

Contents

1. Software Installation and Uninstall.....	1
1.1 Before Installation.....	1
1.2 Software installation.....	2
1.3 Uninstallation Software.....	7
2. Quick Start.....	9
2.1 hardware networks set up.....	9
2.2 Fingerprints Verification Server Setting.....	11
2.3 Fingerprints Enrollment.....	13
2.3.1 enroll finger with fingerprints sensor.....	13
2.3.2 Remote enroll fingerprint on the fingerprint machine.....	18
2.4 Grouping Personnel.....	20
3. System Setting.....	26
3.1 Database.....	26
3.2 Network.....	27
3.3 Validate.....	28
3.4 Recording display.....	29
4. Verification server personnel configuration.....	31
4.1 Domain management.....	31
4.1.1 Add region.....	32
4.1.2 Modification region information.....	33
4.1.3 Cancel domain.....	35
4.2 Remote Verification Server Management.....	36
4.2.1 Add remote Verification Server.....	37
4.2.2 Modify remote verification sever.....	38

4.2.3 Delete remote verification sever.....	39
4.3 Staff Group Management.....	40
4.4 Region Configuration Management.....	41
4.4.1 Configure Verification Server.....	41
4.4.2 Configure corresponding personnel group.....	42
4.5 Operation User Management.....	43
5. User Management.....	44
5.1 User management.....	45
5.1.1 Datasheet Process Tool Bar.....	46
5.1.2 Department management.....	47
5.1.3 Fingerprint enrollment situation.....	48
5.1.4 Import.....	49
5.1.5 Export.....	52
5.2 Equipment Management.....	54
5.2.1 Fingerprint machine Information.....	54
5.2.2 Communication setting.....	55
5.2.3 Validate.....	57
5.2.4 Power management.....	57
5.2.5 Other Setup.....	58
5.3 Databases Setup.....	60
6. Appendices.....	64
6.1 Datasheets processing tool bar operation.....	64
6.2 Arrangement.....	65
6.3 Filter data.....	66
6.4 Record Grouping.....	68
6.5 Count.....	69
7. Trouble shooting.....	70

Summary

the method, traditional Time and Attendance apply to the major industry, is far to satisfy the demand of the business management, main cause rising out of following factor: The an enterprise scope is widespread, and it is distributed into N region; The personnel is multitudinous, total personnel of a medium enterprise is above thousand ; The personnel fluidity is strong, the identical enterprise's staffs allow to flow in the different region, if a personnel who belong to A region works in the B region or after working period of time, who may be directly assigned to the B region. For the traditional Time and Attendance, have to spend the massive manpower to count and process this Time and Attendance result. Facing such as complex work, we conceive build a set of complete Time and Attendance networks to the enterprise through one way , which saves the enterprise all staffs' Time and Attendance data in a large-scale database, enables the staff is allowed to check attendance in enterprise's any terminal, namely front end matching, backstage verification, but all staffs' original Time and Attendance record can be stored up in the database, this is design idea the remote verification server ,the main function of the remote verification server may summarize as following several aspects:

1st, enrollment fingerprint

Enroll fingerprint with the fingerprint sensor, or select the remote verification sever to enroll fingerprint, which take as auxiliary enrollment method, namely remote user registration. After building the remote verification network successfully, the manager may input this enterprise staff's fingerprint on any terminal, and input the user information in the verification server.

2nd, region management

The factory area of an enterprise is possibly to distribute in the quite several regions, therefore the enterprise is divisible into N domain, may build the verification server under the domain. the relations between domain and personnel are such as, the personnel is mobile, but the domain cannot flow, therefore we set a cycle of the personnel mobile in the domain setting, a default cycle is 28 days, namely when the attendance record of personnel in flowing group of an domain exceeds 28 days, the personal will be added into the fixed group in this domain automatically.

3rd, management verification server

A domain is allowed to have many verification server, therefore may carry on the management verification server , like revise the name of the verification server, the IP address; create the verification server; Delete the verification server.

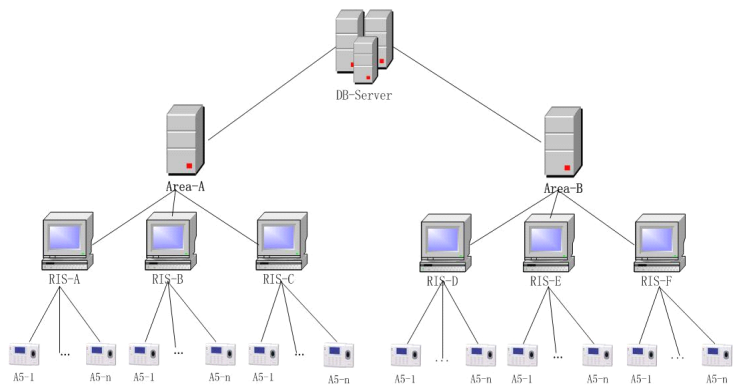
4th, the personnel groups' management

All newly enrolled users in the verification server are regard as users of mobile group in a domain; the manager can group the users in the domain and furthermore add users of flowing group into fixed group. In addition, the administrator can also add or change the grouping depending on the enterprise requirement

5th, the domain configuration management

May configure the domain which is relative the verification server, the domain correspondence personnel group also is able to be configured.

Following is the figure of network structure of remote verification server.



1. Software Installation and Uninstall

1.1 Before Installation

If the computer have been installed 4000 or before the version fingerprint sensor driver, first uninstall it (the Biokey200/URU4000 driver) its steps as follows.

1.Backup the registry:Open 'Run' item in the starts menu to run the 'Regedit', open the registry, then selects the [HKEY_LOCAL_MACHINE\SOFTWARE\DigitalPersona] item in the registry, single-clicks the registry in the menu to export the registry file , export this item in the file.

2. Uninstall 4,000 drivers (the Biokey200/URU4000 drivers)

Uninstall steps as follows:

1) To run "the Add/Remove the program" in the Control Panel, uninstall the fingerprint sensor driver.

2) Open 'Run...' item in the starts menu to run the 'Regedit, examines the HKEY_LOCAL_MACHINE\Software\DigitalPersona key value, if there exist, and the deletes it.

3)Examined the DP* dll which in the Sub- directory system32 under the system installation directory (win98 is windows\system), if it exists, then completely deletes it;

4) Look over the directory of Program files\zksoftware\biokey200, if there exist, then completely deletes it.

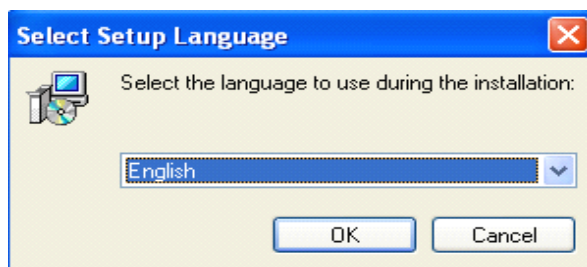
3. The computer has not installed with any fingerprint sensor driver, then directly installs the fingerprint verification server procedure.
4. If the computer has installed with the 4000B fingerprint sensor driver, when is installing the fingerprint verification server, does not need to install the fingerprint sensor driver again

1.2 Software installation

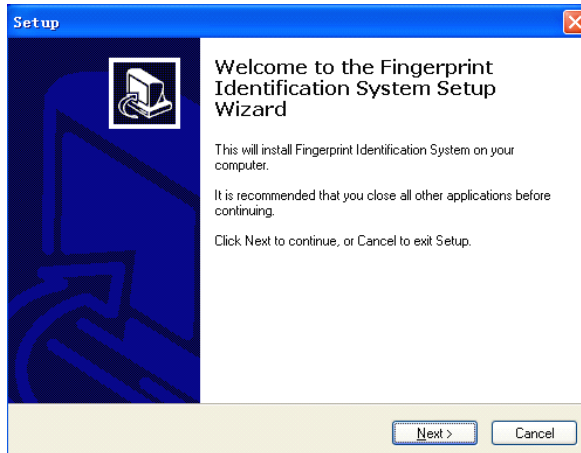
It better to quit other application procedure you are running before installation, like this is helpful installation process to avoid conflict.

Note: The demonstration picture possibly does not tally with the real content of CD; please take the CD as the installation procedure

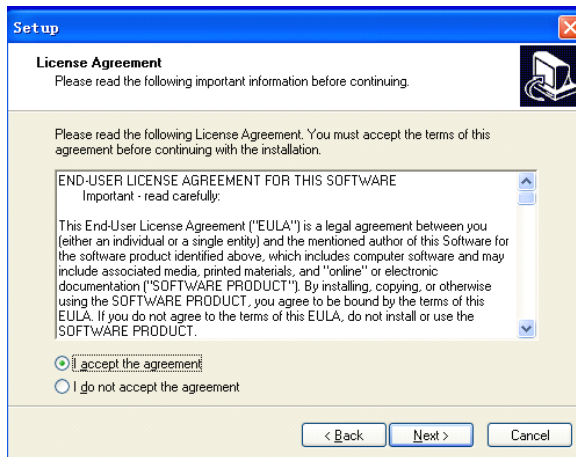
Inset the fingerprint verification Server CD into your CD-ROM, following interface will pop-up



Please select desired language and click OK as following:

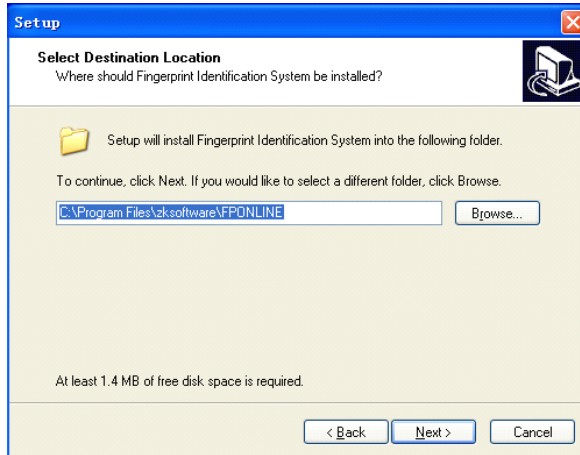


Click "next", enter following interface

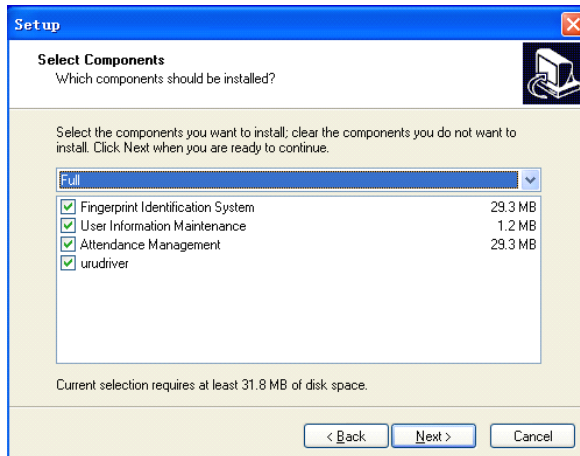


In this interface, this is a legal End-User License Agreement between you, the user, and the mentioned author of this Software, please read carefully. If you accept this content, please choose "I agree", and click "next step", enter the next installation; If you do not agree this agreement, please choose "I don't agree", and exit the installation

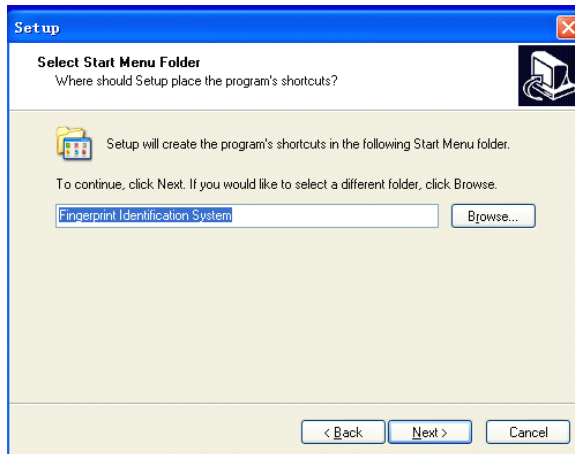
procedure; If needs to return previous operation, please click "Back".
Next installation interface as follows:



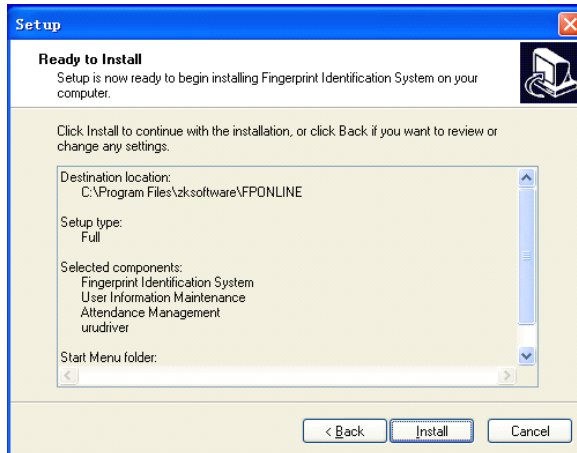
This interface is used to assign the fingerprint verification software installing path, you may choose the default path, also may own or create another path. After determination clicks "next step", demonstration interface as follows:



Choose a module that want to be installed, after the choice, clicks "next step", enter the next interface as follow:



This page is used to create user name in "start/ program". Click "next step", display following interface:



this interface, indicate you have already completed all configuration of installing procedure, if you want to revise configuration, click “Back” to return; Otherwise, click the button “installing” button, the installation procedure will copy file to the hard disk and read in the correlation information, after the installment complete click” Finish” to complete the entire installment flow of the fingerprint verification server. If choose U.r.U driver in the installment module, after completing installment the fingerprint verification server, the interface to install driver will appear, follow installation instruction operation closely. After the installing driver, the system will prompt whether will restart computer. Be sure to restart your computer .so the configuration change take effect.t

1.3 Uninstallation Software

If you do not want to retain this software in Windows, you may follow the below step to operate:

- 1) Close all procedures.
- 2) Enter [my computer], double-click [control panel] to enter.
- 3) Enter [Add/delete program] the window, selects [fingerprint verification server], as following figure shows, single-clicks [delete], follow the prompt to uninstall fingerprint verification server

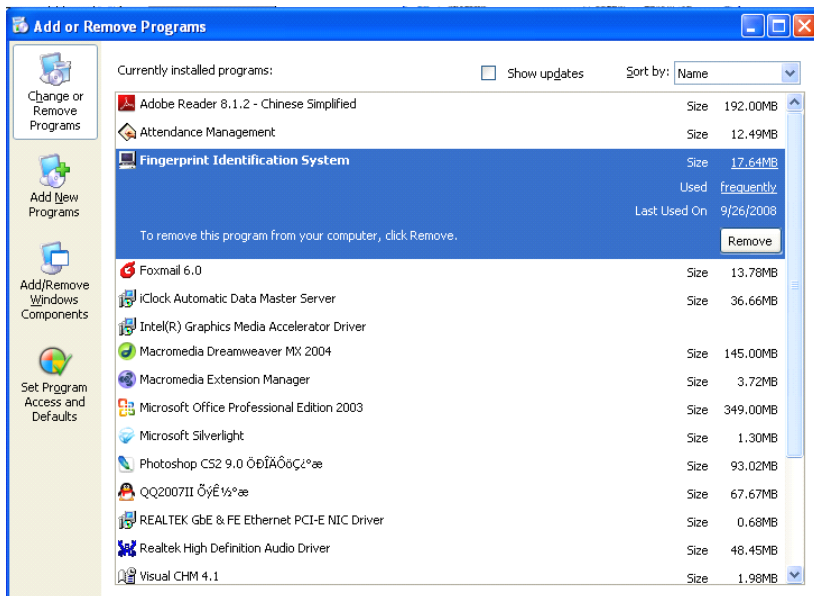


Figure uninstall fingerprint verification server

If this software failed to delete all correlation file through above process, you should enter installing directory of software to delete FPONLINE folder.

2. Quick Start

Remote verification server is very simply and provide user with convenient, moreover to build the entire network environment also is very simply, main step may be divided into following several step.

2.1 hardware networks set up

the remote verification , regard as the name , matching in front end, remote verification in backstage, and all terminals connect with the identical database of the remote verification server , the remote verification server make it possible for the front-end to interact well with the backstage through the TCP/IP way , therefore the effective IP address are assigned to all terminal(fingerprint machine) of remote verification server in this domain, the system has made it possible for the remote verification terminal and network in this domain to build in the same place, guarantee network normal operation. Detail steps as follow:

1st, configure and install all terminal

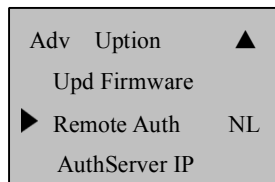
Depending on own actual situation, user is able to reasonably arrange and install all terminals, it is important to take the synthesize wiring, make sure that each the network terminal out of breakdown. For detail operation, please refer to "Installation guide" 3.2.1 introductions.

2nd, configure the remote verification parameter in each terminals

1) Enter machine menu -> option -> communication option, in "communication option" set a effective IP address of local area network

which is in this domain, you must pay attention that this IP address does not conflict with any IP address of terminal, and serial number of each terminals does not overlap. For more detail operation, please refer to "User Handbook" 5.3 introductions.

2) Enters machine menu -> Option -> system Option -> advance option, select "remote verification", and set "verification server address", Exit and save this setting, open the terminal again. The operation interface show as follow:



The remote verification server provide fours way to verify: LO, LN, NO, NL.

LO: Only local verification. User don't pass authentication in this terminal unless there is a fingerprint in the local fingerprint terminal only.

LN: first this locality, then remote, first seeks and match the fingerprint in the local fingerprint terminal, when the fingerprint had not been found or failed to verify in the fingerprint terminal ,then system will look for the fingerprint in the remote database to match.

NO: Only Remote verification, User don't pass authentication in this terminal unless there is the fingerprint in the remote database only

NL: first remote, than this locality, first seek and match the fingerprint in the remote database, if the fingerprint has not been found in the remote database or failed to pass authentication, then system will look for the

fingerprint in the fingerprint terminal to match.

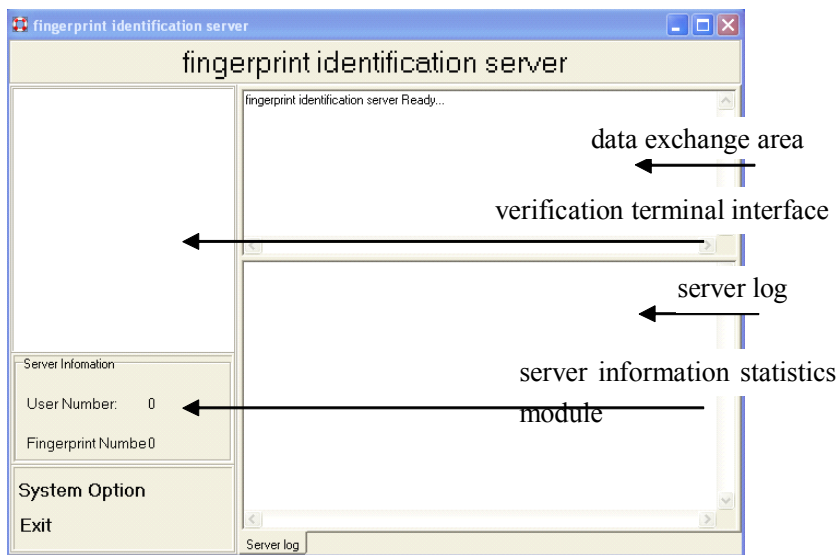
Verification server address: set as the computer IP address which has installed the fingerprint verification software.

2.2 Fingerprints Verification Server Setting

1. there are two ways to open the fingerprint verification server:

- 1) double-click the short-cut icon " fingerprint verification server";
- 2) through [start] - > [program] - > [fingerprint verification server]
single-click [fingerprint verification server];

2. enter the fingerprint verification server interface, this interface include the verification terminal interface, and the server information statistics module (show user number, fingerprint data), the data exchange area and the server log etc、



3.if the fingerprint machine connects with the fingerprint verification server successfully, when open the procedure of fingerprint verification server, the data exchange area will automatically appears, there is packet information as shown in figure 2-2 , If there is not prompt to the data packet information, means that connection between the fingerprint machine and the verification server network or setting existence question, please inspect the fingerprint Time and Attendance machine setting.

Note: After the fingerprint machine connect the fingerprint verification server successfully, the system ability to carry on the remote registration or the verification operation. While the remote enrollment or the verification process, the fingerprint verification server cannot shut down.

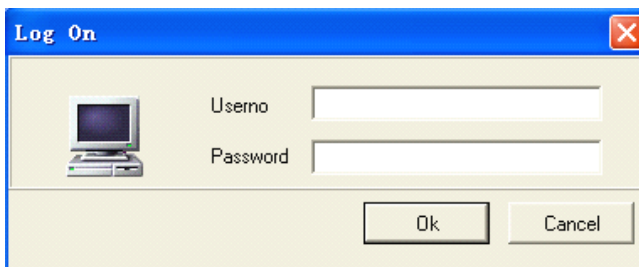
2.3 Fingerprints Enrollment

It is better to use the fingerprint sensor to enroll fingerprint, so that guarantee the fingerprint template precision in the database, after correctly installs the fingerprint sensor, clicks "enroll" in the user management, the fingerprint enrollment interface pop up, after press fingers three times to register fingerprint successful or fail. Also there is another auxiliary way to enroll, after the terminal connecting with system, then place fingerprint on the terminal.

2.3.1 enroll finger with fingerprints sensor

To suit of the software using, the fingerprint sensor should have the SDK permission.

1. there are two ways to open the user management:
 - 1) Double-click the short-cut icon "user management";
 - 2) Through [start] -> [program] -> [fingerprint verification server] to single-click [user management];
2. opens the user management, following login window pop up, the default user code is admin, the user password also is admin. After:



3. after entering the user management, select user management button,

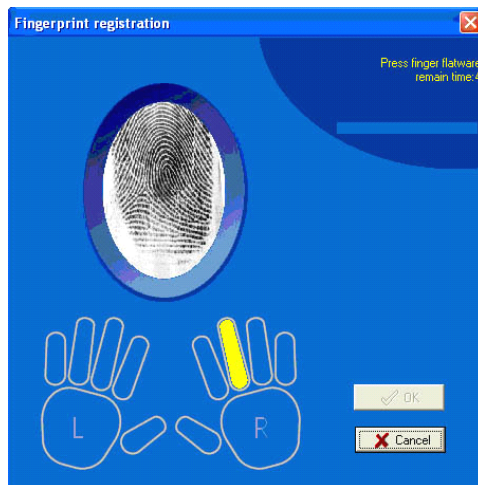
the user management interface appears, shows as the following figure

4.click "+" button, add new user, add the staff information. After adding finish, in fingerprint manager, choice "enroll" button in the "fingerprint sensor" item, enter enrollment fingerprint interface, like following interface

5. Use mouse to click the finger that you want to enroll, prepare to enroll , as shown following figure:

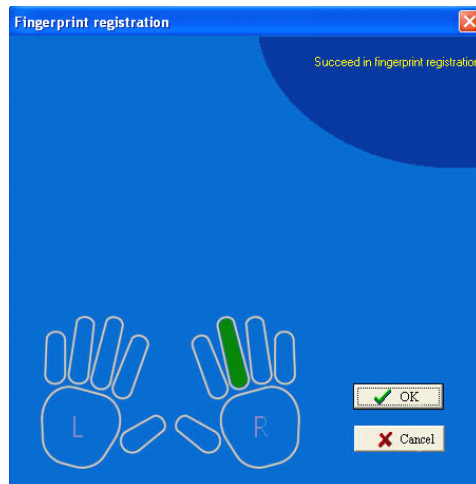


6.place the finger on the sensor, then take it away, enter pressing fingerprint status, like as following figure show



7.follow the information prompt, after, press the same finger four times,

if enroll fingerprint successfully, display interface as follow



8.Click "confirm" button, the enrolled fingerprint will save in system and return under interface.

9.in the fingerprint management item, selects “match” button to examine enrolled fingerprint which is saved successfully or does not



10.put the finger on the fingerprint sensor face, if enrolling fingerprint

successfully, following dialog box appear.



11.if following dialog box appear, that means you fail to enroll fingerprint , please replace 4-8 step to reenroll again

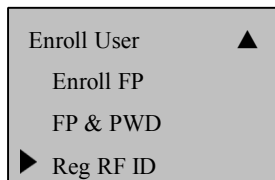


12.if following dialog box appear, that means you are successful to enroll fingerprint.

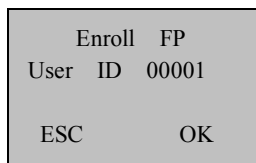


2.3.2 Remote enroll fingerprint on the fingerprint machine

1) when fingerprint machine connect with fingerprint verification server successfully, the Remote fingerprint Enrollment will appear, in the Menu-> User management-> user enrollment item



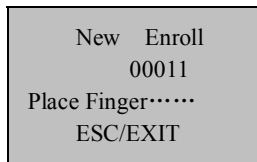
2) Select remote fingerprint enrollment, click “OK” to enter following interface:



Note: the fingerprint machine number is five digital, if the number you input does

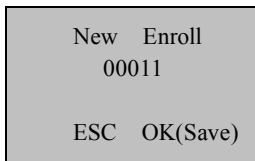
not fulfill five digital, the machine will autos-add Zero in front of figure, E.g the number you input is 1, the shown in the machine is 00001

3) Input number you want in the enrolling number column (number scope 1-65534) , press “ OK” to confirm , enter to next operation, display information as follow



New Enroll
00011
Place Finger.....
ESC/EXIT

4) Follow the prompt to continually press finger three times, if enrolled successfully, shown as follow.



New Enroll
00011
ESC OK(Save)

5) Press “OK” to saves up fingerprint you just enroll, so this enrolling flow is complete, if failed to enroll, the system will ask you return enrollment interface, enroll fingerprint more once again.

Note:

1.After enrolled fingerprint by remote enrollment, total of users and fingerprint in the server stat. area in will produce relative change, fingerprint is saved up in database of the verification server only, there is not information about user and fingerprint in the fingerprint machine.

2.User and fingerprint will be store up in the temporarily group no matter to how to complete the fingerprint enrollment through remote enrollment or fingerprint sensor, enter personnel group management to

list user and user's information which have been registered in the verification server through remote enrollment. For more detail ,please see operation 2.4

2.4 Grouping Personnel

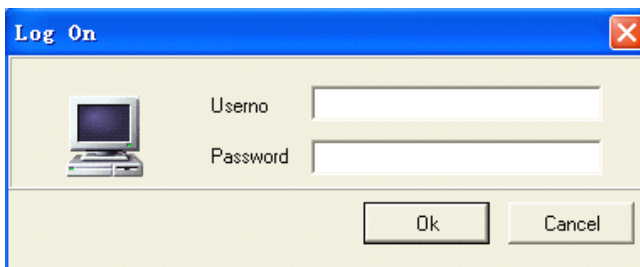
After enrolling all personnel , open "verification server personnel configuration" to enter "personnel group management" grouping personnel, under the default condition all user who is enrolled at the first time are completely mobile group personnel, according to the actual situation the manager effectively assign user into the fixed group

1. there are two ways opens the user management:

1) Double-click short-cut icon "verification server personnel configuration";

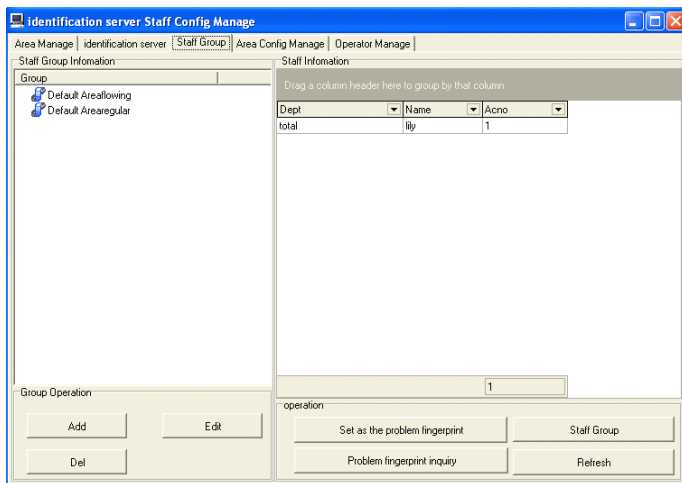
2) through [[starts] - > [program] - > [fingerprint verification server] to single-click [verification server personnel configuration];

2.Open the verification server personnel configuration, login window pop up, as shown in the following figure. The default user code is admin, the user password also is admin.

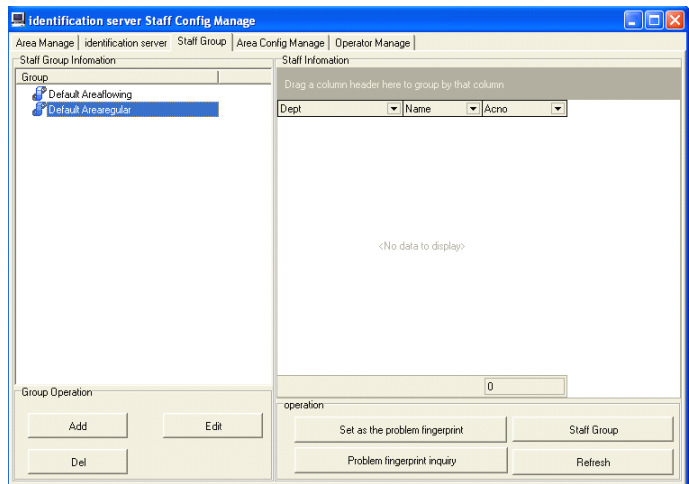


3.Enter the server personnel configuration management interface, chooses the personnel group management window, as shown in the following figure, list the user and its fingerprint which have been

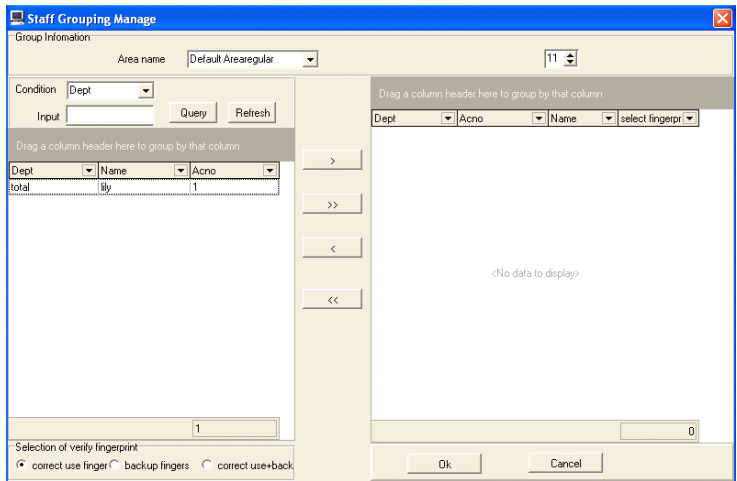
enrolled in the personnel information table in the verification server, as shown in the following figure



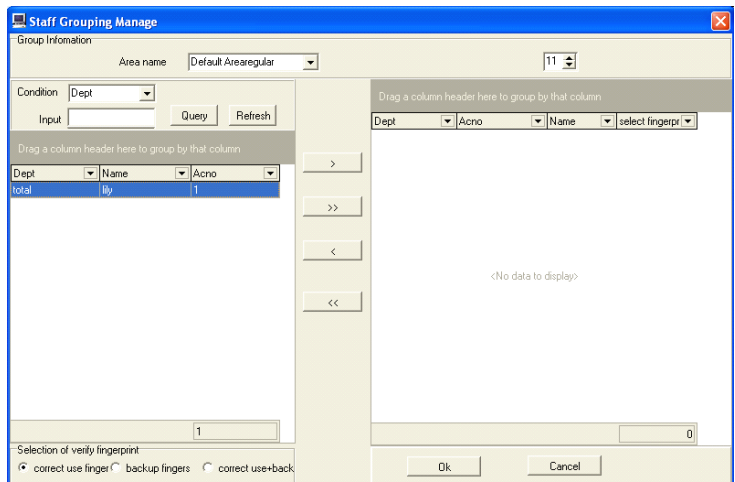
4. Allot personnel onto mobile group or in the fixed group depending on actual need, follow is to take the staff 1 is assigned to the fixed group as the example explanation. First chooses the default domain fixed group, as shown in the following figure.



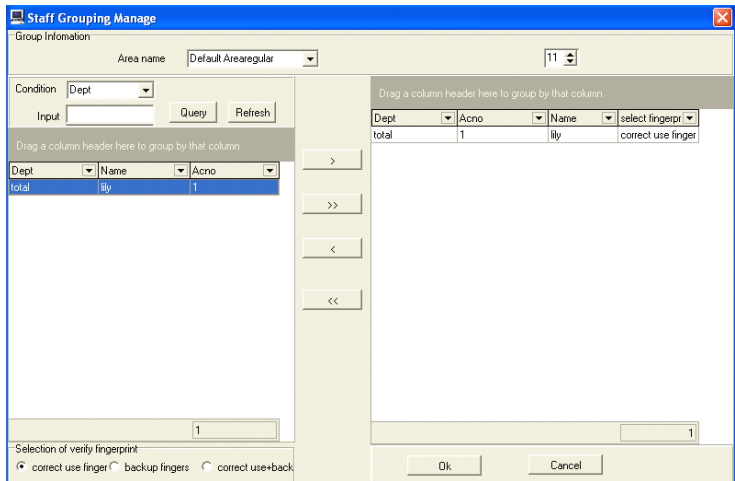
5. Click the Staff Group button again, the grouping personnel management interface pup-up, as shown in the following figure



6. Choose staff 1 in the personnel list area, as shown in the following figure:

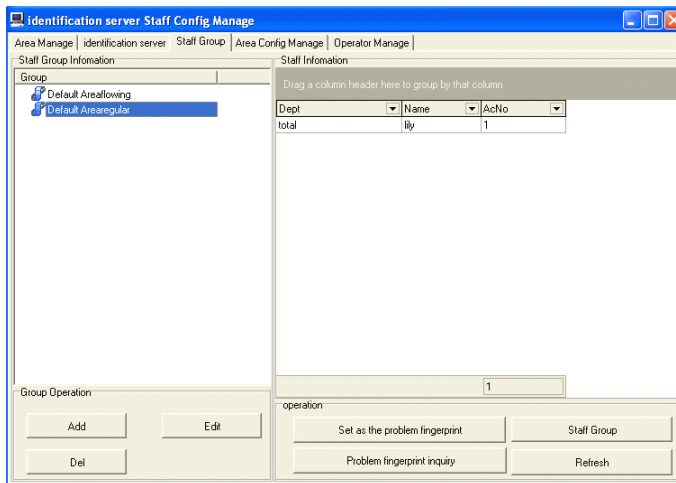


7. Click ">" button, the staff 1 display on the list area in right side, as shown in the following figure:



8. After allotting personnel, use choice button to select verification fingerprint, click "confirm" button to save setting. The system will return to the grouping personnel management interface, in the default

domain the fixed group will add a user 1 in the corresponding list area, the following figure showed:



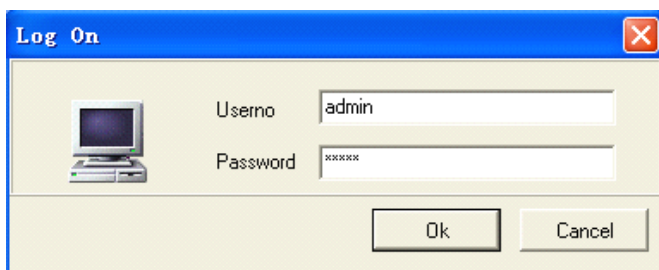
Note:

- 1, in the personnel information group region, choose “Add” button, may add the new group; choose “Modify” button, may modify the designation group name, choose “delete” button, may delete the designated group.
2. In the operation region, for the user who regard as verification rate low, may choose the difficult fingerprint button to set these the difficult fingerprint, thus reduces False Rejection rate.
- 3, choose “difficult fingerprint setting inquiry” button, may view the difficult fingerprint list.
- 4, choose the default domain mobile group, in right side the personnel information will demonstrate users who belong to the mobile group in the list area ; choose the default domain fixed group, in the right side the personnel information will show users who belong to the fixed group

in the list area, choose the refresh button, in the right side the personnel information will display complete user in the list area.

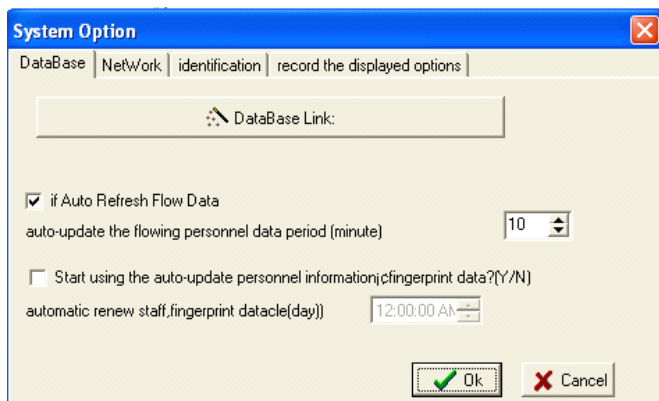
3. System Setting

Start remote verification server, click "the system setting" on the main interface, confirmed manager's dialog box will pup-up, the default manager and password all are "admin", as show in following figure:



3.1 Database

Databases link attribute, personnel information, and fingerprint data parameter setting, as shown in following figure:

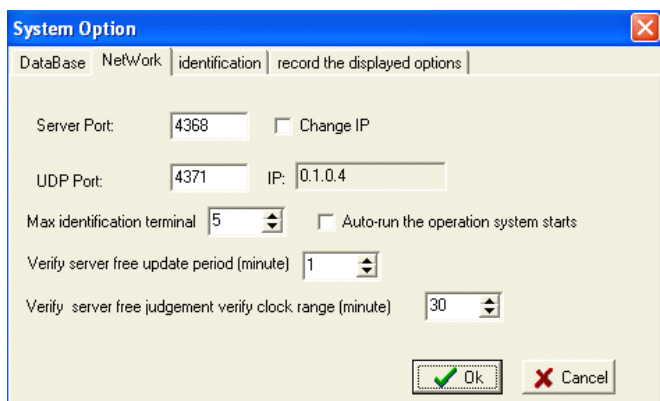


How to set database link, the database link has provided many kinds of common database interface, like Access, SQL and so on, there is a script file in the installation disk.

Whether start to automatically refresh the mobile data, here ability to set the cycle time to automatically refresh the mobile personnel data, the default time is 10 minutes, namely for each 10 minutes the mobile personnel who carry on 1: 1 matching fingerprint join to locally.

Whether start to automatically renew the personnel information, the fingerprint data. Define the time to automatically renew the personnel information, and the fingerprint data cycle every day, set it by user herself.

3.2 Network



The remote verification server port is unified as "4,368", please do not revise it. If the IP address of the remote verification server has to be changed, put "\/" in front of modify IP firstly, then revise this IP.

UDP port, the unification is "4,371", please do not revise it.

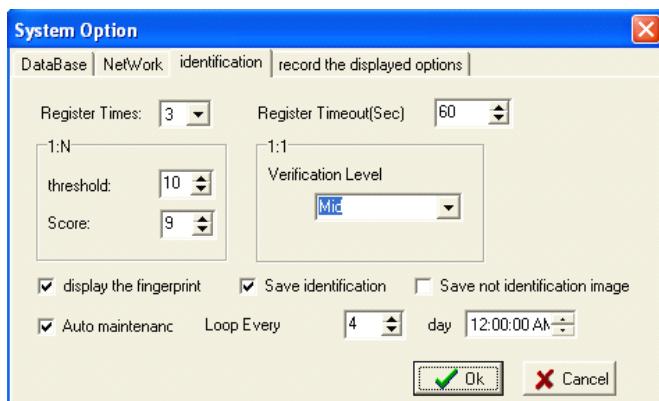
Corresponding the verification terminal quantity generally is "3", most concurrent verification terminal quantity is "5".

Automatically run when the operating system start, if this item has been selected, then in each time when the system start the fingerprint verification server will automatically start and run.

The refresh cycle of the idle time of the verification server, the default time is 1 minute, refresh server idle record to a time per a minute.

The verification server idle is used to estimate the time scope of verification recorded ,the default time is 30 minutes, estimate whether the total of attendance records are least in the set time scope in the verification server, when A5-R does not continually connect with other servers, auto- turn to the idlest Server.

3.3 Validate



Enrollment times: Express how many times to enroll fingerprint through remote enrollment, the default times are 3 and can be set to 4 times at most.

Remote enrollment overtime (second): while remote fingerprint enrolments, the period between previous fingers presses and next finger press is remote registration overtime. The default overtime is 1 minute, which means that it will automatically pop up fingerprint registration menu if there is no next finger press within 1 minute after the previous finger press.

1: N and 1: 1 threshold is adjusted by the manager depending on actual situation of the passing rate, recommend use the default value. Matching score and threshold affects False Rejection Rate (FRR) and False Acceptance Rate. The more Value is bigger, the more False Rejection Rate (FRR) is higher, and then False Acceptance Rate (FAR) is lower. The system default value respectively is: 10, 9

Display fingerprints picture: Indicates whether display fingerprint figure or not in the main interface in the case of remote identification server matching fingerprint after running

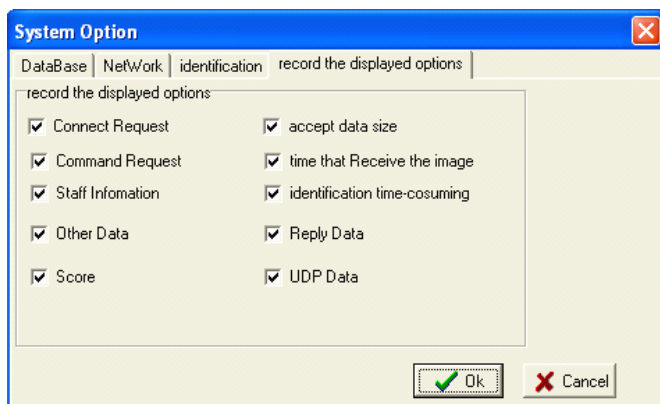
Save verification record: whether the verification record store in the database.

Implement system maintenance: In the set cycle the system of the remote verification server optimize memory, and restart the system.

System maintenance cycle: set time cycle system optimize memory period.

3.4 Recording display

According to own need manager may change each communication parameter in here which demonstrate in the fingerprint verification server main interface, As shown in the following figure, put"√" in front of the information which is needs to be demonstrated



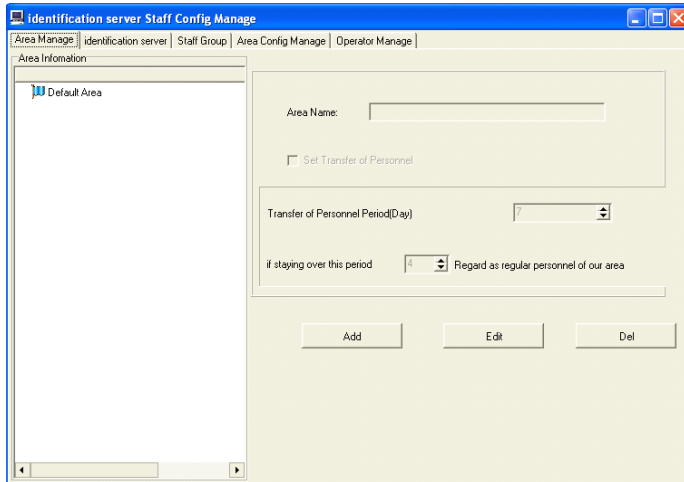
4. Verification server personnel configuration

When “Remote verification server personnel configuration” is opened, also need to validate administrator identity. The default administrator and password are “admin”

4.1 Domain management

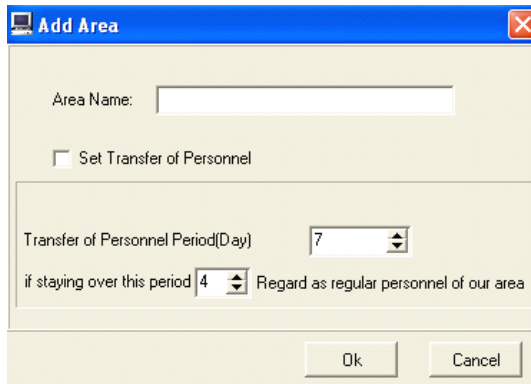
Through Domain management, add and modify select relative domain information and cancel selected domain

The system can set flowing cycle time in the domain and the default value is 28 days, which means the system will rectify the flowing personnel to fixed-group personnel automatically if those personnel remains here exceeding 28 days. In this case, the flowing personnel have been in fixed group in the region.



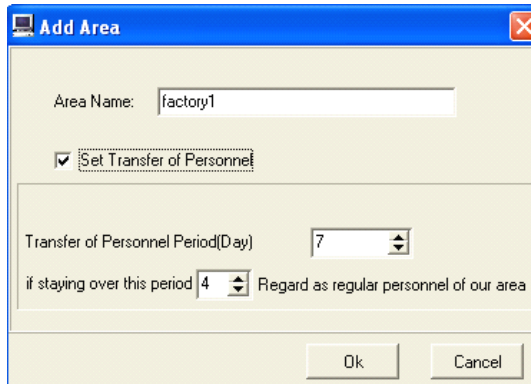
4.1.1 Add region

1) Click add button, the following dialog box appear.:



2) fill full blank with region's name, if want to reset the condition of flowing personal in this region, so put “√” in font of personal name who

will be reset, the setting effect is shown in the following figure



Add Area

Area Name:

☒ Set Transfer of Personnel

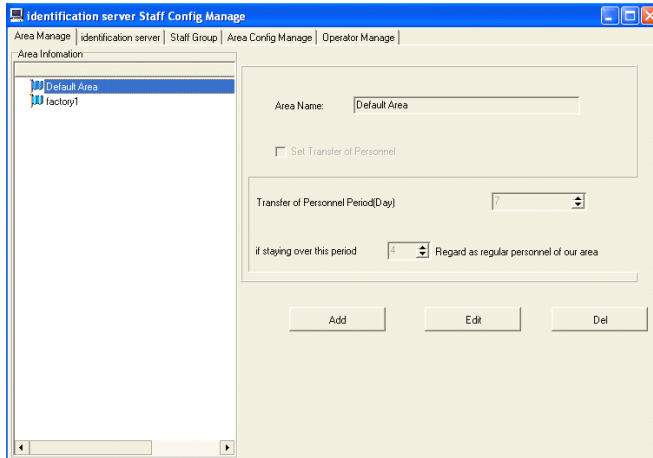
Transfer of Personnel Period(Day)

if staying over this period Regard as regular personnel of our area

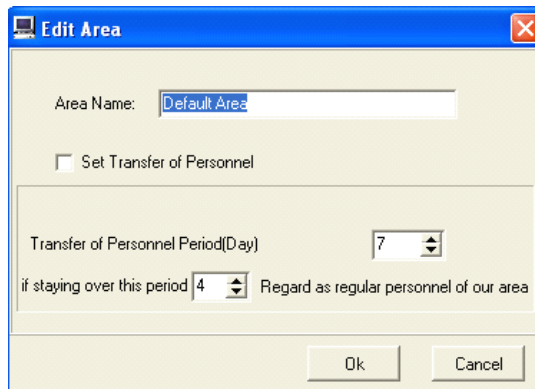
3) After complete setting, Click “confirm” to save this setting, may continue adding new region

4.1.2 Modification region information

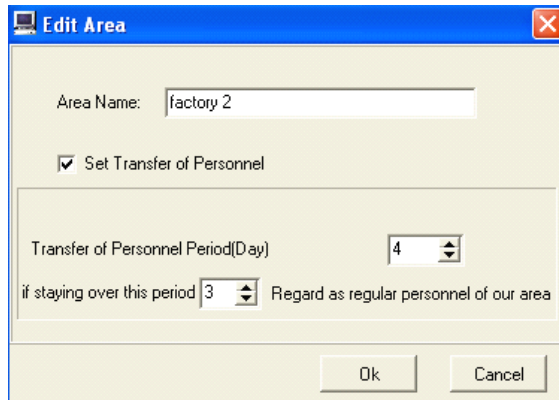
1) Select the domain which want to be modified and make it in bright statue, shown as following figure:



2) Click Edit button, the following dialog box appear.



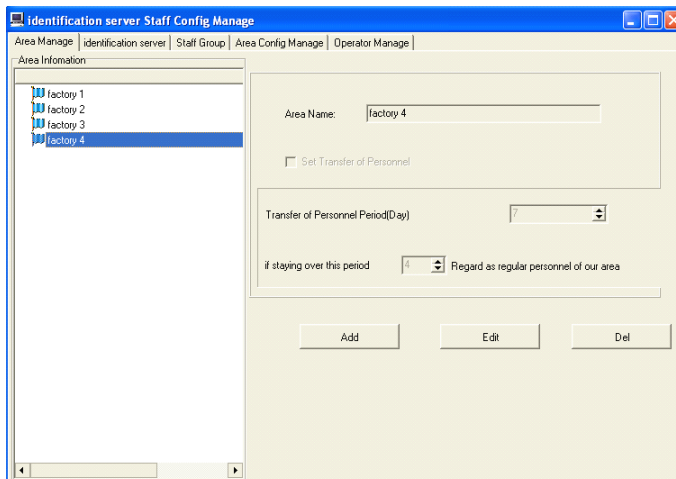
3) Modify the information which is in the region, the modified effect is shown as following figure.



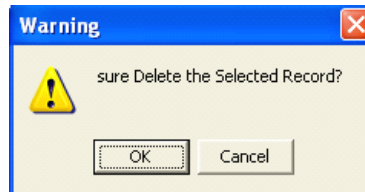
4) after editing, click “OK” to save this setting

4.1.3 Cancel domain

1) Select the region which want to be deleted and make it in bright statue, shown as following figure:



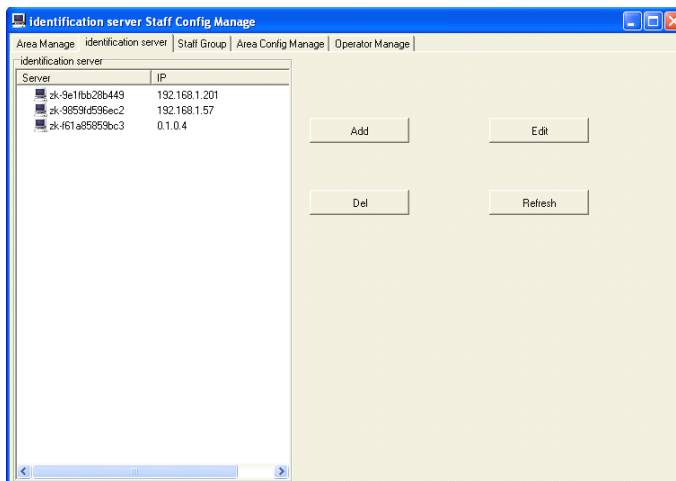
2) Click delete button, shown as following dialog box :



3) click “Ok” button to delete this domain , Click “cancel” button to give up this operation.

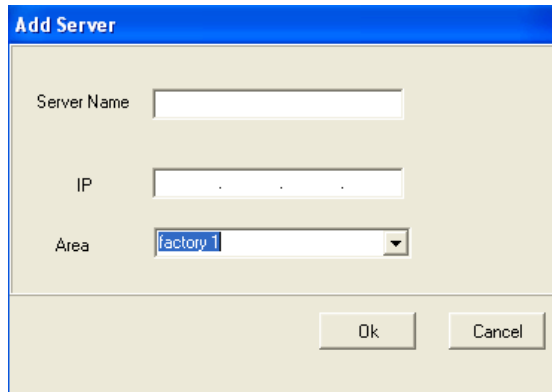
4.2 Remote Verification Server Management

One Remote Verification Server is able to join many terminals, there are many remote verification servers in the one domain, we can maintain, add, modify or delete these server.



4.2.1 Add remote Verification Server

1) Click “**Add**” button, the following dialog box appears.

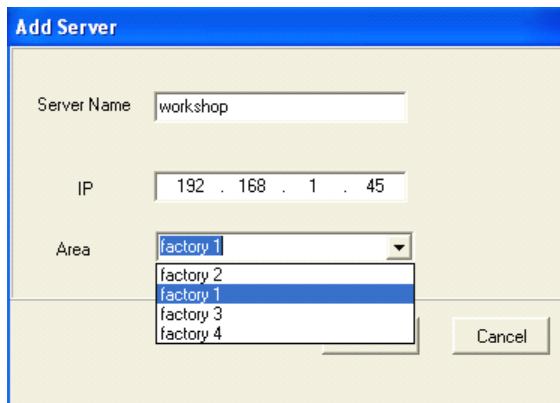


The 'Add Server' dialog box is shown with the following fields:

- Server Name:
- IP:
- Area:

Buttons: Ok, Cancel

2) fill this blank with Saver’s Name. IP address and belong to domain.
As shown following figure.



The 'Add Server' dialog box is shown with the following fields filled:

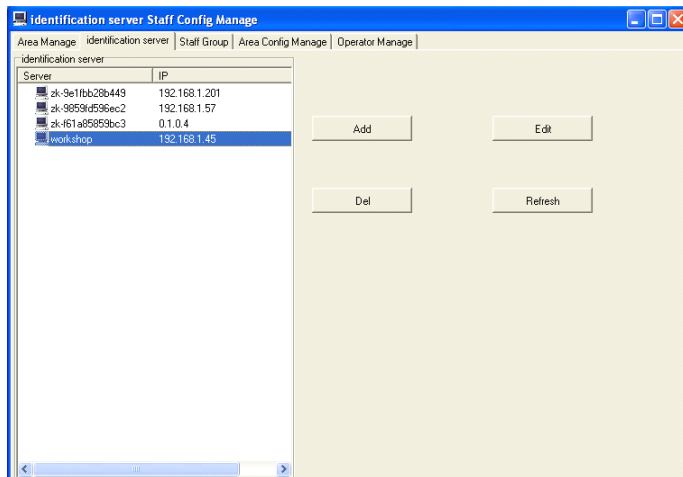
- Server Name:
- IP:
- Area:

Buttons: Cancel

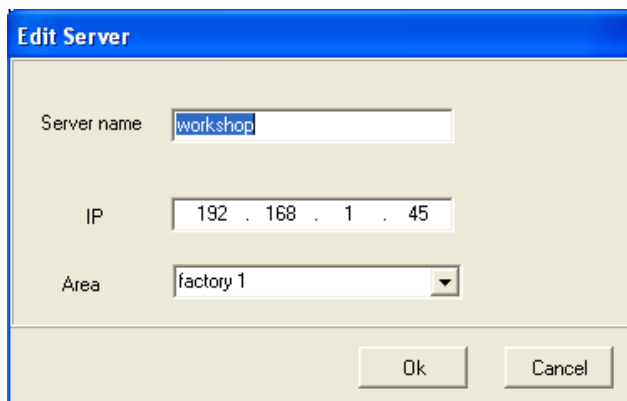
3) After completing setting, Click “confirm” to save, may continue new domain

4.2.2 Modify remote verification sever

1) Select the domain which want to be modified and make it in bright statue, shown as following figure:

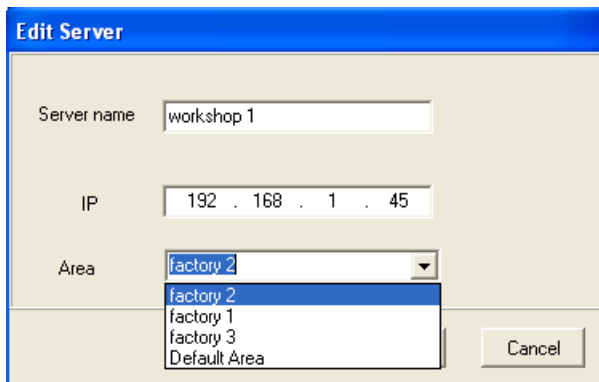


2) click edit button, shown as following dialog box:



3) Can modify Saver's Name. IP address and belong to domain. This

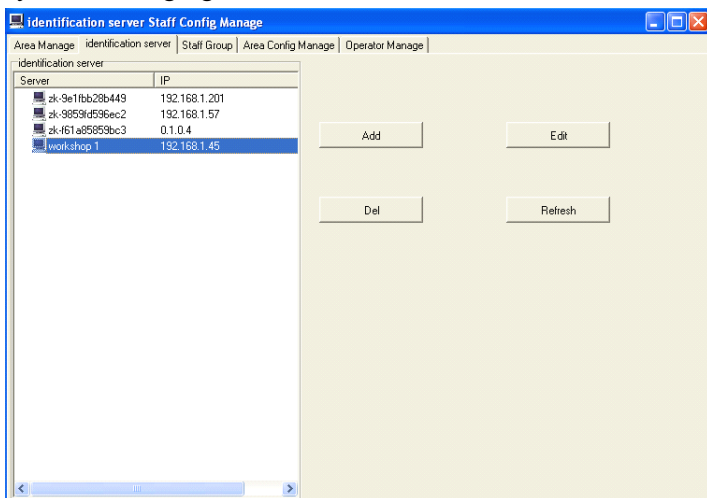
modified effect display as following figure.



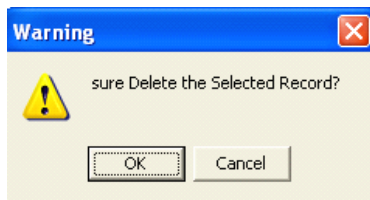
4) after modify finishing, click “confirm” to save it.

4.2.3 Delete remote verification sever

1) Select the region which want to be deleted and make it in bright statue, display as following figure



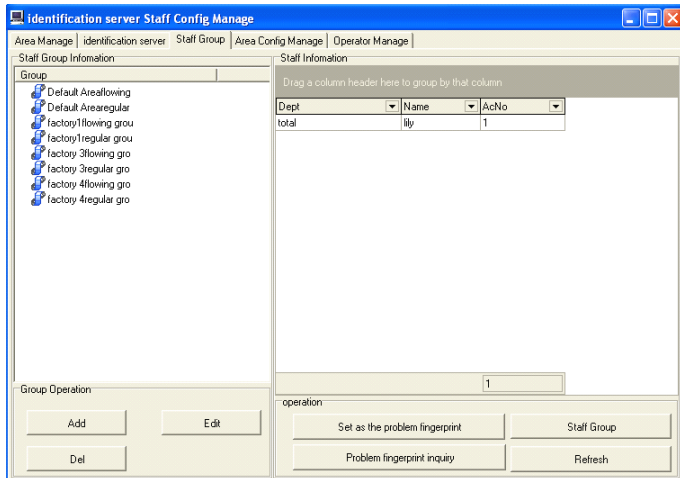
2) Click “cancel” button, following dialog box will appear



3) click “OK” to cancel this domain, click “cancel” button to give up this operation

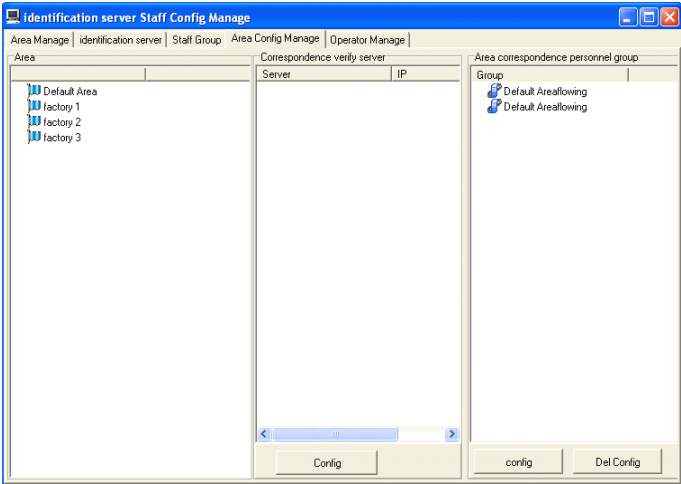
4.3 Staff Group Management

Select personnel group management, the display as follow, for more detail, please refers to 2.4 personnel grouping.



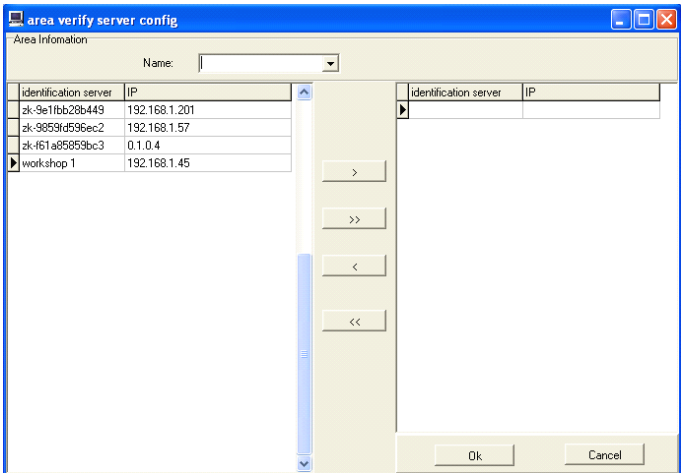
4.4 Region Configuration Management

The system adopts region to manage, the region corresponding personnel group, and the Remote Verification Server, ability to configure region in here, as shown in following figure.



4.4.1 Configure Verification Server

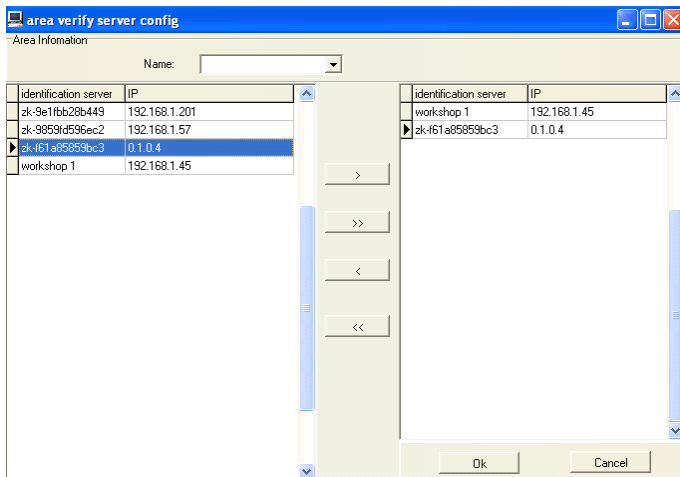
Select the corresponding verification server button



All servers in this system will display in left list box, the right list box will show all servers in this domain, and through move the button it is able to reconfigure Server in the selected area.

4.4.2 Configure corresponding personnel group

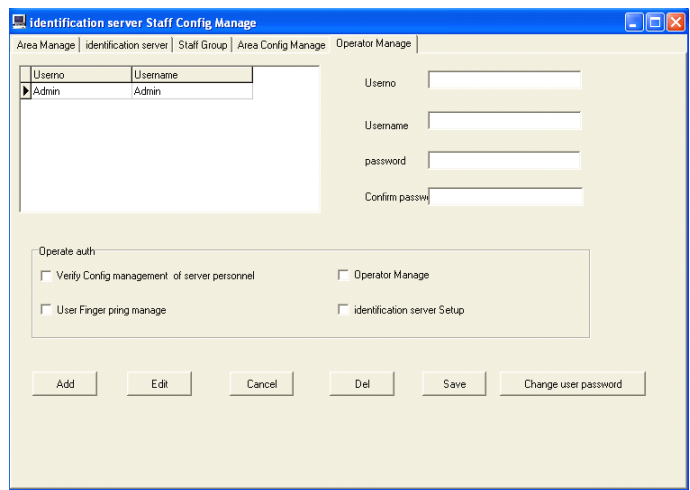
Select following configuration corresponding personnel group



All personnel in this system will display in the left list box, the right list box will show all personnel in this domain, by moving button, the reconfiguration personnel in the selected domain is available.

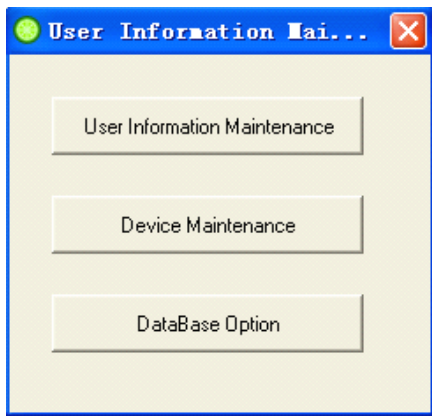
4.5 Operation User Management

Supper administrator code, user name, and password all is "admin" in this system, in order to provide system with security, here to revise user name and password is allowed, otherwise depending on the privilege which "privilege" list supply, it is able to add operator who own different privilege



5. User Management

While open “user management”, the administrator verification is requested, the default administrator and password all are “Admin”, after verify successful, pop-up following dialog-box:



5.1 User management

Enter “User management”. In the User management, there is the user list on the left and there is user maintenance domain on the right. Click “+” or “-” to add or delete a user. Also other information such as name, gender and position can be controlled here.

User Information Maintenance

User List

Drag a column header here to group by that column

ID	Name	Number	Department	Gender
1	111	123123	total	F
2	2		total	F
3	3		total	
4	4		total	
5	5		total	
6	6		total	
7	7		total	
8	8		total	
9	9		total	
10	10		total	

FP enrollment status Import Export

Department

Department: total

Name: 10

No: 10

Number:

Gender: ☐ Male ☐ Female

Title:

Card Number:

Fingerprint manage(Require U.are.U Scanner support)

Enroll with sensor

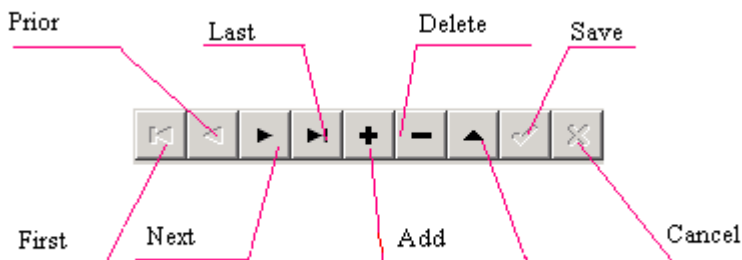
For fingerprint management, we recommend users to use URU fingerprint sensor. After installing URU properly, click “Enrol”, and a fingerprint registration interface pops up. Registration is successful or failing after three finger presses. There is another auxiliary registration method that is to press fingerprint on the terminal after connecting the terminal, detail operation see 2.3 fingerprint operation.

To Transit user information and related fingerprint. It is available to upload the user information and related fingerprint to the terminal and download them to remote verification server database. This is an

emergency function of remote verification server. Because we cannot make sure there is no accident for remote identify sever network, we use this method to upload the fingerprint to the terminal. When accidental occurs in the remote identify sever the terminal will automatic switch to offline matching mode

5.1.1 Datasheet Process Tool Bar

The Datasheet Process Tool Bar contains the following operation buttons:



In the datasheet, the row marked with ► symbol is the current row, and all operations for he sheet is conducted in the current row.

Click buttons to carry out corresponding operations for the datasheet.



First: To move the current row to the first row.



Previous: To move the current row one row upward.



Next: To move the current row one row downward.



Last: To move the current row to the last row.



Add: To add a new row in which new data can be entered in, and the current row is the new row.



Delete: To delete the current row.



Edit: To modify the data in the current row.



Save: To save the data after edition or in the newly added row.



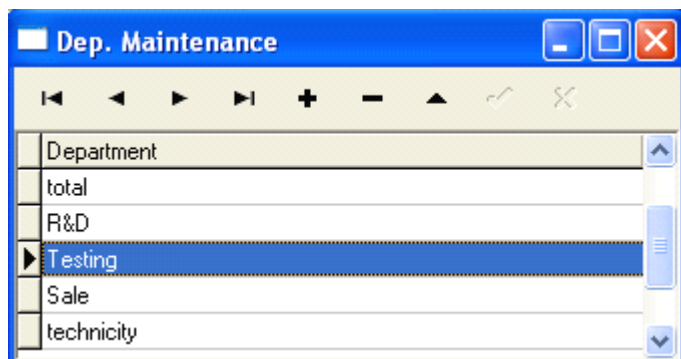
Cancel: To cancel the result of adding a new row or editing the data.

Under the status of adding or editing, the result of moving data will be automatically saved.

In the datasheet, click on the row to select it, and select multiple rows by pressing Ctrl and clicking at the same time when possible. The selected rows will change to blue.

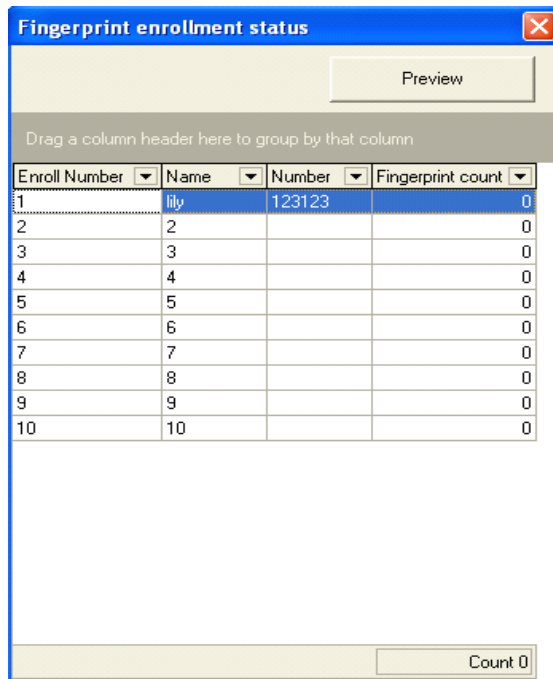
5.1.2 Department management

Select “Department management” button, department maintenance box appear “Department management” can add a department. Use drop-down arrow to move related personnel to corresponding department after adding a new department.



5.1.3 Fingerprint enrollment situation

Choose fingerprint enrollment situation button, may view each user corresponding total of fingerprints which have been enrolled.

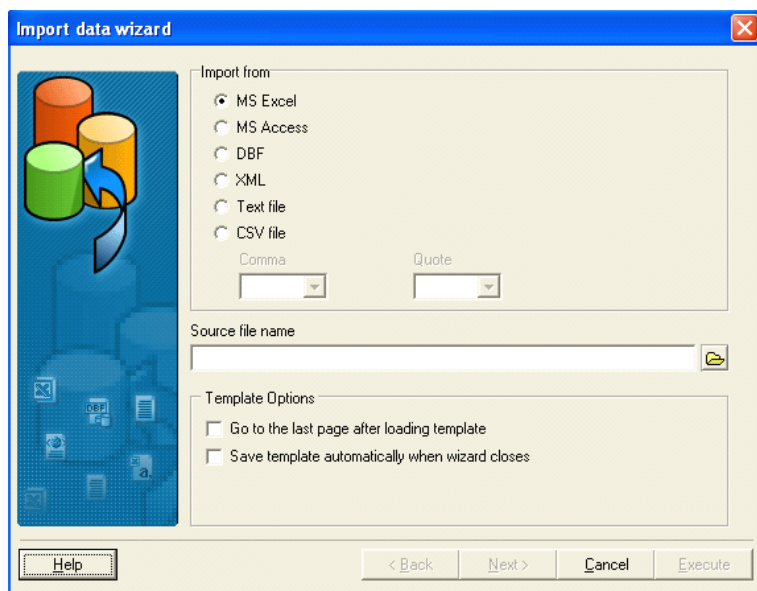


Enroll Number	Name	Number	Fingerprint count
1	lily	123123	0
2	2		0
3	3		0
4	4		0
5	5		0
6	6		0
7	7		0
8	8		0
9	9		0
10	10		0

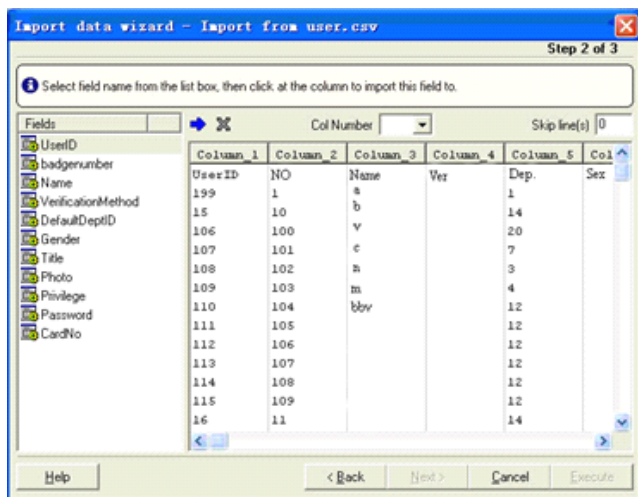
5.1.4 Import

this system support following form to import data : MS Excel, MS Access, DBF, XML, Text File, CSV file, we recommend adopt the CSV file to import, follow the example take the CSV file to import the user data, that explain how to import data:

1. first single-clicks the single selection box of CSV file, then chooses the data file which want to be imported :



2. Click Next, following figure appear:



Fields list in left hand side is the field list, right hand side is the row to import file, there is a Skip line(s) that refer to the total of lines you want to skip on right-up part, if the first line of the file that should import is not the concrete data, may fill in 1 in this, indicated jumps the first line to start to import.

Fields table explanation,

UserID: System interior use ID, while import this field which cannot be used, please do not use this field.

BadgeNumber: The user serial number, this serial number is the user the serial number which uses in software and the fingerprint machine. This field data must exist.

Name: The user name, this field data exist.

VerificationMethod: User confirmation way, when this item does not exist ,may neglect it.

DefaultDeptID: Department serial number, if inducts other origins the data please to neglect this row.

Gender: gender.

Title: job.

Photo: The picture, neglect it.

Privilege: The jurisdiction, may neglect it.

Password: The password, neglect it.

CardNo: The ID card number may neglect it.

3. before importing, first select field which want to be imported in Fields list, then chooses corresponding the row in right hand side list,

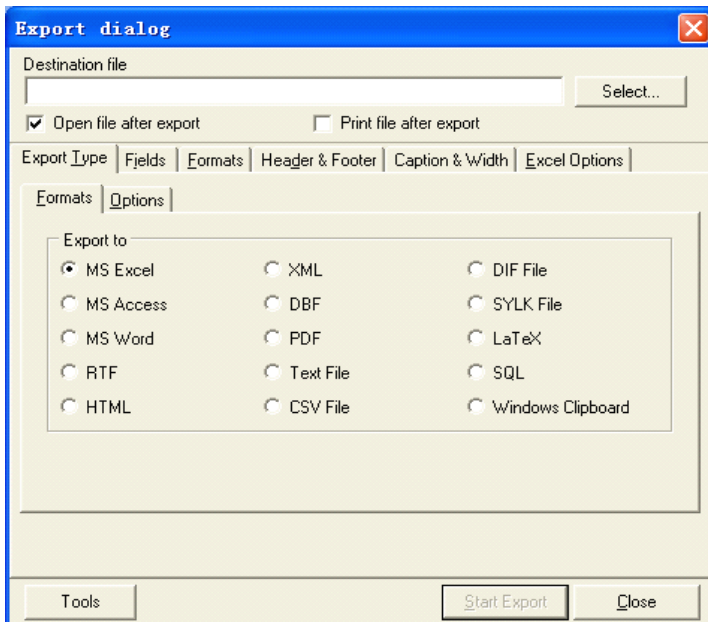
Fields list can automatically add a corresponding row serial number to the field name behind, so after the field and the row meet, single-click next step.

If you want to cancel setting of some field, first chooses this field, then single-click the corresponding row, software cancels this field setting.

4. single-click the Execute button to execute import operation

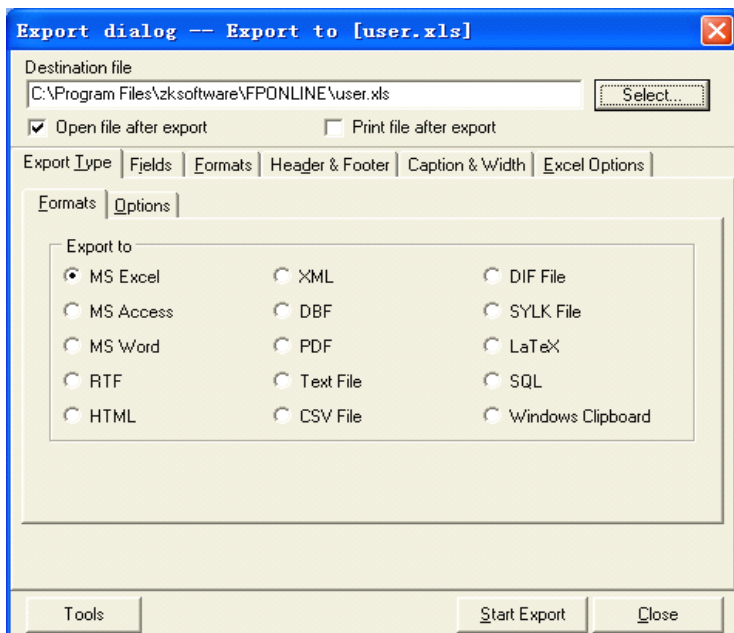
5.1.5 Export

Single-clicks the export button to the following interface appear:



Follow take the MS Excel as the example to explain how to export file,

1. chooses the goal file which want to be exported



2. Single-clicks (Start Export) button to export the default form file. Moreover may single-click the different option card to configure the output content:

Fields: Chooses field which want to be export, default all, when the field have been selected only the field content will be exported.

Formats: Assigns the form for each kind of field output value.

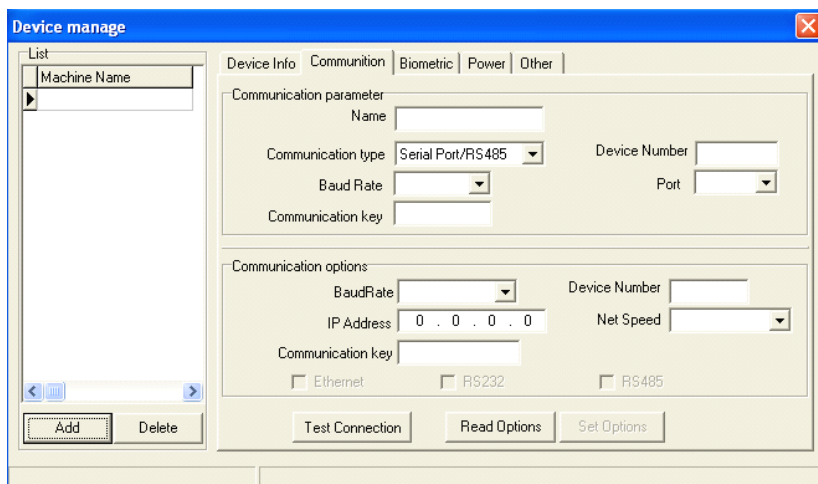
Header & Footer: The text of files to start and end

Caption & Width: Field title and width.

Excel Options: set font

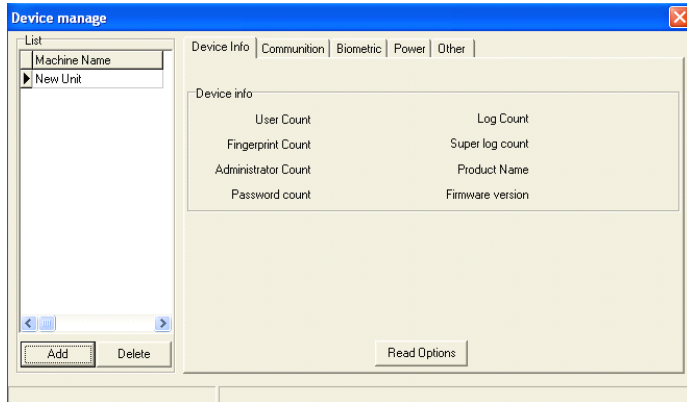
5.2 Equipment Management

Equipment is to manage and maintain the terminal, after opening the terminal; it is able to set each kind of the standalone parameter, like as follow figure.

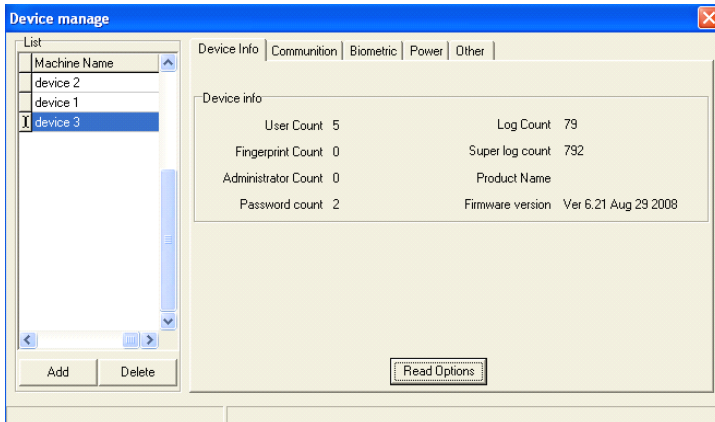


5.2.1 Fingerprint machine Information

1) Click fingerprint machine information page, shown as following figure:

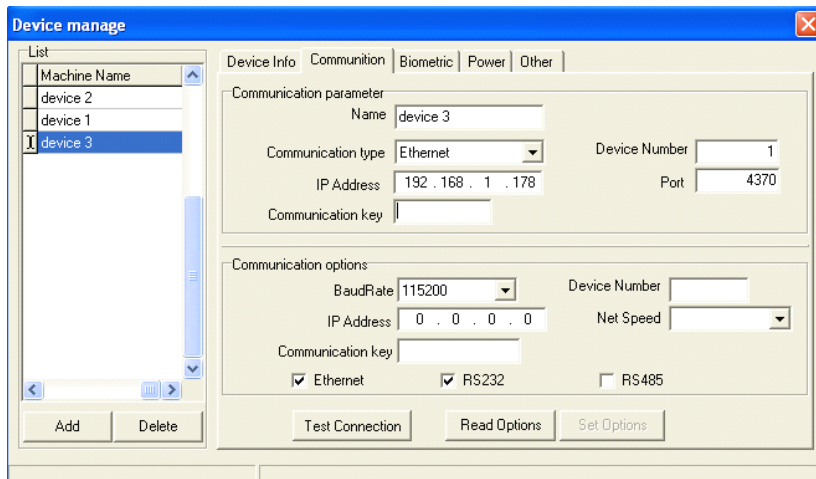


2) select the fingerprint machine you want to view from list column, click “Read-in setup” to show fingerprint machine information on this page, shown as following figure.

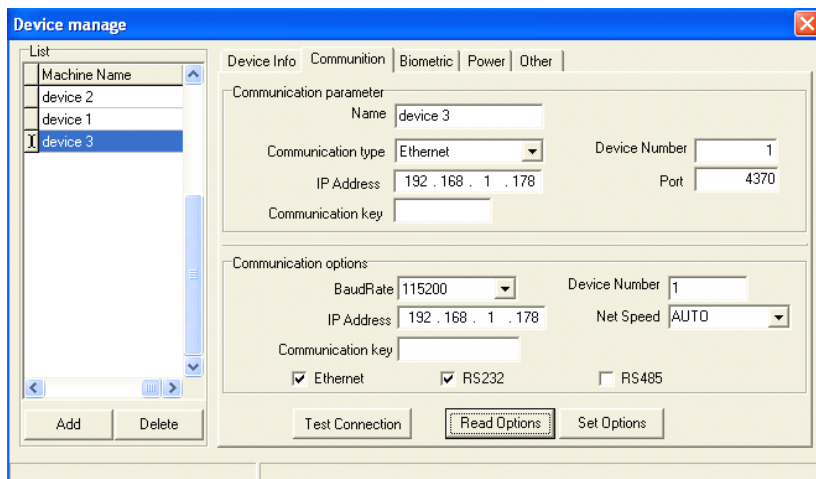


5.2.2 Communication setting

1) Click “communication setting” page, shown as following figure.



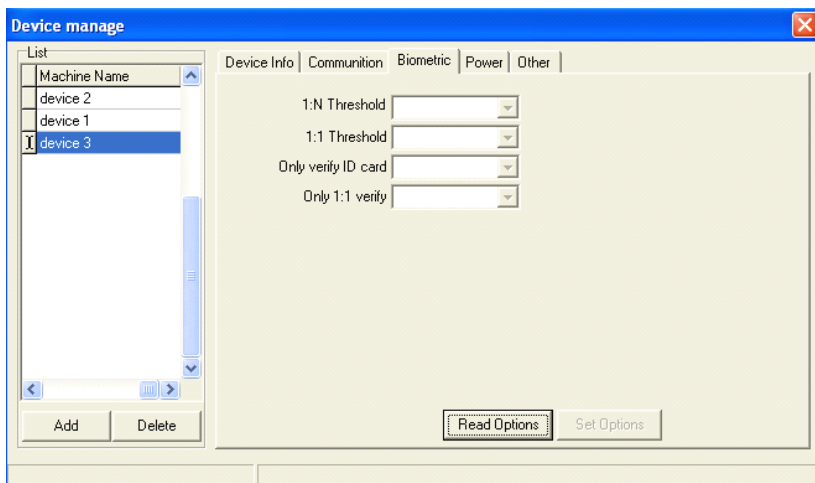
2) select the fingerprint machine you want to view from list column, click “Read-in setup” to show the communication information of fingerprint machine on this page, shown as following figure



3) if you want to modify communication information of this fingerprint machine. After modifying, click “application setting” to take effect.

5.2.3 Validate

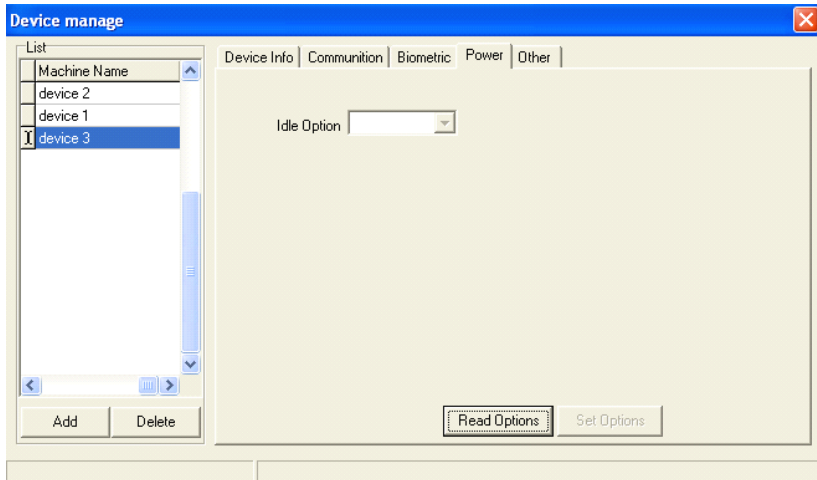
1) click “validate” page, shown as following figure:



2) in order to get the best effect, you are allowed to modify option depending on the actual status,

5.2.4 Power management

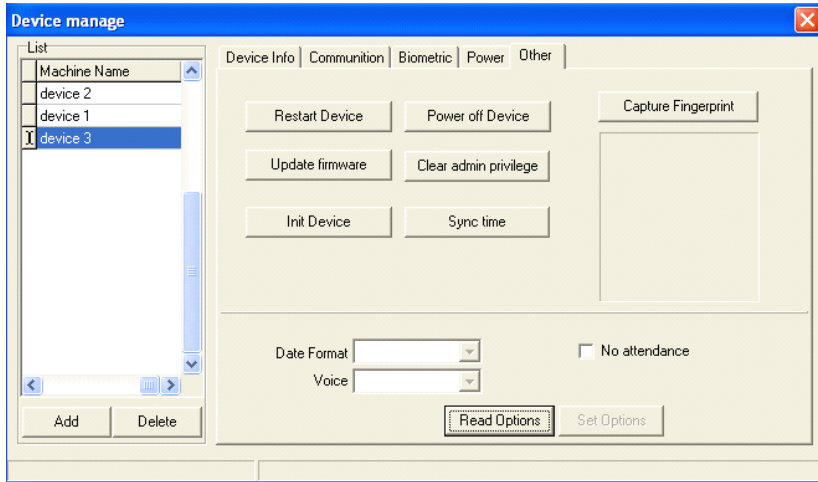
1) click “power management” page, shown as following figure:



Idle setting: modify the state of "Idle Setup" and minutes of "Idle Time", then click the "Application Setup" to complete set. When the idle time is 0, then the idle setup function is off. When the value more than 0, the machine will enter into idle state after arrives at define time

5.2.5 Other Setup

1) Click "Other setup", Shown as following figure.



2) Restart equipment: Click the button to restart fingerprint machine.

Clear Administer Privilege: this function can clear all administer privilege which has registered in the fingerprint machine.

Upgrade Firmware: we suggest that user doesn't use function at random, after receivers the manufactory notice, follow the guide which factory offer

Initialize Equipment: This function is mainly used to clear all data in the fingerprint machine.

Capture Fingerprint Image: This function can be used to view fingerprint, if want to examine fingerprint, please place finger on the sensor window, don't move, and then click the button, and will see the fingerprint image.

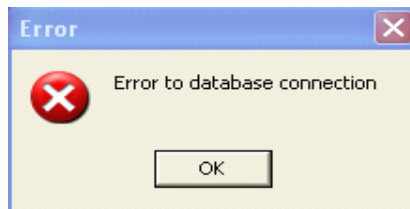
Date format: select date format from down draw box, this date format is the displaying format on the initial interface of the fingerprint machine.

Sound function: select start or shut down whether use with sound

5.3 Databases Setup

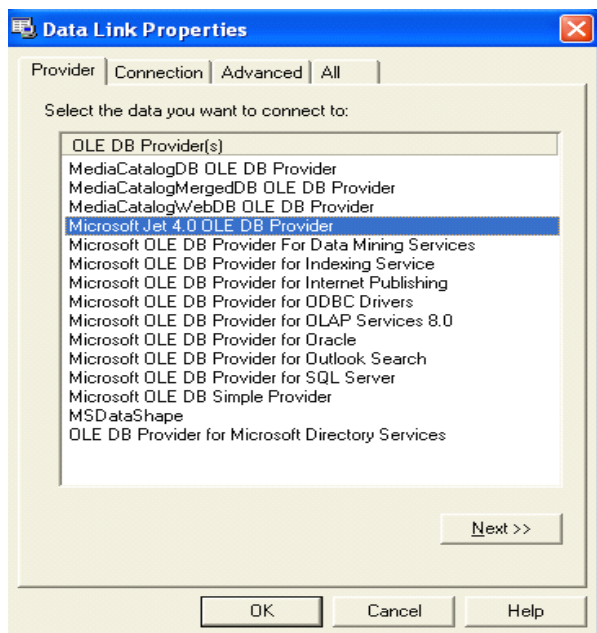
This system adopt Microsoft the ADO database interface, the default database is the single-user Access2000, which file name is att2000.mdb, according to the actual situation you may reset database link.

If the following system prompt error appears, you need to correct your database link setting

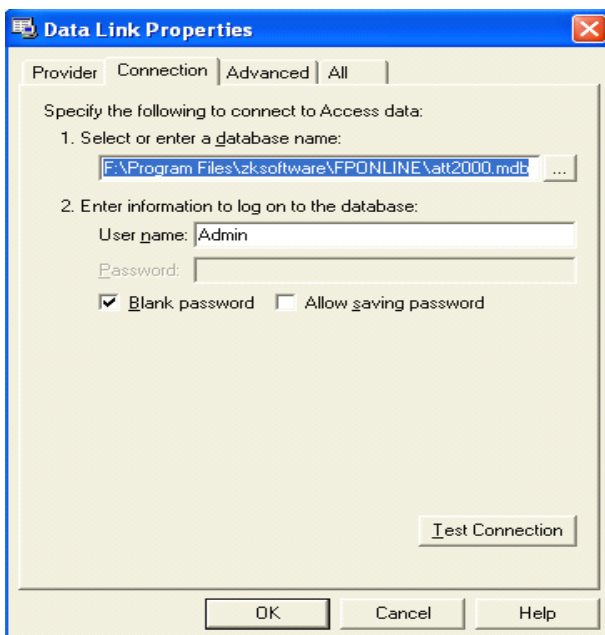


1st, How to connect with Microsoft the Access database :

1) Provider chooses Microsoft Jet 4.0 OLE DB Provider;



- 2) single-click next step or connection, enter the following interface:

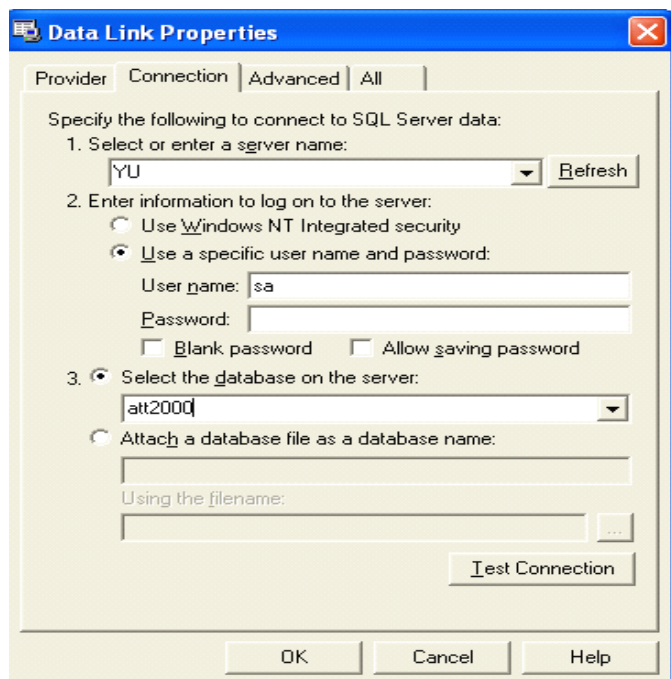


Click  the button, may choose the database file

1.How to set SQL Server database connection :

If you want to use the network database, first you should establish the fingerprint Time and Attendance system database on the database server. In the installation directory of the Time and Attendance system, you may find file with name of sqlserver.sql, this file is SQL script to set the fingerprint Time and Attendance system database in Microsoft SQL 7.0 Server . If you use other database server, please refer to this file fingerprint Time and Attendance system database.

The provider chooses Microsoft OLE DB Provider for SQL Server, click next step or link, enter the following interface:



Confirm server name which is used to store database, register the server information and the database name. Click OK button to complete the setup SQL Server.

6. Appendices

6.1 Datasheets processing tool bar operation



In the datasheet, the line with the blue bar is current line, all operation of form all carry in the current line, click button, performance corresponding operation in the datasheet.



The first record, transfer record from the current line to the first line;



: Previous, from a current line forward moving line;



: Next, moves a line to next line;



: The tail record, transfers record from the current line to the last line



: Inserts the record, add new record;



: Delete the record, delete the current record.



Edit the record, enter the edition condition to modify record;



Save the record, after the edition, save up the value;



Cancel edition, cancel all the revision which apply to the record ;

6.2 Arrangement

According to ascending or descending sort arrange record in the data sheet, directly click row head which is allow to arrange, the following figure illustrate the arrange by the name:

Name	Number	Department	Gender	Title	Privilege	
admin	123123	total	F		User	
10		total			User	
2		total	F		User	
3		total			User	
4		total			User	
5		total			User	
6		total			User	
7		total			User	
8		total			User	
9		total			User	

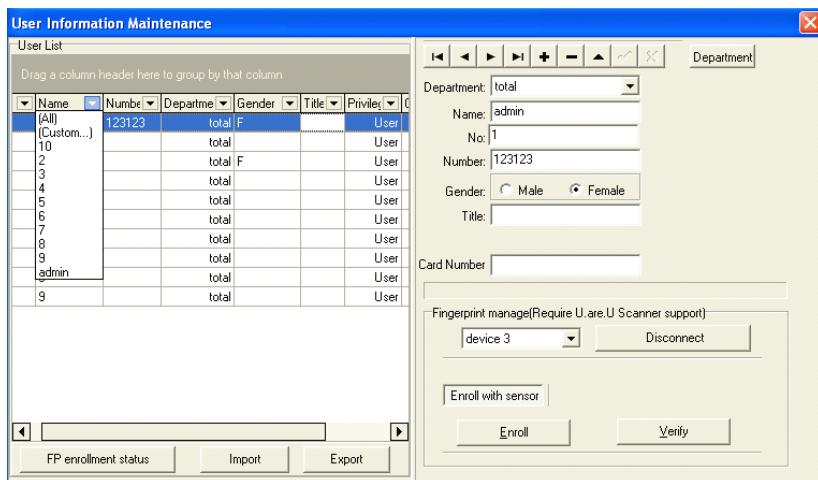
there is a triangle mark nearby the field name which has been selected, if the triangle faces upward, which express that these record are arranged

accordance with ascending sort, the triangle faces downward, which express that these record are arranged accordance with descending sort, you may click the triangle mark to change ascending and descending arrangement.

6.3 Filter data

Filter data is to select records which meet the condition from the original table, which will display in the current window. the operation flow to filter data order

1.click drag down box of the data which you search, the following figure appears



2.click (customize filters) ,the following figure appears

Custom Filter

Show rows where:

Name

like

☒ AND ☐ OR

Use _ to represent any single character
Use % to represent any series of characters

OK Cancel

3.input condition, like show all use who's surnames is Zhang :

Custom Filter

Show rows where:

Name

like a%

☒ AND ☐ OR

Use _ to represent any single character
Use % to represent any series of characters

OK Cancel

Note: % Must be English character, Chinese character is not to be recognized

4.Click confirm, show the result to filters:

☒: Whether uses the filtering condition.

☐: Cancel filter operation.

If want to cancel current filtering result, display all records, then single-click ☒ or ☐ either.

6.4 Record Grouping

According to some or many fields, the record will be grouped. Just draw the row which should be grouped to blank part above row head , realize the grouping, like following figure:

6.5 Count

Software is able to automatically count the total of record, but also may count the total record of the group, like as above department: R& D department Count=1, R&D department has 1 person at present altogether. But there is the Count 50 in below part that indicate total of records at current.

7. Trouble shooting

Questions: Why do some fingerprints fail to pass verification until they have to match many times, some even fail to match to passes

Answer: if the customer use the A5-R itself off-line to enroll fingerprint, upload it to the server database. Because the A5-R machine capture fingerprint template which has been compressed by our standalone fingerprint algorithm and itself performance is limit, this way precision does not match the method which utilize direct on-line to capture fingerprint template . In order to guarantee the saving fingerprint template precision in the database, please use the A5-R on-line enroll fingerprint or uses the U.are.U 4,000 fingerprints sensor to enroll the fingerprint.

Question: why is there non- UDP data in the Server log.

Answer:(1) whether the verification Sever terminal has already set "the remote verification server address" as this machine IP address. After setup, please be sure to restart the verification terminal.

(2) Whether "UDP" setting option is closure or not in the system Setting/record demonstration

(3) Whether this machine has been installed firewall software and UDP port (4,371) is disabling.

(4) Whether two verification servers procedure is open

(5) Make sure that the network is no exceptionally, whether the network port lamp of the verification terminal is normal; use Ping to check the terminal IP in this machine .

Question: after the verification server is starting, the prompt appear, please configure the personnel information in the "server personnel configuration management" for this verification server.

Answer: (1) there is no registered the personnel in the system.

(2) This verification server has not configured the domain.

(3) This verification server has not configured the personnel group to respective domain.

(4) This verification server has not configured personnel respective domain personnel group.

Question: Cannot enroll and verify the fingerprint

Answer: (1) check whether has installed the uru4000 driver or not, reinstalls this driver

(2) Register Biokey.ocx again, copy the biokey.ocx in the files folder into system32. In Start/Run to register Regsvr32 biokey.ocx. if Prompts succeeded appear , OK!

Question: Why have I enrolled two fingers, actually only one finger is able to passé verification?

Answer: (1) the system default only add the first finger which the user registers in the first time, if needs to choose the finger upload, " the server personnel configuration management " to choose the personnel group of respective domain in this verification server, enters " group personnel " interface, in right hand side table, click the mouse right key to choose "changes the finger", may change added finger: Normally uses finger; Spare finger; The normal use + spare finger (namely increase complete finger).

(2) Inspect whether other finger has already registered successfully,

reregistered the finger.

(3) replace finger with the good quality fingerprint to enroll,

Question: Start verification server prompt:Open database error, please setup database Ado lin

Answer: Indicate that formerly set the database link occur error, please reappointed database.