

Installation Guide & Quick Start Guide

2.8" Touch Screen AC Terminal

Version : 1.0

Date : April, 2015

All design and specification declared are subject to change without advanced notice.

Contents

Safety Precautions.....	1
1. Packing List.....	2
2. Overview of Operation Panel	3
3. System Structure.....	4
4. Installation	5
4.1 Installation of Device.....	5
4.2 Connection with peripheral equipment.....	6
4.3 Test and Examination after Installation.....	9
4.4 Reset Button and Tamper Switch.....	10
5. Quick Start Guide.....	11
5.1 Communication Settings.....	11
5.2 System Settings.....	12
5.3 Access Settings.....	12
5.4 User Management.....	14
5.5 Verification	17

5.6 Data Management	18
5.7 U Disk Management.....	19
5.8 Viewing Access Report.....	19
6. Others.....	20

Safety Precautions

Thank you for using our products. Please read this manual carefully before using this product for a comprehensive understanding so as to avoid causing unnecessary damages to the product.

○ Important Notes

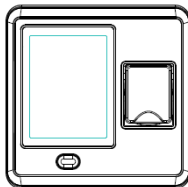
- Do not place the device under strong light.
- Use regulated 12V DC power source (separately purchased; it is recommended to use Uninterrupted Power Supply with backup battery option to avoid power failure).
- Do not place the device in a vulnerable location where it might be subject to vandalism.

○ Before Installation

1. Prior to installation, cut off all power to prevent personal injury and damage to the device and peripheral equipment.
2. Connect the GND first in order to prevent electrostatic damage to the device.
3. Connect 12V DC power supply to the device at last. If the device does not operate properly, cut off power to it before examining/dismantling. Wiring the device when the power is on may cause damage to the terminal; such damage is not covered in warranty.
4. Mount the device at a comfortable height, typically between 1.4~1.5 meters from the ground.
5. After installation, remove the protective film from the device display and fingerprint sensor.
6. To prevent being accidentally locked while testing the exit button, keep a person inside the door.
7. Run the auto test function to confirm that installation is successful.
8. In order to maximize the life of the device, use the auto-sleeping function; sleeping time can be set in the system parameter menu.
9. The rated voltage of the device is DC 12V, and the rated current is 300mA. If an incorrect voltage is used, the device may be damaged or may not operate the electric door lock (if attached).

10. Improper wiring may cause the device's main circuit board and fingerprint sensor to burn out. Damage resulting from improper wiring is not covered in warranty.
11. Only use the supplied transformer and cord. Do not attempt to extend the cord by cutting and splicing.
12. If using RS485 mode of communication with PC, use specialized RS485 cables and powered RS232/485 converter. If the length of RS485 cable exceeds 100 meters, using a 120Ω terminator is recommended.
13. Refer to the user handbook and operating instructions for further information.

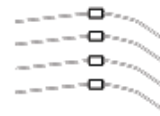
1. Packing List



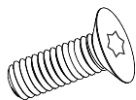
1 Access Device



1 Screw Driver



4 Diodes (FR107)



1 Star-shaped Screw

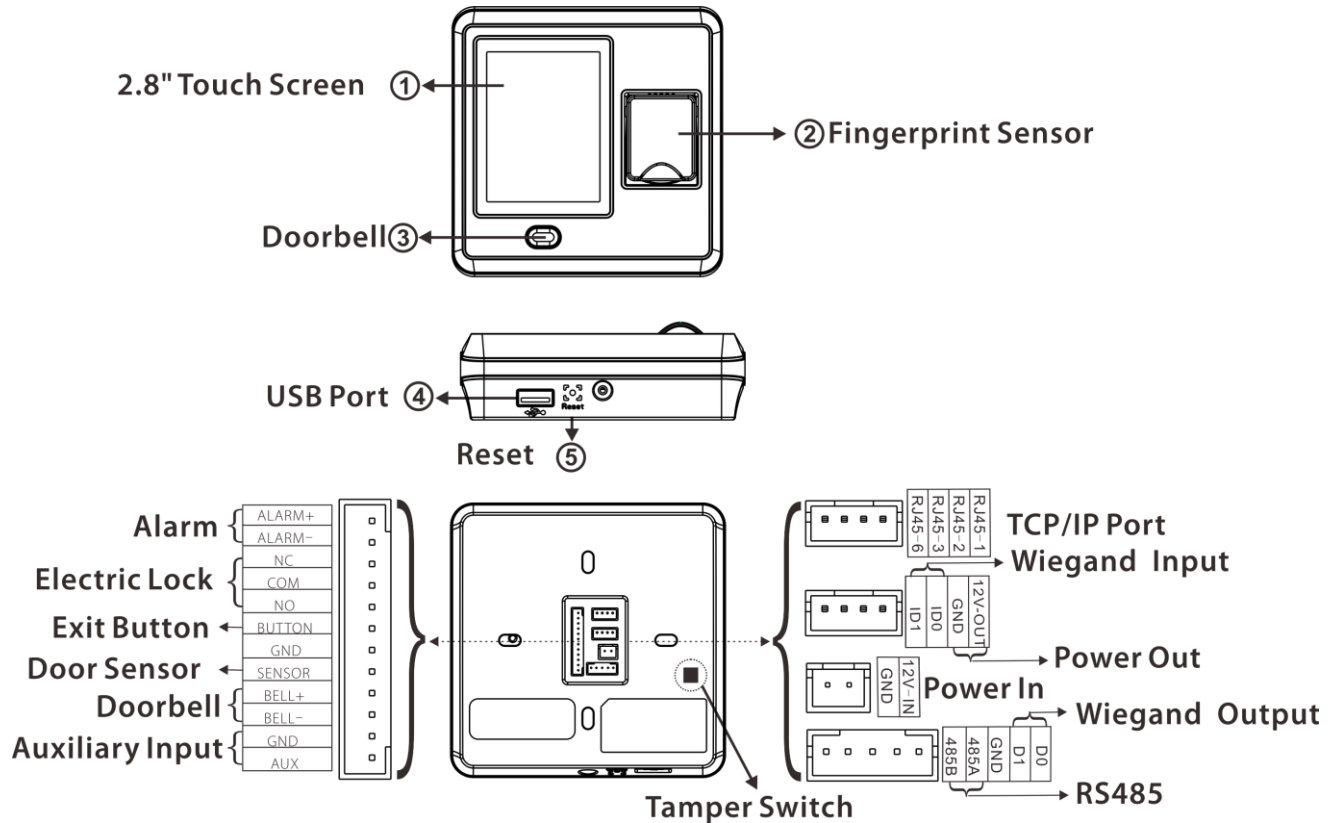


4 Wall Plugs /Screws



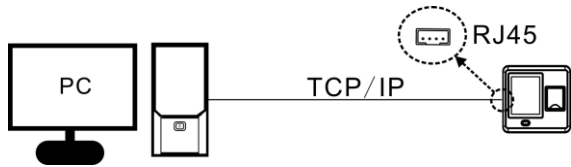
1 CD

2. Overview of Operation Panel

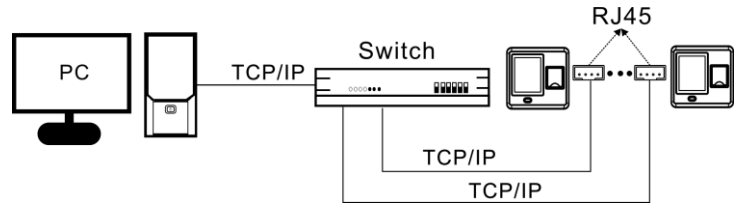


3. System Structure

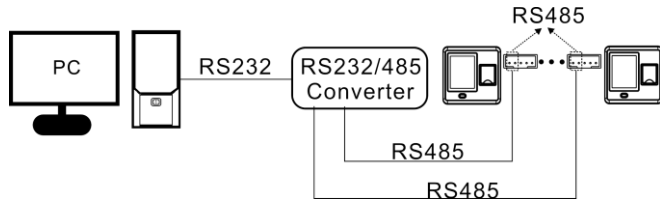
Directly connected with PC through TCP/IP



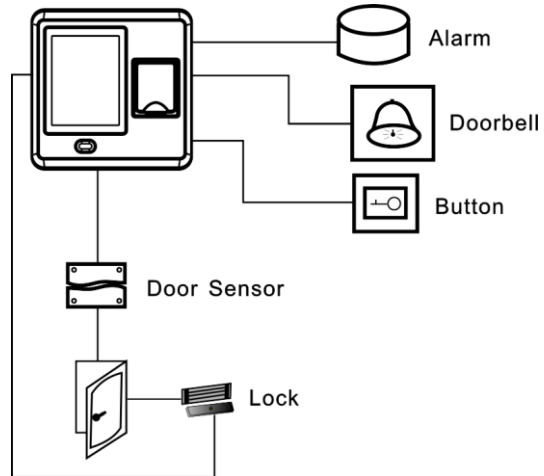
Connected with PC through TCP/IP network



Connected with PC through RS485 network

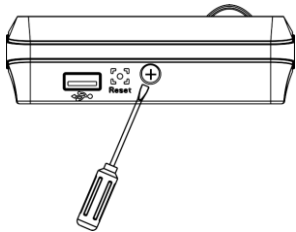


Wiring diagram

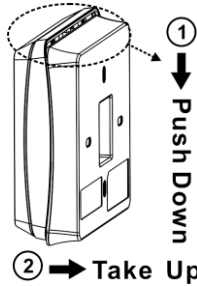


4. Installation

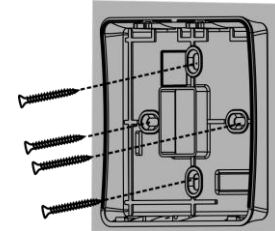
4.1 Installation of Device



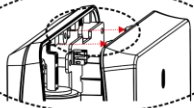
1. Remove the bottom screw.



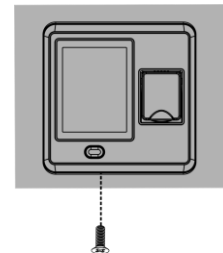
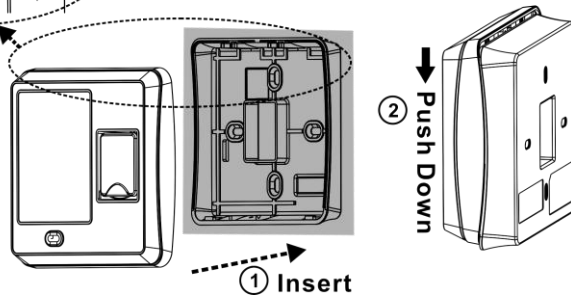
2. Take out the Back Cover.



3. Fix the Back Cover on the wall with screwdriver.




4. Fix the device on the Back Cover.



5. Tighten the bottom screw.

4.2 Connection with peripheral equipment

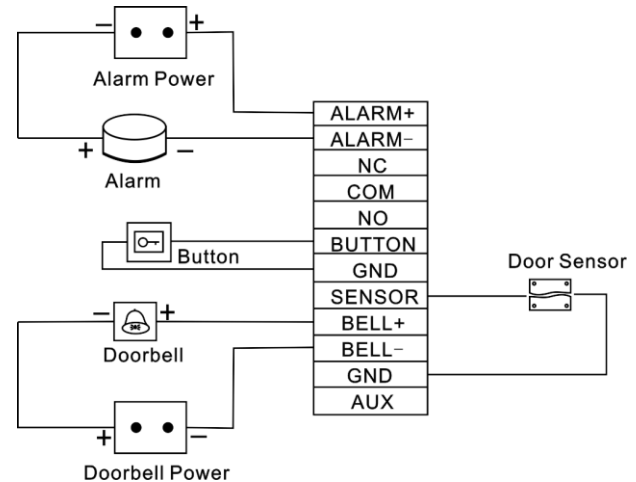
 **Caution:** Please make sure the power is cut off before wiring, otherwise it is possible to damage the device.

● Door Sensor Connection

● Button Connection

● Alarm Connection

● Doorbell Connection



● Lock Connection

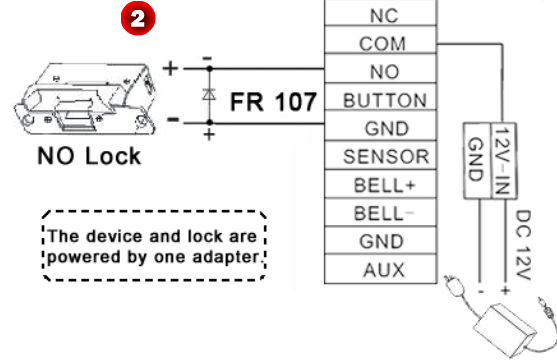
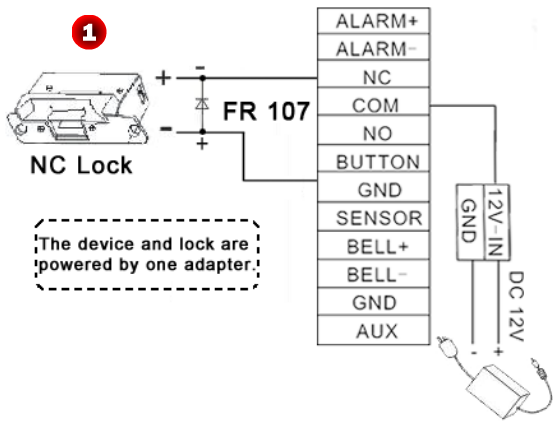
Selecting door lock: The choice of lock depends on the door-electric strikes and bolts, while magnetic locks, turnstiles and barriers are all options depending firstly on the architecture and secondly on the required resistance for attachment. Please consult your supplier for more information.

Connect with electric lock: After the user verifies the identity, the device will output the unlock signal. The device supports NO (Normally Open) LOCK and NC (Normally Closed) LOCK.

NO LOCK: the door is normally open at power on, so it closes the door at power off.

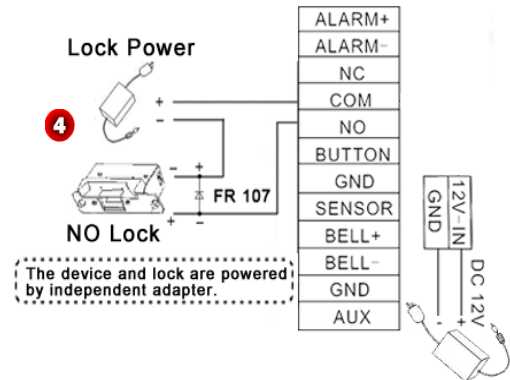
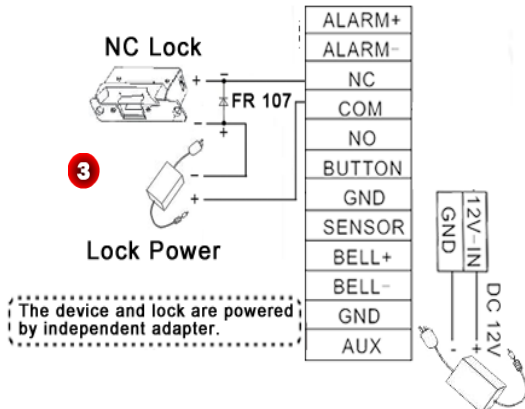
NC LOCK: the door is normally closed at power on, so it opens the door at power off.

The device can supply power directly to a door lock, please refer to **Figure 1, 2**. (Ensure that proper voltages are applied to the lock terminals and check on the current ratings of the locks.)



However, in the following three scenarios, it is recommended that the door lock has an independent power source, and is NOT powered by the device; shown as Figure 3, 4.

- When the door lock voltage is not 12V DC
- When the door lock runs on 12V DC but requires more than 1A (amp)
- When the distance between the device and door lock is greater than 15 feet



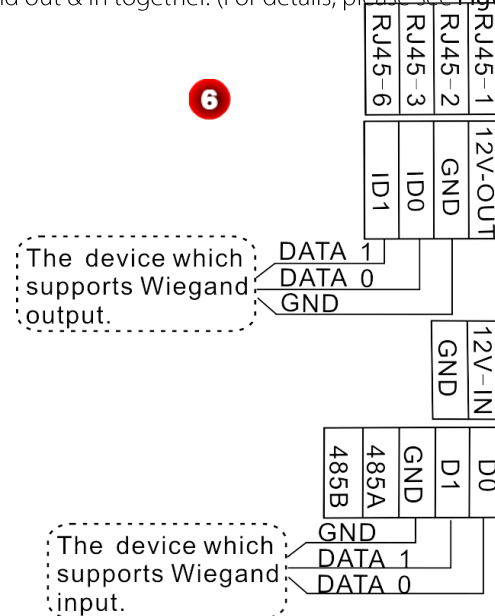
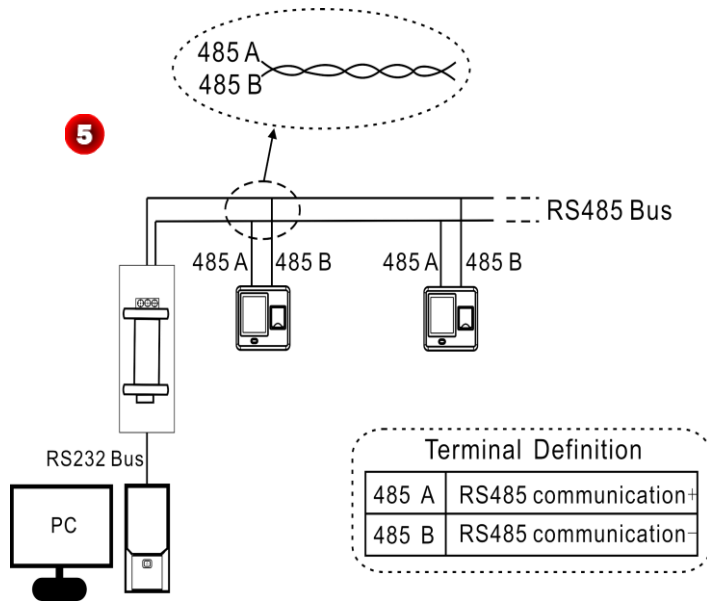
- RS485 Connection


RS-485 systems uses a bus structure configuration connect the driver to the receiver.

- Wiegand Function

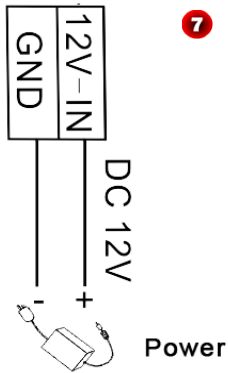
Wiegand Output: This device provides standard Wiegand 26 output, which can be used as reader. The distance from the controller to device cannot be more than 15 meter (If the signal must be transferred much further or there is a strong interference around, please adopt a Wiegand signal amplifier. For details, please see **Figure 6**.)

Wiegand Input: The device with Wiegand input function can be connected to the external card reader. Device and card reader can be installed respectively inside and outside of the door, controlling the lock and out & in together. (For details, please see **Figure 6**.)



 **Note:** No matter the device is powered by access controller or not, the ground ports of them have to be properly together to ensure the Wiegand transferal is reliable.

- **Power Connection: Shown as Figure 7.**




4.3 Test and Examination after Installation

Make a test and examine prior to power on, inspect whether the lock driver is OK or not.

1. The green LED begins to glitter after powering up.
2. Enter [Main menu] > [System] > [Auto Test].
3. Enter [Main menu] > [User Mng] > [New User] > [FP], enroll a fingerprint, and use the fingerprint to test access system and door lock.
4. If there is no any problem, please delete this enrolled fingerprint.

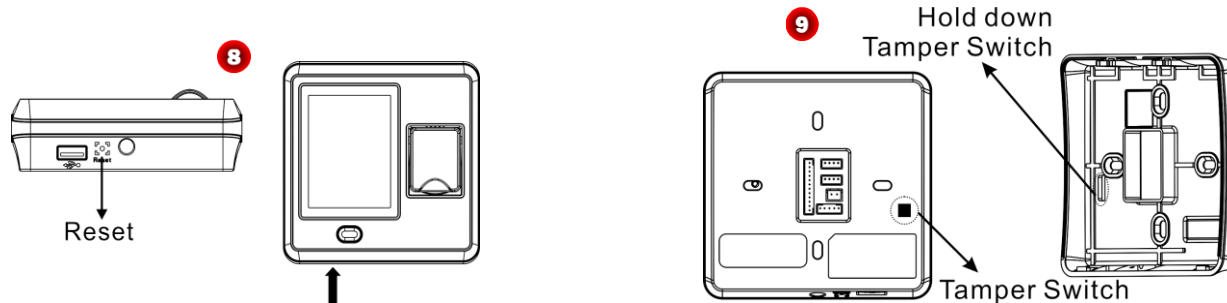
4.4 Reset Button and Tamper Switch

Reset: When the device fails to work due to operation error or other accidents, you can restart device by reset button. To reset the device, use a small tool (e.g. pin or paperclip) to press the reset button (labelled Reset, as shown in **Figure 8**), located on the underside of the device.

 **Note:** It does NOT erase any stored data (i.e. templates, transactions, settings). This information will be available as soon as power is restored.


Tamper Switch is located on the back of the device (**Shown as Figure 9**), when the device detects that it is being “tampered”, it will send an alarm signal.

If the administrator is lost, you can wait for 30 seconds (there is a short beep) after the device is disassembled from the wall, then press the tamper switch for three times to access the device menu.



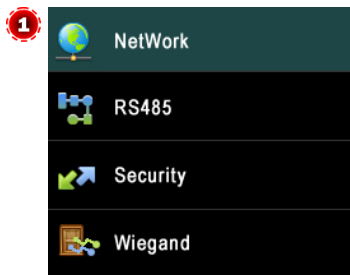
5. Quick Start Guide



Press  to enter Main Menu, which include User Management (User Mng), Access Settings (Access), Communication Settings (Comm.), System Settings (System), Data Management (Data Mng) and U Disk Management (U Disk).

5.1 Communication Settings

Press [Comm.] button in Main Menu to enter the Communication Settings (Comm.) Interface, shown as Figure 1.



Network: To set IP address (The default value is 192.168.1.201), Subnet Mask (The default value is 255.255.255.0) and Gate Way (The default value is 192.168.1.254) for device.

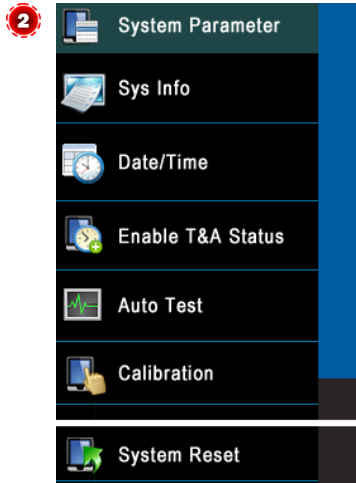
RS485: To set the baud rate for the communication between the device and PC.

Security: To set Device ID and password for the connection between the device and PC. The default password is 0 (no password).

Wiegand: To configure Wiegand Function.

5.2 System Settings

Press [System] button in Main Menu to enter the System Setting (System) Interface, shown as Figure 2.



Sys Parameter: Set Threshold (1:1), Match Threshold (1:N), Date Format, Sleep time, enabling Key tones/Voice and adjust Volume as required.

Date/Time: To set device's Date and Time as required.

Enable T&A: To enable/Disable T&A Status and Auto Switch function as required. In addition, you can set the auto switch time for each status.

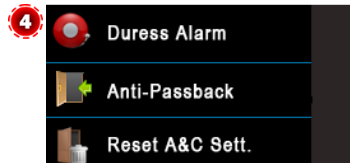
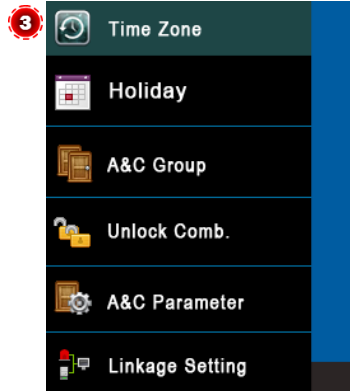
Auto Test: TFT Test, Sensor Test and RTC Test.

Calibration: To calibrate the touch screen.

System Reset: To restore all system parameters to factory default settings.

5.3 Access Settings

Press [Access] button in Main Menu to enter the Access Setting (Access) Interface, shown as Figure 3, 4.



Time Zone: To add Time Zones. The device controls access according to the time zones.

Holiday: To add access holiday, and select Access Time Zone for it.

A&C Group: Access Group refers to one selected time zone or several selected time zones that can be opened by verification. (Note: The A&C Group must be set under Access Setting.)

Unlock Comb.: To add Unlock Combination for device.



Note: The total number of users in the access group must be equal to or smaller than 5.

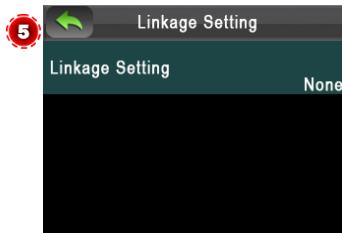
A&C Parameter: Set Lock(S), Door Sensor Delay(S), Door Sensor Mode (Open, Close or No), Alarm Delay(S), Alarm Count (times), Close/Open Time Zone and whether valid holidays.

Linkage Setting: For the specific setting method, please see Linkage Setting.

Duress Alarm: To set the duress alarm delay time as required.

Anti-Passback: To set anti-passback function for device.

Reset A&C Sett.: To reset all the Access Setting to factory defaults and then restart device automatically.

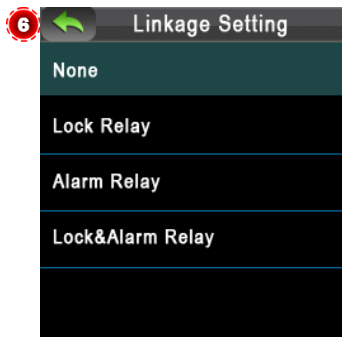


○ Linkage Settings

The device has Auxiliary Input function. When receiving the linkage signals, the device will perform related linkage operations according to the linkage operation type in the linkage settings.

Press [Linkage Settings] in Access Settings to enter the Linkage Settings interface; shown as Figure 5. Press [Linkage Settings] to select linkage type, shown as figure 5.

- ✧ Lock Relay: The lock is opened after the device receives the linkage signal.
- ✧ Alarm Relay: The alarm is triggered after the device receives the linkage signal.
- ✧ Lock & Alarm Relay: The lock is opened and an alarm is triggered after the device receives the linkage signal.

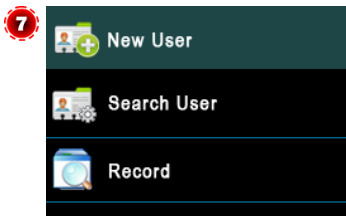


○ Linkage Cancellation

Press  to enter Main Menu. The *Cancel linkage?* message is displayed on the screen. Press [OK] to confirm and cancel linkage.

5.4 User Management

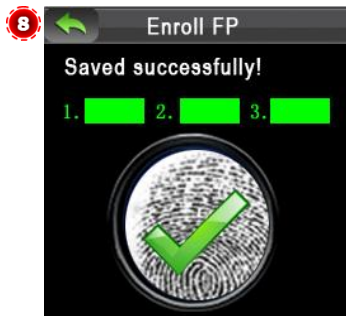
Press [User Mng] Button in Main Menu to enter the User Management (User Mng) Interface, shown as Figure 7 :




New User: To input Id No. (The max length is 9) and password (The maximum length is 6), set user role (user or administrator) and enroll card.

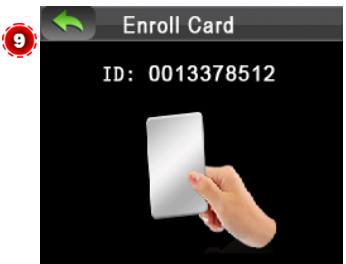
Search User: Input Id No. and press [OK] to start searching, you can also edit and delete the user, and set the user's access.

Record: Input ID NO. and month, press [Search] to search and check the records of this user in the specific month.




○ FP(Fingerprint) Enrollment

1. Press [FP] in New User, the Enroll Fingerprint interface will then be displayed.
2. Follow the operation prompt information to place a finger on the fingerprint sensor properly for three times until the enrollment succeeds, and the system will return to the New User interface automatically.
3. Press  to exit, save user information according to the operation prompt box.




○ Card Enrollment

1. Press [Card] in New User, the Enroll Card interface will then be displayed.
2. Follow the operation prompt information to swipe the card above the card reader (at the fingerprint sensor). After the enrollment succeeds, the system will return to the New User interface automatically.
3. Press  to exit, save user information according to the operation prompt box.

10

○ Searching User

1. Press [Search User] button in Use Mng, shown as figure 10.
2. Input ID Number. (Note: You can press  or [C] to modify or delete the incorrect input.)
3. Press [OK] to search the use, shown as figure 11.

11

○ Editing User

Edit the added user. (Note: In the Search User interface, press [Edit] to enter the Edit interface, the specific operations is the same as New User (Add User).

○ Deleting User

1. Press [Del User] in Edit, shown as figure12.
2. Press [Del User] to enter the Del User interface. Select delete type (Delete Password, Del ID Card only, Delete Fingerprint or Delete User), and then press [OK] to confirm and carry out the corresponding delete operation.

 Note:

- (1) The device displays the operation based on the information registered by the user. For example, if the user does not register the password, the option *Delete Password* will not be available.
- (2) If *Del User* is selected, the user's fingerprint, password, and ID card information will be deleted.

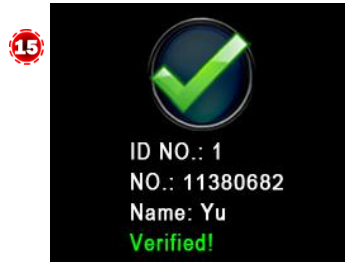
12



○ User Access

1. Press [User Access] in Search User, shown as figure 13.
2. Set the Group No., Use Time Zone and select Duress FP as required.


5.5 Verification



○ Verification by Fingerprint or Card

Place finger on the fingerprint sensor properly or swipe card above the reader (at the Fingerprint Sensor); after verification succeeds, the interface will be as shown in figure 14 (Fingerprint Verification)/ 15 (Card Verification).

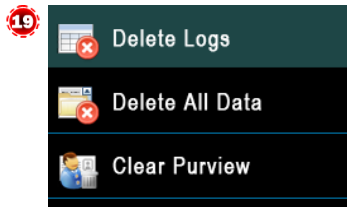
○ Verification by Password

1. Press  to Input ID NO. (for the specific input method, please see Search User), shown as Figure 16.
2. Press [OK] to input password.
3. Input the correct password (same as inputting ID Number), shown as figure 17.
4. Press [OK] to confirm the password, shown as figure 18.



5.6 Data Management

Press [Data Mng] in Main Menu to enter the Data Management (Data Mng) interface, shown as Figure 19.



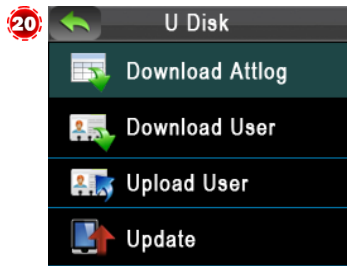
Delete Logs: To delete all attendance logs.

Clear All Data: To delete all attendance logs, user information, and Time Zone, Holiday, A&C Group, Unlock Combination settings.

Clear Purview: Set all the administrators to normal users.

5.7 U Disk Management

Press [U Disk] button in Main Menu to enter the U Disk Management interface, shown as Figure 20.



Download Attlog: To download all attendance logs to the U Disk, imports logs into the Access 3.5 software through Import Data From USB disk function, and then view Access Report as required.

Download User: to download all user information to the U Disk.

Upload User: To upload user information (stored in U Disk) into the device.

Update: You can upgrade the device firmware through this menu; an upgrade file is needed in the U Disk.

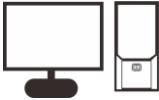
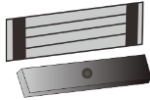
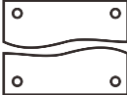
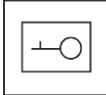

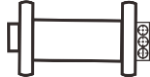
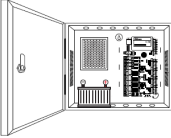

5.8 Viewing Access Report

1. Connect the device to the network.
2. Run *Access3.5* software.
3. Add the device to the software, download logs from device (you can use the U Disk to download logs too), and then analyze logs and view the access report as required.

Bundled *Access3.5 Security System* is unique software. For detailed operations, refer to *Access3.5 software user manual* in the CD.

6. Others

The following equipments are needed for an access control system but are not included in the standard package.

Name	Picture	Name	Picture
PC		Lock	
Door Sensor		Button	
Alarm		485 Converter	
Access Control Panel		Ethernet cable	
Doorbell	