

USER MANUAL

Fingerprint Lock

Version: 1.0

Date: Feb. 2017

About This Manual

- This manual introduces the Fingerprint Lock (FP Lock) interface and menu operations. For the FP Lock installation, see the relevant installation instructions.
- Functions marked with “★” in this manual are only supported by specific product or customized product, and will be marked after that.

i

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

Contents

1. Instructions for Use.....	1
1.1 Device Appearance.....	1
1.2 Precautions.....	5
1.3 User Privileges.....	6
1.4 Time Setting.....	6
2. Enrollment and Verification.....	8
2.1 Enrolling an Administrator.....	8
2.1.1 Enroll a Fingerprint.....	8
2.1.2 Enroll a Password.....	10
2.1.3 Enroll an RFID Card★.....	11
2.2 Enroll an Ordinary User.....	13
2.3 Backup Enrollment.....	14
2.4 User Verification and Set NO Status.....	15
2.5 FP Card Management★.....	17
2.5.1 Create a PIN Card.....	18

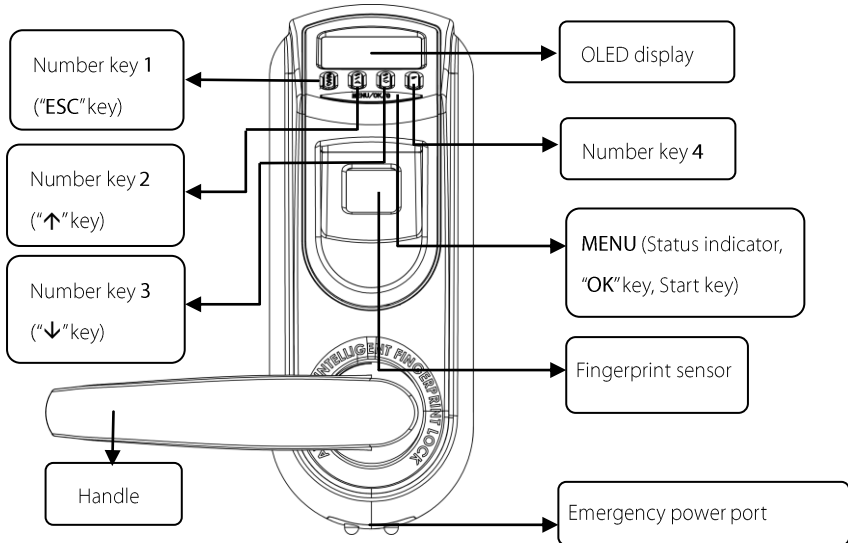
2.5.2 Enroll an FP Card.....	20
2.5.3 Create an FP Card.....	22
2.5.4 Purge an FP Card.....	23
2.6 Delete User Information.....	23
3. Lock Function and Settings.....	26
3.1 Operation Settings.....	26
3.1.1 Operate Alarm.....	26
3.1.2 Illegal Times.....	27
3.1.3 Lock Setting.....	28
3.1.4 Verify Mode.....	28
3.1.5 Normal Open.....	29
3.1.6 Card Only★.....	30
3.2 Language Settings★.....	31
3.3 Advanced Settings.....	32
3.4 Browse System Information.....	33
3.5 Browse Logs.....	35
3.6 USB Pen Drive Management★.....	36

3.6.1 Download Attendance Logs	37
3.6.2 Download User Data.....	37
3.6.3 Upload User Data.....	38
4. Administrator Loss Prevention★	39

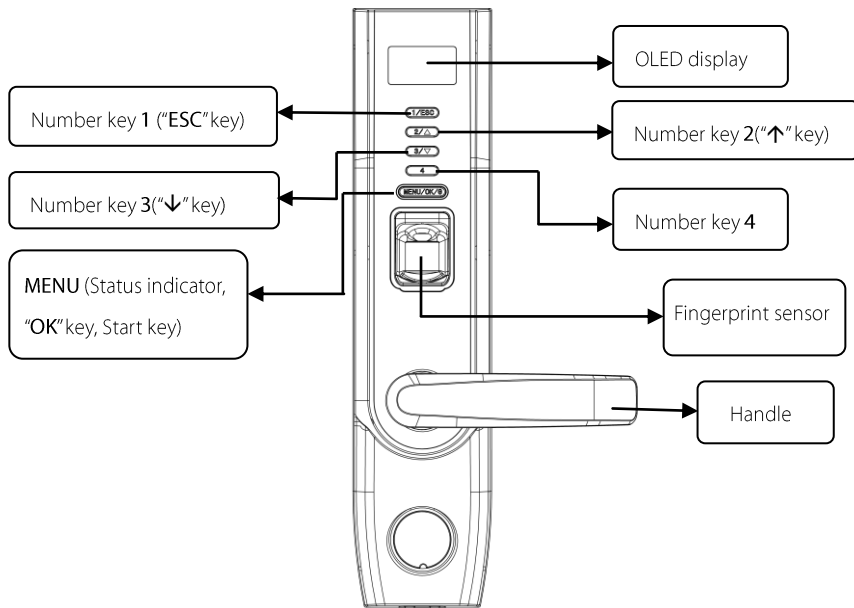
1. Instructions for Use

1.1 Device Appearance

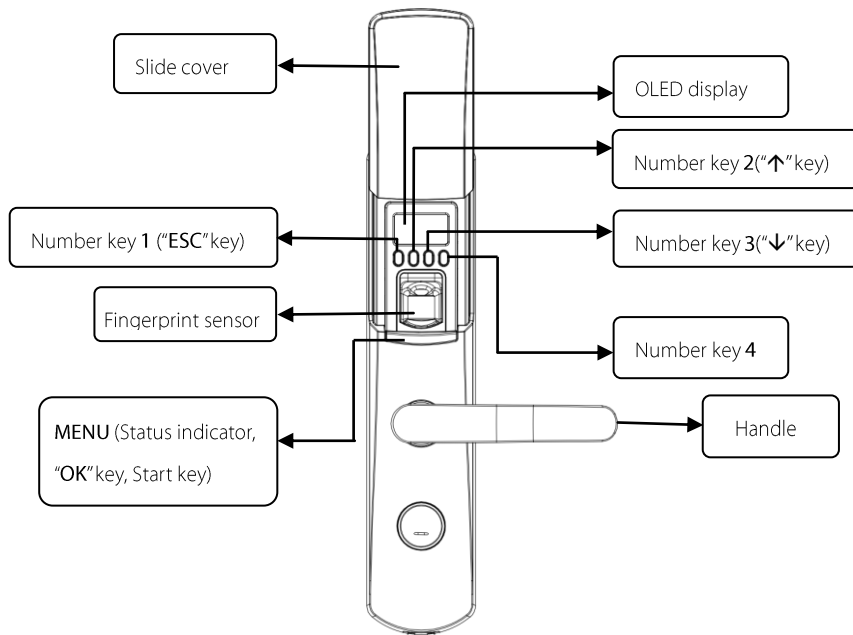
L7000 Series:



L5000/L4000:



L9000:



Number key 1: Press this key to exit current operation, press and hold this key to power off the FP Lock. The number key **1** also doubles as “ESC” key.

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

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

MENU key (Status indicator): This key can be used to start the FP Lock; press and hold this key for three seconds on the initial interface to open the main menu; this key also doubles as the “OK” key. The green LED indicator blinks when the FP 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.

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

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 fingerprint by pressing your finger(s) on the fingerprint sensor when the light in the fingerprint sensor window is on; otherwise nothing happens when you press your finger(s) on the fingerprint sensor.



Note: When you cannot power off the FP Lock due to the exception of program, press and hold the **ESC** key to power off and then restart the FP Lock. It is not recommended to power off the FP Lock by this way when the FP Lock operates normally.

Emergency power port: You can adopt an external backup battery to open the lock in the event of unlocking failure due to insufficient power supply of the FP Lock.

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

USB port★: The USB port is used for uploading or downloading user information and unlocking records through a USB pen drive.

1.2 Precautions

- 1) We strongly recommend you to enroll at least one administrator after installing the FP Lock. And then you can enroll the ordinary users.
- 2) Do not remove batteries when matching, enrolling or deleting fingerprints because the sudden

power-down may result in data loss of FP Locks. Before removing batteries, make sure the FP Lock is not in working state.

- 3) It is recommended to replace the FP Lock batteries once within six months, to avoid the damage to the circuit due to the battery leakage. Do not use batteries with poor quality.
- 4) When installing a FP Lock, connect the plug to the socket properly. Improper connection may lead to FP Lock failure.

1.3 User Privileges

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

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

Administrators(Admin): Refer to users who have access to all operations except performing advanced settings and enrolling super administrators.

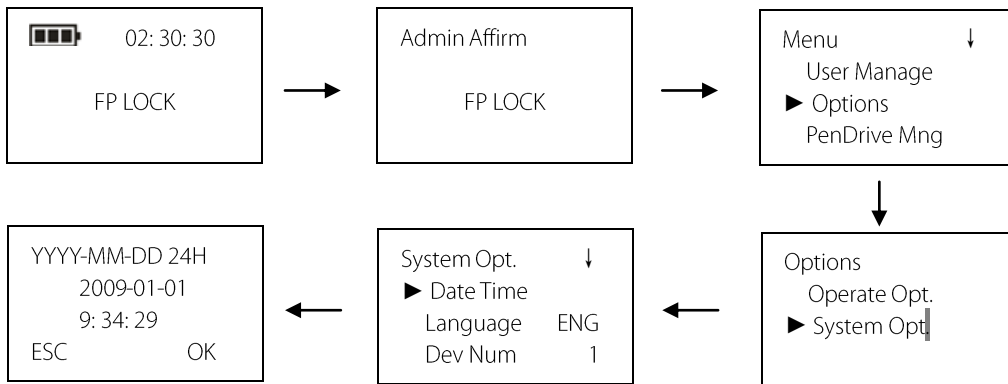
Ordinary users: Refer to all users other than the super administrators and administrators. Ordinary users only have access to the fingerprint matching and unlocking functions.


1.4 Time Setting

You need to set the correct date and time when you first use of a FP Lock, the operations are as follows:

 **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.



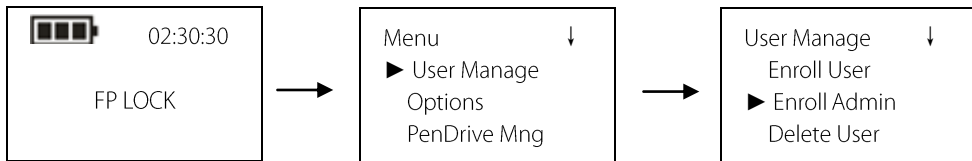
 **Note:** You can set the date between January 1st 2003 and December 31st 2032. To set the date beyond this range, you need to consult our commercial representatives or technical support engineers.

2. Enrollment and Verification

2.1 Enrolling an Administrator

If the FP Lock has no administrator, you must enroll at least one administrator before enrolling ordinary users.

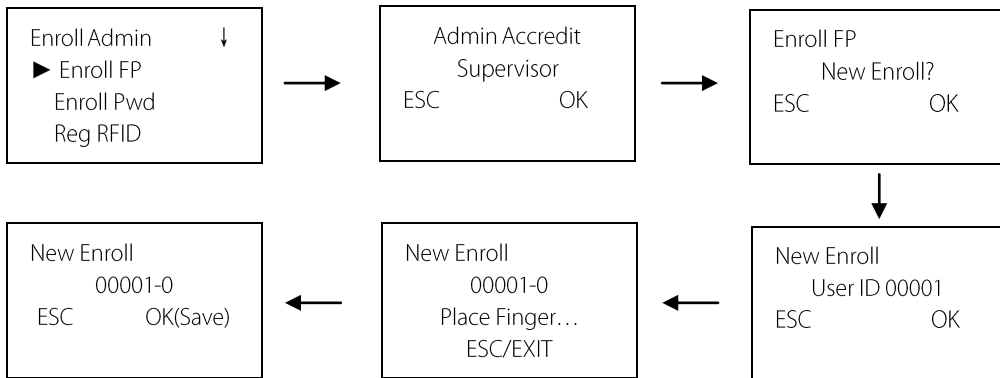
To enroll an administrator, proceed as follows:




After that, the enrolled administrator can perform fingerprint, password and RF card★ enrollment, the operations are as follows.

2.1.1 Enroll a Fingerprint

Enter "Enroll Admin" interface according to the operation in [2.1 Enroll an Administrator](#). Press 2/3 to select "Enroll FP" and then press **MENU**.

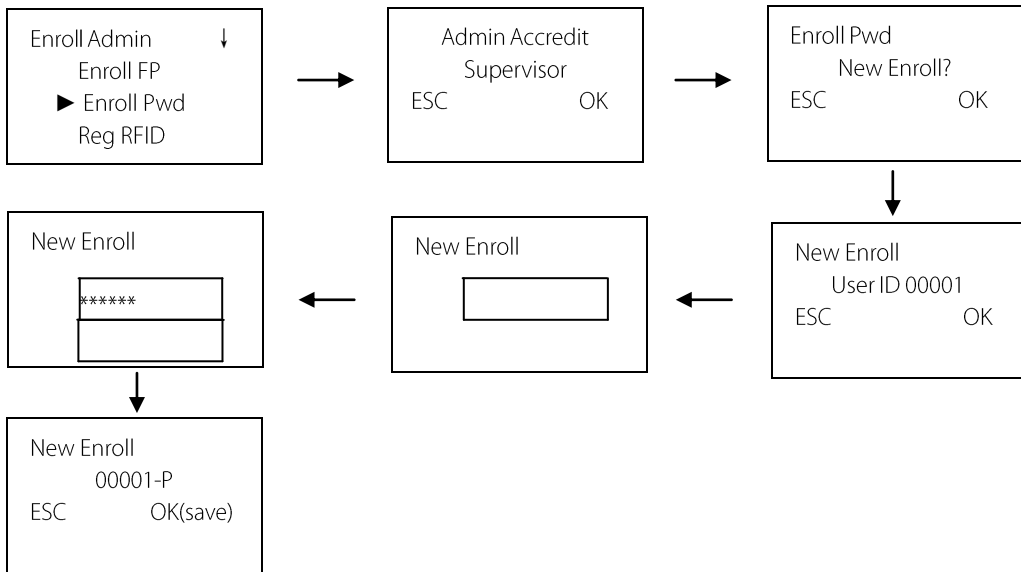


The system will prompt to save the enrollment information after the enrollment is successful. If the enrollment fails, the system will prompt to re-enroll fingerprint. The system returns to the “New Enroll” interface upon successful enrollment. You can continue or exit the fingerprint enrollment at that time.

 **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.

2.1.2 Enroll a Password

Enter “Enroll Admin” interface according to the operation in [2.1 Enroll an Administrator](#). Press 2/3 to select “Enroll Pwd” and then press **MENU**.



After successful password enrollment, the green indicator will light up for 3 seconds. If the enrollment failed, the red indicator will light up for 3 seconds, and prompt you to re-enroll it. Once the password is successfully enrolled, the procedure is completed.



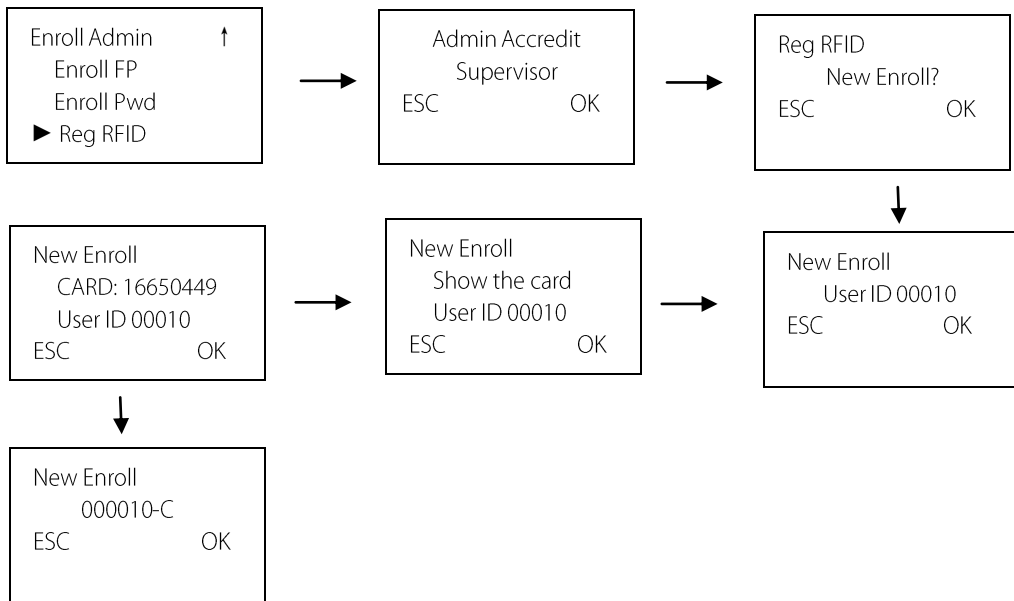
Note: A password consists of 6 to 10 digits. You can enroll only one password for each user ID and repeated passwords are forbidden; otherwise, the system will prompt “Password Error”.


2.1.3 Enroll an RFID Card★



Note: This function is only provided by fingerprint locks that support the RFID card function.

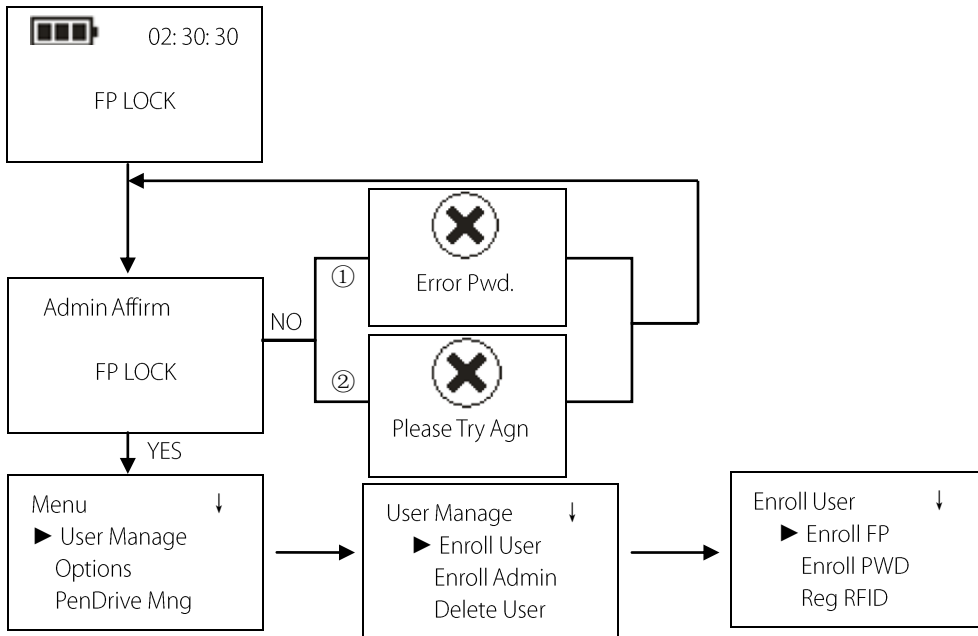
Enter “Enroll Admin” interface according to the operation in [2.1 Enroll an Administrator](#). Press **2/3** to select “Reg RFID” and then press **MENU**.



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

2.2 Enroll an Ordinary User

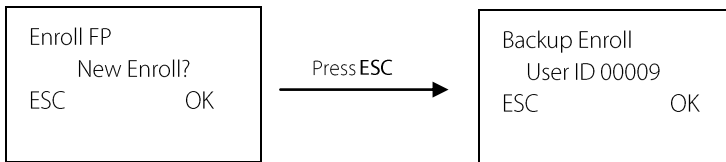
An administrator can enroll another administrator, or enroll ordinary users, with operations as follows:



After that, the enrolled administrator can perform fingerprint, password and RFID card ★enrollment. The rest of the operations are basically the same with those of administrator enrollment. For details, see [2.1 Enroll an Administrator](#).

2.3 Backup Enrollment

On the “New Enroll?” interface of [2.2 Enroll an Ordinary User](#), if you press **ESC** to cancel new enrollment, then the “Backup Enroll” interface will be displayed, as shown in the following figure:



The backup enrollment operations are basically consistent with the new enrollment operations except that “Backup Enroll” instead of “New Enroll” is displayed on the top of the interface. In the preceding chapters have described, here is no longer to restatement.

Note:

1) It is recommended to enroll at least two different fingers for long-standing users.

- 2) If you wish to modify the password after password enrollment finished, you can replace the original password with the password entered in the 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 User Verification and Set NO Status

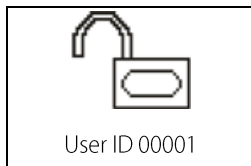
Press your finger with enrolled fingerprint or enter your password (press **MENU** after entering password) until verification successful.




Note:

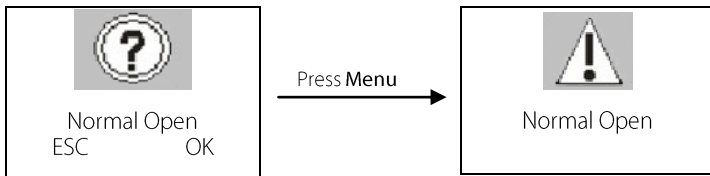
- 1) You can only match fingerprints when the FP Lock is in non-ON state.
- 2) If fingerprint or password verification is unsuccessful, the system will display a prompt "Please Try Agn." or "Error Pwd.". The parameters **Illegal Times** and **Operate Alarm** are set by the administrator. The system will generate an alarm after the illegal operations reach the specified value. For details, see [3.1 Operation Settings](#).

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



 **Note:** The “4 seconds” mentioned in the document, namely Lock (lock actuator time). You can modify it for need. For detail, please see [3.1 Operation Settings](#).

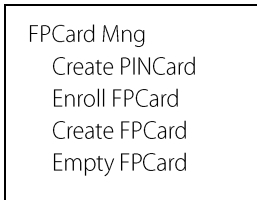
If the NO function is set to “Y” (See [3.1.5 Normal Open](#)), the prompts as shown follow; otherwise, no prompt will be displayed.



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

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 “Y”). 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 FPCard: This option is used to purge all data (fingerprints and numbers) stored in the FP card.



Note:

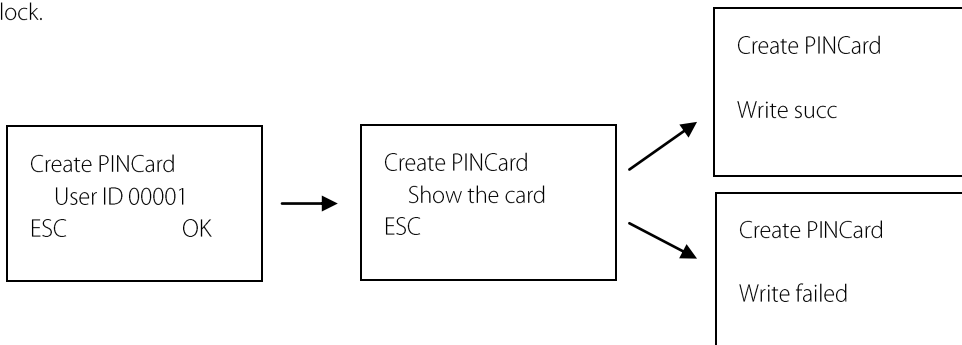
- 1) This function is only provided by fingerprint locks that support the Mifare card function.
- 2) If no administrator is enrolled in the system, the system will prompt you to enroll an administrator first.

2.5.1 Create a PIN Card

1) Create a PIN Card

Enter “Create PINCard” interface according to the operation in [2.5 FP Card Management](#) ★.

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



- 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 system gives a prompt “Write failed”, your PIN card is not written in the system.

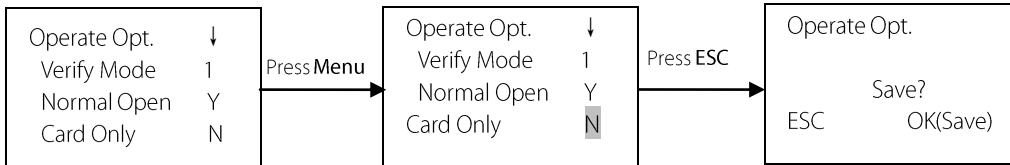


Tips: To create a PIN card, you need to ensure the user ID has already existed in the system; otherwise, the system will display a prompt “No Enroll” and you need to repeat the operation. After the PIN card is successfully created, only the ID number is stored in the PIN card.

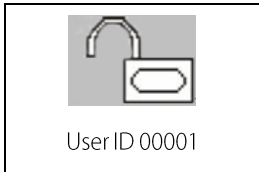
2) Verify the PIN Card



Note: Set the parameter “Card Only” to “Y”. If you set the parameter “Card Only” to “N”, you cannot verify with the created PIN card.



Press **2/3** to select **Y/N**, then press **MENU** to save the setting. Then, you can perform PIN card verification.

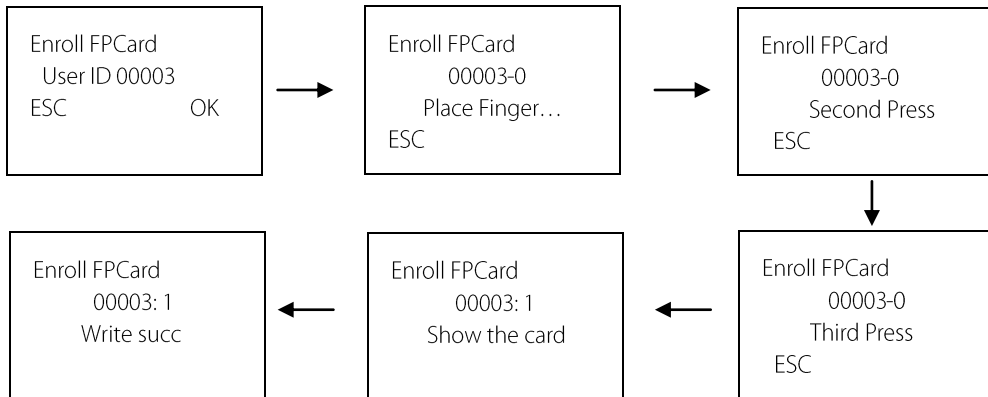


Swipe your PIN card through the card reader when the system returns to the initial interface. If the interface as shown in the figure on the left is displayed, the PIN card is successfully created.

2.5.2 Enroll an FP Card

1) Enroll an FP card

Enter "Enroll FPCard" interface according to the operation in [2.5 FP Card Management](#) ★.



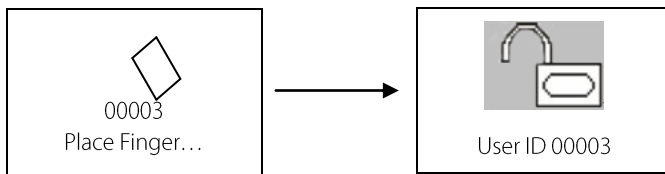
2) Verify an enrolled FP card



Note: Please set the “Card Only” option to “N”. If you set it to “Y”, the fingerprint lock will only verify users' PIN cards.

(1) On the initial interface, swipe an enrolled FP card through the card reader.

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



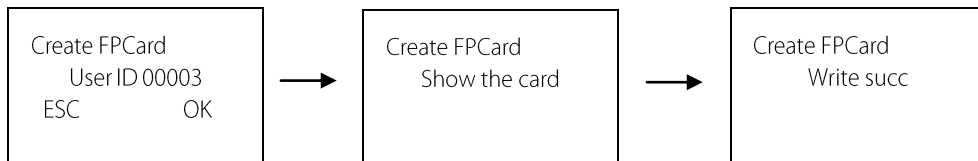
Tips: Through the above operations, you only store your fingerprints in your FP card but not in the fingerprint lock. Therefore, you must show your FP card first before fingerprint comparison. (Your fingerprints are only stored in your FP card.)

2.5.3 Create an FP Card

1) Create an FP card

Enter “Create FPCard” interface according to the operation in [2.5 FP Card Management](#) ★.

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



2) Verify a created FP card



Note: Please set the “Card Only” option to “N”.

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

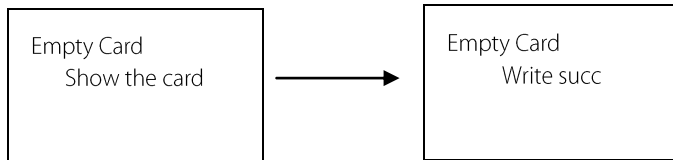


Tips: Through the above operations, you can duplicate fingerprints from the fingerprint lock to an FP card. In this way, you can perform identification either through fingerprint or “FP card + fingerprint”. (Your fingerprints are stored in both the fingerprint lock and your FP card.)

2.5.4 Purge an FP Card

Enter “Empty Card” interface according to the operation in [2.5 FP Card Management](#) ★.

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

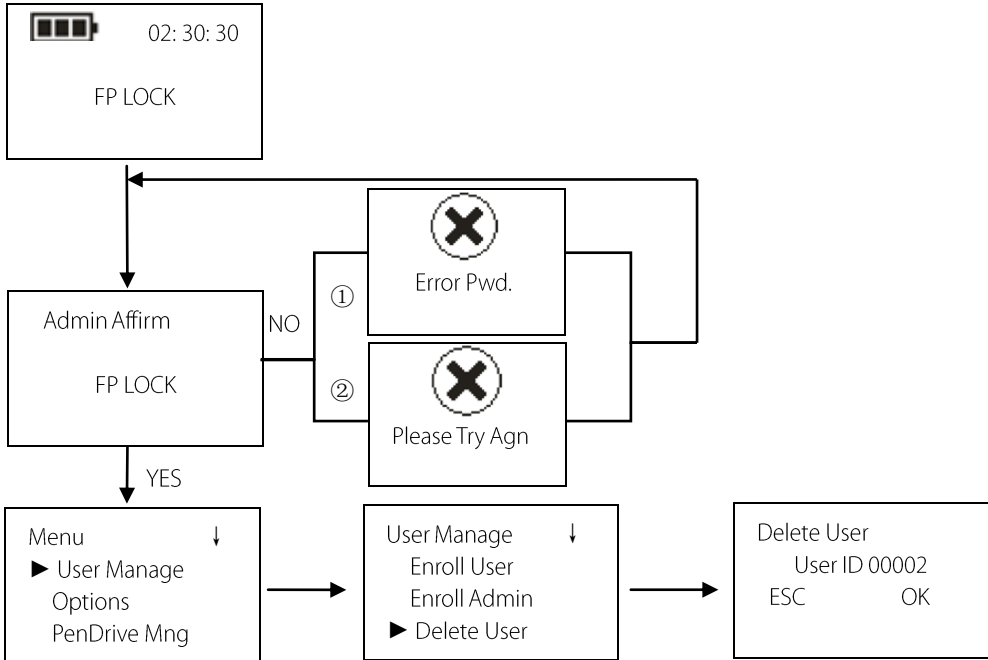


2.6 Delete User Information



Warning: In deleting user information process, it is strictly prohibited to disconnect the power supply, to prevent the deletion of other data by mistake!!!

The operations are as follows:



To delete the user fingerprint: Delete the fingerprint of specific ID number, and press **MENU** to confirm.

```
Dele Fingerprint
  00002—0
  User ID 00002
ESC      OK
```

To delete the user password:

```
Del Password
  00002—P
ESC      OK
```




```
Del User
  00002
ESC      OK
```



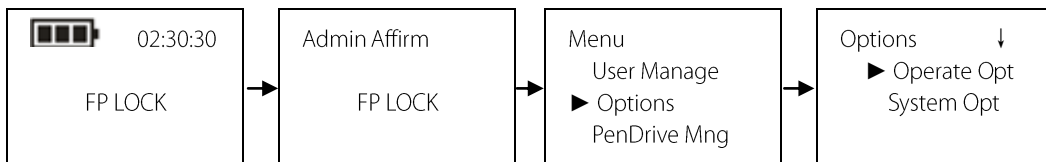
```
Del User
  Delete?
ESC      OK
```

After the user deletion is finished, restart the device, and then verify the deleted user to check if the operation is succeeded.

 **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 and Settings

3.1 Operation Settings



The "Operate options" menu includes **Operate Alarm, Illegal Times, Lock, Verify Mode, Normal Open and Card Only★**.

Operate Opt.	↓
Operate Alarm	Y
Illegal Times	10
Lock	5

Verify Mode	1
Normal Open	Y
Card Only	N

3.1.1 Operate Alarm


This parameter is used to set if the operation failure triggers the alarm.

Operate Opt.	↓
▶ Operate Alarm	Y
IllegalTimes	10
Lock	5

Follow the steps in [3.1 Operation Settings](#), enter the operation menu and select “Operate Alarm”. Press **MENU** to enter the modification state, press **2/3** to select Y/N, after modification press **MENU** to save and quit

3.1.2 Illegal Times

This parameter is used to set the consecutive operation failure count. An invalid operation alarm will be triggered when the consecutive failure count exceeds this threshold.

 **Note:** The failure count starts to cumulate when the FP Lock is started. If the number of cumulative failures exceeds this threshold, the FP Lock will trigger an invalid operation alarm; otherwise, the failure count will be cleared after successful unlocking.

Operate Opt.	↓
Operate Alarm	Y
▶ IllegalTimes	10
Lock	5

Follow the steps in [3.1 Operation Settings](#), enter the operation menu and select “Illegal Times”. Press **Menu** to enter the modification state, press **2/3** to set the value (the value by default is 10, the permit range is 3-99), after modification, press **Menu** to save and quit.

If the number of cumulative failures exceeds this threshold, the FP Lock will automatically power off. After the device restarts the FP Lock will trigger an invalid operation alarm of a buzzing sound. After about 30 seconds it will power off automatically.

3.1.3 Lock Setting

This parameter is used to set the duration from successful matching to unlocking.

Operate Opt.	↓
Operate Alarm	Y
Illegal Times	10
▶ Lock	5

Follow the steps in [3.1 Operation Settings](#), enter the operation menu and select "Lock". Press **MENU** to enter the modification state, press **2/3** to set the value (for this parameter, its unit of quantity is 1 second, the value by default is 5, the permit range is 3-15). After modification, press **MENU** to save and quit.



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

3.1.4 Verify Mode

▶ Verify Mode	1
Normal Open	Y
Card Only	N

Follow the steps in [3.1 Operation Settings](#), enter the operation menu and select "Verify Mode". Press **MENU** to enter the modification state, press **2/3** to set the value. There are three optional values 0, 1, and 2 that represent different matching modes, and the default value is 1. After modification, press **MENU** to save and quit.

Verify Mode 0: Only the administrator can open the lock by successful matching, 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.

3.1.5 Normal Open

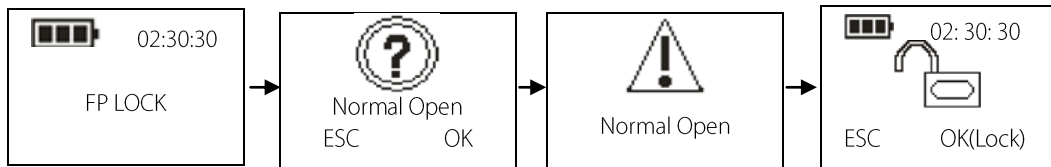
It is used to set the lock always in NO state.

Verify Mode	1
▶ Normal Open	Y
Card Only	N

Follow the steps in [3.1 Operation Settings](#), enter the operation menu and select "Normal Open". Press **MENU** to enter the modification state, press **2/3** to select **Y/N**, after modification, and then press **MENU** to save and quit.

- 1) In the start interface verify the fingerprint and unlock.
- 2) Prompt if you select NO state, and press **MENU** to save.
- 3) After successful setting, the buzzing sound will be heard three times for prompt.

4) To disable the NO function, power on the system and press **MENU** in the “Normal Open” interface. Then the system closes the lock and automatically powers off.

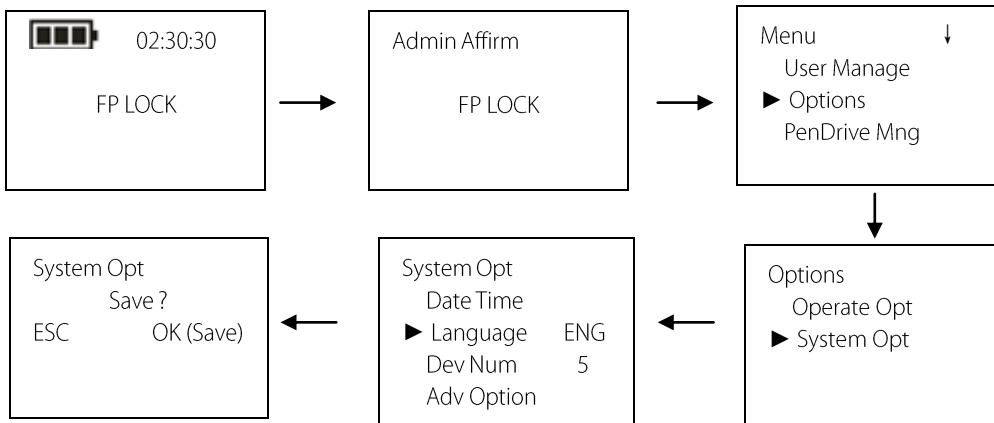


3.1.6 Card Only★


Verify Mode	1
Normal Open	Y
▶ Card Only	N

Follow the steps in [3.1 Operation Settings](#), enter the operation menu and select “Card Only”. Press **MENU** to display the Card Only interface, and press 2/3 to select Y/N. If you select **Y**, you only need to verify your ID card. If you select **N**, you need to verify both your ID card and fingerprint.


3.2 Language Settings★

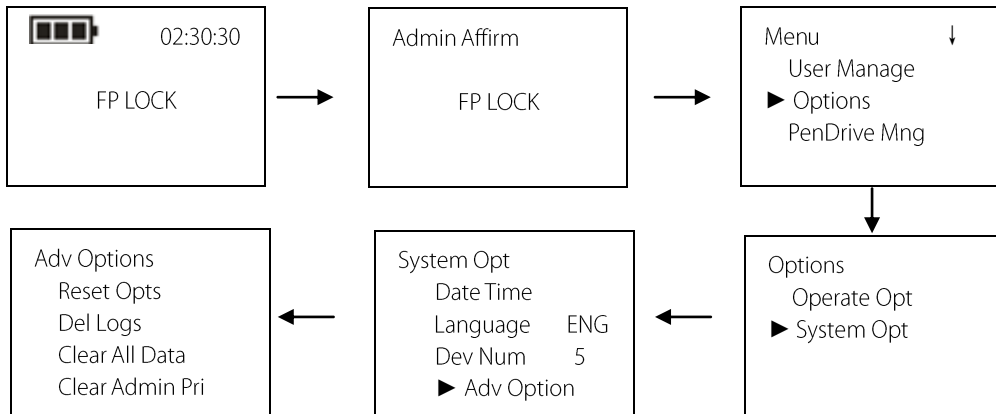


It will take effect after device restart.◦

 **Note:** Language selection is a non-standard function. To use this function, please consult our commercial representatives or technical support engineers.

3.3 Advanced Settings

 **Note:** Only the super administrator has the right to perform advanced settings.



The advanced options include **Reset Options**, **Delete Logs**, **Clear All Data** and **Clear Administrator Privilege**. Press **2/3** to select the desired option, and then press **MENU** to enter the menu. Select the items and press **MENU** to execute the corresponding operation. The screen will return to “Advanced options” menu. If you press **1** (ESC) and quit, it will return to the advanced option menu without any operation.

Reset Options: This parameter is used to restore the FP Lock to factory defaults.

Delete 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.

Clear Administrator Privilege: This parameter is used to change an administrator into ordinary users. This function should be used with caution. It is recommended to register at least one new administrator after using this function.

3.4 Browse System Information

Users can browse the system information, including the enrolled fingerprint counts, enrolled user, and device information. To browse the system information, the operations are as follows.



Sys Info	↓
Browse Attlogs	
User Cnt	5
FP Cnt	1
Log	85

Admin Cnt	2
Pwd Usr	3
Reg RFID	12
Free Space Info	
Dev Info	

User Cnt: The number of enrolled users which can verify and unlock the FP Lock.

FP Cnt: The number of enrolled user fingerprints.

Log: The number of verification records in the FP Lock.

Admin Cnt: The number of enrolled administrators with management privileges (add user, delete user, etc.)

Pwd Usr: The number of users enrolled password.

Reg RFID★: The number of enrolled user RFID cards.


Free Space Info★: Press **2/3** to select “Free space information”, and press **MENU** to see the detail.

Free Space Info	
FP Cnt	499
Log	29915
S Logs	4095

Dev Info: Press **2/3** to select “Device information”, and press **MENU** to see the details as follows:

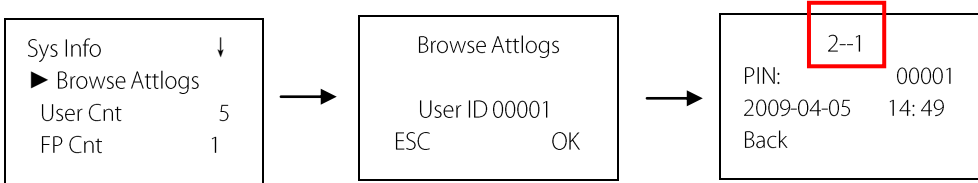
Dev Info	↓
FPCnt(100)	5
Log (10k)	3
S Logs	4095
Manu Time	

Serial Num
Vendor
Device Name
Alg Version
Firmware Ver

 **Note:** Only the fingerprint locks supporting ID cards are configured with the “Reg FPID” and “Free Space Info” options.

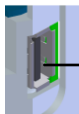
3.5 Browse Logs

The FP Lock supports the offline browsing of unlocking logs, which facilitates users to check whether there is any exceptional unlocking in time. Please refer to [3.4 Browse System Information](#):



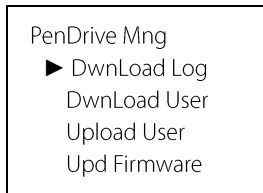
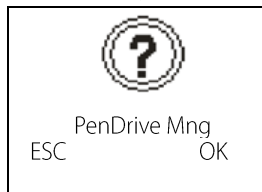
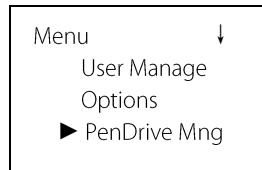
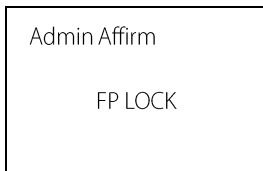
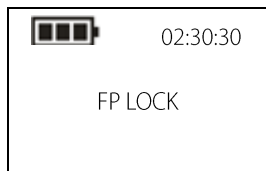
 **Note:** The first digit indicates the total number of records and the last one indicates current record.

3.6 USB Pen Drive Management★



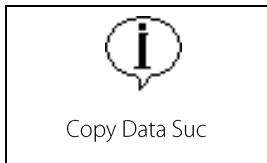
USB port

Insert a USB pen drive into the USB port.



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

3.6.1 Download Attendance Logs



1) User data downloading is similar to the downloading of attendance logs. Enter the “PenDrive Mng” menu according to the procedure steps in [3.6 USB Pen Drive Management](#)★. Press **2/3** to select “DwnLoad Log” and then press **MENU**. When download completes, the screen on left is displayed.

2) Press **1** (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.dat** (Where “X” denotes that the device No.).



Tips: 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.

3.6.2 Download User Data

User data downloading is similar to the downloading of attendance logs. Enter the “PenDrive Mng” menu according to the procedure steps in [3.6 USB Pen Drive Management](#)★. Press **2/3** to select “DwnLoad User”, the files **user.dat** (user information) and **template.dat** (fingerprint template) will be concurrently downloaded to the USB pen drive.

3.6.3 Upload User Data

Uploading user data is similar to the downloading of attendance logs. Enter the “PenDrive Mng” menu according to the procedure steps in [3.6 USB Pen Drive Management★](#). Press **2/3** to select “UpLoad User” and then press **MENU**. The files **user.dat** (user information) and **template.dat** (fingerprint template) stored in the USB pen drive will be concurrently uploaded to the FP Lock.



Tips:

- 1) When uploading user information, if a user ID already exists in the FP Lock, the new uploaded information will overwrite the existing user data; otherwise, the new user data will be directly added.
- 2) 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. Administrator Loss Prevention★

To avoid the menu operation failure as a result of loss of the 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 FP Lock to the left or right. Now you can access the menu as a super administrator for management and operation.

