



LV9000 User Manual

Date: October. 2015

About This Manual

This document introduces the user interface and menu operations of LV9000 Facial Recognition device. For installation, please refer to the **Quick Guide**.

Important Claim

Firstly thank you for purchasing the LV9000, before use, please read this manual carefully to avoid the unnecessary damage! The company reminds you that the proper user will improve the use affect and authentication speed.

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

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

Due to the constant renewal of products, the company can not undertake the actual product in consistence with the information in the document, also any dispute caused by the difference between the actual technical parameters and

Table of Contents

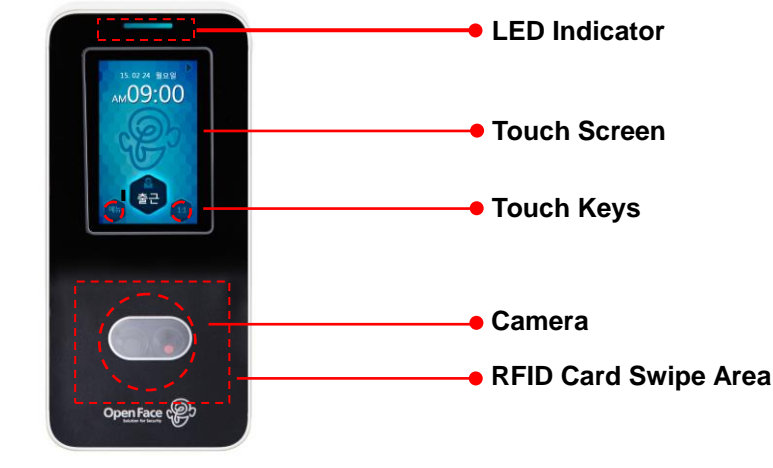
1. Instructions for Use	6
1.1. Appearance of Device	6
1.2. Main Interface	6
1.3. Standing Position and Posture	7
1.3.1. Recommended standing-distance from device:.....	7
1.3.2. Recommended Posture (pose) vs. poor Posture (pose):	7
1.3.3. Face Enrollment.....	7
1.4. Verification Modes	8
1.4.1. Face Verification	8
1.4.2. Password Verification	9
1.4.3. ID Card Verification.....	9
1.4.4. Combination Verification.....	10
2. Main Menu.....	11
3. Add User	13
3.1. Entering a Name.....	13
3.2. Entering a User ID	14
3.3. Enrolling a Password.....	14
3.4. Enrolling an ID card	15
3.5. Enrolling a Face.....	15
3.6. Modifying User Rights	16
3.7. Enroll Photo	16
3.8. User Access Settings.....	17
4. User Management	18
4.1. Query a User	18
4.2. Edit a User	19
4.3. Delete a User.....	19

5. Network Settings	20
5.1. TCP/IP Configuration	20
5.2. RS232/RS485	20
5.3. Wiegand Output	21
5.3.1. Wiegand 26-bits Output Description	21
5.3.2. Wiegand 34-bits Output Description	23
5.3.3. Customized Format	24
5.3.4. Wiegand Input	26
6. System Settings	28
6.1. Sound Parameters	28
6.2. Display Parameters	29
6.3. Face Parameters	29
6.4. Log Settings	30
6.5. Toolbar Definitions	31
6.5.1. Set shortcut key	31
6.5.2. Use shortcut keys	33
6.6. Access Control Settings	33
6.6.1. Time Zone Setting	34
6.6.2. Holiday Setting	34
6.6.3. Group Setting	36
6.6.4. Unlock Combination Setting	37
6.6.5. Access Control Parameters	38
6.6.6. Alarm Parameters	38
6.6.7. Anti-Passback Setting	39
6.6.8. Advance Setting	39
7. Data Management	41
7.1. Search Record	41
7.2. Search Photo	42

8. Date/Time Settings	43
8.1. Set Date/Time	43
8.2. Bell Setting	43
9. Test	45
10. USB Disk Management	47
11. System Information	48
Appendix	49
A. Photo ID Function	49
B. Multi-combination Authentication Mode	50
C. Anti-PassBack	52
D. Print Mode	54

1. Instructions for Use

1.1. Appearance of Device



1.2. Main Interface



Date: The current date is displayed.

Screen Shortcut Keys: Press these shortcut keys to display the attendance status. Users can customize the function of each shortcut key. For details, see [6.5 Toolbar Definitions](#).

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

Attendance Status: The current attendance status is displayed.

1:1 Switch button: By pressing this key, you can switch to the 1:1 verification modes.

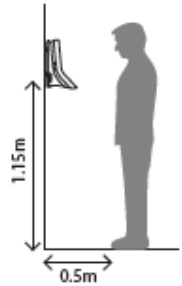
MENU: You can enter the main menu by pressing this key.

1.3. Standing Position and Posture

1.3.1. Recommended standing-distance from device:


For users 5-6 feet tall (1.55m-1.85m), we recommend users stand about 2 feet (0.5m) from the wall.

When viewing your image on the device display window, step away if your image appears too bright. Step closer if your image appears too dark.



1.3.2. Recommended Posture (pose) vs. poor Posture (pose):



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

1.3.3. Face Enrollment

During the enrollment, position your head such way 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 eyes position during the face registration.

The 3 step of face enrollment is as follows:



1.4. Verification Modes

1.4.1. Face Verification

1) 1: N Face Identification

The terminal compares current face image collected by the camera with all face data on the terminal.

- ① The device automatically distinguishes face verification.
- ② Compare the facial in a proper way. For details, see [1.3 Standing Position and Posture](#). Comparison of interface display the current image collected by the camera, an interface as shown in Figure 1 will be displayed.
- ③ If the verification is successful, an interface as shown in Figure 2 on the below will be displayed. If verification is fail, an interface as shown in Figure 3 on the below will be displayed.



Figure 1

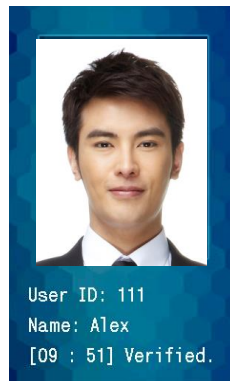


Figure 2



Figure 3

2) 1:1 Face Verification

In the 1:1 face verification mode, the device compares 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] as shown in Figure 4 on the below to enter the 1:1 verification mode.
- ② Enter User ID as shown in Figure 5 on the below, then press the [1:1] button to enter 1:1 face verification mode. If the prompt "Unregistered user!" is displayed, the user ID does not exist.
- ③ Compare the face in a proper way as shown in Figure 6.
- 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.

1. Instructions for Use



Figure 4

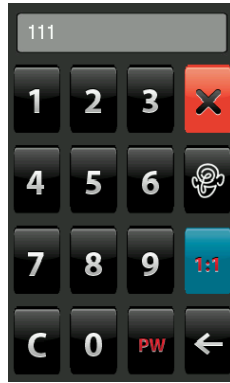


Figure 5

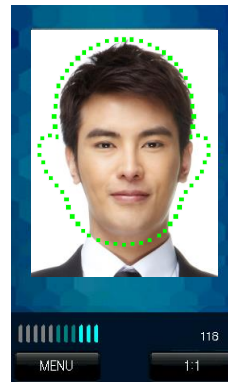


Figure 6

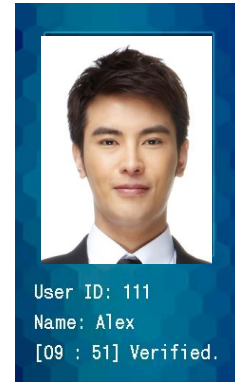


Figure 7

1.4.2. Password Verification

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

- ① Press [1:1] on the screen as shown in Figure 8 to enter the password verification mode.
- ② Enter the user ID and then press the "PW" key as shown in Figure 9 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" key as shown in Figure 10 to start the password comparison.
- ④ If the verification is successful, the device will prompt "Verified". Otherwise, the device will prompt "Verify fail" as shown in Figure 11 and return to password input interface.



Figure 8

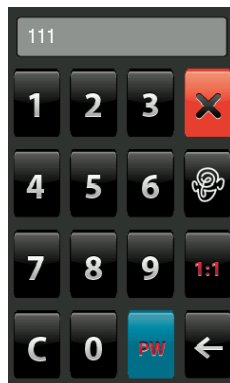


Figure 9

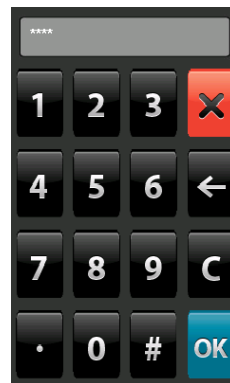


Figure 10



Figure 11

1.4.3. ID Card Verification

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

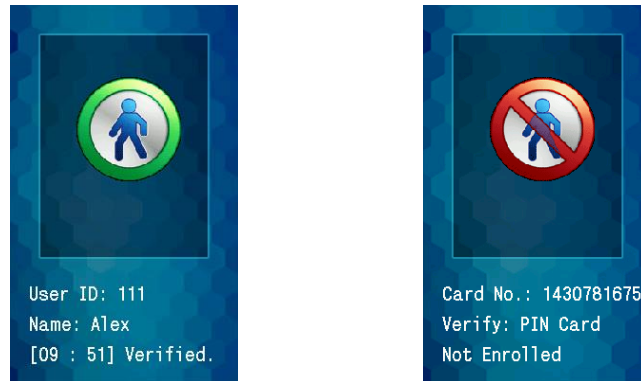
ID Card Only: Users only need to swipe their ID cards for verification.

ID + Facial Verification: After passing the ID card verification, you also need to perform facial verification.

1) ID Card Only

Swipe your ID card on the card swipe area by adopting the proper way. For the card swipe area, see [1.1 Appearance of Device](#).

If the verification is successful, the device will prompt “Verified”. Otherwise, the device will prompt “Not Enrolled”.



2) ID + Facial Verification

(1) Swipe your ID card properly at the swiping area to enter the 1:1 facial verification mode.

(2) Compare the facial in a proper way. For details, see [1.3 Standing Position and Posture](#).

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

1.4.4. Combination Verification

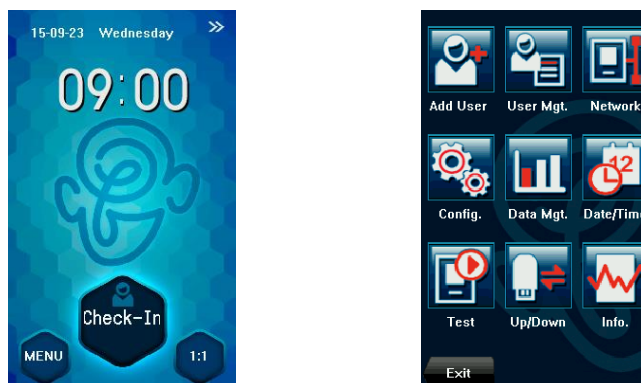
The device supports up to 8 verification modes, including FACE/RF/PW, FACE&PW, FACE&RF, PW, RF, FACE, PW/RF, PW&RF&FACE. For details, see [Appendix B](#).



2. Main Menu

There are two types of rights respectively granted to two types of users: the **Ordinary users** and **administrators**. Ordinary users are only granted the rights of face, 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 9 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, face, card, password, rights, and user access.

User Mgt.: Through this submenu, you can browse the user information stored on the device, including the user ID, name, face, card, password, rights and user access. Here you can also add, modify or delete a user's information.

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

Config. Through this submenu, you can set system-related parameters, including the basic parameters, interface parameters, face and attendance parameters, 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 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.

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

Up/Down: Through this submenu, you can download user information and attendance data stored in the device through a USB disk to related software or other terminal.

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



Any user can access the main menu by pressing the [MENU] 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 using the

3. Add User

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



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

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

Password: Enroll a user's password. The device supports 1-8 digit passwords by default.

Card: Enroll a user's RFID card.

Face: Enroll a user's face.

Role: Set the right of a user. A role is set to **user** by default and can also be set to **administrator**. Ordinary users are only granted the rights of face or password 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. During user verification is succeed, the user's photo is displayed on screen.

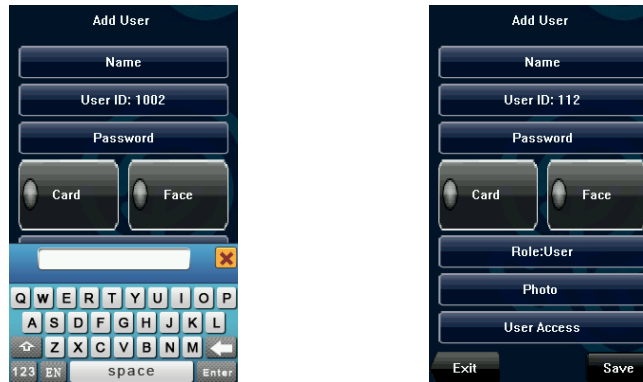
User Access: Set the lock control and access control parameters.


3.1.Entering a Name

Enter the user name through the keyboard.

- ① Press [Name] on the [Add User] interface to display the name input interface.
- ② On the displayed keyboard interface, enter a user name and press [X].
- ③ After the user name 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.




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


3.2.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.

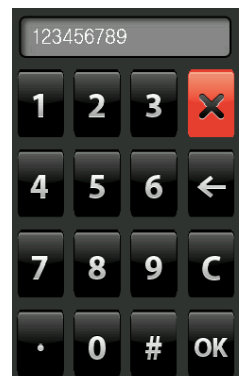
- ① Press [User ID] on the [Add User] interface to display the user ID management interface.

 **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 and press [OK]. If the message “The user ID already exists!” is displayed, enter another ID.

 **Tip:** The device supports 1 to 9 digits user IDs by default. If you need to extend the length of current user ID numbers, please consult our commercial representatives or technical pre-sales.

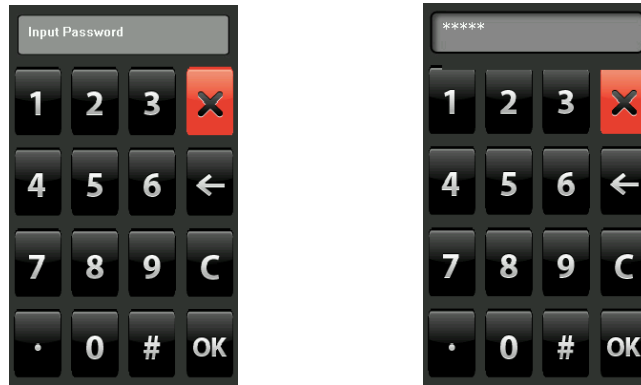
- ③ After the user ID is entered, press [Save] to save the current information and return to the previous interface. Press [Exit] to return to the previous interface without saving the current information.




3.3.Enrolling a Password

- ① Press [Password] on the [Add User] interface to display the password management interface.
- ② On the displayed keyboard interface, enter a password and press [OK]. Re-enter the password according to the system prompt and then press [OK].

4. User Management

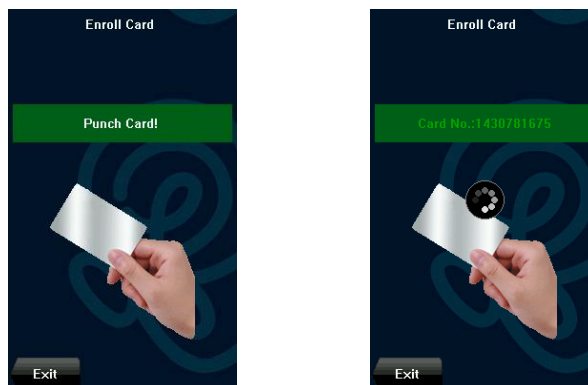


 **Tip:** The device supports 1-8 digit passwords by default.

- 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.

3.4. Enrolling an ID card

- ① Press [Card] on the [Add User] interface to display the [Enroll Card] interface.
- ② The “Punch Card!” message pops up as shown in Figure. Swipe your ID card properly in the swiping area. For details, see [1.1 Appearance of Device](#).
- ③ If the card passes the enrollment, the device will display a prompt message “Card No.: *****”, and returns to the [Add User] interface.



- ④ 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.

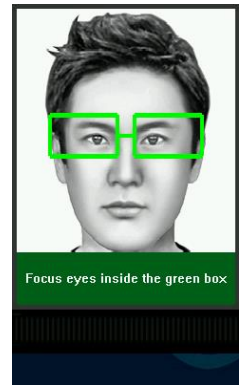
3.5. Enrolling a Face

- ① Press [Face] on the [Add User] interface to display the face enrollment interface.
- ② On the displayed face enrollment interface, position your head such way that your face appears in the center of the

device display window, and follow the voice prompts "Focus eyes inside the green box", so as to enroll different parts of your face into the system to assure the accurate verification.

See [1.3.3 Face Enrollment](#).

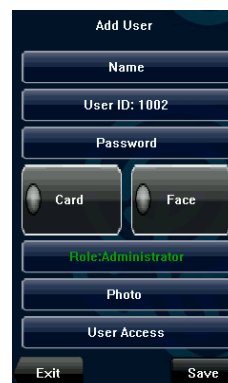
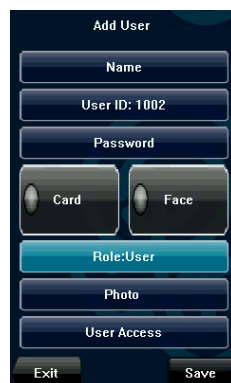
- ③ If your face image is enrolled successfully, the system will display a prompt message and automatically return to the [Add User] interface.
- ④ Press [Save] to save the current information and return to the previous interface. Press [Exit] to return to the previous interface without saving the current information.



3.6.Modifying User Rights

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



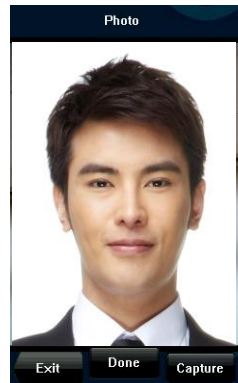
3.7.Enroll Photo

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

- ① Press [Photo] on the [Add User] interface to display the photo enrollment interface.

4. User Management

- ② On the photo enrollment interface, stand naturally in front of the screen. For details, see [1.3 Standing Position and Posture](#). Press [Capture] to capture the photo.
- ③ After taking the photo, press [Exit] to return to the previous interface.
- ④ After the photo is taken, 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. User Access Settings

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

[User Access] settings are to set the user's access rights to verify and open the door, such as the Verify Type, Time Zone.

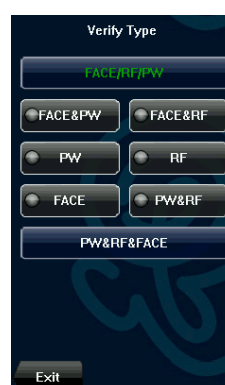
1) Verify Type

Select the verification mode for this user. That will not affect other users.

2) Time Zone

- Group Time Zone: If the user uses the group time zone that he belong to.
- Individual time zone: Select the time zone of this user instead of the group time zone. That will not affect other users in the group.

For details, see [6.6.1 Time Zone Setting](#).



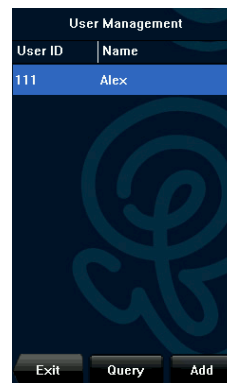
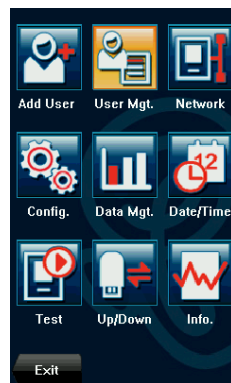
4. User Management

Browse the user information, including the user ID, name, face, ID card, password, rights, and capture mode 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.



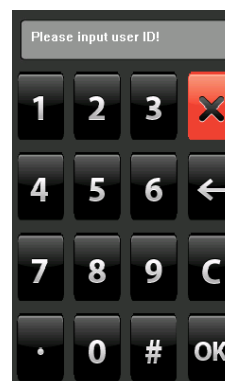
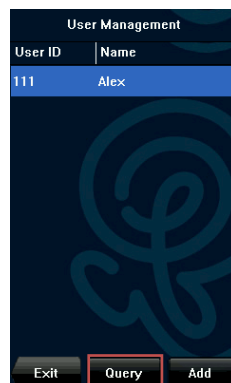
Note: The users are listed in alphabetical order by last name. If you press a user name, you can access the editing interface of this user to edit or delete the related user's information.

4.1. Query a User

To facilitate administrators to locate a user quickly from a large number of enrolled users, the device enables to query by "User ID".

User ID Query:

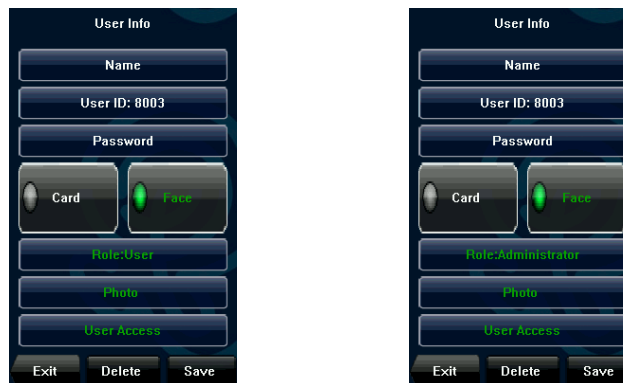
- ① Press [Query] on the [User Management] interface to display the User ID query interface.
- ② Enter the user ID on the displayed interface, and click [OK] to locate the cursor on the desired user.



4.2. 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 add a user. You can re-enroll your face, change your password, and modify the management rights.

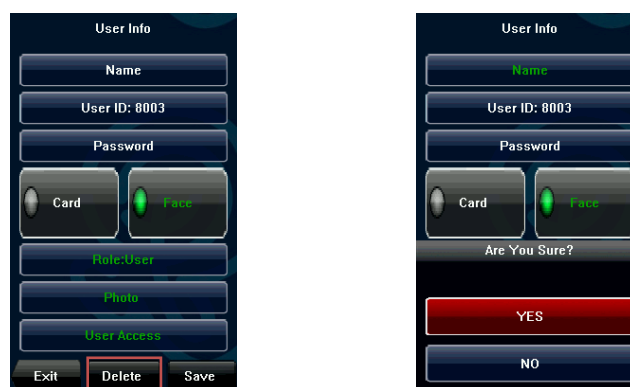
For example: Change the user rights from ordinary user to Administrator as shown below.



4.3. Delete a User

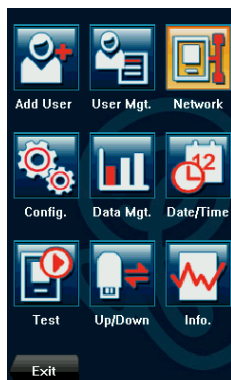
On the [User Info] interface, you can delete all or partial user information.

- 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], [Face] or [Password] to delete the related user information and to re-enroll the new information follow the device prompt.



5. Network Settings

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



5.1. TCP/IP Configuration

IP Address: The IP address is 192.168.1.201 by default and can be changed as required.

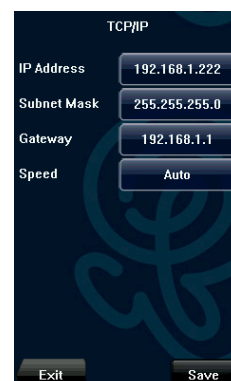
Subnet Mask: The subnet mask is 255.255.255.0 by default and can be changed as required.

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

Speed: The speed is “Auto” by default and can be changed depending on the network environment.



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

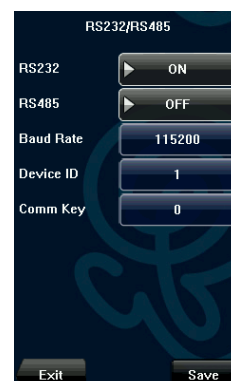


5.2. RS232/RS485

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 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 digits passwords are supported.

5.3. Wiegand Output

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

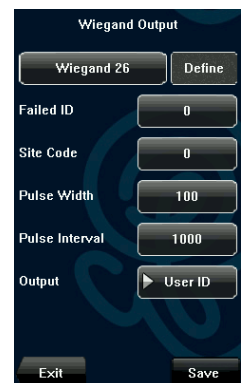
Failed ID: Refers to the value output by the system upon verification failure. The output format is subject to the setting of “Wiegand Format”. The default value scope of Failed ID is 0-65535.

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

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

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

Output: Refers to the contents output upon successful verification. You can select the “User ID” or “Card Number” as the output.



5.3.1. Wiegand 26-bits Output Description

The system has a built-in Wiegand 26-bits format. Press [Wiegand Output], and select “Wiegand 26-bits”.

The composition of the Wiegand 26-bits format contains 2 parity bits and 24 bits for output contents (“User ID” or

“Card Number”). The binary code of 24-bits represent up to 16,777,216 (0–16,777,215) different values.

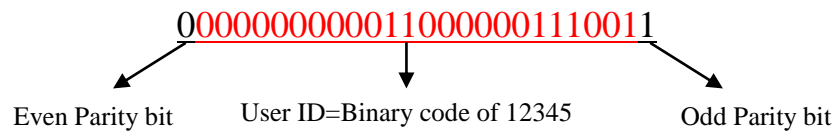
1	2	25	26
Even	User ID/Card Number		Odd

Definition of Fields:

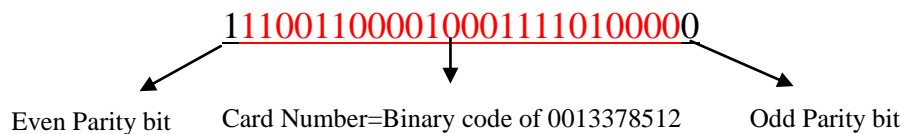
Field	Meaning
Even parity bit	Judged from bit 2 to bit 13. The even parity bit is 1 if the character has an even number of 1 bit; otherwise, the even parity bit is 0.
User ID/ Card Number (bit 2-bit 25)	User ID/Card Number (Card Code, 0–16777215) Bit 2 is the Most Significant Bit (MSB).
Odd parity bit	Judged from bit 14 to bit 25. The odd parity bit is 1 if the character has an even number of 1 bit; otherwise, the odd parity bit is 0.

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

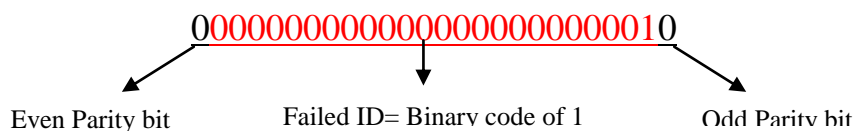
1. When the output is set to “User ID”, the Wiegand output is as follows upon successful verification:




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



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



 **Note:** If the output contents exceed the scope allowed for the Wiegand format, the last several bits will be adopted and first several bits are automatically discarded. For example, the user ID 888 888 888 is 110 100 111 110 110 101 111 000 111 000 in binary format. Wiegand26 only supports 24 bits, that is, it only outputs the last 24 bits, and first 6 bits “110 100” are automatically discarded.

5.3.2. Wiegand 34-bits Output Description

The system has a built-in Wiegand 34-bits format. Press [Wiegand Output], and select “Wiegand 34-bits”.

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

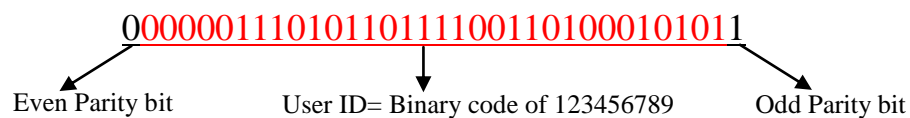
1	2		33	34
Even	User ID/Card Number			Odd

Definition of Fields

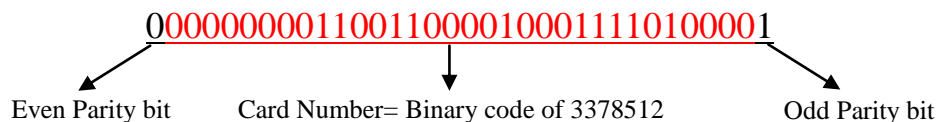
Field	Meaning
Even parity bit	Judged from bit 2 to bit 17. The even parity bit is 1 if the character has an even number of 1 bit; otherwise, the even parity bit is 0.
User ID/Card Number (bit 2-bit 33)	User ID/Card Number (Card Code, 0–4,294,967,295) Bit 2 is the Most Significant Bit (MSB).
Odd parity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

For example, for a user with the user ID of 123456789, the enrolled card number is 0013378512 and the failed ID is set to 1.

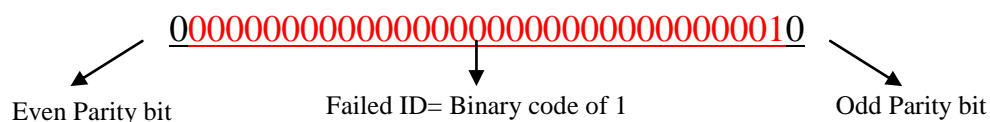
1. When the output is set to “User ID”, the Wiegand output is as follows upon successful verification:



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



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



5.3.3. Customized Format

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

The customized format consists of two character strings: the **Card Format** bits and **Parity Format** bits. These two character strings need to be defined separately.

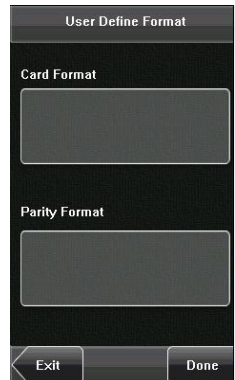
Card Format bits define the number of binary bits output by Wiegand as well as the meaning of each bit. The data bits output by Wiegand can be a card number (C), site code (s), facility code (f), manufacturer code (m) and parity bits (p).


Parity Format bits define the check mode of each bit in data bits and ensure the correctness of data bits during transfer through the parity check. The parity bits can be set to odd check (o), even check (e) and both odd check and even check (b). There is a one-to-one correspondence relationship between the data bits and parity bits.

For example, the Wiegand26 can be customized as follows:

Definition of Card Format bits: psssssssscccccccccccccccp

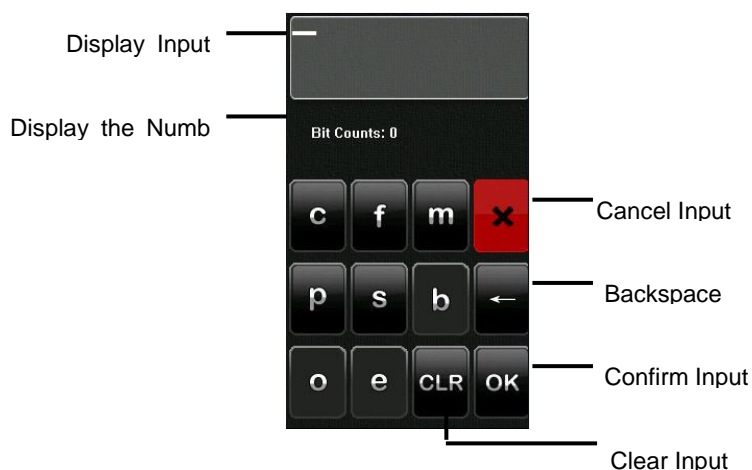
Definition of Parity Format bits: eeeeeeeeeeeeeo00000000000000



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

To customize Wiegand format, proceed as follows:

- ① Select [User Define Format] and the [Define] 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 Card Format 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.

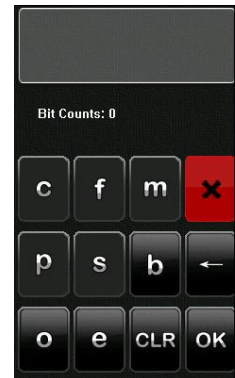
f: Indicates the facility code which is 0 by default. It is not configurable. To modify it, please contact the equipment supplier.

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 Format 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

Card Format bits:

pp

Parity Format bits:

```

eeeeeeeeeeeeeeee000000000000000000

```

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

Card Format bits: pmmmmsssssssssscccccccccccccccccp

Parity Format bits: oeobeobeobeobeobeobeobeobeobeobeobe

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

Card Format bits:

pmmmfrrrrrrrrsssscccccccccccccccccp

Parity Format 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

Card Format bits: psssssssssssscccccccccccccccccccccccccccccccccp

Parity Format bits:

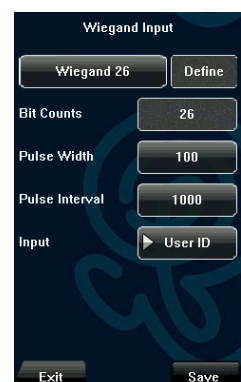
eeeeeeeeeeeeeeeeeeeeoooooooooooooooooooooooooooo

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.

5.3.4. Wiegand Input

Wiegand Format: The system has two built-in formats Wiegand 26-bits and Wiegand 34-bits, and also supports the format customization function to meet individualized requirements. About the Wiegand format, please refer to [5.3 Wiegand Output](#).

Bit Counts: Wiegand data digit length.



5. Communication Settings

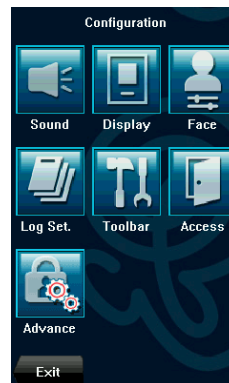
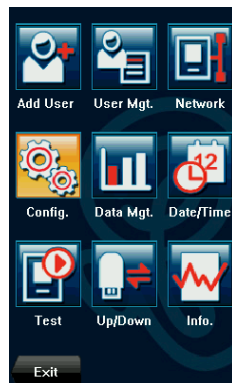
Pulse Width: Pulse width is 100 microseconds by default, which can be adjusted from 20 to 800.

Pulse Interval: It is 1000 microseconds by default, which can be adjusted between 200 and 20000.

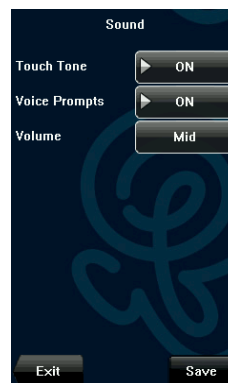
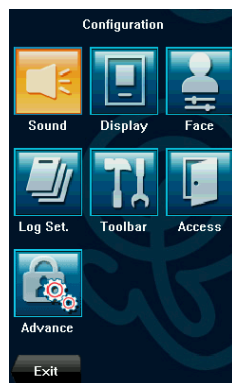
Input: Content contained in Wiegand input signal, including User ID or card number.

6. System Settings

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



6.1. Sound Parameters

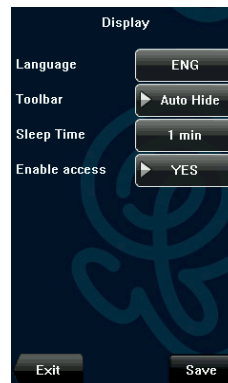
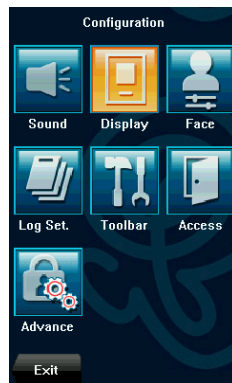


Touch Tone: This parameter is used to set whether to generate beep sound in response to every keyboard touch. Select “ON” to enable the beep sound, and select “OFF” to mute.

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

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

6.2. Display Parameters



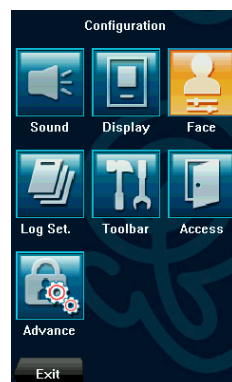
Language: This parameter is used to display the current language used by the device. For multilingual-capable devices, you can switch between different languages through this parameter. Then you should restart the device.

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 “Unhide”. By selecting “Auto Hide”, you can manually display or hide the toolbar. By selecting “Unhide”, you can permanently display the toolbar on the initial interface.

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

Enable access: This parameter is used to set whether to use [Access] on the [Config.] menu.

6.3. 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 all face templates 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.

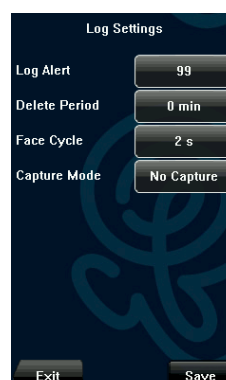
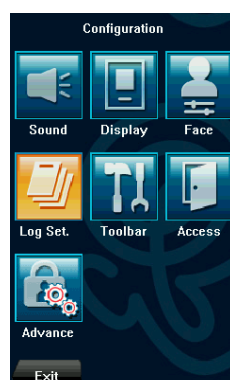
Quality: This parameter is used to set a quality threshold for the face images obtained. The device accepts the face images and processes them by adopting the face algorithm when their quality is higher than the threshold; otherwise, it filters these face images.

Capture Times: When the capture mode is set to “Capture, Capture & Save, Fail to Capture”, you can set how many times 1 user can try to verify.

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.

6.4. 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).

Delete Period: 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).

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

Capture Mode: According to your need, select one among several options.

1. No Capture: Does not capture face photo.
2. Capture: After verification success, face photo is captured but not saved.
3. Capture & Save: After verification success, face photo is captured and saved.
4. Capture the Fail: After verification fail, face photo is captured and saved.

6.5. Toolbar Definitions

Define touch screen functional shortcut keys. Definition method of shortcut keys is described as follows:



6.5.1. Set shortcut key

The method to set shortcut keys is described as follows:

- ① Click the [**Toolbar**] to display the list of the existing shortcut keys; click the shortcut key to modify, as shown in figure 12. Enter the edit screen, and click **Function** box, as shown in figure 13. Enter the **Function** screen, and the user can select desired settings for the type of the shortcut keys according to practical needs, as shown in figure 14.

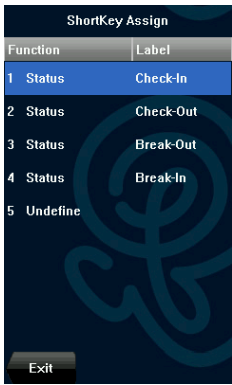


Figure 12

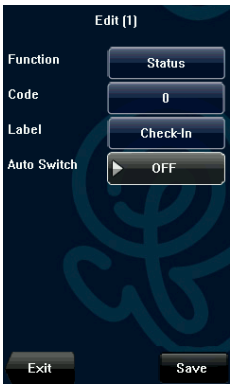


Figure 13

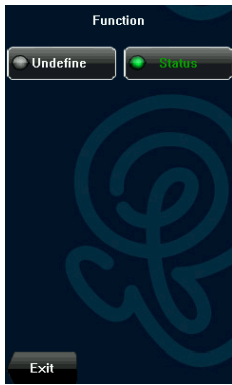


Figure 14

- ② The user can set the shortcut key as status key; click the Status, as shown in figure 12 above; enter the edit screen of the status key and click the Label box, as shown in figure 15 below; enter the Label screen, as shown in figure 16 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 key according to practical needs.

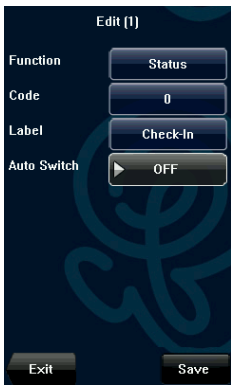


Figure 15



Figure 16

- 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 17 below.

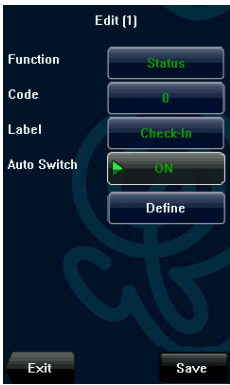


Figure 17

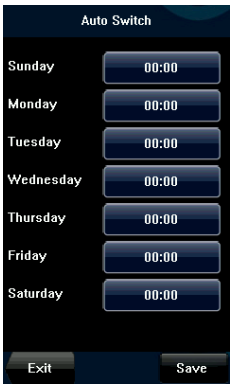


Figure 18

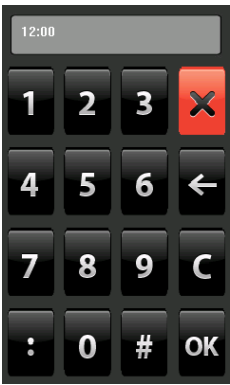


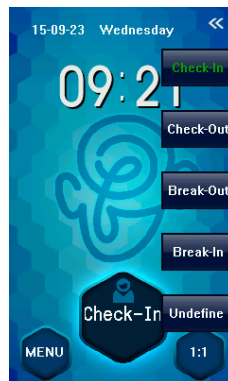
Figure 19

6. System Settings

- ④ Click the time box after “week”, as shown in figure 18 above, to enter the time setting screen, as shown in figure 19 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 **ShortKey Assign** screen.

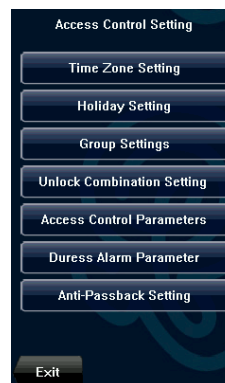
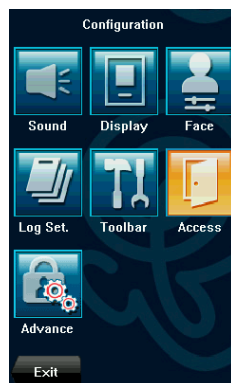
6.5.2. Use shortcut keys

Click << on the initial interface, and the related status and function keys are displayed on the right corner of the interface for use.



6.6. Access Control Settings

Access control settings are to set related device parameters. It is not enabled by factory default, you can click [MENU]-[Config.]-[Display]-[Enable access], select YES or NO.



To unlock, the enrolled user must accord with the following conditions:

- ① The current unlock time should be in the effective time of the user time zone or group zone.
- ② The group where the user is must be in access control (or in the same access control with other group, to open the door together).

The new enrolled user is under the first group by default, and use the No. 1 group time zone, the No. 1 access control

group. The new enrolled user is in unlocking state (if you have modified the related settings of access control, the system will be changed with the modification).

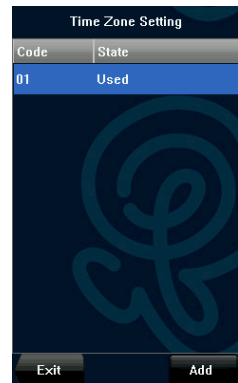
6.6.1. Time Zone Setting

Time Zone is the minimum unit of access control option. The whole system can define 50 time zones. Every time zone consists of seven time sections (that is, one week). Every time section is the effective time zone within 24 hours every day. Every user can set 3 time zones. It's "or" between the three zones. It is effective if only one is satisfied. Every time section format is HH:MM-HH:MM, namely, accurate to minute.

If end time is smaller than start time (23:57- 23:56), the whole day is forbidden. If end time is bigger than start time (00:00- 23:59), it is effective section.

Effective time zone for user unlocking: 00:00-23:59 or end time is bigger than start time.

Notice: System default time zone 1 as whole day open (namely, the new enrolled user is unlocking).



6.6.2. Holiday Setting

Special access control time may be needed during holidays. It is different to modify everybody's access control time. So a holiday access control time can be set, which is applicable for all employees.

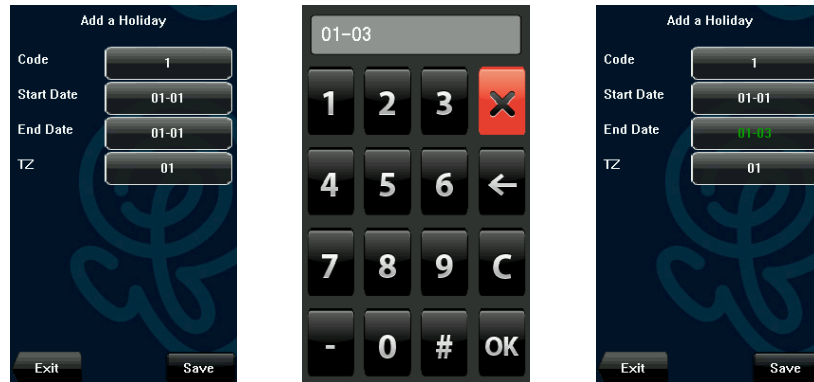
1) Add holiday:

① Press the [Add] to enter [Add a Holiday] interface.

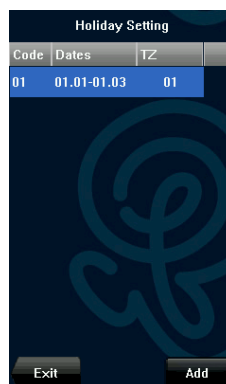


② Press the touch screen number key to set the value(Start/End Date, TZ), after setting, press [OK] to save, and press [X] for exit and return to the previous interface.

6. System Settings



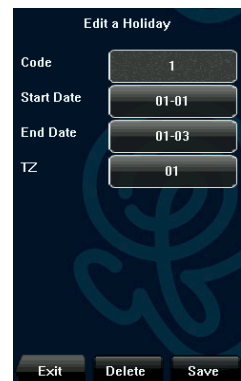
- ③ Press [Save] to save the current information and return to the previous interface; press [Exit] directly to return to the previous interface without saving the current information.



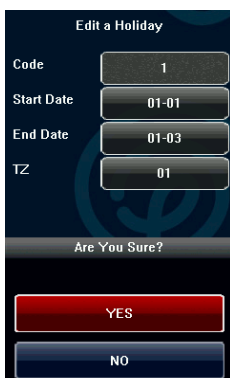
2) Edit holiday

Select the holiday to be edited and enter the edit interface. The edit operation is similar to add holiday. After editing, press [Save] to save and return to the previous interface.

Notice: If holiday access control time is set, user's open door time zone during holiday is subject to the time zone here.



3) Delete holiday

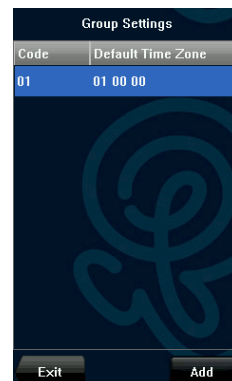


Select the holiday to be deleted. Press [Delete] to popup the confirm interface as follows.

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

6.6.3. Group Setting

Grouping is to manage employees in groups. Employees in group use group time zone by default. Group members can also set 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 the key to edit the items.

Code: Enter the number edit interface to set the value.

Verify Type: Select the Group Verify Type.

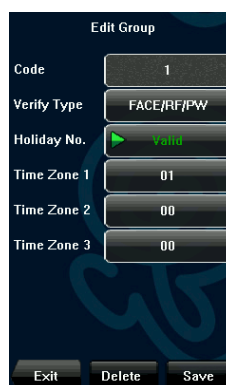
Holiday No.: Select if the Time zone is valid in holiday.

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.

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

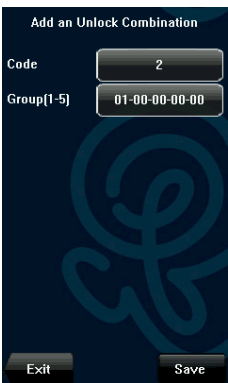
Press the line to be edited, and enter the edit interface. After editing, press [Save] to save the current information and return to the previous interface; press [Exit] directly to return to the previous interface without saving the current information.

3) Delete group time zone

Select the line to be deleted. Press [Delete] to popup the confirm interface as follows. Select [Yes] to delete this holiday, otherwise select [No] to cancel the operation.

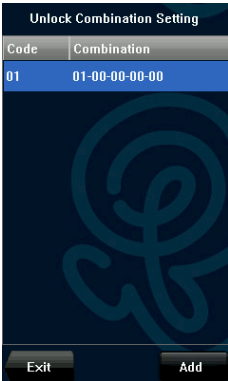
6.6.4. Unlock Combination Setting

Make various groups into different access controls to achieve multi-verification and improve security. An access control can be made up of 5 groups at most.



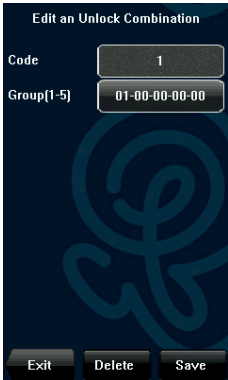
1) Add Unlock Combination

- ① Enter holiday add Combination Setting interface, press the key to edit the items.
- ② Press the touch screen number key to set the value, after setting, press [OK] to save, and press [X] for exit and return to the previous interface.
- ③ 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.

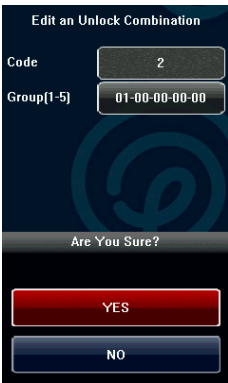


2) Edit Unlock Combination

Select the line to be edited. Press the item directly to enter the edit interface. 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.



3) Delete Unlock Combination



Select the line to be deleted. Press [Delete] to popup the confirm interface as follows. Select [Yes] to delete this holiday, otherwise select [No] to cancel the operation

6.6.5. Access Control Parameters

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

Lock Delay: Indicates the duration for the device to place the electric lock in open state.

(Value scope: 1-10 seconds)

Sensor Delay: Indicates the delay for checking the door sensor after the door is opened. If door sensor state is inconsistent with the normal state set by the door sensor switch, an alarm will be triggered, and this period of time is regarded as the “door sensor delay”. (Value scope:

1-99 seconds)

Sensor Mode: Includes the None, Normally Open (NO), and Normally Closed (NC) modes. “None” indicates that the door sensor switch is not used. “NO” indicates that the door sensor is 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: When the failed press times reach the set times, alarm signal will come out (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.

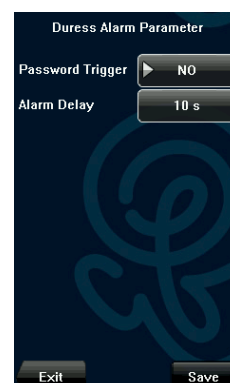
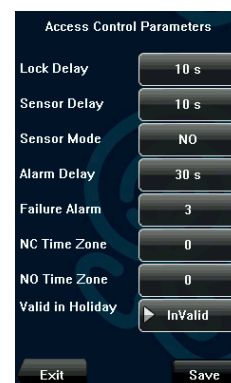
Notice:

- 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.

6.6.6. Alarm Parameters

Password Trigger: If select “Yes”, alarm signal will come out when a user use password verification mode.

Alarm Delay: The alarm signal will not output immediately after alarm gets triggered. After the defined delay time, the alarm signal will be generated automatically (0-255 sec).



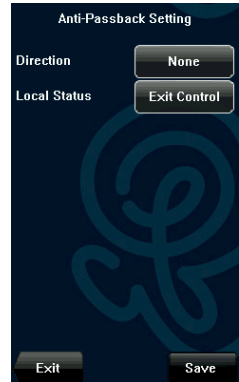
6.6.7. Anti-Passback Setting

Set the device Anti-Passback function.

Direction: There are four options: None, APB-Out, APB-In, APB-Out/In.

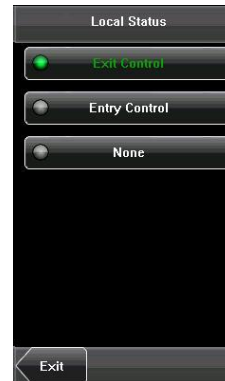
Local Status: There are three options: Exit Control, Entry Control and None.

For Anti-Pass back function, please refer to [Appendix C](#).



Anti-Pass back setting operation:

- ① Enter Anti-Pass back setting interface, press the key to edit the items.
- ② Set the [Direction] and [Local Status], after setting; press [Exit] to return to the previous interface.



- ③ 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.

6.6.8. Advance Setting



1) Firmware Update

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

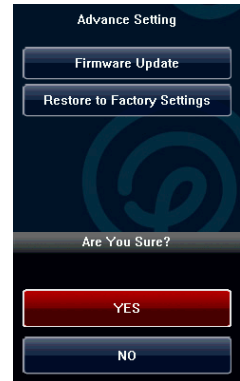
Notice.

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

2) Restore to Factory Settings

Restore all parameters on the device to factory settings.

On the confirm interface as seen in the right, select [Yes] to restore to factory settings, otherwise select [No] to cancel the operation.



7. Data Management

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



Delete Log: Delete all the attendance records.

Delete Picture: Delete the verification succeeded photos and failed photos on the device.

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

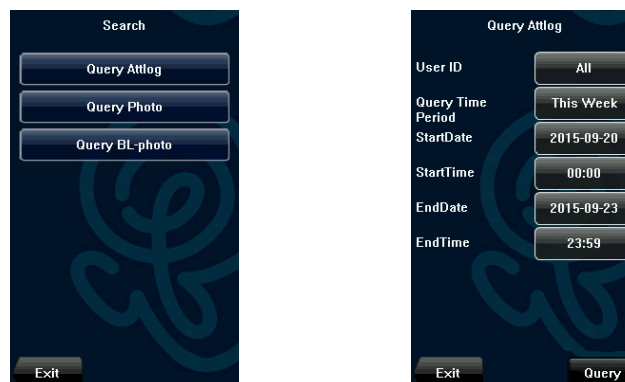
Clear Administrator: Change all administrators to ordinary users.

Search: Query the attendance records.

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

7.1. Search Record

After successful check-in, the employee's attendance records are saved in the device. You can easily query these attendance records.



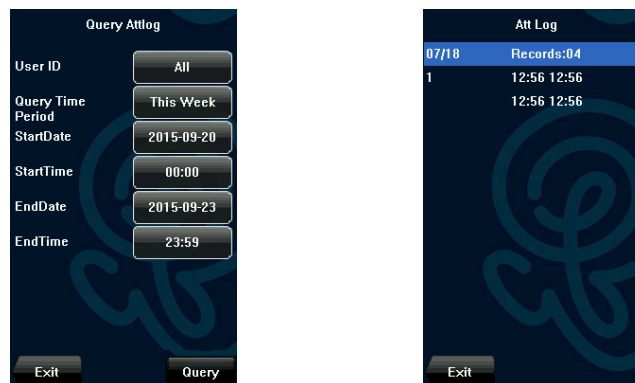
User ID: Enter the user ID of the employee to query. If this field is left blank, you can query the attendance records of all the employees. If you enter a user ID, you can query the attendance records of this employee.

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.

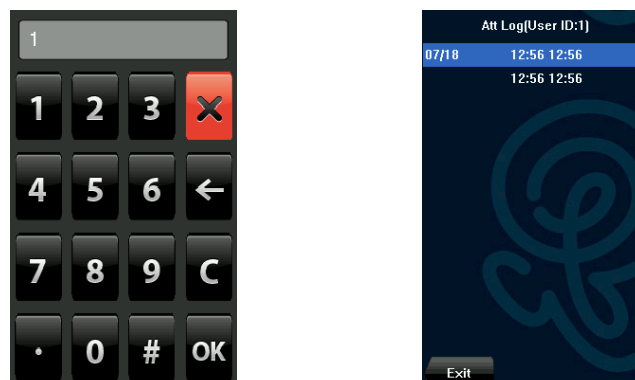
Start and End: When you select a customized time period, you need to input a start time and an end time. When you select other options for the time period, the start and end time will be automatically adjusted to the related time.

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



7.2. Search Photo

After capturing the photo, the employee's success photo(Query photo) or fail photo(Query BL-photo) are saved in the device.

You can easily query these photos by the same operation with attendance record search as described in [7.1 Search Record](#).

8. Date/Time Settings

8.1. Set Date/Time

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



- ① Press **[MENU]** on the initial interface to display the main menu interface.
- ② Press **[Date/Time]** on the main menu interface to display the time setting interface.
- ③ Select the desired date and time by pressing the parameter. For the time format, there are 10 formats to select from.
Both 12-hour and 24-hour time systems are supported.
- ④ 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.

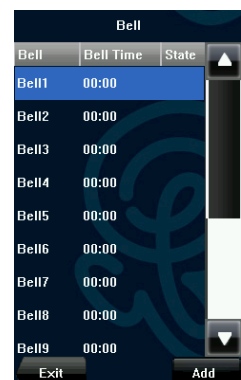
8.2. Bell Setting

Lots of companies need to ring their bells to signal the start and end of work shifts, and they usually manually ring their bells or use electric bells. To lower costs and facilitate management, we 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 and triggers the relay at the alarm time, and stop playing the ring tone after the set duration. Each device can be added with 15 alarm bells at most.

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

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.

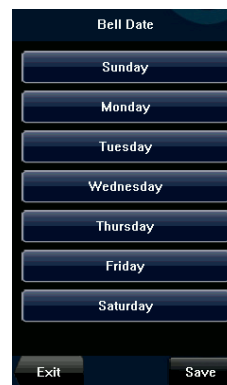
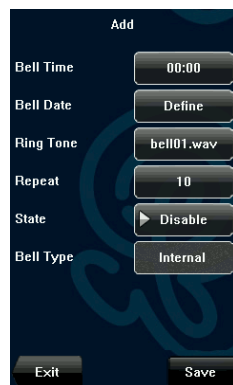
Ring Tone: This parameter is used to set the bell ring tone.

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

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

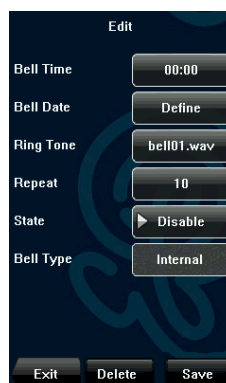
State: This parameter is used to set whether to enable the bell.

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.



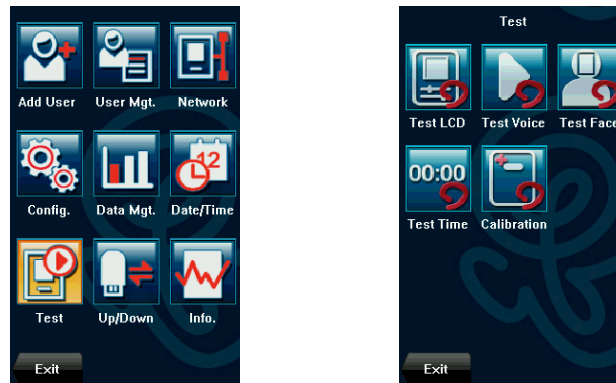
2) Edit and delete a bell

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

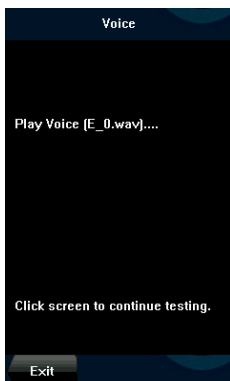
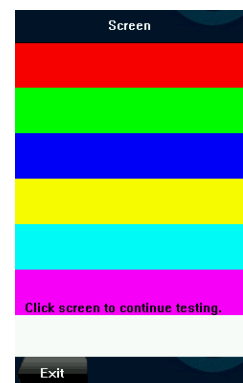


9. Test

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.



Test LCD: 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].

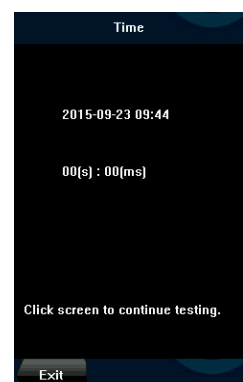


Test Voice: The device automatically tests whether the voice files are complete and the voice quality is good by playing the voice files stored in the device. You can continue the test by touching the screen.

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.

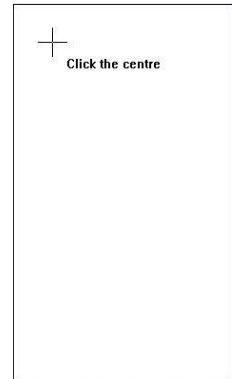
Test Time: The device tests whether its clock works properly by checking the stopwatch of the clock. Touch the screen to start counting, and touch it again to stop to check whether the counting is accurate. Press [Exit] to exit the test.

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 main menu interface.
- ② Press [Calibration] on the [Auto Test] interface to display the screen calibration interface.
- ③ Touch the center of the cross “+”.
- ④ Repeat Step 3 following the move of the “+” icon to different locations on the screen.
- ⑤ Touch the center of the cross at five locations on the screen correctly. When the message “Calibrating screen, pls wait.....” is displayed on screen, the calibration succeeds and the system automatically returns to the main menu. If the calibration fails, the system recalibration will start from Step 3.



10. USB Disk Management

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



Download Log: Download all the attendance data from the device to a USB disk.

Download User: Download all the user information, face images from the device to a USB disk.

Download User Picture: Download the employees' photos from the device to a USB disk.

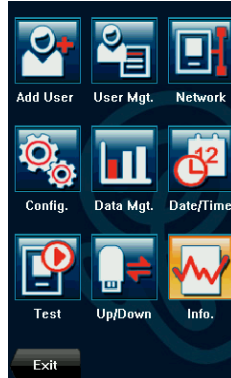
Download Capture: Download the captured attendance picture from the device to a USB disk.

Upload User: Upload the user information, face images stored in a USB disk to the device.

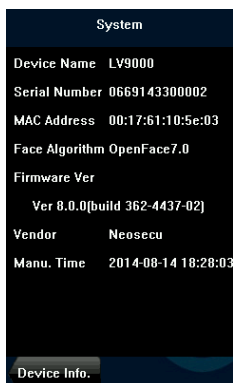
Upload User Picture: Upload the JPG files that are named after the user IDs and stored in a USB disk to the device, so that user photos can be displayed after the employee passes the verification.

11. System Information

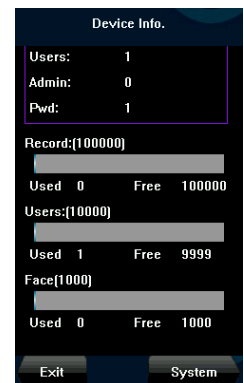
You can check the storage status as well as version information of the device through the [Info.] option.



Device Info.: The number of enrolled users, administrators and passwords are displayed on the [Device Info.] interface; the total face storage capacity and occupied capacity as well as the total attendance storage capacity and occupied capacity are graphically displayed respectively.



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



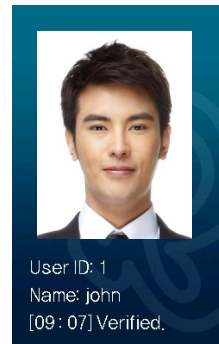
Appendix

A. Photo ID Function

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

[Operation Steps]

1. When the photo taken by the device is used, the photo can be displayed upon successful verification.
2. To use a photo stored in a USB disk, proceed as follows:
 - 1) Create a folder with the name of “photo” in the USB disk, and store users' photos under this folder.
 - 2) The user photos must be in JPG format and named after their IDs. For example, for the user with the user ID of 154, the photo name must be 154.jpg.
 - 3) Insert the USB disk into USB slot on the device, and select [Up/Down] -> [Up.UserPic.]. 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 64K bit.
- 3) The uploaded new user photo will overwrite the existing photo in related to the user ID.
- 4) To download user photos, select [Up/Down] -> [Dn.UserPics.].

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.

B. Multi-combination Authentication Mode

We provide a personal or group Multi-combination Authentication Mode for high security Access control area, verification type main include four elements that are User ID (PIN), Face (FACE), Password (PW) and RF card (RF), which can combine into multi-combination.

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

These symbols illustrate what follow the table different means.

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

If Face, Password and Card have been enrolled for the user, the verification procedure is follow. In order to enter PIN, press [1:1] button in initial interface.

Type	What you do
FACE/RF/PW	FACE or RF or PW are verified
	1) FACE(1:N)
	2) PIN++FACE(1:1)
	3) PIN+PW+"OK"
FACE&PW	4) RF(1:N)
	FACE + PW are verified
	1) FACE(1:N)+PW+"OK"
	2) PIN+FACE(1:1)+PW+"OK"
FACE&RF	3) PIN+PW+"OK"+FACE
	FACE + RF are verified
	1) FACE(1:N)+RF
	2) PIN+FACE(1:1)+RF
PW	3) RF(1:N)+FACE
	Only PW is verified
RF	PIN+PW+"OK"
	Only RF is verified
	RF(1:N)

Appendix

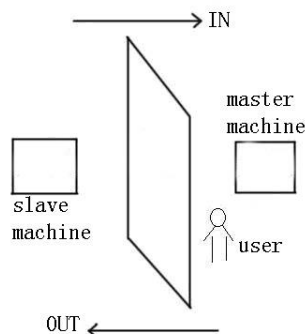
FACE	FACE are verified
	FACE(1:N)
	PIN+FACE(1:1)
PW&RF	PW + RF are verified
	1) PIN+PW+“OK”+RF
	2) RF(1:N)+PW
FP&PW&RF	FACE + PW + RF are verified
	1) FACE(1:N)+PW+“OK”+RF
	2) PIN+FACE(1:1)+PW+“OK”+RF
	3) RF(1:N)+PW+“OK”+FACE
	4) PIN+ PW+“OK”+FACE(1:1)+RF

C. Anti-PassBack

[Overview]

Sometimes, some illegal people follow the other one into the gate, which will cause the 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 of the door (master machine hereinafter), the other is installed outside of the door (slave machine hereinafter). Wiegand signal communication is adopted 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-pass back according to user's recent in-out record. In record and out record must be matched.

This machine supports out, in, or out-in anti-pass back.

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

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

When the master machine is set as "out-in anti-pass back", if the user wants to come in and go out normally, if his

recent record is “out” and “in”, then his next record must be “in” and “out”.

[Operation]

1. Select model

Master machine: The machine with Wiegand in function, except for F10 reader.

Slave machine: The machine with Wiegand Out function.

2. Menu setting of Anti-pass back

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

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

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

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

Control-in: When it is set, the verified 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-pass back 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-> Network->Wiegand..

4. Enroll user

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

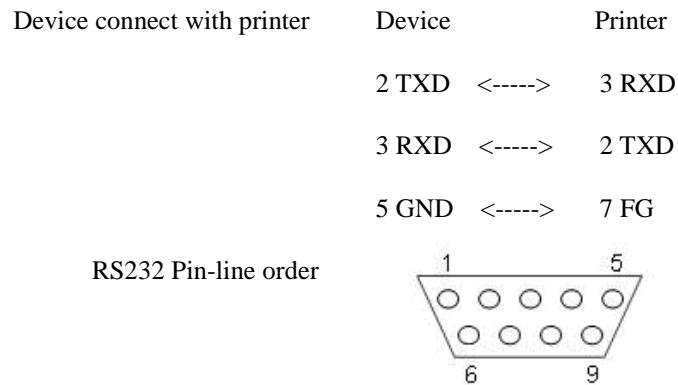
5. Connection instruction

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

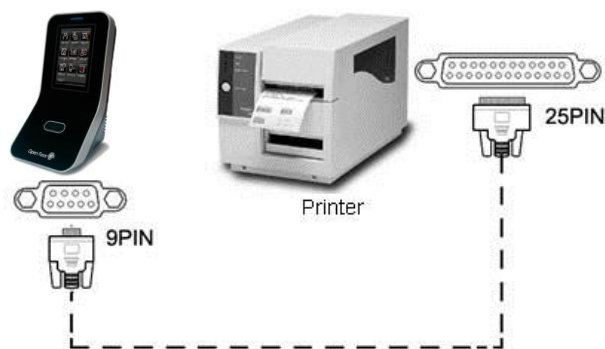
Master		Slave
IND0	<----->	WD0
IND1	<----->	WD1
GND	<----->	GND

D. Print Mode

This function is designed for a serial port printer only, the parallel printer is unavailable. The printing content output via RS232. After a user is verified, the result will be sent out through serial port. If device connect with the printer the result can be printed directly, can also use the Super Terminal to view the output content.



【Connection】



【Instructions】

1. In the device menu, press Menu-Network-RS232/RS485 and select baud rate as 19200.
2. Select the print mode. There are 6 print modes to choose.

Notice:

1. It will print garbled information or can't print when baud is not selected 119200.
2. When print mode is mode 5, it will prompt as the follows after attendance verification.



Press OK to print record in mode 5. Press Cancel to not print record.

Appendix

For example: San punched the card at 13:24:55 on September 1, 2009, there are different print formats to select.

Version 1

00001 San 09/09/01 13 : 24 : 55 I

Version 2

User No : 00001

Date Time Check-In

09/09/01 13 : 24 : 55

Version 3

San 00001 09/09/01 13 : 24 : 55

Version 4

Break-In

15 : 24 : 55 01/09/2009

00001

Version 5

00001 09.09.01 13 : 24 : 55 Check-In

Version 6

00001

Date Check-In

09.09.01 13 : 24 : 55

Version 7

User ID: 00001

Check-In

09.09.01 13 : 24 : 55

Note:

1. Be sure that the device and printer (Super Terminal) have the same baud rate.
 2. If the default print format can not meet your needs, you contact our business deputy our company is able to present other customized format
-

Built-in printer

There are some models with built-in printer, and they have the function of printing in real time. When user verified successful, the device can immediately print attendance record according to the set print mode. And it will not print if the verification is failed.

Notice: If you need to change the print mode, please contact our business representative or technical support.

Safety Precautions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures.

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio, TV technical for help.
- Only shielded interface cable should be used.

Finally, any changes or modifications to the equipment by the user not expressly approved by the grantee or manufacturer could void the user's authority to operate such equipment.

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received,

including interference that may cause undesired operation of this device.

CAUTION

Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

CE WARNING

- Changes and modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

- It is desirable that it be installed and operated with at least 20cm or more between the radiator and person's body(excluding extremities hand, wrists, feet, and ankles)

FCC ID : 2AGPJLV9000FRT**Specification**

CPU	1GHz DSP
Camera	IR, Normal (Dual CMOS Camera)
LCD	3 inch Touch Screen
Max User(Face)	1,000(1:N)
Max User(ID card)	10,000
Log	Max. Text Log 100,000/Max. Image Log 8,000
Communication	TCP/IP, RS232/485, USB-Host
Wiegand	IN & OUT
ID card	13.56 MHz Mifare Card
Power	12V DC
Operation Temp.(°C)	-20 ~ 50
Dimensions(mm)	86.7(W) x 172.0(H) x 86.0(D)