eSSL

Security at Fingertips

User Manual

2.8 inches Color Screen Facial Recognition Serial

About This Manual

- Not all the devices have the function with ★ . The real product prevails.
- The photograph in this manual may be different from that of the real product. The real product prevails.

Important Claim

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

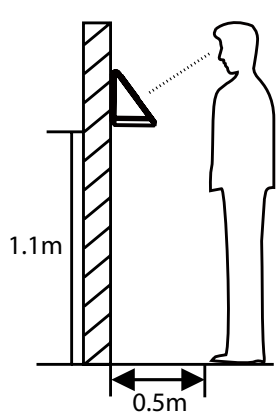
Due to the constant renewal of products, the company cannot undertake the actual product in consistence with the information in the document, also any dispute caused by the difference between the actual technical parameters and the information in this document. Please forgive any change without notice.

Contents

1 Instruction for Use

1.1 Standing Position and Face Expressions

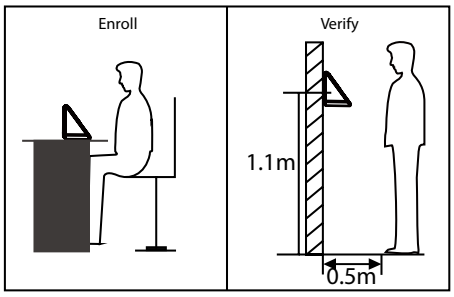
- The best using position:



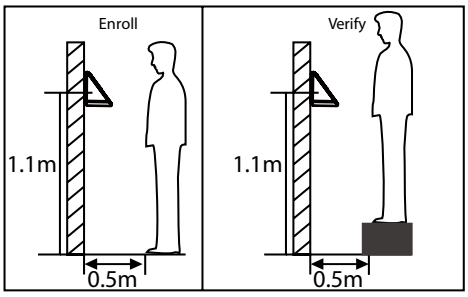
For users 5-6 feet tall (1.55m-1.85m), we recommend users stand about 2 feet (0.5m) from the device. When viewing your image on the device display window, step away if your image appears too bright. Step closer if your image appears too dark.

During enrollment and verification, the installation position of device must remain the same. If need to move the device, keep the same installation height, or else, the recognition function will be poor.

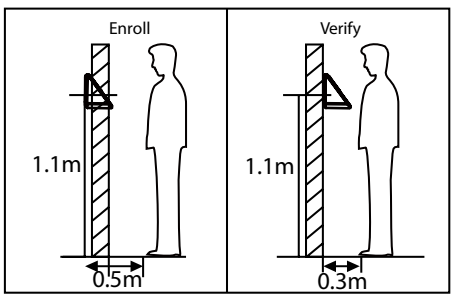
- What are factors make poor verification:



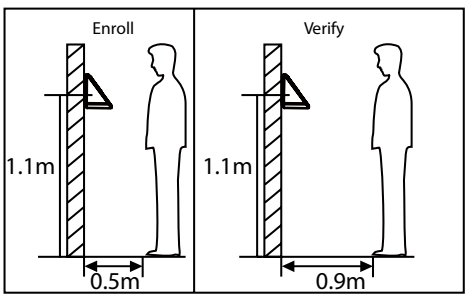
Different Posture



Different Height

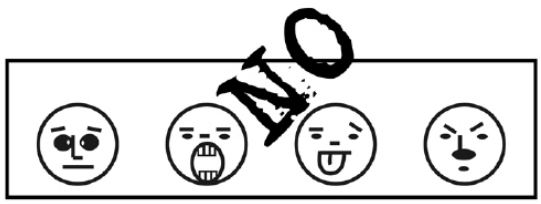


Different Distance

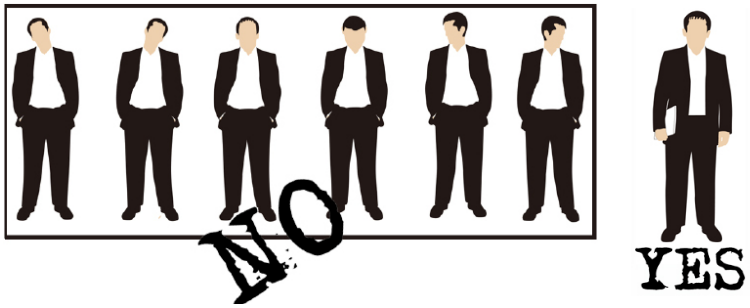


Different Distance

- The best face expressions vs Poor expressions:



• The best posture vs Poor postures:



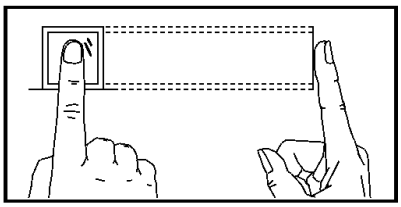
Note: During enrollment and verification, try to have a relaxed face expression and stand upright.

• How to enroll face effectively

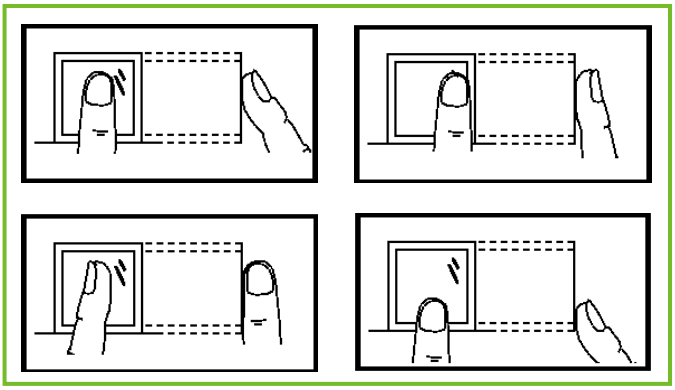
During enrollment, locating your face appears in the center of the screen, and follow the voice prompts "Focus eyes inside the green box". The user needs to move forward and backward to adjust the eyes position during the face registration.

1.2 Finger Placement

Recommended fingers: The index fingers, middle fingers and the ring fingers are recommended to use.
The finger must be flat to the surface and centered on the fingerprint sensor.



Recommended Placement



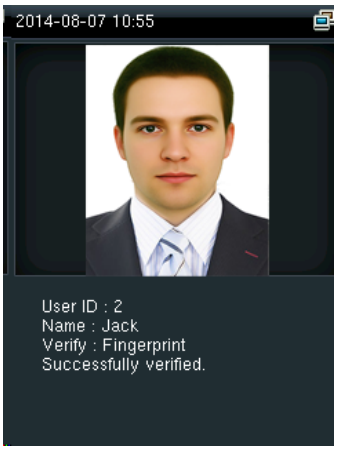
Not Recommended Placement

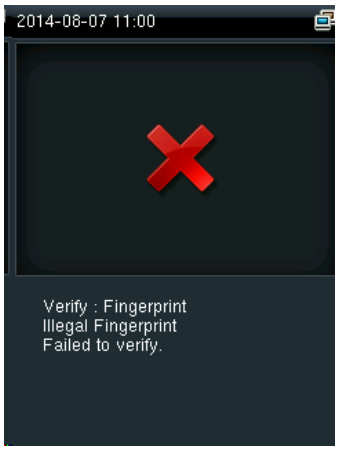
1.3 Verification Modes

1.3.1 Fingerprint verification ★

- 1:N fingerprint verification mode → the device compares current fingerprint with all users fingerprints in the device.

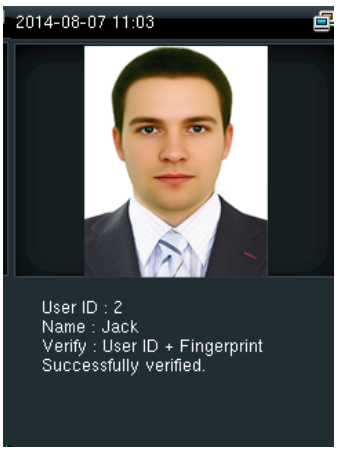
Use the proper way with one of the recommended fingers to enroll and verify.
There are two responses after verification: *Successfully verified* and *Failed to verify*.

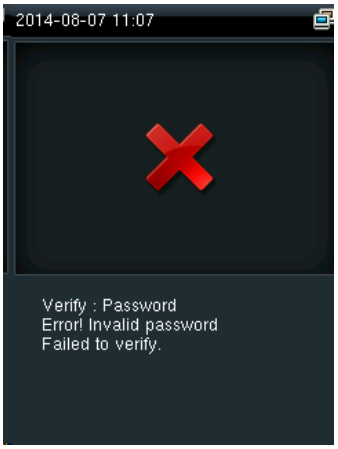




- 1:1 fingerprint verification mode → the device compares current fingerprint with one user's fingerprints whose ID is entered. Users choose this mode unless poor recognition.

Enter User ID and press "*fingerprint*", there are two responses after verification: *Successfully verified* and *Failed to verify*.





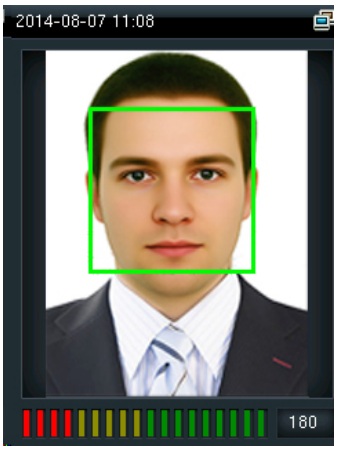
Notes:

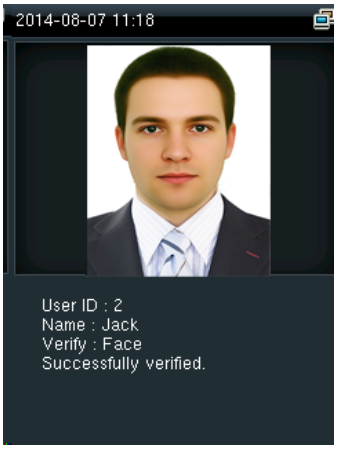
» The device says "*Invalid ID*" when there is no such user.

» The device says "*Please try again*" when failed to verify. You can try another 2 times. If it fails after 3 times, return to the initial interface.

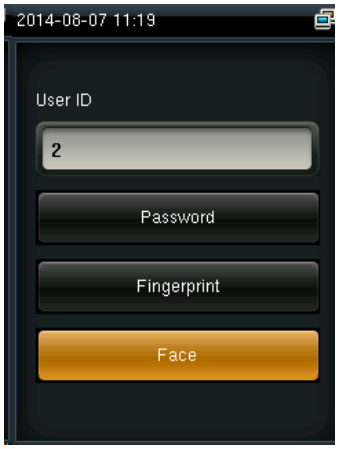
1.3.2 Face verification

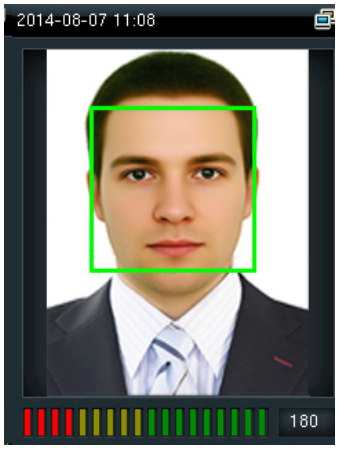
- 1:N face verification mode → the device compares current face with all users' faces in the device. Use the proper way to enroll and verify.

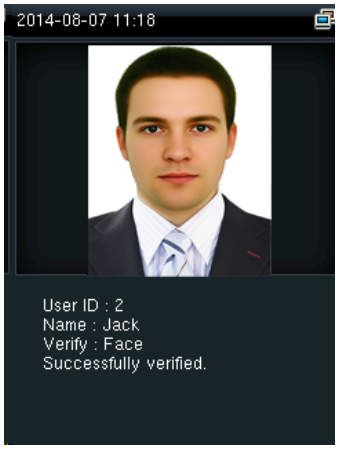




- 1:1 face verification mode → the device compares current face with one user's face whose ID is entered. Enter User ID and press "*Face*".

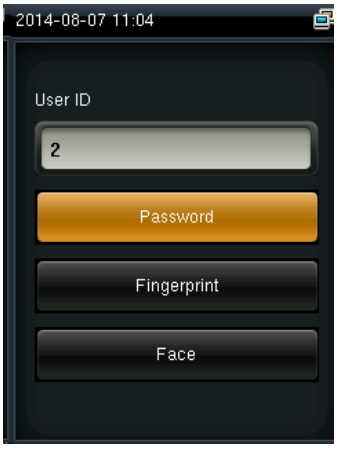


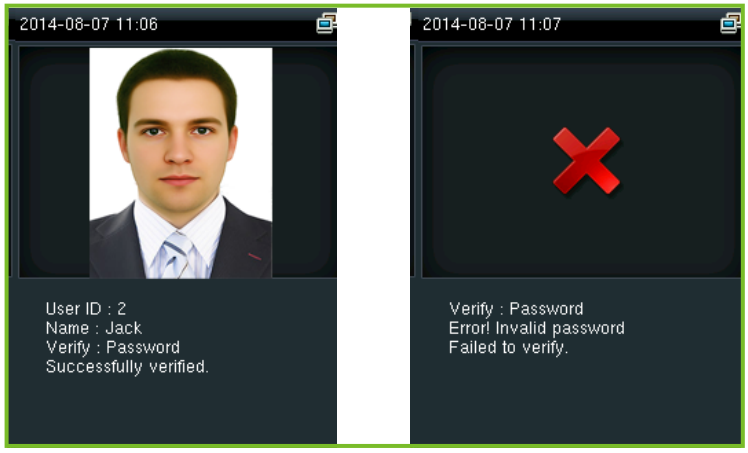




1.3.3 Password verification

The device compares entered password with one user's password whose ID is input. Enter user ID, press "*Password*" and enter your password. There are two responses after verification:

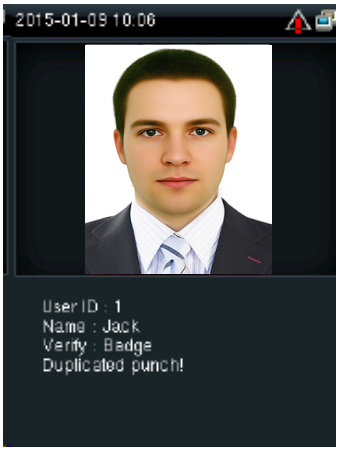




Note: The device says *"Incorrect password"* when failed to verify. You can try another 2 times. If it fails after 3 times, return to the initial interface.

1.3.4 Badge verification ★

Swipe your registered badge surround the fingerprint sensor in standby mode:



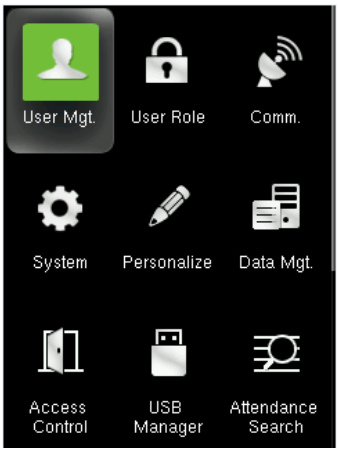
Notes:

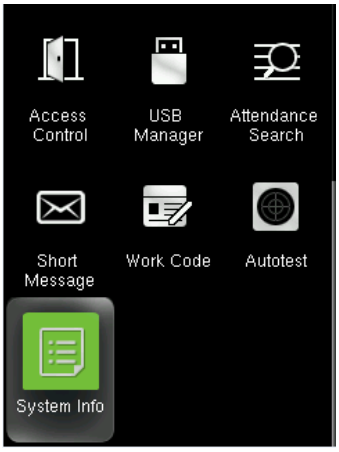
» The device promts *"Duplicated Punch"* when you swipe badge successfully twice.

» The device promts *"Ou-Ou"* when the badge is unregistered.

2 Main Menu

Start the device, press [M/OK] to enter the Main Menu. Press ▼ to scroll page down.





Function introduction:

User Mgt.(User Management): Add, edit and delete users' information, including user ID, name, user role, fingerprint, FC, password, user photo and access control parameters.

User Role: Set the privilege of defined role, that is, the privilege of operating menus.

Comm.(Communication Setting): Set communication parameters between device and PC, such as IP address, subnet mask, gateway, DNS, TCP COMM. Port and so on.

System: Set system parameters, such as date/time, attendance parameters, face and fingerprint parameters, reset and USB upgrade.

Personalize: Set user interface parameters, voice, bell schedules, punch state options and shortcut key mappings.

Data Mgt.(Data Management): Delete/ Backup/ Restore data stored in the device.

Aceess Control: Set access control options, schedule time/holidays/access group/ combined verification group, set anti-passback and duress options.

USB Manager: Download and upload attendance data, user data, work code, short message etc. With USB disk, you can import data restored in the device into attendance software, or import data into other devices.

Attendance Search: It is convenient for employees to search his or her attendance record restored in this device.

Short Message: Add/check/edit/delete public and personal messages. Set options.

Work Code: Add/check/edit/delete work code. If this function is enabled, you must select one or enter an inexistence work code after verification.

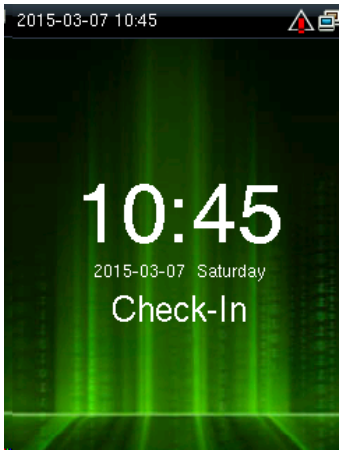
Autotest: Test whether each module is available or not, including LCD, voice, keyboard, fingerprint sensor, face and clock RTC.

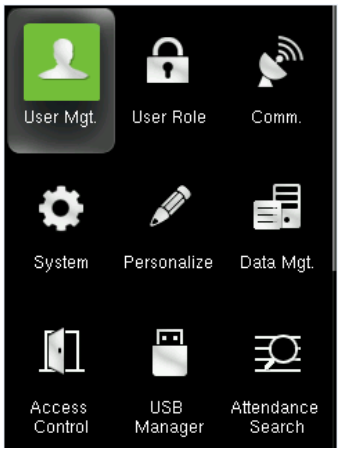
System Info: Check device capacity, basic information and firmware information etc.

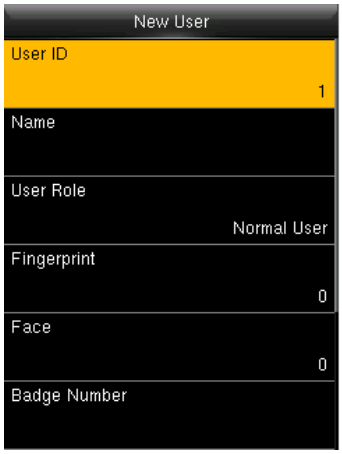
3 User Management

3.1 New User

Only the registered user can make verification in the device.
Start the device, enter into the Main Menu. Enter into "*User Mgt.*" → "*New User*":

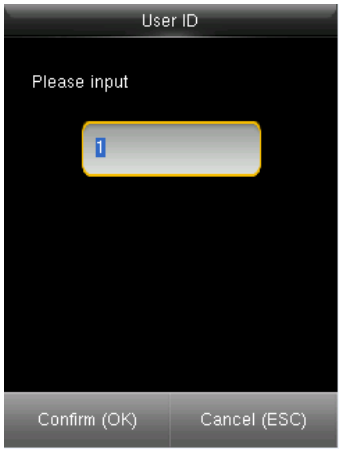


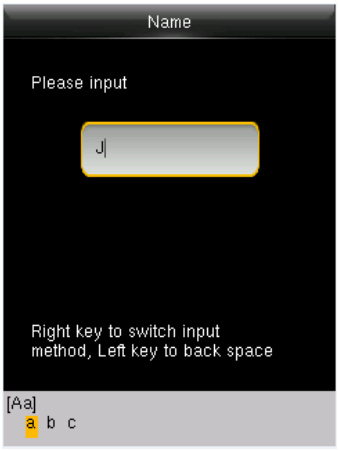




3.1.1 Enter User ID and Name

Press ▼ / ▲ to select "*User ID*"/or "*User Name*" on the **New User** interface , press [M/OK]:

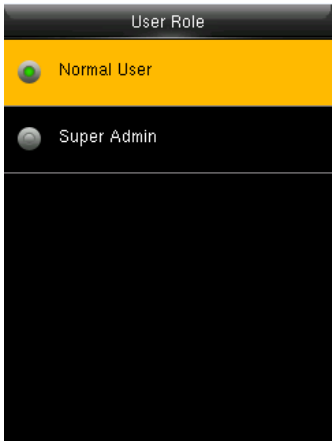




Notes: You can input an ID, or use that the device allocated.
Press ► to switch **T9 Input** character types. Enter name with **T9 Input**. Aout **T9 Input**, refer to "Appendix 1 T9 Input".

3.1.2 Select User Role

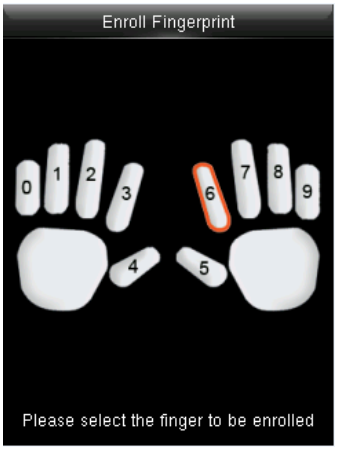
Press ▼ / ▲ to select "*User Role*" on the **New User** interface , press [M/OK]:



Super Admin: A super admin is granted rights to operate all functions and menus in the device.
Normal User: Normal user is only allowed to punch, query its own attendance record, check messages.
Note: You had better to enroll a super admin for ease of management.

3.1.3 Enroll a Fingerprint ★

Press▼ /▲ to select "*Fingerprint*" on the **New User** interface , press [M/OK]:

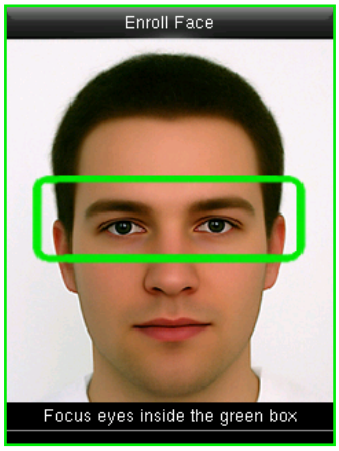


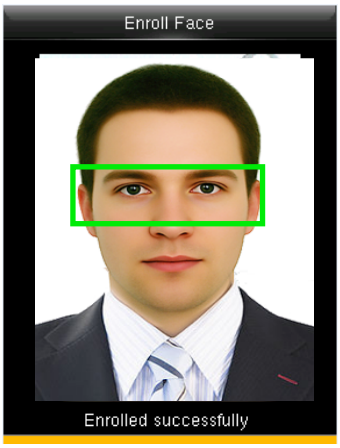
1. Press numeric key corresponding to the fingerprint as you want, then press [M/OK].
2. Press your fingerprint on the sensor three times upon prompting by the device.

Note: You need to reenroll if the device says"*Please try again*".

3.1.4 Enroll a Face

Press▼ /▲ to select "*Face*" on the **New User** interface , press [M/OK]:



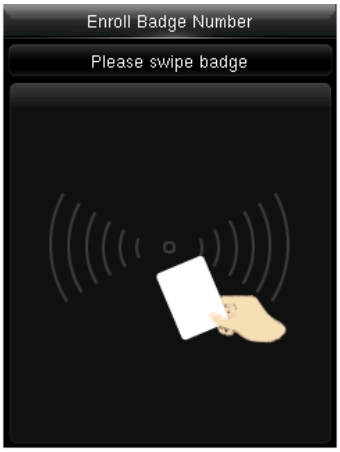


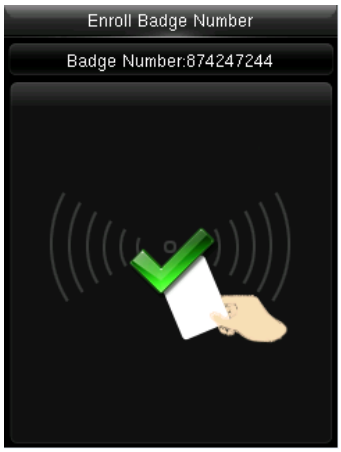
Focus your eyes inside the green box, as the device says.

Note: During face enrollment, a photo will be taken and saved in the device automatically for "*User Photo*" unless another is taken.

3.1.5 Enroll a Badge ★

Press▼ /▲ to select "*Badge Number*" on the New User interface , press [M/OK]:





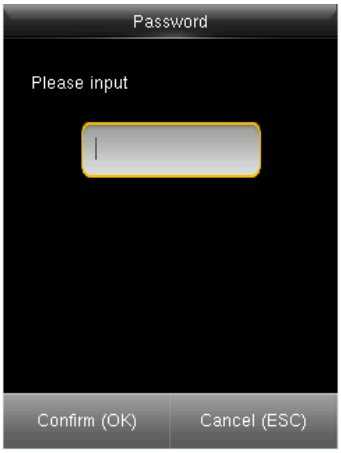
Swipe your badge surround the fingerprint sensor.

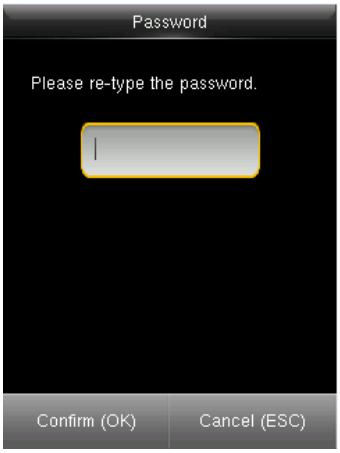
Note: Please take another badge if the device displays "*Error! Badge already enrolled*" .

The Badge must be IC card.

3.1.6 Enroll a Password

Press ▼ / ▲ to select "*Password*" on the New User interface , press [M/OK]:

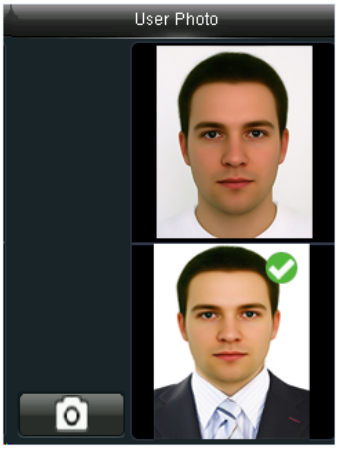




Input 1-8 digits password and press [M/OK], then rewrite the password.

3.1.7 Enroll a Photo

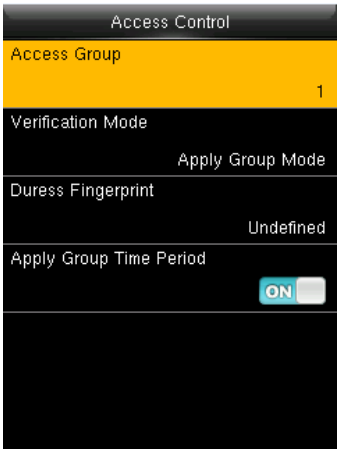
Press ▼ / ▲ to select "*User Photo*" on the New User interface , press [M/OK]:



Keep a good expression and press [M/OK] to take a photo.
The photo displays after the verification is successful.

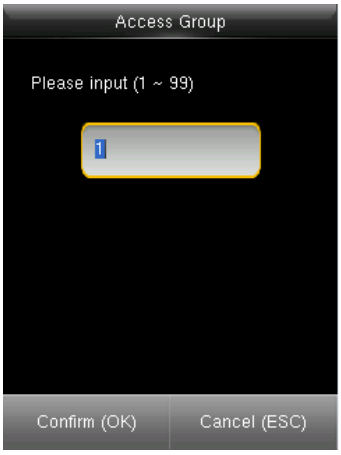
3.1.7 Access Control Role

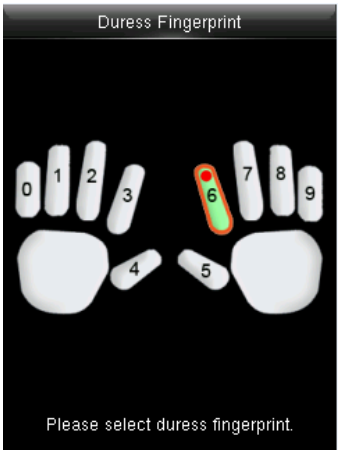
Press ▼ / ▲ to select "*Access Control Role*" on the New User interface , press [M/OK]:

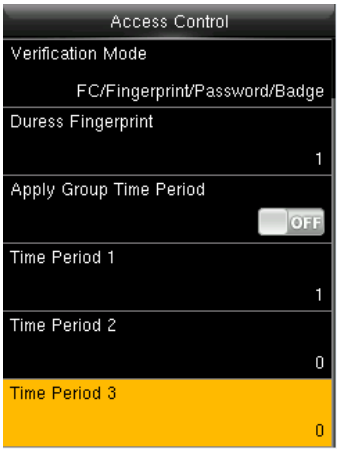


Access Group: Select an access group for the new user.
Verification Mode: Select a mode for the new user to verification.
Duress Fingerprint: Select an enrolled fingerprint as duress fingerprint for the new user.
Apply Group Time Period: Whether to apply group time period for the new user. Select which one to use if not.
Note: For more details about **Access Control**, please refer to "9 Access Control".

- Select Access Group & Duress Fingerprint & Group Time Period

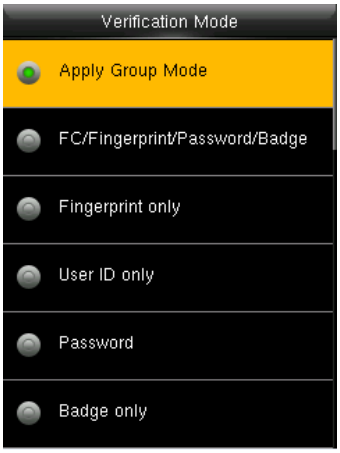






1. The max group number is 99.
2. Choose one or more enrolled fingerprints as duress fingerprints. The device alarms as long as you verify the duress fingerprints.
3. The max time period number is 50.

- Select Verification Mode



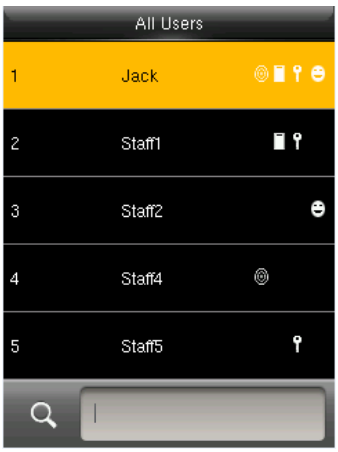
Apply Group Mode: The user use group's verification mode. If you do not use the group's verification mode, there are 21 combination modes: FC/Fingerprint/Password/Badge, Fingerprint only, User ID only, Password, Badge only, Fingerprint/Password etc.
When you choose one of the combination modes, you need to verify all data inside the mode to make the verification done. For example, if the Fingerprint/Password is chosen, you need to verify both fingerprint and password to make the verification done.

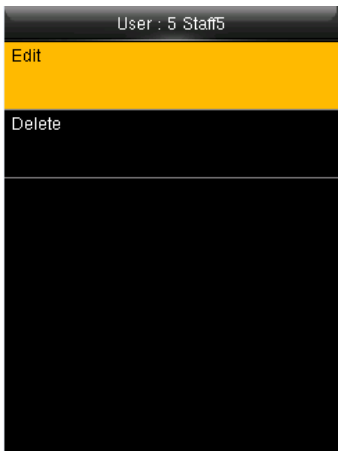
3.2 Manage Users

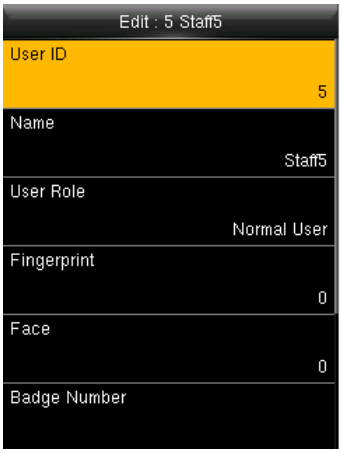
Start the device, enter into the Main Menu. Enter into "*User Mgt.*" → "*All Users*".

- Edit a User

Press ▼ / ▲ to select a user to edit and press [M/OK]. Enter into "*Edit*":



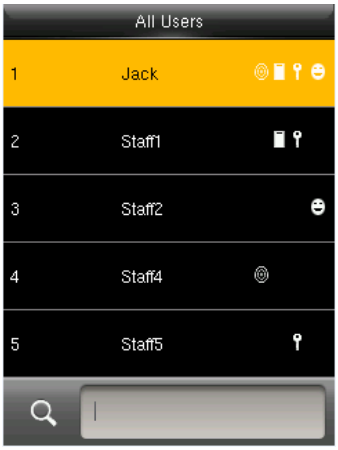


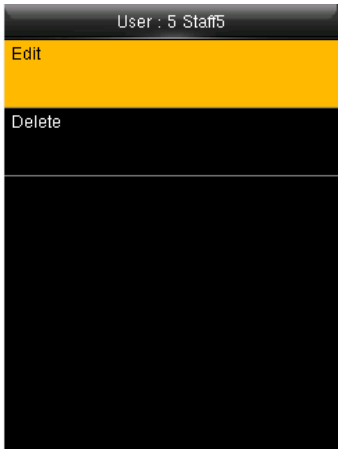


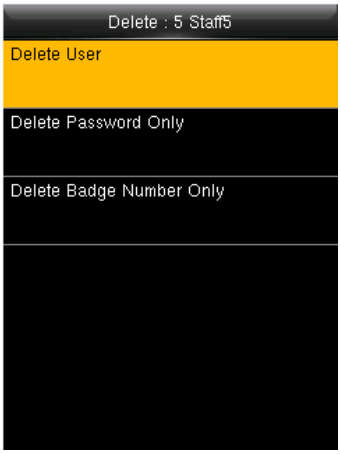
You can modify all information except **User ID**.

- Delete a User

Press ▼ / ▲ to select a user to edit and press [M/OK]. Enter into "*Delete*":

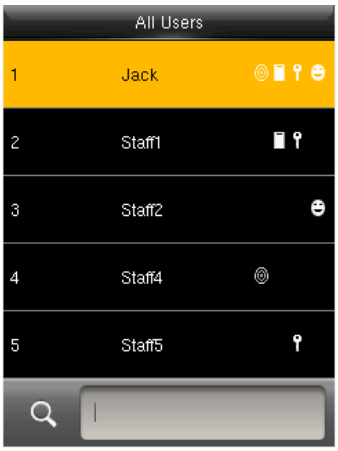


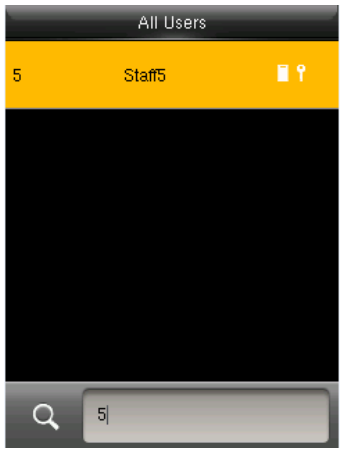




You can choose different kinds of user data to delete.

- Search a User

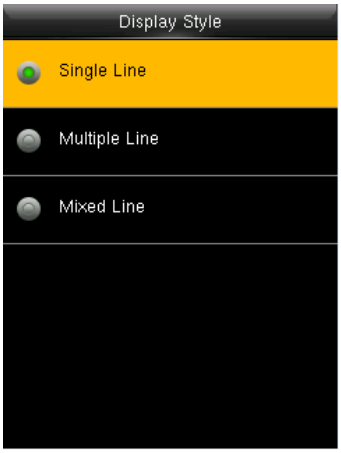




Input the User ID to search a user quickly, then you can edit or delete the user.

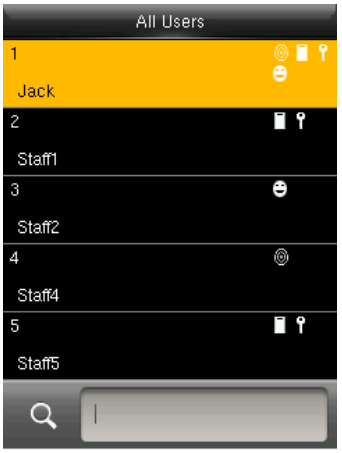
3.3 Display Style

The default style is "*Single Line*". Enter into "*User Mgt.*" → "*Display Style*":



Select a style.

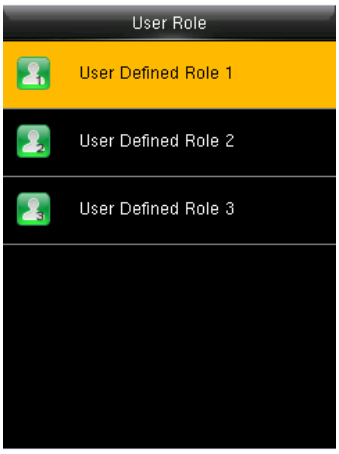
Multiple Line

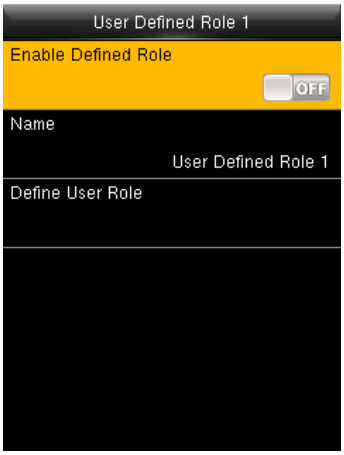


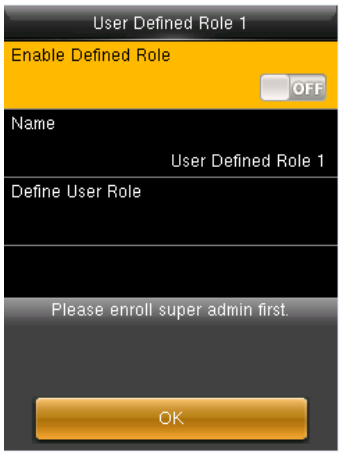
Mixed Line

4 User Role

Defined roles to operate the device. You can specify the available menus to operate for a role. There are 3 roles. Enter into "*User Role*". Press one of the three roles to edit:

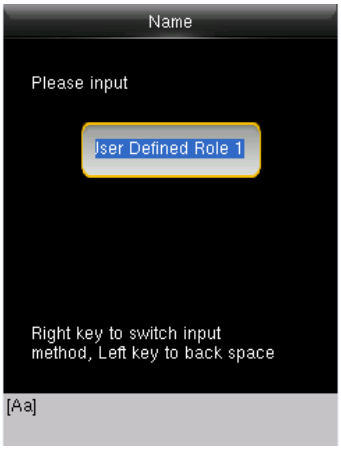


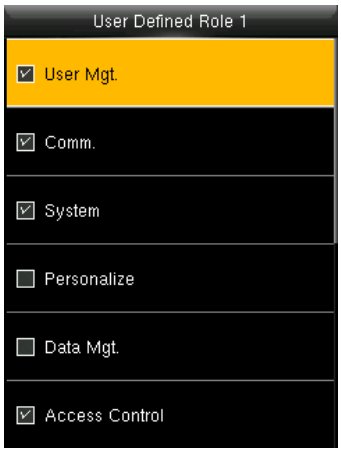




A Super admin must be enrolled before a new role is defined, or it can not be enabled.

- Defining a name and functions

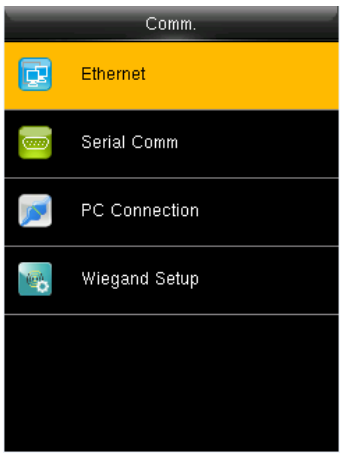




1. Enter name with T9 Input.
2. You can define more than one available menu for a role. Press [M/OK] to select.

5 Communication Setting

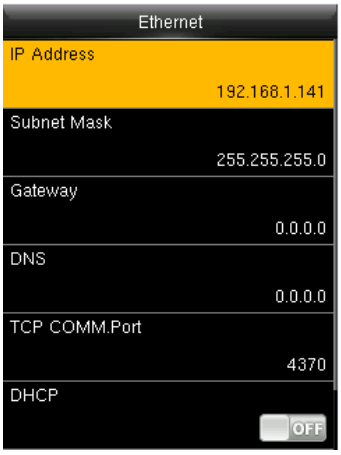
Set communication parameters. Enter into *"Comm."* :



Ethernet: The device can communicate with PC each other via the parameters you set.
Serial Comm: The device can communicate with PC each other via the serial port parameters you set.
PC Connection: Set the password and device ID so that you can connect the device with software in PC.
Wiegand Setup: Set wiegand-out parameters. For details, refer to"5.4 Wiegand Setup".

5.1 Ethernet

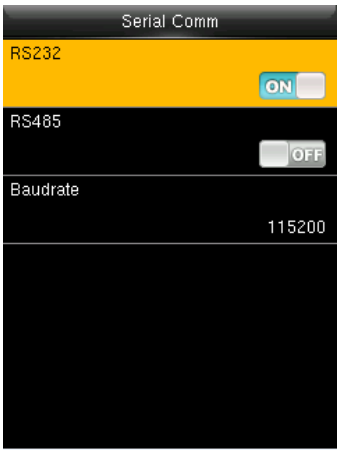
Enter into "*Comm.*" → "*Ethernet*":



IP Address: Modify it if necessary. It cannot be same with PC.
Subnet Mask: Modify it if necessary.
Gateway: It is necessary to set an address if the device and PC are in different network segment. Modify it if necessary.
DNS: Set the address of your DNS server.
TCP COMM Port: Set the TCP communication port.
DHCP: Dynamic Host Configuration Protocol, which is used to allocate dynamic IP addresses to clients by a server.
Display in Status Bar: Whether to display network status icons in the status bar.

5.2 Serial Comm

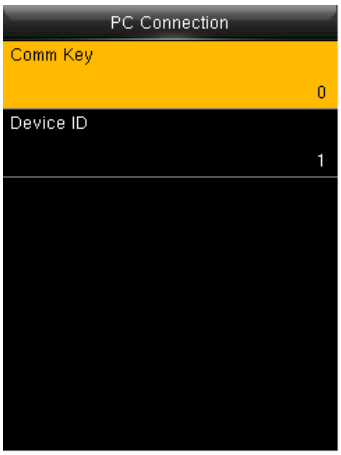
Enter into "*Comm.*" → "*Serial Comm.*":



RS232: Whether to use RS232 to communicate with PC.
RS485: Whether to use RS485 to communicate with PC.
Baudrate: Used for communication with PC. RS232 is recommended for high speed.
Note: There are 5 baudrate types available for RS232: 9600, 19200, 38400, 57600 and 115200; "9600" is not applicable to RS485. Reboot the device to make the change active.

5.3 PC Connection

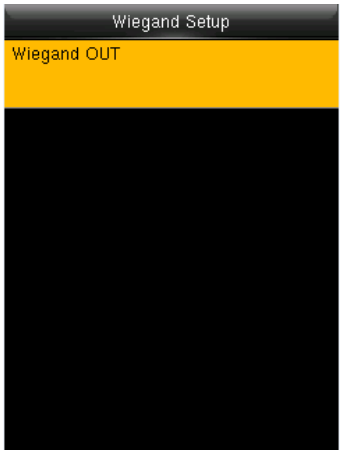
To improve the security of attendance data, connection password needs to be set here. Enter into "*Comm.*" → "*PC Connection*":

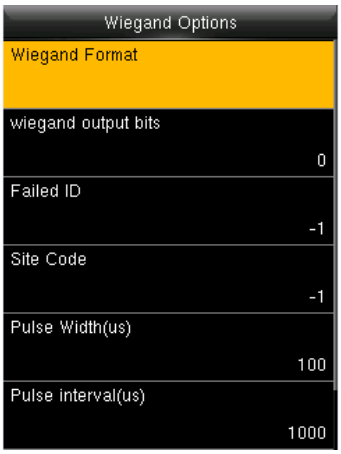


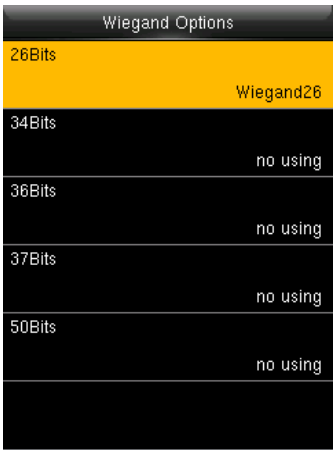
Comm Key: Set 1-6 digits connection password, the password must be input when PC software is to connect device to read data.
Device ID: The ID is in the range of 1-254. If RS232 or RS485 is enabled, this ID needs to be input in the software communication interface.

5.4 Wiegand Setup

Wiegand communication realizes the communication of user ID and badge number among devices. When the host and slave is connected, the verification data in the slave will display in the host. That means, once you verify successfully in the slave, the host will get the signal and open the door. Our device can only be used as a slave, so the wiegand-out must be set.
Enter into "*Comm.*" → "*Wiegand Setup*" → "*Wiegand Out*":







Wiegand Format: The system has five built-in formats: Wiegand 26-bits, Wiegand 34-bits, Wiegand 36-bits, Wiegand 37-bits and Wiegand 50-bits. Every format has two types of WiegandX and WiegandXa except for Wiegand 50-bits. You can select more than one wiegand formats.
Wiegand output bits: Select wiegand format bits based on the wiegand formats you've selected. If you made all five formats being used, there are five bits for you to choose.
Failed ID: Set the output value for failed verification. The output format is determined by the Wiegand format. The value ranges from 0 to 65535.
Site code: Similar to device ID. The value ranges from 0 to 256.

Pulse Width: Pluse width of wiegand delivering data. It can be adjusted from 20 to 100.
Pulse interval: It can be adjusted from 200 to 20000.
ID Type: Select output data by wiegand format. User ID and Badge Number is optional.

- Explaining about wiegand format

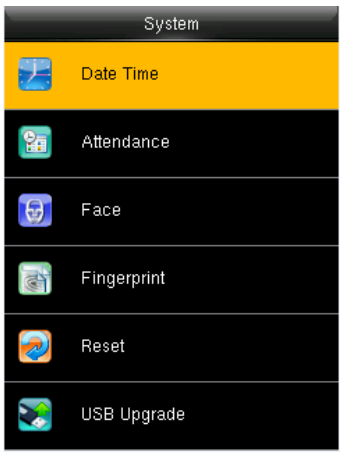
The wiegand format consists of two character strings: the data bits and parity bits. The following table is the definition of those five wiegand format:

Wiegand Format	Instructions
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO consists of 26 bits. The first bit is the even parity bit of second to 13th; the 26th is the odd parity bit of 14th-25th, the second to the 25th bits are the card number.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO consists of 26 bits. The first bit is the even parity bit of second to 13th, the 26th is the odd parity bit of14th-25th, the second to the 9th bits are site codes; the 10th-25th bits are the card number.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO consists of 34 bits. The first bit is the even parity bit of second to 17th, the 34th bit is the odd parity bit of 18th-33th, the second to 25th bits are the card number.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO consists of 34 bits. The first bit is the even parity bit of second to 17th, the 34th bit is the odd parity bit of 18th-33th, the second to the 9th are the site codes, the 10th-25th bits are the card number.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME consists of 36 bits. The first bit is the even parity bit of second to 18th, the 36th is the odd parity bit of19th-35th, the second to 17th bits are facility code, the 18th-33th are the card number, the 34th and 35th are the manufacturer code.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO consists of 36 bits. The first bit is the even parity bit of second to 18th, the 36th is the odd parity bit of 19th-35th, the second to 19th bits are facility code, the 20th-35th are the card number.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE consists of 37 bits. The first bit is the even parity bit of second to 18th, the 37th is the odd parity bit of 19th-36th, the second to 4th bits are manufacturer code, the 5th-16th are the site code, the 21th-36th are the card number.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO consists of 37 bits. The first bit is the even parity bit of second to 18th, the 37th is the odd parity bit of 19th-36th, the second to 4th bits are manufacturer code, the 5th-14th are the facility code, the 15th-20th are the site code, the 21th-36th are the card number.

Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO consists of 50 bits. The first bit is the even parity bit of second to 25th, the 50th is the odd parity bit of 26th-49th, the second to 17th bits are site code, the 18th-49th are the card number.
The Wiegand outputs bits can be a card number (C), site code (S), facility code (F), manufacturer code (M) and parity bits (P). Parity bits define the check mode of each bit in data bits and ensure the correctness of data bits during transferring through the parity check. The parity bits can be set to odd check (O), even parity(E).	

6 System Setting

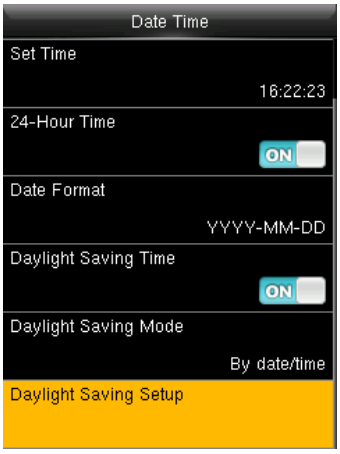
Set system-related parameters. Enter into"*System*" :



The resetting can not clear users' information and attendance data in the device.

6.1 Date Time

Set the system data and time. Enter into *"System"* →*"Date Time"*:



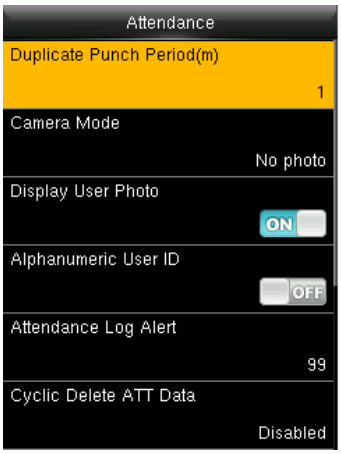
Set Date/Time: Set date and time of device.
24-Hour Time: Whether to use the 24-hour display mode. If not, the 12-hour display mode is adopted.
Date Format: Set the date format: YY-MM-DD, YY/MM/DD, YY.MM.DD, DD-MM-YY etc.

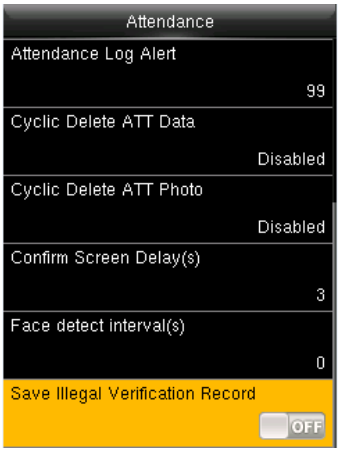
- Daylight Saving Time(DST)

The DST is a widely used system of adjusting the official local time forward to save energy. The uniform time adopted during the implementation of this system is known as the DST. Typically clocks are adjusted forward one hour in the summer to make full use of illumination resources and save electricity. Clocks are adjusted backward in autumn. The DST regulations vary with countries.
The device supports the DST function to adjust forward one hour at ×× (Hour): ×× (Minute) ×× (Day) ×× (Month) and backward one hour at ×× (Hour): ×× (Minute) ×× (Day) ×× (Month). For example, adjust the clock forward one hour at 08: 00 on April 1, and backward one hour at 08: 00 on October 1.
Daylight Saving Mode: Select the date mode or week mode.
Daylight Saving Setup: Set the DST start time and end time.
Note: The end time of DST cannot be set to next year. More specifically, the end time must be later than the start time in the same year.

6.2 Attendance Parameters

Set the attendance parameters. Enter into *"System"*→*"Attendance"*:





Parameters on Attendance interface state as below:

Duplicate Punch Period (m): In set time period (unit: minute), repeated attendance record of a user will not be saved (the valid time is 1~999999 minutes).

Camera Mode: Set whether to capture and save the photos when users verify face.

No Photo: The device does not take photo as users verify.

Take Photo, no save: Take photo, but not save photo as users verify.

Take photo and save: Take and save photo as users verify.

Save on successful verification: Take and save photo as users verify successfully.

Save on failed verification: Take and save photo as users fail to verify.

Display User Photo: Set whether to display user photos as users verify successfully.

Alphanumeric User ID: Set whether User ID supports alphanumeric. User ID with alphanumeric is convenient to sort and manage users.

Attendance Log Alert: When remainder log capacity is less than the set value, the device will prompts an alert message automatically. The valid value is 1~9999.

Cyclic Delete ATT Data: When Attendance records reach to the maximum capacity, the amount to delete attendance Data one time. The valid value is 1~999.

Cyclic Delete ATT Photo: When Attendance photos reach to the maximum capacity, the amount to delete attendance photo one time. The valid value is 1~99.

Confirm Screen Delay (s): The delay to display the verification result, the value is 1~9.

Face detect interval (s): Set interval for the same face verification, the value is 0~9.

Expiration Rule: Once enabled, you can choose3 expiration rules: Keep user, No audit future punch / Keep user, and audit future punch / Delete user.

6.3 Face Parameters

Set the attendance parameters. Enter into *"System"*→*"Face"* :

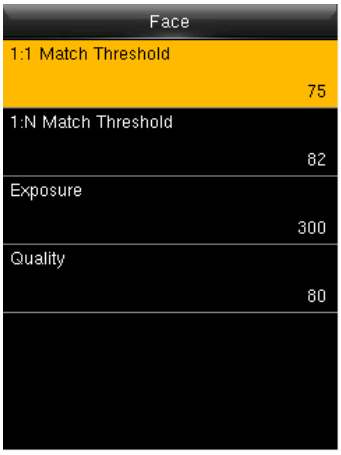
1: 1 Match Threshold: The similarity of a face verification and the enrolled template.

1: N Match Threshold: The similarity of a face verification and all of the templates.

Exposure: Set the exposure value of camera. The value ranges from 40 to 1000.

Quality: Set a quality threshold for the images obtained. The device processes them by

adopting the face algorithm when their quality is higher than the threshold; otherwise, it filters these face images. The value is 50-150.
Note: Improper adjustment of the Exposure and Quality parameters may severely affects the performance of the device. Please adjust the Exposure and Quality parameter under the guidance of our after-sales service personnel.

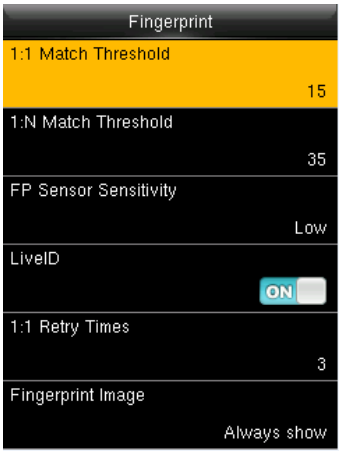


The recommended thresholds are as follows:

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

6.4 Fingerprint Parameters ★

Set the attendance parameters. Enter into "*System*"→"*Fingerprint*" :
1: 1 Match Threshold: The similarity of a fingerprint and the template.
1: N Match Threshold: The similarity of a fingerprint and all of the templates.
FP Sensor Sensitivity: Set the fingerprint sensor sensitivity. It is recommended to use the default value Medium. When dryness results in slow reactions of the fingerprint sensor, you may set this option to High to enhance the fingerprint sensor's sensitivity.
1:1 Retry Times: In 1:1 fingerprint or face password verification, user may forget the enrolled finger or the password, in addition, the finger is placed improper. To reduce press keyboard repeatedly, the device allows retrying after failed verification.
Fingerprint Image: Whether to display the fingerprint image on the screen during **enrollment or verification**: Show for enroll, Show for match, Always show, None.

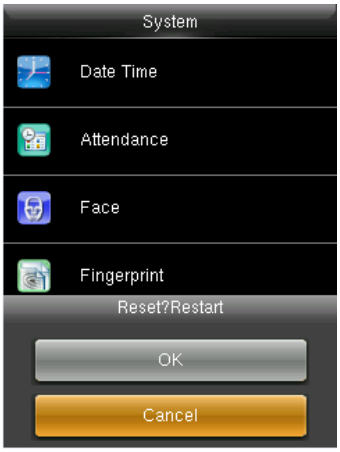


The recommended thresholds are as follows:

FRR	FAR	Threshold	
		1: N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

6.5 Reset

Reset communication settings, system settings, personalize settings etc.

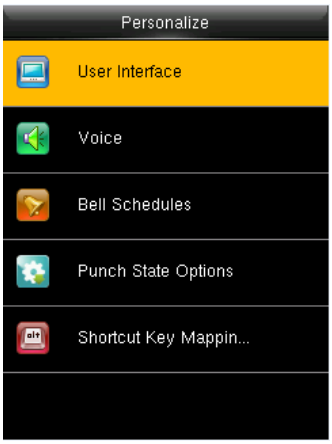


6.6 USB Upgrade

The firmware program of device can be updated with upgrade package in USB disk. You are not suggested to upgrade. If you need the upgrade file, please contact our technical support personnel.

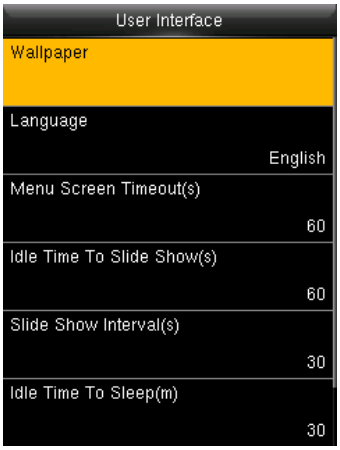
7 Personalize Setting

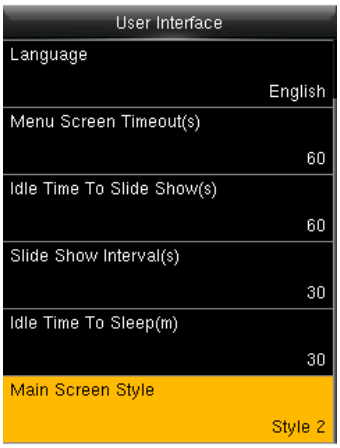
Set some usual parameters. Enter into"*Personalize*" :



7.1 User Interface

Set displayed parameters. Enter into *"Personalize"*→*"User Interface"*:

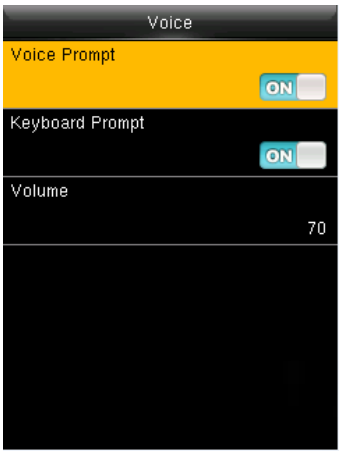




Wallpaper: Select the wallpaper of main screen as required.
Language: Select the language of device as required.
Menu Screen Timeout (s): When operating standby time is larger than this value, the system will return to initial interface. The valid value scope is 60~99999 seconds.
Idle Time To Slide Show (s): When standby time in main screen is larger than this value, the main screen will display a slide show. The valid value scope is 3~999 seconds.
Slide Show Interval (s): Set interval to change displayed pictures in the slide show, the value scope is 3~999 seconds.
Idle Time To Sleep (m): When operating standby time reaches to this value, the device will go to sleep. Pressing any keyboard or fingerprint will wake the device. The valid value scope is 1~999 minutes.
Main Screen Style: Select one displayed style as required (3 styles available).

7.2 Voice Setting

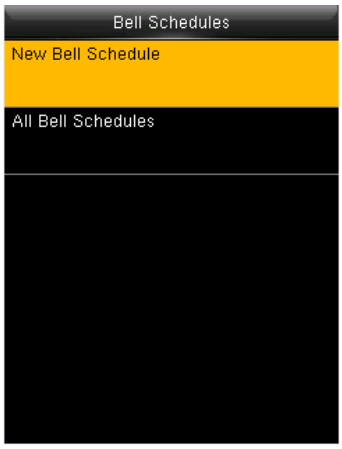
Set voice parameters. Enter into*"Personalize"→"Voice"*:



Voice Prompt: Select whether to enable voice prompts during operating.
Keyboard Prompt: Select whether to enable keyboard voice while pressing keyboard.
Volume: Set the volume of device.

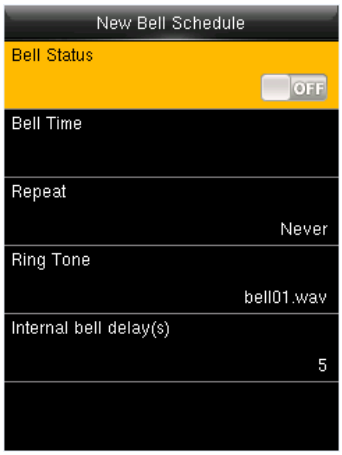
7.3 Bell Schedules

Companies need to ring their bells to signal the start and end of work shifts. You can schedule more than one bell to ring. Enter into *"Personalize"→"Bell Schedules"*:



- Schedule a new bell

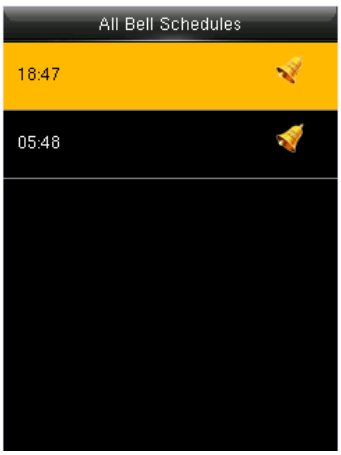
Enter into *"Personalize"→"Bell Schedules"→"New Bell Schedule"*:

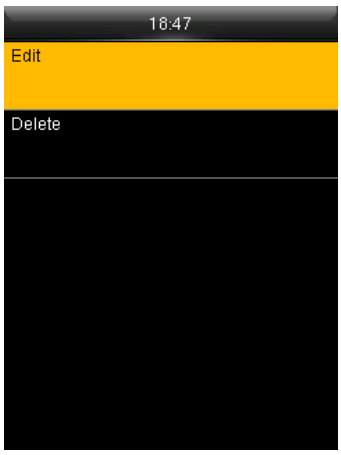


Bell Status: Select whether to enable the bell.
Bell Time: Set a ringing time of the bell during cycling.
Repeat: Set the cycling time of this bell.
Ring Tone: Select a bell ring tone.
Interval bell delay (s): Set the time length of bell ringing. The valid value is 1~999 seconds.

- Edit Bell

Enter into *"Personalize"→"Bell Schedules"→"All Bell Schedules"*:





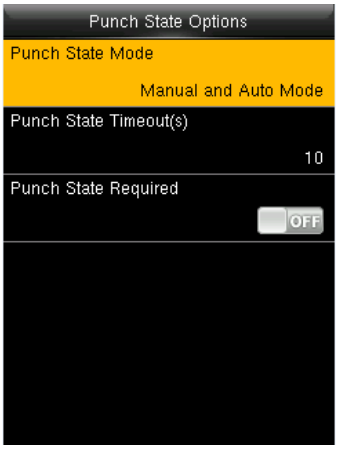
1. Select a bell to edit.
2. Press "*Edit*" to modify data.

- Delete Bell

Enter into"*Personalize*"→"*Bell Schedules*"→"*All Bell Schedules*", select a bell to delete.

7.4 Punch State Options

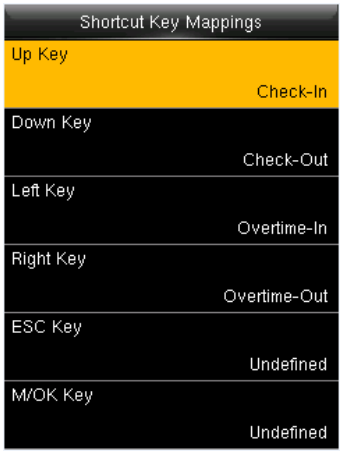
Set the mode of state keys. Enter into "*Personalize*"→"*Punch State Options*":

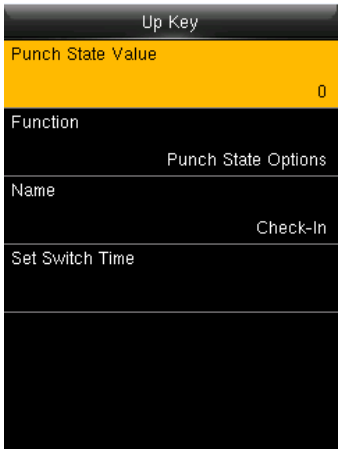


Punch State Mode: Off: Disable the punch state key function.
Manual Mode: User manually switches punch state by pressing corresponding shortcut key.
Auto Mode: The set punch states will auto switch when reaching switch time.
Manual and Auto Mode: A status key manually switching will switch to the automatic plan upon a timeout.
Manual Fixed Mode: After manually switching, it will keep this state until next manual switching.
Fixed Mode: Displaying the fixed punch state.
Punch State Timeout (s): The time of one punch state displays. The punch state will disappear or switch to other punch states as the time is out. The value is 5~999 seconds.
Punch State Required: Set whether to select punch state during verification.
Note: There are four punch states: Check-In, Check-Out, Overtime-In, Overtime-Out.

7.5 Shortcut Key Mappings

Define functions of shortcut keys. You can define ▲ , ▼ , /, [ESC], [M/OK] keys as punch state keys or menu function keys. In initial interface, you can press shortcut keys to display corresponding punch state or enter corresponding menu interface rapidly. Enter into "*Personalize*"→"*Shortcut Key Mappings*". Press any key to define.





Note: Only when Punch State is selected as function, will Punch State Value, Name, Set Switch Time options appear on the interface. The punch state can be set as auto switch. Punch state will switch automatically once the setting switch time is out.

Select Function of shortcut key as Punch State Option, the shortcut key will not take effect under that Punch State Mode is set as OFF.

Punch State Value: The device set 4 different values corresponding to four punch states by default. Value 0 corresponds to punch state Check-In, 1 for Check-Out, 4 for Overtime-In, 5 for Overtime-Out. The value ranges from 0 to 250.

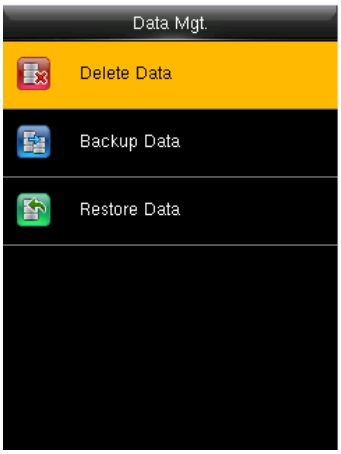
Function: Select punch state options or menu function options.

Name: Enter name of punch state.

Set Switch Time: Set switch time for punch state.

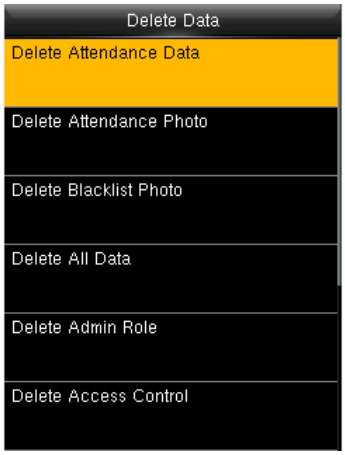
8 Data Management

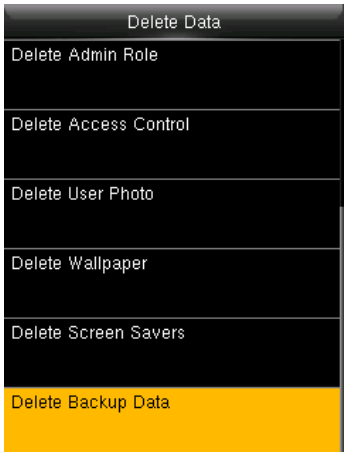
Manage data saved in the device. Enter into"*Data Mgt.*" :



8.1 Delete Data

Enter into "*Data Mgt.*" → "*Delete Data*":



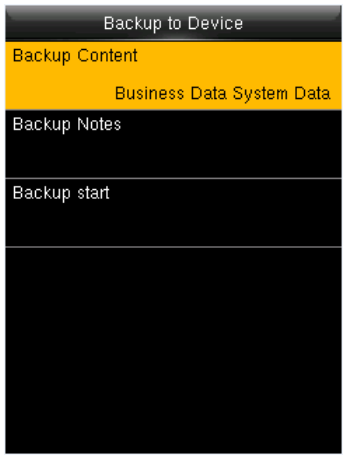


Delete Attendance Data: Delete all attendance data.
Delete Attendance Photo: Delete all users' attendance photos.
Delete Blacklist Photo: Delete captured and saved photos when verification failed.
Delete All Data: Delete all enrolled users' information, fingerprints, attendance records, short messages and work codes etc.
Delete Admin Role: Change all administrators into normal users.
Delete User Photo: Delete all enrolled users' photos.
Delete Wallpaper: Delete all wallpapers in the device.
Delete Screen Savers: Delete all screen savers of the device. (About the methods to upload screen saver, please refer to "Appendix 2 Rules to upload picture".)
Delete Backup Data: Delete data backup to the device.

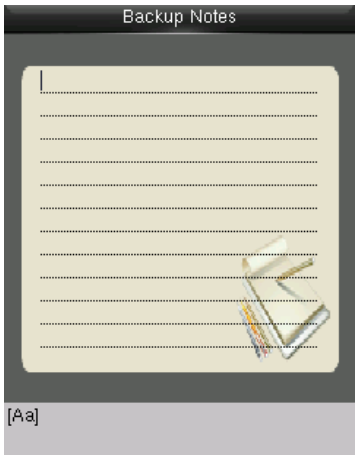
8.2 Backup Data

Backup the business data or system data to the device or USB disk. Enter into"*Data Mgt.*" → "*Backup Data*":

Select a route



Select the data type

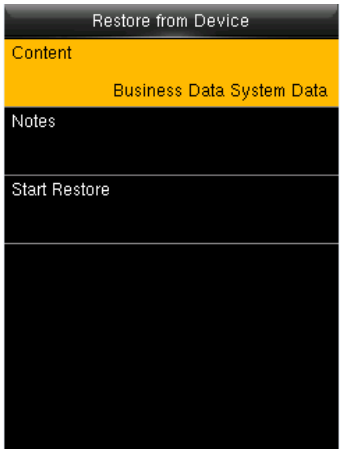


Write backup notes

Note: When Backup data to USB Disk, you need to insert an USB Disk into the device at first, and then press [M/OK] to backup data to USB disk.

8.3 Restore Data

Restore data to the device. Enter into *"Data Mgt."* → *"Restore Data"*:

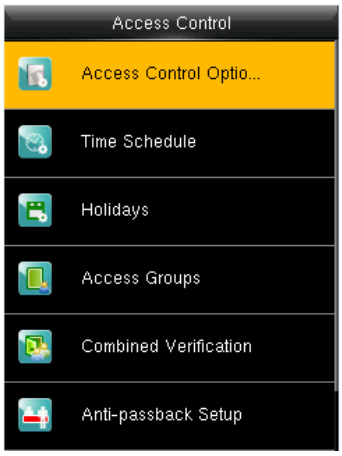


1. Select a route.
2. Select the data type.
3. Start restoring.

Note: When restore data from an USB Disk, you need to insert an USB Disk into the device at first, which has the resotred data.

9 Access Control

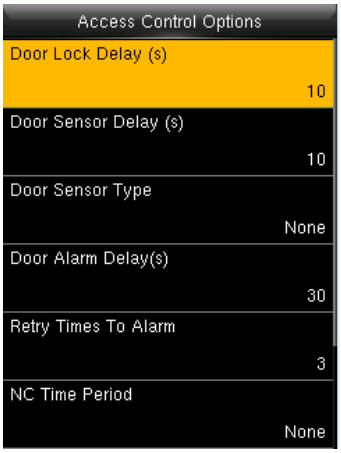
Set users' access controlling parameters. Enter into *"Access Control"* :



To unlock, the enrolled users must owned these conditions:
1. The current unlock time should be in the effective time of user time zone or group zone.
2. The group a user belongs to must be in access controlling.
The new enrolled user is allocated in the group 1 and in time zone 1by default, in time zone as 1. The new enrolled user is in unlock status. You can modify the status in user editting.

9.1 Access Control Options

Enter into *"Access Control"* →*"Access Control Options"*:

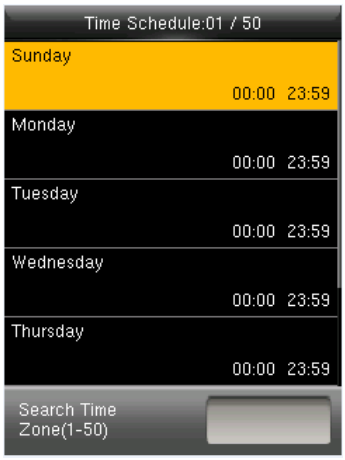


Door Lock Delay(s): The enabling time of electronic lock. The value ranges from 1to10 seconds.
Door Sensor Delay(s): The delayed checking time by door sensor after the door is opened. The value is 1-255seconds.
Door Sensor Type: NONE(no door sensor), NC (door is opened normally)and NO(door is closed normally).
Door Alarm Delay(s): The device alarms in a few seconds once abnormal state is detected, the value is 1-99 seconds.
Retry Times To Alarm: The failed verification times to alarm. The value is 1-9 times.

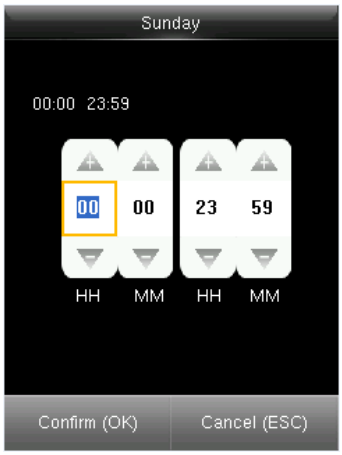
NC Time Period: Set time zone for NC. Nobody can unlock during this time zone.
NO Time Period: Set time zone for NO. The lock is in enabling during this time zone.
Note: When time zone is set for NO or NC, please set door sensor mode as None, or alarm signal may come out during time zone of NO or NC.

9.2 Time Schedule

Schedule door's Opening time. Enter into *"Access Control"* →*"Time Schedule"*:



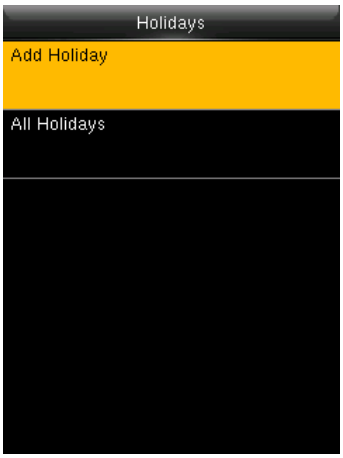
Time zone is the minimum unit of access control options. The whole system can define 50 time zones. Every time zone defines seven time sections (namely, a week). Every time section is the effective time zone within 24 hours everyday. Every user can set 3 time zones. "or" exists among the three zones. Every time zone among these three is effective. Time format is HH:MM-HH:MM, accurate to minute.
You can edit every time zone. Or you can input the time zone number in the searching box to position quickly.

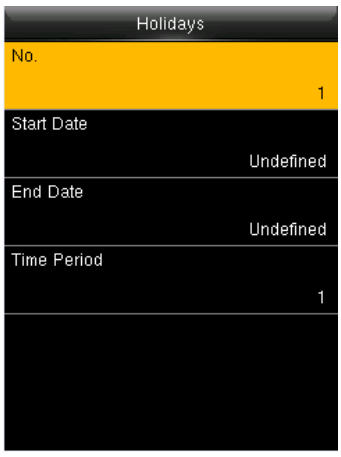


If the end time is in advance than the start time, for instance: 23:57- 23:56 , the whole day is forbidden to open the door. If end time is after than start time 00:00- 23:59 , it is effective section. Effective time zone for user unlocking: 00:00-23:59 or end time is bigger than start time.
Note: The default time period number 1 indicates all-time access (that is, newly registered users are unlocked).

9.3 Holidays

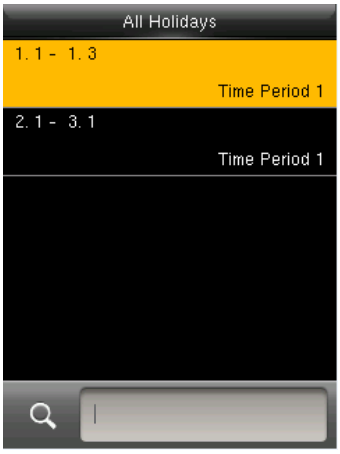
Special access control time may be neccessary during holiday. After holiday access time is set, user's time zone during holiday subjects to the holiday time zone. Enter into *"Access Control"* →*"Holiday"*:

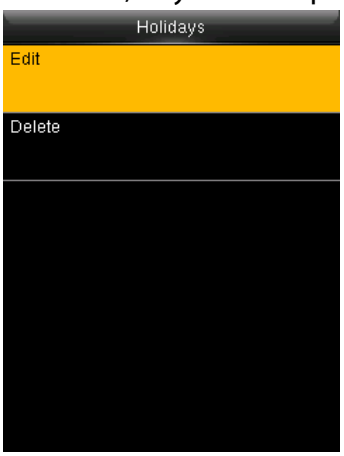




1. Press "*Add Holiday*".
2. Edit the options.

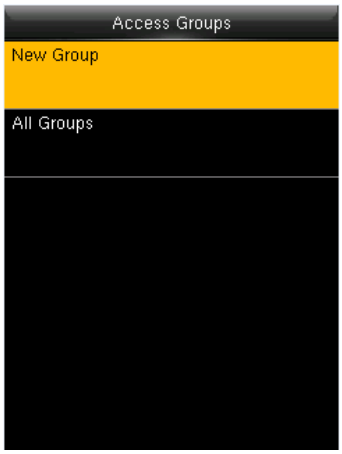
You can choose one to edit or delete, or you can input a holiday number to position.

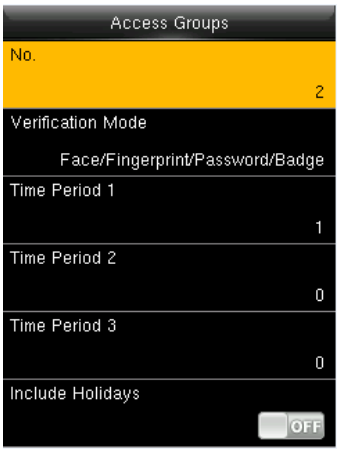




9.4 Access Groups

Grouping is to manage employees in groups. Group members use group time zone by default. The new enrolled user belongs to Group 1 by default. He can also be allocated to other groups. Enter into *"Access Control"* → *"Access Groups"*:

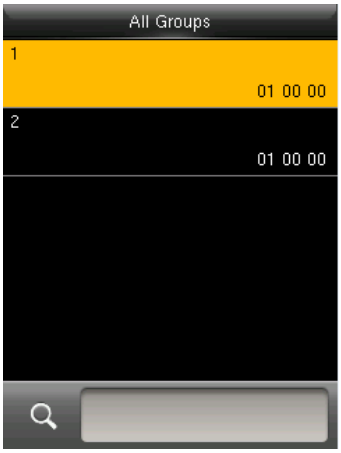


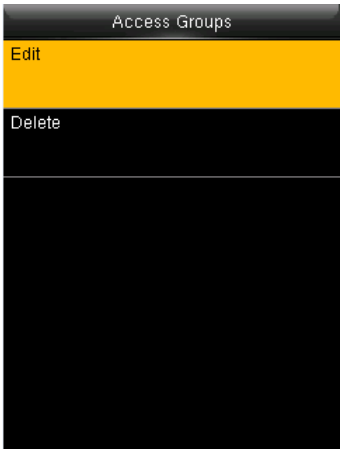


1. Press "New Group".
2. Edit the options.

Note: Only when there is intersection between group zone and holiday time zone can the group members open the door in case of the enabled holiday. Or the access control time of group members are not affected by holiday.

You can choose one to edit or delete, or you can input a group number to position.

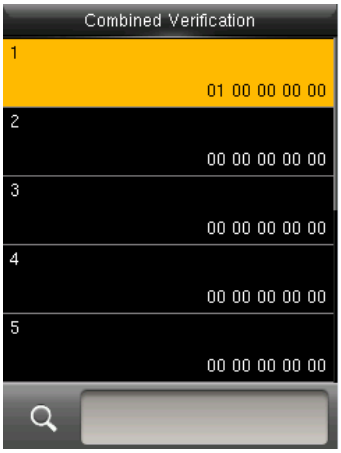


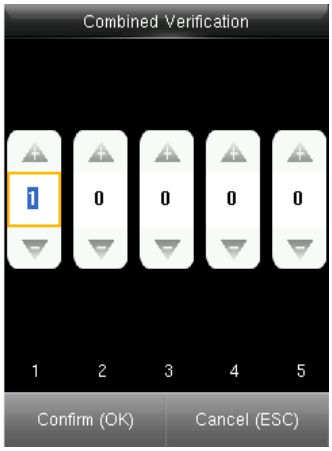


9.5 Combined Verification

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. Enter into

"Access Control" →"Combined Verification":



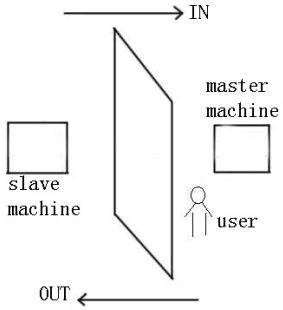


1. Choose one to edit.
2. Input the group number.

Notes: You can choose one to edit or delete, or you can input a group number to position. To delete an unlocking combination group, set all IDs to 0.

9.6 Anti-passback Setup

Sometimes, some illegal person will follow the employee into the gate. This function is enabled to prevent this. In record must match out record, or the gate won't be opened. Host inside the door and slave outside the door work together.



- Working Principle

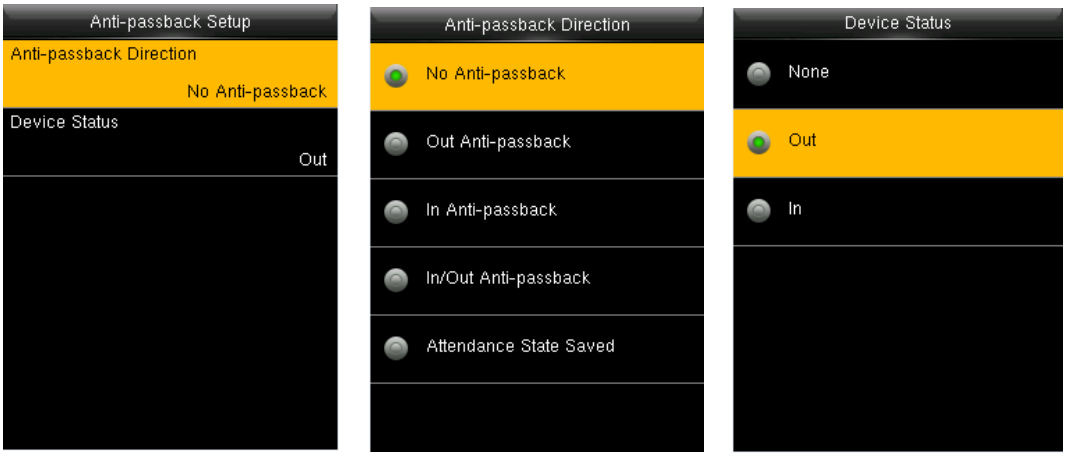
The host has Wigand In and the slave has Wigand Out. Connect Wigand Out of the slave to Wigand In of master machine. Wigand output from a slave must not own a machine ID. The number sent to the host from slave must be found in the host.

- Function

Judge whether it is anti-pass back according to user's recent in-out record. In record and out record must be matched. This machine supports out, in, or out-in anti-pass back (enter machine menu—setting—system setting—advanced setting—anti-pass back).
When master machine is set as "out anti-pass back",if user wants to come in and go out normally, his recent record must be"in"or he cannot go out. Any"out"record will be"anti-pass back refused". For example, a user's recent record is"in", his second record can be"out"or"in". His third record is based on his second record. Out record and in record must match. (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".

• Operations

Enter into *"Access Control"* → *"Anti-passback Setup"*:



» Anti-passback Direction

No anti-passback: The door will be opened only when the verification is done by a host.

Out anti-passback: If the device does not store the record of a person, the person can check out after the first comparison. In case that a person's record has been stored in the device, an alarm will be raised when the person checks out without the corresponding entry record in the device. If only out anti-passback is enabled, entry is allowed at any time.

In anti-passback: If the device does not store the record of a person, the person can check in after the first comparison. In case that a person's record has been stored in the device, an alarm will be raised when the person checks in without the corresponding exit record in the device. If only in anti-passback is enabled, exit is allowed at any time.

In/out anti-passback: If the device does not store the record of a person, the person can check in and out after the first comparison. In case that a person's record has been stored in the device, an alarm will be raised when the person checks in or out without a corresponding exit or entry record in the device.

» Device status

In: When a device is used to control entry, the device saves only the entry records.

Out: When a device is used to control exit, the device saves only the exit records.

None: When the status of a device is set to None, the anti-passback function is disabled on the device.

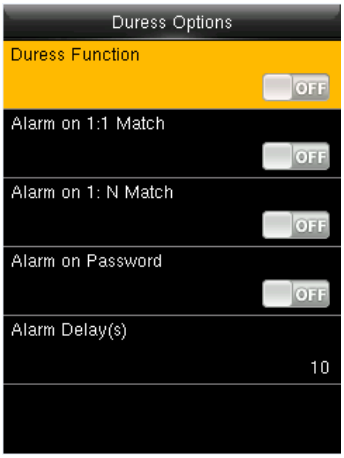
Note: Wiegand communication is adopted for host and slave. Referring to the following for connection:

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

9.7 Duress Options

When employee come across duress, select duress alarm mode, the device will open the door as usual. But the alarm signal will be sent to backstage alarm. Enter into *"Access*

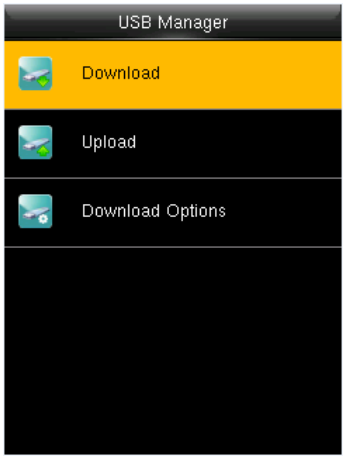
Control" →"Duress Options":



Duress Function: If enabled, a fingerprint or an ID number successful verification in 3 seconds after pressing help,The duress alarm will come out. Help can be set in keyboard.
A**larm on 1:1 Match**: If enabled, alarm signal will come out when user use 1:1mode, Or there is no alarm signal.
Alarm on 1:N Match: If enabled, alarm signal will come out when user use 1:N mode, Or there is no alarm signal.
A**larm on Password**: If enabled, alarm signal will come out when user use password verification.
Alarm Delay(s): After duress alarm gets started, the alarm signal is not output directly. But it can be defined. Alarm signal will be generated automatically in a few seconds.

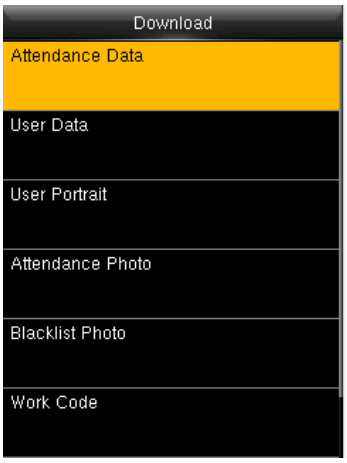
10 USB Manager

The device allows to download user data and attendance data to a USB disk. Meanwhile, user data from other devices can be uploaded to this device. Before downloading and uploading, insert a USB disk to USB slot of the device. Enter into *"USB Manager"* :



10.1 Download

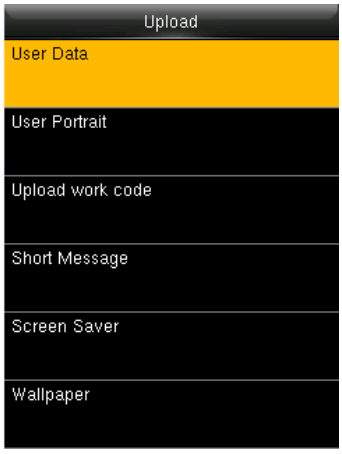
Enter into *"USB Manager"* →*"Download"*:



Attendance Data: Download attendance data to USB disk.
User Data: Download all user data to USB disk.
User Portrait: Download all users' photos to USB disk.
Attendance Photo: Download attendance photos to USB disk, the format of attendance photo is .jpg.
Blacklist Photo: Download attendance blacklist photos to USB disk, format of blacklist photo is .jpg.
Work Code: Download all work codes to USB disk.
Short Message: Download all short messages to USB disk.

10.2 Upload

Enter into *"USB Manager"* →*"Upload"*:

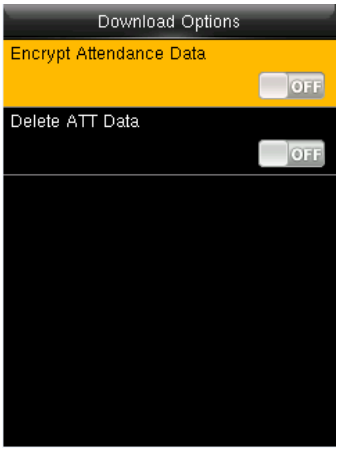


User Data: Upload user data saved in USB disk to the device.
User Portrait: Upload .jpg photos to the device.
Upload work code: Upload all work code saved in USB disk.
Short Message: Upload all short messages in USB disk.
Screen Saver: Upload screen saver saved in USB disk.
Wallpaper: Upload wallpapers saved in USB disk

About format of screen saver, please refer to "Appendix 2 Rules to upload picture".

10.3 Download Options

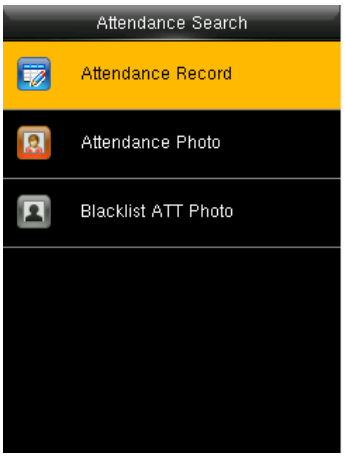
Enter into "*USB Manager*"→"*Download Options*":



You can encrypt the data in a USB disk and set to delete data after being downloaded. When download the attendance records, you can also set the calendar type displayed in the attendance time. The device support hree calendar types which are Gregorian, Iran Gregorian, Iran Lunar to choose.

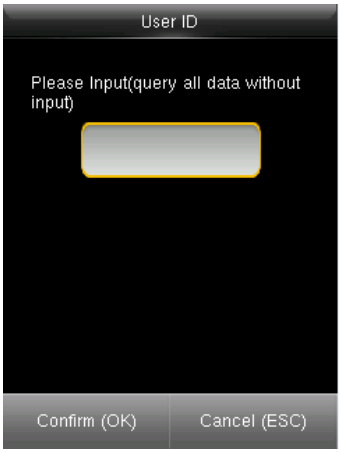
11 Attendance Search

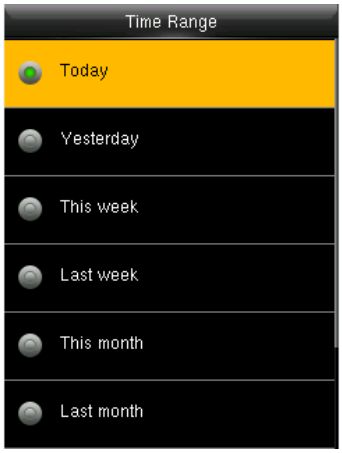
After verified successfully, users' attendance records will be saved in the device. Attendance Search function is convenient for employee to search his attendance record.
Enter into *"Attendance Search"* :



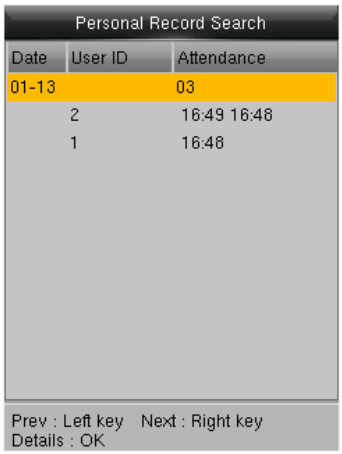
Attendance Record: Search the attendance records in the device. When you verified in the device, the record is saved.
Attendance photo: Search the attendance reccord restored in the device.
When you verified, the device's camera will capture a photo to save in the device.
Backlist ATT photo: When you verified failed for fixed times, the device's camera will capture a photo to save in the backlist of device.

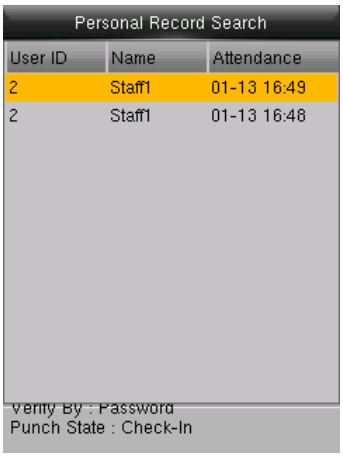
Take "Search Attendance Record" as an example, other two menu is same as this steps:
Enter into *"Attendance Search"* →*"Attendance Record"*:





1. Input the user ID to search.
2. Select the time period of attendance record.
Note: You can input nothing in user ID box to search all users' attendance record.

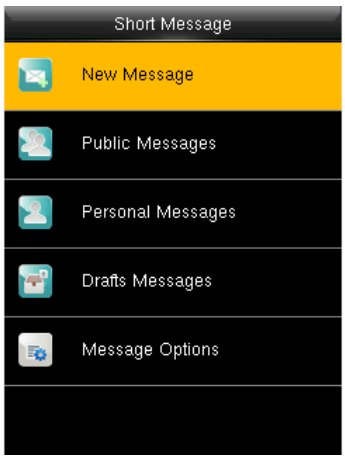




3. The record list is displayed.
4. Select anyone to check details.

12 Short Message

Enter into *"Short Message"* :

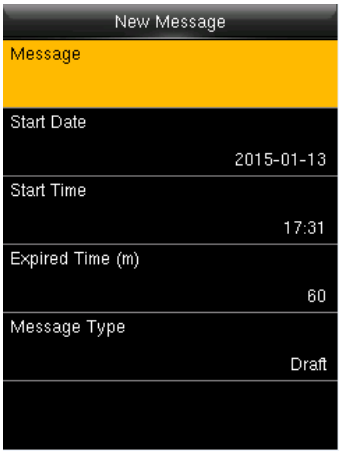


You can add, edit, delete and send public or personal message. And you can save the message in drafts.
In assigned time, the public message will display to all users at the bottom of main screen, and personal message will display to specified user after successful verification.
You can check public, personal or drafts message in corresponding menus.
Public message will display at bottom of main screen in assigned time.Personal message will appear after user verified successfully in assigned time.

12.1 Add and view new message

- Add a personal message

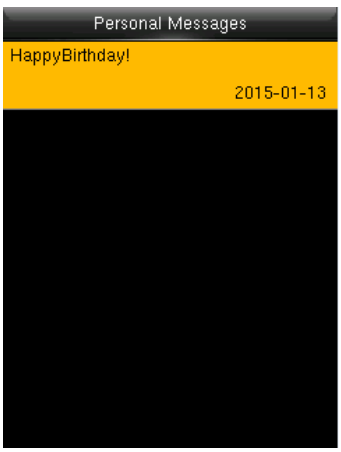
Enter into *"Short Message"* →*"New Message"*:

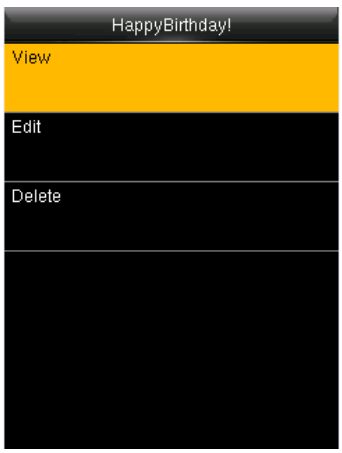


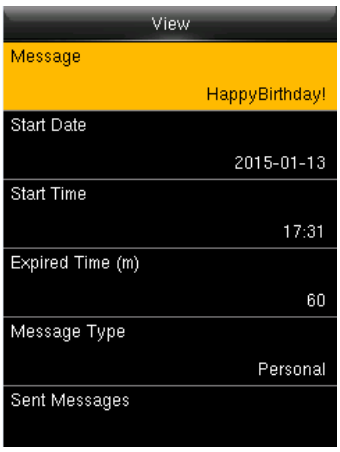
Message: Input the message text.
Start Date/Time: Set the start date & time of message pops.
Expired Time: Time of message expired, calculated from the time you add.
Message Type: Public, Personal, Drafts.

- View a personal message

Enter into *"Short Message"* →*"Personal Message"*, select a message →*"View"*:

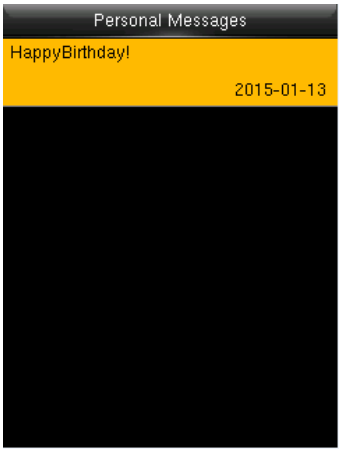


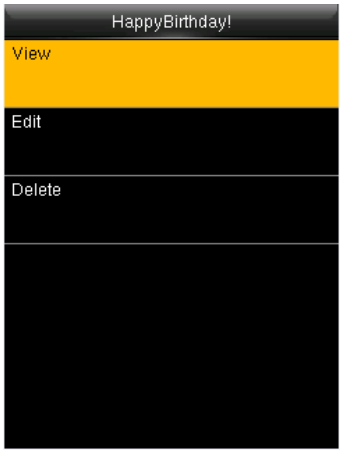




12.2 Edit and delete a personal message

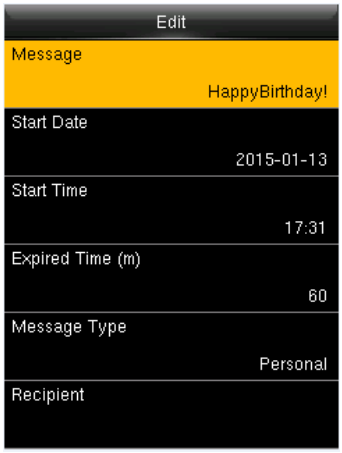
Enter into *"Short Message"* →*"Personal Message"*, select a message:

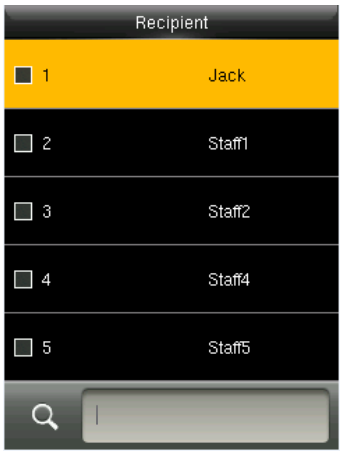




You can edit or delete the selected message.

Selcet the message recipient: enter *"Edit"*→ *"Recipient"*:

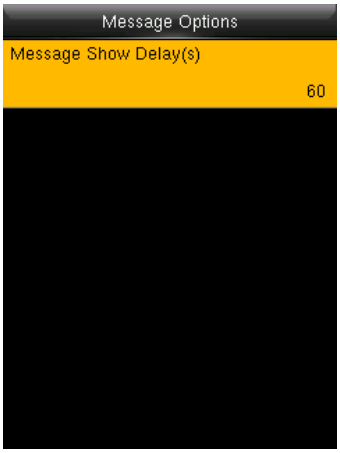




You can select more than one user to receive this message. Press [ESC] to save and exit.

12.3 Message Options

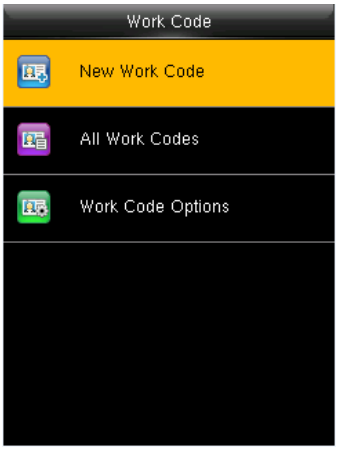
Enter into *"Short Message"* →*"Message Options"*:



Message Show Delay (s): It means the duration that personal message shows. The personal message showing interface will back to initial interface after reaching Message Show Delay. The valid value is 1-99999 seconds.

13 Work Code

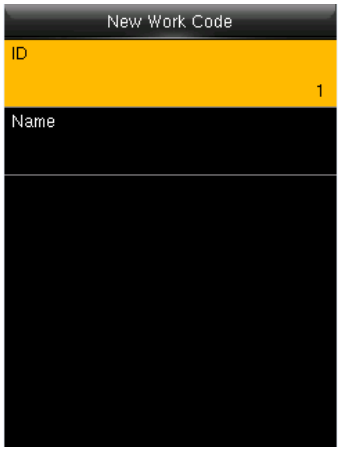
Enter into *"Work Code"* :

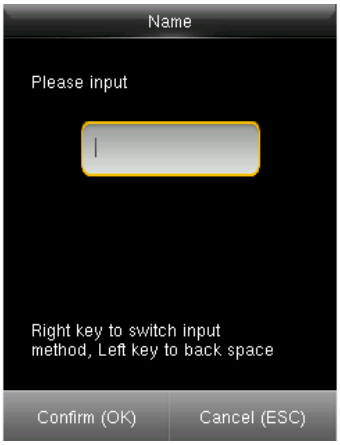


Salary is based on attendance. There are many work types for employees. An employee may have different work type in different time period. Different work types have different pays. Therefore, in order to distinguish different attendance states when user is dealing with attendance data, the device has provided a parameter to mark which attendance record belongs to which work type.
Work codes are downloaded together with attendance records. Users can use relevant data based on the specific attendance software.

13.1 Add a work code

Enter into*"Work Code"* →*"New Work Code"*:

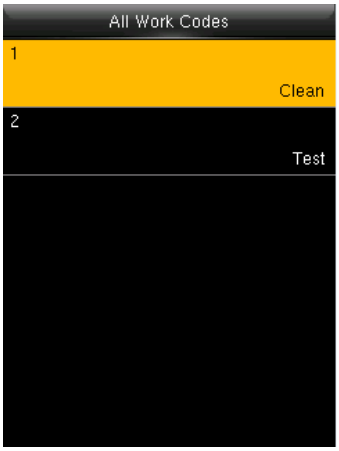


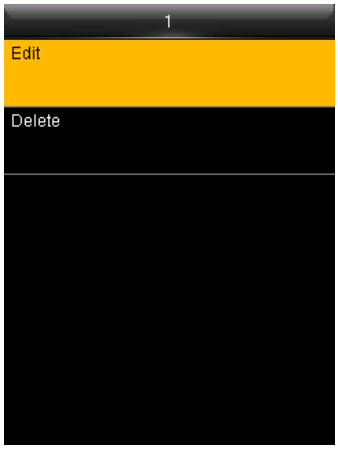


ID: The allocated working number. The range is 1-99999999.
Name: Input a name with T9 input. 23-characters are limited.
Note: The work code can not be modified once confirmed.

13.2 Edit and delete a work code

Enter into*"Work Code"* →*"All Work Codes"*:

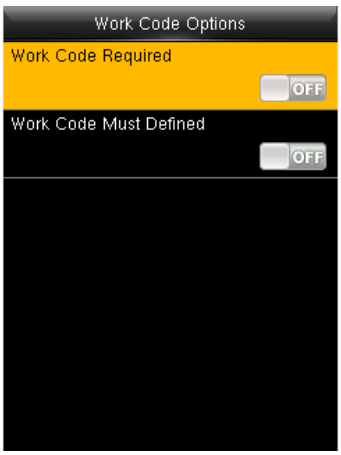




1. Select a work code.
2. Press "*Edit*" to modify the name.
   Press "*Delete*" to delete.

13.3 Work Code Options

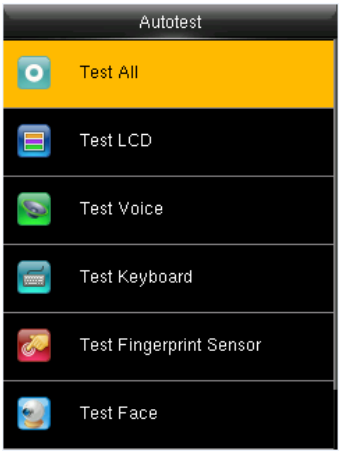
Enter into *"Work Code"* → *"Work Code Options"*:



Work Code Required: The work code must be input during verification. Select whether to enable this function.
Work Code Must Defined: The input work code has to exist during verification. Select whether to enable this function.

14 Autotest

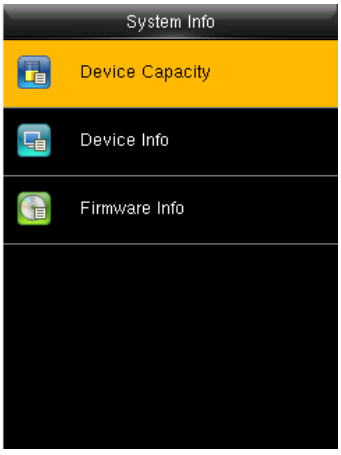
Auto test if the function of each module is available. Enter into *"Auto Test"*:



Test All: Check all modules of device.
Test LCD: Check the LCD(Liquid Crystal Display).
Test Voice: Check if the voice prompts is displayed normally.
Test Keyboard: Check if the keyboard is available.
Test Fingerprint Sensor ★ : Check if the fingerprint sensor is available to use.
Test Face: Check if the camera is normal.
Test Clock RTC: Check if the RTC(Real-Time Clock) is accurate.
The process of modules checking, please follow the prompts in the specific interface.

15 System Information

To check the system and device information. Enter into *"System Info."*:

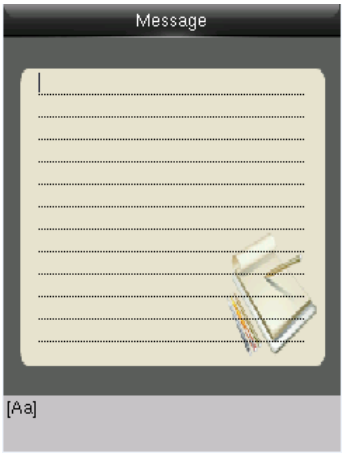


Click specific option to check the parameters:
Device Capacity: number of users, admin users, number and the most capacity of fingerprints, face, badge, attendance record and attendance photos number.
Device Info.(Information): device name, serial number, MAC address, fingerprint algorithm, face algorithm, platform information, manufacturer, manufacturer date.
Firmware info: firmware version, bio service, standalone service, device service.
All information are not allowed to modify but check.

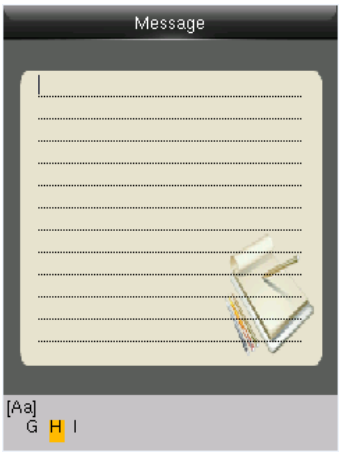
16 Appendixes

Appendix 1 T9 Input

T9 input (intelligent input) is quick and high efficient. There are 3 or 4 letters on numeric keys (2~9), for example, A, B, C are on numeric key 2. Press the corresponding key once, and the program will generate effective spelling. Take writing a message as an example to explain the methods:



Enter into "*New Message*".



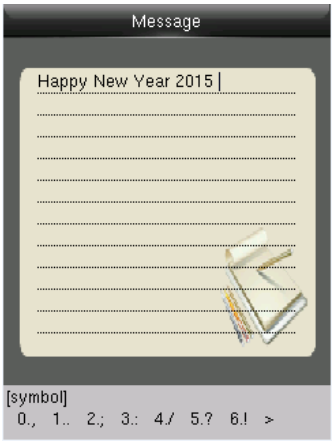
Press [4] twice to input H.

Input"appy"with the same way.

Press ▶to "symbol" type.

Press ▶to find to"3. " .
Press 3 to input a blank.

Input"New Year" with that way
Press ▶to numeric type.



1. Input "2015" , press▶to "symbol"type.
2. Press "6" to input "!".

Appendix 2 Rules to upload picture

1. **User Photo**: First create a directory named "photo" in the root directory of USB disk, and then put user photos in the directory. Max capacity of the directory is 8000 photos. The size of each photo is smaller or equal 15K. Name of photo is X.jpg (X represents User ID, which does not limit digits). The format of photo must be .JPG.
2. **Screen Saver**: First create a directory named "advertise" in the root directory of USB disk, and then put screen savers in the directory. Max capacity of the directory is 20 pictures. The size of each screen saver is smaller or equal 30K. There is no limit on name and format of the screen saver.
3. **Wallpaper**: First create a directory named "wallpaper" in the root directory of USB disk, and then put wallpapers in the directory. Max capacity of the directory is 20 pictures. The size of each wallpaper is smaller or equal 30K. There is no limit on name and format of the wallpaper. It supports format of jpg, png, bmp etc.
Note: If the size of each user photo and attendance photo is smaller or equal 10K, the device can store 10000 user photos and attendance photos in total.

Statement on Human Rights and Privacy

Dear Customers:
Thank you for choosing the hybrid biometric products designed and manufactured by us. As a world-renowned provider of biometric technologies and services, we pay much attention to the compliance with the laws related to human rights and privacy in every country while constantly performing research and development.
We hereby make the following statements:
1. All of our 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 the human rights or privacy when using our products, please contact your employer directly.
Our other police fingerprint equipment or development tools will provide the function of collecting the original fingerprint image of citizens. As for whether such a 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.
Note: The law of the People's Republic of China has the following regulations regarding the personal freedom:
1. Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.
2. The personal dignity of citizens of the People's Republic of China is inviolable.

3. The home of citizens of the People's Republic of China is inviolable.
4. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law.
At last we stress once again that biometrics, as an advanced recognition technology, will be applied in a lot of sectors including e-commerce, banking, insurance and legal affairs. Every year people around the globe suffer from great loss due to the insecurity of passwords. The fingerprint recognition actually provides adequate protection for your identity under a high security environment.

Environment-Friendly Use Description

The Environment Friendly Use Period (EFUP) marked on this product refers to the safety period of time in which the product is used under the conditions specified in the product instructions without leakage of noxious and harmful substances.
The EFUP of this product does not cover the consumable parts that need to be replaced on a regular basis such as batteries and so on. The EFUP of batteries is 5 years.

Names and Concentration of Toxic and Hazardous Substances or Elements

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

○ : Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.
×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in SJ/T11363-2006.
Note: 80% of the parts in this product are manufactured with non-hazardous environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.

#24,Shambavi Building, 23rd Main,Marenahalli,
JP Nagar 2nd Phase, Bangalore - 560078
Phone: 91-8026090500 | Email :
sales@esslsecurity.com www.esslsecurity.com