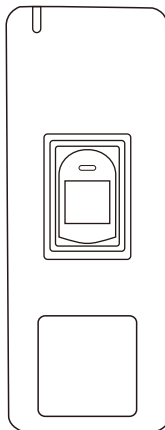




SF4 - Waterproof Fingerprint & RFID Access Control



User Manual

INTRODUCTION

The device is a metal case standalone fingerprint access control with integrated card reader. The card reader is of 3 versions optional: 125KHz EM or 125KHz HID & EM or 13.56MHz Mifare.

With the slim design, it is an ideal choice to install on door frame. IP66 waterproof version is very suitable for outdoor use.

The device supports up to 100 fingerprint users and 900 card users, it equips with an infrared remote control and master fingerprint for easy operation, supports fingerprint access and card access; with external alarm, door contact, exit button.

Two Versions Optional:

- 1) Indoor, Non-waterproof
- 2) Outdoor, Waterproof (IP66)

Main Features:

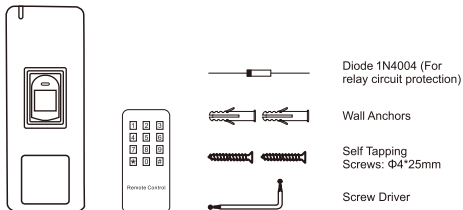
- > Waterproof, conforms to IP66 (Waterproof Version)
- > Metal case, anti-vandal
- > One programming relay output
- > Multi-color LED Status Display
- > 1000 Users (100Fingerprint Users + 890 Card Users + 10 Visitor Users)
- > Latch Mode to hold door or gate open
- > Integrated alarm & buzzer output

Specifications:

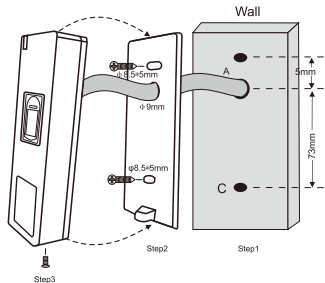
User Capacity Fingerprint Users Card Users Visitor Users	1000 100 890 10
Operating Voltage Idle Current Active Current	12V DC ±10% ≤30mA ≤100mA
Fingerprint Reader Resolution Identification Time FAR FAR	Capacitive Fingerprint Module 500DPI ≤1S ≤0.01% ≤0.1%
Proximity Card Reader Radio Technology Read Range	EM or HID & EM or MIFARE 125KHz / 13.56MHz ≥2cm

Wiring Connections	Relay Output, Exit Button, DOTL, Alarm (Non-waterproof version without DOTL and Alarm)
Relay Adjustable Relay Output Time Adjustable Alarm Output Time Lock Output Load Alarm Output Load	One (NO, NC, Common) 0-99 Seconds (default: 5 seconds) 0-3 Minutes (default: 1 minute) 2 Amp Maximum 5 Amp Maximum
Environment Operating Temperature Operating Humidity	Meets IP66 (Waterproof Version) -30°C~60°C (-22°F~140°F) - Default -40°C~60°C (-40°F~140°F) - Optional 20%RH-90%RH
Physical Surface Finish Dimensions Waterproof Version Unit Weight Shipping Weight Non-waterproof Version Unit Weight Shipping Weight	Zinc-alloy Enclosure Powder Coat L125 × W45 × D25 (mm) 191g 238g 136g 183g

Carton Inventory



INSTALLATION



Wiring

Wire Color	Function	Notes
Basic Stand Alone Wiring		
Red	12V DC	12V DC Regulated Power Input
Black	GND	Ground
Blue	Relay NO	Normally Open Relay Output (Install diode provided)
White	Relay Common	Common Connection for Relay Output
Green	Relay NC	Normally Closed Relay Output (Install diode provided)
Yellow	OPEN	Request to Exit (REX) Input
Advanced Input and Output Features		
Grey	Alarm Output	Negative contact for Alarm
Brown	Contact Input	Door/Gate Contact Input (Normally Closed)

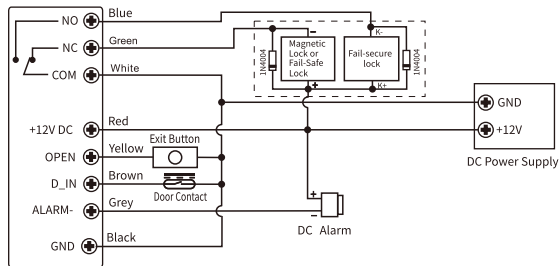
(Non-waterproof version without Alarm Output and Contact Input)

Sound and Light Indication

Operation Status	LED	Finger Sensor Light	Buzzer
Stand by	Red light bright	Off	-
Enter into programming mode	Red light shines	Off	One beep
In the programming mode	Orange light bright	-	One beep
Operation error	-	-	Three beeps
Exit from the programming mode	Red light bright	-	One beep
Open lock	Green light bright	Off	One beep
Alarm	Red light Shines quickly	Off	Beeps

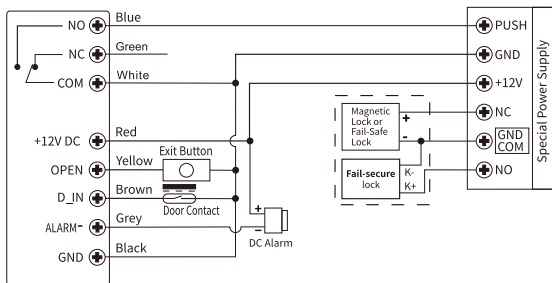
Connection Diagram

Common Power Supply



Attention: Install a 1N4004 or equivalent diode is needed when use a common power supply, or the reader might be damaged. (1N4004 is included in the packing)
(Non-waterproof version without Alarm Output and Contact Input)

Access Control Power Supply



(Non-waterproof version without Alarm Output and Contact Input)

PROGRAMMING

GENERAL PROGRAMMING INFORMATION

>**User ID Number:** Assign a user ID number in order to keep track of the users of access fingerprints or cards. The user ID number can be any number from 1~1000.
IMPORTANT: User IDs do not have to be preceded with any leading zeros.
 Recording of User ID is critical. Modifications to the user require the User ID or card be available.

Remark: Fingerprint User ID: 0~98
 Master Fingerprint User ID: 99
 Card User ID: 100~989
 Visitor User ID: 990~999

>Proximity Card :

EM Version: Any 125KHz industry standard 26bits EM proximity card;
 EM + HID Version: Any 125KHz industry standard 26bits EM / HID proximity card;
 Mifare Version: 13.56MHz Mifare tag / card (ISO14443 Type A)

Set Master Code

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) # (Factory default is 123456)
2. Update Master Code	0 (New Master Code) # (Repeat New Master Code) # (Master code is any 6 digits)
3. Exit Program Mode	*

Add Master Fingerprint by Specific ID (ID Number: 99)

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Add Master Fingerprint	1 (99) # (Fingerprint)(Repeat Fingerprint)(Repeat Fingerprint again)
3. Exit	*

Add Fingerprint Users by Auto ID

(Allows the device to assign Fingerprint to next available User ID, ID number is 0~98)

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Add Fingerprint	1 (Fingerprint) (Repeat Fingerprint) (Repeat Fingerprint again) Fingerprints can be added continuously
3. Exit	*

Add Fingerprint Users by Specific ID

(Allows Master to define a specific ID to the fingerprint, ID number is 0~98)

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Add Fingerprint	1 (User ID) # (Fingerprint) (Repeat Fingerprint) (Repeat Fingerprint again) Fingerprints can be added continuously
3. Exit	*

Add Card Users by Auto ID

(Allows Master to define a specific ID to the Card, ID number is 100-989)

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Add Card : by Reading Card	1 (Read Card) Cards can be added continuously
3. Exit	*

Add Card Users by Specified ID

(Allows Master to define a specific ID to the Card, ID number is 100-989)

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Add Card : by Reading Card	1 (User ID) # (Read Card) Cards can be added continuously
3. Exit	*

Delete Users

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Delete Fingerprint: by Fingerprint OR	2 (Input Fingerprint) Fingerprints can be deleted continuously
2. Delete Card: by Reading Card OR	2 (Read Card) Cards can be deleted continuously
2.Delete Card or Fingerprint : by ID number OR	2 (User ID) #
2. Delete ALL Users	2 (0000) # (Master Fingerprint User will be Deleted when Delete All Users)
3. Exit	*

Master Fingerprint Usage

Using Master Fingerprint to add and delete users	
Add Card or Fingerprint User	1. Input (Master Fingerprint) 2. Read User Card/Input Fingerprint Three Times (Repeat Step 2 for additional users) 3. Input (Master Fingerprint) Again
Delete Card or Fingerprint User	1. Input (Master Fingerprint Twice within 5s) 2. Read User Card/Input Fingerprint Once (Repeat Step 2 for additional users) 3. Input (Master Fingerprint) Again

Visitor User Setting (For card user only)

There are 10 groups Visitor card available,the users can be specified up to 10 times of usage,after a certain number of times, i.e. 5 times,the card become invalid automatically.

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Add Visitor Card User OR 2. Delete Visitor User by ID Number OR 2. Delete Visitor User by Read Card	8 (0-9 #)(User ID #)(Read Card #) 2 (User ID #) 2 (Read Card)
3 Exit	*
Note: Number of time is 0-9,0=10 times User ID number must be any number between 990-999 Visitor card must be unique ,should be distinguished from common card	

Set Access Mode

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2.Card or Fingerprint Access OR 2. Fingerprint Only OR 2. Card Only	3 0 # (Factory Default) 3 1 # 3 2 #
3. Exit	*

Set Relay Configuration

The relay configuration sets the behavior of the output relay on activation.

	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Pulse Mode OR	4 (1-99) # (Factory default) The relay time is 1-99 seconds (1 is 100 ms)(Factory default: 5 seconds)
2. Latch Mode	40 # Sets the relay to ON/OFF latch mode
3. Exit	*

Set Alarm

	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Set alarm time	5 (0-3) # Factory default is 1 minute
3. Exit	*

Set Strike-out Alarm - For Waterproof Version

The strike-out alarm will engage after 10 failed Card/Fingerprint attempts, factory default is OFF, it can be set to deny access for 10 minutes or enable alarm after engaging.

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Strike-out OFF OR	6 0 # (factory default)
2. Strike-out ON OR	6 1 # Access will be denied for 10 minutes
2. Strike-out ON	6 2 # Enable alarm, need enter Valid Card/Fingerprint to silence
3. Exit	*

Set Door Open Detection - For Waterproof Version

Door Open Too Long (DOTL) Detection

When use with an optional magnetic contact or built-in magnetic contact of the lock, if the door is opened normally, but not closed after 1 minute, the inside buzzer will beep automatically to remind people to close the door. The beep can be stopped by closing the door, master users or valid users, or else, it will continue to beep the same time with the alarm time set.

Door Forced Open Detection

When use with an optional magnetic contact or built-in magnetic contact of the lock, if the door is opened by force, the inside buzzer and external alarm (if there is) will both operate, they can be stopped by master users or valid users, or else, it will continue to sound the same time with the alarm time set.

Programming Step	Keystroke Combination
1. Enter Program Mode	* (Master Code) #
2. Disable Door Open Detection OR	6 3 # (factory default)
2. Enable Door Open Detection	6 4 #
3. Exit	*

OTHERS

Users Operation & Reset to Factory Default

> **Open the door** : Read valid user card or input valid fingerprint

> **Remove Alarm** :

Read valid user card or input valid fingerprint or input Master Code # or Master Fingerprint

> **To reset to factory default**

1. Power off

2. Press the exit button,hold it and power on

3. There will be two beeps,still hold it at least 10s,then will have one long beep.

The device reset to factory default successfully.

Remark: Reset to factory default,the users information is still retained.