

QUICK START GUIDE

ProFAC

Version: 1.2

Date: September 2021



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.

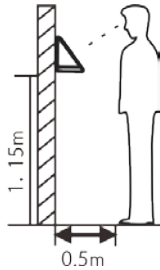


Clean the device often to remove dust on it. In cleaning, do not splash water on the device but wipe it out with smooth cloth or towel.

Contact your supplier in case of a problem!

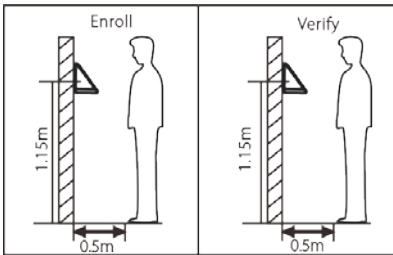
Cautions on Using Face Recognition Device

1) Recommended Standing Position



For user heights between 1.5m to 1.8m, it is recommended to install the device at 1.15m above ground (may be modified according to user average height).

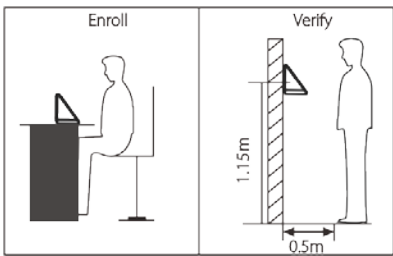
a. Recommended Registration and Verification Position



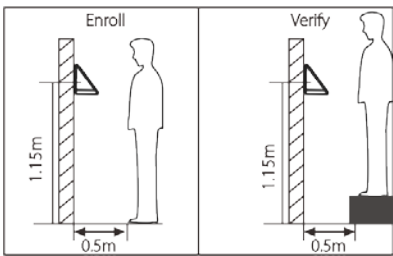
Recommended Procedures (as shown in the left image):

During registration and verification procedures, the position of device should not be changed to prevent deduction in verification preciseness. If it is necessary to move the device, its vertical height should not be changed.

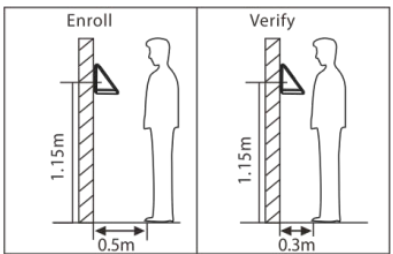
b. Factors Affecting the Preciseness of Verification



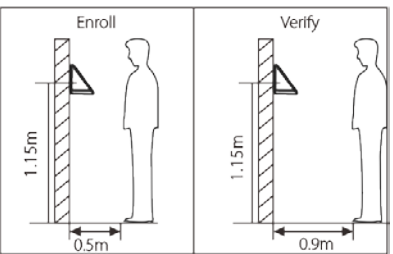
Non-identical registration and verification gestures



Non-identical registration and verification heights



Non-identical registration and verification distances from device



Non-identical registration and verification distances from device

2) Registration

- During registration, it is required to adjust your upper body to fit your eyes into the green frame on the screen.
- During verification, it is required to show your face in the center of the screen and fit your face into the green frame in the screen.

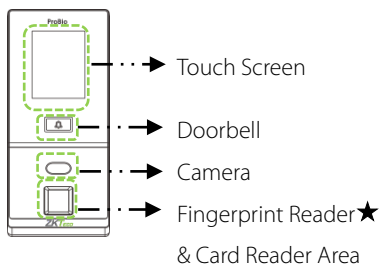


Device Overview

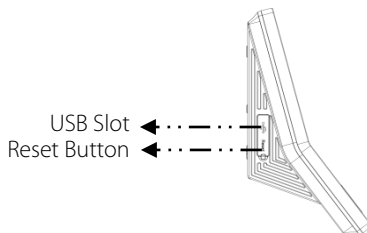
★Not all products have fingerprint or card function, the real product shall prevail.

❖ ProBio

Front

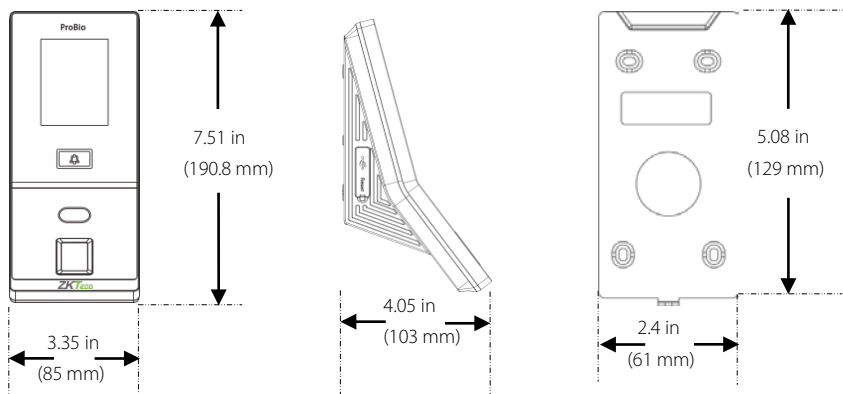


Left Side



Product Dimensions & Installation

❖ Product Dimensions



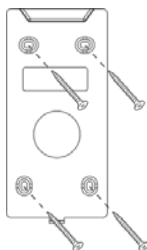
❖ Mounting the Device on Wall

1



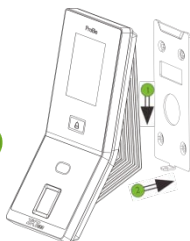
Put the mounting template sticker onto the wall, and drill holes according to the mounting paper.

2



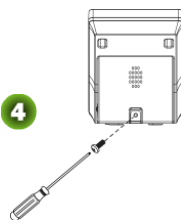
Fix the back plate onto the wall using wall mounting screws.

3



Insert the device into back plate.

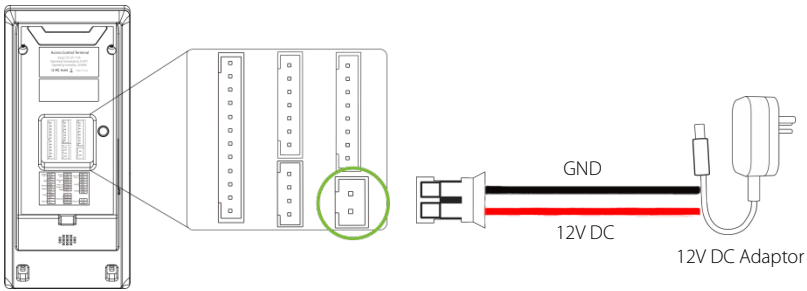
4



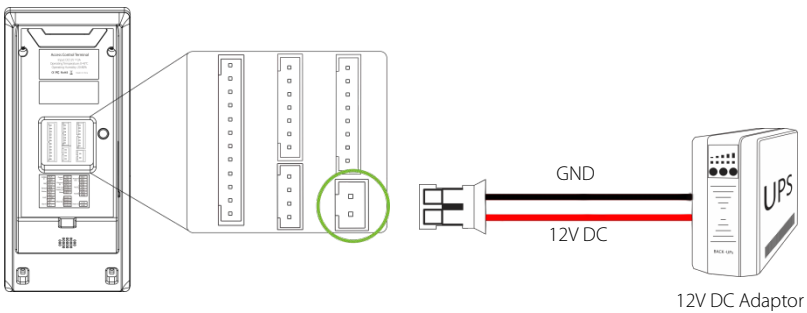
Use security screws to fasten the device to back plate.

Power Connection

❖ Without UPS



❖ With UPS (Optional)

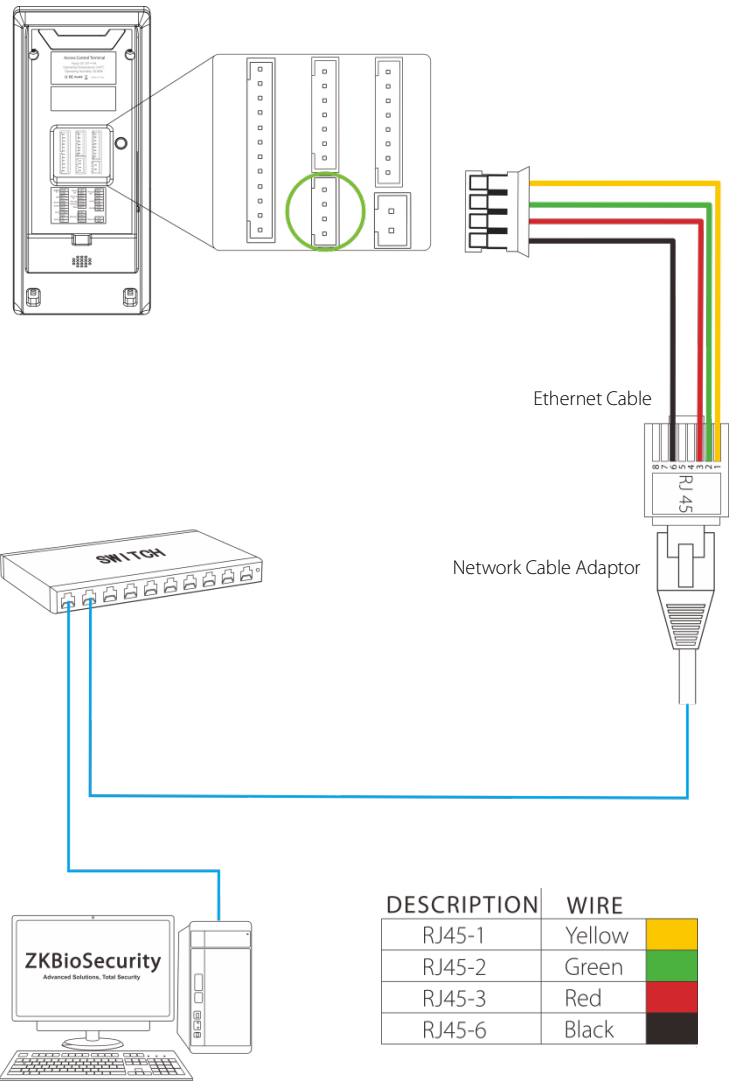


❖ Recommended Power Supply

- 12V±10%, at least 500mA (12V /3A is standard).
- To share the power with other devices, use a power supply with higher current ratings.

Ethernet Connection

❖ LAN Connection



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

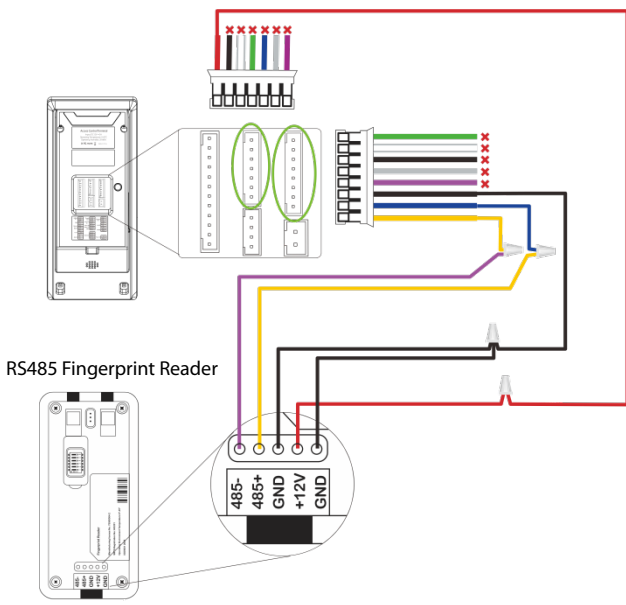
RS485 Connection

❖ RS485 Fingerprint Reader Connection

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

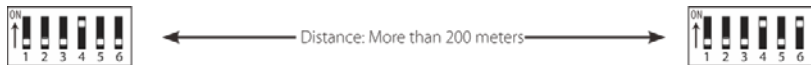
DESCRIPTION	WIRE
WD0	Green
WD1	White
GND	Black
RXD	Gray
TXD	Purple
GND	Black
485A	Blue
485B	Yellow

✗ Do not use



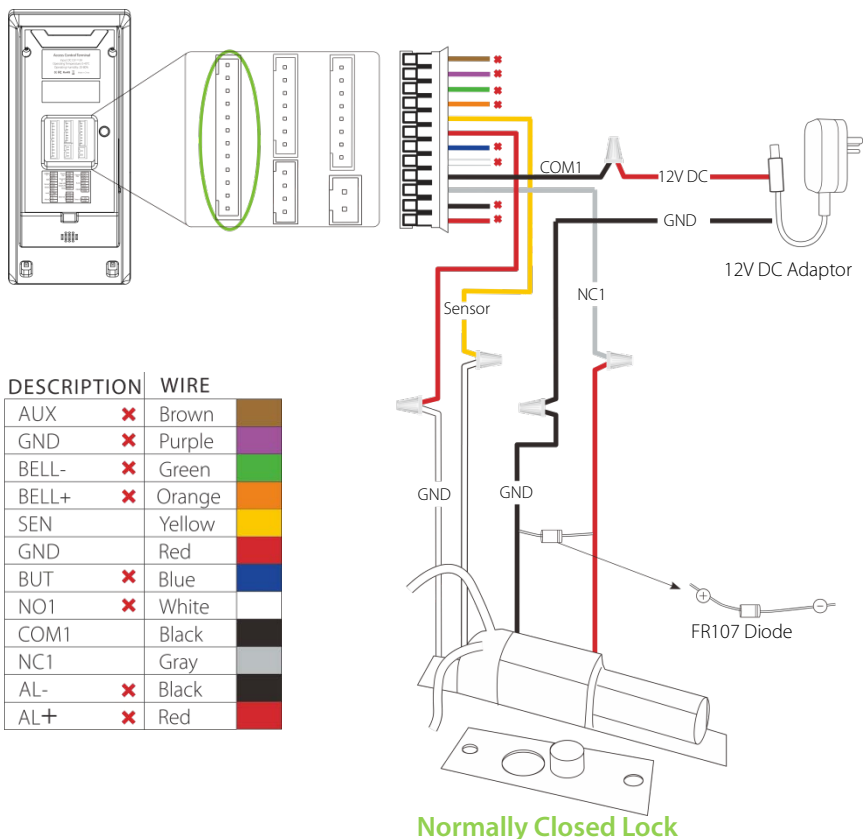
❖ DIP Settings

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



Notes:

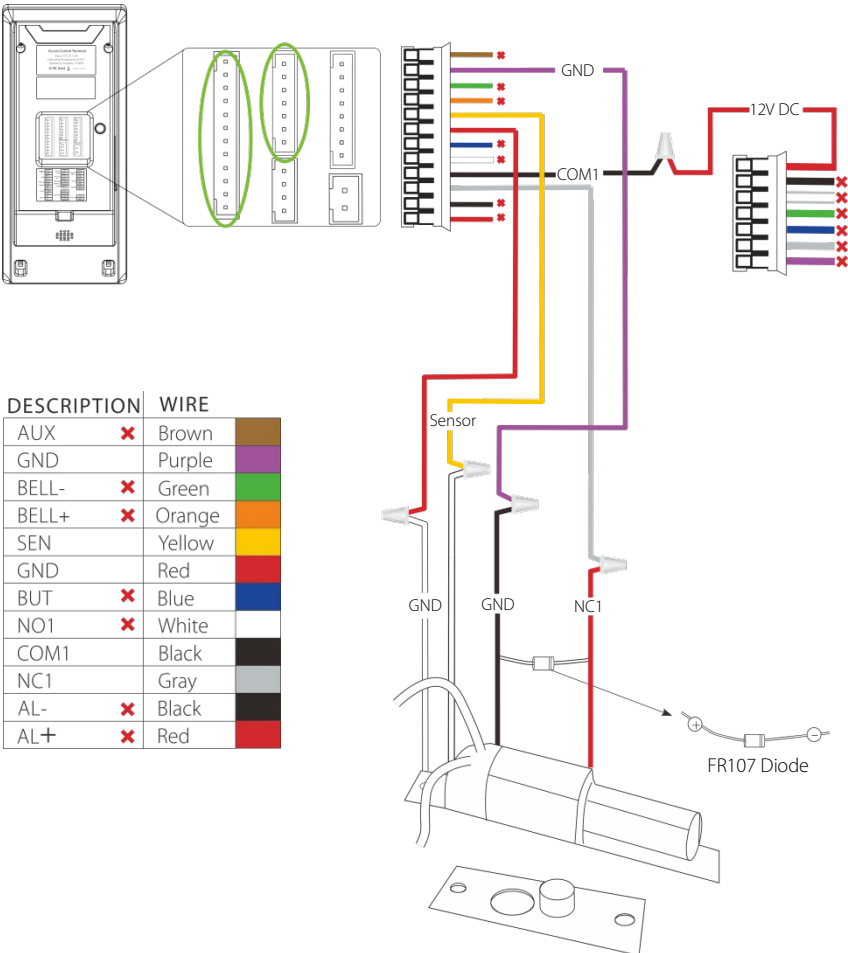
1. The system supports **NO LOCK** and **NC LOCK**. For example the **NO LOCK** (normally opened at power on) is connected with 'NO1' and 'COM1' terminals, and the **NC LOCK** (normally closed at power on) is connected with 'NC1' and 'COM1' terminals.
2. When electrical lock is connected to the Access 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.

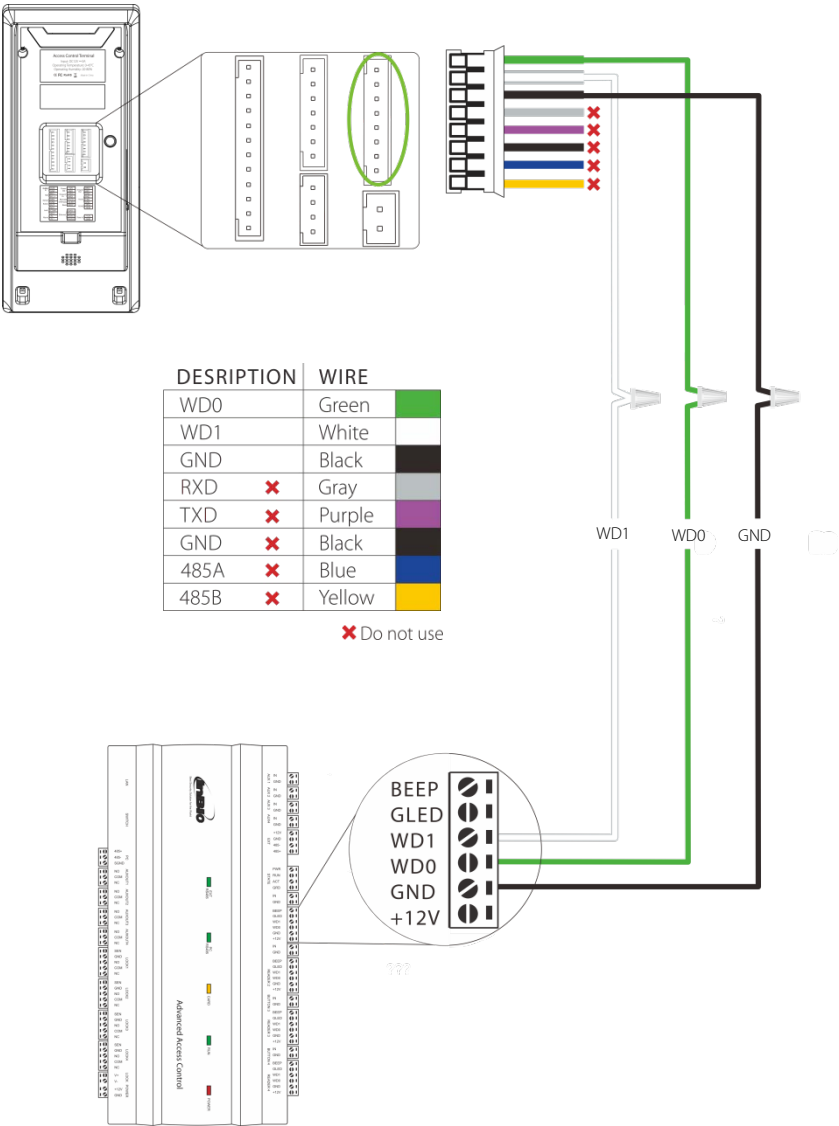
Lock Relay Connection

❖ Device Sharing Power with the Lock

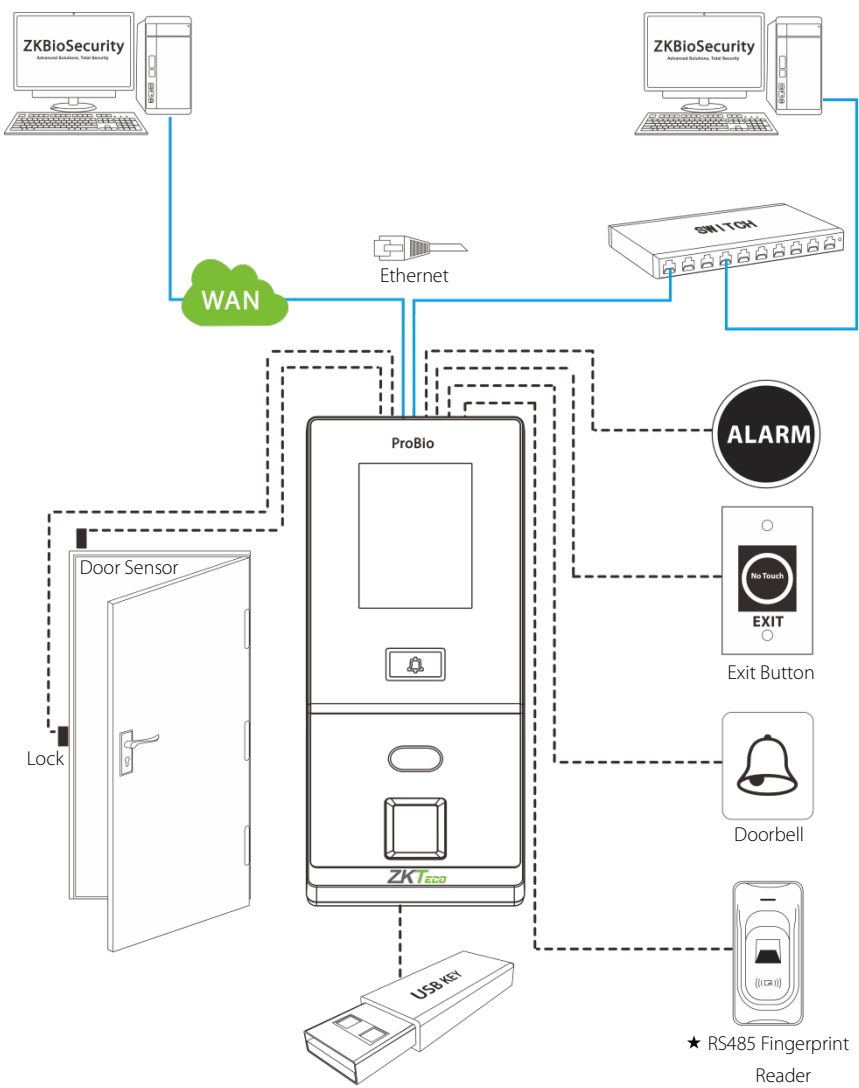


Normally Closed Lock

Wiegand Output Connection

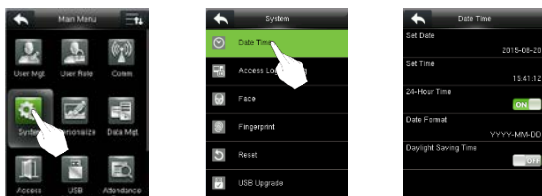



Standalone Installation



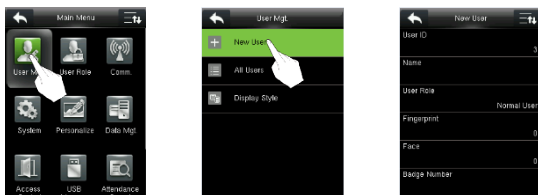
Device Operation


❖ Date / Time Settings



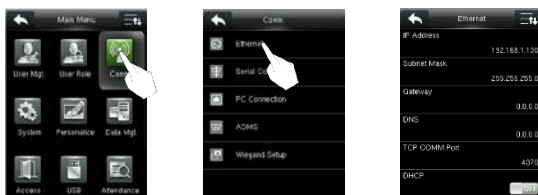
Press  icon to enter the main menu > System > Date Time to set date and time.

❖ Adding User



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

❖ Ethernet Settings



Press  icon to enter the main menu > 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 icon  on the status bar.

Device Operation

❖ ADMS Settings



Press  icon to enter the main menu > 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 .

Enable Domain Name: When this function is turned on, the domain name mode "http://..." will be used, such as <http://www.XXX.com>. XXX denotes the domain name when this mode is on; when this mode is off, enter the IP address format in XXX.

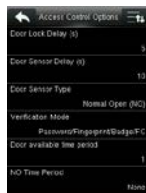
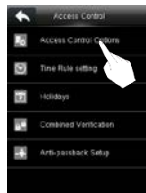
Server Address: IP address of the ADMS server.


Server Port: Port 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  icon to enter the main menu, press Access Control to enter 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, 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.

Device Operation

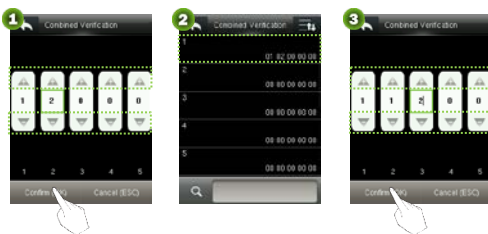
Holidays: To set dates of holiday and the access control time zone for that holiday.

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 this function 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 Access Control Group 1 (set in User Management) and Access Control Group 2.



1. In "Combined Verification" list, click the desired combination to modify, and enter the interface (as shown in figure 1).
2. Click "+" or "-" to set the user access control group no., and then click "Confirm" to save and return to "Combined Verification".

Note:

1. A single access control combination can consist of a maximum of 5 access control groups (in order to open door, verification of all 5 users is required).
2. If the combination is set as shown in figure 3, a user from access control group 2 must obtain verification of 2 users from access control group 1 in order to open door.
3. Set all access control group number to zero to reset access control combination.

❖ Troubleshooting

Q: "Invalid Time Period" is displayed after verification?

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

Q: Verification succeeds but the user cannot gain access?

A: Check whether the lock wiring is correct.

Q: The Tamper Alarm rings?

A: 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.