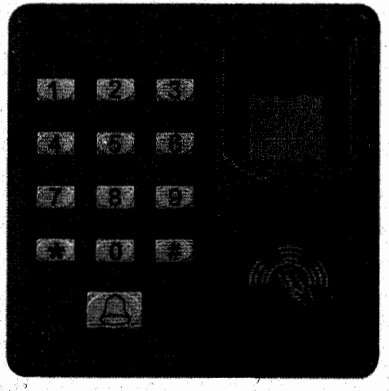
Fingerprint Access Control

Installation/System User Manual

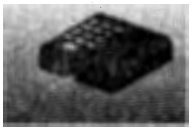
Rev: 1.1.1



Content

Equipment Installation

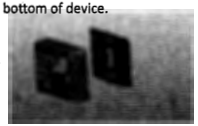
Installation Method A: Wall Mount Installation



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

(2) Take away the back cover.

(3) Fix the back cover on wall according to the hole on wall.



(4) Fix the device to the back cover.

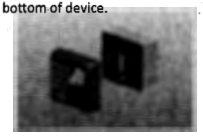
(5) Fix the screw.

Installation Method B: 86-Box Installation

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

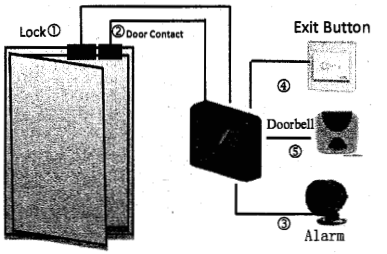
(2) Take away the back cover.

(3) Fix the back cover on the 86-Box that already fixed on wall.



(4) Fix the device to the back cover.

(5) Fix the screw.



Access Control System Function:

①When a registered user verified, device will output the signal to unlock the door.

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

③If the device being removed illegally, the device will output the alarm signal.

④It supports connecting to external exit button. It's convenient to open the door inside.

⑤Support connecting to external doorbell.

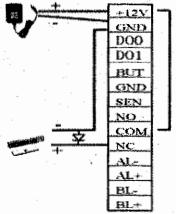
3. Lock Connection

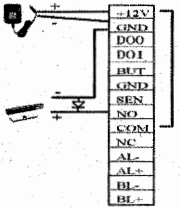
Warning: No operation when power on.

(1) The system supports NO Lock and NC Lock, just need to connect to different socket. For example, the NO Lock (normally open when power on) is connected with "NO" socket. The NC Lock (normally closed when power on) is connected with "NC" socket.

(2) When the Electrical Lock is connected to the Access Control System, we need to parallel one 1N4007 diode (accessory in the small package) to prevent the self-inductance EMF affect the system. DO NOT reverse the polarities.

1) Share power with the lock:



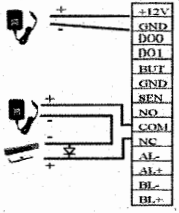


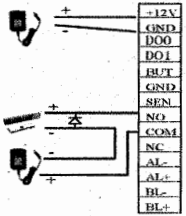
Device share power with the lock:

ULock=12V,I-ILock>1A...①

And the lock is near to the device.

2) DOES NOT share power with the lock:





Device does not share power with the lock:

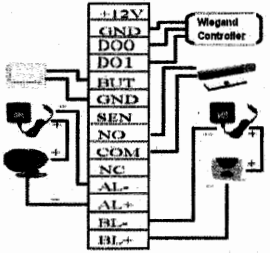
A)ULock=12V and I-ILock≤ 1A;

B)ULock ≠12V;

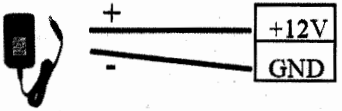
C) The lock is far apart from the device.

① "I": device output current, "ULock": lock voltage, "ILock": lock current

3. Connected with other Device



4. Connect with Power



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

Positive is connected with "+12V", negative is connected with "GND" (Do Not reverse the polarities).

Note: this Access Control Device could only support to the Alarm (Alarm output ≤ DC12V) .

Instructions

Recommended procedure:

Step 1: Install the device and power on.

Step 2: After the administrator password is authenticated and changed, register Users' fingerprints, cards, or passwords. **[Please keep a record of "User ID, group no. of password", refer to the form in the last page]**

Step 3: Configure access control parameters, including modifying 8 passwords for opening the door and configuring the unlocking duration, authentication mode, stealth mode, door contact mode, and alarm.

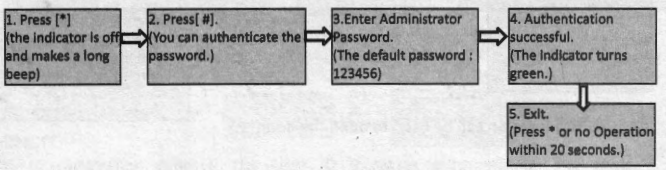
Functions of the Access Control Device

1. User Management

1.1 Administrator Operations

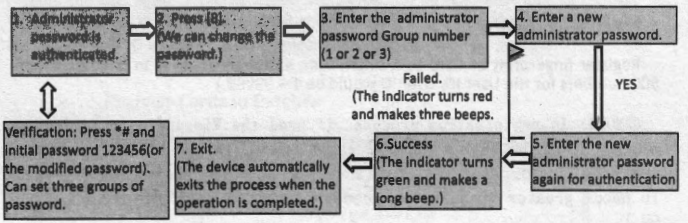
To ensure data security of the device, you can operate the device only after the administrator password is authenticated.

➢ Administrator Authentication



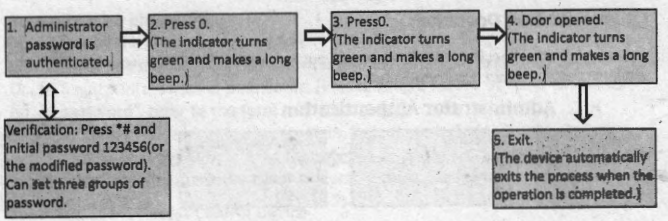
☺NOTE: The administrator password is defaulted as 123456, 3 Groups in total. We need to change all the default administrator password at the beginning.

➢ Change Administrator Password



☺NOTE: 6-digit passwords are automatically verified. For passwords with less than 6 digits, please press "#" to enter the verification process.

➢ Open Door by Administrator Password



☺NOTE: This function can be used to open the door.

➢ **Administrator Password be forgotten**

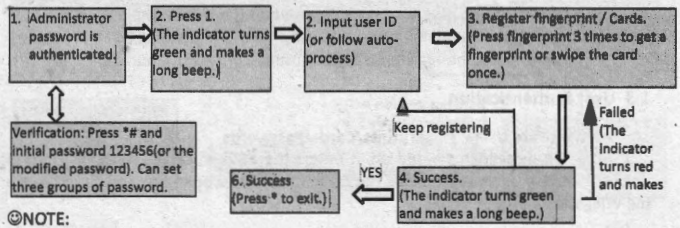
If administrator password is forgotten, we can press the tamper switch 3 times to reset the password to the default administrator password(Default:123456) 30 to 60 seconds after the device is disassembled from the wall or door. (There is a long beep 30 seconds after the device is disassembled from the wall or door.)

1.2 Add New Users

Register fingerprint or Card to a single user, and register cards in batches. (Total 500 numbers for the User ID. User ID would be 1 – 99999.)

☺NOTE: In registration process, if need the Wiegand output signal, please input the User ID number according to the controller software you have. (For example: some access controller software, the User ID needs greater than 99, we need to input the User ID greater than 99.)

➢ **Add New Users**



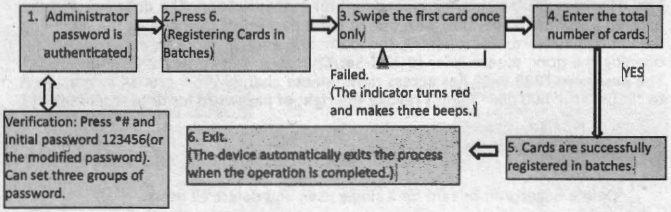
☺NOTE:

1) In registration process, the User ID increases automatically. The device automatically enters the process of registering the next user when a user is successfully registered.

2) The registration process fails if the fingerprint is of poor quality or the fingerprint or the card has been registered. After the device indicator turns green, we can register the user again. (The registered users must not be registered again.)

3. The User ID is 5 digit, please input the 5 digits number and device automatically verified. If User ID less than 5 digits, please press "#" to the next process.

➢ **Register Cards in Batches**



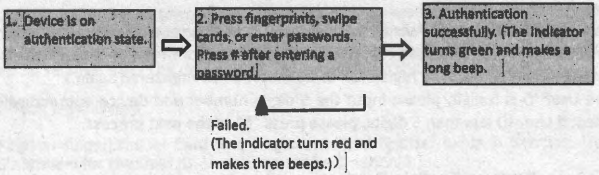
☺NOTE:

1) in process of entering the total number of cards, 3-digit numbers are automatically verified. For numbers with less than 3-digits, press # to enter the verification process. Press * to re-enter the total number of cards.
2) We must clear all the registered users before registering cards in batches. User IDs of to-be-registered cards must be consecutive numbers.

1.3 User Authentication

Authenticate Users' Fingerprints/Cards/Passwords

After the device is powered on, it enters the authentication state for users to unlock the door. Users could make the authentication to open the door, and there's the Wiegand 26 output signal.

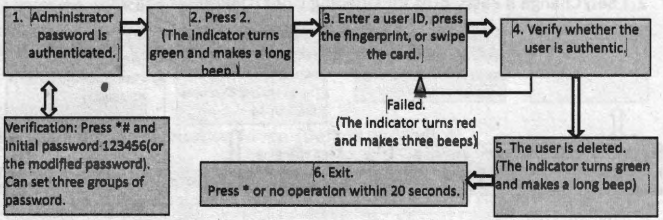


☺NOTE: Press # after entering a password for authentication. The door opens if the entered password is identical with one of the 8 passwords for opening the door. The default 8 passwords for opening the door are empty. To change passwords for opening the door, please refer to "2.1 Set/Change 8 Passwords for Opening Door". **The password "888 888" has access right, please change the 8 groups of password to "000 000".("000 000" means revoke the right of password for door-opening)**

1.4 Delete Users

Delete fingerprint or card for a single user, and delete all users.

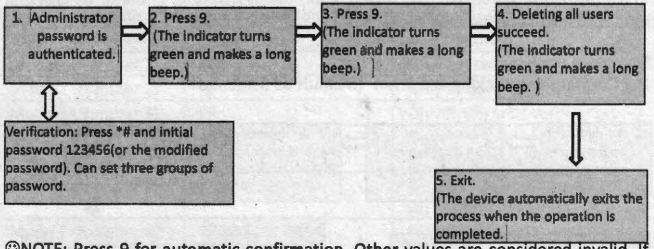
➢ **Delete Single User**



☺NOTE:

1) in process of entering user IDs, 5-digital are automatically verified. For IDs with less than 5-digital, press # to enter the verification process.
2) the device automatically enters the process of deleting the next user when a user is deleted.

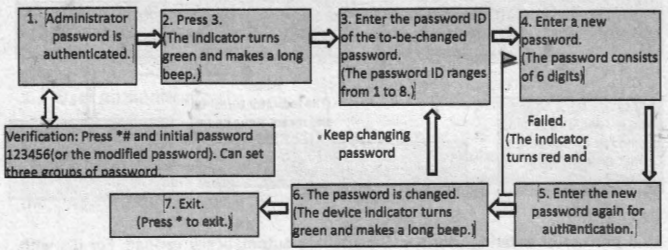
➢ **Delete All Users**



☺NOTE: Press 9 for automatic confirmation. Other values are considered invalid. If and invalid value is entered, the device indicator turns red, and makes a long beep and exits the process.

2. Access Control Management

2.1 Set/Change 8 Passwords for Opening Door (Default as 888 888)

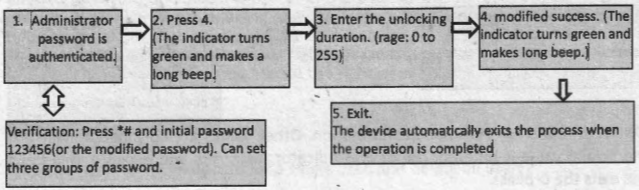


☺NOTE:

1) Enter the password ID of the to-be changed password, if changed to the new password with "0" number only, this Password ID would be disabled. It means we cannot use this password to open the door.

2) If a password is successfully changed, enter the password ID of the to-be-changed password to change the next password.

2.2 Configure Unlocking Duration (Default as 5 seconds)



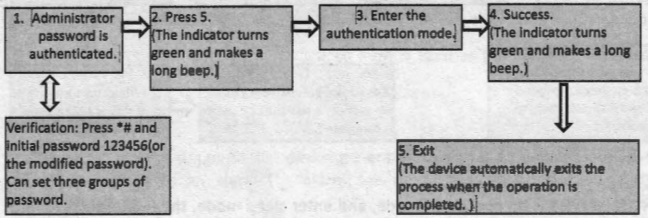
☺NOTE:

1) 3-digit values are automatically verified. For values with less than 3-digits, press # to enter the verification process.

2) Value is 255, door will never be closed.

3) Values greater than 255, need re-enter the value. (Value cannot be greater than 255.)

2.3 Configure Authentication Mode (Default as Mode 4)

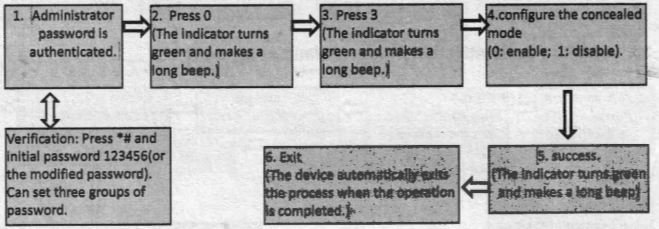


☺ NOTE: Authentication mode description

Authentication Mode	Type	Description
Mode 1 (Number 1)	PW	Only password verification
Mode 2 (Number 2)	RF	Only RF card verification
Mode 1 (Number 3)	FP	Only fingerprint verification
Mode 1 (Number 4)	FP/PW/RF	Fingerprint or password or RF card verification
Mode 1 (Number 5)	RF&PW	RF card and password verification (disorder)
Mode 1 (Number 6)	FP&PW	Fingerprint and password verification (disorder)

2.4 Configure Concealed Mode (Default as disabled)

If the concealed mode is enabled, the indicator is off when the concealed mode is in the sleep mode. We could press any key to active the device (excluding the Doorbell key.)

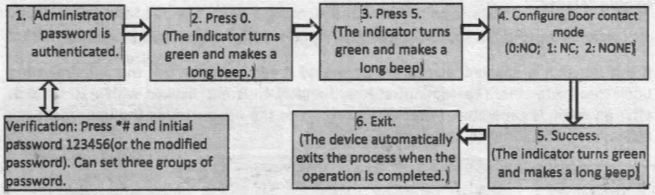


☺

NOTE: Device is on concealed mode, and enter sleep mode, the indicator, keyboard light, fingerprint light, are off, and cannot swipe card. We need to awake the device then swipe card. This mode is defaulted as disable.

2.5 Configure Door Contact Mode (Default as no door contact)

The door contact switch includes 3 models:
NONE: The door contact switch is not used.
NO: The lock is open as long as the door is open.
NC: The lock is closed after the door is closed.



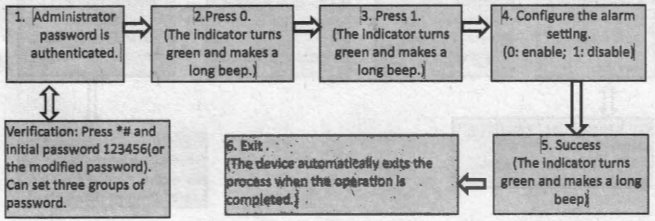
☺ NOTE: the door contact mode configured here is used as the basis for the door sensor alarm.

2.6 Configure Alarm

☛NOTE: If an alarm is triggered, the device generates an alarm. 30 seconds later, the alarm is switched to an alert. The alarm can be terminated after the user is authenticated.

➢ **Configure Alarm setting (Default as Enable)**

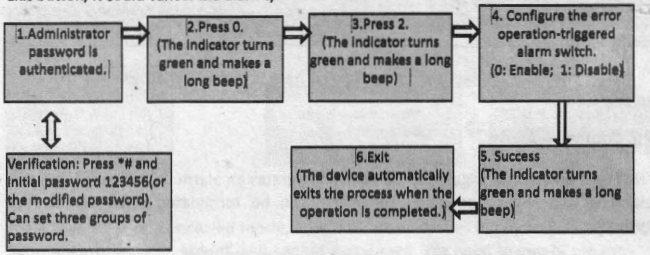
The alarm should be on by default, when it is set to be closed, the error operation-triggered alarm, tamper alarm, the alarm delay for the door status contact will be disabled.



☺NOTE: when we configure "Alarm" to "Disable", "Tamper Alarm" as "Enable", the device has been removed before, then it will send out alarm the next time we enable "Alarm".

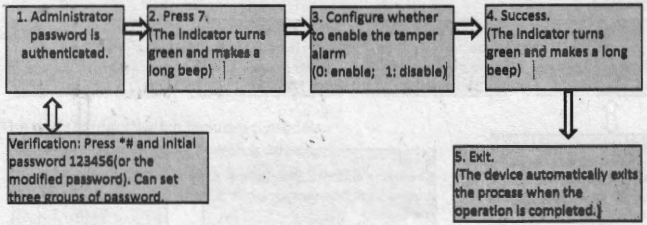
➢ Configure Error Operation Triggered Alarm (Default as enable)

If this function is enabled, alarms are generated if administrator fails the authentication upon three attempts. The administrator authentication is not allowed within 20 seconds after an alarm is generated. (After verify success or the people inside the door press the Exit button, it could cancel the alarm.)



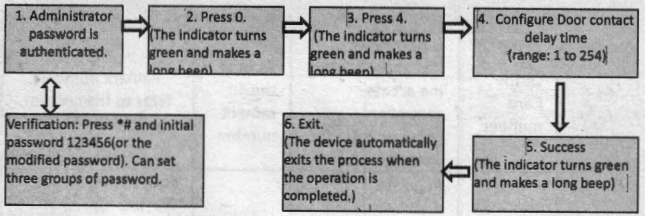
➢ Configure Tamper Alarm (Default as Enable)

If this function is enabled, alarms are generated once the device is disassembled.



➢ Configure Alarm Delay for Door Contact (Default as 5 seconds)

Door contact delay: indicates the delay in checking the door contact after the door is open. If the door contact state is inconsistent with the normal state set by the door contact switch, an alarm will be generated, and this period of time is regarded as the "Door contact delay".



☺ NOTE:

1) 3-digits values are automatically verified. For values with less than 3-digits, press # to enter the verification process.
2) Values greater than 254 are considered invalid.

3. Wiegand Output Details

◆ Wiegand output signal must be registered in this access control device, and signal output after verification successfully on this device.

Authentication mode and Output signal:

Authentication Mode	Card	Fingerprint	Password	Remark
Mode 1/2/3/4	Output Card number	Output User ID. (Set according to the access controller software rules for User ID.)	Output the remark number	Remark number: refer to the content below this table.
Mode 5(Card+Password)	Output User ID number.	NULL	Output the remark number	For example: We use Group NO.1 "Open Door Password" and the registered Card of User ID=3 for the authentication combination, Wiegand signal output number as 1600003. (For the signal 1600003, could separate as two parts: "16" stands the Group NO.1 "Open Door Password", "00003" is the User ID=3.) ***NOTE: the "Group***

				NO.1 "Open Door Password" here is the password we set to enter the door. Please refer to " 2.1 Set/Change 8 Passwords for Opening Door"
Mode 6(fingerprint+password)	NULL	Output the User ID(Set according to the access controller software rules for User ID)	Output the remark number	For example: we use Group NO.2 "Open Door Password" and the registered fingerprint of User ID=101for the authentication combination, Wiegand signal output as : 3200101. (For the signal 3200101, could separate as two parts: "32" stands the Group NO.2 "Open Door Password", "00101" is the User ID=101.)

(1) In Authentication Mode 1/2/3/4, the "Card authentication" output the Card number, "Fingerprint authentication" output the User ID number, "Password authentication" output the remark number of the Group ID as "remark number + 000 00".

Remark number for the "Open Door Password" Group ID as the following:
Group NO.1 password, output as : 16 00000;

Group NO.2 password, output as: 32 00000;
Group NO.3 password, output as: 48 00000;
Group NO.4 password, output as: 64 00000;
Group NO.5 password, output as: 80 00000;
Group NO.6 password, output as: 96 00000;
Group NO.7 password, output as: 112 00000;
Group NO.8 password, output as: 128 00000;

(2) When authentication mode as combination mode:
"Card+Password" output: the User ID of the registered Card (5-digit) + the remark number of the "Open Door Password" Group ID.
"Fingerprint+Password" output: the User ID of the registered Fingerprint(5-digit) + the remark number of the "Open Door Password" Group ID.

NOTE:

1) The "Open Door Password" Group ID here is the password we set to enter the door. There're 8 groups password we could set to enter the door. Please refer to "2.1 Set/Change 8 Passwords for Opening Door"

2) For some access controller software, there's the limitation for the User ID, we need to pay attention to the User ID we register to the access control device in registration process.

Keep a record of "User ID, Group No. for door-opening" for future user data deleting.

Management Group	**Initial Password**	**Modified Password**	**Modified Password(second time)**
Admin Password Group 1	123456		
Admin Password Group 2	123456		
Admin Password Group 3	123456		
Door-Opening Password	**Initial Password**	**Modified Password**	**Modified Password(second time)**
Door-Opening Password Group 1	888 888		
Door-Opening Password Group 2	888 888		
Door-Opening Password Group 3	888 888		
Door-Opening Password Group 4	888 888		
Door-Opening Password Group 5	888 888		
Door-Opening Password Group 6	888 888		
Door-Opening Password Group 7	888 888		
Door-Opening Password Group 8	888 888		
NOTE: The password "888 888" has access right, "000 000" means revoke the right of password for door-opening.			

User ID	User Name	Card Number	Door-Opening Password Group No.