

L9000 Fingerprint Lock User Manual

Version: 1.0

Date: 2011.10

About This Manual

This manual introduces the fingerprint lock interface and menu operations about L9000. For the fingerprint lock installation, browse the animated installation instructions.

Important Claim

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

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

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

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

Table of Contents

1	Instruction for Use.....	1
1.1	Introduction to Fingerprint Lock Functions	1
1.2	List of Installation Accessories	3
1.3	Installation Requirements	5
1.4	Front and Rear Views.....	7
1.5	Precautions.....	10
1.6	User Privileges.....	11
1.7	Set Time	12
2	Enrollment and Verification.....	14
2.1	Enroll an Administrator.....	14
2.1.1	Enroll a Fingerprint.....	15
2.1.2	Enroll a Password	17
2.2	Enroll an Ordinary User.....	20
2.3	Backup Enrollment	21
2.4	User Verification and Set Normal Open Status	22
2.5	Delete User Data.....	24
3.	Lock Function Information and Settings.....	27
3.1	Operate Option.....	27
3.2	System Options.....	29
3.2.1	Set Language.....	29
3.2.2	Set Device Number	30
3.2.3	Advance Option.....	31
3.3	USB Pen Drive Management.....	32
3.3.1	Download Logs	34

3.3.2 Download User Data	35
3.3.3 Upload user Data	35
3.3.4 Upgrade Firmware.....	35
3.4 System Information.....	36
3.4.1 Browse AttLogs.....	37
3.4.2 Free Space Information	38
3.4.3 Device Information.....	39
4 Conventions on Other Functions.....	40
4.1 Routine Operation Indications	40
4.2 Administrator Loss Prevention.....	40
4.3 Automatic Program Exit and System Power-off	40
4.4 Use Description of External Power.....	42
4.5 Unlock With an Emergency Mechanical Key	43
4.6 Alarm of Malicious Detection.....	44
4.7 Battery Low Voltage Protection	44
Appendix	45
Appendix 1 Introduction of Verification Mode 2	45
Appendix 2 Technical Specifications	46

1 Instruction for Use

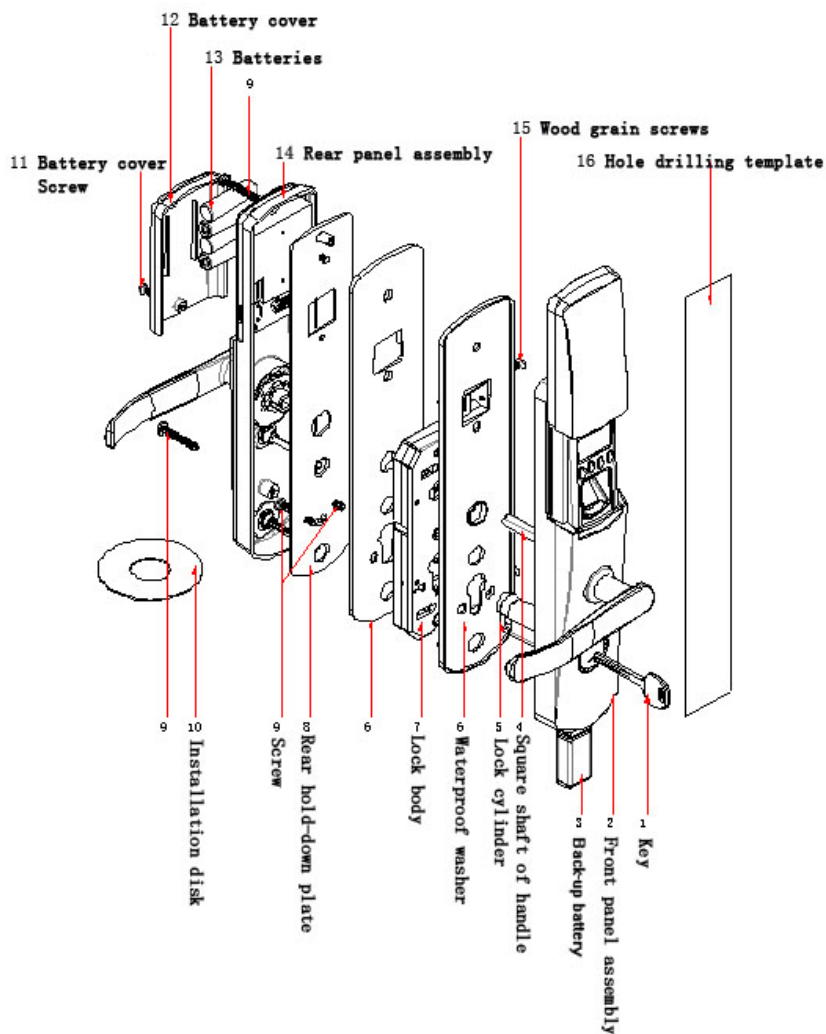
Functions marked with "★" in this manual are only supported by a specific product or a tailor-made product and will be described below.

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 Multi language, firmware upgrade and uploading/downloading of user information and access records through a USB disk.
6. Fingerprint verification module and password registration; 1: N is used for the password, and each password is unique.
7. Dual verification function, i.e., fingerprint + fingerprint or fingerprint + password.
8. The opening records can be viewed in offline status. In the menu, all opening records of the selected user can be directly viewed, in order to find abnormal opening situation.
9. Support accurate display of time and date with annual deviation less than two minutes.

10. Support a temporary connection with back-up batteries.
11. The lock could be set in Normally Open (NO) state in special use.
12. Support display of the battery charge level and generation of low-pressure alarms.
13. Feature an electric clutch handle design which effectively prevents the fingerprint lock failure caused by damage to the internal structure as a result of the forced destruction of the handle.
14. Latch bolt alarm function; if the user is verified successfully and the door is opened, the latch bolt cannot normally eject and is being in the false locking status due to mechanical fault or dislocation of the door being closed, the screen will prompt the user that the door is not properly closed and the buzzer will give an alarm for 5s.
15. **CLOSE DOOR★**: The door is closed after successfully verification. If the door is not properly closed for a period of time, then the screen will remind the user to close the door and the buzzer will give a brief alarm.
16. **Electrical auto locking function**; after the user is verified successfully, the unlocking is executed, i.e., the handle is twisted, the electrical auto locking will be initiated; that is, one comparison is only useful for one unlocking, to prevent the user from being tailed after.
17. **Lost administrator resistant function**; if the administrator is lost due to certain reasons and the menu cannot be entered, the user can press the menu key for 2s, in order to display the administrator verification, and then use the mechanical key to unlock, i.e., the user can act as super-administrator to enter the menu screen to manage the operation.
18. **Abnormal comparison alarm function** is supported, to avoid malicious detection of the password.
19. The door can be locked at the other side by means of raising the handle upward. The size of lock body is the same as that of GB6068 mechanical burglarproof.

1.2 List of Installation Accessories



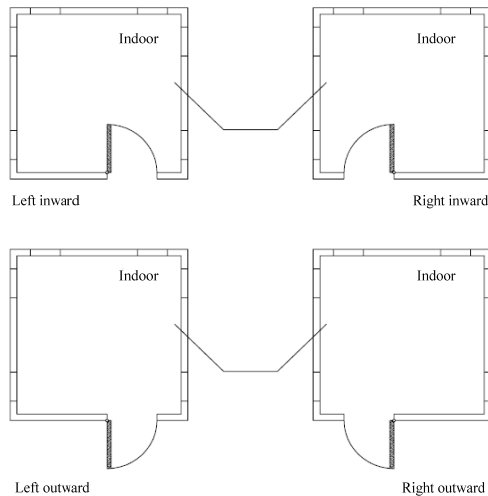
List of Installation Accessories

SN	Name	Quantity	Unit	Remarks
01	Key	2	PCS	
02	Front panel assembly	1	Set	
03	Back-up battery	1	PCS	9V
04	Square shaft of handle	2	PCS	
05	Lock cylinder	1	Set	With the lock cylinder screw
06	Waterproof washer	2	PCS	
07	Lock body	1	Set	
08	Rear hold-down plate	1	PCS	
09	Screw	5	PCS	
10	Installation disk	1	PCS	
11	Battery cover Screw	1	PCS	
12	Battery cover	1	PCS	
13	Batteries	4	PCS	Four pieces of alkaline AA batteries
14	Rear panel assembly	1	Set	
15	Wood grain screws	2	PCS	
16	Hole drilling template	1	PCS	

1.3 Installation Requirements

Precautions:

1. The fingerprint lock is applicable to door thickness from 50 to 80mm. 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. Please make sure of the door opening directions and lock body directions, the lock body's outside and inside can't be set contrary. 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:



3. Ensure the central point of the handle is 1m above the floor.
4. Please follow the animated instructions to install fingerprint locks.

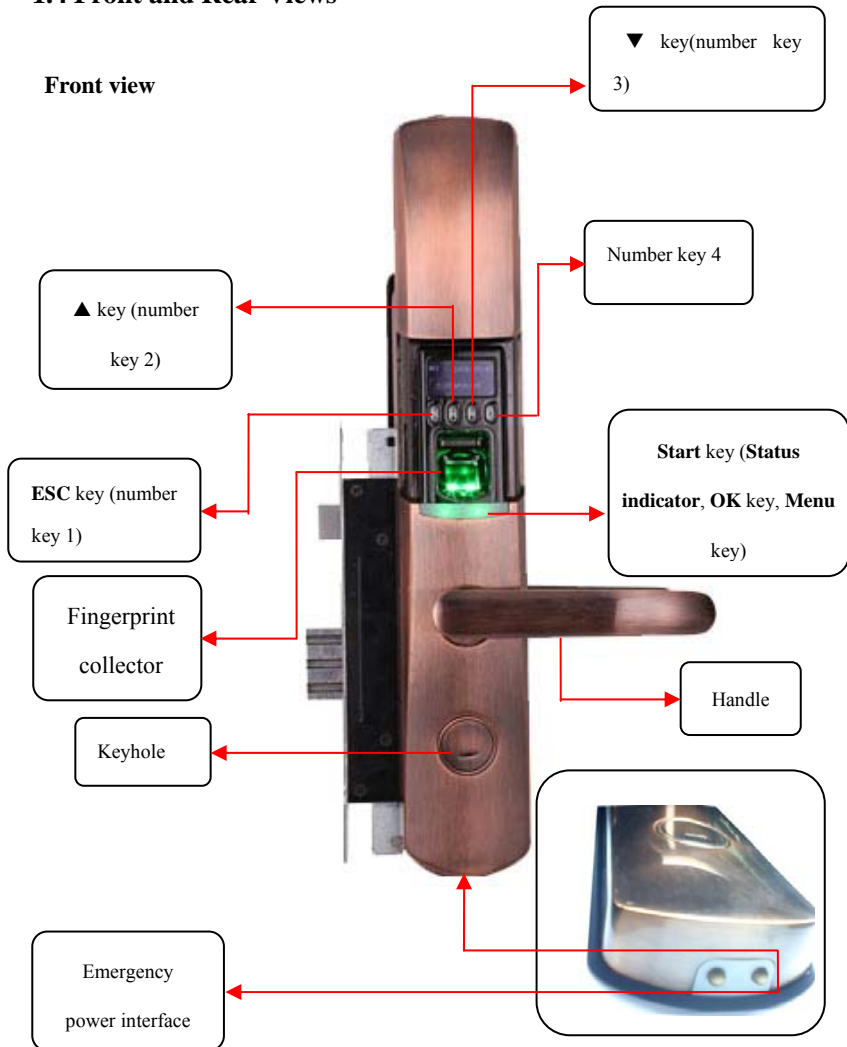
Recommended Tools

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

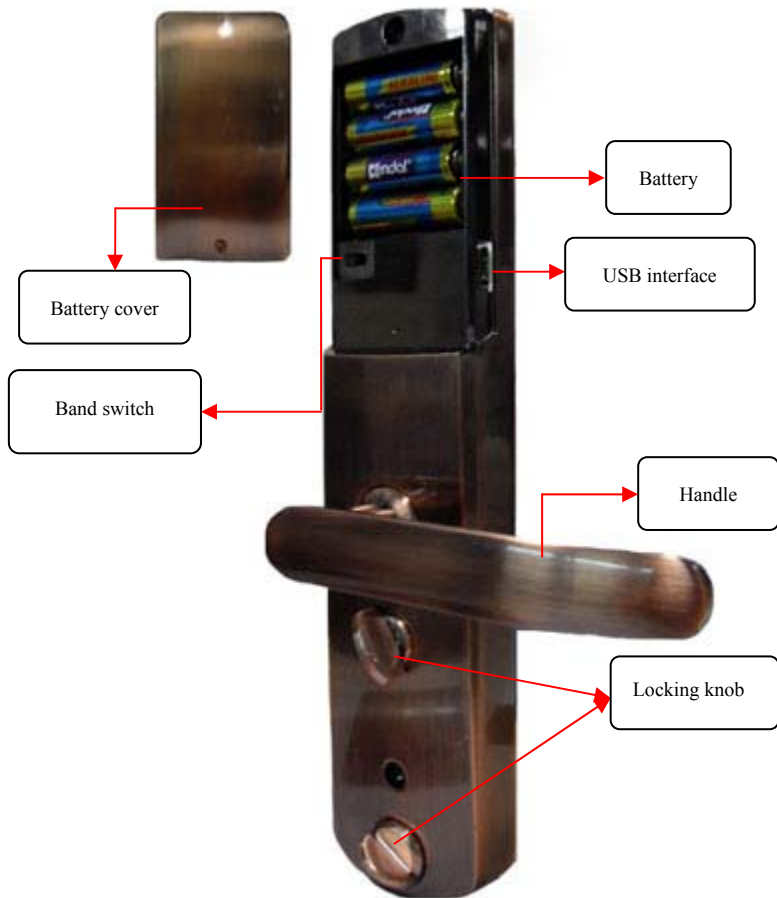
- A ruler.
- A marker pen.
- A drilling tool.
- A cross screwdriver.

1.4 Front and Rear Views

Front view



Rear view



ESC key: The first function is ESC key, mean quit the current operation; the second function is used as the number key "1". Hold this key to power off the fingerprint lock

▲ Key: The first function is increase key, when held, this key will rapidly increase display values or menu item; the second function is used as the number key "2".

▼ **Key:** The first function is decrease key, when held, this key will rapidly decrease display values or menu item. The second function is used as the number key "3".

Number 4 Key: The first function is used as number key "4"; the second function is after the comparison unlocking is successful; the key can be used to set the normal open function and can be used as **OK** key when the door is locked.

Start Key: This key can be used to start the fingerprint lock. If didn't enroll administrator or super administrator, then press and hold this key for five seconds on the initial interface to open the menu options; this key also used as the confirmation (<**OK**>) key, **Menu** key and **Status indicator**.

Band switch: Be located at the back of the lock. This switch can use for switching the purpose of USB Interface, USB Pen Drive or WIFI modular and so on.

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. You also can choose other color. For example: red, white or blue and so on.

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.



Note: 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.

Keyhole: You can use a mechanical key for emergency door opening.

Emergency 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 enroll at least 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.

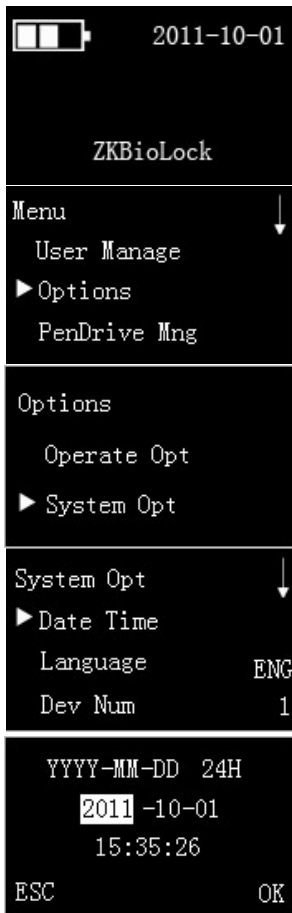
Super administrator (Supervisor): Refer to users who have access to all system functions and modify all system settings.

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

Ordinary user: 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 1 on the left.

Note: 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 five seconds to access the **Menu** interface. Press ▼ key to select **Options** menu item and press **OK** key to display the setting interface. As shown in the figure 2 on the left.

3. Press ▼ key to select **System Opt** menu item on the **Options** interface, as shown in the figure 3 on the left. And then press **OK** key to display **System Opt** interface. As shown in the figure 4 on the left.

4. Press **OK** key to display **Date Time** interface, as shown in figure 5 on the left.



5. Press ▲/▼ key to input right year, and then press **OK** key to confirm, the cursor will automatically switch to month. According to the method of setting year set date and time. Press **OK** key to save. The interface shows "Working...". As shown in figure 1 on the left. After the completion automatically return to the **System Opt** interface.

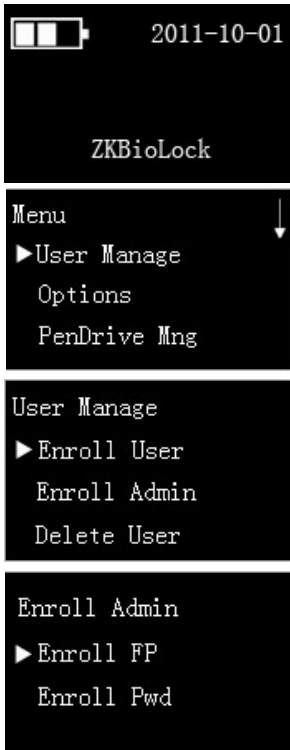


Note: You can set the date between January 1st 2003 and December 31st 2032. To set the date beyond this range, you need to consult our commercial representatives or pre-sales technical support engineers.

2 Enrollment and Verification

2.1 Enroll an Administrator

If the fingerprint lock has no administrator, then you can't enroll ordinary users. Because of the administrator can't enroll super administrator, and only the super administrator can set Advanced Option (**Adv Option**), so 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 display the initial interface. As shown in figure 1 on the left. Press and hold the **Menu** key to display the **Menu** interface. As shown in figure 2 on the left.
2. Press **▲/▼** key to move the cursor before the **User Manage** menu item, and then press **OK** key to display the **User Manage** interface, as shown in figure 3 on the left.
3. Press **▼** key to select **Enroll Admin** menu item, and then press **OK** key to display **Enroll Admin** interface, as shown in figure 4 on the left.

The next step is to enroll fingerprint and password for super administrator. Please see **2.1.1 Enroll a fingerprint** and **2.1.2 Enroll a password**.

2.1.1 Enroll a Fingerprint

```

Enroll Admin
► Enroll FP
  Enroll Pwd
  
```

```

Admin Accredit
  Supervisor
ESC                      OK
  
```

```

New Enroll
  UserID 00001
ESC                      OK
  
```

```

New Enroll
  00001-0
Place Finger...
  ESC/Exit
  
```

Note: 1-3 steps are same as above. Here is no longer to restate.

4. Choose **Enroll FP** on the **Enroll Admin** interface. As shown in figure 1 on the left. Press **OK** key to display **Admin Accredit** interface, as shown in figure 2 on the left.

5. Press **▲/▼** key to select the type of admin accredit, can select as **Supervisor** or **Admin**. Press **OK** key to confirmation; or press **ESC** key to exit, and return to the **Enroll Admin** interface.

6. Choose the type of admin accredit as Supervisor. Press **OK** key to display **New Enroll** interface, as shown in figure 3 on the left. The default User ID is 00001 that is the first User ID. You also can press **▲/▼** key to select the unused User ID; press **ESC** key can give up operation, and then return to the **Enroll Admin** interface.

7. Press **OK** key to start enroll. According to the interface prompts "Place Finger", "Remove Finger",

"Second Press", "Remove Finger", "Third Press", "Remove Finger", and press the same finger on the **Fingerprint Collector** three consecutive times by adopting the proper finger placement mode. As shown in figure 4 on the left.



Note: 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.

```
New Enroll
00001-0
ESC          OK (Save)
```

```
New Enroll
00001-0
Input Again
ESC/Exit
```

```
New Enroll
Continue?
ESC          OK
```

```
Backup Enroll
UserID 00001
ESC          OK
```

```
Backup Enroll
00001-1
Place Finger...
ESC/Exit
```

8. The system will prompt you to save the enrollment information after you enroll the fingerprint successfully. As shown in figure 1 on the left. If enrollment fails, the system will prompt "Input Again", as shown in figure 2 on the left.

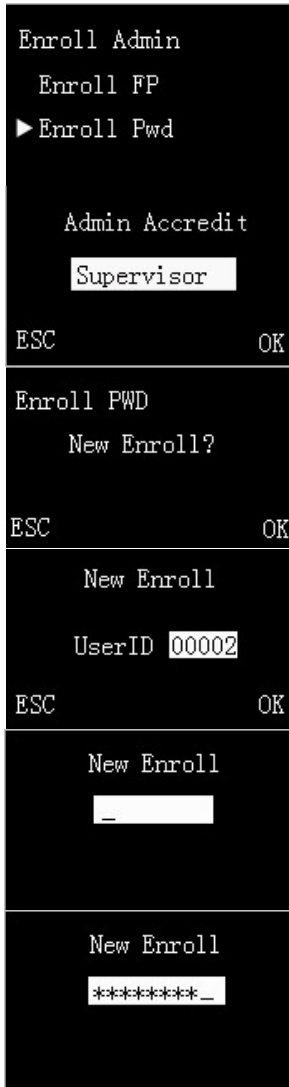
9. Press **OK** key to save, and return to the **New Enroll** interface, as shown in figure 3 on the left. Prompt "Continue?" on the interface, choose whether to continue enroll.

10. Press **OK** key to continue enroll administrator; or press **ESC** key to enter backup User ID selection interface, you can press **▲/▼** key to choose User ID. As shown in figure 4 on the left.

11. Press **OK** key to enter the **Backup Enroll** interface, as shown in figure 5 on the left; or press **ESC** key to return **User Manage** interface.

12. The steps about backup enroll are same as step 7-9, here is no longer to restate.

2.1.2 Enroll a Password



Note: 1-3 steps are same as above. Here is no longer to restatement.

4. Selecting **Enroll Pwd** menu item on the **Enroll Admin** interface, as shown in figure 2 on the left. Then press **OK** key to display **Admin Accredit** interface.

5. Press **▲/▼** key to select the type of admin accredit, you can select as Supervisor or Admin. Press **OK** key to display **Enroll PWD** interface, the interface prompts "New Enroll?" as shown in figure 3 on the left; or press **ESC** key to quit, and then return to **Enroll Admin** interface.

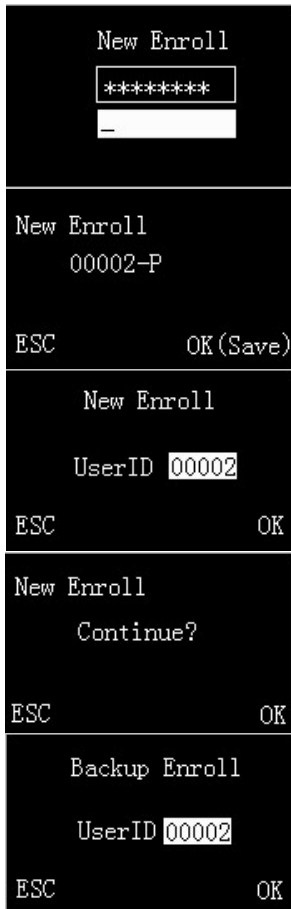
6. Press **OK** key on the **Enroll PWD** interface to enter new enroll user ID selection interface. As shown in figure 4 on the left.

(1) The default new enroll user ID is from 00001 begin incrementing the unused ID, you also can press **▲/▼** key to select unused ID. Because of the **2.1.1 Enroll a fingerprint** has added a user ID as 00001, so the new enroll interface display the user ID is 00002. Press **OK** key to enter **New Enroll** interface, as shown in figure 5 on the left; or press **ESC** key to quit, and then return to the **Enroll Admin** interface.

(2) Press the number key to input password, as shown in figure 6 on the left. Number entered by

the user will be automatically replaced with * display.

Note: A password consists of 6 to 10 digits. You can enroll only one password for each user ID and repeated passwords are not allowed.



(3) Press **OK** key to confirmation, and then enter the input interface of confirm password, as shown in figure 1 on the left. Repeat the password has input at step (2), press **OK** key to enter the interface of save confirmation, as shown in figure 2 on the left. Letter P namely password.

Note: If the input passwords do not same as the password input at step (2), then press **OK** key to input again.

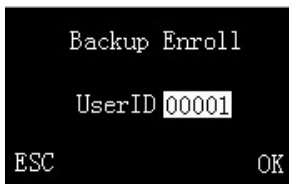
(4) Press **ESC** key to give up operation and return **New Enroll** interface, as shown in figure 3 on the left. If you need to continue enroll, and then repeat step (1) to (3); or press **ESC** key to quit, and then return to the **Enroll Admin** interface. On the interface as shown in figure 2 on the left, press **OK** key to save the enroll information and enter the **New Enroll** interface, the interface prompts "Continue?", as shown in figure 4 on the left.

(5) If you want to continue, then press **OK** key, and then repeat step (1) to (3); or press **ESC** key to cancel, and then return to the interface of **Backup Enroll**. As shown in figure 5 on the left.



(6) Press **OK** key to enter the input password interface of backup enroll, as shown in figure 1 on the left. The operation is same as input password of new enroll, here is no longer to restatement.

Tips: The backup enroll password will replace the original password.



7. On the interface of **Enroll PWD**, press **ESC** key to cancel new enroll, and then enter the interface of **Backup Enroll**, as shown in figure 2 on the left.

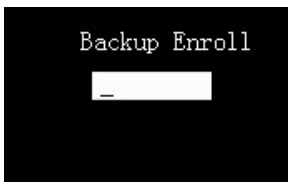
(1) The default user ID is 00001, press **▲/▼** key to switching between the enrolled User ID, you can

select as you need.

Note: The super administrator (Supervisor) has the purview of backup password for itself, all administrators (non supervisor) and all ordinary users. The administrator (Admin) has the purview of backup password for itself and all ordinary users.



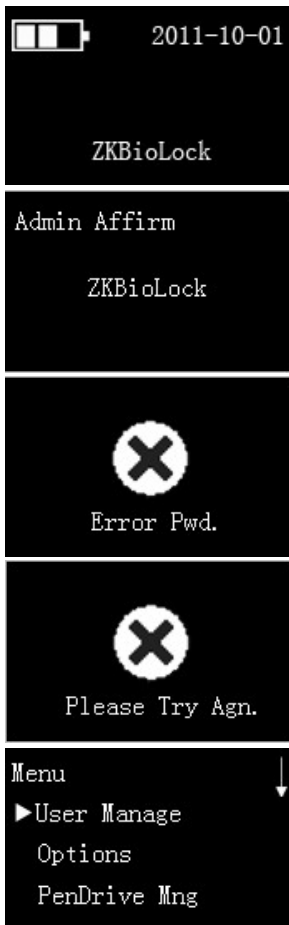
(2) After select user ID, press **OK** key to start backup. If you don't have the backup purview of the user ID you chose, the interface will prompts "Access Deny", as shown in figure 3 on the left. It will automatically return to the **Enroll Admin** interface after three seconds. If you have the purview, then enter the input password interface of backup enroll. As shown in figure 4 on the left.



Note: The backup enroll password will replace the original password, namely modify password.

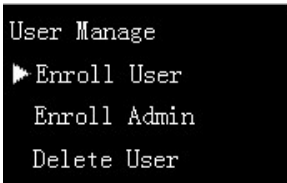
2.2 Enroll an Ordinary User

Note: The super administrator (Supervisor) can enroll supervisor, administrator (Admin) and ordinary user, but the administrator only can enroll admin and ordinary user.



The steps about enroll ordinary user are as bellow:

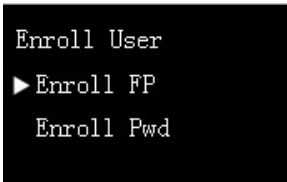
1. Power on the fingerprint lock by pressing the **Start** key to enter the initial interface. As shown in figure 1 on the left.
2. Press and hold the **Menu** key for five seconds to enter the **Admin Affirm** interface, as shown in the figure 2 on the left. Input the administrator password or put finger on the **Fingerprint Collector** to verify. Skip to step 4 if verification succeeds; otherwise, proceed to step 3.
3. If the interface prompts "Error Pwd.", as shown in figure 3 on the left, or prompts "Please Try Agn.", as shown in figure 4 on the left, then return to the **Admin Affirm** interface to verify again, till verification succeeds. The **Menu** interface is displayed upon successful verification.
4. If it is password verification, then after input right password, you should press **OK** key to enter **Menu** interface; if it is fingerprint verification, then after press right fingerprint, will enter **Menu** interface automatically. The **Menu** interface is shown as figure 5 on the left.

A screenshot of a terminal window showing a menu titled "User Manage". Below the title, there are three options: "Enroll User", "Enroll Admin", and "Delete User". A cursor is positioned at the beginning of the "Enroll User" line.

```
User Manage
▶ Enroll User
  Enroll Admin
  Delete User
```

5. Select **User Manage** menu item, press **OK** key to enter the **User Manage** interface, and then press **▲/▼** key to put the cursor before the **Enroll User** menu item, as shown in figure 1 on the left.

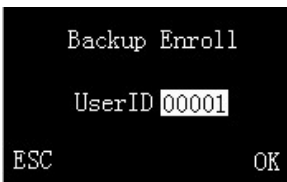
6. Press **OK** key to enter the **Enroll User** interface, as shown in figure 2 on the left.

A screenshot of a terminal window showing a menu titled "Enroll User". Below the title, there are two options: "Enroll FP" and "Enroll Pwd". A cursor is positioned at the beginning of the "Enroll FP" line.

```
Enroll User
▶ Enroll FP
  Enroll Pwd
```

The following you can enroll fingerprint and password. The steps are same as enroll administrator, but do not have the step about admin accredit, for detail please see **2.1 Enroll an Administrator**.

2.3 Backup Enrollment

A screenshot of a terminal window showing the "Backup Enroll" interface. It displays "UserID 00001" with a cursor at the end of the number. At the bottom left is "ESC" and at the bottom right is "OK".

```
Backup Enroll

UserID 00001
ESC                                OK
```

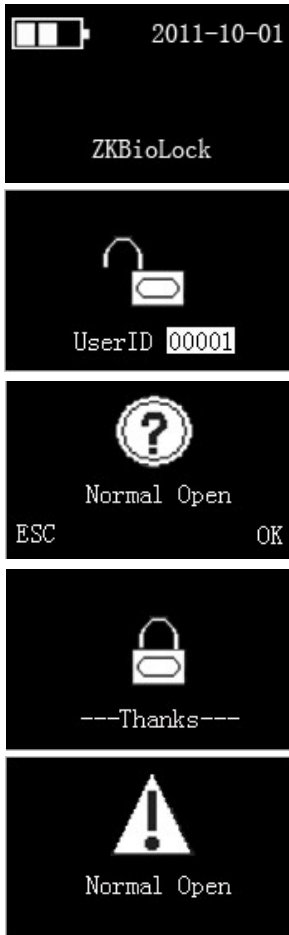
On the **New Enroll** interface, if you press **ESC** to cancel new enrollment, then the **Backup Enroll** interface will be displayed, as shown in the figure 3 on the left.

The steps about **Backup enroll** are same as **New enroll**. The different is the interface display **Backup Enroll** but not **New Enroll**. In the preceding chapters have described, here is no longer to restate.

Note:

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.

2.4 User Verification and Set Normal Open Status



1. Press the **Start** key to display the initial interface. As shown in figure 1 on the left. The **Fingerprint Collector** is in active state.

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

Note: You can only match fingerprints when the fingerprint lock is not on Normal Open status.

3. Your ID number and unlock icon will be displayed on the screen upon successful verification, as shown in figure 2 on the left, and then you can hear the unlocking sound. Rotate the handle of the fingerprint lock within 5 seconds to open the door.

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

4. The screen will prompt whether set Normal Open, as shown in figure 3 on the left. If press **ESC** key, the fingerprint lock will be locked automatically. The Unlock icon on the screen will change into the Lock icon, as shown in figure 4 on the left, and the

system powers off automatically.

5. If you press **OK** key, indicating successful Normal Open setting. The screen displays the Normal Open icon, as shown in figure 5 on the left. At the same time,

the buzzer will beep three consecutive times.



Note: The "5 seconds" mentioned in the document, namely **Lock (lock actuator time)**. You can modify it for need. For detail please see **3.1 Operate Option**.

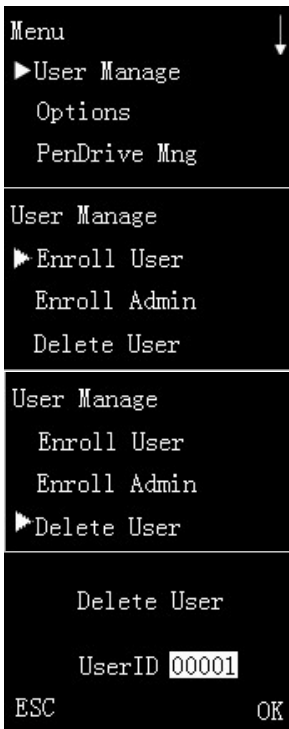
If fingerprint or password verification is unsuccessful, the system will display a prompt "Please Try Agn." or "Error Pwd.". The parameters **Illegal Times** and **Operate Alarm** are set by the administrator. The system will generate an alarm after the illegal operations reach the specified value. For details, see **3.1 Operate Option**.



Note: For example, set the value of the parameter **Illegal Times** as "6". The system will automatically power off if you fail to verify your fingerprint or password 6 consecutive times. Power on again, the buzzer will be intermittent tweets to alarm, after 30 seconds, will automatically power off.

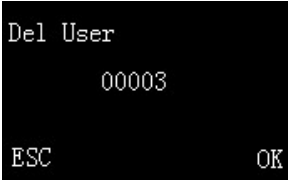
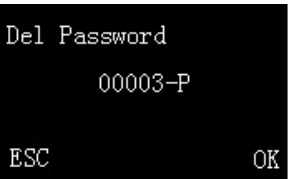
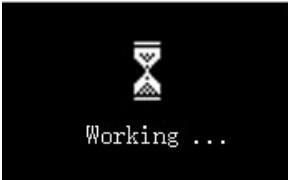
2.5 Delete User Data

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.



The steps shown as bellow:

1. Press the **Start** key to power on the fingerprint lock and then enter the initial interface.
2. Press and hold the **Menu** key for five seconds to enter the **Admin Affirm** interface. Enter the Menu interface after verification succeeds, as shown in figure 1 on the left. The steps about admin affirm, please see step 2-4 in **2.2 Enroll an Ordinary User**.
3. The cursor is before the **User Manage** menu item. As shown in figure 1 on the left. Press **OK** key to enter **User Manage** interface, as shown in figure 2 on the left.
4. Press **▲/▼** key to move the cursor before the **Delete User** menu item, as shown in figure 3 on the left.
5. Press **OK** key to enter the **Delete User** interface, as shown in figure 4 on the left.



6. Press ▲/▼ key to choose the User ID that you want to delete. Press ▲ key to increase, or press ▼ key to decrease.

Take User ID 00003 as an example. When the user simultaneously enrolls the **fingerprint** and **password**, the system will first automatically enter the **Del fingerprint** screen; please refer to Step 7; then enter the **Del password** screen; please refer to Step 8. If the user doesn't enroll the fingerprint, the system will directly enter the **Del password** screen; if the user doesn't enroll password, after **Del fingerprint** in Step 7 is completed, the system will directly enter Step 9, namely enter the **Del user** screen.

7. Press ▲/▼ key to choose user ID as 00003. Press **OK** key to enter the confirm interface of

Delete Password, as shown in figure 1 on the left. Press **OK** key to delete, the interface will prompt "Working..." as shown in figure 2 on the left. It will enter **Del Password** interface after delete successful, as shown in figure 3 on the left.

8. Press **ESC** key to cancel delete operation and return to the **User Manage** interface; or press **OK** key to delete password and enter the **Del User** interface, as shown in figure 4 on the left.

9. Press **OK** key to delete this user and return to the **User Manage** interface; or press **ESC** key to cancel and return to the **User Manage** interface.

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

Note: The supervisor can delete ordinary user and admin, but admin only can delete ordinary. To delete a Supervisor User ID, you need to select "Options" → "System Opt." → "Adv Option" → "Clr Admin Pri", and then select "User Manage" → "Delete User" to delete the ID.

3. Lock Function Information and Settings

3.1 Operate Option

Select "**Options**"→"**Operate Opt**" from the **Menu** interface to display the following information:

Operate Opt	↓	Operate Opt	↑
▶ Operate Alarm	Y	Verify Mode	1
Illegal Times	10	Normal Open	Y
Lock	5	▶ CLOSE DOOR	N

The options under "**Operate Opt**" include: **Operate Alarm**, **Illegal Times**, **Lock**, **Verify Mode**, **Normal Open** and **CLOSE DOOR**★.

Operate 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. This function can prevent the risk about unregistered users continuous try alignment generated mistaken opening.

Illegal Times: 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, then press ▲/▼ key to select value. Press **ESC** key 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** key to display the setting interface, and then press **▲/▼** key to select the 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 or password only once.

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

Appendix 1 Introduction about Verify Mode 2.

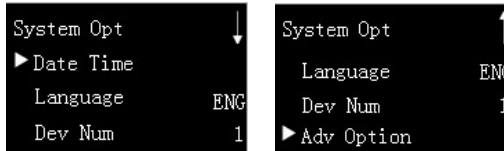
Normal Open: Press **OK** key to display the Normal Open setting interface, and press **▲/▼** key to select **Y** (Yes) or **N** (No). If you select **Y**, a prompt will be displayed after unlocking, inquiring whether you desire to select Normal Open. For detail, please see **2.4 User Verification and Set Normal Open Status**.

To disable the Normal Open function, power on the system and press **OK** key in the Normal Open interface. Then the system closes the lock and automatically powers off.

CLOSE DOOR★: Press **OK** key to enter the setting interface, and then press **▲/▼** key to select **Y** or **N**. If select it as **Y**. **Door closing prompt:** When the user is verified successfully and the door is opened, if the door is not closed for a period of time, the screen will prompt the user to close the door and the buzzer will give a brief alarm.

3.2 System Options

Select "**Options**" → "**System Opt**" from the **Menu** interface to display the following information:



The options under "**System Opt**" include: **Date Time**, **Language**, **Dev Num**, and **Adv Option**.

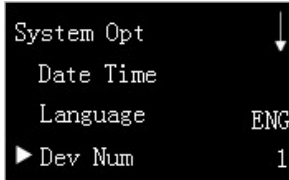
Note: The method about setting Date Time, please see **1.7 Set Time**.

3.2.1 Set Language

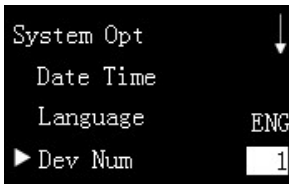


1. Select "Options" → "System Opt." → "Language" from the **Menu** interface, as shown in figure 1 on the left.
2. Press **OK** key to enter setting interface, and then press **▲▼** key to select language, as shown in figure 2 on the left.
3. Select the language type you want. Press **OK** key to confirm, and then press **ESC** key to quit system options, the system will prompt you to save, as shown in figure 3 on the left. Press **OK** key to save. Please restart the device, to take effect.

3.2.2 Set Device Number



1. Select "Options" → "System Opt." → "Dev Num" from the **Menu** interface, as shown in figure 1 on the left.



2. Press **Ok** key to enter setting interface, and then press **▲/▼** key to select device number, as shown in figure 2 on the left. The range of device number is 1-255.

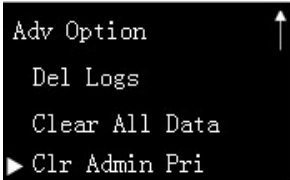
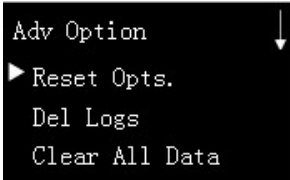
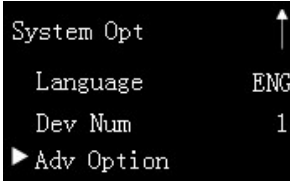
3. Press **OK** key to confirming the selected device number, and then press **ESC** key to quit **System Opt**. The system will prompts you to save. The operation is same as **2.1.1 Set Language**, here is no longer to restatement.



Note: When the user uses the USB flash disk to export the device records, the name of the exported file contains the device number in order to differentiate the data recorded by different devices. Therefore, the user shall set different device numbers for different fingerprint locks to avoid confusion, if the records are downloaded simultaneously from multiple devices.

3.2.3 Advance Option

Note: Only the **Supervisor** have the purview of **Advance Option**.



1. Select "Options" → "System Opt." → "Adv Option" from the **Menu** interface, as shown in figure 1 on the left.

2. Press **OK** key to enter **Adv Option** interface, as shown in figure 2 and figure 3 on the left.

The options under "**Adv Option**" include: **Reset Opts.**, **Del 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 quit current interface without performing any operation, and then return to the **Adv Option** interface.

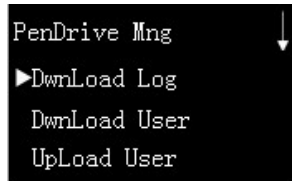
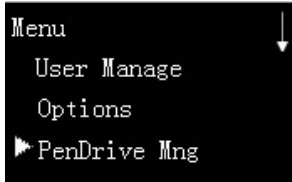
Reset Opts.: This parameter is used to restore the fingerprint lock to factory defaults.

Del 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.

3.3 USB Pen Drive Management



1. Select "PenDrive Mng" from the **Menu** interface, as shown in figure 1 on the left.

2. Move the **Band Switch** back of the fingerprint lock to the middle position, and then press **OK** key to enter the query interface of **PenDrive Mng**, as shown in figure 2 on the left.

3. Press **ESC** key to cancel operation, and then return to the **Menu** interface; or press **OK** key, and then the screen will prompts "Working...", as shown in figure 3 on the left. The **Fingerprint Collector** will show green light, and then enter **PenDrive Mng** interface, as shown in figure 4 and figure 5 on the left.

Note: When the battery voltage is too low, the user cannot enter the **PenDrive Mng** interface, and the green indicator light for **Fingerprint collector** continuously flickers. Please press **ESC** key for 5s to turn off the battery.

The options under "Adv Option" include: **DwnLoad Log**, **DwnLoad User**, **UpLoad User** and **Upd Firmware**.

DwnLoad Log: Download the logs of unlock from the fingerprint lock to the U disk.

DwnLoad User: Download the user information and fingerprint template from the fingerprint lock to the U disk.

UpLoad User: Upload user information and fingerprint lock from U disk to the fingerprint lock.

Upd Firmware: Upgrade the firmware of the fingerprint lock through the upgrade files in the U disk.



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

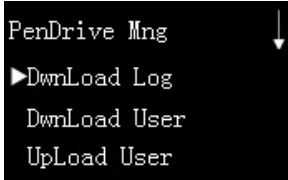


Tip: Please do not perform invalid operations (for example, insert or remove the USB pen drive in a frequent manner or during upload/download) on the USB pen drive, because it may result in system instability. It is recommended to keep the door open during the use of the USB pen drive.



Note: If you want to do **USB Pen Drive management**, the band switch must be set at the middle position. Otherwise the lock can not detect the U disk.

3.3.1 Download Logs



1. Press ▲/▼ key to move the cursor before the **DwnLoad Log** menu item, as shown in figure 1 on the left.

2. Press **OK** key to confirm. If you don't insert the U disk, the screen will prompt "Plug Pen Drive?" as shown in figure 2 on the left.



3. Open the Battery Cover behind the fingerprint lock, and then insert the U disk into the USB Interface. Press **OK** key to confirm, the screen will prompt "Copying Data", as shown in figure 3 on the left.



4. The screen will prompt "Copy Data Suc" after success copying, as shown in figure 4 on the left, and then return to the **PenDrive Mng** interface, as shown in figure 1 on the left.



5. Pull out the U disk. Now the USB pen drive stores the file: 1_atlog.dat (attendance logs) (where "1" denotes that the device No. is 1).

Tip: The number 1 before the file name means the device number is 1. You can set device number for your need. The setting method, please see **3.2.2 Set Device Number**.

Note: If the system displays the prompt "Plug Pen Drive?", please check whether the USB pen drive is plugged in properly.

3.3.2 Download User Data

Press **▲/▼** key on the **PenDrive Mng** interface to move the cursor before the **DwnLoad User** menu item, and then press **OK** key to start download user data. The files **user.dat** (user information) and **template.dat** (fingerprint template) will be concurrently downloaded to the U disk. The method of operation is similar to **3.3.1 Download Logs**, here is no longer to restate.

3.3.3 Upload user Data

Press **▲/▼** key on the **PenDrive Mng** interface to move the cursor before the **UpLoad User** menu item, and then press **OK** key to start upload user data. The files **user.dat** (user information) and **template.dat** (fingerprint template) will be concurrently uploaded to the fingerprint lock. The method of operation is similar to **3.3.1 Download Logs**, here is no longer to restate.

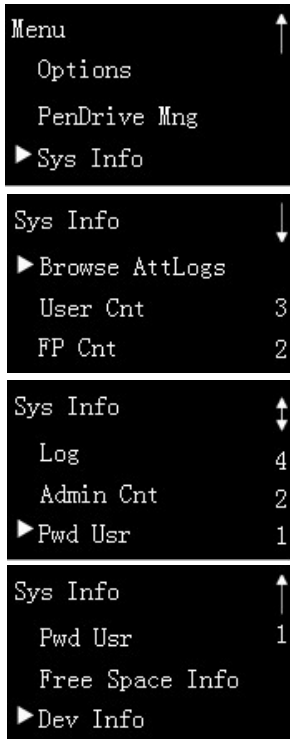
Note: If a user exists with the same User ID in the fingerprint lock, the new upload will overwrite the existing user data; otherwise, the new user data will be directly added.

3.3.4 Upgrade Firmware

Press **▲/▼** key on the **PenDrive Mng** interface to move the cursor before the **Upd Firmware** menu item, and then press **OK** key to start upgrade firmware. Upgrade the firmware of the fingerprint lock through the upgrade files in the U disk. The method of operation is similar to **3.3.1 Download Logs**, here is no longer to restate.

3.4 System Information

User can browse all the system information in **Sys Info**, including **Browse AttLogs**, **User Cnt**, **FP Cnt**, **Log**, **Admin Cnt**, **Pwd Usr**, **Free Space Info** and **Dev Info**.



1. Press **▲/▼** key on the **Menu** interface to move the cursor before the **Sys Info** menu item, as shown in figure 1 on the left.

2. Press **OK** key to enter the **Sys Info** interface, as shown in figure 2 on the left. The number "3" shows on the screen, means had enrolled 3 users in the device (the Fingerprint Lock); the number "2" means had enrolled 2 fingerprints in the device.

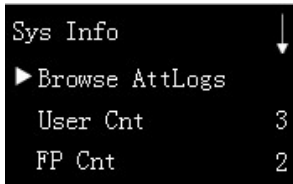
3. Press **▼** key to move the cursor down in order to show the **Log**, **Admin Cnt** and **Pwd Usr** menu, as shown in figure 3 on the left. The number "4" shows on the screen, means there have 4 unlock logs in the device; the number "2" means had enrolled 2 administrators in the device; the number "1" means had enrolled 1 password in the device.

4. Press **▼** key to move the cursor down, in order to show the **Free Space Info** and **Dev Info** menu, as shown in figure 4 on the left.

Note: For the **Browse AttLogs**, **Free Space Info** or **Dev Info** menu, if there is no numeral displayed in the row of the menu as shown in the figure, the user can press **▲/▼** to position the cursor on the menu, and then press **OK** key to enter the corresponding screen to display the desired information. The specific operation will be described in details in the following section.

3.4.1 Browse AttLogs

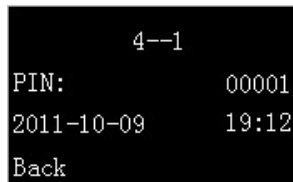
The user can use the **Browse AttLogs** menu to view the unlocking records for the enrollments ID in order to find abnormal unlocking situation. The specific operation is described as follows:



1. Press **▲/▼** key on the **Sys Info** interface to move the cursor before the **Browse AttLogs** menu, as shown in figure 1 on the left.



2. Press **OK** key to enter the **Browse AttLogs** interface, as shown in figure 2 on the left.



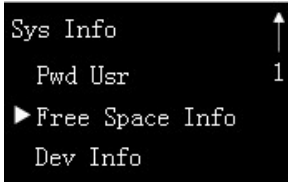
3. Press **▲/▼** key to select User ID. For example, select the User ID as 00001, then press **OK** key to browse logs, the result shown in figure 3 on the left. It shows the User ID, total of unlock logs, the date of unlock log and so on.

4. The number "4" shows in figure 3 means the total of unlock logs; the number "1" means the current shown log is the first one. You can press

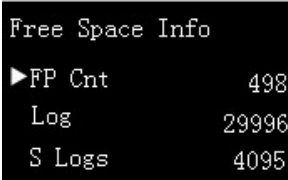
▲/▼ key to browse all unlock logs.

3.4.2 Free Space Information

From the **Free Space Info** menu item, the user can browse the free space of **FP Cnt**, **Log** and **S Logs**. The steps shown below:



1. Press **▲/▼** key on the **Sys Info** interface to move the cursor before the **Free Space Info** menu item, as shown in figure 1 on the left.



2. Press **OK** key to enter the **Free Space Info** interface, as shown in figure 2 on the left. The interface shows the current free space of **FP Cnt**, **Log** and **S Logs**. They are 498, 29996 and 4095.

3.4.3 Device Information

From the **Dev Info** menu, you can browse the **FPCnt**, **Log**, **S Logs**, **Manu Time**, **Serial Num**, **Vendor**, **Device Name**, **Alg Version** and **Firmware Ver**. The detail steps show as below:



1. Press **▲/▼** key on the **Sys Info** interface to move the cursor before the **Dev Info** menu item, as shown in figure 1 on the left.
2. Press **OK** key to enter the **Dev Info** interface, as shown in figure 2 on the left. The interface show the **FPCnt** is 500; **Log** is 30,000; **S Logs** is 4095.
3. Press **▼** key to move the cursor down in order to shown the **Manu Time**, **Serial Num** and **Vendor**. Press **▲/▼** key to move the cursor before the menu item and press **OK** key, and then you can browse the corresponding information.
4. Press **▼** key to move the cursor down, in order to shown the **Device Name**, **Alg Version**, and **Firmware Ver**, as shown in figure 4 on the left. Press **▲/▼** key to move the cursor before the menu item and press **OK** key, and then you can browse the corresponding information.



Note: The **L9000**'s maximum capacity of fingerprint is 500; the password capacity is 100; the log capacity is 30,000; the maximum user is 500. All of the capacities are standard configuration. If you need to increase capacity, you should consult our commercial representatives or pre-sales technical support engineers.

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 5 seconds to display the **Admin Affirm** interface, and then use the key to open the door, namely enter the **Menu** as **Supervisor** and carry through the management operation.

4.3 Automatic Program Exit and System Power-off

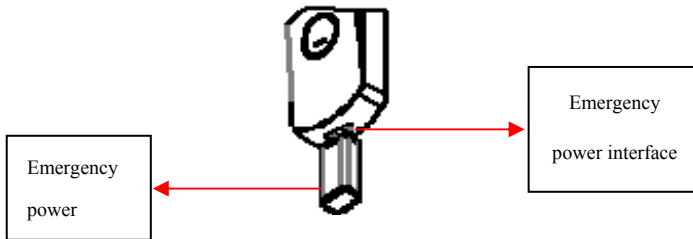
- The Fingerprint Lock powers off automatically upon successful matching and unlocking.
- The Fingerprint Lock powers off automatically when you set **Y** for the "Normal Open" option upon unlocking.

- 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.

4.4 Use Description of External Power

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.

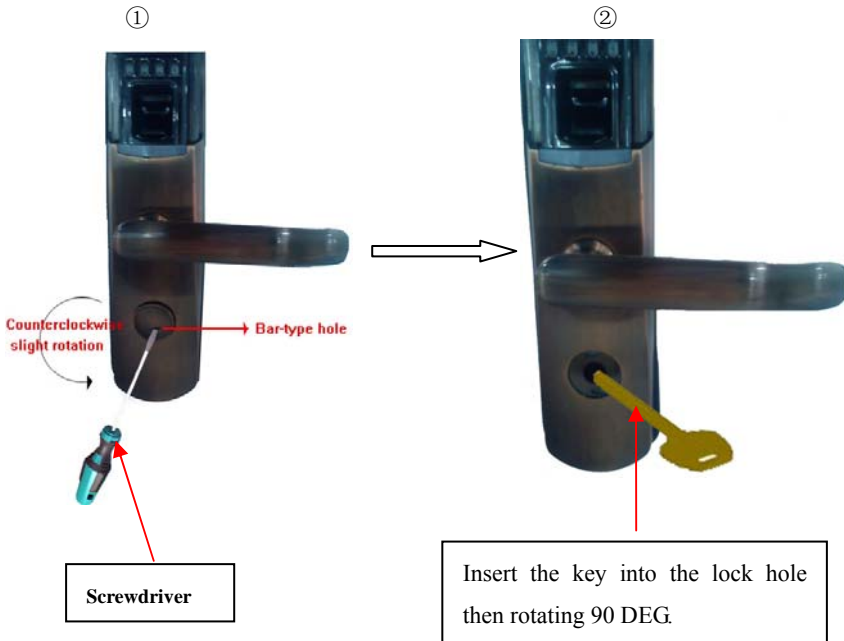


If you power off a Fingerprint Lock without closing the lock during the use of external power, the lock cylinder will not automatically return to its original position. That is, the Fingerprint Lock remains in NO state. To solve this problem, you can replace the battery and then open the lock once to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

4.5 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 Find a slotted screwdriver or flake with diameter less than 3mm. Insert the tip of the screwdriver or the rigid flake into the opening  on the lock cover; turn the screwdriver or the rigid flake counterclockwise to open the unlocking cover;
- ② Insert the emergency key into the keyhole and rotate 90° to unlock.



Note: The key shown in the figure is not a real object; please use the key provided with the device.

4.6 Alarm of Malicious Detection



The fingerprint lock supports the function of abnormal comparison alarm, to guard against malicious detection of the password. When the count of the failure exceeds that of preset illegal operation, the system will initiate the locking, and then the lock cannot be opened through comparison and the buzzer will give intermittent alarm, as shown in figure 1 at the left side; 30s later, the power will automatically switch off. This function is used to prevent the door from being opened accidentally by the non-enrolled user through continuous attempts of comparisons.

Note: Whether the functions of **Operate Alarm** and **Illegal Times** are initiated depending upon the administrator setting; if the count exceeds that of the illegal operation, the system will give an alarm; the specific setting is described in the section **3.1 Operate Option**.

4.7 Battery Low Voltage Protection



As shown in figure 2 on the left. When the battery meter stays at one bar and the user verification, the system prompts "Battery Low!!!", as shown in figure 3 on the left. The battery icon starts flashing. In this case, you press **Menu** key and hold on for 5 seconds, can't enter the **Menu** interface. 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. You must replace the battery for work normally.

Appendix

Appendix 1 Introduction of Verification Mode 2

If the user sets the verification mode as 2 in the **operation setting**, the system will enter the dual verification mode. For the administrator, as long as one comparison is successful, the door can be unlocked; however, for an ordinary user, only after both comparisons (**fingerprint + fingerprint**, **fingerprint + password** or **password +**

fingerprint) are successful for the same enrollment number, the door can be unlocked.

Take the verification mode of **fingerprint + password** as an example; the specific operation and screens are as follows:



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

2. Properly press the area of **Fingerprint collector** by the finger whose fingerprint is enrolled. If the verification is not successful, the screen will display "Please Try Agn.", as shown in figure 2 on the left, you must verify again, till verification succeeds, and then the screen will prompt "First Verify" and the User ID, as shown in figure 3 on the left.

3. Press number key to input password, as shown in figure 4 on the left. After input, press **OK** key to confirm, the screen will prompt unlock icon after

verify success. The following step is same as **2.4 User Verification and Set Normal Open Status**, here is no longer to restatement.



Note: In this verification mode, if the fingerprints for the first verification and the second verification are the same, the screen will prompt "Repeat Verify", that is, the fingerprints for both comparisons cannot be the same and corresponded to the same enrollment number; otherwise, the verification is not successful.

Appendix 2 Technical Specifications

- a) **Screen:** OLED display.
- b) **Collector:** Support 7131 has fingerprint film and 0303 without fingerprint film.
- c) **Capacity:** 500 fingerprints; 100 passwords; 500 users.
- d) **Matching mode:** Fingerprint matching, password matching, fingerprint + password matching and fingerprint + fingerprint matching.
- e) **Record capacity:** 30,000.
- f) **Communication mode:** USB Flash Disk.
- g) **Resolution:** 500 DPI.
- h) **Identification speed:** ≤ 2 seconds.
- i) **False acceptance rate:** $\leq 0.0001\%$.
- j) **False rejection rate:** $\leq 1\%$.
- k) **Power:** Four AA batteries; **working voltage:** 3.7V-6.8V.
- l) **Locking count:** ≥ 4000 times (Four NANFU alkaline batteries).
- m) **Temperature:** 0-45°C.
- n) **Humidity:** 10%-80%.