, and can create new users and set corresponding levels as required.

Role setting steps:

(1) Click [Add] to enter role setting interface;



(2) Set role name, select your desired role setting item, and tick levels to be configured for users of different levels;

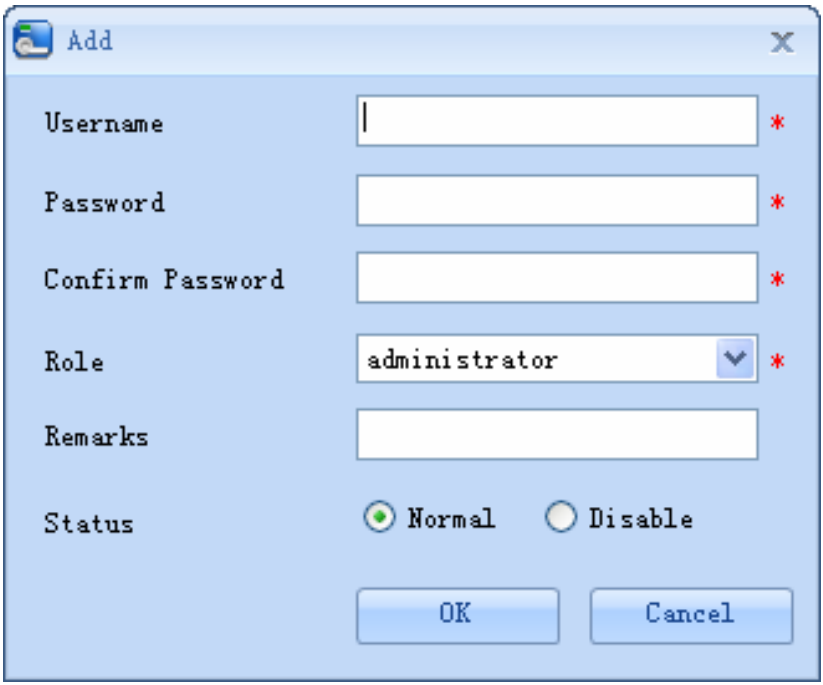
(3) After setting, click [OK] to save and return to the list, and added role settings will be shown in the list.

2. User management:

Add new users to the system, and assign user roles (levels).

Add user:

1. Click [Add], enter new user information, where items with [*] are mandatory. The parameters are as follows:



Username: Not more than 50 characters, only using letters, numbers or characters;

Password: The length must be more than 4 digits and less than 18 digits. The default password is 111111;

Staff Status: Indicates if this user can access the administrator site;

Role: Non-super user needs to select a role. By selecting a preset role configuration, this user will have the levels configured for the role.

2. After editing, click [OK] to complete user adding, and the user will be shown in the list.

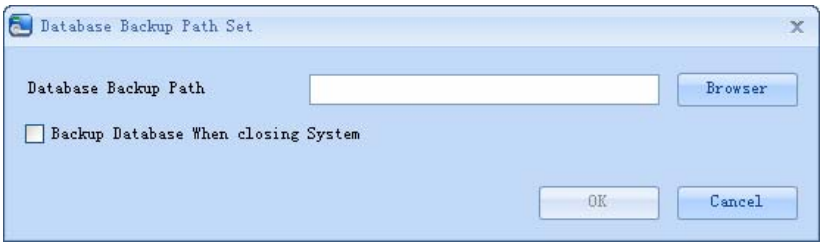
To modify existing user, click [Edit] behind the user name, and enter edit interface. After modification, click [OK] to save and return.

8.2 Database Management

The homepage of the system shows database backup history. The system allows database backup, restoration and initialization.

8.2.1 Database backup path configuration:

Click [System] - [Database Management] - [Database Backup Path Set], the edit interface appears：



Click [Browse] to select the backup path, click [Save] to save the selection and quit.

Notes:

(1) In software installation process, it will prompt to set the database backup path. If you haven't set the backup path, the operation of backup database can't be executed (The server for other computer to access, need to set the backup path in the server firstly).

(2) Proposal that the database backup path and the present system installed path not be under the same disk. Don't set the path to the root of a disk or desktop.

8.2.2 Backup database:

Periodically backup the system's database to ensure data security. To use the backed up data, just restore the data.

[System] - [Database Management] - [Backup Database]

✍ **Note:** We recommended backing up the database after you create the personnel file, device information or part of access control level settings.

8.2.3 Restore Databases

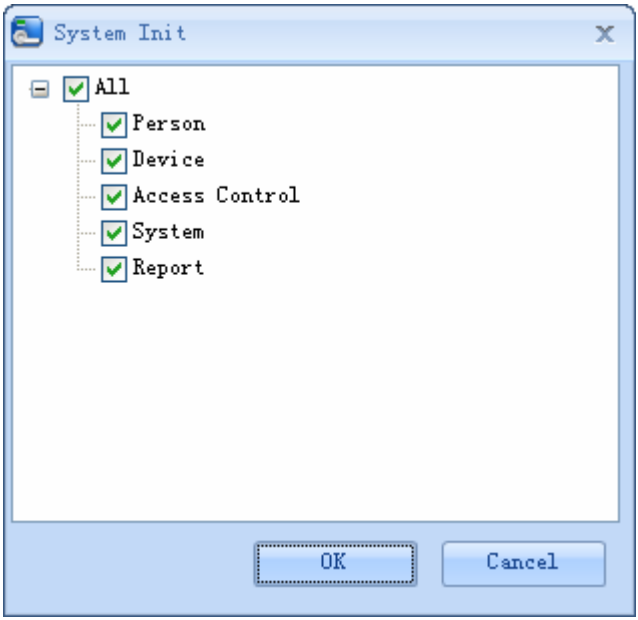
Click [System] - [Database Management] - [Restore Databases], [Open] to select a successfully backed up database from the backup database list. In the pop-up Windows, click [Yes] , system can be restart, it begin database restoration in process.

✍ **Note:** Don't close any command window prompt during the database restore process.

8.2.4 Initialize database

Initialize database is to restore data to system initialization status. Initialized data in the database will be deleted. Please operate with care.

Click [System] - [System Initialization]to enter edit interface, select one or several data-sheets to initialize, and click [OK] to complete initialization and return.



For example:

Select to initialize access level: After selection, it will initialize access control time periods, access control holidays and access levels. All contents on these three pages will restore initial status;

Select to initialize Person: After selection, it will initialize data of Department, Personnel, Issue Card, and only reserve system default settings;

Select to initialize Device: After selection, it will initialize all device information in the system (including access control). If the device is an access control panel, corresponding device parameters and door information will be deleted;

Select to initialize Access Control: After selection, it will initialize Interlock, Anti-passback, Linkage settings, First-Card Normal Open and Multi-Card Opening (including Multi-Card Opening Personnel Group Setting), Access Control Time Zones, Holidays and Access levels. All data will be restoring initial state.

Select to initialize System: After selection, it will initialize Role, User etc., and only reserve system default settings;

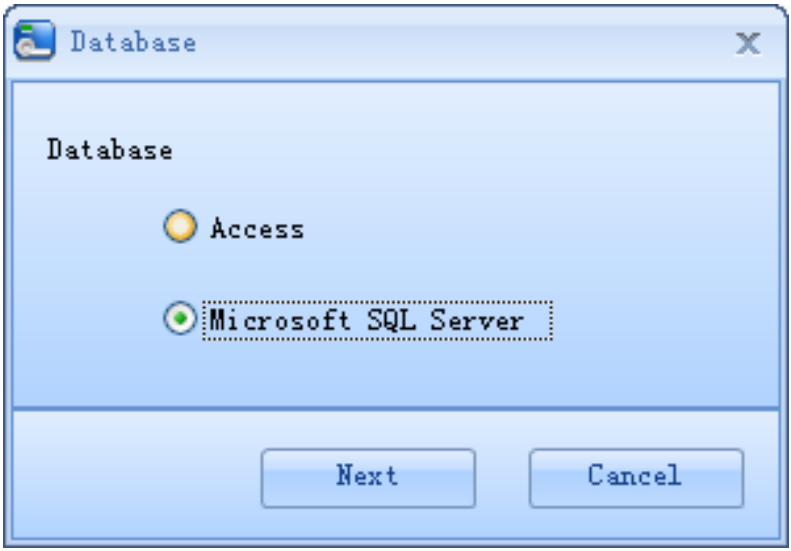
Select to initialize Report: After selection, it will initialize all events records.

✍ **Note:** If the device is still in normal use, please initialize database cautiously, especially when involving access level-related departments and personnel, access levels, door settings, areas, devices, users and roles. It is recommended that if there are still devices in use after database initialization, the user shall [Synchronize all data] for the setting to avoid unexpected errors.

8.2.5 Set Database

This Function mainly used for database change. Software database is MS Access by default. If need change to MS SQLServer database, firstly, you should establish the empty database on the database server. You can find a script file with the name of sqlserver.sql in the directory of installing CD. The empty database establishes in the front of the searcher of SQL Server, and then opens the sqlserver.sql script files, to run database that is to create this software.

Click[System] - [Database Management] - [Database Connection] to enter following interface, select corresponding database and click [Next]，Microsoft SQL Server is a good point case. And then fill in database relevant information, click [OK], whether restart device that popup in the box select [Yes]. After restart can be change database.

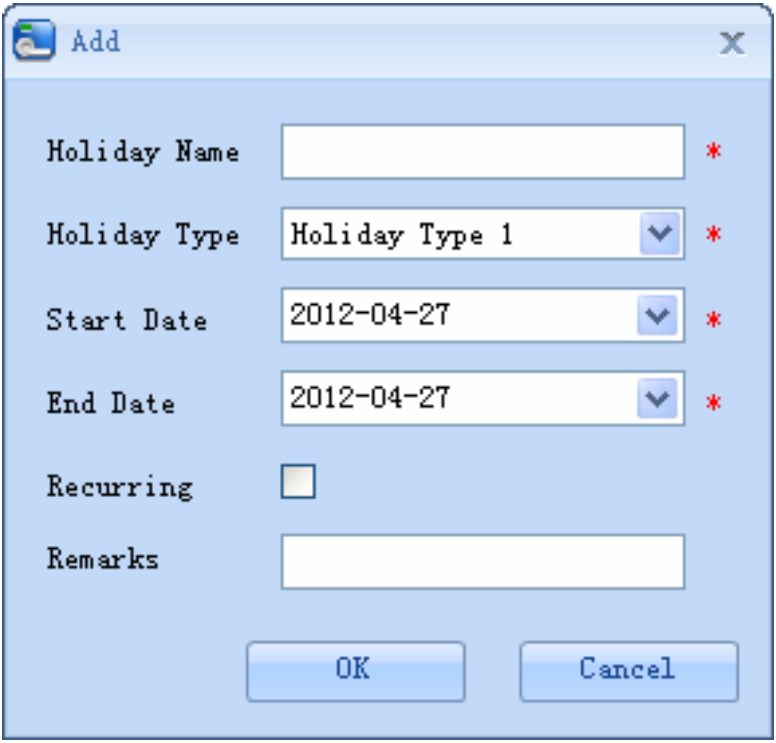

Database
Database
Access
Microsoft SQL Server
Next
Cancel

9. Appendixes

Appendix 1 Common Operation

1. Select date

Click [Access Control System] - [Holidays] - [Add] to enter edit interface:



You can click the pull-down menu to select date. Click on year to activate the scroll button for year selection, and click or button to select an earlier or a later year. Click or button to select an earlier or a later month, and click the desired date. Also can directly to edit Year or Month in editing box.

2. Import (taking importing personnel table as an example):

If there is an electronic personnel file, which may be the information of the personnel or access control, attendance or human resources system of another brand, you can import it into this system through the [Import] function.

(1) Click [Import] to show the import edit interface:

Description of items:

Import file: Click [Browse] to select the file to be imported;

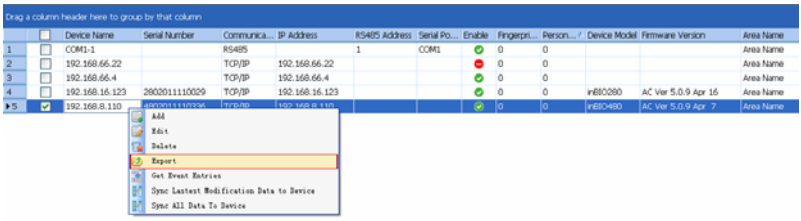
File format: Select the format of the file to be imported;

Choosing corresponding import field, >> means select all, > means single selection, < means cancel the mouse options, << and means deselect all.

Note: When importing personnel table, if there is no personnel number or personnel number is “0”, the import operation can’t execute. If you need import the personnel gender, please use “M” represent male and “F” represent female, then execute import operation.

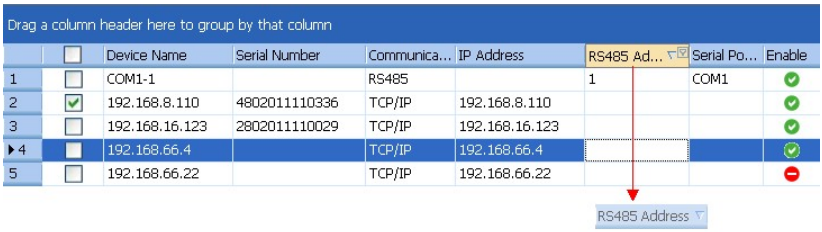
3. Export data (taking exporting "device" as an example):

(1) Click [Device]-[Device],select any equipment, and then right click [export] to show the edit interface:

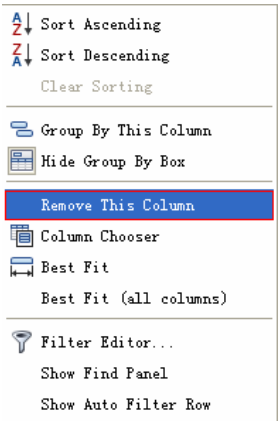


If Export, users can according to requirement, Export a part of the field, with no need for hide. There are two ways to hide as below:

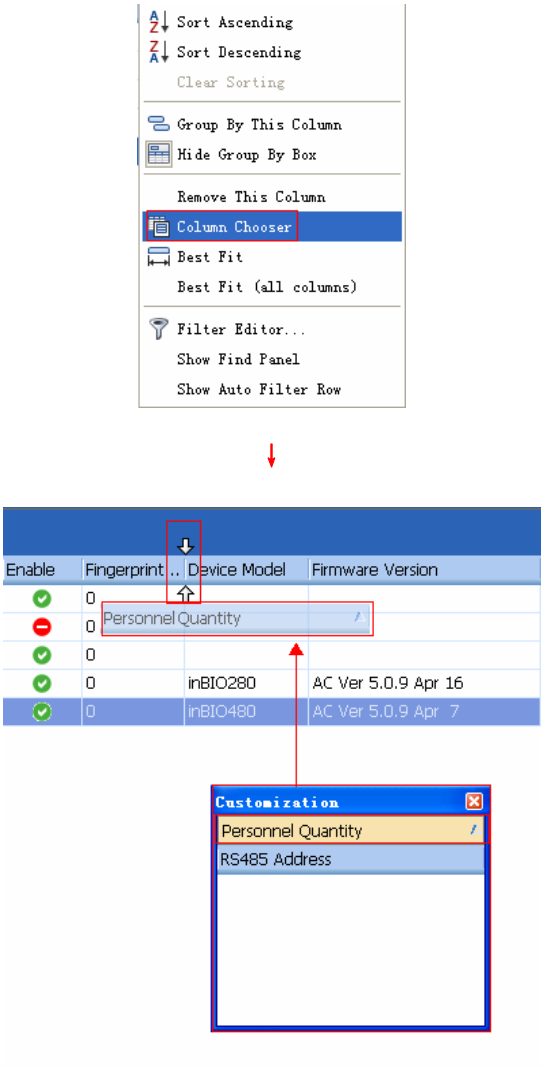
① Choose not need to Export items, left-click mouse drag down field release the mouse button can hide.



② Right-click and select [Remove This Column] can hide.



Note: If need to show the hidden field , can put the mouse on the list head, right-click select [Column Chooser] in popup menu, it will displayed "customization field box " at interface lower right corner, and then Drag reductive field to the list head



(2) Select the format of exported file: If PDF format is selected there will be no file code option (namely, no differentiation between Simplified and Traditional Chinese). Click [Export] to directly show the exported file.

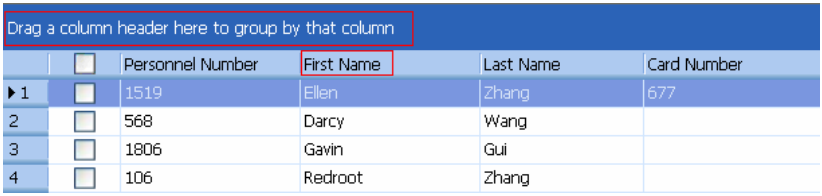
If TXT or EXCEL format is selected, then file codes include Simplified and Traditional Chinese, but Traditional Chinese code can be completely exported only in the operating system in Traditional Chinese. The system prompts Open or Save.

Notes:

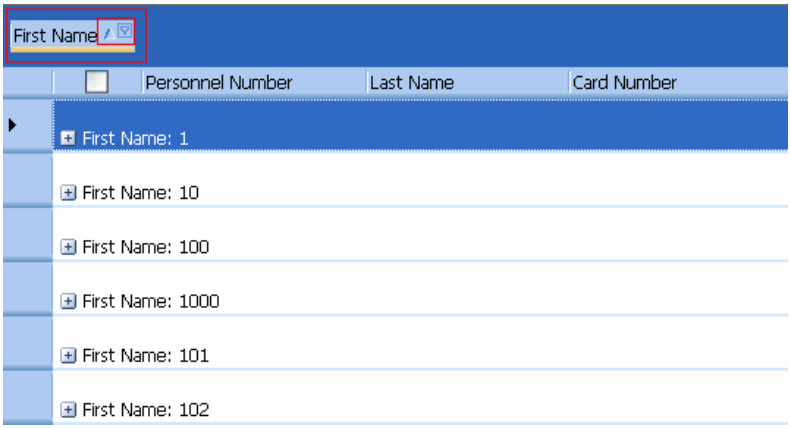
(1) When importing department table;

(2) Exported table is the list currently shown.

4. The use of data list (taking "Personnel" as an example):

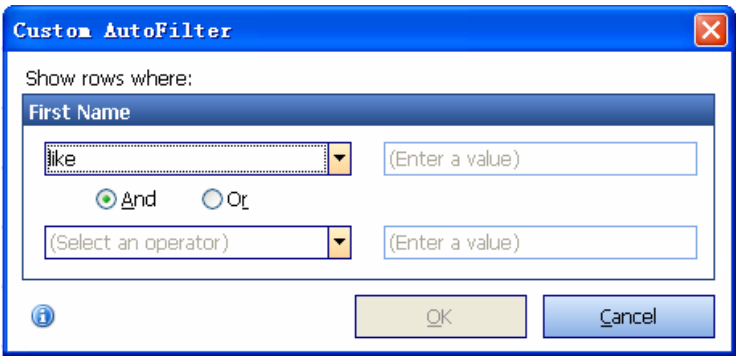


List as above, can take list head drag down to "Drag a column header here to group by that column", process grouping operation as below:

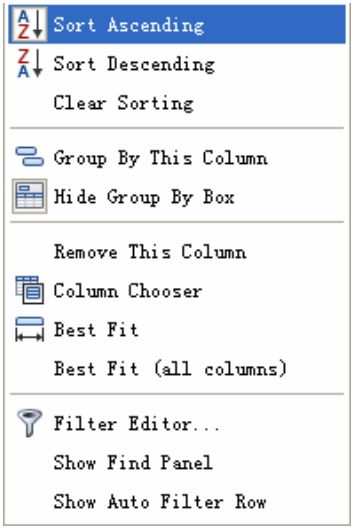


Also can put mouse to icon  at list head, the icon will turn into  , and then

click , select "Custom Auto-filter", according to the conditions for search operation as following:



Fill in the corresponding inquires can search relevant conditions. Also can put mouse to list head, right-click popup menu as below, and then process Sort Ascending, Sort Descending, Group By This Column function etc,.



Appendix 2《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.

Appendix 3 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: What is the use of blacklist?

A: A blacklisted personnel can not achieve departure restoration, namely, this person can not be employed by the Company any longer. To modify, just modify departure information on the departure interface.

Q: How to adjust the department of a person?

A: There are the following ways to adjust personnel department:

1. In personnel list, click personnel number or click "Edit" menu to show personnel details, and modify personnel department in the department item;

2. In personnel list, check the personnel requiring department adjustment, click "Adjust department", and a dialog box will open, then modify the department;

3. On personnel transfer interface, click Add to open the edit interface, select personnel, and check department in the transfer field, and complete other information, thus completing transfer.

Q: How to set access levels for visitors?

A: Setting access levels is as follows:

1. In the system, add these personnel, and enter relevant information;

2. Select access levels suitable for them. If there are no suitable levels, it is required

to enter the access control system to add relevant settings;

3. Set valid time, namely, the start and end dates when they need to use access levels.

Q: What are the ways to cancel personnel access control settings?

A: There are the following ways to cancel personnel access control settings:

1. Close access control only: In the personnel list, click personnel number or click “Edit” menu to show personnel details, and delete access levels and Personnel Group of Multi-Card Verification in access control settings;

2. Delete personnel: In the personnel list, tick the personnel and click “Delete” to delete this person from the system. Corresponding access control information will be deleted;

3. In “Personnel access levels settings”, delete access levels of personnel, and in “Personnel Group of Multi-Card Verification”, delete Multi-Card Opening levels.