

USER MANUAL

RFID & Fingerprint Recognition Series Products

Version: 1.0

Date: November, 2014

About This Manual

This document introduces the user interface and menu operations of the RFID & Fingerprint Recognition series products.

Important Claim

Firstly thank you for purchasing this facial and fingerprint hybrid terminal, before use, please read this manual carefully to avoid the unnecessary damage! The company reminds you that the proper user will improve the use affect and authentication speed.

No written consent by our company, any unit or individual isn't allowed to excerpt, copy the content of this manual in part or in full, also spread in any form.

The product described in the manual maybe includes the software which copyrights are shared by the licensors including our company, Except for the permission of the relevant holder, any person can't copy, distribute, revise, modify, extract, decompile, disassemble, decrypt, reverse engineering, leasing, transfer, sub-license the software, other acts of copyright infringement, but the limitations applied to the law is excluded.



Due to the constant renewal of products, the company cannot undertake the actual product in consistence with the information in the document, also any dispute caused by the difference between the actual technical parameters and the information in this document. Please forgive any change without notice.

CONTENT

Important Claim.....	3
1. Instruction for Use.....	1
1.1 Finger Placement.....	1
1.2 Use of Touch Screen.....	2
1.3 Touch Operations.....	3
1.4 Appearance of the FFR Terminal	4
1.5 Main Interface	5
1.6 Verification Modes.....	6
1.6.1 Fingerprint Verification	6
1.6.2 Password Verification.....	8
1.6.3 ID Card Verification.....	9
2. Main Menu.....	10
3. User Management.....	12
3.1. Adding a User.....	12
3.1.1 Entering a User ID	14
3.1.2 Entering a Name.....	15
3.1.3 Enrolling a Fingerprint	16
3.1.4 Enrolling a Password	16
3.1.5 Enrolling an ID Card	17
3.1.6 Enrolling an Mifare Card	18
3.1.7 Modify User Rights	18
3.2 Edit a User.....	18
3.3 Delete a User.....	19
3.4 Query a User.....	20
3.4.1 Query by User ID	20
3.4.2 Query by Name.....	20
4. Communication-related Settings	21
4.1 Network Settings (TCP/IP).....	21
4.2 WIFI Option ★	22
4.3 Mobile net ★	23
4.4 Webserver Setting	24
5. System Configuration	25
5.1 General	25
5.2 Display	26
5.3 Fingerprint.....	26

5.4 Log Settings	27
5.5 Update.....	28
6. Data Management.....	29
6.1 Query a Record.....	29
6.2 Work Code.....	30
7. USB Disk Management	32
8. Keyboard Definitions	33
9 Auto Test.....	34
10 Screen Calibration	35
11 Bell Setting	36
12 Date/Time Setting.....	38
12.1 Set Date/Time	38
12.2 Set Daylight Saving Time (DST).....	38
13 System Information.....	40
13.1 Records.....	40
13.2 Device	40
13.3 Cont. Info.....	40
Appendix.....	41
Appendix 1 Text Input Instructions.....	41
Appendix 2 USB Host	42
Appendix 3 State Auto Switch	43
Appendix 4 Statement on Human Rights and Privacy	44
Appendix 5 Environment-Friendly Use Description	45

1.2 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.

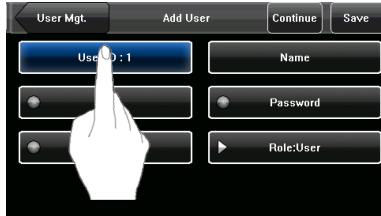


When the touch screen is less sensitive to the touch, you can perform screen calibration through menu operations. Press [Menu] → [Calibration] on the screen and a cross icon will be displayed. After you touch the center of the cross at five locations on the screen correctly, the system automatically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

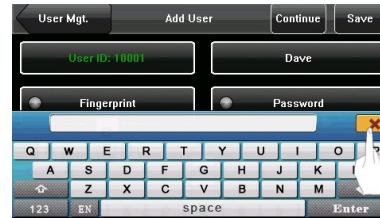
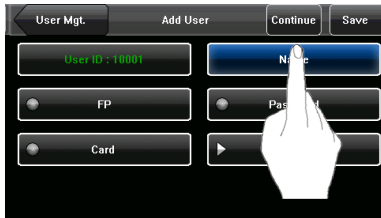
Smear or dust on the touch screen may affect the performance of the touch screen. Therefore, try to keep the screen clean and dust-free.

1.3 Touch Operations

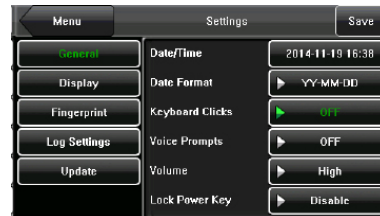
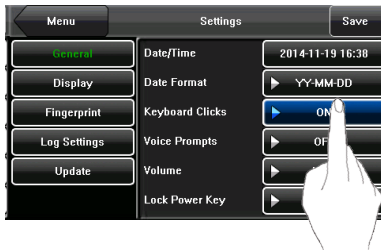
(1) Enter numbers. Press the [User ID] key. The system automatically displays the number input interface. After entering the user ID, press [OK] to save and return to the previous interface.



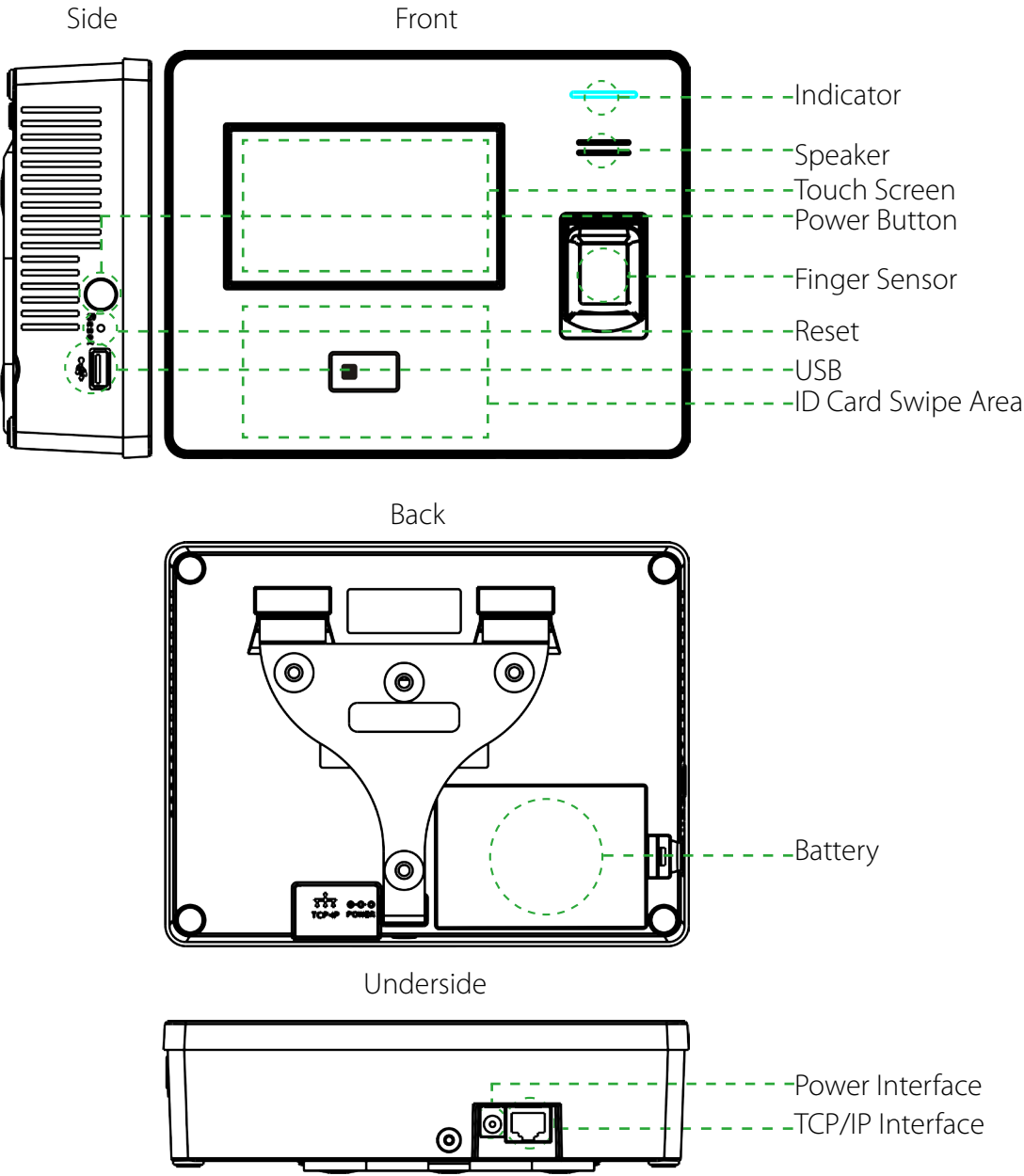
(2) Enter Text. Press the [Name] key. The system automatically displays the text input interface. After entering the user name, press [X] to save and return to the previous interface.



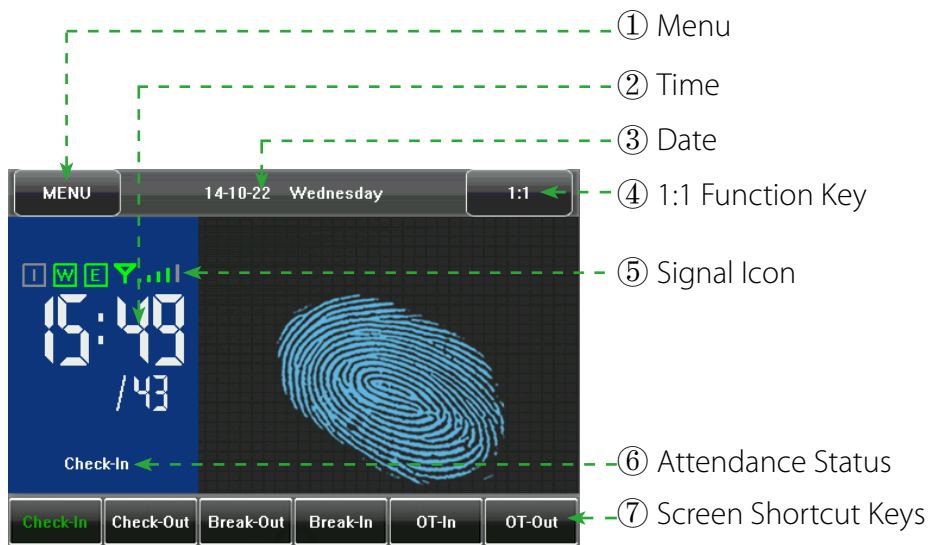
(3) Modify parameters. Press the default value of a parameter and the system automatically switches to another value of this parameter.



1.4 Appearance of the Terminal



1.5 Main Interface



① **Menu:** You can enter the main menu by touching this key.

② **Time:** Current time is displayed. Both the 12-hour and 24-hour time systems are supported.

③ **Date:** Current date is displayed.

④ **1:1 Function Key:** You can enter the digital input interface of 1:1 verification mode by pressing this key.

⑤ Meanings of the signal icons of the above interfaces:

: Indicates the WCDMA signal strength. Five bars represent full signal strength. The more bars you have, the stronger the signal you get. The less bars you have, the weaker the signal you get.

Note: If the icon above is not displayed upon device startup, it is possible that the WCDMA network signal is weak or the SIM card is faulty.

: When it is bright green indicates connection WIFI. On the contrary, it not connected.

G/E : indicates normal WCDMA Modem status.

: indicates successful activation of the WCDMA.

Note: For device with WCDMA automatically activated, if the activation success icon is not displayed, the SIM card may be faulty.

: indicates the device is already connected to the server.

: indicates the device is connecting to the server.

Note: If the WCDMA activation is successful, but the icon "I" is displayed all the

time, the problem may lie in the server.

⑥ **Attendance Status:** Current attendance status is displayed. This key is hidden when Screen Shortcut Keys are displayed.

⑦ **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 Definitions.

1.6 Verification Modes

1.6.1 Fingerprint Verification

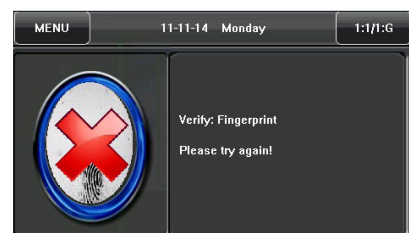
1. 1:N fingerprint verification

The terminal compares current fingerprint collected by the fingerprint collector with all fingerprint data on the terminal.

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

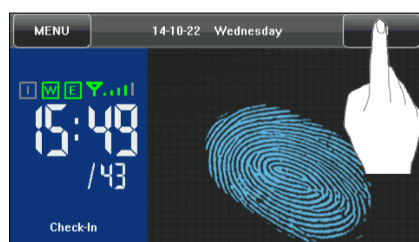
(2) If the verification is successful, an interface as shown in Figure 1 on the right will be displayed.

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



2. 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] on the screen, as shown in Figure 1 on the right.

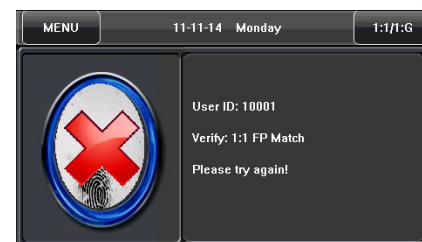
B) Press related shortcut key on the keyboard.

Note: You can enter the 1:1 recognition mode through B) only after setting a shortcut key for “1:1”. For details, see 8 Keyboard Definitions.

(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. If the verification is not successful, show as Figure 4.



1.6.2 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] on the screen, as shown in Figure 1 on the right.

B) Press related shortcut key on the keyboard.

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

(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.



1.6.3 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.

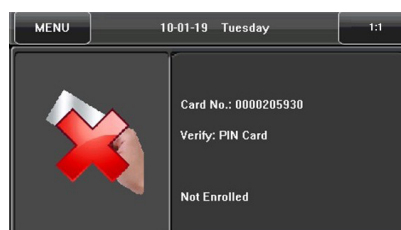
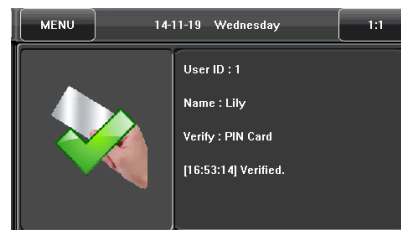
For the settings of these two verification modes, see 5.5 Log Settings.

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. Main Menu

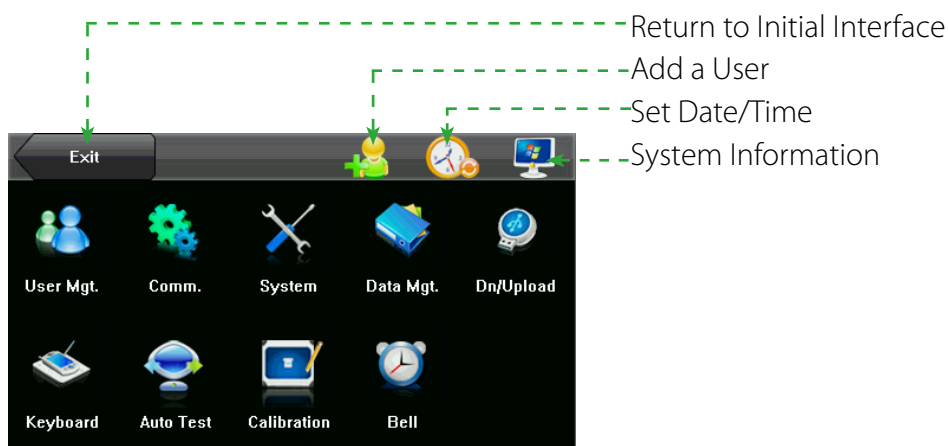
There are two types of rights respectively granted to two types of users: the ordinary users and administrators. Ordinary users are only granted the rights of facial, fingerprint, password or card verification, while administrators are granted the access to the main menu for various operations apart 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 **3.1.9 Modify User Rights**.

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, add, modify or delete the user information.

Comm.: Through this submenu, you can set related parameters for communication between the terminal and PC or the terminal and terminal, including the TCP/IP, WIFI, Webserver Set.

System: Through this submenu, you can set system-related parameters, including the General, Display, Fingerprint and Log Settings, to enable the 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 terminal, for example, Delete Transactions, All Data and Picture, Clear Administrator and Restore to Factory Settings.

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, Fingerprint, Voice, Keyboard and Time.

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

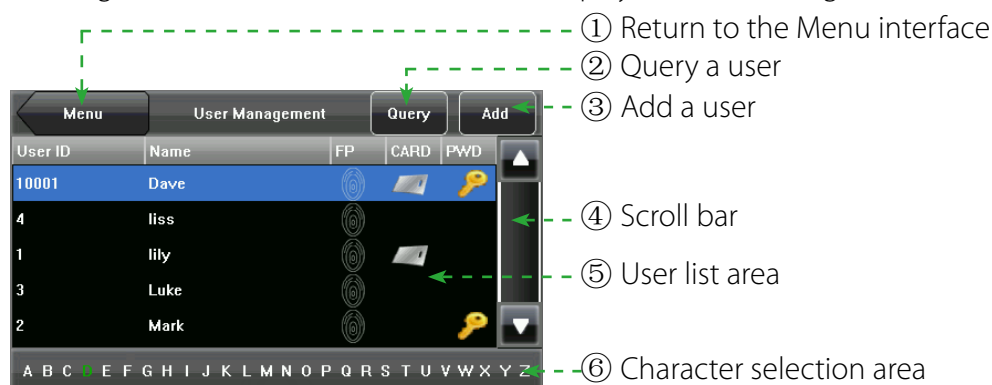
Bell: Through this submenu, you can set the alarm time and duration.

Note: When the user enable access, then you can make access setting, otherwise can't. For detail please see 5.2 Display.

3. User Management

Browse the user information, including the user ID, name, fingerprint, ID card, password, rights. Add, edit or delete the basic information of users.

Press [User Mgt.] 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 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 or 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 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.

The 'Add User' screen has a title bar with 'User Mgt.', 'Add User', 'Continue', and 'Save' buttons. Below the title bar are six input fields arranged in two columns. The left column contains 'User ID : 1', 'FP', and 'Card'. The right column contains 'Name', 'Password', and 'Role:User'.

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.

FP: Enroll a user's fingerprint and the terminal displays the number of enrolled fingerprints.

A user can enroll 10 fingerprints at maximum.

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

Card: Enroll a user card. The length is 10.

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 card 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.



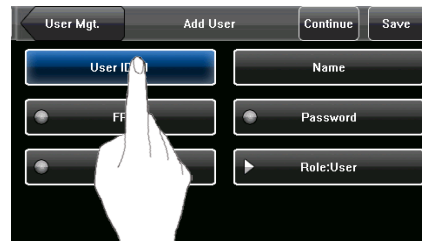
The ID card is an optional function. If you need this function, please consult our commercial representatives or fore-sale technical support personnel.

3.1.1 Entering a User ID

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

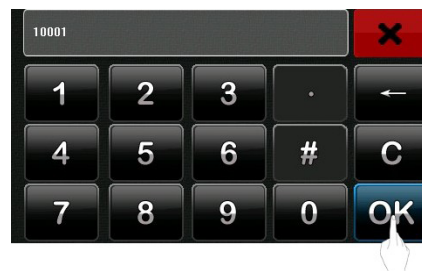
1. Press [User ID] on the Add User interface to display the user ID management interface, as shown in Figure 1 on the right:

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

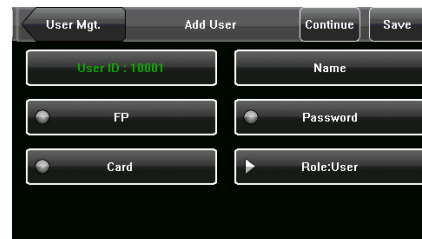


2. On the displayed keyboard interface, enter a user ID and press [OK] as shown in Figure 2 on the right. If a prompt message "The user ID already exists!" is displayed, enter another ID.

Tip: The 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.



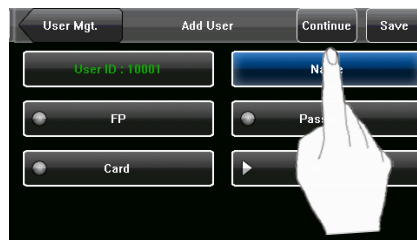
3. After the user ID is entered, an interface is displayed as shown in Figure 3 on the right. Press [Save] to save current information and return to the previous interface. Press [User Mgt.] to return to the previous interface without saving current information.



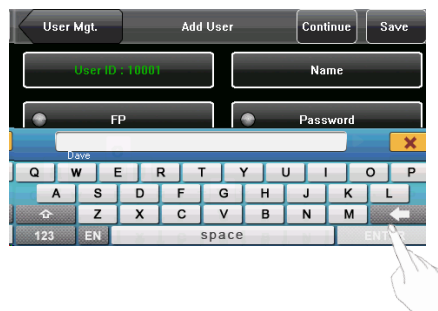
3.1.2 Entering a Name

Enter a user name through the keyboard.

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



2. On the displayed keyboard interface, enter a user name and press [Enter] as shown in figure 2 on the right. For details of operations on keyboard interface, see Appendix1 Text Input Instructions.
Tip: The terminal supports the 1- to 12-character names by default.



3. Press [X] to confirm, as shown in figure 3 on the right.



4. After the user name is entered, the interface is displayed as shown in figure 4 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.



3.1.3 Enrolling a Fingerprint

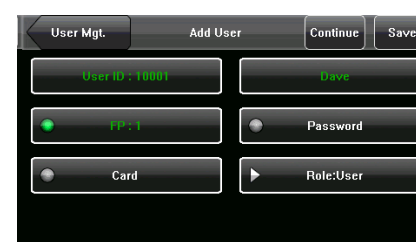
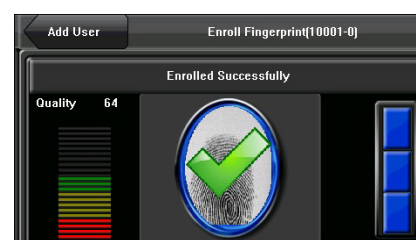
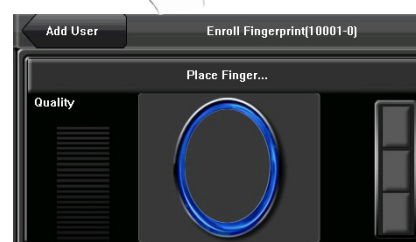
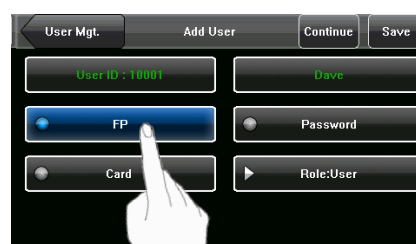
1. Press [Fingerprint] on the Add User interface to display the Enroll Fingerprint interface, as shown in Figure 1 on the right.

2. On the displayed Enroll Fingerprint Interface (as shown in the Figure 2 on the right), place your finger on the fingerprint collector properly according to the system prompts. 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 3 and 4 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.

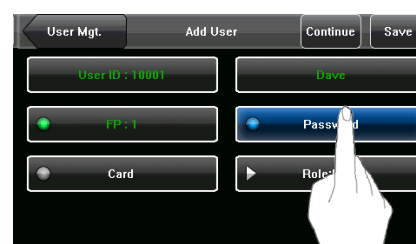


3.1.4 Enrolling a Password

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

2. On the displayed keyboard interface, enter a password and press [OK] as shown in Figure 2 on the right. Re-enter the password according to the system prompt and then press [OK].

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



3. After the password is entered, an interface is displayed as shown in Figure 3 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.



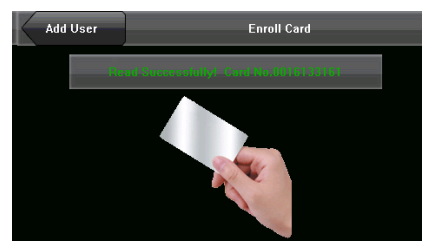
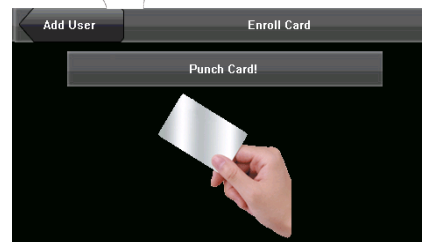
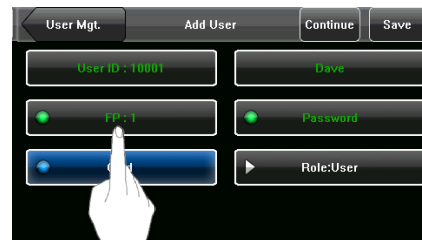
3.1.5 Enrolling an ID Card

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 Terminal".

3. If the card passes the verification, the 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.



3.1.6 Enrolling an Mifare Card

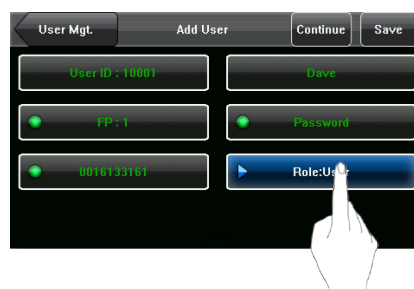
The 4.3 inches Facial & Fingerprint Recognition Series Products only favors Mifare card's being an ID card use. Use step and ID card to register an operation to accord.

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.

3.1.7 Modify User Rights

1. On the Add User interface, press [Role: User] to change the user as 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 User and Administrator. User are only granted the rights of facial, fingerprint, or password verification, while Administrator are granted the access to the main menu for various operations apart from having all the privileges granted to User.

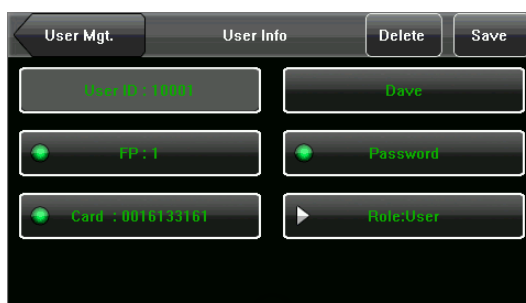


2. After the modification is done, the interface is as shown in Figure 2 on the right. Press [Save] to save current information and return to previous interface, press [User Mgt.] to directly return to previous interface without saving current information.



3.2 Edit a User

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

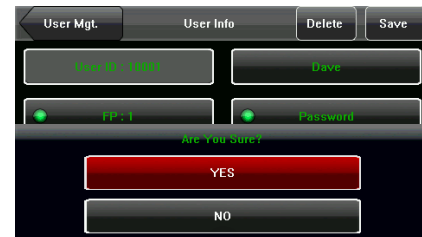
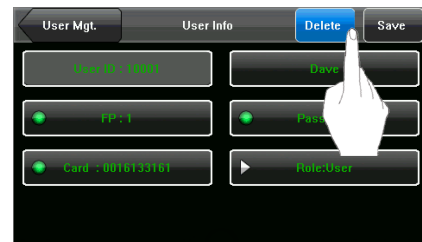


The User ID cannot be modified, and the other operations are similar to those performed to add a user. You can re-enroll your fingerprint and facial image, change your password and modify the management rights (Role).

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 (show as below), click [YES] to delete current user or [NO] to return to previous interface.



3.4 Query a User

To facilitate administrators to locate a user quickly from a large number of enrolled users, the 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.

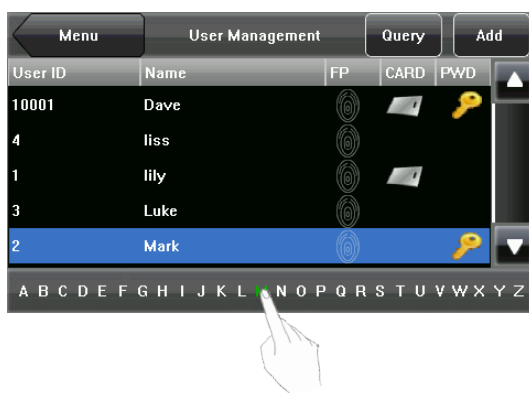


2. Enter the user ID on the displayed interface, and click [OK] (as shown in Figure 2 on the right) to locate the cursor to the desired user (as shown in Figure 3 on the right).



3.4.2 Query by Name

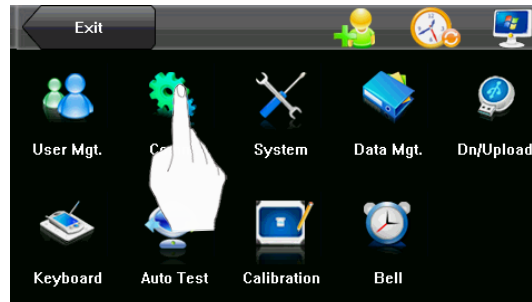
On the [User Mgt.] interface, enter the user name through the "Character Selection Bar" to locate the cursor to the desired user, as shown in the following figure:



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 terminal and PC, including the IP Address, Gateway, Subnet Mask, Baud Rate, Device ID, and Comm Key.



4.1 Network Settings (TCP/IP)

When the 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.

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 and can be changed as required.

DNS Server: The DNS Server is 0.0.0.0 by default and can be changed as required.

Device ID: This parameter is used to set the ID of device from 1 to 254.

Comm Key: To enhance the security of attendance data, you can set a password for the connection between the terminal and PC. Once the password is set, you can connect the PC with the 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 terminal. Otherwise, the connection is unsuccessful. 1- to 6- digit passwords are supported.

4.2 WIFI Option ★

With the WIFI function, our product can connect to the network in wireless mode for data transmission.

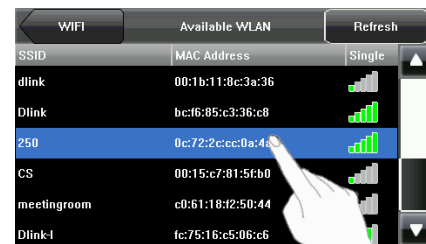
The WIFI function is configured as follows:

1. Available WLAN

1) Press the button Available WLAN, then the device will searching for WIFI networks automatically.




2) Select and click WIFI name to pop-up the Input password box.



3) Input the correct password, and then click [Save] button to connect the select WIFI. You can see the 2) WIFI Configuration



4) After the connection is successfully set up, a green icon  is displayed on the initial interface.

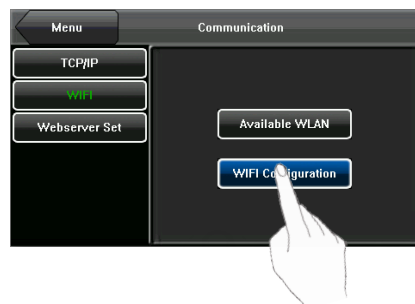
The connection status is also displayed in the Cont. Info. of the system information.



2. WIFI Configuration

On the WIFI Configuration tab page, you can configure the SSID and password of the current or recently connected WIFI network.

Press the button WIFI Configuration to configure the WIFI.

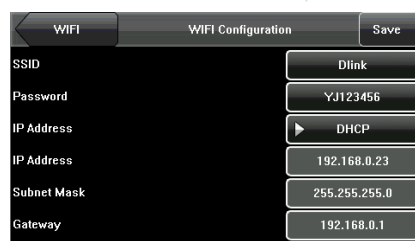


SSID: SSID to be connected to wireless network. (There is difference between small letter and capital letter.)

IP address: In 802.11 wireless networks, there is DHCP. Or enter IP interface to input correct IP address, subnet mask and Gateway.

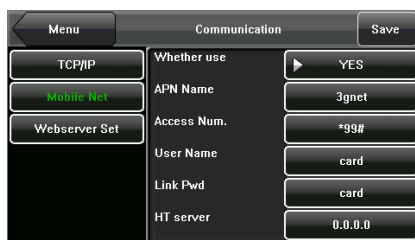
Subnet Mask: The subnet mask is 255.255.255.0 by default and can be changed as required.

Gateway: The gateway is 0.0.0.0 by default and can be changed as required.



4.3 Mobile net ★

When the equipment is in the Dial-Up Network, making sure the device is in the coverage of 3G or WCDMA signal, and it is must know of the APN name and access number and so on.



Whether use: whether to enable access to a mobile network.

APN: Access Point Name, used to identify 3G / WCDMA types of business.

Dial Number: The access number of 3G / WCDMA business.

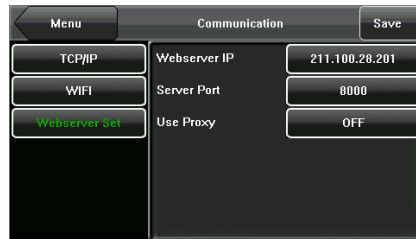
User Name and Password: used to check whether a user has the rights to access a network.

Heartbeat Server: used to test the connection status of the mobile network. The terminal sends ICMP packets to the heartbeat server at regular interval to test whether the terminal is online. When the terminal is offline, the device automatically performs dial-up connection. Therefore, when configuring the heartbeat server, ensure that the heartbeat server can be successfully pinged and is online stably in a long term.

Note: Generally, you can set the address of the heartbeat server to the address of the ADMS server.

4.4 Weerver Setting

This submenu is used to connect the Webserver-related settings, such as Webserver IP address, port settings, and whether to enable proxy settings.



WebServer IP: You can access a website using a domain name in the format of http://, Or enter an IP address for website access.

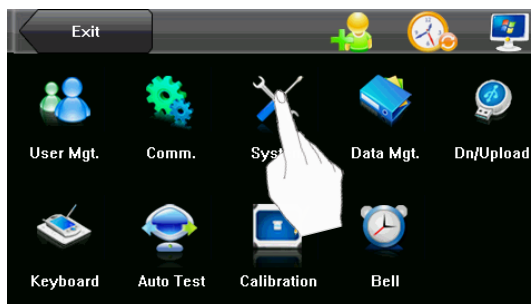
Server port: Port used by Webserver.

Use Proxy: When you enable the proxy function, set the IP address and port number of the proxy server. This option indicates whether to use a proxy IP address. You may choose to enter the proxy IP address or the server address for Internet access, whichever you like.

After the ADMS server is connected, log in to the Web server, access the device, and transmit data. For details, see the ADMS User Manual.

5. System Configuration

Through the System menu, you can set system-related parameters, including the General parameter, Display parameter, Fingerprint parameter and Log Settings parameter and so on, to enable the terminal to meet user requirements to the greatest extent in terms of functions and display.



5.1 General



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

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

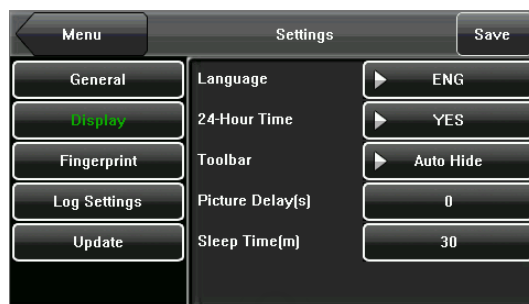
Keyboard Clicks: This parameter is used to set whether to generate beep sound in response to every keyboard touch. Select "ON" to enable the beep sound, and select "OFF" to mute.

Voice Prompts: This parameter is used to set whether to play voice prompts during the operation of the 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.

Lock 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 terminal will be shut down in three seconds.

5.2 Display



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

24-Hour Time: 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: This parameter is used to display style of the shortcut keys on the initial interface. It can be set to “Auto Hide” and “Unhide”. By selecting “Auto Hide”, you can manually display or hide the toolbar. By selecting “Unhide”, you can permanently display the toolbar on the initial interface.

Picture Delay (S): This parameter is used to set the picture cycle interval, the default value is 0 (means not enable this function). The value scope: 3 — 999 seconds).

Sleep Time (S): This parameter is used to specify a period after which the terminal is put in sleep mode if not operated within this period. You can bring up the terminal from sleep by pressing any key or touching the screen.

5.3 Fingerprint



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

The recommended thresholds are as follows:

(FRR)	(FAR)	Threshold	
		1: N	1:1
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.

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 Log Settings



Log Alert: When the available space is insufficient to store the specified number of attendance records, the 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 Work Code.

5.5 Update

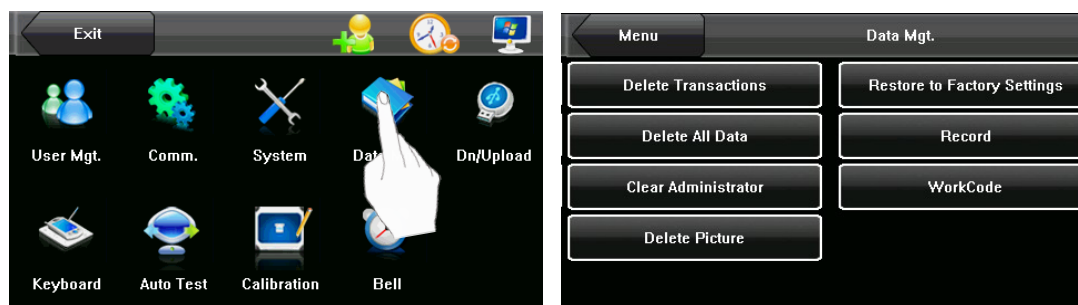
You can upgrade the firmware program of the terminal by using the upgrade file in the USB disk through this parameter.



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 terminal, for example, deleting the attendance record, all data and promotional pictures, purging management rights and resetting the 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 terminal. (For details on how to upload promotional pictures, see "5.4 Upload Picture")

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

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

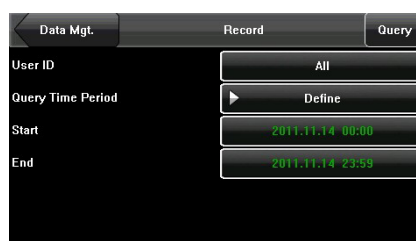
WorkCode: Add, edit or delete the work codes of employees.



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

6.1 Query a Record

After check-in successfully, the employee's attendance records are saved in the 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.

Date	User ID	Att Log
11/14		Total Record:20
	10001	14:29 14:25 14:24 14:23 14:22 14:22 14:13 14:08 14:07 14:05 14:05 14:05 13:50 13:49 13:48 13:48 13:48 13:47 13:46 13:46

User ID	Name	Time	Verify	State
10001	Dave	11-14 14:29	Fa	Check-In
10001	Dave	11-14 14:25	Fa	Check-In
10001	Dave	11-14 14:24	Fa	Check-In
10001	Dave	11-14 14:23	Fa	Check-In
10001	Dave	11-14 14:22	Fa	Check-In
10001	Dave	11-14 14:22	Fa	Check-In
10001	Dave	11-14 14:13	Fa	Check-In
10001	Dave	11-14 14:08	Fa	Check-In

After setting the query conditions, press [Query] and the records that meet the specified query conditions will be displayed on screen. As shown in Figure 2 on the right.

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 10001 on November 14, 2011. As shown in Figure 3 on the right.

6.2 Work Code

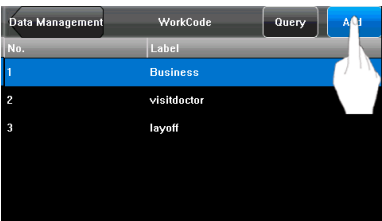
Employees' salaries are subject to their attendance records. Employees may be engaged in different types of work which may vary with time periods. Considering the salaries vary with work types, the terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate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

1. Add a work code

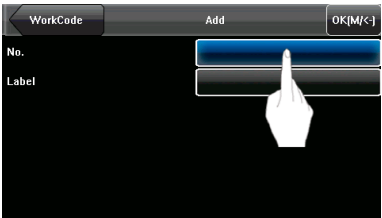
(1) Press [Add] on the WorkCode interface (as shown in Figure 1 on the right) to display the [Add] interface.

No.: A digital code of the work code.

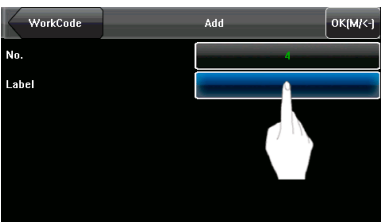
Label: The meaning of the work code.



(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 Input Instructions)



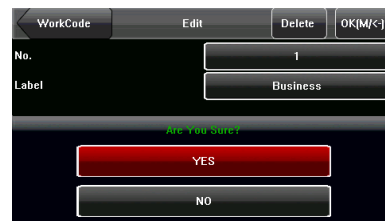
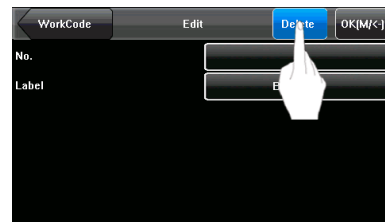
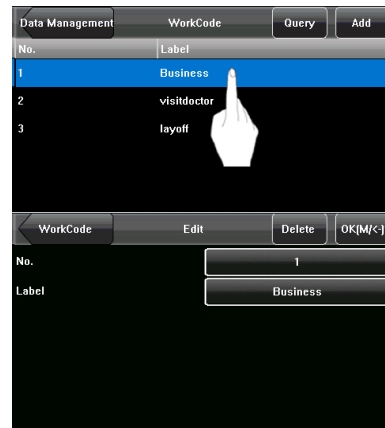
2. Edit and delete a work code

(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".

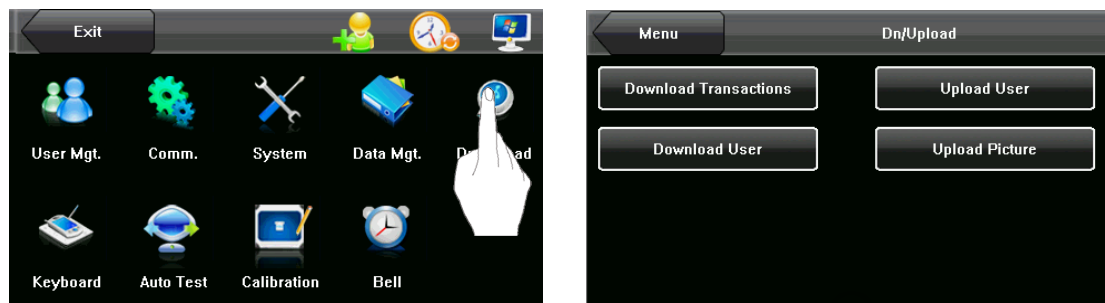
(3) To delete this work code, press [Delete] (as shown in Figure 3 on the right).

(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).



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 terminal to a USB disk.

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

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

Upload Picture: Upload the JPG documents with "ad_" as initial letters of document names stored in a USB disk to the terminal. After the upload, these pictures can be displayed on the initial interface of the 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 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 a shortcut key in the list to display the shortcut key editing interface.

3. Edit the functional introduction of interface

Key: Options include: F1–F6.

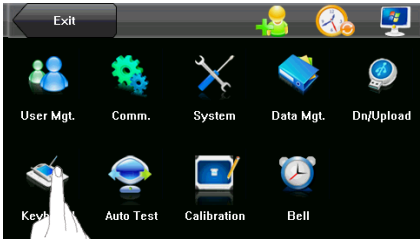
Function: You can set the functions of different shortcut keys, such as Status, 1:1, Work code and Undefine.

1:1: Set the verification type as 1:1, as shown in Figure 3 on the right.

Label: Include Check-In, Check-Out, Break-Out, Break-In, OT-In, OT-Out. The setting interface is shown in Figure 1 on the right.

When setting the attendance status shortcut keys, you can also set the “Auto Switch” parameter. When “Auto Switch” is enabled, the terminal automatically switches the attendance status at the specified time. The “Auto Switch” setting interface is as shown in Figure 2 on the right.

The (work code) shortcut key setting interface is as shown in Figure 3 on the right.



Keyboard			
Key	Function	Code	Label
F1	Status	0	Check-In
F2	Status	1	Check-Out
F3	Status	2	Break-Out
F4	Status	3	Break-In
F5	Status	4	OT-In
F6	Status	5	OT-Out

Keyboard		Edit	Save
Key	F1		
Function	1:1		

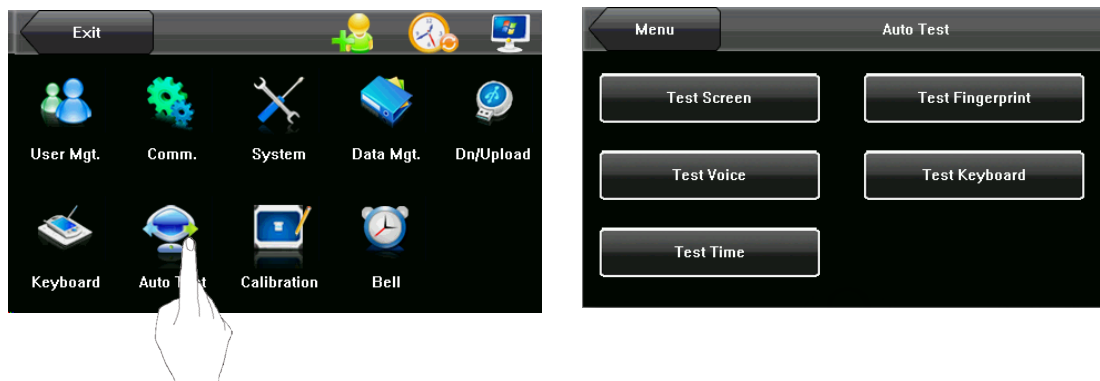
Keyboard		Edit	Save
Key	F1		
Function	Status		
Code	0		
Label	Check-In		
Auto Switch	OFF		

Keyboard		Edit	Save
Key	F1		
Function	Status		
Code	0		
Label	Check-In		
Auto Switch(Sunday~Saturday)	ON		
00:00 00:00 00:00 00:00 00:00 00:00 00:00			

Keyboard		Edit	Save
Key	F1		
Function	Shortcut Key		
Code			
Label			

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 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 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 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.

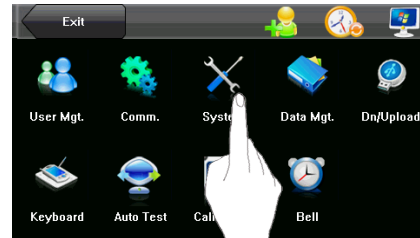
Fingerprint Test: The terminal automatically tests whether the fingerprint collector works properly by checking whether the fingerprint images are clear and acceptable. When the user places his/her finger in the fingered guide, the collected fingerprint image is displayed on the screen in real-time.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

Time Test: The 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.

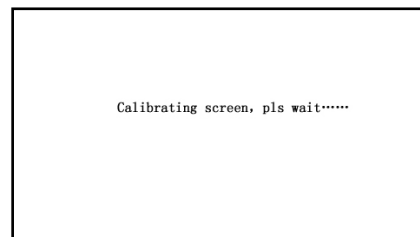
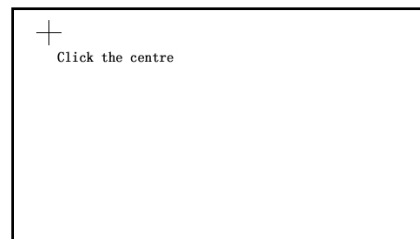
10. Screen Calibration

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 terminal. You can set the alarm time and duration for ringing the bell based on your requirements, so that the terminal will automatically play the selected ring tone and triggers 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. As shown in Figure 3 on the right.

Note: You only can add 15 bells.

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

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

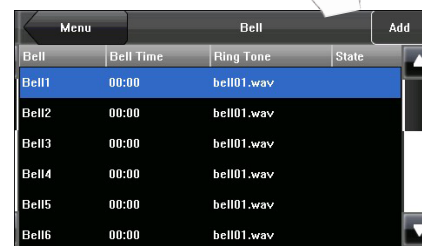
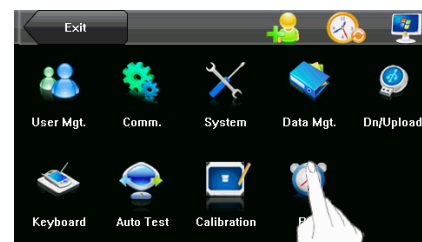
Ring Tone: This parameter is used to set the bell ring tone.

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, external ringing or Int&Ext Bell. For internal ringing, the ring tone is played by the loudspeaker of the terminal. For external ringing, the ring tone is played by an external electric bell that is wired with the terminal.

Notice: Only some machines have external ringing options.

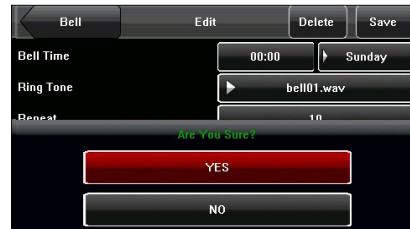


The alarm sounds of the bell and the access control cannot be concurrently generated by the loudspeaker of the FFR terminal or externally connected relay. Therefore, when the bell is set to the external ringing mode, the access limit alarm will automatically change to the internal ringing mode, and vice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

12.1 Set Date/Time

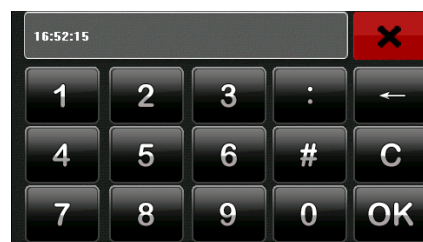
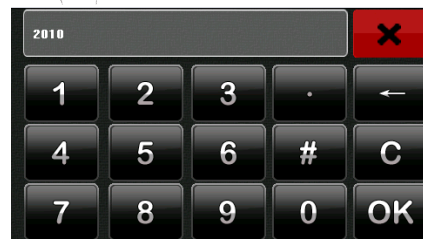
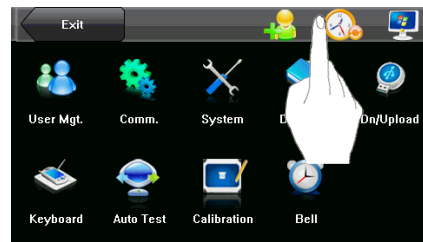
The date and time of the terminal must be set accurately to ensure the accuracy of attendance time.

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 the numbers on the screen, 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.



12.2 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 terminal supports the DST function to adjust forward on hour at xx (Hour): xx (Minute) xx (Day) xx (Month) and backward one hour at xx (Hour):

xx (Minute) xx (Day) xx (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. As shown in Figure 1 on the right.
3. Press [DST] on the time setting interface to display the DST setting interface. As shown in Figure 2 on the right.

4. Set the following parameters on the DST setting interface, as show in figure 3 on the right.

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

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

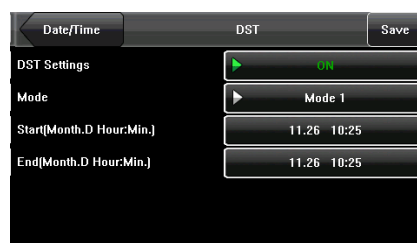
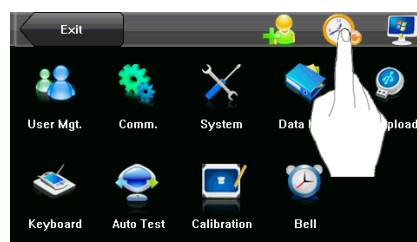
In Mode 1 (the default mode), the DST is set in the “Month-Day Hour: Minute” format. In Mode 2, the DST is set in the “Month-Week-Day Hour: Minute” format. As shown in Figure 1 on the right.

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, 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.

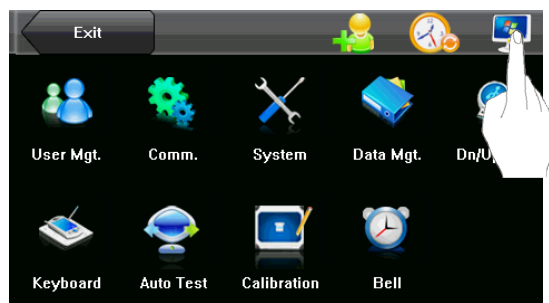
For example, adjust the clock forward one hour at 08: 00 on April 1st and backward one hour at 08: 00 on October 1st. As shown in Figure 2 on the right.

5. After setting the DST, press [Done] to return to the time setting interface. As shown in Figure 3 on the right. 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.



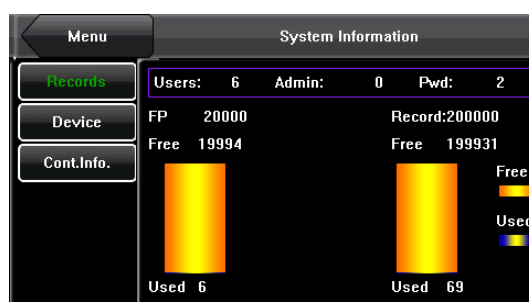
13. System Information

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



13.1 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:



13.2 Device

The Device name, serial number, version information, vendor and date of manufacture are displayed on the Device interface.



13.3 Cont. Info

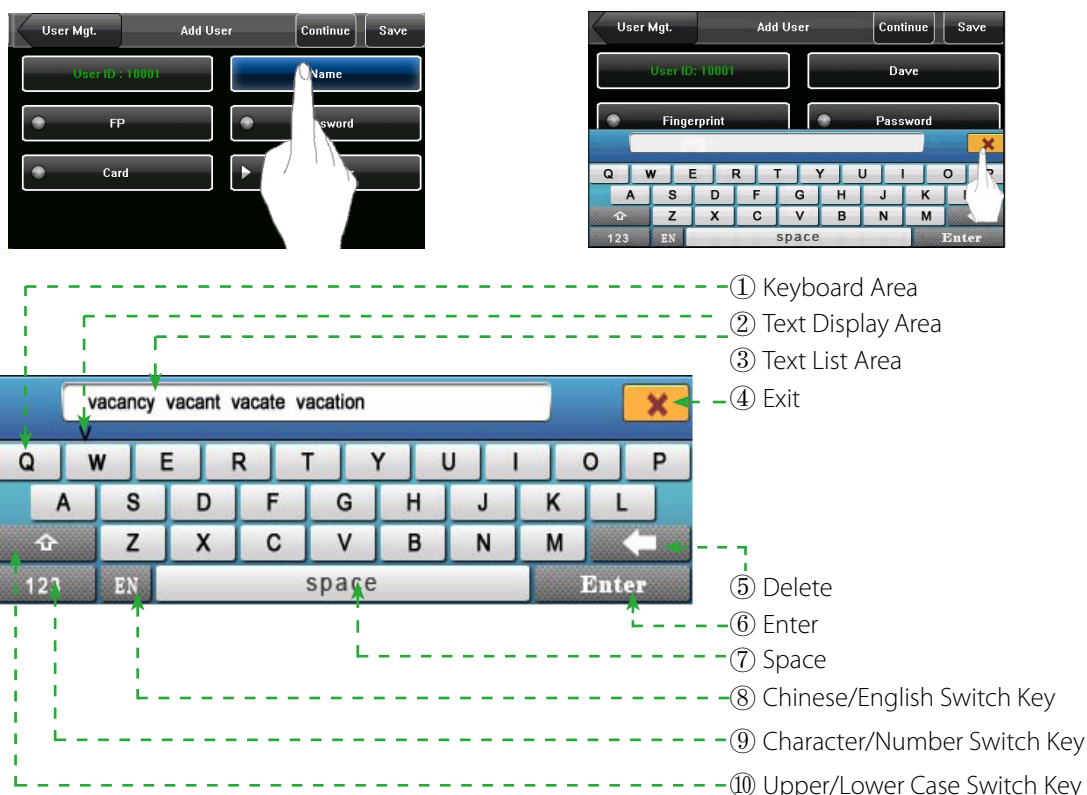
The Power Info interface displays the current Power supply and Battery Info. Show as below:



Appendix

Appendix 1 Text Input Instructions

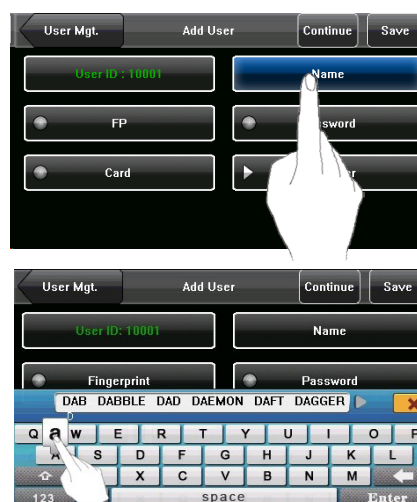
The terminal supports the input of Chinese and English characters, numbers and symbols. Press related button to input text. For example, press [Name] to display the text input interface, as shown in the following figure:



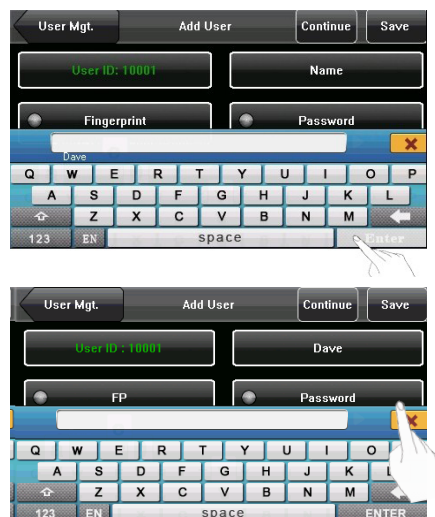
To enter a name, proceed as follows:

1. Press [Name] on the [Add] interface, as show in figure 1 on the right.

2. Enter the characters of name, as shown in Figure 2 on the right. Press [space] or [Enter] to input the character.



3. After finishing the entry of name, press [Enter] to confirm, as shown in figure 3 on the right, and then press [X] to exit keyboard interface and return to the previous interface, as show in figure 4 on the right.



Appendix 2 USB Host

Fingerprint device may be used as USB host to exchange data with external U-disk. The data transmission speed is quick, the traditional fingerprint device only supports the RS232, RS485 or Ethernet way for data transmission, when as a result of physical condition limit, data quantity big, and the data transmission cost quite long time. But the USB data transmission is quicker than any of the former transmission mode, may complete downloading data by U disk in a short period of time, like this greatly enhances the efficiency.

The operational steps of USB Host equipment please refer to 7.USB Disk Management.

Appendix 3 State Auto Switch

The system supports six work states: Check in, Check out, Break out, Break in, Overtime in (OT-In), and Overtime out (OT-Out). The state needs to be modified manually, that is, you can switch to the desired work state by pressing the corresponding button. To decrease the manual operations, the device menu provides a state Auto Switch option. At the time specified by a user, the device automatically switches the state. The current state is displayed on the initial interface.



After the user sets the state Auto Switch in a week, the system checks whether the state needs to be switched by minutes. When the user saves the settings, the saving operation of the same day or same time does not take effect.

Appendix 4 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:

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.

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.

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.

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 5 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.