QUICK START GUIDE

Applicable Models: ProCapture-WP

Version: 1.0

Date: July, 2017

Safety Precautions

Before installation, please read the following safety precautions for user safety and to prevent product damage.

Do not install the device in a place subject to direct sun light, 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.

Do 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.

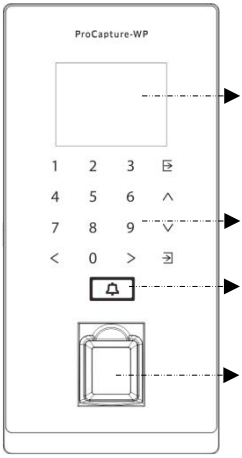
Do not use the device for any purpose other than those specified.

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!

Device Overview

Front



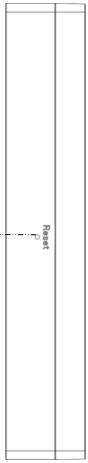
2.4-Inch Color Screen

Touch Keypad

Doorbell & LED Indicator

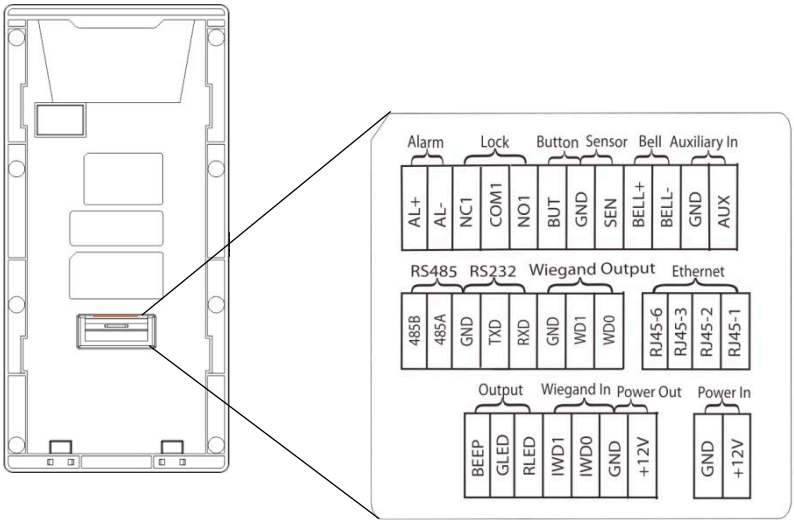
Fingerprint Sensor & Card Reader Area

Left Side



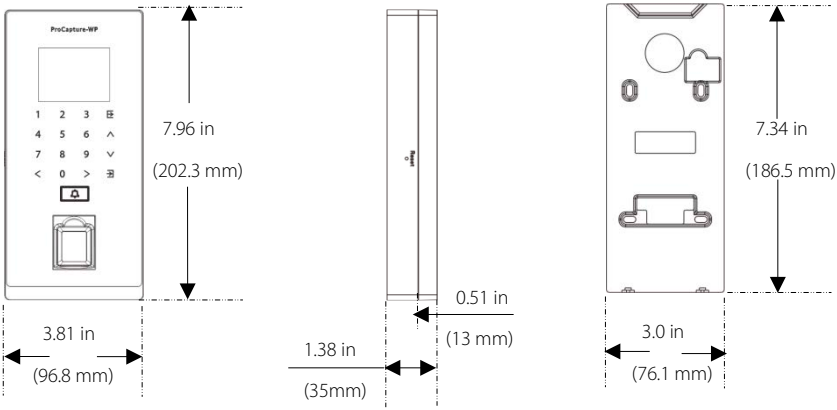
Reset Button

Back

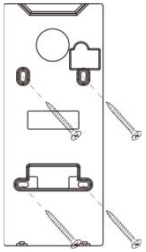


Product Dimensions & Installation

❖ Product Dimensions

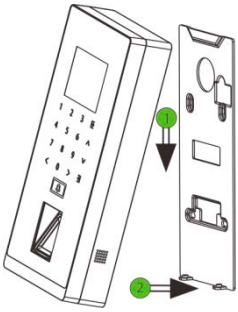


❖ Mounting the Device on Wall

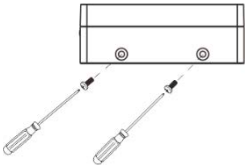


1 Fix the back plate onto the wall using wall mounting screws.

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



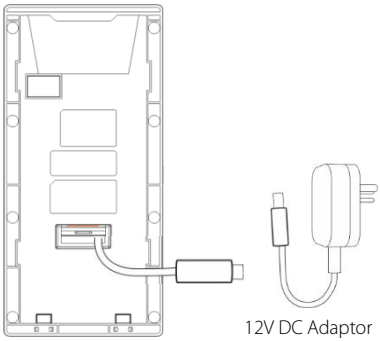
2 Insert the device to back plate.



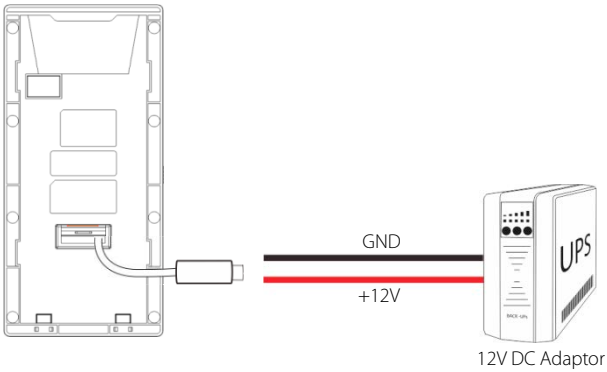
3 Use security screws to fasten the device to back plate.

Power Connection

❖ Without UPS



❖ With UPS (Optional)

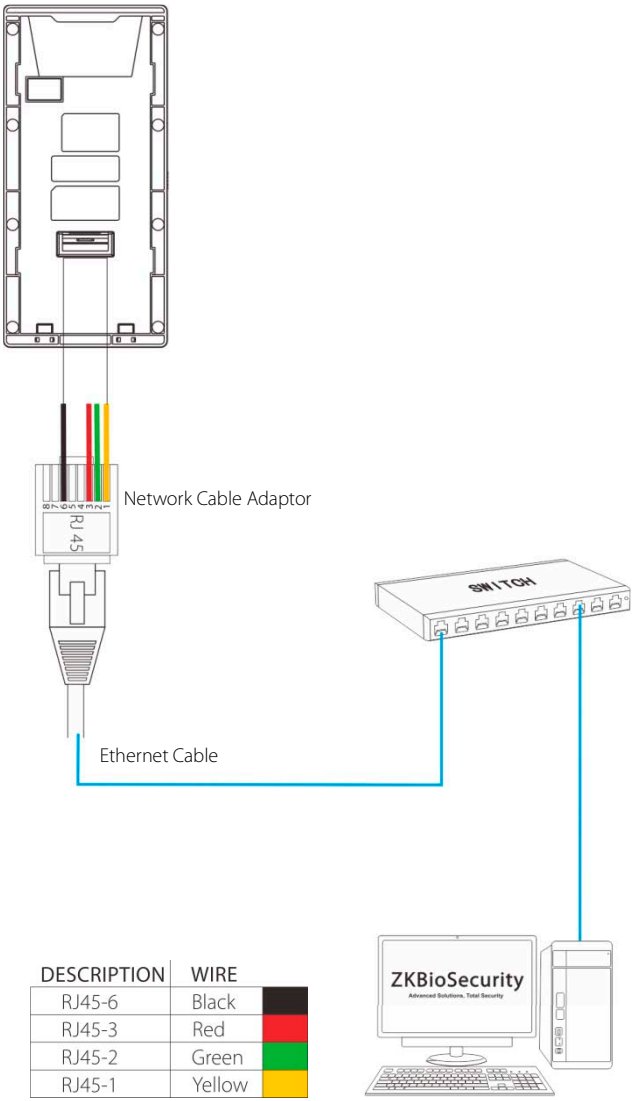


❖ Recommended Power Supply

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

Ethernet Connection

❖ LAN Connection



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

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

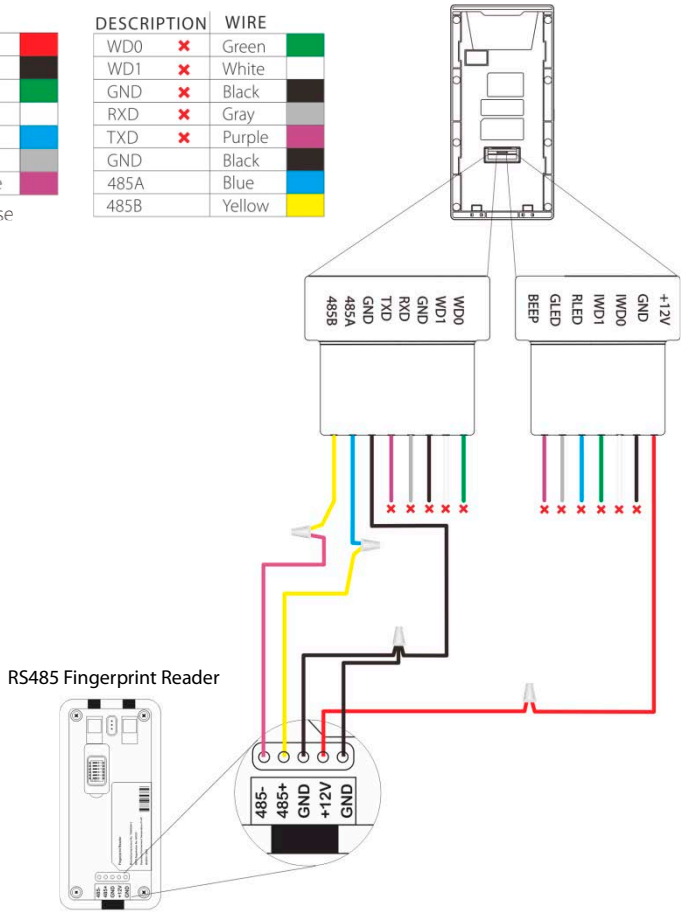
RS485 Connection

❖ RS485 Fingerprint Reader Connection

DESCRIPTION		WIRE
+12V		Red
GND	✖	Black
IWD0	✖	Green
IWD1	✖	White
RLED	✖	Blue
GLED	✖	Gray
BEEP	✖	Purple

✖ Do not use

DESCRIPTION		WIRE
WD0	✖	Green
WD1	✖	White
GND	✖	Black
RXD	✖	Gray
TXD	✖	Purple
GND		Black
485A		Blue
485B		Yellow



❖ DIP Settings

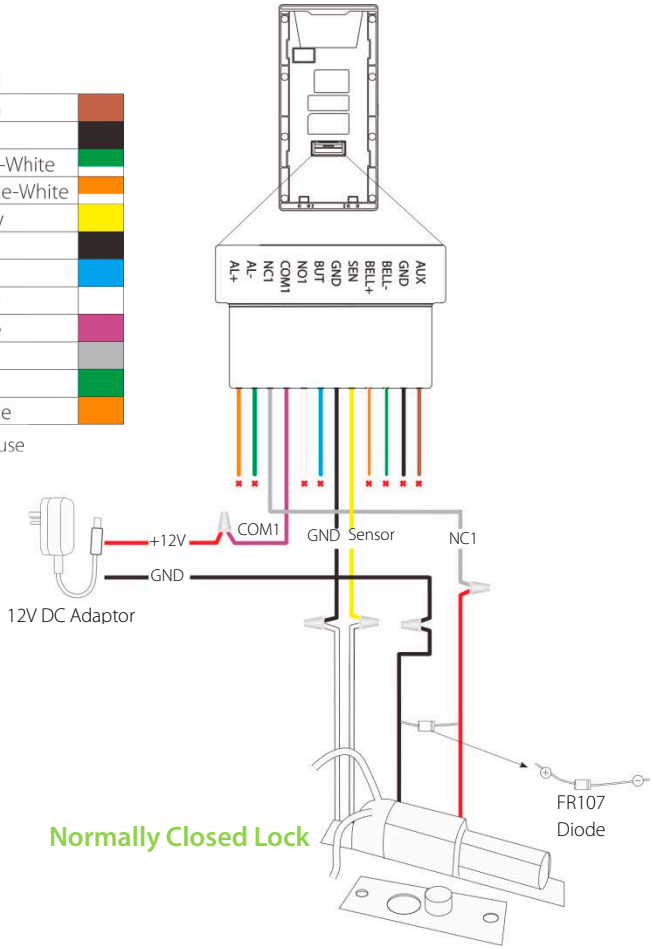
1. There are six DIP switches on the back of RS485 fingerprint reader, switches 1-4 are for RS485 address, switch 5 is reserved, switch 6 is for reducing noise on long RS485 cable.
2. If RS485 fingerprint reader is powered from the terminal, the length of wire should be less than 100 meters or 330 ft.
3. If the cable length is more than 200 meters or 600 ft., the number 6 switch should be ON as below.

Lock Relay Connection

❖ Device Not Sharing Power with the Lock

DESCRIPTION		WIRE
AUX	✖	Brown
GND	✖	Black
BELL-	✖	Green-White
BELL+	✖	Orange-White
SEN		Yellow
GND		Black
BUT	✖	Blue
NO1	✖	White
COM1		Purple
NC1		Gray
AL-	✖	Green
AL+	✖	Orange

✖ Do not use



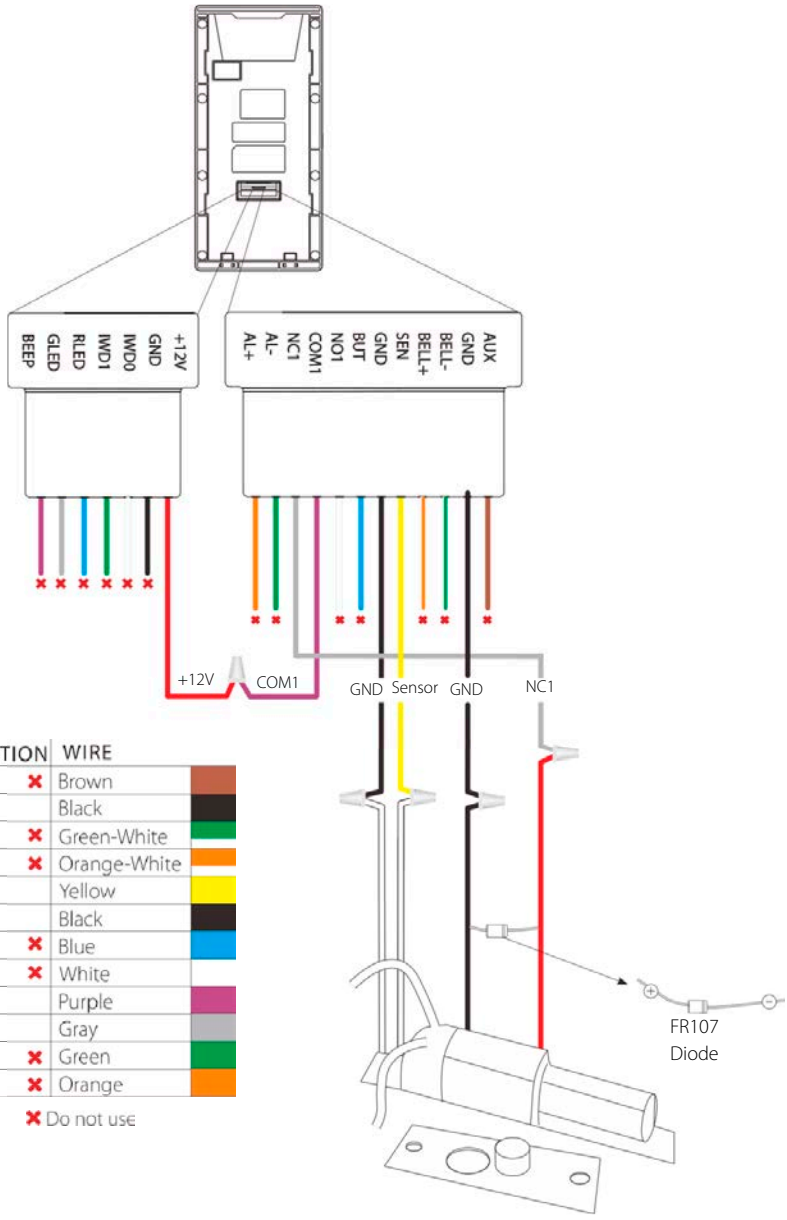
Notes:

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 from affecting the system.

   ⚠Do not reverse the polarities.

Lock Relay Connection

❖ Device Sharing Power with the Lock



DESCRIPTION		WIRE
AUX	✖	Brown
GND		Black
BELL-	✖	Green-White
BELL+	✖	Orange-White
SEN		Yellow
GND		Black
BUT	✖	Blue
NO1	✖	White
COM1		Purple
NC1		Gray
AL-	✖	Green
AL+	✖	Orange

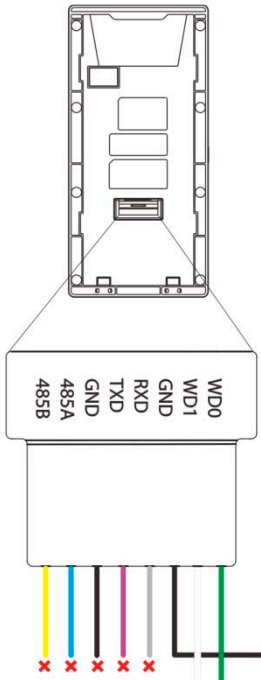
✖ Do not use

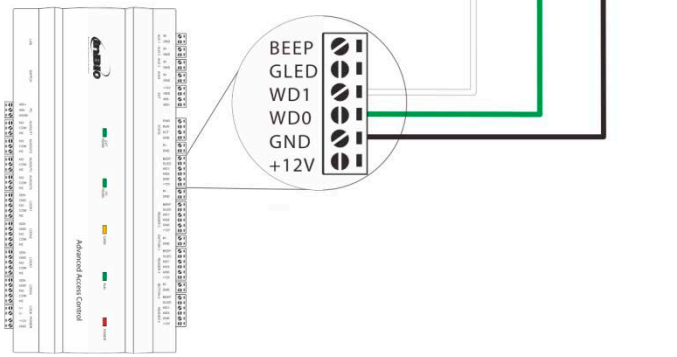
Normally Closed Lock

Wiegand Output Connection

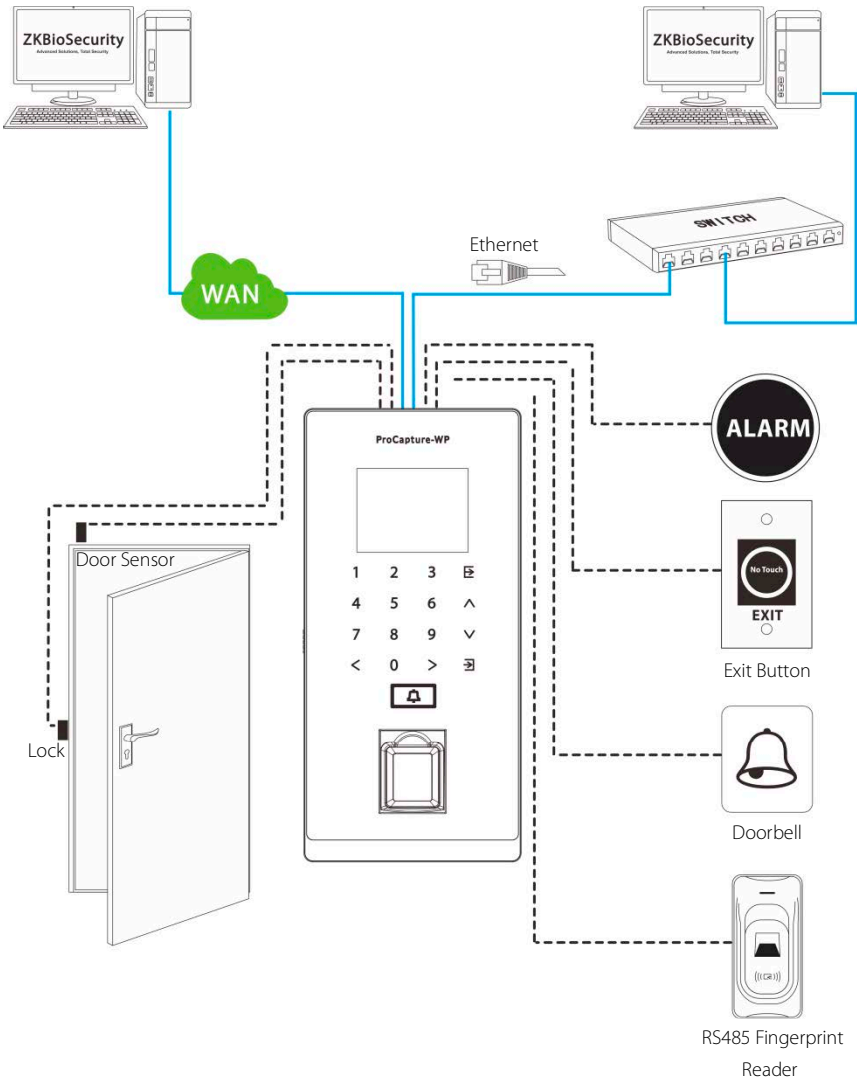
DESCRIPTION		WIRE
WD0		Green
WD1		White
GND		Black
RXD	✖	Gray
TXD	✖	Purple
GND	✖	Black
485A	✖	Blue
485B	✖	Yellow

✖ Do not use





Standalone Installation



Device Operation

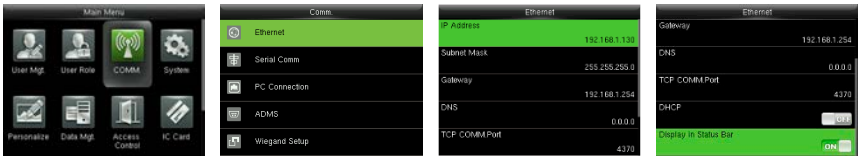
❖ Date / Time Settings

Press [M] to enter the main menu and press > to select System > Date Time to set date and time.

❖ Adding User

Press [M] to enter the main menu and select User Mgt. > New User to enter the adding New User interface. Settings include inputting user ID, choosing user role (Super Admin / Normal User), registering fingerprint / badge number / password and setting access control role.

❖ Ethernet Settings



Press [M] to enter the main menu and press > to select Comm. > Ethernet.

The Parameters below are the factory default values. Please adjust them according to the actual network.

IP Address: 192.168.1.201

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

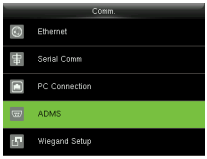
DNS: 0.0.0.0

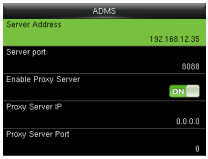
TCP COMM. Port: 4370

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 connection icon , on the status bar of initial interface.

❖ ADMS Settings





Press ⏎ to enter the main menu and press > to select Comm. > ADMS, to set the parameters which are used for connecting with the ADMS server.

When the Webserver is connected successfully, the initial interface will display the logo.

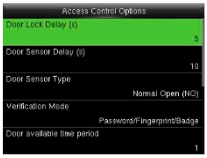
Server Address: Enter IP address of ADMS server (namely, IP address of server where software is installed).

Server Port: Enter Port number used by the ADMS server.

Enable Proxy Server: Method of enabling proxy. To enable proxy, please set the IP address and port number of the proxy server. Entering proxy IP and server address will be the same.

Note: To connect the device to ZKBioSecurity software, Ethernet and ADMS options must be set correctly.

❖ Access Control Settings



Press ⏎ to enter the main menu and press > and ∨ to select Access Control.

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, verification 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 Rule Setting: To set a maximum of 50 time rules. Each time rule consists of 10 spaces (7 spaces for one week and 3 holiday spaces), each space consists of 3 time periods.

Holidays: To set dates of holiday and the access control time zone for that holiday.

Combined Verification: To set access control combinations. A combination consists of a maximum of 5 access control groups.

Anti-Passback Setup: To prevent passing back which causes risks to security. Once it is enabled, entry and exit records must be matched in order to open door. In Anti-Passback, Out Anti-Passback and In / Out Anti-Passback functions are available.

➢ Access Control Combination Settings

E.g.: Add an access control combination which requires 2 persons' verification from both group 1 (set in User Management) and group 2.

1. In "Access Control" interface, press ∨ to select "Combined Verification"; then press → to enter the "Combined Verification" list. Click the desired combination and press → to enter the modification interface (shown as in figure 2).
2. Click ∧ or ∨ to change the number, click < or > to switch editing box, set the user group number, and click → to save and return to "Combined Verification" list (as shown in figure 3).

Note: 1. A single Access Control Combination can consist of a maximum of 5 user groups (in order to open door, verification of all 5 users is required).

2. If the combination is set as shown in figure 4, a user from access group 2 must obtain verification of two users from access group 1 in order to open door.

3. Set all group number to zero to reset access control combination.

❖ 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. "Invalid time zone" is displayed after verification?

- Contact Administrator to check if the user has the privilege to gain access within that time zone.

3. Verification succeeds but the user cannot gain access?

- Check whether the user privilege is set correctly.
- Check whether the lock wiring is correct.
- 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 Tamper Alarm rings?

- To cancel the triggered alarm mode, carefully check whether the device and back plate are securely connected to each other, and reinstall the device properly if necessary.