



**NETWORK
TECHNOLOGIES
INCORPORATED**

1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.networktechinc.com

ENVIROMUX-FACS

Fingerprint Access Control System

Access Control Software User Manual

Version: 2.4.4.1040

Date: Dec. 2011

Table of Contents

| | |
|---|----|
| 1. Install and Uninstall Software | 1 |
| 1.1 Install Software | 1 |
| 1.2 Uninstall Software | 4 |
| 2. Department Management | 5 |
| 3. User Management | 8 |
| 3.1 User Fingerprint | 8 |
| 3.2 Statistic | 14 |
| 3.3 Upload and Download | 18 |
| 4. Device Management | 20 |
| 4.1 Device Information | 22 |
| 4.2 Communication | 23 |
| 4.3 Wiegand | 24 |
| 4.4 Verification | 27 |
| 4.5 Power Management | 28 |
| 4.6 Access Control | 29 |
| 4.7 Mifare | 30 |
| 4.8 Other Setup | 30 |
| 4.9 U disk Settings | 31 |
| 5. U Disk Management | 34 |
| 5.1 Import User Data | 34 |
| 5.2 User Data Export | 36 |
| 5.3 Record Data Import | 36 |
| 5.4 Import Photos | 37 |
| 6. SMS Management | 39 |
| 6.1 SMS Content Management | 39 |
| 6.2 Employee SMS customization | 41 |
| 7. System Management | 44 |
| 7.1 Administrator Management | 44 |

| | |
|---|----|
| 7.2 System Operation Log | 45 |
| 7.3 Data Maintenance | 46 |
| 7.4 System Initialization | 47 |
| 7.5 Set Database..... | 47 |
| 7.6 Set Password of Database..... | 49 |
| 7.7 System Options | 51 |
| 8. Access Settings | 54 |
| 8.1 Time Zone | 54 |
| 8.2 Group..... | 55 |
| 8.3 Unlock Combination | 57 |
| 8.4 Access Levels..... | 59 |
| 8.5 Holidays setting | 65 |
| 8.6 Upload Setting..... | 67 |
| 9. Other Function | 69 |
| 9.1 Start Monitor | 69 |
| 9.2 Download Log | 69 |
| 9.3 Clear Log..... | 70 |
| 9.4 Sync Time..... | 70 |
| 9.5 Update Firmware..... | 70 |
| 9.6 Restart Device..... | 70 |
| 9.7 Property | 70 |
| 9.8 Stop Sound | 71 |
| 9.9 Open Door..... | 71 |
| 10. Record Management..... | 72 |
| 10.1 Record Query | 72 |
| 10.2 Alarm Report | 74 |
| 11. Appendix | 76 |
| 11.1 Common Operation | 76 |
| 11.2 FP, FP Device and Card User Guide..... | 80 |


Table of Contents

11.3 Fingerprint Algorithm License..... 84
11.4 SOFTWARE USE LICENSE AGREEMENT 87

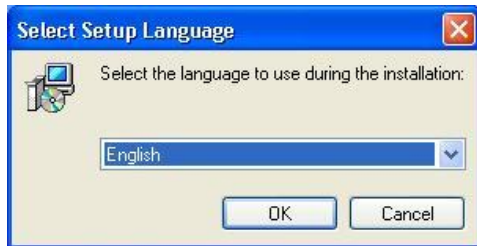
1. Install and Uninstall Software

1.1 Install Software

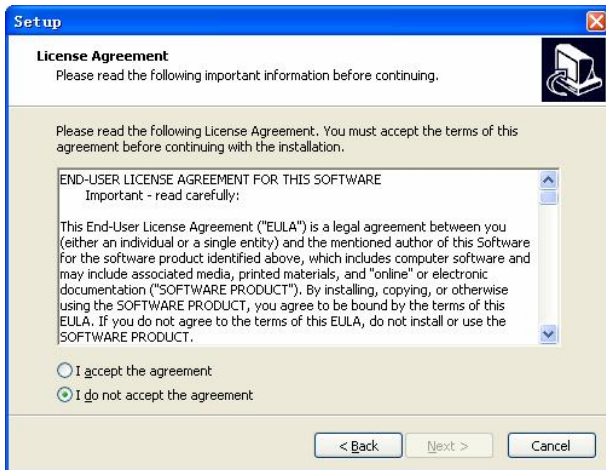
Before installing your software, it is better to shutdown all the other application programs, in order to keep away conflict in installing process.

 **Note:** The following screen may differ from what you see upon CD installation. Please refer to CD installation.

1. Please put the software CD into CD-ROM, it will run automatically and pop up the following dialog.

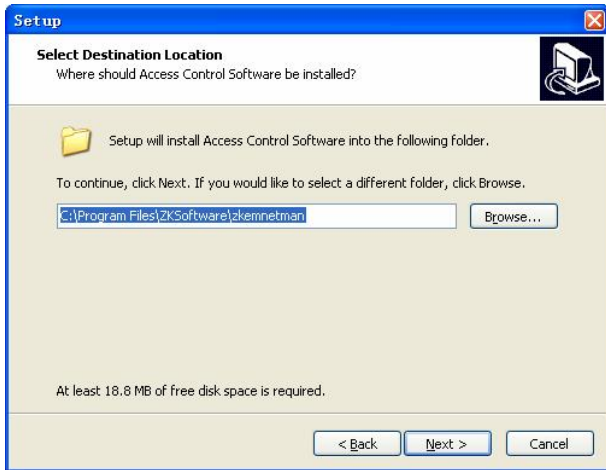


2. Select the Language, click [OK], and enter the following interface.

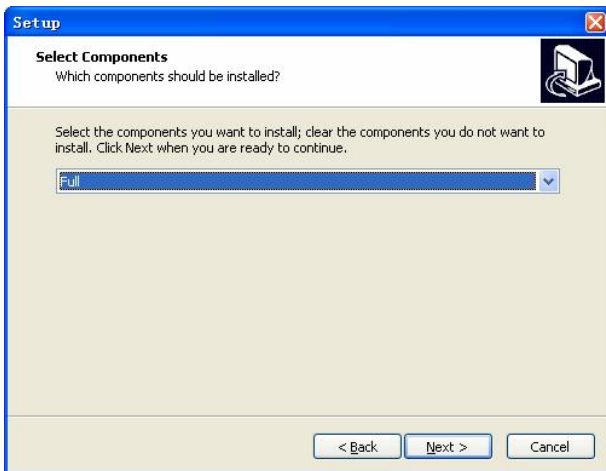


3. Please read the Agreement carefully. If you want to install please select [I

accept the agreement], and click **[Next]**, enter the following interface.

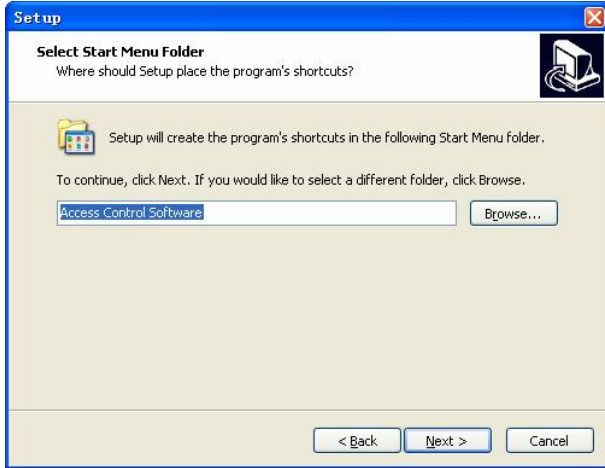


4. Select the folder where to install the software. Click **[Next]** to enter the following interface.



5. Select the install component, and click **[Next]** to continue.

1. Install and Uninstall Software



6. Click **[Install]**, the installing program will copy and write corresponding information into hard disk. After finish installation, click **[Finish]** to complete the process.



1.2 Uninstall Software

If you do not need to use this software any more, and want to uninstall it from your computer, then may follow next steps to operate:




1. Close the Access Control Software complete.
2. Open the **[Control panel]** in the **[Start]** menu.
3. Enter **[Add and Cancel Program]** window, choose Access Control Software, and click **[Remove]** button to uninstall.

Like doing this, you still cannot delete all files. You need enter the installation directory of the software to delete the folder where the software installed.


2. Department Management

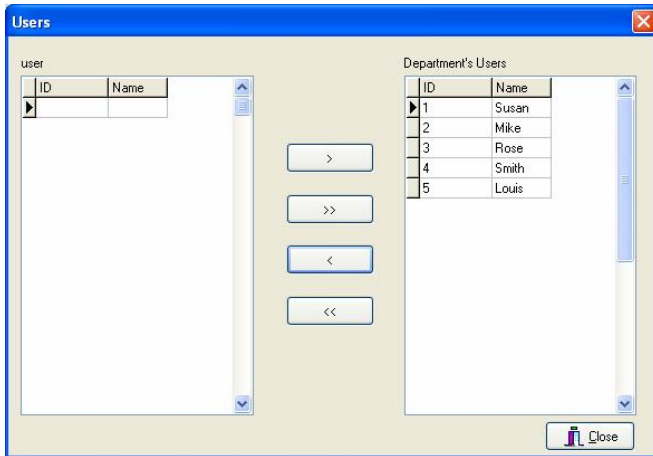
Click [Department Management] in the [Basic Options] menu, popup the department management interface, like as following figure.



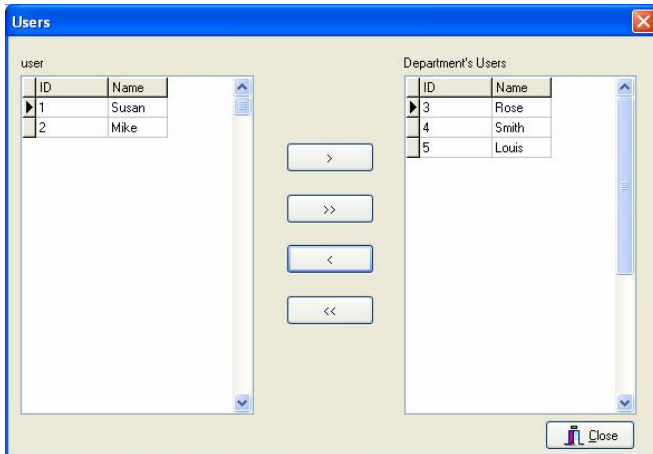
Click  or  to add or delete a department,  is [User] Button.

Employ user to the department: First to select the name of company, then click [User] button, popup following interface.

 **Note:** To shift a user can also directly process in the [User Management] interface.

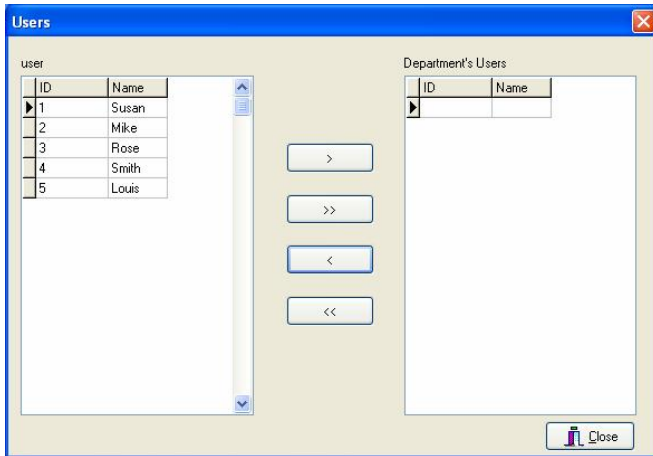


[Department's Users] box at right side is the users list of company, first choose the user to shift, and then click the "<" button to move the user to the left side, or click "<<" button to move all users to the left side.

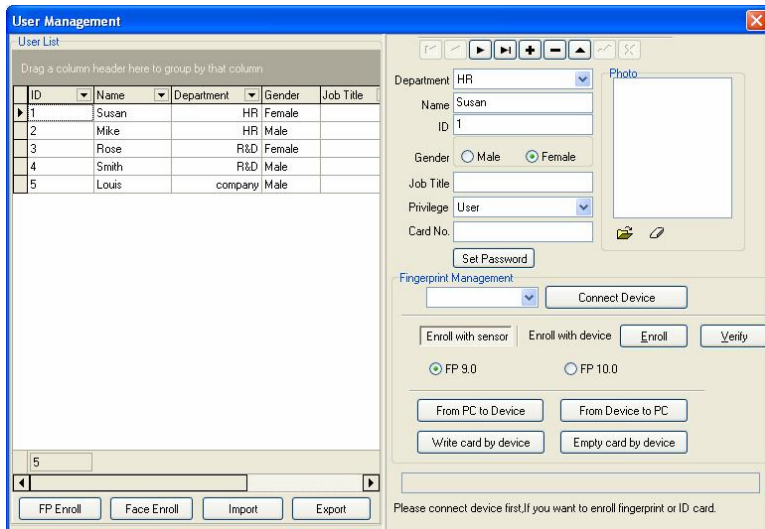


Select a department, click [User] button, the interface as shown below.

2. Department Management

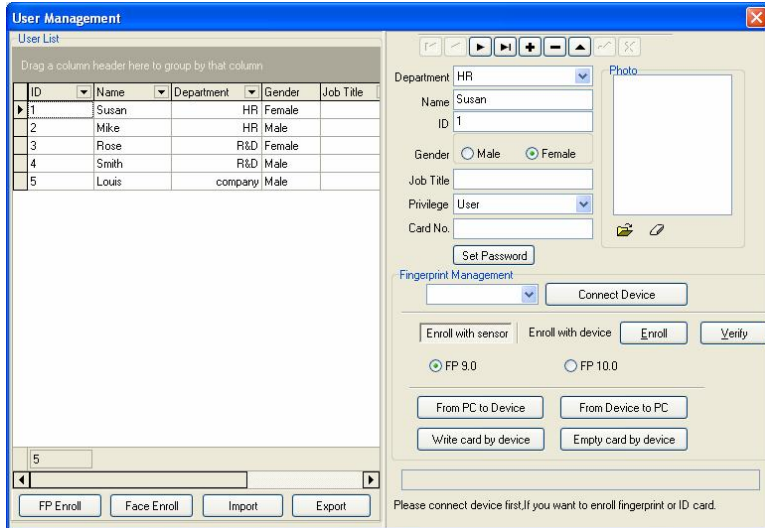


Select the user to employ, click “>” to move the user to the right side of related department, or click “>>” button to move all users to the right side to complete shifting the users.



3. User Management

User Management is the process to manage the user information, click **[User Management]** in the **[Basic Options]** menu or the shortcut button, popup the user management interface, as following.



Add User: Click  button in the user management bar to add new user.


Cancel User: Choose the user you want to delete, and click  button to delete the user.

Photo: Click  button to import user photo, or click  button to delete.

3.1 User Fingerprint

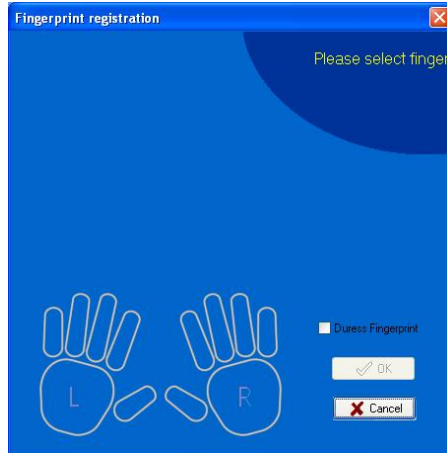
1. Enroll User Fingerprint

Enroll with FP Sensor:

If you need to use the FP Sensor to enroll fingerprint, please install the FP sensor driver program first. The driver is under the **[Driver]** directory in installation CD. After complete to install the driver, connect the FP sensor to the PC USB port. The current software version supports to use the "UareU" series,

FP sensor etc.

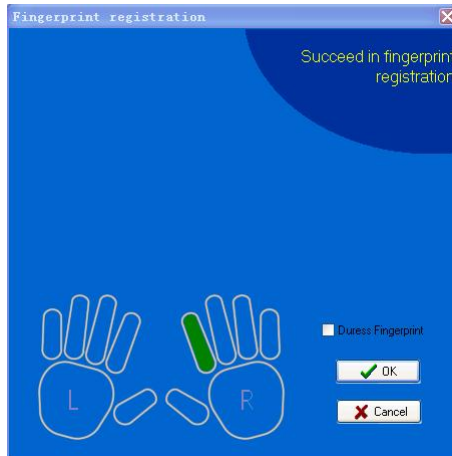
(1) Select **[Enroll with Sensor]** in user management interface, click **[Enroll]** button, and enter the fingerprint enrollment interface, as shown below.



(2) Click the finger image you want to enroll, and the system enter the interface of enrollment, as shown below:



(3) After the finger finishes 3 times press on the FP sensor, the system prompt **[Succeed in fingerprint registration]**, shown as below.



(4) Click **[OK]** after successful enrollment, save the fingerprint and return to user management interface.

(5) Click **[Verify]**, the following interface will appear to check if the fingerprint enrollment is succeed or not.



(6) Press the enrolled finger on the sensor, the following dialog appear when the sensor collect the fingerprint, that is, fingerprint enroll succeeds.



If the following dialog appears, then the enrollment failed, please return to enroll once again.



(7) If you want to delete the fingerprint, please double click this finger, the system prompts the following:




(8) If you select [**Duress Fingerprint**], the enrolled fingerprint will be a duress fingerprint for use.

Enroll with FP Device:

Use the FP device to enroll fingerprint. Select [**Enroll with Device**] in User management interface, click [**Connect Device**], and the button will turn to [**Disconnect**] when the connection completed. Click [**Enroll**] button, and enter the fingerprint enrollment interface. The FP device enrollment is similar to FP sensor, except there is no verification process for FP device.

2. Register Mifare Card:

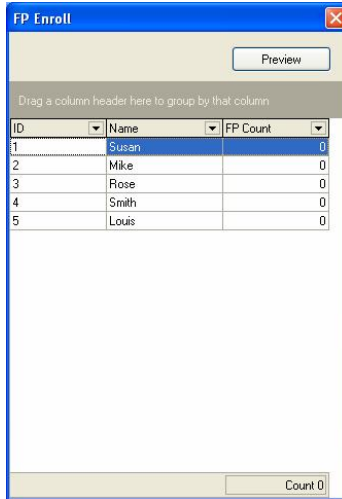
Choose the user who needs to register the Mifare card. Click [**Write Card by Device**], and swipe the card near to the card sensor area of the FP device when the software reminds [**Present Card**]. If the device prompts [**Write Card Successfully**], this user's ID and the fingerprint will be stored in the card. Click [**Empty Card by Device**] to delete user's data in the Mifare, swipe the card near to the card sensor area of the FP device when the software reminds [**Present Card**]. The notice [**Clear Card Successfully**] means the operation completed.

 **Note:** This function is available only for the FP device that supports Mifare

3. User Management

card enrollment.

3. Fingerprints Enroll Status: Shows the detail of user information and fingerprint enroll status.



FP Enroll

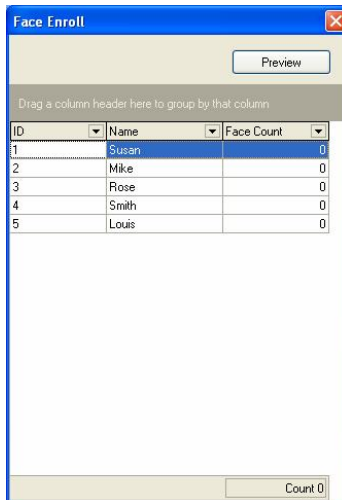
Preview

Drag a column header here to group by that column

| ID | Name | FP Count |
|----|-------|----------|
| 1 | Susan | 0 |
| 2 | Mike | 0 |
| 3 | Rose | 0 |
| 4 | Smith | 0 |
| 5 | Louis | 0 |

Count 0

4. User face Enroll Status: Shows the detail of user and face enroll status.



Face Enroll

Preview

Drag a column header here to group by that column

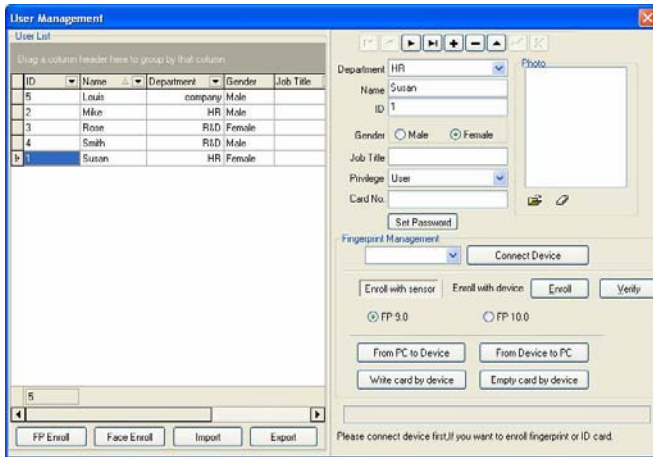
| ID | Name | Face Count |
|----|-------|------------|
| 1 | Susan | 0 |
| 2 | Mike | 0 |
| 3 | Rose | 0 |
| 4 | Smith | 0 |
| 5 | Louis | 0 |

Count 0

5. Sort Order:

You can arrange the records according to the ascending or descending order in the record list, directly click the head of rank to achieve. Choose a triangle symbol, which is beside the field, according to ascending order to arrange when the triangle symbol point upwards, otherwise that means the sort order follow the descending order. You can click the triangle symbol to change the rise or down rank.

As figure below, sort the users as the name order.




3.2 Statistic

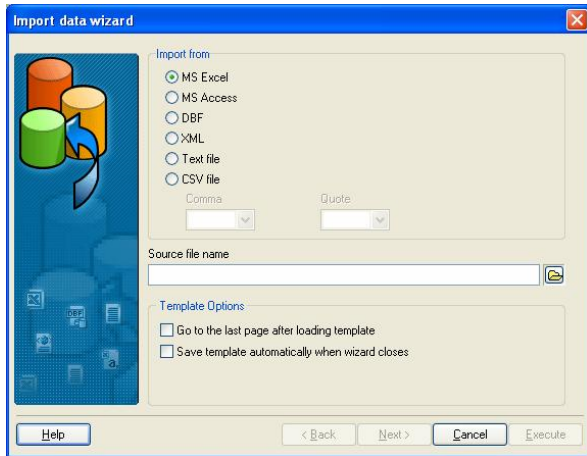
The software can automatically count the total records and count the grouping records.

1. Import

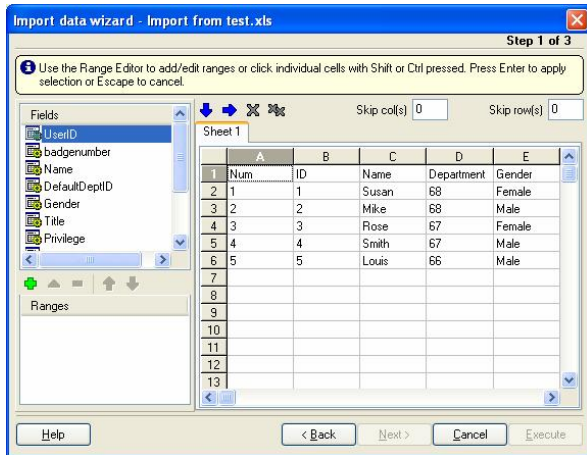
This function enables the user to import many formats of user's data file, such as MS Excel, MS Access, DBF, XML, Text File, CSV file. We recommend using the CSV file to import. The following example is using text file to import user's data.

(1) Firstly, click  button to select a file to be imported.

3. User Management



(2) Click [Next] button, the following figure appears:



On the left side, there is the field list, and the right side is the importing file rank. The Skipcol(s) on the right-up part means how many columns to skip. The Skiprow(s) means how many rows to skip. If the first line of the importing file is not the material data, you can fill "1" in Skiprow(s) blank that shows to skip the first line for importing data.

UserID: The ID is using for system internal, it is useless for file import, please do

not use it.

BadgeNumber: User code, this code is the user number used in the FP device and the software.

Name: User name, this field must exist.

DefaultDeptID: It indicates the Department ID. If you import the data from other sources, you can neglect it.

Gender: Select Male or Female.

Title: Select the title.

Privilege: Privilege, you can neglect it.

Password: Password, you can neglect it.

CardNo: ID card number, you can neglect it.

MverifyPass: The user password used in the device, you can neglect it.

VerificationMethod: The verification method set for user. You can neglect it.

(3) Firstly, choose the field in the fields list as to import, and then select the corresponding rank in the right side list. The fields list will automatically attach the corresponding number to the name of field, such as it is, arrange all fields and corresponding rank after finish it, move to the next step.

If you want to cancel a field, first choose the field, and then click corresponding rank, the software will cancel this field.

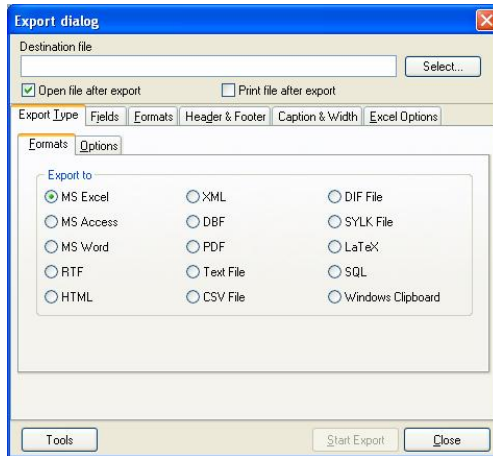
(4) Click the [**Execute**] button to run importing operation.

2. Export:

This function enables the software export user's data via all kinds of format that the software supported. It is convenient to supply for other software to use.

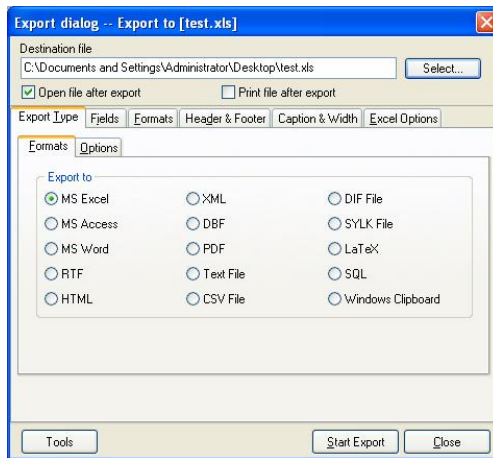
Click the [**Export**] button, the following interface appears.

3. User Management



Take the exporting MS Excel file as an example for explanation.

(1) Select the object file to export.



(2) Click [**Start Export**] button to export the file via default format. Otherwise, you can configure exporting content through the following optional items.

Fields: Select the field to export, the default is all, otherwise it is only to export the selected field's content.

Formats: The exporting format that all kinds of defined field value.

Header & Footer: It indicates the start and the end of the file to export.

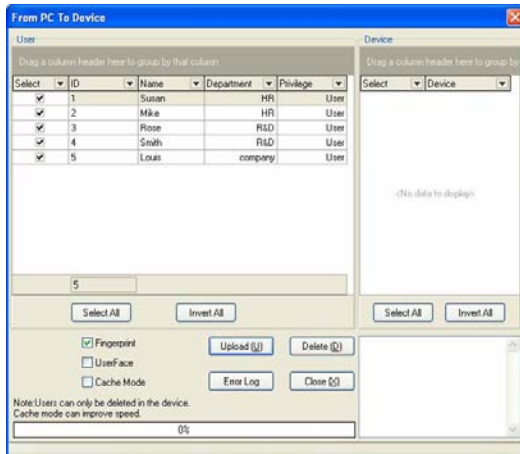
Caption & Width: It indicates the title and width of the field.

Excel Options: Set font.


3.3 Upload and Download

1. From PC to Device:

The user that stored in the database can upload to the FP device, click [**From PC to Device**] in the user management interface, or click the [**PC to Device**] shortcut in the main interface, popup the following interface.



Upload: Based on your need, select the user and an uploading FP device, click [**Upload**], it is able to upload user's data to the defined FP device, it is better to select [**Fingerprint**] and [**User Face**] in the normal condition. If the information needs not to modify, it is no need to choose it.

 **Note:** User's data include user information, fingerprint, and user face.

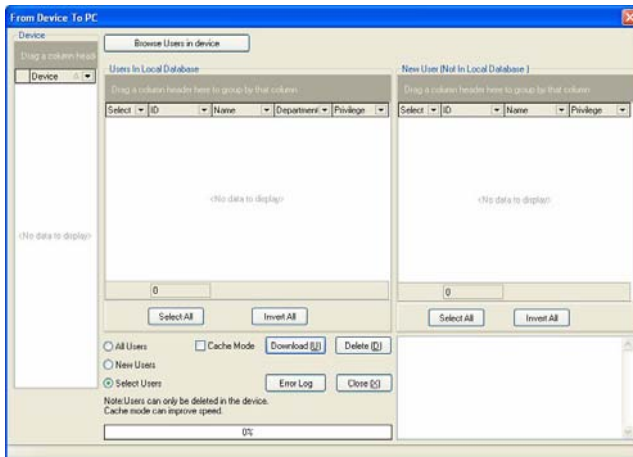
Delete: If you want to delete a user in a FP device, first choose the user and the corresponding FP device, and then click [**Delete**] button.

Operation Log: Indicates the error log during operating process.

Batch: You can use this function to speed up communication when uploading many of user's data, it need not for a few users (such as less than 30 users).

2. From Device to PC:

Download the user data from the FP device to the local database. Click [**Form Device to PC**] in the user management interface, or click the [**Device to PC**] shortcut in the main interface, popup the following interface.



Select a FP device to download user's information that is on the left side list, click [**Browse Users in Device**], all users in the FP device displays. Select the user need to download, click the [**Download**] button to download the user data from FP device to local database.

View User in the Device: Display all users in the FP device.

Download: Download user data.

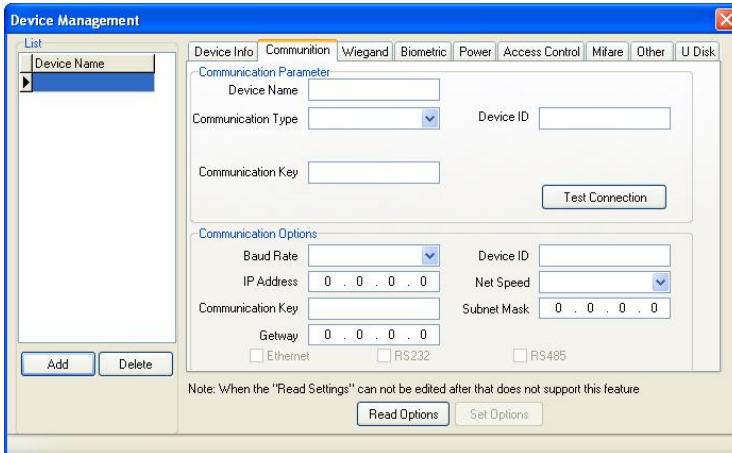
Delete: If you want to delete a user in a FP device, first choose user, and then click [**Delete**] button.

Batch: You can use this function to speed up communication when downloading many users, it need not for a few users.

Operation Log: Indicates the error log during operating process.

4. Device Management

Open [Device Management] in the [Basic Options] menu, or click [Device Management] shortcut on the main interface, and display the interface as following.



Click [Add] button, the following interface displays.



RS232/RS485 Communication:

Device ID: According to the device ID to fill, for example the FP device ID is 1.

Port: Properly select the communication port to connect PC, the default port is COM1.

Baud Rate: Select the same Baud Rate as the FP device. The default value is 38400 at its original setup.

Communication key: It is not need to fill the password in the default condition, if there is a setup password in the FP device, please input the correct password.

Device Name: According to the purpose of the device, input an observable name.

Ethernet Communication:



The screenshot shows a dialog box titled "Connect to Device" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Communication Type:** A dropdown menu set to "Ethernet".
- IP Address:** A text input field containing "192 . 168 . 1 . 201".
- Port:** A text input field containing "4370".
- Communication Key:** An empty text input field.
- Device Name:** A text input field containing "New Unit".

At the bottom of the dialog, there are three buttons: "Connect", "OK" (with a green checkmark icon), and "Cancel" (with a red X icon). Below the buttons, a note reads: "If you don't set the Comm Key in device,you not require input commun".

IP Address: The default IP address is 192.168.1.201. Please input the IP address of the device you want to connect.

Port: The default port is 4370. You need not to change it.

Communication key and Name is the same configure as **RS232/RS485**.

USB Communication:

This communication mode needs the device to support USB communication.



Device ID, Communication key and Device Name is the same configure as **RS232/RS485**.

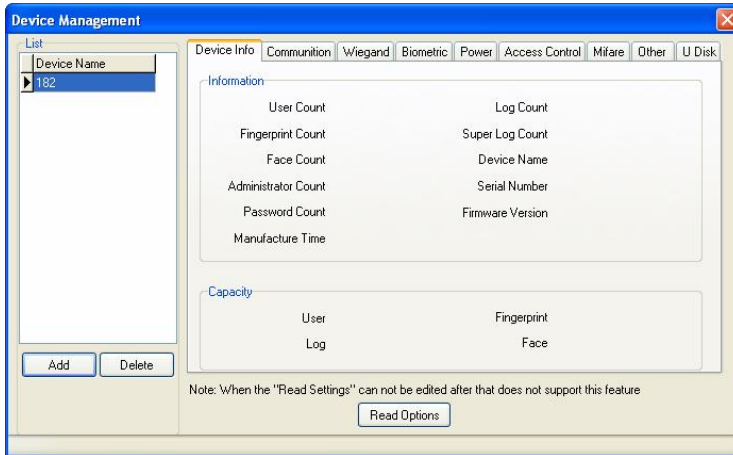
After setup, click [**Connect**] button under the window to test. If the system popup [**Successfully Connect**], click [**OK**] button to save the connecting parameters of this FP device. If the system popup [**Fail Connect**] dialog, please check the parameters and try again. Add the other fingerprint device as this procedure.

If you want to delete a FP device, select this unit, and click [**Delete**] button on underside.

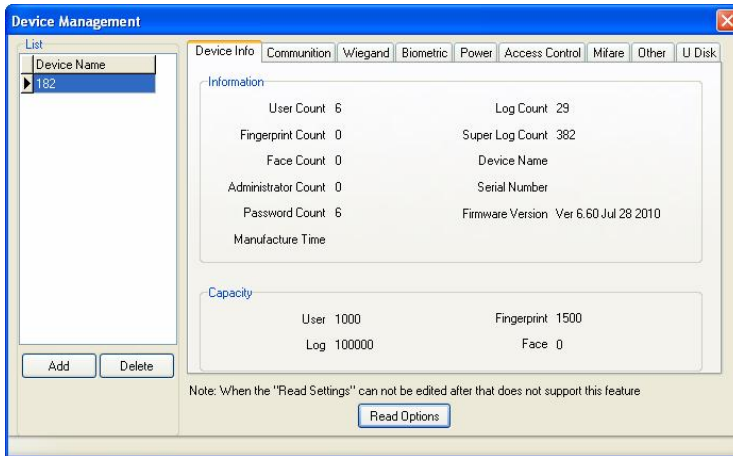
4.1 Device Information

Click [**Device info**] in the [**Device management**] item, display the following interface.

4. Device Management



Click **[Read Options]**, the basic information of FP device will display, as the following figure.



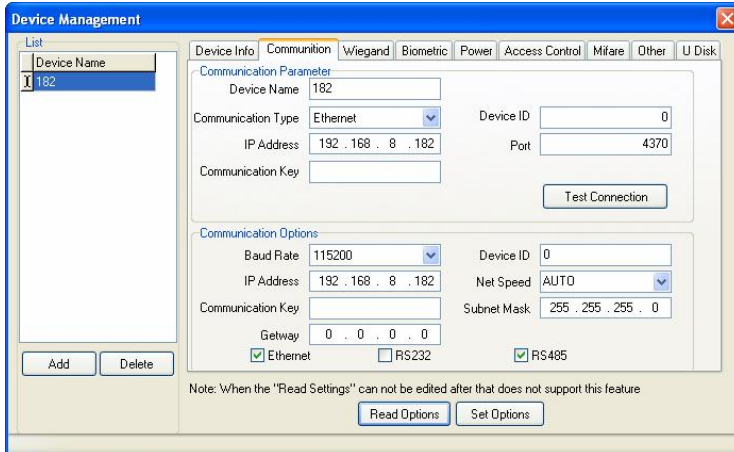
4.2 Communication

Communication Setting: Click **[Read Options]**; it shows the communication information of the current connecting device. Like as below figure.

Communication Parameter: It indicates all kinds of communication parameters

set for the connection of the software and the device.

Communication Options: It indicates the options of FP device communication. If you want to change the communication configure, first click **[Read Options]** to obtain all origin parameters, modify it as needed, and then click **[Set Options]** button, the modification will take effect after you restart the device.

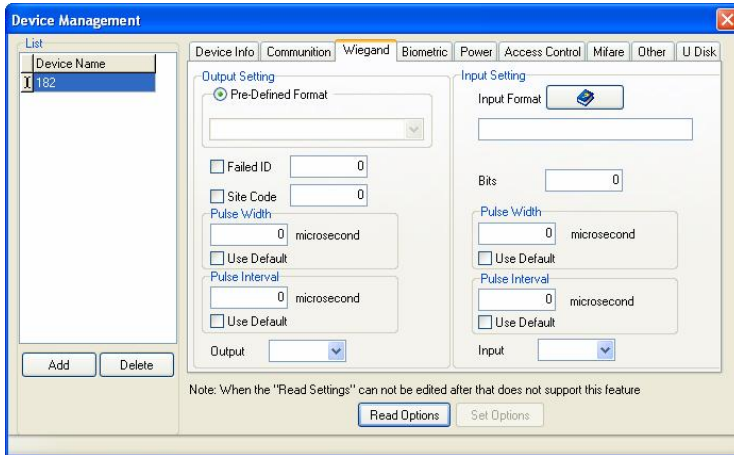


Note: If you use RS232 to communicate, recommend to adopting 115200 Baud Rate, if you use RS485 to communicate, better to use 38400 Baud Rate.

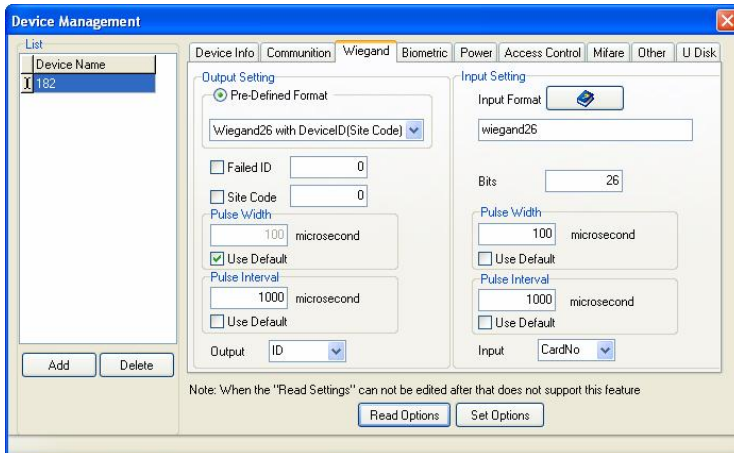
4.3 Wiegand

Click **[Wiegand]** in the **[Device Management]**, display the following interface.

4. Device Management



Click **[Read Options]** can obtain all the device wiegand parameters.



Wiegand Setting includes Wiegand **output** and **input** setting.

Defined Format: Indicates the formats defined and built in the system. User needs not to define the length of bit and the location of information. There are four default defined formats: **wiegand26 with device ID**, **wiegand34 with device ID**, **wiegand26 without device ID**, **wiegand34 without device ID**.

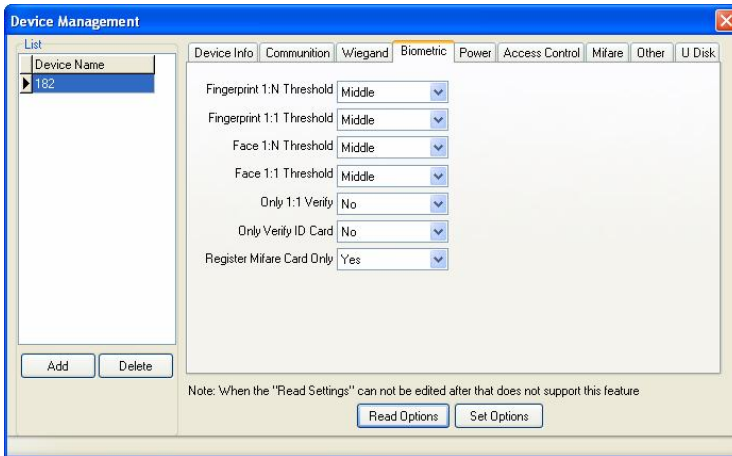
The **wiegand 26 with device ID** means that the wiegand26 output format along

Pulse Interval Time: The default value is 900 μ s, can adjust from 200 to 20000.

Input/Output contents: The options are ID and Card Number.

4.4 Verification

Click [**Biometric**] in the [**Device Management**] item. Click [**Read Options**], the following interface displays.



Fingerprint 1: N Threshold: The default value is Middle. You can modify it properly.

Fingerprint 1:1 Threshold: It means the fingerprint verification threshold after presenting the card. The default value is Middle.

Face 1: N threshold: The default value is Middle. You can modify it properly.

Face 1:1 threshold: It means the threshold of user face verification after presenting the card; the default value is Middle.

Only 1:1 Match: This feature is only available that a user own fingerprint, ID card or Mifare card for verification, if you choose [**Yes**] to this setup, must first present a card, and then press fingerprint. If does not slide a card, there is no reflect to fingerprint in the device.

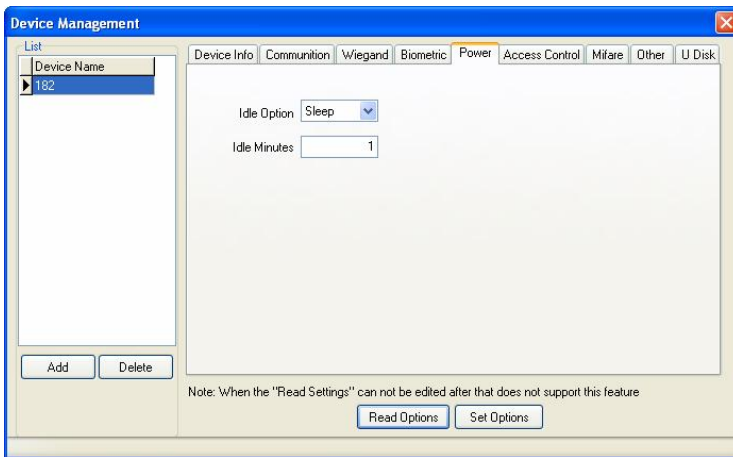
Only Verify ID card: It is mainly design for ID card. When you choose [**Yes**], a

user use ID card to verify directly, and need not to press fingerprint. When you choose it as **[NO]**, you must verify fingerprint after present the card.

Must Register Mifare Card: There are two statuses to register a Mifare card, if the card was configure to **[Must Register]**, it is only to verify the user whose ID has stored in the FP device. The user without ID number cannot verify. When you choose the item as **[NO]**, whether there is user's ID information in the device or not, it will export after the user and fingerprint template verified successfully.

4.5 Power Management

Click **[Power]** button, and then click **[Read Options]** button, display the following interface.

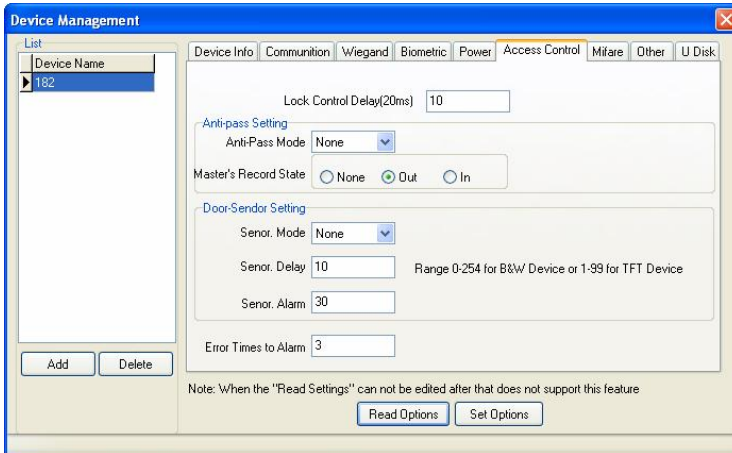


Firstly, read the parameter of **[Power]**, modify the state of **[Idle Setup]** and minutes of **[Idle Time]**, then click the **[Set Options]**, and restart the device to complete setting.

When the idle time is **[0]**, then the idle setup function is invalid. When the value more than **[0]**, the device will enter the idle state after arrives at the defined time. You can resume normal working state by press the button on the device.

4.6 Access Control

Click [**Access Control**], and then click [**Read Options**], display the following interface:



Lock Control Delay: Apply to determine unlock hour, the minimum measured unit is 20 ms, in the normal condition that is 100-200 ms.

Anti-Pass Mode: It can be set to **None**, **Out**, **In**, **InOut**.

Master's record state: It can be set to **None**, **Out**, **In**.

Sensor Mode: Set the door sensor mode. It can be set to **None**, **NOpen**, **NClose** state.

Sensor Delay: Set the sensor delay time when the door is open. The sensor detects the door state only after this defined time. If the door state is not consistent with this parameter, it will trigger the alarm. Black and white screen device range is 0-254. Color screen device range is 0-99.

Sensor Alarm: Set the alarm time delay after triggering the alarm. Range is 0-999 seconds.

Error times to alarm: Define the maximum error times to trigger alarm. When the verification is not through, and exceed this defined times, it will trigger the alarm signal automatically.

4.7 Mifare

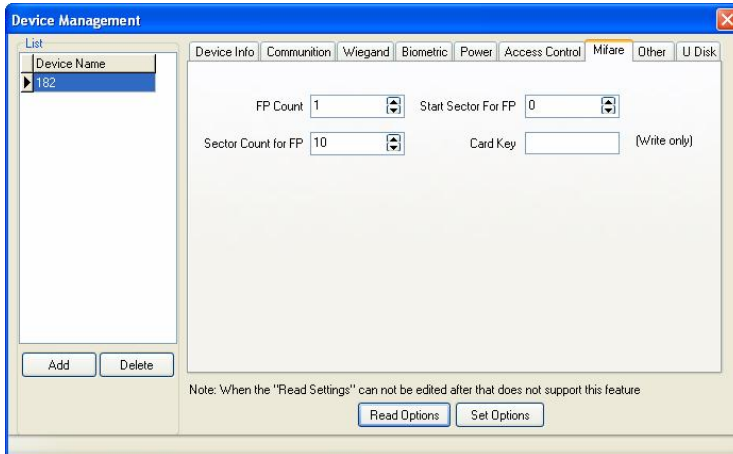
Click **[Read Options]** in **[Mifare]** menu, display as following.

FP Count: How many fingerprints stored in the Mifare card.

Start Sector for FP: The first sector of Mifare card to store fingerprint.

Sector Count for FP: The total sector that fingerprint occupied.

Card Key: Read and write password of card, you can only setup, cannot read it.



4.8 Other Setup

Click **[Other Setup]**, and then click **[Read Options]**, the following interface appears.

Restart Device: Click the button to restart FP device.

Power off Device: Click the button to power off the FP device.

Update firmware: **Note:** Please do not upgrade the firmware at your discretion because it may bring problems and affect the normal use of the device. Contact our distributors for technical support or upgrade notification.

Clear admin privilege: This function can clear all administrators' privilege that have registered in the device.

Initial Device: You can use this function to clear all data in the FP device.

Sync time: Synchronic the device time with the PC time.

Capture Fingerprint: You can use this function to view the fingerprint image. If you want to check the fingerprint image, please place the finger on the sensor window, then click the button, and will see the fingerprint image.

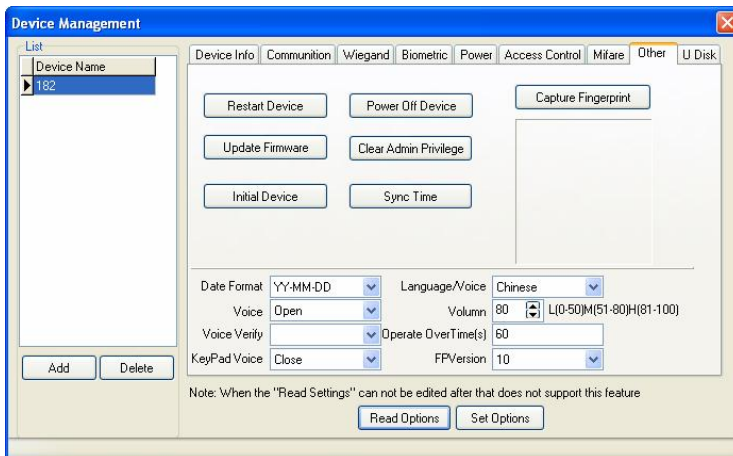
Date format: Select the date format in the down drop menu, this date format is the date display format on the starting interface of the device.

Voice function: Including **voice**, **voice verifies**, **keypad voice**, you can choose to open or close. You can set the **voice volume** too. This function is available in the FP device that supports voice hint function.

Operate over time(s): Set the device operation timeout.

Operate Over Time: Set the device operation overtime, 30s by default.

FPVersion: Select the fingerprint algorithm version (9.0 or 10.0). The two versions are not compatible. Please choose it carefully.

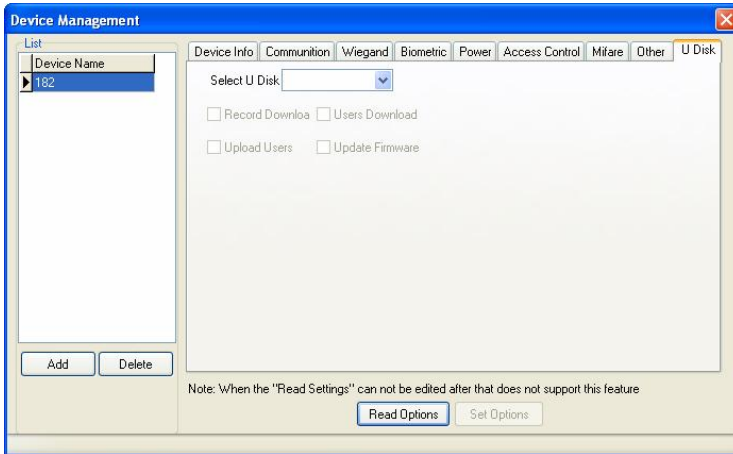


4.9 U disk Settings

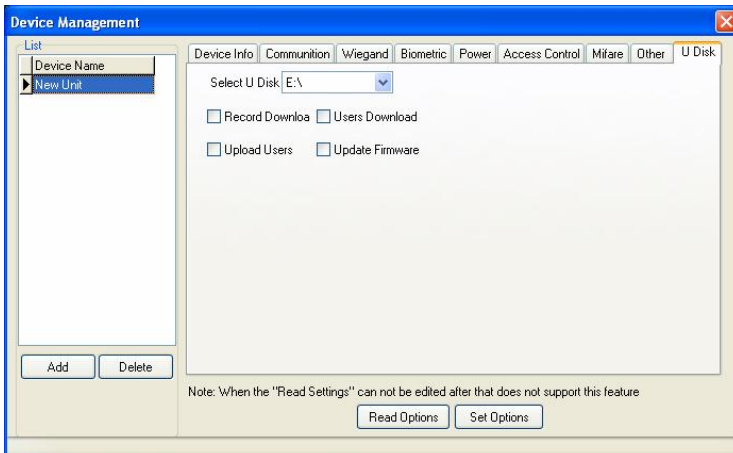
You can use the software to set the configuration file and store in a U disk. When the U disk is plug into a device, it can execute operations such as **Record download**, **User download**, **Upload users** and **Update firmware**.

Using PC software to create and modify the configuration files:

1. Click **[U disk]** in **[Device Management]** menu, enter the following interface.

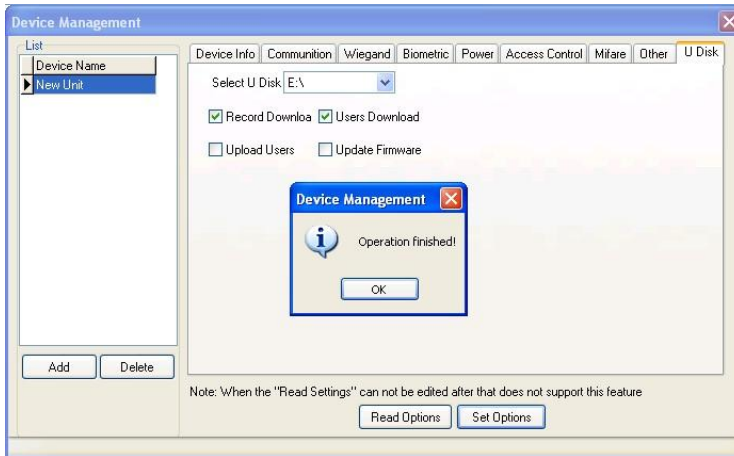


2. Select the U disk from the down drop menu, click **[Read Options]**, the interface display the following options, **Record download**, **User download**, **User upload**, and **Update firmware**.



3. Select the needed operation, click **[Set Options]**, the system will prompt **[Operation finished]**, as shown below.

4. Device Management



Open the U disk you can see the configuration file named **operatemode.cfg**. The operation of execute the U disk configuration file please refer to the related device user manual.

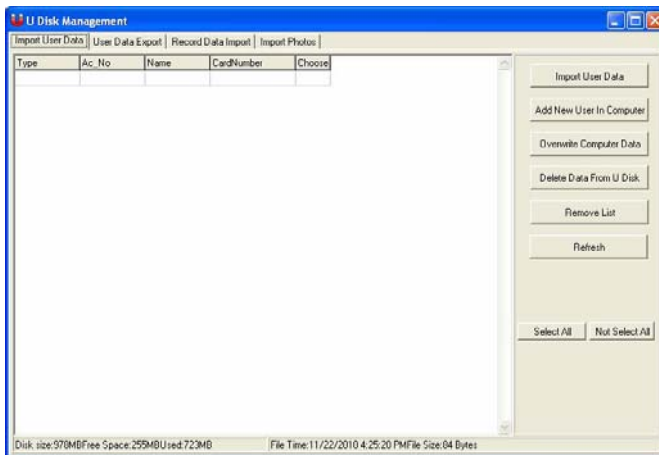
5. U Disk Management

In general, you can use RS232, RS485, TCP/IP, and USB to exchange the user data and attendance records with device.

If the communication method above is not available, you can use U disk to download or upload the user information and fingerprint, or download the attendance records.

5.1 Import User Data

1. Plug the U disk into the PC USB slot. Click [**U Disk Management**] in the [**Basic Options**], and enter the U disk management interface. Like as follow figure.

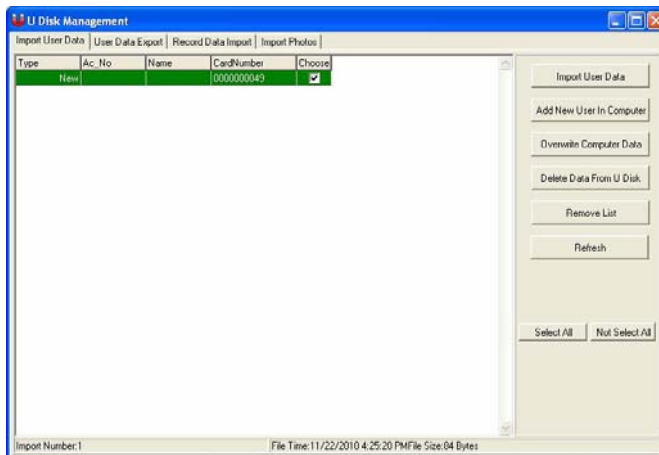


2. Click [**Import User Data**]. The system will prompt [**Select Device**] dialog. The imported user data format is different according to the device type, so you need select the type first.

5. U Disk Management



3. After that, click [OK] button, the system will automatically search the user data and load it into the system from the U disk. If there is a new use, the data will show in green color. In the list, the records with red color indicate that these records do not synchronization with the data in the software.

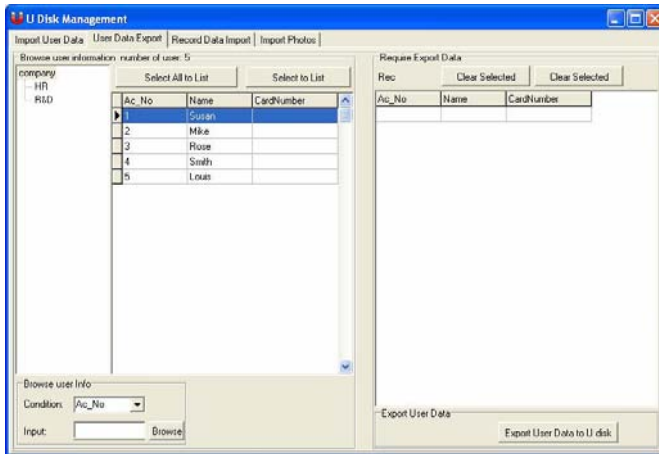


- **Add New User in Computer:** Import the new user in buffer area to the computer.
- **Overwrite Computer Data:** Import the selected user in buffer area to the computer.
- **Delete data from U disk:** Delete user data from U disk.
- **Remove List:** Clear the user list in buffer area.
- **Refresh:** Refresh the user data in buffer area.

5.2 User Data Export

Through interface of the U disk management, you can export the user data to U disk, and then upload the data to the device.

Plug the U disk into the PC USB slot. Click [**U Disk Management**] in the [**Basic Options**] menu, and enter the U disk management interface. Select [**User Data Export**] option, like as follow figure.



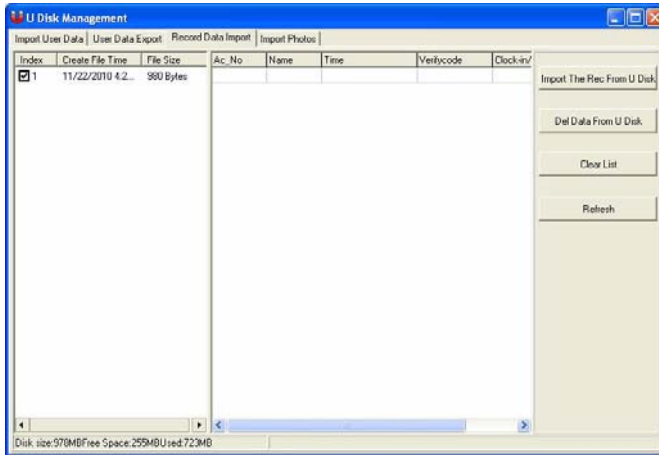
Double click user record or select user and click [**Select to list**], can add the user information to the right side. If there are many of user records, you can query the user information through the query function. The query condition such as Ac_No, Name, CardNumber is available.

Click [**Export User Data to U disk**]. Then export all records shown in the buffer area to the U disk.

5.3 Record Data Import

Through this interface, you can export the record data to U disk, and then import the data to the system.

Click [**U Disk Management**] in the [**Basic Options**], and enter the U disk management interface. Select [**Record data Import**] option, like as follow figure.

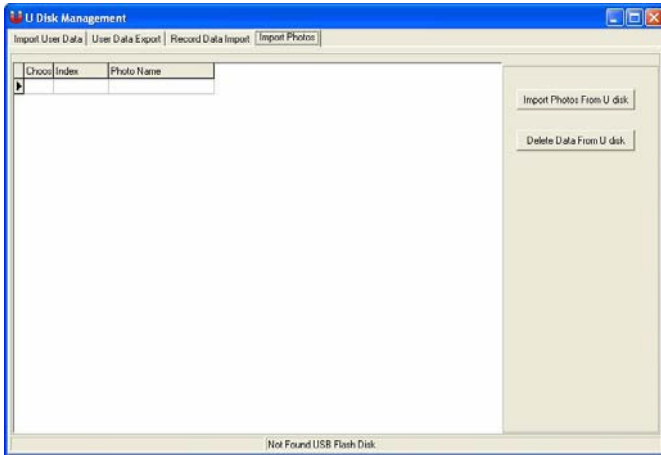


Click [**Import the record from U disk**], then the system import the data. When it has finished, all records will move to the buffer area.

- **Delete Data From U Disk:** Delete the record data from U disk.
- **Clear List:** Clear the record list in buffer area.
- **Refresh:** Refresh the record data in buffer area.


5.4 Import Photos

Plug the U disk into the PC USB slot. Click [**U Disk Management**] in the [**Basic Options**], and enter the U disk management interface. Select [**Import Photos**] option, like as follow figure.



Click [**Import Photos from U disk**], then the system import the user photos. After importing finished, all photos move to the buffer area.

- **Delete Data From U disk:** Delete the photo data from U disk.

 **Note:** U disk function requires the device support.

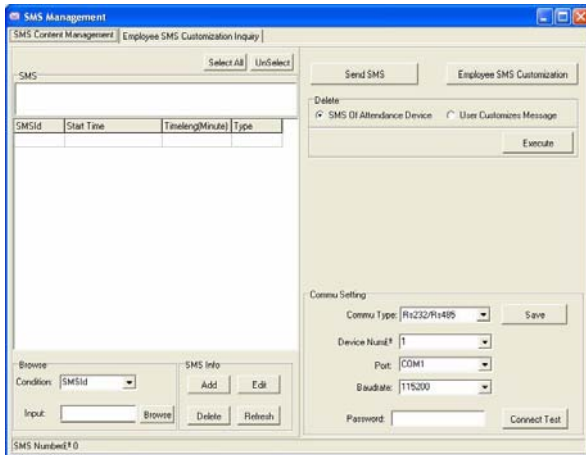
6. SMS Management

In some models of device, we offer the function to send scheduled SMS to the user or public. We just need to set the SMS in the software, and then upload to the device. The public SMS will appear at the device for all users to view, and will appear always. The user SMS will show after user verification, to reduce the user workload and improve the work efficiency.

6.1 SMS Content Management

Enter the SMS management interface:

Click [**SMS Management**] in the [**Basic Options**], like as follow figure.



1. Communication Setting

There are three ways for device communication. Similar to the device connection introduction in [4. Device Management](#). After complete setup, click [**Connect Test**] button to test, if it is succeed, the system popup [**Successfully Connect**] dialog, and the button turn to [**Disconnect**]. If it is fail, the system popup [**Fail Connect**] dialog.

2. SMS Query

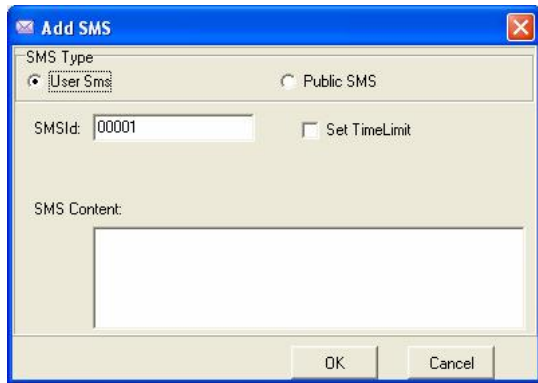
The system supports to query SMS by SMSId, SMS Content, Public SMS, User

SMS, etc. Click [**Condition**] down-drop menu, select the condition and input the information, then you can view the query result in the sms list table by click [**Browse**] button.

3. SMS Management

The system supports to manage the SMS information, such as **Add**, **Edit**, **Refresh**, **Delete** functions.

Add: Add a new SMS. Click [Add], the following interface appears:



Public SMS: Indicate the SMS for the public to view. The SMS will show after the device start, and appear always.

User SMS: Indicate the SMS for the user to view; it will appear after user verification.

Set Time Limit: Click this item, another line will show in the interface, as the following figure. You can define the start time and time length of the SMS valid time.

The screenshot shows a dialog box titled "Add SMS". It has a blue title bar with a close button. The main area is divided into sections. At the top, there are two radio buttons: "User Sms" (selected) and "Public SMS". Below this, there is a text input field for "SMSId" containing "00001". To its right is a checked checkbox labeled "Set TimeLimit". Underneath, the "Start" field is split into a date dropdown menu showing "11/27/2010" and a time dropdown menu showing "10:31:54". To the right of the time dropdown is a "Time Len" dropdown menu set to "60" and the word "Minute". Below these fields is a large, empty text area labeled "SMS Content:". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Delete: Select a SMS and click [**Delete**] button, the system will prompt [Are you sure to delete selected short message?] click [**OK**] and another prompt will show: [Whether delete all short messages in attendance device at the same time], click [**OK**] to confirm deletion.

Edit: Select a SMS, and click [**Edit**] button, to modify the SMS information, such as SMSId, valid time and SMS contents.

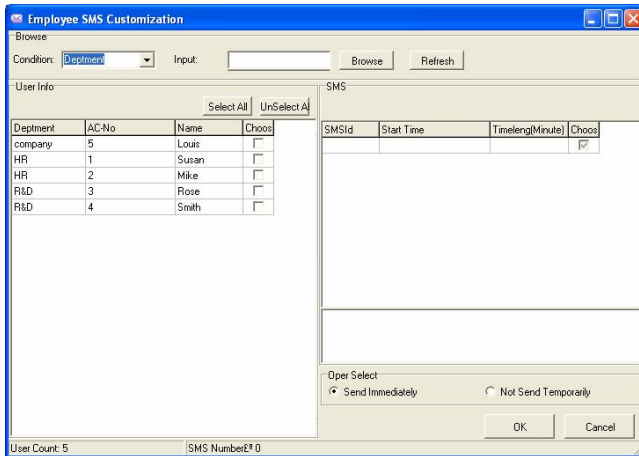
Refresh: After SMS querying, the SMS list will display all query results, click [**Refresh**] to return to the entirely SMS list.

4. Send SMS

Select the SMS in the left SMS list, and click [**Send SMS**] button to send the SMS.

6.2 Employee SMS customization

Click [**Employee SMS customization**], the following interface appears:

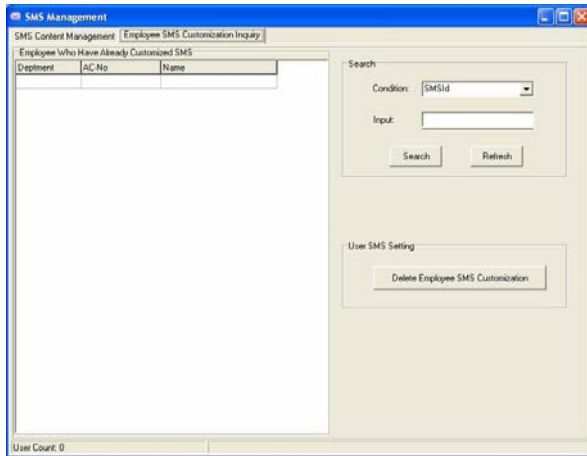


User Info: To list all users in the system, you can select multi user to send the customized SMS.

SMS: To list all the SMS added in the system.

Operation Select: If the software has connected with the device, you can select [**Send immediately**], otherwise, you can select [**Not sent temporarily**], and return to the SMS management interface. Select the SMS you want to send and click [**Send SMS**] to send the SMS. You can also send the SMS through U-disk. Click [**Employee SMS customization inquiry**] and enter the query interface.

6. SMS Management



You can select the query condition from the drop-down menu: query by SMS id, Department, Attendance ID and name.

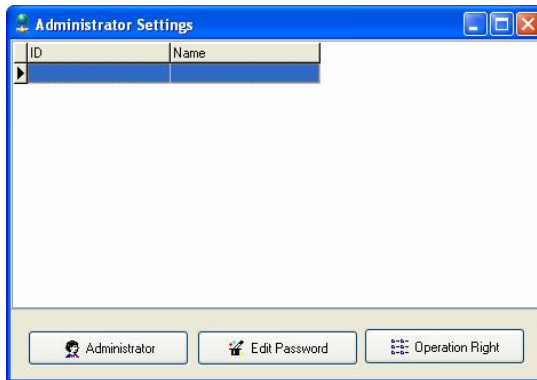
If you do not need the SMS, you can also delete the SMS by click [**Delete employee SMS customization**].

7. System Management

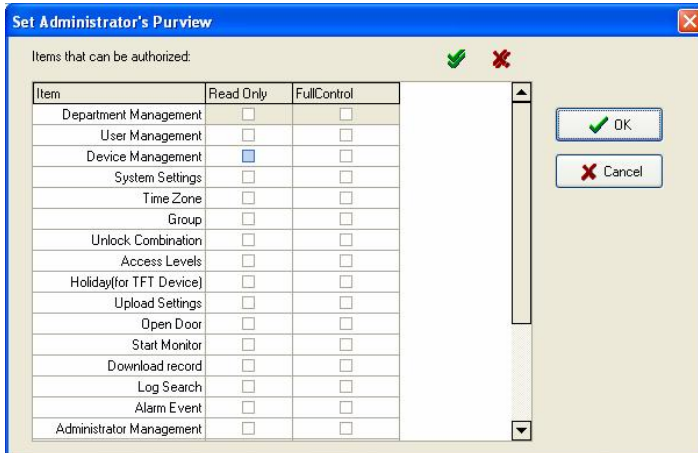
System management includes Administrator Management, System Operation Logs, Backup Database, Clear Obsolete Data, System Initialization, Database Connection, Set Password of Database, and System Settings.

7.1 Administrator Management

Click [**Administrator Management**] in the [**System Management**] menu, Popup the administrator Settings interface, like as following



Click [**Administrator**], popup the three item of [**Add department Administrator**], [**Add Administrator**] and [**Delete Administrator**]. Click [**Add Administrator**], and then popup a user list box, select a user and the click [**OK**] to popup a distributing privilege list, as following figure.



Put a remark in the administrator privilege, and then click **[OK]**.

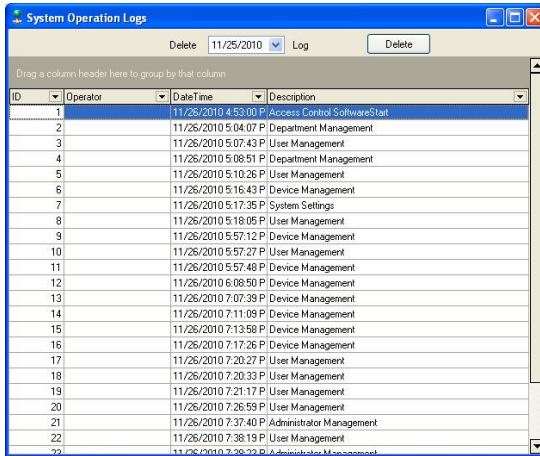
If you want to cancel an administrator, select the administrator firstly, and then click **[Delete Administrator]** to complete the operation process.

The operation of **[Add department Administrator]** is similar to **[Add Administrator]**.

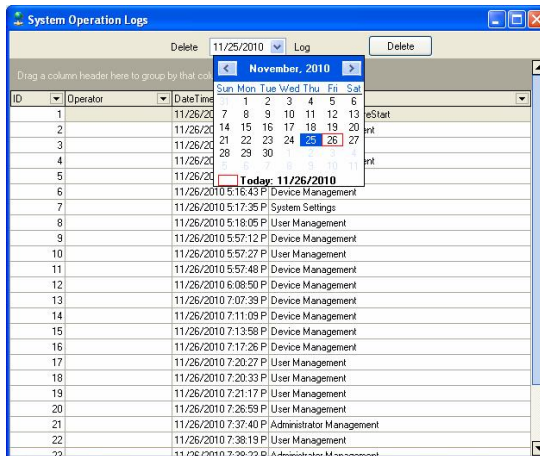
You can also modify the password and operation privilege of an existed administrator.

7.2 System Operation Log

The system operation logs was the records of this software operation history, and being list on the following interface.



Click the down-drop menu to select the end date, and click **[Delete]** button to delete the operation logs to the defined previous date (not include the selected date), as the following figure.



7.3 Data Maintenance

The Data maintenance includes Backup Database, Compact the Database, Clear Obsolete Data.

1. Backup Database

Click [**Backup Database**] in the [**Data Management**] menu, popup a dialog-box to backup database, you can name it as your favor, and save it in the defined location.

2. Compact the Database

Click [**Compact the Database**] in the [**Data Management**] menu, to compact the database, it is only capable for Access database.

3. Clear Obsolete Data

You can use this function to clear old data that are useless, click [**Clear Obsolete Data**] in the [**Data Management**].

Click the down drop menu to choose the date, and select the old record backup directory, then click [**OK**] button to clear the old data.



Note: The delete content does not include the ending date be selected.

7.4 System Initialization

Click [**System Initialization**] in the [**System Management**] menu, popup a warning dialog box, execute the command to initialize the system. This operation will clear all data of the system.

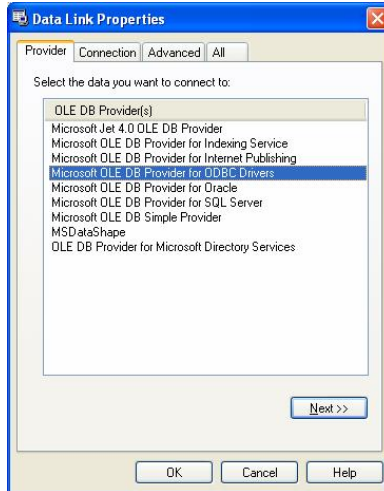


Note: Please use this operation with caution.

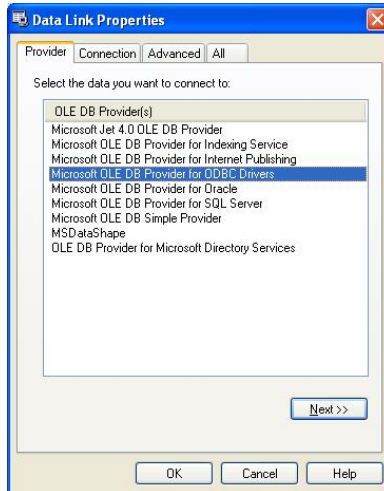
7.5 Set Database


1. Connecting Microsoft Access Database setup

(1) Provide program to select Microsoft Jet 4.0 OLE DB Provider;



(2) Click [Next] or [Connection] enter the following interface.

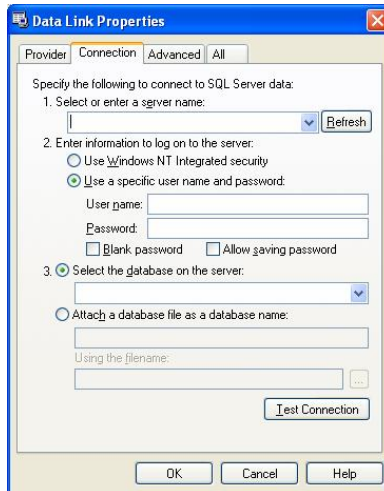


Click  button, can select the database file, the default name is **att200.mdb**, according to real condition to renew setup of the database connection.

2. SQL Server Database Connecting Setup

First, 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.

In the Provider Select Microsoft OLE DB Provider for SQL Server, click [**Next**] or [**Connection**] to enter this following.



Confirm the server name for storing this database, information for logging on this serve, and the database name. After run test connection successfully Click [**OK**] button to complete settings

7.6 Set Password of Database

We suggest user to set the password of database, in order to encrypt the database and ensure the system security. Anytime when you open the database, you should input the database password firstly, to avoid the intended destruction of the database.



Note: This function is only available for Access database.

Click [**Database password**] in the [**System Manage**] menu, input the new password in the popup dialogs box. Please distinctly keep in mind the password after set it.

7.7 System Options

Open [System Settings] in the [Basic Options], the following interface appears.

When program starts, activate automatic monitor

If you select this option, after the program start, it will enable automatic poll all the connected devices. Otherwise, program start will not enable poll.

Default device polling cycle (second)

During device continuing poll, some fingerprint devices may disconnect temporarily due to various reasons. Here, you can modify device-polling cycle in second (120 is recommended).

Keep the number of device

Device record number means user attendance records that downloaded to every device. You can enter a record number. If actual record number exceeds the pre-set value, the software will clear all fingerprint records stored in fingerprint

device. For example, record number to store is set to 30000, when record number downloaded is 30001, all fingerprint records in fingerprint device will be deleted, and record number downloaded resets to 0.

Times of reconnection due to failure:

Count for continuous failure retry (it is recommended to set to 3) that is convenience to reconnect automatically under the condition of fingerprint device recovers normal connection.。

Activate monitor in time zone:

Here, we can define one time zone to run monitoring. If run uninterrupted polling, it will bring huge burthen to whole monitoring network. You can define one time zone to run monitoring, in order to reduce burthen of monitoring network. Please pay attention to time format, such as 06:00-22:00.

Download log time:

Set the cycle to download operation log automatically.

Synchronic time:

You can define a time to synchronize the time of all fingerprint devices with the system. Please pay attention to time format, such as 10:00.

Set alarm sound:

Set all kinds of alarm sounds. Click [**Set**] button browse to select the desired audio file, and then click [**Open**] to complete setting.

The system will use default privilege while it do not assign privilege for user: Tick the box to confirm.

After assigning privilege for user, along with uploading user the system upload user privilege: Tick the box to confirm.

In downloading attendance records process, whether to add the user when there is no local user: Tick the box to confirm.

Company Name: Input the unit name using in the software.

Set Database connection:

Click [**Set Database Connection**], will popup the window of the defined path

database, please refer to [7.5 Set Database](#).

When start-up Windows, start-up this Program:

After select this item, when the PC start, the program will run automatically, otherwise, when the PC start, the program will not run automatically.

8. Access Settings

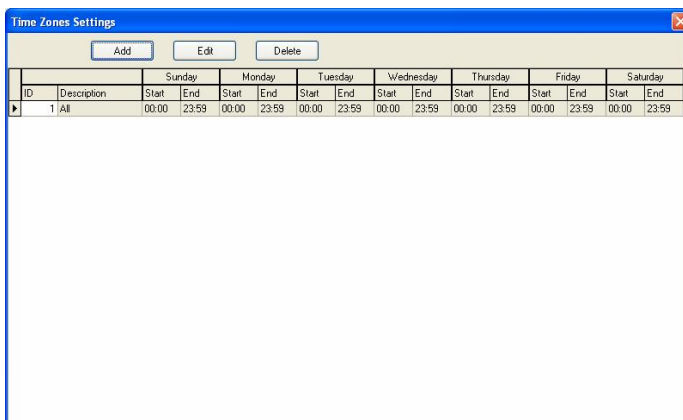
Access setting is to set unlock time and assign privilege for registered users. Settings of each user consist of three time zone settings and one group setting. Relationship between time zones is **OR**. Group also consists of three time zone settings, and the relationship between these three time zones is **OR**.

Simply put, if you want to keep a registered user in unlock status. Firstly the group that this user is in should be defined in unlock combination (one group can be defined in one combination together with other group, but these groups are required to unlock door together). Second, current unlock time is in any availability range of user time zone and time zone of its group.

Under system default, a new registered user is in Group 1 and group combination is Group 1. So new registered user is in unlock status by default. If a group that user is in is not defined in the group unlock combination setting, then the user have no right to unlock the door.

8.1 Time Zone

1. Click [**Time Zone**] from Drag-down menu of [**Access Settings**], or click the [**Time zone**] shortcut in the main interface, adding time zone interface will popup.



| | | Sunday | | Monday | | Tuesday | | Wednesday | | Thursday | | Friday | | Saturday | |
|----|-------------|--------|-------|--------|-------|---------|-------|-----------|-------|----------|-------|--------|-------|----------|-------|
| ID | Description | Start | End | Start | End | Start | End | Start | End | Start | End | Start | End | Start | End |
| 1 | All | 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 |

8. Access Settings

2. Click **[Add]** button and system will pop up a timetable from Sunday to Saturday. Here, you can define any time zone you may use.

Time Zone settings

Select Time Zone ID: 2 Description: test

Sunday: 00:00 - 23:59
Monday: 00:00 - 23:59
Tuesday: 00:00 - 23:59
Wednesday: 00:00 - 23:59
Thursday: 00:00 - 23:59
Friday: 00:00 - 23:59
Saturday: 00:00 - 23:59

Buttons: OK, Cancel

3. Then click **[OK]** to save the time zone.

Time Zones Settings

Buttons: Add, Edit, Delete

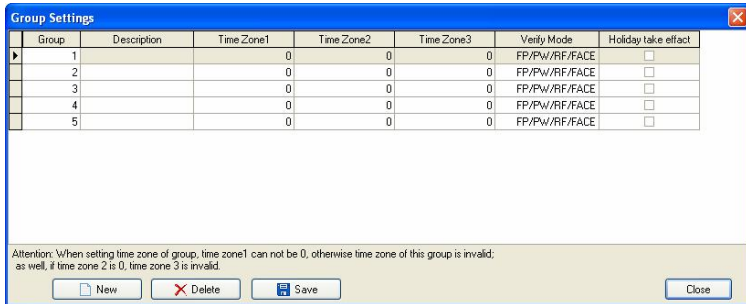
| ID | Description | Sunday | | Monday | | Tuesday | | Wednesday | | Thursday | | Friday | | Saturday | |
|----|-------------|--------|-------|--------|-------|---------|-------|-----------|-------|----------|-------|--------|-------|----------|-------|
| | | Start | End | Start | End | Start | End | Start | End | Start | End | Start | End | Start | End |
| 1 | All | 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 | test | 12:00 | 23:59 | 12:00 | 23:59 | 12:00 | 23:59 | 12:00 | 23:59 | 12:00 | 23:59 | 12:00 | 23:59 | 12:00 | 23:59 |

4. If you want to use several time zones, continue to click **[Add]**. The system supports up to 50 time zones.

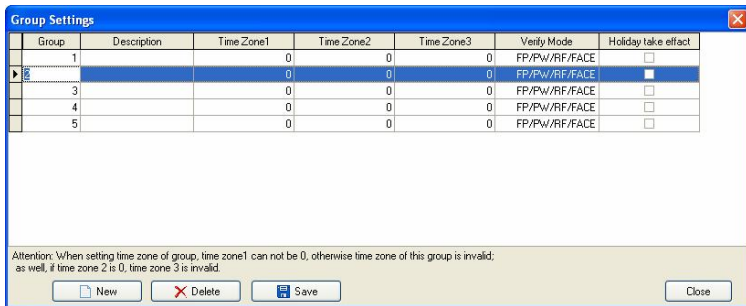
In addition, you can edit or delete the time zone.

8.2 Group

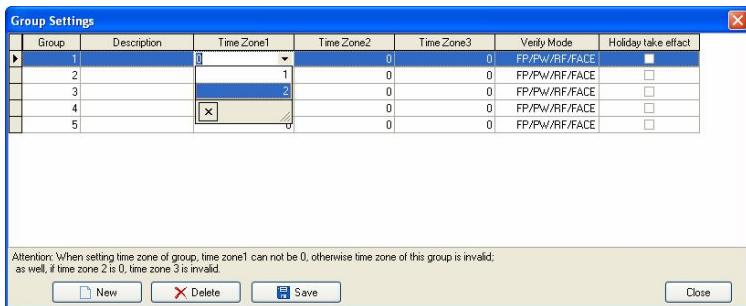
1. Enter the interface: Through the system menu: **[Access Settings]** -> **[Group]**, or through shortcuts button options of the system: **[Group]**, enter the group settings interface.



2. Left click item that need to edit with cursor to enter the editing state.



3. Choose the time zone through the drop-down box.



4. Choose the verification mode through the drop-down box.

8. Access Settings

| Group | Description | Time Zone1 | Time Zone2 | Time Zone3 | Verify Mode | Holiday take effect |
|-------|-------------|------------|------------|------------|---------------|--------------------------|
| 1 | | 0 | 0 | 0 | FP/PW/RF/FACE | <input type="checkbox"/> |
| 2 | | 0 | 0 | 0 | FP/PW/RF/FACE | <input type="checkbox"/> |
| 3 | | 0 | 0 | 0 | 1 FP | <input type="checkbox"/> |
| 4 | | 0 | 0 | 0 | 2 PIN | <input type="checkbox"/> |
| 5 | | 0 | 0 | 0 | 3 PW | <input type="checkbox"/> |

Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

New Delete Save Close

5. If you want the time zone in the group take effective on holiday, select it by cursor clicks.

| Group | Description | Time Zone1 | Time Zone2 | Time Zone3 | Verify Mode | Holiday take effect |
|-------|-------------|------------|------------|------------|---------------|-------------------------------------|
| 1 | | 0 | 0 | 0 | FP/PW/RF/FACE | <input checked="" type="checkbox"/> |
| 2 | | 0 | 0 | 0 | FP/PW/RF/FACE | <input type="checkbox"/> |
| 3 | | 0 | 0 | 0 | FP/PW/RF/FACE | <input type="checkbox"/> |
| 4 | | 0 | 0 | 0 | FP/PW/RF/FACE | <input type="checkbox"/> |
| 5 | | 0 | 0 | 0 | FP/PW/RF/FACE | <input type="checkbox"/> |

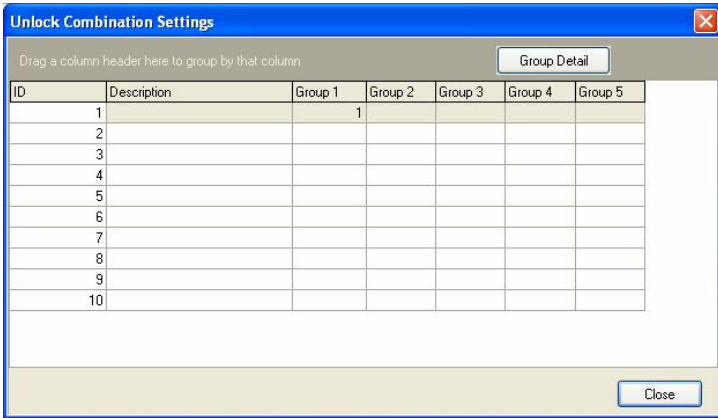
Attention: When setting time zone of group, time zone1 can not be 0, otherwise time zone of this group is invalid; as well, if time zone 2 is 0, time zone 3 is invalid.

New Delete Save Close

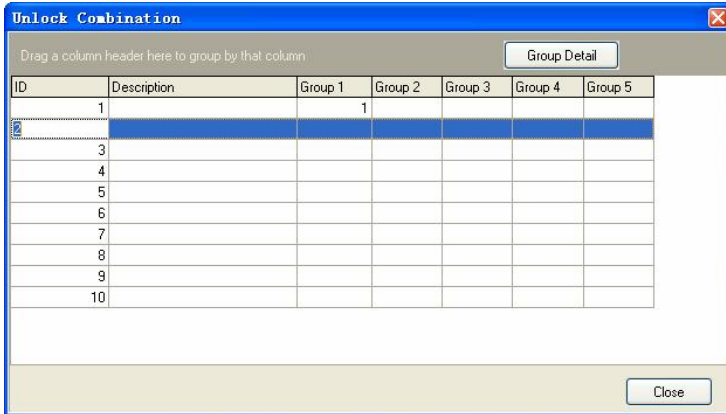
6. Set up is completed. Click [**Save**] to save.

8.3 Unlock Combination

1. Enter the interface: Through the system menu: [**Access Settings**] -> [**Unlock Combination**], or through shortcuts button options of the system: [**Unlock Comb**], enter the unlock combination settings interface.

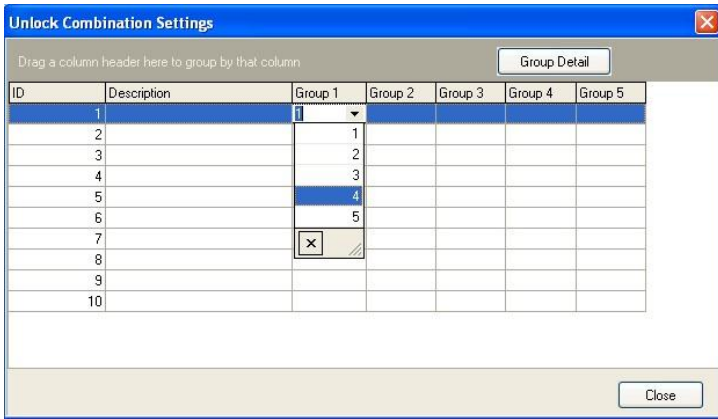


2. Left click item that need to edit with cursor to enter the editing state.

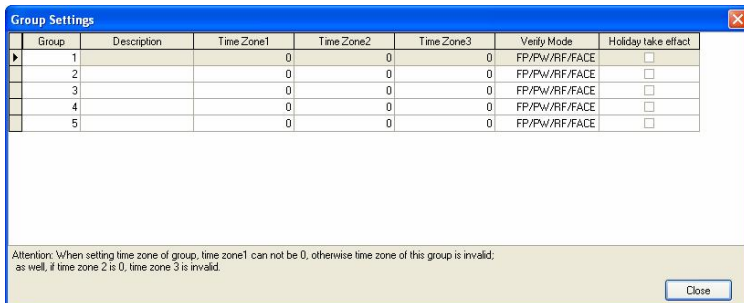


3. Choose the group number through drop-down box.

8. Access Settings



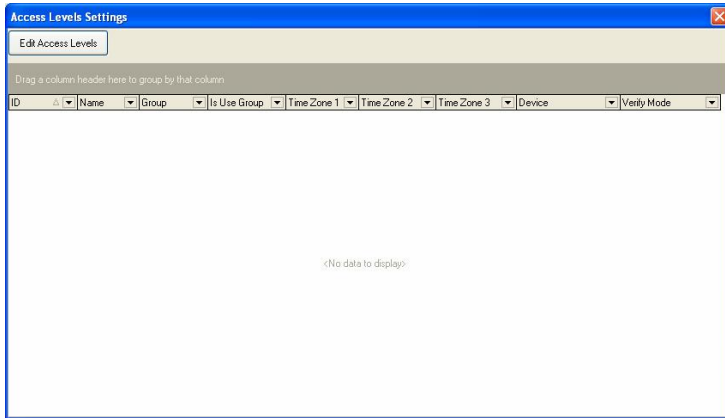
4. If you forgot the group definition, click [**Group Detail**] to see the exist group, and return to step 3 to select group.



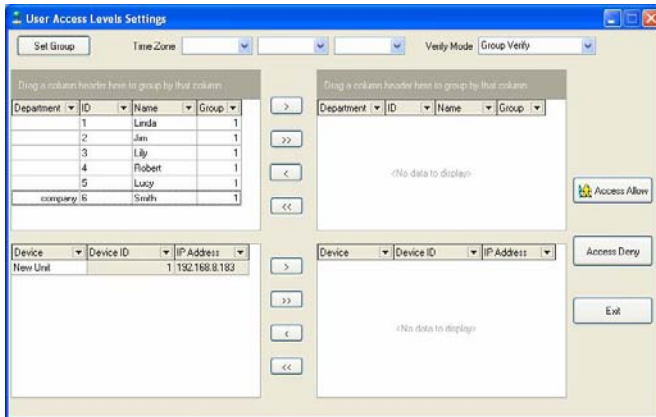
5. You can set others unlock combination as step 3-4. After setting up, click [**Close**] to save and quit.

8.4 Access Levels

1. Enter the Access Levels setting: Through the system menu: [**Access Settings**] -> [**Access Levels**], or through directly shortcuts button of the system: [**Access Levels**], enter the Access Levels setting interface.

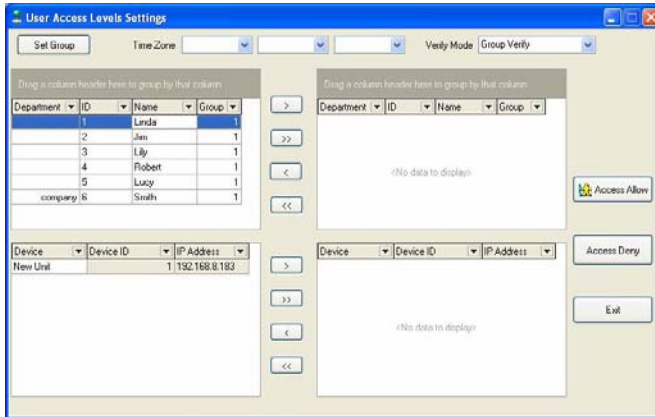


2. Click **[Edit Access Levels]** and enter the Access Levels interface to edit, shown as following.

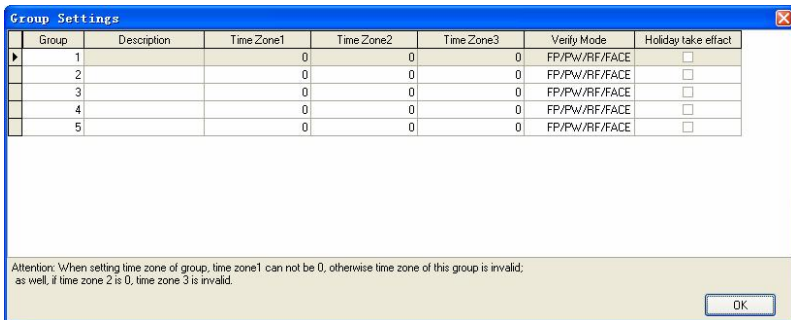


3. Users belong to Group 1 by default. If you need to assign the user to other group, re-allocate the user as the following operation. No. 1 user is belonging to Group 1 by default. First selected No. 1 user, shown as following.

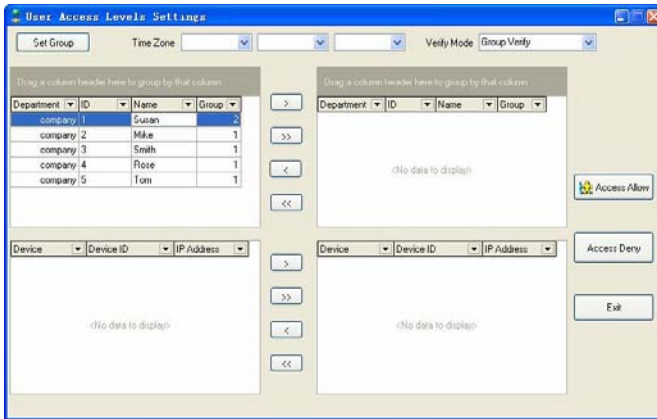
8. Access Settings



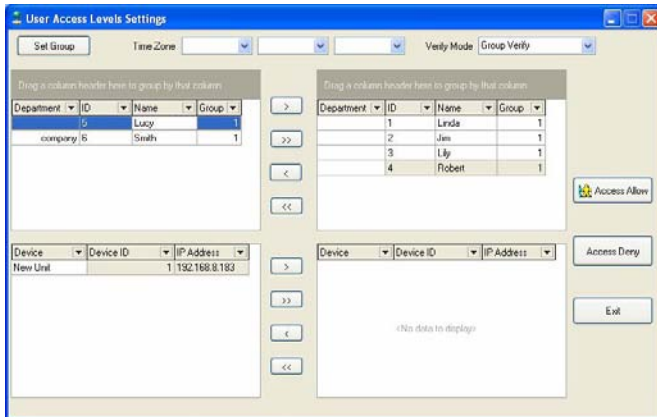
4. Click on the [Set Group] button and enter the [Group Settings] interface, select group 2.



5. Through the above steps, the user move to the group 2, shown as following.

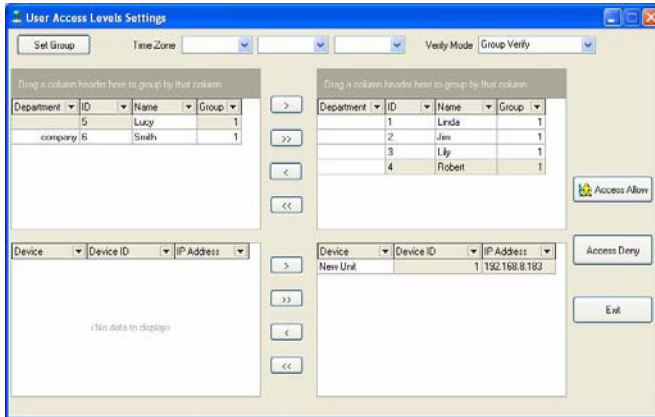


6. Follow the 3-5 steps, set up the group those users respective. After the setting completed, through ">/>>" button, a single or all of users will be moved to the right critical areas, waiting for the Levels setting, shown as following.

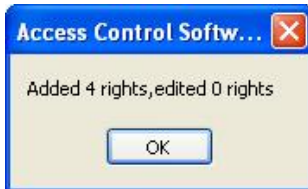


7. Choose the device that need to upload Privilege from the device list. Through ">/>>" button, single or all devices will be moved to the right the critical region, waiting for Levels setting, like as the following interface.

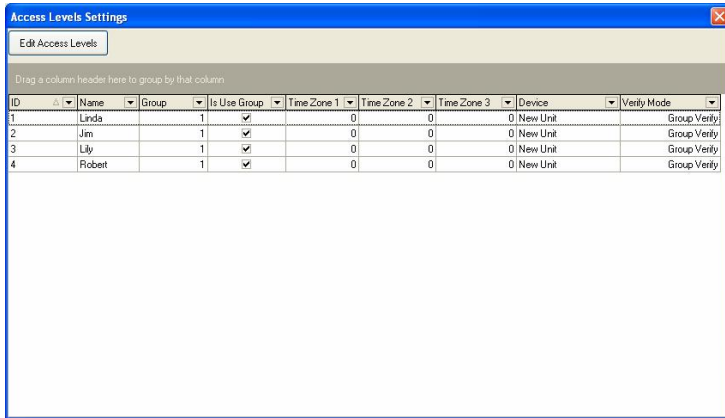
8. Access Settings



8. After users and device selecting, click on **[Access Allows]** button, the group time zone that using by user in the critical periods will be assign to the selected devices. After distribution is successful, prompt will appear shown as following

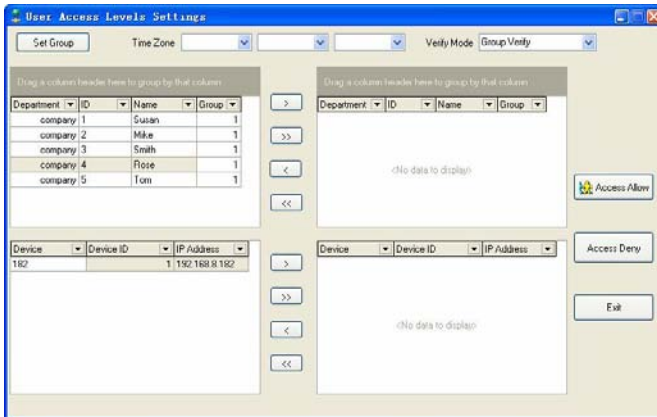


9. Click **[Exit]** button, you will enter the **[Access Levels]** interface, synchronizes set up information of user groups will display in the list, shown as following.



Set up the user does not use the Access Levels of group time zone:

1. If a user do not use group time zone when she/he belong to a group, please enter the [User Access Levels Settings] interface.

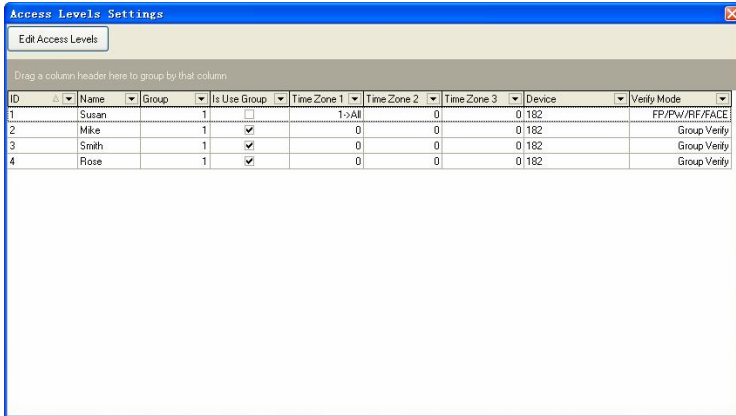


2. Select a user and the applied device, the using time zone and the verification style, and click [Access Allow] button.

8. Access Settings



5. After modification, a new record list in the following interface.

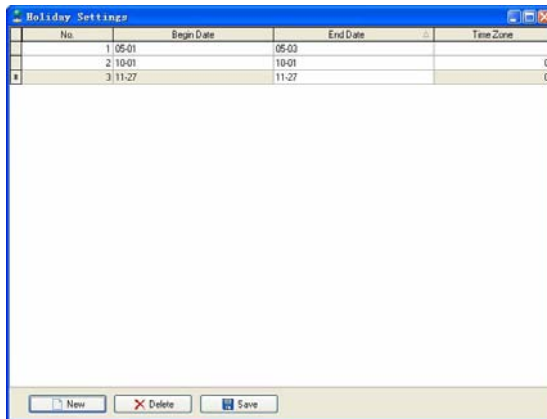


8.5 Holidays setting

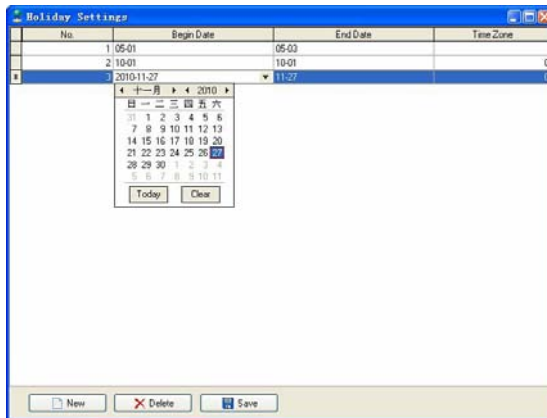
1. Entered the holidays set. Choose [Access Settings] -> [Holiday], shown as following.



2. Click [**New**] button to add a new one, the default date is the current day.



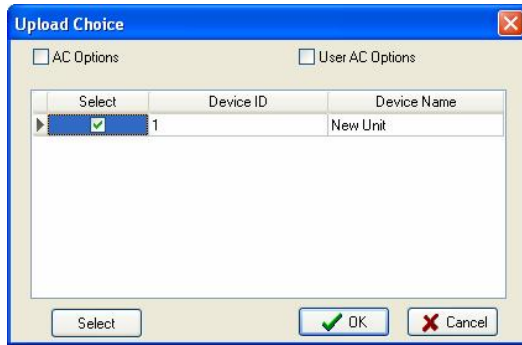
3. Move cursor to the [**Begin date**] and [**End date**] to modify the date.



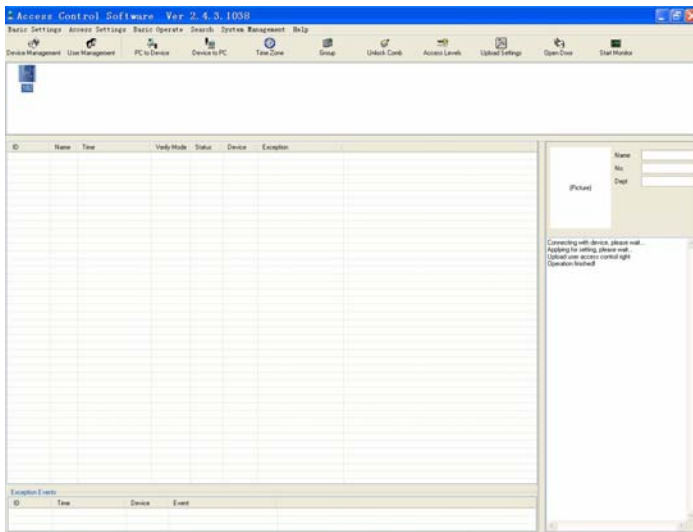
4. Moved the cursor to the Time zone to be set, choose the valid Access Time zone.

Operation] -> [**Upload Settings**], or through the system shortcuts button: [**Upload Settings**], enter the upload interface.

3. There are two choices to upload interface elements, the [**AC options**] and [**User AC options**], and it is better the two selected together at the same time to upload. This can choose to upload multiple devices.



4. Upload success, the successful operation prompt display on the lower right corner, shown as below.



9. Other Function

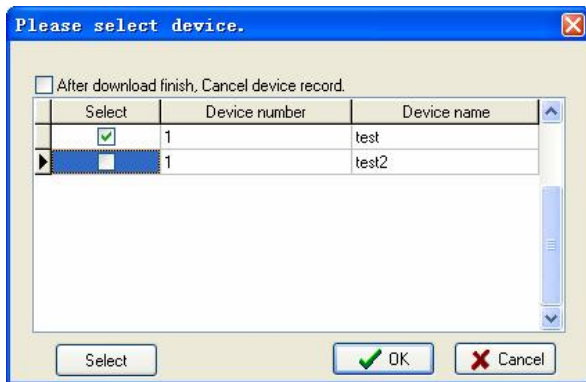
9.1 Start Monitor

You can click the **[Start Monitor]** shortcut on the main interface to start system polling and monitoring, and the button changes to **[Stop]**.

When system is in the monitor status, the information about opening door and fingerprint verification will show on the list field.

9.2 Download Log

In the absence of monitor situation, in order to download the system records, you can right click the device, and then the operation menu appears. Click **[Download Log]**, the dialog popup as below.



Select the device and click **[OK]** to finish the download process. If you select **[After download Finish, Cancel device record]**, the system will delete the device record when downloading complete.

In monitoring state, if you want to download the device record, click **[Download Record]** in **[Basic operation]** menu, the system will download all connected devices' record to system.

9.3 Clear Log

If you want to clear the device record, please right click the device icon, and select **[Clear Log]**, the system will prompt the confirm dialog.

Click **[Yes (Y)]** to clear the device records.


9.4 Sync Time

If the device time is not synchronizing with the system, please right click the device icon, and select **[Sync Time]** button.

9.5 Update Firmware

If the device has the older firmware, you can update the firmware by right click the device, and click the **[Update Firmware]** button. After updating, you need to restart the device. The prompt shown as follows.



 **Note:** Please do not upgrade the firmware at your discretion because it may bring problems and affect the normal use of the device. Contact our distributors for technical support or upgrade notification.

9.6 Restart Device

If you want to restart the device using the software, please right click the device icon, and click **[Restart Device]** button to restart it.

9.7 Property

Please right click the device, and click **[Property]** button in the prompt dialog.

Enter the [**Device Management**] interface, the specific operation please refer to [4. Device Management.](#)

9.8 Stop Sound

After the system alarm has been triggered, right click the device, appears the operation menu, click the [**Stop Sound**] to stop the system sound and light alarm.

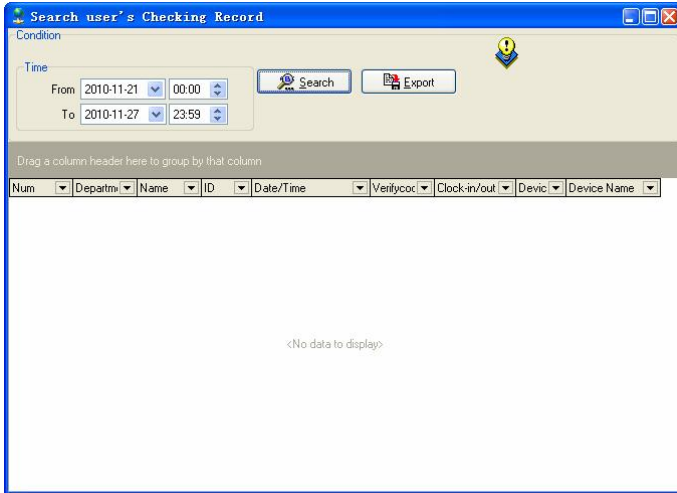
9.9 Open Door

If you want to open the door using the software, please click the device icon, and click [**Open Door**] shortcut on the main interface.

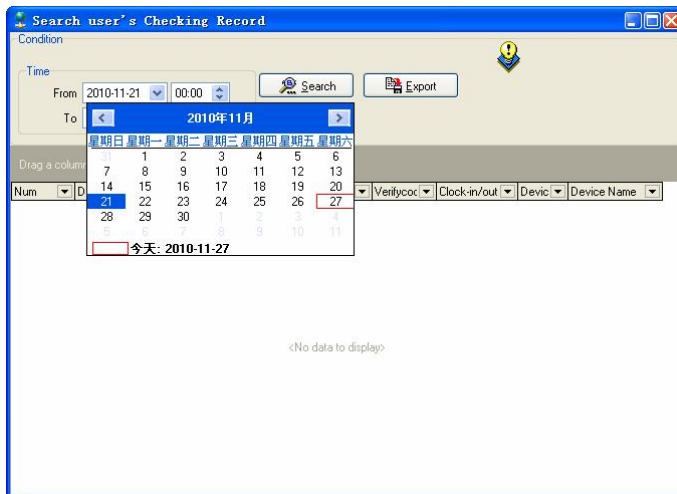
10. Record Management

10.1 Record Query

1. In [Query] down drop menu, you can select [Log Search], show as following.

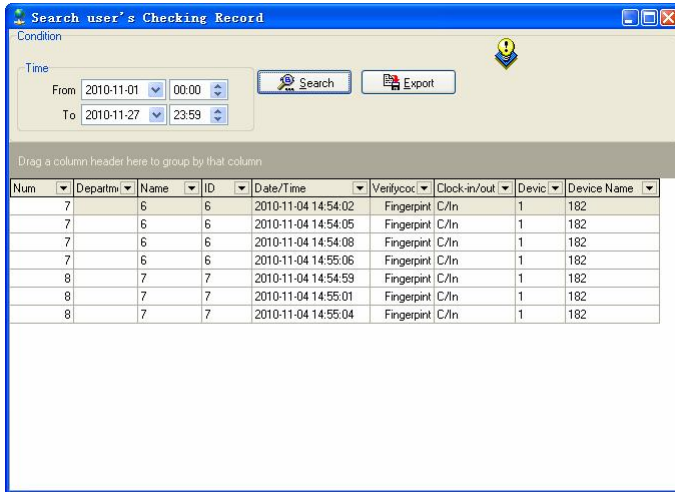


2. Select the start and end date to search the records.

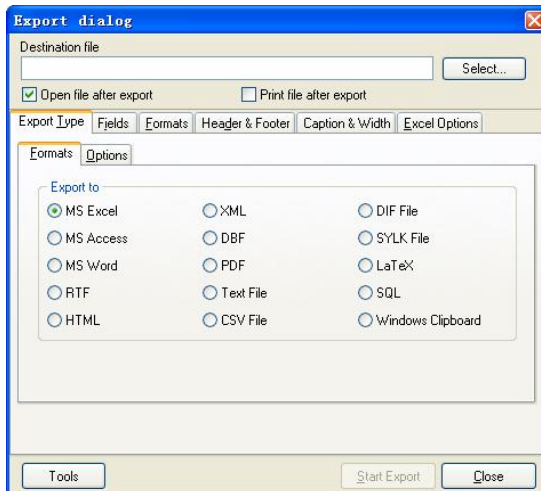


10. Record Management

3. Click [**Query**], the in/out access log within these date will show in the list.



4. Click [**Export**] to output fingerprint records in various formats, such as Excel format, etc. this operation is similar to user management exporting.



10.2 Alarm Report

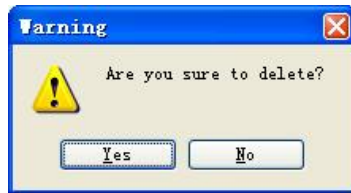
Detect fingerprint that does not pass verification, duress fingerprint that will trigger the alarm. Click **[Alarm Event]** in the **[Search]** drop-down menu, and **[Alarm Event Search]** window will pop up, as shown in the following picture:

| Operator | DateTime | Device | Alarm Type | EnrollNumber |
|----------|--------------------|----------|------------|--------------|
| | 2010-5-14 16:06:57 | New Unit | | -1 |
| | 2010-5-14 16:06:57 | New Unit | | -1 |
| | 2010-5-14 16:06:57 | New Unit | | -1 |
| | 2010-5-14 16:06:57 | New Unit | | -1 |
| | 2010-6-4 22:05:25 | Test | | -1 |
| | 2010-6-5 9:18:51 | Test | | -1 |
| | 2010-6-7 10:01:50 | Test | | -1 |
| | 2010-6-8 14:24:41 | Test | | -1 |
| | 2010-6-8 14:24:41 | Test | | -1 |
| | 2010-6-8 14:24:45 | Test | | -1 |
| | 2010-6-8 14:24:46 | Test | | -1 |
| | 2010-6-8 14:24:53 | Test | | -1 |
| | 2010-6-8 14:24:54 | Test | | -1 |
| | 2010-6-8 14:24:56 | Test | | -1 |
| | 2010-6-8 14:24:58 | Test | | -1 |
| | 2010-6-8 14:25:00 | Test | | -1 |
| | 2010-6-8 14:25:01 | Test | | -1 |
| | 2010-6-8 19:06:32 | Test | | -1 |
| | 2010-6-10 11:54:19 | Test | | -1 |
| | 2010-6-10 11:54:22 | Test | | -1 |
| | 2010-6-10 11:54:25 | Test | | 7 1 |
| | 2010-6-12 16:45:15 | New Unit | | -1 |
| | 2010-6-12 16:45:18 | New Unit | | -1 |

Delete alarm event: Select the end date, as following interface.

| Operator | DateTime | Device | Alarm Type | EnrollNumber |
|----------|--------------------|----------|------------|--------------|
| | 2010-5-14 16:06:57 | | | |
| | 2010-5-14 16:06:57 | | | |
| | 2010-5-14 16:06:57 | | | |
| | 2010-5-14 16:06:57 | | | |
| | 2010-6-4 22:05:25 | | | |
| | 2010-6-5 9:18:51 | Test | | -1 |
| | 2010-6-7 10:01:50 | Test | | -1 |
| | 2010-6-8 14:24:41 | Test | | -1 |
| | 2010-6-8 14:24:41 | Test | | -1 |
| | 2010-6-8 14:24:45 | Test | | -1 |
| | 2010-6-8 14:24:46 | Test | | -1 |
| | 2010-6-8 14:24:53 | Test | | -1 |
| | 2010-6-8 14:24:54 | Test | | -1 |
| | 2010-6-8 14:24:56 | Test | | -1 |
| | 2010-6-8 14:24:58 | Test | | -1 |
| | 2010-6-8 14:25:00 | Test | | -1 |
| | 2010-6-8 14:25:01 | Test | | -1 |
| | 2010-6-8 19:06:32 | Test | | -1 |
| | 2010-6-10 11:54:19 | Test | | -1 |
| | 2010-6-10 11:54:22 | Test | | -1 |
| | 2010-6-10 11:54:25 | Test | | 7 1 |
| | 2010-6-12 16:45:15 | New Unit | | -1 |
| | 2010-6-12 16:45:18 | New Unit | | -1 |

2. Click [**Delete**] and the following prompt will show:



3. Click [**Yes**] to delete the events before this date. After that, these events will not show in the list.

11. Appendix

11.1 Common Operation

1. The toolbar for datasheet operation:



The line where the blue bar is located is the current line. All operation for datasheet is performing on the current line. Only black button is operational, it cannot operate when it is gray.

Click button, put it to corresponded operate.



: First, move from the current line to the first line.



: Previous, move from the current line to the previous line.



: Next, move from the current line to the next line.



: Last, move from the current line to the end line.



: Insert, add new record.



: Delete, cancel current record.



: Edit, enter edit status to modify record.



: Save, save the record to be edited.

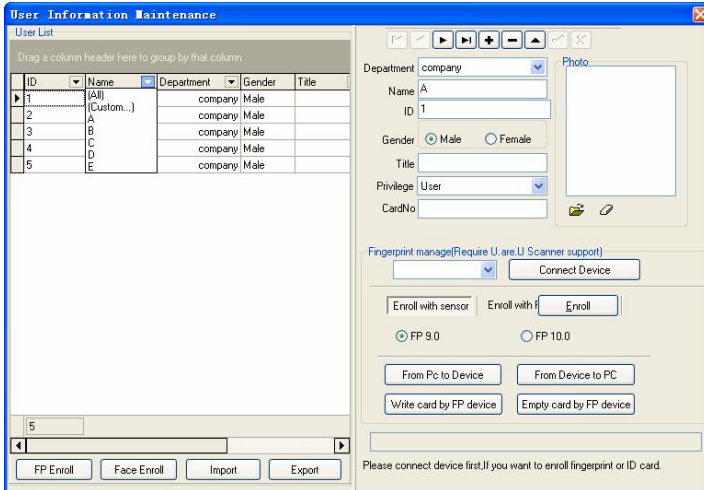


: Cancel Edition, cancel modification for the record.

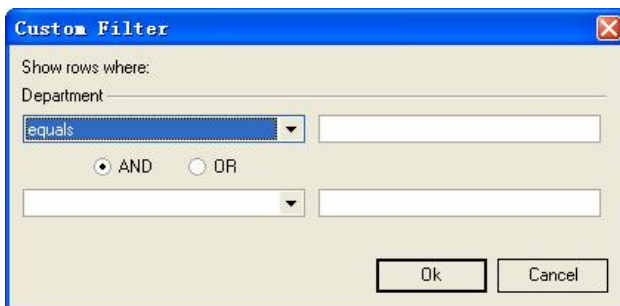
2. Filtrate Data

Filtrate data is that select the record that meets defined condition from the original table sheet, the current display window is following, the operation flow of the filtration data's command.

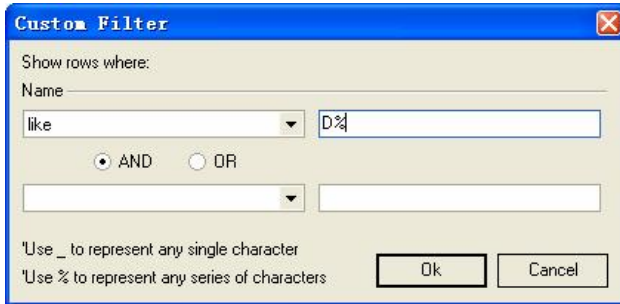
(1) Click down drop menu of the data rank, appear the following figure.




(2) Click [Custom Filter], appear the following figure.

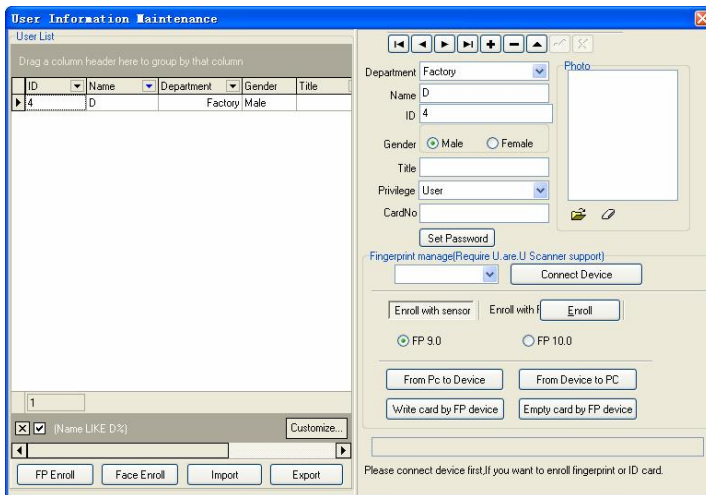


(3) Input condition, such as show all user whose name contain character D, appear following figure.



 **Note:** “%” must be English symbol. Chinese symbol is rejecting to know.

(4) Click [OK], to show the result of filtration.



: Whether do use the filtrate condition.

: Cancel filtrate operation.

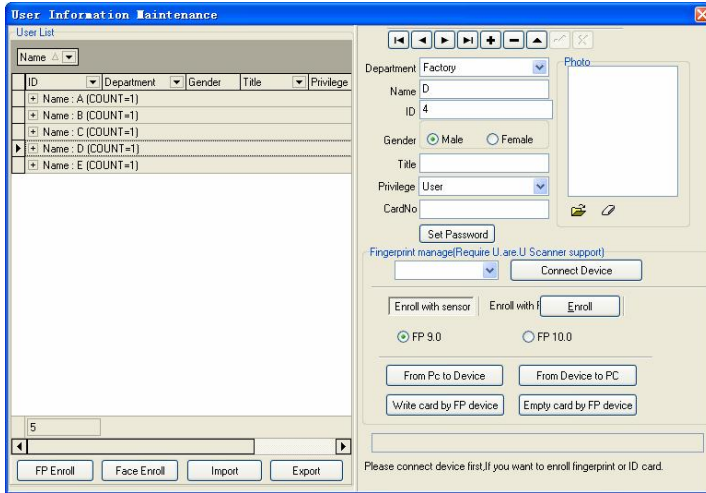
If you want to cancel the current filtration result, and display all records, click or .

3. Record Group

According to a field or multi-field, you can group the record. If you want to realize

11. Appendix

group that can draw the rank head to upper side empty part, as the following figure.



User Information Maintenance

User List

| ID | Department | Gender | Title | Privilege |
|------------------------|------------|--------|-------|-----------|
| [-] Name : A (COUNT=1) | | | | |
| [-] Name : B (COUNT=1) | | | | |
| [-] Name : C (COUNT=1) | | | | |
| [+] Name : D (COUNT=1) | | | | |
| [-] Name : E (COUNT=1) | | | | |

5

Department: Factory
Name: D
ID: 4
Gender: Male Female
Title:
Privilege: User
CardNo:
Set Password
Fingerprint manage(Require U.are.U Scanner support)
Connect Device
Enroll with sensor | Enroll with
 FP 9.0 FP 10.0
From Pc to Device | From Device to PC
Write card by FP device | Empty card by FP device
Please connect device first, If you want to enroll fingerprint or ID card.

FP Enroll | Face Enroll | Import | Export

11.2 FP, FP Device and Card User Guide

The system offers Fingerprint user, Card user, Card, and fingerprint multi-user verification.

1. ID Card User

(1) Enroll ID card

There are two statuses to enroll ID card.

A. Only Own ID card User

It is suit the user who own the higher privilege or the too poor fingerprint to verify, refer to the **[User Management]** part of FP device user guide to enroll, the enroll process is that: Add User → Input User Basic Information → Connect to the FP device with ID card Reader → Wave Card → Save ID Number → Upload User Information.

B. User Verified by FP and Card

It is optimized for the general user, user must enroll the card and fingerprint, there are two ways to verify for user, one is to present the card to verify, the other way is verify the fingerprint after waving card near the properly place of the device. The enroll process is that: Add User → Input User Basic Information → Connect to the FP device with ID Card Reader → Enroll Fingerprint → Wave Card → Save ID Number → Upload User fingerprint and Information.


(2) ID Card User Verification

There are two following verification models for ID card user.

A. Only verification ID card

User can verify the identity by waving the registered ID card near to the front of the device, or place the finger on the sensor. This verification way applies to the low security requirement area, but it is easy to use. That is optimizing for officer site that owns the high public security. Please refer to the **[Verification]** part of FP device of enroll user, the set process is that: Open **[Device Management]** → **[Biometric]** → **[Verification]** → **[Read Options]** → Remark on **[Verification ID**

Card] item to **[Yes]** → **[Apply Options]**.

 **Note:** There are only **[Only verify ID card]** and **[Only 1:1 verify]** to suit ID card setup in the verification option, the **[Register Mifare card only]** is just used for Mifare user. When you set to verify ID card, the **[Only 1:1 verify]** must be remarked as **[NO]**, the **[Register Mifare card only]** is set to read the default.

B. Only 1:1 verify

User must to wave the card near the front of the device before placing the finger on the sensor to verify until it is positive answer. This verification way applies to the higher security requirement area. It is optimized for a lot of user site, the set process is that: Open **[Device Management]** → **[Biometric]** → **[Read Options]** → Remark on **[Only verify ID card]** item and **[Only 1:1 verify]** item to **[Yes]** → **[Apply Options]**.

We suggest adopt this verification method when the device store fingerprints up to 500, because the more fingerprints there are, the more slowly is the device matching speed, the FAR (False Acceptance Rate) will be much more, the Only verify ID card can speed up to identify and keep away fingerprint false acceptance.

2. Mifare Card User

(1) Enroll Mifare Card

Please refer to the **[User Management]** part of FP device user guide to enroll user, the enroll process is that: Add User → Input User Basic Information → Connect to the FP device with Mifare Card Reader → Use UareU Sensor or FP device to enroll fingerprint → Write Card via FP device → Wave Card → Write Card Successfully,

The fingerprint can store in the Mifare card, they have the same result and efficacy of wave a card and place finger to verify. Select device with Mifare is optimal option for user.

(2) Mifare Card Verification Model

There are following verification modals for Mifare card user.

A. Only verify Mifare Card

The same as ID card, it only need to present the card for passing verification, in order to strengthen security of the application in the normal condition, the item is set as **[NO]**, so and must place the finger to verify after presenting a card to verify .

B. Only Verify 1:1

The same as ID card, first must present card and then place the finger on the sensor, if do not present the card, the finger will be reject to accept.

Register Mifare card only:

This item set as **[Yes]**, the User ID of Mifare must be store in the device, otherwise it is fail to pass, if this item set as **[NO]**, it is no need to store user ID in the device to perform the verification.

Fingerprint Card user Table:

| Only verify ID Card | Only verify 1:1 | User type | Note |
|---------------------|-----------------|-------------------------------------|--|
| Y | Y | Only Card | Only support Card |
| Y | NO | Card or Fingerprint | Support Card or Fingerprint |
| NO | Y | Card+Fingerprint | Only support to fingerprint match after to present card |
| NO | N | Car+Fingerprint or Fingerprint Only | After to present the card to press finger or only to match fingerprint |

Suggest Select Setup Type:

| Version | Name | Only verify ID Card | Only verify 1:1 | Note |
|----------|----------|---------------------|-----------------|---------------------|
| Standard | Standard | NO | NO | Card+fingerprint or |

11. Appendix

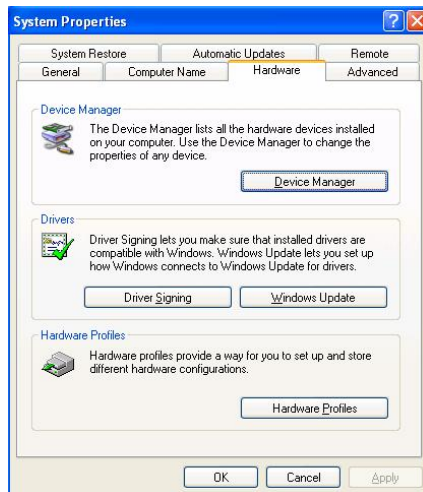
| | | | | |
|-----------------|--------------------------------|----|---|--------------------|
| | Fingerprint Device | | | Fingerprint Only |
| Build In ID | Build in ID Fingerprint Device | NO | Y | Card + Fingerprint |
| | Build in ID Fingerprint Device | NO | Y | Card + Fingerprint |
| Build in Mifare | Build in IC Fingerprint Device | NO | Y | Card + Fingerprint |

11.3 Fingerprint Algorithm License

1. Right click **[My Computer]** by the mouse, and select **[Properties]**, as shown below:

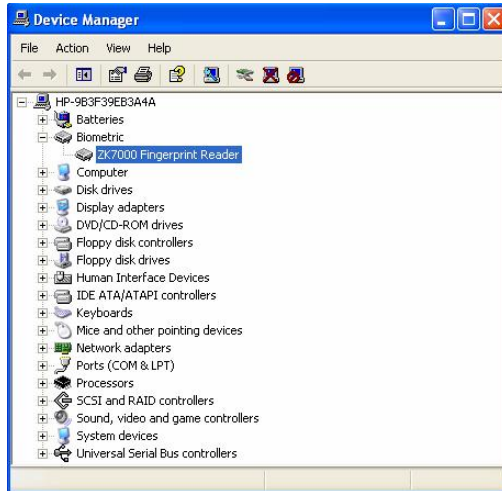


2. Enter the dialogue box of system properties, select **[Hardware]**, and click **[Device Manager]**, as shown below:

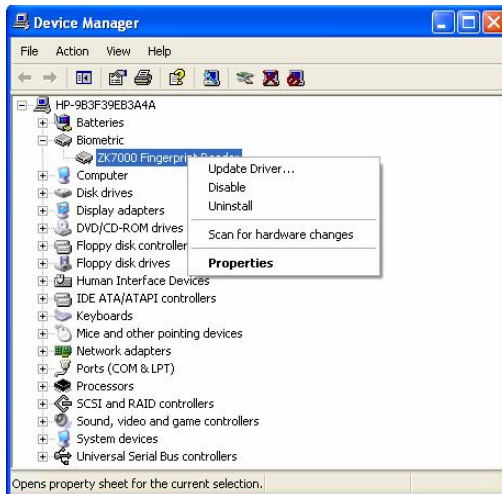


3. Device named **[Biometric]** will display in **[Device Manager]**, as shown below:

11. Appendix



4. Right click the device, and select **[Properties]** in the menu, as shown below:



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



11.4 SOFTWARE USE LICENSE AGREEMENT

《End User Software License Agreement》

LICENSE:

Our company will grant you the use right of this software program, but you must ensure: do not 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 use 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 that 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, 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.

Copyright laws and international treaty provisions protect the software and its documents.

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:

Our company 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, our responsibility is to change good software for you as the only compensation.

If the defects 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, our company and our 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 our company is informed in advance that such things can happen.

TERMINATION

Without prejudice to any other rights, our company 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 our company.

GOVERNING LAWS:

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