User Manual

MA300

Version: 2.0

Date: December, 2013

Notational Conventions

This document includes such notational conventions as tips, important notices and precautions. The notations contained in this manual include:

 : indicates important information, including precautions, which must be read carefully to achieve the optimal equipment performance.

 : indicates the voice prompt generated by the device. In the event of discrepancy between the voice prompts in this document and those generated by the actual products, the latter shall prevail.

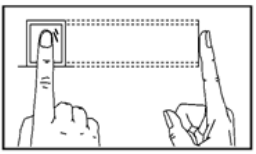
Table of Contents

1 Instruction for Use

1.1 Finger Placement

Recommended fingers: The index finger, middle finger or the ring finger; the thumb and little finger are not recommended (because they are usually clumsy on the fingerprint collection screen).

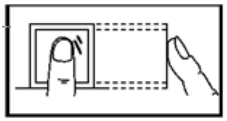
1. Proper finger placement:



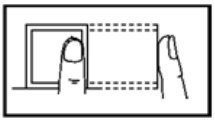
The finger is flat to the surface and centered in fingered guide.

2. Improper finger placement:

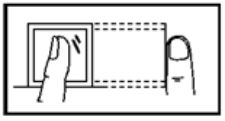
Not flat to the surface



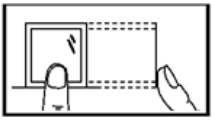
Off-center



Slanting



Off-center



Please enroll and verify your fingerprint by using the proper finger placement mode to avoid degradation of verification performance due to improper operations. ZKSoftware reserves all rights for the final interpretation and modification of these rules.

1.2 Instruction for Card Swipe

Integrated with a non-contact RF card reader module, this device supports the ID cards and MIFARE cards (optional and only used as PIN cards). By offering multiple verification modes such as fingerprint verification and RF card verification, this device can accommodate to diversified user needs.

Swipe your card across the sensor area following the voice prompt and remove your card after the device has sensed it. For the swipe area, see 2.2 Product Appearance.

1.3 Precautions

Protect the device from exposure to direct sunlight or strong beam as strong beam greatly affects the fingerprint collection and leads to fingerprint verification failure.

It is recommended to use the device under a temperature of 0–50°C so as to achieve the optimal performance. In the event of exposure of the device to the outdoors for long periods of time, it is recommended to adopt sunshade and heat dissipation facilities because excessively high or low temperature may slow down the device operation and result in high false rejection rate (FRR) and false acceptance rate (FAR).

When installing the access control device, please connect the power cable after connecting other cables. If the device does not operate properly, be sure to shut down the power supply before performing necessary inspection. Note that any live-line working may cause damage to the device and the device damage arising out of live-line working falls beyond the scope of our normal warranty.

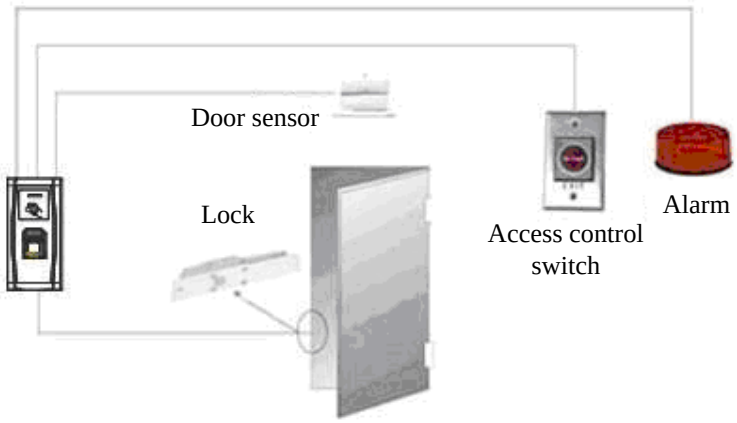
For matters that are not covered in this document, please refer to related materials including the Device Installation Guide, Access Control Management Software User Manual.

2 Introduction of Access Control Device

2.1 Overview of Device Functions

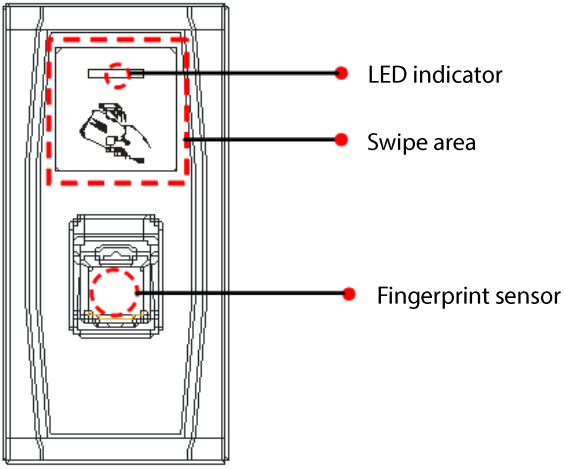
As an integrated fingerprint & access control device, our product can be connected with either an electronic lock or an access controller. This device features simple and flexible operations and supports the use of management cards. With a management card, you can perform such functions as offline enrollment, user enrollment and pen drive management. The voice prompts will guide you through all the operations without screen display. This device comes without a keyboard, but it allows you to connect an external keyboard and offers multiple operation modes. It supports multiple communication modes. The pen drive features simple and convenient operations. The waterproof design and metal case of the device allow it to withstand a heavy impact without damage.

Featuring a compact and simple design, this device allows users to connect several devices through a PC and perform real-time monitoring.



2.2 Product Appearance

Front view:



- **LED indicator: The LED indicator is used to display device operation results and exceptional statuses which are defined as follows:**

  Common rules: If an operation succeeds, the green indicator is solid on for one second; otherwise, the red indicator is solid on for one second.

  Enrollment state: The green LED blinks three times every other three second.

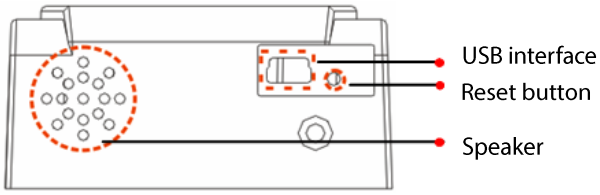
  Single user deletion: The red LED blinks three times every other three second.

  Verification state: The green LED blinks once every other two second.

- **Swipe area**: refers to the area in the red dashed-line box as shown in the figure above.

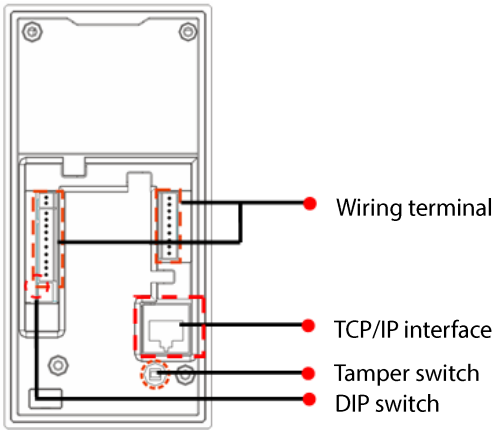
- **Fingerprint sensor**: Used to collect and match fingerprints and delete users.

Bottom view:



- USB interface: used to connect with a pen drive or a keyboard.
- **Reset button**: used to restart the device.
- **Speaker**: used to play the BEEP sound and voice prompts. If a user passes the verification, the speaker beeps once; if the user fails to pass the verification, the speaker produces one short beep and one long beep. The default prompts during operation: Beep + voice prompts.

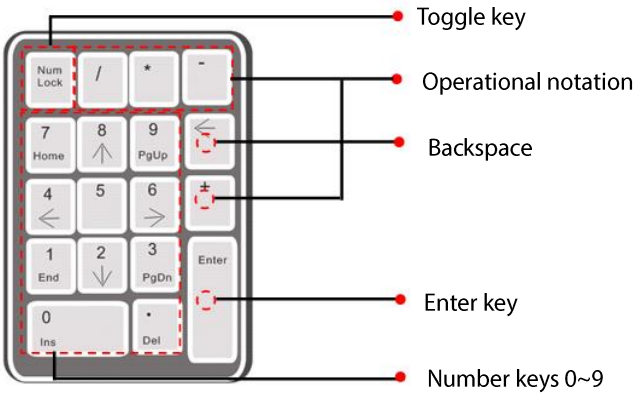
Rear view:



- **Wiring terminal**: connects with locks and power supply through cables.
- **TCP/IP interface:** The TCP/IP interface connects with a PC through a network cable (for detailed connection, see the Installation Guide).
- **Tamper switch**: used to generate a tamper alarm. For details, see 3.5 Tamper Switch.
- **DIP switch**: The DIP switch has four pins numbered 1, 2, 3 and 4. In the RS485 communication mode, the first 1, 2 and 3 pins are used to set hardware device number and the fourth pin is used to select the break-make status of terminal resistance. For detailed settings, see the Installation Guide.

2.3 Use of an External USB Keyboard

To facilitate device operations, you can connect the device with an external USB keyboard (purchased by users) and conveniently perform such operations as user enrollment, deletion and restoring factory defaults, especially when specifying user IDs during user enrollment and deletion.



An external USB keyboard is shown above (please refer to the actual product):

NumLock is a numeric keypad toggle key. It is activated by default. If it is activated, the LED indicator is on. When the device is connected with an external keyboard, you can only use the numerical keys, backspace key and Enter key in the NumLock activated state.

2.4 Verification State

Verification state: After the device is powered on, the device enters the verification state if you have enrolled or successfully enrolls a management card or in the event of timeout of any operation.

In the verification state, all users are allowed to verify their identity and unlock (the administrator bearing a management card can only unlock using his/her fingerprint(s) previously enrolled); the administrator can perform such operations as user enrollment/deletion, pen drive management and keyboard operation.
Note: A management card only works on the MA300.

2.5 Management Card

The device users are classified into administrators and ordinary users.

Administrators: An administrator is allowed to perform all operations including user enrollment/deletion (deleting all the other users except him/her) and pen drive management. The privileges of the device administrators are implemented through the management cards.

Ordinary users: Ordinary users are only allowed to verify their identity and unlock.

A management card is a card specially allocated for a super administrator. Each device must at least enroll one management card. If no management card is enrolled, you cannot perform any operation and the system will generate a voice prompt "🗣: Please register the management card".

You can implement different functions by swiping a management card for different times in a row:

No pen drive and external keyboard are connected:

- By swiping the management card once, you can go into the single user enrollment state.
- By swiping the management card five times in a row, you can enter the single user deletion state.

Pen drive is connected:

- By swiping the management card once, you can go into the pen drive management state.

An external keyboard is connected:

- By swiping the management card once, you can activate the external keyboard.

Consecutive swipes: Consecutive swipes mean the interval between two swipes in a row is less than 5 seconds.

The management cards can be deleted through the "Clear All" function of the keyboard, or have their administration privileges cleared through software before they are deleted as ordinary ID cards. For details, see the *Access Control Software Operating Instruction*.

The fingerprints of the user who bears a management card can only be enrolled through software. For details, see the *Access Control Software Operating Instruction*.

Tip: Users who bear management cards can only verify their identity and unlock using their fingerprints previously enrolled.

2.6 System Password

A system password is a password used to enhance the security of device data in TCP/IP or RS485 communications.

Tip: The system password can be modified through the access control software. For details, see the *Access Control Software Operating Instruction*.

2.7 Operation Timeout

The default operation timeout time is 30 seconds. When you enroll a management card or delete/enroll a user (including in the external keyboard enrollment and user deletion states), the system automatically prompts you once every other 10 second if there is no operation and returns to the verification state after prompting you three times. The voice prompt is "Operation timeout. The system returns to verification state".

Tip: You can set the timeout time through the access control software.

3 Device Operations

3.1 Management card

3.1.1 Enroll Management Card

To enroll a management card, proceed as follows:

1. The device automatically detects whether there exists a management card.

2. If the device fails to detect the presence of a management card, it enters the management card enrollment state. Then proceed with step3; otherwise skip to step 5.

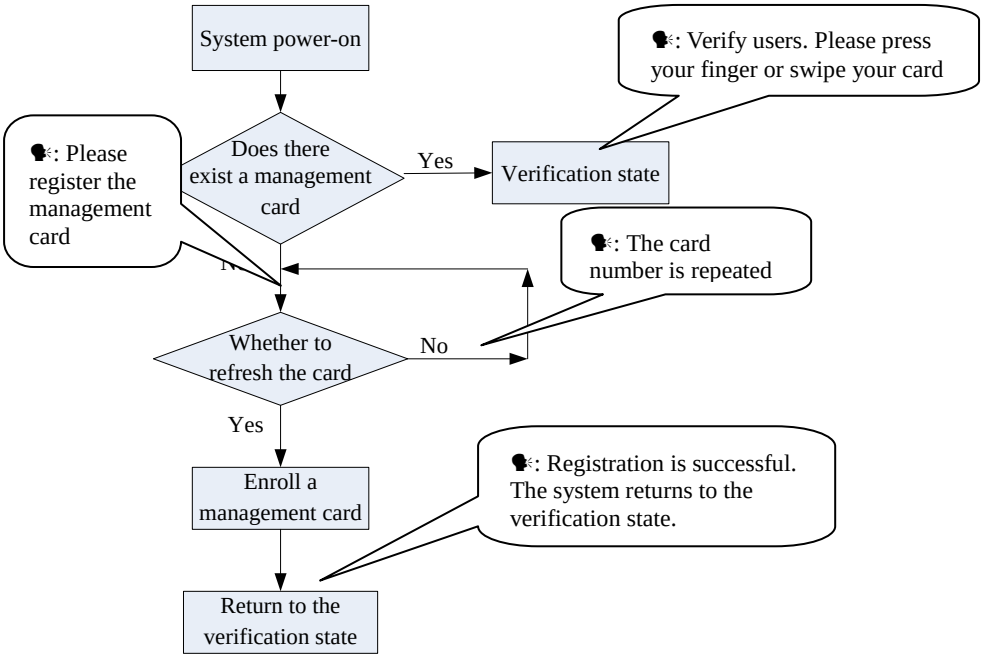
3. After the system generates the voice prompt "🗣: Please register the management card", you can swipe your card across the sensor area.

4. If enrollment fails, the system generates the voice prompt "🗣: The card number is repeated" and returns to step 3; if enrollment succeeds, the system generates the voice prompt "🗣: Registration is successful. The system returns to verification state".

5. After returning to the verification state, the system generates the voice prompt "🗣: Verify users. Please press your finger or punch your card".

Tip: The system returns to the verification state if any operation in step 3 times out and only prompts you to enroll the management card again after you power on the device again.

The management card enrollment flow chart is shown below:



3.1.2 Enroll Ordinary User

◆ **Enroll ID Card**

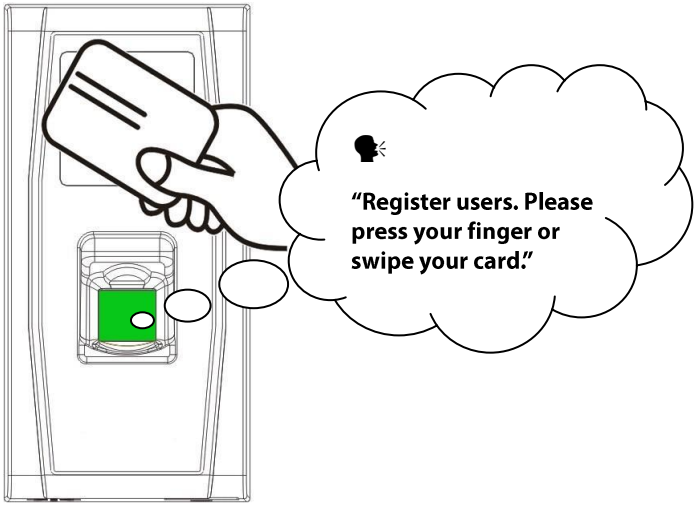
The mode for you to enter the enrollment state using the management card is known as the **management card enrollment mode**. In this mode, you can only enroll one user. When you enroll a new user, the system automatically assigns a minimum idle ID to the user. Furthermore, you can also use the **external keyboard enrollment mode** (for details, see 3.2.2 **Enroll a User Through Keyboard**) to implement enrollment of the user with ID.

In both these two enrollment modes, you can enroll new users. Each user is allowed to enroll 10 fingerprints and one ID card at most.

To enroll a user, proceed as follows:

1. In the verification state, the system goes into the ordinary user enrollment state after you swipe a management card once (In the enrollment state, swiping a management card once will return you to the verification state).

2. After the system generates the voice prompt "🗣: Register users. Please press your finger or swipe your card", you can start user enrollment. There are the following two cases:



(1) Swipe ID card first

a. When you swipe your new ID card and succeed in enrolling a user, the device will generate a voice prompt "🗣: User number **. Registration is successful!" (** refers to the ID automatically assigned to the user by the system; same below) and you can proceed to step **b**; if user enrollment fails, the system generates the voice prompt "🗣: The card number is repeated" and returns to the enrollment state, waiting for you to press your finger or swipe your card.

b. After the device generates the voice prompt "🗣: Register. Please press your finger", the system enters the specified fingerprint enrollment state. Press the same finger over the sensor three times following the voice prompts.

c. If fingerprint enrollment succeeds, the system generates the voice prompt "🗣: Registration is successful. Register. Please press your finger" and directly enters the next fingerprint enrollment state; if fingerprint enrollment fails, the system generates the voice prompt "🗣: Please press your finger again" and repeats step b.

d. The system automatically returns to the verification state when both 10 fingers and ID card are enrolled, the management card is swiped once or operation times out.

(2) Press finger(s) first

a. Press the same finger over the sensor three times following the voice prompts by adopting the proper fingerprint placement. If fingerprint enrollment succeeds, the system generates the voice prompt "🗣: User number **. Registration is successful" and you can proceed to step b; if fingerprint enrollment fails, the system generates the voice prompt "🗣: Please press your finger again" and returns to the enrollment state, waiting for your to press your finger or swipe your card.

b. After generating the voice prompt "🗣: Register. Please press your finger or swipe your card", the system enters the specified user information enrollment state, waiting for you to swipe your new ID card or press your finger.

c. If the ID card enrollment succeeds, the system generates the voice prompt "🗣: Registration is successful. Please press your finger" and enters the fingerprint enrollment state directly; if you press a finger that is not enrolled before and succeeds in enrollment of this finger, the system generates the voice prompt: "🗣:

Registration is successful. Please press your finger or swipe your card" and you can continue enrolling new fingerprints and card. After you enroll 10 fingerprints, the system will generate the voice prompt "🗣: Please swipe your card" to enroll your ID card if your ID card is not enrolled.

d. The system automatically returns to the verification state when both 10 fingers and ID card are enrolled, the management card is swiped once or operation times out.

3. If you are already assigned with an ID, then there are the following two cases for you to enroll your fingerprint(s) or card:

(1) Enroll fingerprint(s) when you have already enrolled card

a. After you swipe the enrolled card, the system will generate the voice prompt "🗣: User number **. Register. Please press your finger" (** refers to the ID assigned to you; same below) and enter the fingerprint enrollment state. Your enrolled fingerprint(s) will overwrite all previous fingerprints.

b. Press the same finger over the sensor three times following the voice prompts by adopting the proper fingerprint placement. If fingerprint enrollment succeeds, the system generates the voice prompt "🗣: User number **. Registration is successful" and gets ready for enrollment of next fingerprint.

c. The system automatically returns to the verification state when both 10 fingers and ID card are enrolled, the management card is swiped once or operation times out.

Tips:

1. The fingerprint(s) enrolled in this step will overwrite all your previously enrolled fingerprints.

2. In this mode, the fingerprint of the user who bears the management card cannot be enrolled because swiping the management card will return the system to the verification state automatically.

(2) Enroll card and fingerprint(s) when you have already enrolled fingerprint(s)

a. Press the finger with fingerprint already enrolled three times following the voice prompts. If you are identified as the same person in each of verification attempt, the system enters the fingerprint enrollment state.

b. After generating the voice prompt "🗣: User number **. Register. Please press your finger or swipe your card", the system starts to enroll your fingerprint. Your fingerprint(s) enrolled in this step will overwrite all your previous fingerprints.

c. If the ID card enrollment succeeds, the system generates the voice prompt "🗣: Registration is successful. Register. Please press your finger" and enters the fingerprint enrollment state directly; if you press a finger that is not enrolled before and succeeds in enrollment of this finger, the system generates the voice prompt: "🗣: Registration is successful. Please press your finger or swipe your card" and you can continue enrolling new fingerprints and card. After you enroll 10 fingerprints, the system will generate the voice prompt "🗣: Please swipe your card" to enroll your ID card if your ID card is not enrolled.

d. The system automatically returns to the verification state when both 10 fingers and ID card are enrolled, the management card is swiped once or operation times out.

◆ **Enroll Mifare Card**

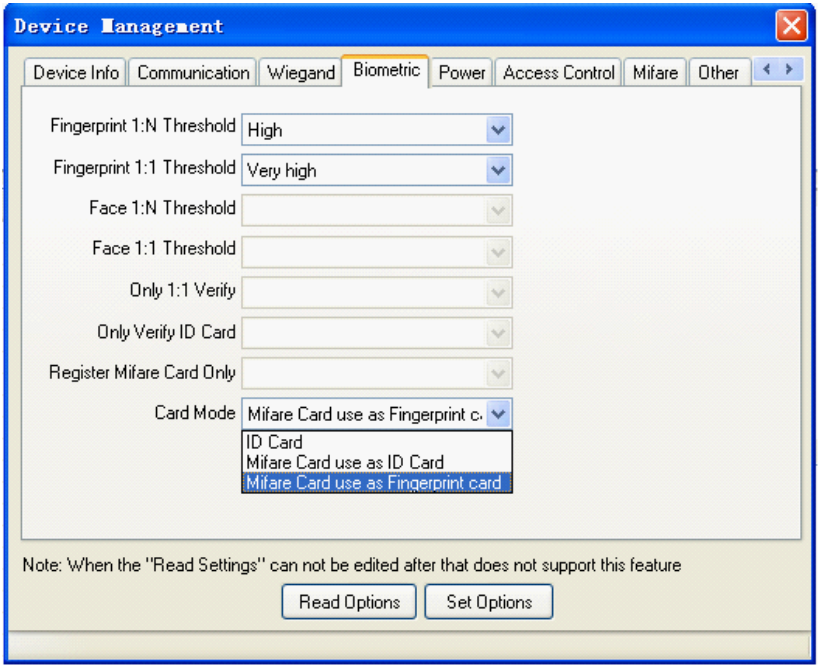
1. Use for ID Card, please refer to the above setups of Enroll ID Card.

2. Use for fingerprinting card, steps similar Enroll ID Card, the only difference is that enroll ID card means single swipping card, but Mifare card registration need to write the fingerprint in the Card, procedure is as follows:

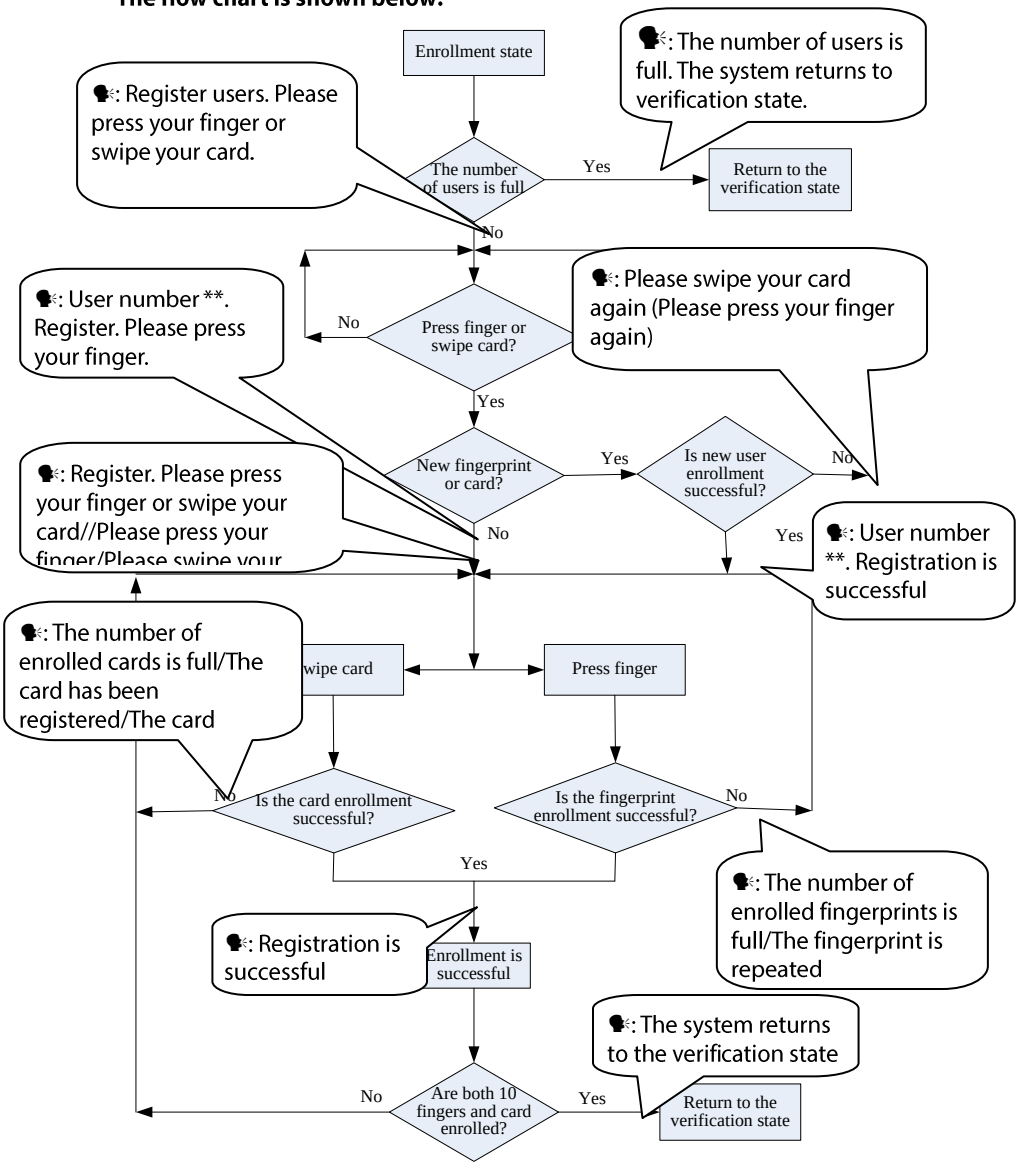
In the verification state, Swipe your admin card for one time enter to goes into the ordinary user enrollment state (In the enrollment state, swiping a management card once will return to the verification state). After the system generates the voice prompt "🗣: Register users. Please press your finger or swipe your card", you can start user enrollment. When you swipe new ID card in card area, start register fingerprints card, now the voice prompt "🗣: Please press your finger for three consecutive times and succeed in enrolling a user, the device will generate a voice prompt "🗣: Write fingerprints card, please wait later, please swipe card again". succeed in enrolling a user after swipe card, the voice prompt "🗣: User number **. Registration is successful!" (** refers to the ID automatically assigned to the user by the system).

Tip: If Mifare card regard as ID card or fingerprinting card for change use, should get through "Access Control software" operation, the details as follows setups:

With equipment through the Ethernet connection, then open the "Access Control software"—【Device Management】(choose device name)—【 Biometric 】—【 Card Mode 】, can select what you want.


Device Management
Device Info
Communication
Wiegand
Biometric
Power
Access Control
Mifare
Other
Fingerprint 1:N Threshold
High
Fingerprint 1:1 Threshold
Very high
Face 1:N Threshold
Face 1:1 Threshold
Only 1:1 Verify
Only Verify ID Card
Register Mifare Card Only
Card Mode
Mifare Card use as Fingerprint c
ID Card
Mifare Card use as ID Card
Mifare Card use as Fingerprint card
Note: When the "Read Settings" can not be edited after that does not support this feature
Read Options
Set Options

The flow chart is shown below:



3.1.3 Register FPCard

To use an FP card of an FRT on another FRT, you must register a new FP card on current FRT.

Swipe your admin card for consecutive twice, enter to the "registration fingerprint card" operation.

Note: there were fingerprint card, were related the MA300 machine.

3.1.4 Unregister FPCard

To prohibit the use of an FP card on an FRT, you must deregister this card from this FRT.

Swipe your admin card for three consecutive times, enter to the "logout fingerprint card" operation.

Note: there were fingerprint card, uncorrelated the MA300 machine.

3.1.5 Empty FPCard

Delete all the data (fingerprints and numbers) of the FP card.

Swipe your admin card for four consecutive times, enter to the "empty fingerprint card" operation.

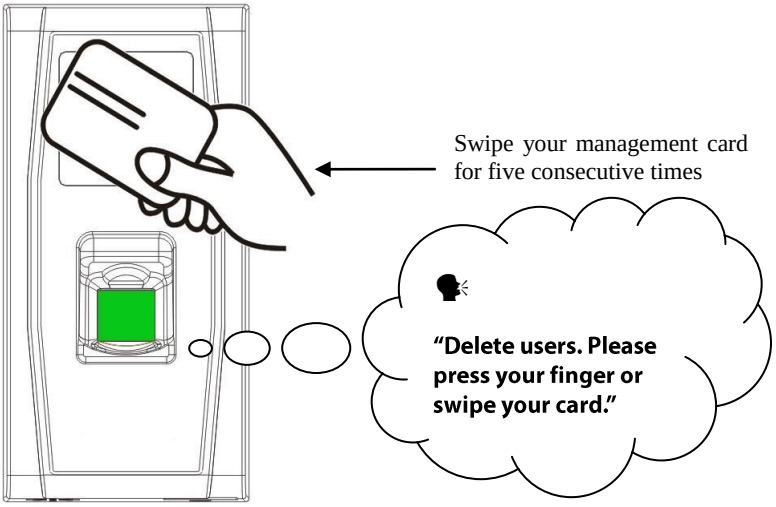
Note: Empty all the fingerprint data within card.

3.1.6 Delete a Single User

Deleting a user by using a management card is called the **simple single-user deletion mode**. Deleting a user by using an external keyboard is called the **specified user deletion mode**. (See 0_3.2.3 Delete a Specified User)

The operation steps for simple single-user deletion:

1. In verification state, swipe your management card for five consecutive times to enter the simple single-user deletion state (swipe your card one more time to return to the verification state).



2. The system checks whether the user has been enrolled. If not, the system will generate the voice prompt "🗣: Unregistered user. The system returns to verification state."; otherwise, the system will generate the voice prompt "🗣: Delete users. Please press your finger or swipe your card."

3. Press your finger onto the fingerprint sensor or swipe card over the card reader.

(1) Press your finger onto the sensor to delete a user.

Press one of your enrolled fingers properly onto the sensor. If the verification succeeds, the system will generate the voice prompt "🗣: User number **. Deletion is successful. Delete users. Please press your finger or swipe your card." (** indicates the ID number of the user) and automatically return to the deletion state. If the verification fails, the system will generate the voice prompt "🗣: Please press your finger again."

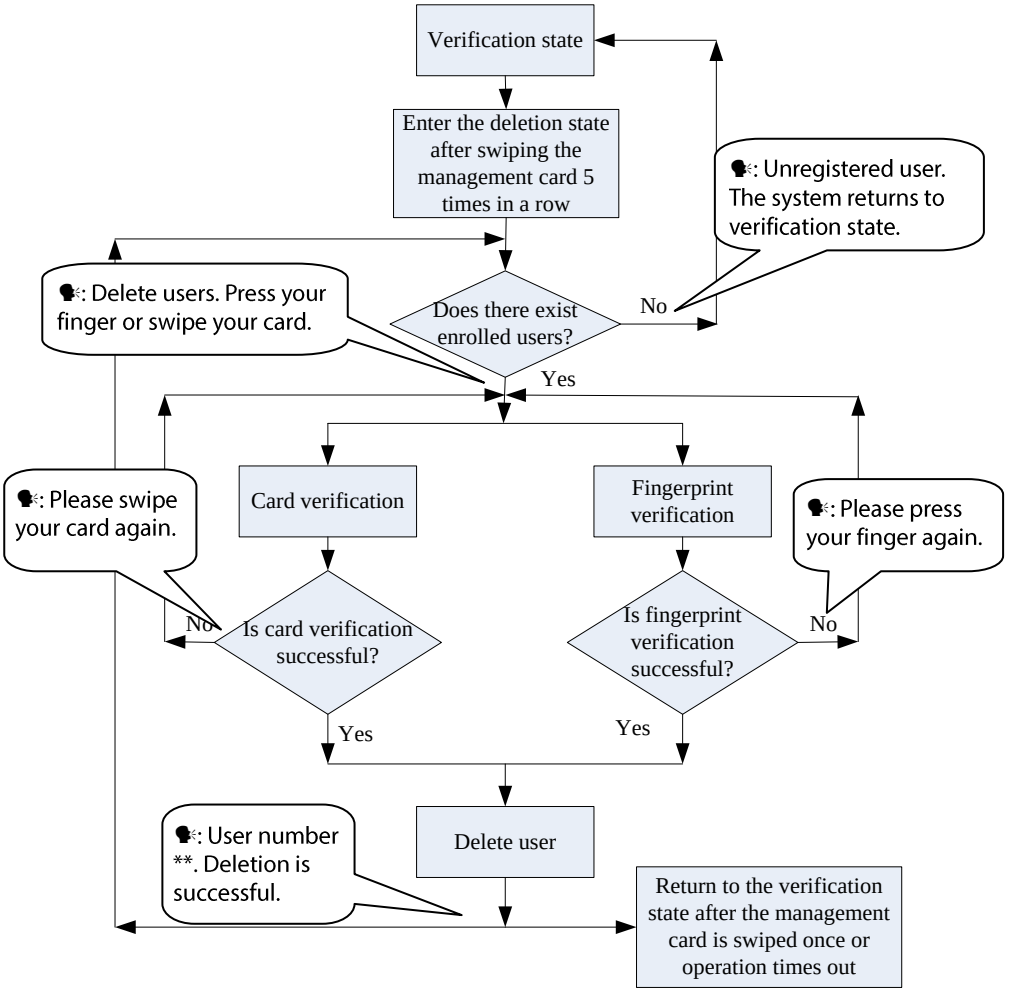
(2) Swipe your card over the reader to delete a user.

Swipe a registered card over the reader. If the verification succeeds, the system will generate the voice prompt "🗣: User number **. Deletion is successful. Delete users. Please press your finger or swipe your card." and automatically return to the deletion state. If the verification fails, the system will generate the voice prompt "🗣: Please swipe your card again."

4. If you swipe your management card one more time or your operation times out, the system will return to the verification state.

Tip: In simple single-user deletion mode, management card users cannot be deleted because swiping the management card will return the system to the verification state.

Simple Single-User Deletion Procedure:



3.1.7 Switching RS485 Reader Function

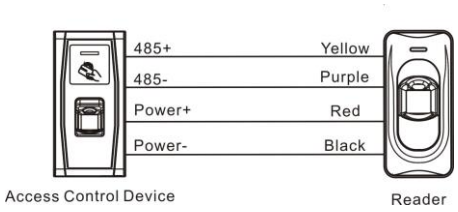
The MA300 supports the RS485 reader function, and it can be connected to the FR1200 reader through the RS485. The RS485 reader function can be switched by swiping the management card seven times.

1) After a user swipes the management card seven times, if the last time MA300 beeps once, that means RS485 reader function has been disabled. The MA300 communicates with the computer in RS485 mode.

2) After a user swipes the management card seven times, if the last time MA300 beeps twice, that means RS485 reader function has been enabled. The MA300 communicates with the RS485 reader.

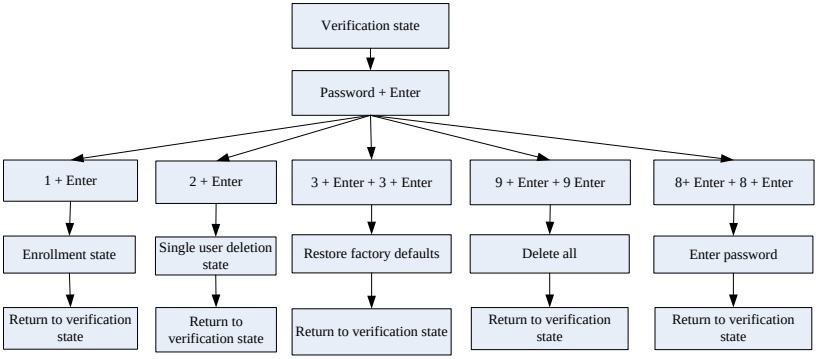
Note: To switch the communication function of the RS485 reader, you need to restart the device.

Besides, The MA300 can be connected to the external RS485 reader to work in master/slave mode. That is, the MA300 serves as the master and the RS485 reader serves as the slave. In addition, the RS485 anti-passback function is supported. If the RS485 reader function is enabled, the MA300 cannot communicate with the computer in RS485 mode.



3.2 USB Keyboard Operations

The keyboard operations flow chart is shown below:



3.2.1 Set Keyboard Password

If the user needs an external keyboard, he/she can connect the keyboard to the device and then swipe his/her management card to activate the external keyboard.

The system enables the user to set a dedicated password for the external keyboard.

Operation steps:

1. In verification state, connect an external keyboard with the device through the USB interface.

2. Swipe your management card once to activate the keyboard. The system generates the voice prompt "🗣: Please press the keyboard."

3. Type in "8" and press **Enter**. Then type in "8" and press **Enter** again. The system generates the voice prompt "🗣: Please set password." Type in your desired password and press **Enter**. The system generates the voice prompt "🗣: The operation is successful. The system returns to verification state." If there are no keystrokes within 30 seconds, the system will generate the voice prompt "🗣:

Operation timeout. The system returns to verification state." (**The password must be between 4 and 6 digits long.**)

The user can enter this password to activate the functions of the external keyboard at the next use, or swipe a management card once (which is mandatory for the first use of the external keyboard).

1. If you enter a wrong password for six consecutive times, the keyboard will be locked and you will have to power on the keyboard again to unlock it.
2. If there are no keystrokes within 30 seconds after the keyboard is activated, the keyboard function will be automatically deactivated and you will have to reactivate it.
3. The keyboard must to be inserted or removed at an interval of over 15 seconds, otherwise the system cannot identify its state.

3.2.2 Enroll a User Through Keyboard

Enrolling a user by using a USB keyboard is called **keyboard based enrollment mode**. In this mode, the user can enroll a user with the specified user ID.

Operation steps:

1. As shown in 3.2 USB Keyboard Operations flow chart, type in "1" and press **Enter** to enter the enrollment state.
2. When the system generates the voice prompt "🗣: Register users. Please input the user number.", enter a user ID.
3. The system generates the voice prompt "🗣: User number **. Register. Please press your finger or swipe your card." (** indicates the ID number of the user; same below) The system enters the specified ID enrollment state.

Tips:

1. If a user has enrolled in the system with a management card, the system will generate the voice prompt "🗣: User number **. Please press your finger."

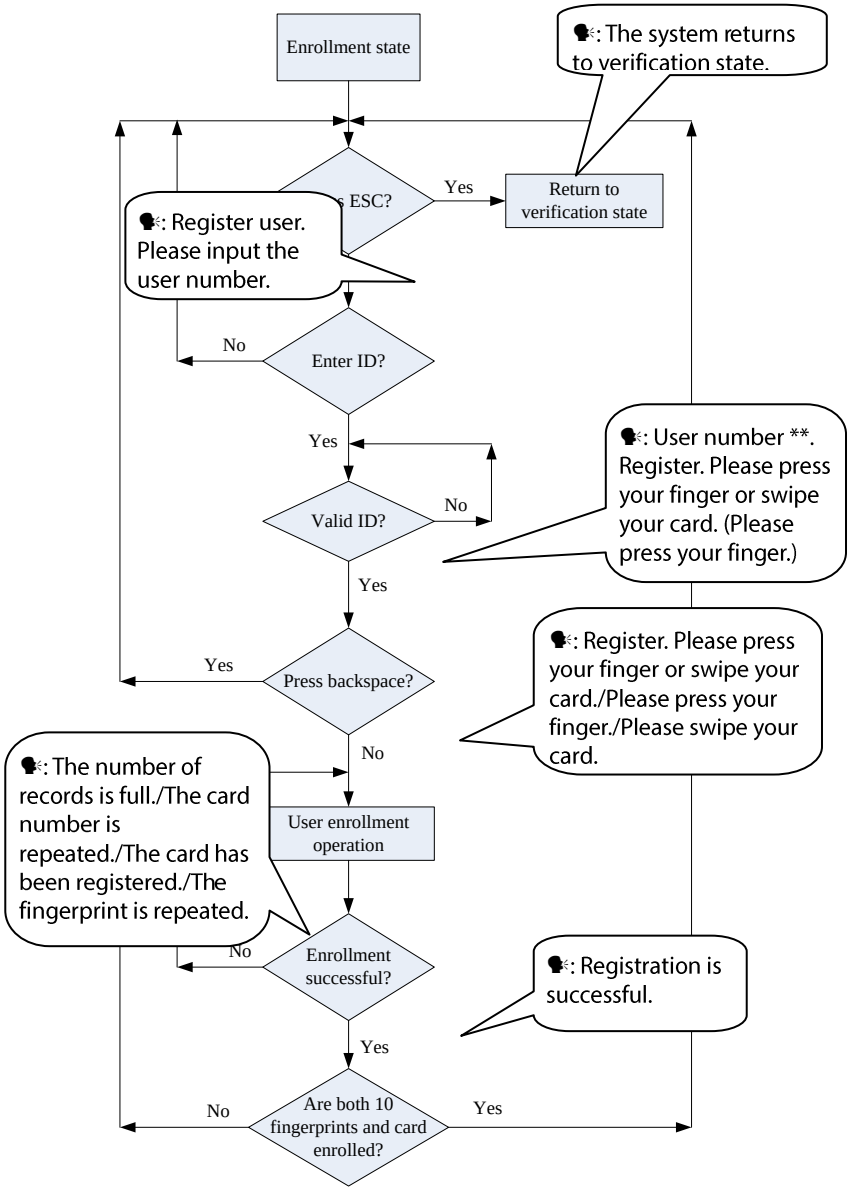
2. If a user has enrolled in the system with a user ID and 10 fingerprints, the system will generate the voice prompt "🗣: User number **. Please swipe your card."

4. The user enroll operation in the specified ID enrollment state is similar to the specified ID enroll operation in the management card enrollment mode. For details, see 0 3.1.2 Enroll Ordinary User.

5. In the enrolled user ID standby state, press **ESC** to return to the verification state. In the specified user ID enrollment state, press **ESC** twice to return to the verification state.

Tip: In keyboard based enrollment mode, you can enroll users consecutively. Upon successful enroll, the system automatically returns to the enrollment state.

The keyboard based enrollment flow chart is shown below:



Important Statement:

1. In keyboard based enrollment mode, if any operation times out, the system automatically prompts you of this operation once every other 10 second and returns to the verification state after prompting you three times.

2. Newly enrolled fingerprints will overwrite all the original ones in management card based enrollment mode, and keyboard based enrollment mode likewise.

3. A user can only enroll one card. When the user with an enrolled card enrolls in the system, the system generates the voice prompt "🗣: Register. Please press your finger." When the user swipes the card, the system generates the voice prompt "🗣: The card has been registered."

4. One card cannot be enrolled repetitively, otherwise the system will generate the voice prompt "🗣: The card number is repeated." during card swiping. Different users cannot enroll the same fingerprint, otherwise the system will generate the voice prompt "🗣: The fingerprint is repeated." during fingerprint enrollment. A user's new fingerprints will overwrite the existing ones.

The difference between two user enrollment modes with respect to the enrollment exit state:

1. In management card based enrollment mode with a specified user ID, the system returns to the verification state after you swipe your card once.

2. In keyboard based enrollment mode with a specified user ID, when you press **Esc**, the system returns to the enrollment state and generates the voice prompt "🗣: Register users. Please input the user number." You can enroll a user ID and press **Esc**. Then the system generates the voice prompt "🗣: The system returns to verification state."

3.2.3 Delete a Specified User

Deleting a user by using an external keyboard is called the **specified user deletion mode**.

Operation steps:

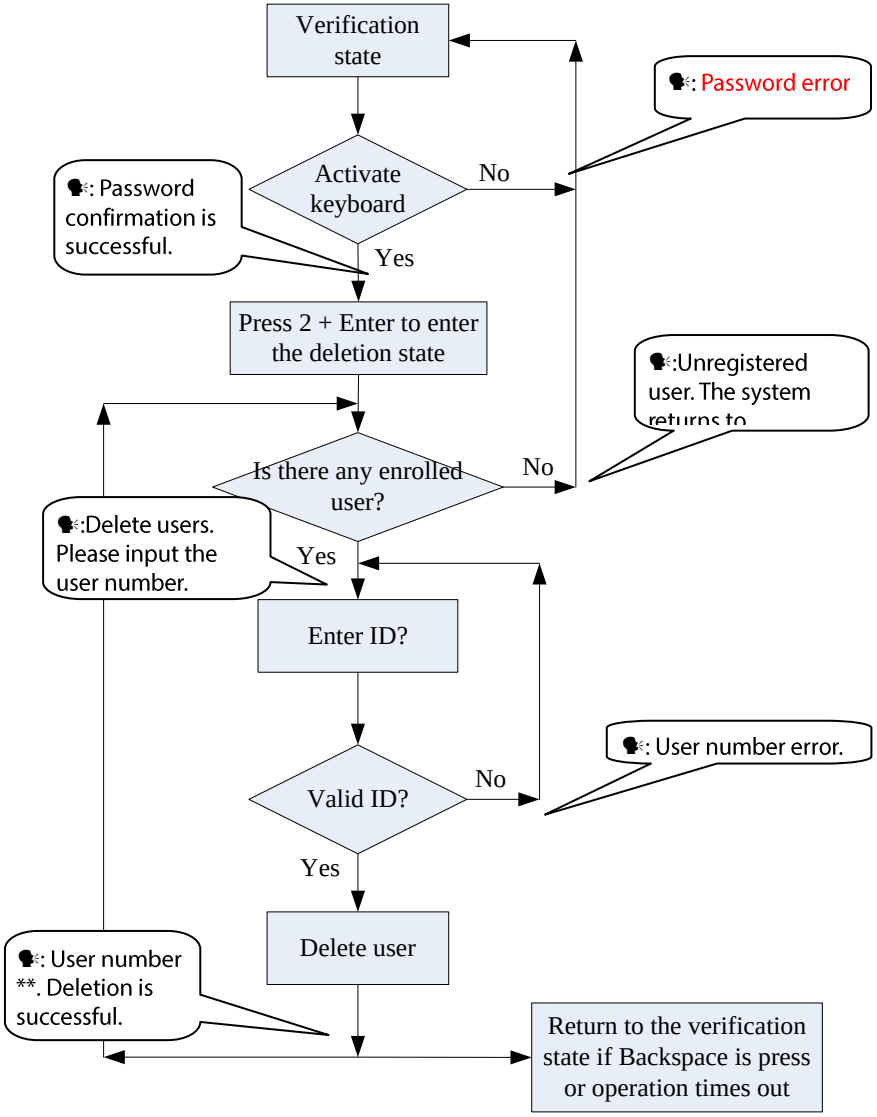
1. Connect a USB keyboard to the device, and swipe your management card once or enter your password to activate the keyboard.
2. Type in "2" and press **Enter** to enter the specified user deletion mode. The system checks whether there exists any enrolled user.
3. If there is any enrolled user, the system will generate the voice prompt "🗣: Delete users. Please input the user number." and you may proceed to the next step; otherwise, the system will generate the voice prompt "🗣: Unregistered user. The system returns to verification state".
4. Enter a user ID and the system checks whether the user ID is valid.
5. If the user ID is valid, the system will generate the voice prompt "🗣: User number **. Deletion is successful. Delete users. Please input the user number." and automatically return to the deletion state. If the user ID is invalid, the system will generate the voice prompt "🗣: Wrong user ID".
6. If you press **Esc** or your operation times out, the system will return to the verification state.

Tips:

1. In specified user deletion mode, user IDs and management card user IDs that are enrolled in the system are all deemed invalid.

2. In keyboard based deletion mode, the system shields the fingerprint sensor and card reader and therefore any operation on them is invalid.

The specified user deletion flow chart is shown below:



3.2.4 Delete All Users

Operation steps:

1. Connect a USB keyboard to the device, and swipe your management card once or enter your password to activate the keyboard.
2. Type in "9" and press **Enter**. Then type in "9" and press **Enter** again. The system deletes all the users.
3. If the operation succeeds, the system will generate the voice prompt "🗣: Delete all users. The operation is successful. The system returns to verification state. Please register the management card."

Tips:

1. You can delete a management card using the Delete All function.

2. You can use the Delete All function to delete all enrolled users, fingerprints and records.

3. Extreme caution should be exercised while performing this operation, as once deleted, the data cannot be recovered.

3.2.5 Restore Factory Defaults.

Operation steps:

1. Connect a USB keyboard to the device, and swipe your management card once or enter your password to activate the keyboard.
2. Type in "3" and press **Enter**. Then type in "3" and press **Enter** again. The system restores the factory defaults.

3. After the operation succeeds, the system generates the voice prompt "🗣: Restore to default settings. The operation is successful. The system returns to verification state."

You can also restore the factory defaults by resetting the tamper switch. See 0 3.5 Tamper Switch.

After the device is restored to factory defaults, the device information is restored to factory defaults, including the device number, system password, IP address, 485 address, and keyboard password.

Note: The user information stored on device will not be cleared after the device is restored to factory defaults.

3.3 User Verification

Operation steps:

1. When the device is in verification state, the system generates the voice prompt "🗣: Verify users. Please press your finger or swipe your card.""

2. Start user verification. The device supports two verifications modes: fingerprint verification and card verification.

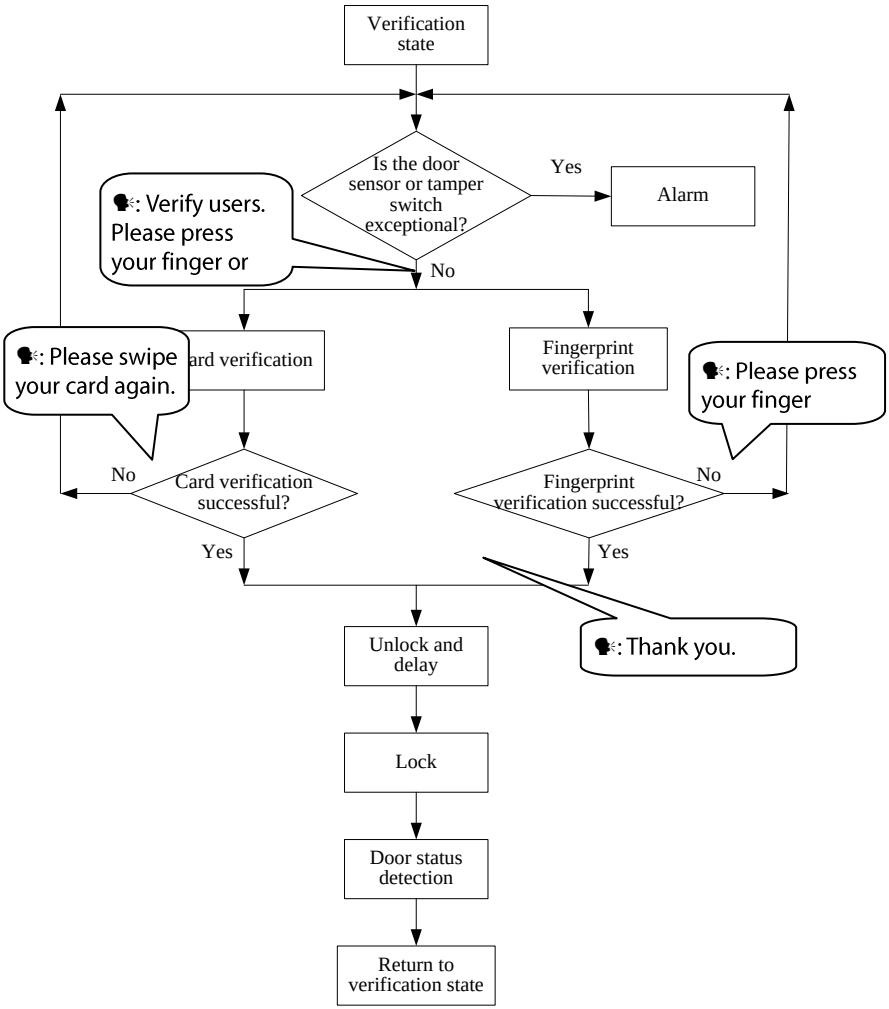
(1) Fingerprint verification

Press your finger on the fingerprint sensor in a proper way. If the verification succeeds, the system generates the voice prompt "🗣: Thank you." and concurrently triggers an unlocking signal. If the verification fails, the system generates the voice prompt "🗣: Please press your finger again."

(2) Card verification

Swipe your card over the card reader. If the verification succeeds, the system generates the voice prompt "🗣: Thank you." and concurrently triggers an unlocking signal. If the verification fails, the system generates the voice prompt "🗣: Please swipe your card again."

The user verification flow chart is show as below:



Tip: The user can unlock by use of his/her enrolled fingerprints instead of management card.

3.4 U-disk

The user can perform **record download**, **user download**, **user upload**, and **firmware upgrade** through a U-disk.

a. Record download: Download the attendance records of all users from the device to a U-disk.

b. User download: Download all user information such as fingerprints and card numbers from the device to a U-disk.

c. User upload: Upload the user information from a U-disk to the device.

d. Firmware upgrade: Upgrade the device firmware through a U-disk.

The configuration files in the U-disk can be created and modified by using the access control management software. Run the access control management software and proceed as follows:

1. Choose Device Management > U-disk Setting to access the operation interface.
2. Select **U-disk** from the dropdown menu to display four items: **Download records**, **Download users**, **Upload users**, and **Upgrade firmware**.
3. Select the desired option and click **Apply**. When the system displays the prompt "Operation is completed", the configuration file **operatemode.cfg** is created in the U-disk.

U-disk operations include the following two cases:

1. If you connect a U-disk without configuration file to the device, the system will automatically prompt you of the operations in sequence.

(1) After connecting a U-disk to the device, you can swipe your card once to enter the U-disk management state.

(2) The system generates the voice prompt "🗣: ****. Please swipe your management card for confirmation." (**** indicates the four operation items from a to d in sequence; same below)

(3) If you want to perform U-disk management, swipe your card for confirmation. If your operation succeeds, the system will generate the voice prompt "🗣: The operation is successful." and prompt you to proceed to the next step. After you finish the four items, the system generates the voice prompt "🗣: The system returns to verification state." If your operation fails, the system will generate the voice prompt "🗣: The operation fails. The system returns to verification state."

(4) If you do not swipe your management card, the system will automatically skip over this step upon 5 seconds and prompt you of the next step. After you finish the four items, the system returns to the verification state automatically.

2. If you connect a U-disk with configuration file to the device, the system will carry out operations based on the settings of the configuration file.

(1) After connecting a U-disk to the device, you can swipe your card once to enter the U-disk management state.

(2) The system obtains operation commands by reading the configuration file on the U-disk and generates the voice prompt "🗣: Run configuration files in the U-disk. Please swipe your management card for confirmation."

(3) After you swipe your card and perform all operations successfully, the system will generate the voice prompt "🗣: ****. The operation is successful." in sequence for every operation step. If any of the operations fails, the system will generate the voice prompt "🗣: ****. The operation fails."

(4) After you finishing all the operations, the system generates the voice prompt "🗣: The system returns to verification state."

Please do not upgrade the firmware at your discretion because it may bring problems and affect the normal use of the device. Contact our distributors for technical support or upgrade notification.

3.5 Tamper Switch

The tamper switch is pressed and held down with a rear cover. When the device is dismantled, the tamper switch will be lifted up and then it will send an alarm signal to trigger an alarm.

Clear alarm: The user can clear the alarm by unlocking the door upon successful matching.

Restore factory defaults: The factory defaults can be restored through the tamper switch.

When the system generates an alarm for 30–60 seconds, the user can press the tamper switch three times (till the speaker sounds) to restore default settings, including the device number, system password, IP address, 485 address, and keyboard password.

Tips:

1. The user information stored on device will not be cleared after the device is restored to factory defaults.

2. The factory defaults can be restored through the USB keyboard. For details, see 3.2.5 Restore Factory Defaults.

4 Appendix

4.1 List of Parameters

The following table lists the basic functional parameters of the device.

Item	Note
Power Supply	12V 3A
Function	Access control device, door status/alarm/lock/access control switch
	One Wiegand input and one Wiegand output
User quantity	10000 (fingerprint and ID card)
Record capacity	100000 pieces of records
Enrollment capacity (fingerprint/card)	1500 fingerprints/10000 cards
Verification mode.	ID (Mifare) card, fingerprint
Communications	TCP/IP, RS485, U-disk
Speaker	Voice prompt
LED	Bi-color indication (red/green)
Keyboard	Valid keys: 0-9, Enter, Esc.

4.2 Statement on Human Rights and Privacy

Dear Customers:

Thank you for choosing the hybrid biometric products designed and manufactured by us. As a world-renowned provider of biometric technologies and services, we pay much attention to the compliance with the laws related to human rights and privacy in every country while constantly performing research and development.

We hereby make the following statements:

1. All of our fingerprint recognition devices for civil use only collect the characteristic points of fingerprints instead of the fingerprint images, and therefore no privacy issues are involved.
2. The characteristic points of fingerprints collected by our products cannot be used to restore the original fingerprint images, and therefore no privacy issues are involved.
3. We, as the equipment provider, shall not be held legally accountable, directly or indirectly, for any consequences arising due to the use of our products.
4. For any dispute involving the human rights or privacy when using our products, please contact your employer directly.

Our fingerprint products or development tools for police use support the collection of the original fingerprint images. As for whether such a type of fingerprint collection constitutes an infringement of your privacy, please contact the government or the final equipment provider. We, as the original equipment

manufacturer, shall not be held legally accountable for any infringement arising thereof.

Note: The law of the People's Republic of China has the following regulations regarding the personal freedom:

1. Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.
2. The personal dignity of citizens of the People's Republic of China is inviolable.
3. The home of citizens of the People's Republic of China is inviolable.
4. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law.

At last we stress once again that biometrics, as an advanced recognition technology, will be applied in a lot of sectors including e-commerce, banking, insurance and legal affairs. Every year people around the globe suffer from great loss due to the insecurity of passwords. The fingerprint recognition actually provides adequate protection for your identity under a high security environment.

4.3 Environment-Friendly Use Description

The Environment Friendly Use Period (EFUP) marked on this product refers to the safety period of time in which the product is used under the conditions specified in the product instructions without leakage of noxious and harmful substances.

The EFUP of this product does not cover the consumable parts that need to be replaced on a regular basis such as batteries and so on. The EFUP of batteries is 5 years.

Names and Concentration of Toxic and Hazardous Substances or Elements

Parts Name	Toxic and Hazardous Substances or Elements					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	×	○	○	○	○	○
Chip capacitor	×	○	○	○	○	○
Chip inductor	×	○	○	○	○	○
Chip diode	×	○	○	○	○	○
ESD components	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in SJ/T11363-2006.

Note: 80% of the parts in this product are manufactured with non-hazardous environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

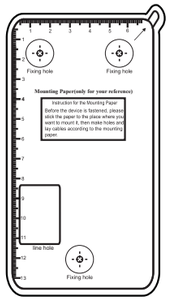
Fax: +86 755-89602394

www.zkteco.com

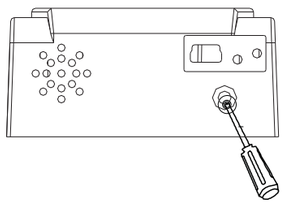
Installation Guide

Version: 1.1
Date: Dec. 2010

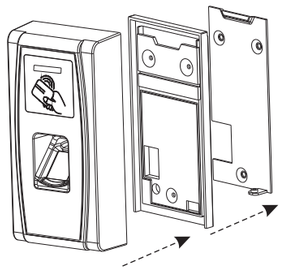
1.Equipment Installation



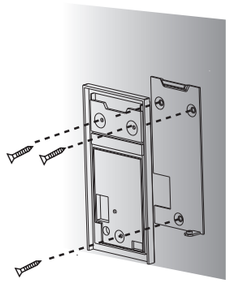
(1) Post the mounting template on the wall. Drill the holes according to the marks on the template (holes for screw and wiring).



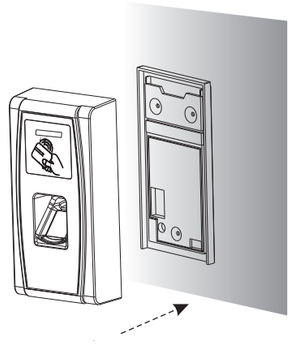
(2) Remove the screw on the bottom of device.



(3) Take away the back cover and waterproof pad.



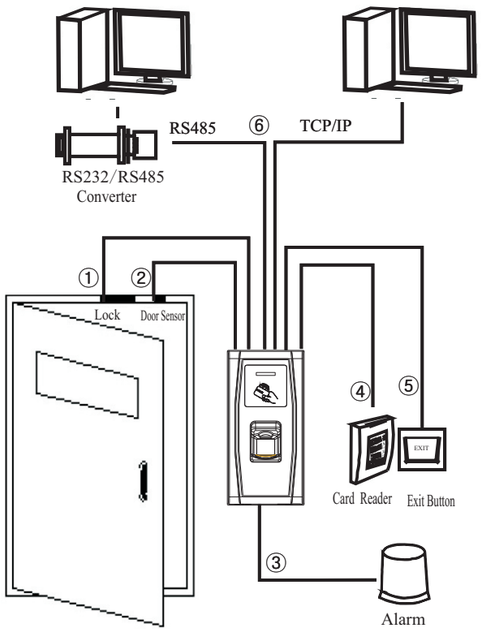
(4) Fix the back cover and waterproof pad on the wall according to the mounting paper.



(5) Set the device to the fixed waterproof pad.

(6) Fix the device to the back cover.

2. Structure and Function



Access Control System Function:

(1)If a registered user verified, the device will export the signal to unlock the door.

(2)Door sensor will detect the on-off state. If the door is unexpected opened or improperly closed, the alarm signal (digital value) will be triggered.

(3)If the device being illegally removed, the device will export alarm signal.

(4)External card reader is supported.

(5)External exit button is supported; it is convenient to open the door inside.

(6)Supports RS485, TCP/IP modes to connect with PC. One PC can manage multiple devices.

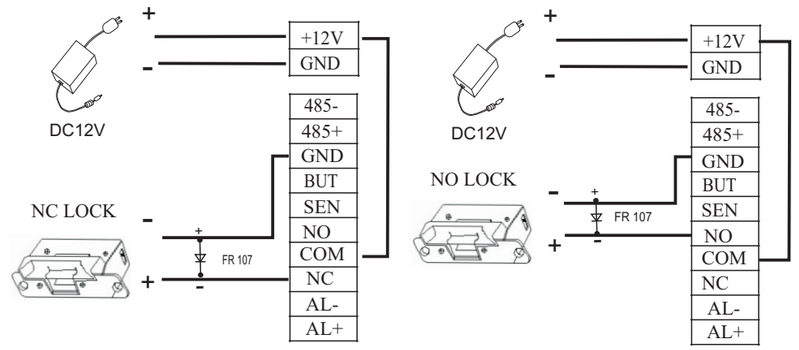
Warning: No operating with power on!

3. Lock Connection

(1) The system supports NO LOCK and NC LOCK. For example the NO LOCK (normally open at power on) is connected with 'NO' terminal, and the NC LOCK is connected with 'NC' terminal.

(2) When the Electrical Lock is connected to the Access Control System, you need to parallel one FR107 diode (equipped in the package) to prevent the self-inductance EMF affect the system, do not reverse the polarities.

(I) Share power with the lock:

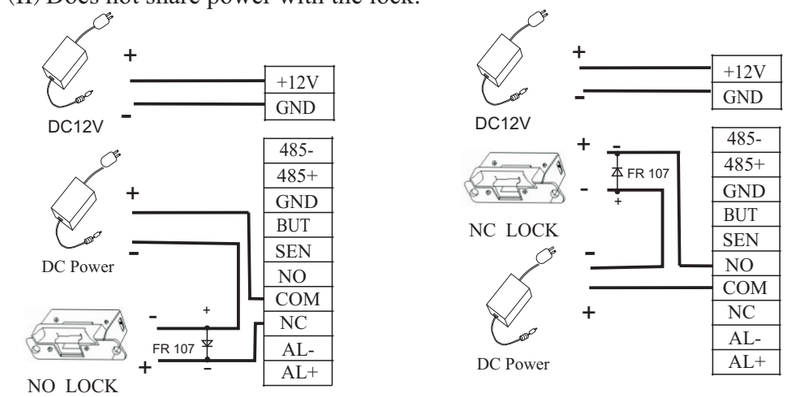


Device share power with the lock:

U_{LOCK}=12V, $I\text{-}I_{LOCK}$>1A…… ①

And the lock is near to the device.

(II) Does not share power with the lock:



Device does not share power with the lock:

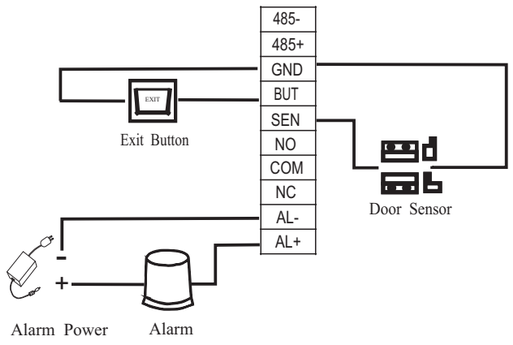
A. U_{LOCK}=12V $I\text{-}I_{LOCK} \leqslant$ 1A;

B. $U_{LOCK} \neq$ 12V;

C. The lock is far apart from the device.

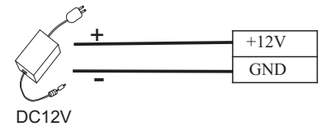
① : 'I': device output current, 'U_{LOCK}': lock voltage,' I_{LOCK}': lock current.

4. Connected with Other Parts:



Voltage output ⩽ DC 12V for Alarm

5. Connected with Power:

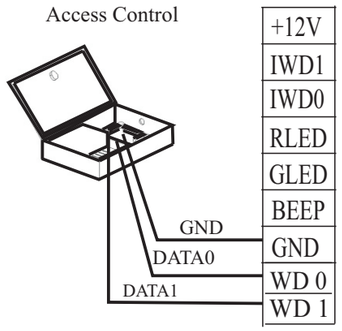


Input DC 12V, 500mA (50mA standby)

Positive is connected with '+12V', negative is connected with 'GND' (**do not reverse the polarities**).

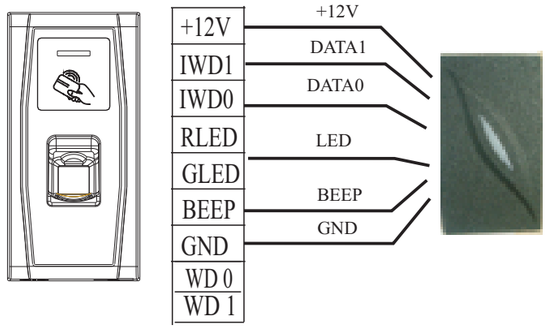
6.Wiegand Output

The device supports standard Wiegand 26 output, as a reader device it has a very good compatibility.



7.Wiegand Input

The device has the function of Wiegand signal input. It supports to connect with an independent reader. They are installed each side of the door, to control the lock and access together.



(1) Please keep the distance between the device and Access Control or reader less than 90 meters (Please use Wiegand signal extender in long distance or interference environment).

(2) To keep the stability of Wiegand signal, connect the device and the Access Control or reader in same 'GND' in any case.

8. Other Functions:

(1) Manual Reset:

If the device does not work properly because of misoperation or other abnormality, you can use 'Reset' function to restart it. Remove the black rubber cap, then stick the Reset button hole with a sharp tool(the tip diameter less than 2mm).

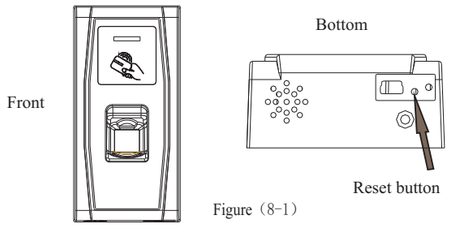


Figure (8-1)

(2)External USB Keyboard (Refer to your own keyboard):

The device supports external keyboard to offer more flexible operations. The keyboard need to purchase separately. It's convenient to enroll users, remove users, recovery factory settings, set the keyboard password and so on. The operation please refer to the user manual.

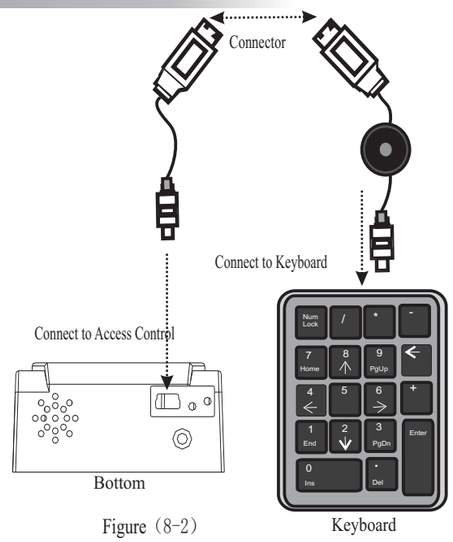


Figure (8-2)

(3)Recovery Factory Settings:

You can use the tamper switch (As figure (8-3)) to recovery factory setting, such as device number, system password, IP address, RS485 address, etc. More information please refers to the user manual.

Press the tamper switch three times after the alarm being triggered 30 seconds but no more than 60 seconds.

Notes: The user data won't be cleared.

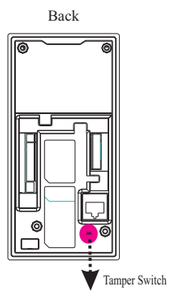


Figure (8-3)

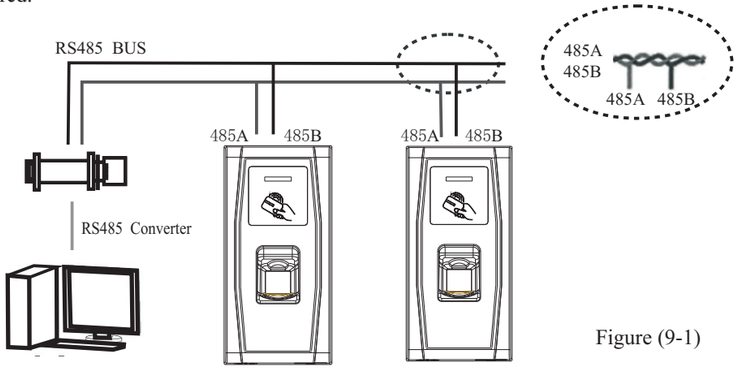


Figure (9-1)

Warning: No operating with power on!

9. Communication

There're two modes that the PC software communicate and exchange information with the device: RS485 and TCP/IP, they all support remote control.

Terminal	PC Serial Ports
485A	RS485 +
485B	RS485 −

(1) RS485 Mode:

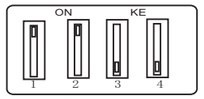
Please use specified RS485 wire, RS485 active converter and bus-type wiring.

(I) To prevent the interference, the last device in the RS485 bus connect a 120 Euro resistor. That is turning the switch '4' (terminal resistor switch) to 'ON'.

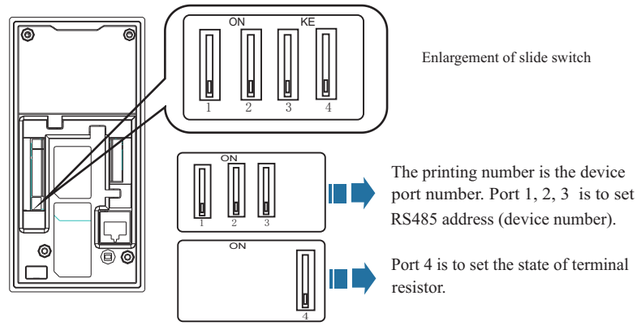
(II) The RS485 device No. is shown in PC software. You can change it as follows. (The default switch state is 'OFF').

Machine No.	Port 1	Port 2	Port 3
Switch State	'ON'	'ON'	'ON'
No.1	✓		
No.2		✓	
No.3	✓	✓	
No.4			✓
No.5	✓		✓
No.6		✓	✓
No.7	✓	✓	✓

The symbol '✓' means turning the switch to 'ON' position.



No.3 machine's slide switch



Enlargement of slide switch

The printing number is the device port number. Port 1, 2, 3 is to set RS485 address (device number).

Port 4 is to set the state of terminal resistor.

(2) TCP/IP Mode:

(I) **Crossover cable**: The device and PC connected directly. As figure (9-2).

(II) **Straight cable**: The device and PC connected to LAN/WAN through switch/Lanswitch. As figure (9-3).

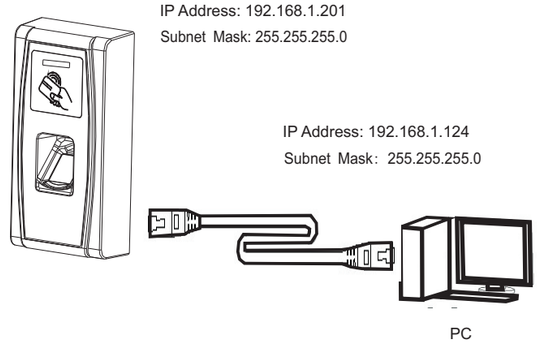


Figure (9-2)

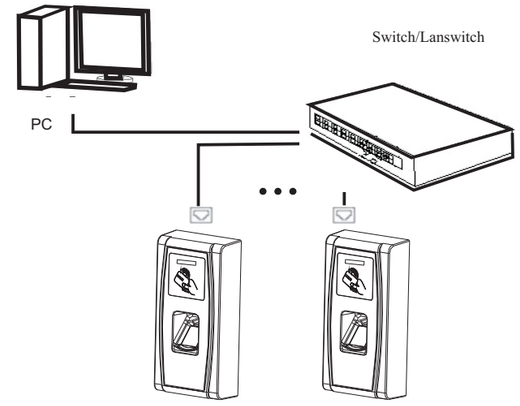


Figure (9-3)

10. Cautions:

(1) **Power cable is connected after all the other wiring.** If the device is working abnormally, please shut down the power first, then make the necessary check . Kindly reminds you that any hot-line work may damage the device, and it is not included in the warranty.

(2) We recommend the 3A/12V DC Power supply. Please contact our technical staff for details.

(3) **Please read carefully the terminal description and wiring by rule strictly**. Any damage caused by improper operations will not under warranty.

(4) **Keep the exposed part of wire less than 5mm**, to avoid unexpected connection.

(5) **Please connect the 'GND'** before all the other wiring especially under the environment with much electrostatic.

(6) Do not change the cable type because of long distance between the power and the device. Pay attention to the distance voltage decay when you choose the power cable.