HDWR
Hardware for business

User Manual

Time recorder

TimeLok-400N

Specification:

- **Model:** TimeLok-400N
- **Material:** ABS
- **Verification type:** Fingerprint, card, pin
- **Frequency of operation:** 125 kHz
- **Max number of employees in the base:** 3000
- **Max. number of fingerprints in the base:** 1000
- **Max. number of passwords in the base:** 1000
- **Max. capacity of logs in the database:** 100 000
- **Number of buttons:** 16
- **Display:** 2.4 inch TFT LCD
- **Power supply:** 12V
- **Error rate:** 1/1 000 000
- **Operating temperature:** -10 ~ 60
- **Operating humidity:** 20 ~ 80%
- **Weight of the device:** 440 g
- **Device dimensions:** 190 mm* 135 mm*40 mm

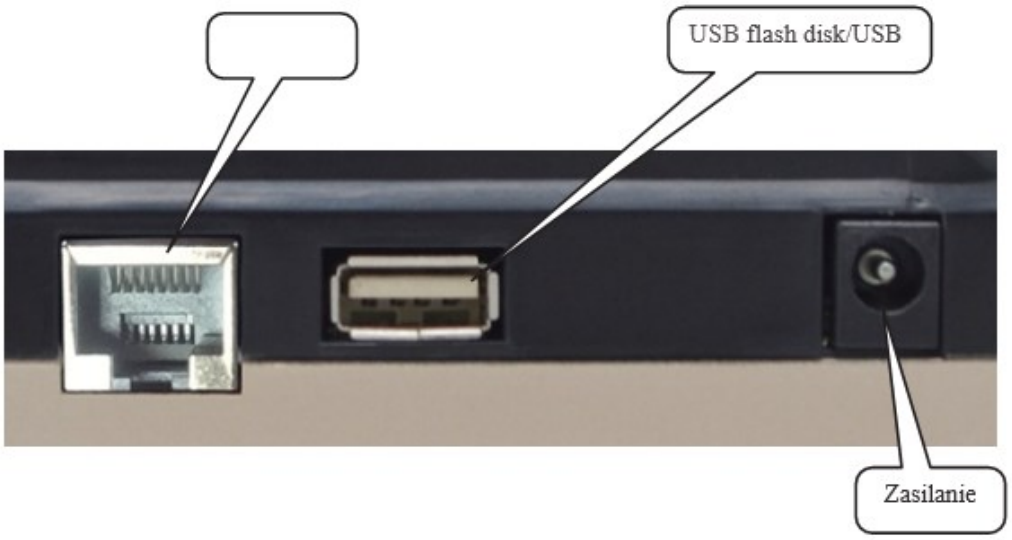
Table of contents

1 Introduction

This manual is intended to introduce the functions of the fingerprint device. After reading this manual, the user knows how to use and manipulate this fingerprint device. This manual provides a detailed explanation of each function with corresponding graphics for easy understanding.

2 Communication with the computer

There are two types of communication. They are TCP/IP and USB flash disk.



3. Power management

After connecting the power supply and pressing the in/out button, the machine will be turned on. If you have automatic shutdown enabled, the machine will be turned off automatically after a predefined period of inactivity in minutes.

To manually turn off the machine, simply press and hold the in/out button for more than 4 seconds. We can also turn the machine on or off via the computer.

4. User management

The machine operator can be divided into 2 types. One is the administrator and the other is the user. The user can only perform verification on the machine, while the administrator can operate the machine's menu. The role of the administrator is to save or delete the fingerprint, password or proximity card for the user.

5 User registration

There are 3 types of registration in the fingerprint machine. These are fingerprint, password and proximity card (optional). Each user can register a maximum of 3 fingerprints, 1 password and I proximity card (optional). The password has a maximum of 4 highlights, ranging from I to 9999.

6 User ID and password

Each user or administrator must have a unique user ID. It has a range from I to 99999999, 8 digits. This user ID is to match the user ID in the attendance software.

7 Machine operation status

The machine has 3 kinds of statuses. They are: presence status, working status and

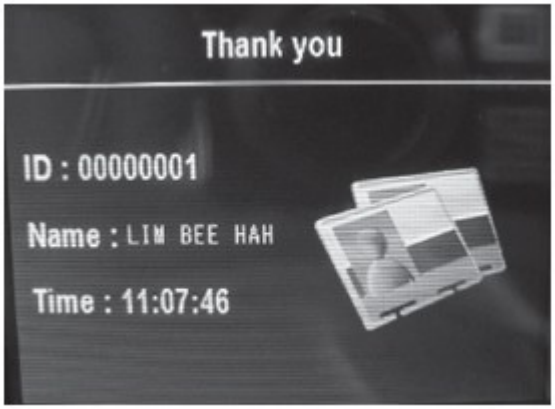
presence prohibition status.

In presence status, you can press your finger into the fingerprint sensor or enter a user ID and password or swipe a proximity card to make the machine start verification. If it is passed, the corresponding user will appear on the display.

In addition, the punching record will be stored in the machine's flash memory. In addition, the door lock signal will be released to open the door.

In operation mode, we can add, modify or delete records, machine settings and transaction queries. If the machine has at least one administrator, access to the menu system requires administrator verification. On the other hand, if there is no administrator, anyone can access the machine's menus.

In no-presence mode, the user cannot perform verification or any operations. This is due to the computer software communicating with him.



8. Record of attendance

Various data are stored in the machine. These are glog, slog and enroll infonnation data. GLog is input and output transactions. Slog is a log of changes in machine settings. Enroll infonnation is the records of each user. It stores the user ID and verification information such as fingerprint, card and password. Since these records are stored in flash memory, power failure will not cause data loss. However, the user is encouraged to download the data from the machine at least twice a month to have a backup in the computer software.

Slog and Glog content

Record type	Operation	Pola zapisu
Management register	Enrolluscr	Dme. Time. Tcmiinal. Operator User ID. Enrolltx! User ID
	Delete user	Date. Time. Tcmiinal. Operator User ID. Deleted User ID
	Delete all records	Date. Time. Tcm1inal. Operator User ID
	Advanced management	Date. Time, Tcm1inal. Operator User ID
	Time setting	Date, Time, Temiinal. Operator User ID
	Request for Quote	Date, Time, Terminal. Operator User ID
Presence Record	User verification	Date. Time, Tcmiinal. Verified User ID

9. Advanced management

Advanced management allows you to change the advanced settings of the device.

9.1 Terminal setting

Terminal setting allows you to change the device number. The default device number is.

If you have more than one machine on the network, each device requires a unique device number. The range of device number is from I to 255. When you communicate a device through computer software, the software device number must be the same as the hardware machine.

9.2 Manager Count

Used to set the number of managers allowed when writing. The default is 5.

9.3 Language
This item is used to set the device's display language. The default options are English, Traditional Chinese and Simplified Chinese. To display another national language, negotiate.

9.4 Power 011'
This is the 10 idle time setting for the IO machine to turn off automatically. The default value is "no" - enter the idle time when changing the setting. The range is from 1 to 9999 minutes.

9.5 Date and time
If you find that the date and time of the machine are not correct, you can correct it using this menu item. It can also be corrected using the computer software.

9.6 Sound
The fingerprint device will make "thank you" or "please press your finger again" sounds for positive, or negative verification, respectively. If you do not want to hear this voice, you can turn it off in this menu item. If the sound is disabled, even pressing the device's keyboard will not have a sound. When the user passes verification, you can only rely on the display for the phrase "thank you." If it fails, the display will show "Access denied, press finger again." The default value is "yes" with an audible output.

9.7 Restore factory settings
Selecting this item will restore all settings to factory defaults. Be careful when using this item.

Log settings

9.8.1 Low memory warning.
It is used to set the remaining records to display the warning.
When the remaining memory space is less than the number of warning records, the device will inform you on the display or by voice.
The default value is 100 records. You can set from 1 to 255 records.
If you do not set this function, the device will not display any warning

9.8.2 GLng warning

When the remaining amount of unused records is less than the glog warning, the device warns the user by voice or on the display. If the user is warned of this case, retrieve the in out records as soon as possible. The default value is 1000, and can be set from 1 to 1500 or "no". "No" means no warning at all.

9.8.3 Re-verification time

Used to prevent the user from performing verification more than once in a given time period. You can enter a range from I to 255 minutes. If you enter 3 minutes, a user performing verification a second time within 3 minutes will be rejected to save the transaction. The default value is "no".

10 Keypad

The keypad allows you to enter a user ID and password to verify or perform device settings. The key layout is as follows:

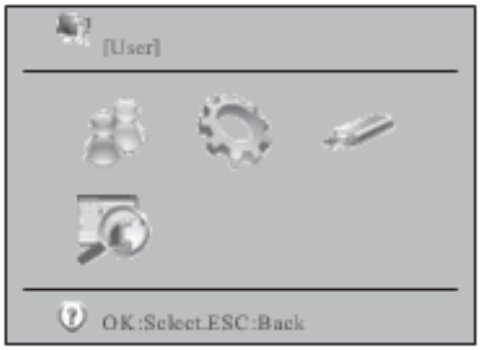
• ESC	escape key
• MENU	access the menu system
· OK	confirm action (same as enter)
■ I	move cursor up one item
' ; ;	move cursor down one item
• O --g	numeric key for input number
• c'J	on/off button

11. Recorder menu

The menu structure of the fingerprint machine is grouped into different categories so that you can easily find the targeted information.

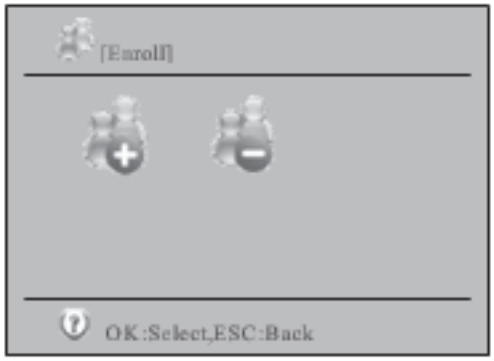
We have divided our menu items into 4 categories. They are: operation, settings, USB drive and status. The operation category is for managing users. The settings category is used to set various arguments for the device. USB disk is used to upload or download data from or to a USB flash drive. Status category is used to check the status of the device.

When you press the "menu" button, you will be taken to the main menu of the system. It consists of 4 icons that represent the first level menu. They are: user management, device settings, USB drive and system information. Each level of the menu has its own submenus.



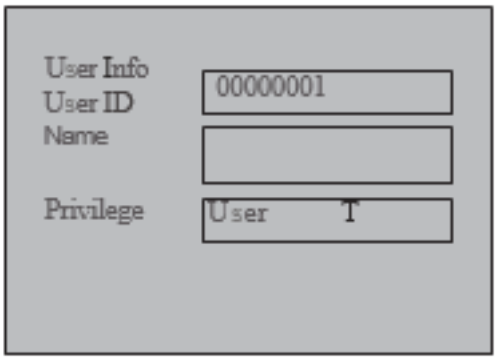
11.1 User management

The first item in the main menu is user management. It consists of two sub-items. These are "Sign up" and "Delete".



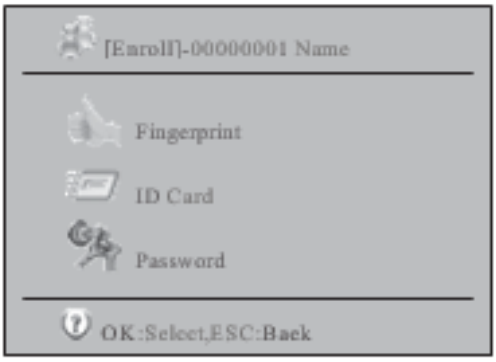
After selecting the "enroll" option, the data entry screen will be displayed. You need to enter the user ID. Then you can change the default "user" permission to "manager" or "s.manager". "s.manager" means "super manager." To change the privilege, move the cursor in the area and press the "ok" button. Then you can use the "up" or "down" arrow to switch between different arguments.

If you enter an existing user ID, the corresponding name will be displayed, provided it has a name.

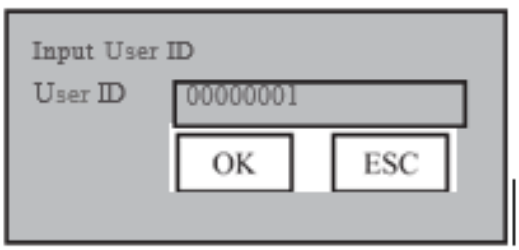


For adding a user, you must choose to save a fingerprint, card and password. ID card is an optional function. For fingerprint registration, you need to swipe your finger 3 times to get the best template. For ID card, swipe the card to enter the card number.

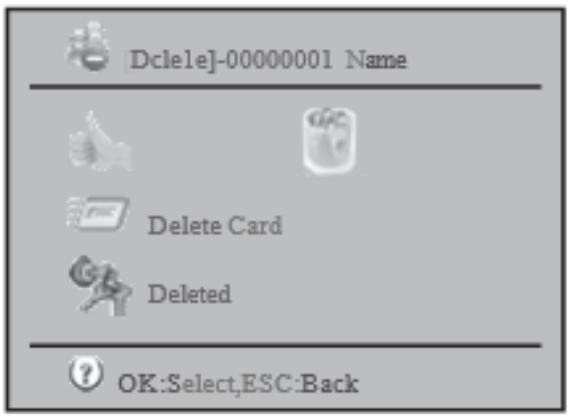
Use "A", "T" button to move the cursor up or down and press "ok" button to confirm.



In user management, when you select the "delete" icon and press "ok", you will see the user ID entry screen. Enter the desired user ID and press "ok" to select the user to delete.

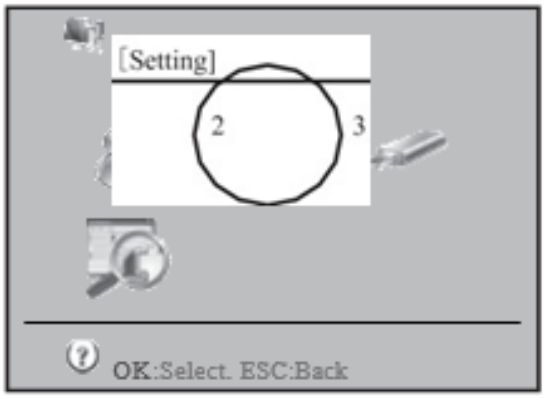


Następnie zobaczysz kolejny ekran do wyboru, który pokazuje, który tryb weryfikacji ma zostać usunięty. Możesz wybrać usunięcie odcisku palca, karty, hasła lub wszystkich z nich.



11.2 Setting

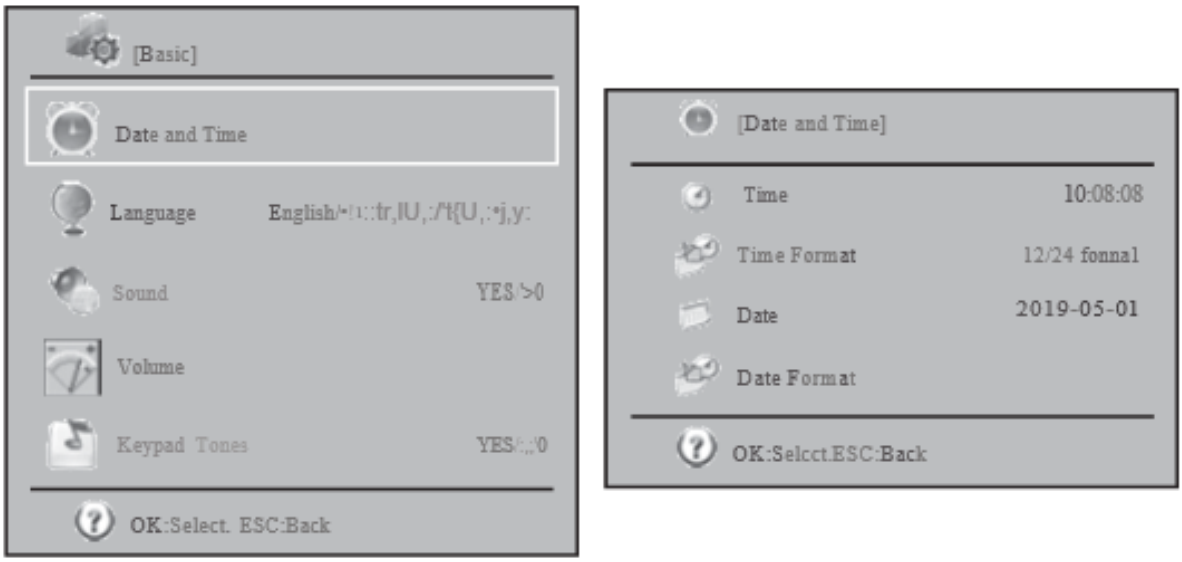
Setting is a first-level menu that allows you to change the arguments of the fingerprint machine.



After selecting the "Setting" menu item, another submenu will be secured. It has 7 icons. They represent basic settings, advanced settings, power management, communication settings, log settings, access control settings and auto test.

11.2.1 Basic settings

In the basic settings, you can change the device's date and time, display language, enable or disable voice, voice level, and whether pressing a button produces sound.



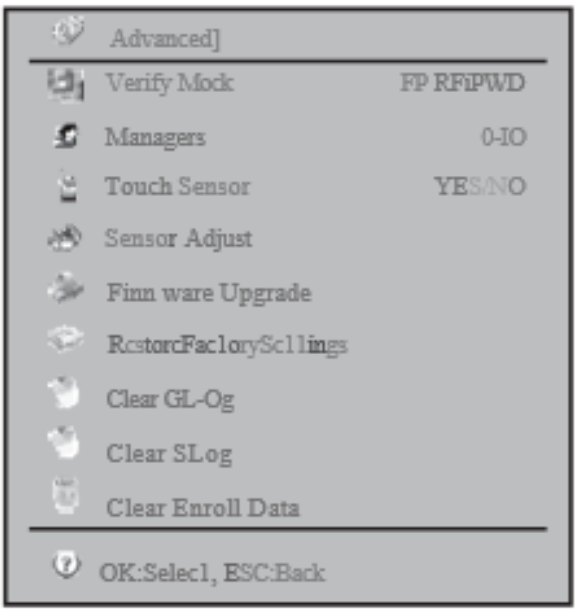
In date and time we can correct the date and time of the machine. Besides, the format of the displayed date and time can be changed. In language item, you can change the displayed language between English, traditional Chinese and simplified Chinese. For other language, please negotiate with your supplier. If the voice is enabled, "thank you" will be heard after verification passes, while "please press your finger again" will be heard after verification fails.

For the voice level, you can tune the volume of the voice. If the voice is off, this item cannot be adjusted.

For the button voice, you can turn it on or off If it is on, you can hear the button sound for each button press.

11.2.2 Advanced settings

In the advanced settings, we can tune the more important arguments for the fingerprint machine.



The first element is the verification mode. When you choose fp/card/pwd, the user can verify using both methods. When you choose fp+pwd, the user needs both fp and password entry for verification. Options include fp/rf/pwd, rf+fp, fp+pwd, rf+pwd, fp+rf+pwd.
The second item is the number of administrators. You can choose a value from Oto 10. The default value is 5. Too many administrators will cause a security problem. So you should choose a compromise between convenience and security.

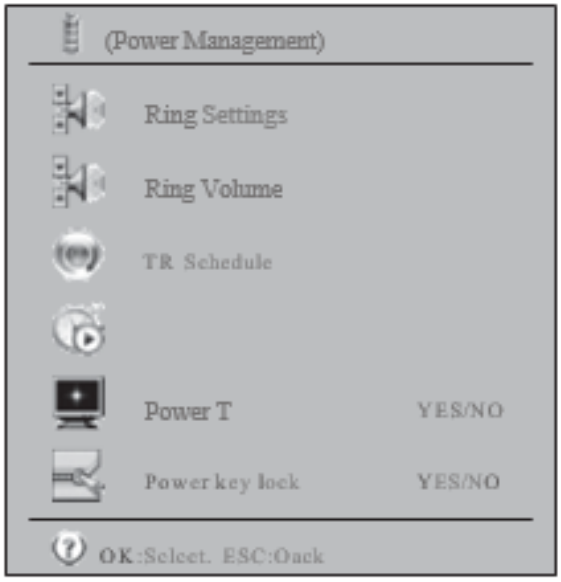
The third item is to enable or disable the "touch sensor". When the "touch sensor" is on, the fingerprint sensor will be turned off after a period of inactivity. When you apply your finger to the fingerprint sensor, it will be turned on automatically. This is to extend the life of the fingerprint sensor. The next item is sensor adjustment. When you select this item, the sensor will adjust to the current light intensity to provide the most accurate sensitivity. When you find that the fingerprint sensor is not sensitive enough, you can select this item lo adjust the fingerprint sensor. The fifth item is firmware update. If necessary, you can use the USB drive to update the firmware by adding more functions or debugging it. For example, you can set 23:05:10 as the auto power-off time.

The sixth item is "Restore Factory Settings." It is used to restore all settings to factory values. This will not affect the registration and our transaction data.

The ninth item is to delete all saved data. Be careful when using this item, as deleted records cannot be restored. The eighth item is to delete all management log records. When the management log records are close to being full, you can use this item to delete all management log records.

11.2.3 Power management

In power management, we can change the argument related to the power of the machine.



The first item is "bell settings." You can set the bell up to 12 times during the day. This setting can also be entered using the included attendance software.

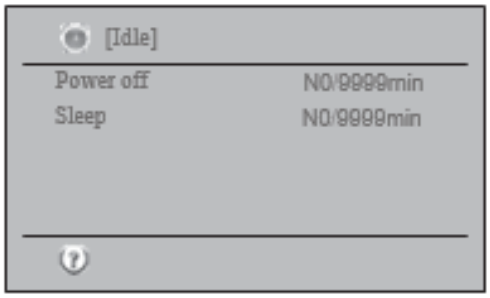
No.	STime	Use/No Use
1	00,00	Disable
2	00,00	Disable
3	00,00	Disable
4	00,00	Disable
..	00,00	Disable

The second item is "ring count". It is used to set the number of ringing repeats. The acceptable range is from I to 255. If you set the ringing time and the ring count is zero, the bell will not ring. For the bell to ring at a certain time, the number of rings should be>= I.

The third item is "TR schedule." Here you can set 10 time zones for different verification statuses. There are 6 statuses to choose from. They are duty on, duty off, overtime on, overtime off, go out on and go out off. When retrieving data from the machine, there is a flag in our transaction to indicate what status the record has.

No.	STime	ETime	Status
1	08,00	11,59	Duty On
2	12,00	13'00	Duty On
3	00,00	00,00	Duty On
4	00,00	00,00	Duty On
5	00,00	00,00	Duty On
6	00,00	00,00	Duty On
7	00,00	00,00	Duty On
8	00,00	00,00	Duty On
9	00,00	00,00	Duty Off
10	00,00	00,00	Duty Off

The fourth item is the idle setting. It consists of two sub-items - shutdown and sleep. You can set the number or minutes of idle time for the device to turn off or enter sleep mode. When the device enters sleep mode, you can press your finger on the fingerprint sensor or press any key on the keyboard to wake it up. The recorder has been turned off, you can press the power button to turn it on again.



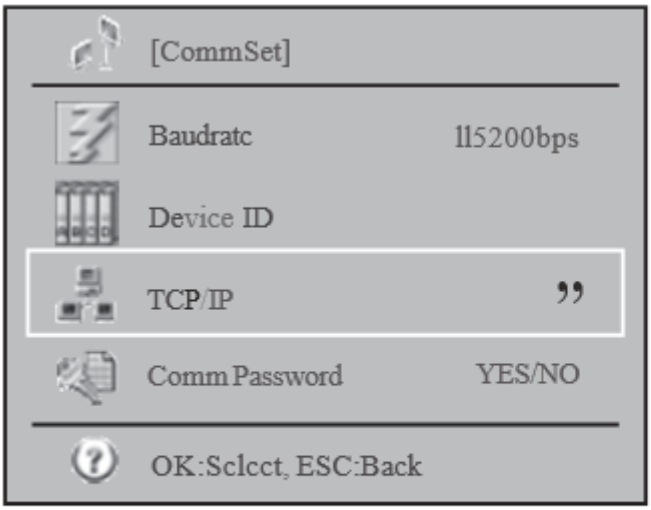
The fifth item is power off. With this item, you can set the time for the automatic shutdown of the device.

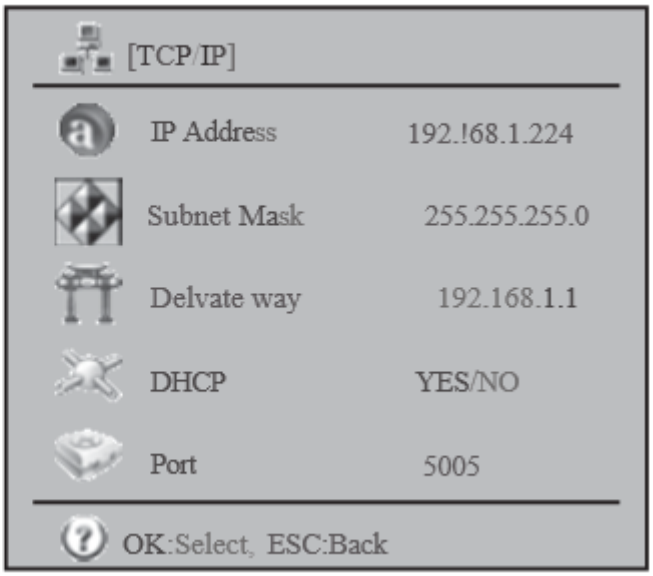
You can enter a time up to one second. The default value is no power-off schedule.

The last item is "power key lock". When "power key lock" is set to yes, you cannot turn off the device with the power button, but you can use it to turn on the device. In this case, the only way to turn off the device is to unplug the power supply. When the fingerprint machine is used for access control, we will tum on "power key lock" to prevent the machine from being turned off by mistake.

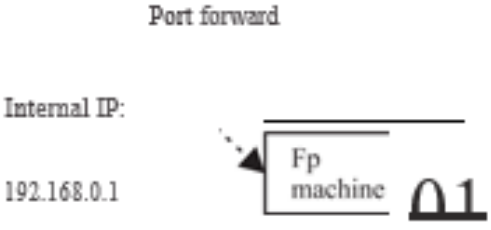
11.2.4 Communication settings

This is to change the configuration of the fingerprint machine in terms of communication with the computer software. First of all, we need to know what kind of physical communication is used.





This fingerprint machine can have communication or TCP/IP and USB cable. For the network, we need to configure the TCP/IP element, which consists of IP address, subnet mask, gateway, whether to use dynamic IP assignment and port number. If you have set a forward port on your router for an external computer to connect to an internal fingerprinting device, you need to set the IP address of the gateway. If your network has a DHCP server, you can enable dynamic IP address assignment to get a dynamic IP address from the DHCP server. The port number acts like a cell phone number that listens for service requests.

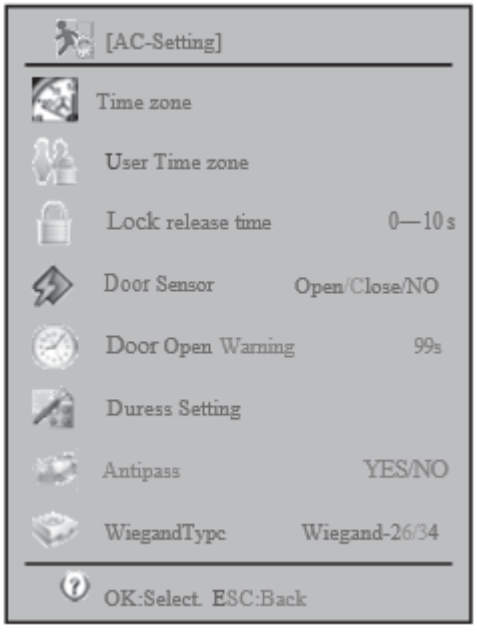


The last parameter is the communication password. It is used to prevent communication with other people. We will change the communication password the first time we use it.

11.2.5 Login Settings

11.2.6 Control At.'Ct.''S (Option).

Access control involves setting a parameter in the door opening control. The first parameter is to set the time zone. Time zone means the period with entry time and exit time. 50 time zones can be set in the device. For each time zone, entry and exit times can be set for Monday through Sunday and holidays.



Time zone (50 sets)

Time zone
1
2
....

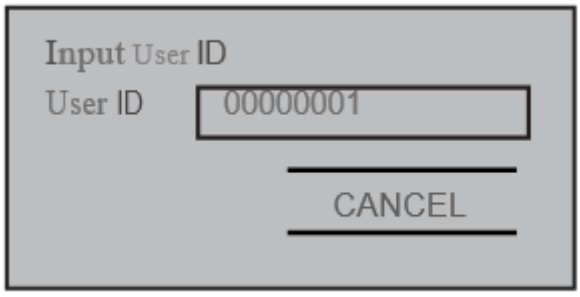
Day	Time
	00:00-23:59
Monday	00:00-23:59
Tuesday	00:00-23:59
Wednesday	00:00-23:59
Thursday	00:00-23:59
Friday	00:00-23:59
	00:00-23:59
Holiday	00:00-23:59
M o o	

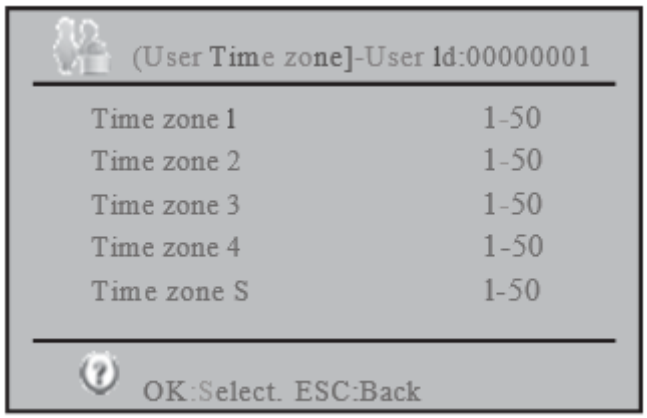
In user access control, we can assign a time zone to each user. Each user can have a maximum of 5 time zones. If more than I time zone is assigned, the time zones are additive. For example, we have time zone 1 and time zone 2.

Time zone	Day or Week	Time Range
	Mon	9-18
	Mon	19-23

When user 11 is assigned these 2 time zones, he can enter on Monday from 9am to 6pm and 7pm to 11pm.

When you make an assignment, you must first enter the user ID. Then you can enter from 1 to 50 time zones to the time zone of 5 users.



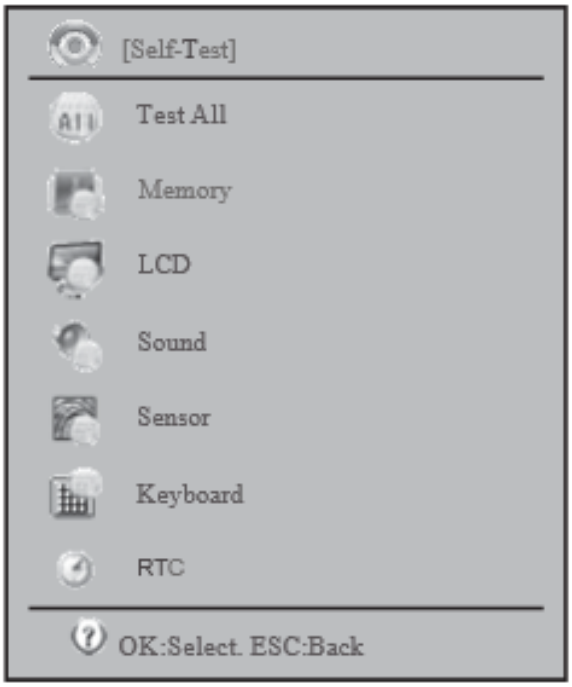


When you connect the fingerprint machine to the door sensor to detect the status of the door opening, you must tell the machine what type of door sensor you are using. There are normal open type and normal closed type.

The open door alarm is the time to keep the door open, which will cause an alarm to fire. This is to prevent someone who is not authorized to enter. So, when someone comes inside, the door must be closed within a certain period of time.

11.2.7 Auto test

It is used when problems are found in the use of the device. For example, a user presses a button on the keyboard without responding. Then run an auto test to see if the keyboard has a problem. You can test all hardware components or just one of them. The components you can select are memory, LCD, voice, fingerprint sensor, keyboard and real-time clock.

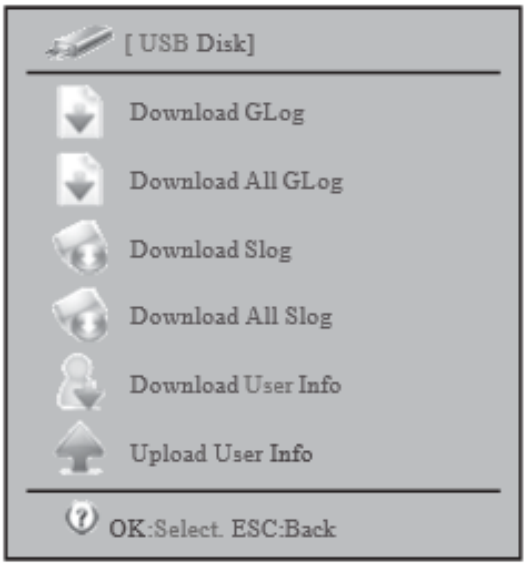


11.3 USB flash drive management

Contains a list of items for downloading/uploading data to/from the USB flash drive. Using this menu, we can download data for recording (all or by user ID) to the USB flash drive. The save file is encrypted, it cannot be seen by opening it. It can only be read by other FP machines. We can also download all/part of the management log record to the USB flash drive. The management log file is a text file. It can be viewed with an ordinary editor such as Notepad. First, we can download all input/output transactions or by range?

These transactions can be read by the included turnout software to record the write verification. The file is in text format, which can be read by an ordinary editor.

The system query contains system information, device information and advanced query. In the system information, the status of various figures can be used.



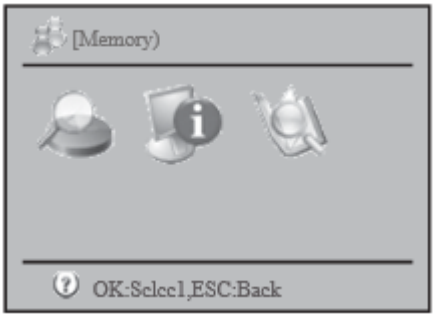
For example, the use of a fingerprint template is 1/1000. This means that the total number of fingerprints in the device is 1000, and only one has been used.

In the device information, we can check the manufacturing date, serial number, manufacturer, device stock name, device model, fingerprint algorithm and firmware version. The serial number is the most important. It is used for maintenance by the vendor. The fingerprint algorithm is useful for checking whether a fingerprint is compatible with another fingerprint model.

In advanced queries, we can use various input criteria to query the input/output transaction record, management log and registration.

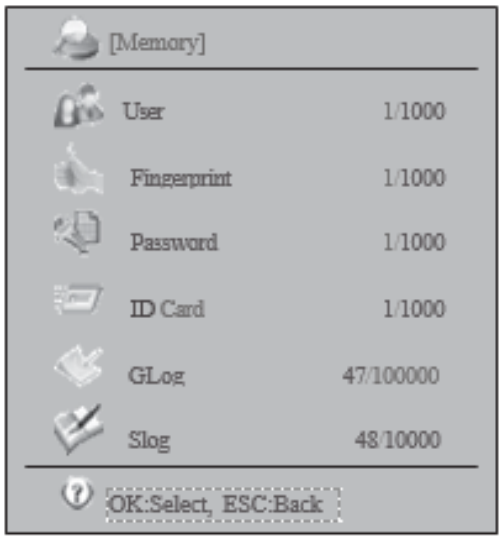
11.4 System information

The fourth item in the main menu is system information. Here you can check memory, device information, operation, and perform advanced search for registration and verification records.



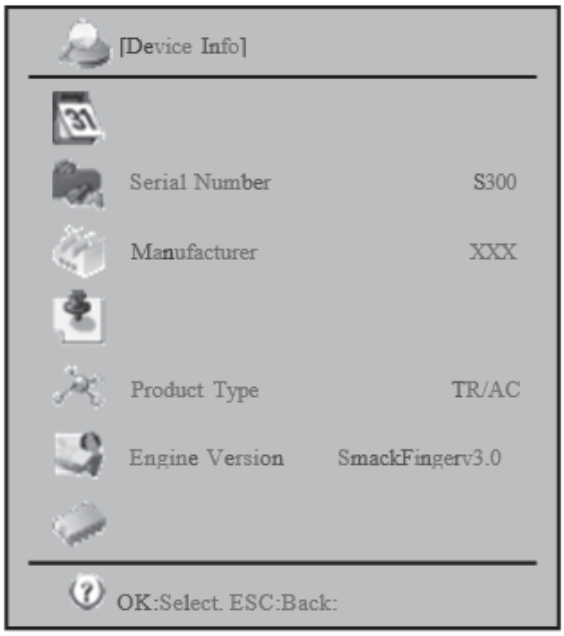
11.4.1 Memory

For example, the use of a fingerprint template is 1/1000. This means that the total number of fingerprints in the device is 1000, and 1 template has been used.



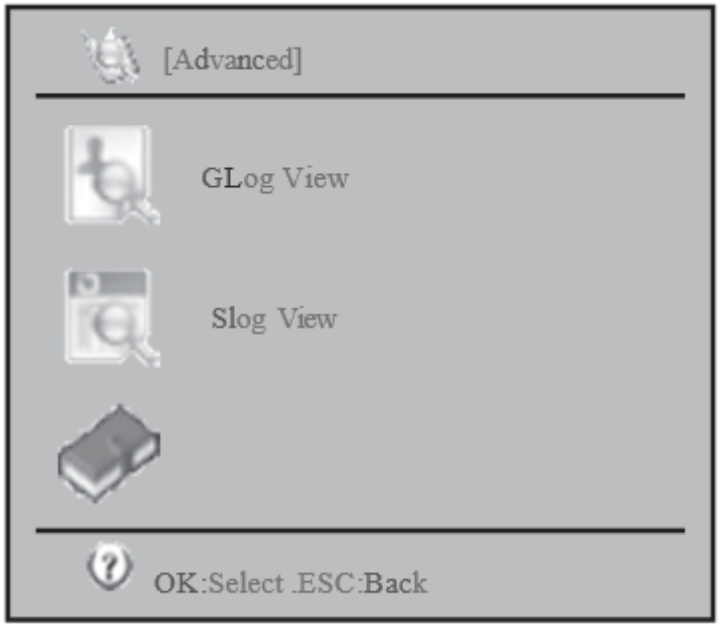
11.4.2 Device information

In the device information, we can check the manufacturing date, serial number, manufacturer, device firmware name, device model, fingerprint algorithm and firmware version. The most important is the serial number. It is used for maintenance by the vendor. The fingerprint algorithm is useful for checking whether the fingerprint is compatible with another fingerprint model.



11.4.3 Advanced

In the advanced query, we can use different input criteria to query input/output transaction record, management log and records.



12. Questions and answers

12.1 We cannot verify the fingerprints of some users.

This may be because the fingerprint is polished, has many folds or is heavily exfoliated.

The solution is to remove the fingerprint and enter another fingerprint. The person will almost have all 10 fingerprints fail in registration or verification. Besides, the fingerprint machine has a 1:1 matching method.

12.2 Unable to communicate with the fingerprint machine.

First, check whether the com port of the software is equal to the corn port of the computer. To check the computer's corn port, right-click on the "my computer" icon and select "manage". In the left panel, select "device management "and explore the right panel "corn and lpt". Check the com port number. Also check that the baud rate of the machine and the software are the same.

Besides, check if the fingerprint machine is enabled.

The device number on the machine must also match the one entered in the software. Finally, we can check that the connected cable and converter are normal. For the connected cable, we can use a cable tester to check if the cable is suitable.

12.3 When the fingerprint remover is turned on, the LCD tips are displayed or only half of the screen is displayed.
Try replacing the LCD screen with a new one and see if the problem is solved. If so, it means that the
LCD has a problem. If it still can't display normally, the motherboard may have a problem. Then we can swap the problematic LCD screen to another machine and see if it works.

12.4 How to bypass the administrator
Sometimes we can't access the fingerprint machine's menu because it requires administrator verification. The administrator may have left. We can use turnout software to remove the administrator. It will change the administrator user to a regular user. This can be found in the download module - clear admin.

12.5 When the fingerprint device is turned on, the voice "please press your finger again" appears.
The fingerprint sensor may be dirty. Use some alcohol to clean it.
Or the cable of the fingerprint sensor is loose. Disassemble the machine and check if it is not.
Finally, it may be caused by a motherboard chip set. In this case, send the board back to the vendor.

12.6 When you use the serial cable for communication, you are downloading the registration data from the fingerprint machine, but not the data.
Reduce the transmission speed and try again. Remember to reduce both the fingerprint machine and the
software.

12.7 Using TCP/IP, you can download several days of data from a remote location. When downloading 2 weeks of data, the download fails.

This is due to the router waiting too short again.

12.8 When the fingerprint machine is hooked to the wall, a large number of users cannot enroll or perform verification. This is normal when the device is placed in a different location. Since the fingerprint sensor uses an optical image algorithm, strong light shines on the fingerprint sensor, the performance will be greatly degraded. Try placing the device in a place with less light.

13. Appendix

13.1 Power supply.

This fingerprint machine comes with a free power adapter. Just connect the adapter to 220V AC Power and connect the adapter head to the fingerprint machine. Then press button 10 and the machine will be turned on. Until then, the machine is in stand by mode. You can perform registration or verification.

13.2 Communication with the computer

We can communicate with the fingerprint machine through computer software in 2 ways USS cable

Ethernet

For Ethernet to work, the machine must have an IP address. The network part of the IP address must be the same as the computer's

For example, the IP of the computer: I 92.168.0.100, IP of fingerprint machine: 192.168.0.224

13.3 Connection of external scale reader (FP Reader).

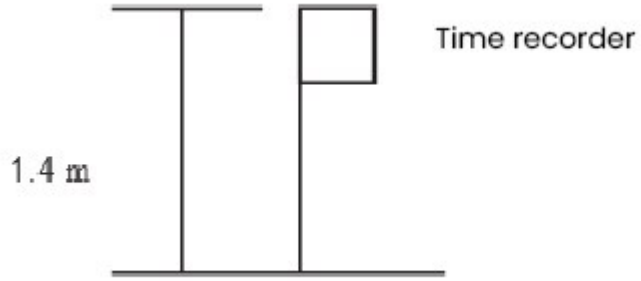
The first 3 numbers represent the network. They must be the same.

To connect the fingerprint machine to the computer directly, we need a 10/100 Base-T Ethernet cross cable. To connect them through a hub/switch, we need a 10/100 Base-T straight Ethernet cable.

Installation

We used to install T6 in the wall. This is because it can avoid the strong light shining on the optical fingerprint sensor. This will seriously affect the recognition ability of the fingerprint device.

Normally, we will mount the device to the wall at about 1.4 meters high.



On the back of the device is a metal rack with which the fingerprint device can be mounted on the wall.