

SF Series User Manual

Version: 1.2

Date: July, 2011

About This Document:

This document introduces the operations of SF series product. For the product installation, please refer to *installation instruction*.

Important Notice:


Firstly thank you for purchasing this SF series terminal, before use, please read this manual carefully to avoid the unnecessary damage! The company reminds you that the proper using will improve the using affect and verification speed.

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

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

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.



We can neither promise that the information consistent with the actual product because of the constantly updated of product, nor assume any dispute resulting from the actual technical parameters does not match this information, any change without prior notice.

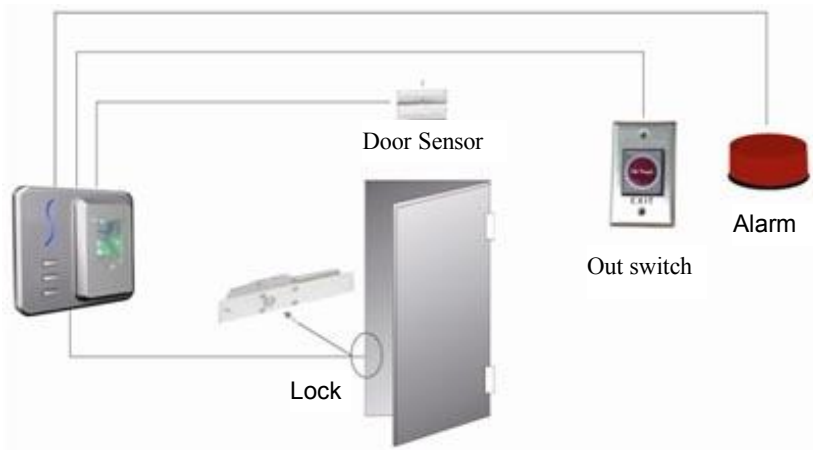
Contents

1. Instruction for Use	- 1 -
1.1 Overview of Device Functions	- 1 -
1.2 Front View	- 2 -
1.3 Verification State	- 2 -
1.4 Operation Time out	- 3 -
1.5 Finger Placement	- 4 -
1.6 LED and Buzzer	- 5 -
1.7 Administrator Lost	- 5 -
2. Basic Operations	- 6 -
2.1 Enroll an Administrator	- 6 -
2.2 Enroll an Ordinary User	- 9 -
2.3 User Verification	- 10 -
2.4 Delete Singer User	- 11 -
2.5 Delete All Users	- 13 -
3. Appendix	- 15 -
3.1 List of Parameters	- 15 -
3.2 Statement on Human Rights and Privacy	- 16 -
3.3 Environmental protection	- 18 -

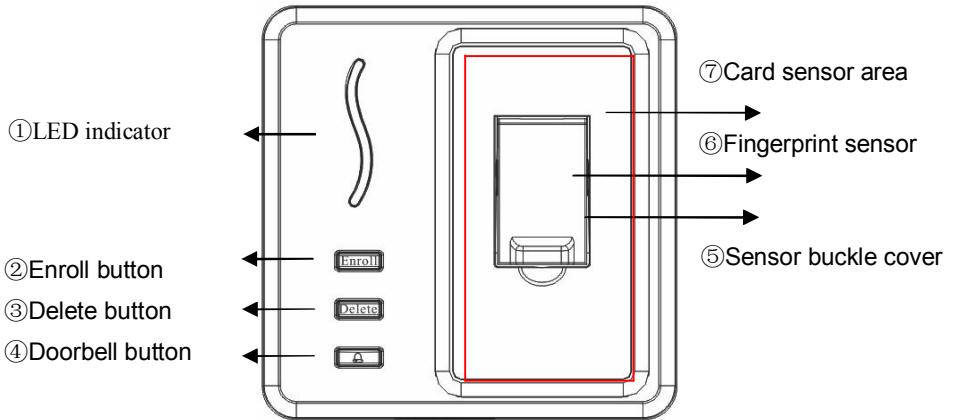
1. Instruction for Use

1.1 Overview of Device Functions

SF Series product can directly use the lock control, and also can use the fingerprint access controller connected. The product have only Enroll, Delete, and doorbell buttons, the operation of every step have the voice prompts, make the customer more simple and convenient to operate. No LCD and sensor buckle cover played a good role to ensure the product clean. USB-client communication greatly reduces the tedious wiring. Standard ID card module provides customers with greater choice. This product is suitable for small office environment, enterprise internal and some lower security level sites.



1.2 Front View



① **LED indicator:** Display operation results and abnormal state. For details, see [1.6 LED and Buzzer](#).

② **Enroll button:** Operation key, used to register users and administrators.

③ **Delete button:** Operation key, delete users and administrators.

④ **Doorbell button:** Press to send a ring signal, the doorbell will ring after receiving this signal.

⑤ **Sensor buckle cover:** Protection fingerprint sensor, with anti-dust, anti-glare and so on.

⑥ **Fingerprint sensor:** Enroll and verify the fingerprint.

⑦ **Card sensor area** (with the red line box): Enroll and verify the card.

1.3 Verification State

The device is in verification state after powering on. User can verify and then unlock the door in this state. During this state, the user can also enter or exit the normal user registration state, administrator registration state, single user deletion state and clear users state, each step has voice and light prompt,

the system will automatically return to the verification status when it's time out.

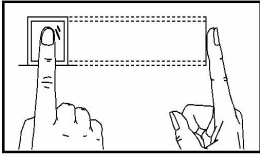
1.4 Operation Time out

During an operation, if a step last on N seconds with no user response ("N" representing the number, you can set through the access control software), the device will repeat the prompts for this operation. If there is no user response after twice prompts, the device will automatically return to verify state and prompt "🔒: The operation timed out, system back to validated status".

1.5 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).

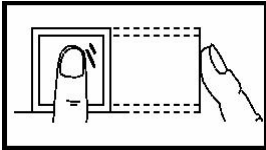
1. Proper finger placement:



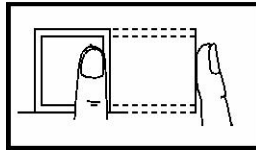
The finger must be flat to the surface and centered on the fingerprint sensor.

2. Improper finger placement:

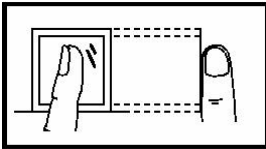
Not flat to the surface



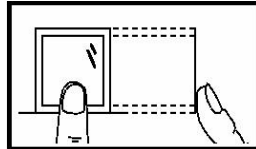
Off-center



Slanting



Off-center



Please enroll and verify your fingerprint by using the proper finger placement mode. We shall not be held accountable for any consequences arising out of the degradation in verification performance due to improper user operations. We shall reserve the right of final interpretation and revision of this document.

1.6 LED and Buzzer

1. LED indicator lights up in blue and flashes every 2 seconds in verification state. LED indicator light is off when the device is in registration or deletion state.
2. LED light is green and solid on for 1 second if the verification, registration or deletion is successful. Otherwise, the LED light is red and solid on for 1 second.
3. After you open the door, the device will check the door state when the time exceed "Door Sensor Delay" ("Door Sensor Delay" is set through the access control software). If the door is not closed, the buzzer will beep for 1 minute, the device will trigger the alarm signal if the buzzer beep longer than 1 minute and the door is still unclosed.



If the device's LED and buzzer indicator does not match the description above, please contact the relevant technical staff.

1.7 Administrator Lost

If the administrators is lost, you can press the Enroll or Delete key after dismantle alarming lasted for 30 to 60 seconds, to re-register an administrator without administrator verification.

2. Basic Operations

2.1 Enroll an Administrator

The users are divided into two types: administrators and ordinary users. For the first time of using this device, which is the case the administrator has not registered, ordinary users can not register, and you must register at least one administrator first.

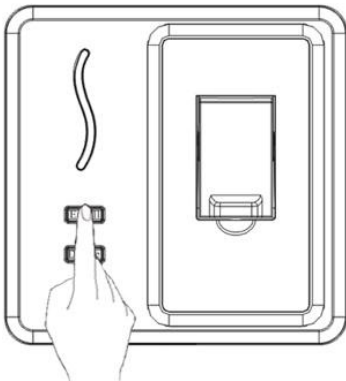
The privilege of administrator and ordinary user are as follows:

Administrator: Has all operating privilege, can enroll, delete all of the administrators and ordinary users (except himself).

Ordinary users: Only has the privilege of verification and unlock the door.

Enroll administrator steps are as follows:


1) During **verification state**, press the Enroll key for 3 seconds, the device prompts "👤: Enter the Administrator enrollment status", and the device enters the administrator register status.



👤: Enter the Administrator
enrollment status

2) When the device prompts "👤: Please confirm with the administrator, press Enroll button to exit", please press the administrator fingerprint by the

proper way or swipe the administrator card. Please refer to [1.5 Finger Placement](#) for more details.

 **Note:** If the device does not register an administrator, go directly to step (4).

3) If the verification is successful, the device enters the register mode, continue with step (4). If the verification fails, the device prompts "👤: Please try again" or "👤: Please punch card again". After three consecutive verification failures, the device will prompt "👤: Administrator failed to confirm, system back to validated status", and return to verify status.

4) When the device prompt "👤: Please press fingerprint or punch card, press Enroll button to exit" to start register administrator. The device supports two kinds of register methods, fingerprint registration and card registration, follow these steps:

① Fingerprint registration

a. Use the proper way to press a finger on the fingerprint sensor, the device prompts "👤: Please press the finger again".

b. Press the same finger for another time, the device prompts "👤: Please press the fingerprint for the last time".

c. Press the same finger for the third time, the registration is successful, the device prompts "👤 : User ID ×××, enrollment succeeded (××× indicates the user's ID number, starting from 001, the valid user ID is 001 to 999). If the registration is failed, the device prompts "👤: Fingerprint repeat, please try again" and return to the register state, repeat the step a.

② Card registration

Swipe the card near to the card sensor area, if the registration is successful, the device prompts "👤: User number ×××, registration is successful". If the registration is failed, the device prompts "👤: Duplicated card number" and return to register state, waiting for swipe card or press fingerprint.

5) After successful registration, the device will enter the register state

automatically. Repeat the step (4) and register other administrators.

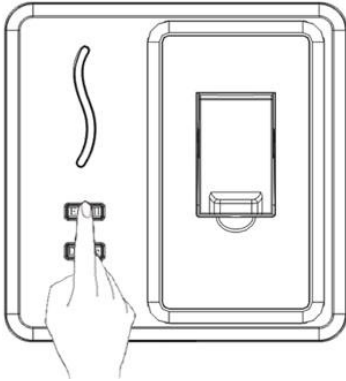


- 1) Each administrator or ordinary user can only register one fingerprint or one card.
- 2) In finger pressing process, if the fingerprint with a bad quality, the device prompts “👉: Please try again”.
- 3) If the capacity is full in user enrolling, the device prompts “👉: Users are full, system back to validated status”.

2.2 Enroll an Ordinary User

Ordinary user enrollment steps:

1) During verification state, press the Enroll key, the device prompts "👤: Enter the user enrollment status", then device enter the ordinary user register status.



👤: Enter the user enrollment status, please confirm with the administrator, press Enroll button to exit.

🌐 **Note:** If the device did not register an administrator, the device prompts "👤: Extended press the Enroll button to enroll an administrator", enter the administrator enrollment process.

2) The following steps are same to the administrator enrollment. Please refer to [2.1 Enroll an Administrator](#) for specific operations.

3) After successful registration, the device will enter the register state automatically, and continue to register other users.

2.3 User Verification

User verification operations:

- 1) System enters the verify state and prompts "🗨️: User verify, please press fingerprint or punch card".
- 2) Start to verify the user. The device supports fingerprint verification and card verification, operations are as follows:

① Fingerprint verification

Press a finger on the fingerprint sensor in proper way. If the user verified successful, the device prompts "🗨️: User ID xxx, thank you "(xxx indicates the user ID number), and trigger the unlock signal. If the user fails to verify, the device prompts "🗨️: Please try again".

② Card verification

Swipe a card near to the card sensor area, if the validation is successful, the device voice prompt "🗨️: User ID xxx, thank you "(xxx indicates the user ID number), and trigger the unlock signal. If the user fails to verify, the device prompts "🗨️: Please punch card again".

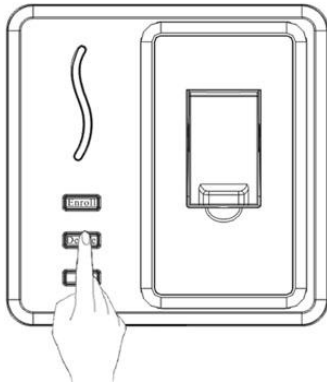


Note: In the verification state, if the door sensor or dismantle switch is in abnormal state, the device will trigger the alarm signal. After making the door sensor and dismantle switch work normally, the user can disarm the alarm by fingerprint or card verification successfully.

2.4 Delete Singer User

The operations of deleting a single user:

1) During verification state, press the Delete key, the device prompts "🗨️: Enter the delete a user status, please confirm with the administrator, press Enroll button to exit".



🗨️: Enter the delete a user status, please confirm with the administrator, press Enroll button to exit.

🌈 **Note:** If there is no user, the voice prompt"🗨️: No users enrolled, system back to validated status", and automatically returns to the verify status.

2) Please press the administrator fingerprint by the proper way or swipe the administrator card. Please refer to [1.4 Finger Placement](#) for more details.

3) If the verification is successful, the device enters the delete mode, continue with step (4). If the verification fails, the device prompts"🗨️: Please try again" or"🗨️: Please punch card again". After three consecutive verification failures, the device will prompt"🗨️: Administrator failed to confirm, system back to validated status", and return to verify status.

4) The user can press a fingerprint or swipe card, follow these steps:

① Fingerprint verification

Press a finger on the fingerprint sensor in proper way. If the user verified

successful, the device prompts "🗣️ : User ID xxx, delete successfully" (xxx indicates the user ID number). If the user fails to verify, the device prompts "🗣️: Please try again".

② Card verification

Swipe a card near to the card sensor area, if the validation is successful, the device voice prompt "🗣️: User ID xxx, delete successfully" (xxx indicates the user ID number). If the user fails to verify, the device prompts "🗣️: Please punch card again".

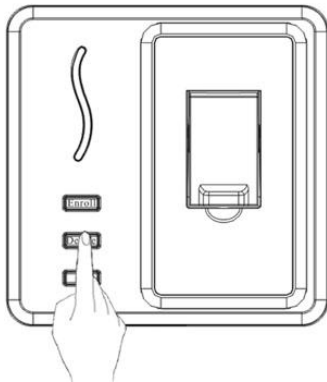


- 1) If the deleting user was the last administrator, the device will prompt "🗣️: Forbid to delete the last administrator, system back to validated status", and automatically returns to the verify status.
- 2) In finger pressing process, if the fingerprint with a bad quality, the device prompts "🗣️ : Please try again".

2.5 Delete All Users

The operations of deleting all users:

1) During verification state, press the Delete key for 3 seconds, the device prompts "🗨️: Enter the clear user status, please confirm with the administrator, press Enroll button to exit".



🗨️: Enter the clear user status, please confirm with the administrator, press Enroll button to exit

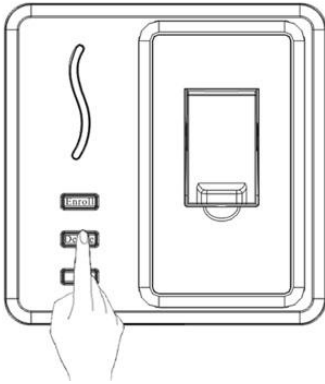
🚩 **Note:** If there are no user, the voice prompt "🗨️: No users enrolled, system back to validated status", and automatically returns to the verify status.

2) Please press the administrator fingerprint by the proper way or swipe the administrator card. Please refer to [1.4 Finger Placement](#) for more details.

3) If the verification is successful, the device prompts "🗨️: Clear users successfully, please long press Delete key to clear the administrator, press Delete button to exit", and continue with step (4). If the verification fails, the device prompts "🗨️: Please try again" or "🗨️: Please punch card again". After three consecutive verification failures, the device prompts "🗨️: Administrator failed to confirm, system back to validated status", and return to verify status.

4) Long press the Delete key to delete the administrator, the device prompts

“🔊: Clear administrator successfully, system back to validated status”. The device will automatically return to the verification status.



🔊: Clear administrator successfully,
system back to validated status.

3. Appendix

3.1 List of Parameters

Basic function parameters are shown as follows:

Power	DC12V
Function	Access control device, has the detection functions such as door sensor, dismantle switch etc.
	One Wiegand output (only SF101)
User number	200 (fingerprint, ID card and MF card)
Record memory	30000 records
communication	USB
	RS232/485 (monitors the device running)
Fingerprint head	Optical fingerprint sensor
Fingerprint algorithm	9.0/10.0 (switch by software)
Door bell	Supports the wired doorbell
Speaker	The voice prompts
Buzzer	Alarm when the device is dismantled
LED	Three indicators (Red, green, blue)
Language	Supports multi-national voices
Sleep	Supports the sleep function



Access control parameters and the sleep function are set by the access control software.

3.2 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 for police use, or development tools 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.

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

3. Appendix

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 biometric products actually provide adequate protection for your identity under a high security environment.

3.3 Environmental protection



The environmental protection use period marked on our products is the safety period of our products used under the conditions specified by this manual without toxic and harmful substances leaking happened

The environmental protection use period marked on our products does not include the easy wear and tear components required to be replaced regularly such as the battery etc. The battery's environmental protection use period is 5 years.

The toxic and harmful substances or element names and the content table

Part name	The toxic and harmful substances or elements					
	Lead (Pb)	Merc ury (Hg)	Cadmiu m (Cd)	Hexavalent Chromium (Cr6 +)	Polybrominate d biphenyls (PBB)	Polybrominated diphenyl ethers (PBDE)
SMD resistor	×	○	○	○	○	○
SMD capacitor	×	○	○	○	○	○
SMD inductance	×	○	○	○	○	○
SMD diode	×	○	○	○	○	○
ESD components	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screw	○	○	○	×	○	○

○: Indicate that the content of the toxic and harmful substance contained in all homogeneous materials of this part is in the limitation requirement stipulated in SJ / T 11363-2006.

×: Indicate the content of the toxic and harmful substance contained in at least one homogeneous material of this part is beyond the limitation requirement stipulated in SJ / T 11363-2006.

Note: The 80% product has adopted the manufacture with non-toxic and harmless environmental protection materials, the non-toxic and harmless substances or elements instead of the toxic and harmful substances or elements contained can not be achieved because of the current technology and economic constraints.