User Manual

C3-X00 Plus Series

Date: October 2024

Doc Version: 1.1

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zkteco.com.

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or

relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/ unit/ equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.com.

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face template-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of the **C3-X00 Plus Series**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**.
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>.
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/ Folder].

Symbols

Convention	Description
	This implies about the notice or pays attention to, in the manual.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

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 Overview

2.1 Introduction

ZKTeco's C3 Plus series is an IP-based controller offering RFID cards and dynamic QR code authentication for access control solutions.

The C3 Plus series includes three models: C3-100 Plus, C3-200 Plus, and C3-400 Plus. This series is designed for small-to medium-sized enterprises and can handle up to 100,000 multi-tech card users and 100,000 dynamic QR code transactions.

The C3 Plus series has RS-485 interfaces, which ZKTeco's RS-485 protocols and OSDP (Ver 2.1.7) for accessing card readers. It is also compatible with ZKTeco's QR code reader, including QR50, QR500, and QR600. C3 Plus series is highly versatile, with the Wiegand interface (Wiegand format: W26/ W34/W66) for seamless integration with third-party access control readers.

The C3 Plus Series levels up data storage encryption by AES 256-bit algorithm. Also, C3 Plus Series adopts the AES 128-bit algorithm encryption to ensure the communication between controller, readers and I/O expansion boards secure. Also, the C3 Plus Series support HTTPS / TLS1.2 protects communications between the server and the web client.

2.2 Features

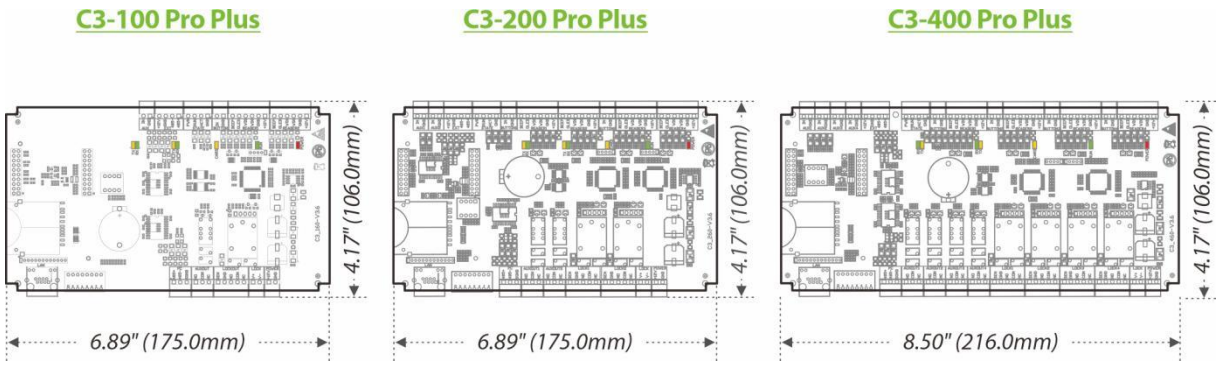
- Access points capacity: 1 / 2 / 4 Access Points.
- Multiple Authentication Methods: RFID Cards / Dynamic QR Code / Password.
- Optimal Capacity for small to medium enterprise. Supports 100,000 QR Code capacity and 100,000 RFID card capacity.
- Features ZKTeco's RS-485 protocols and OSDP (Ver 2.1.7) for connecting card readers, and it is compatible with ZKTeco's QR code readers such as QR50, QR500, and QR600.
- Highly versatile with Wiegand interfaces (Input) for integrating with third party card reader equipped with Wiegand interface (Wiegand format W24/W34/W66).
- Supports the I / O expansion board, EX0808 with 8 inputs and 8 outputs (via RS-485 connection).
- Supports firmware protocol access control push and compatible with ZKBio CVAccess.

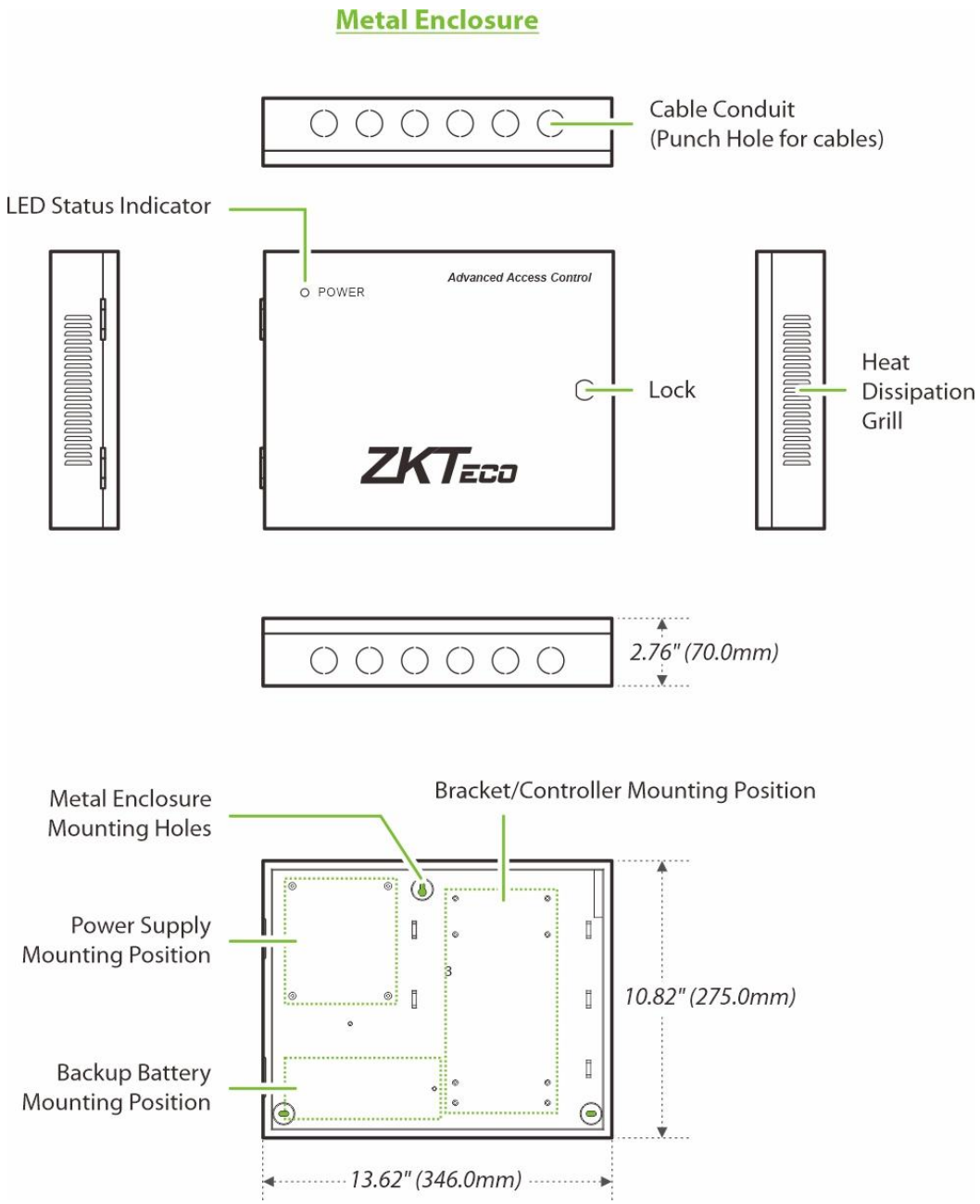
2.3 Specifications

Model	C3-100 Plus	C3-200 Plus	C3-400 Plus
Operation System	Linux OS		
Hardware	CPU: Single Core @ 1.0GHz RAM: 128MB; ROM: 256MB		
Authentication Method	Card / Password / QR Code		
Access Point Capacity	1 Access Point	2 Access Point	4 Access Point
Reader Capacity	2*RS-485 Readers (ZKTeco RS-485 / OSDP), 2* 26 / 34 / 66 bit Wiegand Readers	4*RS-485 Readers (ZKTeco RS-485 / OSDP), 4* 26 / 34 / 66 bit Wiegand Readers	8*RS-485 Readers (ZKTeco RS-485 / OSDP), 4* 26 / 34 / 66 bit Wiegand Readers
IO Expansion Board Capacity	8pcs EX0808 (RS-485 connection)		
User Capacity	100,000		
Card Capacity	100,000 (1:N) (Standard)		
QR Code Capacity	100,000 (Static QR Code / Dynamic QR Code)		
Transaction Capacity	500,000 (Standard)		
Number of Inputs	1 * Exit Button, 1 * Door Status, 1 * AUX Inputs or 64 (with 8pcs of EX0808 IO expansion board)	2 * Exit Button, 2 * Door Status, 2 * AUX Inputs or 64 (with 8pcs of EX0808 IO expansion board)	4 * Exit Button, 4 * Door Status, 4 * AUX Inputs or 64 (with 8pcs of EX0808 IO expansion board)
Number of Outputs	1*Form C Relay forLock, 1*Form C Relay for Aux Output or 64 (with 8pcs of EX0808 IO expansion board)	2*Form C Relay forLock, 2*Form C Relay for Aux Output or 64 (with 8pcs of EX0808 IO expansion board)	4*Form C Relay forLock, 4*Form C Relay for Aux Output or 64 (with 8pcs of EX0808 IO expansion board)
Max. Card Length	Supports up to 66 bits Card Length		
QR Code	QR code, PDF417, Data Matrix, MicroPDF417, Aztec scanning in third-party development projects. Dynamic QR codes on the ZKBio CVAccess mobile application.		
Communication	TCP/IP *1 RS-485: ZKTeco RS-485/OSDP *1 Wiegand (Input)*1 USB: Type A (USB Drive Only)*1 Aux Inputs *1, Aux Outputs *1, Electric Lock*1, Door Sensor*1, Exit Button*1, Alarm*1	TCP/IP *1 RS-485: ZKTeco RS-485/OSDP *1 Wiegand (Input)*1 USB: Type A (USB Drive Only)*1 Aux Inputs *2, Aux Outputs *2, Electric Lock*2, Door Sensor*2, Exit Button*2, Alarm*2	TCP/IP *1 RS-485: ZKTeco RS-485/OSDP *1 Wiegand (Input)*1 USB: Type A (USB Drive Only)*1 Aux Inputs *4, Aux Outputs *4, Electric Lock*4, Door Sensor*4, Exit Button*4, Alarm*4

Standard Functions	Webserver, Upto 14-digit User ID, Access Levels, Access Groups, Holidays, Anti-passback, Anti-tailgating, Linkage, Global Linkage, Multiple Verification Methods		
Access Control Interface	Wiegand (Card Reader) RS-485 (RS-485 Card Reader / QR Code Reader)		
Power Supply	9.6V - 14.4V DC		
Operating Temperature	0°C to 45°C		
Operating Humidity	20% to 80% RH (Non-condensing)		
Dimensions (mm)	175 mm*99 mm*19.3 mm (L*W*H)	175 mm*99 mm*19.3 mm (L*W*H)	215.88 mm*99.14 mm*19.3 mm(L*W*H)
Gross Weight	0.263 Kg	0.296 Kg	0.357 Kg
Net Weight	0.158 Kg	0.190 Kg	0.252 Kg
Supported Software	ZKBio CVAccess		
Installation	Supported Wall-mount with Metal Enclosure (Optional)		
Enclosure (Optional)	Size: 350 mm*90 mm*300 mm (L*W*H) Material: SPCC steel Power Supply Unit: input 110V~240V AC, output 12V 4A+1A DC Backup Battery: Space reserved [Recommended Backup Battery size: 151 x 94 x 65 mm (L*W*H)] Gross Weight: 3.35Kg	Size: 350 mm*90 mm*300 mm (L*W*H) Material: SPCC steel Power Supply Unit: input 110V~240V AC, output 12V 4A+1A DC Backup Battery: Space reserved [Recommended Backup Battery size: 151 x 94 x 65 mm (L*W*H)] Gross Weight: 3.35Kg	Size: 350 mm*90 mm*300 mm (L*W*H) Material: SPCC steel Power Supply Unit: input 110V~240V AC, output 12V 4A+1A DC Backup Battery: Space reserved [Recommended Backup Battery size: 151 x 94 x 65 mm (L*W*H)] Gross Weight: 3.56Kg
Certifications	ISO14001, ISO9001, CE, FCC, RoHS		
Factory ID	AC02-C11H-U10	AC02-C12H-U10	AC02-C14H-U10

2.4 Dimension





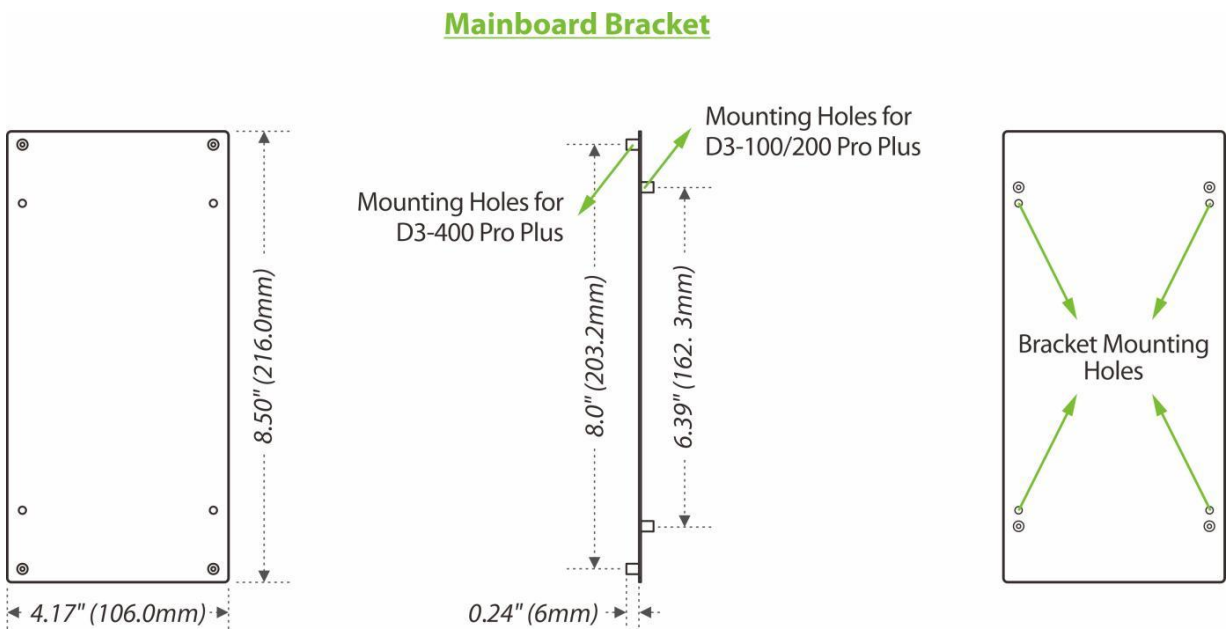


Figure 2-1 Product Appearance

2.5 Control Panel Indicators

When the C3-100/200/400 Plus 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): Reader 485 communication indicator, indicates sending of 485 data if it flashes;
- EXT RS485 (RX) indicator (green): Reader 485 communication indicator, indicates receiving of 485 data if it flashes;
- PC RS485 (TX) indicator (yellow): PC485 communication indicator, indicates sending of 485 data if it flashes;
- PC RS485 (RX) indicator (green): PC485 communication indicator, indicates receiving of 485 data if it flashes;
- CARD indicator (yellow): indicates input of Wiegand signal if it is lit.

Indicator Diagram:

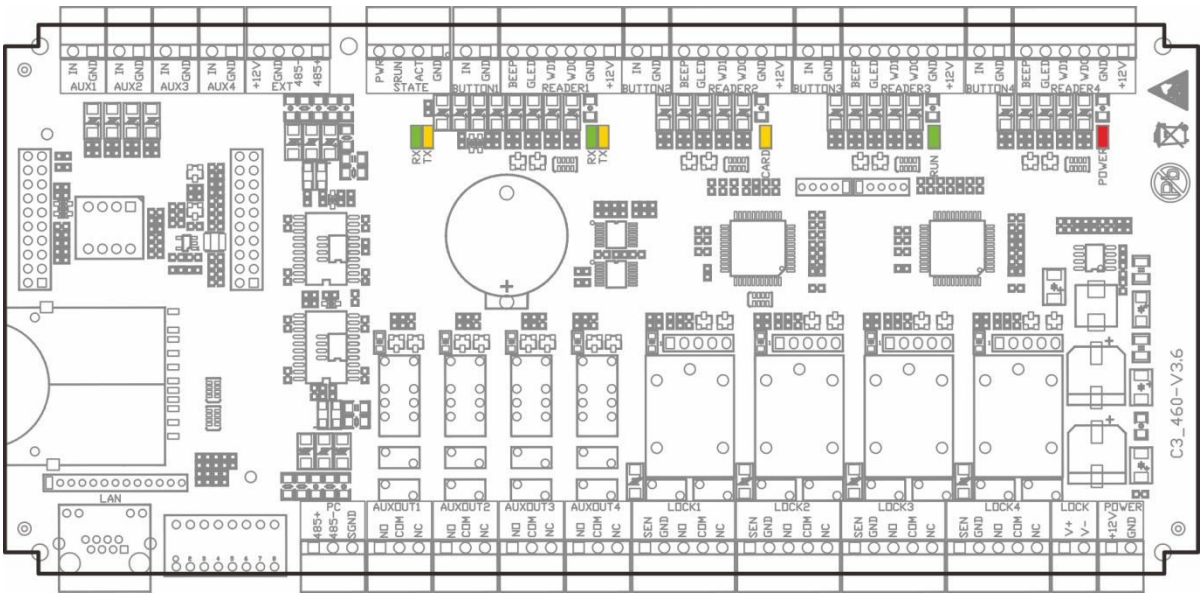


Figure 2-2 Indicators in the InBio460 Pro

3 Installation and Connection

Ensure that the device is installed following the provided installation instructions. Failure to do so may result in voiding of the devices warranty.

3.1 Installing the metal enclosure on the wall

1. According to the mounting holes position of the metal enclosure. Drill three mounting holes in a suitable spot on the wall and make sure it is about **114 inches (2.9m)** above the ground, which can be adjusted according to actual needs. Take care to leave at least **3.937 inches (100 mm)** on the left side of the metal enclosure.
2. Place the Anchors in the mounting holes.
3. Then f ix the metal enclosure with the self-tapping screws as shown below.

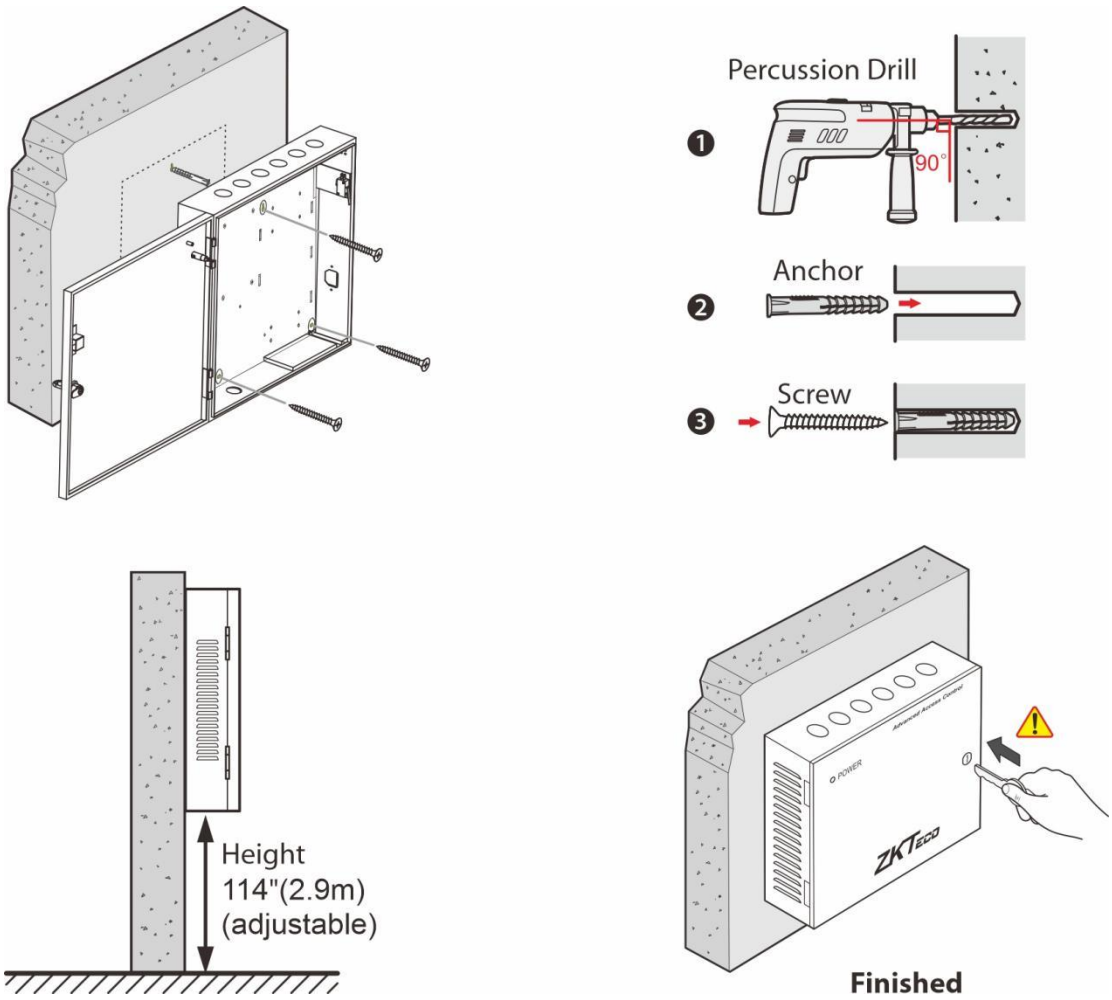


Figure 3-1 Installation the metal enclosure on the wall

Note: *The metal enclosure is equipped with an tamper alarm switch. When it is working normally, please keep the enclosure closed.*

3.2 Installation of access control panel wires

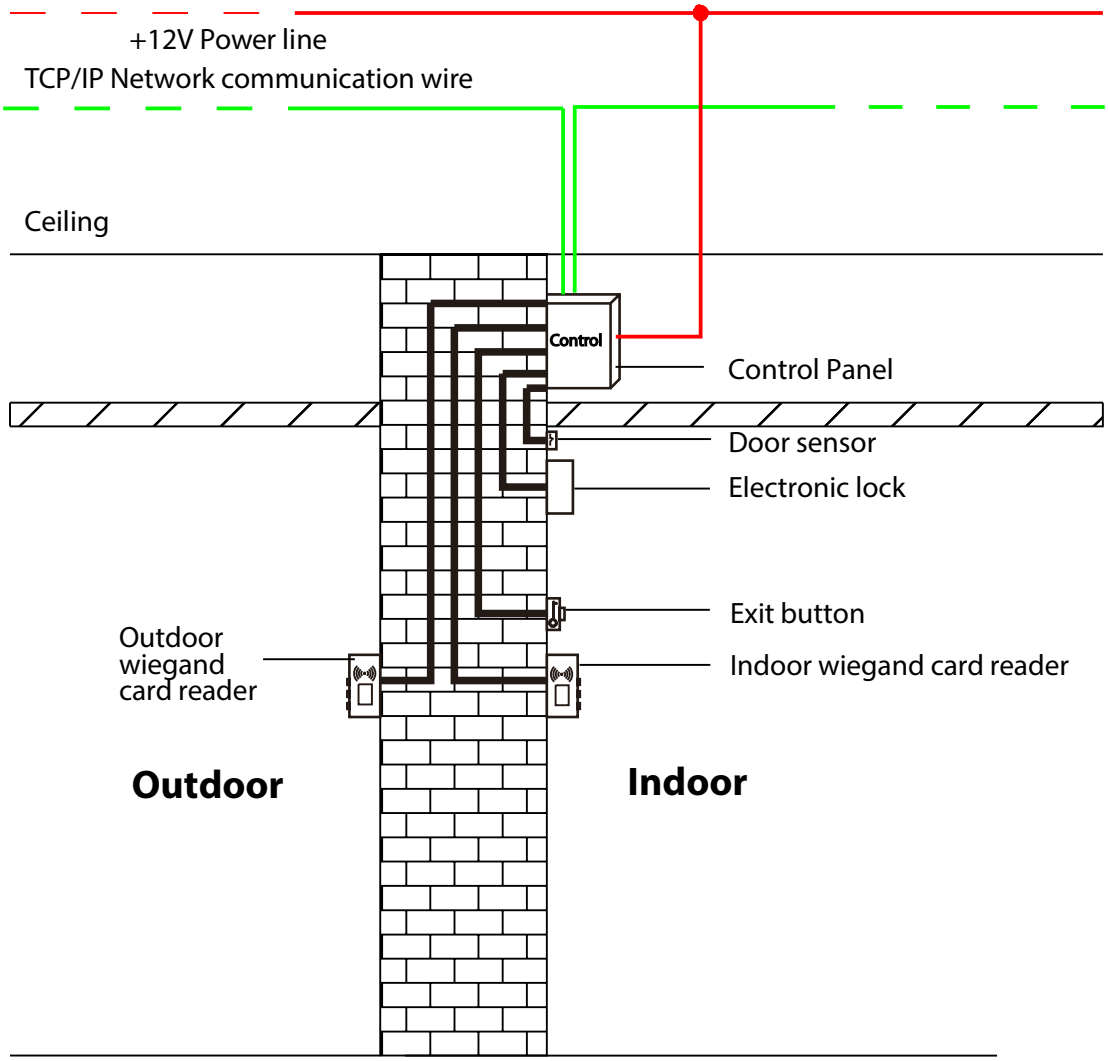


Figure 3-2 Access Control Panel Wire Installation Diagram

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 Controller System Installation

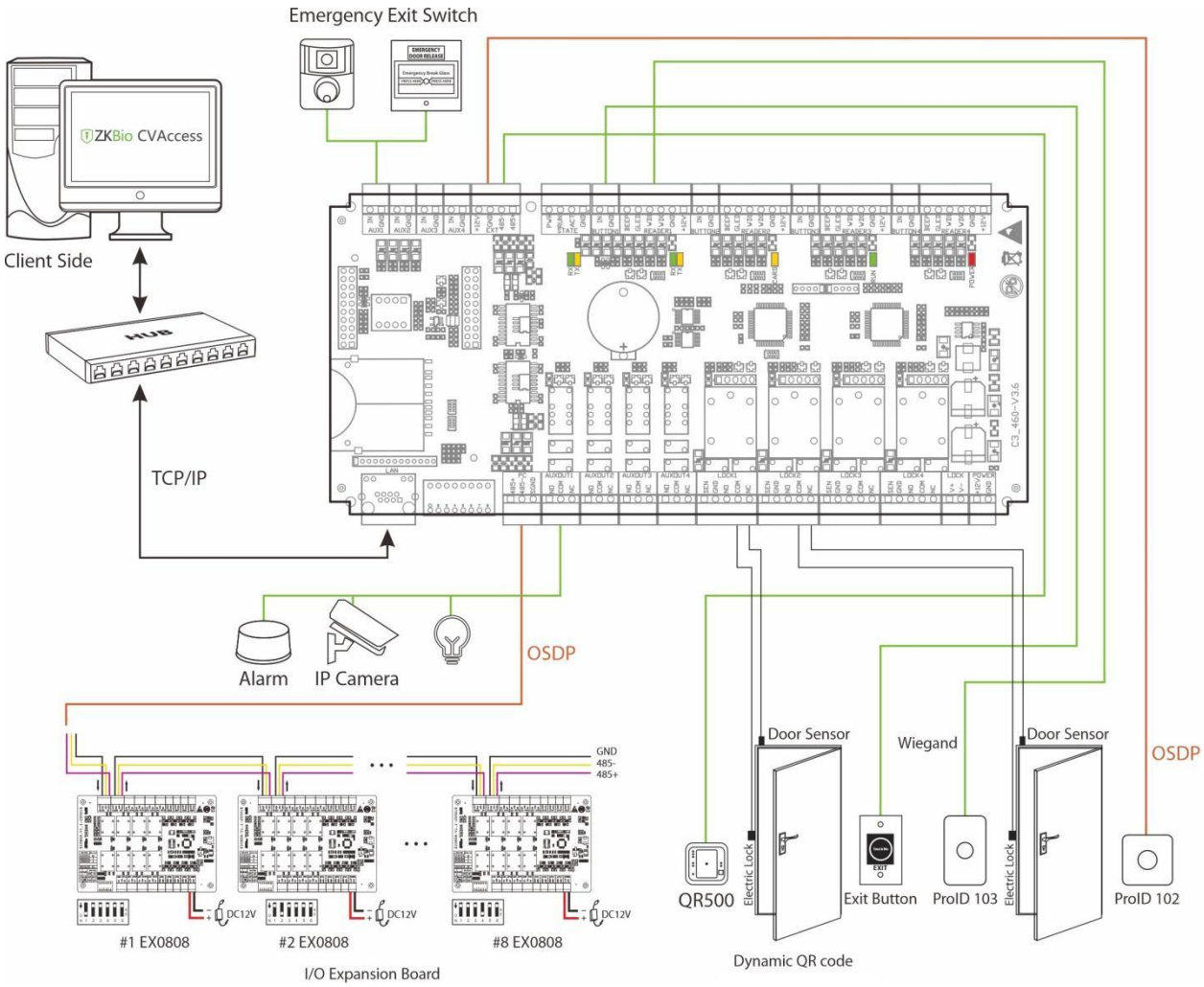


Figure 3-3 Schematic Diagram of System Installation

Notes:

- *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 Access Control Operator Panel System Power Supply Structure

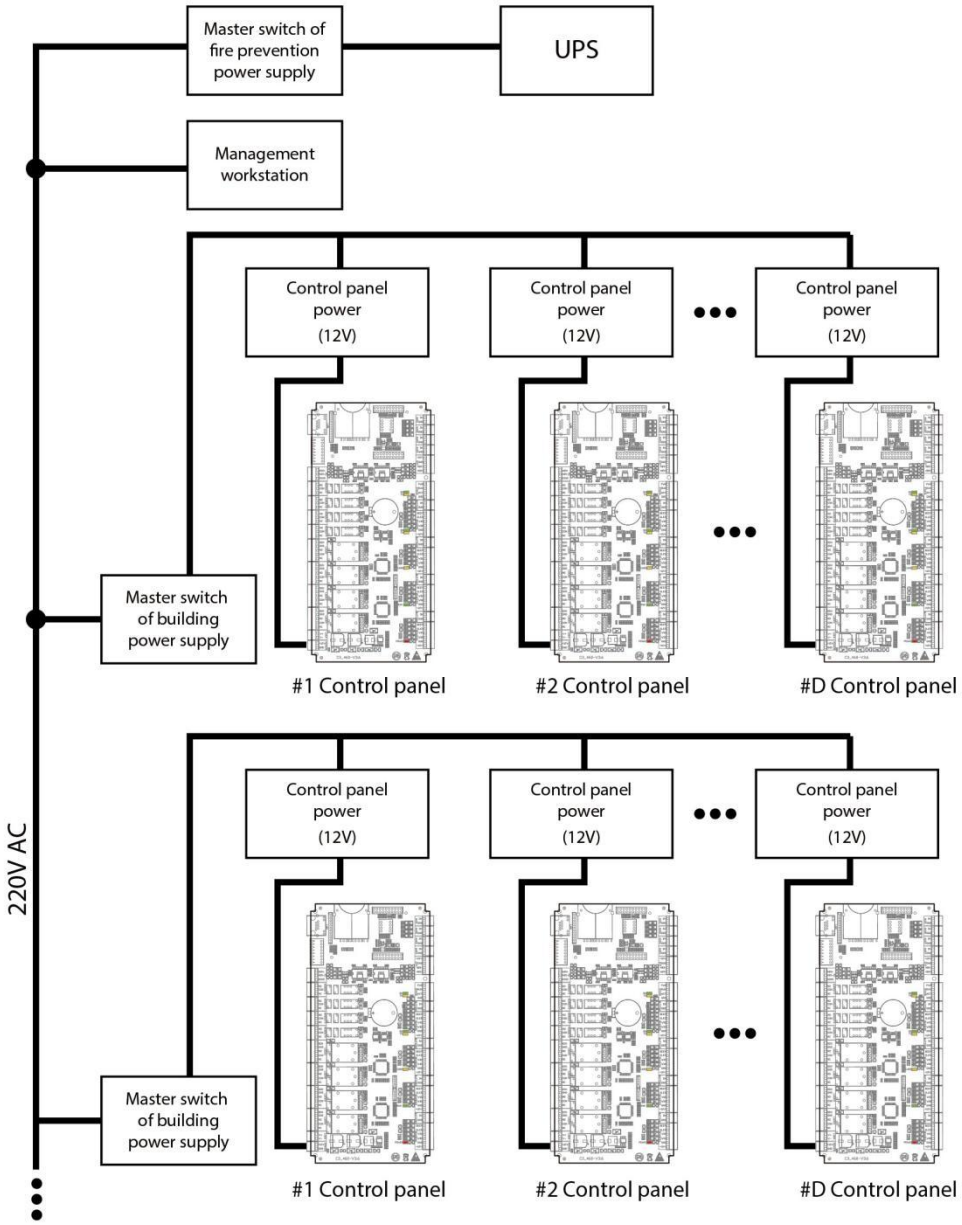


Figure 3-4 Access Controller System Power Supply

Remarks:

- *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 Terminal and Wiring Description

4.1 Terminal Description

4.1.1 C3-100 Plus

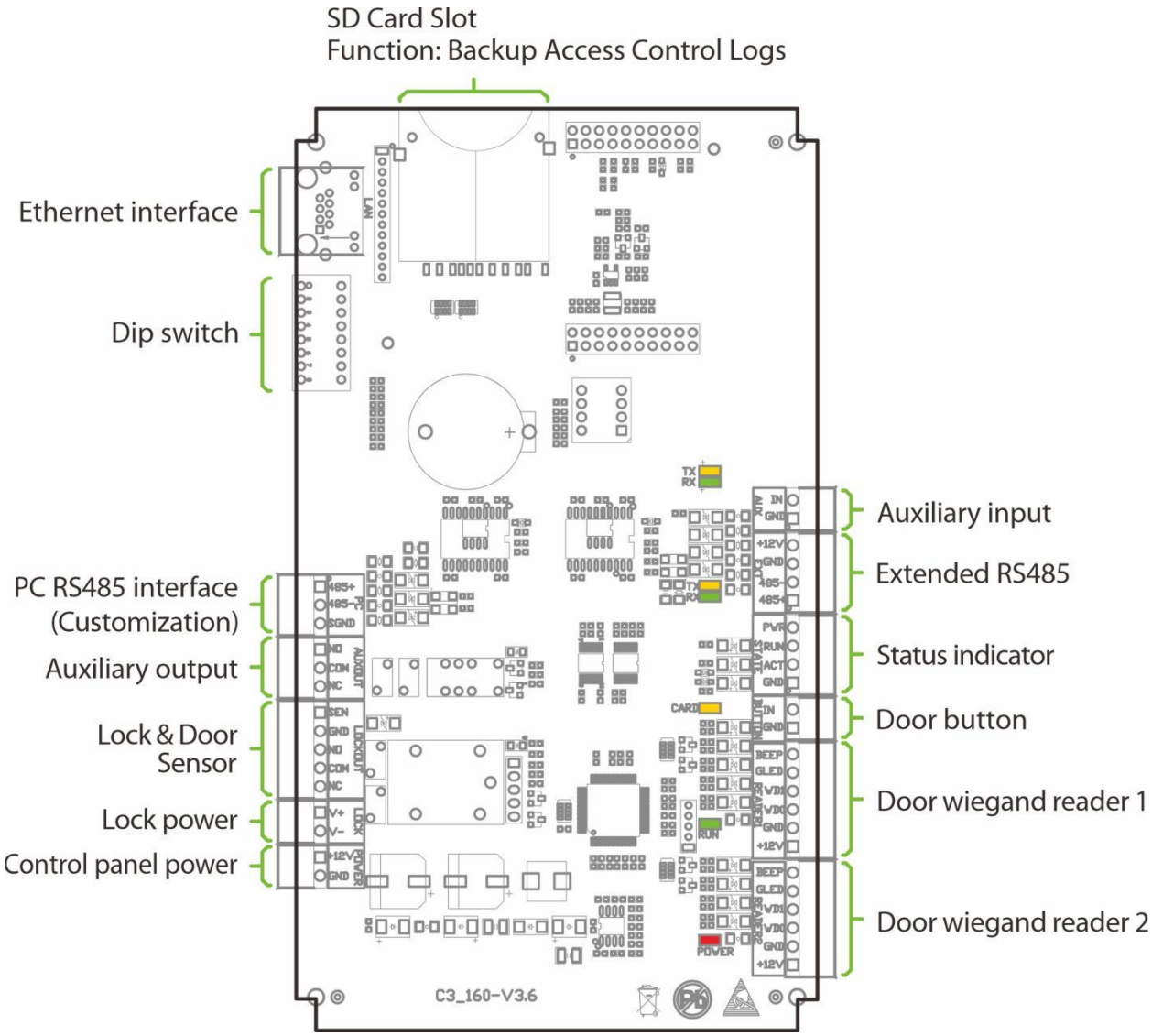


Figure 4-1 C3-100 Plus terminal description

4.1.2 C3-200 Plus

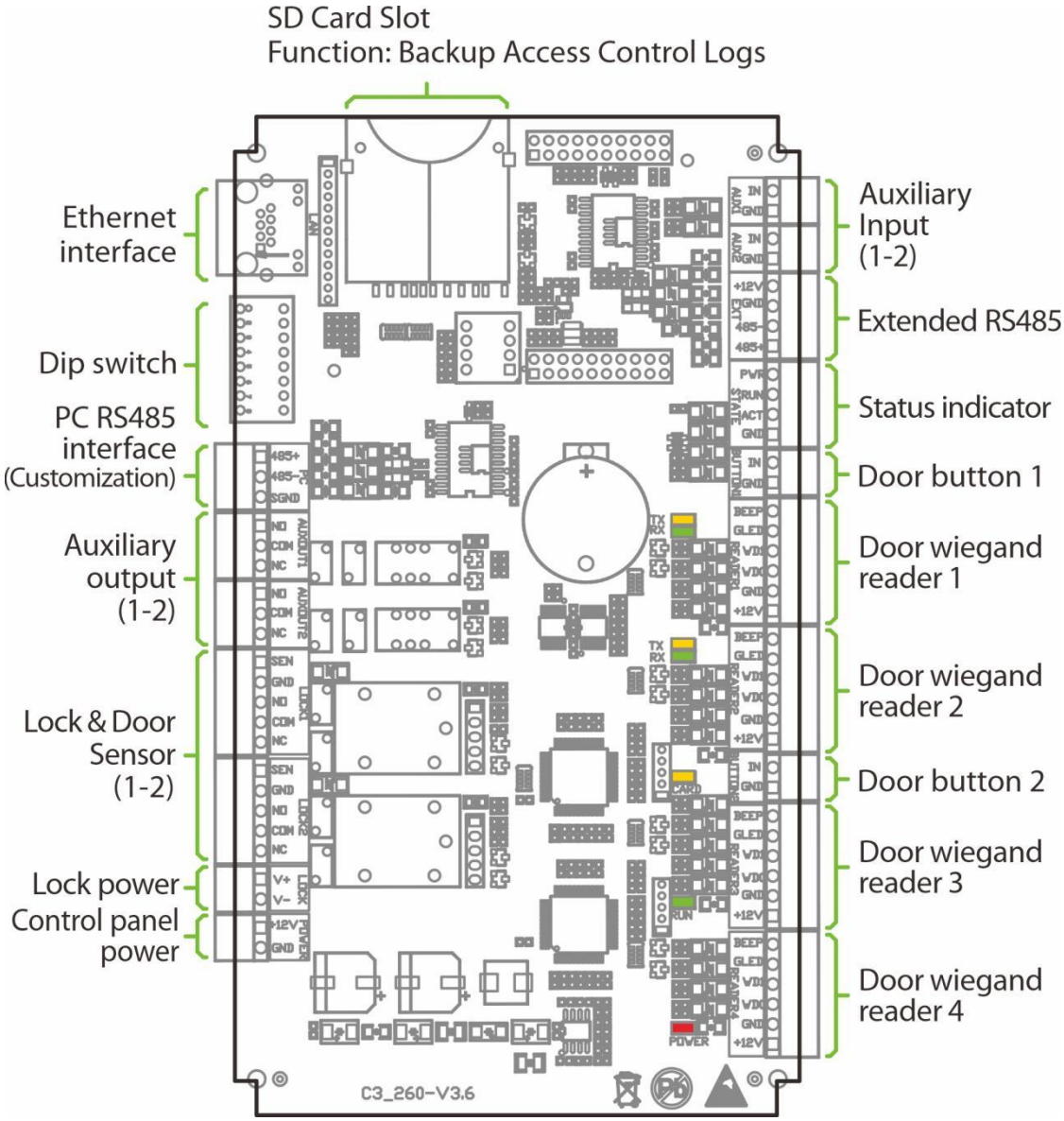


Figure 4-2 C3-200 Plus terminal description

4.1.3 C3-400 Plus

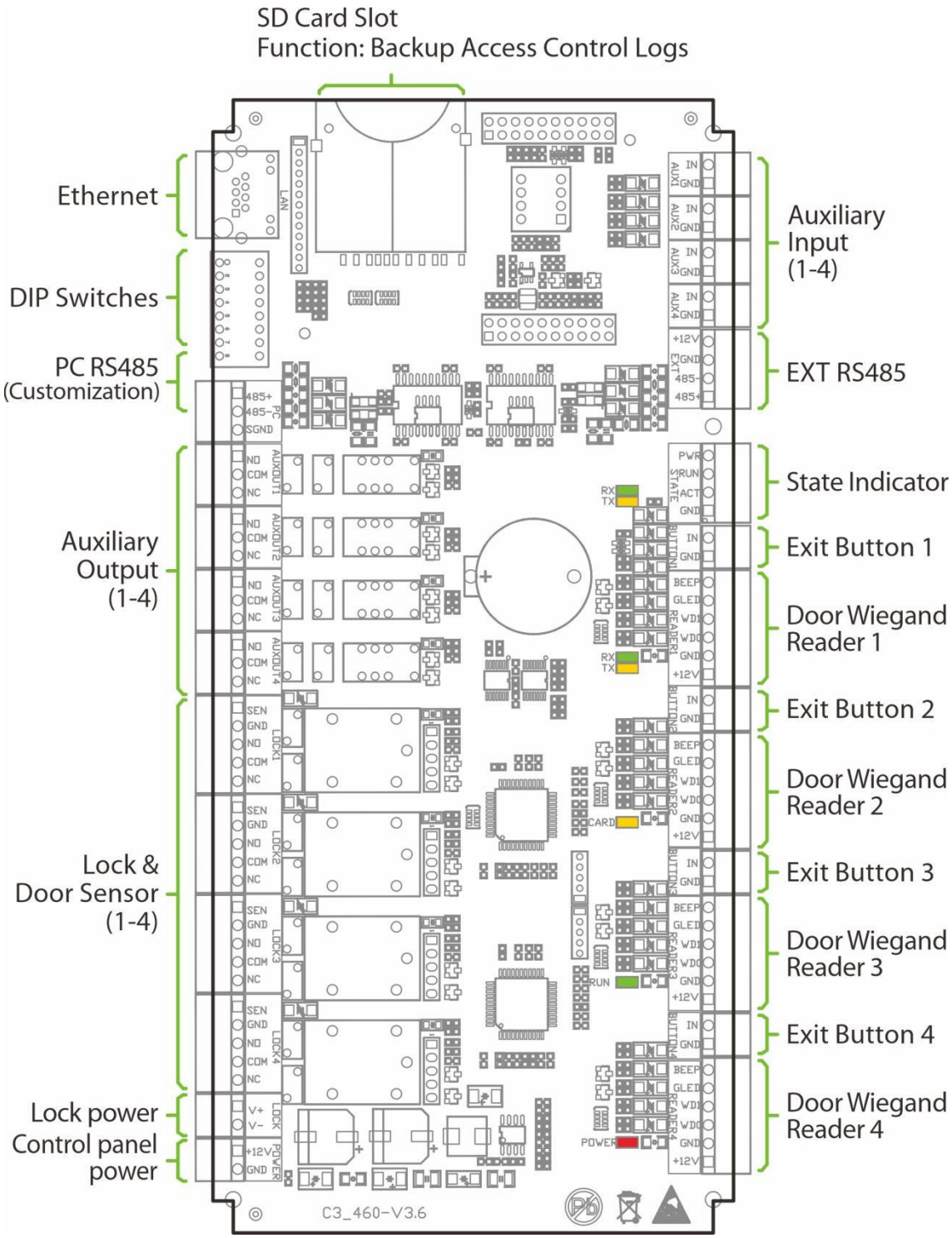


Figure 4-3 C3-400 Plus terminal description

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 EXT RS485 Reader port can be connected externally to RS485 reader.
4. The PC RS485 communication port can be externally connected to EX0808 expansion board (for customized function, please contact your dealer if needed).
5. 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. Supports connection of 32GB SD card.

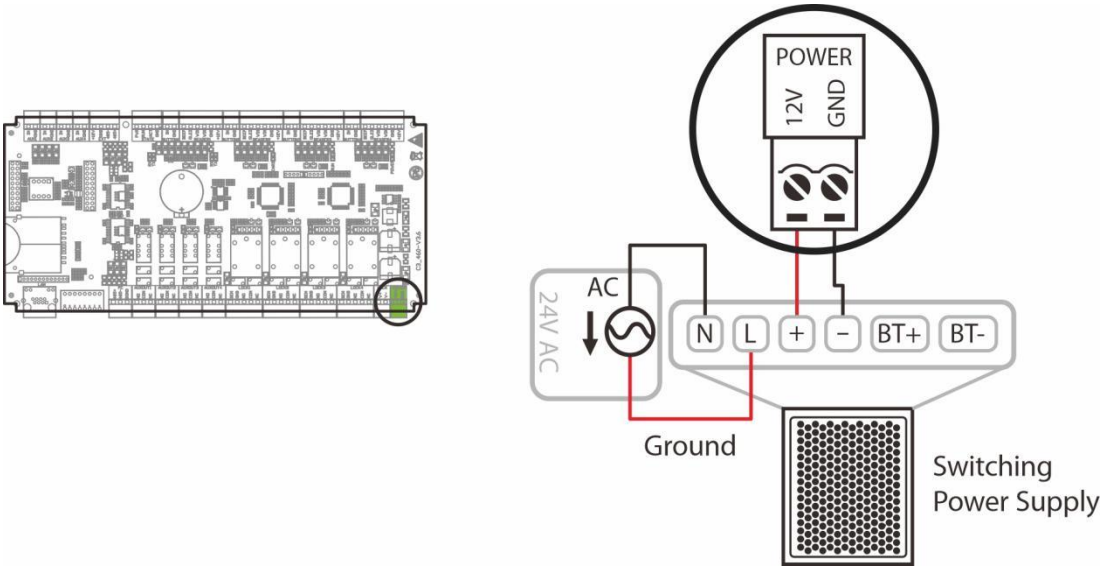
Ports of C3-100/200/400 Plus Control Panel:

No.	Functional Port	C3-100 Plus	C3-200 Plus	C3-400 Plus
1	**Number of doors controller**	1	2	4
2	**Wiegand card reader interface**	2	4	4
3	**Exit button**	1	2	4
4	**Control lock relay**	1	2	4
5	**Door sensor**	1	2	4
6	**Extension input**	1	2	4
7	**Extension output**	1	2	4
8	**TCP/IP**	✓	✓	✓
9	**RS485 extension communication**	✓	✓	✓
10	**PC485 communication**	Customization	Customization	Customization

4.2 Wiring Description

4.2.1 Power Wiring

- **Without Backup Battery**



- **With Backup Battery**

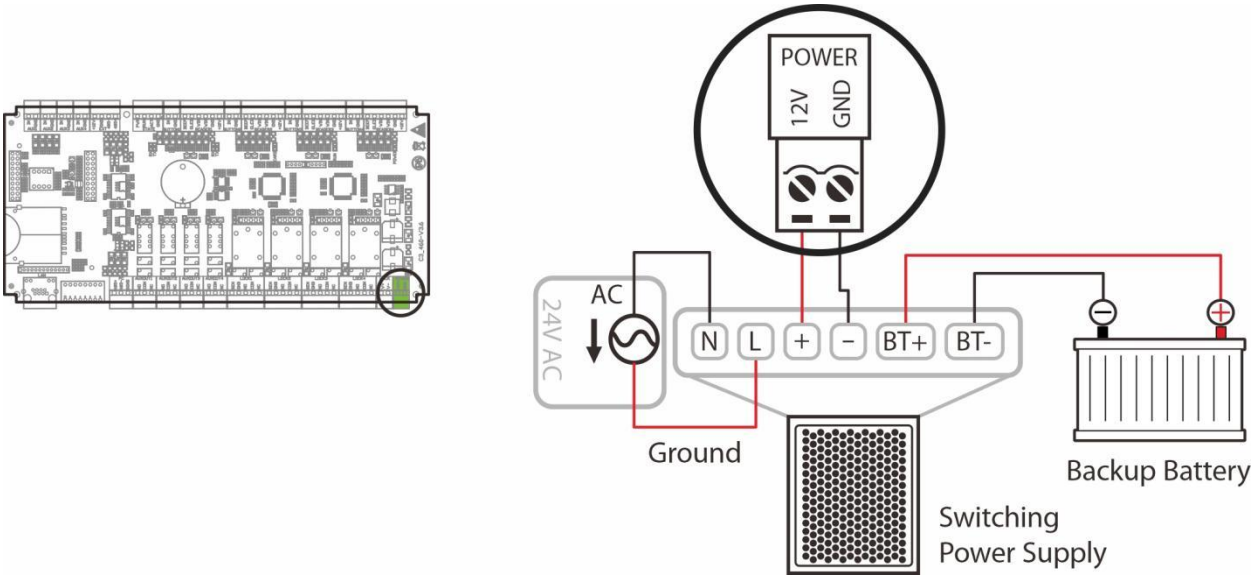


Figure 4-4 Power supply wiring diagram

4.2.2 Network Wiring

Establish the connection between the device and the software using an Ethernet cable. An illustrative example is provided below:

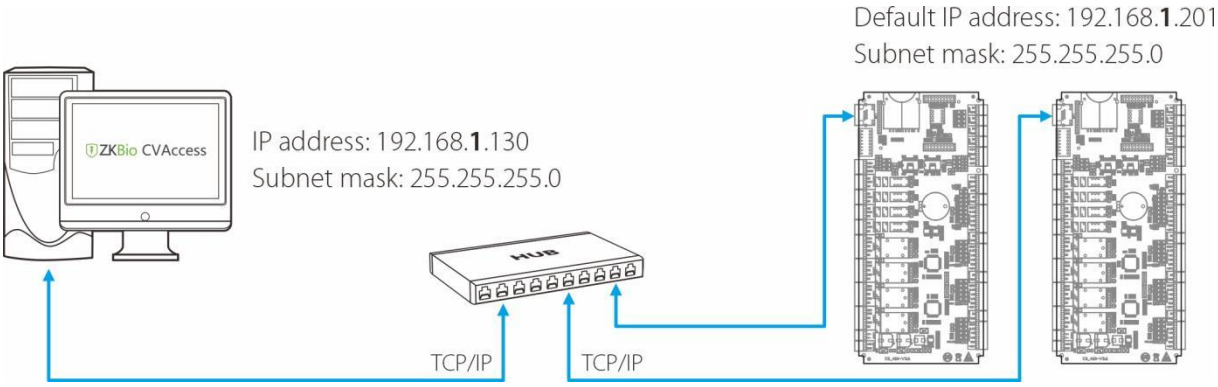


Figure 4-5 Network wiring diagram

Note:

- *In LAN, IP addresses of the server (PC) and the device must be in the same network segment when connecting to the software.*

4.2.3 Wiegand Reader Wiring

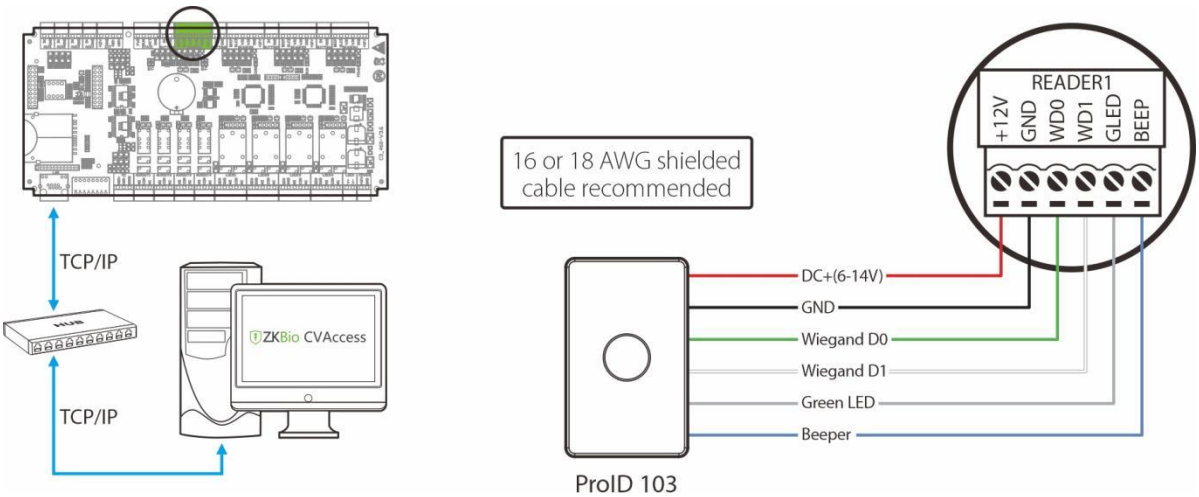


Figure 4-6 Wiegand reader wiring diagram

The C3-100 Plus can connect two Wiegand readers in the one-door two-way mode. The C3-200 Plus provides four readers, which can be connected in the two-door two-way mode. The C3-400 Plus 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 C3 Plus 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.

- **The following Wiegand reader models are supported for connection:**

Reader Model	Wiegand26/34	Wiegand66
KR100/101/102E/M	✓	✕
KR200/201/202E/M	✓	✕
KR310	✓	✕
KR500E/501M/502E/M/503E	✓	✕
KR600/601/602E/M	✓	✕
KR610/611/612E	✓	✕
KR610/611/612D	✓	✓
KR610/611/612DL	✓	✓
ProID10/20/30/40 E/M	✓	✕
ProID10/20/30/40 D	✓	✓
ProID20/30BEMD-RS	✓	✓

Remarks: ✓ *indicates support,* ✕ *indicates no support.*

4.2.4 Auxiliary Input Wiring

The C3-100 Plus provides one auxiliary input interface; the C3-200 Plus provides two and the C3-400 Plus 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 refer to the relevant user manual for details. The following is an example of wiring with fire alarm only.

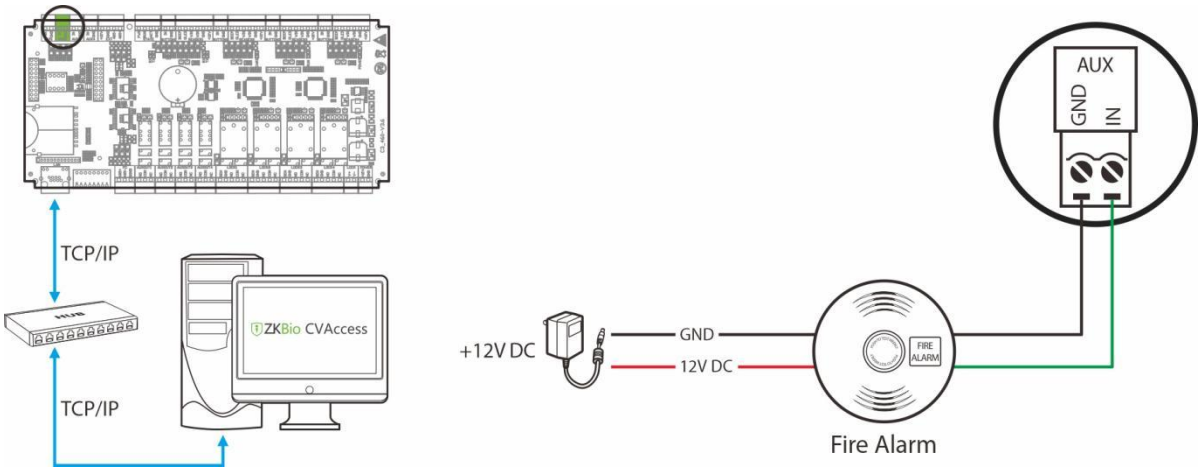


Figure 4-7 Auxiliary input wiring diagram

4.2.5 Auxiliary Output Wiring

The C3-100 Plus has two relays (one used as control lock by default, and the other one used as auxiliary output); the C3-200 Plus has four relays (two used as control locks by default, and the other two used as auxiliary outputs); the C3-400 Plus 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. The following is an example of wiring with alarm only.

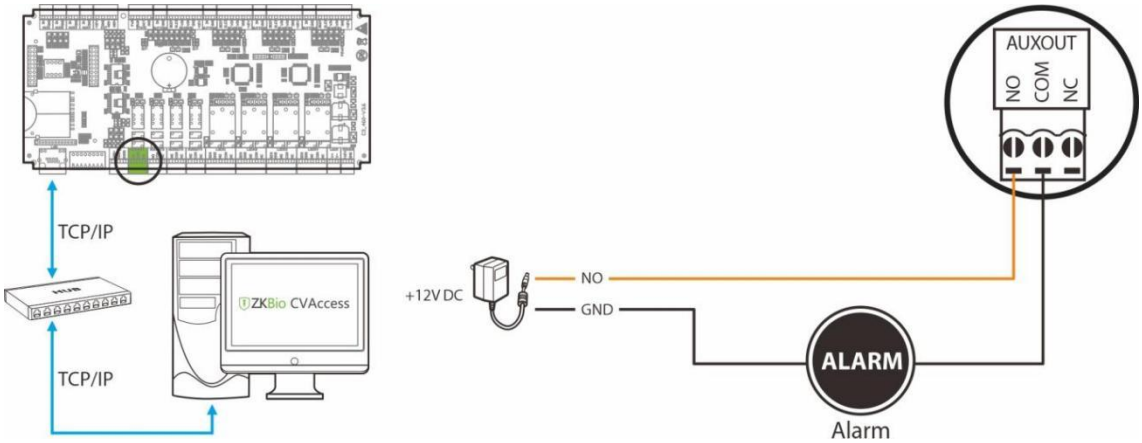


Figure 4-8 Auxiliary output wiring diagram

4.2.6 Exit Button Wiring

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 0.3mm^2 as the connection wire between an exit switch and the Control panel.

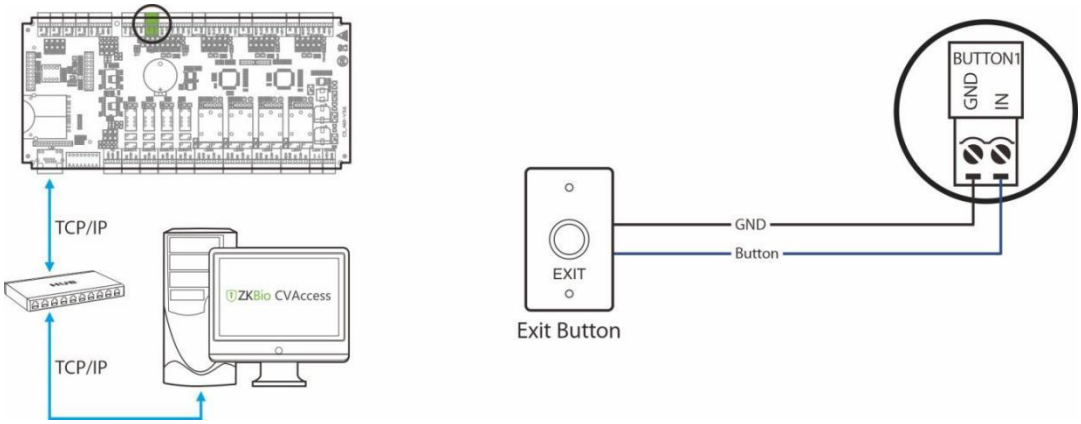


Figure 4-9 Exit button supply wiring diagram

4.2.7 RS485 Reader Wiring

The C3-100 Plus can connect two RS485 readers in the one-door two-way mode. The C3-200 Plus provides four readers, which can be connected in the two-door two-way mode. The C3-400 Plus provides four readers, which can be connected in the two-door two-way or four-door two-way mode.

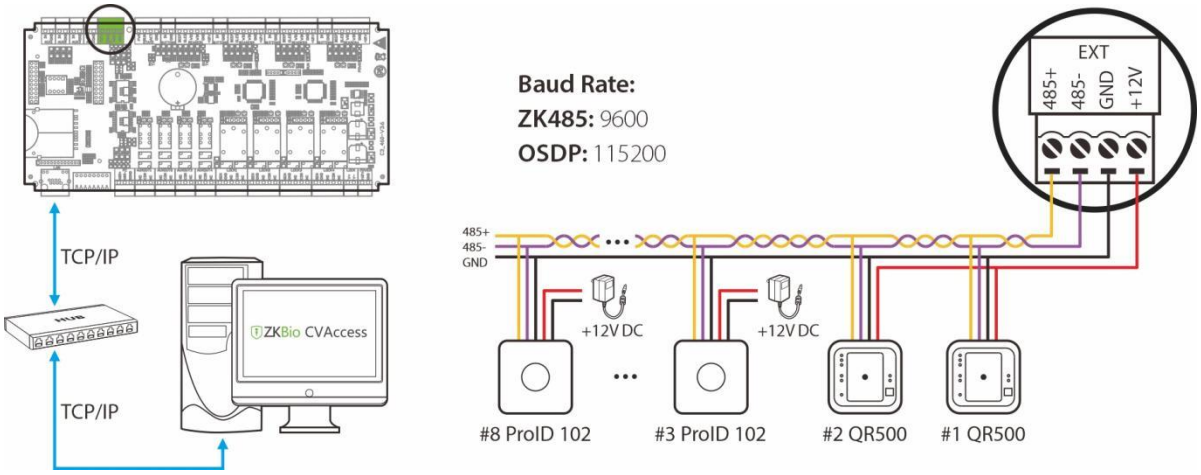


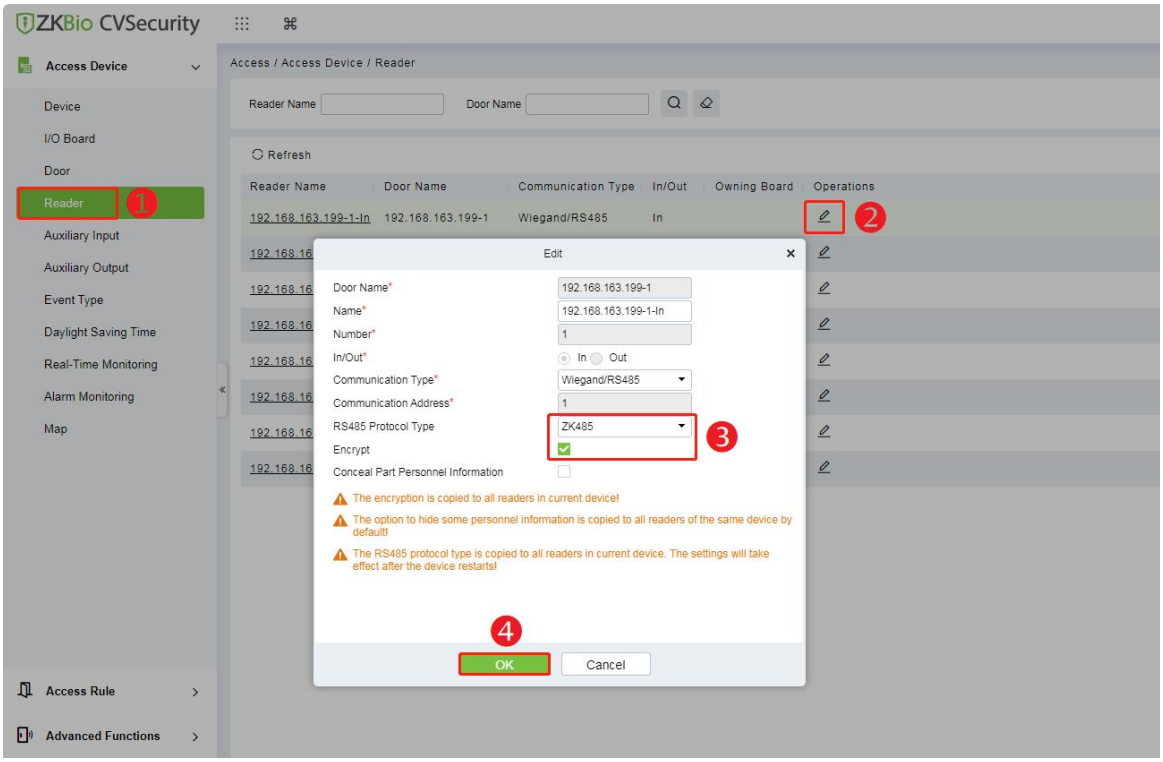
Figure 4-10 Connection between C3-400 Plus and RS485 Readers

- **Controller Supported Reader Models:**

Reader Model	485 Unencrypted	485 Encryption	OSDP Unencrypted	OSDP Encryption
ProID101/102/103/104	✓	✕	✓	✕
ProID20/30BEMD-RS	✓	✕	✓	✕
QR50/QR500/QR600	✓	✓	✕	✕

Remarks:

1. *✓ means connectable, ✕ means not connectable.*
2. *In 485 communication encryption mode, the ProID100 reader supports tamper alarm function. When the reader is illegal tampering, it will send a tamper signal to the controller via 485, and the controller will report to the software to form a tamper alarm event. Users can configure the alarm linkage on the software side and connect the alarm to the auxiliary output. The tamper switch for the ProID100 reader is on the back case of the unit.*
3. *On the software side, click **Access > Access Device > Reader**, select the reader and check **Encrypt** in the pop-up editing window to enable the encryption function. This is shown in the figure below.*



Setting the RS485 Address

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

RS485 address / Control Panel	1	2	3	4	5	6	7	8
C3-100 Plus	#1Door IN	#1Door OUT						
C3-200 Plus	#1Door IN	#1Door OUT	#2Door IN	#2Door OUT				
C3-400 Plus	#1Door IN	#1Door OUT	#2Door IN	#2Door OUT	#3Door IN	#3Door OUT	#4Door IN	#5Door OUT

Important Notes:

1. RS485 communication wires should be a shielded twisted pair cable. RS485communication wires should be connected in a bus cascade topology instead of a star topology, to achieve a better shielding effect by reducing signal reflection during communications.
2. A single RS485 bus can connect up to 63 access control panels, but preferably 32 is recommended maximum.
3. To eliminate signal attenuation in communication cables and suppress interference, if the bus is longer than 200 meters, set the number **8** DIP switch to the **ON** position. The number 8 DIP switch is for setting the RS485 termination resistance. This is equivalent to a parallel connection of one 120ohm resistance between the 485+ and 485- lines.

4. When the EXT RS485 port is configured with ZK485 or OSDP protocol, the corresponding baud rate is set to **9600** for **ZK485** and **115200** for **OSDP**.
5. 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.
6. 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.
7. For some of the devices with much greater consumption, we suggest to use the separately power supplies, to make sure the steady operation.

• QR50 Connection

The QR50 code reader does not need to be connected to the lock body when it is used as a reader. The figure below shows the connection to the controller via RS485:

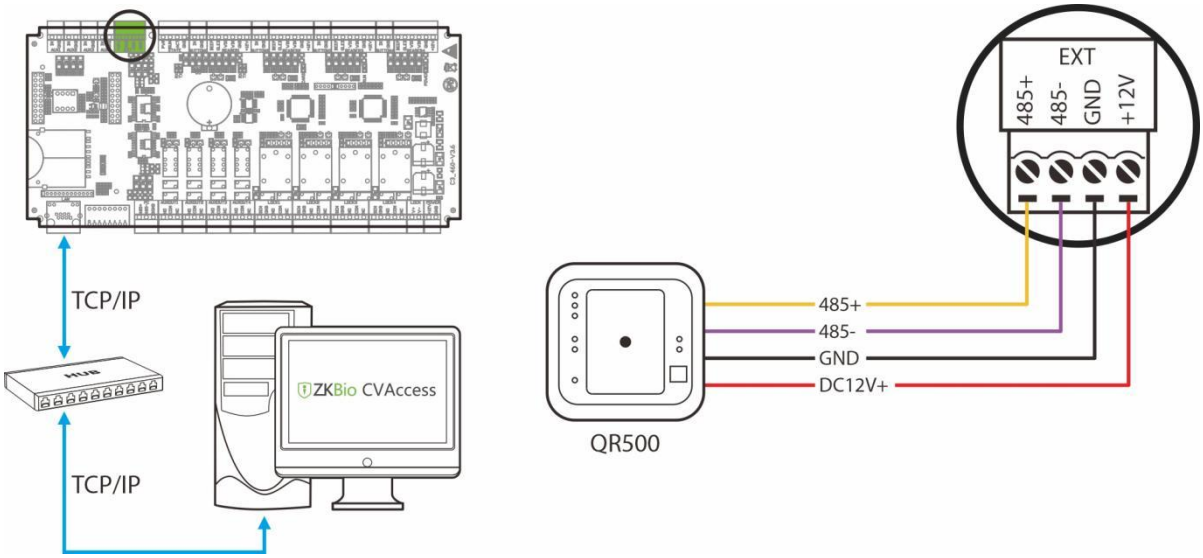


Figure 4-11 QR50 wiring diagram

• External Readers Verification Status

After the external reader is connected to the controller, the status of the buzzer and LEDs are shown below.

Items	Voice Prompt	Indicator Status	Buzzer Status
Standby Status / Online	/	Breathing light interval frequency 1s, white light on	/
Standby Status / Offline	/	Breathing light interval frequency 1s, red light on	/
Successfully verified	Voice prompt: Successfully verified	The indicator (green) lights up	The buzzer rings once.
Verification failure	Voice prompt: Failed to verify	The indicator (red) lights up briefly twice.	The buzzer sounds twice fast.
Unauthorized personnel	Voice prompt: Unauthorized	The indicator (red) briefly light three times	The buzzer sounded three times fast.
Authentication mode error	Voice prompt: Verification error	The indicator (red) long light three times.	The buzzer beeps twice fast and once long.
Combined verification timeout	Voice prompt: Combined verification timeout	The indicator (red) lights up briefly four times.	The buzzer sounded four times fast (timeout is **10** seconds).
Verification timeout	Voice prompt: Verification timeout	The indicator (red) lights up briefly four times.	The buzzer sounded four times fast (timeout is **8** seconds).

4.2.8 PC485 Extension Communication Wiring

The C3 Plus series can be connected to the EX0808 expansion board via PC485. **Note:** PC software communication is a customized feature and not supported by default, please contact your dealer if you need it.

What is EX0808?

EX0808 is an extended module for controllers which is used for connecting more number of auxiliary devices.

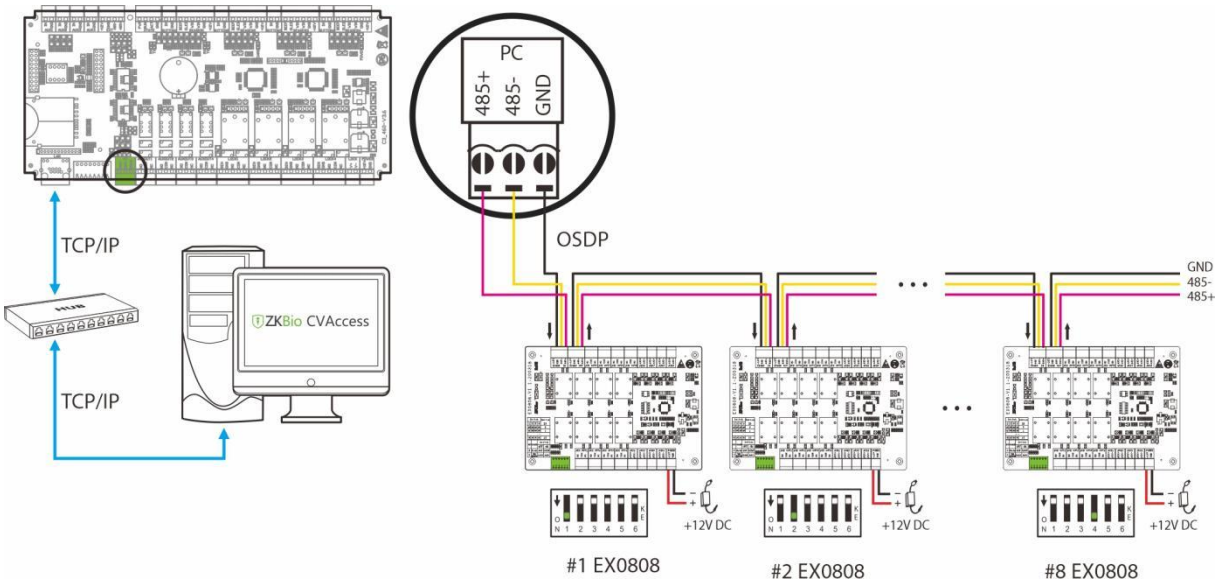


Figure 4-12 Connecting the EX0808 expansion board via PC485

Important Notes:

1. Conf igure the **ZK485** protocol through the PC485 port to connect up to eight EX0808 expansion boards to expand a certain number of auxiliary inputs and auxiliary outputs.

   Note: *Set DIP switch **#5** of the expansion board to the **OFF** position.*

2. Conf igure the **OSDP** protocol through the PC485 port to connect up to eight EX0808 expansion boards to expand a certain number of auxiliary inputs and auxiliary outputs.

   Note: *Set DIP switch **#5** of the expansion board to the **ON** position.*

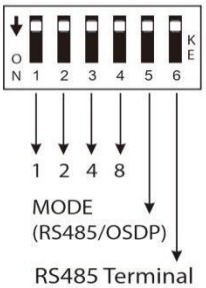
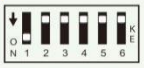
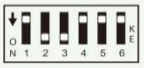
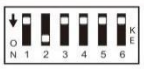
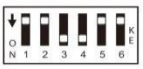
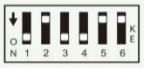
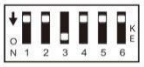
3. The RS485/OSDP address of each EX0808 is set via the DIP switch before power is applied.
4. Each EX0808 requires a separate power supply. Up to eight auxiliary input devices and eight auxiliary output devices can be connected to one EX0808.

- **DIP Switch Setting for RS485/OSDP Communication**

There are six DIP switches on the EX0808 expansion board and their functions are:

1. Switches 1-4 are used to set the RS485/OSDP addresses.
2. Switch **5** is for RS485/OSDP mode switching. When set to **OFF**, RS485 mode is used, and when set to **ON**, OSDP mode is used.
3. If the cable length is more than 200 meters, the switch **6** should be **ON** for noise reduction on long RS485 cables.
4. The detailed settings of the DIP switches are shown in the table 4-1 below.

Table 4-1 - DIP Switch Setting for RS485/OSDP Communication

Description	RS485 Address	DIP Switch	RS485 Address	DIP Switch	RS485 Address	DIP Switch
	1		6		11	
	2		7		12	
	3		8		13	
	4		9		14	
	5		10		15	

4.2.9 Door Sensors Wiring

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 mm^2. 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.

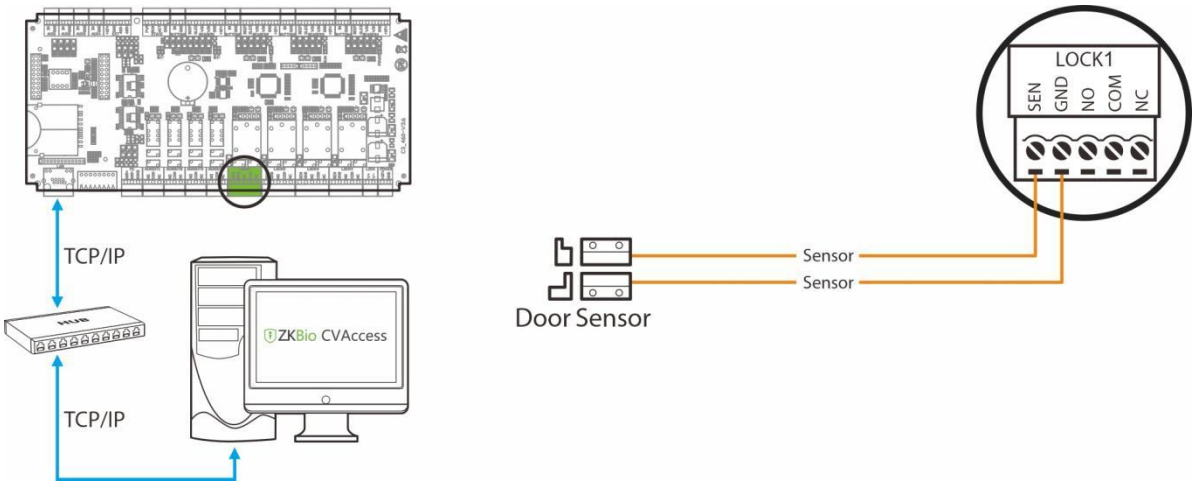


Figure 4-13 Door sensors wiring diagram

4.2.10 Lock Relay Wiring

The C3-100 Plus has one lock relay, the C3-200 Plus has two lock relays, and the C3-400 Plus has four lock relays.

1. 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.
2. 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.
3. In general, the default connection mode of the door lock is "Dry Mode". Dry mode supports separate power supply for the door lock using an external independent power supply. Wet mode supports the door lock sharing power with the controller.
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). The factory default jumper setting is **Dry Mode**.

Method of switching between wet and dry modes:

- **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.

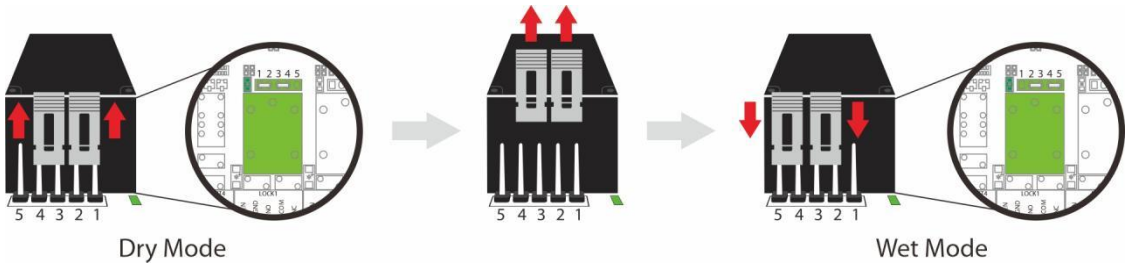


Figure 4-14 Schematic diagram for switching between wet and dry modes

- **Controller not sharing power with the lock (Dry Connect)**

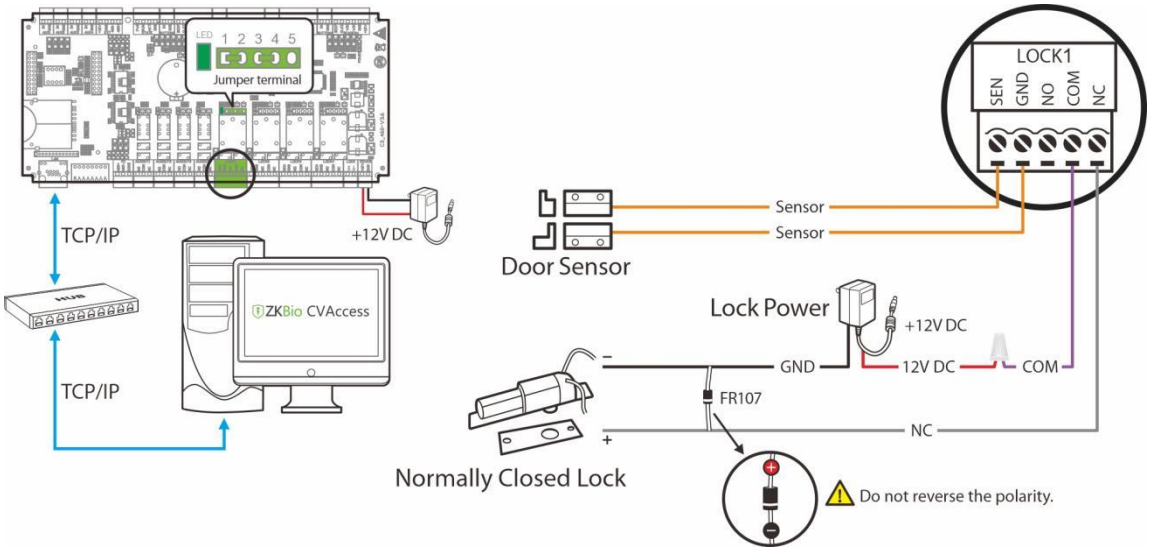


Figure 4-15 Schematic diagram of the controller not sharing power with the lock

- **Controller sharing power with the lock (Wet Connect)**

The system supports both **Normally Opened Lock** and **Normally Closed Lock**. The **NO LOCK** (normally opened at power on) is connected with '**NO**' and '**COM**' terminals, and the **NC LOCK** (normally closed at power on) is connected with '**NC**' and '**COM**' terminals.

<u>Normally Opened Lock Powered From Lock Terminal:</u>

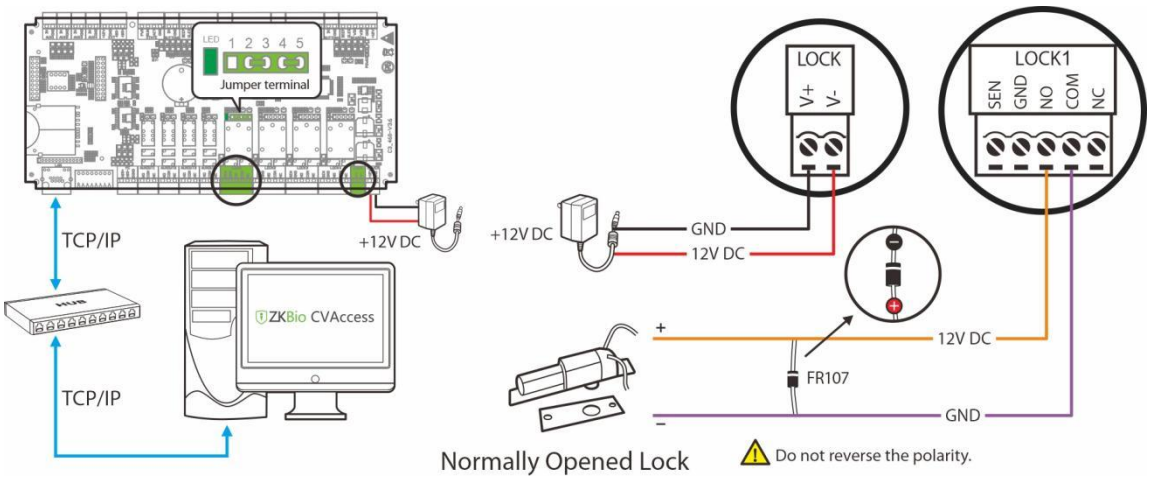


Figure 4-16 Schematic diagram of the controller sharing power with the NO Lock

Normally Closed Lock Powered From Lock Terminal:

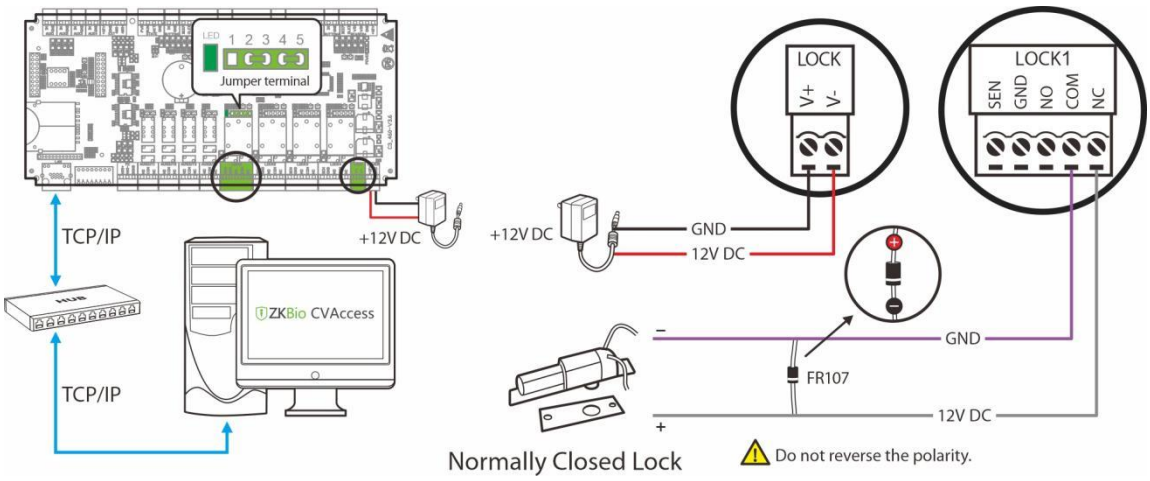


Figure 4-17 Schematic diagram of the controller sharing power with the NC Lock

Important Notes:

1. The access controller comes standard with a 12V/3A power supply, and this power supply only takes into account the power consumption of the controller itself, the output power consumption of the Wiegand reader and the RS485 reader. So usually, it is not recommended to share the power supply between the lock and the device. If you do need to share the power supply between the lock and the device, it is recommended to replace the power supply with a larger capacity, such as 12V/5A power supply. At this time, in addition to the reserved 3A current, there are 2A current can be used by the lock. If you connect our common electric lock (static loss 300mA, maximum dynamic current 500mA), you can connect up to 4 electric locks.
2. For equipment with high power consumption, it is recommended to use separate power supply to ensure stable operation of the equipment.

5 Equipment Communication

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

5.1 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 2.5mm^2).

5.2 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.

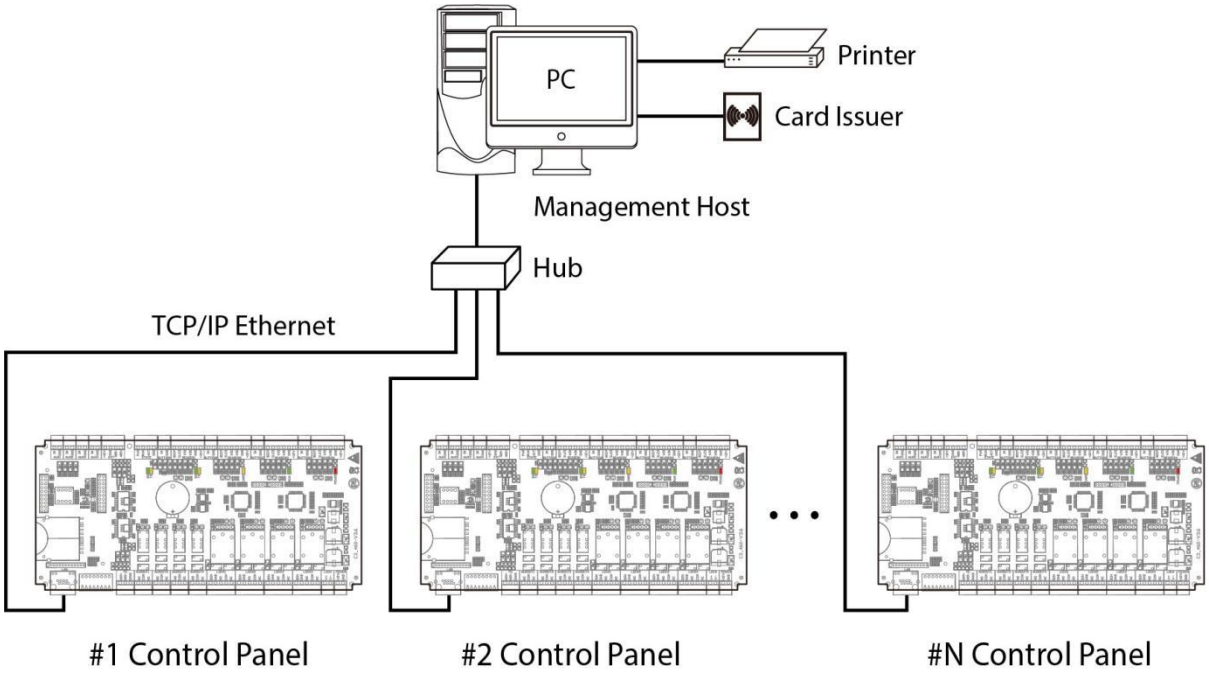


Figure 5-1 TCP/IP Communication System Networking

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

5.3 DIP Switch Settings

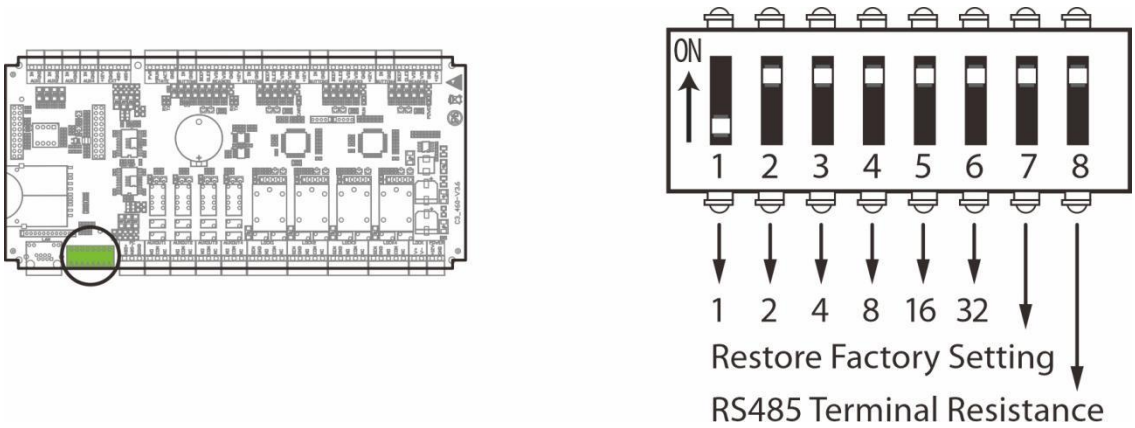


Figure 5-2 DIP switch diagram

- **485 address setting**

1. Number 1-6 are reserved to set the device number for RS485 communication. The code is binary, and the numbering starts from left to right. When the switch is set to ON position, it indicates 1 (on); when the switch is set downwards, it indicates 0 (OFF).
2. For example, to set a device number 39=1+2+4+32, which corresponds to the binary code 111001, put number 1, 2, 3, and 6 to ON position, as illustrated below.

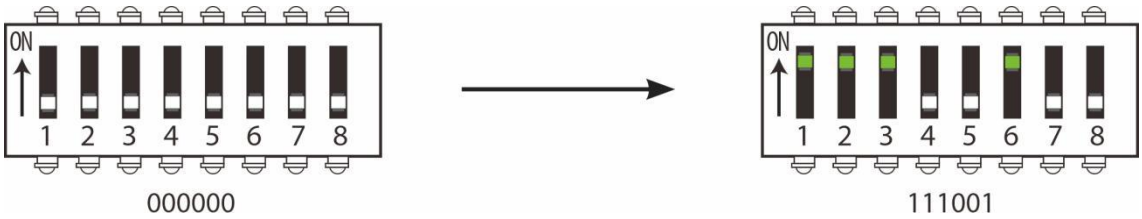


Figure 5-3 DIP switch setting diagram

Table 5-1 485 address setting table

Place Address	Switch Setting					
	1	2	3	4	5	6
Address No.	**1**	**2**	**4**	**8**	**16**	**32**
01	**ON**	OFF	OFF	OFF	OFF	OFF
02	OFF	**ON**	OFF	OFF	OFF	OFF
03	**ON**	**ON**	OFF	OFF	OFF	OFF
04	OFF	OFF	**ON**	OFF	OFF	OFF
05	**ON**	OFF	**ON**	OFF	OFF	OFF
06	OFF	**ON**	**ON**	OFF	OFF	OFF
07	**ON**	**ON**	**ON**	OFF	OFF	OFF
08	OFF	OFF	OFF	**ON**	OFF	OFF

09	**ON**	OFF	OFF	**ON**	OFF	OFF
10	OFF	**ON**	OFF	**ON**	OFF	OFF
11	**ON**	**ON**	OFF	**ON**	OFF	OFF
12	OFF	OFF	**ON**	**ON**	OFF	OFF
13	**ON**	OFF	**ON**	**ON**	OFF	OFF
14	OFF	**ON**	**ON**	**ON**	OFF	OFF
15	**ON**	**ON**	**ON**	**ON**	OFF	OFF
16	OFF	OFF	OFF	OFF	**ON**	OFF
17	**ON**	OFF	OFF	OFF	**ON**	OFF
18	OFF	**ON**	OFF	OFF	**ON**	OFF
19	**ON**	**ON**	OFF	OFF	**ON**	OFF
20	OFF	OFF	**ON**	OFF	**ON**	OFF
21	**ON**	OFF	**ON**	OFF	**ON**	OFF
22	OFF	**ON**	**ON**	OFF	**ON**	OFF
23	**ON**	**ON**	**ON**	OFF	**ON**	OFF
24	OFF	OFF	OFF	**ON**	**ON**	OFF
25	**ON**	OFF	OFF	**ON**	**ON**	OFF
26	OFF	**ON**	OFF	**ON**	**ON**	OFF
27	**ON**	**ON**	OFF	**ON**	**ON**	OFF
28	OFF	OFF	**ON**	**ON**	**ON**	OFF
29	**ON**	OFF	**ON**	**ON**	**ON**	OFF
30	OFF	**ON**	**ON**	**ON**	**ON**	OFF
31	**ON**	**ON**	**ON**	**ON**	**ON**	OFF
32	OFF	OFF	OFF	OFF	OFF	**ON**
33	**ON**	OFF	OFF	OFF	OFF	**ON**
34	OFF	**ON**	OFF	OFF	OFF	**ON**
35	**ON**	**ON**	OFF	OFF	OFF	**ON**
36	OFF	OFF	**ON**	OFF	OFF	**ON**
37	**ON**	OFF	**ON**	OFF	OFF	**ON**
38	OFF	**ON**	**ON**	OFF	OFF	**ON**
39	**ON**	**ON**	**ON**	OFF	OFF	**ON**
40	OFF	OFF	OFF	**ON**	OFF	**ON**
41	**ON**	OFF	OFF	**ON**	OFF	**ON**
42	OFF	**ON**	OFF	**ON**	OFF	**ON**
43	**ON**	**ON**	OFF	**ON**	OFF	**ON**
44	OFF	OFF	**ON**	**ON**	OFF	**ON**
45	**ON**	OFF	**ON**	**ON**	OFF	**ON**
46	OFF	**ON**	**ON**	**ON**	OFF	**ON**
47	**ON**	**ON**	**ON**	**ON**	OFF	**ON**

48	OFF	OFF	OFF	OFF	**ON**	**ON**
49	**ON**	OFF	OFF	OFF	**ON**	**ON**
50	OFF	**ON**	OFF	OFF	**ON**	**ON**
51	**ON**	**ON**	OFF	OFF	**ON**	**ON**
52	OFF	OFF	**ON**	OFF	**ON**	**ON**
53	**ON**	OFF	**ON**	OFF	**ON**	**ON**
54	OFF	**ON**	**ON**	OFF	**ON**	**ON**
55	**ON**	**ON**	**ON**	OFF	**ON**	**ON**
56	OFF	OFF	OFF	**ON**	**ON**	**ON**
57	**ON**	OFF	OFF	**ON**	**ON**	**ON**
58	OFF	**ON**	OFF	**ON**	**ON**	**ON**
59	**ON**	**ON**	OFF	**ON**	**ON**	**ON**
60	OFF	OFF	**ON**	**ON**	**ON**	**ON**
61	**ON**	OFF	**ON**	**ON**	**ON**	**ON**
62	OFF	**ON**	**ON**	**ON**	**ON**	**ON**
63	**ON**	**ON**	**ON**	**ON**	**ON**	**ON**

- ## Restoring factory setting

1. If you forget the IP address of the C3-X00 Plus series panel or the device does not work normally, you can use the number 7 DIP switch to restore it to factory default settings. The parameters which gets reset are device IP address, communication password, gateway, and subnet mask.

   Note: *Restoring the factory settings will empty the user data, please be careful.*

2. The switch is OFF by default. When it is moved up and down for three times within 10 seconds and f inally returned to OFF position, the factory settings will be restored after the access control panel is restarted.
3. The procedure is shown below.

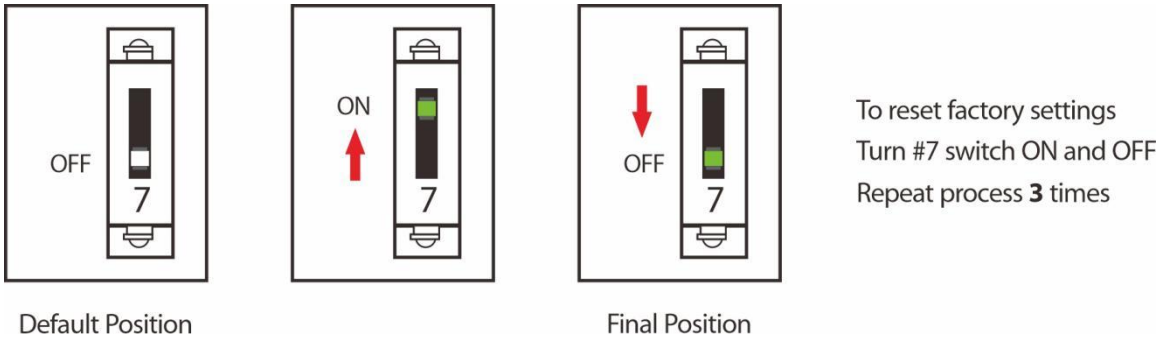


Figure 5-4 DIP switch setting diagram

- ## RS485 Terminal Resistance

To eliminate signal attenuation in communication cables and suppress interference, if the bus is longer than 200 meters, set the number 8 DIP switch to the ON position. The number 8 DIP switch is for setting the RS485 termination resistance. This is equivalent to a parallel connection of one 120ohm resistance between the 485+ and 485- lines.

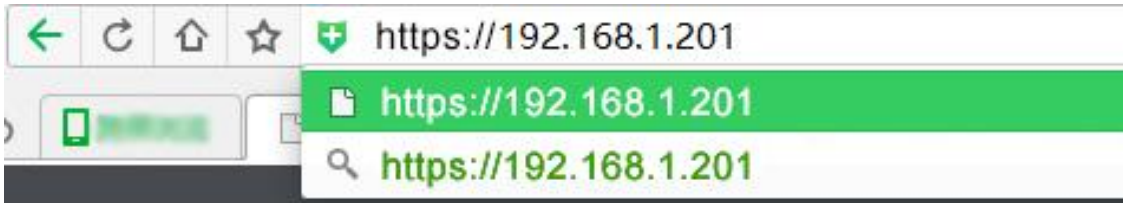
Figure 5-5 Restoring factory setting

6 Login to the Web Server

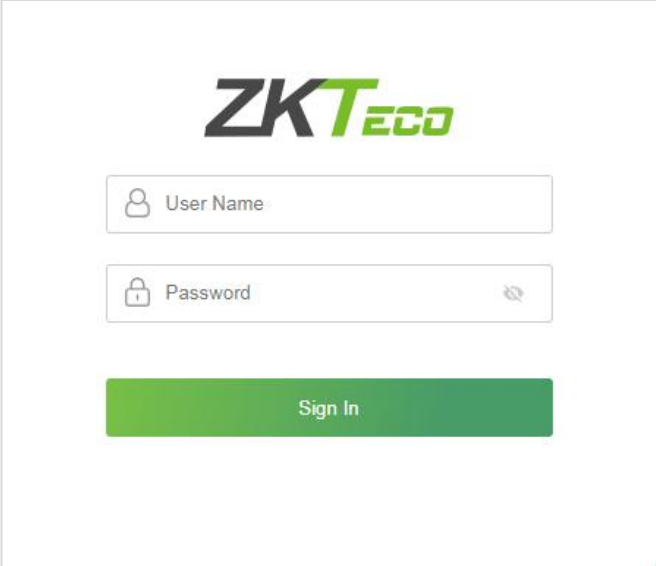
To help users conveniently manage controllers, the built-in Web Server function is added to some models. With this function, a user can connect to the controller through a PC, and enter the IP address of the controller to access the web. Users can also use the Web Server function to perform other operations,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

6.1 Login Web Server

1. Connect the controller to the network or PC, start the browser, enter the IP address of the controller, which is **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 Web Server.

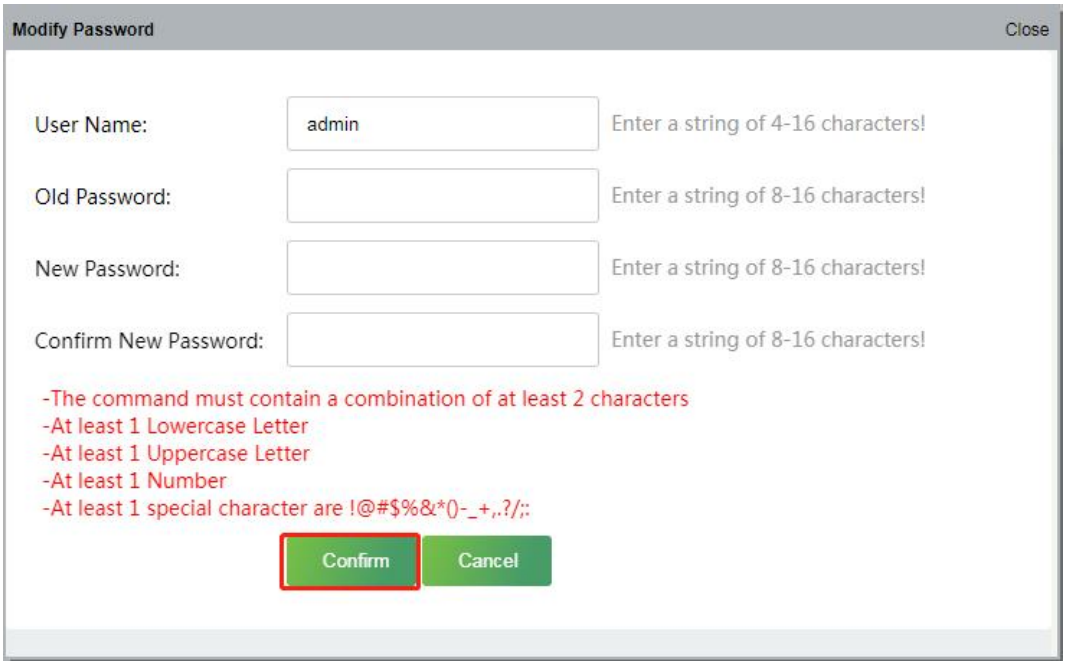
Notes:

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**]).*

6.2 Basic Operation Bar of the Web Server

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

1. Click to modify the password.
2. Enter the old and new passwords in the pop-up window and click **Confirm** to change the administrator login password.



- **Language Settings**

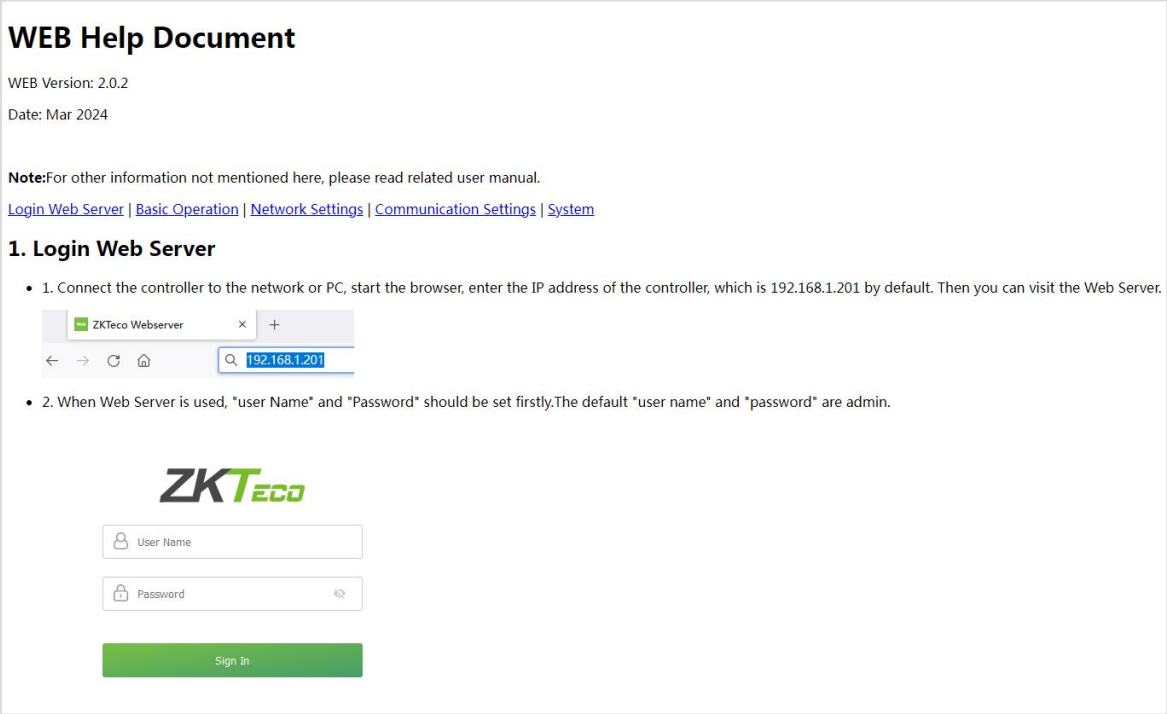
Click , change the language in which the server interface is displayed, and click **Confirm**.

- ## Use Conditions of the Server

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

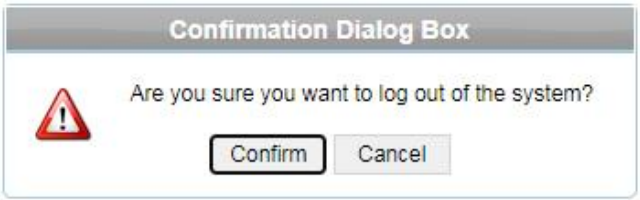
- ## Online Help of the Server

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



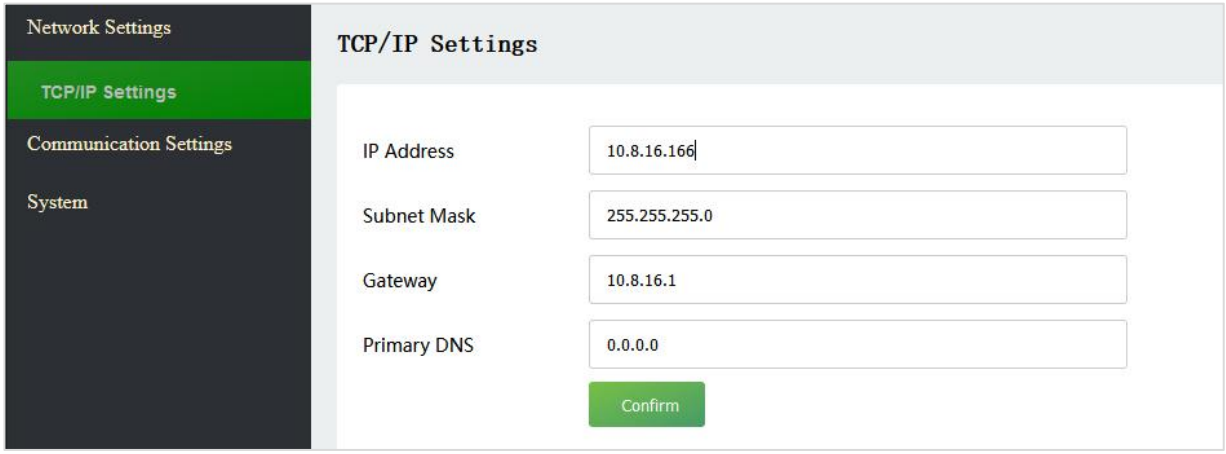
- **Exit**

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



6.3 Network Settings

- **TCP/IP Settings**



Function introduction:

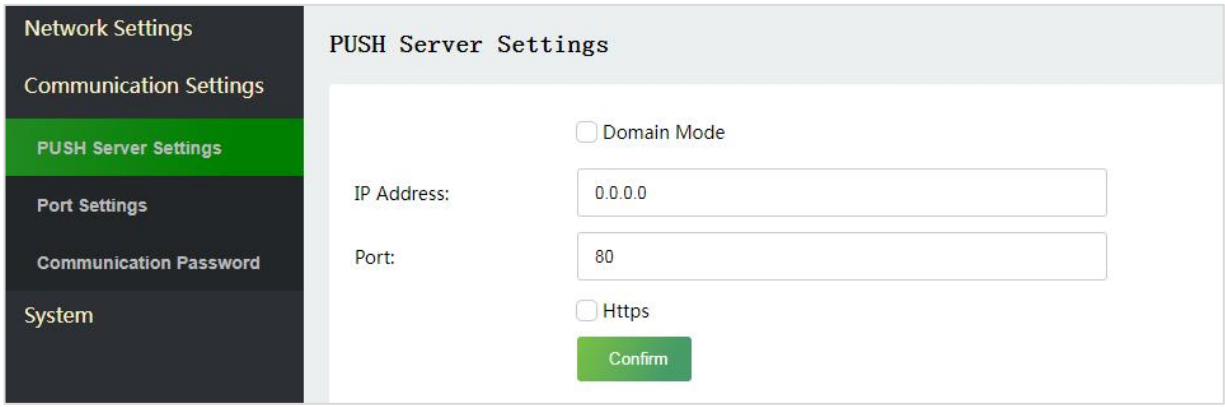
Set the TCP/IP communication parameters, which are used in the communications between device and PC.

➢ **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

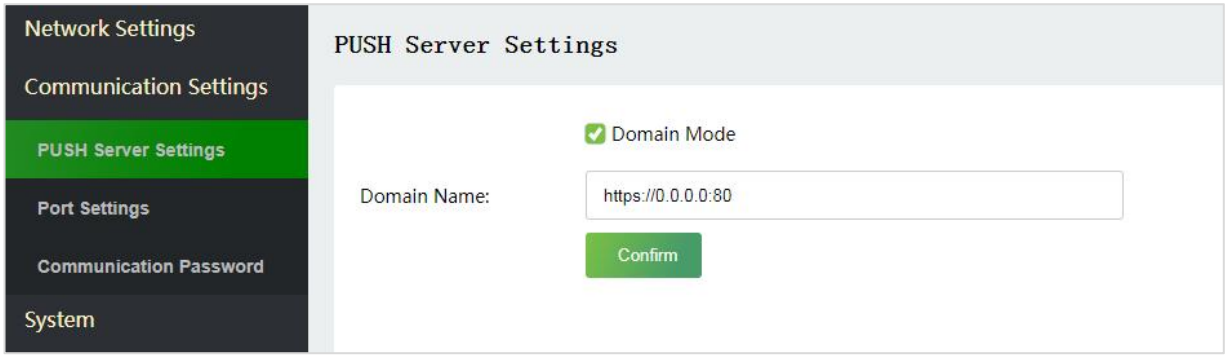
PUSH Server Settings



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

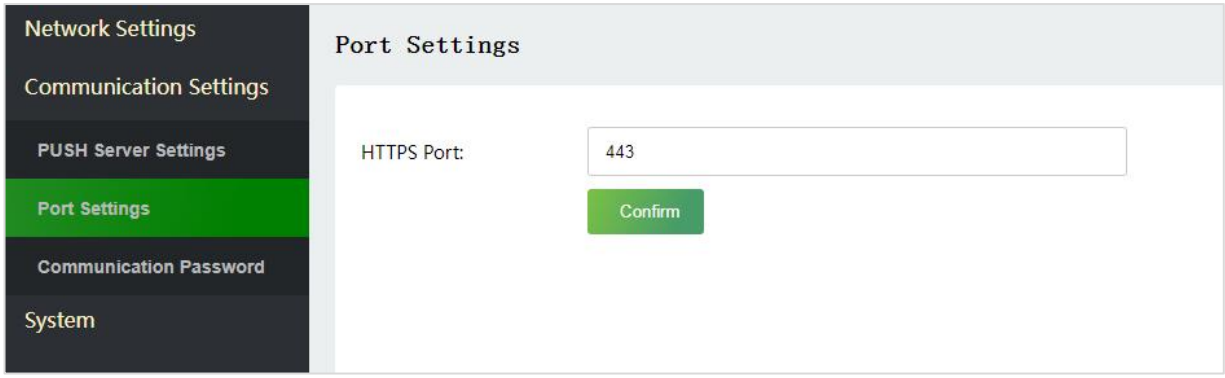
IP Mode:

- **IP Address:** 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.



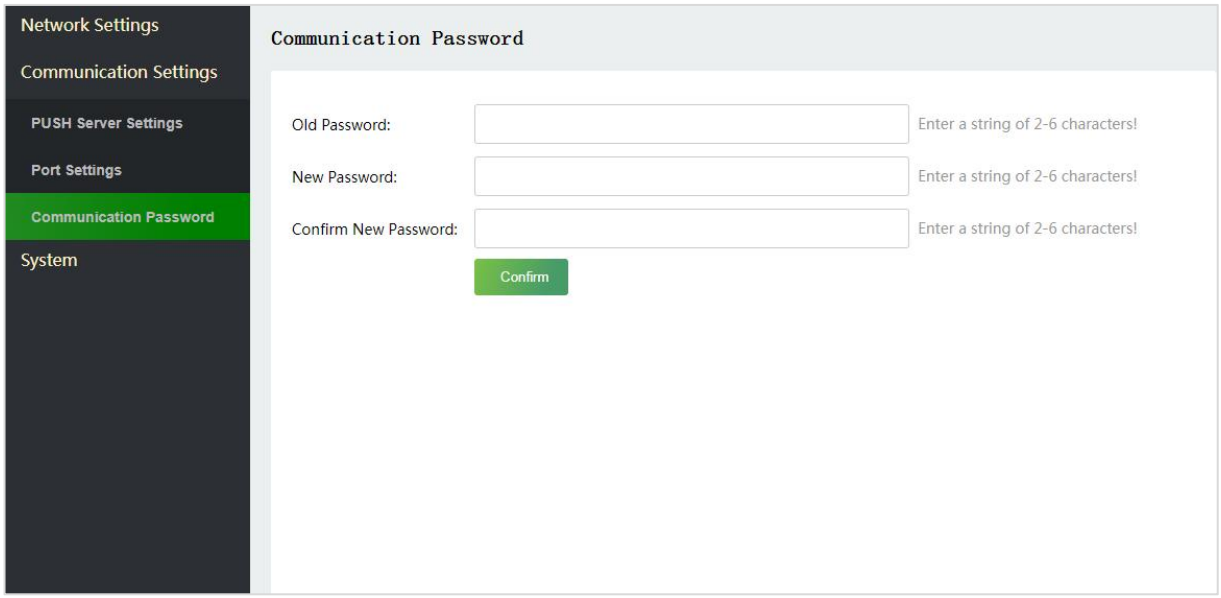
Domain Mode: The default value is null, and you can set its value.

• 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

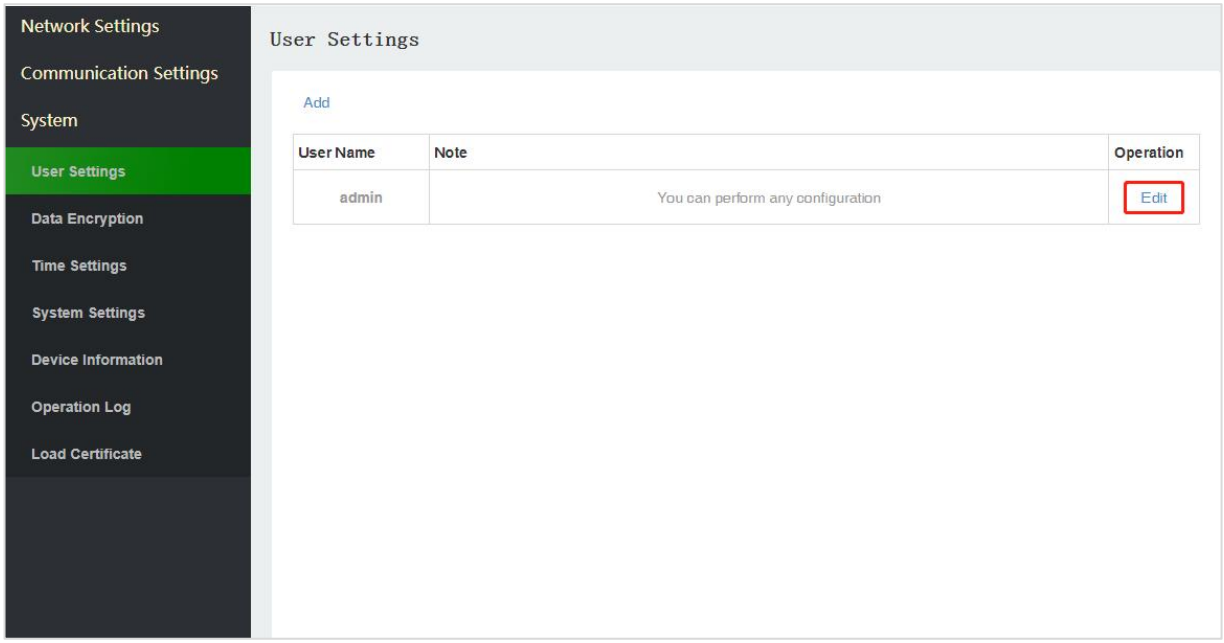


Communication Password: Indicates that network communication is encrypted. The default value is null, and you can set its value.

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

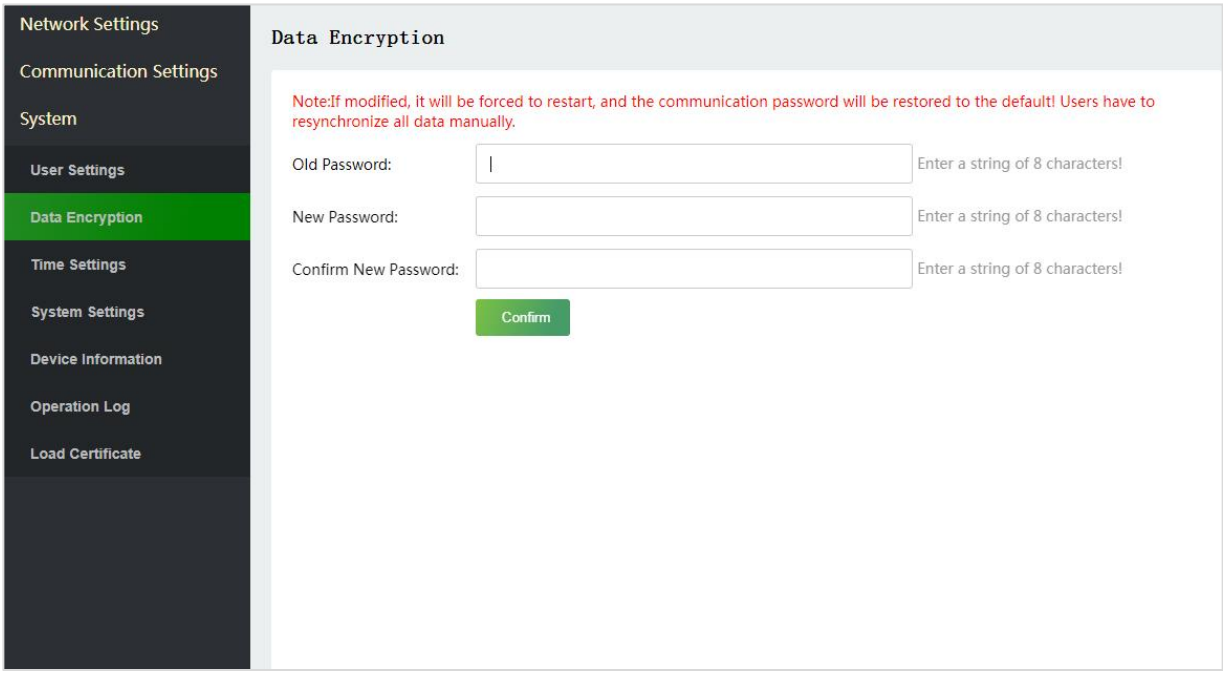
- ## System

User Settings



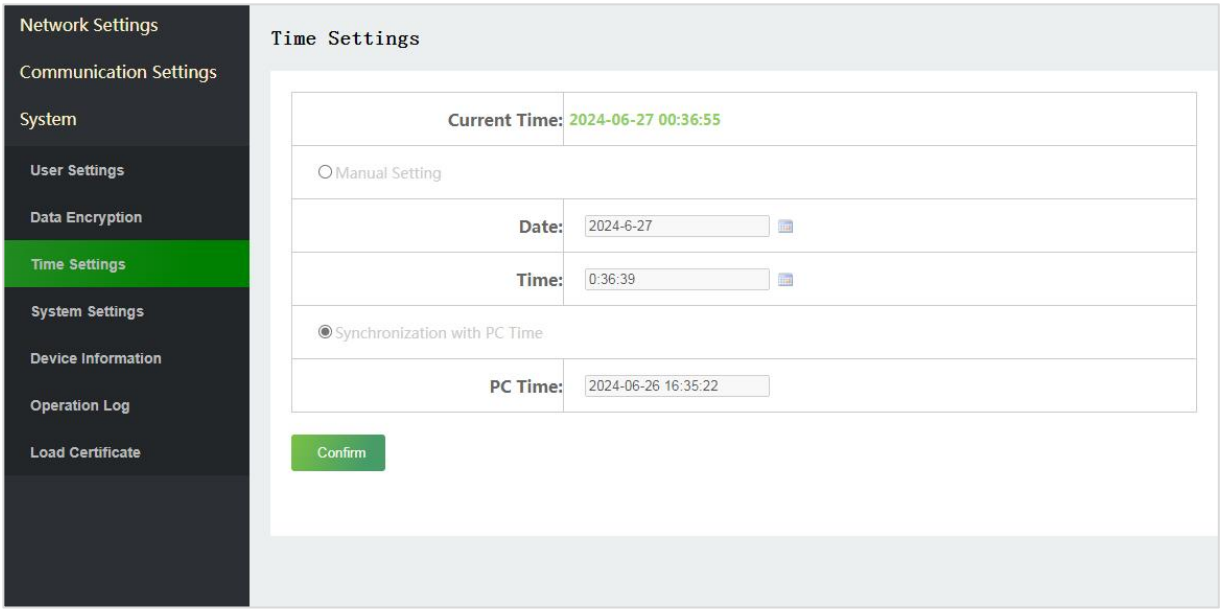
Click **Edit** to change the login password of an administrator or a user.

Data Encryption



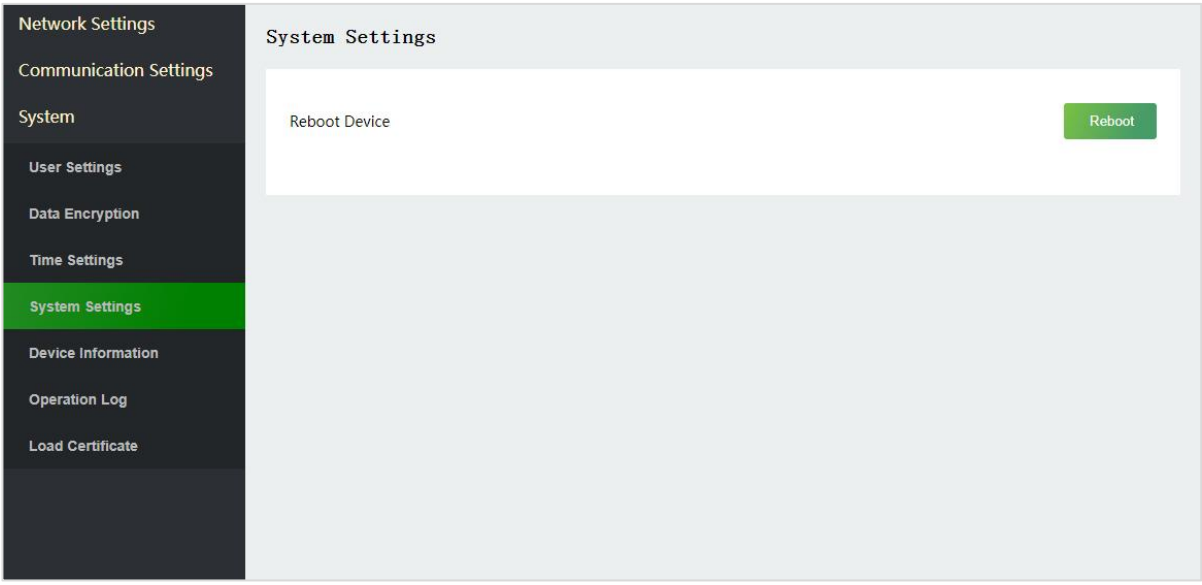
Data Encryption: This feature ensures user data is encrypted and stored securely in the device firmware, preventing unauthorized access. By default, data is encrypted, and users can customize the encryption password (after modification, the communication password will be restored to the default password for data re-synchronization).

Time Settings



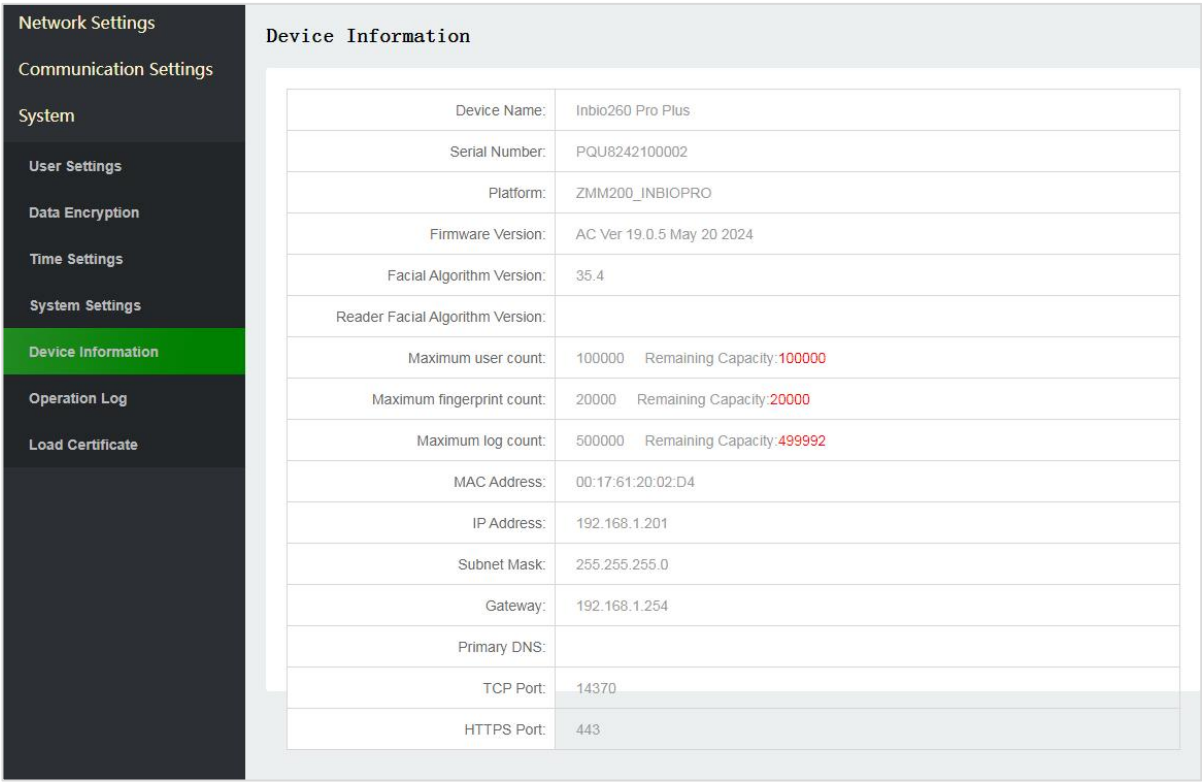
You can manually configure the controller time or synchronize the controller time with the PC time, and click Confirm to complete the setting.

System Settings



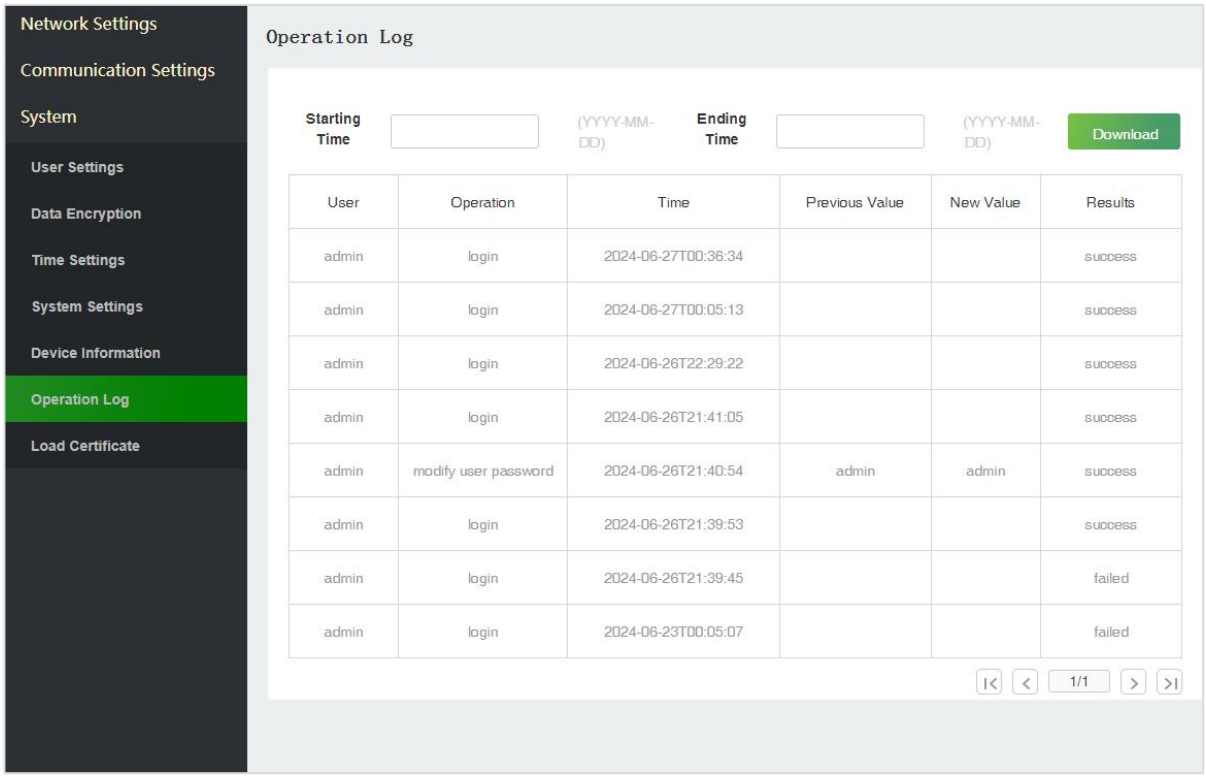
Click **Reboot**. The device will be restarted.

Device Information



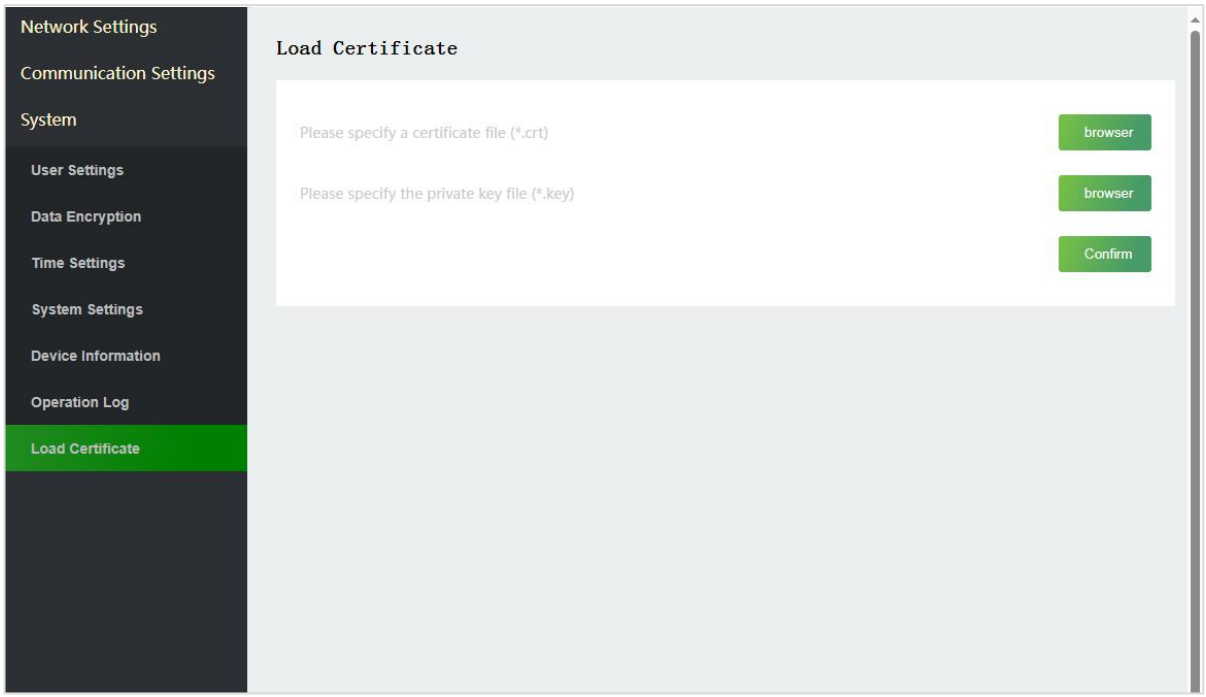
You can view the basic information, remaining capacity, and network information of the current device.

Operation Log



Users can view and download webserver operation logs here.

Load Certificate

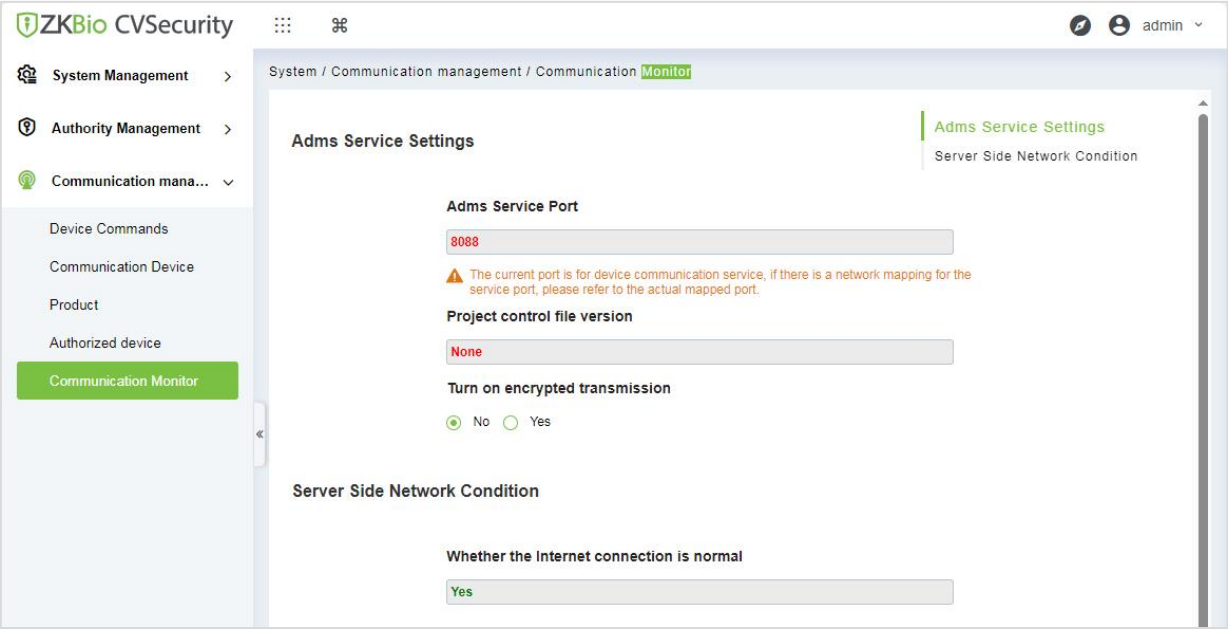


This feature enables users to upload their authenticated browser certificate for accessing the C3 Plus series's webserver.

7 Connect to ZKBioCVSecurity Software

7.1 Set the Communication Address

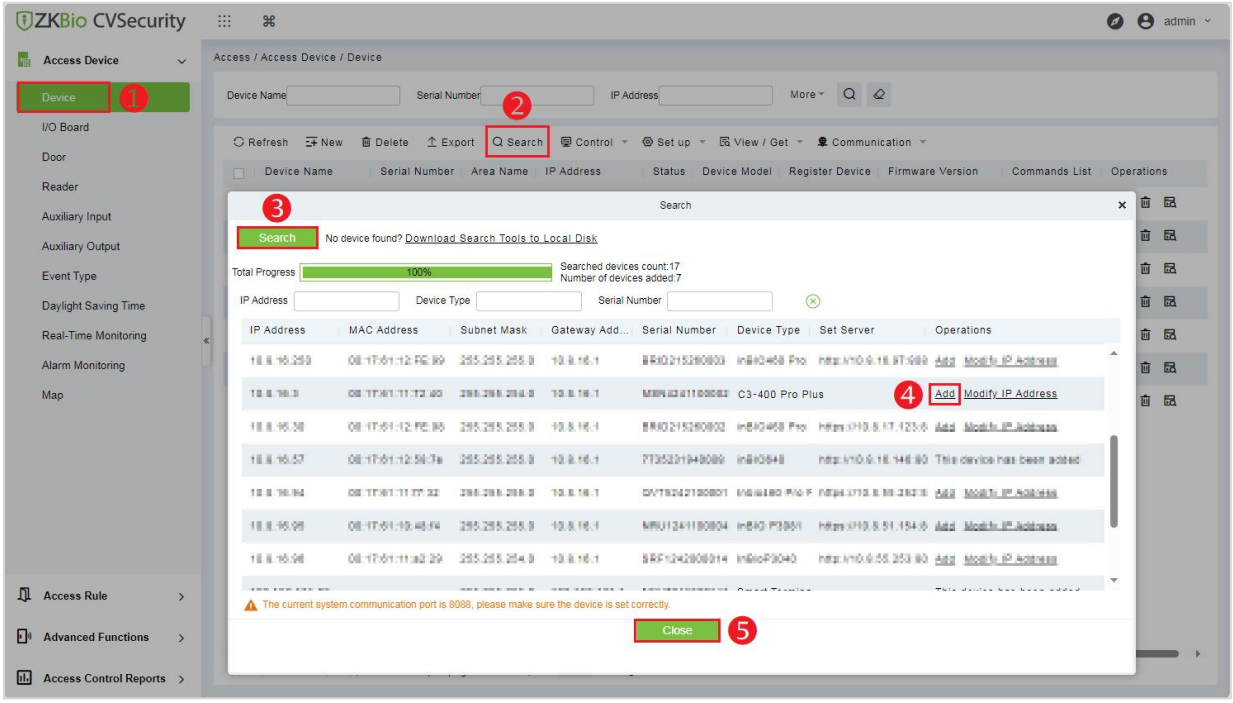
Login to ZKBioCVSecurity software, click **System** > **Communication management**> **Communication Monitor** to set the ADMS Service Port, as shown in the figure below:



7.2 Add Device on the Software

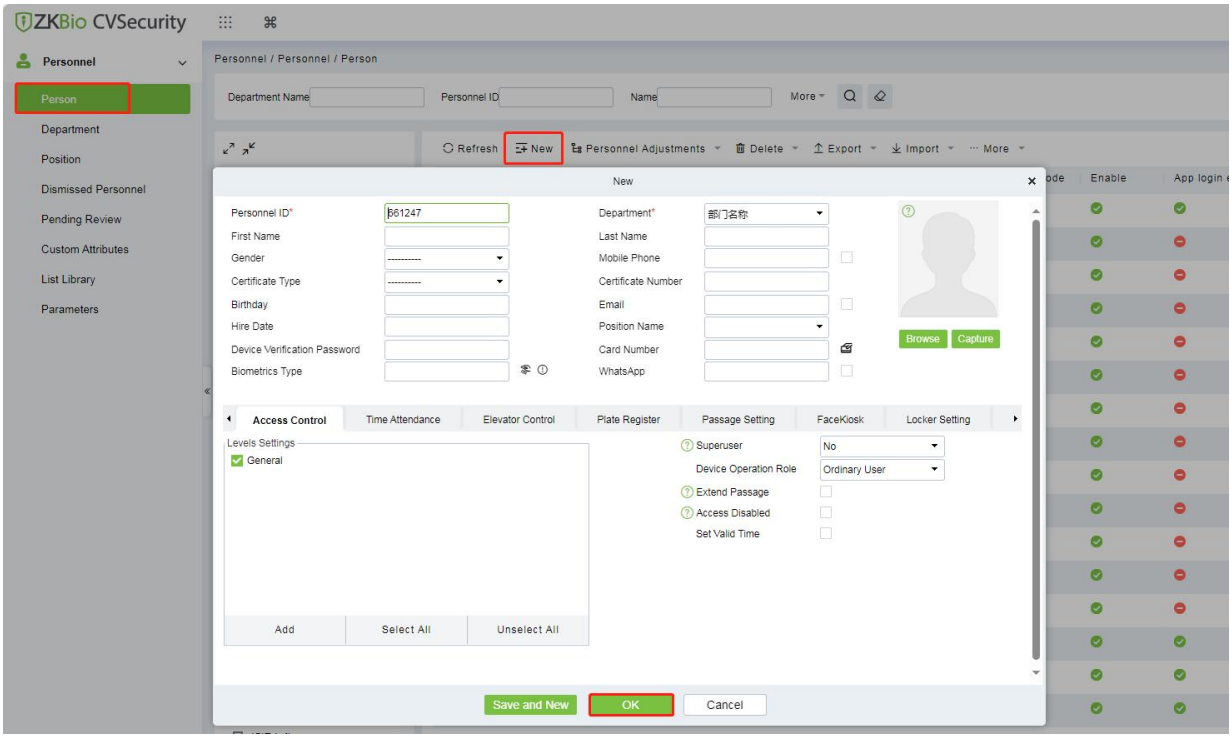
Add the device by searching. The process is as follows:

1. Click **Access** > **Access Device** > **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.

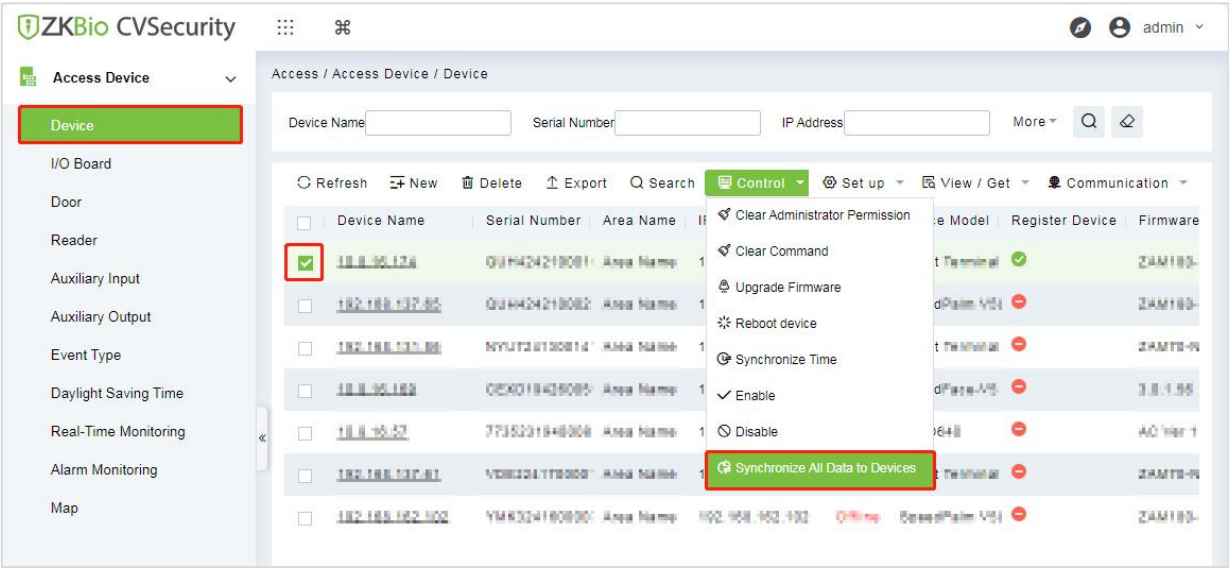


7.3 Add Personnel on the Software

1. Click **Personnel** > **Person** > **New** to register a new user.



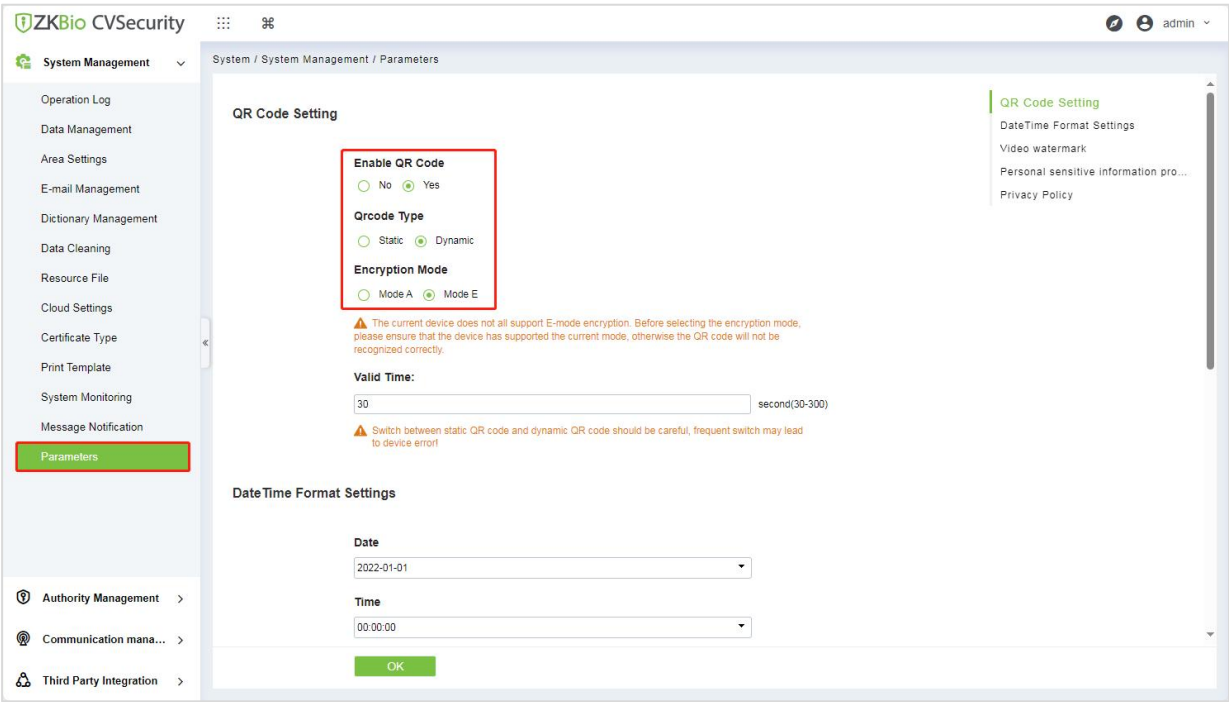
2. Fill in all the required fields and click **OK**.
3. Click **Access Device** > **Device** > **Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.



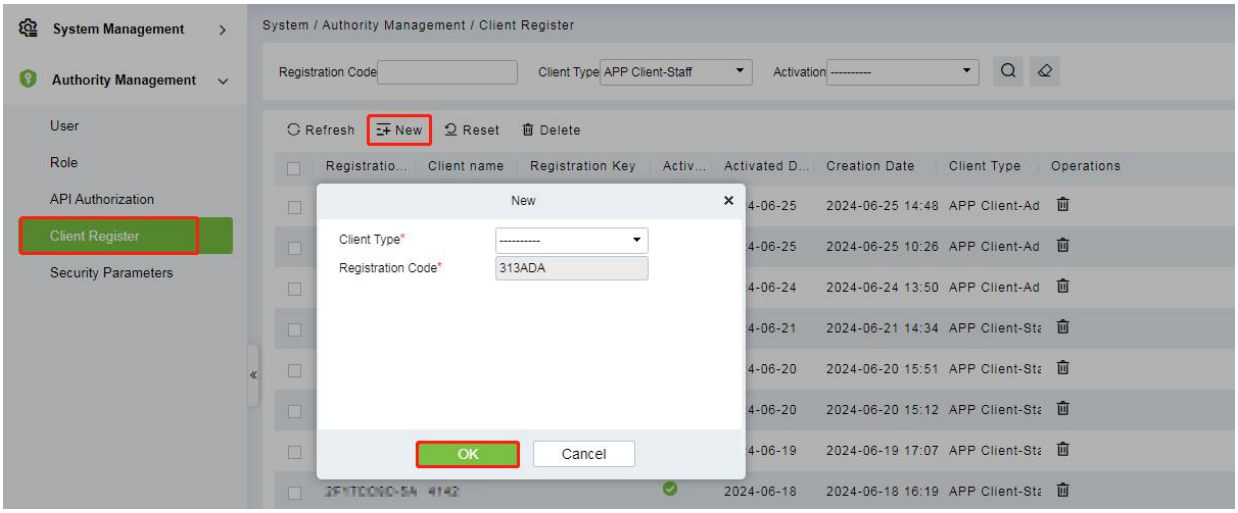
7.4 Mobile Credential★

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

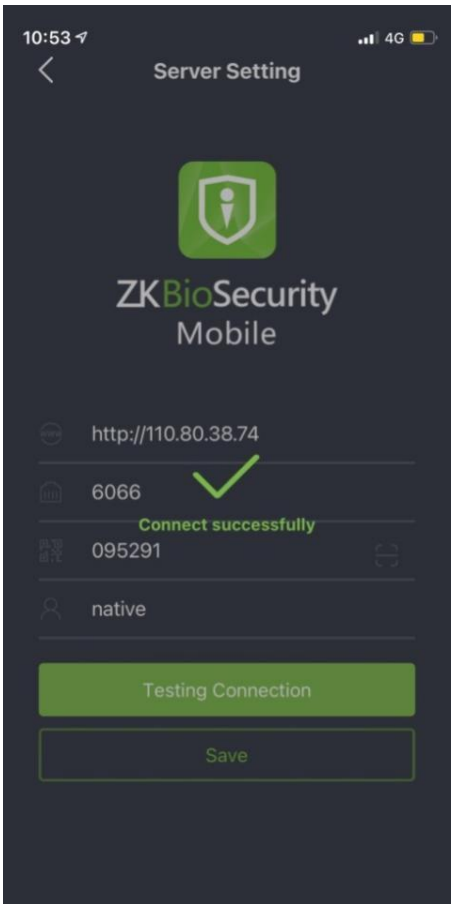
1. In **System** > **System Management** > **Parameters**, set **Enable QR Code** to "Yes", and select the QR code status according to the actual situation. The default is **Dynamic**, the valid time of the QR code can be set.



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

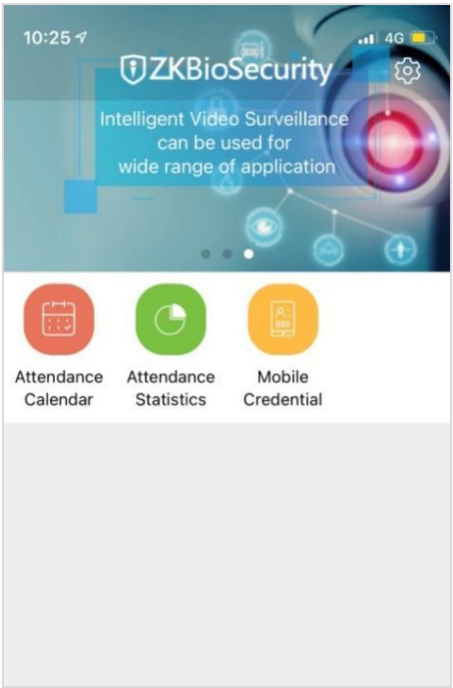


3. Open the App on the Smartphone. On the login screen, tap **Server Setting** and type the IP Address or the Domain Name of the Server, and its Port Number.
4. Tap the **QR Code** icon to scan the QR code of the new App client. After the client is identified successfully, set the Client Name and tap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

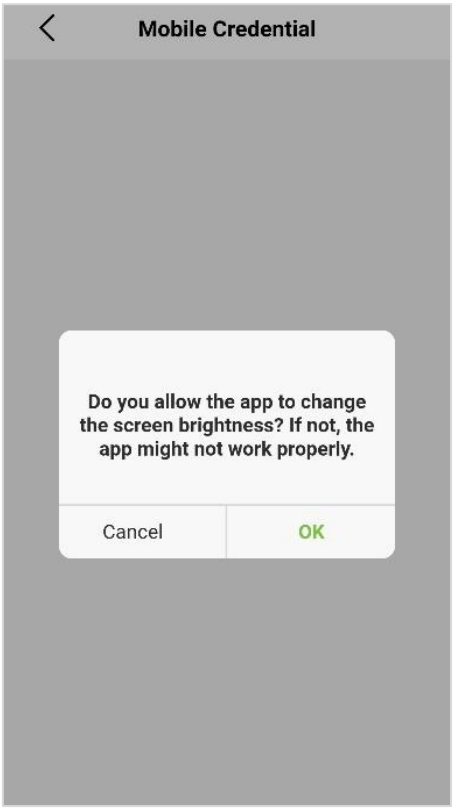


The Mobile Credential function is only valid when logging in as an employee, tap on Employee to switch to Employee Login screen. Enter the Employee ID and Password (Default: **123456**) to login.

6. 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.
7. The QR code can replace a physical card on a specific device to achieve contactless authentication to open the door.



8. 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:



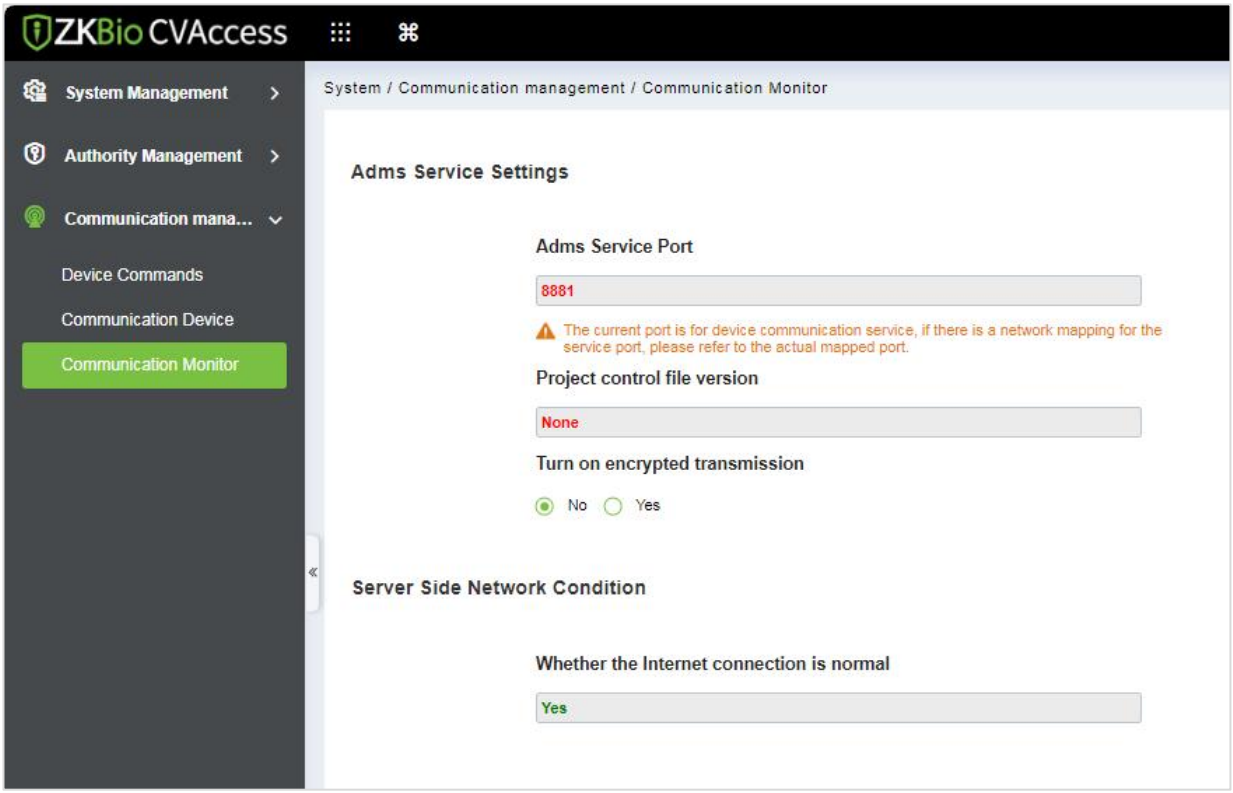
9. The QR code is automatically refreshed for every 30s, and it also supports manual refresh.

Note: *For other specific operations, please refer to* ***ZKBioCVSecurity Mobile App User Manual***.

8 Connect to ZKBio CVAccess Software

8.1 Set the Communication Address

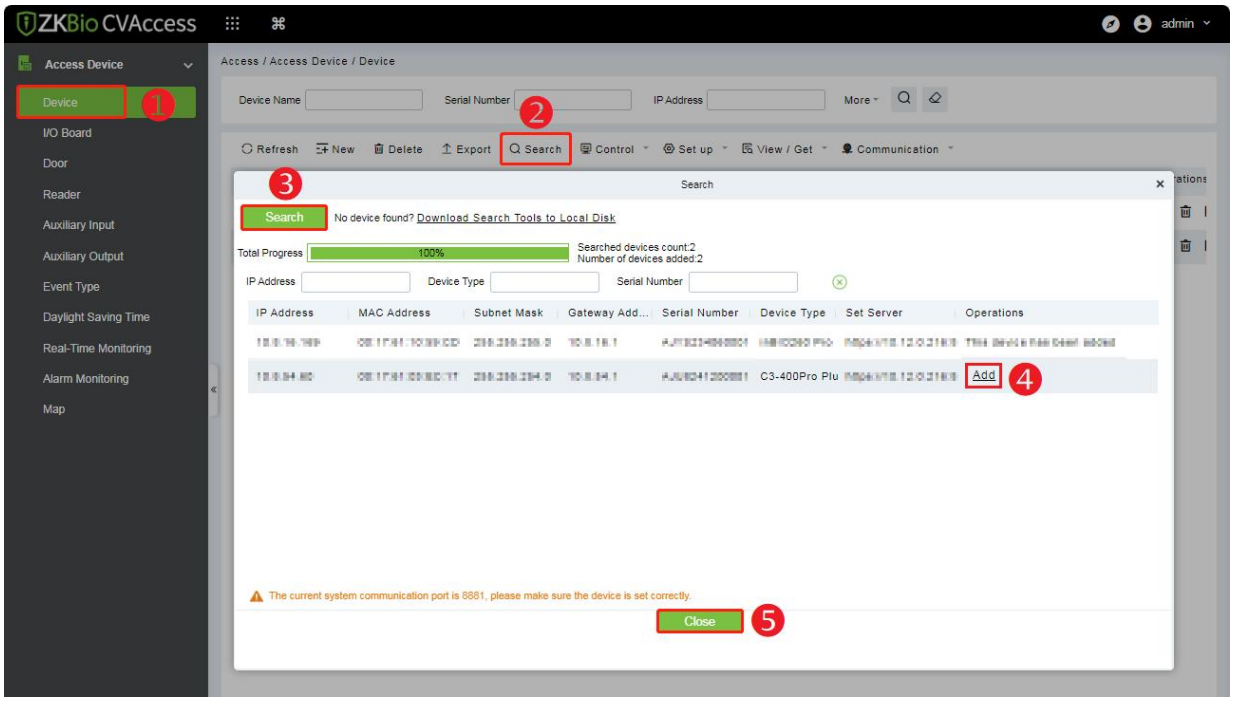
Login to ZKBio CVAccess software, click **System** > **Communication management** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:



8.2 Add Device on the Software

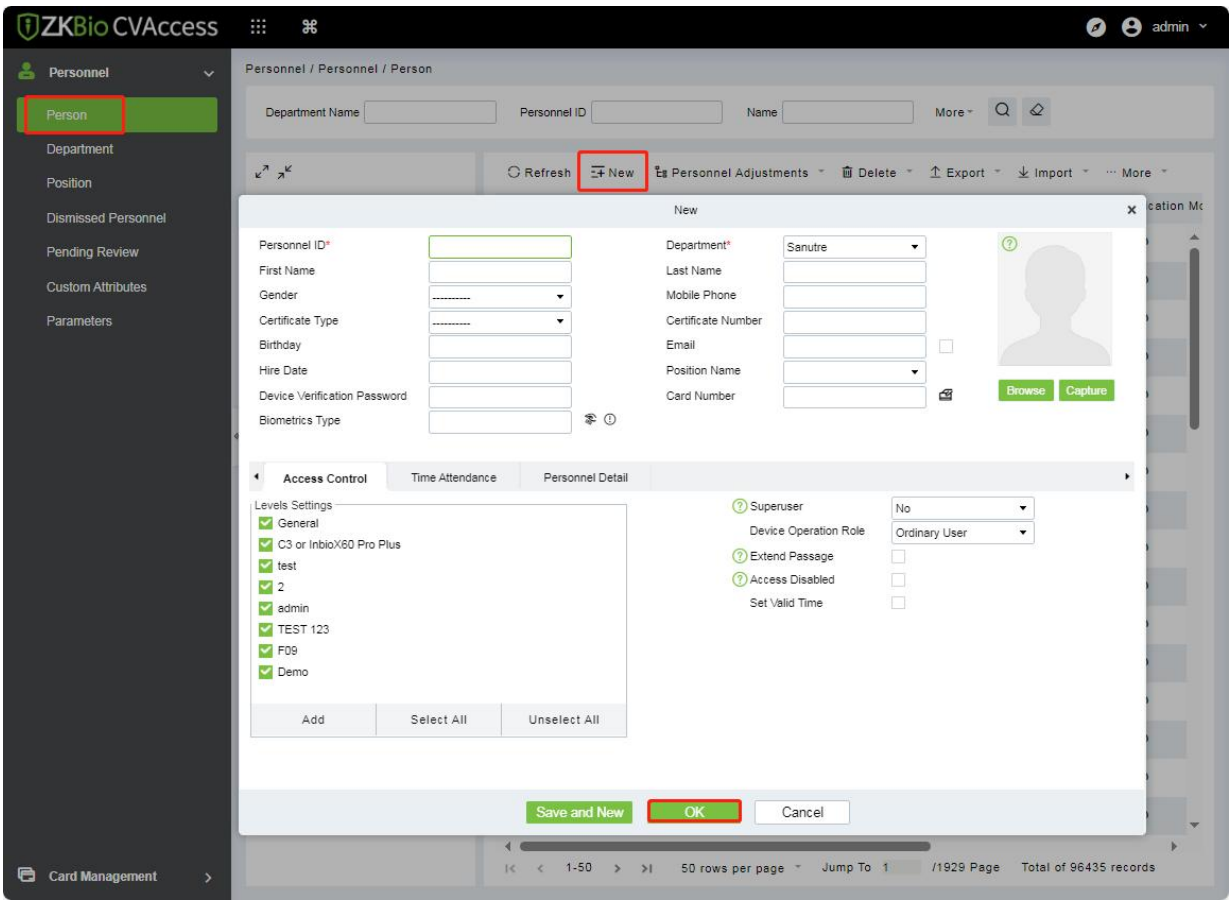
Add the device by searching. The process is as follows:

1. Click **Access** > **Access Device** > **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 **Confirm**, then the added devices are displayed automatically.

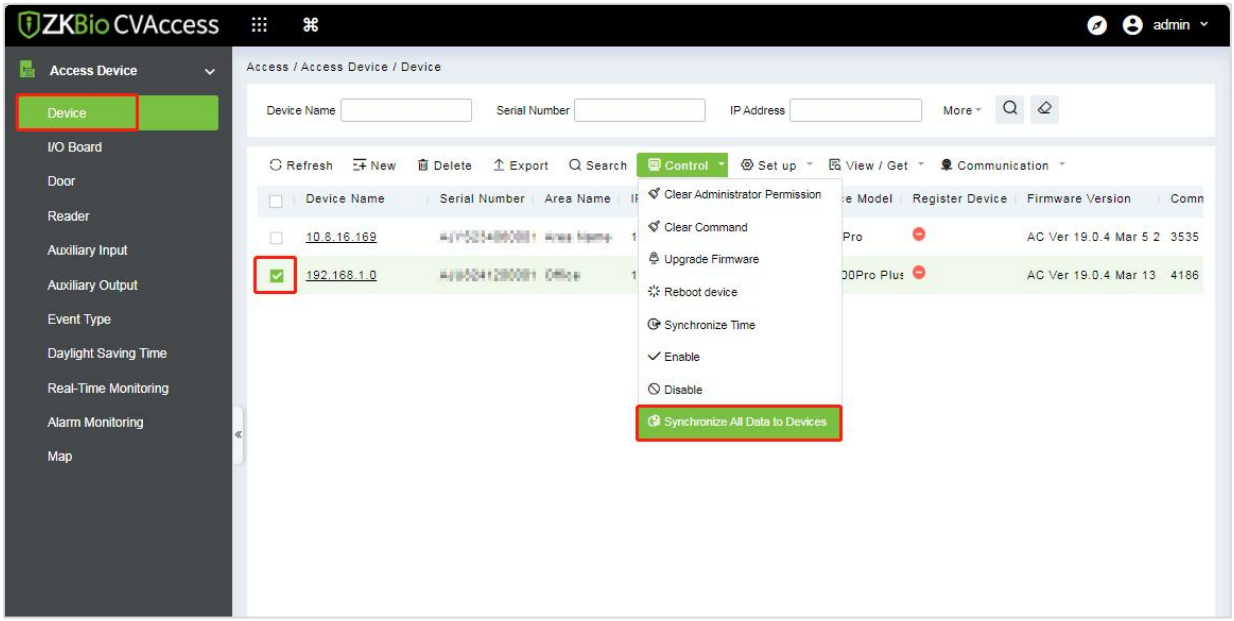


8.3 Add Personnel on the Software

4. Click **Personnel** > **Person** > **New** to register a new user.



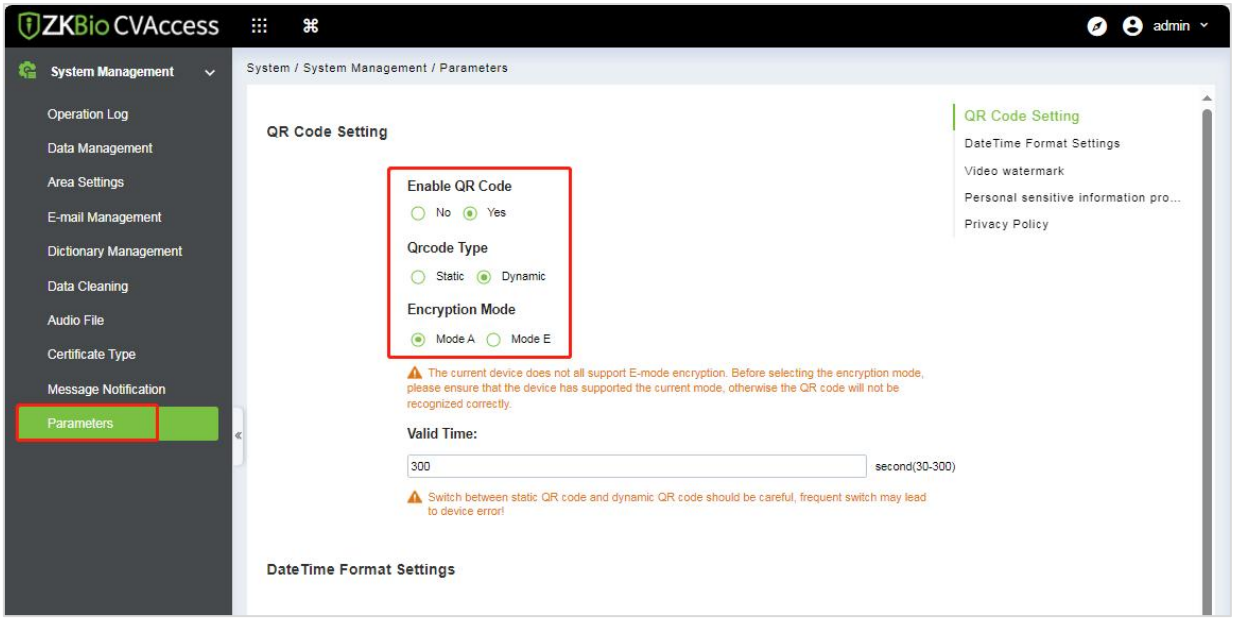
5. Fill in all the required fields and click **OK**.
6. Click **Access Device** > **Device** > **Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.



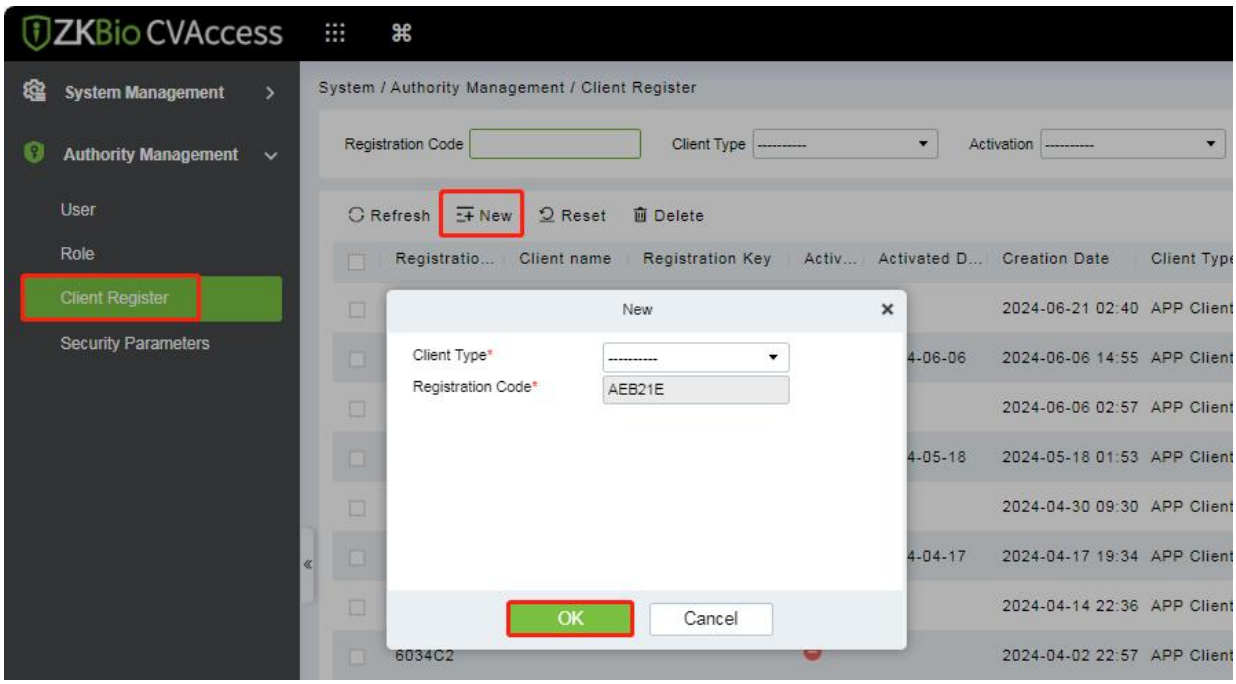
8.4 Mobile Credential★

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

1. In **ZKBio CVAccess** > **System** > **System 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.

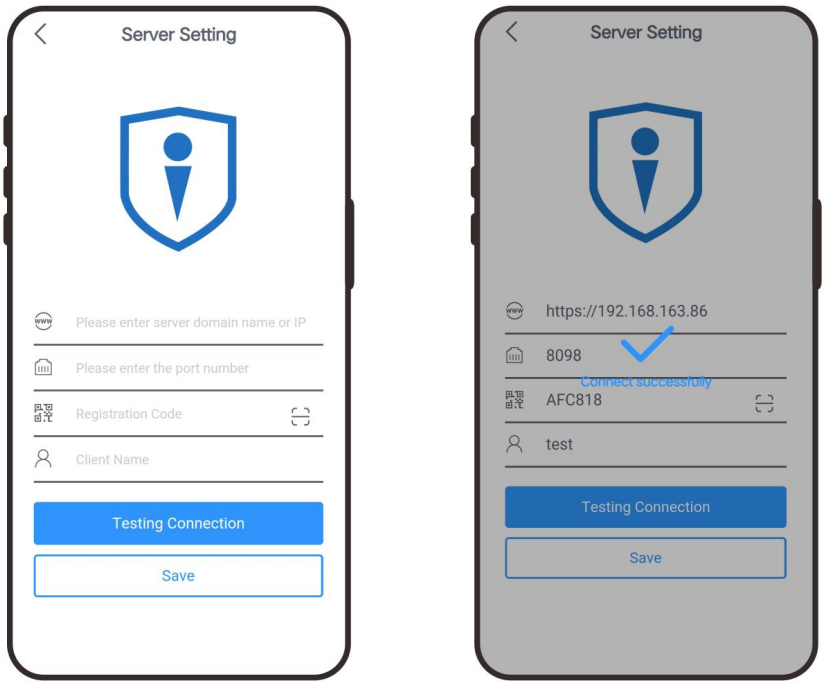


3. Open the App on the Smartphone. On the login screen, tap **Server Setting** and type the IP Address or the domain name of the Server, and its port number.

   Note: *Smartphone and the Server must be in the same network segment.*

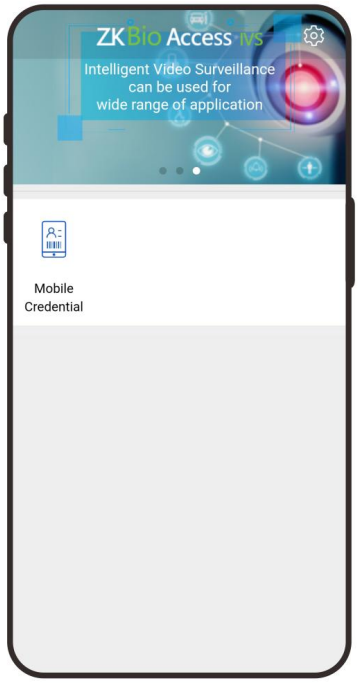
4. Tap the **QR Code** icon to scan the QR code of the new App client. After the client is identified successfully, set the client's name and tap **Connection Test**.

5. After the network is connected successfully, tap **Save**.

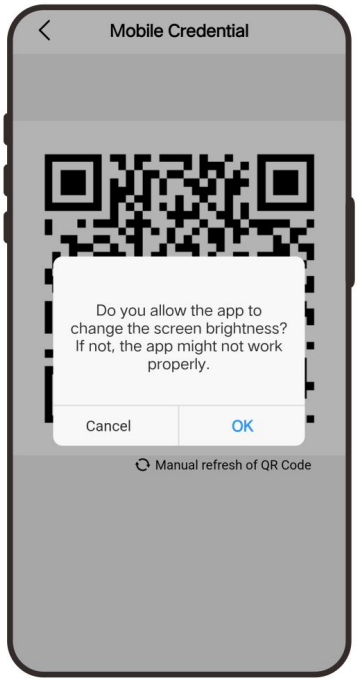


The Mobile Credential function is only valid when logging in as an employee, tap on Employee to switch to employee login screen. Enter the employee ID and password (Default: 123456) to login.

6. 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.
7. The QR code can replace a physical card on a specific device to achieve contactless authentication to open the door.



8. 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:



9. The QR code refreshes automatically for every 30s and supports manual refresh.

Note: *For other specific operations, please refer to ZKBio CVAccess User Manual.*

9 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.

10 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.

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com