

3 Inches Facial & Fingerprint Recognition Series Product User Manual

Version: 3.0

Date: Nov. 2011

About This Manual

This document introduces the user interface and menu operations of the 3 Inches Facial & Fingerprint Recognition Series product. For installation, please refer to the **Installation Guide** or **Quick Guide**.

Table of Contents

1. Instructions for Use	1
1.1 Standing Position, Posture and Face Expressions.....	1
1.2 Enrollment Facial Expressions	1
1.3 Finger Placement★	2
1.4 Use of the Touch Screen.....	3
1.5 Touch Operations.....	4
1.6 Appearance of Device.....	5
1.7 Main Interface	7
1.8 Verification Modes.....	8
1.8.1 Fingerprint Verification★	8
1.8.2 Face Verification.....	10
1.8.3 Password Verification.....	11
1.8.4 ID Card Verification★	12
1.8.5 Combination Verification★	12
2. Main Menu	14
3. Add User	16
3.1 Entering a User ID	16
3.2 Entering a Name.....	17
3.3 Enrolling a Fingerprint★	18
3.4 Enrolling a Password	19
3.5 Enrolling an ID card★	19
3.6 Enrolling a Face	20
3.7 Entering a Group No. ★	21
3.8 Modifying User Rights.....	21
3.9 Enroll Photo★	22
3.10 User Access Settings★	23
4. User Management	25
4.1 Edit a User	25
4.2 Delete a User	26
4.3 Query a User.....	27
5. Communication Settings	28
5.1 Network Settings.....	28
5.2 Serial Port Settings	30
5.3 Wiegand Output★	30
5.3.1 Wiegand 26-bits Output Description	30

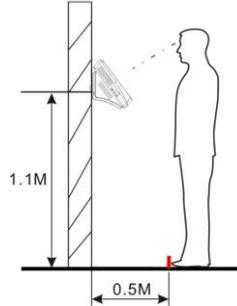
5.3.2 Wiegand 34-bits Output Description	31
5.3.3 Customized Format.....	32
5.4 Wiegand Input★	34
6. System Settings	35
6.1 General Parameters.....	35
6.2 Interface Parameters	37
6.3 Fingerprint Parameters★	38
6.4 Face Parameters	39
6.5 Log Settings	40
6.6 Shortcut Definitions.....	41
6.7 Access Settings★	42
6.7.1 Time Zone Setting	43
6.7.2 Holiday Setting	43
6.7.3 Group Time Zone Setting	44
6.7.4 Unlock Combination Setting.....	46
6.7.5 Access Control Parameter	48
6.7.6 Duress Alarm Parameters	49
6.7.7 Anti-Passback Setting	49
6.8 Update	50
7. Data Management	51
7.1 Query Record.....	51
7.2 Work Code	52
8. Date/Time Setting	54
8.1 Set Date/Time	54
8.2 Bell Setting★	54
8.3 Daylight Saving Time (DLST)★	56
9. Auto Test.....	57
10. USB Disk Management	59
11. System Information	60
12. Appendix.....	61
12.1 T9 Input Instructions	61
12.2 USB Pendrive	62
12.3 9-Digit Enrollment Number	62
12.4 Introduction of Wiegand★	63
12.5 Photo ID Function★	65
12.6 Work Code ★.....	66

12.7 Multi-combination Authentication Mode★66
12.8 Anti-Pass Back★69
12.9 Statement on Human Rights and Privacy71
12.10 Environment-Friendly Use Description72

1. Instructions for Use

1.1 Standing Position, Posture and Face

1. Recommended Standing-distance from
For users 5-6 feet tall (1.55m-1.85m) we recommend
When viewing your image on the device display
bright. Step closer if your image appears too dark.

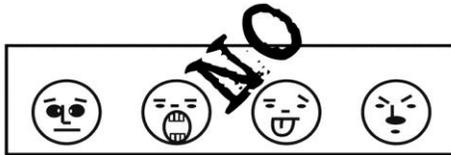


Expressions

Device:

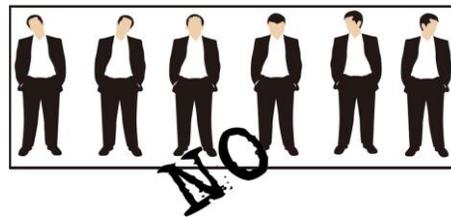
standing about 2 feet (0.5m) from the wall.
window, step away if your image appears too

2. Recommended Facial Expressions vs. Poor



Expressions:

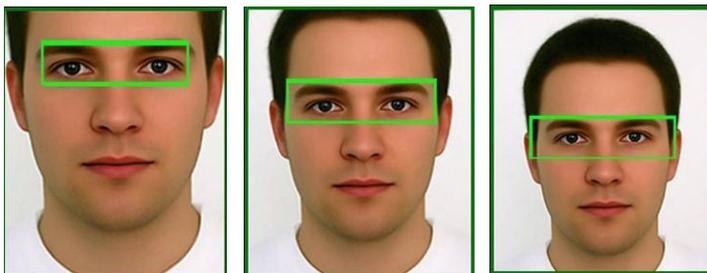
3. Recommended Posture (Pose) vs. Poor Posture (Pose):



 **Note:** During enrollment and verification, try to have a relaxed unstrained facial expression and stand upright.

1.2 Enrollment Facial Expressions

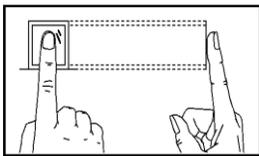
During the enrollment, position your head so that your face appears in the center of the device display window, and follow the voice prompts "Focus eyes inside the green box". The user needs to move forward and backward to adjust the eye position during the face registration. **The enrollment face expressions are as follows:**



1.3 Finger Placement★

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

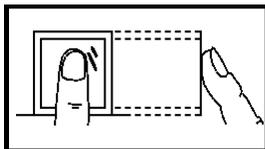
1. Proper Finger Placement:



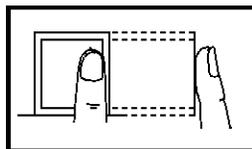
The finger must be flat to the surface and centered on the fingerprint sensor.

2. Improper finger placement:

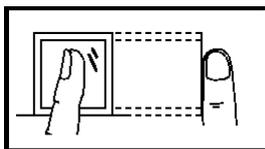
Not flat to the surface



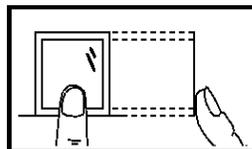
Off-center



Slanting



Off-center



i

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 operation. We shall reserve the right of final interpretation and revision of this document.

1.4 Use of the Touch Screen

Touch the screen with one of your fingertips or the 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 a screen calibration through the following menu operations. Press **[Menu]** -> **[Auto Test]** -> **[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 will automatically returns to the **Auto Test** menu. Press **[Exit]** to return to the **Menu** interface. For details, see the description in [9. Auto Test](#).

A 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

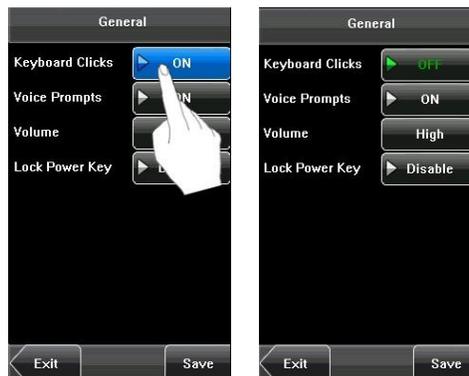
1. Enter Numbers: Press the [User ID] key. The system will automatically display the number input interface. After entering the user ID, press [OK] to save or press [X] to cancel and return to the previous interface.



2. Enter Text: Press the [Name] key. The system will automatically display 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 will automatically switch to another value of this parameter.

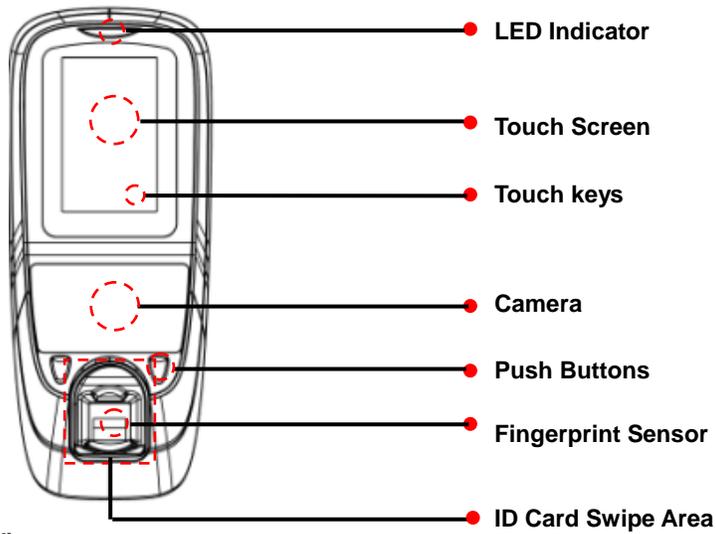


☺ **Note:** The Enroll Fingerprint, User Access and 1: G are optional functions not available on all machines.

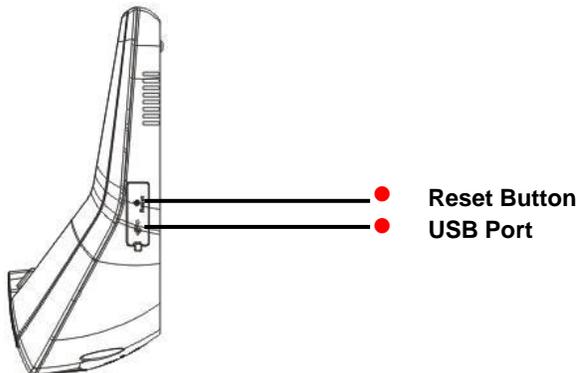
1.6 Appearance of Device

1. Type 1

(1) Front View

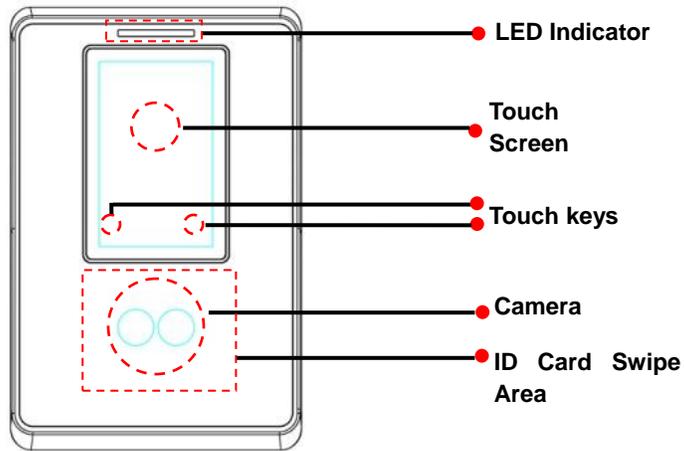


(2) Side View

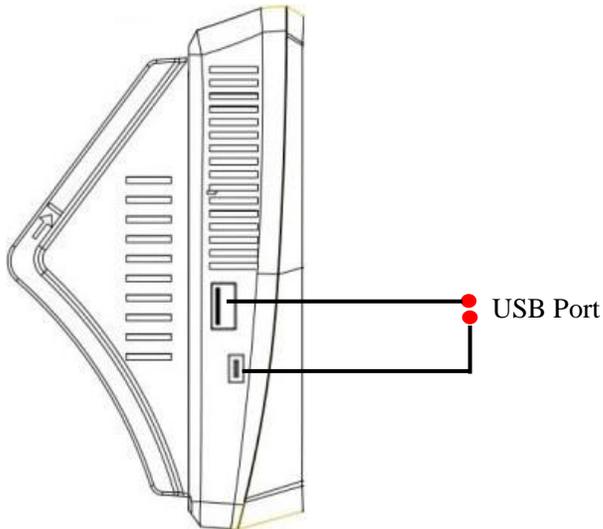


2. Type 2

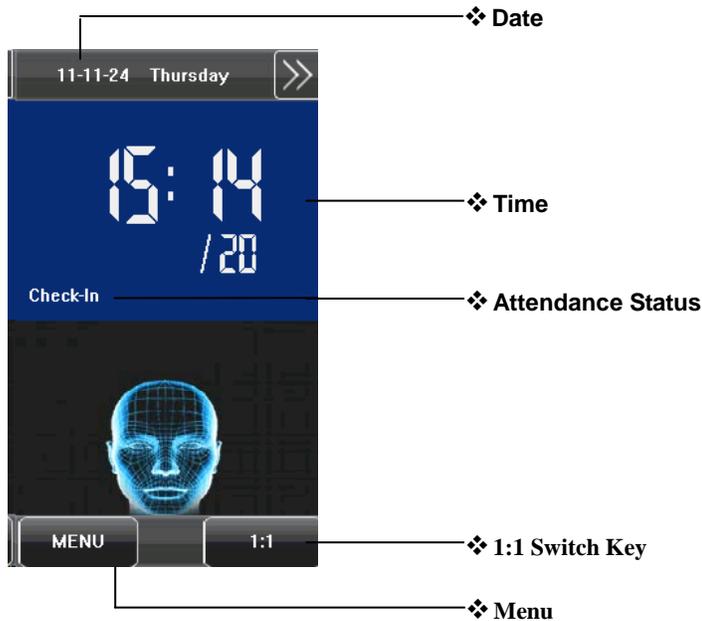
(1) Front View



(2) Side View



1.7 Main Interface



① **Date:** The current date is displayed.

② **Screen Shortcut Keys:** Press these shortcut keys to display the attendance status. Users can customize the function of each shortcut key. For details, see [6.6 Keyboard Definitions](#).

③ **Time:** The current time is displayed. Both 12-hour and 24-hour time systems are supported.

④ **Attendance Status:** The current attendance status is displayed.

⑤ **1:1 Switch Key:** By pressing this key, you can switch to the 1:1 verification modes, and enter the digital input interface.

⑥ **Menu:** You can enter the main menu by pressing this key.



Note: 1. The Enroll Fingerprint, User Access, Door Bell Button and 1:1 Switch Button are optional functions. These functions are not available on all machines.

2. The 1: G is an optional function. If you need this function, please consult our commercial representatives or pre-sale technical support personnel.

1.8 Verification Modes

1.8.1 Fingerprint Verification★

1. 1: N Fingerprint Verification

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

(1) To enter the fingerprint verification mode: The device automatically distinguishes between face and fingerprint verification.

Just press a finger on the collector to start the fingerprint authentication mode.

(2) Press your finger on the fingerprint sensor by using the proper finger placement. For details, see [1.3 Finger Placement](#).

(3) If the verification is successful, the device will prompt “Verified”.

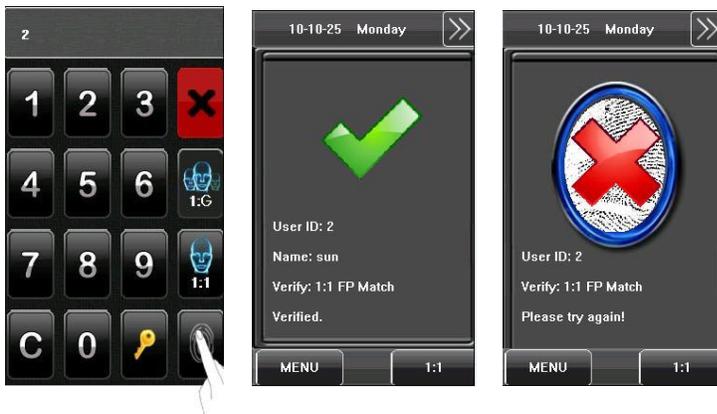
(4) If the verification is not successful, the device will prompt “Please try again”.



2. 1:1 Fingerprint Verification

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

- (1) Press [1:1] on the screen or [1:1] button to enter the 1:1 fingerprint recognition mode.
- (2) Enter User ID or Group No., then press the "Fingerprint" icon to enter the 1:1 fingerprint recognition mode. If the prompt "Unregistered user!" is displayed, the user ID does not exist.
- (3) Press your finger on the fingerprint sensor using proper finger placement. For details, see [1.3 Finger Placement](#).
- (4) If the verification is successful, the device will prompt "Verified", otherwise the device will prompt "Please try again".



1.8.2 Face Verification

1. 1: N Face Verification★



The terminal collected by the terminal.

(1) The device fingerprint

(2) Compare the face Standing Position.

Compare interface camera, with the the right.

(3) If the verification

as shown in Figure 2 on the right will be displayed.



compares the current face image camera with all face data on the

automatically distinguishes face and verification.

in a proper way. For details, see 1.1 Posture and Face Expressions.

display with the current image collected by the image shown in

is successful,



Figure 1 on

an interface

2. 1:1 Face Verification

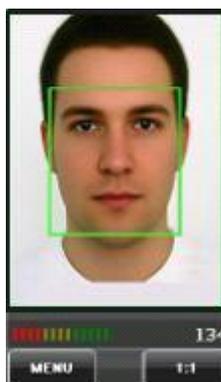
In the 1:1 face verification mode, the device compares the current face collected through the camera with that in relation to the user ID entered through the keyboard. Adopt this mode only when it is difficult to recognize the face.

(1) Press [1:1] on the screen to enter the 1:1 recognition mode.

(2) Enter User ID, then press the "1:1 Face" icon to enter 1:1 face recognition mode. If the prompt "Unregistered user!" is displayed, the user ID does not exist.

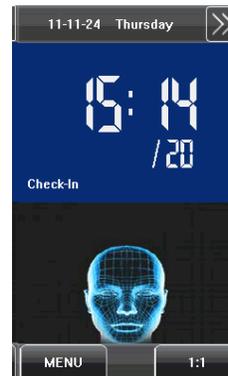
(3) Compare the face in Expression.

(4) If the verification is interface if the verification



a proper way. For details, see 1.1 Standing Position, Posture and Face

successful, the device will prompt "Verified". The system will return to the main is not passed within 20 seconds.



3. 1: G Face

When you open the 1: G facial verification. For The current group No. (a

Verify detail valid



Verification★

function, then you can make a 1:G please see 6.5 Log Settings group number is 1-5) is displayed on

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

(1) Press [1:1/G] on the screen to enter the 1: G recognition mode.

(2) Enter user Group No. and then press the "1: G" icon (shown as following figure 1) to enter 1: G facial recognition mode.

(3) Compare the face in a proper way. For details, see [1.1 Standing Position, Posture and Face Expressions](#). Current Group No.



is displayed on the



Note: Check

1.

(4) If the

3.



Note: The 1:

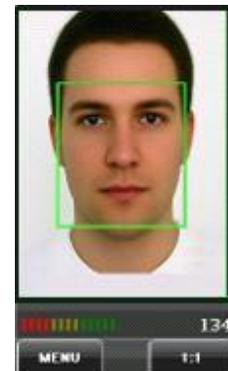
optional function.



comparison interface, shown as figure 2 below.

if you are in the current group; if not, return to Step

verification is successful, shown as following figure



G Face group is an

Some machines have this

function and some do not. Face group function is unchecked by factory default. Users can set it in **System--Log Settings--1:G**. Open it to verify this function.

1.8.3 Password Verification

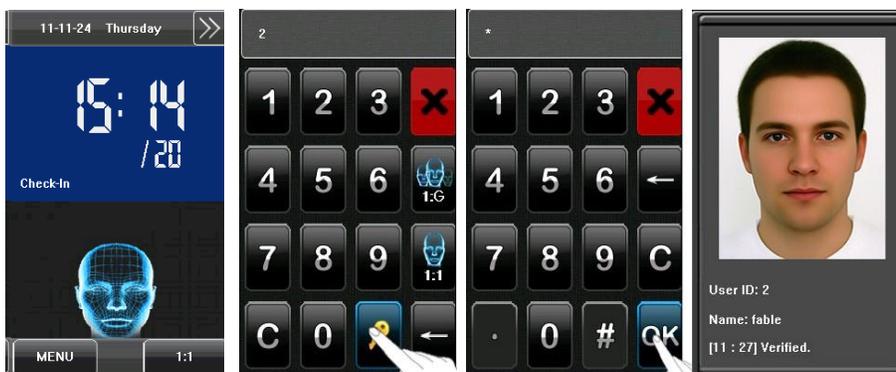
In the password verification mode, the device compares the password entered with that associated with the user ID.

(1) Press [1:1] on the screen or [1:1] button to enter the password verification mode.

(2) Enter the user ID and press the "Key" icon to enter the password verification mode. If the prompt "Unregistered user!" is displayed, the user ID does not exist.

(3) Enter the password and press the "OK" icon to start the password comparison.

(4) If the verification is successful, the device will prompt "Verified", otherwise the device will prompt "Verify fail" and return to the password input interface.



1.8.4 ID Card Verification★

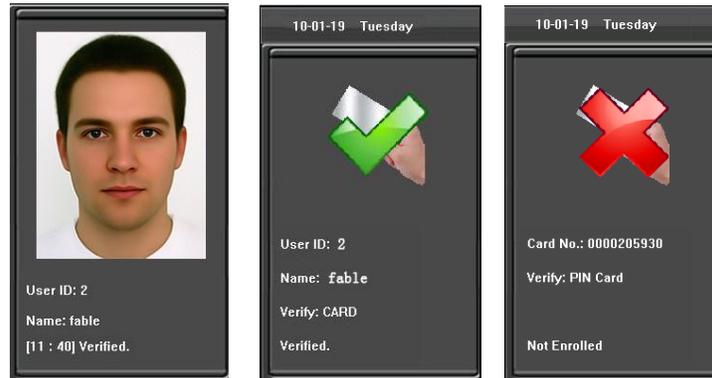
Only the products with a built-in ID card module support the ID card verification. The products with a built-in ID card module support the following two verification modes:

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.

1. ID Card Only

1. Swipe your ID card on the card swipe area in the proper manner. For the card swipe area, see [1.6 Appearance of Device](#).
3. If the verification is successful, the device will prompt “Verified”.
4. If the verification is not successful, the device will prompt “Not Enrolled”.



Note: (1) The machines that have Photo ID function, successful verification interface is shown as figure 1 above;

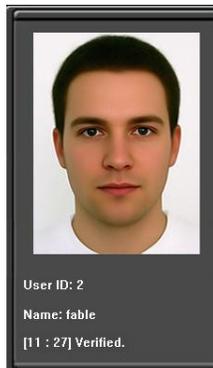
(2) The machines that don't have Photo ID function, successful verification interface is shown as figure 2 above.

2. ID + Facial Verification

(1) Swipe your ID card properly at the swiping area to

(2) Compare the face in a proper way. For details, see [Expressions](#)

(3) If the verification is successful, an interface as displayed. The system will return to the main interface if seconds.



enter the 1:1 facial verification mode.

[1.1 Standing Position, Posture and Face](#)

shown in Figure 3 on the right will be the verification is not passed within 20

1.8.5 Combination Verification★

The device supports up to 20 verification modes, including FACE&PIN/FP/RF/PW、FP&PW、FP&RF、FACE&FP、FACE&PW、FACE&RF、FP、PW、RF、FACE&PIN、FP/RF、PW/RF、FP/PW、PW&RF、PIN&FP、FP&PW&RF、PIN&FP&PW、FP&RF/PIN、FACE&FP&RF、FACE&FP&PW etc. For details, please refer to [Appendix 8 Multi-combination Authentication Mode★](#)



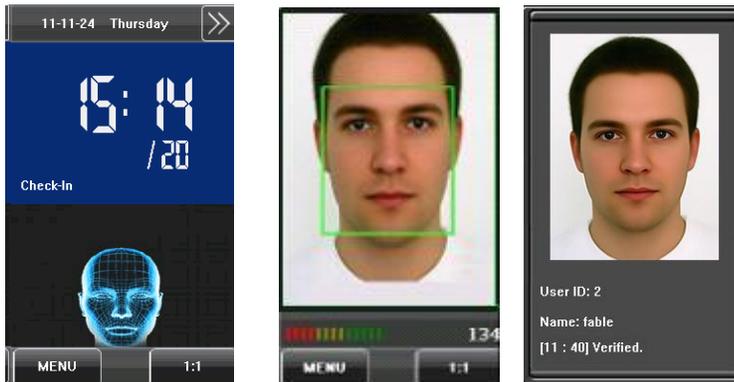
Note: RF means ID card verification. Only the products with the built-in ID card module support the ID card verification.



Here is the combination verification operation; we will use the FACE&FP verification for an example.

If you verify the fingerprint first and then the face, the operations are as follows:

- (1) The default main interface is the fingerprint verification mode, see the figure below.
- (2) Press your finger on the fingerprint sensor using proper finger placement. For details, see [1.3 Finger Placement](#).
- (3) If the verification is successful, the device will enter the 1:1 face recognition mode. Compare the face in a proper way. For details, see [1.1 Standing Position, Posture and Face Expression](#).
- (4) If the verification is successful, the device will prompt “Verified”. The system will return to the main interface if the verification is not passed within 20 seconds.

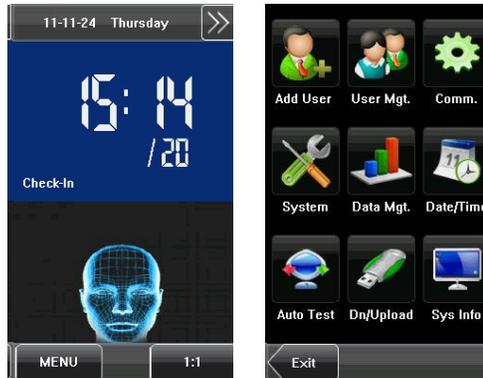


Otherwise, the FACE&FP combination verification can perform such as FACE (1: N) + FP, PIN + FACE (1:1) + FP, PIN + FP (1:1) + FACE etc. The operation is similar to the procedure previously introduced.

2. Main Menu

There are two types of rights respectively granted to two types of users: the **Ordinary users** and the **administrators**. Ordinary users are only granted the rights of face, fingerprint, password or card verification, while administrators are granted 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:



The main menu includes nine sub menus:

Add User: Through this submenu, you can add a new user and input the information on the device, including the user ID ★, name, fingerprint ★, face, card ★, password, rights, group No. ★ and user access ★.

User Mgt.: Through this submenu, you can browse the user information stored on the device, including the user ID, name, fingerprint ★, face, card ★, password, rights, group No ★. and user access ★. Here you can also add, modify or delete a user's information.

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

System: Through this submenu, you can set system-related parameters, including the basic parameters, interface parameters, fingerprint ★, face and attendance parameters, Keyboard definitions, Access settings ★, firmware update etc. to enable the device to meet the user's requirements to the greatest extent in terms of functionality and display.

Data Mgt.: Through this submenu, you can perform management of data stored on the device, for example, deleting the attendance records, all data, clear an administrator, restore to factory settings and query records.

Date/Time: Through this submenu, you can set the alarm time and duration, or set the Bell.

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

Dn/Upload: Through this submenu, you can download user information and attendance data stored in the device through a USB disk to related software or other fingerprint recognition equipment.

Sys Info.: Through this submenu, you can browse the records and device information.



Any user can access the main menu by pressing the **[Menu]** key if the system does not have an administrator. After administrators are configured on the device, the device needs to verify the administrators' identity before granting them access to the main menu. To ensure device security, it is recommended to set an administrator when initially using the terminal. For detailed operations, see **3.8 Modifying User Right**.

3. Add User

Press **[Add]** on the **[User Mgt.]** interface to display the **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 device displays the number of fingerprints enrolled fingerprints.
Password: Enroll a user's password. The device supports 1-8 digit passwords by default.
Face: Enroll a user's face.
Group No.★: Setting in the group of user.
Role: Set the rights of a user. A user is set to **ordinary administrator**. Ordinary users are only granted the verification, while administrators are granted access to the main menu for various operations apart from having all the privileges granted to ordinary users.
Photo★: Enroll a user's photo. If the user verification is successful, the user's photo is displayed on screen.
User Access★: Set the lock control and access control parameters.



[Add User] interface as shown below.
 supported by default.
 supported by default.
 displays the number of fingerprints enrolled fingerprints.
 1-8 digit passwords by default.
user by default and can also be set to rights of face, fingerprint or password the main menu for various operations apart successful, the user's photo is displayed on parameters.

3.1 Entering a User ID

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

1. Press **[User ID]** on the **[Add User]** interface to display the user ID management interface.

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 already exists!" is displayed, enter another ID.

Tip: The device 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 pre-sales technicians.

3. After the user ID is entered, press **[Save]** to save the current information and return to the previous interface. Press **[Exit]** to return to the previous interface without saving the current information.



1 for every user in sequence. If you use the ID allocated by the device, you may skip this section.
 display the user ID management interface.
 enrollment, but once enrolled, it cannot be modified.
 and press **[OK]**. If the message "The user ID already exists!" is displayed, enter another ID.
 by default. If you need to extend the length of current user ID numbers, please consult our commercial representatives or pre-sales technicians.
 current information and return to the previous interface without saving the current information.

3.2 Entering a Name

Use the T9 input method to enter the user name

1. Press **[Name]** on the **[Add User]** interface to
2. On the displayed keyboard interface, enter a user name
3. After the user name is entered, press **[Save]** to previous interface. Press **[Exit]** to return to the information.



through the keyboard.
display the name input interface.
name and press **[X]**.

[T9 Input Instructions.](#)

save the current information and return to the previous interface without saving the current

 **Tip:** The device supports 1 to 12 character names by default.

3.3 Enrolling a Fingerprint★

1. Press [**Fingerprint**] on the [**Add User**] interface to
2. On the displayed [**Enroll Fingerprint**] interface, properly according to the system prompt. For details, see [1.3 Finger Placement](#).
3. Place the same finger on the fingerprint sensor enrollment succeeds, the system will display a prompt [**User**] interface. 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 enroll a backup fingerprint by pressing maximum of 10 fingerprints.
5. Press [**Save**] to save the current information and return to the previous interface without saving the current information.



display the [**Enroll Fingerprint**] interface.

place your finger on the fingerprint sensor see [1.3 Finger Placement](#).

three consecutive times correctly. If the message and automatically return to the [**Add User**] interface. 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.

[**Fingerprint**] again. A user can enroll a

return to the previous interface. Press [**Exit**] to



3.4 Enrolling a Password

1. Press **[Password]** on the **[Add User]** interface to
2. On the displayed keyboard interface, enter a password at the system prompt and then press **[OK]**.

 **Tip: The device supports 1-8 digit passwords**

3. After the password is entered, an interface to save the current information and return to the previous interface without saving the current



display the password management interface. password and press **[OK]**. Re-enter the

by default.

displayed as shown below. Press **[Save]** to interface. Press **[Exit]** to return to the information.



3.5 Enrolling an ID card★

1. Press **[Card]** on the **[Add User]** interface to display
2. The **[Punch Card!]** interface pops up as shown below. For details, see [1.6 Appearance of the Device](#).
3. If the card passes the verification, the device will display Card No.: '*****', and returns to the **[Add User]**
4. Press **[Save]** to save the current information and return to the previous interface without saving the

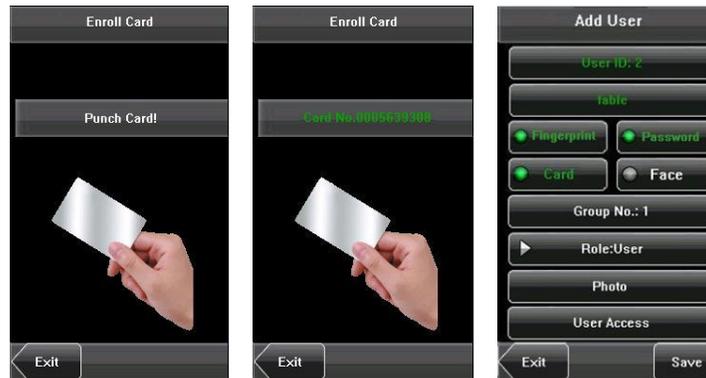


the **[Enroll Card]** interface.

Swipe your ID card properly in the swiping area.

display a prompt message "Read Successfully!" interface.

return to the previous interface. Press **[Exit]** to current information.



Note: 3 Inches Facial & Fingerprint Recognition support Mifare card function. It is an option function, if you want to customize the Mifare card function, please consult our commercial representatives or pre-sales technical support engineers.

3.6 Enrolling a Face

1. Press **[Face]** on the **[Add User]** interface to display
2. On the displayed face enrollment interface, turn and lower your head according to the voice prompts, the system to assure accurate verification. See [1.2](#)
3. If your face image is enrolled successfully, the automatically return to the **[Add User]** interface.
4. Press **[Save]** to save the current information and return to the previous interface without saving the

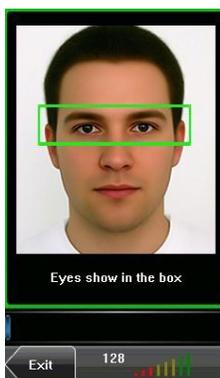


the face enrollment interface.

your head to the left and right slightly, raise so as to enroll different parts of your face into [Enrollment Face Expressions](#).

system will display a prompt message and

return to the previous interface. Press **[Exit]** to current information.



3.7 Entering a Group No.★

1. Press [**Group No.**] on the [**Add User**] interface to display the group No. management interface.
2. On the displayed keyboard interface, enter your group No. and press [**OK**].
3. After the group No. is entered, an interface is displayed as shown below. Press [**Save**] to save the current information and return to the previous interface. Press [**Exit**] to return to the previous interface without saving the current information.



3.8 Modifying User Rights



Note: There are two types of rights respectively granted to two types of users: **ordinary users** and **administrators**.

Ordinary users are only granted the rights of face, 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.

1. On the [**Add User**] interface, press [**Role: User**] to change the user to an administrator.
2. After the modification is done, the interface is as shown below. Press [**Save**] to save the current information and return to the previous interface; press [**Exit**] to return to the previous interface without saving the current information.



3.9 Enroll Photo★

If you had enrolled your photo in the system, the addition to your ID and name after you pass the

1. Press **[Photo]** on the **[Add User]** interface to
2. On the photo enrollment interface, stand naturally Standing Position, Posture and Face Expression.
3. After taking the photo, press **[Exit]** to return to the
4. After the photo is taken, press **[Save]** to save the interface; press **[Exit]** to return to the previous information.



system will display your enrolled photo in verification.
display the photo enrollment interface.
in front of the screen. For details, see [1.1](#)
Press **[Capture]** to capture the photo.
previous interface.
current information and return to the previous interface without saving the current

3.10 User Access Settings★

Press [User Access] on the [Add User] interface to display the user access settings interface.

User Access settings are to set the user's rights to verify and open doors, such as the Verify Type, Time Zone and Duress FP management.



1. Verify Type:

(1) **Group Verify Mode:** If the user uses the group verify mode that he belongs to.

(2) **Individual Verify Mode:** Select the verification mode for this user instead of the group verify mode. That will not affect other users in this group.

Note:

(1) Only the products with the built-in ID card module support the ID card verification.

(2) For the Verify Type, please refer to Appendix 4 Multi-combination Authentication Mode. Only some devices support Multi-combination authentication mode.



2. Time Zone:

(1) **Group Time Zone:** If the user uses the group time

(2) **Individual Time Zone:** Select the time zone of the will not affect other users in the group.

3. Duress FP:

zone that he belong to.

user instead of the group time zone. That



The user can register a new duress fingerprint or cancel registered duress fingerprints. If a finger is registered with a duress fingerprint, when it is compared, it will trigger the duress alarm signal.

If the duress fingerprints are cancelled, it does not delete the fingerprint data. The normal fingerprint comparison process can still be used.

Duress FP Management:

(1) Register Duress FP:

Press **[Reg. Duress FP]** on the **[User Access]** interface to display the **[Enroll Fingerprint]** interface. On the displayed **[Enroll Fingerprint]** interface, place your finger on the fingerprint sensor properly according to the system prompt. For details, see [1.3 Finger Placement](#).



(2) Cancel Duress FP:

Press **[Can. Duress FP]** on the **[User Access]** interface to pop-up the confirmation message. Select **[YES]** to delete the enrolled duress FP, otherwise select **[NO]** to cancel the operation.



4. User Management

Browse the user information, including the user ID, name, fingerprint★, face, ID card★, password, rights, group No.★ and user access settings★ through this interface. To add, edit or delete the basic information of users.

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

 This user is an administrator.

 **Note:** The users are listed in alphabetical order by last name. If you press a user name, you can access the editing interface of this user to edit or delete the related user's information.



4.1 Edit a User

Press a user name from the list to enter the **[User Info]** interface.

The User ID cannot be modified, and the other operations are similar to those performed in adding a user. You can re-enroll your fingerprint★ and face, change your password, modify the management rights and Group No.★

For example: Change the user rights from administrator to ordinary user as shown below:



4.2 Delete a User

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

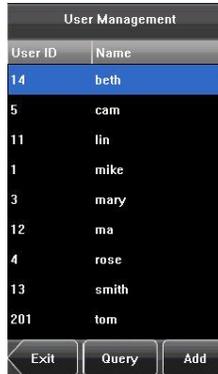
1. Press [Delete] to delete a user.
2. On the displayed interface, click [YES] to delete the current user or [NO] to return to the previous interface.
3. On the [User Info] interface, press [Name], [Fingerprint], [Face] or [Password] to delete the related user information and to re-enroll the new information following the device prompt.



4.3 Query a User

To facilitate administrators to locate a user quickly the device enables the administrator to query by “User ID Query”:

1. Press **[Query]** on the **[User Management]**
2. Enter the user ID on the displayed interface, and user.



from a large number of enrolled users, the ID”.

interface to display the User ID query interface. click **[OK]** to locate the cursor on the desired

5. Communication Settings

You can set related parameters for the communication between the device and PC, including the **IP address**, **Gateway**, **Subnet Mask**, **Baud Rate★**, **Device ID**, and **Comm Key**.



Note: The comm. (RS232/RS485), Wiegand In and Wiegand Out are optional functions, only some machines have these functions.

5.1 Network Settings

When the device 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.

(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 device and the PC. It includes five options: 9600, 19200, 38400, 57600, and 115200. The higher baud rate is recommended for the RS232 communication to

achieve high speed communication, while the lower 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 the 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 device and PC. Once the password is set, you can connect the PC with the device 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 device; otherwise, the connection is unsuccessful. 1 to 6 digit passwords are supported.



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

5.2 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.

5.3 Wiegand Output★

Wiegand Format: The system has two built-in formats also supports the format customization function to

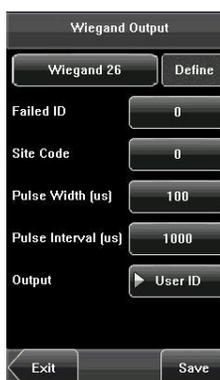
Failed ID: Refers to the value output by the system subject to the setting of “Wiegand Format”. The

Site Code: The site code is used for a customized the device ID, but the site code is customizable and The default value scope of the Site Code is 0–255.

Pulse Width: Refers to the width of the Wiegand pulse the pulse width is 1–1000.

Pulse Interval: Refers to the interval of the Wiegand 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.



Wiegand 26-bits and **Wiegand 34-bits**, and meet individualized requirements.

upon verification failure. The output format is default value scope of **Failed ID** is 0–65535.

Wiegand format. The site code is similar to can be duplicated among different devices.

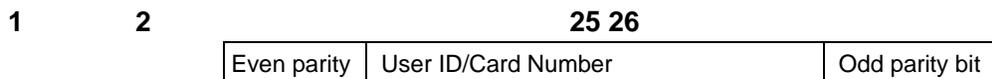
in microseconds. The default value scope of

pulse in microseconds. The default value

5.3.1 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.

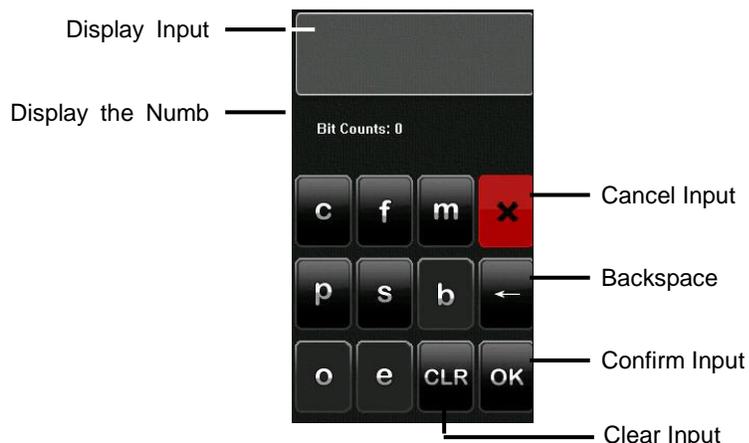


Definition of Fields:

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 bit; otherwise, the even parity bit is 0.
User ID/ Card	User ID/Card Number (Card Code, 0–16777215)

To customize the 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:

pp

Parity bits:

eeeeeeeeeeeeeeeeoooooooooooooooooooooooooo

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: pmmmmsssssssssscccccccccccccccccp

Parity bits: oeobeobeobeobeobeobeobeobeobeobeoe

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:

pmmmmffffffsssssscccccccccccccccccp

Parity bits:

eeeeeeeeeeeeeeeeeeoooooooooooooooooooo

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: psssssssssssssscccccccccccccccccccccccccccccccccp

Parity bits:

eeeeeeeeeeeeeeeeeeeeeeeeoooooooooooooooooooooooooooo

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.

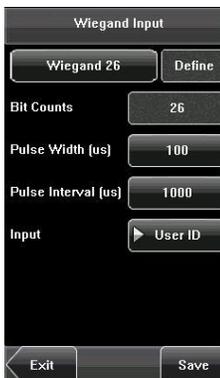
5.4 Wiegand Input★

Wiegand Format: The system has two built-in **34-bits**, and also supports the format customization. For more about the Wiegand format, please refer to **Bit counts:** Wiegand data digit length.

Pulse width: Pulse width is 100 microseconds by

Pulse interval: It is 900 microseconds by default, 20000.

Input: Content contained in Wiegand input signal,



formats **Wiegand 26-bits** and **Wiegand** function to meet individualized requirements. [5.2 Wiegand Output.](#)

default, which can be adjusted from 20 to 800. which can be adjusted between 200 and including User ID or card number.

6. System Settings

Through the [System] menu, you can set system-related parameters, including the General, Display, Fingerprint★, Face, Log settings, Shortcut Def, Access Control Set★, and Firmware Update, to enable the device to meet user requirements to the greatest extent in terms of functionality and display.

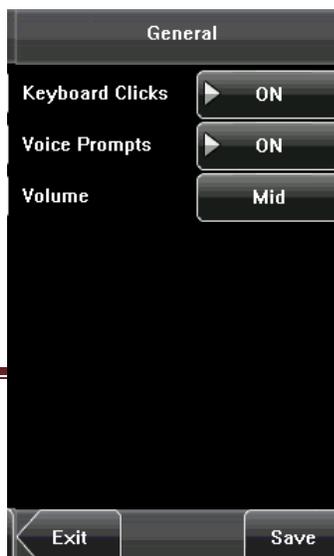


6.1 General Parameters

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

Voice Prompts: the operation of the mute.

Volume: This



This parameter is used to set whether to play voice prompts during device. Select “ON” to enable the voice prompt, and select “OFF” to

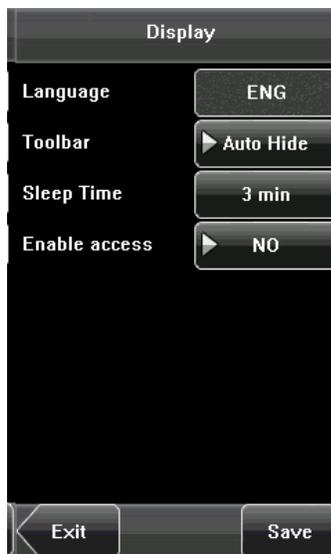
parameter is used to adjust the volume of voice prompts.

6.2 Interface Parameters

Language: This parameter is used to display the current language used by the device. For multilingual-capable devices, you can switch between different languages through this parameter. Then you should restart the device.

Toolbar: This parameter is used to display the 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.

Sleep Time (S): This parameter is used to specify a period after which the device is put in sleep mode if there is no operation within this period. You can wake up the device by pressing any key or touching the screen. The numerical range is 1 ~ 30 minutes. The factory default is set for 3 minutes.



6.3 Fingerprint Parameters★

1: 1 Threshold: This parameter is used to set the threshold of matching between the current fingerprint and the fingerprint template enrolled in the device in the 1:1 verification mode. If the similarity between the current fingerprint and the fingerprint template enrolled in the device 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 the current fingerprint and the fingerprint template enrolled in the device in the 1: N verification mode. If the similarity between the current fingerprint and the fingerprint template enrolled in the device 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

Fingerprint Image: This parameter is used to set whether to display the fingerprint image on the screen during fingerprint enrollment or comparison. It has four options:

Show for Enroll: Display the fingerprint on the screen in the enrolling process.

Show for Match: Display the fingerprint on the screen in the verification process.

Always Show: Display the fingerprint on the screen in the enrolling and verifying process.

Never Show: Never display the fingerprint on the screen in any case.



6.4 Face Parameters

1: 1 Threshold: This parameter is used to set the threshold of matching between the current face and the face template enrolled in the device in the 1:1 verification mode. If the similarity between the current face and the face template enrolled in the device is larger than this threshold, the matching is successful; otherwise, the matching is not successful. The valid value scope is 70-120. The higher the threshold, the lower the FAR and the higher the FRR are, and vice versa.

1: N Threshold: This parameter is used to set the threshold of matching between the current face and the face template enrolled in the device in the 1: N verification mode. If the similarity between the current face and the face template enrolled in the device is larger than this threshold, the matching is successful; otherwise, the matching is not successful. The valid value scope is 80-120. The higher the threshold, the lower the FAR and the higher the FRR are, and vice versa.

The recommended thresholds are as follows:

FRR	FAR	Threshold	
		1: N	1:1
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

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

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



Note: Improper adjustment of the Exposure and Quality parameters may severely affect the performance of the device. Please adjust the Exposure parameter only under the guidance of the after-sales service personnel from our company.



6.5 Log Settings

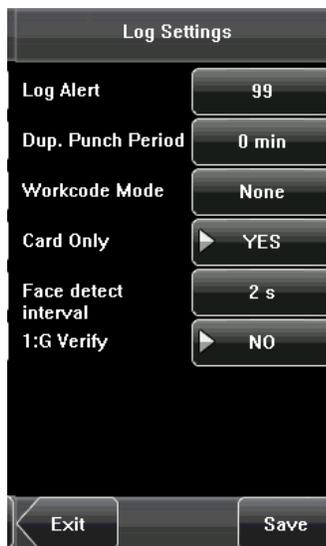
Log Alert: When the available space is insufficient to store the specified number of attendance records, the device will automatically generate an alarm (Value scope: 1-99).

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

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.

Face interval: According your need to set it. The default value is 0, namely don't have interval.

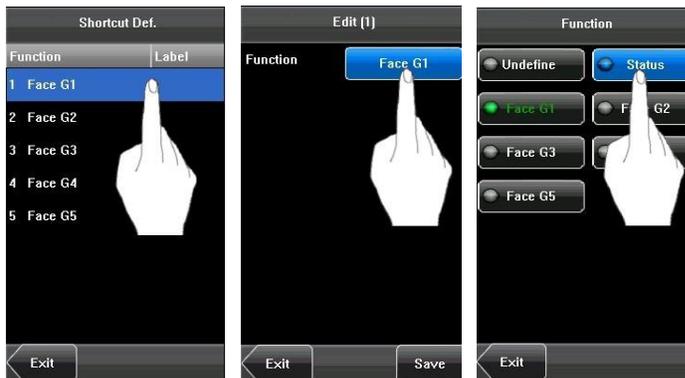
1: G Verify★: Select it as YES or NO, namely set whether or not to start this function.



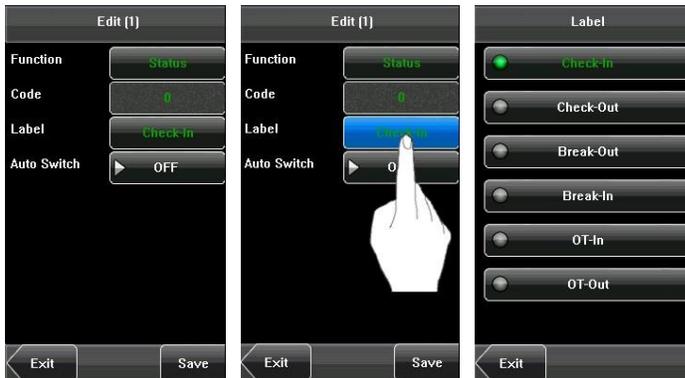
6.6 Shortcut Definitions

Define touch screen functional shortcut keys. For devices with the face grouping function (MENU--System--Log Settings--1:G Verify), the way to define shortcut keys is described as follows:

(1) Click the **Shortcut Def.** item to display the list of the existing shortcut keys; click the shortcut key to modify, as shown in figure 1. Enter the edit screen, and click the **Function** box as shown in figure 2. Enter the **Function** screen, and the user can select desired settings for the type of shortcut keys according to practical needs, such as face groups 1-5 (enable the Group Verify function), undefined and status.



(2) The user can set the shortcut key as status key; click **Status** as shown in figure 3 above; enter the edit screen of the status key as shown in figure 1 below; click the **Label** box as shown in figure 2 below; enter the **Label** screen as shown in figure 3 below; click the row of the label (six options for the status) to change it to the corresponding label; the user can modify the label of the status keys according to practical needs.



(3) The **Code** cannot be modified; it is changed accordingly with the selected label of the status key. Select **Auto switch**, and select **On**, as shown in figure 1 below.



(4) Click the time box after “week” as shown in figure 2 above to enter the time setting screen as shown in figure 3 above. Click the key on the touch screen to set the time; click **[OK]** to save and return to the edit screen.

(5) After the setting is completed, click **[Save]** to save the setting and return to the **Shortcut Def.** screen.

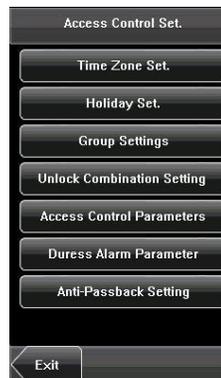
6.7 Access Settings★

Access Control Settings are to set user’s open door parameters. It is not enabled by factory default. You -- **[Enable Access]** . Select YES or NO.

To unlock, the enrolled user must agree with the

1. The current unlock time should be in the effective
2. The group where the user is must be in access another group, to open the door together).

The new enrolled user is under the first group by No. 1 access control group. The new enrolled user is related settings of access control, the system will be



time zone, control lock and set related device can click **[MENU] -- [System] -- [Display]**

following conditions:

time of the user time zone or group zone.

control (or in the same access control with

default and use the No. 1 group time zone, the in unlocked state (if you have modified the changed with the modification).

6.7.1 Time Zone Setting

Time zone is the minimum unit of access control zones. Every time zone consists of seven time sections is the effective time zone within 24 a hour day. between the three zones. It is effective if only one is **HH:MM-HH:MM**, accurate to the minute.

If the end time is smaller than the start time (23:57-end time is bigger than the start time (00:00- 23:59), it The effective time zone for user unlocking: start time.

 **Notice:** System default time zone 1 as whole unlocking).



option. The whole system can define 50 time sections (that equal one week). Every time Every user can set 3 time zones. It's "or" satisfied. Every time section format is

23:56), the whole day is not allowed. If the is an effective section.

00:00-23:59 or an end time bigger than the day open (namely, the new enrolled user is

6.7.2 Holiday Setting

Special access control time may be needed during access control time. So a holiday access control time

1. Add Holiday:

- (1) Enter holiday add interface, press the key to edit
- (2) Press the touch screen number key to set the press [X] to exit and return to the previous interface.
- (3) Press [Save] to save the current information and return to the previous interface without saving the



holidays. It is difficult to modify everybody's can be set that is applicable for all employees.

the items.

value. After setting, press [OK] to save and

return to the previous interface. Press [Exit] to current information.



2. Edit Holiday

Select the holiday to be edited and enter the edit Holiday. After editing, press **[Save]** to save and

Notice: If holiday access control time is set, subject to the time zone here.



interface. The edit operation is similar to Add return to the previous interface.

user's open door time zone during holiday is

3. Delete Holiday

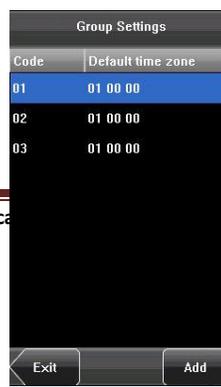
Select the holiday to be deleted. Press **[Delete]** to delete this holiday, otherwise select **[No]** to cancel



popup the confirmation interface. Select **[Yes]** to the operation.

6.7.3 Group Time Zone Setting

Grouping is to manage employees in groups.



Employees in a group use the group time zone

by default. Group members can also set the user time zone. Every group can hold three time zones. The new enrolled user belongs to Group 1 by default and can also be allocated to other groups.

1. Add Group Time Zone

(1) Enter the Add Group interface. Press a key to edit the corresponding item.
Code: Enter the number edit interface to set the value.
VerType: Select the Group Verify Type.

Holiday No.: Select if the Time zone is valid in holiday.
Time Zone: Select the Group Time Zone.

(2) After editing, press [**Save**] to save the current information and return to the previous interface. Press [**Exit**] directly to return to the previous interface without saving the current information.



edit the corresponding item. value.

holiday.

information and return to the previous interface. interface without saving the current information.

Note:

- (1) RF means ID card verification. Only the products with the built-in ID card module support the ID card verification.
- (2) For Multi-combination verification, please refer to [Appendix 4 Multi-combination Authentication Mode](#).



Notice:

(1) If the holiday is valid, only when there is an intersection between group zone and holiday time zone, can the group member open the door.

(2) If the holiday is invalid, the access control time of

group member won't be affected by holiday.

2. Edit Group Time Zone

Press the line to be edited, and enter the edit current information and return to the previous previous interface without saving the current

interface. After editing, press [**Save**] to save the information. interface; press [**Exit**] directly to return to the information.

3. Delete Group Time Zone

Select the line to be deleted. Press [**Delete**] to

popup the confirm interface. Select [**Yes**] to



delete this holiday, otherwise select [**No**] to cancel the operation.

6.7.4 Unlock Combination Setting

Make various groups into different access controls to
An access control can be made up of 5 groups

1. Add Unlock Combination

- (1) Enter holiday add Combination Setting interface
- (2) Press the touch screen number key to set the
press [**X**] to exit and return to the previous interface.
- (3) Press [**Save**] to save the current information and
return to the previous interface without saving the



achieve multi-verification and improve security.
maximum.

and press the key to edit the items.

value. After setting, press [**OK**] to save, and

return to the previous interface. Press [**Exit**] to
current information.



2. Edit Unlock Combination

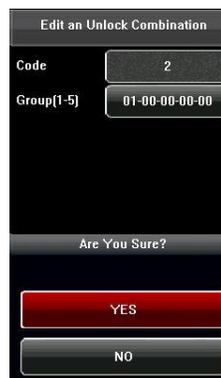
Select the line to be edited. Press the item to enter save the current information and return to the previous interface without saving the current



the edit interface. After editing, press **[Save]** to previous interface. Press **[Exit]** to return to the information.

3. Delete Unlock Combination

Select the line to be deleted. Press **[Delete]** to delete this holiday, otherwise select **[No]** to cancel



popup the confirmation interface. Select **[Yes]** to the operation.

6.7.5 Access Control Parameter

Through the [Access] menu, you can set the access control devices.

Lock Delay: Indicates the duration for the device to scope: 1-10 seconds)

Door Sensor Delay: Indicates the delay for checking door sensor state is inconsistent with the normal state triggered, and this period of time is regarded as the seconds)

Door Sensor Mode: Includes the None, Normally “None” indicates that the door sensor switch is not open in the normal state. “NC” indicates that the door sensor is closed in the normal state.

Alarm Delay: Indicates the duration from the detection of the door sensor exception to the generation of alarm signal. (Value scope: 1-99 seconds)

Failure Alarm Threshold: When the number of times failed reach the set limit, an alarm signal will go off (effective value: 1-9 times).

NC Time Zone: Set time zone for access control NC. Nobody can unlock during this time zone.

NO Time Zone: Set time zone for access control NO. The lock is always in valid state during this time zone.

Valid in Holiday: Define time zone for NO or NC. Whether the time zone set in holiday time zone is valid.



parameters of the electronic locks and related

place the electric lock in open state. (Value

the door sensor after the door is opened. If set by the door sensor switch, an alarm will be “door sensor delay”. (Value scope: 1-99

Open (NO), and Normally Closed (NC) modes. used. “NO” indicates that the door sensor is

Notice:

1. If the Time Zone of normally open or normally closed has been set, please switch door sensor to NO, otherwise it will produce alarm signal during Normal Close Time Zone or Normal Open Time Zone.
2. If the normally open or normally closed Time Zone is not defined yet by the time, the equipment will prompt that you to define the Time Zone, and transfer you to the Time Zone interface to add.

6.7.6 Duress Alarm Parameters

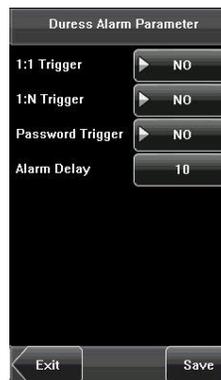
There are duress alarm parameter settings in the duress situation, he can use the set duress alarm as usual, but the alarm signal will be sent to the alarm.

1: 1 Trigger: If set to “Yes”, when user uses 1: 1 match alarm signal.

1: N Trigger: If set to “Yes”, when user uses 1: N is no alarm signal.

Password Trigger: If set to “Yes”, when a user uses go off or there is no alarm signal.

Alarm Delay: After duress alarm gets started, the defined. After the set time period, the alarm signal will be generated automatically (0-255 seconds).



device. When an employee comes across a mode to verify. The device will open the door mode, alarm signal will go off or there is no match mode, alarm signal will go off or there password verification mode, alarm signal will alarm signal will not output directly. It can be

6.7.7 Anti-Passback Setting

Set the device Anti-Passback function.

APB Direction: There are four options: None,

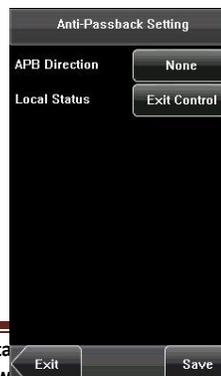
Device Status: There are three options: Exit Control,

For Anti-Passback function, please refer to [Appendix](#)

Anti-Passback Setting Operation:

(1) Enter Anti-Passback Setting interface, press the

(2) Press the touch screen number key to set the press [X] for exit and return to the previous interface.



APB-Out, APB-In, APB-Out/In.

Entry Control and None.

5 Anti-Passback.

key to edit the items.

value. After setting, press [OK] to save, and

(3) Press **[Save]** to save the current information and return to the previous interface. Press **[Exit]** to return to the previous interface without saving the current information.



6.8 Update

You can upgrade the device firmware by using the upgrade file in the USB disk through this function.



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

7. Data Management

Through the [Data Mgt.] menu you can perform management of data stored on the device, for example, delete attendance records, delete all data, clear the administrator, restore the device to factory settings, and query user records.



Delete Transactions: Delete all the

attendance records.

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

information of enrolled personnel, including their

Clear Administrator: Change all administrators to ordinary users.

Restore to Factory Settings: Restore all parameters on the device to factory settings.



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

7.1 Query Record

After successful check-in, the employee's attendance records are saved in the device. 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 records of this employee.

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.

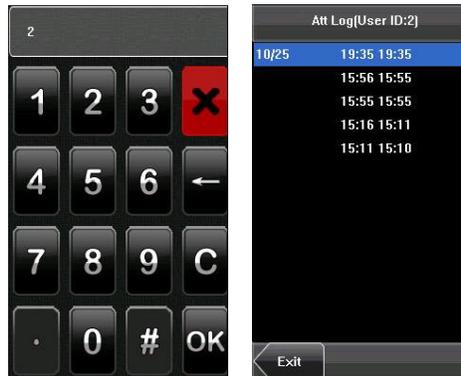
Start and End: When you select a customized time period, you need to input a start time and an end time. When you select other options for the time period, the start and end time will be automatically adjusted to the related time.

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

Select the row where the desired record is located. You can query the detailed information of this record.



For example, press User ID and enter the edit interface. Input the ID number and press **[Query]**. The query result will display as follows:



7.2 Work Code

This makes it easy for users to quickly deal with data of different situations. Click **[System]**--**[Shortcut Definitions]**--**[Undefine]**, select **[Workcode]** and save, to open the work code function. For detailed operations click **[Data Management]**--**[Workcode]**. Here you can edit, add, delete and query.

1. Add a Work Code

(1) Press **[Add]** on the **WorkCode** interface to display the **[Add]** interface as in the figures below:

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 display. On this interface, enter a number.

(3) Press the corresponding entry button of **[Label]** on the **Workcode** interface to display the text entry interface. On this interface, enter a label for the work code. (See [12.1 T9 Input Instructions](#))

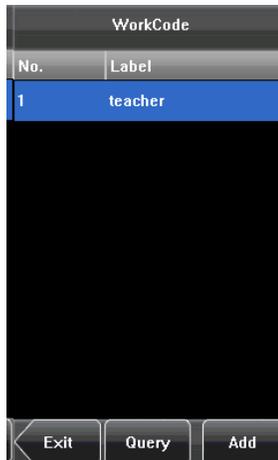
2. Edit and Delete a Work Code

(1) Press the row of a work code on the **WorkCode** interface to display the **[Edit]** interface.

(2) To edit this work code, enter a new number and label with the same operation steps as described in “Add a Work Code”.

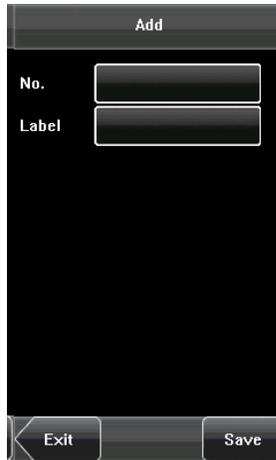
(3) To delete this work code, press **[Delete]**.

(4) On the
the deletion
deletion



3. Edit

Press
keyboard
want to query



displayed prompt interface, press **<YES>** to confirm of this work code, and press **<NO>** to cancel the operation.

and Delete a Work Code

[Delete] on the **WorkCode** interface, display the interface. At the prompt enter the code number you and then click OK.

8. Date/Time Setting

8.1 Set Date/Time

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

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 formats to select from. Both 12-hour and 24-hour time parameters are supported.
4. Press [**Save**] to save the current information and return to the previous interface without saving the



accurately to ensure the accuracy of main menu interface.

display the time setting interface.

parameter. For the time format, there are 10 systems are supported.

return to the previous interface. Press [**Exit**] to current information.



8.2 Bell Setting★

A lot 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 aid management, we integrated the time bell function into the device. You can set the alarm time and duration for ringing the bell based on your requirements, so that the device will automatically play the selected ring tone, trigger the relay at the alarm time, and stop playing the ring tone after the set duration. Each device can add a maximum of 15 alarm bells.

Press [**Bell**] on the [**Date/Time**] menu to display the bell setting interface, as shown in figure below:



1. Add a Bell

1) The displayed bell setting interface 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 device automatically plays a bell ring tone every day.

Bell Date: This parameter is used to set which day the device automatically plays a bell ring tone.

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 and external ringing. For internal ringing, the ring tone is played by the loudspeaker of the device. For external ringing, the ring tone is played by an external electric bell that is connected with the device.

2. Edit and Delete a Bell

Press a bell in the list on the bell setting interface to operation of "Add a Bell".



display the **[Edit]** interface, with similar

 **Notice:** Only some models have this function. If representative or technician.

you need it, please contact our business

8.3 Daylight Saving Time (DLST)★

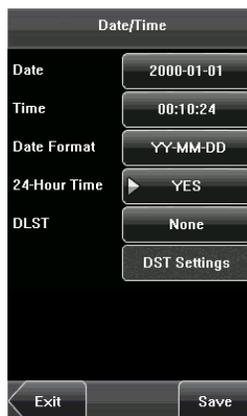
DLST, also called Daylight Saving Time, is a system to prescribe local time in order to save energy. The unified time adopted during the system date is called “DLST”. Usually, can help people go to bed earlier and wake up power. In autumn, the time will be recovered. The At present, nearly 110 countries adopt DLST.

To meet the demand of DLST, a special option can Attendance recorder. Make the time one hour (month), and make the time one hour backward at necessary.

Operation:

Select the DLST mode first including Mode 1, Mode

- 1) Click [None] to display the DLST mode selecting
- 2) Select the DLST mode and return to the Date/Time interface:



the time will be one hour forward in summer. It earlier. It can also reduce lighting to save regulations are different in different countries.

be customized on our RF Card Time & forward at XX (minute) XX (hour) XX (day) XX XX (minute) XX (hour) XX (day) XX (month) if

2 and None. The default setting is None. interface.



- 3) Click [DST settings], enter the DLST edit interface.

Mode1

Mode2



4) After setting, click [Save] to complete and return.

9. Auto Test

The Auto Test enables the system to automatically test whether functions of various modules are normal, including the screen, sensor, voice, face, keyboard and clock tests.



1. Test Screen: The device 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 [Exit].

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

3. Test Voice: The device automatically tests whether the voice files are complete and the voice quality is good by playing the voice files stored in the device. You can continue the test by touching the screen,

4. Test Face: The device automatically tests whether the camera works properly by checking whether the collected face images are clear and acceptable. Press [Exit] to exit the test.

5. Test Keyboard★: The device 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 [**Exit**] to exit the test.

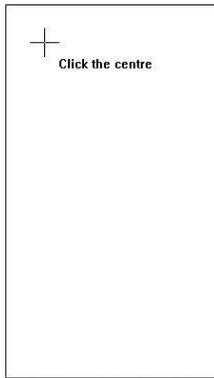
6. Test Time: The device tests whether its clock works properly by checking the stopwatch of the clock. Touch the screen to start counting, and touch it again to stop to check whether the counting is accurate. Press [**Exit**] to exit the test.

7. 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 a screen calibration through menu operations.

The Screen Calibration Operation:

- (1) Press [**Menu**] on the initial interface to display the
- (2) Press [**Calibration**] on the [**Auto Test**] interface to
- (3) Touch the center of the cross “+”.
- (4) Repeat Step 3 following the move of the “+” icon to
- (5) Touch the center of the cross at five locations on “Calibrating screen, pls wait.....” is displayed on system automatically returns to the main menu. If the start from Step 3.



main menu interface.

display the screen calibration interface.

different locations on the screen.

the screen correctly. When the message screen, the calibration succeeds and the calibration fails, the system recalibration will

10. USB Disk Management

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



- 1. Download Transactions:** Download all the attendance data from the device to a USB disk.
- 2. Download User:** Download all the user information, fingerprints and face images from the device to a USB disk.
- 3. Download User Photos★:** Download the employees' photos from the device to a USB disk.
- 4. Upload User:** Upload the user information, fingerprints and face images stored in a USB disk to the device.
- 5. Upload User Photo★:** Upload the JPG documents that are named after the user IDs and stored in a USB disk to the device, so that user photos can be displayed after the employee passes the verification. See [Appendix 3 Photo ID Function](#).

11. System Information

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

Records: The number of enrolled users, on the [Records] interface; the total fingerprint well as the total attendance storage capacity and respectively.

Device: The device name, serial number, version are displayed on the [Device] interface.



information of the device through the [System

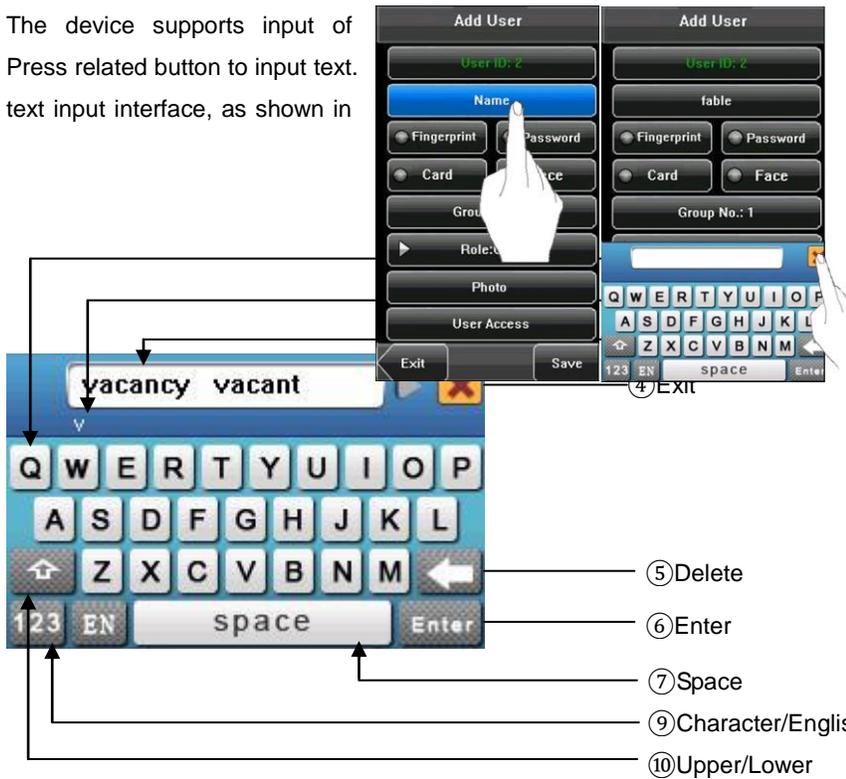
administrators and passwords are displayed storage capacity and occupied capacity as occupied capacity are graphically displayed

information, vendor and date of manufacture

12. Appendix

12.1 T9 Input Instructions

The device supports input of English characters, numbers and symbols. Press related button to input text. text input interface, as shown in



English characters, numbers and symbols. For example, press [**Name**] to display the the figure:

To enter a name, proceed as follows:

1. Press [**Name**] on the [**Add**] interface, as shown in the figure below.
2. Enter the letter characters, and a list of characters in relation to the letter is presented in the text display area.
3. If the desired character is displayed in the text display area, press this character. This character is at the same time displayed on the [**Name**] button. Enter the next character by repeating Step 2.
4. After finishing the entry of the name, press [**X**] to exit the keyboard interface and return to the previous interface.



12.2 USB Pendrive

The FRT is used as the USB Host to externally connect with a USB pendrive for data exchange.

The conventional fingerprint readers transfer data only through the RS232, RS485 or Ethernet. Bulk data transfer may take a long time due to the restriction of physical conditions. The USB far outperforms any other previous transfer modes in terms of data transfer rate. Insert the USB pendrive to the USB slot on the FRT, download data to the USB pendrive, and then connect the USB pendrive to a computer to import the data to the computer. Further, the FRT also supports the exchange of user information and fingerprint data between two devices, which helps dispense with the hassle of conventional cable connection for data transfer between the FRT and computers.

For operation of the FRT used as the USB host, see 7. USB Pendrive Management.

12.3 9-Digit Enrollment Number

The standard user IDs supported by the FRT for user enrollment are 5 digits long (ranging between 1 and 65534). In practice, customers may require user IDs with more than 5 digits. We can customize devices supporting 9-digit user IDs to meet your needs.

12.4 Introduction of 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

The figure below 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 20 us and 100 us, and the pulse jump time ranges between 200us and 20ms). Data1 and Data0 are high level (larger than V_{oh}) signals till the card reader prepares to send a data stream. The asynchronous low-level pulse (smaller than V_{ol}) generated by the card reader is sent to the access control panel (The saw-tooth wave as shown in the Figure below) through Data1 or Data0. Data1 and Data0 pulses will neither overlap nor be generated synchronously. The table below 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 device.

Figure: Sequence Diagram

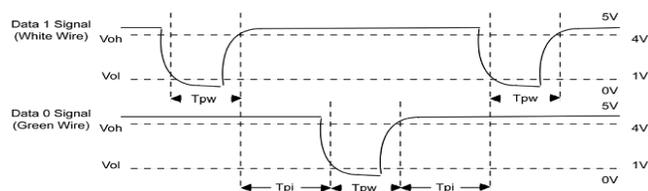


Table: Pulse Time

Symbol	Definition	Typical Value of Reader
T_{pw}	Pulse Width	100 μ s
T_{pi}	Pulse Interval	1 ms

12.5 Photo ID Function★

The Photo ID function is used to display the photo the screen in addition to such information as the user

Operation Steps

- 1) When the photo taken by the device is used, the verification.
- 2) To use a photo stored in a USB disk, proceed as
 - 1) Create a folder with the name of “photo” in the folder.
 - 2) The user photos must be in JPG format and user with the user ID of 154, the photo name must be
 - 3) Insert the USB disk into USB slot on the device, 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 64 kb.
- 3) The uploaded new user photo will overwrite the existing photo 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.



enrolled by a user or stored in a USB disk on ID and name.

photo can be displayed upon successful

follows:

USB disk, and store users' photos under this

named after their IDs. For example, for the 154.jpg.

12.6 Work Code ★

Function Description

The concept of work code is introduced to facilitate the software in handling the verification records according to different cases. For example, we define “1” for eating, “2” for seeing a doctor and “3” for smoking, and input corresponding value when performing a specific action. In this way, the software can easily differentiate among events 1, 2 and 3.

Operation Description

You can set the “**Work Code**” by selecting **Menu** → **Data Management**. For details, please refer to [7.2 Work Code](#).

12.7 Multi-combination Authentication Mode★

This function is owned by the designated fingerprint access control machine. Most of the fingerprint machines only have two ways to verify by: fingerprint and password. We provide personal or group Multi-combination Authentication Modes for high security access control areas. Verification types include five elements: User Number (PIN), Fingerprint (FP), Face (FACE), Password (PW) and RF card (RF), which can be combined into multi-combination.



Note: The RF card is used for ID card verification, the function of ID card verification only is valid in the machine which ID card function is provided.

These symbols clarify what the following table means.

- “/” is or
- “&” is and
- FP (fingerprint)
- RF (RF card)
- “+” follow next operation
- FACE (Face)
- PWD (Password)
- PIN (user ID)

If Fingerprint, Face, Password and Card have been enrolled for the user, the verification procedure is as follows:

Type	What you do
FACE&PIN/FP/PW/RF	FACE+PIN or RF or PW or RF are verified
	1) PIN++FACE(1:1)
	2) FP(1:N)
	3) PIN+PW+“OK” 4) RF(1:N)
FP&PW	FP + PW are verified
	1) FP(1:N)+PW+“OK”
	2) PIN+FP(1:1)+PW+“OK” 3) PIN+PW+“OK”+FP
FP&RF	FP + RF are verified
	1) RF+FP(1:1)
	2) FP(1:N)+RF 3) PIN+FP(1:1)+RF

FACE&FP	FACE + FP are verified
	<ol style="list-style-type: none"> 1) FP(1:N)+FACE 2) FACE(1:N)+FP 3) PIN+FACE(1:1)+FP 4) PIN+FP(1:1)+FACE
FACE&PW	FACE + PW are verified
	<ol style="list-style-type: none"> 1) FACE(1:N)+PW+"OK" 2) PIN+FACE(1:1)+PW 3) PIN+PW+FACE
FACE&RF	FACE + RF are verified
	<ol style="list-style-type: none"> 1) FACE(1:N)+RF 2) PIN+FACE(1:1)+RF 3) RF(1:N)+FACE
FP	Only FP is verified.
	<ol style="list-style-type: none"> 1) PIN+FP(1:1) 2) FP(1:N)
PW	Only PW is verified
	PIN+PW+"OK"
RF	Only RF is verified
	RF(1:N)
FACE&PIN	FACE + PIN are verified
	PIN+FACE(1:1)
FP/RF	FP or RF is verified
	<ol style="list-style-type: none"> 1) PIN+FP(1:1) 2) RF(1:N) 3) FP(1:N)
PW/RF	FP or RF is verified
	<ol style="list-style-type: none"> 1) PIN+PW+"OK" 2) RF(1:N)
FP/PW	FP or PW is verified
	<ol style="list-style-type: none"> 1) PIN+FP(1:1) 2) FP(1:N) 3) PIN+PW+"OK"
PIN&FP	PIN + FP are verified
	PIN+FP(1:1)
FP&PW&RF	FP + PW + RF are verified
	<ol style="list-style-type: none"> 1) FP(1:N)+PW+"OK"+RF 2) PIN+FP(1:1)+PW+"OK"+RF 3) RF(1:N)+PW+"OK"+FP

	4) PIN+ PW+“OK”+FP(1:1)+RF
PIN&FP& PW	PIN + FP + PW are verified
	1) PIN+PW+“OK”+FP(1:1) 2) PIN+FP(1:1)+PW+“OK”
FP & RF/PIN	FP + PIN, or FP + RF are verified
	1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)
FACE&FP&RF	FACE + FP + RF are verified
	1) FACE(1:N)+FP+RF 2) FP+FACE(1:1)+RF 3) RF(1:N)+FACE+FP 4) PIN+FP(1:1)+FACE+RF 5) PIN+FACE(1:1)+FP+RF
FACE&FP&PW	FACE + FP + PW are verified
	1) FACE(1:N) +PW+“OK”+FP 2) FP+PW+“OK”+FACE(1:1) 3) PIN+FP(1:1) +PW+“OK”+FACE 4) PIN+FACE(1:1) +PW+“OK”+FP 5) PIN+PW+“OK”+FP+FACE



Note: For combined verification, it is better to enroll all the elements needed for using verification mode, or verification will fail.

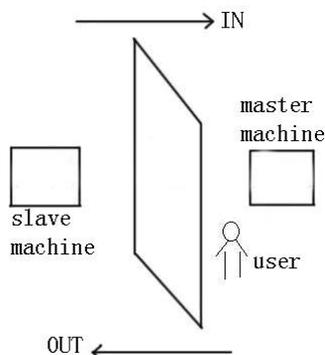
For example: If user “A” uses a fingerprint for enrollment, while a password is used for verification, the user cannot pass the verification.

12.8 Anti-Pass Back★

Overview

Sometimes, prohibited people follow other into the gate, which cause security problems. To prevent such risks, this function is enabled. The In record must match the Out record, or the gate won't open.

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



Working Principle

The master machine has Wiegand In and slave machine has Wiegand Out functions. Connect Wiegand Out of slave machine to Wiegand In of master machine. Wiegand 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-passback according to user's recent in-out record. The in record and out record must be matched. This machine supports out, in, or out-in anti-passback.

When the master machine is set as "out anti-passback", if user wants to come in and go out normally, his latest record must be "in", or he cannot go out. Any "out" attempt will be refused by the "anti-passback" function. For example, a user's latest record is "in", his second record can be "out" or "in". His third record is based on his second record. The out record and in record must match. (Notice: If customer has no previous record, then he can come in but cannot go out.)

When the master machine is set as "in anti-passback", 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-passback 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-passback", 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: The machine with Wiegand in function, except for F10 reader.

Slave machine: The machine with Wiegand Out function.

2. Menu Setting

Anti-Passback

There are four options: in/out anti-passback, out anti-passback, in anti-passback, and none.

Out Anti-Passback: Only if the user's last record is an in-record can the door be open.

In Anti-Passback: Only if the user's last record is an 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 records on the device are in-records.

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

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

3. Modify Device's Wiegand Output Format

When the two devices are communicating, only the 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 the master machine and slave machine at the same time and user PIN must be the same. Therefore, it is necessary to enroll user on the master machine and the slave machine at the same time.

5. Connection Instruction

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

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

12.9 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 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 fingerprint recognition devices for civil use only collect the characteristic points of fingerprints instead of the fingerprint images, and therefore no privacy issues are involved.
2. The characteristic points of fingerprints collected by our products cannot be used to restore the original fingerprint 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 human rights or privacy when using our products, please contact your employer directly.

Our fingerprint products for police use, or development tools support the collection of the original fingerprint images. As for whether such type of fingerprint 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 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.

12.10 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	x	o	o	o	o	o
Chip capacitor	x	o	o	o	o	o
Chip inductor	x	o	o	o	o	o
Chip diode	x	o	o	o	o	o
ESD components	x	o	o	o	o	o
Buzzer	x	o	o	o	o	o
Adapter	x	o	o	o	o	o
Screws	o	o	o	x	o	o

o: 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.

x: 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.