

Access Control Terminal Quick Start Guide



Important Notes

- Do not place the Access Control Terminal under strong light.
- Use regulated DC 12V/3A power source (supplied from control panel or separately purchased power supply).
- Do not place the Access Control Terminal in a vulnerable location where it might be subjected to vandalism.

Contents

1. Features	1
2. Specification	1
3. Basic Contents	2
4. Optional Accessories	2
5. Product Introduction	3
5.1 Front View	3
5.2 Rear View	3
6. Installation Diagram	4
7. Product Dimensions	4
8. Cable Specification	5
9. Mounting the Unit	6
10. Hardware Setup	6
11. Management Card	6
12. Enrolling an Ordinary User	7
13. Delete an Ordinary User	8
14. Buzzer and LED Indicator	8

1. Features

- **Rugged structure for outdoor installation and extra durability**
 - * IP65 rated waterproof and dustproof structure
- **Fast and accurate fingerprint algorithm**
 - * Fingerprint identification in 1 second
 - * Stores 3,000 fingerprint templates, 30,000 cards and 100,000 transactions
- **Easy installation and connectivity**
 - * Wiegand input & output
 - * Network interface by TCP/IP or RS485
- **Full access control features**
 - * Anti-passback
 - * Access control interface for 3rd party electric lock, door sensor, exit button, alarm
- **Slim and elegant design**
 - * One of the world's smallest fingerprint terminals
 - * Sleek and slim design for narrow space

2. Specification

Algorithm Version	Finger V10.0
Communication	TCP/IP, RS485
Fingerprint Capacity	3,000 Fingerprints
Card Capacity	30,000 Cards
Log Capacity	100,000 transactions
RF Card	EM(standard)/Mifare(optional)
Authentication	Finger/Card
Wiegand Signal	Wiegand in & out
Ingress Protection Rate	IP65
Operating Voltage	12VDC 3A
Operating Temperature	0°C ~ 45°C (32°F ~ 113°F)
Size	62.5mm x 185mm x 41.5mm (W x H x D)

3. Basic Contents



Access Control Terminal



Metallic Mounting Plate



Wall Mounting Screws
& Holders



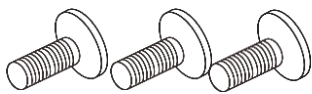
Software CD



Installation Guide



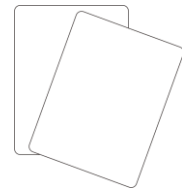
Mounting Paper



Star-shape Screw
for Mounting Plate

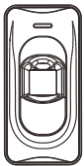


Star-shape Screw Driver



ID Card(1pcs)

4. Optional Accessories



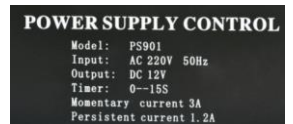
Fingerprint Slave Reader



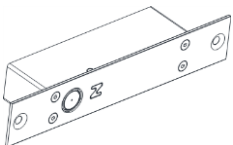
Exit Button



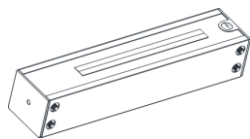
Alarm



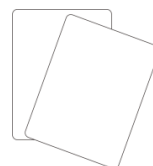
Power Supply Controller



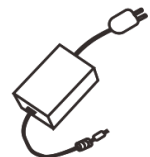
Electric Bolt



Electric Magnetic Lock



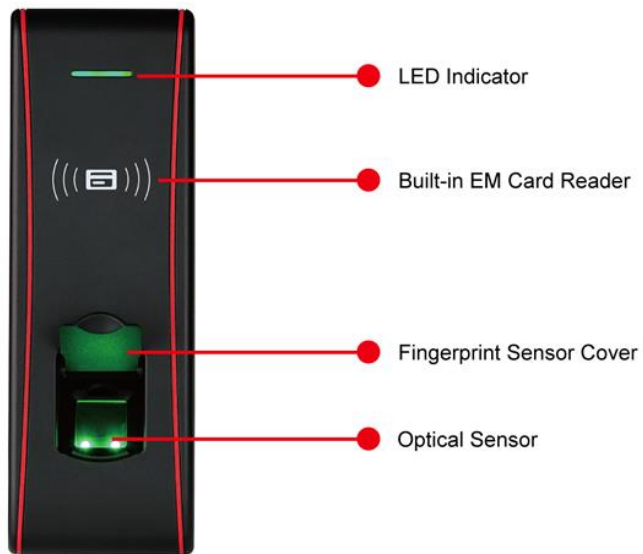
Mifare Card



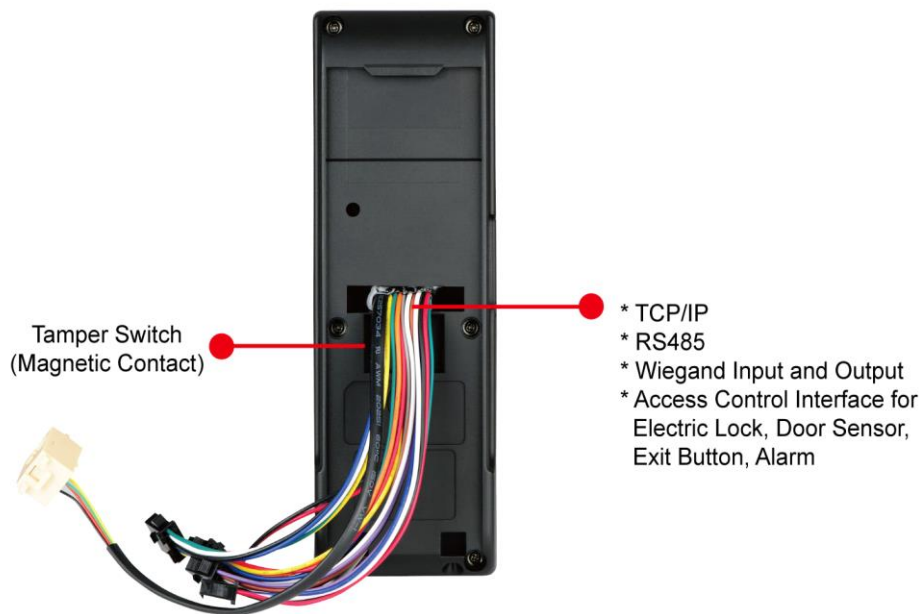
12V3A Power Adaptor

5. Product Introduction

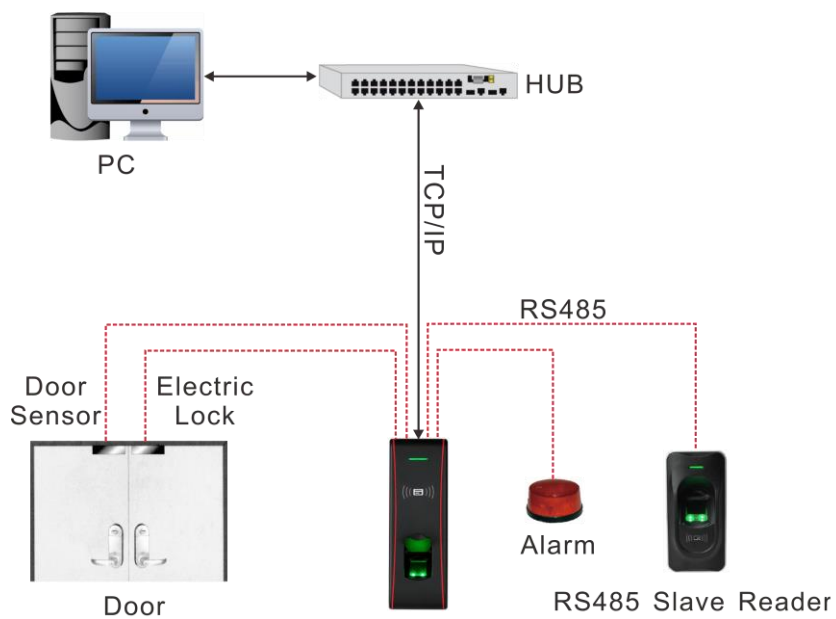
5.1 Front View



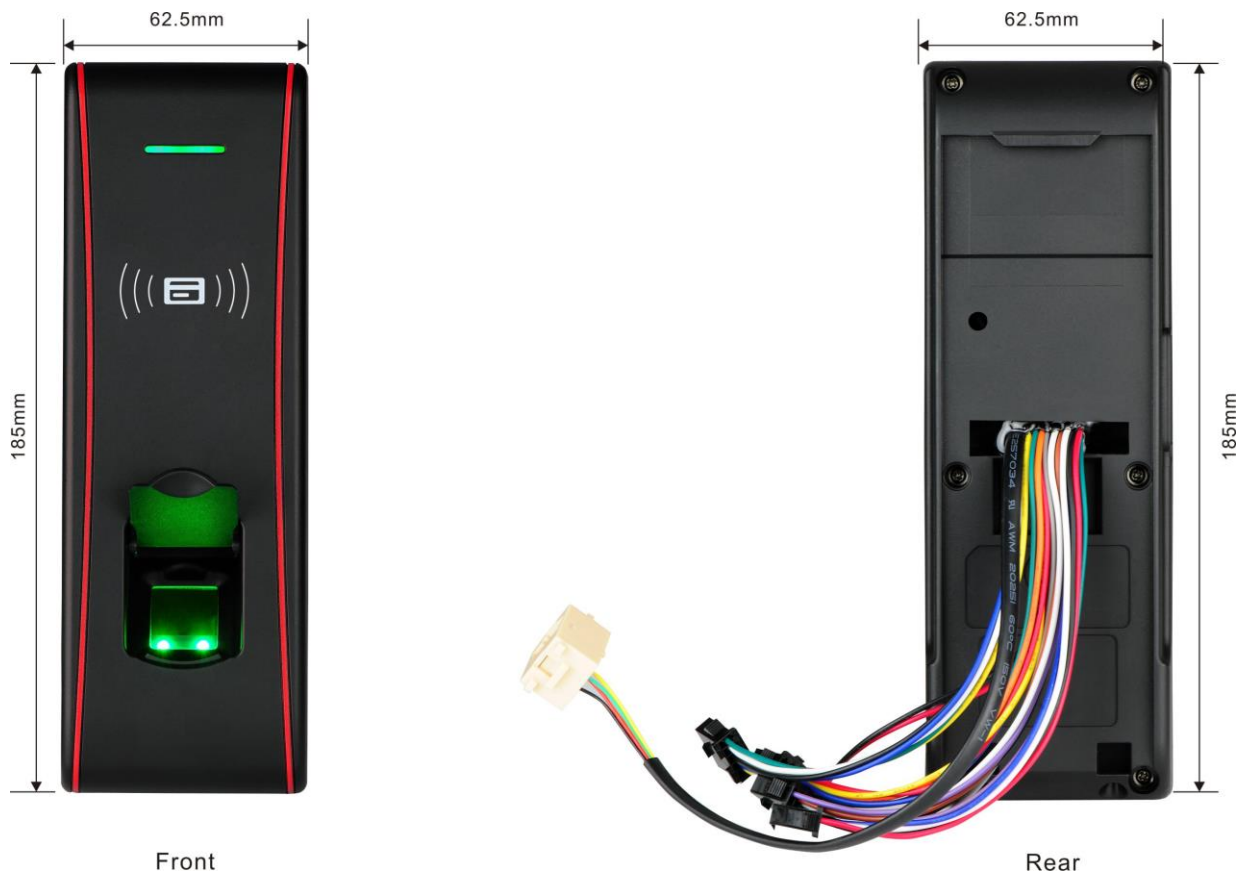
5.2 Rear View



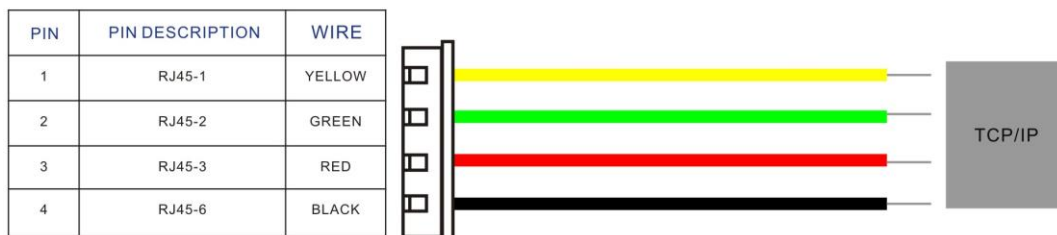
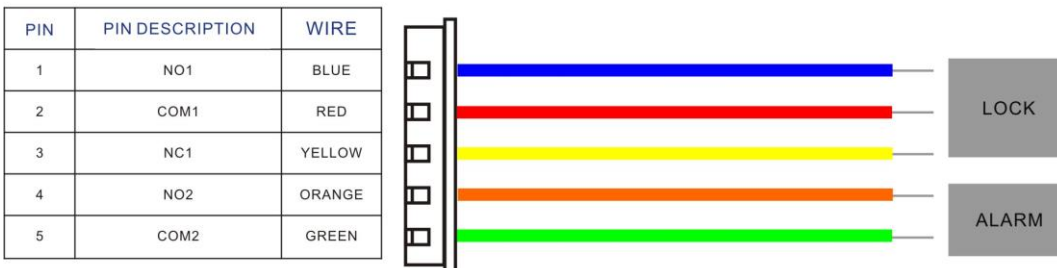
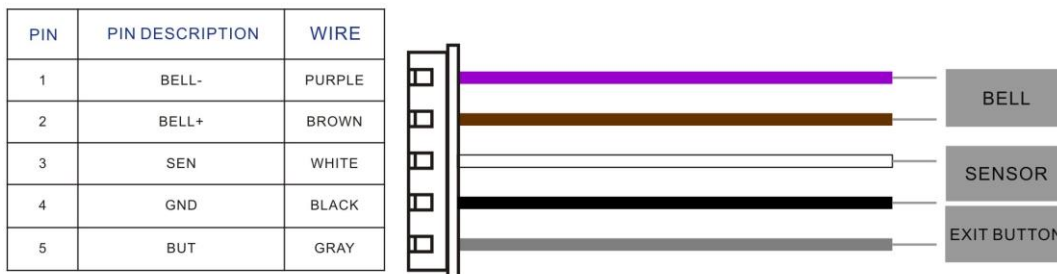
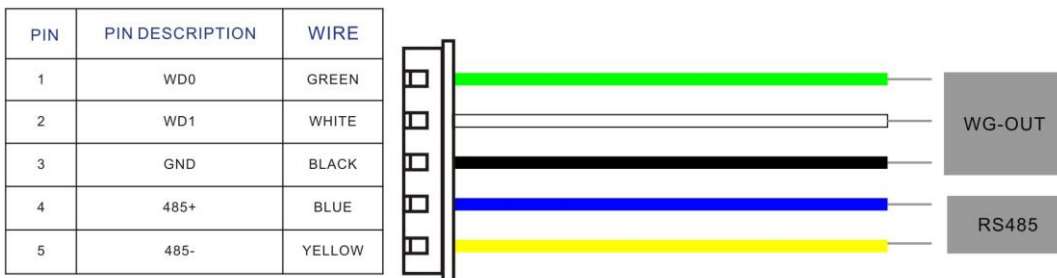
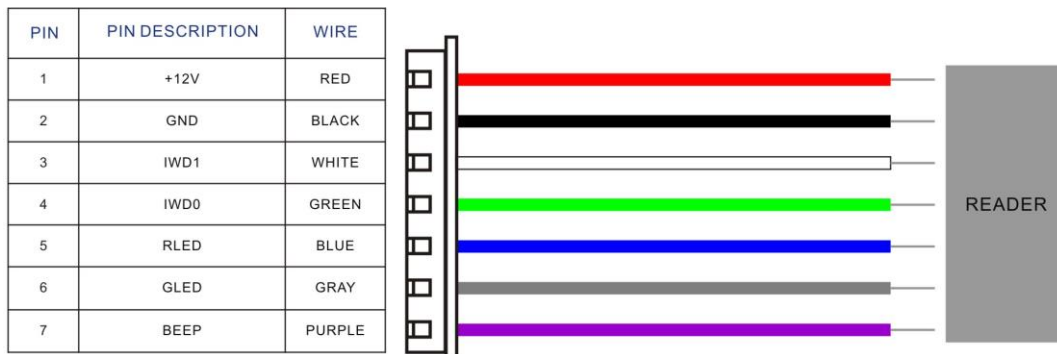
6. Installation Diagram



7. Product Dimensions



8. Cable Specification



9. Mounting the Unit

- Locate the appropriate area for the unit. Place the unit approximately 5 ½ feet above the ground level so that the users are comfortable in using the unit with fewer chances of errors.
- Create conduits for the power and network cable on the wall so that the unit receives the connections from the back of the wall.
- Remove the screw at the bottom of the unit when held vertically.
- This will remove the back plate of the unit.
- Install the back plate of the unit on to the wall and connect the power and network cables from the behind the back plate.
- Connect the wires of the access control terminal of the device, including lock control, exit button, door sensor and alarm etc.
- Secure the front of the unit on the back plate by reinstalling the removed screw from the bottom of the unit earlier.

10. Hardware Setup

- Power on the unit by supplying 12V DC to the power and GND pins on the back of the unit. The power supply is not supplied with the unit. Please make sure that the power requirements are strictly met to avoid permanent damage to the unit.

11. Management Card

Note: You can use **USB fingerprint scanner with Access3.5 software to register user fingerprint and information, alternatively you can add or delete users by a 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). 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 the door.

Management Card

A management card is a card specially assigned to an administrator to delete or add ordinary users; but it cannot be used to unlock the door. Each device could only register one management card. If no management card is registered, you are not able to perform operation on the device directly.

Note: The fingerprints of the user who holds a management card shall be enrolled through software. Users who hold management cards can only verify their identity and unlock the door by their fingerprints.

To register a management card, proceed as follows:

- Power on the device till the buzzer has a short beep at first then a long beep (or Green LED starts to blink).
- If the device detects there is no management card registered, The Green LED blinks once every three seconds, at the same time the buzzer has one long beep every three seconds. It enters the **management card registration state**.
- Please swipe the card near the proximity area to register.
- If register succeeds, the Green LED is normally on for one second, at the same time the buzzer has one

long beep.

After that the system returns to verification state, the Green LED blinks once every two seconds (the buzzer has no beep).

Note: You have to reboot device again to register management card if it's operation timeout. You can use the Software to configure or modify the management card once it is registered.

Operation Timeout: When there is no operation after 15 seconds, the device will automatically return to verification state.

Verification State: It is a state that for users to verify their identity and unlock the door. The Green LED blinks once every two seconds (the buzzer has no beep).

You can add or delete users by swiping a management card for different times in a row:

- By swiping the management card once, the system enters to **single user enrollment state**.
- By swiping the management card five times in a row, the system enters to **single user deletion state**.

Note: the interval between each two swipes in a row should be less than **5 seconds**

12. Enrolling an Ordinary User

To enroll an ordinary user by management card, the system will automatically generate an ID number to the user and it enters to enrollment state.

Enrollment state: It is a state to enroll single users. The green LED blinks twice every three seconds, at the same time the buzzer has two short beeps every three seconds.

Note: It is allowed to enroll one user only each time. Each user is allowed to enroll one ID card only and 10 fingerprints at most.

To enroll a user, proceed as follows:

- Swipe the management card once, The green LED blinks twice every three seconds, at the same time the buzzer has two short beeps every three seconds, thus you can start user enrollment.
- Press the same finger over the sensor three times or swipe a new ID card to the proximity area, if enrollment succeeds, the Green LED is normally on for one second, the buzzer has one long beep; If it fails, the Red LED is normally on for one second, the buzzer has one long beep. (Generally it is denied if the card or the finger has already been enrolled or each press of fingers are not qualified enough, please pay attention to place the finger in a right way)
- The system returns to enrollment state and waiting to swipe the card or press new finger (three times) to continue enrollment for the same user.
- Swipe the management card once again to quit enrollment state, the system returns to verification state.

Please do the same to enroll new users by following above steps.

Note: If there is no operation for 20 seconds in enrollment state or enrollment of 10 fingerprints and one ID card for the same user completed, the system automatically returns to verification state. Otherwise you have to swipe management card once to quit enrollment state.

13. Delete an Ordinary User

Swipe the management card by five times in a row to enter the single user deletion state. The Red LED blinks twice every three seconds, at the same time the buzzer has two short beeps every three seconds.

- Swipe the card near the proximity area or press the finger over the sensor. If verification succeeds, the Green LED is normally on for one second, the buzzer has one long beep, and it means deletion is successful. If verification fails, the Red LED is normally on for one second, the buzzer has one long beep, it means the user is not existed or each press of fingers are not qualified enough, please pay attention to place the finger in a right way).
- The system automatically returns to deletion state no matter verification is successful or failed. Swipe the management card once to quit deletion state, the system will return to verification state.

Please do the same to delete other users by following above steps.

Note: Once the registered card or one of the enrolled fingerprints is deleted, the associated user is completely deleted even he/she has enrolled more than one fingerprint.

14. Buzzer and LED Indicator

Operation succeeds: The green LED is normally on for one second, at the same time the buzzer has one long beep.

Operation failed: The red LED is normally on for one second, at the same time the buzzer has two short beeps.

Management Card Registration State: The green LED blinks once every three seconds, at the same time the buzzer has one long beep.

Enrollment State: The green LED blinks twice every three seconds, at the same time the buzzer has two short beeps every three seconds.

Deletion State: The red LED blinks twice every three seconds, at the same time the buzzer has two short beeps.

Verification State: The green LED blinks once every two seconds, the buzzer has no beep.