

USER MANUAL

Applicable Models:

InBio160/260/460 Pro Access Control Panel

Version: 1.1

Important Statement

Thank you for choosing our product. Before use, please read this manual carefully to avoid damage to the device. We remind you that through proper use, you may experience good effect and verification speed.

No part of this document can be extracted, copied or transmitted by any means without prior written consent of our company.

The products described in this manual may contain software belonging to our company or licensors possessing copyright. Unless permitted by obligees, no one can copy, distribute, modify, extract, decompile, disassemble, decode, reverse engineer, rent, transfer, sub-license such software in any form or conduct other behaviors infringing software copyright, exclusive of cases with prohibition of such limitation by applicable laws.



Due to product update, our company does not promise the consistency of the manual with actual products, and not assume responsibilities for any dispute arising from the discrepancy between actual technical parameters and this manual. The manual is subject to change without prior notification.

About This Manual

- This manual introduces the operation of user interfaces and menu functions of Applicable Models: InBio160/260/460 Pro Access Control Panel. For the installation, Please refer to Applicable Models: InBio Pro Series Access Control Panels Installation Guide.
- Not all the devices have the function with★, the real product prevails.
- The pictures in this manual may not be exactly consistent with those of your purchased product; the actual product's display shall prevail.

Table of Contents

1 SAFETY INSTRUCTIONS	1
1.1 IMPORTANT SECURITY INSTRUCTIONS	1
1.2 INSTALLATION INSTRUCTIONS	2
2 SYSTEM INTRODUCTION	4
2.1 SYSTEM FUNCTIONAL PARAMETERS	4
2.2 PRODUCT TECHNICAL PARAMETERS	4
2.3 CONTROL PANEL INDICATORS	5
3 INSTALLATION AND CONNECTION	6
3.1 INSTALLATION PROCEDURE	6
3.2 INSTALLATION OF ACCESS CONTROL PANEL WIRES	7
3.3 CONTROL PANEL SYSTEM INSTALLATION	8
3.4 CONTROL PANEL CONNECTION TERMINALS	9
3.5 CONNECTION WITH DOOR SENSORS, EXIT SWITCHES, AUXILIARY INPUT DEVICES, AND PC485 EXTENSION COMMUNICATION	12
3.6 CONNECTION WITH READERS	15
3.7 RELAY OUTPUT CONNECTION	18
3.8 ACCESS CONTROL OPERATOR PANEL SYSTEM POWER SUPPLY STRUCTURE	20
4 EQUIPMENT COMMUNICATION	21
4.1 ACCESS CONTROL NETWORKING WIRES AND WIRING	21
4.2 TCP/IP COMMUNICATION	22
4.3 DIP SWITCH SETTINGS	22
4.4 ZKPANELWEB	23
4.5 CONNECT TO ZKBIOSECURITY SOFTWARE	30
4.6.1 ADD DEVICE ON THE SOFTWARE	30
4.6.2 MOBILE CREDENTIAL	31
5 PRIVACY POLICY	34
6 ECO-FRIENDLY OPERATION	36

1 Safety Instructions

1.1 Important Security Instructions

1. Read and follow the instructions carefully before operation. Please keep the instructions for future reference.
2. Accessories: Please use the accessories recommended by the manufacturer or delivered with the product. Other accessories are not recommended, including major alarming systems and monitoring systems. The primary alarming and monitoring system should comply with the local applicable fire-prevention and security standards.
3. Installation cautions: Do not place this equipment on an unstable table, tripod mount, support, or base, lest the equipment falls and get damaged or any other undesirable outcome resulting in severe personal injuries. Therefore, it is essential to install the equipment as instructed by the manufacturer.
4. All peripheral devices must be grounded.
5. No external connection wires can be exposed. All the connections and idle wire ends must be wrapped with insulating tapes to prevent any damage to the equipment by accidental contact of the exposed wires.
6. Repair: Do not attempt to have an unauthorized repair of the equipment. Disassembly or detachment is risky and likely to cause shock. All repairs should be done by a qualified technician.
7. If any of the following cases arise, disconnect the power supply from the equipment first and intimate the technician immediately.
 - The power cord or connector is damaged.
 - Any liquid or material spilled into the equipment.
 - The equipment is wet or exposed to bad weather (rain, snow, etc.).
 - If the equipment cannot work properly, even if it is operated as instructed, please be sure to adjust only the control components specified in the operating instructions. Incorrect adjustments on other control components may cause damage to the equipment; even the equipment may fail to operate permanently.
 - The equipment falls, or its performance changes dramatically.
8. Replacing components: If it is necessary to replace a component, only the authorized technician can replace the accessories specified by the manufacturer.
9. Security inspection: After the equipment is repaired, the technician must conduct security inspection to ensure proper working of the equipment.

10. Power supply: Operate the equipment with only the type of power supply indicated on the label. Contact the technician for any uncertainty about the type of power supply.



Violation of any of the following cautions is likely to result in personal injury or equipment failure. We will not be responsible for the damages or injuries caused thereby.

- Before installation, switch off the external circuit (that supplies power to the system), including locks.
- Before connecting the equipment to the power supply, ensure the output voltage is within the specified range.
- Never connect the power before completion of installation.

1.2 Installation Instructions

1. The conduits of wires under relay must match with the metal conduits; other wires can use PVC conduits, to prevent failure caused by rodent damage. The Control panel is designed with proper antistatic, lightning-proof, and leakage-proof functions, ensure its chassis and the AC ground wire are correctly connected and the AC ground wire is grounded physically.
2. It is recommended not to plug/unplug connection terminals frequently when the system is powered on. Be sure to unplug the connection terminals before starting any relevant welding job.
3. Do not detach or replace any control panel chip without permission, and an unpermitted operation may cause damage to the control panel.
4. It is recommended not to connect any other auxiliary devices without permission. All non-routine operations must be communicated to our engineers in advance.
5. A control panel should not share the same power socket with any other large-current device.
6. It is preferable to install card readers and buttons at the height of **1.4 to 1.5m** above the ground or subject to customers' usual practice for proper adjustment.
7. It is advised to install control panels at places where maintenance is easy, like **a weak electric well**.
8. It is strongly recommended that the exposed part of any connection terminal should **not be longer than 4mm**, and specialized clamping tools may be used to avoid short-circuit or communication failure resulting from accidental contact with excessively exposed wires.
9. To save access control event records, export the data periodically from control panels.
10. Prepare countermeasures according to application scenarios for unexpected power failure, like **selecting power supply with UPS**.

11. To protect the access control system against the self-induced electromotive force generated by an electronic lock at the instant of switching off/on, it is necessary to **connect a diode in parallel** (please use the FR107 delivered with the system) with the electronic lock to release the self-induced electromotive force during onsite connection for application of the access control system.
12. It is recommended that an electronic lock and a control panel should use separate power supplies.
13. It is recommended to use the power supply delivered with the system as the control panel power supply.
14. In a place with substantial magnetic interference, galvanized steel pipes or shielded cables are recommended, and proper grounding is required.

2 System Introduction

The Access Control management system is a new modernized security management system, which is an effective measure of security and protection management. It is mainly used to manage the entrances and exits of highly secured places, such as banks, hotels, equipment rooms, offices, smart communities, and factories.

2.1 System Functional Parameters

- High-speed 32-bit 1.2GHz CPU, 128M RAM, and 256M Flash.
- Embedded LINUX operating system.
- One-door/two-door two-way access or four-door one-way access.
- Fingerprint capacity: 20,000.
- A maximum of 60,000 cardholders and 100,000 offline event records.
- Support of multiple Wiegand card formats and a password keypad, compatible with various types of cards.
- Control Panel with a watchdog (hardware) built in to prevent a crash.
- Over-current, over-voltage, and inverse-voltage protection for the input of the power supply to the control panel.
- Over-current protection for the power supply to card readers.
- Instant over-voltage protection for all input/output ports.
- Instant over-voltage protection for communication ports.

2.2 Product Technical Parameters

- Working Power supply: Rated voltage 12V ($\pm 20\%$) DC, rated current is 2A.
- Working environment: Temperature 0°C to 45°C; Humidity 20% to 80%.
- Electronic lock relay output: The maximum switching voltage is 12V(DC); The maximum switching current is 2A.
- Auxiliary relay output: The maximum switching voltage is 12V(DC); The maximum switching current is 1.25A.
- The detachable connection terminals are made of alloy-steel non-magnetic flange materials.
- Outline dimensions of the control PCB: 181mm(length) \times 106mm (width) for InBio160/260 Pro; 226mm (length) \times 106mm (width) for InBio460 Pro.
- External box dimensions: 350(L)mm \times 300(W)mm \times 90(H)mm.

Valve regulated lead-acid battery:

- Constant voltage charge voltage regulation

- Cycle use : 14.5V~14.9V(25)
- Initial current: less than 2.88A1
- Standby use: 13.6V~13.8V(25)
- Capacity: 12V, 7.2Ah/20hr
- Battery Type: LC-RA127R2T1

Battery Caution:

- Do not charge in a gas tight container.
- Do not short the battery terminals.
- Do not incinerate.
- Flush with water at once if contact is made with electrolyte (Acid).
- Do not attempt to disassemble the battery.

2.3 Control Panel Indicators

When the InBio160/260/460 Pro is powered on, normally the POWER indicator (red) is lit constantly, the RUN indicator (green) shall flash slowly (indicating the system is normal), and other indicators are all off.

- LINK indicator (green): indicates proper TCP/IP connection if it is lit constantly;
- ACT indicator (yellow): indicates transmission of TCP/IP data if it flashes;
- EXT RS485 (TX) indicator (yellow): indicates sending of 485 data if it flashes;
- EXT RS485 (RX) indicator (green): indicates receiving of 485 data if it flashes;
- CARD indicator (yellow): indicates input of Wiegand signal if it is lit.

Indicator Diagram:

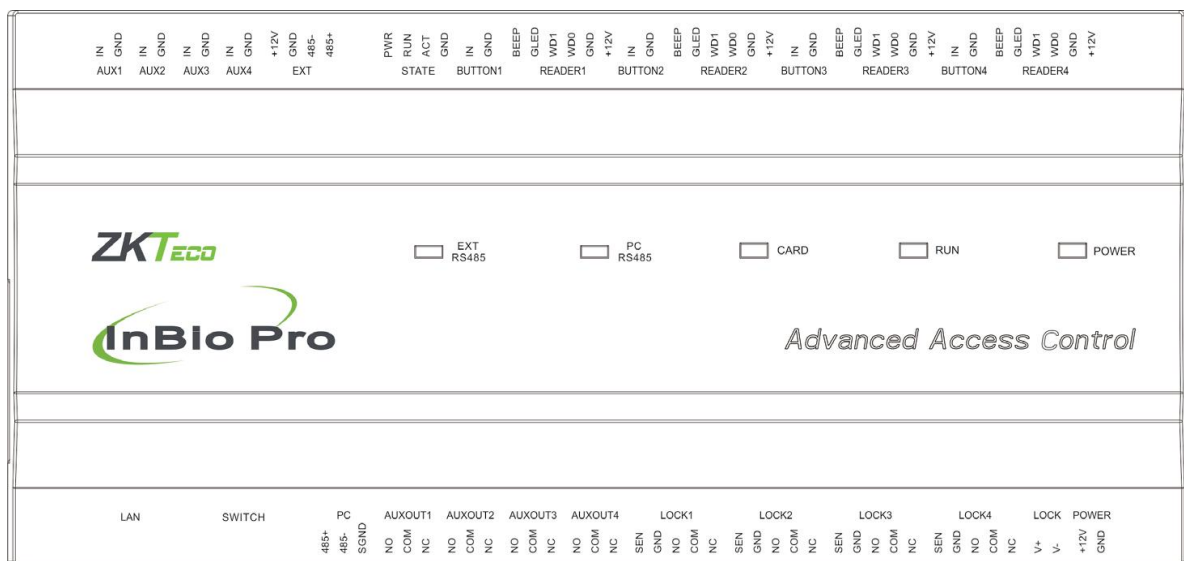
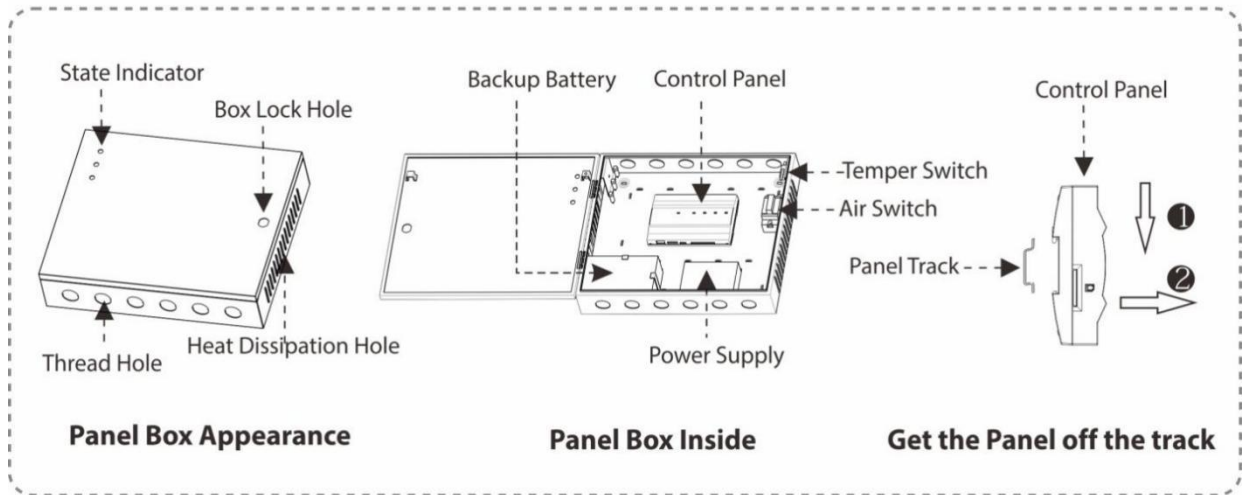


Figure 2-1 Indicators in the InBio460 Pro

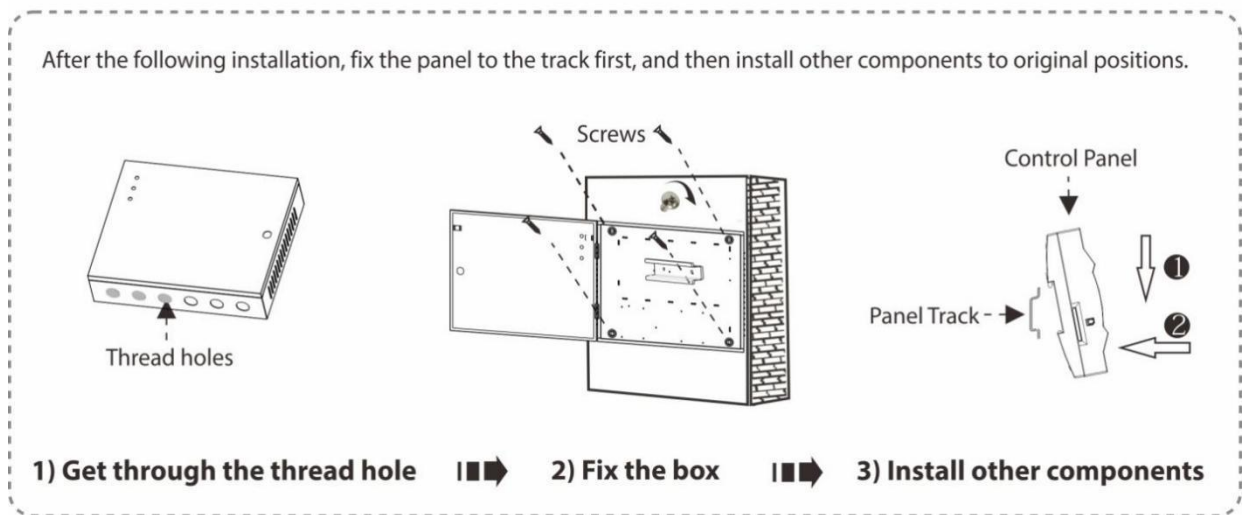
3 Installation and Connection

3.1 Installation Procedure

Appearance and Internal of the panel box:



Installation steps for the control panel:



3.2 Installation of Access Control Panel Wires

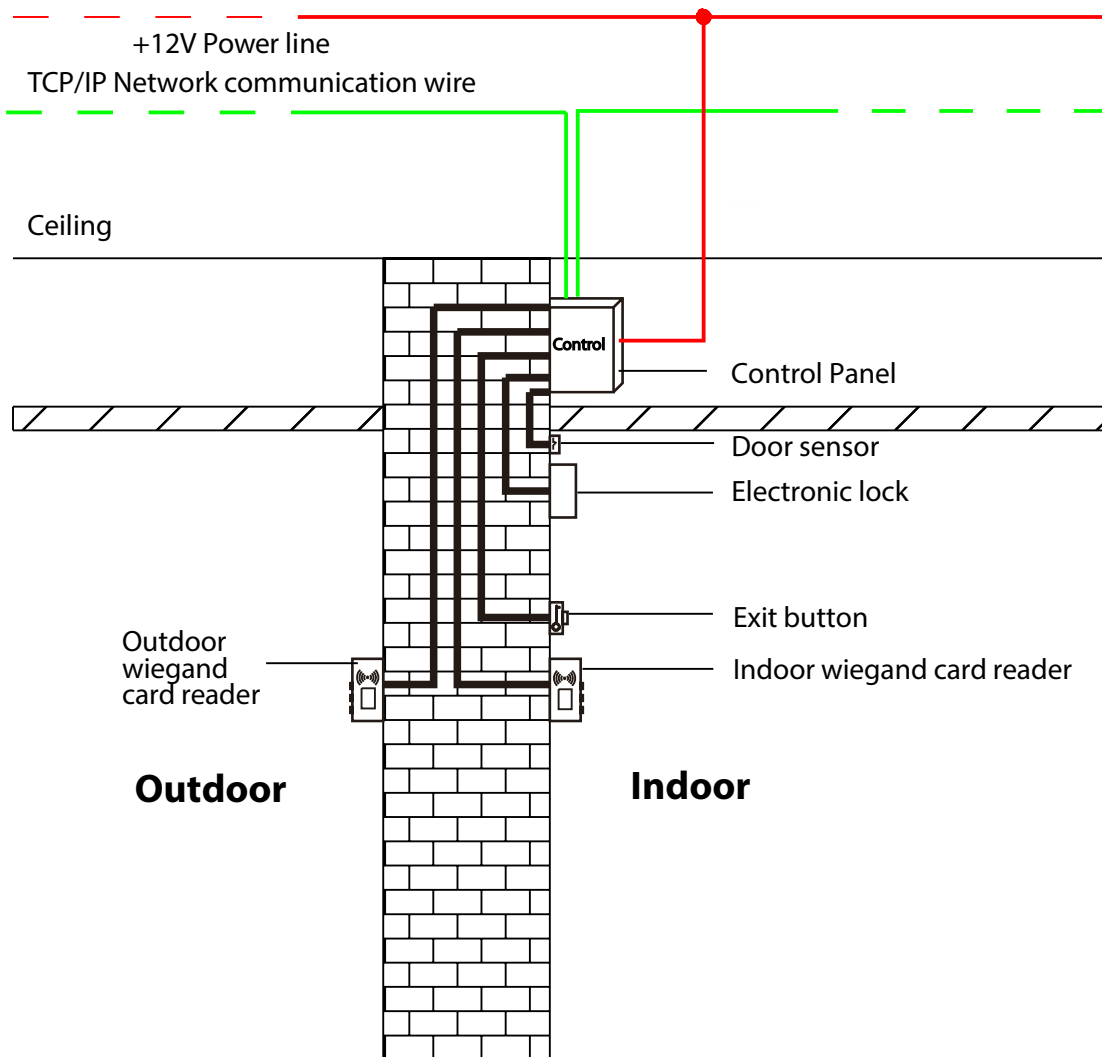


Figure 3-1 Access Control Panel Wire Installation Diagram

Remarks:

- Ensure the power supply is disconnected before connecting the wires; otherwise, it may cause severe damage to the equipment.
- The access control wires must be separated according to heavy and light current; the control panel wires, electronic lock wires, and exit button wires must run through their casing pipes, respectively.

3.3 Control Panel System Installation

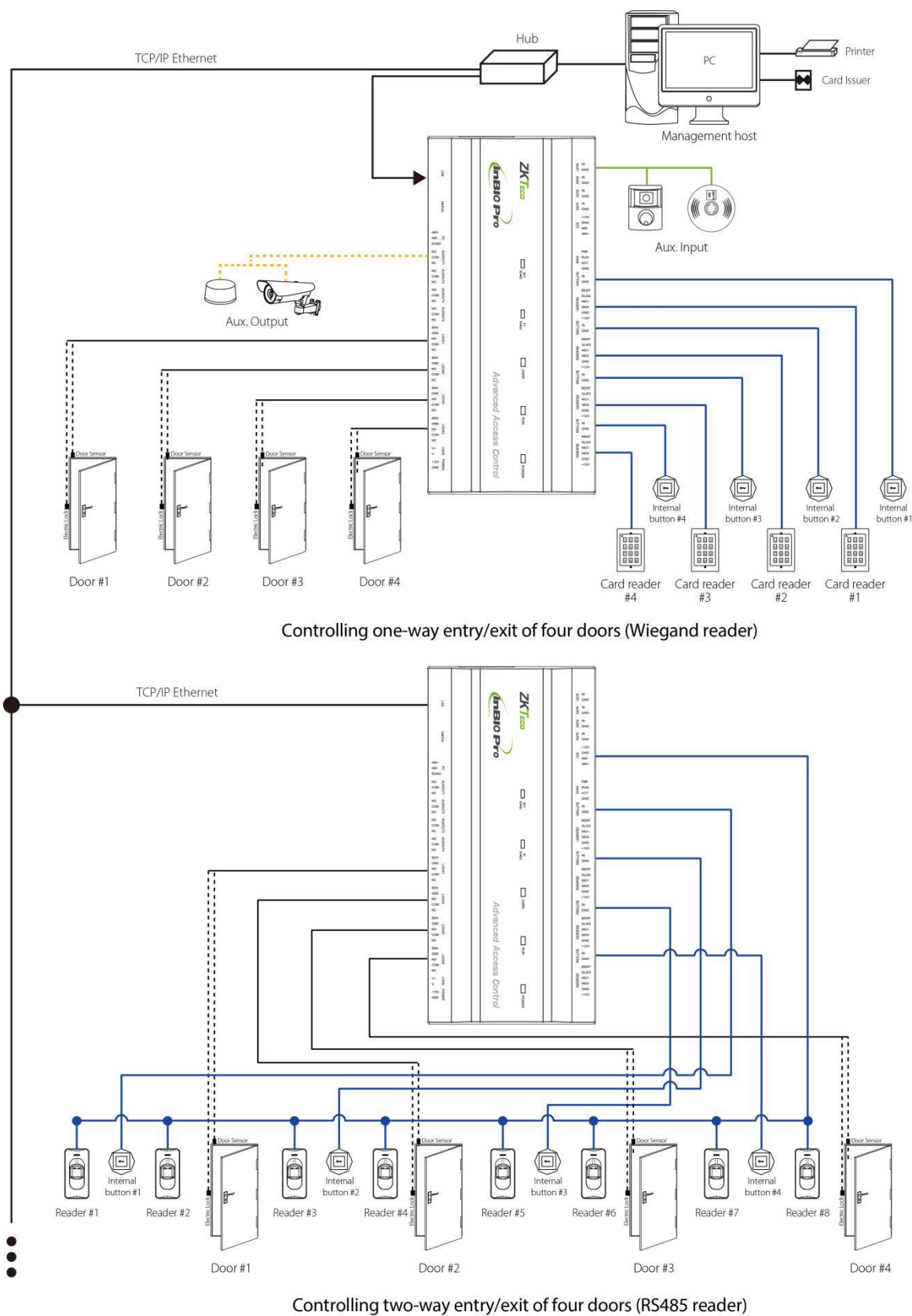


Figure 3-2 Schematic Diagram of System Installation

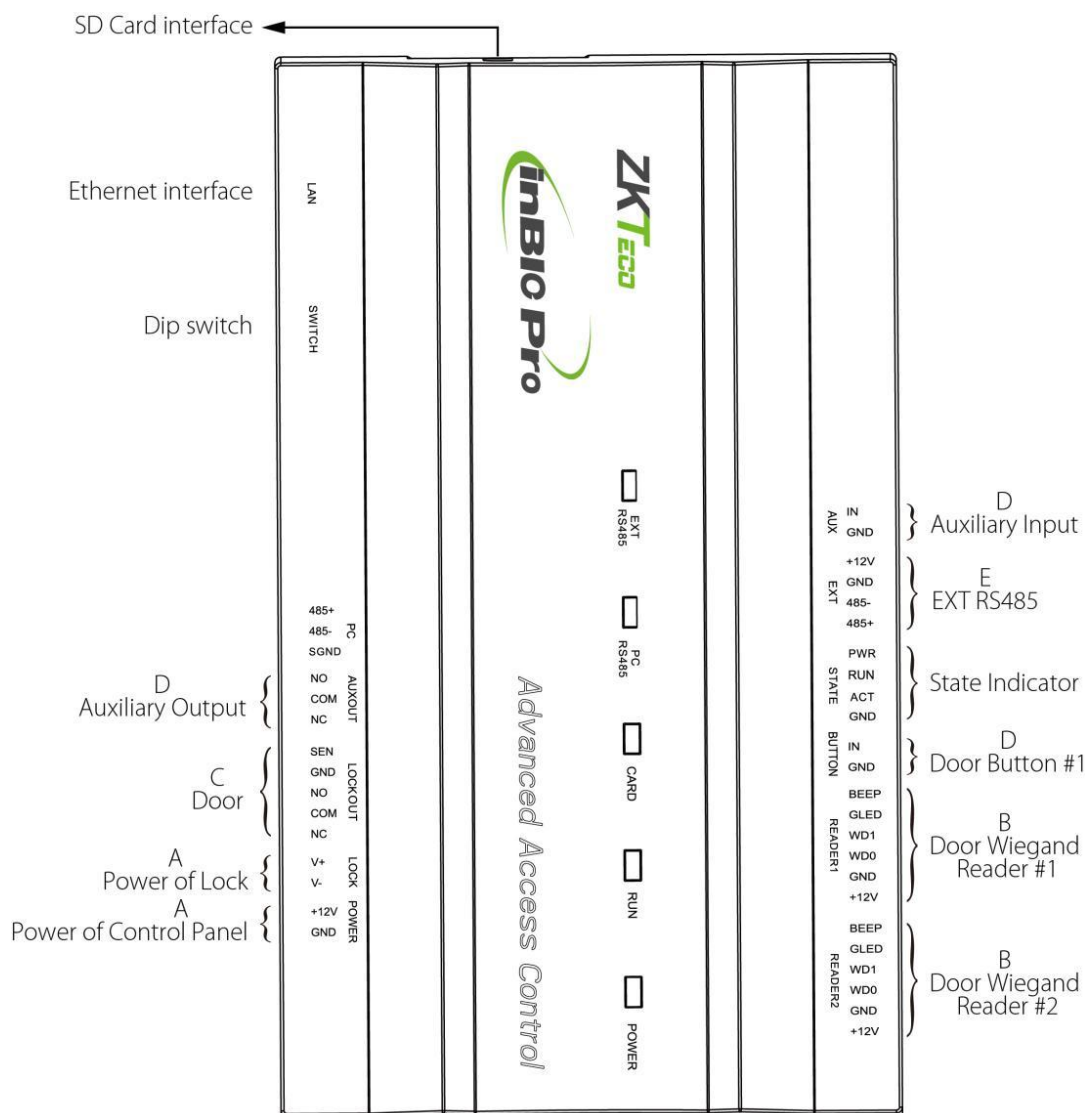
NOTE: The diagram above takes the InBio460 Pro for example. By contrast, only one-door two-way access is applicable to the InBio160 Pro system; only two-door one-way or two-door two-way access is applicable to the InBio460 Pro system.

The access control management system consists of two parts: Management Workstation (PC) and Control panel. The management workstation and control panel communicate through TCP/IP. The communication wires should be kept away from high-voltage wires as far as possible and should be neither routed in parallel with nor bundled with power wires.

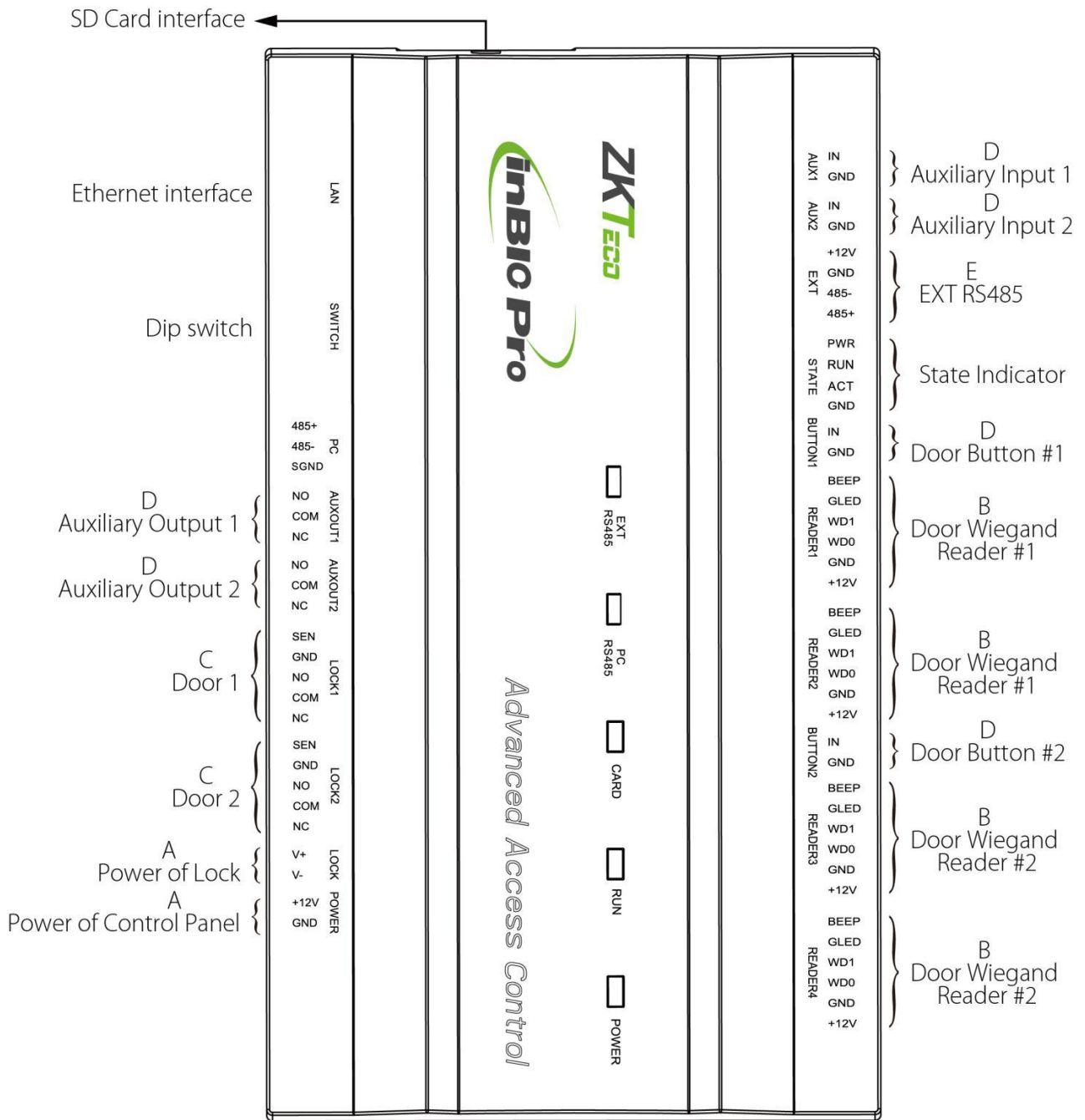
A management workstation is a PC connected with the network. By running the access control management software installed in the PC, access control management personnel can remotely perform various management functions, like adding/deleting a user, viewing event records, opening/closing doors, and monitoring the status of each door in real-time.

3.4 Control Panel Connection Terminals

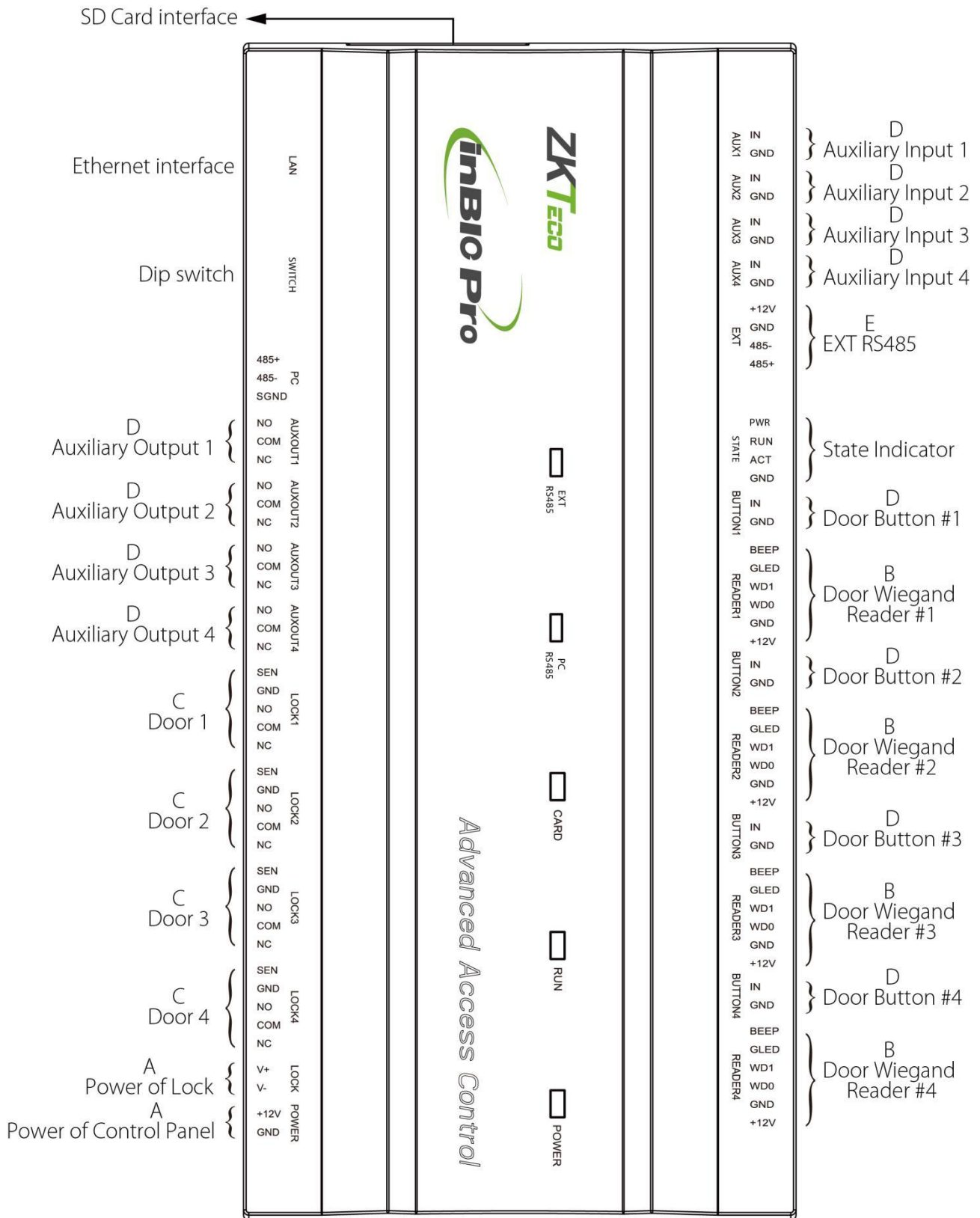
InBio160 Pro Terminal connection diagram



InBio260 Pro Terminal connection diagram



InBio460 Pro Terminal connection diagram



- **Description of the terminals:**
 1. The auxiliary input may connect to infrared body detectors, fire alarms, or smoke detectors.
 2. The auxiliary output may connect to alarms, cameras or doorbells, etc.
 3. The RS485 Reader port can be connected externally to RS485 reader.
 4. The terminals above are set through the relevant access control software. Please see the respective software manual for further details.
- **SD card function:**
Backup event records of access control for client.
- **Ports of InBio160/260/460 Pro Control Panel:**

No.	Functional Port	InBio160 Pro (One-Door Two-Way)	InBio260 Pro (Two-Door Two-Way)	InBio460 Pro (Four-Door One-Way/ Two-Door Two Way)
1	Wiegand card reader interface	2	4	4
2	Exit button	1	2	4
3	Control lock relay	1	2	4
4	Door sensor	1	2	4
5	Extension input	1	2	4
6	Extension output	1	2	4
7	RS485 extension communication	✓	✓	✓
8	TCP/IP	✓	✓	✓

3.5 Connection with Door Sensors, Exit Switches, Auxiliary Input Devices, and PC485 Extension Communication

- **Door sensor**

A Door Sensor is used to sense the open/close status of a door. With a door sensor switch, an access control panel can detect the unauthorized opening of a door and will trigger the output of alarm. Moreover, if a door is not closed within a specified period after it is opened, the door control panel will also raise the alarm. It is recommended to select two-core wires with a gauge over 0.22 mm². A door sensor can be omitted if it is unnecessary to monitor the open/closed status of a door, raise the alarm when the door is not closed for a long time, monitor if there is unauthorized access, and

use the interlock function.

- **Exit switch**

An exit switch is a switch installed indoor to open a door. When it is switched on, the door will be opened. An exit button is fixed at the height of about 1.4m above the ground. Ensure it is located in the right position without slant, and its connection is correct and secure. (Cut off the exposed end of any unused wire and wrap it with insulating tape.) Make sure to avoid electromagnetic interference (such as light switches and computers). It is recommended to use two-core wires with a gauge over 0.3mm² as the connection wire between an exit switch and the Control panel.

- **Auxiliary input**

The InBio160 Pro provides one auxiliary input interface; the InBio260 Pro provides two and the InBio460 Pro provides four, which may connect to infrared body detectors, smoke detectors, gas detectors, window magnetic alarms, wireless exit switches, etc. Auxiliary inputs are set through the relevant access control software. Please see the **ZKAccess 4.0 user manual** for further details.

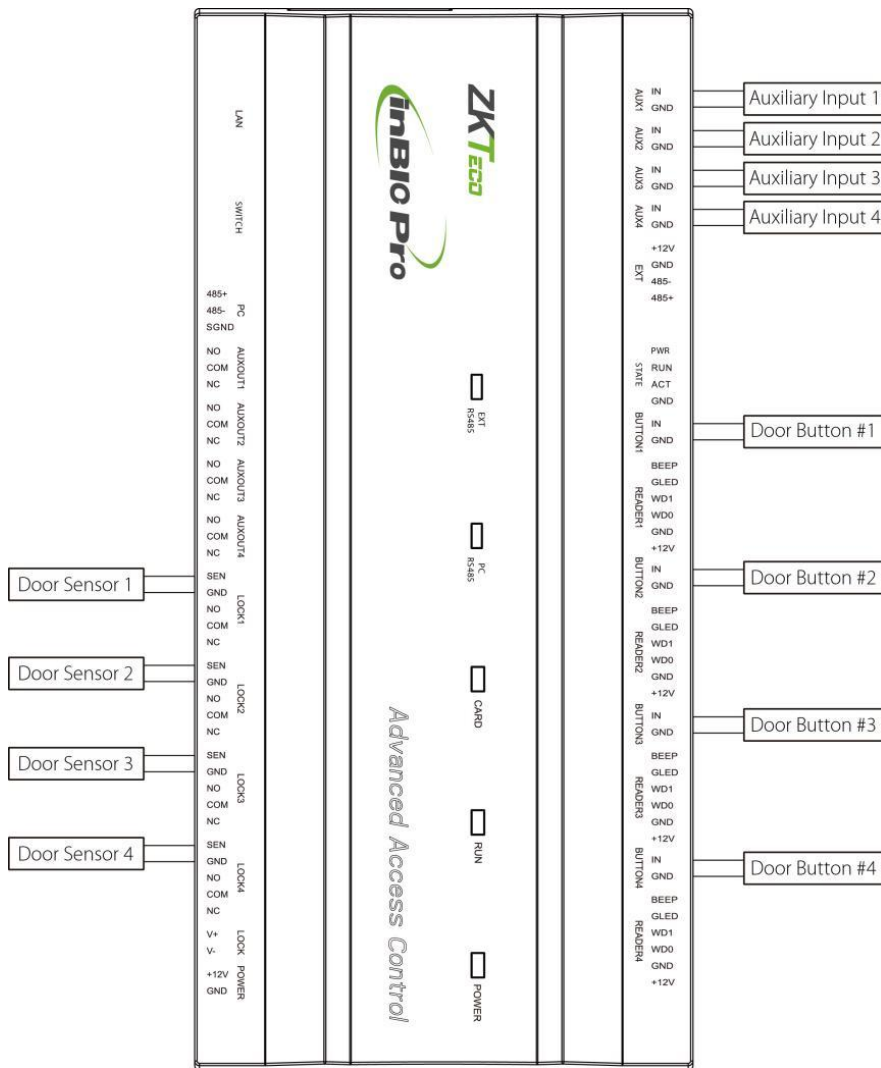


Figure 3-3 Connections between InBio460 Pro and Door Sensors, Exit Switches, and Auxiliary Input Devices

- **PC485 extension communication**

The Control panel supports extensive modules which like **EX0808**, through PC485. An inBioX60 Pro can connect eight EX0808 at most. As shown in the following figure.

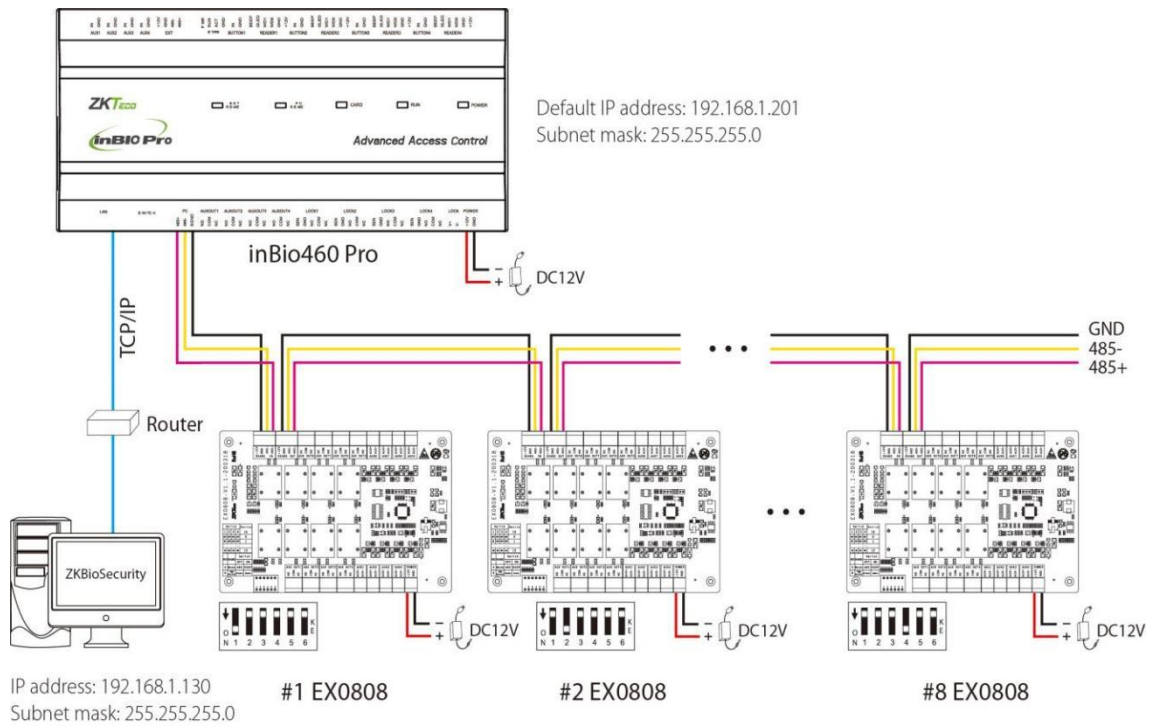


Figure 3-4 Connection between inBio460 Pro and EX0808 through PC485

NOTE:

1. A maximum of eight EX0808 extended boards can be connected to an inBio460 Pro controller.
2. Each EX0808 can connect a maximum of eight auxiliary input devices and eight auxiliary output devices.
3. A separate power supply is required for each EX0808.
4. Set the RS485/OSDP addresses of each EX0808 by the DIP switch before power is supplied.

Description	RS485 Address	DIP Switch	RS485 Address	DIP Switch	RS485 Address	DIP Switch
<p>MODE (RS485/OSDP)</p> <p>RS485 Terminal Resistance</p>	1		6		11	
	2		7		12	
	3		8		13	
	4		9		14	
	5		10		15	

DIP Switch Setting for RS485/OSDP Communication

3.6 Connection with Readers

The Control panel supports RS485 reader and Wiegand reader.

- **Connection with RS485 readers**

The InBio160 Pro can connect two RS485 readers in the one-door two-way mode. The InBio260 Pro provides four readers, which can be connected in the two-door two-way mode. The InBio460 Pro provides four readers, which can be connected in the two-door two-way or four-door two-way mode.

RS485 reader connection: Set the RS485 address (device number) of the reader by DIP switch or other ways.

Control Panel \ RS485 address	1	2	3	4	5	6	7	8
InBio160 Pro	#1Door IN	#1Door OUT						
InBio260 Pro	#1Door IN	#1Door OUT	#2Door IN	#2Door OUT				
InBio460 Pro	#1Door IN	#1Door OUT	#2Door IN	#2Door OUT	#3Door IN	#3Door OUT	#4Door IN	#5Door OUT

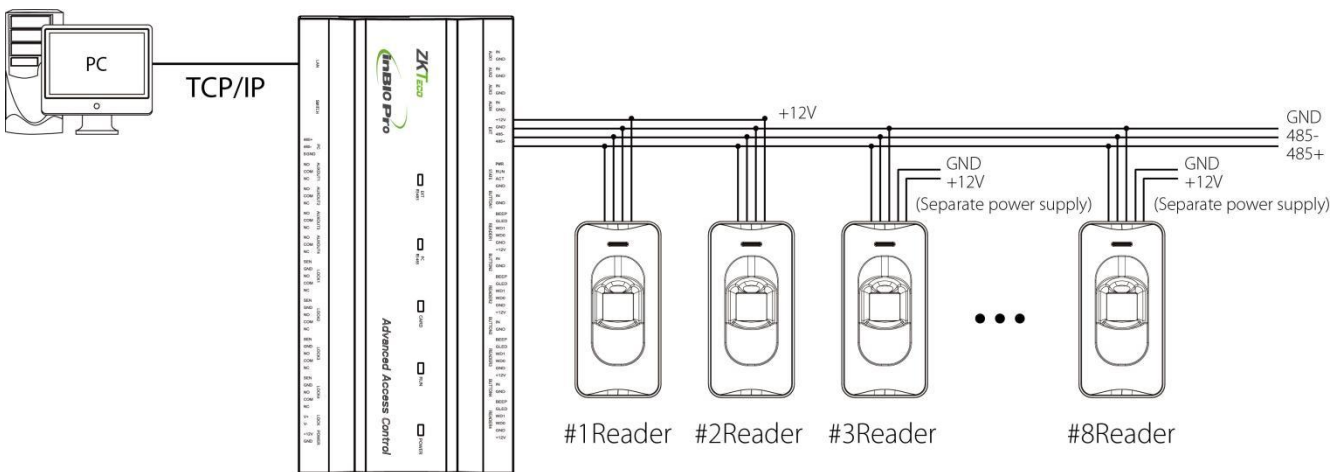
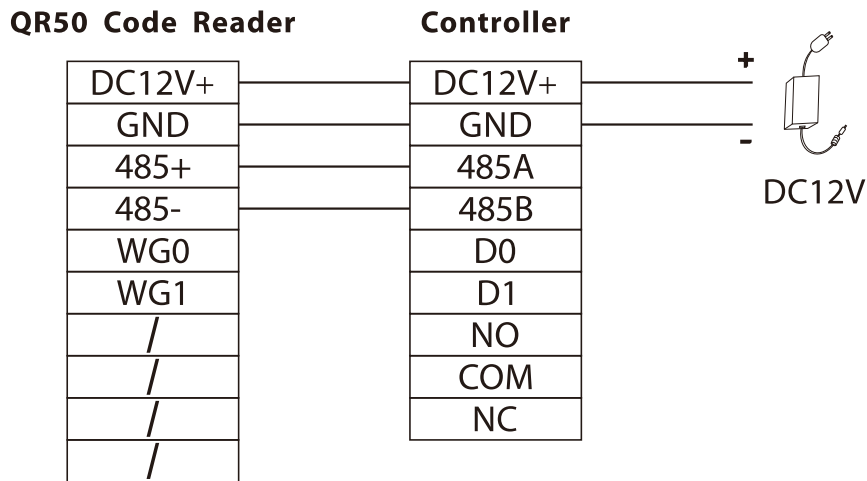


Figure 3-5 Connection between inBio460 Pro and RS485 Readers

The QR50 code reader does not need to be connected to the lock body when it is used as a reader. The controller in the figure only lists some of the wirings, and there are many kinds of connections between the machines. RS485 common connection reference as shown below:



Reader Mode

A single EXT RS485 interface can supply for maximum 750 mA (12V) current. So the entire current consumption should be less than this max value when the readers share power with the panel. For calculation, please use max current of the reader, and starting current is usually more than twice of the normal work current, please consider this situation.

Using the KR502M-RS card reader as an example, the standby current is less than 80mA, the max current is less than 90mA. When starting the device, Instantaneous current can reach for 180 mA. For RS485 reader, considered that the starting current is bigger, there are only four readers can connect for power supply through the EXT RS485 interface. So the power of control panel can only connect up to 4 readers.

If RS485 reader is connected externally and shares the power supply with the device, it is recommended that the connection between the EXT RS485 port and the reader be no longer than 100m. Otherwise, it is recommended that using a separate power supply for the reader.

For some of the devices with much greater consumption, we suggest to use the separately power supplies, to make sure the steady operation.

- **Connection with Wiegand Readers**

The InBio160 Pro can connect two Wiegand readers in the one-door two-way mode. The InBio260 Pro provides four readers, which can be connected in the two-door two-way mode. The InBio460 Pro provides four readers, which can be connected in the two-door two-way or four-door one-way mode.

The Wiegand interfaces provided by the InBio160/260/460 Pro series can be connected to different types of readers. If your card reader does not use the voltage of DC 12V, an external power supply is needed. A reader should be installed at a height of about 1.4m above the ground and at a distance of 30-50mm away from a door frame.

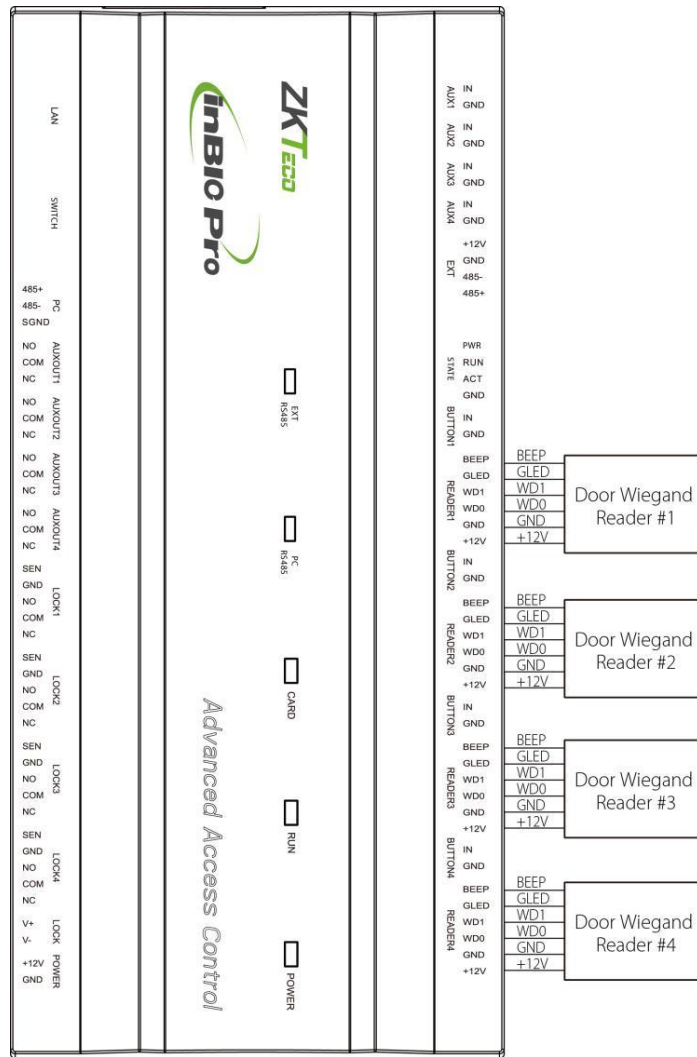
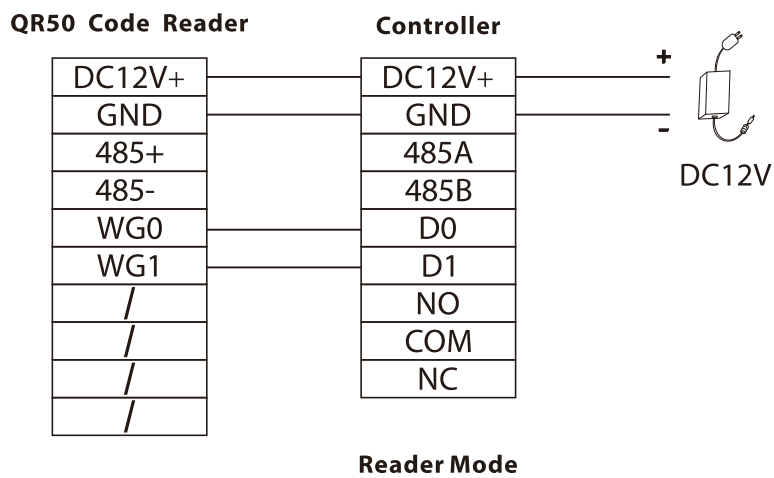


Figure 3-6 The connection between the Control Panel and Wiegand Readers

Wiegand common connection reference as shown below:




NOTE: For more detailed information on the use of QR50 such as connection and software configuration, please refer to the **QR50 user manual**.


3.7 Relay Output Connection

InBio160 Pro has two relays (one used as control lock by default, and the other one used as auxiliary output); InBio260 Pro has four relays (two used as control locks by default, and the other two used as auxiliary outputs); InBio460 Pro has eight relays (four used as control locks by default, and the other four used as auxiliary outputs).

The relays for auxiliary outputs may connect to monitors, alarms, doorbells, etc. Auxiliary outputs are set through the relevant access control software. Please refer to the respective software manual for details.

1. The default connection mode of the door lock is “dry mode.” In general, the electronic lock uses an external power supply separately. The wiring mode of the door lock relay cannot be changed, except that the auxiliary output relay. The diagram below uses the example of a door lock connection to demonstrate the output relay connection.
2. An access control panel provides multiple electronic lock outputs. The COM and NO terminals apply to the locks that are unlocked when power is connected and locked when power is disconnected. The COM and NC terminals use the locks that are locked when power is connected and unlocked when power is disconnected.
3. To protect the access control system against the self-induced electromotive force generated by an electronic lock at the instant of switching off/on, it is necessary to connect a diode in parallel (please use FR107 delivered with the system) with the electronic lock to release the self-induced electromotive force during the onsite connection for application of the access control system.
4. By setting the jumper terminal beside the lock relay, you can select the device power supply or lock power supply for the lock (that is, the wet mode or dry mode).

- **Dry mode jumper setting:** short 1-2 and 3-4  , and the device power supply will be used for the relay output.

- **Wet mode jumper setting:** short 2-3 and 4-5  , and the lock power supply will be used for the relay output.

NOTE: The default connection mode of the door lock is “**Dry mode**”.

Take the InBio160 Pro as an example here, as shown in the following figure.

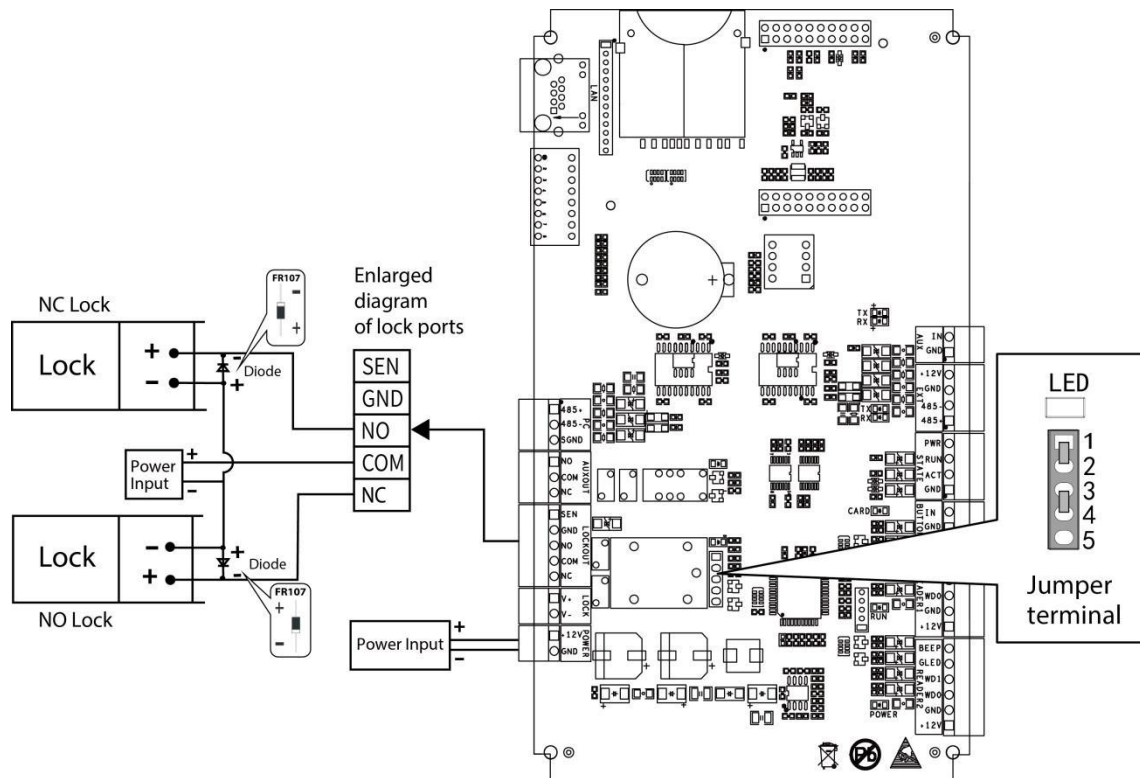


Figure 3-7 "Dry mode" wiring diagram of lock connecting with external power supply(recommend)

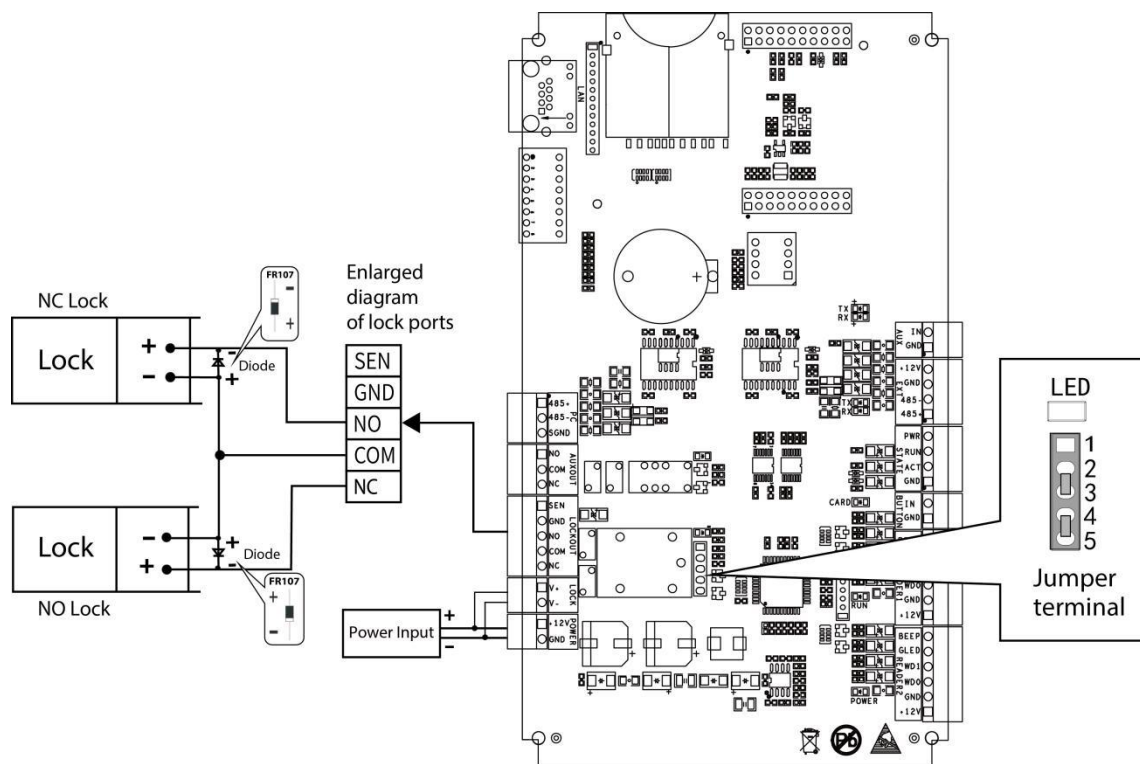
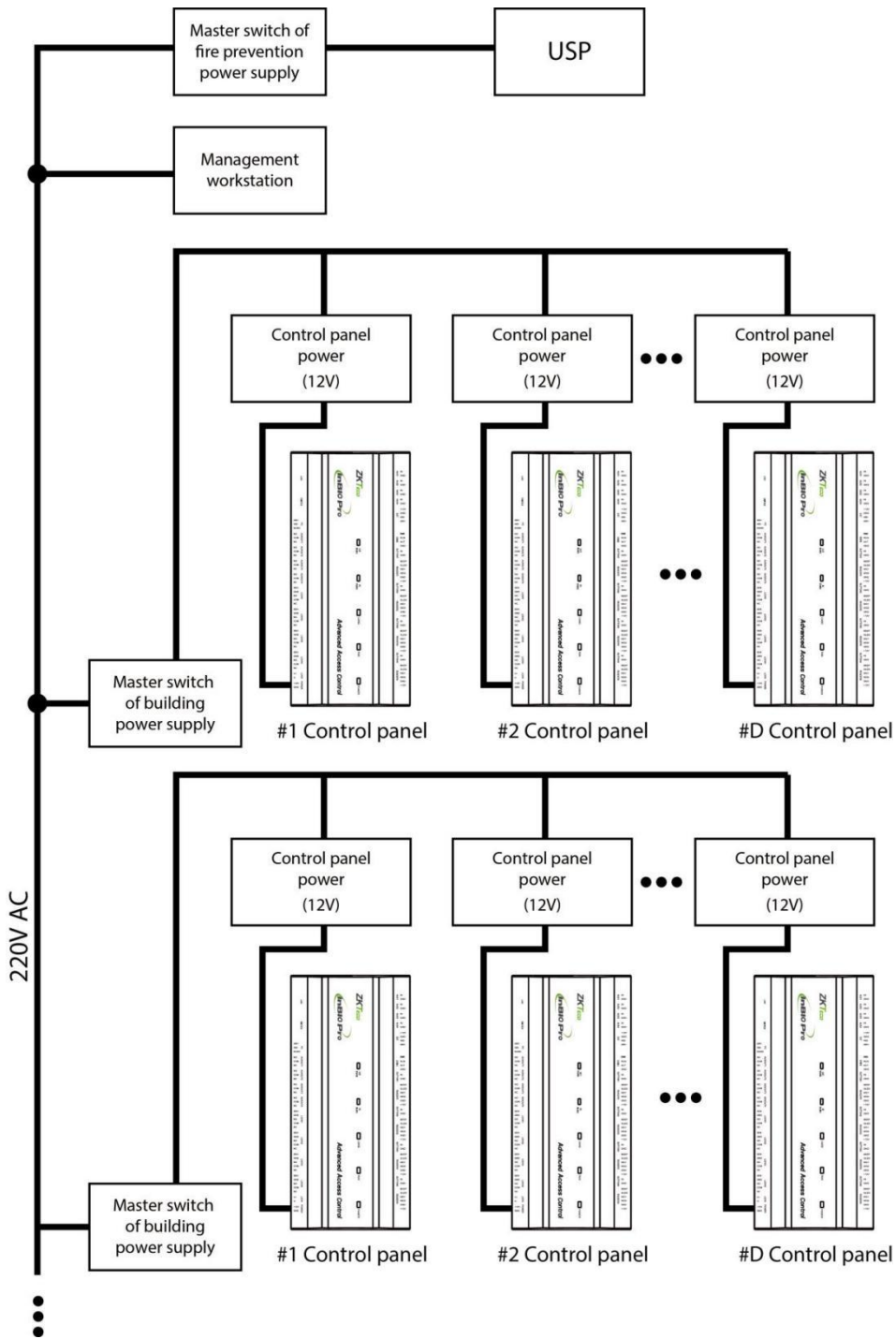


Figure 3-8 "Wet mode" wiring diagram of lock and controller common power supply

3.8 Access Control Operator Panel System Power Supply Structure



An access control operator panel is powered by +12V DC. Generally, to reduce power interference between control panels, each control operator panel should be powered separately. When high reliability is required, control panels and electronic locks should be powered respectively.

To prevent power failure of a control operator panel from making the whole system unable to work normally, the access control management system is usually required to have one UPS at least, and access control locks are powered externally to guarantee the access control management system can still work normally during power failure.

4 Equipment Communication

The background PC software can communicate with the system according to two protocols for data exchange and remote management.

4.1 Access Control Networking Wires and Wiring

1. The power supply is 12V DC converted from 220V.
2. As an electronic lock has a large current, it generates a strong interference signal while functioning. To reduce such an effect, 4-core wires (RVVP 4×0.75mm², two for a power supply, and two for a door sensor) are recommended.
3. RS485 communication wires are made of internationally accepted shielded twisted pairs, which prove effective to prevent and shield interference.
4. The Wiegand readers use 6-core communication shielded wires (RVVP 6×0.5mm) (usually there are 6-core, 8-core, and 10-core types available for users to select according to the ports) to reduce interference during transmission.
5. Other control cables (like exit switches) are all made of 2-core wires (RVVSP 2×0.5mm²).
6. Notes for wiring:
 - Signal wires (like network cables) can neither run in parallel with nor share one casing pipe with large-power electric wires (like electronic lock wires and power cables). If parallel wiring is unavoidable for environmental reasons, the distance must be above 50cm.
 - Try to avoid using any conductor with a connector during distribution. When a connector is indispensable, it must be crimped or welded. No mechanical force can be applied to the joint or branch of conductors.
 - In a building, the distribution lines must be installed horizontally or vertically. They should be protected in casing pipes (like plastic or iron water pipes, to be selected according to the technical requirements of the indoor distribution). Metal hoses are applicable to ceiling wiring, but they must be secure and good-looking.
 - Shielding measures and shielding connection: If the electromagnetic interference in the wiring environment is found substantial in the survey before construction, it is necessary to consider the shielding protection of data cables when designing a construction scheme. Overall, shielding protection is required if there is a large radioactive interference source or wiring has to be parallel with a large-current power supply on the construction site. Generally, shielding measures includes keeping a maximum distance from any interference source, and using metal wiring troughs or galvanized metal water pipes to ensure reliable grounding of the connection between the shielding layers of data cables and the metal troughs or pipes. Noted that a shielding enclosure can have a shielding effect only when it is grounded reliably.

- Ground wire connection method: Reliable large-diameter ground wires in compliance with applicable national standards are needed on the wiring site and should be connected in a tree form to avoid DC loop. These ground wires must be kept far away from lightning fields. No lightning conductor can serve as a ground wire and ensure there is no lightning current through any ground wire when there is lightning. Metal wiring troughs and pipes must be connected continuously and reliably and linked to ground wires through large-diameter cables. The impedance of this section of wire cannot exceed 2 ohms. Also, the shielding layer must be connected reliably and grounded at one end to guarantee a uniform current direction. The ground wire of the shielding layer must be connected through a large-diameter wire (not less than 2.5mm²).

4.2 TCP/IP Communication

The Ethernet 10/100Base-T Crossover Cable, a type of crossover network cable, is mainly used for cascading hubs and switches or used to connect two Ethernet endpoints directly (without a hub). Both 10Base-T and 100Base-T are supported.

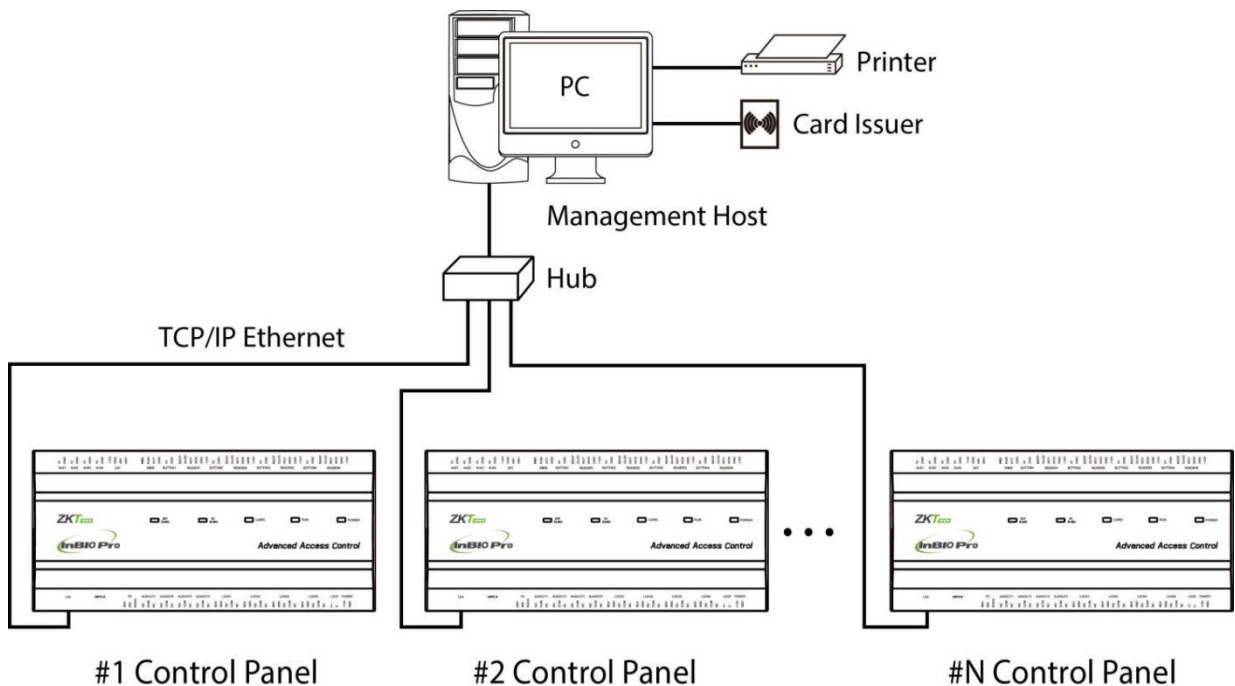


Figure 4-1 TCP/IP Communication System Networking

In Access software: Click **Device** > **Search Device** to search for access controllers in the network, and directly add from the search result.

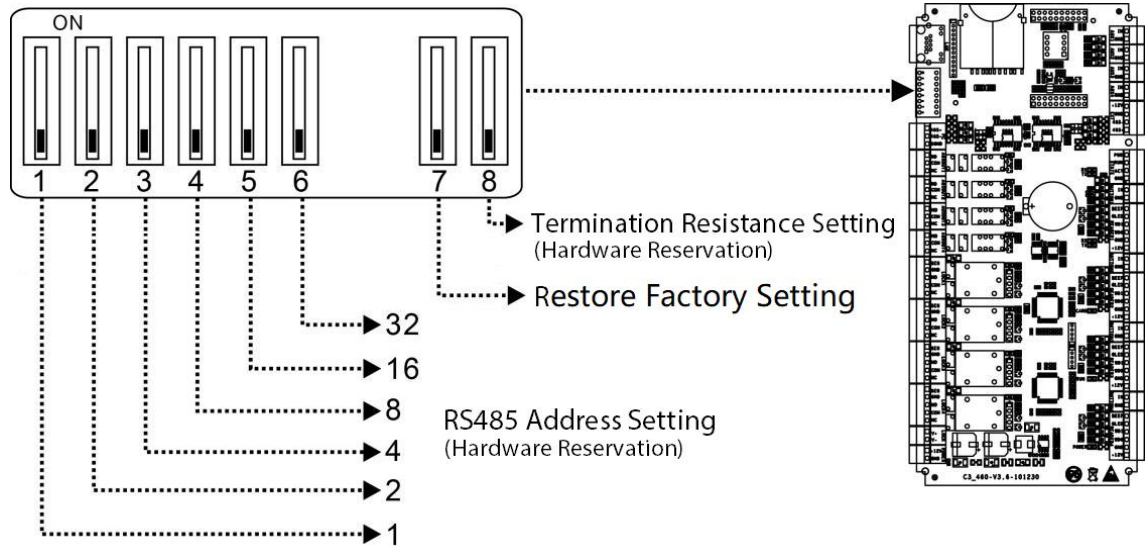
4.3 DIP Switch Settings

This part introduces how to restore the factory settings through the DIP switch.

NOTE: RS485 Address Setting and Termination Resistance Setting for the control panel are hardware reserved features and are not currently supported.

- **Restoring factory setting**

The silk-screened **7** (place 7) of the DIP switch is the switch for restoration of system settings. The place is set to **OFF** by default. When place 7 is moved upwards and downwards for three times within 10 seconds and finally returned to the **OFF** position, the factory settings will be restored after the access control operator panel is restarted.

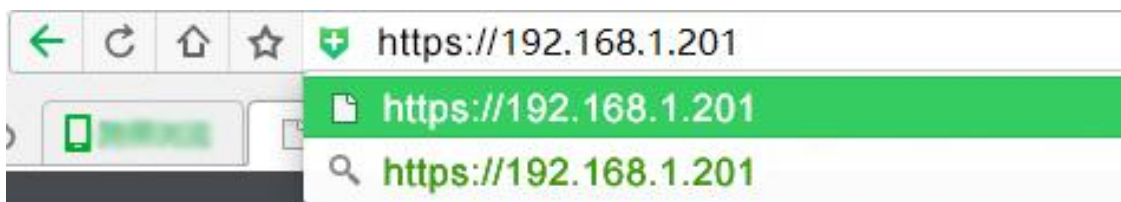


4.4 ZKPanelWeb

To help users conveniently manage controllers, the built-in Web Server function is added to some models. With this function, a user can connect to the controller through a PC, and enter the IP address of the controller to access the web. Users can also use the Web Server function to perform other operations, such as network configuration, Push communication configuration, time synchronization, and user account management.

Log on to the Web Server

1. Connect the controller to the network or PC, start the browser, enter the IP address of the controller, which is **https://192.168.1.201** by default. Then you can visit the Web Server.



2. When Web Server is used, "User Name" and "Password" should be set firstly. The default "user name" is **admin** and the default "password" is **zkteco@12345**.



3. Click **Sign In** to access the ZKPanelWeb.

NOTE:

1. IP addresses of both the server (PC) and the controller must be in the same network segment.
2. IP address of the controller could be found by searching devices with the BioSecurity software ([**Access - Access Device - Device - Search Device**]).

Basic Operation Bar of the Web Server




- **Change of the Administrator's Password**

1. Click . The following page is displayed:

Modify Password		Close
User Name:	<input type="text" value="admin"/>	
Old Password:	<input type="password"/>	* Enter a string of 4-30 characters!
New Password:	<input type="password"/>	* Enter a string of 4-30 characters!
Confirm New Password:	<input type="password"/>	* Enter a string of 4-30 characters!
<input type="button" value="Confirm"/> <input type="button" value="Cancel"/>		


2. Enter the old and new passwords, and click Confirm to change the administrator's login password.

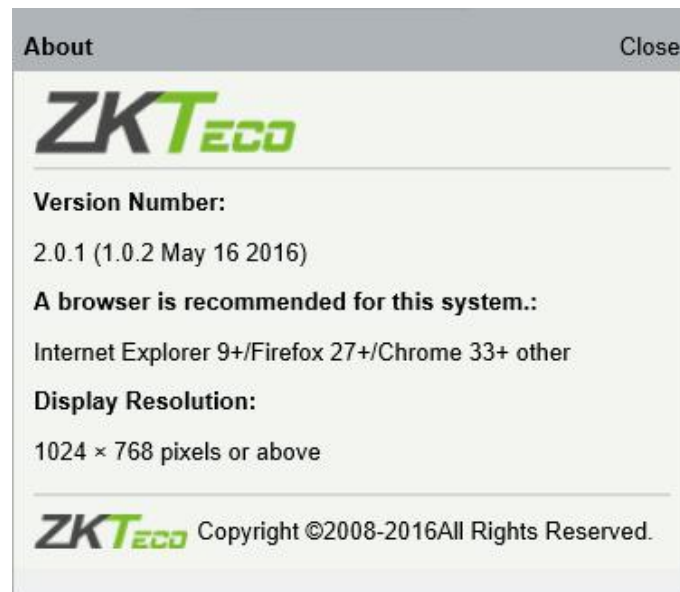
- **Language Settings**

Click , change the language in which the server interface is displayed, and click Confirm.




- **Use Conditions of the Server**

Click , and you can view the version of the current server, as well as the browser and resolution recommended for the server.



- **Online Help of the Server**

If you met some problems when using the server, click  to view or download the user help document.

WEB Help Document

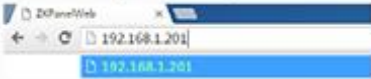
WEB Version: 2.0
Date: July 2016

Note:For other information not mentioned here, please read related user manual.


[Login Web Server](#) | [Basic Operation](#) | [Network Settings](#) | [Communication Settings](#) | [System](#)

1. Login Web Server

- 1. Connect the controller to the network or PC, start the browser, enter the IP address of the controller, which is 192.168.1.201 by default. Then you can visit the Web Server.




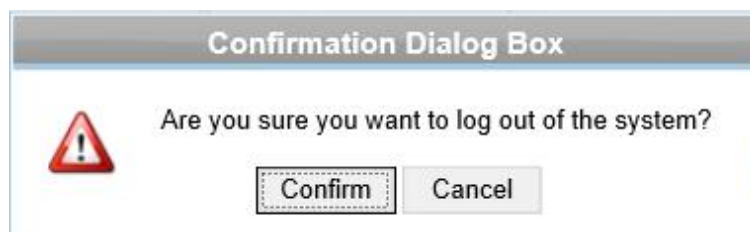
- 2. When Web Server is used, "user Name" and "Password" should be set firstly. The default "user name" and "password" are admin.



- 3. Click [Sign in] to enter the Web Server.

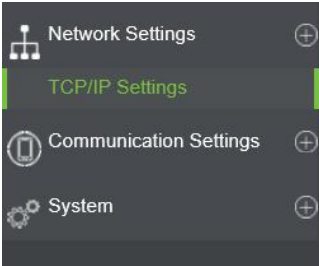
- **Exit**

Click , and then click Confirm to return to the server login page.



Network Settings

- **TCP/IP Settings**



TCP/IP Settings	
IP Address:	192.168.1.129 <input type="text"/> ✕ *
Subnet Mask:	255.255.255.0 *
Gateway:	192.168.1.254 *
Primary DNS:	<input type="text"/>
<input type="button" value="Confirm"/> <input type="button" value="Cancel"/>	

- **Function introduction:**

Set the TCP/IP communication parameters, which are used in the communications between device and PC.

- **Operating steps:**

1. Click **Network Setting > TCP/IP Settings**.

2. Input the device's IP address, Subnet Mask, Default Gateway.

- ✧ IP address: the default IP is 192.168.1.201, and you can modify according to the actual.
- ✧ Subnet Mask: the default subnet mask is 255.255.255.0, and you can modify according to the actual.
- ✧ Default Gateway: the default gateway is 0.0.0.0, and you can modify it according to the actual.
- ✧ Primary DNS: the default value is null, and you can set its value.

3. Click **Confirm** to write parameters into the device. please restart the device by manual.

Communication Settings

- **PUSH Server Settings**

PUSH Server: Indicates that the controller proactively pushes information to the server.

IP Mode: the default server IP is 0.0.0.0, and you can modify it according to the actual.

Port: The default Port is 80, and you can modify it according to the actual.

Domain Mode: The default value is null, and you can set its value.

- **Port Settings**

Http Port: Indicates that the client initiates an HTTP request to a specified port on the server. the default HTTP Port is 80, and you can modify it according to the actual.

- **Communication Password**

Communication Password: Indicates that network communication is encrypted. The default value is null, and you can set its value.

If you configure the communication password here, the same communication password must be configured on the server before the connection can be set up.

System

- **User Settings**

User Name	Note	Operation
admin	You can perform any configuration	Edit
user	You can only view the device information and modify password of the current user	Edit

Click **Edit** to change the login password of an administrator or a user.

- **Time Settings**

Time Settings	
Current Time:	2016-06-01 17:36:52
<input type="radio"/> Manual Setting	
Date:	2016-06-01
Time:	17:36:49
<input checked="" type="radio"/> Synchronization with PC Time	
PC Time:	2016-06-01 17:37:15
<input type="button" value="Confirm"/> <input type="button" value="Cancel"/>	

You can manually configure the controller time or synchronize the controller time with the PC time, and click **Confirm** to complete the setting.

- **System Settings**

System Settings	
Reboot Device:	<input type="button" value="Reboot"/>

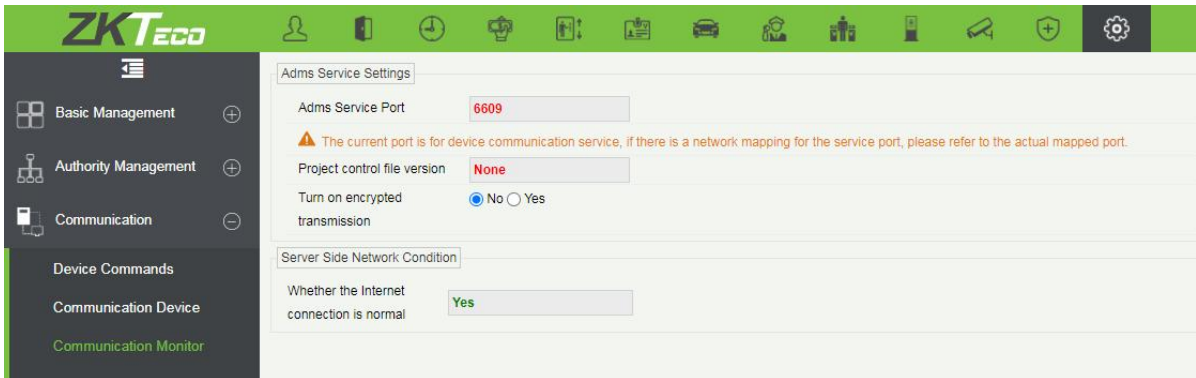
Click **Reboot**. The device will be restarted.

- **Device Information**

Device Information		
Device Name:	192.168.1.129	
Serial Number:	192.168.1.129	
Platform:	192.168.1.129	
Firmware Version:	AC Ver 5.7.6.3029 May 20 2016	
Maximum user count:	60000	Remaining Capacity: 60000
Maximum fingerprint count:	20000	Remaining Capacity: 20000
Maximum log count:	100000	
MAC Address:	00:17:61:D0:FA:32	
IP Address:	192.168.1.129	
Subnet Mask:	255.255.255.0	
Gateway:	192.168.1.254	
Primary DNS:		
TCP Port:	14370	
HTTP Port:	80	

4.5 Connect to ZKBioSecurity Software

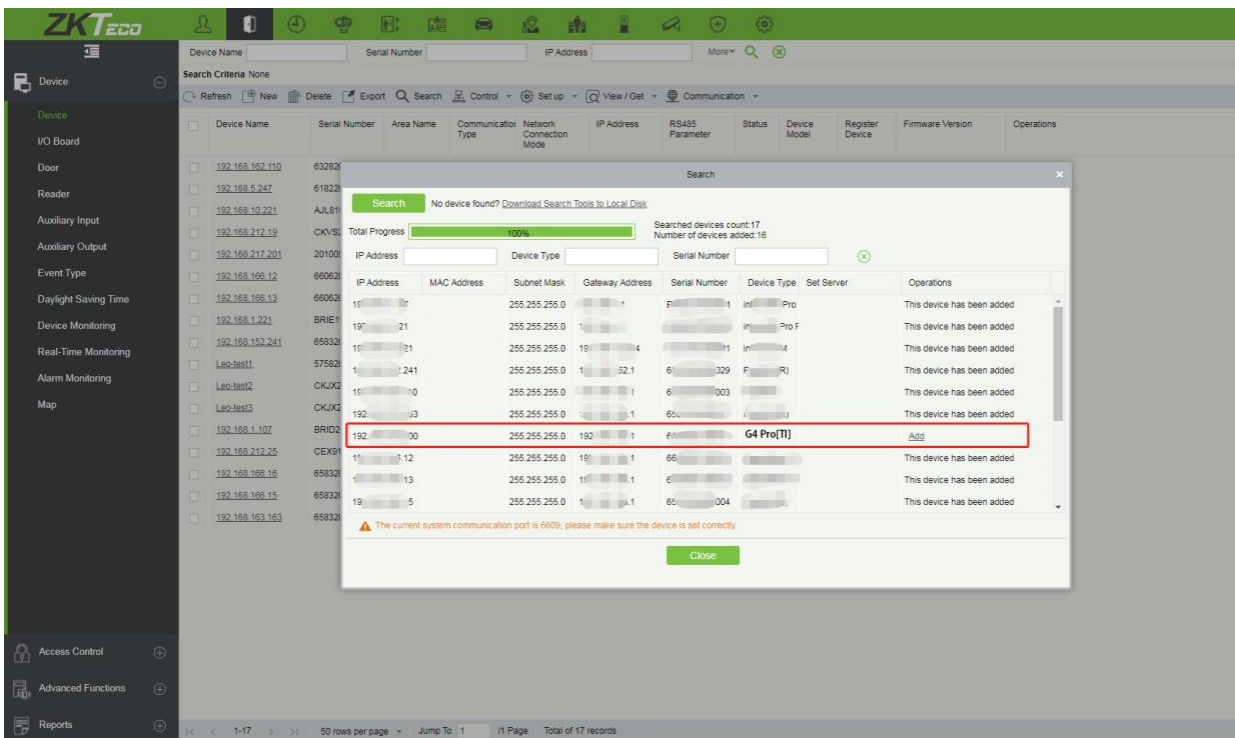
Login to ZKBioSecurity software, click **System** > **Communication** > **Communication Monitor** to set the ADMS Service Port, as shown in the figure below:



4.6.1 Add Device on the Software

Add the device by searching. The process is as follows:

1. Click **Access** > **Device** > **Search**, to open the Search interface in the software.
2. Click **Search**, and it will prompt [**Searching**,.....].
3. After searching, the list and total number of access controllers will be displayed.

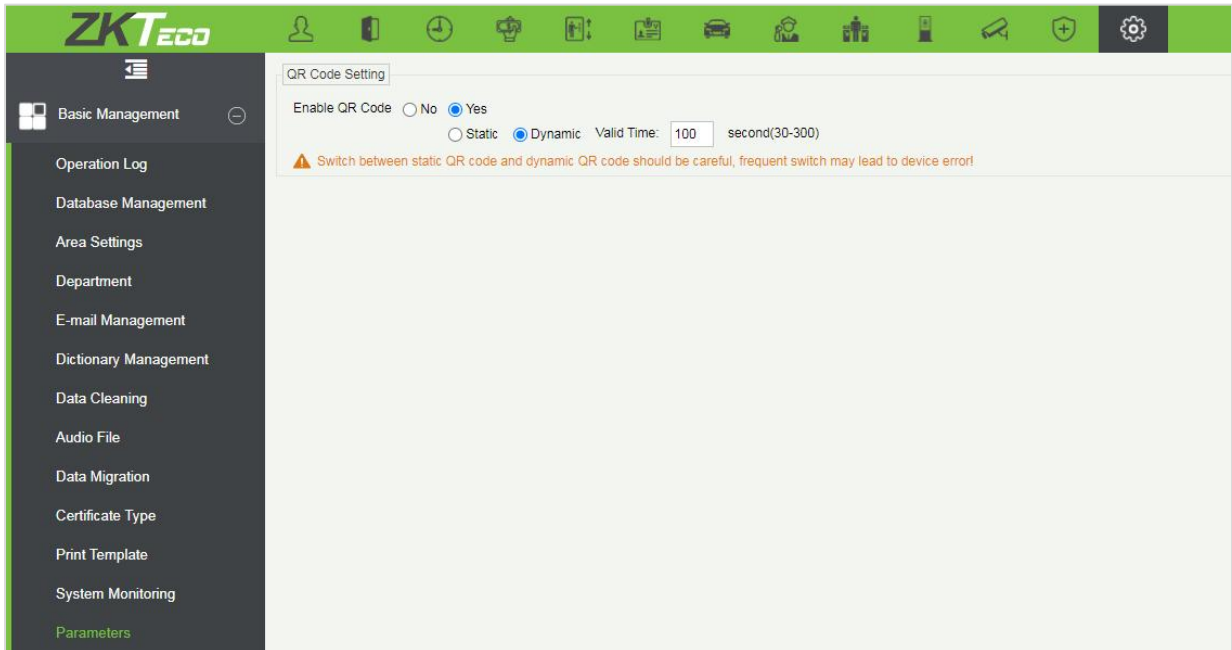


4. Click [**Add**] in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click [**OK**] to add the device.

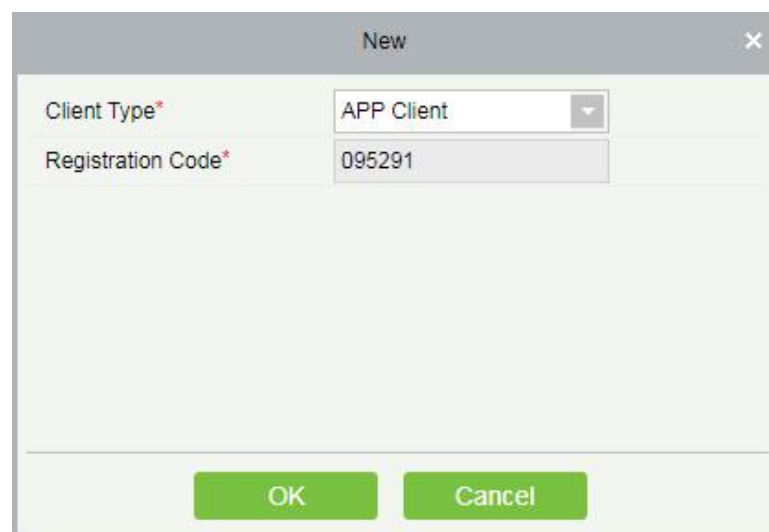
4.6.2 Mobile Credential

After downloading and installing the App, the user needs to set the Server before login. The steps are given below:

1. In **[System] > [Basic Management] > [Parameters]**, set **Enable QR Code** to "Yes", and select the QR code status according to the actual situation. The default is **Dynamic**, the valid time of the QR code can be set.

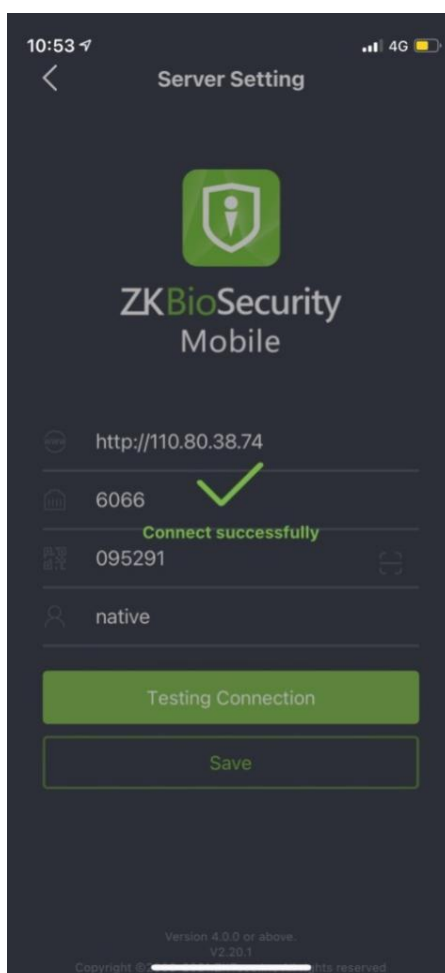


2. On the Server, choose **[System] > [Authority Management] > [Client Register]** to add a registered App client.



Registration Code	Client name	Registration Key	Activator	Activated Date	Creation Date	Client Type	Operations
<input checked="" type="checkbox"/> 095291			+		2021-04-27 10:50:14	APP Client	Delete Register QR-code
<input type="checkbox"/> 97B4EB	Julia		✓	2021-04-26	2021-04-25 17:03:33	APP Client	Delete Register QR-code
<input type="checkbox"/> 74231C			✓	2021-04-25	2021-04-25 15:10:59	APP Client	Delete Register QR-code
<input type="checkbox"/> A25536	Vanessa		✓	2021-04-23	2021-04-23 10:38:19	APP Client	Delete Register QR-code
<input type="checkbox"/> A55A1D			✓	2021-04-23	2021-04-23 10:38:19	APP Client	Delete Register QR-code

- Open the App on the Smartphone. On the login screen, tap [**Server Setting**] and type the IP Address or the Domain Name of the Server, and its Port Number.
- Tap the **QR Code** icon to scan the QR code of the new App client. After the client is identified successfully, set the Client Name and tap [**Connection Test**].
- After the network is connected successfully, tap [**Save**].



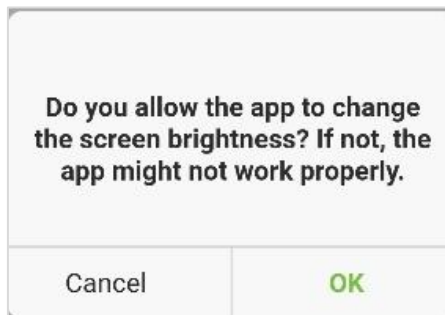
The Mobile Credential function is only valid when logging in as an employee, tap on Employee to switch to Employee Login screen. Enter the Employee ID and Password (Default: 123456) to login.

- Tap [**Mobile Credential**] on the App, and a QR code will appear, which includes employee ID and card number (static QR code only includes card number) information.

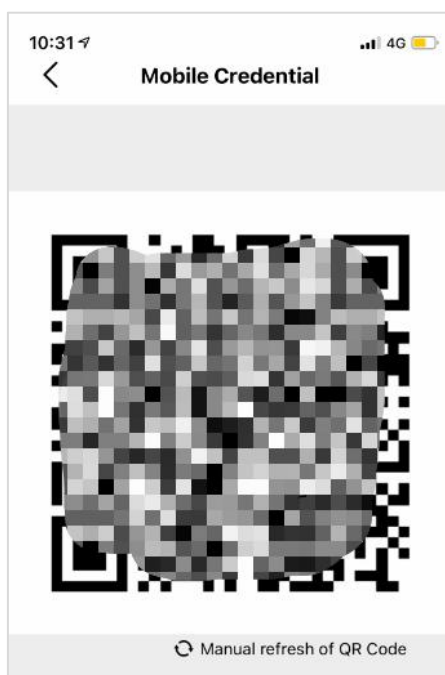
The QR code can replace a physical card on a specific device to achieve contactless authentication to open the door.



When using this function for the first time, the App will prompt to authorize the modification of screen brightness settings, as shown in the figure:



The QR code is automatically refreshed for every 30s, and it also supports manual refresh.



NOTE: For other specific operations, please refer to ***ZKBioSecurity Mobile App User Manual.***

5 Privacy Policy

Notice:

To help you better use the products and services of ZKTeco and its affiliates, hereinafter referred as “we”, “our”, or “us”, the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

- 1. User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.
- 2. Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**
2. All the functions of displaying the biometric information are disabled in our products by default.

You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**
4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**
5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.
6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

6 Eco-friendly Operation



The product's "eco-friendly operational period" refers to the time period during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down, and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

Green Label

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com

