User Manual

Applicable Model: P160/P200/P260

Version 1.0

Date: August, 2017

Important Claim

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

No written consent from 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.

The title with ★ represents the optional function.

Copyrights

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.

Table of Contents

1. Introduction

P160 is a multibiometric identification time & attendance and access control terminal, which can connect with third party electric lock, door sensor, and exit button etc.

With the latest palm/fingerprint identification algorithm and streamlined technology, it can hold 600 palm templates and up to 20,000 fingerprint templates without dividing into groups.

Communicating via Wi-Fi(Optional) , TCP/IP, and USB client, it ensures a smooth connection and data transfer. Amazing verification speed and intuitive operation process make it popular. Elaborately designed and finely processed, it matches your slap-up office perfectly.

2. Features

Palm, Fingerprint, RFID Ready

Elegant ergonomic design; Easy installation.

Wi-Fi(Optional), TCP/IP, and USB communication.

Professional ZKTeco Palm and fingerprints identification algorithm.

Optional Modules:

PoE module/3G module/ high (general) level access control module/battery module/printer

3. Specifications

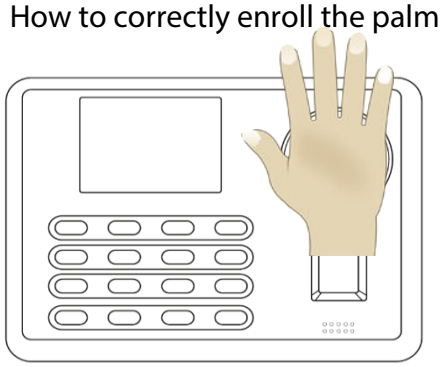
Display	2.8-inch TFT color Display
Capacity	Palm templates:600(Standard) Fingerprint templates 3,000
ID Card Capacity	10,000(Optional)
Logs Capacity	100,000

Communication	TCP/IP, USB, Wi-Fi(Optional)
Standard Functions	Automatic Status Switch, Self-Service Query, AC module 1: Exit Button, Door Lock, Alarm,12V OUT, AUX IN; Work Code, T9 Input, 9 Digit User ID, DST, Scheduled-bell and SMS
Optional Functions	ID Card, Mifare Card AC module 2: Exit Button, Door Lock, Alarm,12V OUT, AUX IN, Door Sensor, RS485, Wiegand IN/OUT. PoE,3G, Battery Module,ADMS
Power Supply	12V/1.5A
Verification Speed	≤1 sec
Operating Temperature	0-45 °C
Operating Humidity	20%-80%

4. Instructions for Use

4.1 Palm placement

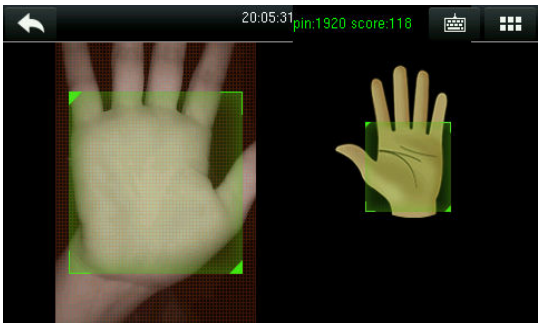
➢ How to correctly enroll the palm



Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device.
Make sure to keep space between your fingers.

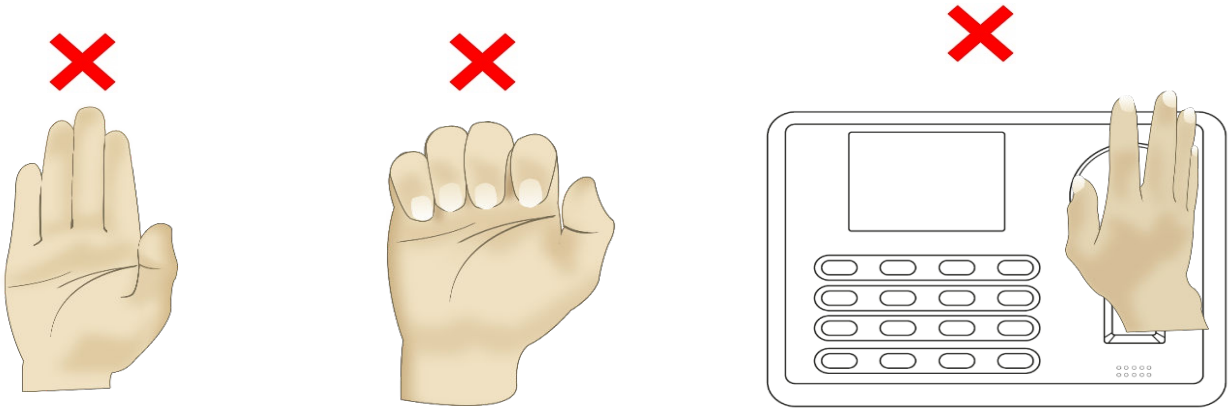
During enrollment locate your palm at the center of the screen, and follow the voice prompts "Focus the center of the palm inside the green box". The user needs to move forward and backward to adjust the palm position during the palm registration.

➢ Verification



Place your palm in the green area parallel to the device with space between the fingers.

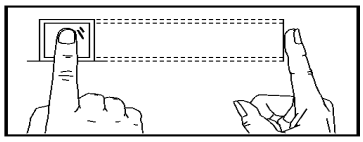
➢ Incorrect palm gestures

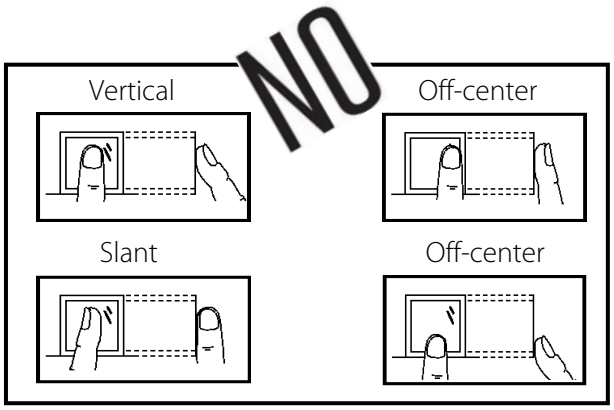


4.2 Finger placement

Recommended fingers: The index finger, middle finger or ring finger; avoid using the thumb and little finger (because they press the collection window is usually very clumsy).

➢ **Recommended placement**



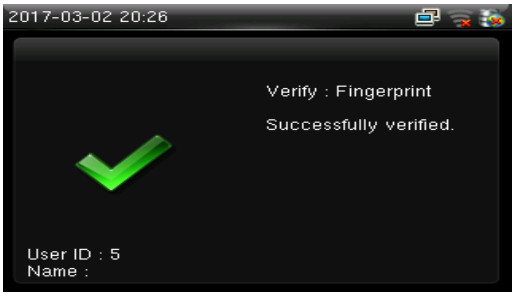


4.3 Verification Modes

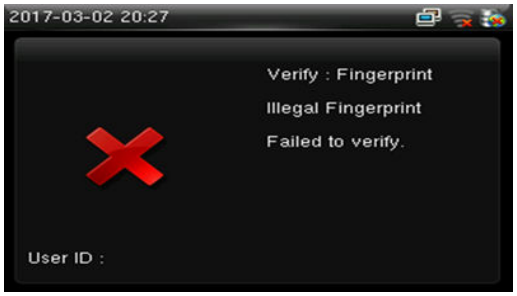
4.3.1 Fingerprint verification

➢ **1:N fingerprint verification mode**

The device compares the 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*.



Successfully verified



Failed to verify

➢ **1:1 fingerprint verification mode**

The device compares the current fingerprint with the fingerprint of the user whose ID is entered. The user chooses this mode unless poor recognition. Enter User ID and press "fingerprint", there are two responses after verification: ***Successfully verified*** and ***Failed to verify***.

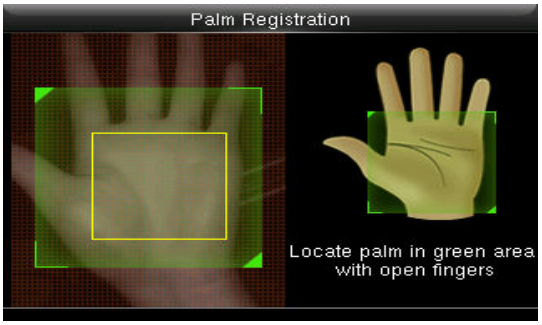
Note:

- The device prompts" Invalid ID" when there is no such user.
- The device prompts "Please try again" when failed to verify. After 2 attempts, if it fails the 3rd time, it returns to the initial interface.

4.3.2 Palm Verification

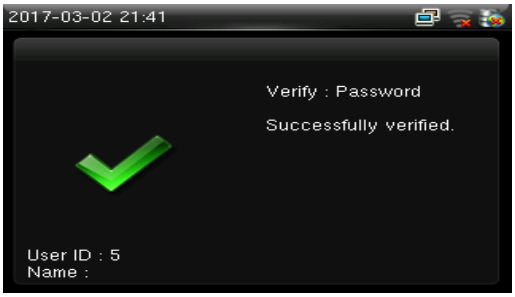
➢ **Palm verification mode**

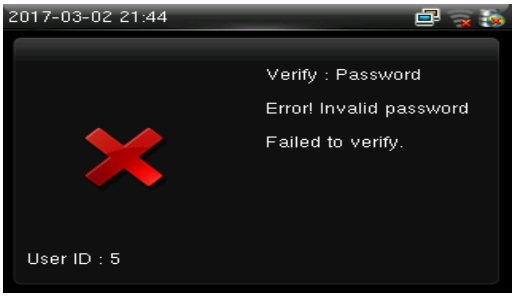
The device compares the current palm with users' palm in the device. Use the proper way to enroll and verify.



➢ **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 prompts "Incorrect password" when failed to verify. After 2 attempts, if it fails after the 3rd time, it returns to the initial interface.

4.3.3 Badge verification ★

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

The device “prompts” Duplicated Punch” when you swipe badge twice. The device prompts “Ou-Ou” when the badge is unregistered.

5. Main Menu

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

Function Definition:

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

User Role: Set the privilege of defined roles, that is, the privilege of operating menu.

Comm. (Communication Setting): Set the 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, palm 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.

Access 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.

Print: To set printing information and functions (if printer is connected to the 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 existence work code after verification.

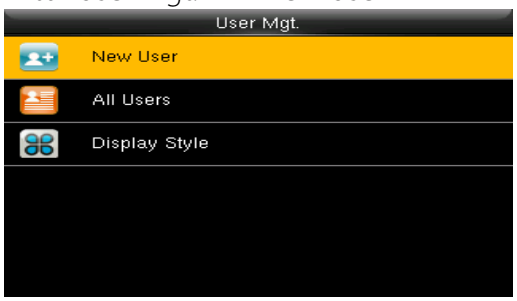
Autotest: Test whether each module is available or not, including LCD, voice, keyboard, fingerprint sensor, palm and clock RTC.

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

6. User Management

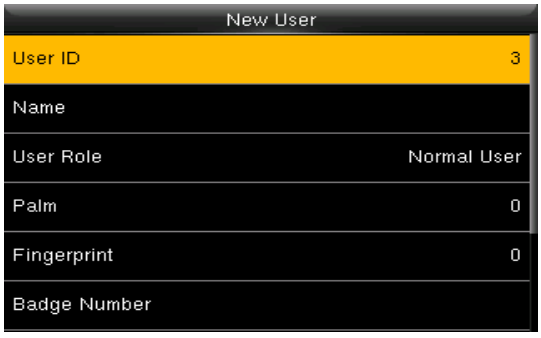
6.1 New User

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



6.1.1 Enter User ID and Name

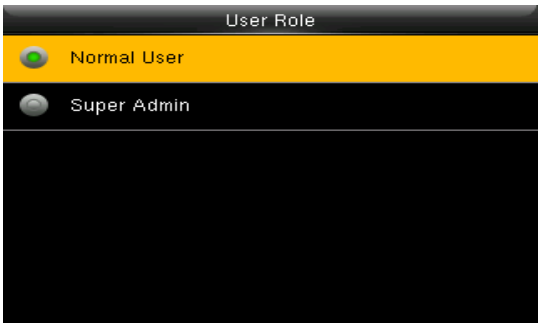
Press ▼/▲ to select any of the fields on the New User interface, press [M/OK]:



Note: You can input an ID, or use which is allotted by the device.

6.1.2 Enter User Role

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

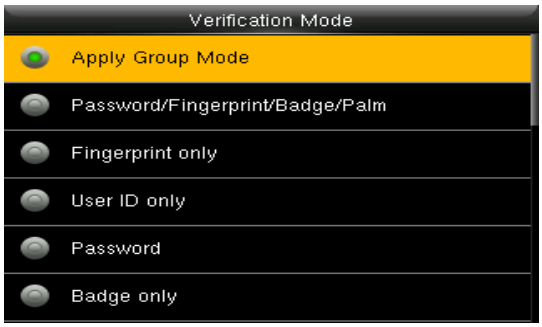


Super Admin: A super admin is granted rights to operate all functions and menus in the device.

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.

6.1.3 Verification Mode

Enter into "New user"→"Access Control role" , Press ▼ / ▲ to select "Verification Mode" on the interface, press [M/OK]:



There are several optional modes to set the verification way.

6.1.4 Enrolling a fingerprint

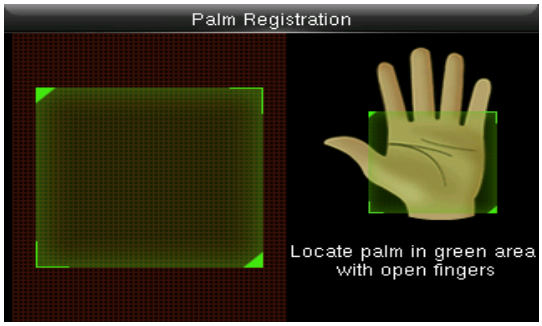
Press ▼ / ▲ to select "Fingerprint" on the New User interface, press [M/OK]:

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 re-enroll if the device says "Please try again".

6.1.5 Enrolling a palm

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



Note: Place your palm vein inside the green box, as the device says.

6.1.6 Enrolling a Badge★

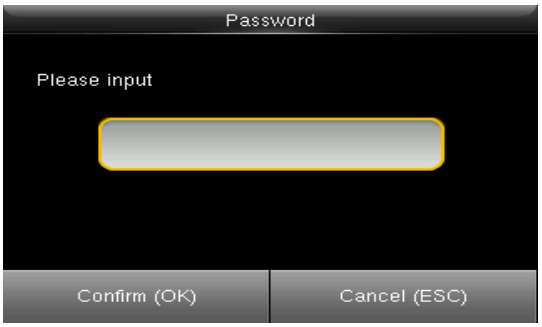
Press ▼ / ▲ to select "Badge Number" on the New User interface, press [M/OK]:

Swipe your badge around the fingerprint sensor.

Note: Please take another badge if the device displays "Error! Badge already enrolled". The Badge must be IC card.

6.1.7 Enrolling a password

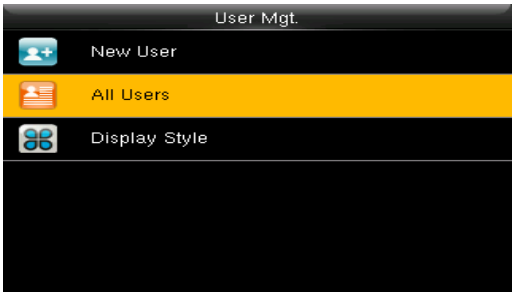
Press ▼ / ▲ to select "Password" on the New User interface, press [M/OK]:

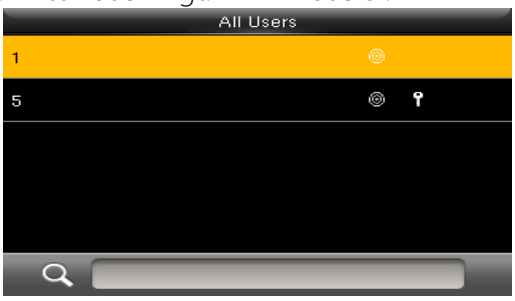


Input 1-8 digits password and press [M/OK], then re-type the password.

6.2 All Users

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



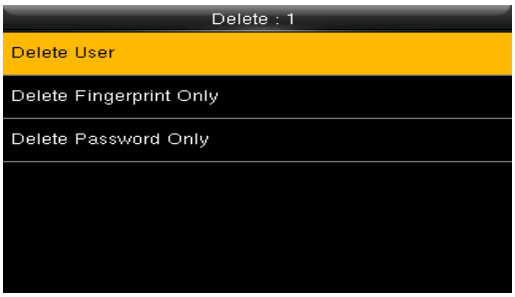


6.2.1 Editing a user

All information can be modified except User ID.

6.2.2 Deleting a User

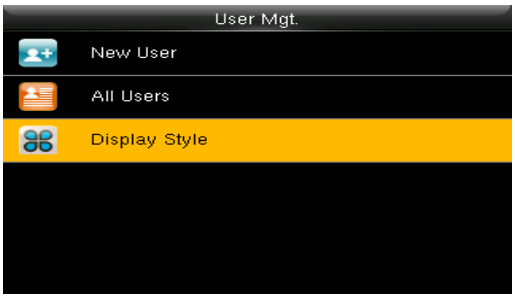
Press ▼ / ▲ to select a user to edit and press [M/OK]. Enter into "Delete":



You can choose different kinds of user data to delete.

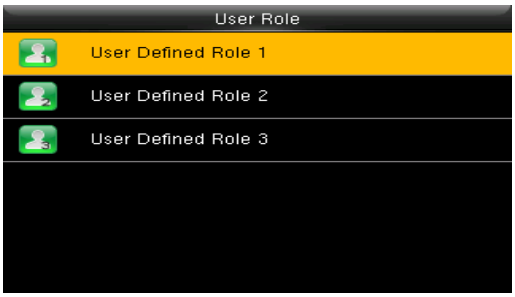
6.3 Display Style

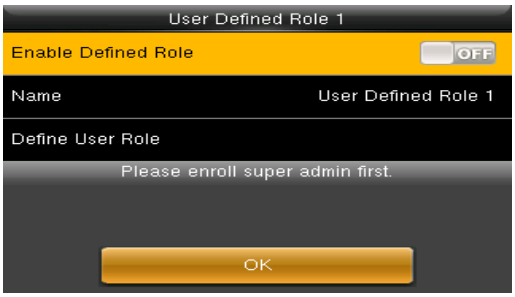
The default style is "Single Line". Enter into "User Mgt." → "Display Style":



7. User Role

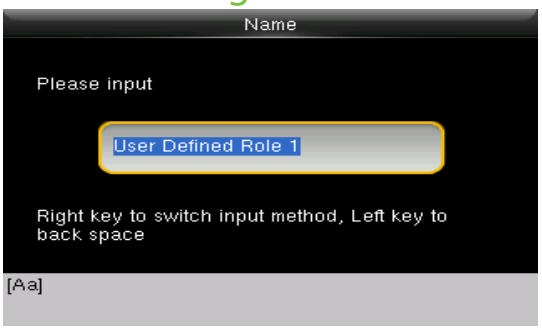
Use to define roles to operate the device. You can specify the available menus to operate for a role. There are 3 roles.
Enter into "User Role". Press one of the three roles to edit:





A Super admin must be enrolled before a new role is defined.

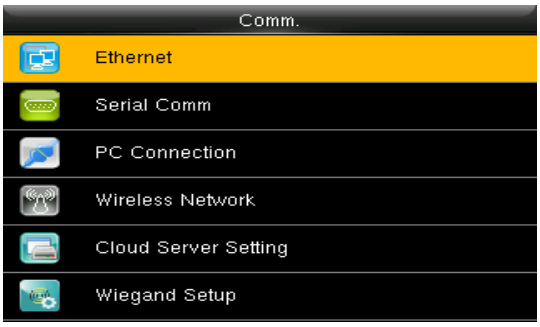
7.1 Creating a new role and its function



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

8. Communication Setting

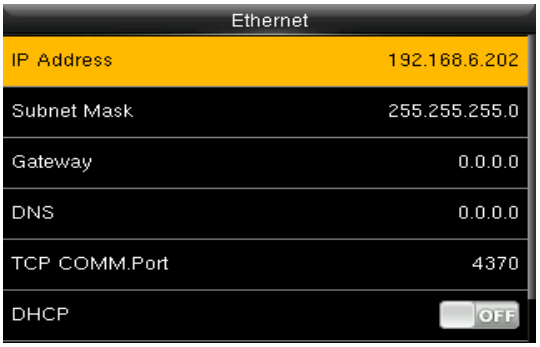
Set communication parameters. Enter into "Comm."



1. **Ethernet:** The device can communicate with PC each other via the parameters you set.
2. **Serial Comm:** The device can communicate with PC each other via the serial port parameters you set.
3. **PC Connection:** Set the password and device ID so that you can connect the device with software in PC.
4. **Wireless Network**：Turn on /off the WIFI setting.
5. **ADMS:** Settings used for connecting with ADMS server'
6. **Wiegand Setup:** The device can communicate with other device via the parameters you set.

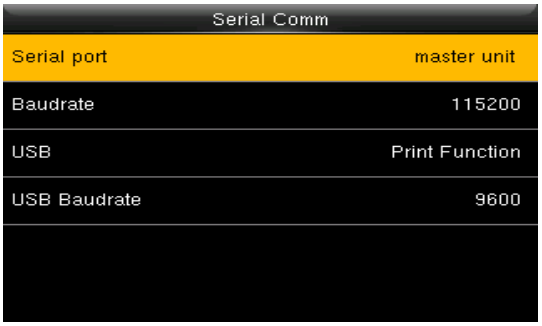
8.1 Ethernet

Enter into "Comm."→"Ethernet"



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

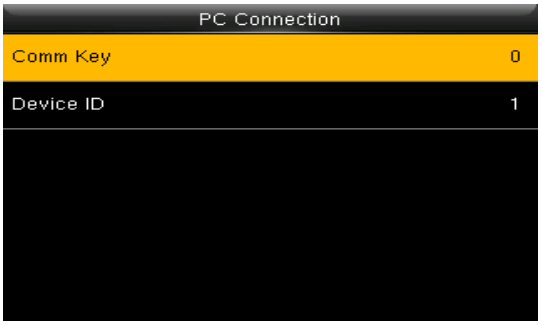
8.2 Serial Comm



1. **Serial port:** When serial port （RS232/RS485）is used for communication of device and PC, this setting need to be checked:
2. **Baudrate:** Used for communication with PC. RS232 is recommended for high speed.
3. **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.

8.3 PC Connection

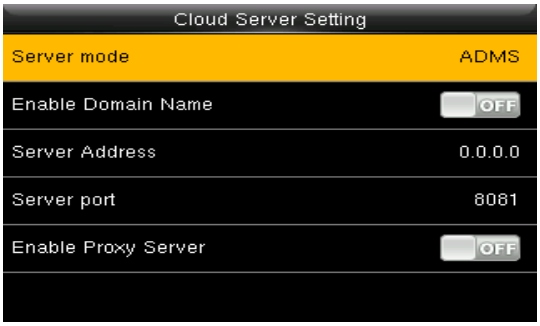
To improve the security of attendance data, connection password needs to be set here. Enter into Comm.→"PC Connection"



1. **Comm Key:** Set 1-6 digits connection password, the password must be input when PC software is to connect device to read data.
2. **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.

8.4 ADMS★

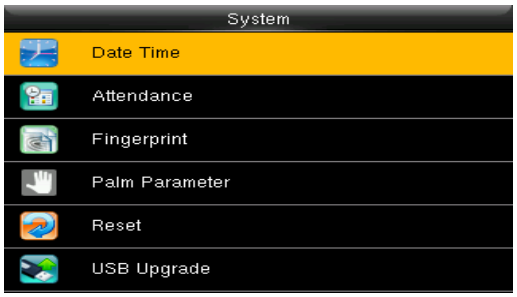
Settings used for connecting with ADMS server. Enter into "Comm"→"Cloud Server Setting".



1. **Enable Domain Name:** When the domain name mode is enabled, you access a website using a domain name in the format of http://; otherwise, you must enter an IP address for website access.
2. **Server Address:** IP address of Webserver
3. **Server port:** Port used by Webserver
4. **Enable Proxy Server:** When you enable the proxy function, set the IP address and port number of the proxy server. This option indicates whether to use a proxy IP address. You may choose to enter the proxy IP address or the server address for Internet access, whichever you like.

9. System

Set system parameters to meet user's demand as many as possible. Including the Date Time, Attendance, Fingerprint and so on



9.1 Date Time

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

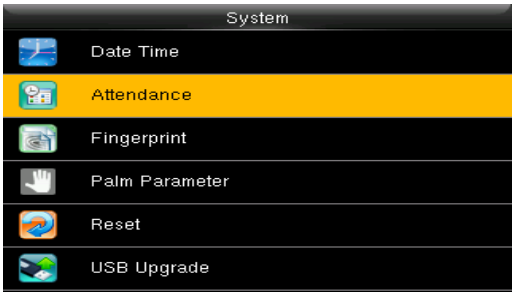
1. **Set Date/Time:** Set date and time of device.
2. **24-Hour Time:** Whether to use the 24-hour display mode. If not, the 12-hour display mode is adopted.
3. **Date Format:** Set the date format: YY-MM-DD, YY/MM/DD, YY.MM.DD, DD-MM-YY etc.

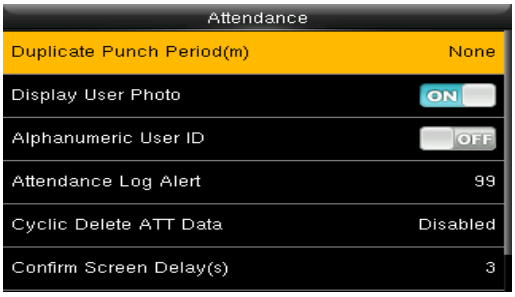
Daylight Saving Time:
The DST is a widely-used system of adjusting the local time forward to save energy. The uniform time adopted during the implementation of this system is known as the DST. Typically, clocks are adjusted forward one hour in the summer to make full use of illumination resources and 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 for next year. More specifically, the end time must be later than the start time in the same year.

9.2 Attendance

Enter into "System"→"Attendance"





Parameters of 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).

Display User Photo:

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.

Attendance Log Alert: When remainder log capacity is less than the set value, the device will prompt 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.

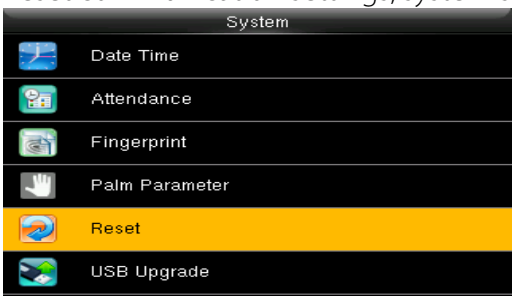
Confirm Screen Delay (s): The delay to display the verification result, the value is 1~9.

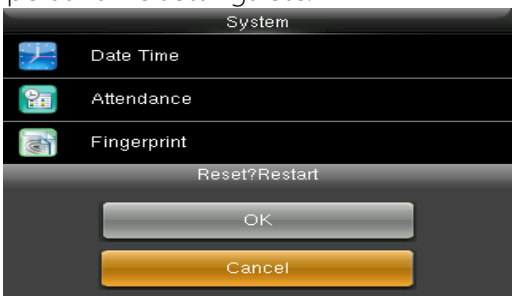
Expiration Rule: The choices for the function of the users' validity.

Expiration Rule Options: The settings for the end of validity.

9.3 Reset

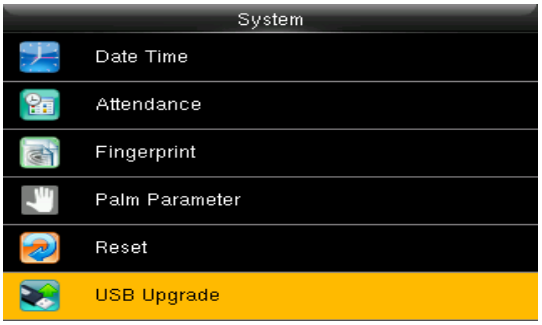
Reset communication settings, system settings, personalize settings etc.





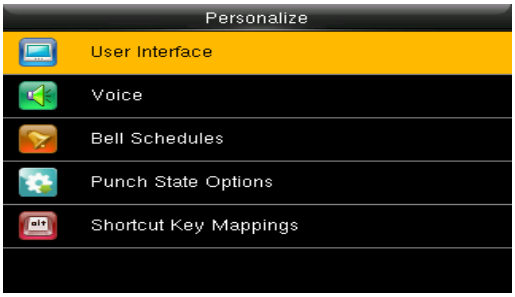
9.4 USB Upgrade

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.


System
Date Time
Attendance
Fingerprint
Palm Parameter
Reset
USB Upgrade

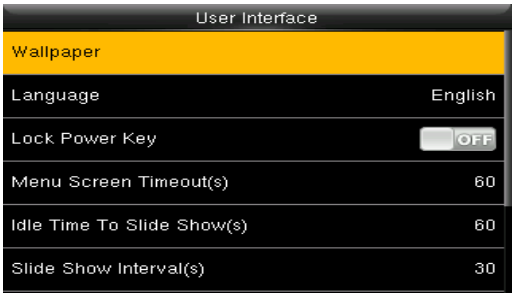
10. Personalize

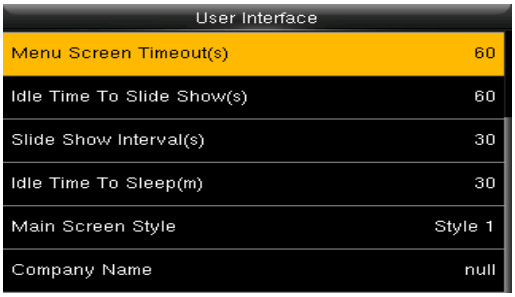
To set some usual parameters. Enter into "Personalize".



10.1 User Interface

To set displayed parameters. Enter into "Personalize"→"User Interface"





Wallpaper: Select the wallpaper of the 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.

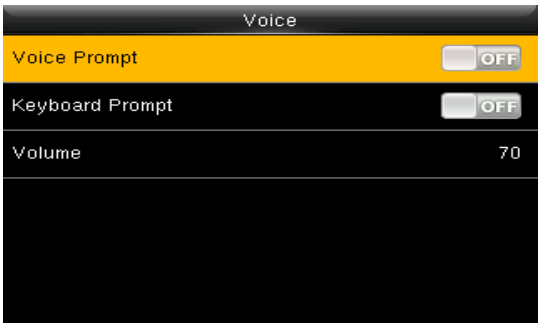
Idle Time To Slide Show (s): When standby time in main screen is larger than this value, the main screen will display a slide show. The valid value scope is 3~999 seconds.

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).

10.2 Voice



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

Keyboard Prompt: 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.

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

10.3 Bell Schedule

Many companies need a bell for on-duty and off-duty. Some uses manual bell and some uses electronic. To save cost and provide convenience to management, we integrate bell functions to fingerprint sensor. You can set the time for the bell. When it is the scheduled time, the device will automatically play the selected ringtone and trigger the relay signal. The ringtone playing does not stop until the ringing duration has elapsed.

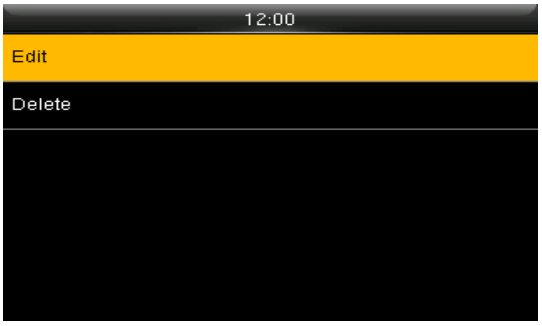
10.3.1 New Bell Schedule

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

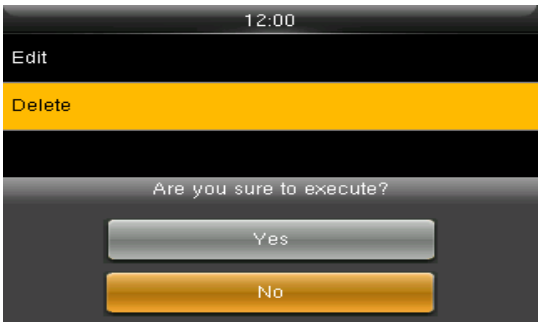
Bell Status: Enable/Disable this bell.
Bell Time: The bell rings automatically when it is the specified time.
Repeat: Specifies whether to repeat the ringtone.
Bell Type: You can select between internal ringing and external ringing. For internal ringing, the ring tone is played by the loudspeaker of the terminal. For external ringing, the ring tone is played by an external electric bell that is wired with the terminal.
Ring Tone: Bell ring
Internal bell delay (s): Specifies the duration for ringtone play. The value ranges from 1 s to 999s.

10.3.2 All Bell Schedule

For editing the scheduled bells



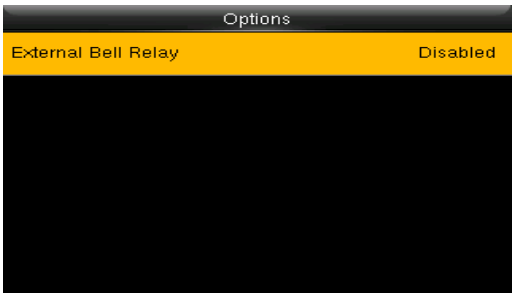
1. Select a bell to edit.
2. Press “Edit” to modify data.



1. Select a bell to delete it.
2. Press “Delete” to remove bell.

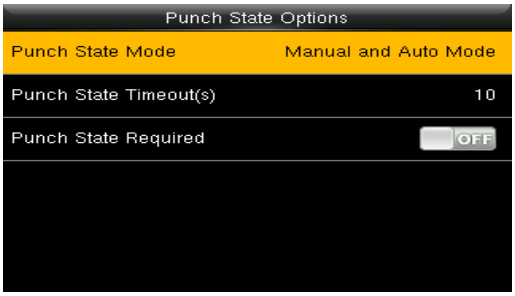
10.3.3 Options

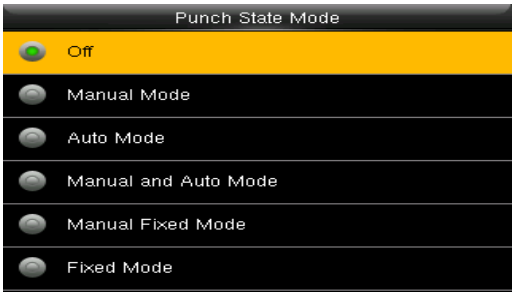
When the function of external ringing is used, set the output terminal of external ringing.



10.4 Punch State Options

To 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, and Overtime-Out.

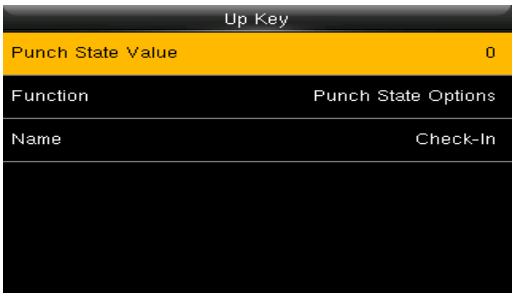
10.5 Shortcut Key Mappings

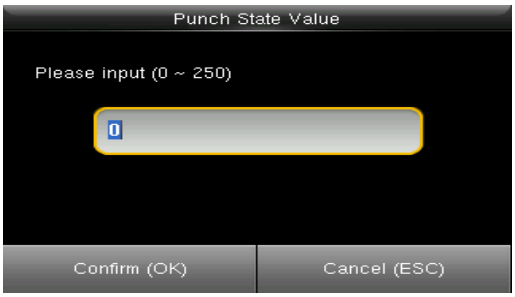
You can define six shortcut keys as attendance status shortcut keys or functional shortcut keys. On the main interface of the FFR terminal, press corresponding keys and the attendance status will be displayed or the function interface will be rapidly displayed.

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.

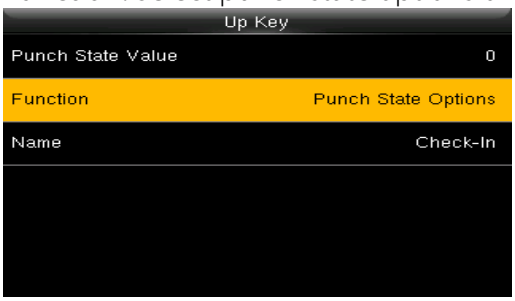
Select Function of shortcut key as Punch State Option, the shortcut key will not take effect under that Punch State Mode is set as OFF.

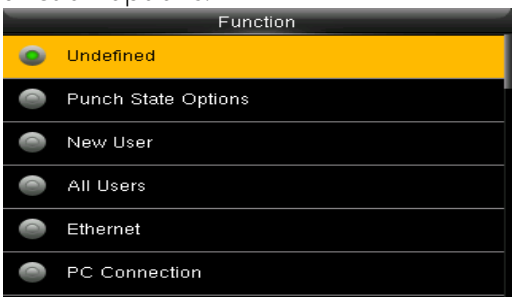
Punch State Value: The device sets 4 different values corresponding to four punch states by default. Value 0 corresponds to punch state Check-In, 1 for Check-Out, 4 for Overtime-In, 5 for Overtime-Out. The value ranges from 0 to 250.



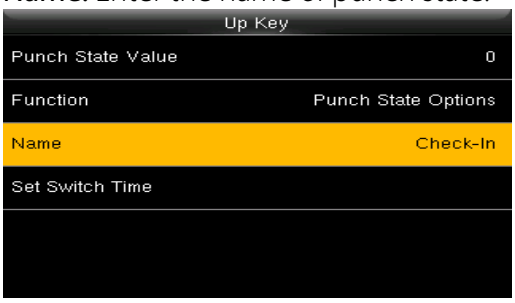


Function: Select punch state options or menu function options.

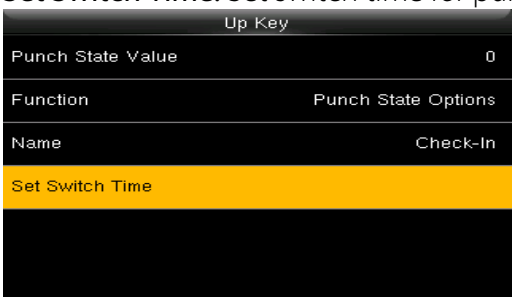




Name: Enter the name of punch state.

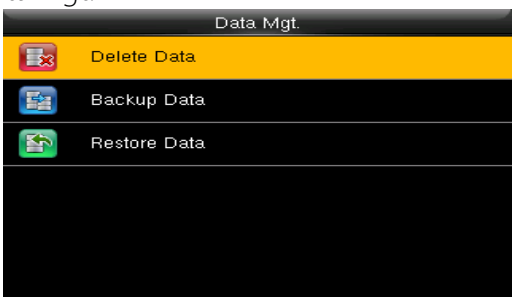


Set Switch Time: Set switch time for punch state.



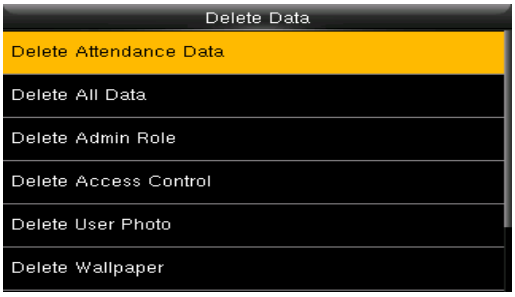
11. Data Mgt.

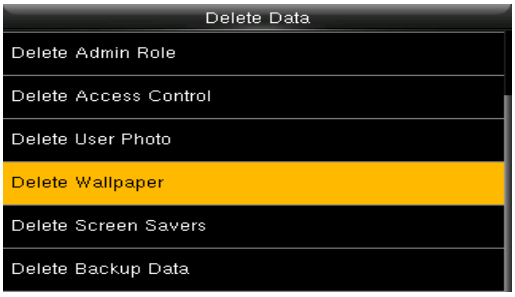
Manage data saved in the device. Enter into "Data Mgt."



11.1 Delete Data

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





Delete Attendance Data: Delete all attendance data.

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 Access Control ： Delete the settings of access control.

Delete User Photo: Delete all enrolled users' photos.

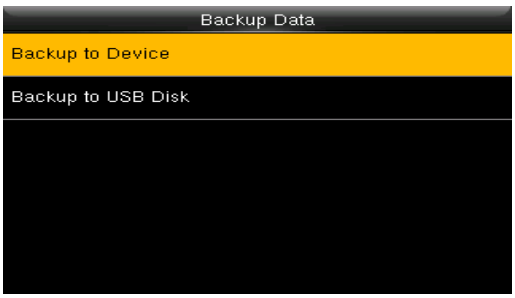
Delete Wallpaper: Delete all wallpapers in the device.

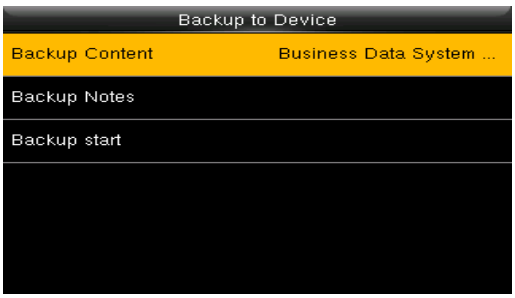
Delete Screen Savers: Delete all screen savers of the device.

Delete Backup Data: Delete data backup of the device.

11.2 Backup Data

Back up the service data or configuration data of the device to the device or a USB drive.

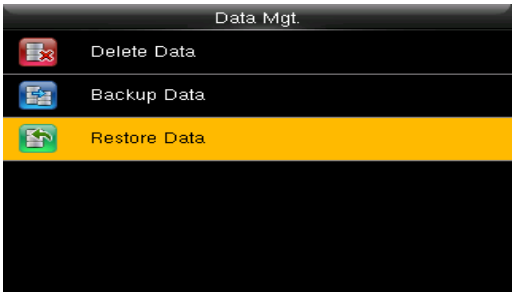




Note: When Backup data to USB Disk, you need to insert a USB Disk into the device at first, and then press [M/OK] to backup data to USB disk.

11.3 Restore Data

Restore the data stored on the device or on the USB drive inserted into the device.

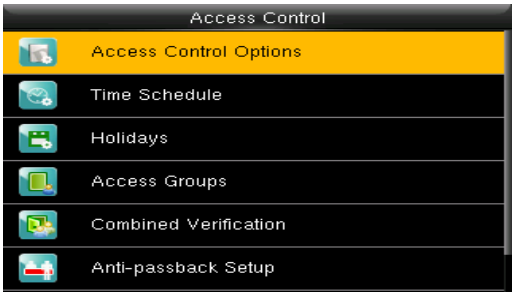


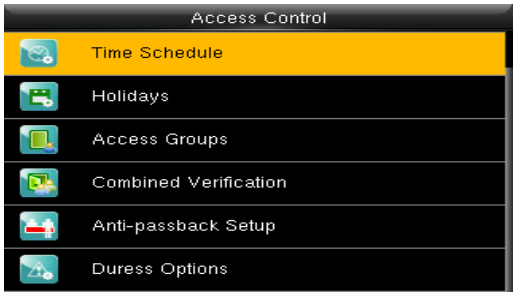
1. Select a route.
2. Select the data type.
3. Start the restore.

Note: When restoring data from a USB Disk, you need to insert a USB Disk into the device at first, which has the restored data.

12. Access Control

Access control option is to set user's open door Lock delay.





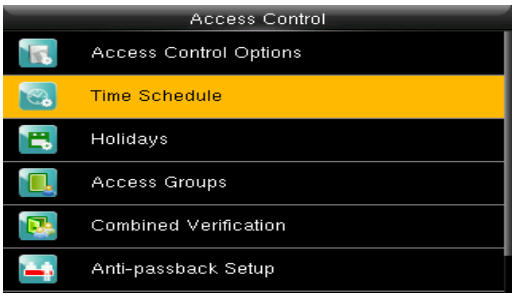
To unlock, the enrolled users must have owned these conditions:

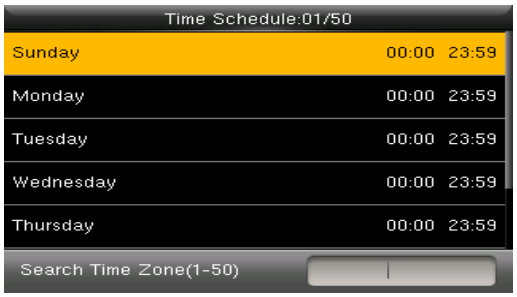
1. The current unlock time should be within the effective time of user time zone or group zone.

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 editing.

12.1 Time Schedule

Time Schedule is the minimum time unit of access control settings; at most 50 **Time Schedules** can be set for the system. Each **Time Schedule** consists of 7 time sections (a week), and each time section is the valid time within 24 hrs. Enter into "Access Control"→ "Time Schedule".



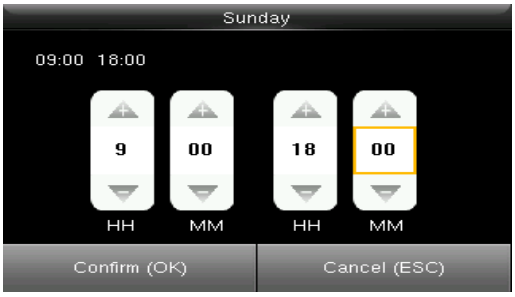


The default Time Schedule No. is 1 (whole-day valid), which can be edited.

Valid Time Schedule: 00:00 ~ 23:59 (Whole-day valid) or when the end time is greater than the start time.

Invalid Time Schedule: When the end time is smaller than the start time.

The following examples as explanation:



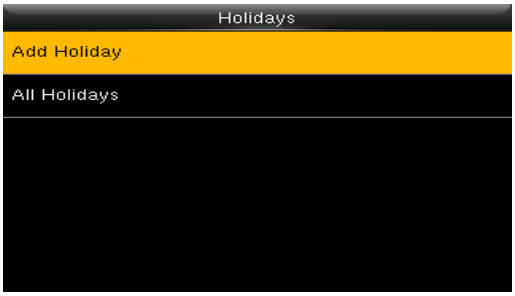
Valid

Invalid

Note: The **Time Schedule** cannot be set across two days, which means that the end time must be greater than the start time.

12.2 Holidays

The holiday access control time can be set, which is applicable for all users during holiday. Enter into "Access Control"→"Holidays", press "Add Holiday" and enter into the interface .



Settings include number, start time, end time and time period.

Note: Start/End Date only requires to set the month (MM) and date (DD), which is applicable to all years.

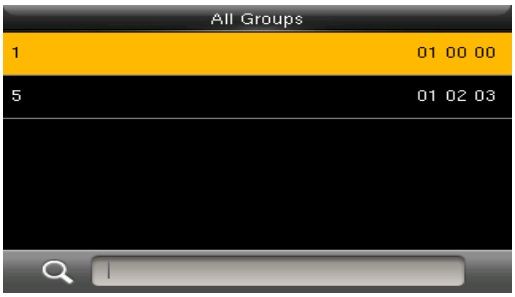
Time period: the valid time Schedule used in the holiday.

As shown in above figure: Holiday 1 starts on the May 1 every year, ends on the May 3 every year

12.3 Access Groups

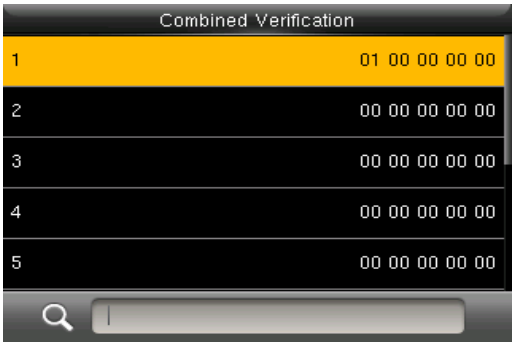
Grouping is to manage users in groups.
Group users' default time zone is set to be the group time zone, while users can set their personal time zone. Each group can set 3 time zones at most, as long as one of them is valid, the group can be verified successfully.
By default, the new enrolled user belongs to Access Group 1, and can also be allocated to other access group. Enter into "Access Control"→"Access Groups" →"New Group".

As shown in the following figures, the **Verification Mode** of **Access Group 5** is fingerprint only; Time Zone 1, 2 and 3 are set, while the Holiday function is enabled.



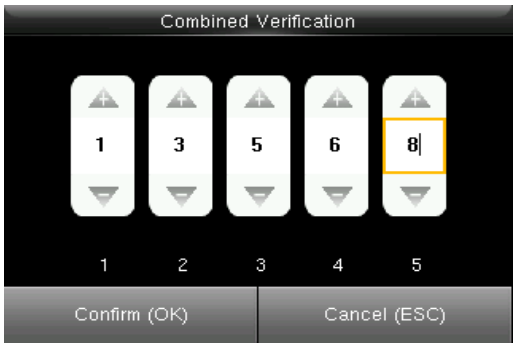
12.4 Combined Verification★

Combine two or more members to achieve multi-verification and improve security.
In a Combined Verification, the range of user number is: 0 ≤ N ≤ 5; the users can all belong to a single group, or belong to 5 different groups at most.



Note: Only group No. set in Access Group interface, can it be selected in the Combined Verification setting.

For Example, (The following access groups have been set in **Access Group** interface**):**



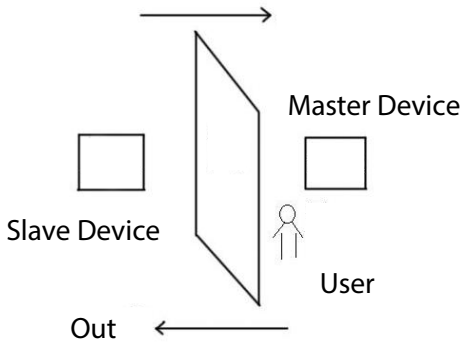
As the figure says, Combined Verification 1 is made up of five members coming from five different groups---access group 1 / 3 / 5 / 6 / 8 respectively.

Note: To delete a Combined Verification, set all access group numbers to 0.

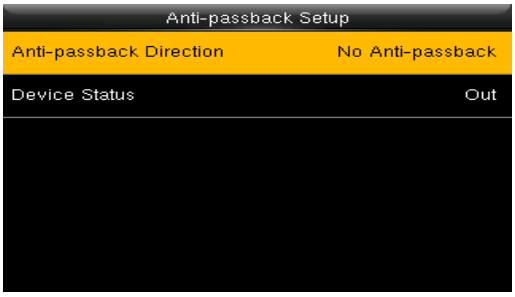
12.5 Anti-passback Setup★

To avoid some persons following users to enter the door without verification, resulting in security problem, users can enable anti-passback function. The check-in record must match with check-out record so as to open the door.

This function requires two devices to work together: one is installed inside the door (master device), the other one is installed outside the door (slave device). The two devices communicate via Wiegand signal. The Wiegand format and Output type (User ID / Badge Number) adopted by the master device and slave device must be consistent.



- Anti-Passback Direction



No Anti-passback: Anti-Passback function is disabled, which means passing verification of either master device or slave device can unlock the door. Attendance state is not reserved.

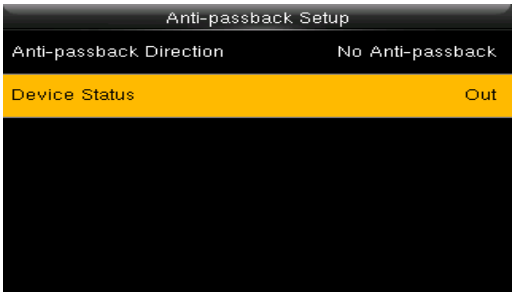
Out Anti-passback: After a user checks out, only if the last record is a check-in record can the user check out again; otherwise, the alarm will be triggered. However, the user can check in freely.

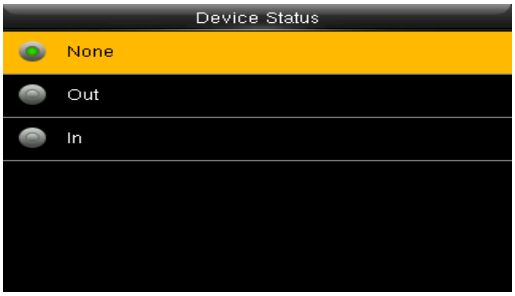
In Anti-passback: After a user checks in, only if the last record is a check-out record can the user check in again; otherwise, the alarm will be triggered. However, the user can check out freely.

In/Out Anti-passback: After a user checks in/out, only if the last record is a check-out record can the user check in again, or a check-in record can the user check out again; otherwise, the alarm will be triggered.

Null and Save: Anti-passback function is disabled, but attendance state is reserved.

- Device Status

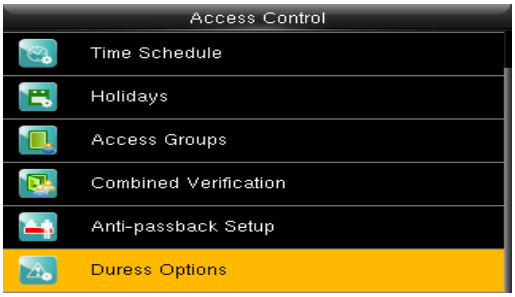


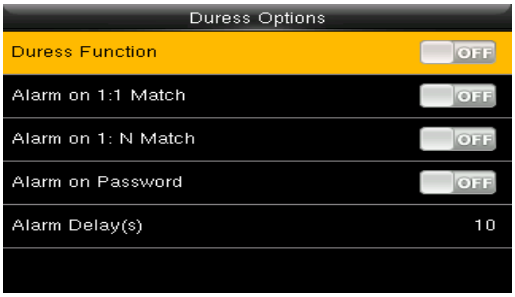


None: To disable the Anti-Passback function.
Out: All records on the device are check-out records.
In: All records on the device are check-in records

12.6 Duress Option

When users come across duress, select duress alarm mode, the device will then open the door as usual and send the alarm signal to the backstage alarm.





Duress Function: In **[ON]** state, press "Duress Key" and then press any registered fingerprint (within 10 seconds), duress alarm will be triggered after successful verification. In **[OFF]** state, pressing "Duress Key" will not trigger the alarm.

Alarm on 1:1 Match: In **[ON]** state, when a user uses 1:1 Verification Method to verify any registered fingerprint, alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.

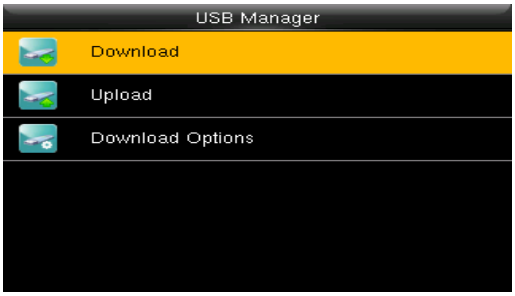
Alarm on 1: N Match: In **[ON]** state, when a user uses 1:N Verification Method to verify any registered fingerprint, alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.

Alarm on Password: In **[ON]** state, when a user uses password verification method, alarm will be triggered. In **[OFF]** state, no alarm signal will be triggered.

Alarm Delay (s): When duress alarm is triggered, the device will send out alarm signal after 10 seconds (default); the alarm delay time can be changed (value ranges from 0 to 999 seconds).

13. USB Manager

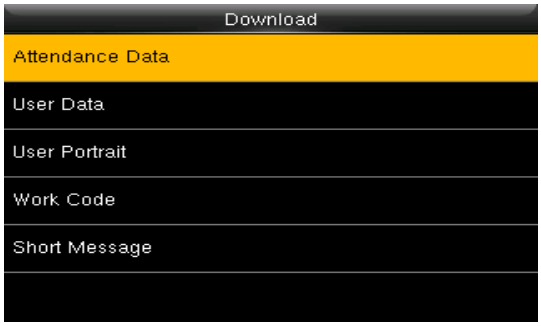
Import user information, fingerprint template, attendance data and so on in the device to attendance software or import user information and fingerprint to other devices through U disk. Enter into" USB Manager "→"Download"/"Upload"



Note: Before you upload/download data from/to a USB drive, insert the USB drive into the USB interface of the device.

13.1 Download

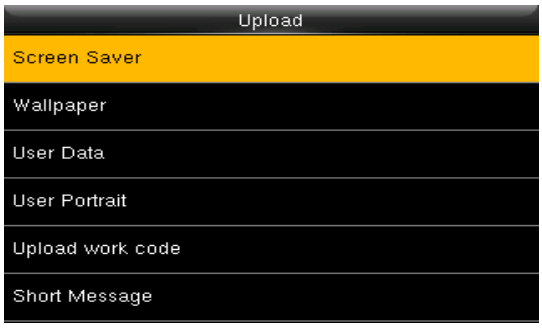
Download data to USB drive from the device.



Attendance Data: Download attendance data to USB disk.
User Data: Download all user data to USB disk.
User Portrait: Download attendance photos to USB disk.
Work Code: Download all work codes to USB disk.
Short Message: Download all short messages to USB disk.

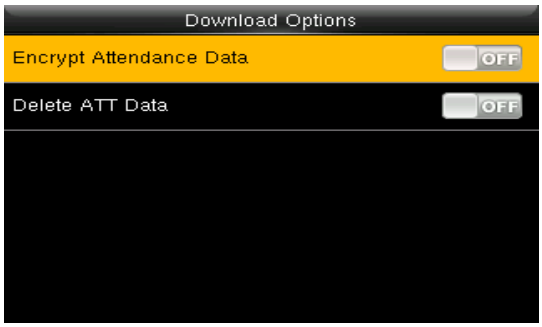
13.2 Upload

Upload data to the device through the USB drive



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

13.3 Download Options



You can encrypt the data in a USB drive and set to delete data after being downloaded.
During downloading the attendance records, you can also set the calendar type displayed in the attendance time.
The device supports three calendar types which are Gregorian, Iran Gregorian, and Iran Lunar.

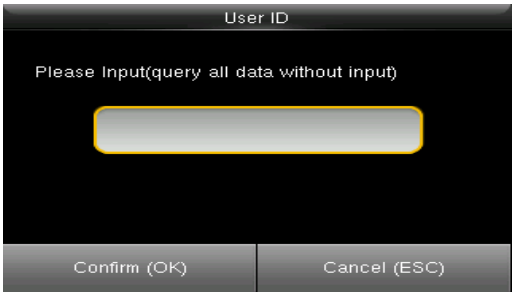
14. Attendance Search

Employee's attendance record will be saved in the device. For query convenience, the attendance search function is provided.

Attendance Record: Search the attendance records in the device. When you have verified in the device, the record is saved.

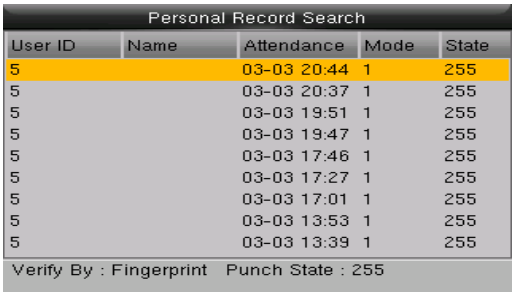
Attendance photo: Search the attendance record restored in the device. When you have verified, the device's camera will capture a photo to save in the device.

Go to 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.



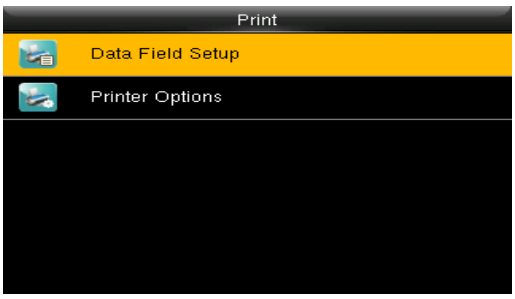
3. The record list is displayed.
4. Select any to check details.

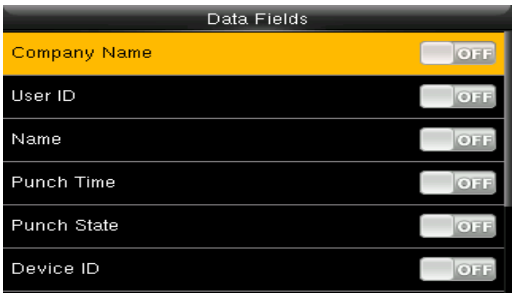
15. Print

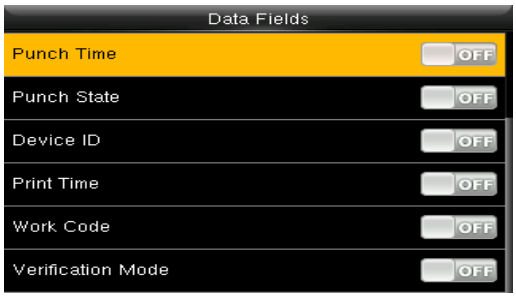
Devices with printing function can print attendance records out when a printer is connected

15.1 Data Field Setup

In the initial interface, press **[M/OK]** > **Print** > **Data Field Setup** > press **[M/OK]** to turn on / off the fields needing to be printed.

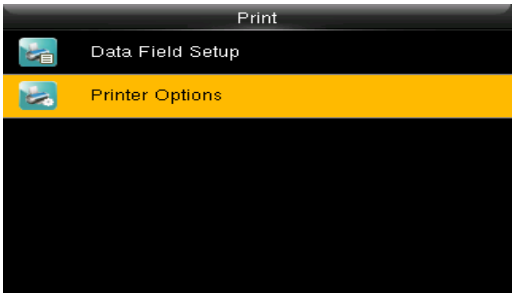


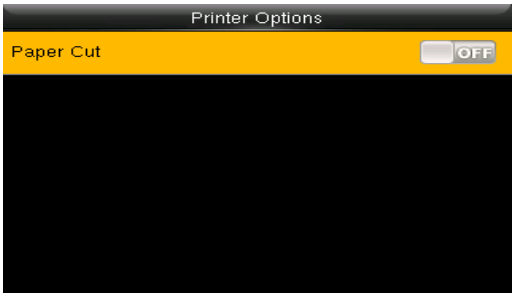




15.2 Printer Options

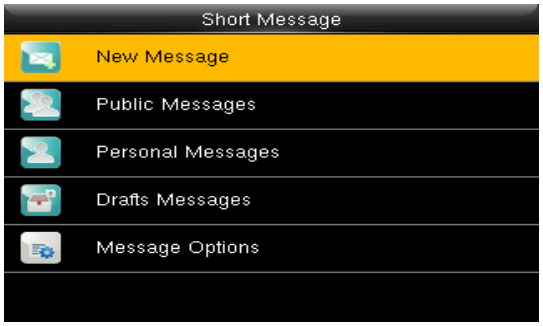
Enter into "Print"→"Printer Options". Press **[M/OK]** to turn on / off the **Paper Cut** function.





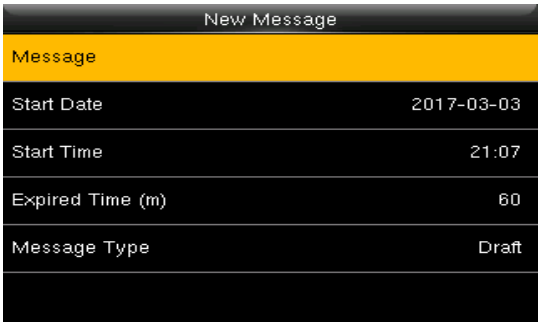
Note: To turn on the **Paper Cut** function, it is required to connect the device with a printer with paper cutting function, so that the printer will cut papers according to the selected printing information when printing.

16. Short Message

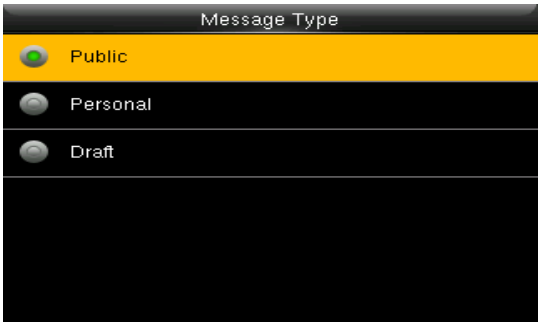


You can add, edit, delete and send public or personal message. And you can save the message in drafts. In assigned time, the public message will display to all users at the bottom of main screen, and personal message will display to specified user after successful verification.
You can check public,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

16.1 Creating a New Message



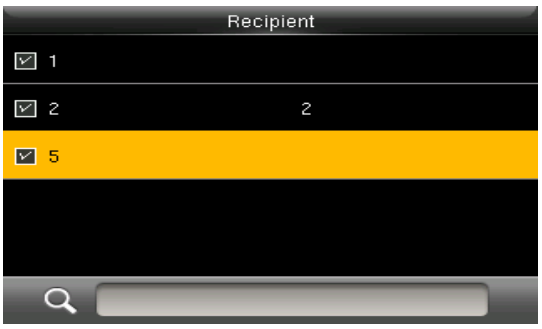
Message: Input the message text.
Start Date/Time: Set the start date & time of message pops.
Expired Time: Time of message expired, calculated from the time you add.
Message Type: Public, Personal, Drafts.



Public: SMS able to be seen by all employees.
Personal: SMS aimed at individual only.
Draft: Pre-set SMS, no difference of individual SMS or common SMS.

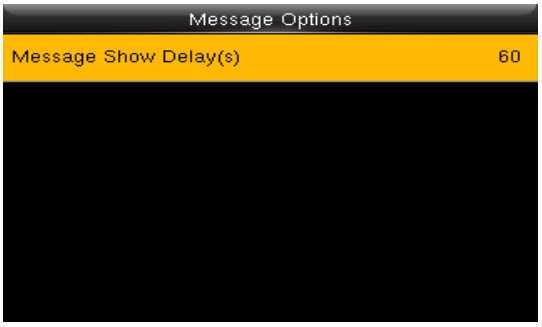
➢ **Viewing or editing the message:**

Press ▼ **to select the message list,** then press OK. You can view, edit or delete the one you selected. When editing message, the operations are similar to those performed to add SMS.



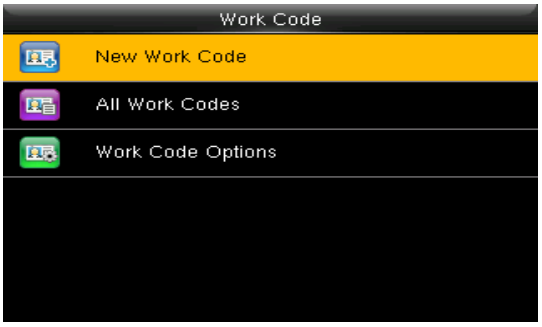
While editing personal message, you can select more than one user to receive this message. Press [ESC] to save and exit.

16.2 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.

17. 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.

17.1 New Work Code

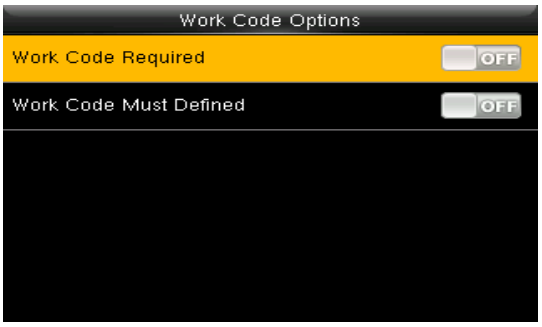
ID: The allocated working number. The range is 1-99999999.
Name: Input a name with T9 input. 23-characters are limited.
Note: The work code cannot be modified once confirmed.

17.2 All Work Code

You can view, edit or delete the work code from the work codes list. The ID cannot be modified, and the other operations are similar to those performed to add a work code when edit.

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

17.3 Work Code options

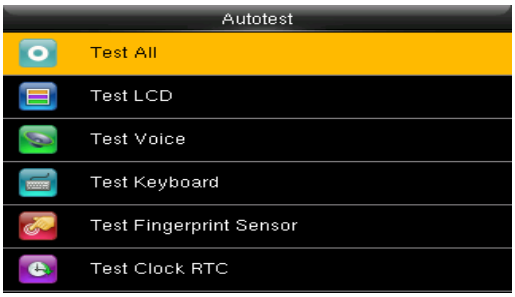


Work Code Required: The work code must be input during verification. Select whether to enable this function.

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

18. Autotest

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



Test All: The terminal automatically tests the LCD, voice, sensor, keyboard and click, press [OK] to continue and press [ESC] to exit.

Test LCD: Checks the LCD (Liquid Crystal Display).

Test Voice: Checks if the voice prompts are displayed normally.

Test Keyboard: Checks if the keyboard is available.

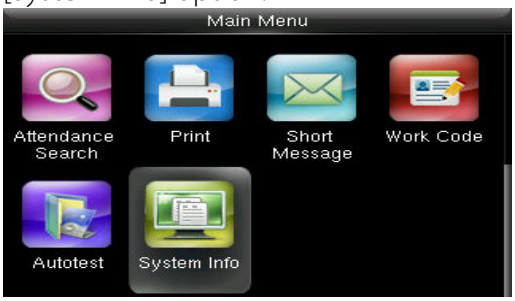
Test Fingerprint Sensor: Checks if the fingerprint sensor is available to use.

Test Clock RTC: Checks if the RTC (Real-Time Clock) is accurate.

While checking modules, please follow the prompts in the specific interface.

19. System Info

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



Click specific option to check the parameters:

Device Capacity: Number of users, admin users, number and the most capacity of fingerprints, palm, badge, attendance record and attendance photos number.

Device Info. (Information): Device name, serial number, MAC address, fingerprint algorithm, palm algorithm, platform information, manufacturer, manufacturer date.

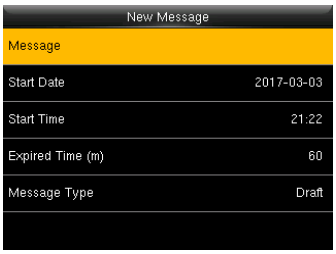
Firmware info: Firmware version, bio service, standalone service, device service.

All information here is not allowed to modify.

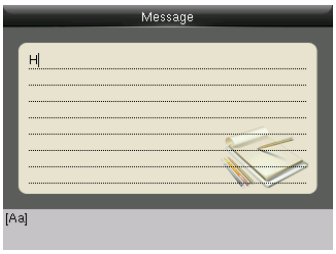
20. Appendix

1. T9 Input

T9 input (intelligent input) is quick and high efficient. There are 3 or 4 letters on the 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. Refer below example to understand the methods:

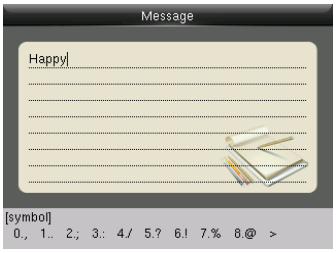


Enter into “New Message”.

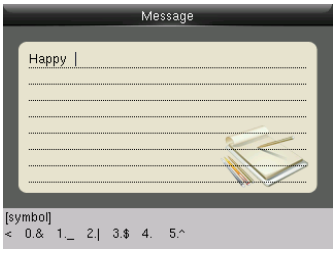


Press [4] twice to input H.

Input ”appy” with the same way. \

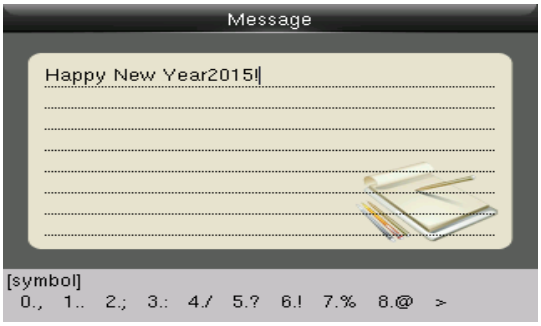


Press ►to ”symbol” type



Press ►to find to ”4. ”
Press 4 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 "!"

2. Rules to upload picture

- **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 the photo is X.jpg (X represents User ID, which does not limit digits). The format of the photo must be .JPG.

- **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 the name and format of the screen saver.

- **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 the 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 of Human 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 world suffers a 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 the 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	✕	o	o	o	o	o
Chip Capacitor	✕	o	o	o	o	o
Chip Inductor	✕	o	o	o	o	o
Chip Diode	✕	o	o	o	o	o
ESD component	✕	o	o	o	o	o
Buzzer	✕	o	o	o	o	o
Adapter	✕	o	o	o	o	o
Screws	o	o	o	✕	o	o

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

✕ 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 economic constraints.