

Access Control Software Manual

CONTENTS

1. Function overview.....	1
2. Installation environment.....	2
3. Concept description.....	3
4. Installation and Uninstallation	4
4.1 Installation	4
4.2 Uninstallation.....	10
5. Function introduction.....	11
5.1 Add device	11
5.2 Department management.....	16
5.2.1 Add department.....	16
5.2.2 Modify department's name	18
5.2.3 Modify administrative subordination relationship.....	19
5.2.4 Delete department.....	20
5.3 User management.....	21
5.3.1 Add user.....	21
5.3.2 Modify employee's information	22
5.3.3 Enroll fingerprint through fingerprint device	24
5.3.4 Enroll the fingerprint through fingerprint reader.....	29
5.3.5 Upload & download user's information and fingerprint.....	32
5.3.6 Data import & export through U disk.....	36
5.4 Privilege management	38
5.4.1 Time zone setting	39
5.4.2 Management of access control group	43
5.4.3 Group setting.....	45

5.4.4 Unlocking combination setting	47
5.4.5 Holiday setting	49
5.4.6 User's specified privilege.....	51
5.5 Report.....	57
5.5.1 Monitor record report	57
5.5.2 Alarm report.....	58
5.6 Device management	60
5.6.1 Read information from fingerprint reader.....	60
5.6.2 Communication setting.....	60
5.6.3 Wiegand.....	61
5.6.4 Verification.....	63
5.6.5 Power management	64
5.6.6 Access control	65
5.6.7 Mifare.....	65
5.6.8 Other settings	66
5.7 System management.....	69
5.7.1 Build database.....	69
5.7.2 Set database.....	70
5.7.3 Database management	71
5.7.4 Operator management.....	74
5.7.5 System parameter setting	76
MSDE installation.....	81
6. Appendix	82
6.1 Connection of access control machine and system.....	82
6.1.1 Connection through RS232.....	82
6.1.2 Connection through RS485	86
6.1.3 Connection through TCP/IP.....	90
6.2 Real-time monitor	94

6.3 Map	96
6.4 License to detect the fingerprint device	99
7. Solution to problem.....	102
8. SOFTWARE USE LICENSE AGREEMENT	104

1. Function overview

Access control is a device system supervises in-and-out passage. It is mainly used to authorize in-and-out personnel and record their process. Access control software can set in-and-out privilege easily and manage the personnel effectively.

Access control software is applicable for access control machines of various modes. It can connect a number of access control machines working at the same time and monitor in-an-out personnel at the real time.

Refer to the following for detailed functions:

- I Manage personnel's basic files and record personnel's basic information
- I Provide various database interfaces.
- I Upload and download personnel's information
- I Control personnel's in-and-out time zone .
- I Monitor in-and-out state with machines connected with network.
- I Download records from fingerprint reader regularly.
- I Operator sets up the system to ensure security.
- I Query in-and-out record & alarm record and export the data in various formats.
- I Detect the positions where access control devices lie in the way of map.
- I Control access control machine remotely, initializing machine and operating machine synchronously.
- I Group the devices or carry out subarea management.
- I Manage personnel's privileges in group.

2. Installation environment

Computer: above Pentium I66, more than 64M Memory, at least 100M hard disk space

Operation system:

Microsoft Windows 2000 or Microsoft Windows XP

Windows 2000 operation system is suggested and Pentium III 500+128M computer is the least requirement.

3. Concept description

Machines connected with network, and real time monitor: either connected with Ethernet or 485, fingerprint reader can be added to the management software to execute management. After adding all the fingerprint readers, click “Monitor”, and the monitor starts in turns.

Record the monitoring information at the real time: able to monitor the fingerprint identification records and going-out button records on each fingerprint reader and save these records to the database for later query.

Query record: able to query the records when they are enough. While querying, a variety of conditions are specified, such as fingerprint reader identification, time zone , and department and so on.

Privilege management: add and modify user’s privilege on each fingerprint reader and upload the information to the reader.

Department management: add and modify departments’ information.

User management: download user and his fingerprint. Modify user’s information and privilege. Add code for user. Add user and upload user and his fingerprint by using U are U.

Open the door remotely: press “Open” button to open the selected door remotely.

Synchronous time: reader’s time agrees with computer’s time.

Upgrade firmware: upgrade reader’s running program.

Initialize fingerprint reader: able to initialize the fingerprint reader during device management

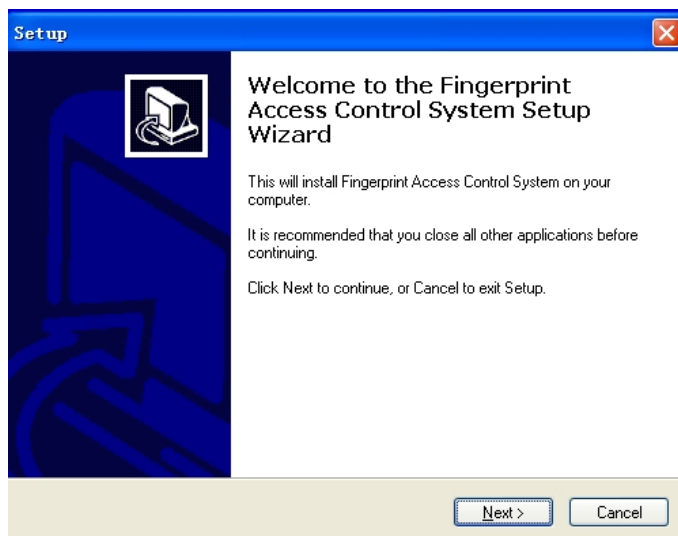
4. Installation and Uninstallation

4.1 Installation

Before installation, other running programs are suggested to be closed to avoid conflict.

Notice: The displayed picture may seem different from the actual content in the compact disk. If so, the contents in the compact disk prevail.

Put compact disk into CD driver, and the installation program will run automatically.



Picture 4-1 Select using method

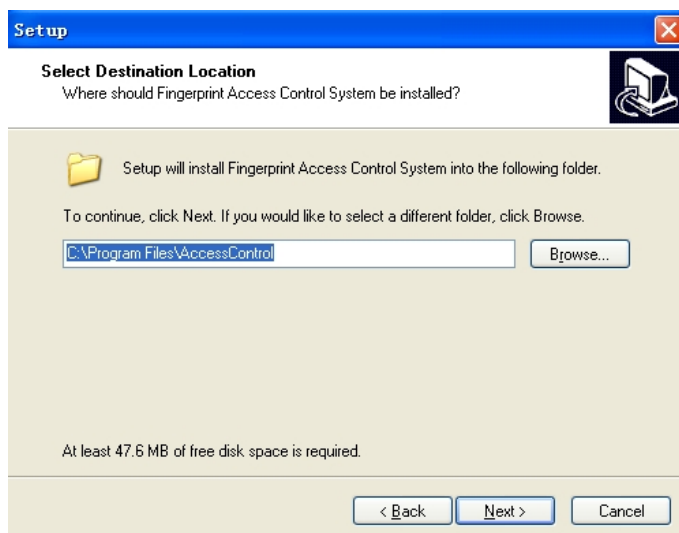
Tip: Select **【Cancel】** button in the window of installation program, installation can be cancelled.

- 1) A dialogue box of End User Software License Agreement will be shown later, as in picture 4-2. Select **【Agree】**, and click **【Next】**.



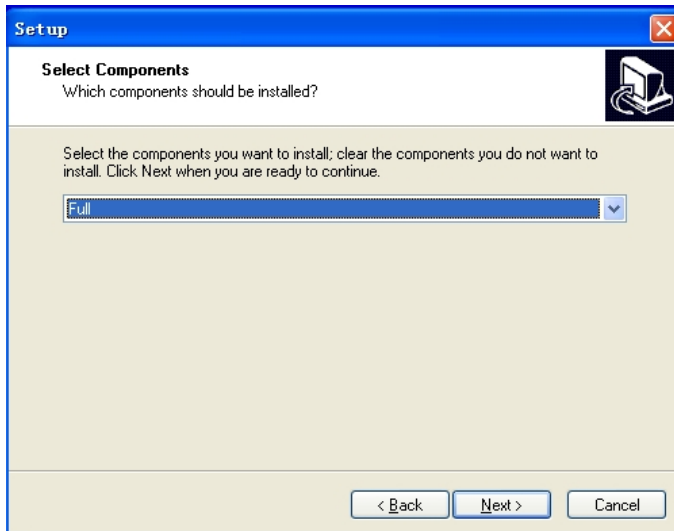
Picture 4-2 End User Software License Agreement

- 2) The installation path will be shown in later dialogue box, as in picture 4-3. You can select your desired path and click **【Next】**.



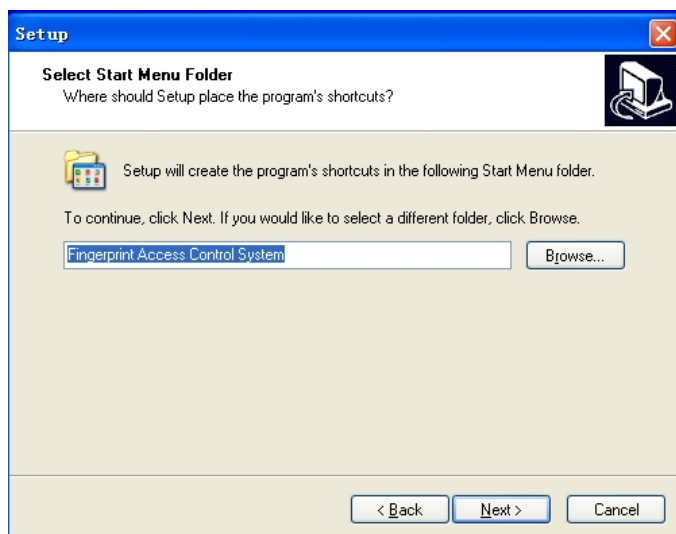
Picture 4-3 Select installation position

- 3) You will be asked to install what kinds of components in the next window, as shown in picture 4-4. All components are suggested to be installed. Then click **【Next】**



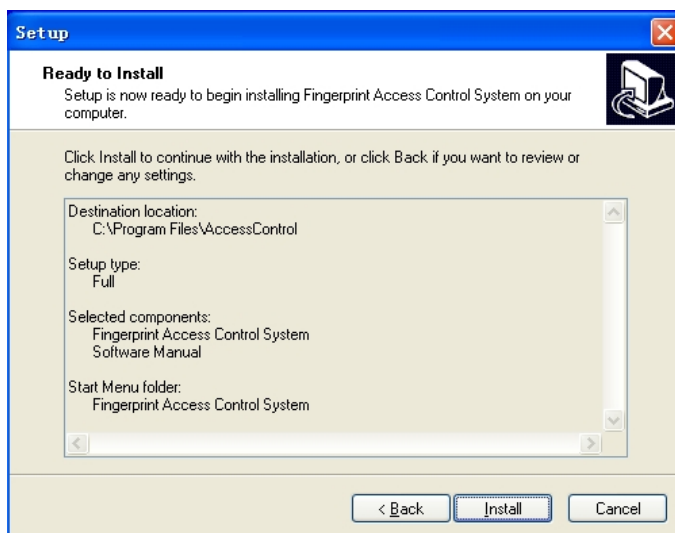
Picture 4-4 Select installation components

- 4) The position where shortcut is created will be shown later, as in picture 4-5. You can select your desired position and name and click **Next** .

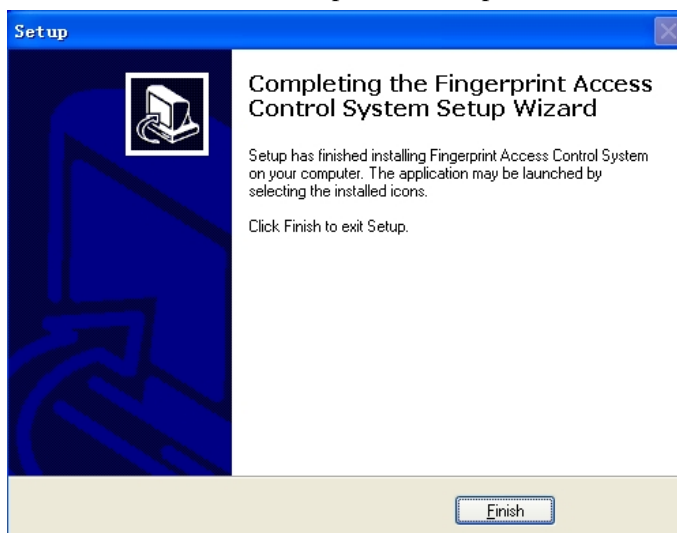


Picture 4-5 Select shortcuts' position

Then installation path and mode will be shown, as in picture 4-6. Click **【Installation】** to start copying files. In the end, a dialogue box indicating installation completed appears, as shown in picture 4-7. Click **【Finish】** , and the whole installation is over.



Picture 4-6 Installation path and components show



Picture 4-7 Installation complete

4.2 Uninstallation

If you don't want to preserve this software in Window, you can operate as the following steps:

- 1) Close access control software.
- 2) Enter **【My Computer】**, enter **【Control Panel】** with double clicks.
- 3) Enter **【add/delete program】** window with double clicks, select **【Fingerprint Access Control Management System】**, and click **【delete】**, then start uninstallation according to the tips.
- 4) The above processes cannot delete all the files related with this software. It is necessary to enter the installation catalog to delete access control's folders.

5. Function introduction

5.1 Add device

【Function Introduction】 To achieve real time monitor, data upload & download, remote open and other functions, the software needs communication connection between fingerprint and software. It only needs to add and save the device communication parameters to the system during the first employment.

【Operation Steps】

1. Two methods to enter access control system:

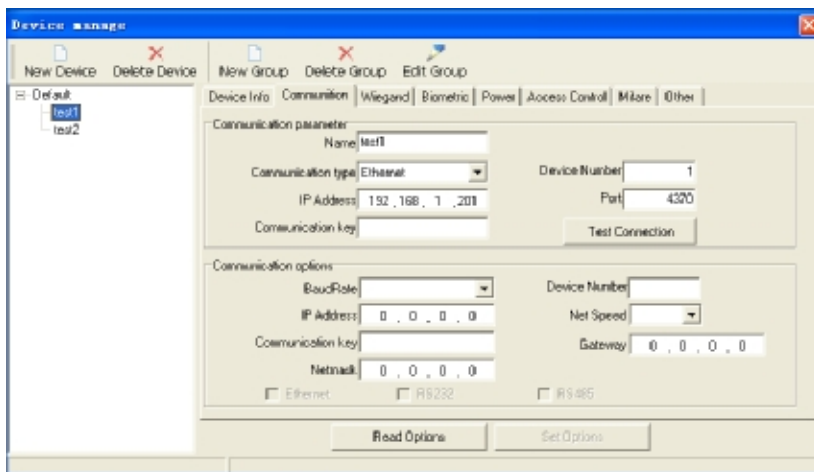
1) doubly click shortcut “Fingerprint Access Control Management System”

2) Click menu: start->program->fingerprint access control management system->fingerprint access control management system

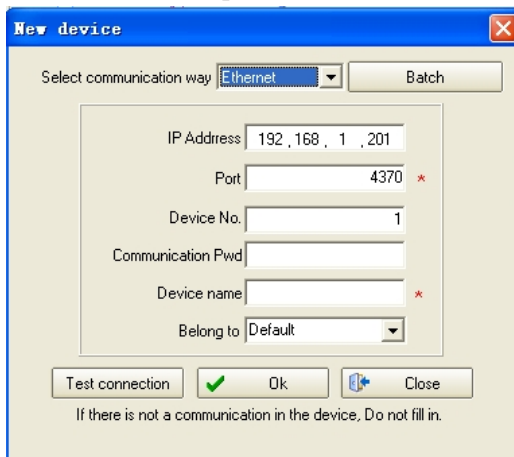
2. Method to enter device management and add machine:

Click menu: access control management->equipment management.

Shortcut key F2

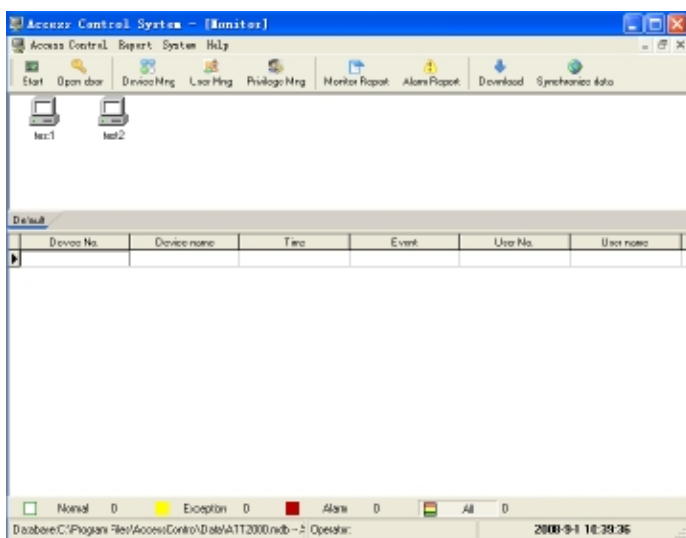


3. Click “add device”, a window will appear, as shown in the following picture. The system supports RS232/485 and Ethernet communication. Refer to the appendix for specific connecting methods. After setting connecting parameters, click “test connection” to verify the connection. If you want to add a number of devices once, please click “batch add”.



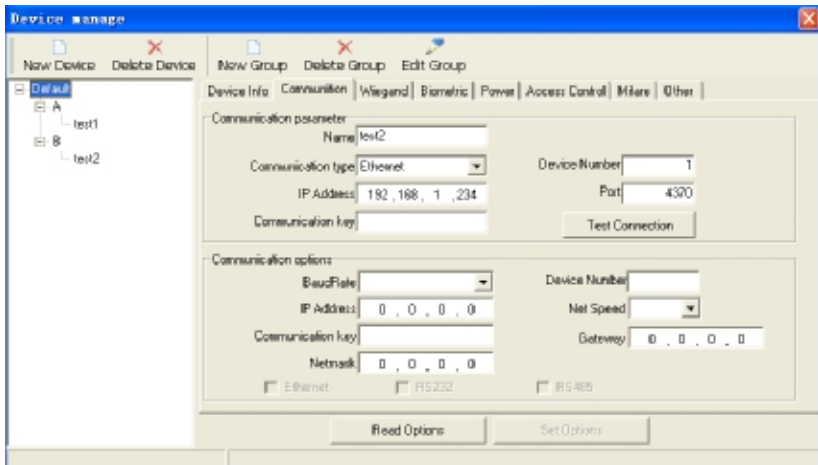
4. Click “OK”, the machine will be listed in the form of machine name. The privilege side shows the machine’s communication parameters.
5. After exit from the device management window, you can catch sight of the device’s icon shown on the program’s main interface, as in the following picture. The device’s connecting parameters will be preserved in the system. If you want to operate the device, you can only click its icon.

Tip: Click the right key of the mouse, and you can see a shortcut menu which shows the related operation items.

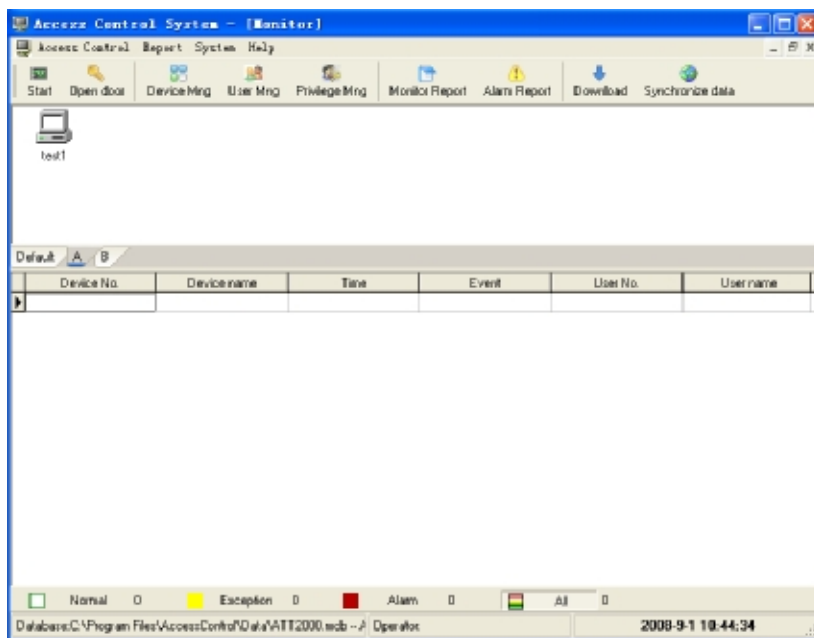


6. Device classification: Device classification means setting up subarea of the device or carrying out group management. Click “add classification” on the main interface of the device management, open the window to add classification, input related names, save and exit. Then drag the device to the related groups

on the management interface.



Different classifications and their devices can be seen on the interface of monitor center, as shown in the following picture.

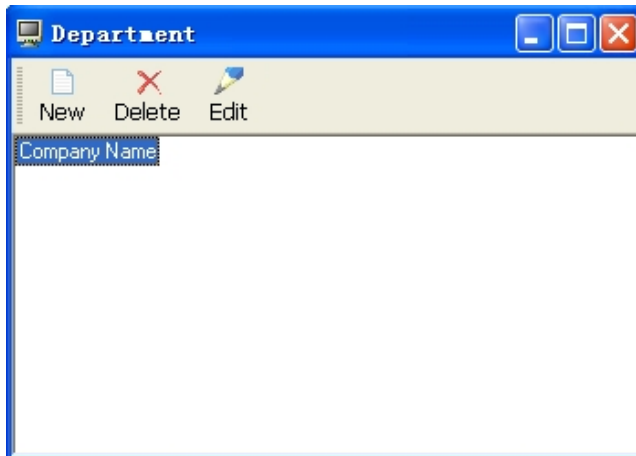


5.2 Department management

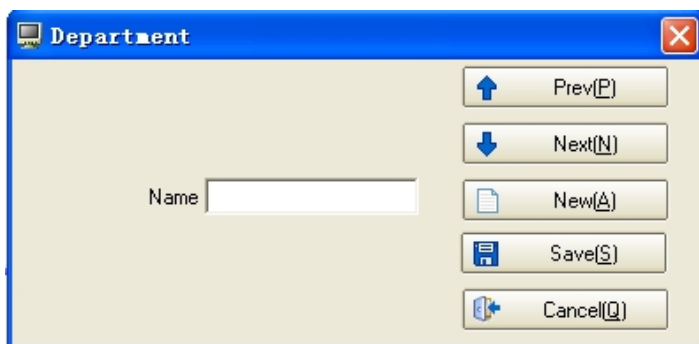
5.2.1 Add department

【Operation Steps】

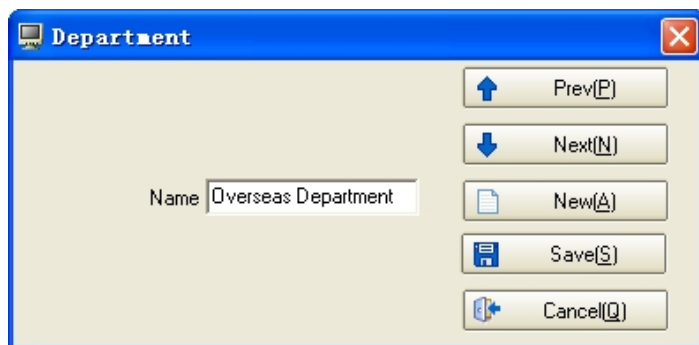
1. Enter “department management” interface, click menu: access control management->department management, as shown below:



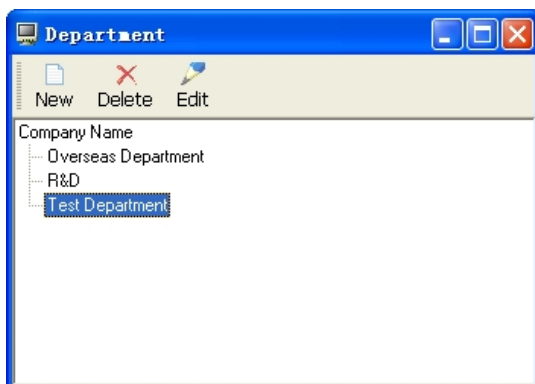
2. The company's name can enter: system management->system parameter setting, to modify company's information.
3. Click “add” to add department, and input the department's name, as shown below:



4. If a number of departments need to be added once, input one department's name, click "save and add", and input another department's name, as shown below:



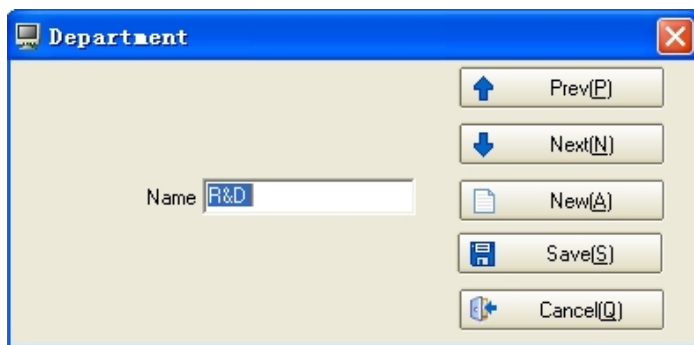
5. After inputting department's name, click " save and exit", thus the department is added to the list, as shown below:



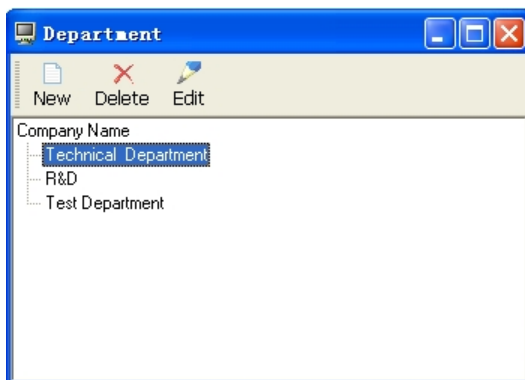
5.2.2 Modify department's name

【Operation Steps】

- 1、 Select the department which needs modification and click “modify”, modify the name on the modification interface.



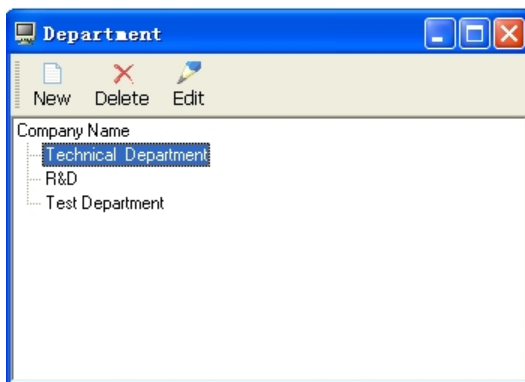
- 2、 After modification, click “ save and exit”, as shown below: “Overseas Department” has been changed into “Technical Department”.



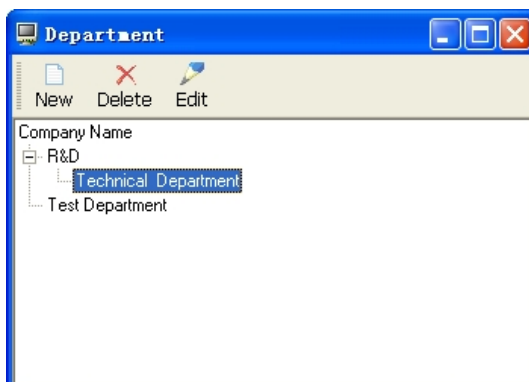
5.2.3 Modify administrative subordination relationship

【Operation Steps】

- 1、 Select the department which is to be dragged by clicking left key of the mouse, as shown below:



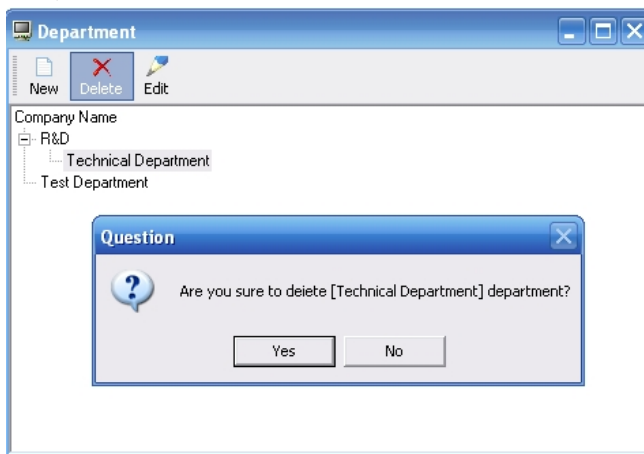
- 2、 Drag the department to target position, as shown below:



5.2.4 Delete department

【Operation Steps】

Select the name of the department which is to be deleted, click “delete”, and select “yes” or “no”, as shown below:



Notice: If a department has recruited employees, or there is subordination department under a department, then the department cannot be deleted.

5.3 User management

5.3.1 Add user

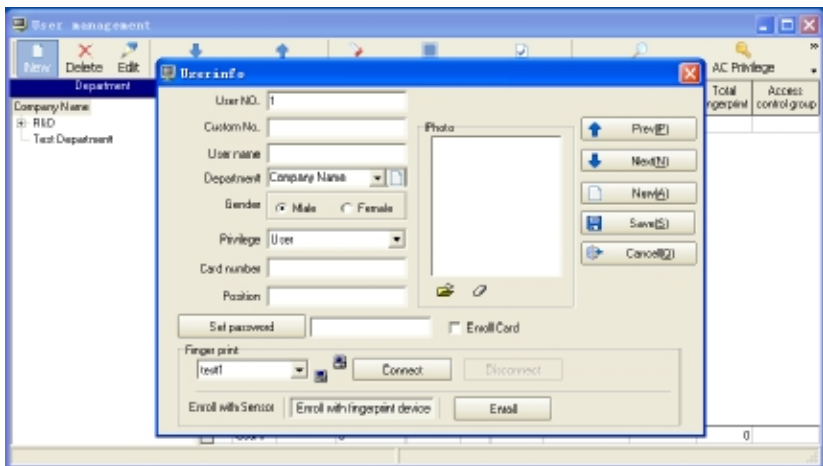
【Operation Steps】

1.Method to enter interface of “user management”:

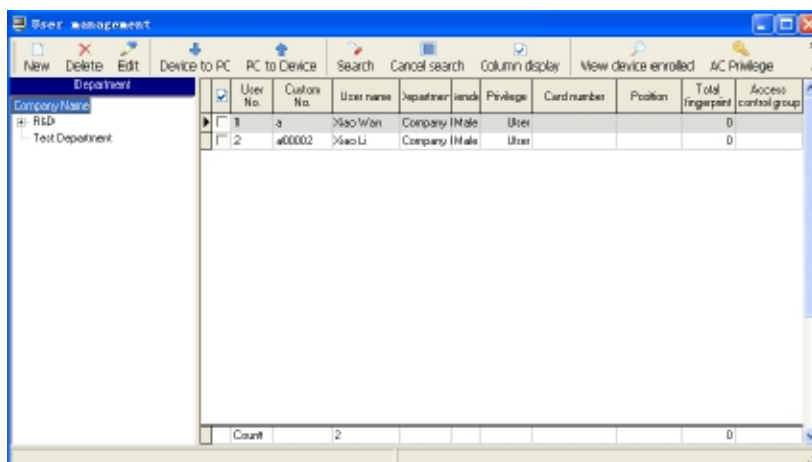
Click menu:: access control management->user management

shortcut key F4

2.Click “add”, add new user, as shown below. Input user’s number, name and so on, click “save and exit”, or click “save and add” to add another employee’s information.



3. Then the added user’s information will be shown on the management interface.



5.3.2 Modify employee's information

【Function introduction】 Set user's photos, subordination department, fingerprint enrollment and so on. The fingerprint reader supports Chinese display but does not support Chinese input. If you need to display the name on the reader, you can download user's information from the reader to the software. After the name has been changed into Chinese, upload it to the reader.

【Operation Steps】

1.Method to enter "user management":

Click menu: Access control management->user management

Select employee: select user in "user list", click "modification", and modify user's information on the pop-up interface, as shown below:

The screenshot shows a Windows-style dialog box titled "Userinfo". It contains the following elements:

- User NO.:** Text box with "1".
- Custom No.:** Text box with "a00001".
- User name:** Text box with "Xiao Wan".
- Department:** Text box with "Company Name" and a document icon.
- Gender:** Radio buttons for "Male" and "Female" (selected).
- Privilege:** Dropdown menu with "User".
- Card number:** Text box.
- Position:** Text box.
- Photo:** A large empty rectangular area with a "Get from files" icon (folder with a magnifying glass) below it.
- Buttons on the right:** "Prev(P)", "Next(N)", "New(A)", "Save(S)", and "Cancel(Q)".
- Buttons at the bottom left:** "Set password" and a text box.
- Enroll Card:** A checkbox.
- Finger print section:** A dropdown menu with "test1", a "Connect" button, a "Disconnect" button, and an "Enroll" button.

3. Add picture: the system support directly selecting photos from files. Click “obtain from files”, enter the dialogue box of image file select, select an image file, click “open”, and the image file will be added successfully, as shown below:

The screenshot shows a window titled "Userinfo" with a blue title bar. It contains several input fields and buttons for user management. On the left, there are fields for "User NO." (value: 1), "Custom No." (value: a00001), "User name" (value: Xiao Wan), "Department" (value: Company Name), "Gender" (radio buttons for Male and Female, with Female selected), "Privilege" (dropdown menu showing User), "Card number", and "Position". To the right of these fields is a "Photo" section containing a grayscale image of a woman. Below the photo are icons for a folder and a pencil. On the far right, there is a vertical stack of buttons: "Prev(P)" with an up arrow, "Next(N)" with a down arrow, "New(A)" with a document icon, "Save(S)" with a floppy disk icon, and "Cancel(Q)" with a plus icon. At the bottom left, there is a "Set password" button and a text field. To its right is an "Enroll Card" checkbox. Below these is a "Finger print" section with a dropdown menu showing "test1", a "Connect" button, and a "Disconnect" button. At the very bottom, there are three buttons: "Enroll with Sensor", "Enroll with fingerprint device", and "Enroll".

5.3.3 Enroll fingerprint through fingerprint device

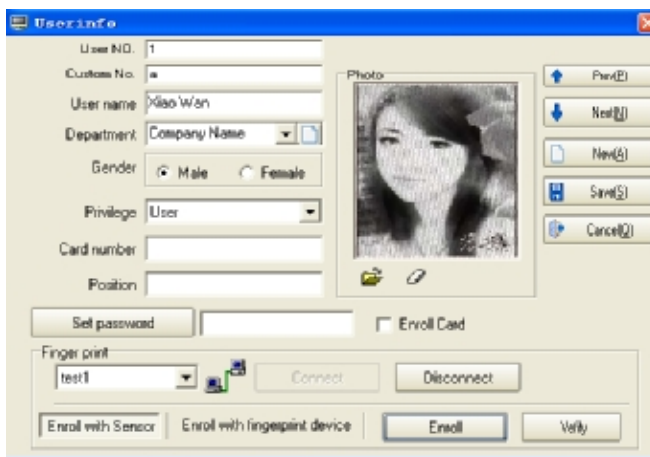
【Function Introduction】 Collect user's fingerprint and preserve it in the database. After fingerprint enrollment, please upload fingerprint information to the specified reader.

【Operation Steps】

1.Method to enroll fingerprint through fingerprint device:

Click menu: access control management->user management

2.Click "add", add new user or select user in user list and click "modification".



3. Select “enrollment with sensor”, click “enroll”, and enter the fingerprint enrollment interface, as shown below:



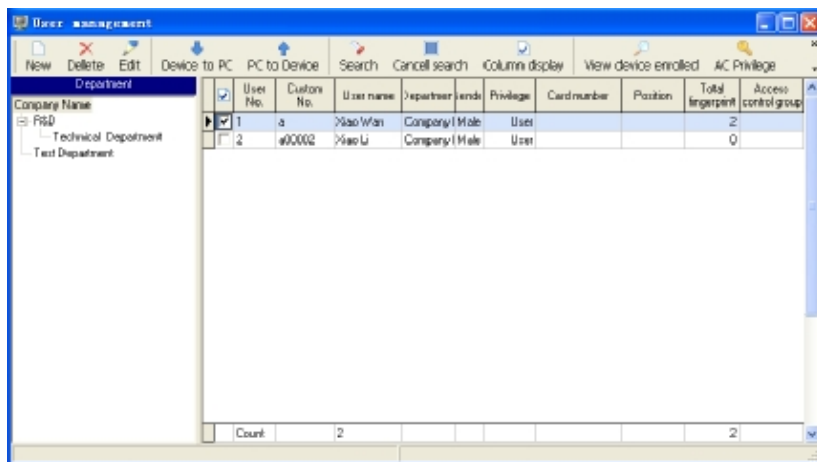
4. Click the finger whose fingerprint is to be enrolled, and the system enters a state to receive enrollment, as shown below:



5. After the finger finishes its press on the fingerprint collecting device, the system enters the following state shown in the picture:



6. Press 3 times with the same finger according to the tips, click “yes” after successful enrollment, return to user’s information editing interface, and click “save and exit” as shown below:



7. Fingerprint verification: select “enrollment with sensor”->click “verification”, the following interface will appear to check if the fingerprint enrollment is done or not.



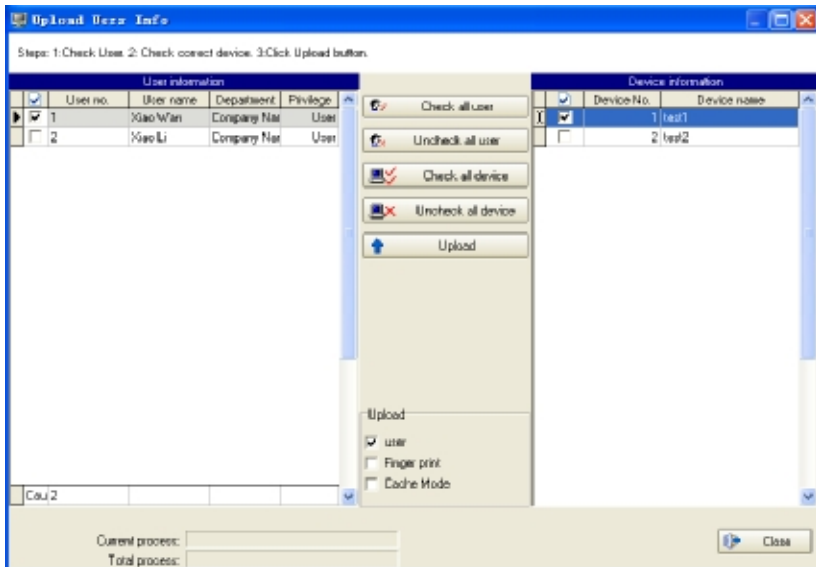
9. Press the finger on the device, if the following dialogue box appears, then the enrollment failed, please return to step 3-6 for another enrollment.



10.The enrollment succeeds if the following dialogue box appears.



11.After enrollment, click “upload user’s information” on user management interface, and upload the user’s information and fingerprint to specified device after entering the following interface:



12. You can select “Cache Mode” to upload user’s information. In this way, if the transmission fails, the entire user’s information won’t be uploaded to the device, or the user’s information will be uploaded to the device before the transmission fails.

5.3.4 Enroll the fingerprint through fingerprint reader

【Function Introduction】 Enroll fingerprint directly on the specified fingerprint reader. After enrollment, the information has been preserved into the reader and the local database. Therefore, there is no need to upload fingerprint data to the enrolling fingerprint reader.

【Operation Steps】

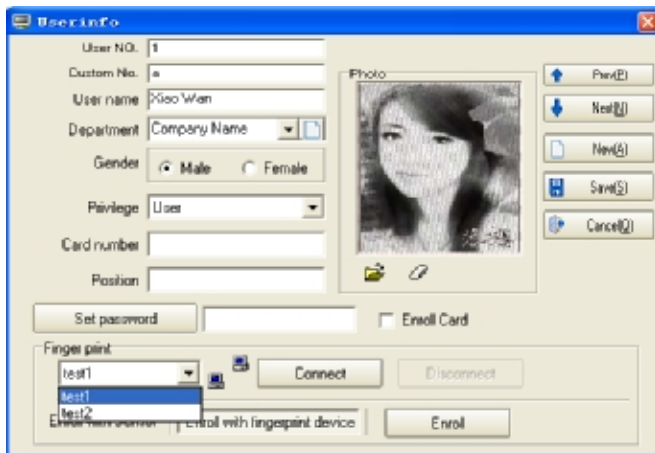
1. Method to enroll fingerprint on fingerprint reader

Click menu: access control management->user management

2. Click “add” in user list, add new user or select user in user list and click “modification”, then enter user’s information editing

interface.

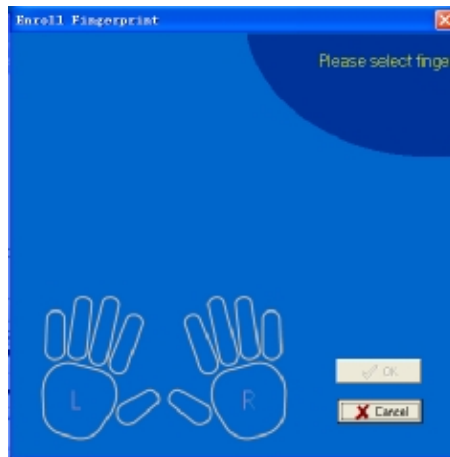
3. Select reader's name, as shown below:



4. Click “connect device” to connect fingerprint reader, as shown below:



5. Click “enrollment” to enter “fingerprint enrollment” interface, as shown below:



6. Click the finger whose fingerprint is to be enrolled, and the system enters a state to receive enrollment, as shown below:



7. Place your finger on the reader according to the tips, as shown below:



8. Press 3 times with the same finger according to the tips. If the enrollment is successful, the following picture will appear. If failed, please repeat the operation of step 6-8 until successful.

5.3.5 Upload & download user's information and fingerprint

5.3.5.1 Download user from device

【 Function Introduction 】 Download user's information and fingerprint data in reader to the computer. The information modification can be done through this way.

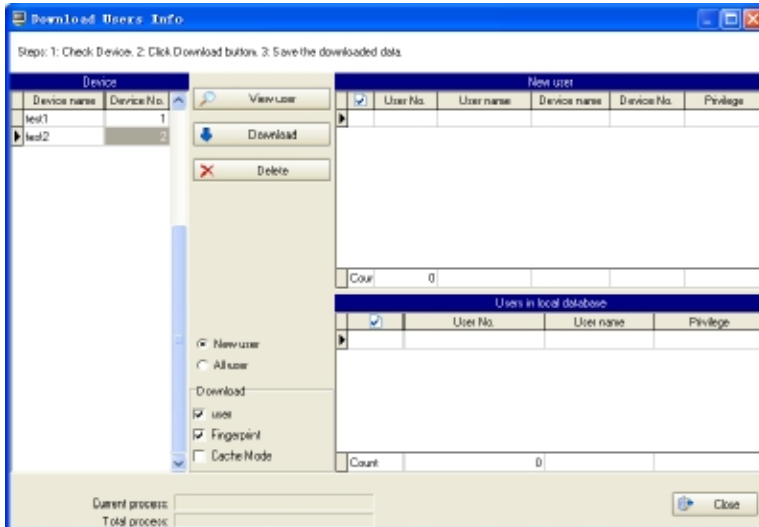
【 Operation Steps 】

1. Method to enter "download user from device":

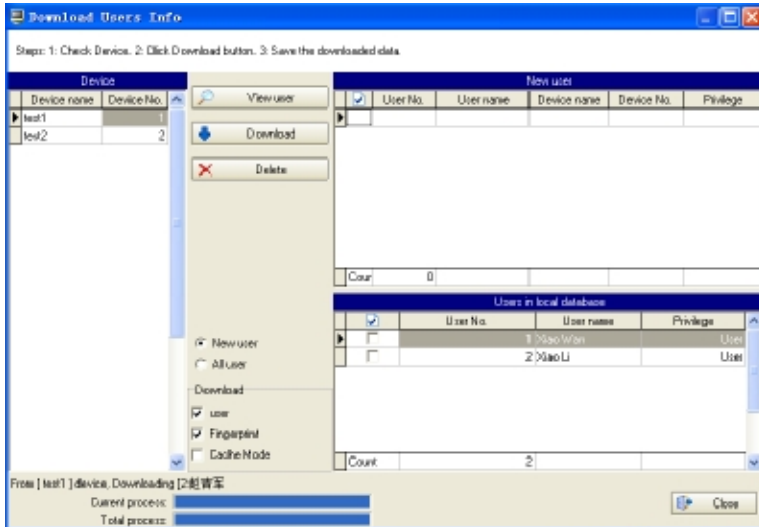
Click menu:: access control management->user management, and select "download from device"

2. Enter "download user's information" interface as shown below. All the readers in this system will be shown in the device information form. Select the target reader, as shown in the following picture:

Notice: Select "user's information" and "fingerprint information"



3.Download user's data. Click "download" to download user and fingerprint data. The system will automatically preserve user's information and fingerprint data to the database.



5.3.5.2 Upload user's information

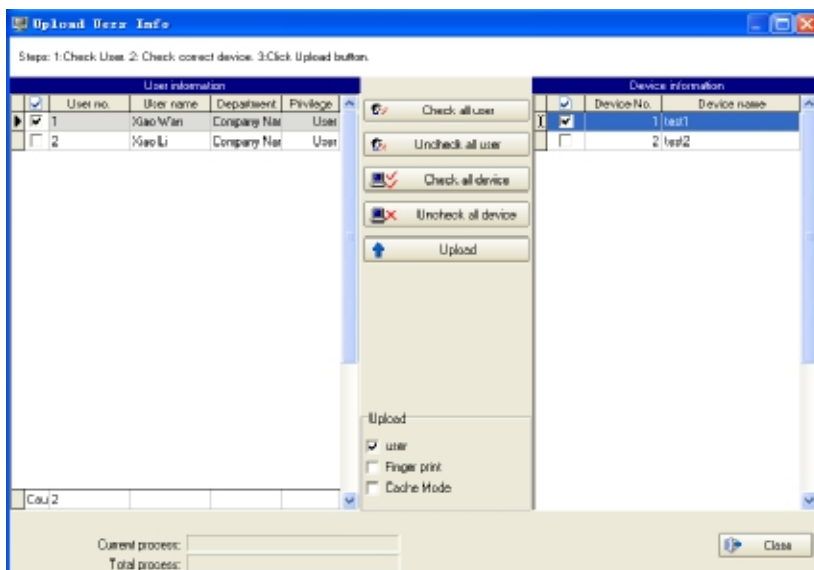
【Function Introduction】 Upload user's information and fingerprint data in computer to the fingerprint reader. The modification of user's information in reader or uploading user's fingerprint to the reader can be achieved in this way.

【Operation Steps】

1. Method to enter "upload user's information":

1) Click menu: access control management->user management, select "upload user's information"

2. Enter "upload user's information" interface, as shown below:



3. Select employee and fingerprint reader, and click “upload” to upload information. You can select “high speed mode” to upload user’s information. In this way, the user’s information can be uploaded wholly. If transmission fails, the entire user’s information won’t be uploaded to the device, or the user’s information will be uploaded to the device before the transmission fails.

Notice: Select user’s information or fingerprint data to upload user’s information or fingerprint data.

Tips: While uploading or downloading user’s information, device monitor must be stopped first if the communication method between PC machine and fingerprint reader is RS485/232. However, there is no need to stop device monitor first if the communication method is Ethernet and the user’s information can be directly uploaded and downloaded.

5.3.6 Data import & export through U disk

5.3.6.1 Import user's data through U disk

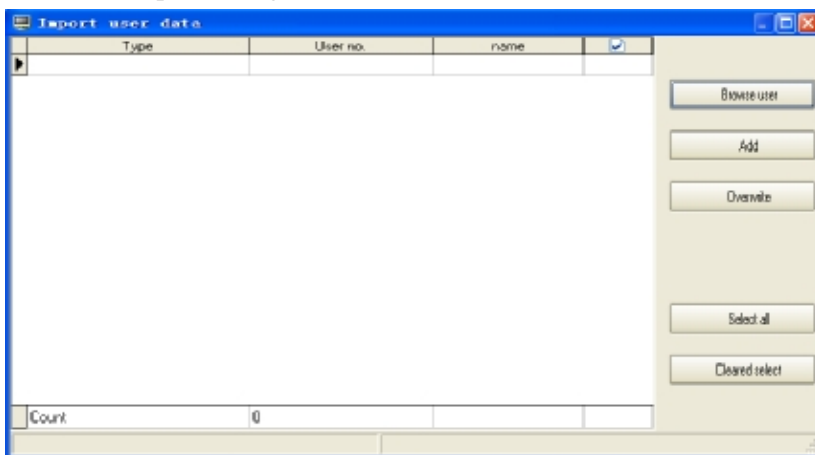
【Function Introduction】 Import user's data preserved in U disk to the system.

【Operation Steps】

1.Method to enter “ import through U disk”

Click right key of the mouse on user management interface, and select “import through U disk”

2. Enter “import through U disk” interface, as shown below:



3.Click “detect U disk user” to detect user's data in U disk. Click “add new user to computer” to add new user or select the user that is to be added to the database in the list and click “cover computer data”. Close the window after operation, then you can see the imported user's data in user list.

5.3.6.2 Export data to U disk

【Function Introduction】 Export the selected user to U disk and save there .

【Operation Steps】

1. Select the user to be exported to U disk
2. Method to enter “export to U disk”

Click right key of the mouse on user management interface, and select “export to U disk”.

3. The system will give tips after selection of “export to U disk”.



4. Verify the exported data, and the operation will be completed after “export successfully” appears.

5.4 Privilege management

【Function Introduction】 Privilege management is to set unlocking time of enrolled user and access control. Every user's privilege setting consists of three time zone setting and a grouping setting. "or" exists among time zones. There are three time zone in grouping too, and "or" exists among them as well.

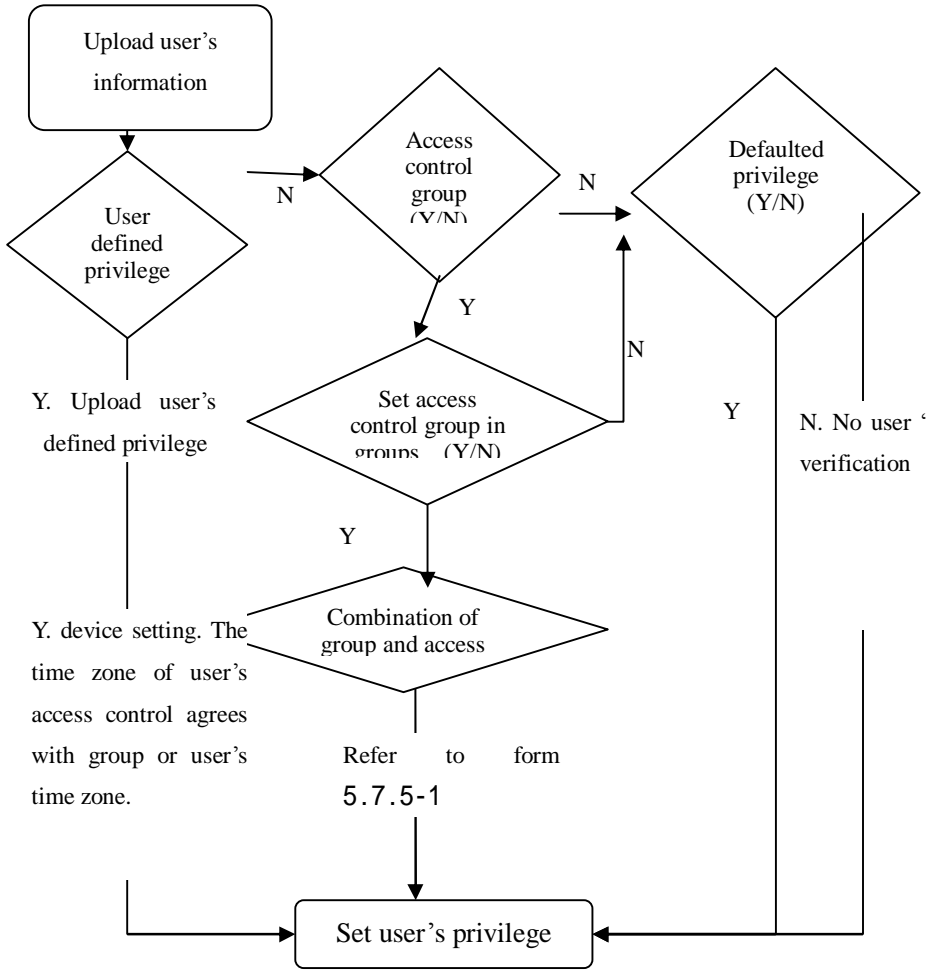
Simply speaking, to make enrolled user in unlocking state: firstly, the subgroup user belongs to must exist in unlocking combination (it is allowed to be in a combination with other subgroups); secondly, the present unlocking time should be during the user's time zone or any effective time of group's time zone .

The system default the unlocking combination as well as the new enrolled user as the first group. Therefore, it is normal to default the new enrolled user as unlocking state. If there is no subgroup user belongs to in unlocking combination settings, the user cannot unlock.

All the users must be in one subgroup which can be : subgroup 1, subgroup 2, subgroup 3, subgroup 4, and subgroup 5. Assign group information to the users to execute management of unlocking combination privilege.

The following passage will describe how to set time zone, grouping, unlocking combination, etc. and how to upload the information to the fingerprint reader.

Relationship diagram of user defined privilege, access control group and group



5.4.1 Time zone setting

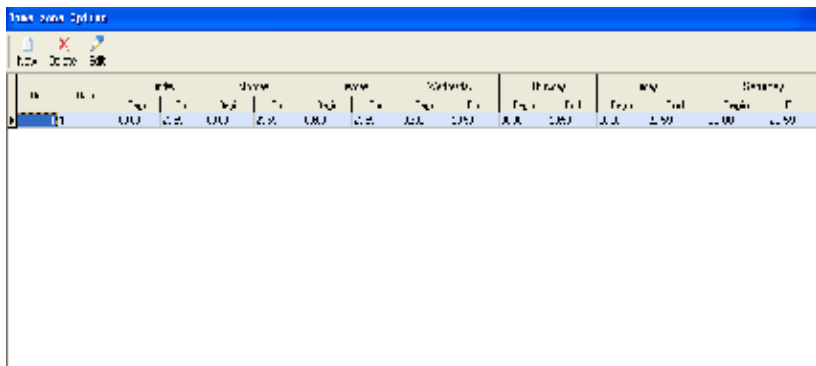
【Function Introduction】 Set time zone when unlocking happens if user's fingerprint verification gets done.

【Operation Steps】

1.Method to enter “time zone setting”:

Click menu: access control management->time zone option to enter the interface of time zone setting.

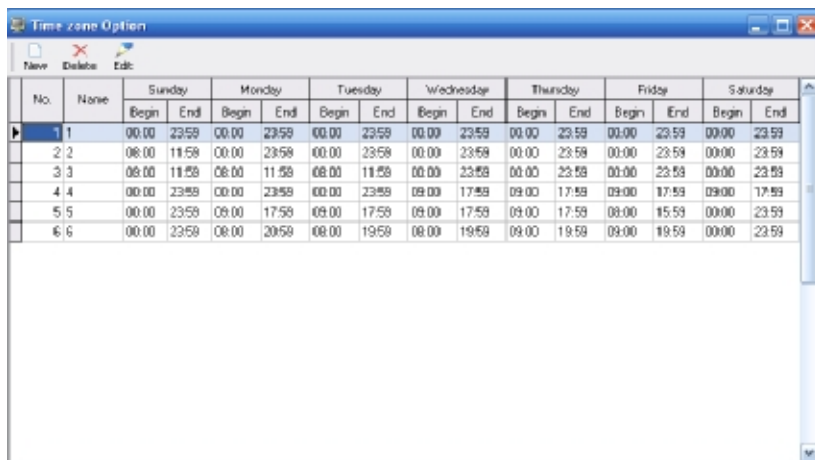
2.Enter “time zone settings” interface, as shown below:



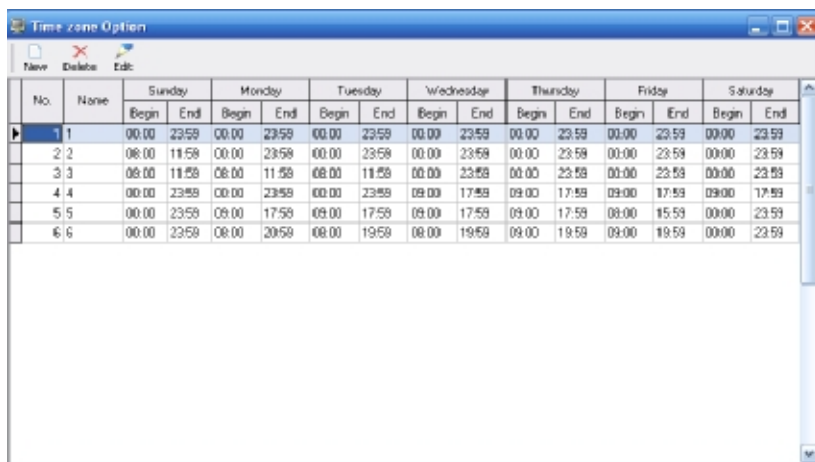
3.Add time zone. Select “add” to enter time zone setting interface and set time zone that can be used by users.



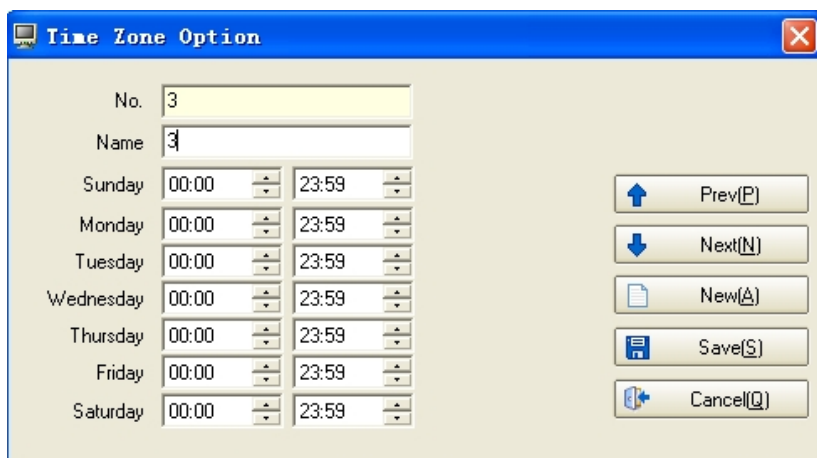
4.After setting, click “save and exit”, the setting will be saved and displayed synchronously in the list, as shown below:



5. Modify time zone. If it is necessary to modify some time zones which have been specified, select the time zone in the list, as shown below:



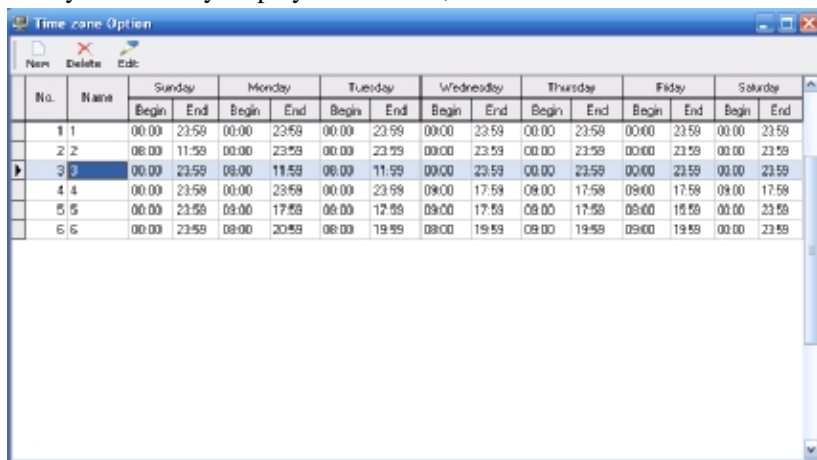
6. Click “modification” to enter time zone setting interface and modify the time zone.



The dialog box titled "Time Zone Option" contains the following fields and buttons:

- No.: 3
- Name: 3
- Sunday: 00:00 to 23:59
- Monday: 00:00 to 23:59
- Tuesday: 00:00 to 23:59
- Wednesday: 00:00 to 23:59
- Thursday: 00:00 to 23:59
- Friday: 00:00 to 23:59
- Saturday: 00:00 to 23:59
- Buttons: Prev(P), Next(N), New(A), Save(S), Cancel(Q)

7. After modification, click “save and exit”, the new one will be saved and synchronously displayed in the list, as shown below:



The window titled "Time zone Option" displays a list of time zones. The table below represents the data shown in the window:

No.	Name	Sunday		Monday		Tuesday		Wednesday		Thursday		Friday		Saturday	
		Begin	End	Begin	End	Begin	End	Begin	End	Begin	End	Begin	End	Begin	End
1	1	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59
2	2	00:00	11:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59
3	3	00:00	23:59	00:00	11:59	00:00	11:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59
4	4	00:00	23:59	00:00	23:59	00:00	23:59	00:00	17:59	00:00	17:59	00:00	17:59	00:00	17:59
5	5	00:00	23:59	00:00	17:59	00:00	17:59	00:00	17:59	00:00	17:59	00:00	15:59	00:00	23:59
6	6	00:00	23:59	00:00	20:59	00:00	19:59	00:00	19:59	00:00	19:59	00:00	19:59	00:00	23:59

Notice: Set a day's starting time bigger than ending time, then only fingerprint verification can be done. For example, the starting time of Sunday is 12:00, and the ending time is 11:00. After setting, please upload the time zone to the device.

5.4.2 Management of access control group

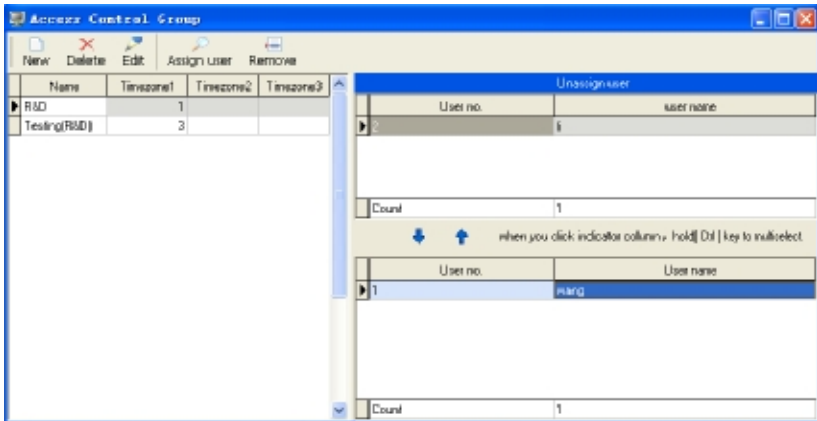
【Function Introduction】 Access control group is to make users into groups. It is convenient for the management of access control with many devices. For example: a factory has many access control machines. User's access control time differs on different machines. Therefore, a number of access control groups can be set to define user's time on different machines. The setting can be uploaded to the access control machine once, then the machine will work effectively.

【Operation Steps】

1.Method to enter “ access control group management”:

Click menu: access control management->access control group management

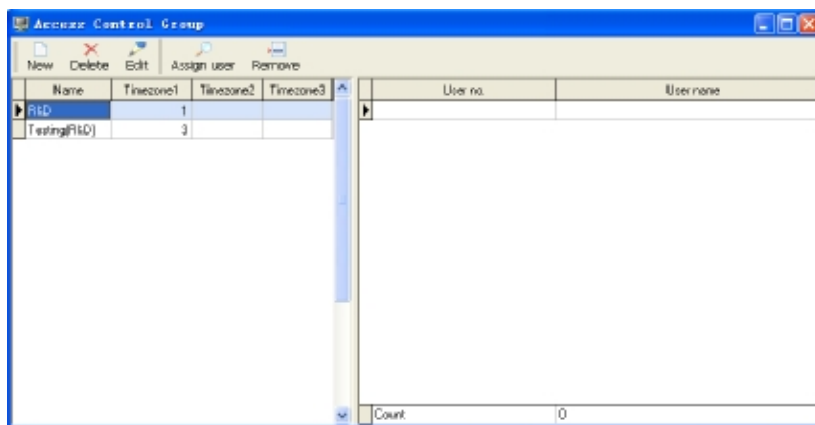
2.Enter “access control group management” interface, as shown below:



3.Build access control group. Click “add” and input name and select time zone in the editing interface. Then click “save and exit” or click “save and add” to add new access control group, as shown below:



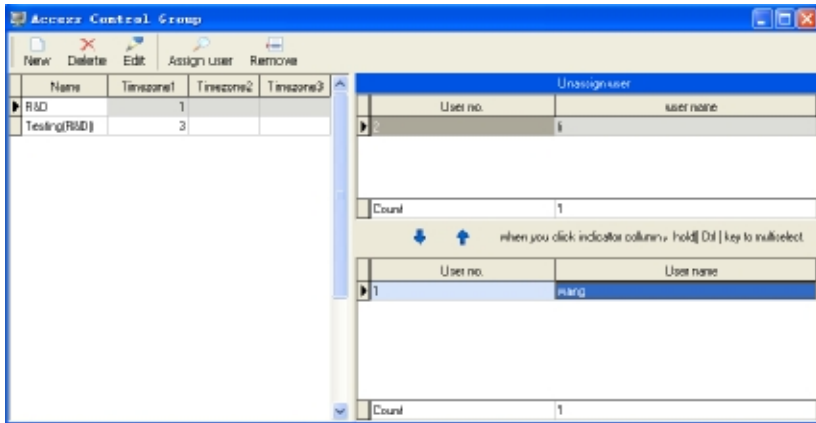
4. Then the added access control group will be shown on the management interface. For access control group modification, please click “modification”



Name	Timezone1	Timezone2	Timezone3	User no.	User name
R&D	1				
Testing(R&D)	3				

Count 0

5. Personnel distribution: the personnel will be distributed to different access group to execute management. Click “personnel distribution” on the management interface, as shown below:



Tips:

1. The access control group is to manage the users in groups. It is different from the group setting in privilege management.
2. “Group” in group setting means group in devices. One device can own 5 groups.
3. “Group” in access control group is subordinate to group. To make user employ time zone of access control group, please select access control group in menu: “privilege management”-> “group setting” and upload access control privilege.

5.4.3 Group setting

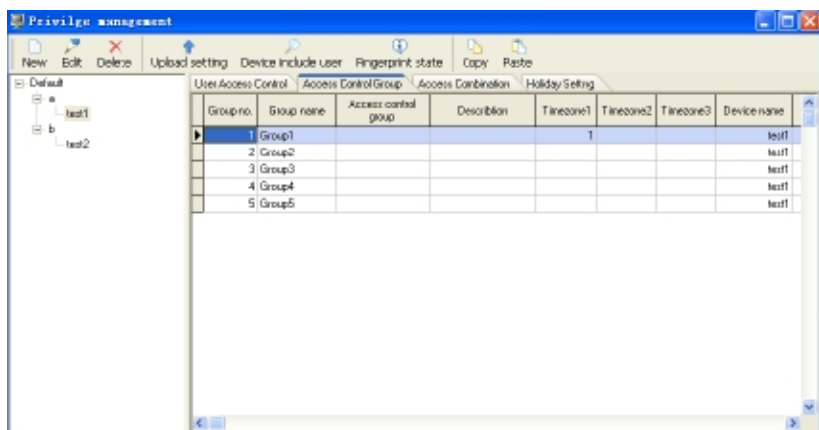
【Function Introduction】 Set time zone when fingerprint verification gets done for user’s subgroup.

【Operation Steps】

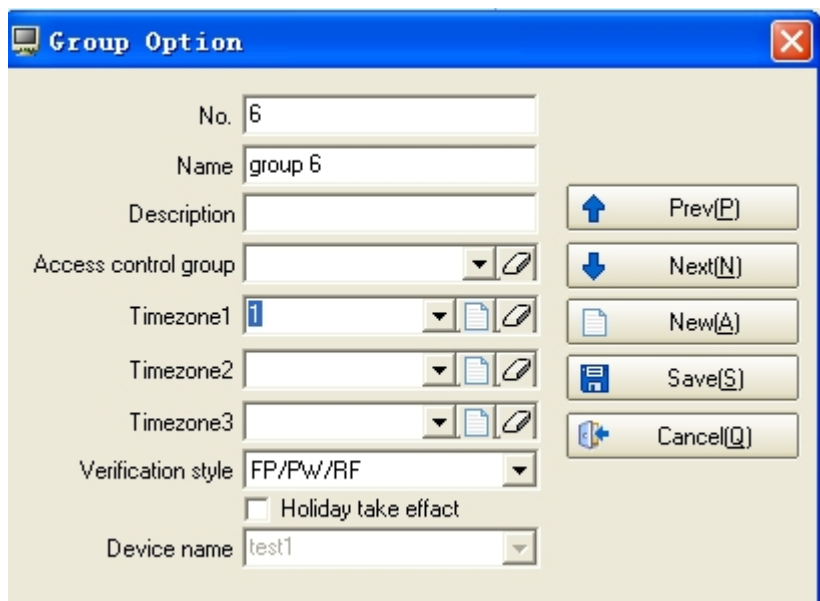
1. Method to enter “group setting”:

Click menu: access control management-> privilege management and select group setting interface.

2. Enter “group setting” interface as shown below:



3. Edit the groups. Select the group needing editing and click “modification”, as shown below:



4. Select time zone when fingerprint verification gets done in the drop-down list, click “save and exit” and the data gets saved.

No.	Name	Sunday		Monday		Tuesday		Wednesday		Thursday		Friday		Saturday	
		Begin	End	Begin	End	Begin	End	Begin	End	Begin	End	Begin	End	Begin	End
1	1	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59
3	3	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59
5	5	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59

Device name: test1

5.4.4 Unlocking combination setting

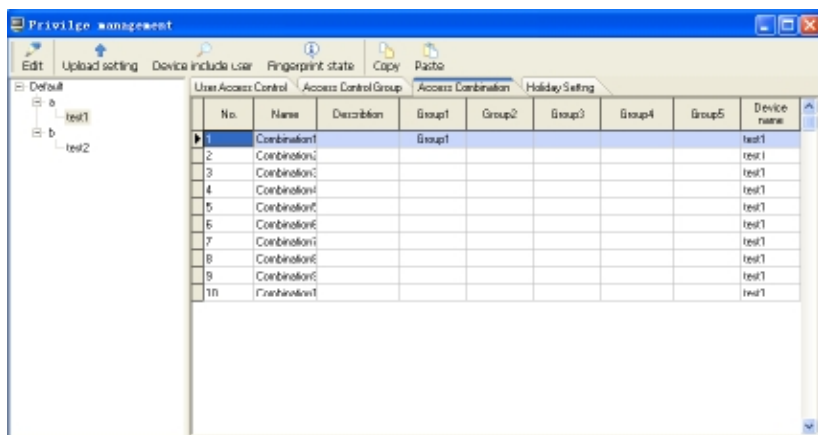
【Function Introduction】 Set user’s unlocking combination: one or more than one (5 persons at most) person’s fingerprint verification can lead to unlocking.

【Operation Steps】

1. Method to enter “unlocking combination”

Click menu: access control management-> privilege management, and select unlocking combination setting interface.

2. Enter “unlocking combination setting” interface, as shown below



3. Edit unlocking combination. Select an unlocking combination record and click “modification”, or click unlocking combination record twice to enter modification interface, as shown below:



Select subgroup in the drop-down list. Select unlocking

combination subgroup from group 1 to group 5. Click “save and exit” to save the setting.

Tips:

1. If you select subgroup 2 & 3 in group 1&2, employees in subgroup 2&3 are the ones whose fingerprint verification can lead to the unlocking.
2. It is the same with subgroup 2&3 in group 1 &3.
3. If you select subgroup 1 in group 1 &2, two persons in one group can lead to unlocking after their fingerprint verifications get done.
4. No order needs when a number of people engaged in fingerprint verifications.

5.4.5 Holiday setting

【Function Introduction】 Access control time in holiday may be different from usual access control time. In order to make operation easy, the system provides holiday setting to solve the problem of the special access control time in holiday.

【Operation Steps】

Click menu: access control management-> privilege management and select holiday setting interface.

2.Click “add” to add holiday.

Holiday Setting

No.

Begin Date

End Date

Timezone

Device name

Prev(P)

Next(N)

New(A)

Save(S)

Cancel(Q)

3. Input the starting date and ending date of the holiday, and select the access control time zone during the holiday.

Holiday Setting

No.

Begin Date

End Date

Timezone

Prev(P)

Next(N)

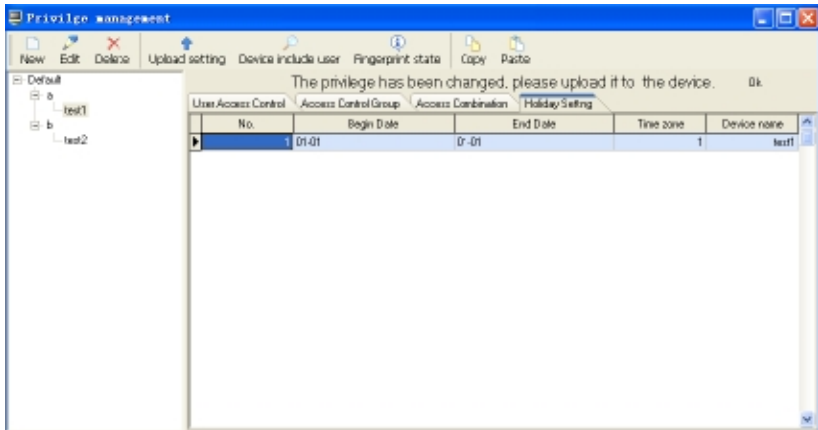
New(A)

Save(S)

Cancel(Q)

No.	Name	Sunday		Monday		Tuesday		Wednesday		Thursday		Friday		Saturday	
		Begin	End	Begin	End	Begin	End	Begin	End	Begin	End	Begin	End	Begin	End
1	1	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59
3	3	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59
5	5	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59	00:00	23:59

4. Click “save and exit” and the set holiday will be shown.



5.4.6 User's specified privilege

1) Set the access control privilege used by user during group time zone

【Operation Steps】

1.Method to enter “ user defined privilege setting”

Click menu: access control management-> privilege management, and select user defined privilege interface.

2.Enter “user defined privilege” and edit user defined privilege. Click “add”, enter “user’s access control privilege setting guide” interface to select user that needs editing privilege or select all the users, as shown below:

User Access Control Privilege Option Guide

Select user please, locate record by input No. into the grid.

Department: List whole per No. Name Search Cancel search

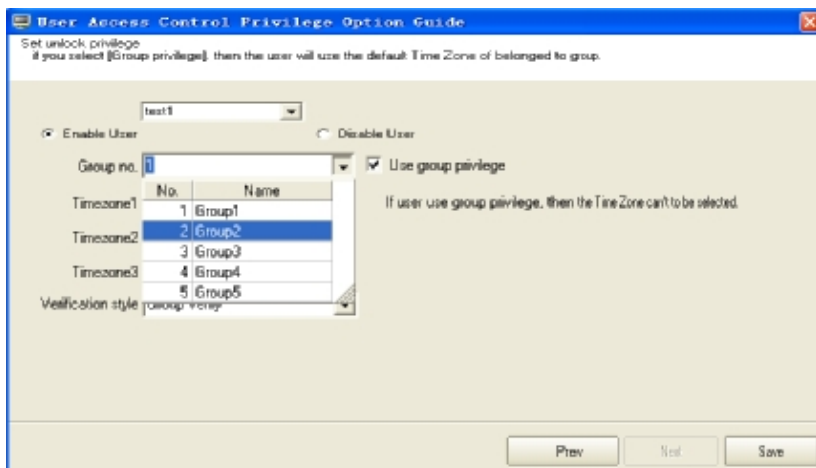
	No.	Name	Company Name	Department
<input checked="" type="checkbox"/>	1	Zhang Wan	Company Name	Department
<input type="checkbox"/>	2	Zhang Li	Company Name	Department

Count 2

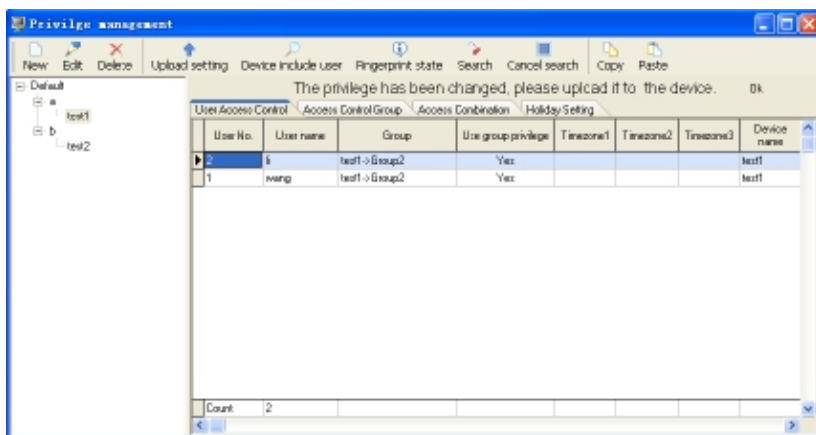
Check All Uncheck All Prev Next Save

3.Users belong to group 1. If users need to be distributed to other groups, it is necessary to redistribute users to different groups. For example: to distribute User 1 to group 2, User 1 should be selected. After the selection, click “next”.

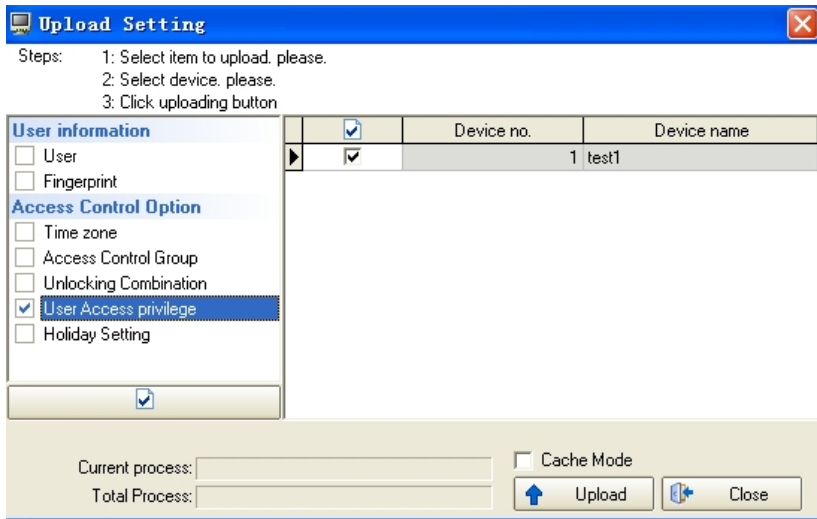
4.Click “group number”, and select “group 2”. Click “save” to save the set privilege.



5. After the above steps, User 1 is distributed to group 2, as shown below:



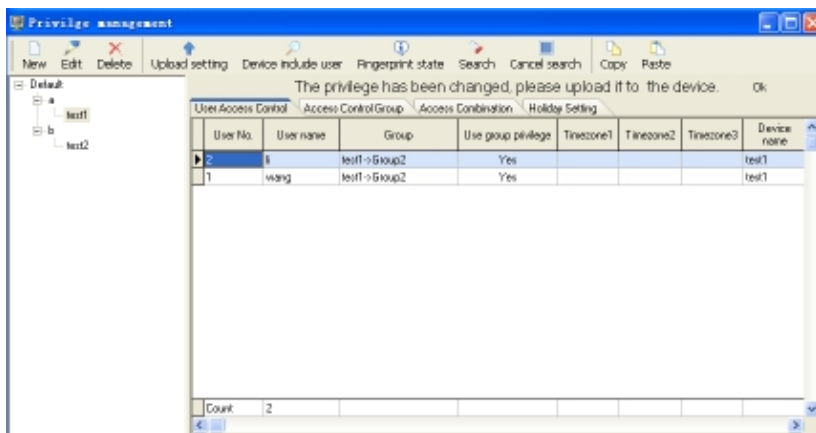
6. According to step 3-4, set the subgroup users belong to. Then click “upload setting” to upload user’s access control privilege. Select the device and the privilege item that needs to be uploaded in the window, and click “upload”.



2) Set the privilege under the condition that user will not use group time zone.

【Operation Steps】

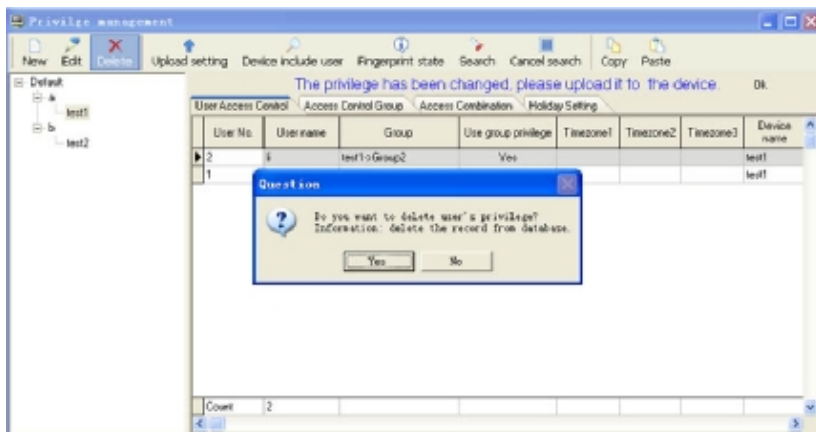
- 1.To make user belong to a group but not use group time zone, “use group privilege” is ignored in the privilege setting interface. But he can select his needed time zone.
- 2.Then click “save” and enter “privilege management” interface. User defined information is shown synchronously in the list, as shown below: User 1 employs group privilege while User 2 does not employ group privilege.



3) Delete user defined privilege

【Operation Steps】

1. Select the user that need deleting privilege on “user defined privilege setting” interface, and click “delete”.



Tips:

1. The access control privilege distributed to the fingerprint reader cannot be deleted while deleting user defined privilege.

2. If you want to forbid user unlocking, click “modification” to enter “user defined privilege editing” window, select “forbid user”. After saving the privilege, click “upload setting” to upload access control privilege.

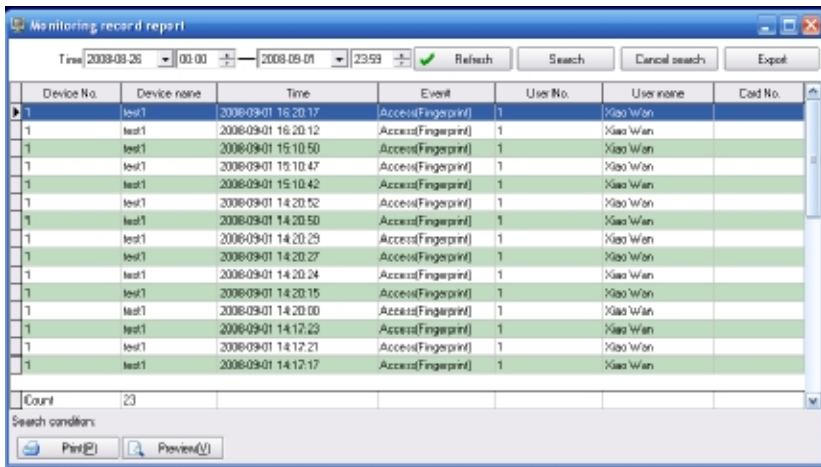
5.5 Report

5.5.1 Monitor record report

【Function Introduction】 Query all the employees' in-and-out record during some time zone. There are two ways to query records: one is inputting the starting & ending time and clicking “refresh” to get all records during some period. The other is clicking “query” and inputting detailed query conditions to get the records.

【Operation Steps】

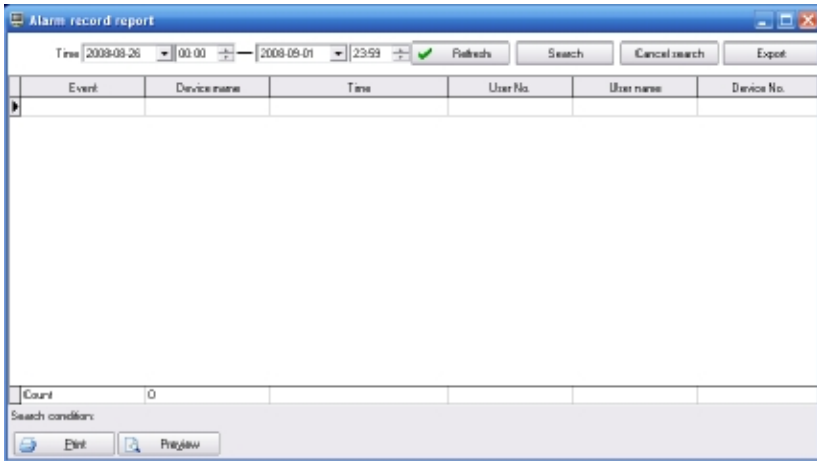
- 1、Click menu: “report”-> “monitor record report” and “monitor record report” window will pop up, as shown below:



- 2.Input refreshed time zone in “starting & ending time”, and click “refresh”

【Operation Steps】

1.Click “alarm record report” in the drop-down menu, and “alarm record report” window will pop up, as shown in the following picture:



The "Alarm record report" window displays a search interface for alarm records. It includes a title bar, a search criteria section with date and time pickers, a table of results, and a search condition editor at the bottom.

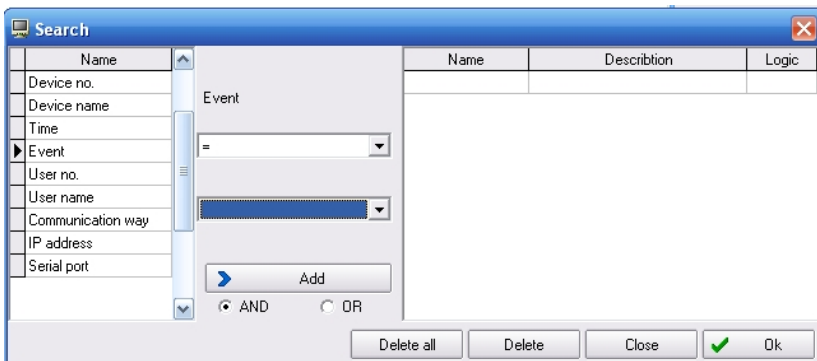
Time: 2009-09-26 00:00 - 2009-09-01 23:59 [Refresh] [Search] [Cancel search] [Export]

Event	Device name	Time	User No.	User name	Device No.

Count: 0

Search condition: [Edit] [Preview]

2.Click “query” to set querying conditions according to different demands. Select various abnormal events in “events” to query alarm records, as shown below:



The "Search" window allows users to define query conditions. It features a list of fields on the left, a central configuration area for events and logic, and a results table on the right.

Fields: Name, Device no., Device name, Time, Event, User no., User name, Communication way, IP address, Serial port

Event: [=] [Add]

Logic: ☒ AND ☐ OR

Name	Description	Logic

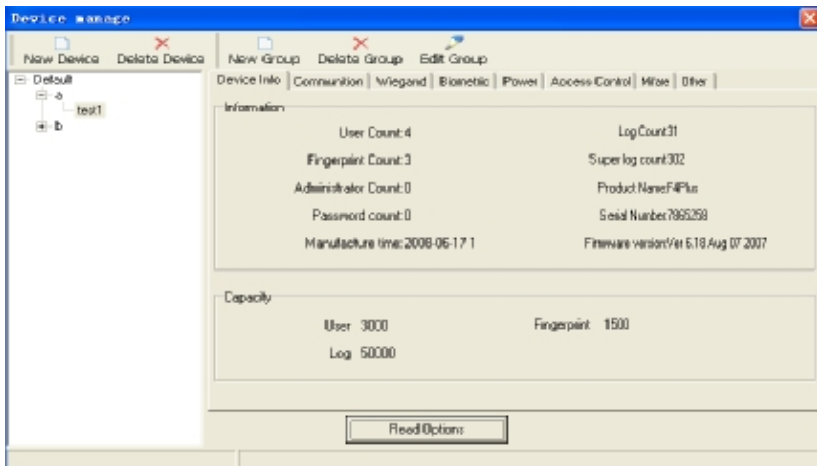
[Delete all] [Delete] [Close] [Ok]

5.6 Device management

5.6.1 Read information from fingerprint reader

【Operation Steps】

1.Click “device management” in the “access control management” list, users’ number, fingerprints’ number and other information can be seen on “fingerprint reader information” interface. Select fingerprint reader and click “read setting”. The access control software will connect the selected devices automatically and read their information, as shown below:

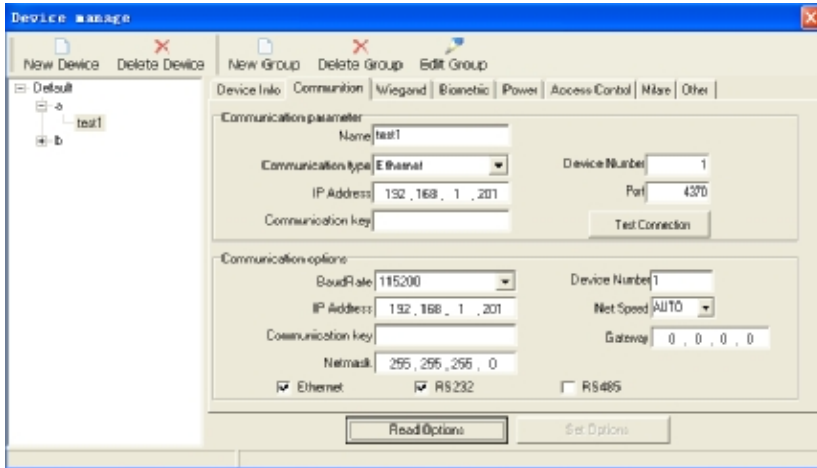


5.6.2 Communication setting

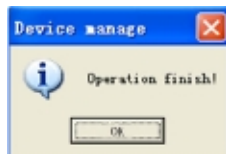
【Operation Steps】

- 1.Click “communication setting” to see its interface.
- 2.Click “read setting” to read the communication setting of the selected device. Then modify the device’ communication manner

and communication method, such as baud rate, communications password, network rate and so on. Later, click “application setting” to upload the modified setting to the selected device.



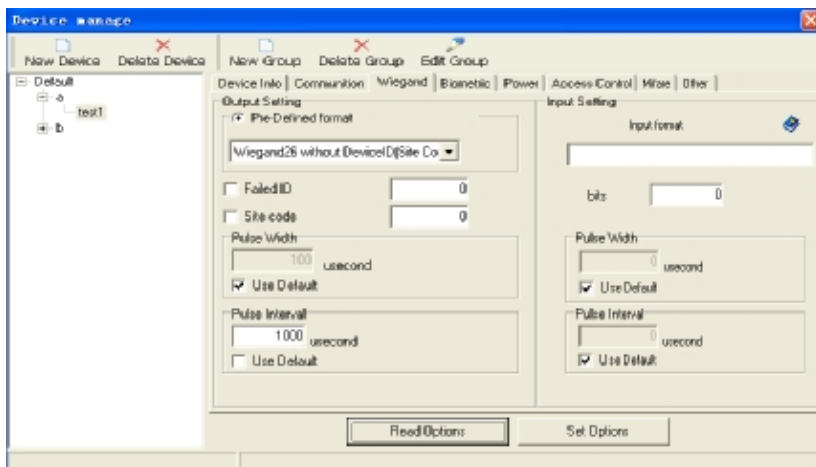
3. After parameter modification, click “application setting”, then “operations complete” will appear, as shown below:



5.6.3 Wiegand

【Operation Steps】

1. Click wiegand item on “device management” interface.
2. **Read setting:** 4 choices will be shown in the drop-down list whose format is specified. According to your demands, 26 bit or 34 bit can be set.



3.The meanings of various choices:

Specified format refers to the specified format built-in system. It is no longer necessary for user to define the total bit length and the position where information locates.

System default 4 specified formats: wiegand26 with device ID. wiegand34 with device ID. wiegand26 without device ID. wiegand34 without device ID. Wiegand26 with device ID refers to W26 (with device ID) format export. Wiegand26 without device ID refers to export of W26 (with no device ID) format. Device ID is specified as the following: the export is fingerprint reader ID if there is no zone bit code setting, and the export is the set zone bit code (similar to machine ID, but specified by user, able to be repeated by different machines, ranging from 0 to 255) if zone bit code is set. **Failed ID:** the failed ID (0~65534) exported after failed verification won't be exported if you don't select it.

Zone bit code (0~255): it is similar to machine ID, but specified by user. It can be repeated by different machines.

User defined format: user defines the exporting format of Wiegand.

Total bit: the length exported by present format

ID start: the position where ID starts in total bit

ID bit digit: bit length that ID occupies

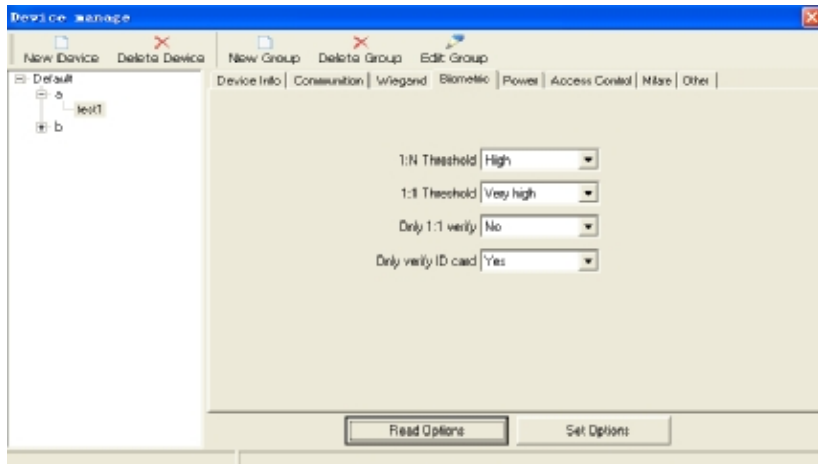
Pulse Width : pulse (generated by Wiegand) width defaults 100 microseconds. It can be adjusted between 20 and 800 if the administrator can not receive Wiegand.

Pulse interval's default value is 900 microseconds, and can be adjusted between 200 and 20000.

5.6.4 Verification

【Operation Steps】

1.Click “verification” main interface of “device management” interface, as shown below, click “read setting” to read the verification information from fingerprint reader.



2.You can change your selection to achieve best effect.

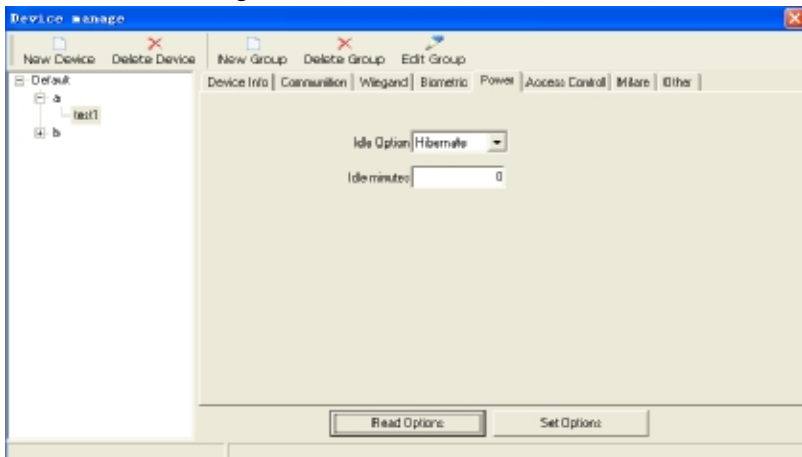
3.Definitions of various choices

1:1 Verification only: “1:1 verification only” can be set “yes” for a user who has fingerprint and ID card or Mifare card. While verifying, the user has to use his card, then press fingerprint. If the card is not used, there will be no result while pressing finger. **ID card verification only:** it is set aimed at ID card. When selecting “yes”, the user can be verified with ID card only. When selecting “no”, the user has to use ID card and press finger to get verification.

5.6.5 Power management

【Operation Steps】

1.Click “power management” on “device management” interface, then click “read setting”, as shown below:

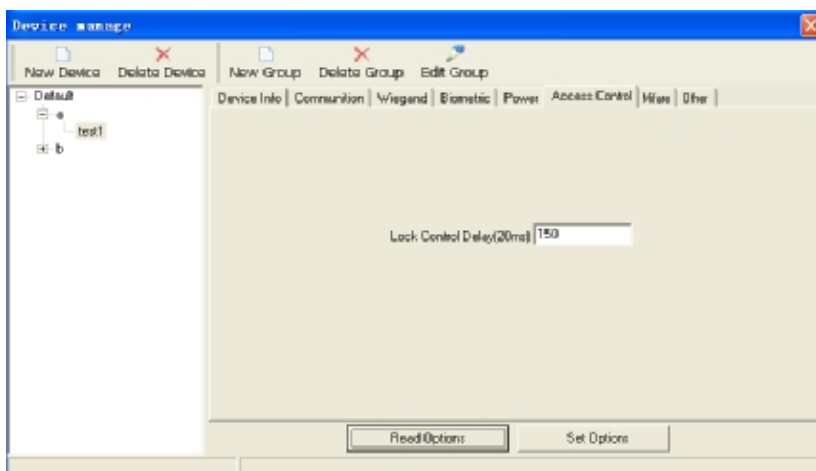


3.Idleness setting: set the state during idle period---shutdown or dormant. The idleness setting will be inefficient if there is no idle period.

5.6.6 Access control

【Operation Steps】

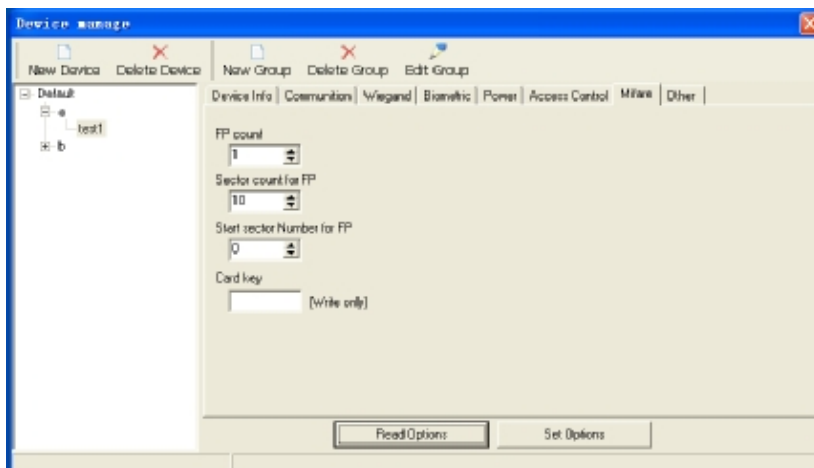
1.Click “access control” on “device management” interface, and read setting as shown below. Lock control delay (its least unit is 20ms, with general setting of 100~200ms) is used to control the unlocking time.



5.6.7 Mifare

【Operation Steps】

1.Click “Mifare” on “device management” interface to read setting as shown below:



2.Definitions of various choices:

Fingerprint number: the fingerprint number stored in Mifare card

Fingerprint starting sector: the first sector for fingerprint storage in Mifare card

Sector number: the number of sectors where fingerprints are stored

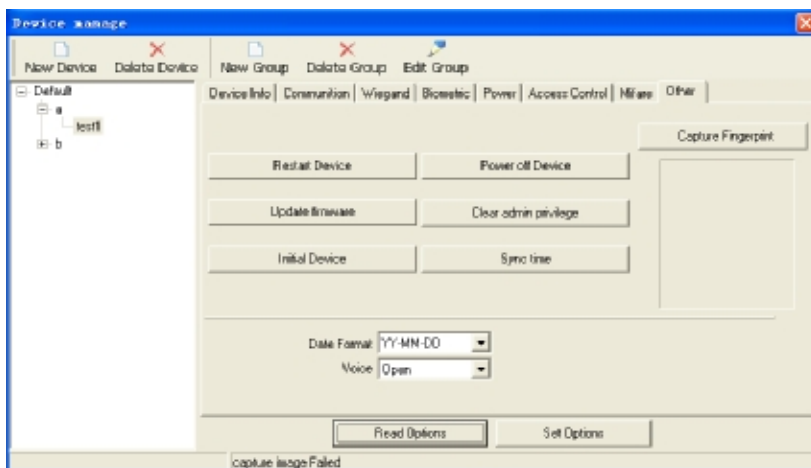
Card password: password to read and write card, only to be set, not able to be read

5.6.8 Other settings

This part is mainly for the convenience of device setting.

【Operation Steps】

1.Click “other settings” on “device management” interface to read setting, as shown below:



2. Definitions of various choices:

Restart device: click machine's name in the list, and click "restart device" to restart the device.

Shutdown: click "shutdown" to stop working of this device.

Upgrade firmware: To avoid abnormal process, it is not suggested for user to upgrade the firmware without consulting dealers or getting informed from dealers.

Clean out administrator's privilege: select the machine name that administrator belongs to in the list, and clean it out.

Initialize device: click "initialize device" to initialize the device.

Synchronous time: make device's time and computer's time synchronous.

Grasp fingerprint image: click it and you can see your recent fingerprint image (except for F4 plus) .

Date format: select data format in the drop-down list. The date format here means the format displayed on the starting interface of fingerprint reader.

Voice function: you can select “open” or “close” to decide whether the reader will use voice or not.

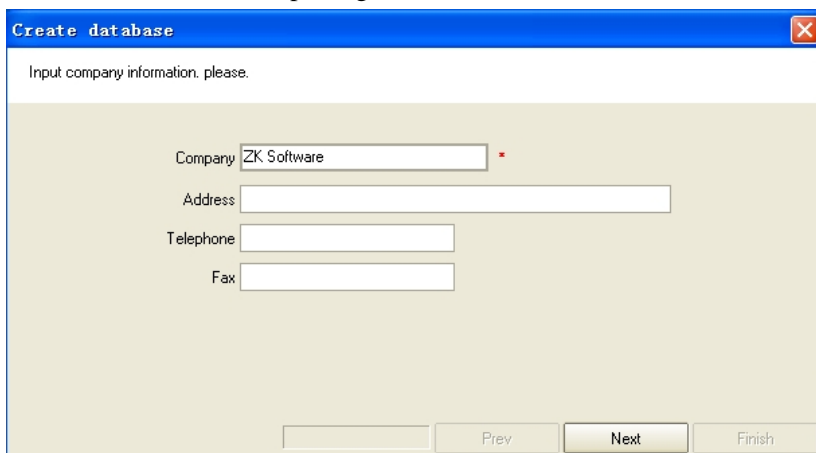
5.7 System management

5.7.1 Build database

【Operation Steps】

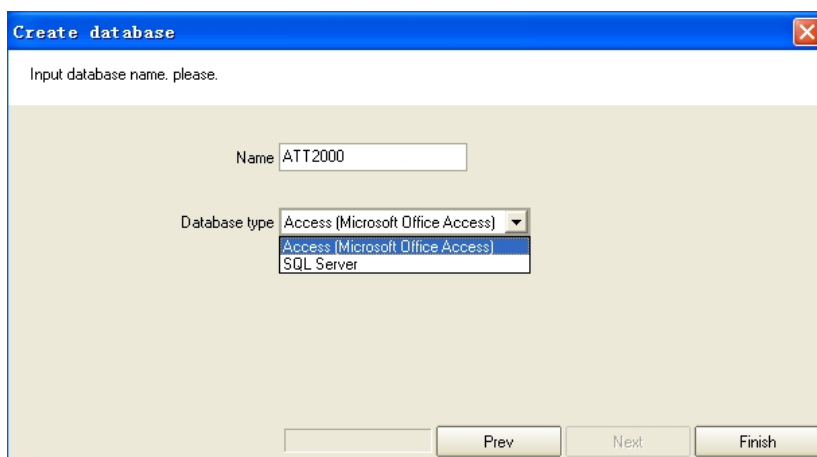
1.Click“build database” in the drop-down list of “system management”, and its window will pop up, as shown below:

Click “next” after inputting the information.



The screenshot shows a window titled "Create database" with a blue header bar. Below the header, the text "Input company information, please." is displayed. The main area contains four input fields: "Company" (with "ZK Software" entered), "Address", "Telephone", and "Fax". At the bottom right, there are four buttons: a disabled "Prev" button, a "Next" button, and a "Finish" button. A small red asterisk is visible next to the "Company" input field.

2.Select database type to input database’s name, click “finish”, and the system starts building database.



Input database name. please.

Name: ATT2000

Database type: Access (Microsoft Office Access)

Access (Microsoft Office Access)

SQL Server

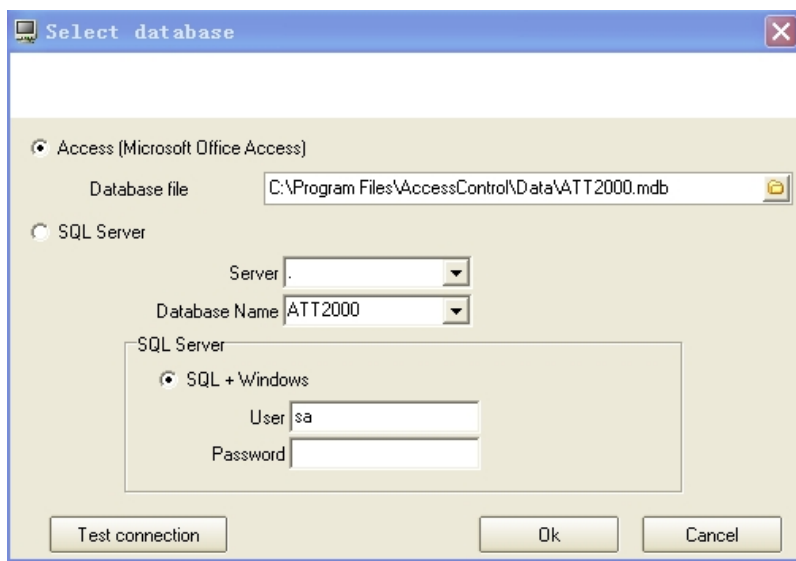
Prev Next Finish

Notice: Only English letters or numbers are acceptable. Don't input special symbols. If SAL Server is selected by database type, please install SQL Server of MSDE before building database.

5.7.2 Set database

【Operation Steps】

- 1、 Click “set database” in the drop-down list of “system management” to get the window as shown below. Select database type to input database information, then click “test connection”. If test connection succeeds, click “yes”



Notice: If SQL SERVER database is needed by the system, please select mixed verification mode when you are installing it.

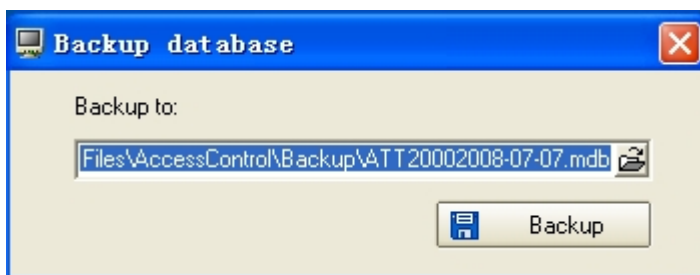
5.7.3 Database management

【Function Introduction】 Prepare back-up, recovery, and compression for database, delete out-of-date data, set database password and so on.

5.7.3.1 Prepare back-up

【Operation Steps】

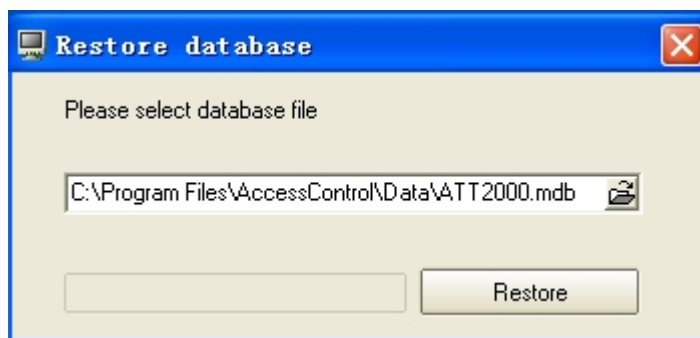
- 1.Prepare back-up: click “system management”-> “database management”->“database back-up” to get a dialogue box, name and save the database under the safe directory, then click “ back-up”, as shown below:



5.7.3.2 Recover database

【Operation Steps】

1. Click “system management”-> “database management”-> “recover database” to get the window, select the back-up file and click “recover”.



5.7.3.3 Compress database

【Operation Steps】

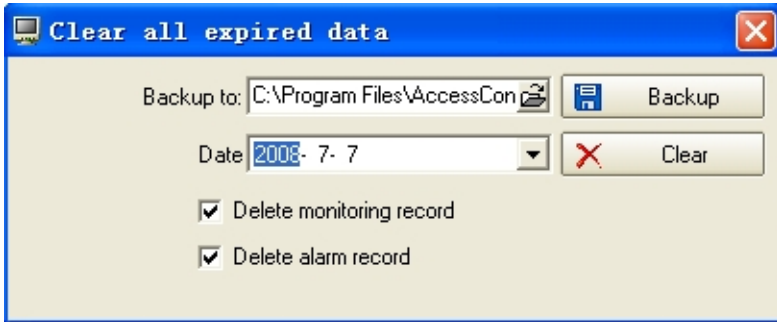
1. Click “system management”->“database management”->“compress database” to compress the database.

Notice: This function only works for Access database.

5.7.3.4 Delete out-of-date data

【Operation Steps】

1. The out of date data can be deleted. Click “system management”-> “database management” -> “delete out-of-date”, as shown below:



Notice: Records on the expired day will not be deleted.

5.7.3.5 Set database password

【Operation Steps】

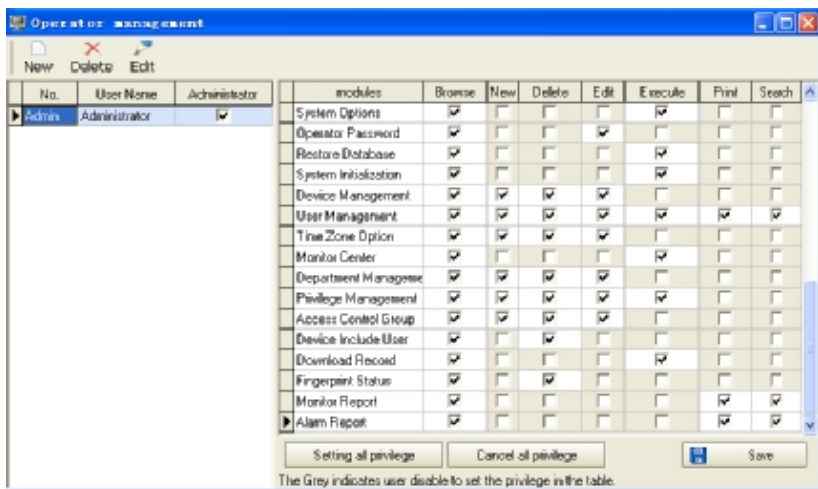
1. Click “system management”->“database management”->“set database password” to input the password in the window as shown below, then click “ set”.



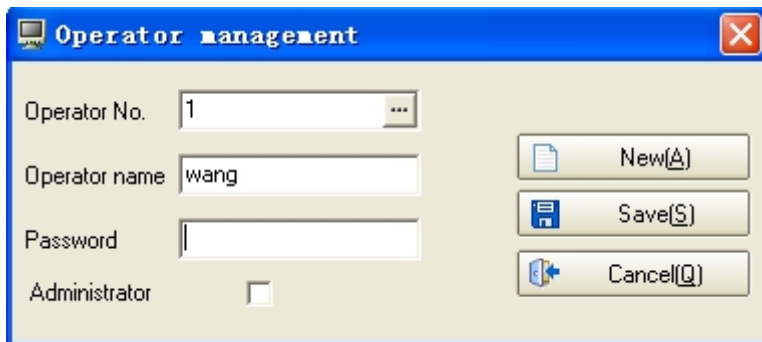
5.7.4 Operator management

【Operation Steps】

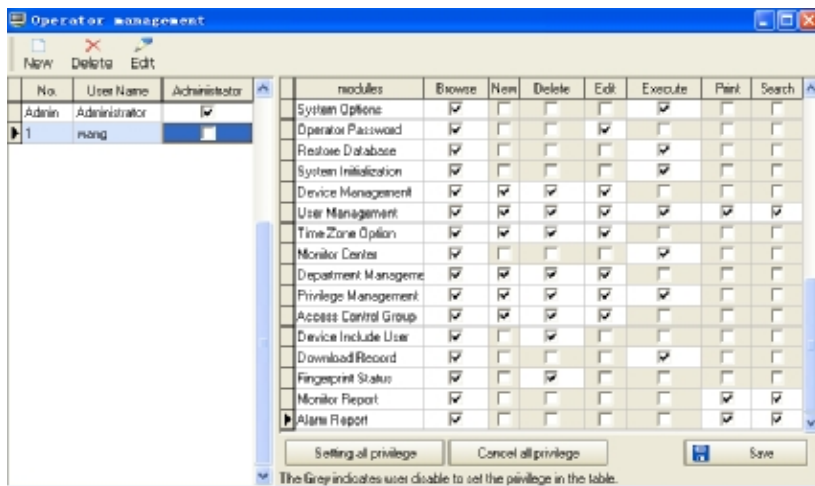
1. Click “operator management” in the drop-down list of “system management” to get the interface as shown below:



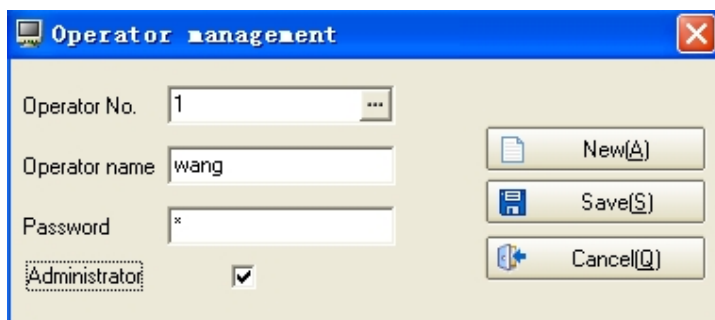
2. Click “add”, input operator’s number, name and password in the pop-up window. You can select the super administrator, as shown below:



3. Click “save and exit”, and set privilege of the new-added administrator on “operation administrator” interface, as shown below. You can select “set all privileges” or “cancel all privileges”.



4. To modify password, select the employee on the “operation administrator” interface, click “modification”, then “ save and exit”, as shown below:

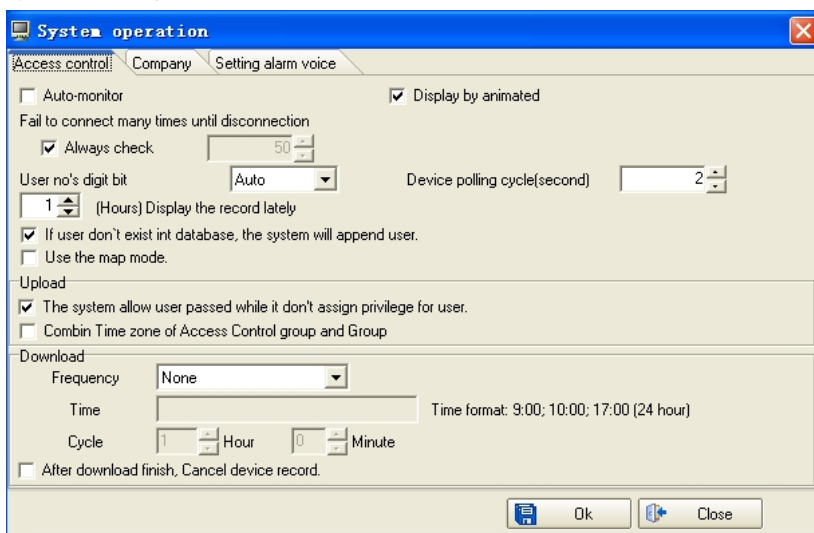


5.7.5 System parameter setting

【Operation Steps】

1. Access control setting

1) Click “system management”->“system parameter setting” to enter system setting interface, as shown below:



2) Parameter setting

1.1 Parameter [automatic start control]

Automatic start control refers to whether the program is under control automatically when access control software is working. If you select it, the program will start monitor over fingerprint reader when your access control software is working.

1.2 Parameter [monitor display in animation]

Monitor display in animation refers to whether the software's icon is displayed in green & white alternately when reader monitor is normal.

If you select this parameter, the software's icon will be displayed in green & white alternately, or it will be displayed in green.

1.3 Parameter [**There will be no connection with device any more if repeated connection fails.**]

This parameter refers to whether the connection between software and fingerprint reader is broken or not during the specified period. If you select “ detect all along”, the software will try to connect with reader all along after the connection is broken. Or the software will try to connect with the reader during the specified times, and the software will stop connecting with the reader when it fails in the specified times. For example: when the software fails to connect with the reader in the first floor, the software will try to connect with the reader for 50 times with 2 seconds' interval. If the software fails 50 times, then it won't connect with reader any more.

1.4 Parameter [**Default privilege is employed when there is no specified access control privilege to upload user (use time zone of group 1)**]

It refers to default privilege is employed as user's access control privilege when user uploads his information without privilege specified in privilege management. While using default access control privilege, all users belong to access control group 1. The default time zone of group 1 is time zone 1. Using access control time zone 1 means that all the users can open the door through fingerprint verification in 24 hours.

1.5 Parameter [**access control group combined with group time zone**]

We can manage the user in subgroups, and set time zone for user's subgroup. Three time zones can be set in access control group and limitless access control groups can be set in the software. The group seen in privilege management is group in the device. There are

only 5 groups in the device, and 3 time zones can be set in each group. Please distinguish access control group from the group in privilege management. When access control group is employed to combine with group time , add access control group to a user and set 3 time zones for access control group. The group in group setting is also set with 3 time zones. At this time, user will employ the group time zone in group setting firstly. If only one time zone is set in group setting, while selecting [access control group combined with group time zone], the time zone in access control group will combine with time zone in group setting. After user's information is uploaded, there will be 3 time zones in user's access control privilege. They are group time zone 1 in group setting, time zone 2 &3 in access control group, **as shown in form 5.7.5-1**

Form 5.7.5-1

Name	Access control group combined with group time zone	Time zone 1	Time zone 2	Time period 3
Access control group		1	3	5
Group		2		
	yes	2	3	5

	no	2		
--	----	---	--	--

1.6 Parameter [**download frequency**]

It is to control download: periodic download, download in the specified time, or no download.

1.7 Parameter [**Delete device's record after download**]

Delete the record stored in the device automatically after download of device's record.

1.8 Parameter [**digit used to number user**]

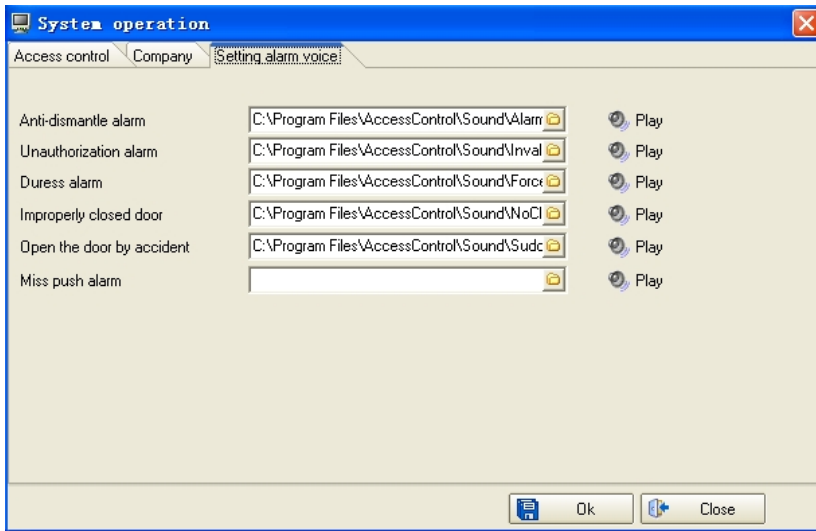
It refers to display user's number in digits. For example: if user's number is 1, 1 can be displayed automatically, while its five digits display is 00001 and 000000001 for nine digits.

1.9 Parameter [device's inquiry period]

It refers to the interval while software is examining the device.

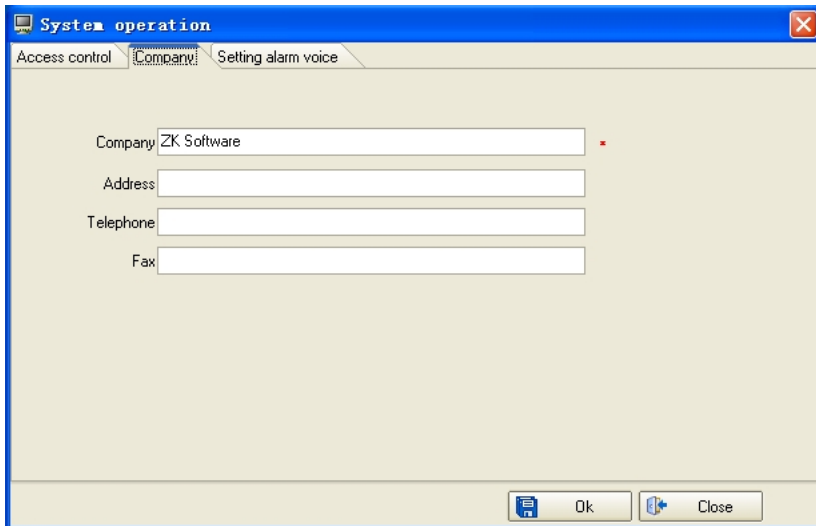
2.Company's information

Set company's information on the page. Input and modify company's information, as shown below:



3. Alarm voice setting

Set voices of various alarm



MSDE installation

1. Download free MSDE install from Microsoft Web site.
2. Start installation. Click: start->operation, input “cmd” in “operation” window and press “enter” to get “command line” window. Enter MSDE install directory, input setup securitymode=sql sapwd=“1” then press “enter”, and MSDE start installing. Employ securitymode=sql to express the installing example specified by SQLServer with mixed mode used. Under the mixed mode, the example supports identity verification enrollment both through windows and SQL. Sapwd=“1” means specify a powerful password for administrator’s entry. Here, 1 can be changed into your own password. After the installation, restart the computer.

6. Appendix

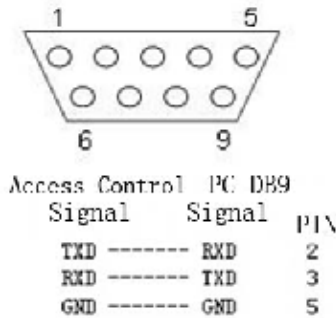
6.1 Connection of access control machine and system

The system provides three connection methods: RS232.RS485.TCP/IP.

6.1.1 Connection through RS232

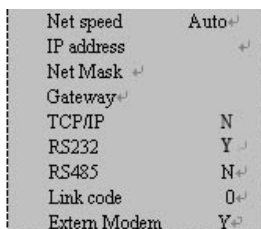
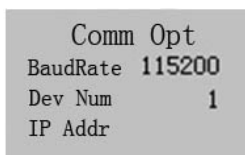
【Operation Steps】

1.Connect machine and computer through RS232 according to the following picture of signal lines connection.



2.Click “menu->setting->communication setting” to Set RS232 communication manner for the machine. The following picture displays the set result. Please pay attention to baud rate, machine ID, Ethernet, RS232 and the setting of connection password.

Notice: Connection with Ethernet must be broken when RS232 connection is open.



3. After setting, press “ESC” to enter “save” interface, as shown below, select “OK” to save the above settings and select “ESC” to cancel saving the settings.

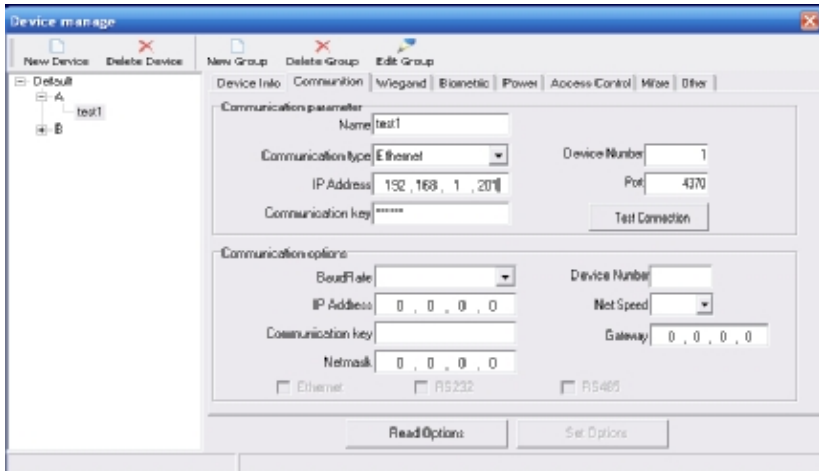
Notice: After saving the settings, the machine needs to be shut down and restarted.



4. Open the software, enter “device management” menu to add machine. There are 2 ways:

- ┆ Click menu: basic setting-〉 device management
- ┆ Select “device management” directly through shortcut

5. Click “add” in “device management” window to start connection of system and machine.



6.This interface is the communication interface which connects software and machine. The information input here must agree with the “communication setting” of Step 2 machine.

Fingerprint ID must agree with “machine ID” setting of access control machine’s “communication setting”. If the reader’s setting is 1, input 1 here.

Port: Select the communication port number to connect PC and reader, and default COM1. It can be other ports, please select it carefully.

Baud rate: It is connected through RS232. 115200 (whose value agrees with the baud rate of access control machine’s “communication setting” is suggested.

Communication password can be ignored under the condition of default. If communication password is set, input the corresponding password(5 digits at most)

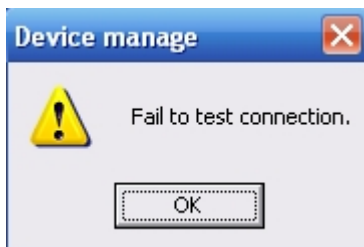
Name: Input name which is easy to remember according to device’s purpose. Later, while using this software, the reader can be

selected by selecting this name.

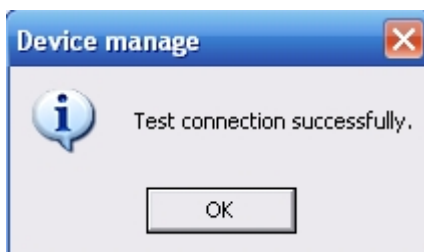


7.After setting, click “test connection”.

8.If the dialogue box of “test connection fail” appears, as shown below, please check the settings in Step 2 & 6, and repeat setting in Step 7.



9.If dialogue box of “test connection succeeds” appears, as shown below, then the connection between access control machine and system has been done.



10. Through the above operation, the access control machine can be added to the system.

6.1.2 Connection through RS485

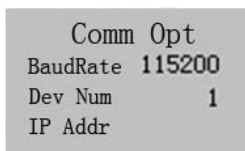
【Operation Steps】

1. Use RS485 to connect fingerprint reader and computer. Refer to *INSTALLATION GUIDE* for detailed connection methods.

Notice: RS232/RS485 converter is not contained in the standard configuration.

2. Enter “menu->setting->communication setting” to set RS485 communication method for the machine. Refer to the following picture for set result. Please pay attention to baud rate, machine ID, Ethernet, RS485 and the setting of connection password.

Notice: Connection with Ethernet must be broken when RS485 connection is open.



Net speed	Auto
IP address	
Net Mask	
Gateway	
TCP/IP	N
RS232	N
RS485	Y
Link code	0
Extern Modem	Y

3. After setting, press “ESC” to enter “save” interface, as shown below, select “OK” to save the above settings and select “ESC” to cancel saving the settings.

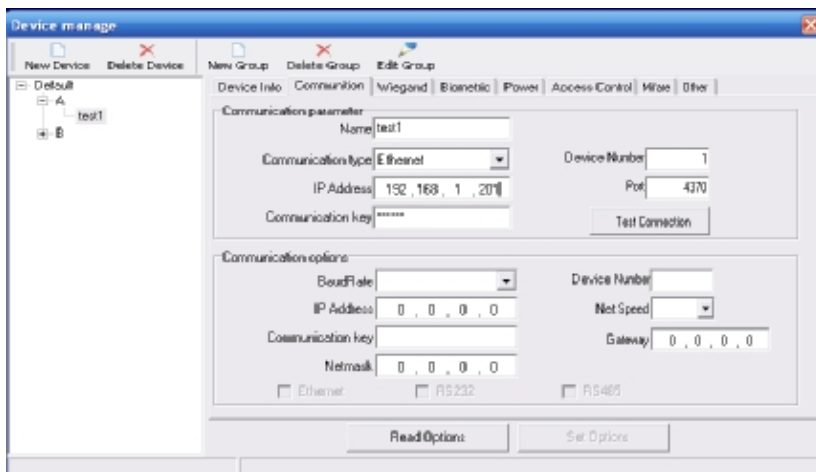
Notice: After saving the settings, the machine needs to be shut down and restarted.

Comm Opt	
Save ?	
ESC	OK (Save)

4. Open the software, enter “device management” menu to add machine. There are 2 ways:

- ┃ Click menu: basic setting-》device management
- ┃ Select “device management” directly through shortcut

5. Click “add” in “device management” window to start connection of system and machine.



6.This interface is the communication interface which connects software and machine. The information input here must agree with the “communication setting” of Step 2 machine.

Fingerprint ID must agree with “machine ID” setting of access control machine’s “communication setting”. If the reader’s setting is 1, input 1 here.

Port: Select the communication port number to connect PC and reader, and default COM1. It can be other ports, please select it carefully.

Baud rate: It is connected through RS485. 9600 (whose value agrees with the baud rate of access control machine’s “communication setting”) is suggested..

Communication password can be ignored under the condition of default. If communication password is set, input the corresponding password(5 digits at most)

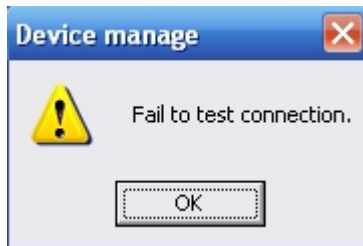
Name: Input name which is easy to remember according to device’s purpose. Later, while using this software, the reader can be

selected by selecting this name.

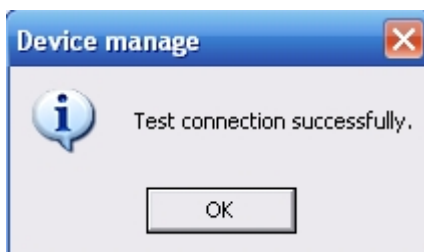


7.After setting, click “test connection”.

8.If the dialogue box of “test connection fail” appears, as shown below, please check the settings in Step 2 & 6, and repeat setting in Step 7.



9.If dialogue box of “test connection succeeds” appears, as shown below, then the connection between access control machine and system has been done.



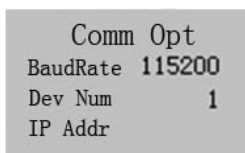
10. Through the above operation, the access control machine can be added to the system.

6.1.3 Connection through TCP/IP

【Operation Steps】

1. Use Ethernet to connect fingerprint reader and computer. Refer to *INSTALLATION GUIDE* for detailed connection methods.
2. Enter “menu->setting->communication setting” to set TCP/IP communication method for the machine. Refer to the following picture for set result. Please pay attention to IP address, network speed, Ethernet, and the setting of connection password.

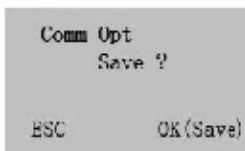
Notice: When RS232, RS485 and Ethernet are open together, only connection with Ethernet is employed. The connections with RS232 and RS485 must be broken.



Net speed	Auto↵
IP address	↵
NetMask	↵
Gateway	↵
TCP/IP	Y
RS232	N↵
RS485	N
Link code	0↵
Extern Modem	Y↵

3.After setting, press “ESC” to enter “save” interface, as shown below, select “OK” to save the above settings and select “ESC” to cancel saving the settings.

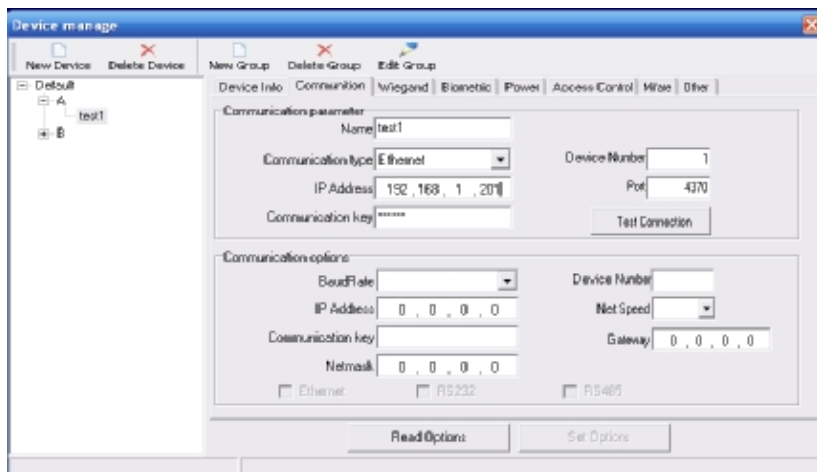
Notice: After saving the settings, the machine needs to be shut down and restarted.



4.Open the software, enter “device management” menu to add machine. There are 2 ways:

- ┃ Click menu: basic setting-〉 device management
- ┃ Select “device management” directly through shortcut

5.Click “add” in “device management” window to start connection of system and machine.



6.This interface is the communication interface which connects software and machine. The information input here must agree with the “communication setting” of Step 2 machine.

Fingerprint ID address: the default value is 192.168.1.201. IP address can be modified according to your LAN network segment. But it cannot bring conflict with any terminal address.

Port: default value is 4370, which need not modify.

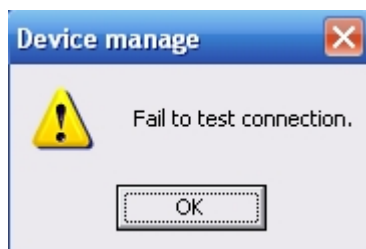
Communication password can be ignored under the condition of default. If communication password is set, input the corresponding password (5 digits at most)

Name: Input name which is easy to remember according to device’s purpose. Later, while using this software, the reader can be selected by selecting this name.

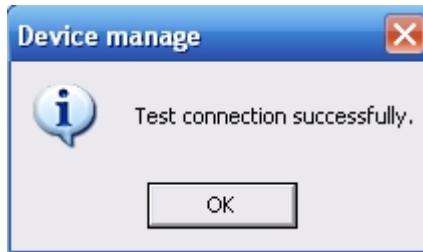


7. After setting, click “test connection”.

8. If the dialogue box of “test connection fail” appears, as shown below, please check the settings in Step 2 & 6, and repeat setting in Step 7.



9. If dialogue box of “test connection succeeds” appears, as shown below, then the connection between access control machine and system has been done.



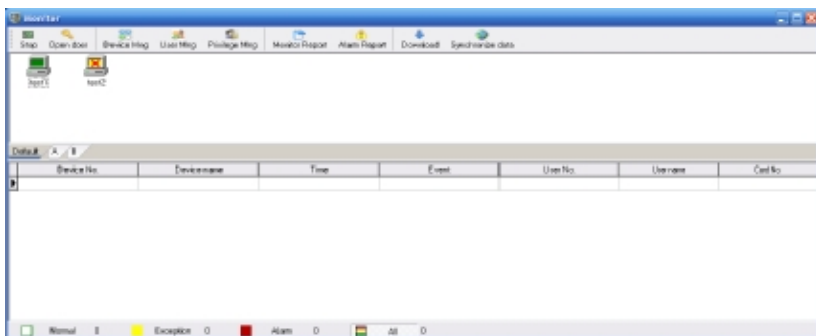
10. Through the above operation, the access control machine can be added to the system.

6.2 Real-time monitor

【Function introduction】 Monitor personnel's in-and-out at the real time and discover various abnormal state in time to ensure security.

【Operation Steps】

1. Please refer to 5.7.5 system parameter settings for parameter setting of real time monitor
2. Open real time monitor and the software will connect all the access control machines listed in the device form automatically
3. The monitoring state can be queried in monitor center.



Device of connected access control machine will glitter in red and white.

Device of unconnected access control machine will display Red Cross in the middle.

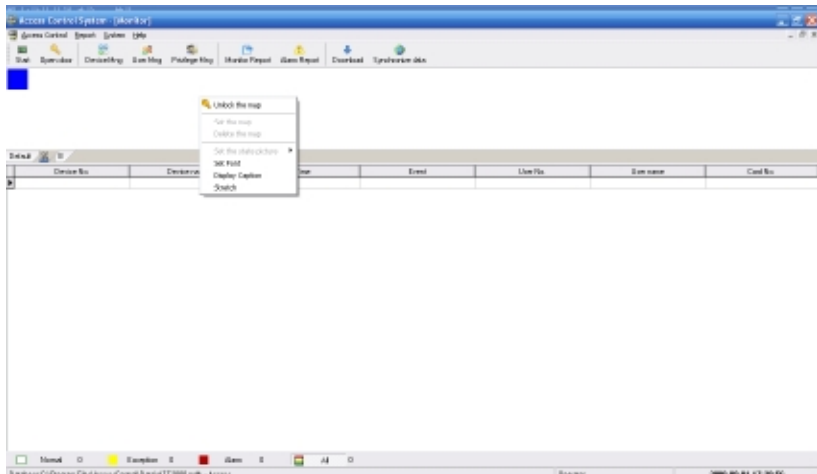
All the in-and-out states and alarm events will be recorded and displayed in the report form.

6.3 Map

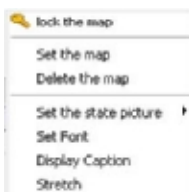
【Function Introduction】 In order to make the operator get well known in the position where various access control machines locate rapidly and clearly, electronic map function is provided by this version. The distribution of the machines is displayed in the way of map.

【Operation Steps】

1. Click “system management”->“system parameter setting”, and select [use electronic map mode].



2. Click the right key of the mouse in the blank area of the device list to select [set map].
3. Click the right key of the mouse in the blank area of the device list to select [set map] again and import the source file of the map.



Lock the map: save the edited map and exit edition.

Set the map: import the source file of the map.

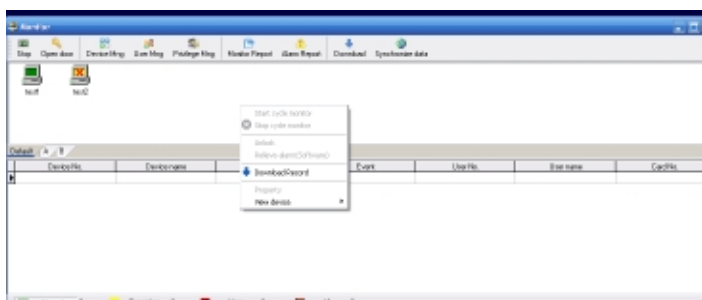
Delete the map: delete the imported source file of the map.

Auto-align: align the devices' icons.

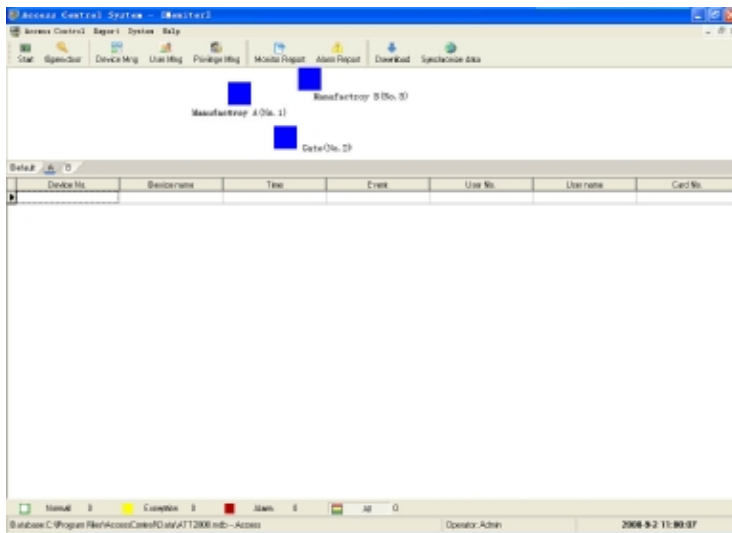
Set pictures: set the pictures in various states.



4.Click the right key on “device” and select “properties” , you can detect the device’s information.



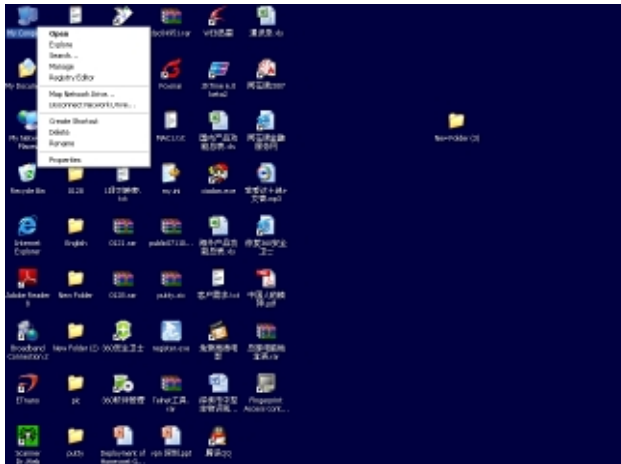
5.Move the device to the corresponding position on the map, and click the right key to select [lock the map].



6.4 License to detect the fingerprint device

【Operation Steps】

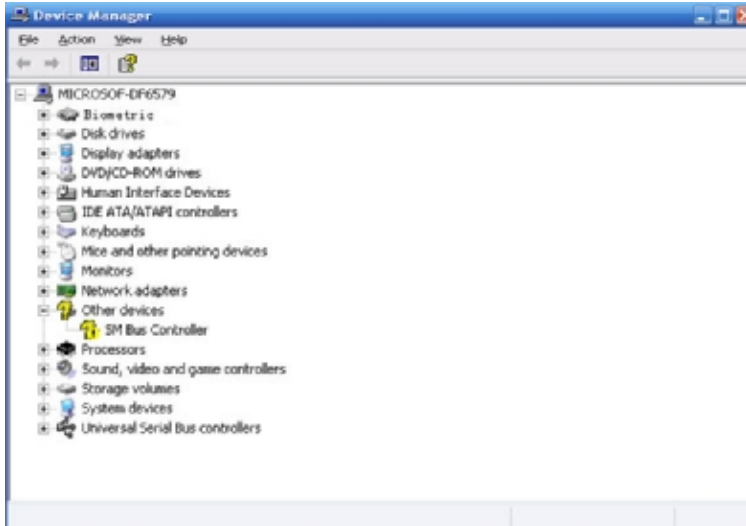
1. Click “my computer” by using the right key of the mouse, and select “properties”, as shown below:



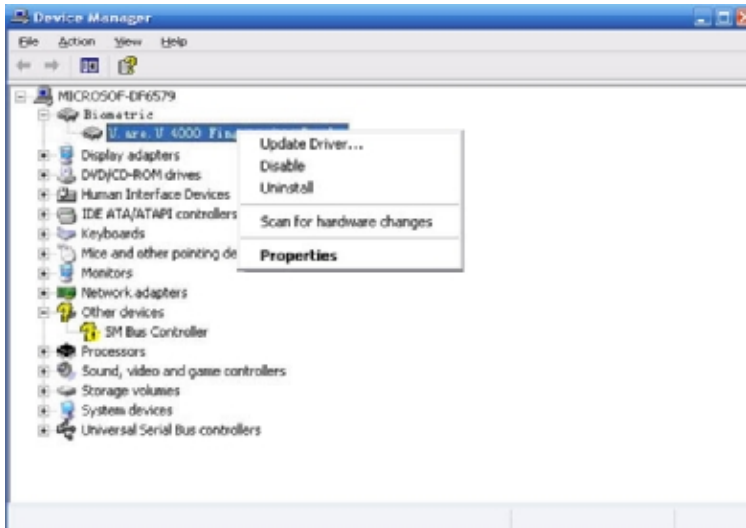
2. Enter the dialogue box of system properties, select “hardware”, and click “device manager”, as shown below:



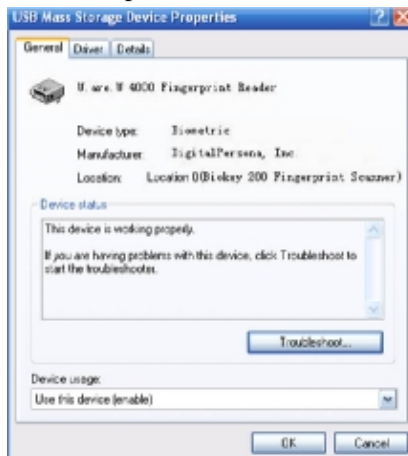
3. Device named “Biometric” can be found in “device manager”, as shown below:



4. Click the device with right key, and select “properties”, as shown below:



5. Detect the device's properties, type, manufacturer and position as shown below. The device possesses SDK license.



7. Solution to problem

Q: How to set Wiegand?

R: For Wiegand26/34, input 26 or 34 in Wiegand item of “device manager”, the definitions of other formats are as the following:

Wiegand26: with DeviceID:PeEEEEEEEEEEOOOOOOOOOOOOP

Efficacy bit, E (even) O (odd), e device ID, E UserID

Without DeviceID: PEEEEEEEEEEEEEOOOOOOOOOOOOP

Q: What baud rate is suitable for 485?

R: Sometimes, baud rate of 115200 can be employed to connect the machine, but 38400 is recommended in this software to ensure high communication quality.

Q: How to delete a user’s information from one or more than one device?

R: Enter “user management” interface, select the user to be deleted, click “detect affiliated device”, select user in the pop-up window, and click “delete user from device”.

Q: How to delete more than one user from a device”?

R: Enter “privilege management” interface, select “device” in the list, click “detect device user”, select the user to be deleted in the pop-up window and click “delete user from device”.

Q: How to delete user’s unwanted fingerprint information from the device?

R: Select and click “user” on “user management” interface with the

right key, click “detect fingerprint state”, select the fingerprint to be deleted in the pop-up window, and click “ delete from device”.

Q: How to control user’s privilege?

R: Refer to the relation diagram (user defined privilege, access control group and group) in Chapter 5.3.

8. SOFTWARE USE LICENSE AGREEMENT

《End User Software License Agreement》

LICENSE:

ZKSoftware will grant you the use right of this software program, but you must ensure: don't use, copy, edit, rent or attorn this software or any parts of this software beyond the terms in this agreement.

YOU MUST ENSURE:

1. Only use this software in one computer.
2. In order to be used in this computer, the system's copy must be made in readable format to prepare backup or manage files.
3. The system and the license agreement can be attorney to the third party under the condition that the third party accepts the terms of this agreement. When attornment happens, the original files and their copies must be attorned together, or destroy all the copies which are not attorned.
4. Only use this software in multi-user environment or network system in one of the conditions below:
 - ⊙There is proclamation which allows using this software in multi-users environment or network system;
 - ⊙or every node/end has purchased the using license of this software.

OTHER RESTRICTIONS:

1. Don't attorney the system's license again,
2. Don't decompile, disassemble, or reverse-engineer this software,
3. Don't copy or attorney this system or any parts of the system beyond the terms of this agreement. Your license will end automatically when this system or all or parts of this system are

attorned to the third party.

COPYRIGHT AND PROPERTY:

The name of this software and its duplications must be together with the company indicated in CD or in software.

The software and its documents are protected by copyright laws and international treaty provisions.

You cannot delete the copyright announcement from the software, and guarantee to replicate the copyright announcement for the duplications of the software. You agree to stop any illegal duplicating actions for this SOFTWARE and its documents.

LIMITED WARRANTY:

ZKSoftware warrants that if use the software in normal condition, there will be no materials or craft defects in software in 90 days since the sell date. If there is defect indeed after validation, ZKSoftware's responsibility is to change good software for you as the only compensation.

If the defects are caused by accidents, or misuse or incorrect use, this warranty will be of no effect.

The warranty days for the exchanged software are the rest of the warranty days of the original software, or 30 days if the rest of days are less than 30 days.

NO OTHER WARRANTIES:

There are no any other warranties besides the above ones.

LIMITED LIABILITY:

The above warranty refers to all, both pointed content and implied content, including, commodity and adaptability of special application purpose. Whether both parties abide by this agreement or not, ZKSoftware and its agent & seller have no responsibility for the profit loss, lost availability, business interruption, or any indirect, special,

inevitable damage, or any compensation claim brought by this system, even if ZKSoftware is informed in advance that such things can happen.

TERMINATION

Without prejudice to any other rights, ZKSoftware may terminate this agreement if you fail to comply with the terms and conditions of this agreement. In such event, you must destroy all copies of the software and all of its component parts, or give them back to ZKSoftware.

GOVERNING LAWS:

INTELLECTUAL PROPERTY RIGHTS PROTECTION ,
COPYRIGHT LAW, and PATENT LAW and so on.