ZK Technology EU

The Advanced Biometric Solutions

ZKSoftware

Facial & Fingerprint Recognition Product Series User Manual

Version: 2.0

Date: June 2011

About This Manual

This document introduces the user interface and menu operations of the Facial & Fingerprint Recognition (FFR) terminal series. For the installation of the FFR terminal, see *Facial & Fingerprint Recognition Product Series Installation Manual*

Content

1 Instruction for Use 1
1.1 The Distance，Facial Expression and Stand Pose 1
1.2 Enrollment Pose 2
1.3 Finger Placement 3
1.4 Use of Touch Screen 4
1.5 Touch Operations 5
1.6 Appearance of the FFR Terminal 6
1.7 Main Interface 7
1.8 Verification Modes 9
1.8.1 Fingerprint Verification 9
1.8.2 Facial Verification 11
1.8.3 Password Verification 13
1.8.4 ID Card Verification ★ 14
2. Main Menu 16
3. User Management 19
3.1. Adding a User 20
3.1.1 Entering a User ID 21
3.1.2 Entering a Name 23
3.1.3 Enrolling a Fingerprint 25
3.1.4 Enrolling a Password 26
3.1.5 Enrolling a Face 28
3.1.6 Entering a Group No. 30
3.1.7 Enrolling an ID Card ★ 32
3.1.8 Enrolling an HID Card ★ 33
3.1.9 Enrolling an Mifare Card ★ 33
3.1.10 Modify User Rights 34
3.1.11 Enroll Photos 35
3.2 Edit a User 36

3.3 Delete a User....37
3.4 Query a User....38
3.4.1 Query by User ID....38
3.4.2 Query by Name....39
4. Communication-related Settings....40
4.1 Network Settings....40
4.2 Serial Port Settings....41
4.3 WIFI option ★....42
4.4 Modem option ★....43
4.4.1 GPRS option....43
4.4.2 GPRS option....45
4.5 Wiegand Input ★....46
4.6 Wiegand Output....46
4.6.1 Wiegand 26-bits Output Description....47
4.6.2 Wiegand 34-bits Output Description....49
4.6.3 Customized Format....50
5. System Configuration....55
5.1 Basic Parameters....55
5.2 Interface Parameters....56
5.3 Fingerprint Parameters....57
5.4 Face Parameters....58
5.5 Log Settings....60
5.6 Update....61
6. Data Management....62
6.1 Query a Record....63
6.2 Work Code....64
6.3 SMS ★....66
6.3.1 Set Message....66
6.3.2 Employee Check Message....68

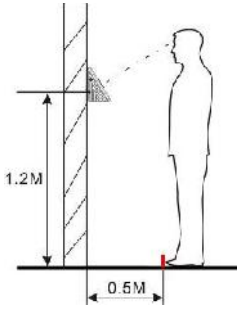
7. USB Disk Management 69
8. Keyboard Definitions 71
9 Auto Test 73
10 Screen Calibration 75
11 Bell Setting 76
12 Access Control Setting ★ 78
13 Date/Time Setting 80
13.1 Set Date/Time 80
13.2 Set Daylight Saving Time (DST) 81
14 System Information 83
14.1 Records 83
14.2 Terminal 84
Appendix 85
Appendix 1 Text Input Instructions 85
Appendix 2 Rules for Uploading Promotional Pictures 87
Appendix 3 Introduction to Wiegand 88
Appendix 4 Photo ID Function 89
Appendix 5 Attendance Status Selection Function ★ 91
Appendix 6 Anti-pass back ★ 92
Appendix 7 Multi- verification methods ★ 95
Appendix 8 GPRS ★ 100
Appendix 9 Webserver ★ 100
Appendix 10 Soap ★ ..... **¡Error! Marcador no definido.**
Appendix 11 Statement on Human Rights and Privacy 104
Appendix 12Environment-Friendly Use Description 106

1 Instruction for Use

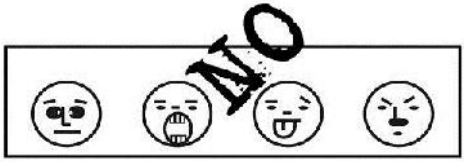
1.1 The Distance，Facial Expression and Stand Pose

1)The recommended distance:

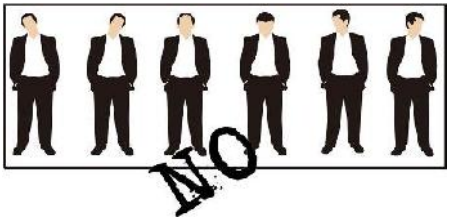
The recommended distance between person and device is 0.5m (applied to height range 1.5~1.85m). According to the obtained face image from device to adjust, when the face image is comparatively bright, please move backwards appropriately; when the face image is comparatively dark, please move forwards appropriately.



2)The recommended facial expression and several poor-effect facial expressions:



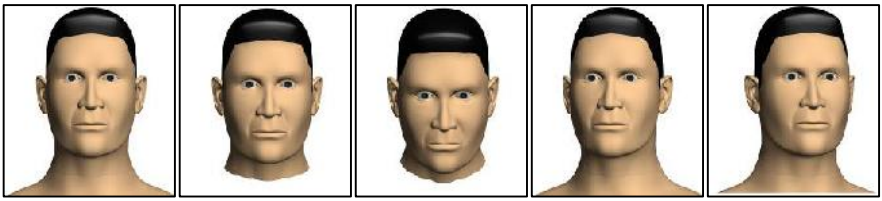
3)The recommded stand pose and several poor-effect stand poses:



Note: During the enrollment and verification, please remain the normal facial expression and stand pose.

1.2 Enrollment Pose

During the enrollment, display the face in the centre of screen as possible. According to the device's voice prompts, do some small-scope head actions such as turn left, turn right, rise, bow and so on to ensure that the different parts of face are inputted into system to improve the verification accuration. The enrollment poses are as follows:

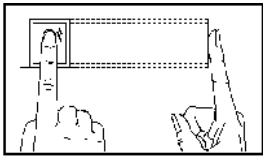


Look ahead (rise)	Focus on the screen	Focus on the camera (bow)	Turn left slightly	Turn right slightly

1.3 Finger Placement

Recommended fingers: The index finger, middle finger or the ring finger; the thumb and little finger are not recommended (because they are usually clumsy on the fingerprint collection screen).

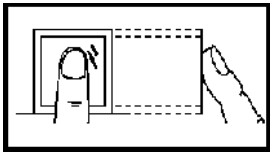
1) Proper finger placement:



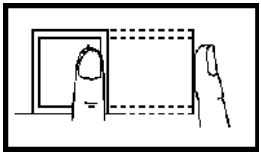
The finger is flat to the surface and centered in fingered guide.

2) Improper finger placement:

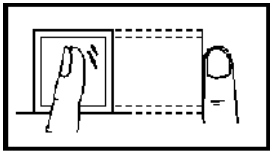
Not flat to the surface



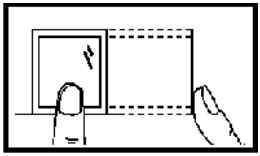
Off-center



Slanting



Off-center



Please enroll and verify your fingerprint by using the proper finger placement mode. We shall not be held accountable for any consequences arising out of the degradation in verification performance due to improper user operations. We shall reserve the right of final interpretation and revision of this document.

1.4 Use of Touch Screen

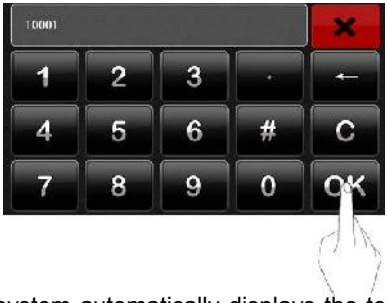
Touch the screen with one of your fingertips or the top of the forward edge of a fingernail, as shown in the following figure. A broad point of contact may lead to inaccurate pointing.

When the touch screen is less sensitive to the touch, you can perform screen calibration through menu operations. Press [Menu] → [Calibration] on the screen and a cross icon will be displayed. After you touch the center of the cross at five locations on the screen correctly, the system automatically returns to the main menu. Press [Return] to return to the initial interface. For details, see *10 Screen Calibration* in this manual.

Smear or dust on the touch screen may affect the performance of the touch screen. Therefore, try to keep the screen clean and dust-free.

1.5 Touch Operations

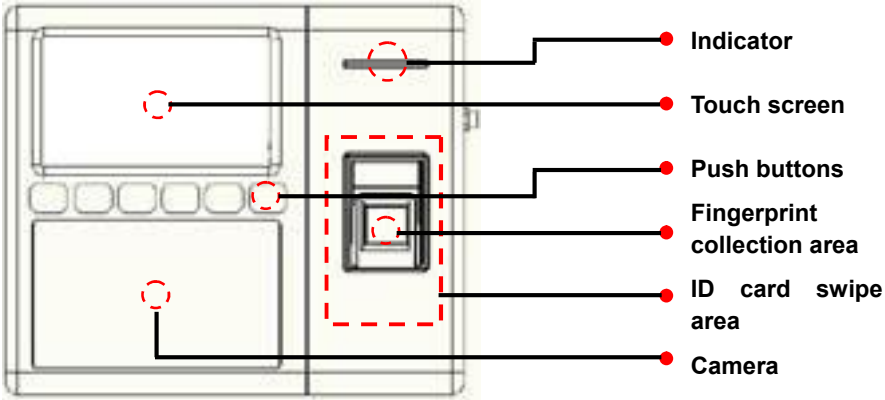
1) Enter numbers. Press the [User ID] key. The system automatically displays the number input interface. After entering the user ID, press [OK] to save and return to the previous interface.



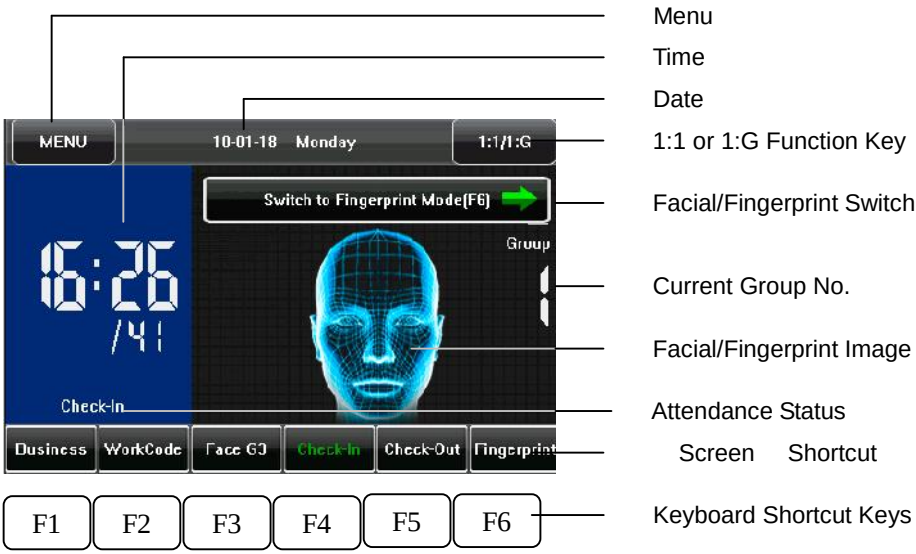
2) Enter Text. Press the [Name] key. The system automatically displays the text input interface. After entering the user name, press [X] to save and return to the previous interface.

3) Modify parameters. Press the default value of a parameter and the system automatically switches to another value of this parameter.

1.6 Appearance of the FFR Terminal



1.7 Main Interface



□**Menu**: You can enter the main menu by touching this key.

□**Time**: Current time is displayed. Both the 12-hour and 24-hour time systems are supported.

□**Date**: Current date is displayed.

□**1:1 or 1:G Function Key:** You can enter the digital input interface of 1:1 or 1:G verification mode. You can set the "1:1/1:G" shortcut key through □ Screen Shortcut Keys. This key is automatically hidden if the [Toolbar Style] is set to "Permanent Display".

□**Facial/Fingerprint Switch Key**: By pressing this key, you can switch between the facial and fingerprint recognition modes. You can set the "**Facial/Fingerprint Switch Key**" shortcut key through ⑨ Screen Shortcut Keys. This key is automatically hidden if the [Toolbar Style] is set to "Permanent Display".

□**Current Group No.**: When the terminal is currently in the facial recognition mode, users in current group can perform facial comparison directly, while users of another group need to enter the group No. before performing the facial comparison.

□**Facial/Fingerprint Image**: If a facial image is displayed, the terminal is currently in the facial recognition mode; if a fingerprint image is displayed, the terminal is currently in the fingerprint recognition mode. You can change current recognition mode of the terminal through □ **Facial/Fingerprint Switch Key**, the Facial/Fingerprint Key in □ Screen Shortcut Keys or related key in □ Keyboard Shortcut Keys.

□**Attendance Status**: Current attendance status is displayed. This key is hidden when □ Screen Shortcut Keys are displayed.

□**Screen Shortcut Keys**: Press related shortcut keys to display the attendance status or enter the functional interface quickly. Users can customize the function of each shortcut key. For details, see 8 Keyboard.

□**Keyboard Shortcut Keys**: The Keyboard Shortcut Keys have a one-to-one relationship with □ Screen Shortcut Keys. Press related shortcut keys to display the attendance status or enter the functional interface quickly.

1.8 Verification Modes

1.8.1 Fingerprint Verification

(1) 1:N fingerprint verification

In the fingerprint verification mode, the terminal compares current fingerprint collected by the fingerprint collector with all fingerprint data on the terminal.

1. To enter the fingerprint verification mode (Figure 1 on the right), you can:

A) Press [Facial/Fingerprint Switch Key] on the screen, or

B) Press [Facial/Fingerprint] shortcut key on the screen, or

C) Press the keyboard shortcut key [F6].

2. Press your finger on the fingerprint collector by adopting the proper finger placement. For details, see 1.1 Finger Placement.

3. If the verification is successful, an interface as shown in Figure 2 on the right will be displayed.

4. If the verification is not successful, an interface as shown in Figure 3 on the right will be displayed.

(2) 1:1 fingerprint verification

In the 1:1 fingerprint verification mode, the terminal compares current fingerprint collected through the fingerprint collector with that in relation to the user ID entered through keyboard. Adopt this mode only when it is difficult to recognize the fingerprint.

1. To enter the 1:1 recognition mode, you can:

A) Press [1:1/1:G] on the screen, as shown in Figure 1 on the right, or:

B) Press [1:1/1:G] shortcut key on the screen, or

C) Press related shortcut key on the keyboard.

Note: You can enter the 1:1 recognition mode through B) and C) only after setting a shortcut key for "1:1/1:G". For details, see 8 Keyboard.

2. Enter user ID and then press the "Fingerprint" icon (Figure 2 on the right) to enter 1:1 fingerprint recognition mode. If the prompt "Unregistered user!" is displayed, the user ID is nonexistent or the user ID bearer has not enrolled his/her fingerprint.

3. Press your finger on the fingerprint collector by adopting the proper finger placement. For details, see 1.1 Finger Placement.

4. If the verification is successful, an interface as shown in Figure 3 on the right will be displayed. 4. If the verification is not successful, an interface as shown in Figure 4 on the right will be displayed.

1.8.2 Facial Verification

(1) 1:G facial verification

Current group No. is displayed on the facial recognition interface. Users in current group can perform facial comparison directly. Users of another group can perform facial comparison only after entering the group No. or selecting it using the shortcut key. And the system will set the group entered or selected by users to be the current group instantly.

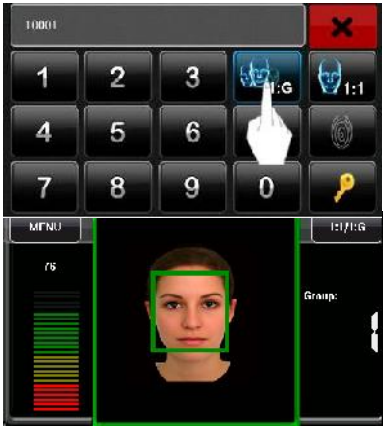
1. To enter the 1:G recognition mode, you can:

A) Press [1:1/1:G] on the screen, as shown in Figure 1 on the right, or:

B) Press [1:1/1:G] shortcut key on the screen, or

C) Press related shortcut key on the keyboard.

Note: You can enter the 1:1 recognition mode through B) and C) only after setting a shortcut key for "1:1/1:G". For details, see 8 Keyboard.



2. Enter user Group No. and then press the "1:G" icon (Figure 2 on the right) to enter 1:G fingerprint recognition mode.

3. Compare the facial in a proper way. For details, see *1.1 Standing Position and Posture, and Facial Expression.* Current Group No. is displayed on the comparison interface, as shown in Figure 3 on the right.

Note: Check whether you are in current group; if not, return to Step 1.

4. If the verification is successful, an interface as shown in Figure 4 on the right will be displayed.

(2) 1:1 facial verification

In the 1:1 facial verification mode, the terminal compares current facial collected through the facial collector with that in relation to the user ID entered through keyboard. Adopt this mode only when it is difficult to recognize the facial.

1. To enter the 1:1 recognition mode, you can:

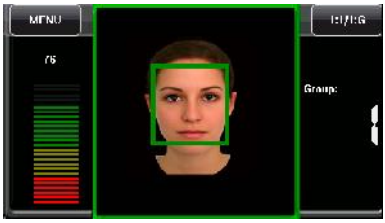
A) Press [1:1/1:G] on the screen, as shown in Figure 1 on the right, or:

B) Press [1:1/1:G] shortcut key on the screen, or

C) Press related shortcut key on the keyboard.

Note: You can enter the 1:1 recognition mode through B) and C) only after setting a shortcut key for "1:1/1:G". For details, see 8 Keyboard.

2. Enter user ID and then press the "1:1 Facial" icon (Figure 2 on the right) to enter 1:1 facial recognition mode. If the prompt "Unregistered user!" is displayed, the user ID is nonexistent or the user ID bearer has not enrolled his/her face in the system.



3. Compare the facial in a proper way. For details, see *1.1 Standing Position and Posture, and Facial Expression.* Current Group No. is displayed on the comparison interface, as shown in Figure 3 on the right.

4. If the verification is successful, an interface as shown in Figure 4 on the right will be displayed. The system will return to the main interface if the verification is not passed within 20 seconds.

1.8.3 Password Verification

In the password verification mode, the terminal compares the password entered with that in relation to the user ID.

1. To enter the password verification mode, you can:

   A) Press [1:1/1:G] on the screen, as shown in Figure 1 on the right, or:

   B) Press [1:1/1:G] shortcut key on the screen, or

   C) Press related shortcut key on the keyboard.

   Note: You can enter the 1:1 recognition mode through B) and C) only after setting a shortcut key for "1:1/1:G". For details, see 8 Keyboard.

2. Enter the user ID and then press the "Key" icon (Figure 2 on the right) to enter password verification mode. If the prompt "Unregistered user!" is displayed, the user ID is nonexistent or the user ID bearer has not enrolled his/her password in the system.

3. Enter the password and press the "OK" icon to start the password comparison, as shown in Figure 3 on the right.

4. If the verification is successful, an interface as shown in Figure 4 on the right will be displayed.

1.8.4 ID Card Verification ★

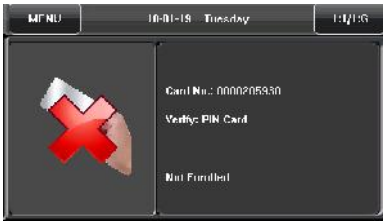
Only the products with a built-in ID card module support the ID card verification. The products with a built-in ID card module support the following two verification modes:
ID Card Only: Users only need to swipe their ID cards for verification.
ID + Facial Verification: After passing the ID card verification, you also need to perform facial verification.
For the settings of these two verification modes, see *5.5 Attendance Parameters*.

1) ID Card Only

1. If you have your ID card number enrolled in the system, you can pass the verification by swiping your ID card at the swiping area in a proper way.

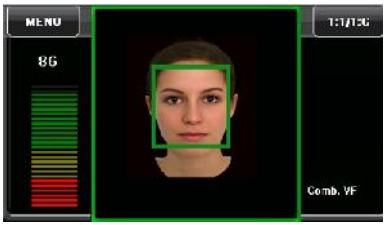
2. If the verification is successful, an interface as shown in Figure 1 on the right will be displayed.

3. If the verification is not successful, an interface as shown in Figure 2 on the right will be displayed.



2) ID + Facial Verification

1. Swipe your ID card properly at the swiping area to enter the 1:1 facial verification mode, as shown in Figure 1 on the right:



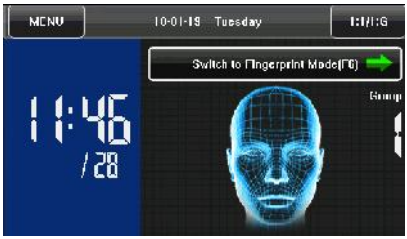
2. Compare the facial in a proper way. For details, see *1.1 Standing Position and Posture, and Facial Expression.*

3. If the verification is successful, an interface as shown in Figure 3 on the right will be displayed. The system will return to the main interface if the verification is not passed within 20 seconds.

2. Main Menu

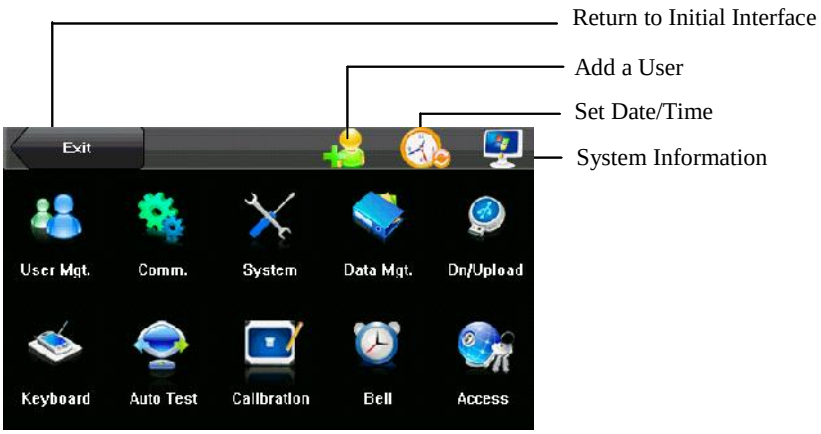
There are two types of rights respectively granted to two types of users: the ordinary users and administrators. Ordinary users are only granted the rights of facial, fingerprint, password or card verification, while administrators are granted the access to the main menu for various operations apart from having all the privileges granted to ordinary users.

Press [Menu] on the initial interface to access the main menu, as shown in the following figure:



Any user can access the main menu by pressing the [Menu] key if the system is free from administrators. After administrators are configured on the terminal, the terminal needs to verify the administrators' identity before granting them access to the main menu. To ensure terminal security, it is recommended to set an administrator when using the terminal initially. For detailed operations, see 3.1.8.

The main menu includes ten submenus and three shortcut keys, as shown in the following figure:



User Mgt.: Through this submenu, you can browse the user information stored on the terminal, including the user ID, name, fingerprint, facial, card, password, rights and group No.; add, modify or delete the user information.

Comm.: Through this submenu, you can set related parameters for communication between the FFR terminal and PC, including the IP address, gateway, subnet mask, baud rate, equipment No. and communication password.

System: Through this submenu, you can set system-related parameters, including the basic parameters, interface parameters, fingerprint, facial and attendance parameters, to enable the FFR terminal to meet user requirements to the greatest extent in terms of functions and display.

Data Mgt.: Through this submenu, you can perform management of data stored on the FFR terminal, for example, deleting the attendance record, all data and promotional pictures, purging management rights and resetting the FFR terminal to factory defaults.

Dn/Upload: Through this submenu, you can import user information and attendance

data stored in a USB disk to related software or other fingerprint recognition equipment.

Keyboard: Through this submenu, you can customize six shortcut keys. Related status will be displayed by pressing related status key.

Auto Test: This submenu enables the system to automatically test whether functions of various modules are normal, including the screen, collector, voice, facial, keyboard and clock tests.

Calibration: When the touch screen is less sensitive to the touch, you can calibrate the screen on the calibration interface through this submenu.

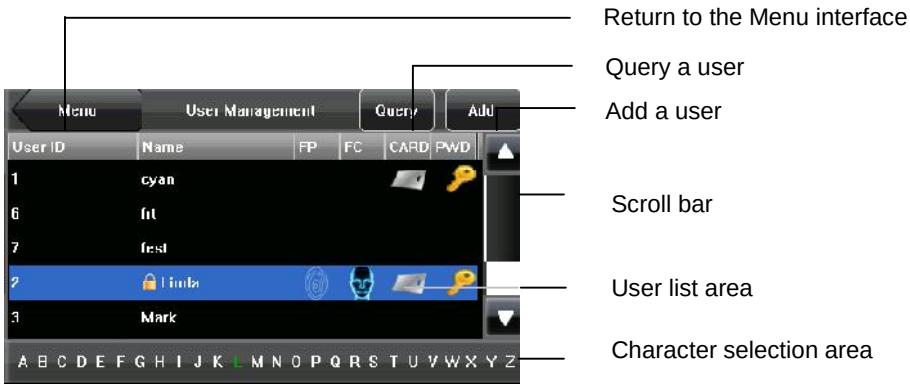
Bell: Through this submenu, you can set the alarm time and duration.

Access: Through this submenu, you can set the parameters of the electronic locks and related access control devices.

3. User Management

Browse the user information, including the user ID, name, fingerprint, face, ID card, password, rights and the group that the user belongs to. Add, edit or delete the basic information of users.

Press [User Management] on the main menu interface to display the user management interface.



The user is an administrator.

The user has enrolled his/her fingerprint.

The user has enrolled his/her facial image.

The user has enrolled his/her ID card.

The user has enrolled his/her password.

Note:

1) In **User List Area**, users are listed in alphabetical order by last name. If you select a user in User List Area, you can access the editing interface of this user to edit or delete related user information.
2) In Character Selection Bar, users are listed in alphabetical order by last name by default and you can locate the desired user quickly. You can press [Query]

to locate and query a user through the user ID. For details, see Section 3.4 Querying a User.

3.1. Adding a User

Press [Add] on the [User Mgt.] interface to display the [Add User] interface as shown below.

User ID: Enter a user ID. 1- to 9-digit user IDs are supported by default.

Name: Enter a user name. 12-character user names are supported by default.

Fingerprint: Enroll a user's fingerprint and the FFR terminal displays the number of enrolled fingerprints. A user can enroll 10 fingerprints at maximum.

Face: Enroll a user's face.

Password: Enroll a user's password. 1- to 8-digit passwords are supported by default.

Role: Set the rights of a user. A user is set to **ordinary user** by default and can also be set to **administrator**. Ordinary users are only granted the rights of facial, fingerprint or password verification, while administrators are granted the access to the main menu for various operations apart from having all the privileges granted to ordinary users.

Group No.: Set the group that the user belongs to. Valid group No.: 1–24.

Photo: Enroll a user's photo. During user verification, the user's photo is displayed on screen.

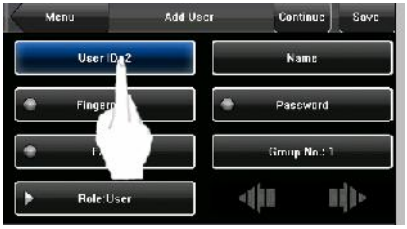
Reg.Duress FP: Enroll a user's fingerprint, and setting it as Duress FP.

The ID card is an optional function. If you need this function, please consult our commercial representatives or fore-sale technical support personnel.

3.1.1 Entering a User ID

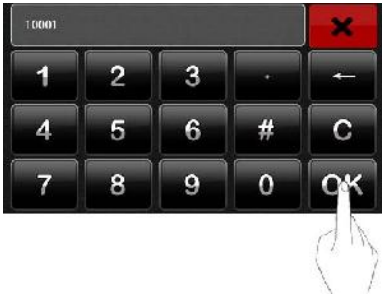
The FFR terminal automatically allocates an ID starting from 1 for every user in sequence. If you use the ID allocated by the FFR terminal, you may skip this section.

1. Press [User ID] on the [Add User] interface to display the user ID management interface, as shown below:



Tip: The user ID can be modified during initial enrollment, but once enrolled, it cannot be modified.

2. On the displayed keyboard interface, enter a user ID and press <OK> as shown below. If a prompt message “The user ID already exists!” is displayed, enter another ID.



Tip: The FFR terminal supports 1- to 9-digit user IDs by default. If you need to extend the length of current user ID numbers, please consult our commercial representatives or fore-sale technical support personnel.

3. After the user ID is entered, an interface is displayed as show below on the right. Press [Save] to save current information and return to the previous interface. Press [User Mgt.] to return to the previous interface without saving current information.

3.1.2 Entering a Name

Enter a user name through the keyboard.

1. Press [Name] on the [Add User] interface to display the name input interface, as shown below.

2. On the displayed keyboard interface, enter a user name and press [X] as shown below. For details of operations on keyboard interface, see “Keyboard Instructions”.

Tip: The FFR terminal supports the 1- to 12-character names by default.

3. After the user name is entered, the interface is displayed as shown below. Press [Save] to save current information and return to the previous interface. Press [User Mgt.] to return to the previous interface without saving current information.

3.1.3 Enrolling a Fingerprint

1. Press [Fingerprint] on the [Add User] interface to display the [Enroll Fingerprint] interface, as shown below.

2. On the displayed [Enroll Fingerprint] interface (as shown in the Figure 1 on the right), place your finger on the fingerprint collector properly according to the system prompt. For details, see “Finger Placement”.

3. Place the same finger on the fingerprint collector for three consecutive times correctly. If the enrollment succeeds, the system will display a prompt message “Enrolled Successfully” and automatically return to the [Add User] interface (as shown in Figure 2 on the right). If the enrollment fails, the system will display a prompt message and return to the [Enroll Fingerprint] interface. In this case, you need to repeat the operations of step 2.

4. You can back up the enrolled fingerprint of a user by pressing [Fingerprint]. A user can enroll 10 fingerprints at maximum.

5. Press [Save] to save current information and return to the previous interface. Press [User Mgt.] to return to the previous interface without saving current information.

3.1.4 Enrolling a Password

1. Press [Password] on the [Add User] interface to display the password management interface, as shown below.

2. On the displayed keyboard interface, enter a password and press <OK> as shown below. Re-enter the password according to the system prompt and then press <OK>.

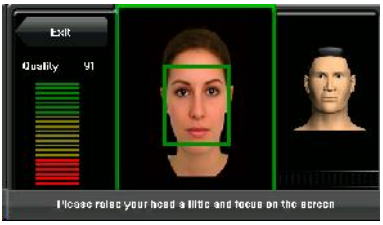
Tip: The FFR terminal supports the 1- to 8-digit passwords by default.

3. After the password is entered, an interface is displayed as shown below. Press [Save] to save current information and return to the previous interface. Press [User Mgt.] to return to the previous interface without saving current information.

3.1.5 Enrolling a Face

1. Press [Face] on the [Add User] interface to display the face enrollment interface, as shown below.

2. On the displayed face enrollment interface (as shown below), turn your head to the left and right slightly, raise and lower your head according to the voice prompts, so as to enroll different parts of your face into the system to assure accurate verification. See *1.1 The distance, Facial Expression and Stand Pose.*



3. If your facial image is enrolled successfully, the system will display a prompt message and automatically return to the [Add User] interface (as shown below).

4. Press [Save] to save current information and return to the previous interface. Press [User Mgt.] to return to the previous interface without saving current information.

3.1.6 Entering a Group No.

The FFR terminal enables the facial comparison function by default. During face enrollment, the FFR automatically allocates a group No. starting from 1 for every user in sequence. When the number of users in Group No.1 reaches the upper limit, the rest users fall under Group No.2 automatically. Up to 100 facial images can be enrolled in Group No.1 and only 50 facial images can be enrolled in other groups. If you use the group No. allocated by the FFR terminal, you may skip this section.

1. Press [Group No.] on the [Add User] interface to display the group No. management interface, as shown below.

2. On the displayed keyboard interface, enter your group No. and press <OK> as shown below.

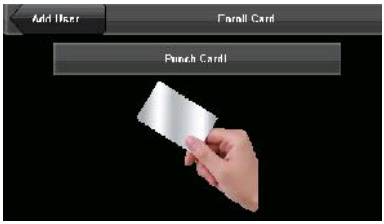
Tip: A valid group No. contains 1–24 digits.

3. After the group No. is entered, an interface is displayed as shown below. Press [Save] to save current information and return to the previous interface. Press [User Mgt.] to return to the previous interface without saving current information.
   Tip: Please remember your own group No.

3.1.7 Enrolling an ID Card ★

1. Press [Card] on the [Add User] interface to display the [Enroll Card] interface, as shown in Figure 1 on the right.

2. The [Punch Card!] interface pops out as shown in Figure 2 on the right. Swipe your ID card properly in the swiping area. For details, see “1.6 Appearance of the FFR Terminal”.



3. If the card passes the verification, the FFR terminal displays a prompt message “Read Successfully! Card No.: **********”, as shown in Figure 3 on the right, and returns to the [Add User] interface. Press [Card] to display the enrolled card number as shown in Figure 4 on the right.

4. Press [Save] to save current information and return to the previous interface. Press [User Mgt.] to return to the previous interface without saving current information.

3.1.8 Enrolling an HID Card ★

This operation procedure is same as ID Card operation, use HID card only by Using 125MHZ,13.56 MHz contactless smart card technology only, these fingerprint products provide users with new options for supporting multi-authentication of identity. Combine a contactless card presentation with a fingerprint biometric. Or, use a personal identification number (PIN) number along with a contactless card presentation. (See multi-authentication)

HID standard card is encrypted by using specify format encode card ID and the equipment code.

Note：HID card apply to fingerprint -machine, this is an option function on the fingerprint machine, if you want to customize fingerprint machine with HID card function, please contacts our market supporter and salesman.

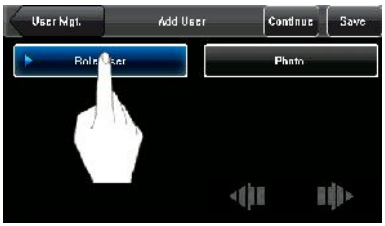
3.1.9 Enrolling an Mifare Card ★

The iface series only favors Mifare card's being an ID card use. Use step and ID card to register an operation to accord.

Note：Mifare card is an option function on the fingerprint machine, if you want to customize the fingerprint machine with Mifare card function, please contacts our market supporter and salesman's.

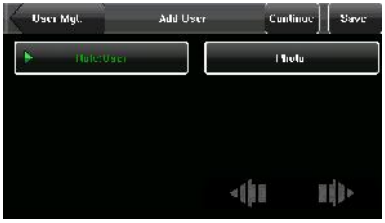
3.1.10 Modify User Rights

1. On the [Add User] interface, press [Role: User] to change the user into an administrator, as shown in Figure 1 on the right.



Note: There are two types of rights respectively granted to two types of users: the ordinary users and administrators. Ordinary users are only granted the rights of facial, fingerprint, or password verification, while administrators are granted the access to the main menu for various operations apart from having all the privileges granted to ordinary users.

2. After the modification is done, the interface is as shown in Figure 2 on the right. Press [Save] to save current information and return to previous interface; press [User Mgt.] to directly return to previous interface without saving current information.



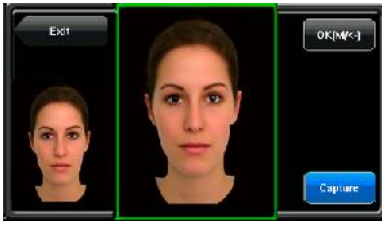
3.1.11 Enroll Photos

If you have enrolled your photo in the system, the system will display your enrolled photo in addition to your ID and name after you pass the verification.

1. Press [Photo] on the [Add User] interface to display the photo enrollment interface, as shown in Figure 1 on the right.

2. On the photo enrollment interface, stand naturally in front of the screen. For details, see *1.1 Standing Position and Posture, and Facial Expression*. Press [Capture] to display the photo taken at the lower left corner, as shown in Figure 3 on the right.

3. After taking the photo, press [Exit] to return to previous interface.



4. After the photo is taken, the interface is as shown in Figure 4 on the right. Press [Save] to save current information and return to previous interface; press [User Mgt.] to directly return to previous interface without saving current information.

3.2 Edit a User

Select a user from the User List to enter [User Info] interface.

The User ID cannot be modified, and the other operations are similar to those performed to add a user. You can re-enroll your fingerprint and facial image, change your password and modify the management rights and group No.

3.3 Delete a User

On the [User Info] interface, you can delete all or partial user information.

1. Press [Delete] to delete a user, as shown below.

2. On the interface displayed (as shown below), click [YES] to delete current user and [NO] to return to previous interface.

3. On the [User Info] interface, press [Name], [Fingerprint], [Face] or [Password] to delete related user information.

3.4 Query a User

To facilitate administrators to locate a user quickly from a large number of enrolled users, the FFR terminal enables user query by his/her “User ID” and “Name”. (Location Search)

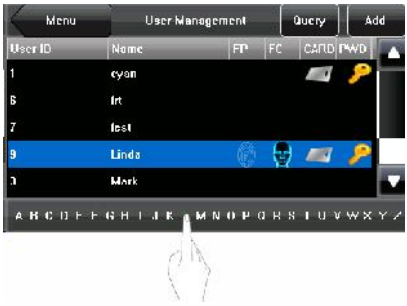
3.4.1 Query by User ID

1. Press [Query] on the [User Management] interface to display the User ID query interface, as shown in Figure 1 on the right.

2. Enter the user ID on the displayed interface, and click [OK] (as shown in Figure 2 on the right) to locate the cursor to the desired user (as shown in Figure 3 on the right).

3.4.2 Query by Name

On the [User Management] interface, enter the user name through the “Character Selection Bar” to locate the cursor to the desired user, as shown in the following figure:



By selecting a character from the “Character Selection Bar”, you can quickly locate the users whose names start with this character. Users are listed in alphabetical order by last name by default.

4. Communication-related Settings

You can set related parameters for the communication between the FFR terminal and PC, including the IP address, gateway, subnet mask, baud rate, equipment No. and communication password.

4.1 Network Settings

When the FFR terminal communicates with the PC over Ethernet, you need to check the following settings:

IP Address: The IP address is 192.168.1.201 by default and can be changed as required; the IP address of the FFR terminal and that of the PC cannot be duplicated.

Subnet Mask: The subnet mask is 255.255.255.0 by default and can be changed as required.

Gateway: The gateway is 0.0.0.0 by default. If the FFR terminal and the PC are not located in the same network segment, you need to set the gateway.

4.2 Serial Port Settings

When the FFR terminal communicates with the PC over serial ports (RS232/RS485), you need to check the following settings:

RS232: This parameter is used to enable or disable the RS232 communication. If the RS232 communication cables are used, set this parameter to “ON”.

RS485: This parameter is used to enable or disable the RS485 communication. If the RS485 communication cables are used, set this parameter to “ON”.

Baud Rate: This parameter is used to set the baud rate for the communication between the FFR terminal and the PC. It includes five options: 9600, 19200, 38400, 57600, and 115200. The high baud rate is recommended for the RS232 communication to achieve high communication speed, while the low baud rate is recommended for the RS485 communication to achieve stable low-speed communication.

Device ID: This parameter is used to set the ID of device from 1 to 254. If the RS232/RS485 communication is adopted, you need to enter the device ID on the software communication interface.

Comm Key: To enhance the security of attendance data, you can set a password for the connection between the FFR terminal and PC. Once the password is set, you can connect the PC with the FFR terminal to access the attendance data only after entering the correct password. The default password is 0 (that is, no password). Once a password is set, you need to enter this password before connecting the PC software with the FFR terminal; otherwise, the connection is unsuccessful. 1- to 6-digit passwords are supported.

Considering the massive data including the fingerprint and facial templates stored in the FFR terminal, it is recommended to transfer the data between the FFR terminal and PC over network to enhance the transfer speed.

4.3 WIFI option ★

Before the device is used for wireless network, other physical groupware of 802.11 network, such as joint, distributing system, wireless medium must be in existence. ESSID to connect to the network must be known (network ID).

Network ID: Network ID to be connected to wireless network. (There is difference between small letter and capital letter.)

Network model: there are two models: infrastructure model (for star structure) and ad－hoc model (for peer-to-peer-network).

Authentication mode: Infrastructure mode includes five authentication modes: OPEN, SHARED, WEPAUTO, WPAPSK and WPA2PS002E.

ad－hoc model includes four authentication modes: OPEN, SHARED, WEPAUTO and WPANONE.

Encrypt type:when the selected encrypt type is NONE,the password in WEP (Wired equivalent privacy) and WPA (WiFi protested access) cannot be edited, namely, it is not necessary to input password.

Device IP address :In 802.11 wireless network, there is DHCP. Or enter IP interface to input correct IP address, subnet mask and so on.

Operation

Press ▲/▼ to switch cursor to the input box or button. Use T9 input to input network ID, which must be input, or the cursor cannot be moved to other input box. Then press ◀/▶ to select the item to be set or press OK to do corresponding operation.

1）set password :

According to the selected authentication mode and different encrypt types, the interface where password is set is also different. There are two interfaces: WEP and WPA.

WEP password

2）specify IP:

Specify the device IP in wireless network. It has nothing to do with network option in communication option.

After IP is specified, press Save button to save the setting, and then return to wireless option interface.

After setting, press Save button to return to the last interface.

4.4 Modem option ★

4.4.1 GPRS option

When the equipment is in the Dial-Up Network, make sure the device is in the coverage of GPRS or CDMA signal, and it is must known of the used modem type,

APN name and access number and so on.

Frequency: Select the appropriate frequency according to the business operators.

APN Name: Access Point Name, used to identify GPRS / CDMA types of business.

User name and password: Verify whether the user has permission to use this network.

Access Number: The access number of GPRS / CDMA business.

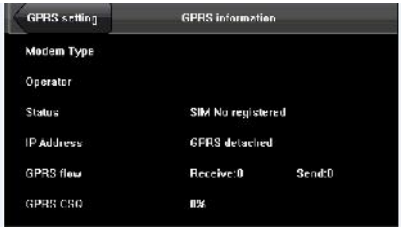
Redial interval:The interval of automatic redial after the network is disconnected.

Redial times: The times of attempt to redial the number if the network is disconnected.

Whether Use: According to needs to choose is or otherwise, the choice is when single-clicks the 

button to be possible to enter the GPRS establishment page, the following chart shows:

Single-clicks the “GPRS Information” item can see the detail, show below:



Notice:Dial-Up setting function is only available on some models.

Operation :

Press on the desired item，then start the T9 method to input APN name, user name, Link Psw and Access Num. directly enter the value in the input box. When finished all this settings, you just press the Save button to save them and return to the previous screen.

4.4.2 GPRS Use

1) Dial-Up

After dialup settings are completed, reboot the device, the device will automatically begin dialing, when dial-up is successful, the screen will be displayed the GPRS icon below:

2) Data download

When Dial-up is successful, open the data download program in the server, when the user is verified through the terminal, the device will automatically transmit data to the server, the interface will prompt "in Communication ... ..." when download;

4.5 Wiegand Input ★

Wiegand Input Format: User defined Wiegand input format. Include three Input Format: Standard Wiegand 34-bits, Standard Wiegand 34-bits, User Define Format .

Pulse width: Pulse width is 100 microseconds by default, which can be adjusted from 20 to 800.

Pulse interval: It is 900 microseconds by default, which can adjusted between 200 and 20000.

Input content: Content contained in Wiegand input signal, including User ID or card number.

Operation

4.6 Wiegand Output

Wiegand Format: The system has two built-in formats **Wiegand 26-bits** and **Wiegand 34-bits**, and also supports the format customization function to meet individualized requirements.

Failed ID: refers to the value output by the system upon verification failure. The

output format is subject to the setting of "**Wiegand Format**". The default value scope of **Failed ID** is 0–65535.

Site Code: The site code is used for customized Wiegand format. The site code is similar to the device ID, but the site code is customizable and can be duplicated among different devices. The default value scope of the site code is 0–255.

Pulse Width: refers to the width of the Wiegand pulse in microseconds. The default value scope of the pulse width is 1–1000.

Pulse Interval: refers to the interval of the Wiegand pulse in microseconds. The default value scope of the pulse width is 1–10000.

Output: refers to the contents output upon successful verification. You can select the "User ID" or "Card Number" as the output.

4.6.1 Wiegand 26-bits Output Description

The system has a built-in Wiegand 26-bits format. Press [**Wiegand Format**], and select "Standard Wiegand 26-bits".

The composition of the Wiegand 26-bits format contains 2 parity bits and 24 bits for output contents ("User ID" or "Card Number"). The binary code of 24-bits represent up to 16,777,216 (0–16,777,215) different values.

1	**2**	**25 26**
Even parity	User ID/Card Number	Odd parity bit

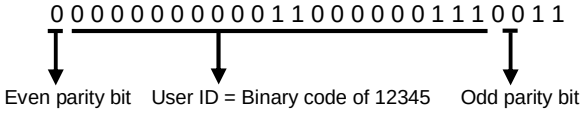
Definition of Fields:

Field	**Meaning**
Even parity bit	Judged from bit 2 to bit 13. The **even parity bit** is 1 if the character has an even number of 1 bits; otherwise, the

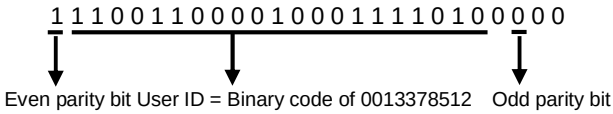
	even parity bit is 1.
User ID/Card Number (bit 2-bit 25)	User ID/Card Number (Card Code, 0–16777215) Bit 2 is the Most Significant Bit (MSB).
Odd parity bit	Judged from bit 14 to bit 25. The **odd parity bit** is 1 if the character has an even number of 1 bits; otherwise, the odd parity bit is 0.

For example, for a user with user ID of 12345, the enrolled card number is 0013378512 and the failed ID is set to 1.

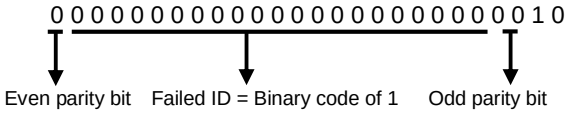
1) When the output is set to “User ID”, the Wiegand output is as follows upon successful verification:



2) When the output is set to “Card Number”, the Wiegand output is as follows upon successful verification:



3) The Wiegand output is as follows upon verification failure:



Note: If the output contents exceed the scope allowed for the Wiegand format, the last several bits will be adopted and first several bits are automatically discarded. For example, the user ID 888 888 888 is 110 100 111 110 110 101 111

000 111 000 in binary format. Wiegand26 only supports 24 bits, that is, it only outputs the last 24 bits, and first 6 bits "110 100" are automatically discarded.

4.6.2 Wiegand 34-bits Output Description

The system has a built-in Wiegand 34-bits format. Press [**Wiegand Format**], and select "Standard Wiegand 34-bits".

The composition of the Wiegand 34-bits format contains 2 parity bits and 32 bits for output contents ("User ID" or "Card Number"). The binary code of 32-bits represent up to 4,294,967,296 (0–4,294,967,295) different values.

1	**2**	**33 34**
Even	User ID/Card Number	Odd parity bit

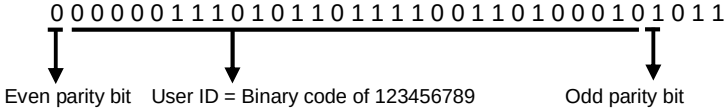
Table 2 Definition of Fields

Field	**Meaning**
Even parity bit	Judged from bit 2 to bit 17. The **even parity bit** is 1 if the character has an even number of 1 bits; otherwise, the even parity bit is 1.
User ID/Card Number (bit 2-bit 33)	User ID/Card Number (Card Code, 0–4,294,967,295) Bit 2 is the Most Significant Bit (MSB).
Odd parity bit	Judged from bit 18 to bit 33. The **odd parity bit** is 1 if the character has an even number of 1 bits; otherwise, the odd parity bit is 0.

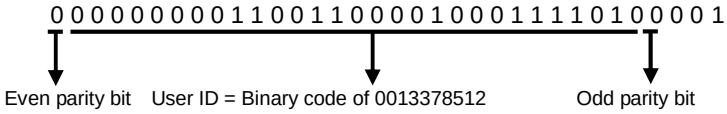
For example, for a user with user ID of 123456789, the enrolled card number is

0013378512 and the failed ID is set to 1.

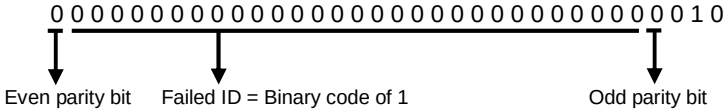
1) When the output is set to “User ID”, the Wiegand output is as follows upon successful verification:



2) When the output is set to “Card Number”, the Wiegand output is as follows upon successful verification:



3) The Wiegand output is as follows upon verification failure:



4.6.3 Customized Format

Apart from the two built-in formats **Wiegand 26-bits** and **Wiegand 34-bits**, the system also supports the format customization function to meet individualized requirements.

The customized format consists of two character strings: the **data bits** and **parity bits**. These two character strings need to be defined separately. **Data bits** define the number of binary bits output by Wiegand as well as the meaning of each bit. The data bits output by Wiegand can be a card number (C), site code (s), facility code (f), manufacturer code (m) and parity bits (p). **Parity bits** define the check mode of each bit in data bits and ensure the correctness of data bits during transfer through the parity check. The parity bits can be set to odd check (o), even check (e) and both odd check and even check (b). There exists a one-to-one correspondence

relationship between the data bits and parity bits.

For example, the Wiegand26 can be customized as follows:

Definition of data bits: pssssssssccccccccccccccccp

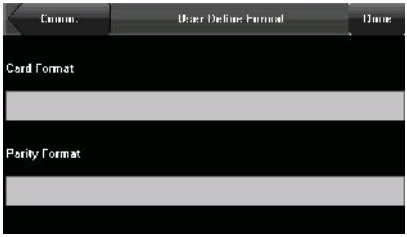
Definition of parity bits: eeeeeeeeeeeeeeoooooooooooooo

Note: **Wiegand26 consists of 26 bits. The first bit is the even parity bit of bits 2 to 13; the 26th bit is the odd parity bit of bits 14 to 25; the second to the ninth bits are the site code; the 10th to the 25th bits are the card number.**

For details about the Wiegand protocol, see Appendix 3 Introduction to Wiegand.

To customize Wiegand format, proceed as follows:

1) Select [Define Format] and the [Set] key is then enabled.
2) Press [Set] to display the [User Define Format] interface, as shown in the following figure:



3) Click the entry box below “Card Format” to display the following interface:

Characters used to define data bits and their meanings:

c: indicates the card number, that is, the output contents, it can be set to User ID/Card Number through menu operations.

f: indicates the facility code which is 0 by default. It is not configurable. To modify it, please contact the equipment supplier.

m: indicates the manufacturer code which is 0 by default. It is not configurable. To modify it, please contact the equipment supplier.

p: indicates the parity position.

s: indicates the site code which can be set from 0 to 255 by default.

4) Click the entry box below “Parity Format” to display the following interface:

Characters used to define parity bits and their meanings:

o: indicates the odd check, that is, there is an odd number of 1’s in the bit sequence (including one parity bit). For example, for 1000110(0), the parity bit is 0 and there are already three 1’s. After 0 is suffixed to 1000110, there is still an odd number of 1’s.

e: indicates the even check, that is, there is an even number of 1’s in the bit sequence (including one parity bit). For example, for 1000110(1), the parity bit is 1 and there are already three 1’s. After 1 is suffixed to 1000110, there is an even number of 1’s.

b: indicates both odd check and even check.

For example: Definitions of several universal Wiegand formats.

Wiegand34

Data bits:

pccccccccccccccccccccccccccccccp

Parity bits:

eeeeeeeeeeeeeeeeoooooooooooooooo

Note: **Wiegand34 consists of 34 bits. The first bit is the even parity bit of bits 2 to 17; the 34th bit is the odd parity bit of bits 18 to 33; the second to the ninth bits are the site code; the 10th to the 25th bits are the card number.**

Wiegand37a

Data bits: pmmmmsssssssssssscccccccccccccccccccp

Parity bits: oeobeobeobeobeobeobeobeobeobeobeobeoe

Note: Wiegand37a consists of 37 bits. The first bit is the odd parity bit of bits 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 18, 19, 21, 22, 24, 25, 27, 28, 30, 31, 33, 34 and 36; the 37th bit is the odd parity bit of bits 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29, 31, 32, 34 and 35; bits 4, 7, 10, 13, 16, 19, 22, 25, 28, 31 and 34 participate in both odd and even parity check. Bits 2 to 5 are manufacturer code; bits 6 to 17 are the site code; bits 18 to 36 are the card number.

Wiegand37

Data bits:

pmmmfffffffffssssssccccccccccccccccp

Parity bits:

eeeeeeeeeeeeeeeeeoooooooooooooooooo

Note: Wiegand37 consists of 37 bits. The first bit is the even parity bit of bits 2

to 18; the 34th bit is the odd parity bit of bits 19 to 36; the second to the fourth bits are the manufacturer code; the 5th to the 14th bits are facilitate code; the 15th to the 20th bits are the site code; the 21st to the 36th bits are the card number.

Wiegand50

Data bits: pssssssssssssssssccccccccccccccccccccccccccccccccp

Parity bits:

eeeeeeeeeeeeeeeeeeeeeeeeoooooooooooooooooooooooooo

Note: Wiegand50 consists of 50 bits. The first bit is the even parity bit of bits 2 to 25; the 50th bit is the odd parity bit of bits 26 to 49; the second to the 16th bits are the site code; the 17th to the 49th bits are the card number.

5. System Configuration

Through the [System] menu, you can set system-related parameters, including the basic parameters, interface parameters, fingerprint, facial and attendance parameters, to enable the terminal to meet user requirements to the greatest extent in terms of functions and display.

5.1 Basic Parameters

Date/Time: This parameter is used to set the date and time of the FFR terminal.

Date Format: This parameter is used to set the format of the date displayed on the initial interface of the FFR terminal.

Keyboard Beep: This parameter is used to set whether to generate beep sound in response to every keyboard touch. Select “ON” to enable the beep sound, and select “OFF” to mute.

Voice: This parameter is used to set whether to play voice prompts during the operation of the FFR terminal. Select “ON” to enable the voice prompt, and select

“OFF” to mute.

Volume (%): This parameter is used to adjust the volume of voice prompts.

Power Key: This parameter is used to set whether to lock the power key. Select “ON” to disable the power key. If you select “OFF” and press the power key, the FFR terminal will be shut down in three seconds.

5.2 Interface Parameters

Language: This parameter is used to display the current language used by the FFR terminal. For multilingual-capable FFR terminals, you can switch between different languages through this parameter.

Display Style: This parameter is used to set the time display mode of the initial interface. Select “ON” to adopt the 24-hour display mode. Select “OFF” to adopt the 12-hour display mode.

Toolbar Style: This parameter is used to display style of the shortcut keys on the initial interface. It can be set to “Auto Hide” and “Permanent Display”. By selecting “Auto Hide”, you can manually display or hide the toolbar. By selecting “Permanent Display”, you can permanently display the toolbar on the initial interface.

Default Verify Mode: This parameter is used to set the default verification mode, that is, the "Fingerprint" or “Face” verification mode.

Picture Delay (S): This parameter is used to set the picture cycle interval (value scope: 3–999 seconds).

Sleep Time (S): This parameter is used to specify a period after which the FFR terminal is put in sleep mode if not operated within this period. You can bring up the

FFR terminal from sleep by pressing any key or touching the screen.

5.3 Fingerprint Parameters

1: 1 Threshold: This parameter is used to set the threshold of matching between current fingerprint and the fingerprint template enrolled in the FFR terminal in the 1:1 verification mode. If the similarity between current fingerprint and the fingerprint template enrolled in the FFR terminal is larger than this threshold, the matching is successful; otherwise, the matching is not successful.

1: N Threshold: This parameter is used to set the threshold of matching between current fingerprint and the fingerprint template enrolled in the FFR terminal in the 1:N verification mode. If the similarity between current fingerprint and the fingerprint template enrolled in the FFR terminal is larger than this threshold, the matching is successful; otherwise, the matching is not successful.

The recommended thresholds are as follows:

		Threshold	
False Rejection Rate (FRR)		1: N	1:1
False Acceptance Rate (FAR)			
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

1:1 Retry Times: This parameter is used to set the retry times in the event of failure of 1:1 verification or password verification due to absence of fingerprint enrollment or improper finger placement, so as to avoid repetitive operations.

Algorithm Version: This parameter is used to select the fingerprint algorithm version between 9.0 and 10.0. Please select the algorithm version with caution because the fingerprint templates of these two algorithm versions are incompatible.

Fingerprint Image: This parameter is used to set whether to display the fingerprint image on the screen during fingerprint enrollment or comparison. It has two values: Permanent Display and No Display.

5.4 Face Parameters

1: 1 Threshold: This parameter is used to set the threshold of matching between current face and the facial template enrolled in the FFR terminal in the 1:1 verification mode. If the similarity between current face and the facial template enrolled in the FFR terminal is larger than this threshold, the matching is successful;

otherwise, the matching is not successful. The valid value scope is 55–120. The higher the threshold, the lower the FAR and the higher the FRR, and vice versa.

1:1: N Threshold: This parameter is used to set the threshold of matching between current face and the facial template enrolled in the FFR terminal in the 1:N verification mode. If the similarity between current face and the facial template enrolled in the FFR terminal is larger than this threshold, the matching is successful; otherwise, the matching is not successful. The valid value scope is 65–120. The higher the threshold, the lower the FAR and the higher the FRR, and vice versa.

The recommended thresholds are as follows:

FRR	FAR	Threshold	
		1: N	1:1
High	Low	90	80
Medium	Medium	80	70
Low	High	75	65

Enroll Mode: This parameter is used to select the facial enrollment mode between “Combined Enroll” and “Face”. In the “Combined Enroll” mode, users need to enroll their fingerprints or passwords after facial enrollment; in the “Face” mode, users only need to enroll their facial images. The “Face” mode is unavailable for the administrators because the “Combined Enroll” mode is mandatory for them by default.

Exposure: This parameter is used to set the exposure value of the camera.

Gain: This parameter is used to set the gain value of the camera.

Quality: This parameter is used to set a quality threshold for the facial images obtained. The FFR terminal accepts the facial images and processes them by adopting the facial algorithm when their quality is higher than the threshold; otherwise, it filters these facial images.

Algorithm Version: Face Algorithm can choose 5.0Algorithm or 7.0Algorithm.

Note: Improper adjustment of the Exposure, Gain and Quality parameters may

severely affect the performance of the FFR terminal. Please adjust the Exposure parameter only under the guidance of the after-sales service personnel from our company.

5.5 Log Settings

Log Alert: When the available space is insufficient to store the specified number of attendance records, the FFR terminal will automatically generate an alarm. (Value scope: 1–99)

Dup. Punch Period (m): If a user's attendance record already exists and the user punches in again within the specified period (unit: minute), his/her second attendance record will not be stored. (Value scope: 1–60 minutes)

Workcode Mode: This parameter is used to select the work code input mode among Mode 1, Mode 2 and None during attendance verification. If you select Mode 1, the attendance verification starts after you input the work code on the initial interface; if you select Mode 2, the attendance verification starts before you input the work code on the initial interface; if you select None, you do not need to input the work code during attendance verification on the initial interface. For the input of the work code, see 6.2 Workcode.

Card Only: If this parameter is set to "YES", you pass the verification only after card verification. If this parameter is set to "NO", you need to verify your face or fingerprint after card verification.

5.6 Update

You can upgrade the firmware program of the FFR terminal by using the upgrade file in the USB disk through this parameter.

If you need the firmware upgrade file, please contact our technical support personnel. Generally the firmware upgrade is not recommended.

6. Data Management

Through the [Data Mgt.] menu, you can perform management of data stored on the FFR terminal, for example, deleting the attendance record, all data and promotional pictures, purging management rights and resetting the FFR terminal to factory defaults.

Delete Transactions: Delete all the attendance records.

Delete All Data: Delete all the information of enrolled personnel, including their fingerprints, facial images and attendance records.

Clear Administrator: Change all administrators to ordinary users.

Delete Picture: Purge the promotional pictures uploaded from USB disks to the FFR terminal. (For details on how to upload promotional pictures, see “5.4 Upload Picture”.)

Restore to Factory Settings: Restore all parameter settings on the FFR terminal to factory settings.

Record: Query the attendance records of employees within a specified time range.

WorkCode: Add, edit or delete the work codes of employees.

SMS: Checking about message.

The employee information and attendance records will not be deleted during restoration to factory

6.1 Query a Record

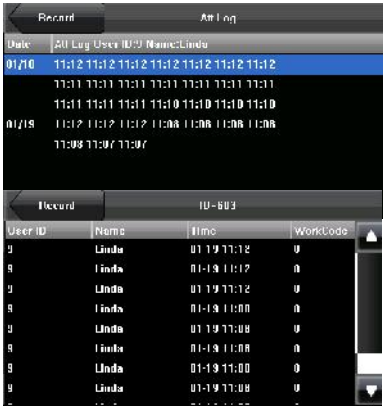
After check-in successfully, the employee's attendance records are saved in the FFR terminal. You can easily query these attendance records.

User ID: Enter the user ID of the employee to query. If this field is left blank, you can query the attendance records of all the employees. If you enter a user ID, you can query the attendance record of the employee with this user ID.

Query Time Period: Select a time period to query, including the customized time period, yesterday, this week, last week, this month, last month, and all time periods.

Start and **End**: When you select a customized time period, you need to input a start time and an end time. When you select other options for time period, the start and end time will be automatically adjusted to the related time.

After setting the query conditions, press [Query] and the records that meet the specified query conditions will be displayed on screen.

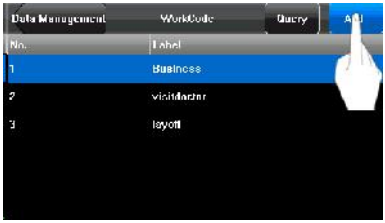


Select the row where the desired record is located, you can query the detailed information of this record, for example, the detailed attendance record of the employee with user ID 2 on January 7th.

6.2 Work Code

Employees' salaries are subject to their attendance records. Employees may be engaged in different types of work which may vary with time periods. Considering the salaries vary with work types, the FFR terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate rapid understanding of different attendance situations during the handling of attendance data.

1. Add a work code



1) Press [Add] on the [WorkCode] interface (as shown in Figure 1 on the right) to display the [Add] interface.

No.: A digital code of the work code.

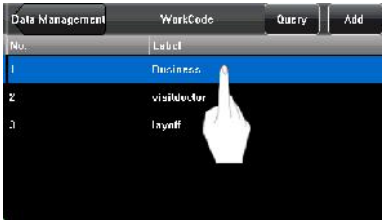
Label: The meaning of the work code.

2) Press the corresponding entry button of [No.] on the [Add] interface (as shown in Figure 2 on the right) to display the No. entry interface. On this interface, enter a No.

3) Press the corresponding entry button of [Label] on the [WorkCode] interface (as shown in Figure 3 on the right) to display the text entry interface. On this interface, enter a label of work code. (See Appendix 1 Text Entry Operation Instruction)

2. Edit and delete a work code

1) Press the row of a work code on the [WorkCode] interface (as shown in Figure 1 on the right) to display the [Edit] interface.



2) To edit this work code, enter a new No. and label with the same operation steps as described in “Add a work code”.

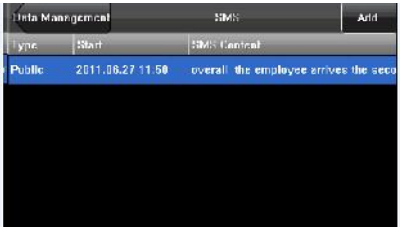
3) To delete this work code, press [Delete] (as shown in Figure 3 on the right).

4) On the displayed prompt interface, press <YES> to confirm the deletion of this work code, and press <NO> to cancel the deletion operation (as shown in Figure 4 on the right).

6.3 SMS ★

SMS is similar to notice. The operator can edit the notice content in advance and make it into SMS displayed on the screen. SMS includes common SMS and individual SMS. If common SMS is set, SMS will be displayed in main interface in the specified time. If individual SMS is set, the employee who can receive SMS can see SMS after successful attendance.

Operation



Notice: The picture may be different from your device. The real product prevails.

6.3.1 Set Message

1）add SMS

Start time: The time when SMS comes into effect

Valid[minute]: SMS appears in the effective time. After the effective time, it won't appear.

Information type:

Personal: SMS aimed at individual only

Public: SMS able to be seen by all employees

Reserved: Preset SMS, no difference of individual SMS or common SMS.

Operation:

When the cursor is on the text box, press shortcut to enable T9 input, input SMS content. Show below:

（1）If the selected type is individual SMS, Assign is usable. Here, it is to distribute individual SMS to employee:

Press on the UserID to search employee.

Press “page down & page up” to search employee.

Press on the employee will select it, and SMS will be distributed to him.

Press Save button to save it and then exit.

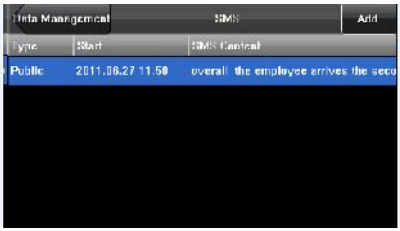
Notice: 1. If exit without selecting any employee, the SMS type will become preset.

2. If nobody is selected, it will show a warning " Please choose user! " when assign or save the message.

2) If the selected type is common SMS or preset SMS, Assign cannot be used. After setting, press menu to save it and return to SMS list.

2. Edit SMS

Press on the message show below to select “edit”, and SMS can be edited. The operation is the same with that of add SMS.



3. Delete SMS

Press the 

button to select “delete”, and the selected SMS can be deleted. At the same time, all information related with this record can be cleared. Show below:

6.3.2 Employee Check Message

1) check common SMS

When the device is in standby state, the main interface will display pictures and current effective common SMS content in cycle. The display time interval is the same with that of

picture display.

2）check individual SMS

When user passes verification, if the user has SMS, the SMS content will be displayed.

The information display time length is 30 seconds. During this period, user verification can be done. Close the current display to enter verification interface.

7. USB Disk Management

Through the [Dn/Upload] menu, you can import user information and attendance data stored in a USB disk to related software or other fingerprint recognition equipment.

Download Transactions: Import all the attendance data from the FFR terminal to a USB disk.

Download User: Import all the user information, fingerprints and facial images from the FFR terminal to a USB disk.

Download user photos★: Import the employees' photos from the FFR terminal to a USB disk.

Download Message: Import the message from the FFR terminal to a USB disk.

Only several types of the FFR terminals support the download of user photos.

Upload User: Upload the user information, fingerprints and facial images stored in a USB disk to the FFR terminal.

Upload User: Upload the message stored in a USB disk to the FFR terminal.

Upload User Photo: Upload the JPG documents that are named after the user IDs and stored in a USB disk to the FFR terminal, so that user photos can be displayed after the employees pass the verification. See Appendix 4 Photo ID Function.

Upload Picture: Upload the JPG documents with "ad_" as initial letters of document names stored in a USB disk to the FFR terminal. After the upload, these pictures can be displayed on the initial interface of the FFR terminal. (For details on picture specifications, see Appendix 2.)

8. Keyboard Definitions

You can define six shortcut keys as attendance status shortcut keys or functional shortcut keys. On the main interface of the FFR terminal, press corresponding keys and the attendance status will be displayed or the function interface will be rapidly displayed.

1. Press [Keyboard] on the main menu interface to display the [Keyboard] interface, as shown in Figure 1 on the right.

2. All the defined shortcut keys and their functions are listed on the [Keyboard] interface (as shown in Figure 2 on the right). Press [Add] to display the shortcut key adding interface. Press a shortcut key in the list to display the shortcut key editing interface.

3. Add and edit the functional introduction of interface

Shortcut Key: Options include: F1–F6.

Note: When the FFR terminal supports both fingerprint and face recognition modes, F6 is defined as a recognition mode switch key by default and cannot be modified.

Function: You can set the functions of

different shortcut keys, such as functional shortcut keys, attendance status shortcut key and work code shortcut key.

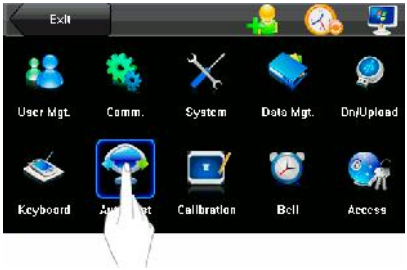
Functional shortcut status include: 1:1/1:G, Face Group No.1, Face Group No.2, Face Group No.3, Face Group No.4 and Face Group No.5. The setting interface is shown in Figure 3 on the right.

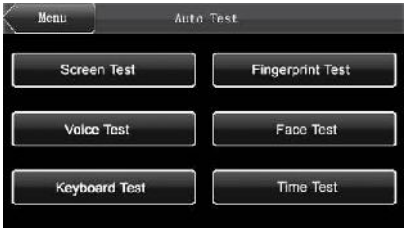
The status shortcut keys include: Check-In, Check-Out, Leave, Back, Overtime Check-In, and Overtime Check-Out. The setting interface is shown in Figure 4 on the right. When setting the attendance status shortcut keys, you can also set the “Auto Switch” parameter. When “Auto Switch” is enabled, the FFR terminal automatically switches the attendance status at the specified time. The “Auto Switch” setting interface is as shown in Figure 5 on the right.

The work code shortcut key setting interface is as shown in Figure 6 on the right.

9 Auto Test

The auto test enables the system to automatically test whether functions of various modules are normal, including the screen, collector, voice, facial, keyboard and clock tests.





Screen Test: The FFR terminal automatically tests the display effect of the color TFT display by displaying full color, pure white and pure black and checks whether the screen displays properly. You can continue the test by touching the screen or exit it by pressing [Auto Test].

Voice Test: The FFR terminal automatically tests whether the voice files are complete and the voice quality is good by playing the voice files stored in the terminal. You can continue the test by touching the screen or exit it by pressing [Auto Test].

Keyboard Test: The FFR terminal tests whether every key on the keyboard works normally. Press any key on the [Keyboard Test] interface to check whether the pressed key matches the key displayed on screen. The keys are dark-gray before pressed, and turn blue after pressed. Press [Auto Test] to exit the test.

Fingerprint Test: The FFR terminal automatically tests whether the fingerprint collector works properly by checking whether the fingerprint images are clear and acceptable. When the user places his/her finger in the fingered guide, the collected fingerprint image is displayed on the screen in real-time. Press [Auto Test] to exit the test.

Face Test: The FFR terminal automatically tests whether the camera works properly by checking whether the collected facial images are clear and acceptable. Press [Auto Test] to exit the test.

Time Test: The FFR terminal tests whether its clock works properly by checking the stopwatch of the clock. Touch the screen to start counting, and touch it again to stop to check whether the counting is accurate. Press [Auto Test] to exit the test.

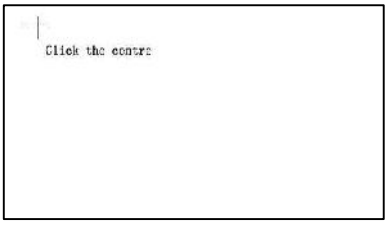
10 Screen Calibration

You can perform all the menu operations by touching the screen with one of your fingers or a touch pen. When the touch screen is less sensitive to the touch, you can perform screen calibration through menu operations.

1. Press [Menu] on the initial interface to display the main menu interface.

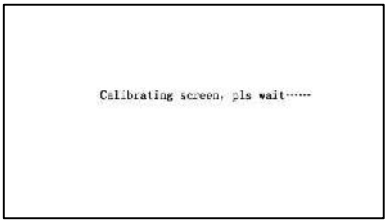
2. Press [Calibration] on the main menu interface to display the screen calibration interface.

3. Touch the center of the cross “+”.



4. Repeat Step 3 following the move of the “+” icon to different locations on the screen.

5. Touch the center of the cross at five locations on the screen correctly. When the message “Calibrating screen, pls wait……” is displayed on screen, the calibration succeeds and the system automatically returns to the main menu.



If the calibration fails, the system will request recalibration starting from Step 3.

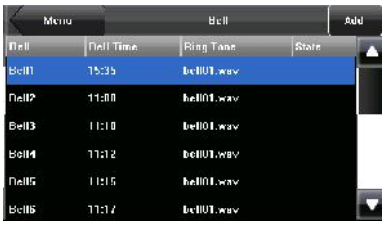
11 Bell Setting

Lots of companies need to ring their bells to signal the start and end of work shifts, and they usually manually ring their bells or use electric bells. To lower costs and facilitate management, we integrate the time bell function into the FFR terminal. You can set the alarm time and duration for ringing the bell based on your requirements, so that the FFR terminal will automatically play the selected ring tone and trigger the relay at the alarm time, and stop playing the ring tone after the set duration.

Press [Bell] on the main menu interface to display the bell setting interface, as shown in Figure 1 on the right.

1. Add a bell

1) The displayed bell setting interface (as shown in Figure 2 on the right) lists all the bells. Click [Add] to display the [Add] interface.



2) On the [Add] interface, set the following parameters:

Bell Time: This parameter is used to set a time point when the FFR terminal automatically plays a bell ring tone everyday.

Ring Tone: This parameter is used to set the bell ring tone.

Volume: This parameter is used to set the volume of ring tone.

Repeat: This parameter is used to set the alarm times.

State: This parameter is used to set whether to enable the bell.

Bell Type: You can select between internal ringing or external ringing. For internal ringing, the ring tone is played by the loudspeaker of the FFR terminal. For external ringing, the ring tone is played by an external electric bell that is wired with the FFR terminal.

Notice: Only some models have external ringing options.

The alarm sounds of the bell and the access control cannot be concurrently generated by the loudspeaker of the FFR terminal or externally connected relay. Therefore, when the bell is set to the external ringing mode, the access limit alarm will automatically change to the internal ringing mode, and vice versa.

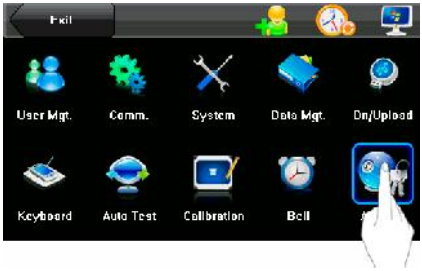
2. Edit and delete a bell

Press a bell in the list on the bell setting interface to display the [Edit] interface, with the similar operation as “Add a bell”.

Press [Delete] on the [Edit] interface and the system displays a prompt window as shown in the figure on the right. In the prompt window, press <YES> to delete the current bell and <NO> to cancel the deletion.

12 Access Control Setting ★

Through the [Access] menu, you can set the parameters of the electronic locks and related access control devices.



Time Zone Set: Is the definition of everyday Time period that can unlock door in one week;

Lock Control Para: setting the Lock Delay[s], Door Sensor Delay[s] and alarm Delay[s] Para, show below:

(1**). Lock Delay[s]:** Fingerprint scanner controls the time to open electronic lock. (Functioning value for 1~10)-the language document apply(second) behind and check all language documents.

(2). Door Sensor Delay[s]: Some segment time which begin after open door just begin alarm; (The functioning value is 1~99)

(3). Door Sensor Mode: there are three option that is none(NONE), normal open (NO), normal close(NC) .the none means the door Sensor doesn't apply, Normal Open is defined that Thee door can be set to a Passage Mode in the normal

condition, Normal Close means that the door is close in the normal work condition.

Holiday Set: Set special access control time during holiday.

TimeZone Control Para: Can set the NC Time Zone and NO Time Zone, show below:

Group Settings: Set TimeZone as group.

Duress Alarm Parameter: include 1:1 Trigger, 1:N Trigger Alarm Delasy and Password Trigger setup item, show below.

Unlock combination Setting: defines different unlocking combinations, each combination is composed of different groups.

Anti-Passback Setting: APB Direction setting, can set as APB-Out, APB-In, APB-Out/In and None; Local Status can set as Exit Control, Entry Control and None. Show below:

13 Date/Time Setting

13.1 Set Date/Time

The date and time of the FFR terminal must be set accurately to ensure the accuracy of attendance time.

1. Press [Menu] on the initial interface to display the main menu interface.
2. Press [Time/Date] on the main menu interface to display the time setting interface.

3. Select the desired date and time by pressing ▲ or ▼, or enter the related values into the date and time entry boxes through the keyboard (as shown in Figures 3 and 4 on the right).

4. Press [Save] to save current information and return to the previous interface. Press [Cancel] to return to the previous interface without saving current information.

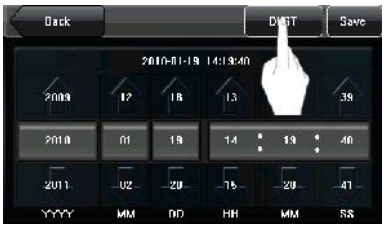
13.2 Set Daylight Saving Time (DST)

The Daylight Saving Time (DST) is a widely used system of adjusting the official local time forward to save energy. The uniform time adopted during the implementation of this system is known as the DST. Typically clocks are adjusted forward one hour in the summer to make people early to bed and early to rise so as to make full use of illumination resources and save electricity. Clocks are adjusted backward in autumn. The specific DST regulations vary with countries.

To meet the DST requirement, the FFR terminal supports the DST function to adjust forward on hour at ×× (Hour): ×× (Minute) ×× (Day) ×× (Month) and backward one hour at ×× (Hour): ×× (Minute) ×× (Day) ×× (Month).

1. Press [Menu] on the initial interface to display the main menu interface.
2. Press [Time/Date] on the main menu interface to display the time setting interface.

3. Press [DLST] on the time setting interface to display the DST setting interface.



4. Set the following parameters on the DST setting interface:

DST Settings: This parameter is used to enable or disable the DST.

Mode: You can select between Mode 1 and Mode 2.

In Mode 1 (the default mode), the DST is set in the "Month-Day Hour: Minute" format; in Mode 2, the DST is set in the "Month-Week-Day Hour: Minute" format.

The value scope of week (WS): 1 – 6. 1 means the first week, 2 the second week and so on and so forth. The value scope of day (WK): 0 – 6. 0 means Sunday, 1 means Monday and so on and so forth.

Start and End: These two parameters are respectively used to set the start and end time of the DST.

For example, adjust the clock forward one hour at 08: 00 on April 1st, and backward one hour at 08: 00 on October 1st.

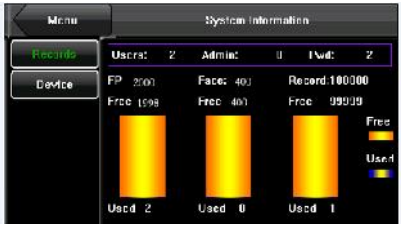
5. After setting the DST, press [Done] to return to the time setting interface. Press [Save] on the time setting interface to save current settings and return to the previous interface; press [Cancel] to directly return to previous interface without saving current information.

14 System Information

You can check the storage status as well as version information of the FFR terminal through the [System Information] option.

14.1 Records

The number of enrolled users, administrators and passwords is displayed on the [Records] interface; the total fingerprint storage capacity and occupied capacity as well as the total attendance storage capacity and occupied capacity are graphically displayed respectively, as shown in the following figure:



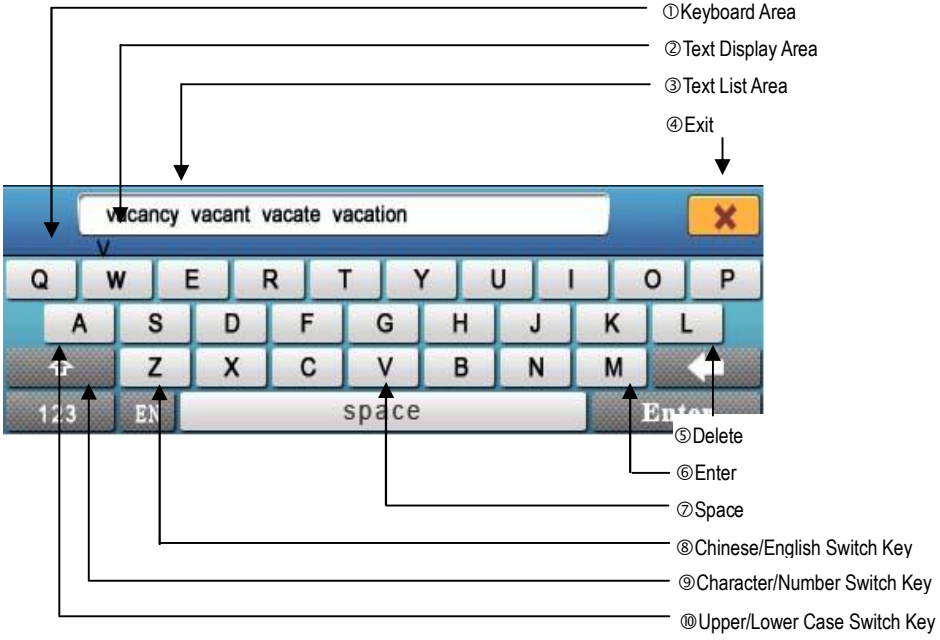
14.2 Terminal

The terminal name, serial number, version information, vendor and date of manufacture are displayed on the [Terminal] interface.

Appendix

Appendix 1 Text Input Instructions

The FFR terminal supports the input of Chinese and English characters, numbers and symbols. Press related button to input text. For example, press [Name] to display the text input interface, as shown in the following figure:



To enter a name, proceed as follows:

1. Press [Name] on the [Add] interface, as show below.

2. Enter the Pinyin characters, and a list of Chinese characters in relation to the Pinyin is presented in the text display area, as shown in Figure 1 on the right.

3. If the desired character is displayed in the text display area, press this character. And this character is at the same time displayed on the [Name] button, as shown in Figure 2 on the right. Enter next character by repeating Step 2.

4. After finishing the entry of name, press [X] to exit keyboard interface and return to the previous interface.

Appendix 2 Rules for Uploading Promotional Pictures

1. All pictures must be in JPG format as other formats are not supported.
2. The file name of a promotional picture must be ad_0 - ad_9. For example, ad_1.jpg is a valid file name.
3. After a picture is uploaded to the FFR terminal, its name does not change. To replace this picture, you need to upload a new picture with the same file name to overwrite it.
4. The size of each picture cannot exceed 20K; otherwise, the upload will be unsuccessful.
5. The recommended resolution of the picture is 320 × 240. Pictures with resolution higher or lower than 320 × 240 are not recommended.
6. A maximum of 10 promotion pictures can be uploaded.

Appendix 3 Introduction to Wiegand

Wiegand26 is an access control standard protocol established by the Access Control Standard Subcommittee affiliated to the Security Industry Association (SIA). It is a non-contact IC card reader interface and output protocol.

Wiegand26 defines the interface between the card reader and controller used in the access control, security and other related industrial fields. Wiegand26 helps standardize the work of the card reader designers and controller manufacturers. The access control products manufactured by our company are also designed by following this protocol.

Digital Signals

Figure 1 is a sequence diagram in which the card reader sends digital signals in bit format to the access controller. In this sequence diagram, Wiegand follows the SIA's access control standard protocol for the 26-bit Wiegand card reader (one pulse time ranges between 20us and 100us, and the pulse jump time ranges between 200us and 20ms). Data1 and Data0 are high level (larger than Voh) signals till the card reader prepares to send a data stream. The asynchronous low-level pulse (smaller than Vol) generated by the card reader is sent to the access control panel (The saw-tooth wave as shown in Figure 1) through Data1 or Data0. Data1 and Data0 pulses will neither overlap nor be generated synchronously. Table 1 lists the maximum and minimum pulse width (a consecutive pulse) and pulse jump time (time between pulses) allowed by the F series fingerprint access control terminal.

Table 1 Pulse Time

Symbol	Definition	Typical Value of Reader
Tpw	Pulse Width	100 μs
Tpi	Pulse Interval	1 ms

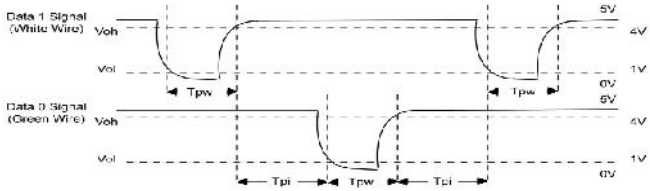


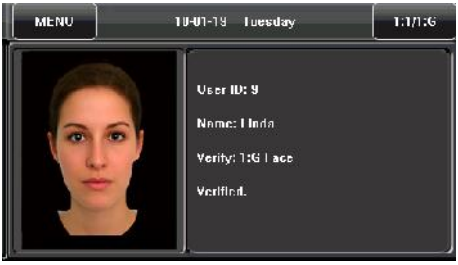
Figure 1 Sequence Diagram

Appendix 4 Photo ID Function

Some FFR terminals also support the Photo ID function. The Photo ID function is used to display the photo enrolled by a user or stored in a USB disk on the screen in addition to such information as the user ID and name.

[Operation Steps]

1. When the photo taken by the FFR terminal is used, the photo can be displayed upon successful verification.



2. To use a photo stored in a USB disk, proceed as follows:
   1) Create a folder with the name of “photo” in the USB disk, and store users’ photos under this folder.
   2) The user photos must be in JPG format and named after their IDs. For example, for the user with user ID of 154, the photo name must be 154.jpg.
   3) Insert the USB disk into USB slot on the FFR terminal, and select USB Disk Management -> Upload -> Upload Photos. Then user photos can be displayed upon successful verification.

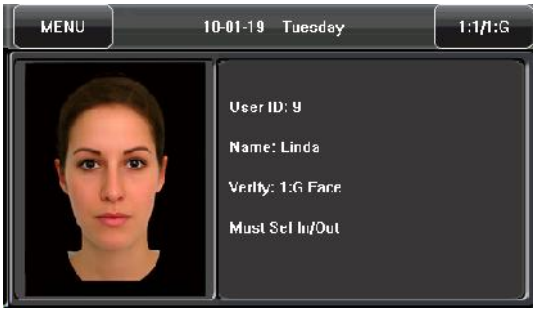
      Note: 1) The length of a user name cannot exceed 24 digits.

2) The recommended size of a user photo is less than 30K.
3) The uploaded new user photo will overwrite the existing photo in related to the user ID.

4) To download user photos, select USB Disk Management -> Download -> Download User Photos. A folder with the name of “photo” will be automatically created on the USB disk, and all downloaded user photos are stored under this folder.

Appendix 5 Attendance Status Selection Function ★

Some FFR terminals also support the attendance status selection function which requires users to select attendance status prior to verification. If verification is performed without selection of the attendance status, the record is “No Work Status”, that is, the record is not used as the attendance record, as shown in the following figure:



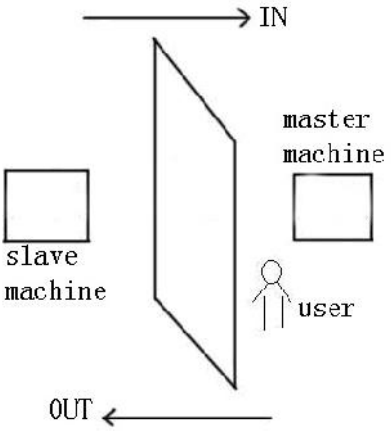
You cannot set the timed status switch function on the FFR terminal capable of attendance status selection.

Appendix 6 Anti-pass back ★

[overview]

Sometimes, some illegal person follows the employee into the gate, which will bring security problem. To prevent such risk, this function is enabled. In record must match out record, or the gate won't be open.

This function needs two machines to work together. One is installed inside the door (master machine hereinafter), the other is installed outside the door (slave machine hereinafter). Wigand signal communication is adopted between the two machines.



[working principle]

The master machine has Wigand In and slave machine has Wigand Out. Connect Wigand Out of slave machine to Wigand In of master machine. Wigand output from slave machine must not own machine ID. The number sent to master machine from slave machine must be found in the master machine.

[function]

Judge whether it is anti-pass back according to user's recent in-out record. In record

and out record must be matched. This machine supports out, in, or out-in anti-pass back (enter machine menu—setting—system setting—advanced setting—anti-pass back).

When master machine is set as “out anti-pass back”,if user wants to come in and go out normally, his recent record must be “in”, or he cannot go out. Any “out” record will be “anti-pass back refused”. For example, a user’s recent record is “in”, his second record can be “out” or “in”. His third record is based on his second record. Out record and in record must match.（Notice: if customer has no record before, then he can come in but cannot go out. ）

When the master machine is set as “in anti-pass back”,if the user wants to come in and go out normally, his recent record must be “out”, or he cannot go out. Any out record will be “anti-pass back refused” by the system. (Notice: if the customer has no former record, then he can go out, but cannot come in. ）

When the master machine is set as “out-in anti-pass back”,if the user wants to come in and go out normally, if his recent record is “out” and “in”, then his next record must be “ in” and “out”.

[operation]

1) Select model

Master machine: Machine with Wiegand in function, except for F10

Reader.

Slave machine: Machine with Wiegand Out function.

2) Menu setting

Anti-pass back:

There are three options: Out anti-pass back, in anti-pass back and nonanti-pass back.

out anti-pass back: Only user’s last record is in-record, can the door be open.

in anti-pass back: Only user’s last record is out-record, can the door be open.

Device status

There are three options: Control-in, control-out and none.

Control-in: When it is set, the verified record on the device is in-record.

Control-out: When it is set, the verified record on the device is out-record.

None: When it is set, close the device's anti-pass back function.

Press ▲/▼ to switch the input box. Press ◀/▶ to modify setting. Then press **save** to save it.

3) modify device's Wiegand output format

When the two devices are communicating, only Wiegand signals without device ID are received. Enter device menu—>communication option—>Wiegand option or enter software-〉basic setting-〉device management-〉Wiegand,to modify "defined format" as "wiegand26 without device ID".

4) enroll user

The user must be on master machine and slave machine at the same time, and user PIN must be the same. Therefore, it is necessary to enroll user on master machine and slave machine at the same time.

5) connection instruction

Wiegand communication is adopted for master machine and slave machine. Refer to the following for connection::

Master		Slave
IND0	<----->	WD0
IND1	<----->	WD1
GND	<----->	GND

Appendix 7 Multi- verification methods ★

To meet the demand of high security, we have provided multi- verification modes. Aimed at individual or group setting, various verification types are set. They are the combinations of PIN,FP, PW and RF, for example: single fingerprint, single password, ID+FP, FP+PW, FP+PW+card, PIN+FP+PW and so on.

Notice: 1）Mifare can be looked as RF in the real dispose. Only device with Mifare card function can use it.

2）Except for some special models, most devices have only fingerprint verification and password verification. Only device with Mifare card function has Mifare card verification.

"/"--- or ,"&"--- and "←"---Enter

The following is the description of user enrolled fingerprint card and the verification mode with password enrolled.

type	description
FP	Only fingerprint verification 1）PIN+FP（1:1 verification ） 2）FP (1:N verification) 3）RF+FP(1:1 match)
PIN	only number verification 1）PIN+“←”
PW	only password verification 1） PIN+“←”+PW 2） RF+PW
RF	only RF Card verification 1）RF+FP
FP/PW	fingerprint or password verification

	1）PIN+FP(1:1) 2）FP(1:N) 3）PIN+“←”+PW 4）RF+PW
FP/RF	fingerprint or RF verification 1）PIN+FP(1:1) 2）FP(1:N) 3）RF+FP
PW/RF	password or RF verification 1） RF+FP 2） PIN+“←”+PW
FP/PW/RF	fingerprint or password or RF verification 1） PIN+FP(1:1) 2） FP(1:N) 3） PIN+PW 4） RF+FP
FP&PIN	fingerprint and number verification 1）PIN+“←”+FP(1:1) 2）RF +“←”+FP(1:1)
FP&PW	fingerprint and password verification 1） FP(1:N)+PW+“←” 2） PIN+FP(1:1)+PW+“←” 3） RF+PW +“←”+ FP(1:1)
FP&RF	fingerprint and RF verification 1）RF+FP(1:1) 2）FP(1:N)+RF 3）PIN+FP(1:1)+RF
PW&RF	password and RF verification

	1） RF+PW 2） PIN+“←”+PW+RF
FP&PW&RF	fingerprint, password and RF verification
	1） FP(1:N)+PW+RF 2） PIN+FP(1:1)+PW+RF 3） RF+ PW+ FP(1:1)
FP&PIN&PW	fingerprint,number and password
	1） PIN+“←”+PW+FP(1:1) 2） RF+“←”+PW+“←”+FP(1:1)
FP&RF/PIN	Fingerprint and RF verification or fingerprint and number.
	1）RF+FP(1:1) 2）FP(1:N)+RF 3）PIN+“←”+FP(1:1)

If enroll user with fingerprint card or password +card, refer to the following for various verifications:

type	description	
	fingerprint enroll	password enroll
FP	Only fingerprint verification	
	1 ） PIN+FP （ 1:1 verification ） 2）FP (1:N verification 3）RF+FP(1:1)	cannot pass
PIN	only number verification	
	1）PIN+“←”	1）PIN+“←”
PW	only password verification	

	password error	1） PIN+“←”+PW 2）RF+PW
RF	Only RF Card verification	
	1）RF+FP	1）RF
FP/PW	fingerprint or password verification	
	1） PIN+FP(1:1) 2） FP(1:N) 3） PIN+“←”+ FP(1:1) 4） RF+FP(1:1)	1） PIN+“←”+PW 2） RF+PW
FP/RF	fingerprint or RF verification	
	1） PIN+FP(1:1) 2） FP(1:N) 3） RF+FP	1）RF
PW/RF	password or RF verification	
	1） RF 2） PIN+“←”+RF	1） PIN+”←”+PW 2） RF
FP/PW/RF	fingerprint or password or RF verification	
	1） PIN+FP(1:1) 2） FP(1:N) 3） PIN+“←”+ FP(1:1) 4） RF+FP	1） PIN+”←”+PW 2） RF
FP&PIN	fingerprint and number verification	

	1） PIN+“←”+FP(1:1) 2） RF+ PIN+“←”+FP(1:1)	cannot pass
FP&PW	fingerprint and password verification	
	cannot pass	cannot pass
FP&RF	fingerprint and RF verification	
	1） RF+FP(1:1) 2） FP(1:N)+RF 3） PIN+FP(1:1)+RF	cannot pass
PW&RF	password and RF verification	
	cannot pass	1） RF+PW 2） PIN+“←”+PW+RF
FP&PW&RF	fingerprint, password and RF verification	
	cannot pass	cannot pass
FP&PIN&PW	fingerprint,number and password	
	cannot pass	cannot pass
FP&RF/PIN	fingerprint and RF verification or fingerprint and number	
	1）RF+FP(1:1) 2）FP(1:N)+RF 3）PIN+“←”+FP(1:1)	cannot pass

Notice:1）If user enrolls a card and fingerprint at the same time.

Only card is needed during RF verification.

2）For combined verification, it is better to use **fingerprint +password** to enroll user, or verification will fail.

For example:User A use fingerprint for enrollment, while password is used for verification, then the user cannot pass the verification.

Appendix 8 GPRS ★

General Packet Radio Services (GPRS) is a packet-based wireless communication service that promises data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users. The higher data rates allow users to take part in video conferences and interact with multimedia Web sites and similar applications using mobile handheld devices as well as notebook computers. GPRS is based on Global System for Mobile (GSM) communication and complements existing services such circuit-switched cellular phone connections and the Short Message Service (SMS).

We fingerprint machine has also realized the GPRS function. GPRS modules can be built-in fingerprint machine , also can be an external GPRS module to achieve the GPRS systems for data transfer.

How to operate GPRS fingerprint machine, please see 4.5 dail-up settings.

Appendix 9 Webserver ★

At the first time use the Webserver, should be configure the setting, enter menu -> communications settings fingerprints IP address, such as set up the IP address of the fingerprint machine to 192.168.1.225; type the “//192.168.1.225 in IE address bar

The default the system user name of super administrator: administrator; Password: 123456.

Enter view records

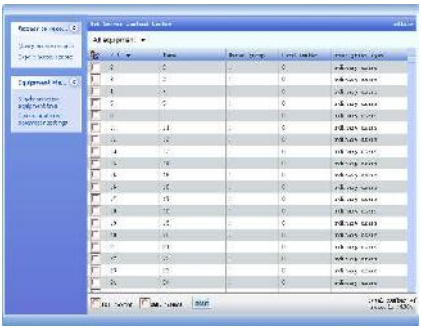
① Left-click option "View In-Out records" interface;

② to select staff you want to view in the list;

③ designate the time scope for view.

2) Export In –Out records: Save these logs to local disk.

① left click "Export logs" option;



② choose staff you want save his records in the list; ③ select file format to save.

④ click "start the download" and save the file to the local disk.

synchronization equipment time

① left click "synch equipment time" option on the interface;

② select the adjustment method

Auto: Time of computer and equipment will be automatically synchronized.

Manual adjustments: manually set the time of the equipment and defined time synchronization.

③ local equipment date

Choose automatic adjustment, this machine‘s date and time is the computer date.

Choice of manual adjustments can manually enter the time.

④ click the "modified" button to change the time of equipment

communication parameter

① left click "communication parameters" option on interface

② enter the communications parameters

• Ethernet:

(1) Through the hub: with cable (for connecting Net cards and hubs) connect machines to the network.

(2) Directly connection: Use the cross-cable (direct connect the two Ethernet endpoint) to connect machines and PC .

IP Address: The default IP is 192.168.1.201, you can make changes based on the actual situation;

Subnet Mask: The default subnet mask 255.255.255.0, you can make changes based on the actual situation;

Gateway Address: default gateway address 0.0.0.0, you can make changes based on the actual situation;

• RS232: the use of RS232 serial port.

Baud rate: the communications and computer communications rate, high-speed communications faster, the proposed use of RS232 communications 115200,57600 the baud rate.

RS232/RS485: whether or not to use RS232 communications, select On the RS232 apply .

• RS485 way

Baud rate: the communications and computer communications rate, low-speed communication stability, the proposed RS485 communications the baud rate 9600,38400.

RS232/RS485: whether or not to use RS485 communications, select On the way to use RS485.

③ click "Save settings" button to write into the parameters of communications equipment.

Appendix 10 Statement on Human Rights and Privacy

Dear Customers:

Thank you for choosing the hybrid biometric products designed and manufactured by us. As a world-renowned provider of biometric technologies and services, we pay much attention to the compliance with the laws related to human rights and privacy in every country while constantly performing research and development.

We hereby make the following statements:

1. All of our multibio recognition devices for civil use only collect the characteristic points of multibio instead of the multibio images, and therefore no privacy issues are involved.
2. The characteristic points of multibio collected by our products cannot be used to restore the original multibio images, and therefore no privacy issues are involved.
3. We, as the equipment provider, shall not be held legally accountable, directly or indirectly, for any consequences arising due to the use of our products.
4. For any dispute involving the human rights or privacy when using our products, please contact your employer directly.

Our multibio products for police use or development tools support the collection of the original multibio images. As for whether such a type of multibio collection constitutes an infringement of your privacy, please contact the government or the final equipment provider. We, as the original equipment manufacturer, shall not be held legally accountable for any infringement arising thereof.

The law of the People's Republic of China has the following regulations regarding the personal freedom:

1. Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.

2. The personal dignity of citizens of the People's Republic of China is inviolable.
3. The home of citizens of the People's Republic of China is inviolable.
4. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law.

At last we stress once again that biometrics, as an advanced recognition technology, will be applied in a lot of sectors including e-commerce, banking, insurance and legal affairs. Every year people around the globe suffer from great loss due to the insecurity of passwords. The biometric products actually provide adequate protection for your identity under a high security environment.

Appendix 11 Environment-Friendly Use Description

The Environment Friendly Use Period (EFUP) marked on this product refers to the safety period of time in which the product is used under the conditions specified in the product instructions without leakage of noxious and harmful substances.

The EFUP of this product does not cover the consumable parts that need to be replaced on a regular basis such as batteries and so on. The EFUP of batteries is 5 years.

Names and Concentration of Toxic and Hazardous Substances or Elements

Parts Name	Toxic and Hazardous Substances or Elements					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	×	○	○	○	○	○
Chip capacitor	×	○	○	○	○	○
Chip inductor	×	○	○	○	○	○
Chip diode	×	○	○	○	○	○
ESD components	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in SJ/T11363-2006.

Note: 80% of the parts in this product are manufactured with non-hazardous environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.