QUICK START GUIDE

2.4 Inch Finger Vein Terminal Time Attendance & Access Control

Version: 1.0
Date: Apr., 2017

Safety Precautions

The following precautions are to keep user safe and prevent any damage.
Please read carefully before installation.


Do not install the device in a place subject to direct sunlight, humidity, dust or soot.

Do not place a magnet near the product. Magnetic objects such as magnet, CRT, TV, monitor or speaker may damage the device.

Do not place the device next to heating equipment.

Be careful not to let liquid like water, drinks or chemicals leak inside the device.

Do not let children touch the device without supervision.

Do not drop or damage the device.

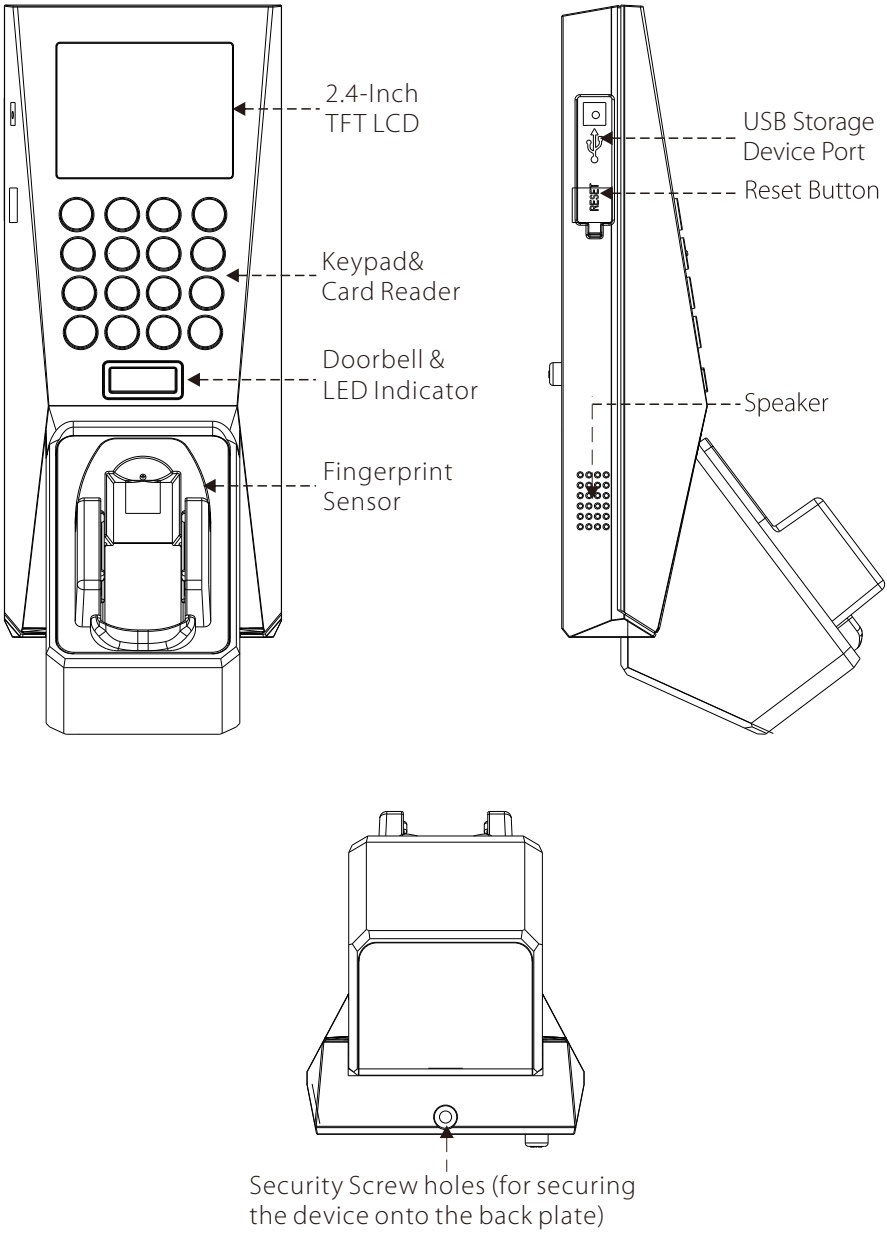
Do not disassemble, repair or alter the device.

Do not use the device for any purpose other than those specified.

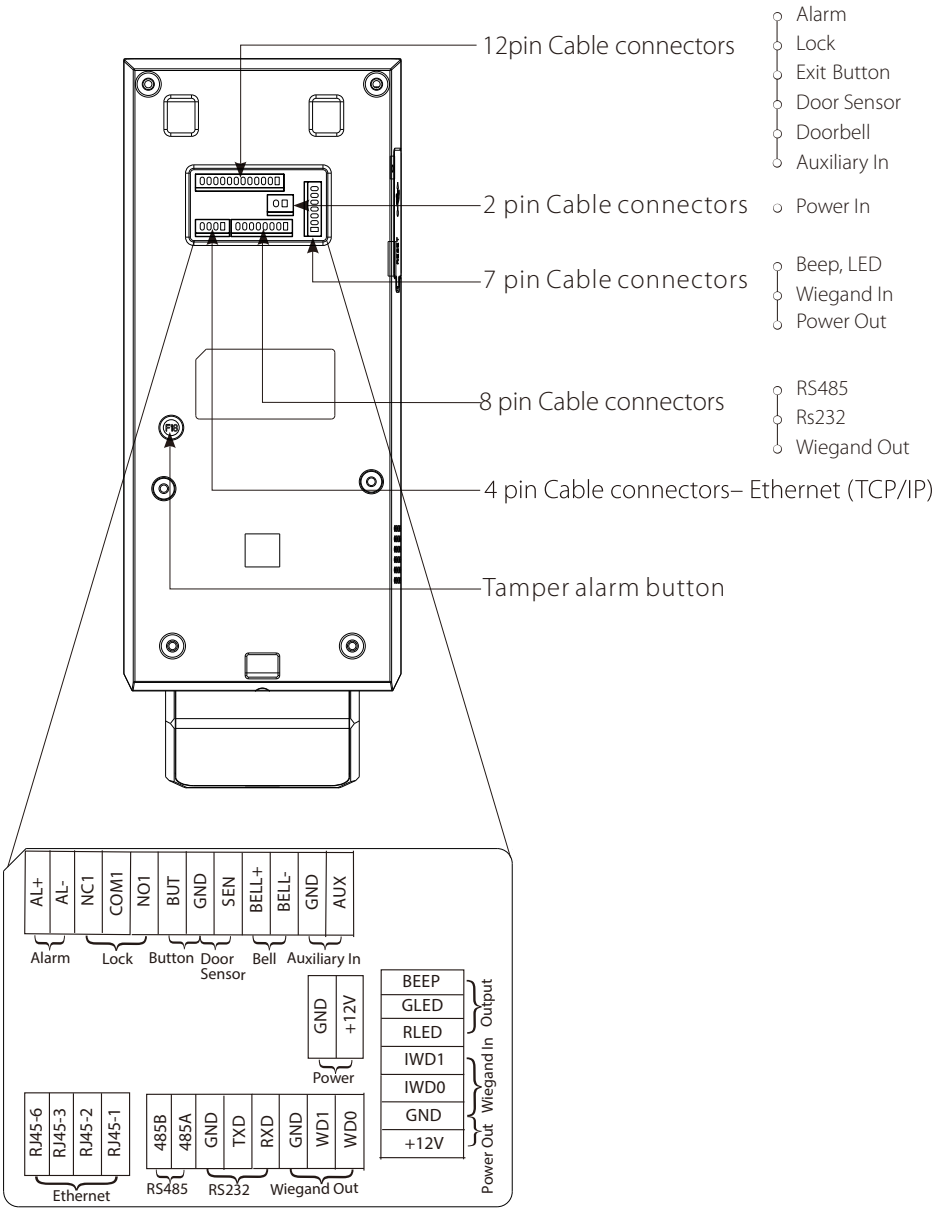
Clean the device often to remove dust on it. In cleaning, do not splash water on the device but wipe it out with smooth cloth or towel.

Contact your supplier in case of a problem.

Product PIN Diagram

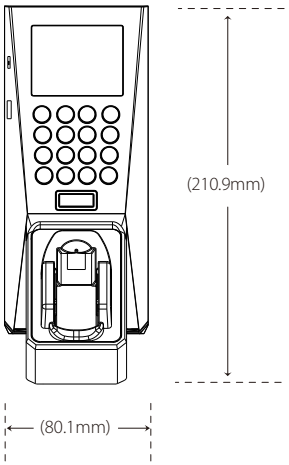


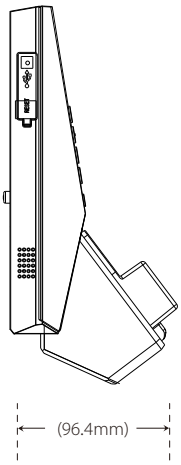
Product PIN Diagram



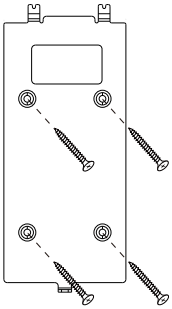
Product Dimensions & Installation

Product Dimensions



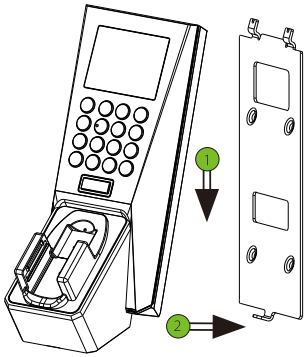


Mounting the device onto the wall

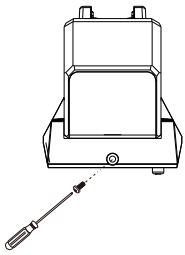


1 Fix the back plate onto the wall using wall mounting screws

Note: We recommend drilling the mounting plate screws into solid wood (i.e. stud/beam). If a stud/beam cannot be found, then use the supplied drywall plastic anchors.



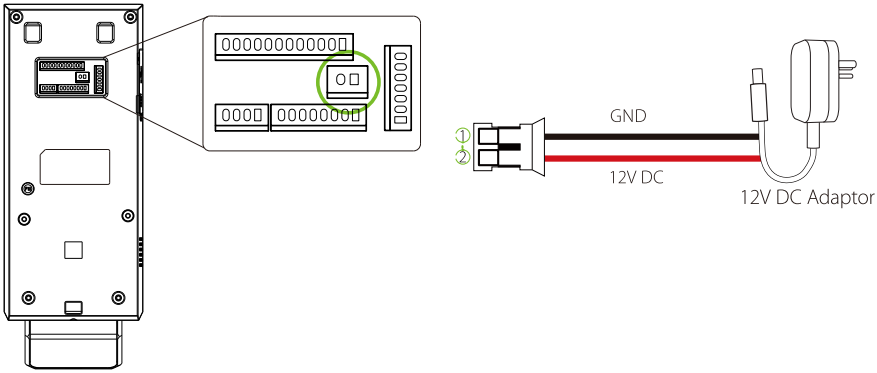
2 Inserting the device to backplate



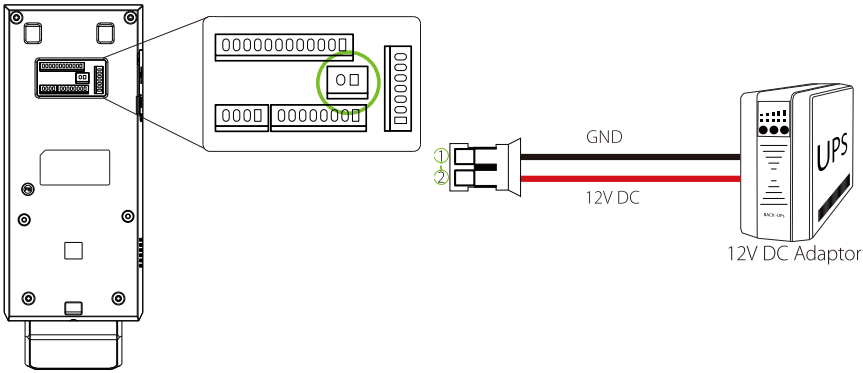
3 Use security screws to fasten the device to back plate

Power Connection

Without UPS



With UPS (Optional)

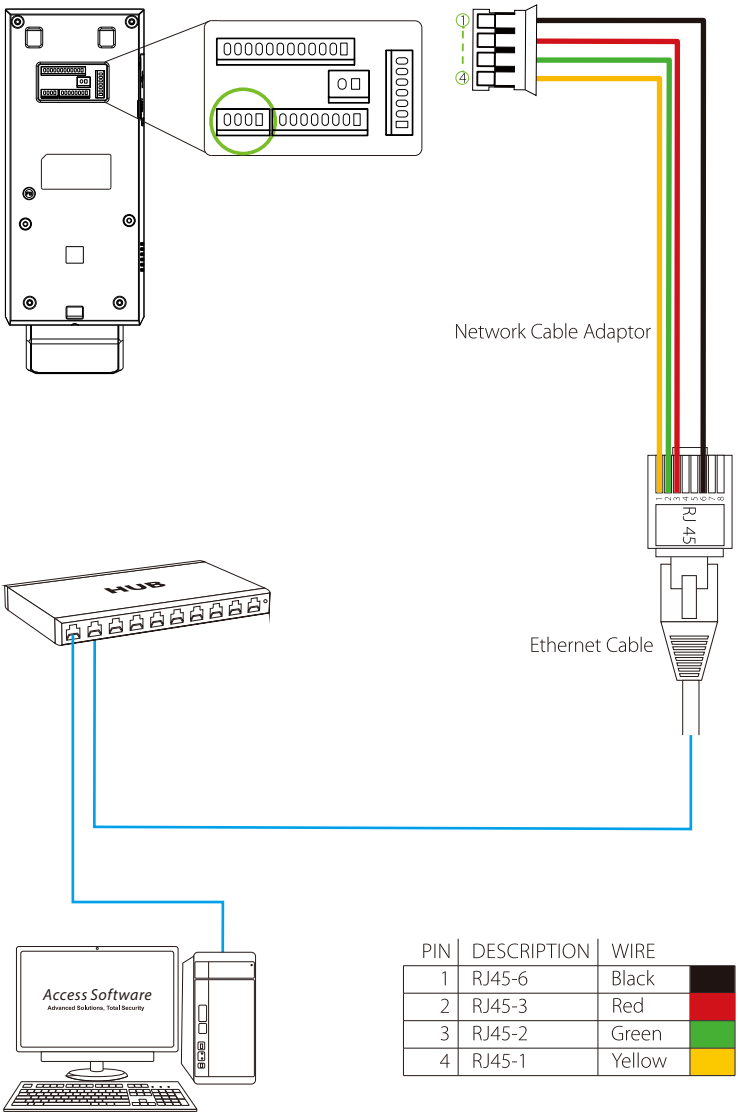


Recommended power supply

- 12V ± 10%, at least 500mA.
- To share the power with other devices, use a power supply with higher current ratings

Ethernet Connection

LAN Connection

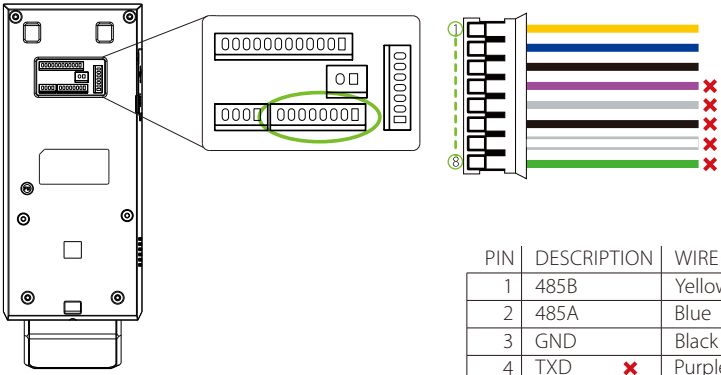


PIN	DESCRIPTION	WIRE
1	RJ45-6	Black
2	RJ45-3	Red
3	RJ45-2	Green
4	RJ45-1	Yellow

Note: The device can be connected to PC directly by ethernet cable.

RS485 Connection

PC Connection



PIN	DESCRIPTION	WIRE
1	485B	Yellow
2	485A	Blue
3	GND	Black
4	TXD ✖	Purple
5	RXD ✖	Gray
6	GND ✖	Black
7	WD1 ✖	White
8	WD0 ✖	Green

✖ Do not use

Important Notes:

1.RS485 communication wires should be a shielded and twisted pair of cable.

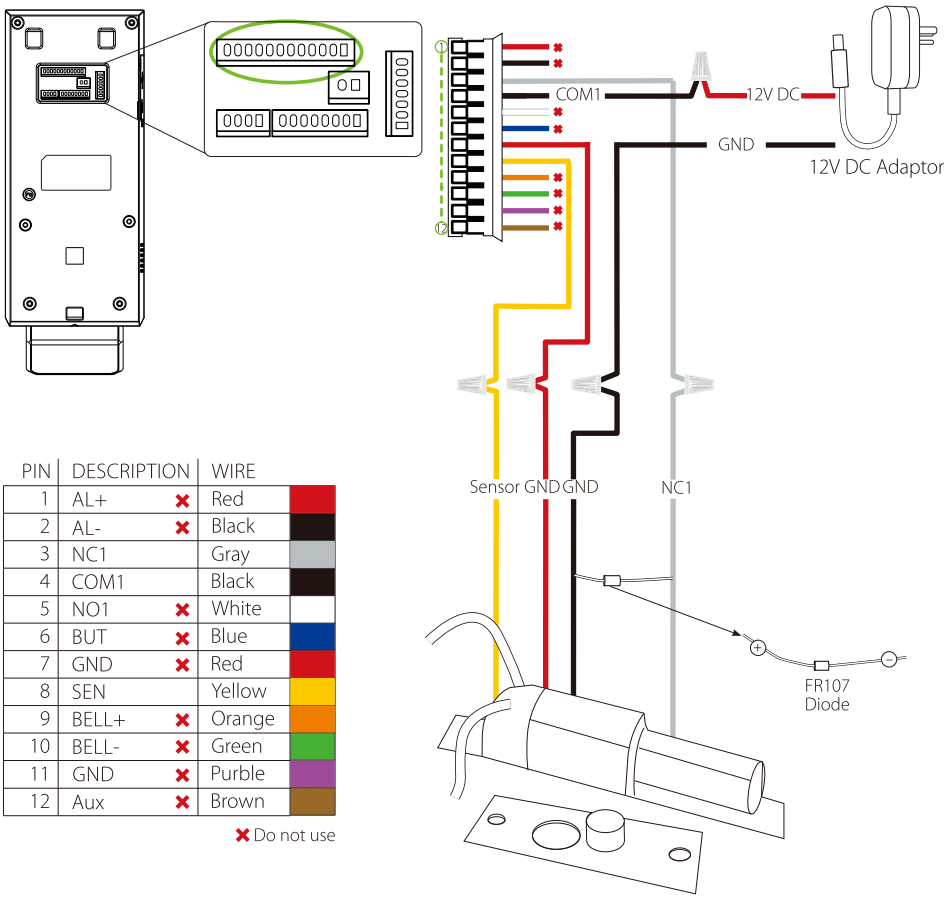
2.RS485 communication wires should be connected in a bus cascade instead of a star form, to achieve a better shielding effect by reducing signal reflection during communications.

3.Adjust the communication speed as needed. The signal quality varies with wiring conditions, and it may be necessary to lower the baud rates.

4.The GND signal may be omitted if and only if the GND potential difference is less than ±5V.

Lock Relay Connection

Device Does Not Share Power With The Lock



PIN	DESCRIPTION	WIRE
1	AL+ ✖	Red
2	AL- ✖	Black
3	NC1	Gray
4	COM1	Black
5	NO1 ✖	White
6	BUT ✖	Blue
7	GND ✖	Red
8	SEN	Yellow
9	BELL+ ✖	Orange
10	BELL- ✖	Green
11	GND ✖	Purble
12	Aux ✖	Brown

✖ Do not use

Normally Closed Lock

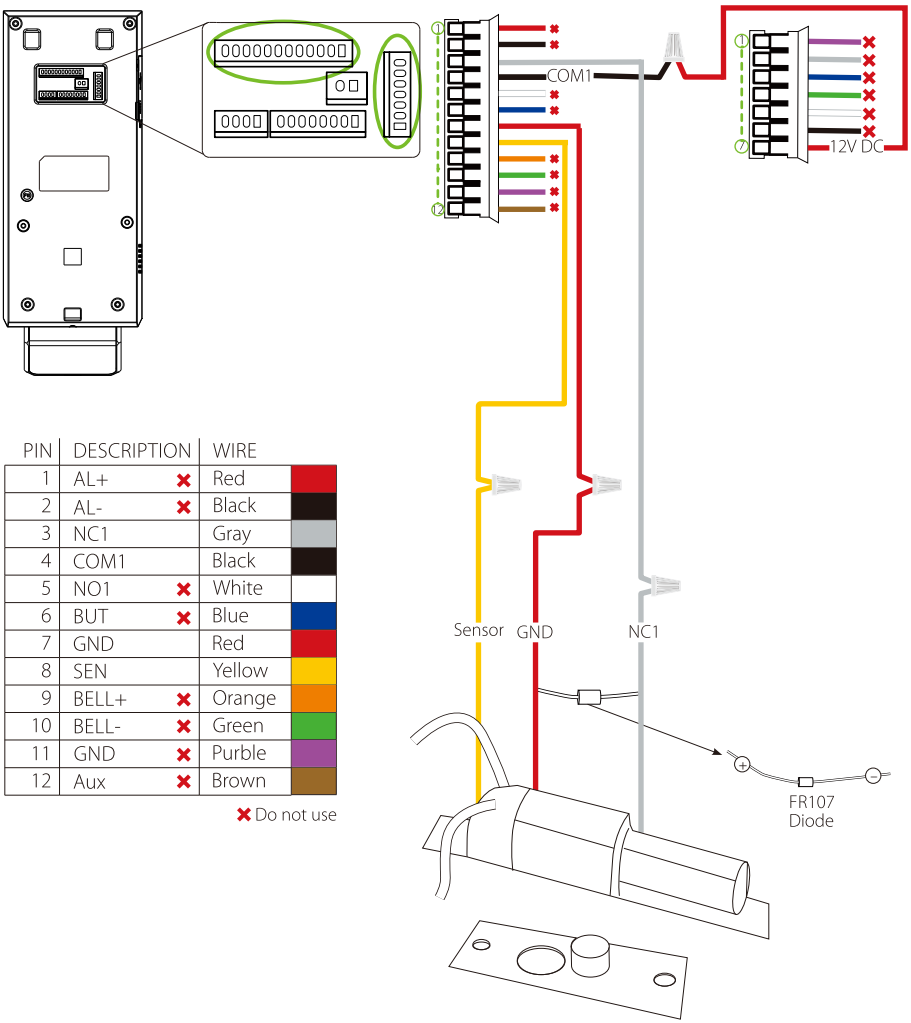
Notes:

1. The system supports **NO LOCK** and **NC LOCK**. For example the **NO LOCK** (normally opened at power on) is connected with '**NO1**' and '**COM1**' terminals, and the **NC LOCK** (normally closed at power on) is connected with '**NC1**'and '**COM1**' terminals.
2. When electrical lock is connected to the Access Control System, you must parallel one FR107 diode (equipped in the package) to prevent the self-inductance EMF affecting the system.

⚠ Do not reverse the polarities.

Lock Relay Connection

Device Shares Power With The Lock

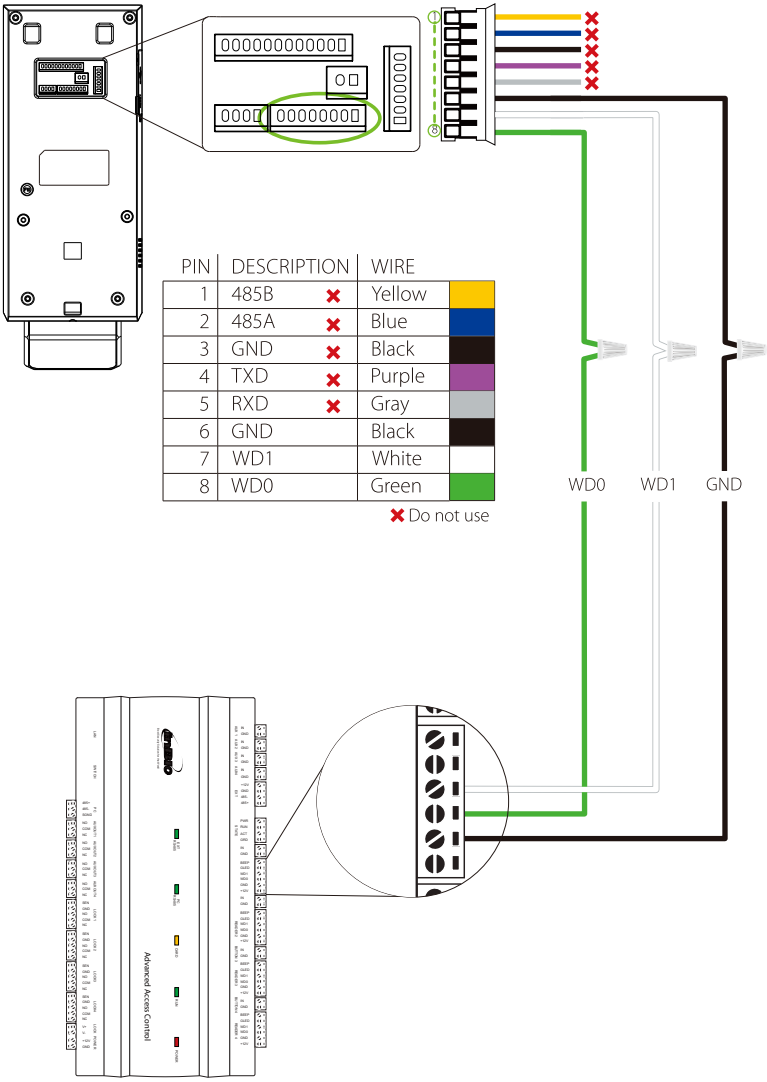


PIN	DESCRIPTION	WIRE
1	AL+ ✖	Red
2	AL- ✖	Black
3	NC1	Gray
4	COM1	Black
5	NO1 ✖	White
6	BUT ✖	Blue
7	GND	Red
8	SEN	Yellow
9	BELL+ ✖	Orange
10	BELL- ✖	Green
11	GND ✖	Purble
12	Aux ✖	Brown

✖ Do not use

Normally Closed Lock

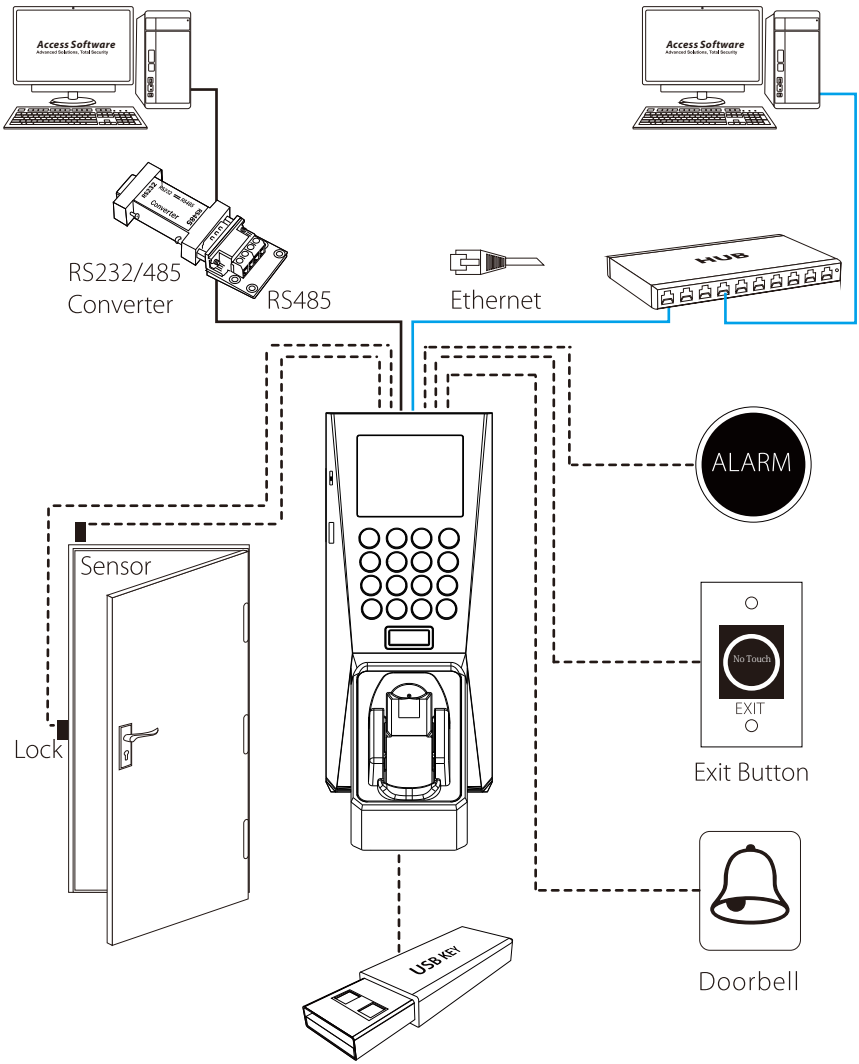
Wiegand Output Connection



PIN	DESCRIPTION	WIRE
1	485B ✖	Yellow
2	485A ✖	Blue
3	GND ✖	Black
4	TXD ✖	Purple
5	RXD ✖	Gray
6	GND	Black
7	WD1	White
8	WD0	Green

✖ Do not use

Standalone Installation



Device Operations

Date / Time Settings

Press M/OK > System > Date Time to enter Date Time setting interface.

Adding User

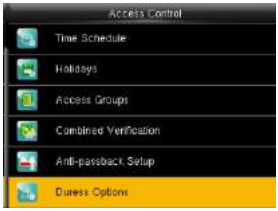
Press M/OK > User Mgt. > New User to enter the adding New User interface. Settings include inputting user ID , choosing user role (Super Admin / Normal User), registering finger vein / fingerprint / badge number / password, taking user photo, and setting access control role.
Adding a Super Admin: Select Super Admin in User Role to add a super admin.
Adding a Normal User: Select Normal User in User Role to add a normal user.

Ethernet Settings

Press M/OK > Comm. > Ethernet to enter the Ethernet setting interface.
The parameters below are the factory default values, please adjust them according to the actual network situation.
IP Address: 192.168.1.201
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
DNS: 0.0.0.0
TCP COMM. Port: 4370
DHCP: Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server. If DHCP is enabled, IP cannot be set manually.
Display in Status Bar: To set whether to display the network icon on the status bar.

Device Operations & Troubleshooting

Access Control Settings



Press M/OK > Access Control to enter the Access Control setting interface.
To gain access, the registered user must meet the following conditions:
1. User's access time falls within either user's personal time zone or group time zone.
2. User's group must be in the access combo (when there are other groups in the same access combo, verifications of members of those groups are also required to unlock the door)

Access Control Options: To set parameters of the lock and other related devices.
Time Schedule: The smallest unit for access control.
Holidays: To set dates of holiday and the access control time zone for that holiday.
Access Groups: To divide and manage users in groups. Group members can either use the default group time zone or customize a personal time zone.
Combined Verification: Combinations of verification methods
Anti-passback Setup: To avoid unverified individuals from following the registered users to enter the door.
Duress Options: If users unlock the door under threat, the device will open the door, meanwhile send signals to the backstage to trigger the alarm.

Troubleshooting

1. Fingerprint cannot be read or it takes too long.

- Check whether a finger or fingerprint sensor is stained with sweat, water, or dust.
- Retry after wiping off finger and fingerprint sensor with dry paper tissue or a mildly wet cloth.
- If a fingerprint is too dry, blow on the finger and retry.

2. Fingerprint is verified but authorization keeps failing.

- Check whether the user is restricted by group or time zone.
- Check with administrator whether the enrolled fingerprint has been deleted from the device for some reasons.

3. Verification succeeds but door does not open.

- Check whether the lock open duration is set to appropriate time, which opens the lock.
- Check whether anti-passback mode is in use. In anti-passback mode, only the person who has entered through that door can exit.

4. The device displays “system broken“ and the alarm is ringing.

- Check whether the device and back plate are securely connected to each other. If not, a tamper switch will be activated which triggers the alarm and keeps it rinng.