USER MANUAL

Fingerprint Lock

Version: V1.2

Date: April 2012

About This Manual

This manual introduces the fingerprint lock interface and menu operations. For the fingerprint lock installation, see the animated installation instructions.

Our products are subject to update from time to time, so our company will neither make a commitment to guarantee the consistency between the actual products and this document, nor assume any responsibility for any dispute arising out of the discrepancy between the actual technical parameters and this manual. This document is subject to change without prior notice.

Table of Contents

1 Instruction for Use

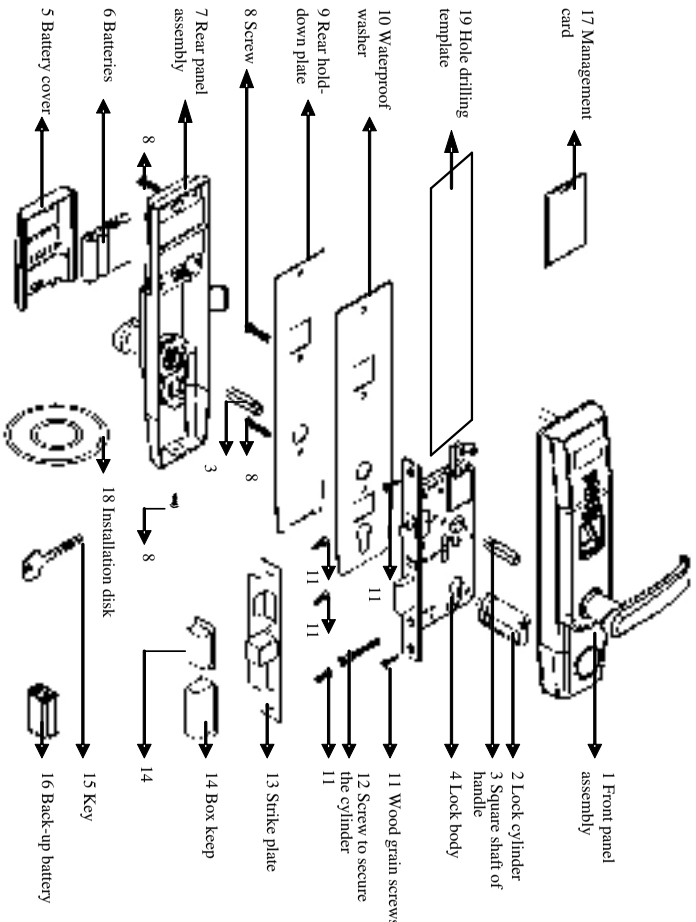
Functions marked with "★" in this manual are only supported by a specific product or a tailor-made product and will be described below.

1.1 Introduction to Fingerprint Lock Functions

1. By leveraging the perfect combination of biometrics and cryptography, our fingerprint locks ensure double security through the fingerprint + password unlocking feature
2. The state-of-the-art Organic LED (OLED) display affords crisp bright readouts and makes our fingerprint locks intuitive and easy to use. You can simply use our fingerprint locks with ease after following the operation instructions for once
3. Support setting of classified privileges for super administrators, administrators and ordinary users
4. Support deletion of all or the specified registration data
5. Support firmware upgrade and uploading/downloading of user information and locking records through a USB pen drive
6. Support offline view of locking records
7. Support accurate display of time and date with annual deviation less than two minutes
8. Support a temporary connection with back-up batteries
9. You can set the fingerprint locks to be in the Normally Open (NO) state in special cases
10. Support display of the battery charge level and generation of low-pressure alarms

11. Feature an electric clutch handle design which helps effectively prevent the fingerprint lock failure caused by damage to the internal structure as a result of the forced destruction of the handle
12. Supporting remote unlock, which is convenient and swift.
13. Supporting Zigbee PC-monitoring for door opening, which monitors unlock information in real time.

1.2 List of Installation Accessories



List of Installation Accessories

SN	Name	Quantity	Unit	Remarks
01	Front panel assembly	1	Set	

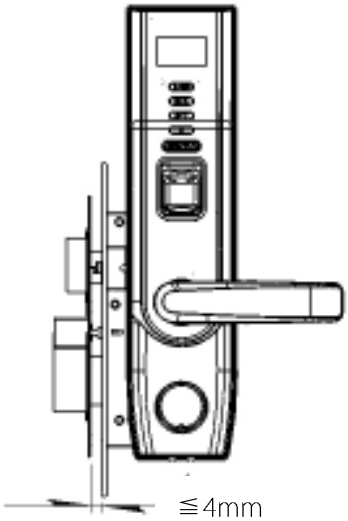
02	Lock cylinder	1	Set	
03	Square shaft of handle	2	PCS	
04	Lock body	1	Set	
05	Battery cover	1	PCS	
06	Batteries	4	PCS	Four pieces of alkaline AA batteries
07	Rear panel assembly	1	Set	
08	Screw	6	PCS	Reserve two screws and select proper screw size based on the door thickness
09	Rear hold-down plate	1	PCS	
10	Waterproof washer	2	PCS	Including the one on the front panel assembly
11	Wood grain screws	5	PCS	
12	Screw to secure the cylinder	1	PCS	
13	Strike plate	1	Set	
14	Box keep	2	PCS	
15	Key	2	PCS	
16	Back-up battery		PCS	9V
17	Management card	1	PCS	Optional
18	Installation disk	1	PCS	
19	Hole drilling template	1	PCS	

1.3 Installation Requirements

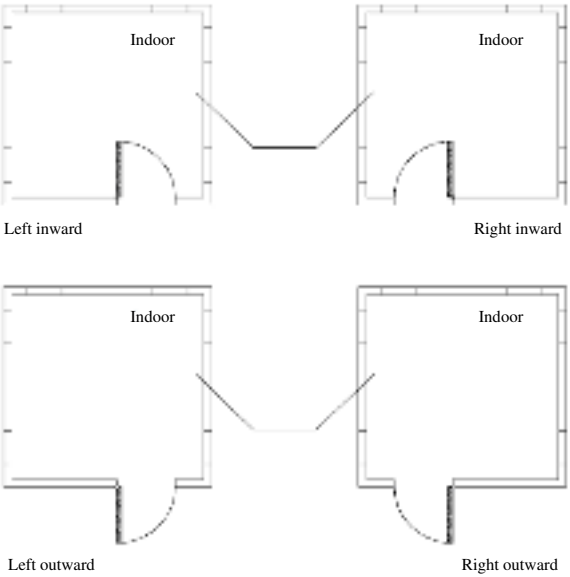
Precautions:

1. The fingerprint lock is applicable to doors of 35–50 mm in thickness. Be sure to list your special requirements or remarks for fingerprint locks to be installed on doors in excess of 50 mm in thickness before placing an order.

2. The gap between the lock body and the box keep cannot exceed 4 mm; otherwise, you need to adopt a liner plate to ensure the gap between them is not more than 4 mm, as shown in the following figure:

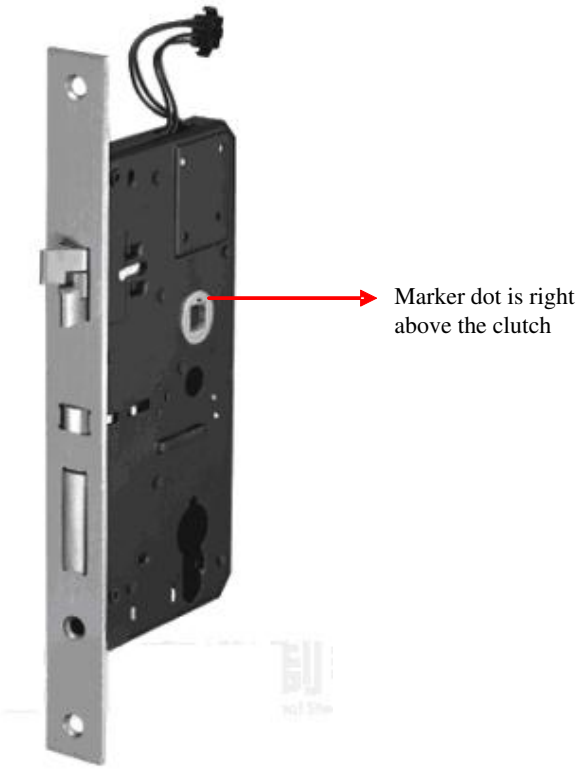


3. Please make sure of the door opening directions and lock body. Assume you are standing outside and facing a door and then there are four door opening directions: Left inward, left outward, right inward and right outward. Left inward/outward means the door swings inward/outward with hinges on the left; right inward/outward means the door swings inward/outward with hinges on the right, as shown in the following figure:



4. Ensure the central point of the handle is about 1m above the floor.

5. Ensure the marker dot of clutch is right above the clutch.



6. Please follow the animated instructions to install fingerprint locks.

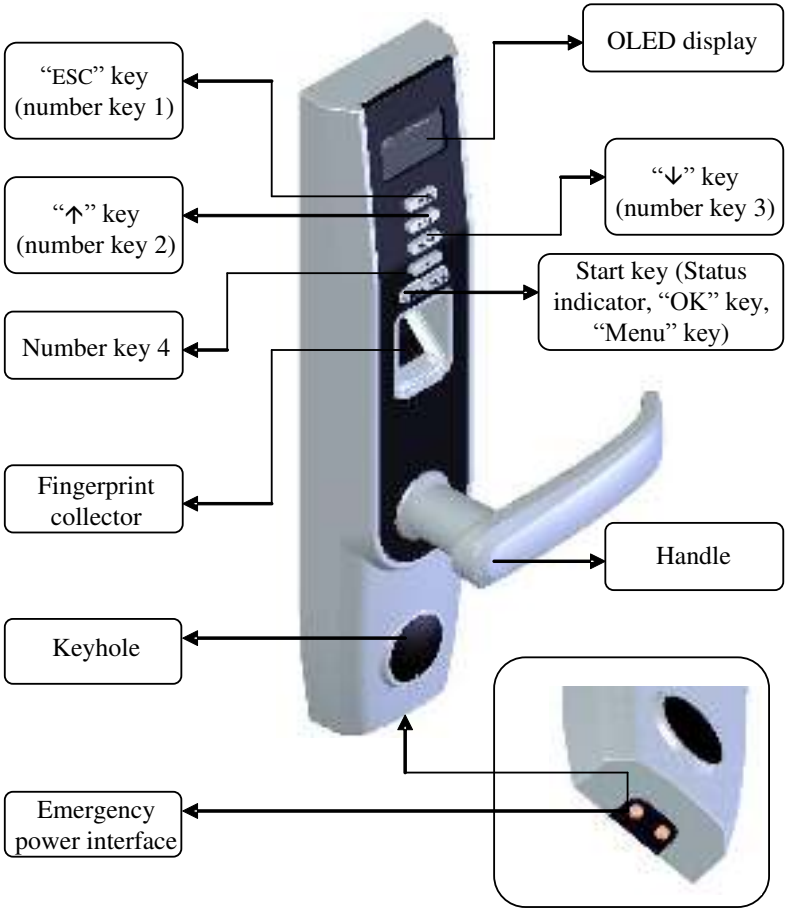
Recommended Tools

You may need the following tools while following the instructions to install fingerprint locks:

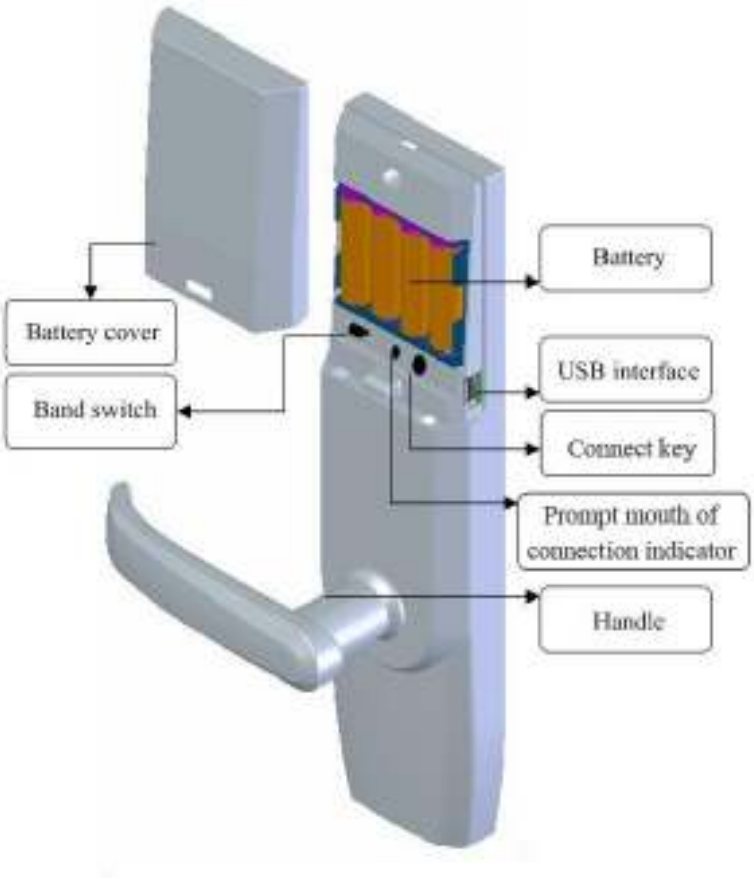
- A ruler.
- A marker pen.
- A drilling tool.
- A cross screwdriver.

1.4 Front and Rear Views

Front view



Rear view



ESC key: Press this key to exit current operation and press and hold this key to power off the fingerprint lock. ESC key doubles as the number key "1".

↑ key: This key is used to manually increase (when held, this key will rapidly increase display values) the setup value or navigate among menu options. ↑ key doubles as the number key "2".

↓ ***key***: This key is used to manually decrease (when held, this key will rapidly decrease display values) the setup value or navigate among menu options. ↓ key doubles as the number key "3".

Start key: This key can be used to start the fingerprint lock; press and hold this key for three seconds on the initial interface to open the menu options; this key also doubles as the confirmation (<OK>) key.

Band switch: If you cannot access the menu options due to the loss of administrators for some reason, proceed as follows: Press and hold the ***Menu*** key for three seconds to display the administrator verification, and then turn the ***Band*** switch at the back of the lock to the left or right to open up the menu as a super administrator.

Connect key: Before remote unlock, press connect key to connect the device to the remote control.

Prompt mouth of connection indicator: During connection, you can view the connection indicator through this prompt mouth to check the connection status.

Status indicator: You can awake the fingerprint lock in dormant state by pressing the ***Start*** key. The green LED indicator blinks when the fingerprint lock operates properly and the red LED indicator is on for three seconds if an error occurs. The green LED indicator is on for three seconds when an operation succeeds.

OLED display: The black-and-white OLED display features white graphics or text against a black background.

Fingerprint sensor: You can only collect or match fingerprints by pressing your finger(s) at the fingerprint sensor when the light in the

fingerprint sensor window goes on; otherwise nothing happens when you press your finger(s) at the fingerprint sensor.

Notice: When you cannot power off the fingerprint lock due to the exception of program, press and hold the ***ESC*** key to power off and then restart the fingerprint lock. It is not recommended to power off the fingerprint lock by pressing and holding the ***ESC*** key when the fingerprint lock operates normally.

Emergency interfaces

Keyhole: You can use a mechanical key for emergency door opening.
Temporary external power interface: You can adopt an external back-up battery to open the lock in the event of unlocking failure due to insufficient power supply of the fingerprint lock.

USB interface

The USB interface is used for firmware upgrade and uploading/downloading of user information and locking records through a USB pen drive.

1.5 Precautions

1. We strongly recommend you to enroll at least one administrator after installing the fingerprint lock. You must at least enroll one administrator before enrolling ordinary users.
2. Do not remove batteries when matching, enrolling or deleting fingerprints because the sudden power-down may result in data loss of fingerprint locks. Prior to removing batteries, make sure the fingerprint lock is not in working state.

3. It is recommended to replace the fingerprint lock batteries at least once every six months to avoid damaging the circuit due to the battery leakage. Do not use batteries with poor quality.

4. When installing a fingerprint lock, connect the plug to the socket properly. Improper connection may lead to fingerprint lock failure.

1.6 User Privileges

The user privileges are classified into three types: Super administrators, administrators and ordinary users.

Super administrators: refer to users who have access to all system functions and modify all system settings.

Administrators: refer to users who have access to all operations except performing advanced settings and enrolling super administrators.

Ordinary users: refer to all users other than the super administrators and administrators. Ordinary users only have access to the fingerprint matching and unlocking functions.

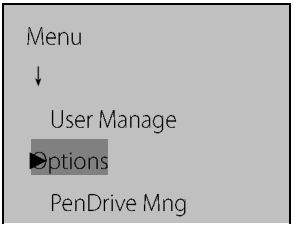
1.7 Set Time

You need to set the correct date and time on first use of a fingerprint lock in the following steps:

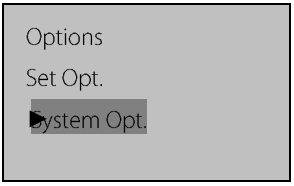
1. Power on the fingerprint lock by pressing the ***Start*** key to open up the initial interface, as shown in the figure on the left.

Notice: The "▪▪▪▪" icon on the initial interface is the battery icon indicating

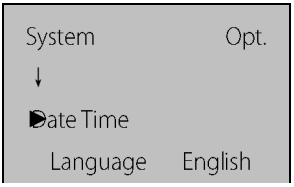
how much charge remains. On the top right corner of the initial interface, the display alternates between date and time every 5 seconds.



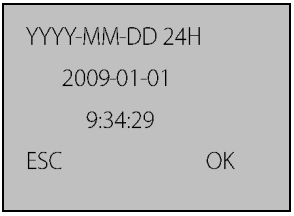
2. Press and hold the ***Menu*** key for three seconds to access the menu interface. Press ▼ to select "Options" and press ***OK*** to display the setting interface.



3. Press ▼ to select "System Opt." and then press ***OK***.



4. Press ***OK*** to select "Date Time".



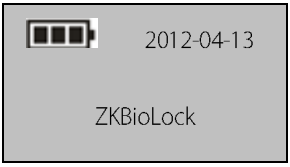
5. To modify date or time, press ▲/▼ to move the cursor to the desired option, and then press ▲/▼ again to enter correct date or time. Press ***OK*** to save your settings.

Notice: You can set the date between January 1st 2003 and December 31st 2032. To set the date beyond this range, you need to consult our commercial representatives or pre-sales technical support engineers.

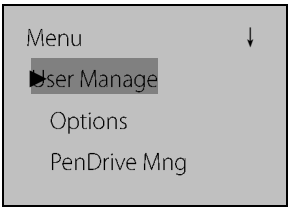
2. Enrollment and Verification

2.1 Enroll an Administrator

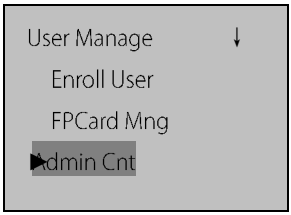
If the fingerprint lock has no administrator, you must at least enroll one administrator before enrolling ordinary users. To enroll an administrator, proceed as follows:



1. Power on the fingerprint lock by pressing the ***Start*** key to open up the initial interface. Press and hold the ***Menu*** key to display the menu interface.



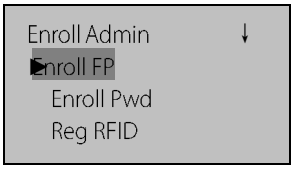
2. Press ***OK*** to display the user management interface.



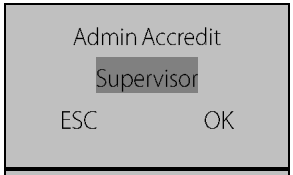
3. Press ▼ to select "Admin Cnt" and then press ***OK***.

After that, the enrolled administrator can perform fingerprint, password and RF card enrollment.

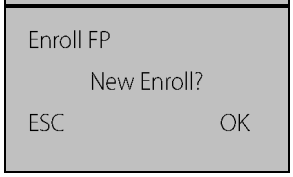
2.1.1 Enroll a Fingerprint



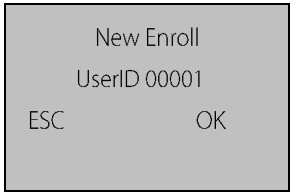
4. Press ▼ to select "Enroll FP" and then press ***OK***.



5. Press ▲/▼ to select "Admin Accredit", and then select "Supervisor" (Super administrator) or "Admin" (Administrator). Press ***OK*** to confirm your selection.



6. Press ***OK*** to continue.



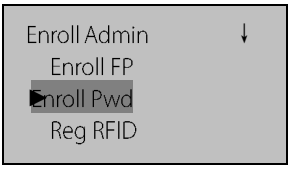
7. The system by default assigns unused user IDs from 00001 and you may also manually enter an unused user ID.

8. Press finger according to device's prompt, press the same finger on the fingerprint sensor three consecutive times by adopting the proper finger placement mode. The system will prompt you to save the enrollment information after you enroll the fingerprint successfully. If enrollment fails, the system will prompt you to re-enroll your fingerprint. The system returns to the "New

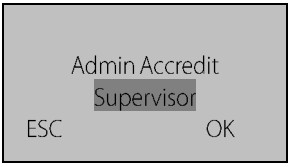
Enroll" interface upon successful enrollment. You can continue or exit the fingerprint enrollment.

Notice: The last digit in "00001–0" refers to the fingerprint count. "0" refers to the first fingerprint, "1" refers to the second fingerprint and so on and so forth.

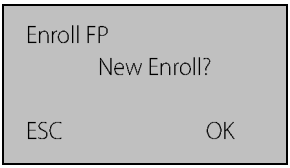
2.1.2 Enroll a Password



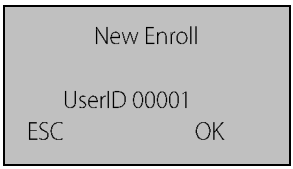
4. Press ▼ to select "Enroll Pwd" and then press ***OK***.



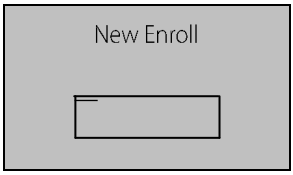
5. Press ▲/▼ to select "Admin Accredit", and then select "Supervisor" (Super administrator) or "Admin" (Administrator). Press ***OK*** to confirm your selection.



6. Press ***OK*** to continue.

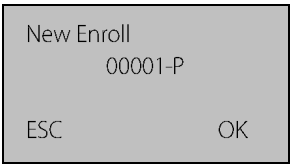


7. The system by default assigns unused user IDs from 00001 and you may also manually enter an unused user ID.



8. Input a password by pressing the number keys and press ***OK*** to confirm your input.

9. Input the password again by pressing the number keys and press ***OK*** to confirm your input. Press ***OK*** after successful password enrollment to return to the "New Enroll" interface.

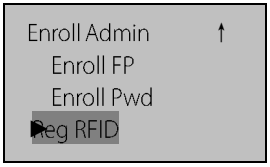


10. Press ***OK*** to save the enrolled data and exit the password enrollment.

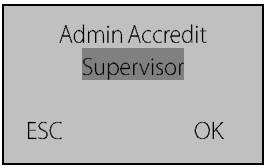
Notice: A password consists of 6 to 10 digits. You can enroll only one password for each user ID and repeated passwords are allowed; otherwise, the system will display the prompt "Password Error".

2.1.3 Enroll an RF ID Card ★

Notice: This function is only provided by fingerprint locks that support the RF ID card function.

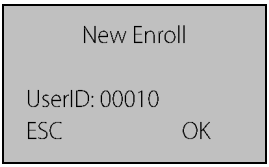


4. Select "Reg RFID" and press ***OK***.

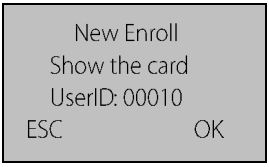


5. Press ▲/▼ to select "Admin Accredit", and then select "Supervisor" (Super administrator) or "Admin" (Administrator). Press ***OK*** to confirm your selection, as shown in the figure on the left.

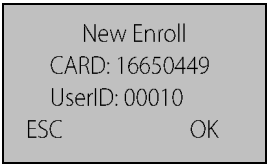
6. Press ***OK*** to proceed to the next step. The interface displayed is shown in the figure on the left.



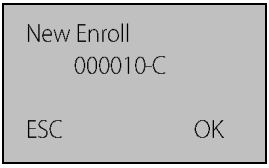
7. Enter the ID (ranging between 1 and 65534) to be enrolled behind the "UserID" option, and press ***OK***, as shown in the figure on the left:



8. Show the card by following the prompt, as shown in the figure on the left:



9. The displayed card number is shown in the figure on the left.



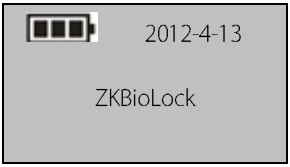
10. Press ***OK*** to proceed to the next step. The interface displayed is shown in the figure on the left.

Note: The last letter "C" in "00010-C" refers to the ID card.

11. Press ***OK*** to save the enrolled data and exit the ID card enrollment.

2.2 Enroll an Ordinary User

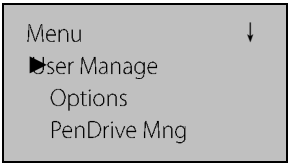
An administrator can enroll only ordinary users, with operation steps as follows:



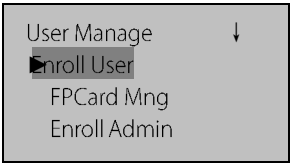
1. Power on the fingerprint lock by pressing the ***Start*** key to open up the initial interface.

2. Press and hold the ***Menu*** key to access the menu options. The system will then prompt you for administrator confirmation. Enter the administrator password or match your fingerprint once. Skip to step 4 if verification succeeds; otherwise, proceed to step 3.

3. The system displays the prompt "Error Pwd." on the screen and return to the "Admin Affirm" interface for re-verification. The following menu interface is displayed upon successful verification.



4. Press ***OK*** to display the user management interface.

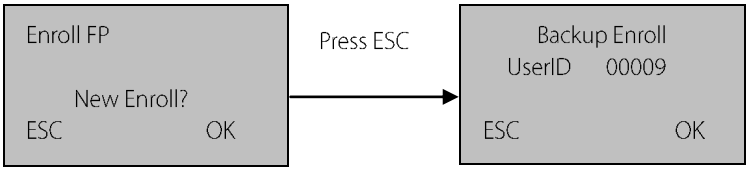


5. Press ▼ to select "Enroll User" and then press ***OK***.

After that, the enrolled administrator can perform fingerprint, password and RFID card enrollment. The rest operation steps are basically the same with those of administrator enrollment except that you do not have to select the administrator privileges. For details, see 2.1 Enroll an Administrator.

2.3 Backup Enrollment

On the "New Enroll?" interface, if you press ***ESC*** to cancel new enrollment, then the "Backup Enroll" interface will be displayed, as shown in the figure on the right.



The backup enrollment steps are basically consistent with the new enrollment steps except that "Backup Enroll" instead of "New Enroll" is displayed on the top of the interface.

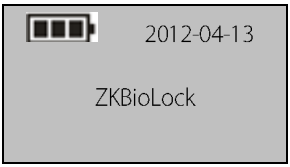
Notice:

(1)It is a wise choice to enroll fingerprints of at least two different fingers for long-standing users.

(2)If you wish to modify the password after finishing password enrollment, you can replace the original password with the password entered in backup enrollment.

(3)If you perform backup enrollment after enrolling the RFID card, the original RFID card number will be replaced by the ID card number entered in backup enrollment.

2.4 Set User Verification and NO Status



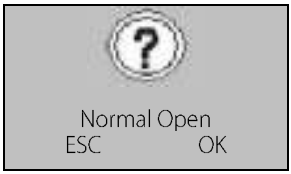
1. Press the ***Start*** key to display the initial interface. The fingerprint sensor is in active state.

2. Press your finger with fingerprint already enrolled or enter your password (press ***OK*** after entering password.)

Note: You can only match fingerprints when the fingerprint lock is in non-NO state.

3. Your ID number will be displayed on the screen upon successful verification and then you can hear the unlocking sound. Rotate the handle of the fingerprint lock within 4 seconds to open the door.

If the NO function is set to "YES" (See 3.1 Operation Settings), the prompts as shown in step 4 and step 5 will be displayed upon successful verification; otherwise, no prompt will be displayed.



4. If you press ***ESC*** when the system prompts whether to set the NO function, the fingerprint lock will be automatically locked. The "Unlocking" icon on the screen will change into the "Locking" icon and the system automatically powers off.

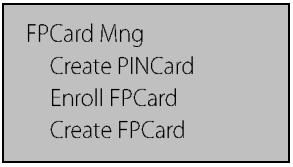
5. If you press ***OK***, the interface as shown in the figure on the left will be displayed, indicating successful NO setting. In the meantime, the buzzer will beep three consecutive times.

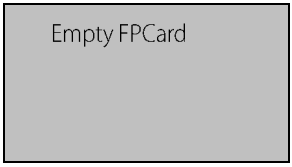
If fingerprint or password verification is unsuccessful, the system will display a prompt "Please press your finger again" or "Password error". The parameters "Illegal Cnt." and "Illegal Alarm" are set by the administrator. The system will generate an alarm after the illegal operations reach the specified value. For details, see 3.1 Operation Settings.

Notice: If the value of the parameter "Illegal Cnt." is larger than 6, the system will automatically power off if you fail to verify your fingerprint or password 6 consecutive times.

2.5 FP Card Management ★

Select "FPCard Mng" from the "User Manage" interface, as shown below:





Create PINCard: This option is used to create an ID card for a user who has already been enrolled in the fingerprint lock. You can verify your ID card instead of your fingerprint (only after the parameter "Card Only" is set to "***Yes***". For details, see 3.1 Operation Settings).

Enroll FPCard: This option is used to store an enrolled fingerprint directly in the FP card instead of in the fingerprint lock. You can verify user identify

in the form of "FP card + fingerprint", that is, swipe the FP card before pressing the finger.

Create FPCard: This option is used to duplicate the enrolled fingerprints (stored in the fingerprint lock) to the FP card. You can verify user identity either through the "Fingerprint" or in the form of "FP card + fingerprint".

Empty FP***Card:*** This option is used to purge all data (fingerprints and numbers) stored in the FP card.

Notice:

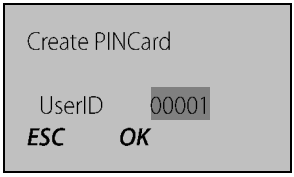
(1)This function is only provided by fingerprint locks that support the Mifare card function.

(2)If no administrator is enrolled in the system, the system will prompt you to enroll an administrator first.

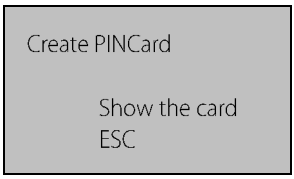
2.5.1 Create a PIN Card

1. Create a PIN Card

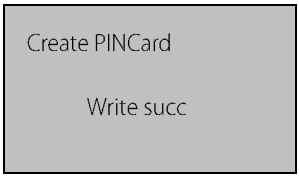
Every user will be assigned with an ID number, for example, 00001, after users are enrolled in the fingerprint lock.



(1)Select "User Manage" → "FPCard Mng" → "Create PINCard" from the main menu. The interface as shown in the figure on the left is displayed:



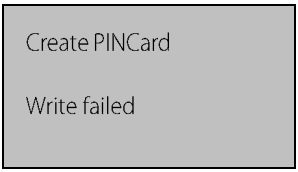
(2)When prompted to enter the user ID number, press ▲/▼ to select the desired user ID, and press ***OK***. The system then prompts you to "Show the card" (If the selected user ID does not exist in the system, the system will display a prompt "No Enroll"), as shown in the figure on the left:



(3)Swipe your FP card through the card reader.

- The interface as shown in the figure on the left is displayed:

If the system gives a prompt "Write succ", your PIN card is successfully created. You can replace the fingerprint verification with the PIN card verification.



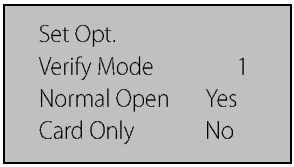
- If the interface as shown in the figure on the left is displayed:

If the system gives a prompt "Write failed", your PIN card is not written in the system.

Tips: To create a PIN card, you need to ensure the user ID has already existed in the system; otherwise, the system will display a prompt "No Enroll" and you need to repeat the operation. After the PIN card is successfully created, only the ID number is stored in the PIN card.

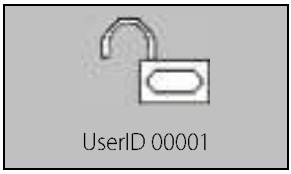
2. Verify the PIN Card

Note: Set the parameter "Card Only" to "Yes". If you set the parameter "Card Only" to "No", you cannot verify with the created PIN card.



(1)Select "Set" → "Set Opt." from the main menu. The interface as shown in the figure on the left is displayed:

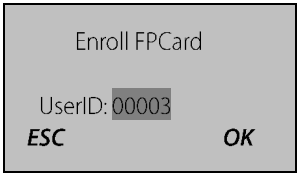
(2)Select "Card Only" and press ***OK***. Then press ▲/▼ to select "Yes". Press ***OK*** to save the setting. Then, you can perform PIN card verification.



(3)Swipe your PIN card through the card reader when the system returns to the initial interface. If the interface as shown in the figure on the left is displayed, the PIN card is successfully created.

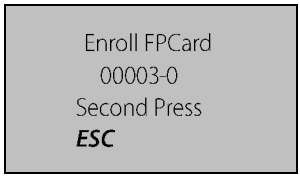
2.5.2 Enroll an FP Card

1. Enroll an FP card

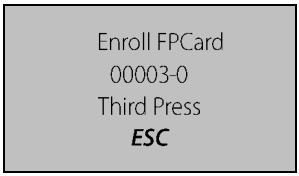


(1)Select "User Manage" → "FPCard Mng" → "Enroll FPCard" from the main menu to display the interface as shown in the figure on the left:

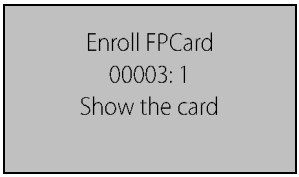
(2)Press ▲/▼ to select an ID and then press ***OK*** to confirm your selection and proceed to the next step. Place one of your fingers on the fingerprint sensor.



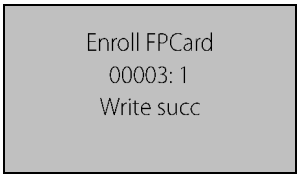
(3)Place the same finger on the fingerprint sensor again.



(4)Place the same finger on the fingerprint sensor for the third time.



The interface as shown in the figure on the left is displayed:



(5)Swipe your card through the card reader until the interface as shown in the figure on the left is displayed.
Now the FP card is enrolled successfully.

2. Verify an enrolled FP card

Note: Please set the "Card Only" option to ***No***. If you set it to ***Yes***, the fingerprint lock will only verify users' PIN cards.

(1)On the initial interface, swipe an enrolled FP card through the card reader. The interface as shown in the figure on the left is displayed:

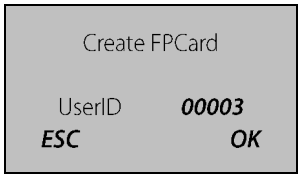
(2)Place one of your fingers with fingerprint enrolled on the fingerprint sensor window properly. When the interface as shown in the figure on the left is displayed, the FP card passes the verification successfully.

Tip: Through the above operations, you only store your fingerprints in your FP card but not in the fingerprint lock. Therefore, you must show your FP card first before fingerprint comparison. (Your fingerprints are only stored in your FP card.)

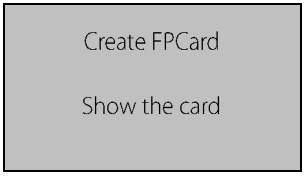
2.5.3 Create an FP Card

1. Create an FP card

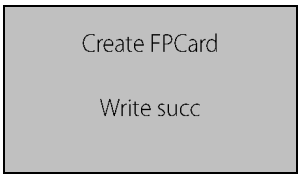
Every user is allocated with an ID, for example, 00003, during the enrollment of fingerprint.



(1)Select "User Manage" → "FPCard Mng" → "Create FPCard" from the main menu to display the interface as shown in the figure on the left:



(2)Press ***OK*** and the interface as shown in the figure on the left is displayed.



(3)Swipe your card through the card reader until the interface as shown in the figure on the left is displayed.

Now an FP card is created successfully.

2. Verify a created FP card

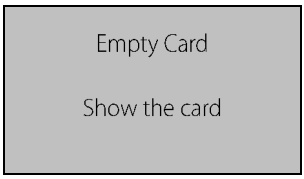
Note: Please set the "Card Only" option to ***No***.

The operations of verifying a created FP card is the same with that of verifying an enrolled FP card.

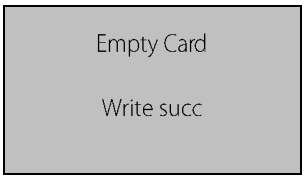
Tip: Through the above operations, you can duplicate fingerprints from the fingerprint lock to an FP card. In this way, you can perform identification either through fingerprint or "FP card + fingerprint". (Your fingerprints are stored in both the fingerprint lock and your FP card.)

2.5.4 Purge an FP Card

To purge all the information in an FP card, proceed as follows:



1. Select "User Manage" → "FPCard Mng" → "Empty Card" from the main menu to display the interface as shown in the figure on the left:



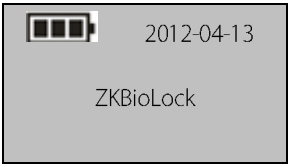
2. Swipe your card through the card reader until the interface as shown in the figure on the left is displayed.

Now the FP card is purged successfully.

2.6 Delete User Data

Warning:It is prohibited to power off the fingerprint lock while deleting user data so as to prevent the program from accidentally deleting other data.

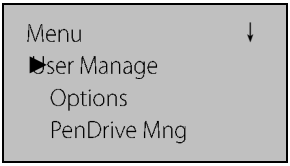
To delete user data, proceed as follows:



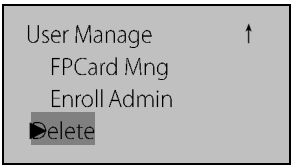
1. Press the start key to power on the fingerprint lock and then enter the initial interface.

2. Enter the administrator password or fingerprint once. If the verification succeeds, jump to Step 4; otherwise, go to Step 3.

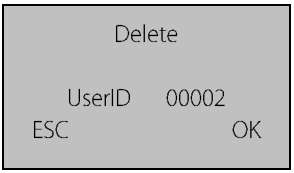
3. The system displays the prompt "Error Pwd." on the screen and returns to the "Admin Affirm" interface for re-verification. If you pass the verification, you can access the "Menu" interface.



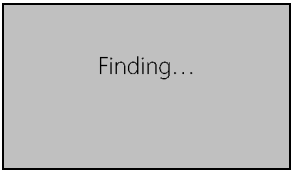
4. Press ***OK*** to display the "User Manage" interface.



5. Press ▼ to select "Delete", and press ***OK***.

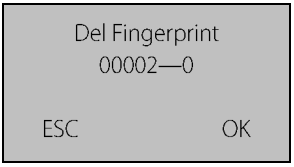


6. Press ▲/▼ to select the user ID that you want to delete and then press ***OK*** to confirm your selection.

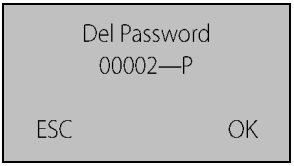


7. If ***Finding…*** is displayed as shown in the left figure, the device is automatically searching the user's registration information and will display the information for the administrator to select and delete the information.

If the user has enrolled his/her fingerprints,

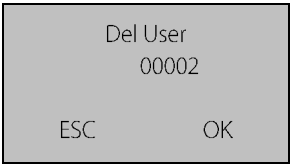


8. Press ***OK*** to delete the fingerprints.



If the user has enrolled a password,

9. Press ***OK*** to delete the password.



10. Confirm the deletion of this user. Press ***OK*** to confirm the deletion, or press ***ESC*** to return to the "User Manage" interface.

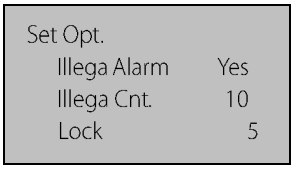
11. After deleting the user data, you can restart the fingerprint lock and match the deleted fingerprints again to check whether the user data is deleted for sure.

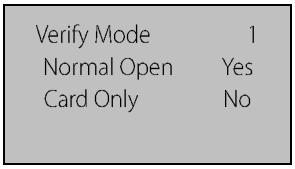
Note: The administrators (including super administrators) can delete only ordinary users. To delete an administrator ID, you need to select "Options" → "System Opt." → "Adv Option" → "Clr Admin Pri", and then select "User Manage" → "Delete" to delete the ID.

3. Lock Function Information and Settings

3.1 Operation Settings

Select "Options" → "Set Opt." from the main menu to display the following information:





The options under "Set Opt." include: ***Illega Alarm, Illega Cnt., Lock, Verify Mode, Normal Open,*** and ***Card Only.***

Illega Alarm(Illegal Alarm): The fingerprint lock will power off automatically when the number of consecutive operation failures exceeds the set value. After restart, its buzzer will sound discontinuously for 30 seconds to generate an invalid operation alarm and then power off automatically.

Illega Cnt.(Illegal Operation Count): This parameter is used to set the consecutive operation failure count. An invalid operation alarm will be generated when the consecutive failure count exceeds the threshold. Value range: 3–99. Default value: 10.

Note: The failure count is cumulated when the fingerprint lock is started next time. If the number of cumulative failures exceeds the threshold, the fingerprint lock will generate an invalid operation alarm; otherwise, the failure count will no longer be accumulated after successful unlocking.

Lock: This parameter is used to set the duration from successful matching to unlocking. Select ***Lock*** and press ***OK*** to display the Lock interface. Press ▲/▼ to select a value. Press ***ESC*** to exit current interface and save your settings. For this parameter, its unit of quantity is 1 second and value range is 3–15, that is, 3–15 seconds.

Note: The unit of quantity and the maximum value of this parameter here are standard configurations. If you need larger parameter values, please consult our commercial representatives or pre-sales technical support engineers.

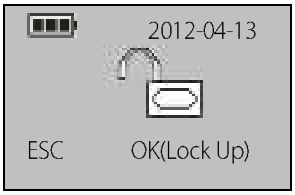
Verify Mode: Press ***OK*** to display the Verify Mode interface, and press ▲/▼ to select a value. There are three optional values 0, 1, and 2 that represent different matching modes respectively, and the default value is 1.

Verify Mode 0: Only the administrator can open the lock, while the unlocking function is disabled for ordinary users.

Verify Mode 1: This is a default matching mode. Users can open the lock by successfully matching their fingerprints only once.

Verify Mode 2: This is a dual verification mode. The administrator can open the lock by successfully matching his/her fingerprint only once, but an ordinary user has to pass the verification in any two matching modes by using the same ID.

Normal Open: Press ***OK*** to display the Normal Open interface, and press ▲/▼ to select ***Yes*** or ***No***. If you select ***Yes***, a prompt will be displayed after unlocking, inquiring whether you desire to select ***Normal Open***. If you press ***OK***, the system will prompt you that the NO function is enabled and then power off automatically and immediately. The Normal Open interface is shown as follows:

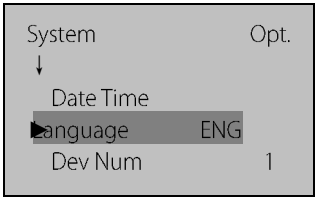


To disable the NO function, power on the system and press ***OK*** in the Normal Open interface. Then the system closes the lock and automatically powers off.

Card Only: Press ***OK*** to display the Card Only interface, and press ▲/▼ to select ***Yes*** or ***No***. If you select ***Yes***, you only need to verify your ID card. +If you select ***No***, you need to verify both your ID card and fingerprint.

3.2 Language Settings

Select "Options" → "System Opt." → "Language" from the main menu to display the following information:

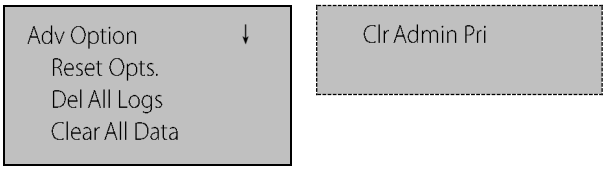


Press ***OK*** to display the Language interface, and press ▲/▼ to select a desired language. Press ***OK*** to confirm your settings and then press ***ESC*** to exit ***System Opt***. When the system prompts whether to save your settings, press ***OK*** and your settings will take effect after system restart.

Note: Language selection is a non-standard function. If you need this function, please consult our commercial representatives or pre-sales technical support engineers.

3.3 Advanced Settings

Notice: Only the super administrator has the right to perform advanced settings. Select "Options" → "System Opt." → "Adv Option" from the main menu to display the following information:



The options under "Adv Option" include: ***Reset Opts.***, ***Del All Logs***, ***Clear All Data***, and ***Clr Admin Pri***. Select any one of these options and press ***OK*** to display the related setting interface. Press ***OK*** according to the prompt to confirm your settings and return to the Adv Option interface, or press ***ESC*** to exit current interface without performing any operation.

Reset Opts.: This parameter is used to restore the fingerprint lock to factory defaults.

Del All Logs: This parameter is used to delete all the verification records from a memory chip.

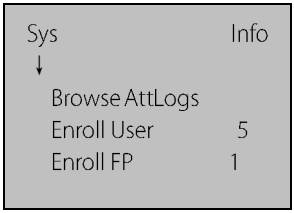
Clear All Data: This parameter is used to delete all the enrolled fingerprint images, passwords and records.

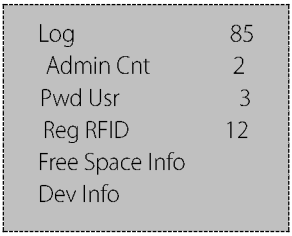
Clr Admin Pri: This parameter is used to change an administrator into an ordinary user. This function shall be used with caution. It is recommended to

register at least one new administrator in time after clearing the priority of an administrator.

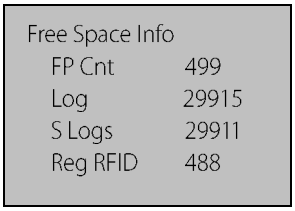
3.4 Browse System Information

Users can browse all the system information, including the enrolled fingerprint counts, enrolled user, and device information. Select "Sys Info" from the main menu, and press ***OK*** to proceed to the next step and display the following information:



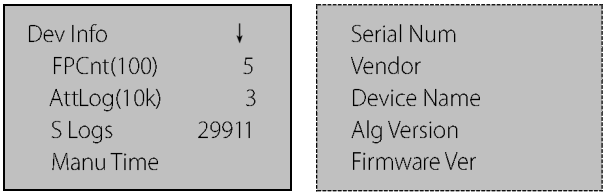


Press ▲/▼ to select ***Free Space Info*** and then press ***OK*** to browse the following information:



Notice: Only the fingerprint locks supporting ID cards are configured with the "Reg FPID" and "Free Space Info" options.

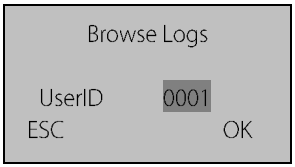
Press ▲/▼ to select ***Dev Info*** and then press ***OK*** to browse the following information:



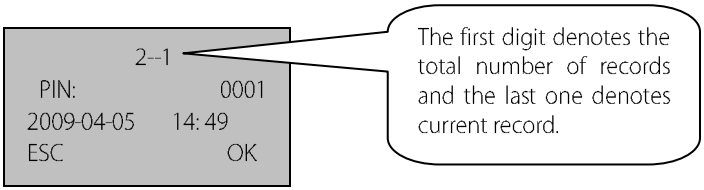
3.5 Browse Logs

The fingerprint locks support the offline browsing of unlocking logs, which facilitates users to check whether there is any exceptional unlocking in time.

Select "Browse Logs" from the main menu to display the following information:



Press ▲/▼ to select a registered number that you want to browse logs and then press ***OK*** to confirm the log date and time:



3.6 USB Pen Drive Management

Step 1： Insert a USB pen drive into the USB interface.

Step 2：Select "PenDrive Mng" from the main menu. Press ***OK*** in the prompt dialog box to display the following interface:

1. Download Attendance Logs

(1)Press ▲/▼ to select "Dwn AttLog" and then press ***OK***. When download completes, the following interface is displayed:

(2)Press ***ESC*** to return to the initial interface and then remove the USB pen drive. Now the USB pen drive stores two files: X_attlog.dat (attendance logs) and X_user (where "X" denotes that the device No. is X).

Tip: If the download succeeds, a prompt "Copy Data Suc" will pop up. If the system displays the prompt "Plug Pen Drive?", please check whether the USB pen drive is plugged in properly.

2. Download User Data

User data downloading is similar to the downloading of attendance logs. Press ▲/▼ to select "DwnLoad User" from the "PenDrive Mng" menu. The files user.dat (user

information) and template.dat (fingerprint template) will be concurrently downloaded to the USB pen drive.

3. Upload User Data

Press ▲/▼ to select "UpLoad User" from the "PenDrive Mng" menu and then press ***OK***. The files user.dat (user information) and template.dat (fingerprint template) stored in the USB pen drive will be concurrently uploaded to the fingerprint lock.

😐***Tip***: If a user exits with the same ID in the fingerprint lock, the new upload will overwrite the existing user data; otherwise, the new user data will be directly added.

4. Upgrade Firmware

You can select "Upd Firmware" to upgrade the firmware of a fingerprint lock through the upgrade files in the USB pen drive.

☺***Notice***: If you need firmware upgrade files, please contact our technical support engineers. Generally it is not recommended to upgrade the firmware.

😐***Tip: Please do not perform invalid operations (for example, insert or remove the USB pen drive in a frequent manner or during upload/download) on the USB pen drive, because it may result in system instability. It is recommended to keep the door open during the use of the USB pen drive.***

4. Conventions on Other Functions

4.1 Routine Operation Indications

User operation success indication: The buzzer sounds once and the green LED indicator is solid on for 3 seconds.
User operation failure indication: The buzzer sounds short tone twice and the red LED indicator is solid on for 3 seconds.
Warning indication: The buzzer sounds short tone five times intermittently.

4.2 Administrator Loss Prevention

To avoid the menu operation failure as a result of loss of administrator, you may take the following measures: Press and hold the ***Menu*** key for 3 seconds to display the administrator verification interface. Then move the band switch on the rear of the fingerprint lock to the left or right. Now you can access the menus as super administrator for management and operation.

4.3 Battery Low Voltage Protection

Low Voltage Protection: When the battery meter stays at one bar, the system prompts you to replace the battery and the battery icon starts flashing. If you press and hold the ***Menu*** key, the system prompts you that you cannot access menus. In addition, the menus are also inaccessible during use of external power so as to prevent data loss caused by power instability. When the battery meter stays less than one bar, the battery shuts itself off automatically.

4.4 Automatic Program Exit and System Power-off

- The fingerprint lock powers off automatically upon successful matching and unlocking.
- The fingerprint lock powers off automatically when you set ***Yes*** for the "Normal Open" option upon unlocking.
- The fingerprint lock powers off automatically when the number of invalid operations exceeds the threshold. The fingerprint lock powers off automatically when an alarm is generated for 30 seconds upon restart.
- The fingerprint lock powers off automatically when the supply voltage is lower than level-3 detection voltage.
- The fingerprint lock powers off automatically if there is no keystroke within 10 seconds on the initial interface.

4.5 External Power Use Description

The fingerprint lock supports temporary use of external DC power for fingerprint or password matching and unlocking, but when connected with an external battery, the fingerprint lock cannot provide such special functions as enrollment, deletion and setting, so as to prevent data loss as a result of power instability.

As shown in the figure below, connect a 9V battery to the two access points at the bottom of a fingerprint lock, regardless of polarity.

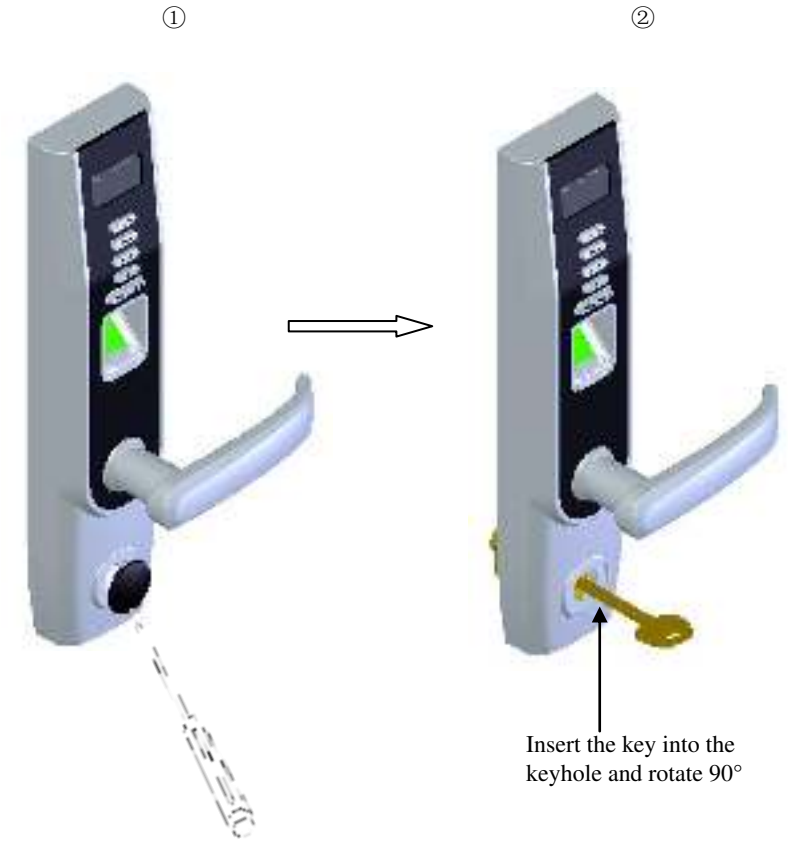
If you power off a fingerprint lock without closing the lock during the use of external power, the lock cylinder will not automatically return to its original position. That is, the fingerprint lock remains in NO state. To solve this problem, you can replace the battery and then open the lock once to have the lock cylinder in position.

4.6 Unlock With an Emergency Mechanical Key

You can open the door using an emergency mechanical key in case the electronic component does not operate.

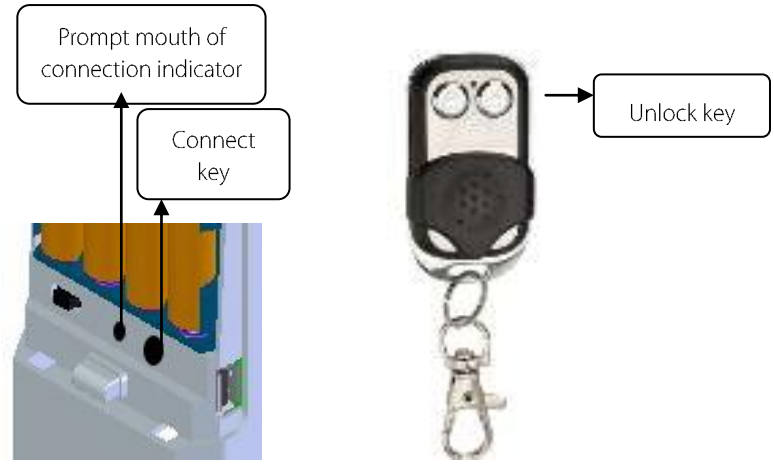
1. Pry open the keyhole cover by inserting the sharp end of a ball-pen or screwdriver with a diameter of less than 3 mm. Remove the cover.

2. Insert the emergency key into the keyhole and rotate 90° to unlock.



4.7 Remote Unlock★

On power-off mode, some devices have remote unlock function. The user can remotely unlock the door by using the remote control. (Keep the remote unlock distance within the line of sight of the device, not exceeding 10 m.) Before enabling remote unlock function, you must connect the device to the remote control to build up communication relationship between the remote control and the device.



1. Device Connection

The specific procedure is as follows:

(1)Press the Connect key on the rear of the device (as shown in the preceding figure) until the connection indicator blinks once.

(2)Press the Unlock key on the remote control (as shown in the preceding figure) and the connection indicator will continuously blink in certain frequency.

(3)Press the Connect key again and the connection indicator will be off.

(4)Press Unlock key and the connection indicator will continuously blink in a faster frequency. When the connection indicator no longer blinks, device connection is complete.

☺***Note***: Both the remote control and device support one-to-many connection (up to one-to-four). That is, a remote control can connect to up to four devices and a device can connect to up to four remote controls.

2. Device Unlock: After the device is connected to the remote control and is powered off, long-press Unlock key of the remote control for about 3 seconds until the green light of the fingerprint collector blinks. When the screen displays unlock pattern, the device is unlocked. Then the device is powered off automatically. For the duration from unlock to power-off, refer to Section 3.1 Operation Settings to set the lock driver duration.

Note:

(1)When the device is powered on, the remote unlock function is unavailable.

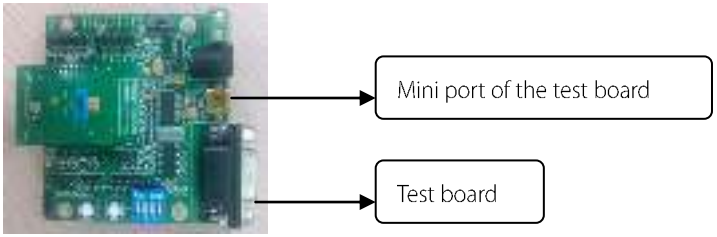
(2)During remote unlock, do not press any key.

4.8 Zigbee Real-time Monitoring★

The device with Zigbee real-time monitoring function can realize communication between the lock and PC through the Zigbee communication module. Then the user can monitor the unlock status in real time on the PC end.

The specific procedure is as follows:

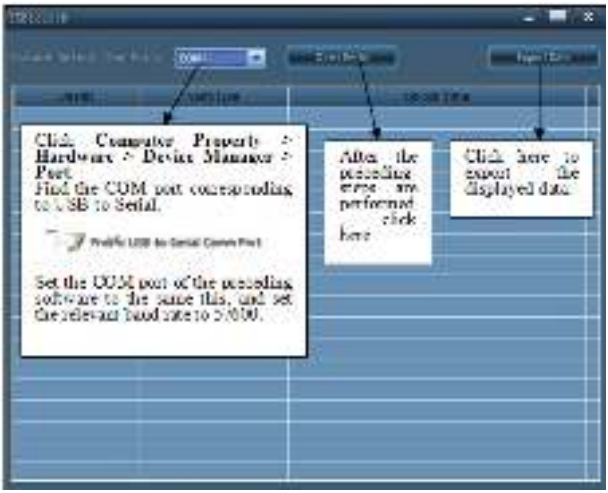
1. Connect the mini port of the USB line to the mini port of the test board. (The other port of the USB line is connected to the PC.) Then the a red indicator and three green indicators on the test board are lightened.



Note: When the first time you enable this function, a tip of installing new

hardware is display in the Toolbar on the desktop of the PC. You just need to install the USB driver  according to the tips.

2. Double click  to open the communication lock display software. The window is as follows:



According to the figure to set the software before using.

After the device is powered on and the user is verified by the fingerprint, password or scanning the card, the software display the user's (who unlocks the device) information, such as ID, verification type, unlock date and time. This software supports sequencing by unlock time, ID, verification type. You can just click the corresponding area (such as ***UserID***, ***VerifyType*** or ***Unlock Time***) to sequence the information.

☺***Note***: If no information is displayed after the user is verified, firstly check that the software information (such as the communication COM port and baud rate) is set

completely before using. Then check the COM port. It is not recommended to use the ports after COM10. If a port after COM10 is assigned automatically, modify it manually.

Appendix

Technical Specifications

- Display ： OLED display
- Sensor: Optics sensor without coating
- Capacity: 300 fingerprint images; 100 passwords; 300 users.
- Matching mode: Fingerprint only , password only, MF card only, ID card only, combination of fingerprint and matching password, combination of fingerprint and matching card.
- Record capacity: 30000
- Communication： USB Flash Disk
- Resolution: 500 DPI
- Identification speed: ≤ 2 seconds
- False acceptance rate: ≤ 0.0001%
- False rejection rate: ≤ 1%
- Power: Four AA batteries; working voltage: 4.2V–6V.
- Locking count: ≥ 4000 (Four NANFU alkaline batteries)
- Temperature: 0–45℃
- Humidity: 10%–80%

This document is subject to change without prior notice.

Printed in China