F18 User Manual

Version: 1.0
Date: Dec. 2011

Introduction:

This document mainly introduces the windows and operations of the F18 model 2.4 inch color TFT product.

About this manual

1. Not all the devices have the function with ★. The actual product prevails.
2. The photograph in this manual may be different from that of the actual product. The actual product prevails.
3. Key functions of various models are different. Please initially read the key board instruction in the appendix.
4. Due to the constant updating of products, the company cannot maintain the information in the document with the actual product. Please forgive any difference between the actual technical parameters of the product and the information in this document. The information in this document is subject to change without notice.

Contents

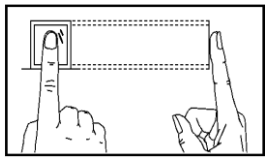
1. Operating Instruction

1.1 Abbreviated Operating Procedures

Step 1: Install the device and power it up.
Step 2: Enroll users by registering his/her fingerprints, passwords or card. Assign user's security privileges directly on the device.
Step 3: After enrolling users, verify that his/her enrolled fingerprint, passwords or card is valid.
Step 4: Configure the device communication settings. Then download the user's newly enrolled information from the device to the Attendance Management on the computer. Data can be transmitted via TCP/IP, RS232, RS485 and USB client or by using a USB flash drive.
Step 5: Modify user's information in the Attendance Management, and upload this new information to the device after connecting. Then the user's new information will be displayed on the screen attendance. (Some models allow name editing and other operations directly on the device. Therefore, it is not necessary to connect to the device.)
Step 6: Verify the device displays the correct day and time. Then start attendance.
Step7: Download attendance records to the Attendance Management and analyze at the end of the month.

1.2 Introduction to Fingerprint Recognition Technology

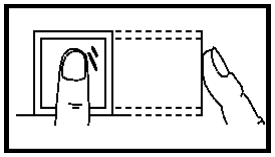
Enroll fingerprint by pressing index finger, middle finger or ring finger.
Proper press:



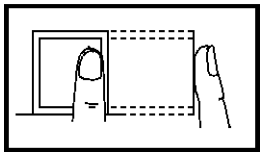
Press finger on the center of the sensor window

Improper press:

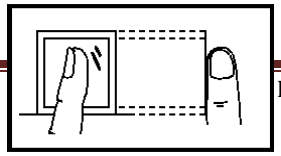
Upright



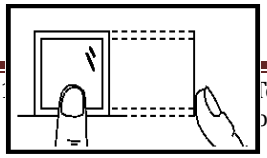
Off Center



Slant



Too Low

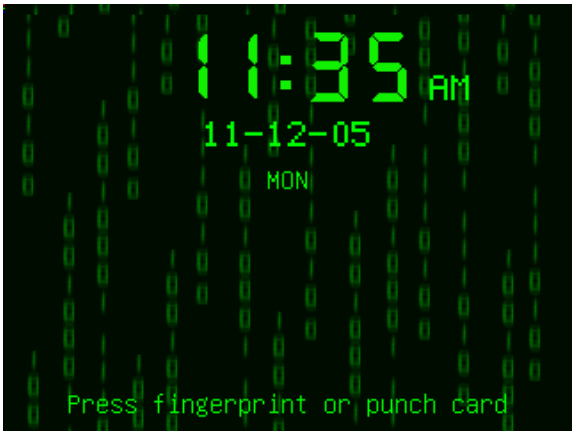


Please adopt the correct way to place the finger to avoid improper operation leading to identification performance degradation.

1.3 About Verification Mode

When the device is on Initial Interface, only after successful Fingerprint or Password or Card verification, can a user save an attendance record on the device.

Initial Interface (As shown below**)**:



Notice:

If the device has an ID module, Matrix and Magic style Interface can be displayed "Press fingerprint or punch card". If the device does not have an ID module, it can only display "Please Press fingerprint".

1) The device has three interface styles options. Each style displays different contents on the screen. For details please refer to 4.4 Display Setting.

2) As above, on the "Name" screen, editing different names can be executed by using "Access Control Management Software ".

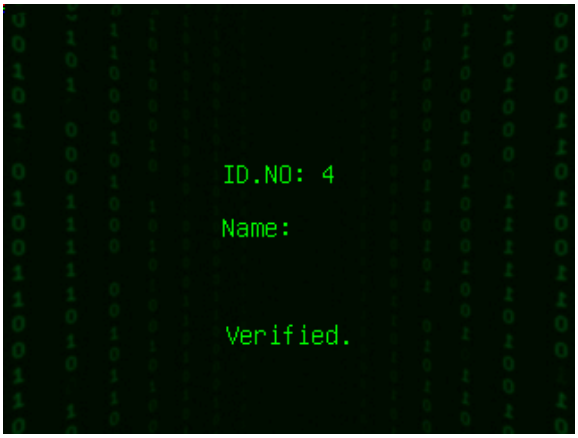
- **Fingerprint Matching**

(1) 1:N Fingerprint Matching

Verify the fingerprint currently pressed on the sensor with all fingerprint data in the fingerprint reader.

Step 1: Press fingerprint properly on the sensor on initial interface.

Step 2: If device says ‘Thank you”, verification is complete.



If device says “Please press again”, and displays "Verify fail" on the screen, Return to Step 1 for the second operation.

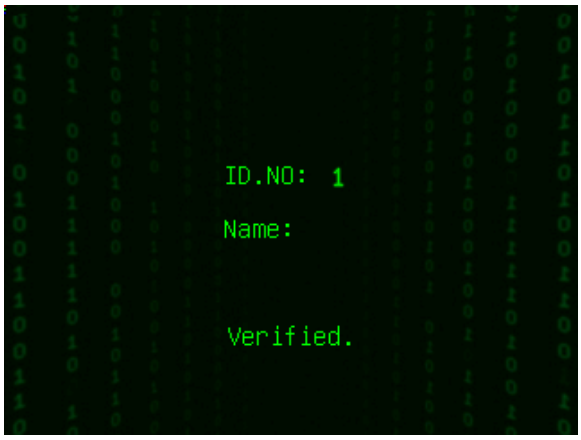
(2) 1:1 Fingerprint Match（User ID＋fingerprint)

Verify the fingerprint currently pressed on the sensor with a stored fingerprint and related user number. Use this method when it is difficult to identify a user’s fingerprint.

Step 1: Input User ID of employee to be verified on initial interface.

Step 2: Press fingerprint properly on the sensor.

Step 3: If device says 'Thank you", the verification is complete.



☺**Notice**:

①If device says "Please press again", return to Step 2 for the second operation.

②If device says “Error ID”, that means the entered ID number is wrong, please return Step 1 for the second operation.

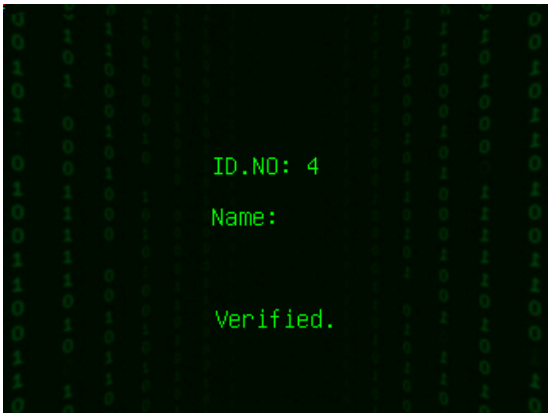
- **Password Matching**

Step 1: Input User ID of employee to be verified on initial interface. Then press **OK.**

Step 2: If it says that the enroll number is wrong, it means that there is no such number or the employee does not have an enrolled password.

Step3: Input password when the interface appears.

Step 4: If device says ‘Thank you”, the verification is complete.



When the screen displays "password error" and "Input password again" as shown below:

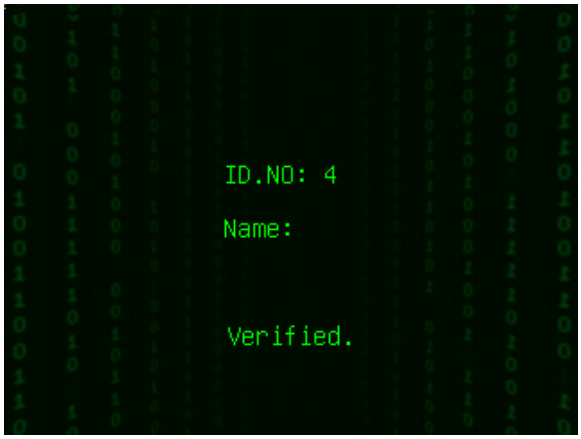
Please return to Step 3 and input the password again for the second operation. Ranges of the input password time is 0~9. Employee can set default time what you want. For details please refer to 4.4 Display Setting.

- **Card Matching ★**

The card area is round the keyboard.

Step 1: Wave the card near the induction area on the initial interface. After the induction equipment finds the card, please remove the card.

Step 2: When the equipment displays "Thank you", the certification is complete.



Step 3: If the card has not been registered yet, the device prompts that the card is not registered.

1.4 Connection with PC

The device only records attendance time. The report can be prepared by software on a PC. Therefore, it is necessary for the device to connect to a PC to download attendance records to attendance software.
The following are some connection methods:

- Ethernet:

（1) Through hub: Use parallel net cable (to connect network card and hub) to connect the device to a network.
（2) Direct connection: use cross net cable（connect two Ethernet terminals directly) to connect the device to a PC.
Set device: Enter **Menu**—**Communication option**—**Network** to set the following items:
IP address: Default IP as 192.168.1.201. You can modify it as necessary.
Subnet mask: Default subnet mask as 255.255.255.0. You can modify it as necessary.
Gateway address: Default gateway address0.0.0.0. You can modify it as necessary.

Network speed: There are three options: AUTO, 10M, and 100M.
Connection password: Set it in "**Menu—Communication option—Security**". It is optional. If it is set, input corresponding numerical value on connection interface of PC software.

- RS232: Use RS232 serial port wire for connection.

Set device: Enter **Menu—Communication option** to set the following options:
Baud rate: Set it in "RS232/485". Communication speed rate (with computer), if the communication speed is high, RS232 （115200, 57600) is recommended.
RS232: Set it in "RS232/485".Select "Yes" for RS232.
Communication password: Set it in "Security". It is optional. If it is set, input corresponding numerical value on connection interface of PC software.

- RS485

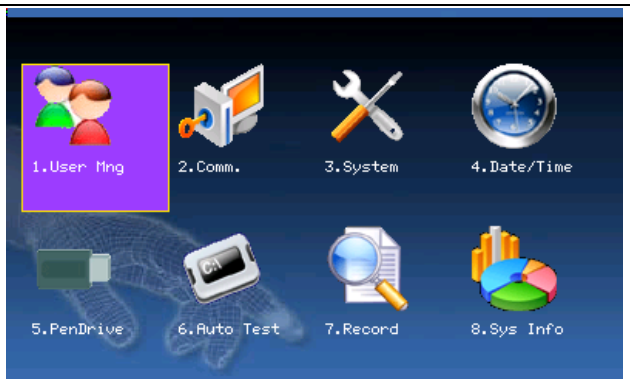
Set device: Enter **Menu—Communication option** to set the following options:
Device ID: Set it in "Security". It can be set from 1—254.
Baud rate: Set it in "RS232/485". Communication speed rate (with computer), if the communication speed is low and stable, RS 485 （9600, 38400) is recommended.
RS485: Set it in "RS232/485". Select "Yes" for RS485
Communication password: Set it in "Security". It is optional. If it is set, input corresponding numerical value on connection interface of PC software.

- USB

Set device: Enter **Menu—Communication option** to set the following items:
Device ID: Set it in "Security". It can be set from 1—254.
USB: Set it in "RS232/485". Select "Yes" for USB communication.
Communication password: Set it in "Security". It is optional. If it is set, input corresponding numerical value on connection interface of PC software.

1.5 Main Menu

On the initial interface, press the Menu key for 3 seconds to open the Main Menu as shown in the following figure:



User Management: Browse the users' basic information like ID, name, fingerprint, card, password, privilege and so on; Increase, edit or delete basic information; Set the work code for user and card management.

Communication: Set up communication parameters between the equipment and the PC, including IP address, gateway, subnet mask, baud rate, device number, communications password etc.

System: Manage the data and set the system parameters, including basic parameters, interface parameters, fingerprint and attendance parameters, to meet user's needs in the functional, display and other areas.

Date/Time: Device time and date should be set accurately to ensure the accurate attendance time.

PenDrive: By USB, the user info and attendance data etc. can be imported to the appropriate software to distribute to other fingerprint devices to use.

Auto Test: automatically test the function of each module if it is workable, including the screen, sensor, voice, keyboard and clock tests.

Record: For convenient querying of the records saved in the device, the **query record** function is provided.

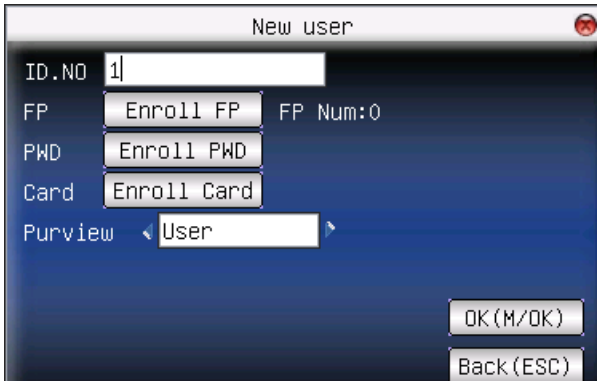
Sys Info: Use **system information** to check the current device's saving status, its version information and so on.

2. User Management

The user's basic information on the device includes fingerprint, password and management access. When employee information changes in the company's attendance management, , the information on the device also needs modification. Therefore, operations including "add, delete, check, modify and so on" can be done on the device.

2.1 Add User

First, enroll the employee's fingerprint or password in the device.
Enter **New User** interface:



Notice: Only some models have name and card options.

ID.NO: Staff's attendance number.

FP (Fingerprint): enroll employee's fingerprint. A maximum of ten fingerprints can be enrolled.
Employees with enrolled fingerprints can use fingerprints to record attendance.

PWD (Enroll password): enroll user's password. 1～8 digits may be used. The employee with an enrolled password can use the password to record attendance.

Card: Registered staff's Card. Only the registered card is permitted to check attendance.

Purview: Users are people whose identity must be authenticated before entering a menu. The ordinary consumer can track attendance by the card or the password only; the manager may check daily attendance with the ordinary consumer access, but may also enter the menu to operate each option.

Notice: When there is no manager appointed, any person may enter all the menu operations; after a manager is appointed, all are unable to enter the menu until the manager status is confirmed.

For example, the following is the flow to **add a user**.

Input User ID

1) Allocate User ID by default.

2) Press "←" to delete the allocated User ID by default. Input User ID from keyboard. If the User ID is wrong, press "←" to input it again.

Input Name★

Use T9 input to input employee's name.

Press OK or ▲/▼ to select "enroll fingerprint", then press OK to start fingerprint.

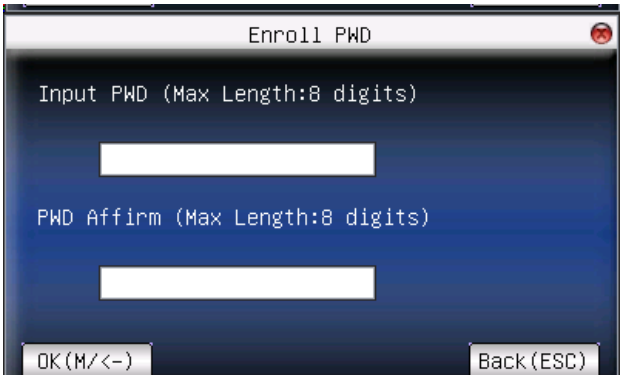
Enroll Fingerprint

Press finger at device prompt. Press the finger three times in the proper way.

If one fingerprint is enrolled successfully, press **OK** to continue another finger, then press **menu** and **ESC** to return to the last interface.

Press ▲/▼ to select "enroll password" and press **OK** to enroll a password.

Enroll Password



Input password (1～8) at device prompt, and press **OK** to verify it. Then press **OK** save it or press **ESC** to

exit without saving it.

After saving, display will be on the device, which means the password has been set.

Enroll Card★

Scroll ▲ / ▼keys to locate the cursor on "enroll card" button, and press "OK" to enter the registration card.

Pass the card near the induction area. After the equipment finds the card number, press OK key to save it, press to quit, then remove the card from the equipment, after the "Enroll successfully" prompt, the card number will display on the register button.

Privilege setting

Scroll the▲/▼ key and local cursor on the "Privilege" option box, scroll ◀/▶ key to choose privilege.

Save/Exit User Registration

To confirm the registration information is correct, after getting confirmation, save it.

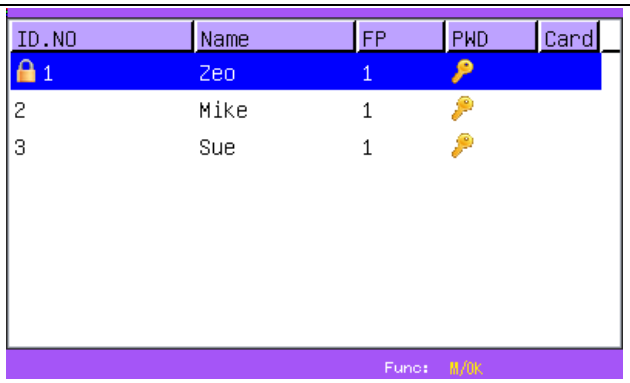
Saving:

1) Scroll ▲/▼key to locate the cursor on the "completes (M/↵)"button, press "OK" key again. The prompt "the data has been changed, Are you sure you want to save it?" appears on the equipment. Press the "OK" key to save it. If you do not want to save it, press "ESC" to exit. If the prompt "Save successfully! Continue to input?" appears on the equipment, and you want to continue, press "OK", if you want to abandon this operation, press the "ESC" key.

2) Press the ESC key or scroll ▲/▼key to locate the cursor on the "return (ESC)" button and press the "OK" key. The prompt "the data has been changed, Are you sure you want to save it?" appears on the equipment. Press the "OK" key to save it and return to the preceding menu. If you are not returned to the preceding menu, press the "ESC" key.

2.2 Manage User

All user's information saved in the current device can be queried in **Manage User,** including user name, fingerprint count, whether to enroll password or card, user attendance record and so on. Editing or deleting a user can also be done here.



Notice:1) means this employee is the administrator. means a password has been enrolled. means an ID Card has been enrolled.

2) The picture may be different on your device. The actual product prevails.

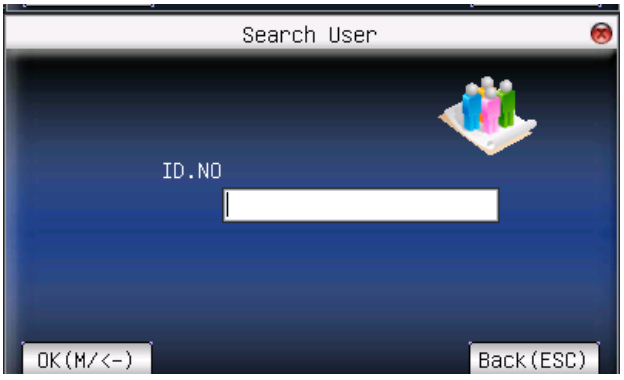
Press **menu** on the above interface, and the operating menu will pop up:

Press ▲/▼ to select the item.

2.2.1 Search User

If many users are enrolled, in order to find an employee quickly, the device has provided “User ID” to search the employee.

Press **menu** on **manage user** interface to get the operating menu. Select “Search User” or press any numeric key to enter the following page:

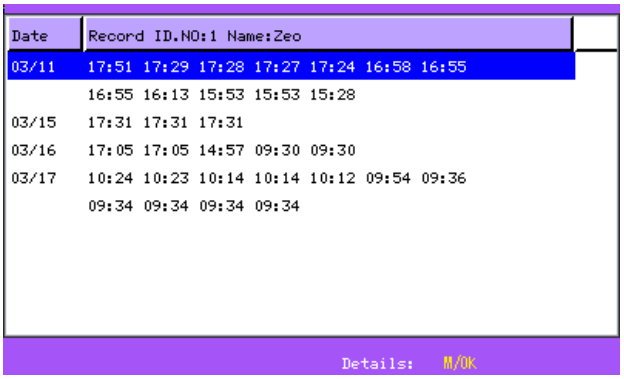


Input User ID of an employee to be queried. Press **OK.** After a successful query, the blue cursor will point to the employee. If there is no such employee, “no enrolled data” will appear.

2.2.2 Query Attendance Record

When an administrator is checking an employee’s fingerprint and other enrolled information, he can also check the employee’s attendance record during that month.

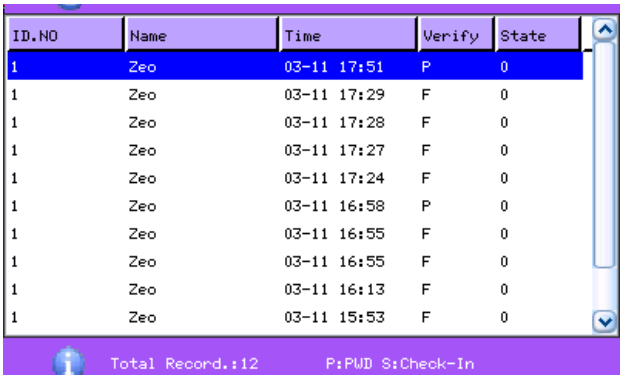
Press **menu** on **manage user** interface to get the operating menu, select “Record” and the employee’s monthly attendance record can be checked:



Notice: The picture may be different on your device. The actual product prevails.

Press ▲/▼ to read the attendance record.

Press **OK**/**menu** to query detailed information.

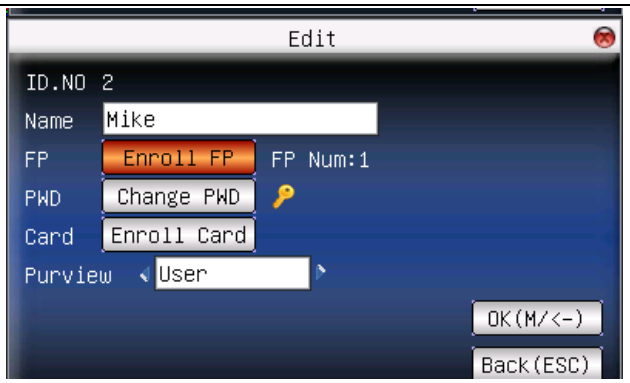


Then press “**ESC**” to return to the **manage user** interface.

2.2.3 Edit User

Edit user information saved in the device. For example, if the former enrolled fingerprints are unusable, enter “Edit User” to re-enroll fingerprint, password or card.

Use ▲/▼ or **query user** on **manage user** interface to select an employee to be edited. Then press **menu** to select “Edit” or press **shortcut** to verify it. All enrolled information can be displayed on the device:



Notice: Only some models have Name and Card options.

User ID cannot be modified. The operation is similar to that of **add user**. Fingerprint can be re-enrolled. Click “enroll password” directly to set password or modify password. The access can also be modified.

Save Edit/Exit Edit

Press **menu** or ▲/▼ to select “**complete**(M/↵)”, press **OK** to save and return to **manage user** interface.
Press “**ESC**” or ▲/▼ to select “**Return**（**ESC**)” and then press **OK** and the device will prompt “data has been changed. Are you sure to save?”. If you want to save it, press **OK** and return to the last menu or press “**ESC**” to return to the last menu.

2.2.4 Delete User

“Del User” is to delete an employee’s partial information or all information from the device. It is used when the following happens:
1) When an employee’s fingerprint or password is not needed any more.
2) When an employee leaves the position.
Press ▲/▼ on **manage user** interface or use **query user** to select the employee to be edited. Click **menu** to get the operating menu, and select “Delete User”.
Delete User

Notice: Only some models have Del ID Card Only options.

If the user has no fingerprint or password, the corresponding item is blue and cannot be operated. Press ▲/▼ to select the item to be operated. Press **OK** to pop out a dialog box and verify whether to delete this item or not. Then the device will give corresponding prompt. Press "**ESC**" to return to the **manage user** page.

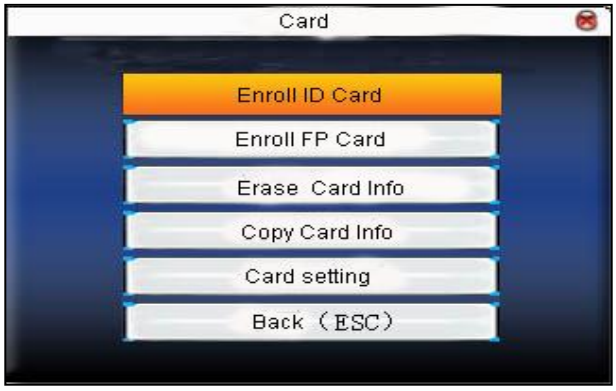
2.2.5 Add User

In order to add a user conveniently for operator, **Add User** is configured here. The function is the same as that of 2.1 add user.

2.3 Card Management★

Support Mifare non-touch intelligent card with working frequency of 13.56MHZ. Integrate fingerprint attendance to other systems and support multi-verification mode to meet the demands of different people.

Operation:



Press ▲/▼ to select your desired item, press **OK** to execute the current selected item.

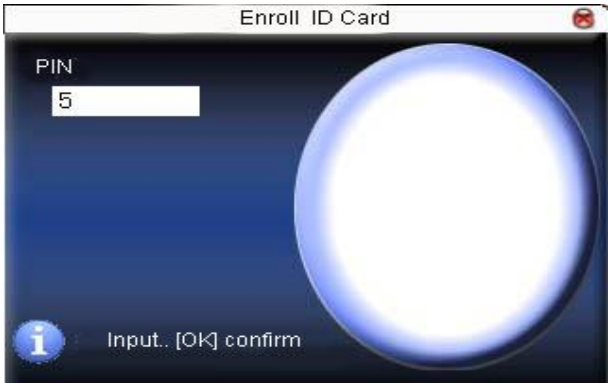
2.3.1 Enroll Card

Regard Mifare card as an ID card use, just register the card number. There is no need to enroll the fingerprint.

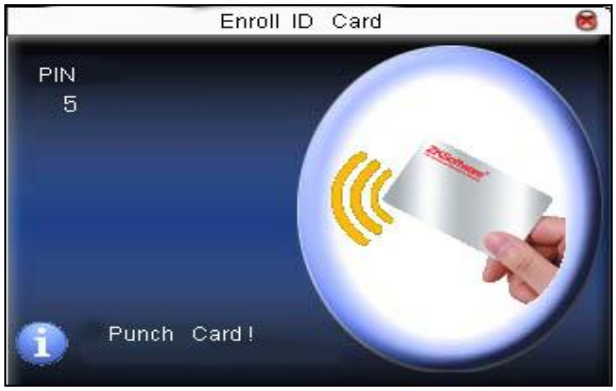
Operation:

1. Enrollment

Step 1: Select **Enroll Card** and then press **OK.**



Step 2: press keyboard to input the number to be enrolled（if the number is there already, the device will prompt you to copy the information to the card.), and then press **OK**.



Step 3: The device prompts the user to show the card.

Step 4: Put the card in the induction area until the operation is successful.

2. Verification:

Wave the card in the induction area. After the device reads the card, move the card off. When the verification is successful, the device will give prompt.

Tips: Please enter user **access control option** to modify the verification mode as RF, or verification will not be successful.

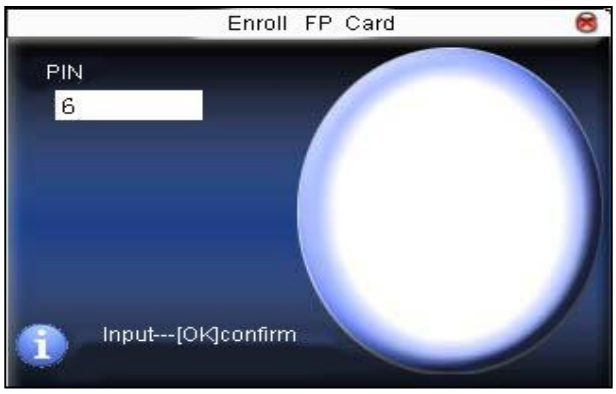
2.3.2 Enroll Fingerprint Card

Enroll fingerprint and write fingerprint onto card.

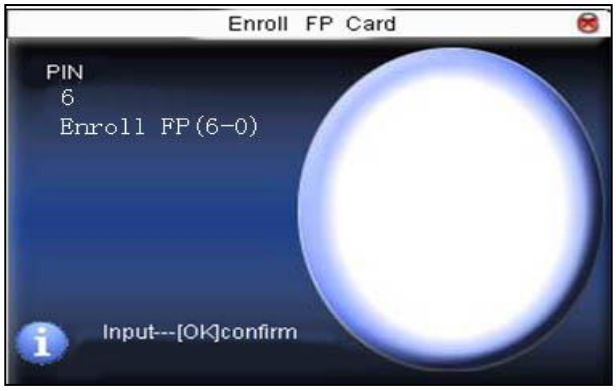
Operation:

1. Enrollment

Step 1: Select **Enroll Fingerprint Card** and press **OK**.

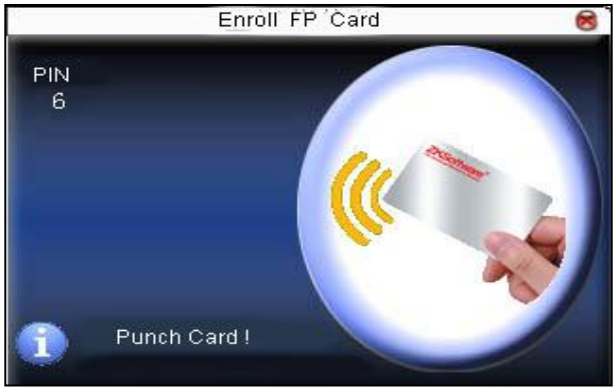


Step 2:Use keyboard to input the number to be enrolled（if the number is there already, the device will prompt you to copy the information to the card.), and then press **OK**. The device will prompt you to move off your finger.



Step 3: Press finger properly three times.

Step 4: Device prompts “please show card”.



Step 5: Put the card in the induction area, waiting for the device to read the fingerprint data into the card until the enrollment succeeds.

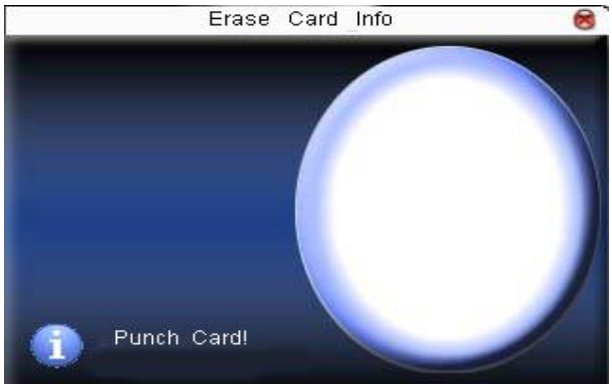
2. Verification:

Wave the card in the induction area. After the device reads the card, move the card off. When the verification is successful, the device will give prompt. If the pressed fingerprint is different from that stored in the card,

the verification will fail.

2.3.3 Clear Card Information

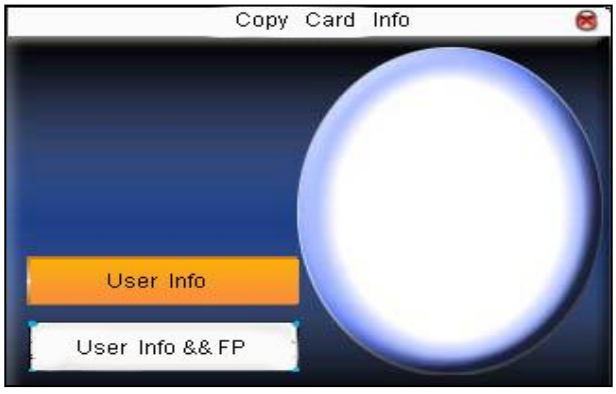
Delete all the information on the card currently being operated.
Operation:



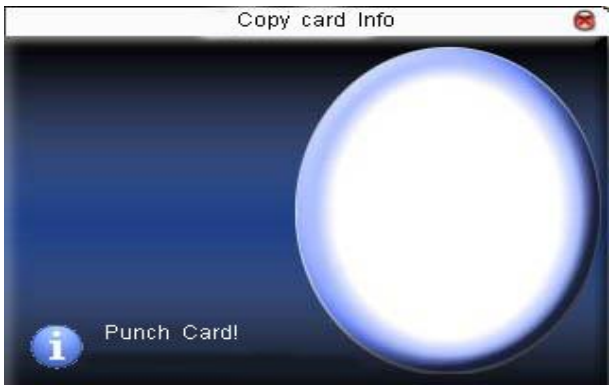
Put the card in the induction area, wait for device to delete all the information on the card. If the card data has been stored in the device, the device will remind you whether to delete the information in the device or not. “Yes” is to delete the user’s fingerprint and information in the device. “No” is to keep the information.

2.3.4 Copy Card Information

Copy Card Information to the device（after copy, the fingerprint is still in the card), then press **Fingerprint Attendance** directly on the device. There is no need to use a Mifare card.
Operation:

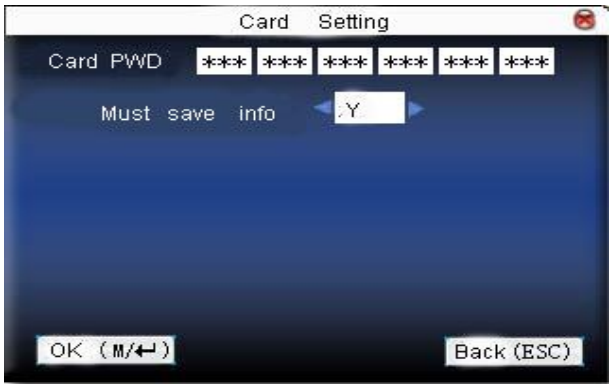


Press ▲/▼ to select “only copy user information” or “copy user information and fingerprint”, and then press **OK.**



2.3.5 Set Card Parameter Value

Set password of Mifare card and decide whether the information should be saved or not.
Fingerprint Card Password: After the password is set, the device will write the password into the enrolled fingerprint card. Then the fingerprint card can only be used on this device.
Save the information: Decide whether to save the enrolled information to the device when enrolling card or fingerprint card. “No” means the information is only saved in the card. “Yes” means the information is saved in both card and device.
Operation:

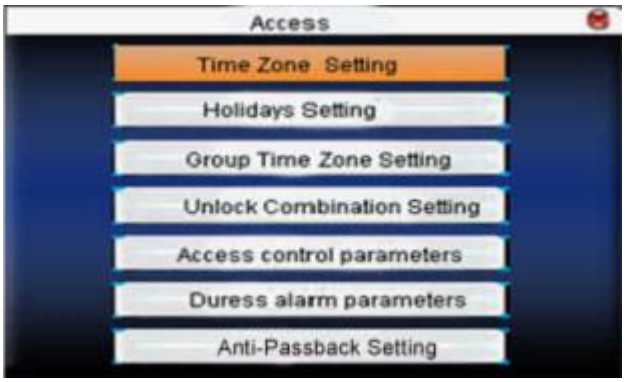


Press ▲/▼to move cursor to the item to be set. If it is the input box, press numeric keys on small keyboard to input the value. If it is the roll box, press ◄/► to switch the values. After setting, press **menu** directly to return to the last interface. Press “**ESC**” to cancel setting and return to the last interface.

☺**Notice**: Card induction area is 3cm—5cm above the fingerprint reader.

2.4 Access Control Option★

Access control option is to set user's open door time zone, control lock and related device's parameters.
If the device supports an external facial instrument, it cannot support the camera and advanced access control at the same time.
To unlock, the enrolled user must meet the following conditions:
1. The current unlock time should be in the effective time of user time zone or group zone.
2. The group where user is must be in access control (or in the same access control with other group, to open the door together).
The system defaults the new enrolled user as the first group, default group time zone as 1, access control as the first group, and the new enrolled user is in unlock (if user has modified the related setting of access control, the system will be changed with user's modification) .
Operation:
Press **Menu** -> **User Management** -> **Access Setting** （as shown below)



Press ▲/▼ to select your desired item, press **OK** to execute the current selected item.

2.4.1 Time Zone Setting

Time zone is the minimum unit of access control option. The whole system can define 50 time zones. Every time zone defines seven time sections (namely, a week). Every time section is the effective time zone within 24 hours every day. Every user can set 3 time zones, "or" exists among the three zones. It is effective if only one is satisfied. Every time section format is **HH:MM-HH:MM**, namely, accurate to the minute.
If the end time is smaller than the start time （23:57- 23:56), the whole day is prohibited. If end time is bigger than start time（00:00- 23:59), it is effective section.
Effective time zone for user unlocking: 00:00-23:59 or the time zone when end time is bigger than start time.

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

Operation:
Press **Menu** -> **User Management** -> **Access Setting** -> **Time Zone Setting**（shown as below)

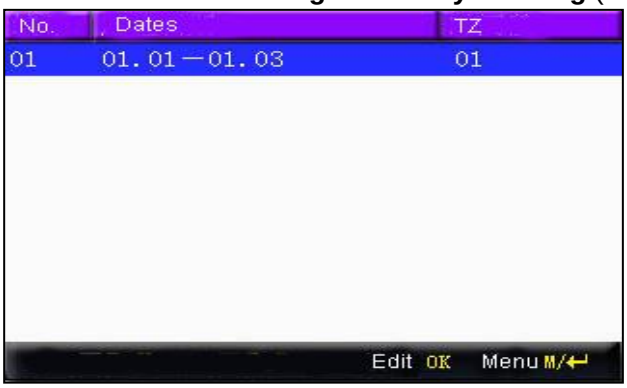
Input the time zone number. If the enrolled time zone has a number already, then the time zone setting will be displayed automatically. Press ▲/▼, ◄/► to move the cursor to the input box, press the numeric keys on the small keyboard to input value. Then press **Menu** to save it and press **ESC** to exit.

2.4.2 Holidays Setting

Special access control times may need during holidays. It is difficult to modify everybody's access control time. So a holiday access control time (as access control exceptions) can be set, which is applicable for all employees.

Operation:

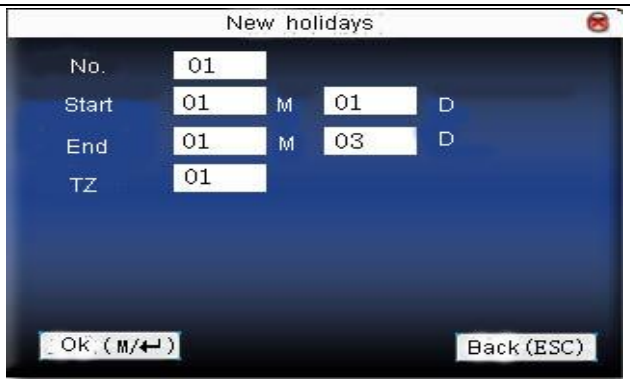
Press **Menu** -> **User Management** -> **Access Setting** -> **Holidays Setting** (as shown below).



Add holidays

Press **Menu** to get operation menu

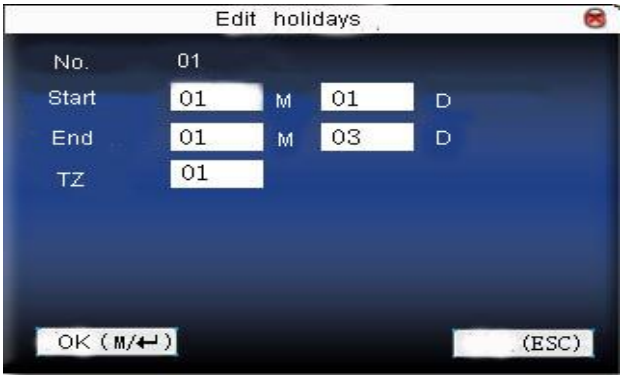
Press ▲/▼ to select **add.**



Press ▲/▼ to move cursor to the input box. Press the numeric keys on the small keyboard to input the value. After setting, press **Menu** to save it. Then press **ESC** to exit.

Edit holidays

Select the line to be edited. Press **OK** directly or press **Menu** to select **Edit** in the operating menu.



Press ▲/▼ to move cursor to the input box. Press the numeric keys on the small keyboard to input the value. After setting, press **Menu** to save it. Then press **ESC** to exit.

Delete holidays

Select the line to be deleted. Press **Menu** to select **Delete** in the operating menu.

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

2.4.3 Group Time Zone Setting

Grouping is to manage employees in groups. Employees in groups use the group time zone by default. Group members can also set user time zones. Every group can hold three time zones. The new enrolled user belongs to Group 1 by default. He can also be allocated to other groups.

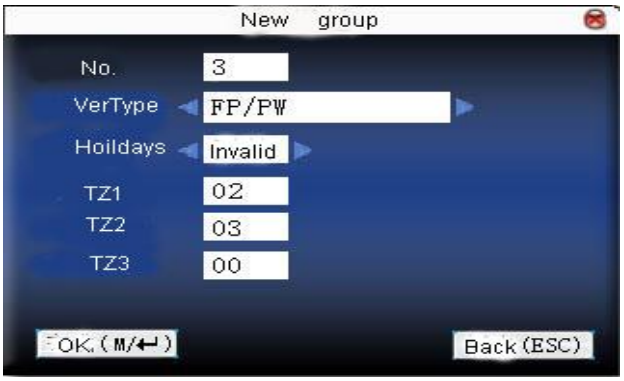
Operation:

Press **Menu** -> **User management** -> **Access setting** -> **Group Time Zone Setting**:

1. Add group time zone

Press **Menu** to get the operating menu.

Press ▲/▼ to select **add**. For example, to add a group whose time zone is 2 and 3, as shown below:



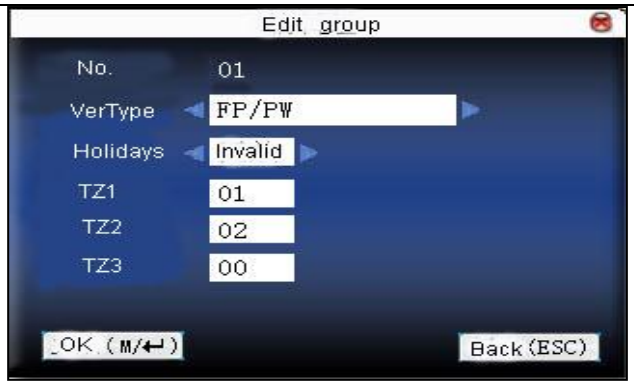
☺**Notice**: 1) If holiday is effective, only when there is intersection between group zone and holiday time zone, can the group member open the door.

2) If holiday is ineffective, the access control time of group member won't be affected by holiday.

Press ▲/▼to move cursor to the item to be set. If it is the input box, press numeric keys on small keyboard to input the value. If it is the roll box, press ◄/► to switch the values. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel setting and return to the last interface.

2. Edit Group time zone

In the Access Group setting interface, select the line to be edited. Press **OK** directly or press **Menu** to select **Edit** in the operating menu.



Press ▲/▼to move cursor to the item to be set. If it is the input box, press the numeric keys on the small keyboard to input the value. If it is the roll box, press ◄/► to switch the values. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

3. Delete group time zone

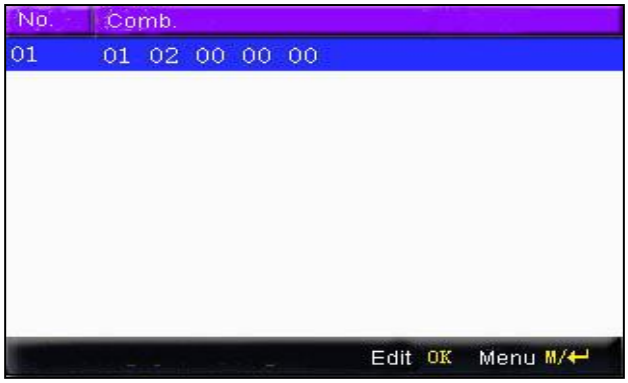
In the Access Group setting interface, select the line to be deleted. Press **Menu** to select **Delete** in the operating menu.

2.4.4 Set Unlock Combination

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.

Operation:

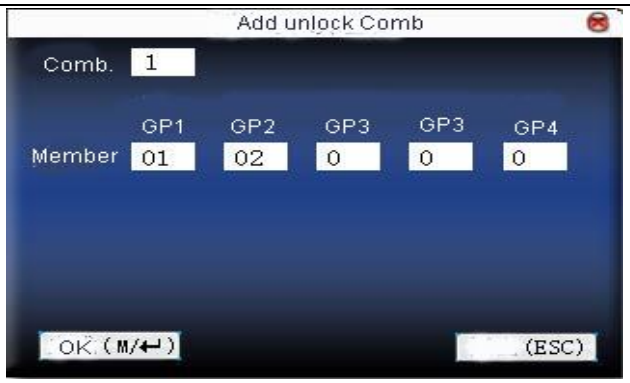
Press **Menu** -> **User Management** -> **Access Setting** -> **Unlock Combination setting**:



1. Add unlock combination

Press **Menu** to get the operating menu:

Press ▲/▼ to select **add.** For example, to add an unlocking combination, this needs the verification of both groups 1 and 2, as shown below:



Press ▲/▼ to move cursor to the input box. Press the numeric keys on the small keyboard to input value. After setting, press **Menu** to save it. Then press **ESC** to exit.

2. Edit unlock combination

Select the line to be edited. Press **OK** directly or press **Menu** to select **Edit** in the operating menu.

Press ▲/▼ to move cursor to the input box. Press the numeric keys on the small keyboard to input value. After setting, press **Menu** to save it. Then press **ESC** to exit.

3. Delete unlock combination

Select the line to be deleted. Press **Menu** to select **Delete** in the operating menu.

2.4.5 Access Control Parameters

Set device control locks and related device parameters.

Lock driver time length: Device control electronic lock is in enabling time.（effective value 1～10 seconds)

Door Sensor Delay: After the door is open, delay the time to check door sensor. If door sensor state is different from the normal state of door sensor mode, alarm will be go off. This time is called door sensor delay. （effective value: 1～99 seconds)

Door Sensor Mode: It includes NONE, NC and NO. NONE means there is no door sensor. NO means the door is normally open. NC means the door is normally closed.

Door Sensor Alarm: When abnormal door sensor state is detected, alarm will be go off after some time. This time is door sensor alarm. （effective value: 1～99 seconds)

Alarm Count: When the failed press times reach the set times, alarm signal will go out.（effective value 1～9 times)

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

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

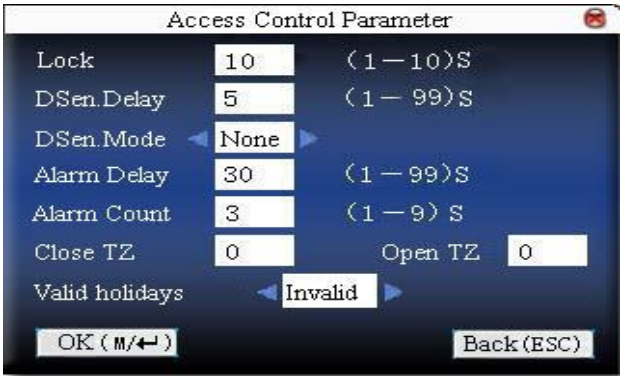
Whether Holiday is Effective: Define time zone for NO or NC. Whether the time zone set in time zone is effective.

☺ **Notice**: 1) when time zone is set for NO or NC, set door sensor mode as **"None"**, or alarm signal may go out during time zone of NO or NC.

2) If time zone of NO or NC has no definition, the device will prompt it and add the definition in time zone setting.

Operation:

Press **Menu** -> **User Management** -> **Access Setting** -> **Access Control Parameters**:



Press ▲/▼to move cursor to the item to be set. If it is the input box, press the numeric keys on the small keyboard to input the value. If it is the roll box, press ◄/► to switch the values. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

2.4.6 Duress Alarm Parameters

There is a duress alarm parameter setting in the device. When employees come under duress, select duress alarm mode, the device will open the door as usual. But the alarm signal will be sent to the alarm.

Help Key: If "Yes", press **help** then press fingerprint in the following 3 seconds or press ID number, and the duress alarm will go out after successful identification. If "No", it is useless to press **help.** （**help** can be set in keyboard definition.)

1:1 Trig: if "Yes", when user uses 1:1 match mode, alarm signal will go out or there is no alarm signal.

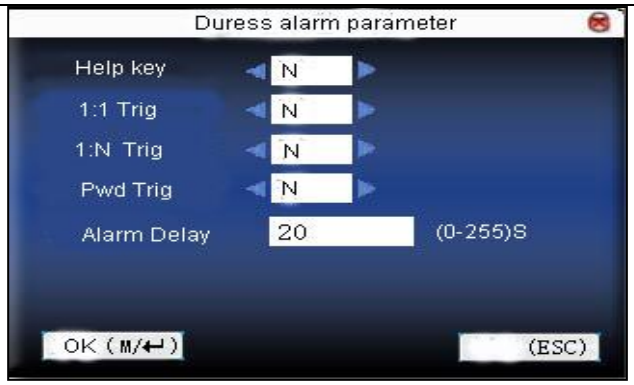
1: N Trig: if "Yes", when user uses 1: N match mode, alarm signal will go out or there is no alarm signal.

Pwd Trig: If "Yes", when user uses password verification mode, alarm signal will go out or there is no alarm signal.

Alarm Delay: After duress alarm gets started, the alarm signal is not output directly. But it can be defined. After some time, alarm signal will be generated automatically.（0-255 seconds).

Operation:

Press **Menu** -> **User Management** -> **Access Setting** -> **Duress alarm parameters** (as shown below).



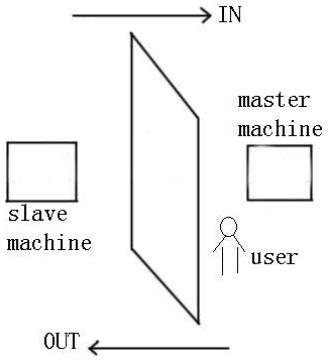
Press ▲/▼to move cursor to the item to be set. If it is the input box, press the numeric keys on the small keyboard to input the value. If it is the roll box, press ◄/► to switch the values. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

2.4.7 Anti-Passback Setting★

【overview】

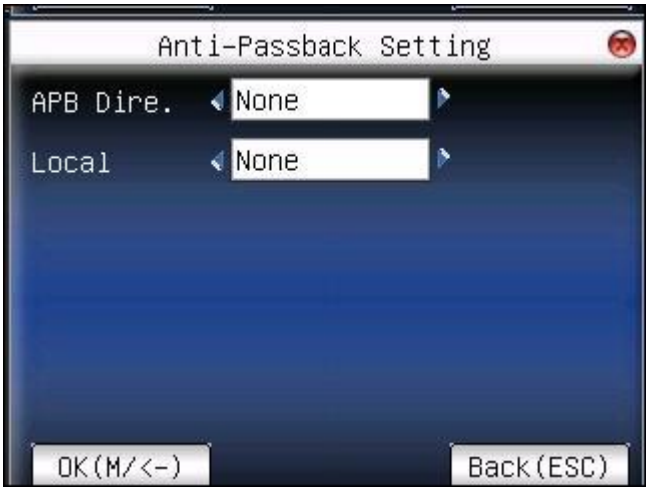
Sometimes, some illegal person follows the employee into the gate, which will bring a security problem. To prevent such risk, this function is enabled. In record must match out record, or the gate won't be open.

This function needs two machines to work together. One is installed inside the door (master machine), the other is installed outside the door (slave machine). Same Wigand signal communication is adopted between the two machines. Same user and user ID number enrolled.



Operation:

Press **Menu** -> **User Management** -> **Access Setting** -> **Anti-Passback setting** (as shown below).



Choose the Machine model: Press ▲/▼ to switch the input box. Press ◄/► to modify the setting. Select Anti-Out, referring to out anti-pass back, only if the user's last record is in-record, can the door be opened. Otherwise it will trigger the alarm signal as illegal access. Select "**None"**, referring to no anti-pass back, and no alarm will be triggered. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

Anti-Passback Function:

The master machine control OUT and the slave machine control IN.

- In anti-passback (APB-In):

Only if the user's last record is out-record, can the door be opened. Otherwise it will trigger the alarm signal as illegal access.

Enter: New user's first time access will pass.

In anti-passback mode not restrict of OUT.

- Out anti-passback (APB-Out):

Only if the user's last record is in-record, can the door be opened. Otherwise it will trigger the alarm signal as illegal access.

Out: New user's first time access will pass.

In anti-passback mode not restrict of IN.

- In-Out anti-passback (APB-Out/In):

New user's first time access will pass. Only user's last record is out-record, can the door be open when he/she wants IN. Otherwise it will trigger the alarm signal as illegal access. Only user's last record is in-record, can the door be open when he/she wants out. Otherwise it will trigger the alarm signal as illegal access.

- None anti-passback:

Slave machine can verify to open the door, and the prompt "no enrolled data" on the master machine.

Anti-passback function is available.

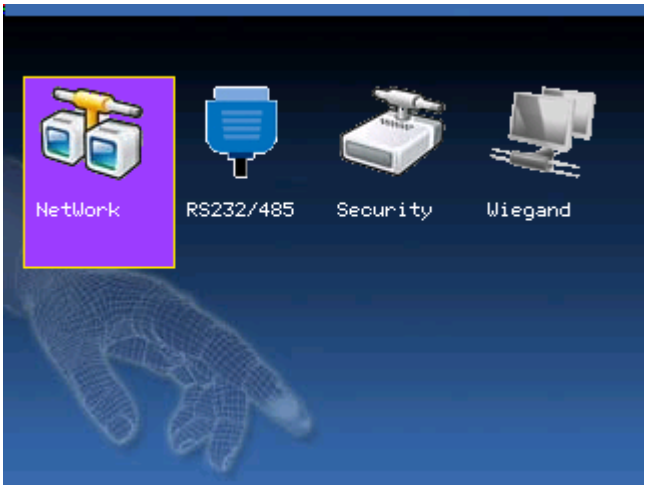
Machine status:

Press ◄/► to move cursor to the item to be set. If you select “Control Out”, the master control is out, the other machine control is entry. Need two machines to cooperate.

3. Communication Option

When the device and PC are used to transmit data, it is necessary to use a communication wire to set communication parameters in the device. When the device is in communication, “communicating…” appears. Do not operate the device then.

☺**Notice**: When the device is communicating with a computer, please check the setting here. The parameters here must be in accordance with that of the software communication interface.



3.1 Network Option

When Ethernet is used for the communication of the device and PC, the following settings need to be checked:

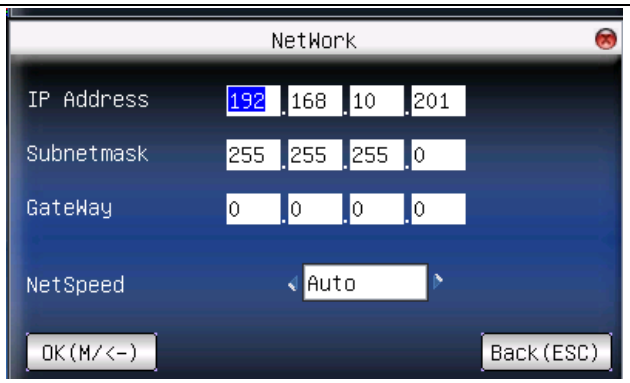
Device IP Address: IP is 192.168.1.201 by default. You can modify it if necessary. But it cannot be the same as that of the PC.

Subnet mask: It is 255.255.255.0 by default. You can modify it if necessary.

Gateway address: It is 0.0.0.0 by default. If the device and PC are in different net segments, it is necessary to set the address.

Net speed: Set the speed according to the LAN where the device is.

Operation:



Press ▲/▼to move cursor to the item to be set. If it is the input box, press the numeric keys on the small keyboard to input the value. If it is the roll box, press ◄/► to switch the values. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

3.2 Serial Port Option★

When serial port (RS232/RS485) is used for communication of the device and PC, the following settings need to be checked:

Baud rate: Used for communication with the PC. There are five options: 9600, 19200, 38400, 57600 and 115200. If the communication speed is high, RS232 is recommended. If the communication speed is low, RS 485 is recommended.

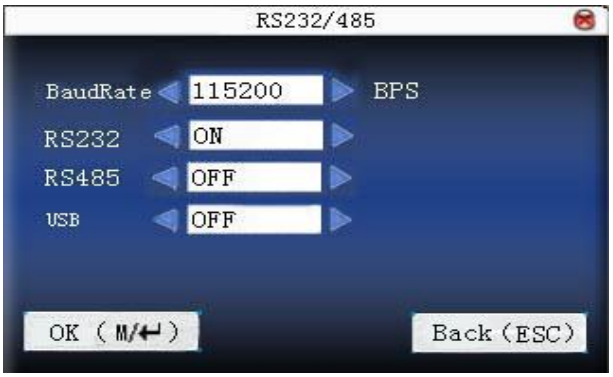
RS232: Whether use RS232 to communicate. Select "ON" if RS232 is to be used.

RS485: Whether use RS485 to communicate. Select "ON" if RS485 is to be used.

USB: Whether use USB to communicate. Select "ON" if USB is to be used.

RS232, RS485 and USB cannot be used at the same time.

Operation:



Press ▲/▼to move cursor to the item to be set. Press ◄/► to switch the values. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

☺ **Notice**: 1) Only some models have RS232/RS485/USB communications.

2) The picture may be different from your device. The actual product prevails.

3.3 Security

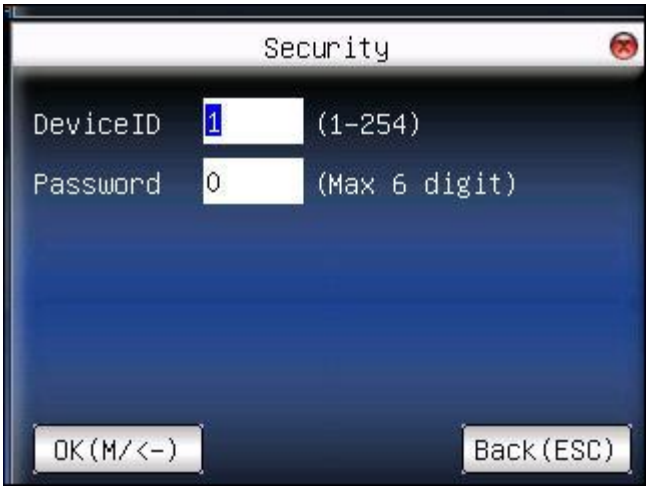
When RS232/RS485 is used for communication of the device and PC, it is necessary to set the device ID.

Device ID: 1—254. If RS232/RS485 is used, this ID needs to be input on the software communication interface.

To improve the security of attendance data, a connection password needs to be set here. The connection password must be input when PC software is to connect to the device to read data.

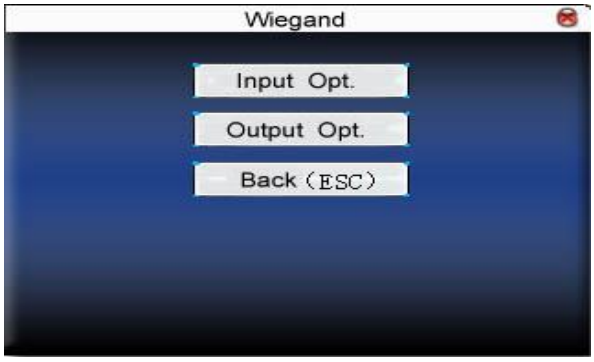
Connection Password: System password is **0** by default.（namely, there is no password.) it can be set as other value. After setting, the password must be input if software is to communicate with the device or the connection will fail. The password length is 1～6 digits.

Operation:



3.4 Wiegand Option★

Define Wiegand input & output format.



3.4.1 Input Configuration

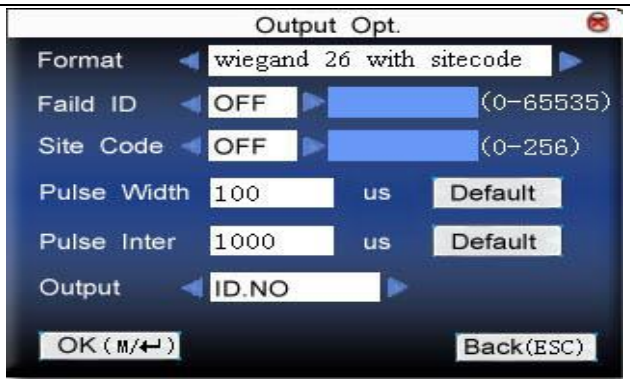
User defined format: User defined Wiegand input format

Bit digit: Wiegand data digit length
Pulse width: Pulse width is 100 microseconds by default, which can be adjusted from 20 to 800.
Pulse interval: It is 900 microseconds by default, which can adjusted between 200 and 20000.
Input content: Content contained in Wiegand input signal, including User ID or card number.
Operation:

Input the name of the user-defined format. Press ▲/▼to move cursor to the item to be set. If it is the input box, press the numeric keys on the small keyboard to input the value. If it is the roll box, press ◀/▶ to switch the values. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

3.4.2 Output Configuration

Format: It is the defined format in the system. User need not specify total digit and the information position. There are 4 definition formats by default in the system: Wiegand 26 with site code. Wiegand26 with site code means W26 format output with device ID. If there is no site code, then the signal not to be output does not contain the information. If there is site code, the output is the set site code（similar to device ID but this code is specified by the user and different devices can be repeated, with range of 0-255.) .
Failed ID: It is the failed ID after unsuccessful verification. "Close" means not to output it. (With range of 0-65534)
Site code: Similar to device ID but the code is specified by user. Different devices can be repeated. (With range of 0-255)
Pulse width: Pulse width is 100 microseconds by default, which can be adjusted from 20 to 800.
Pulse interval: It is 900 microseconds by default, which can adjusted between 200 and 20000.
Output content: Content contained in Wiegand output signal, choose User ID or card number.
Operation:



Input the name of the user-defined format. Press ▲/▼to move cursor to the item to be set. If it is the input box, press the numeric keys on the small keyboard to input the value. If it is the roll box, press ◄/► to switch the values. For example, to modify failed ID as 10, first press◄/► to select "Yes", then enter 10 in the input box. After setting, press **Menu** directly to return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

4. System Option

Set system parameters to meet as many user demands as possible.

4.1 System Parameters

1: 1 matching threshold value: The similarity of ID + fingerprint verification and the enrolled template

1: N matching threshold value: The similarity of verification and the enrolled template

Recommended matching threshold value:

FRR	FAR	Matching threshold value	
		1:N	1:1
high	low	45	25
middle	middle		35
15			
low	high	25	10

Time format: Time format displayed on initial interface. Press ◄/► to set 24H or 12H.

Date format: Press ◄/► to select format. The fingerprint sensor supports ten date format: YY-MM-DD, YY/MM/DD, YY.MM.DD, MM-DD-YY, MM/DD/YY, MM.DD.YY, DD-MM-YY, DD/MM/YY, DD.MM.YY and YYYYMMDD. Select your desired date format. Press ◄/► to set 24H or 12H.

Keyboard voice: Press ◄/► to set whether the key has voice or not. “Yes” means having voice, and “No” means no voice.

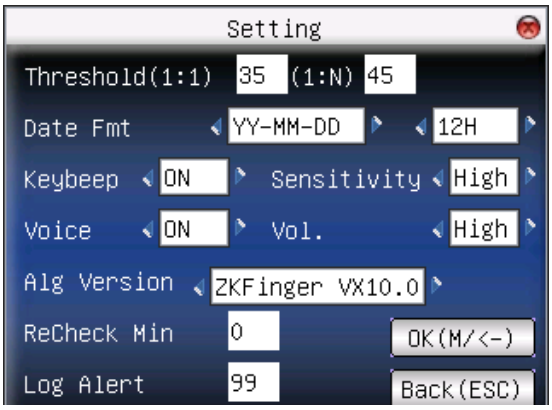
Voice prompt: Press ◄/► to select whether to give voice prompt or not. The device will give corresponding voice prompts during Operation.

Volume: Press ◄/► to set it.

Attendance record alarm: when the free space reaches the set value, the device will give an alarm automatically (effective value is 0～99,0 means the space is all used and there is no alarm.)

Repeat verification time: it is in the set time range（unit: Minute). If somebody's attendance record has been there, then the record of second attendance won't be saved. (effective value is 0～60 minutes. 0 means all the records after verification are saved.)

Operation:



Press ▲/▼ to move cursor to the input box. Press the numeric keys on the small keyboard to input the value. If it is the roll box, press ◄/► to switch the values. After setting, press **OK** or **menu** directly to save the setting and return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

4.2 Data Management

Delete Attendance Record: Delete all attendance records.

Delete All Data: Delete all enrolled employees' information, fingerprints and attendance records.

Clear Management Access: Change all administrators into common users.

Operation: Press **System Menu→ Data Mng (as below :)**

Press ▲/▼ to move cursor to the selected button. Press **OK** or **menu** to start operation. The device will remind you whether to continue the current operation or not. Then press **OK** or **menu** to delete all the data, which won't be recovered after deletion. Press "**ESC**" to return to the last interface.

Clear propaganda picture: Clear the propaganda pictures uploaded to the device from U disk.（refer to Upload User Defined Picture in 6.2 Upload data for how to upload the propaganda pictures.)

Operation:

Press "▲/▼" to preview the propaganda pictures in the device. Click **OK** to delete all these pictures. After deletion, the next picture will appear. Click **"delete all"** to delete all the propaganda pictures in the device. Then press "**ESC**" to return to **data management** interface.

4.3 Upgrade Firmware

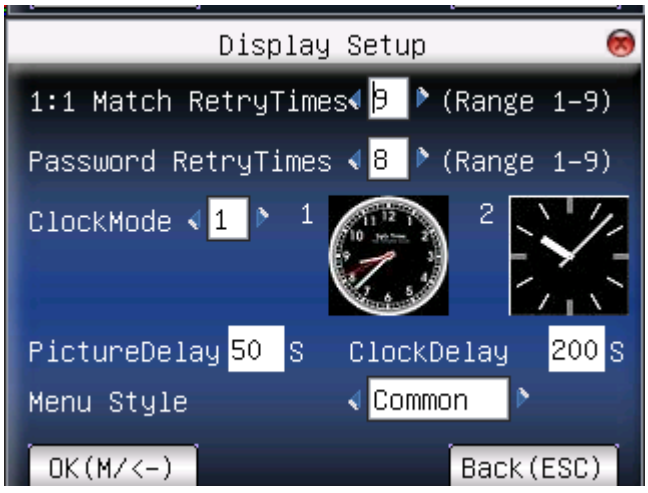
Update the firmware by utilizing the USB Pen Drive (flash drive)

☺**Notice**: If you need such upgrade file, please contact a technician. Usually, firmware upgrade is not recommended.

Operation:

Insert U disk with upgrade file into the slot. The device will identify the file automatically. The device will prompt whether it is successful or not.

4.4 Display Setting



Press ▲/▼ or ◄/► to move cursor to the input box. Press the numeric keys on the small keyboard to input the number. After setting, press **menu** directly to save the setting and return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

4.4.1 Verification

When a user is using 1:1 match or password verification, he may forget to enroll his fingerprint or does not press the finger in the proper way. For user's convenience and to reduce repeat key, the device allows retry.

4.4.2 Time Display

There are two clock modes for Select. After verification, the selected clock mode will be displayed on the screen.

4.4.3 Picture Cycle Interval

Picture cycle interval means how soon the picture will be changed（effective value is 3～999 seconds.)
Display propaganda picture: User can display some propaganda pictures on the screen. The operation refers to this manual 10.4 Propaganda picture upload rules

4.4.4 Clock Display Delay

Time display delay means the clock picture display time length after verification. After the display delay, the propaganda picture will be displayed on initial interface again (with effective value of 0～999 seconds, and 0 means displaying clock all along).

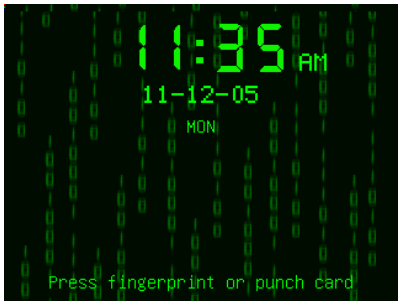
4.4.5 Interface Style

User can set initialize interface's style. Press **menu → System → Display→ Initialize style.**
There are three modes: common, matrix (default), and magic. If the interface change is successful, the machine displays: "Standby Interface modified success". Then you should restart the device.

☺**Notice**:

"4.4.3 Picture cycle interval" and "4.4.4 Clock display delay" functions are fit use common mode of interface style only. When you select matrix or magic mode, these functions are invalid. Display screen show the

Common-Style



Matrix-Style

Magic-Style

4.5 Reset

Make device's communication option, system option and so on reset to the factory settings.

Factory reset: Make all the parameters in the device reset to the factory settings.

Reset keyboard definition: Reset the corresponding setting of keyboard definition to the factory settings.

Reset bell option: Only reset bell option to the factory settings.

Reset other parameters: only reset communication option, system parameter and interface option and so on to the factory settings.

Press ▲/▼ to move cursor to the button to be operated. Press **OK** to start operation. The device will say "Are you sure you want to execute the current operation?" Press **OK** to reset it to factory state and press "**ESC**" to cancel operation.

☺**Notice**: The employee's information and attendance data will not be deleted when this operation is being done.

4.6 Other Options

Set sleep time, external bell and other parameters for the device.

Scheduled sleep: When it is the scheduled sleep time, the device is not in operation and will enter sleep status. Press any key or finger to awake it.

External bell: whether to enable external bell (it is the bell ring given from an external electronic bell connected to the internal of the device, instead of the device speaker.

Fingerprint image display: Select whether to display the fingerprint image on the screen when it is enrolling or verifying there are 4 options: display upon both enrollment and verification, only display upon enrollment, only display upon verification, not display upon enrollment and verification.

Lock power-off: To prevent hostile power-off. Select whether to lock power-off or not.

"Disable": the power is off 3 seconds after pressing **power-off.**

"Enable": it is ineffective after pressing **power-off.**

Language: To choose the display language.

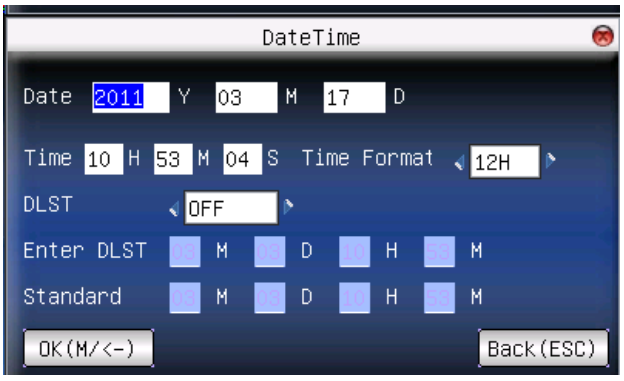
Master Slave: Select whether to establish a master slave connection or not.

Push: Select whether to use the PUSH function or not.

5. Date Time

5.1 Date Time Option

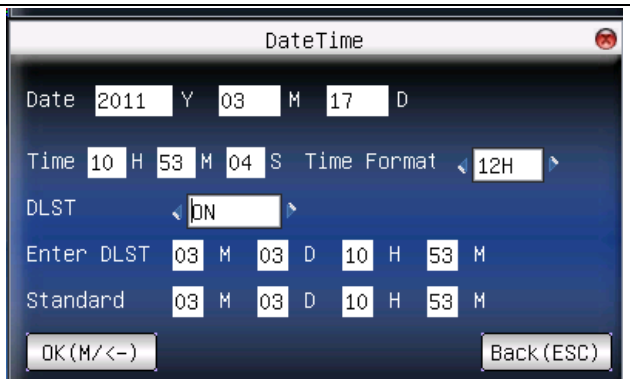
Accurate attendance time is based on accurate time date.
Enter **time date** to set options:
Operation:



Press ▲/▼ to move cursor to the input box. Press the numeric keys on the small keyboard to input the value. After setting, press **menu** directly to save the setting and return to the last interface. Press "**ESC**" to cancel the setting and return to the last interface.

5.2 DLST★

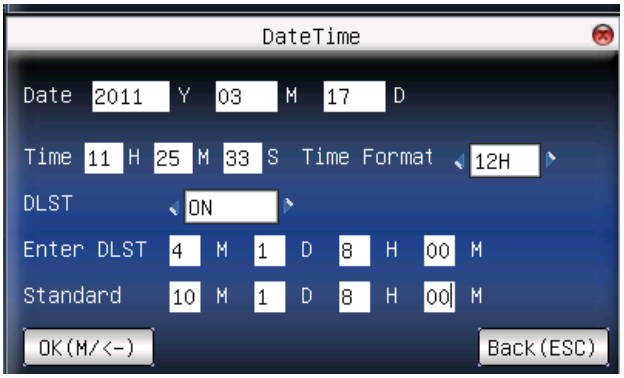
DLST, also called Daylight Saving Time, is a system to prescribe local time in order to save energy. The unified time adopted during the system date is called "DLST". Usually, the time will be one hour forward in summer. It helps people go to sleep earlier and wake up earlier. It can also reduce lighting to save power. In autumn, the time will be recovered. The regulations are different in different countries. At present, nearly 110 countries adopt DLST.
To meet the demand of DLST, a special option can be customized on our RF Card Time & Attendance recorder. Set the time one hour forward at XX (minute) XX (hour) XX (day) XX (month), and set the time backward to the standard time at XX (minute) XX (hour) XX (day) XX (month) if necessary.
Operation:



1) Set DLST as “ON”.

2) Input DLST start time and end time.

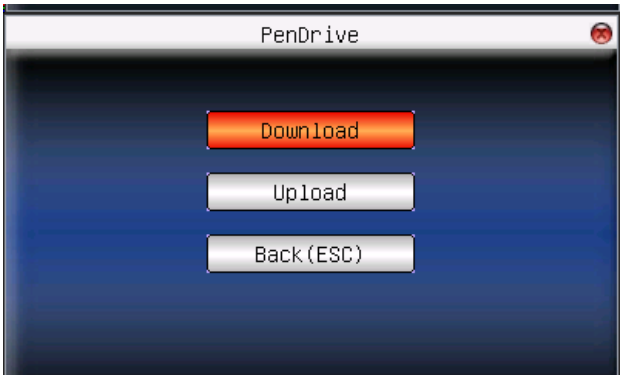
For example, if 08:00, April 1st is set, the device enters DLST, and the time will be set one hour forward. If it is 08:00, August 1st, the device will reset to normal time.



3) Press M/↵/“OK” to save the setting. Press “**ESC**” to exit without saving.

6. PenDrive Management

Import user information, fingerprint template, attendance data and so on in the device to attendance software or export user information and fingerprints to other devices through U disk.



6.1 Download Data

1. Download Attendance Data

Save all attendance data in the device to a U disk.

Operation:

1) Insert a U disk into USB slot of the device through the mini USB.

2) Press "▲/▼" to Download Record.

Press OK for verification. "Downloading data, please wait…" will appear on the display when the device is downloading attendance data until it is successfully downloaded.

3) Press "ESC" to return to the initial interface. Pull out the U disk. X_attlog.dat (attendance log) will be saved to the U disk. (X stands for device ID).

2. Download User Data

Save all users' information and fingerprint in the device to a U disk.

Operation:

Insert a USB flash disk into the USB slot of the device, press "▲/▼" to **download user**, then user.dat (user information) and template.dat (fingerprint template) will be saved to the U disk.

6.2 Upload Data

1. Upload User Data

Upload user information and fingerprints saved on the U disk to the device.

Operation:

Insert the U disk into the USB slot of fingerprint sensor. Press "▲/▼" to select **upload user data**, then press

OK, and user.dat（user information) and template.dat（fingerprint template) on the U disk will be uploaded to the device. If there are no such files, “data copy error” will appear.

2. Upload User Defined Picture

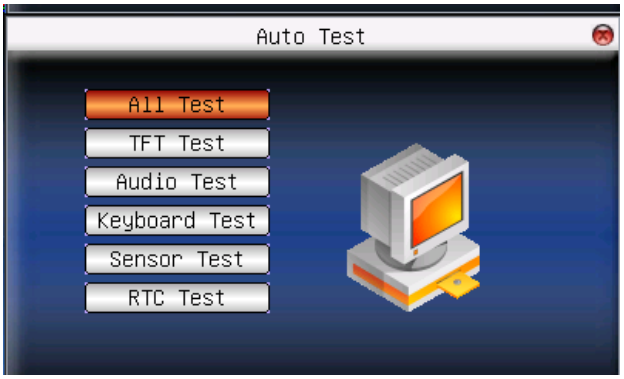
Upload JPG picture started with “ad_” on the U disk to the device. Then this picture will be displayed on the initial interface. (Refer to appendix 10.4)

Operation:

Insert the U disk into the USB slot of device. Press “▲/▼” to preview the pictures on the U disk. If you want to upload the picture, click **OK**. Then the next picture will appear automatically. After uploading, press ESC to exit.

7. Auto Test

The device can test various modules automatically to help the operator to judge the module with a fault quickly. Auto test includes TFT display Test, Audio Test, Keyboard Test, Sensor Test and RTC Test.



Press "▲/▼" to select the item to be selected. Press OK to start it.

7.1 TFT Display Test

The device can automatically test TFT color display effects through color display, white display and black display to see whether the screen works normally.
Press OK to continue and press ESC to exit.

7.2 Audio Test

The device can automatically test voice prompt effects through playing voice files in the device to see whether the files are complete and the voice effects are good or not.
Press OK to continue and press ESC to exit.

7.3 Keyboard Test

The device can automatically test various keyboards to see whether the keys work normally or not.
Press any key on the test interface (**except for OK and ESC**) to check whether the pressed key is in accordance with that displayed on the screen.
Will appear if it is the right key, and will appear if it is not the right key.
Press ESC to exit.

7.4 Sensor Test

The device will automatically test the sensor to see whether it works normally. Press fingerprint to see whether the image is clear and usable.
Press fingerprint on the sensor window and the fingerprint image will appear on the screen.

Press ESC to exit.

7.5 Real-Time Clock

The device can automatically test the clock to see whether it works normally.
Press OK to start time and then press OK to stop time.
Press ESC to exit.

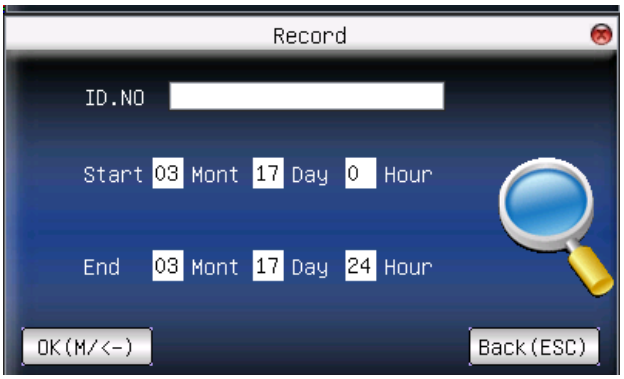
8. Query Record

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

According to user's input query condition, the record will be displayed on the screen for the user to check.

Notice: The picture may be different from your device. The actual product prevails.

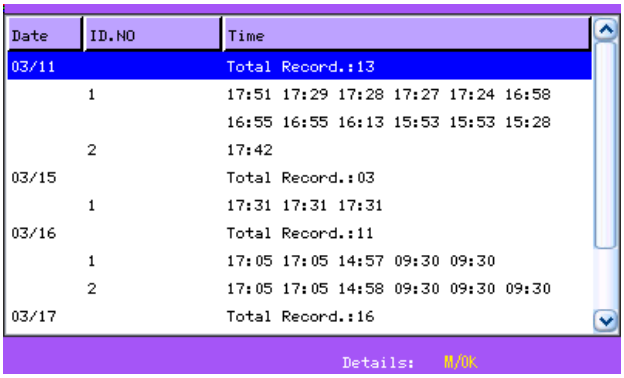
Enter **Query Attendance**, input corresponding information in the **Query Condition** input box.



When the User ID is blank, all employees are queried.

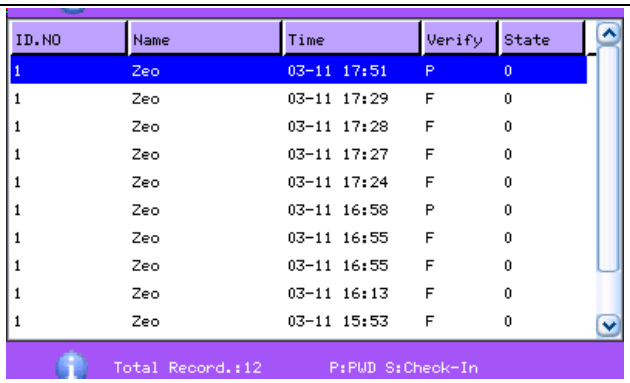
When inputting a User ID, only this employee's attendance record can be queried.

After querying, the records in meeting the conditions will be displayed on the screen:



Press "▲/▼" to move the cursor to the line to be queried and press OK to check attendance record.

For example, the detailed attendance information of employee 10001 on May8th are as follows:



At the bottom of the screen, there are some remarks and the capital letters with their meanings:

Verification:

F: means Fingerprint verification

P: means Password verification

C: means ID card verification

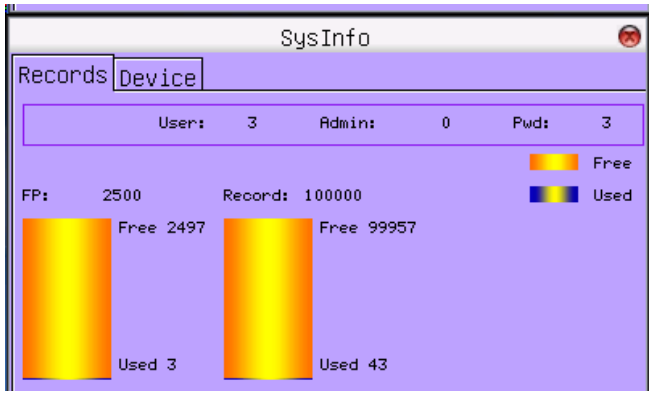
Status: is the attendance status. The code displayed in the list is the status code. The status name will be displayed in the information column.

9. System Information

Use **system information** to check the current device's saving status, its version information and so on.

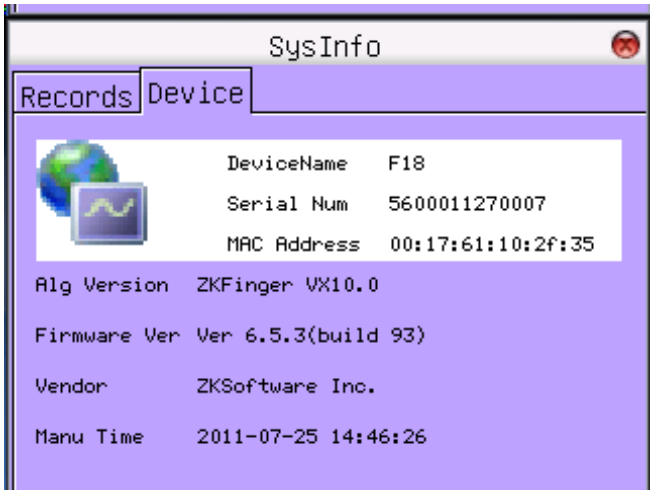
9.1 Record Capacity

Display the count of enrolled users, administrator, password enrollment, the current enrolled fingerprint and the current saved attendance record. Also display the capacity of the fingerprint and attendance record, as show below:



9.2 Device Information

Display the device name, serial number, version information, vendor and manufacture date in device information for check.



10. Appendix

10.1 Keyboard

Different devices have different kinds of keyboards and the function of the keyboard is different. Please check the following:

Keyboard Type 1:

key	function
Numeric key	1. 0～9, used to input employee number, password and so on. 2. 0 on **manage user** interface is **shortcut** of "query user".
▲	1. Upward. 2. Status key.
▼	1. Downward. 2. Status key.
▶	1. Modify current item value. 2. Status key.
⦿/◀	1. Power-off. Press it on initial interface for 3 seconds to enter power-off count down state. 2. Space back. Press it when User ID, password and system value are input incorrectly to delete the wrong value and input the value again. 3. Status key.
M/OK	Menu, OK
ESC	1. Cancel the operation and return to the higher menu 2. Press ESC on initial interface to display the keyboard definition of the present device.

Keyboard Type 2:

key	Function
Numeric key	1. 0～9, used to input employee number, password and so on. 2. 0 on **manage user** interface is **shortcut** of "query user".
▲	1. Upward. 2. Shortcut.
▼	1. Downward. 2. Shortcut.

Keyboard Type 3:

*/▶	1. Modify current item value. 2. Shortcut. 3. Enable T9 input. 4. Switch input method in T9 input.
◀/⬅	1. Modify current item value. 2. Space back. Press it when User ID, password, and system value are input incorrectly to delete the wrong value and input the value again.
key	Function
Numeric key	1. 0~9, used to input employee number, password and shortcut.
0/⦿	1. 0, used to input employee number, password and shortcut. 2. **power off**. In the initial interface press this **shortcut** key for 3 seconds to enter power-off count down state.
▲	1. Upward. 2. Shortcut.
M/OK	Menu, OK.
ESC	1. Cancel the operation and return to the higher menu. 2. Shortcut.
▼	1. Downward. 2. Shortcut.
▶	1. Right. 2. Shortcut.
◀	1. Left. 2. Shortcut.
⦿/⬅	1. Shutdown. In the initial interface press this key for 3 seconds to enter a shutdown countdown status. 2. Space back. Press it when User ID, password, and system value are input incorrectly to delete the wrong value and input the value again.
MENU	Menu, OK, after verification press this key to inquire records.
OK	OK
N/A	Invalid key (Access machines do not have this key)
F1	Sign in state key.
F2	Sign out state key.
🔔	Doorbell key (Access machines have this key)
ESC	Cancel the operation and return to the higher menu.

10.2 USB

- **USB Host**

The device may be used as USB Host to exchange data with external an U disk.

The data transmission speed is quick. The traditional fingerprint machine only supports the RS232, RS485 or Ethernet mode of data transmission. As a result of physical condition limits, data quantity is large, and the data transmission lasts a long time but the USB data transmission is quicker than the former downloading data mode. Complete requires a shorter by a U disk greatly enhances period of time and the efficiency.

For the operational steps of using the device as USB Host please refer to the manual "6. PenDrive management" detailed information.

- **USB Client★**

The device will be used as a removable storage device and the data in the device will transfer to a PC via connected USB cable.

When the device is a USB Client, the Communication Option will have USB communication options. For more details please refer to the manual "3. Communication Option".

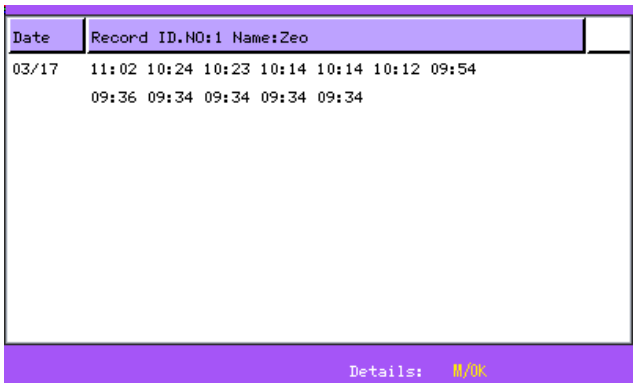
10.3 Quick Query of Attendance Record

It is used for the common user to query his intraday attendance record to see whether there is something wrong with his attendance time and notify an administrator of the abnormal time record.

Operations:

Press M/↵ to display the employee's intraday records after successful fingerprint or password verification in 10 minutes.

For example: the employee with User ID of 1 can check his intraday attendance record by pressing M/↵ after fingerprint verification.



☺ **Notice**: The picture may be different from your device. The actual product prevails.

Press ▲/▼ to read attendance record.

Press M/↵ to query detailed information.

Press **ESC** to return to the initial interface.

10.4 Propaganda Picture Upload Rules

The picture format must be JPG. Other formats are not accepted here.

The file name of propaganda picture must be ad_0～ad_9, for example ad_1.Jpg.

The file name will not be changed after it is uploaded to the device. If it is necessary to change this picture, upload another picture with the same file name to replace it.

Pictures cannot be over 30K, or they cannot be uploaded.

The picture's resolution is 320 wide and 240 high. Any other size is less than optimal.

There can be no more than 10 propaganda pictures .

If you want it, please contact our sales department or technician.

10.5 Card Support (ID/EM, MIFARE Card) ★

In order to meet security market needs, our fingerprint biometric verification reader can be embedded EM, MIFARE reader module**.**

ID/EM Card

The FRT supports ID cards with working frequency of 125KHz and card reading distance of 2m to 5m.

Mifare Card

The FRT supports MIFARE non-contact smart cards with working frequency of 13.56 MHz and card reading distance of 3m to 5m.

Using 125MHZ, 13.56 MHz non-contact smart card technology, these fingerprint products provide users with new options for supporting multi-authentication of identity. Combine a non-contact card presentation with a fingerprint biometric or use a personal identification number (PIN) number along with a non-contact card presentation. (See multi-authentication).

The fingerprint products provide three levels of fingerprint verification. During the enrollment process, the LCD prompt will guide the user to place their finger on the sensor. The fingerprint template is collected at the unit and immediately transferred to the card. During this enrollment process, the fingerprint template is stored on the card or the fingerprint machine.

During verification at the door, the LCD graphical display will assist the user with instructions about finger placement on the biometric sensor.

For more detail see ID/EM, Mifare Card user Guide.

10.6 Web Time & Attendance ★

Summary

The T & A system is based on Web Server technology and uses Page Request technology to process and manage data. It integrates many features, such as local data collection, intellectualized port (RS232/RS485) communication protocol conversion, image collection, alarm data storage, and WEB server etc. This equipment is based on creating a unifying monitoring platform that supplies one solution for equipment management, Time & Attendance, as well as monitoring. In addition, the Web Time & Attendance solution is independent of regional limits, does not need to install other software because it utilizes IE or Netscape browsers for downloading and remote on-line management. It also handles time sheet corrections and creates report tables on the fingerprint terminal. It provides an easy way for managers of the enterprise to know the employee's position or attendance status at any moment in time, search for information, statistical data, and deal with operations while at the same time, provide a solution for staff attendance, check in or out management, pay roll management, in word and deed realize that anywhere at any moment the information is synchronization, and it goes far beyond traditional Time & Attendance solutions.

Why embed Web Server into the device?

1. A few or nobody to keep watch

Through TCP/IP and Ethernet, WEB Server is able to reliably use local networks to watch and manage the data fingerprint machine store up via long distance networks with a browser. There is no need for an administrator or specially assigned person to go on site to collect, upload/download data, or upgrade the system. No other software and tools are needed.

2. Fully compatible with our company Inc program

WEB Server platform may be fully compatible with current programs. Each is entirely mutually beneficial with the ability to be much more flexible to meet customer need.

3. More reliable, fast through long distance data transfer

Through WEB Server, data is able to be reliably and quickly downloaded to local systems. It utilizes your browser's ability to download all data in short time, without having to worry about reliability.

4. More flexible, easy for data management and source share

via the platform created by Web server, the application program, data management becomes more easy and flexible.

5. May easy integration of OA, CRM system, reliable

base of network of human workforce management.

10.7 9 Digit Code★

When enrolling users in the fingerprint machine, the standard enrolling code is five digits long（its range is 1-65534), if you need longer enrolling codes, we can provide a customized design that provides for a nine digit code.

10.9 Daylight Saving Time★

Some devices provide correct and current times in any world time zone, country or major city. Accurate adjustments for Daylight Saving Time (or Summer Time) are made according to each location's rules and laws. No matter what time zone a country or city is located in, this is your top choice for a clock resource site.

This function can be set in the fingerprint machine option, Press Menu key, enter the **Date Time**. In the XX Month XX Date XX minute move forward an hour, and that in the XX Month XX Date, XX Minute move Back an hour.

Refer to the manual 5.2 DLST for this operation.

10.10 Master-Slave Function ★

- **Overview**

In order to reduce the repeated enrollment operation in multiple devices, we can use the master-slave option. It only needs to enroll user information in one master device; other slave units will send synchronization requests to the master according to set master-slave parameters. The master unit sends all its user information and fingerprint template data to slave units when it has checked a synchronization request on the network. Slave units receive and save the data from the master. So the user enrolled in the master unit may record attendance in multiple slave units.

- **Operation**

1) Menu setup

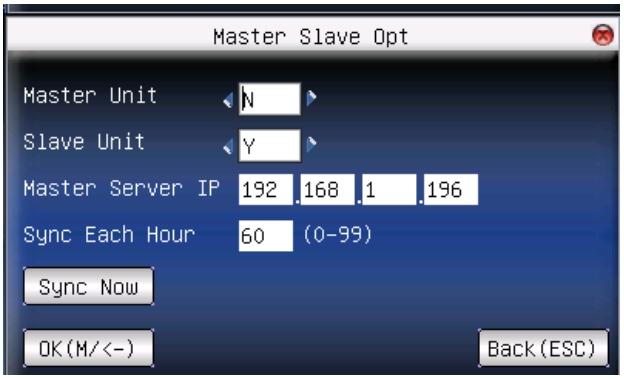
Enter "**Menu - Communication option - Master-slave option**", there are four relevant options:

Master unit: Whether set this device to be a master unit. Select "Y" if you want to.

Slave unit: Whether set this device to be a slave unit. Select "Y" if you want to.

Master Server IP: Input the master server IP manually if you set this device as a slave unit.

Sync Each hour: The synchronization frequency after the connection -- You can set every few hours to synchronize. (With range of 0-99, only the device is set as master unit, this setting is valid)



2) Connection

Choose the master unit and slave unit. Connect them to the LAN through the switch.

Restart the devices after connection. The master unit is an ordinary fingerprint device. After the device is restarted, the slave unit will automatically search the master unit and send a request.

If the message “Fail to sync” shows on the slave unit, it means the slave unit can’t find the master unit, and the data update failed. Please check the settings through the device menu.

If there is no prompt in the client, this means the connection is successful. The process in the master unit is same to the ordinary fingerprint device. The data in the master unit will be synchronized to the slave units according to the parameters set in master slave option.

10.11 About the Human Rights Privacy Statement

Dear customer：

First, thank you for using the Multi-biometric identification product we design and produce. As one of the renowned global fingerprint identification core technology provider, we are constantly continuing the development and research, also we believe such action is necessary to: (a) comply with the law or legal process served on our company; (b) protect and defend the rights or property of our company (including the enforcement of our agreements); or (c) be governed by related law or legal that involve human rights and privacy in each country.

We are committed to protecting your privacy.

We state as follows:

1. Our civil fingerprints identification equipment merely captures fingerprint features points, but not the fingerprint image, does not involve and retain privacy.
2. The fingerprint features points are not to be recovered. The primitive fingerprint image, will not involve the privacy.
3. We are an equipment provider. In no event shall we be liable for any direct or indirect illegal behavior arising out of use or inability to use our equipment.
4. If you have a dispute regarding human rights or privacy arising out of the use of our equipment, please contact your employer. Our police fingerprint equipment or development kit provides the ability to capture citizen's original fingerprint image, as to whether or not that constitutes infringement of your rights, please contact your local government or the final equipment provider. As the original equipment producer, we have no legal liability for any damage it cause.

Note: There are limited rights to privacy and human rights in the Chinese Constitution.

The personal dignity of citizens of the People's Republic of China is inviolable and further, that insult, libel, false accusation or false incrimination directed against citizens by any means is prohibited, the protection of freedom of the person and the residence .The Constitution provides for the freedom and privacy of correspondence of the citizen.

Finally we hereby stressed that once again, as one kind of advanced identification technology the fingerprint identification will apply to electronic commerce, bank, insurance, law service industry in the future, every year, all world cause from the lack of security password , the humanity are suffering the heavy loss. In under high safe and secure environment the fingerprint identification protect your status from damage in fact.

10.12 Environmental Protection

- The environmental protection use period marked on our products is the safety period of our products used under the conditions specified by this manual without toxic and harmful substances leaking happened
- The environmental protection use period marked

on our products does not include the easy wear and tear of components required to be replaced regularly such as the battery etc. The battery's environmental protection use period is 5 years.

Toxic and harmful substances or element names and the content table

Part name	The toxic and harmful substances or elements					
	Pb	Hg	Cd	Cr6 +	PBB	PBDE
SMD resistor	×	○	○	○	○	○
SMD capacitor	×	○	○	○	○	○
SMD inductance	×	○	○	○	○	○
SMD diode	×	○	○	○	○	○
ESD components	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screw	○	○	○	×	○	○

○：Indicate that the content of the toxic and harmful substance contained in all homogeneous materials of this part is in the limitation requirement stipulated in SJ / T 11363-2006.

×：Indicate the content of the toxic and harmful substance contained in at least one homogeneous material of this part is beyond the limitation requirement stipulated in SJ / T 11363-2006.

Note: The 80% product has adopted the manufacture with non-toxic and harmless environmental protection materials, the non-toxic and harmless substances or elements instead of the toxic and harmful substances or elements contained cannot be achieved because of the current technology and economic constraints.