



新开普电子股份有限公司
NEWCAPEC ELECTRONICS CO., LTD.

I2 Access Control Controller User Manual

Newcapec Electronics Co., Ltd.

Declaration

Registered Trademark:



Company Address: No. 18 Yingchun Street, High-tech Industrial Development Zone,
Zhengzhou, Henan Province, China

Tel: +86-19069626452

Email: sales@newcapecglobal.com

Website: www.newcapecglobal.com

Privacy Protection Notice

- Newcapec respects user privacy and customer data ownership. Data generated by our products and devices belongs to the customer and is managed in accordance with the customer's system configuration and privacy management policies.
- Without the customer's explicit authorization, Newcapec will not proactively collect, access, or store customer terminal data. Device data remains under the customer's control. Data transmission or remote access will only be performed with the customer's authorization for specific purposes, such as technical maintenance, after-sales support, or system administration.
- Newcapec is committed to providing secure and reliable smart hardware solutions and helping customers meet applicable data protection requirements.

About This Document

- The copyright of this manual belongs to Newcapec. Without prior authorization from the company, modification or reproduction of this manual is strictly prohibited.
- This document applies to multiple product models. The actual product appearance and functions shall be subject to the physical product.
- Any loss or damage caused by failure to operate the product according to the instructions provided in this document shall be borne by the user.
- This document will be updated periodically in accordance with relevant laws and regulations in different regions. For the latest version, please refer to the printed manual or the official website. In case of any inconsistency between the printed version and the electronic version, the electronic version shall prevail.
- Newcapec reserves the right to modify any information contained in this document at any time. Updated content will be incorporated into the latest version of this document without prior notice.
- This document may contain technical inaccuracies, discrepancies with product functions or operations, or printing errors. Newcapec reserves the final right of interpretation.
- If the obtained PDF document cannot be opened, please use the latest version or a mainstream PDF reader to open it.

Document Revision History

No.	Version	Change Status*	Content	Date
1	1.0	A	Initial Version	2026-8-18

*Change Status: A——Added; M——Modified; D——Deleted

CONTENTS

1. Product Introduction	4
1.1. Purpose and Introduction	4
1.2. Product Appearance	4
1.3. Technical Specifications	5
2. Installation Instructions	5
2.1. Package Contents	5
2.2. Interface Description	5
2.2.1. I220	5
2.2.2. I240	8
2.3. Installation Steps	9
2.3.1. Cable Selection and Wiring	9
2.3.2. Device Installation and Wiring	12
2.3.2.1. Installation of Access Control Controller	12
2.3.2.2. Installation and Connection of Card Reader	12
3. Operation Instructions	16
3.1. Device Startup	16
3.2. Device Web Interface Overview	16
3.2.1. Web Login	16
3.2.2. Operating Status Display	16
4. Precautions / Daily Maintenance	20

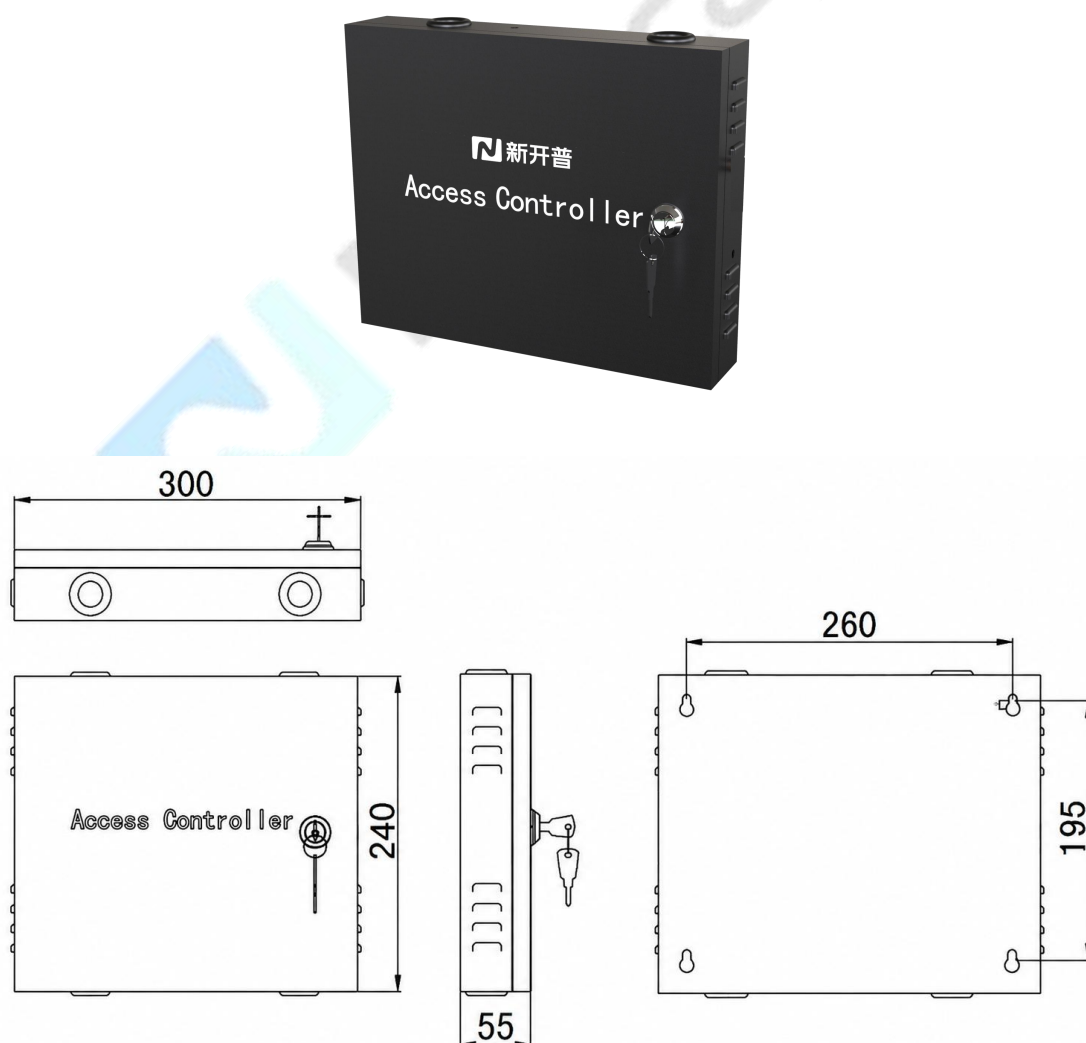
1. Product Introduction

1.1. Purpose and Introduction

The I2 Series Access Control Controller is based on TCP/IP communication and supports RFID card and dynamic QR code authentication, enabling centralized management of personnel access permissions. With strong compatibility, it can integrate with various terminal devices, including card readers and facial recognition terminals, access control terminals, and electronic door locks, making it suitable for a wide range of access control application scenarios.

1.2. Product Appearance

Model: I2. Product dimensions are shown below



1.3. Technical Specifications

Mode	I220	I240
Access Control Channels	2 channels: Single-door two-way control / Two-door one-way control	4 channels: Two-door two-way control / Four-door one-way control
User Capacity	200,000 users	400,000 users
External Interfaces	Wiegand × 2, Exit Button × 2, Relay × 2, Door Sensor × 2, Alarm Input × 2, Output × 2	Wiegand × 4, Exit Button × 4, Relay × 4, Door Sensor × 4, Alarm Input × 4, Output × 4
Power Supply Voltage	AC 220V ± 10%	
Authentication Methods	QR Code, Card, PIN	
PIN Keypad	Supported	
Reader Data Format	WG26, WG34	
Communication Interface	TCP/IP	
Dimensions	300 × 240 × 55 mm	
Operating Temperature	-10°C to 65°C	

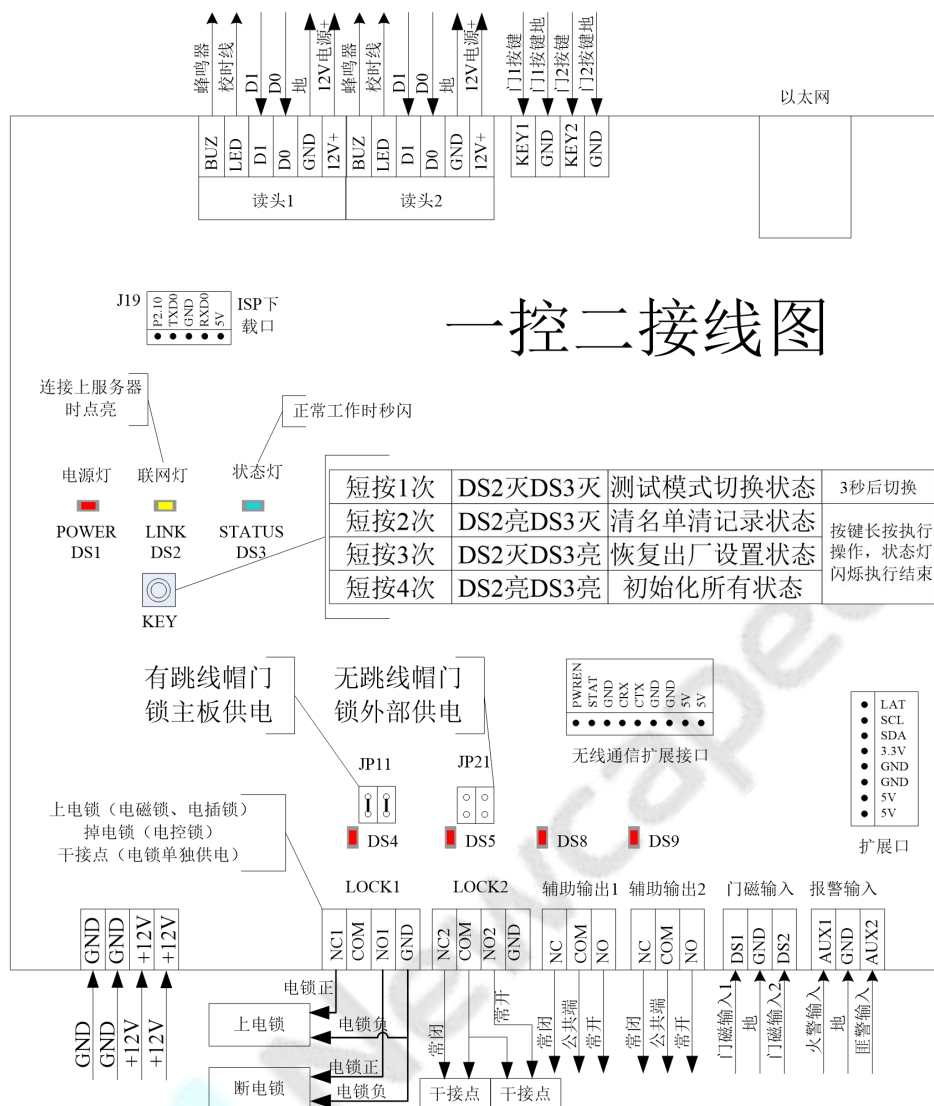
2. Installation Instructions

2.1. Package Contents

Accessory Name	Unit	Quantity
Access Control Controller	Set	1
Phillips Pan Head Self-Tapping Screw	pcs	4
Expansion Tube	pcs	4
User Manual	copy	1
Access Control Controller	Set	1

2.2. Interface Description

2.2.1. I220

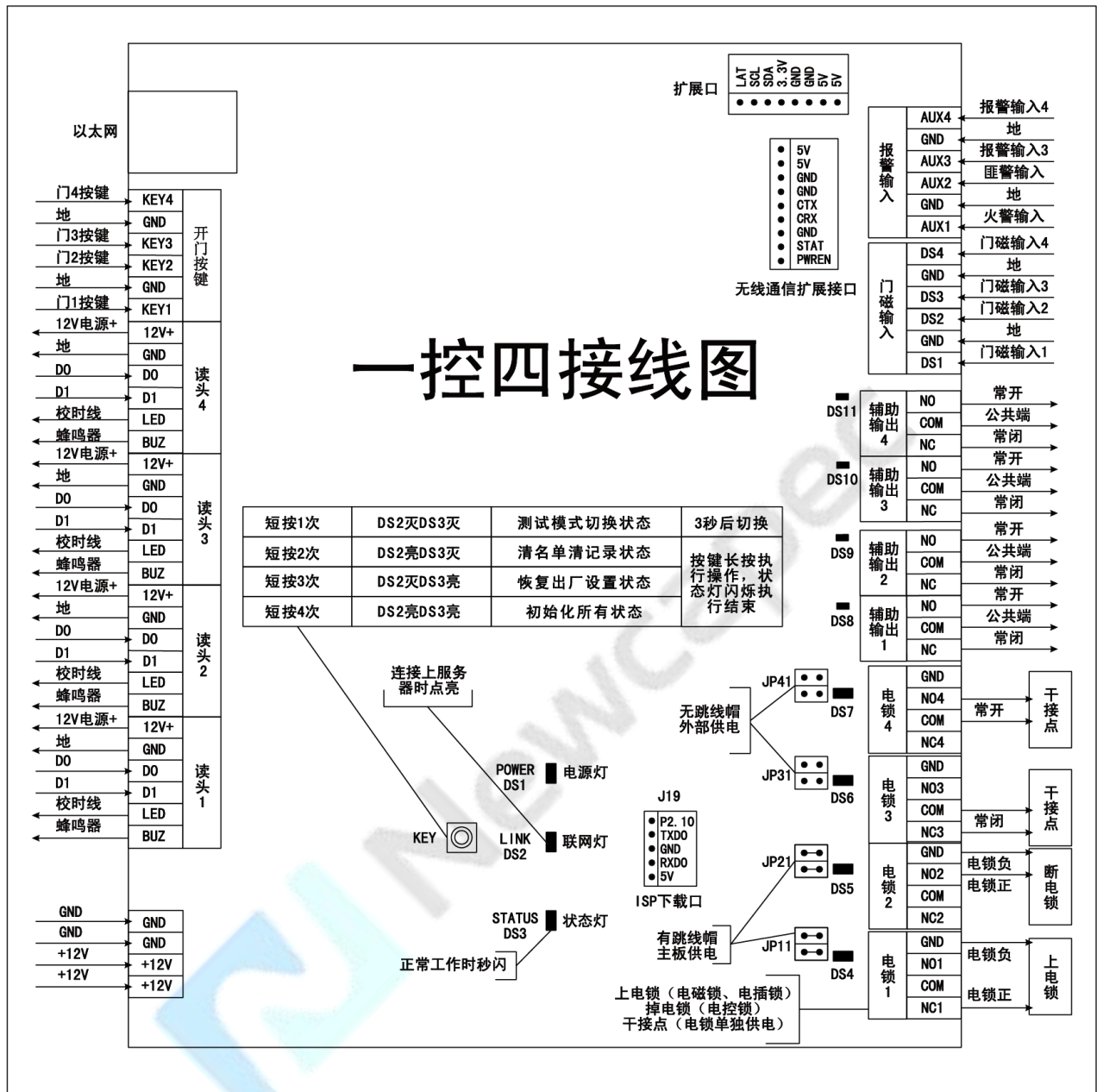


- The KEY function button can be used to enter/exit test mode, clear user data, clear access records, restore factory settings, and perform initialization operations.
- Single-door or double-door mode settings are configured through the Web interface. The default mode is two-door one-way control (each access control channel includes one lock and one reader).
- In single-door two-way mode: RD1 is connected to the entry card reader, RD2 is connected to the exit card reader, and the exit buttons can be connected to either KEY1 or KEY2. In this mode, LOCK1 and LOCK2 operate simultaneously.
- In two-door one-way mode:
LOCK1, RD1, KEY1, MAG1, ALM1, and Alarm Output 1 form one access control channel; LOCK2, RD2, KEY2, MAG2, ALM2, and Alarm Output 2 form another access control channel.
- LOCK1 and LOCK2 correspond to the door locks of Door 1 and Door 2

respectively. Select NO for power-off unlocking (fail-safe lock) and NC for power-on unlocking (fail-secure lock).

- P11 and JP21 are power supply jumpers for the electric locks of the two access control channels, corresponding to Door 1 and Door 2 respectively. With the jumper cap installed, the lock is powered by the controller mainboard; without the jumper cap, an external power supply is required.
- Auxiliary Outputs 1–4 correspond to access control channels 1–4 respectively. The auxiliary output control can be configured through software as alarm output relays or linkage control relays. Alarm outputs can be used to control alarm lights or alarm devices. The alarm output function must be enabled in the software. When enabled, the relay will activate upon illegal card access attempts.
- ALM1 is the fire alarm input, and ALM2 is the security alarm input. Both require dry contact signals provided by the alarm system. When ALM1 or ALM2 is short-circuited with GND, the controller will unlock the corresponding door and keep it open. Normal operation can only be restored by restarting the controller.
- When controlling turnstiles or sliding gates, be sure to remove JP11 and JP21 and use COM and NO relay outputs for control.

2.2.2. I240



- The KEY function button can be used to enter/exit test mode, clear user data, clear access records, restore factory settings, and perform initialization operations.
- Single-door or multi-door mode settings are configured through the Web interface. The default mode is four-door one-way control (each channel includes one lock and one reader), and it can be configured as two-door two-way control.
- In two-door two-way mode:
RD1 connects to the entry card reader of Door 1, and RD2 connects to the exit card reader of Door 1. The exit button can be connected to either KEY1 or KEY2. LOCK1 and LOCK2 operate simultaneously.

RD3 connects to the entry card reader of Door 3, and RD4 connects to the exit card reader of Door 3. The exit button can be connected to either KEY3 or KEY4. LOCK3 and LOCK4 operate simultaneously.

- Electric Locks 1–4 correspond to the four door locks respectively. Select NO for power-off unlocking (fail-safe lock) and NC for power-on unlocking (fail-secure lock).
- JP11, JP21, JP31, and JP41 are power supply jumpers for the four electric lock channels, corresponding to Door 1, Door 2, Door 3, and Door 4 respectively. With the jumper cap installed, the lock is powered by the controller mainboard; without the jumper cap, an external power supply is required.
- Auxiliary Outputs 1–4 correspond to access control channels 1–4 respectively. The auxiliary output control can be configured through software as alarm output relays or linkage control relays. Alarm outputs can be used to control alarm lights or alarm devices. The alarm output function must be enabled in the software. When enabled, the relay will activate upon illegal card access attempts.
- ALM1 is the controller's general fire alarm input and requires a dry contact signal from the fire alarm system. When ALM1 is short-circuited with GND, the controller will unlock all doors and keep them open. Normal operation can only be restored by restarting the controller.
- When controlling turnstiles or sliding gates, be sure to remove JP11, JP21, JP31, and JP41, and use the COM and NO relay outputs for control.

2.3. Installation Steps

2.3.1. Cable Selection and Wiring

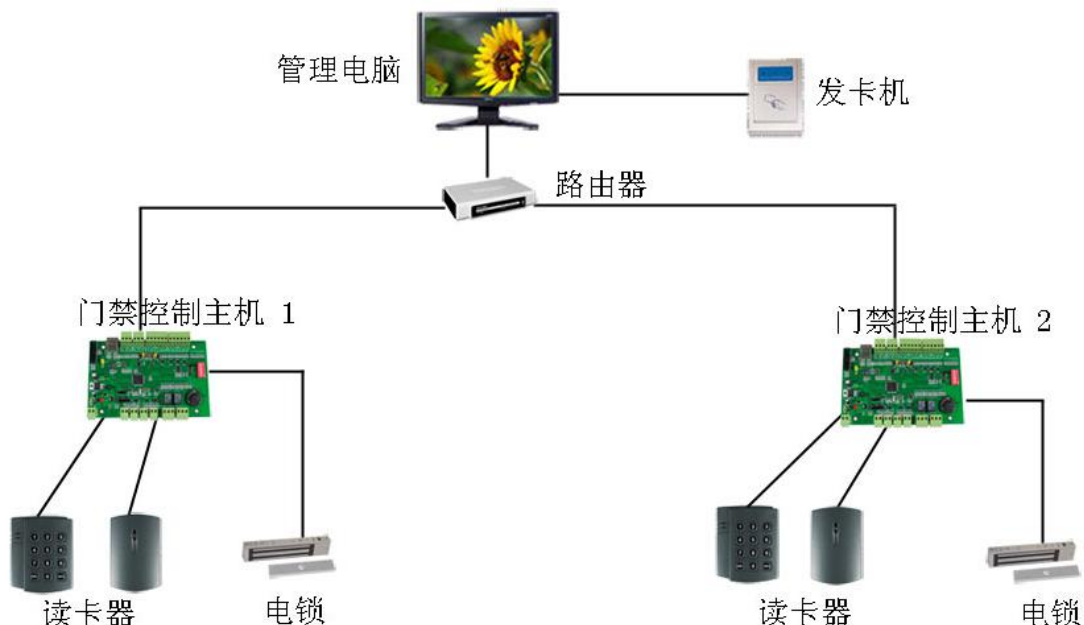
2.3.1.1. Wiring and Connection Precautions

- All wiring must be installed inside protective conduits. Both PVC conduits and galvanized metal conduits are acceptable to prevent cable damage caused by rodents. It is strongly recommended that all system wiring be routed separately from 220V high-voltage power cables in independent conduits.
- Although the controller is designed with excellent ESD protection, lightning protection, and leakage protection, ensure that the controller enclosure is properly connected to the AC grounding wire, and that the AC ground is reliably connected

to earth.

- Avoid frequently plugging or unplugging terminal blocks while the device is powered on. Always disconnect the terminal blocks before performing any wiring or soldering operations.
- Do not disassemble or replace controller chips without authorization. Improper operations by non-professionals may cause permanent damage to the controller.
- Do not connect additional third-party devices without authorization. For any non-standard installation or operation, please consult our engineers in advance.
- For power supply, do not connect the controller to the same power outlet as other high-current devices.
- The recommended installation height for card readers and exit buttons is 1.45 meters above the ground. The height can be adjusted according to customer usage requirements.
- The controller is recommended to be installed on the indoor side of the door, such as on the ceiling or inside a weak-current equipment room, where maintenance is convenient.
- Follow proper wiring practices for terminal blocks. Avoid excessive exposed metal wire length to prevent short circuits and communication failures.
- For wire connections, it is recommended to use soldering or wire crimp caps. Twisted wire connections may easily result in poor contact and unstable operation.

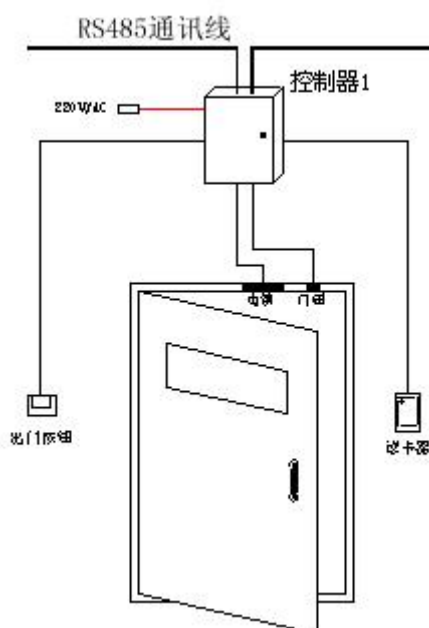
2.3.1.2.TCP/IP Network Cabling Guidelines



- TCP/IP communication supports multiple controllers operating simultaneously.
- The controller can be directly connected to a computer via an Ethernet cable for configuration.

2.3.1.3.Each Access Control Unit — Cable Selection and Wiring Guidelines

Each access control unit consists of an access control controller, card reader, electric lock, exit button, door sensor, infrared sensor, and other devices. The distance between the access control controller and the door should generally not exceed 100 meters. The following diagram shows a single-door access control system configuration:



1) Card Reader Cable:

The cable between the card reader and the controller port is recommended to use RVVP $6 \times 0.5 \text{ mm}^2$ shielded signal cable (two of the wires are used for the exit button). The maximum cable length should not exceed 100 meters. The shield wire should be connected to the controller GND.

2) Exit Button Cable:

The cable between the exit button and the controller port is recommended to use a 2-core cable with a conductor cross-sectional area of 0.5 mm^2 or above.

3) Electric Lock Cable:

The cable between the electric lock and the controller port is recommended to use a 2-core power cable with a conductor cross-sectional area of 1.0 mm^2 or above.

If the cable length exceeds 50 meters, it is recommended to use a 2.5 mm² cable, or adjust the power supply output voltage to approximately 14V using the power supply adjustment knob. The maximum cable length should not exceed 100 meters. For longer distances, an independent power supply method can be considered, where the electric lock and card reader are powered by a dedicated power supply installed near the door. In this case, the lock control cable requirements can be reduced, but the cable size should still be no less than 0.5 mm².

4) Door Sensor Cable:

The cable between the door sensor and the controller port is recommended to use a 2-core cable with a conductor cross-sectional area of 0.5 mm² or above.

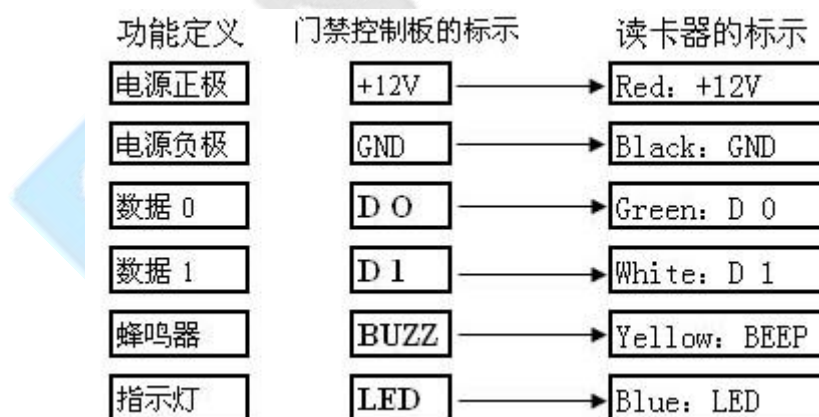
If real-time door status monitoring, door-open timeout alarms, or illegal entry alarms are not required, the door sensor cable can be omitted.

2.3.2. Device Installation and Wiring

2.3.2.1. Installation of Access Control Controller

It is recommended to install the controller on the indoor wall, ceiling, or inside a weak current equipment room where maintenance is convenient.

2.3.2.2. Installation and Connection of Card Reader



- Install the card reader outside or inside the door. The recommended installation height is 1.45 meters above the ground, which can be adjusted according to customer usage requirements. When card readers are required for both entry and exit, the two readers should be installed at least 1 meter apart. Avoid installing them directly opposite each other to prevent signal interference.
- Buzzer (BUZ) Connection Function:

When the controller detects an unauthorized card, the card reader buzzer will sound two or three beeps as an alarm indication. For a valid card, the buzzer will sound one beep.

- LED Indicator Connection Function:

When the controller detects an unauthorized card, the reader indicator light will only change momentarily. For a valid card, the indicator changes from red to green for several seconds (the same duration as the controller relay unlock time).

- The interface definitions and wire assignments of the card reader shall be based on the specifications provided in the card reader user manual.

2.3.2.3.QR Code Scanner Installation (Special Access Control Controller Models)

The installation requirements are basically the same as those for the card reader. The wiring connection between the QR code scanner and the access control controller is shown below:

门禁控制器（扫码版）	扫码头
12V（5V）	电源正
GND	电源负
RX(B)	TX(B)
TX(A)	RX(A)

The access control controller provides DC 12V and DC 5V power outputs to supply QR code scanners with different voltage requirements. It supports RS232 and RS485 communication interfaces (TTL serial communication is reserved).

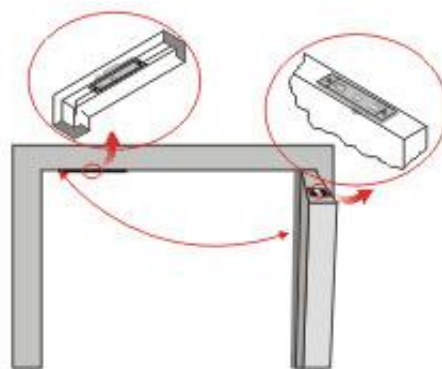
For long-distance transmission, a DC 12V / RS485 QR code scanner is required. The communication baud rate is 9600 bps.

2.3.2.4.Installation and Connection of Electric Lock and Power Supply

2.3.2.4.1.Electric Drop Bolt Lock Installation

The electric drop bolt lock is commonly used for single/double glass doors, framed glass doors with no bottom frame, frameless glass doors, and single/double wooden doors. It is typically installed above the door on the handle side.

The following figure shows an installation example for a single wooden door.

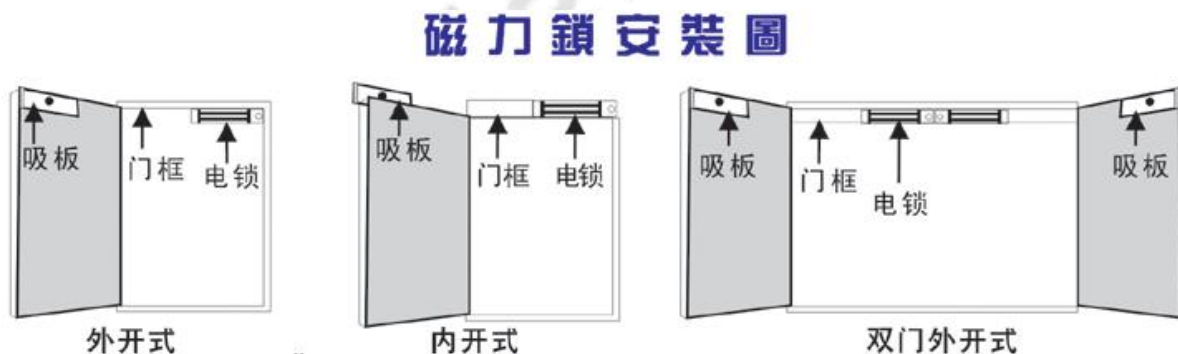


电插锁安装效果图

The electric drop bolt lock uses magnetic sensing for locking. The lock can only engage after detecting the magnet on the strike plate. The strike plate is generally installed on the upper part of the door leaf. When the door is closed, the magnet on the strike plate aligns with the internal sensor of the lock, triggering automatic locking. Therefore, the door can automatically lock after it is properly closed.

2.3.2.4.2. Magnetic Lock Installation

The magnetic lock is commonly used for metal doors and fire doors. The following figure shows an installation example for a fire door.



2.3.2.4.3. Wiring of Electric Lock, Access Control Controller, and Electric Lock Power Supply

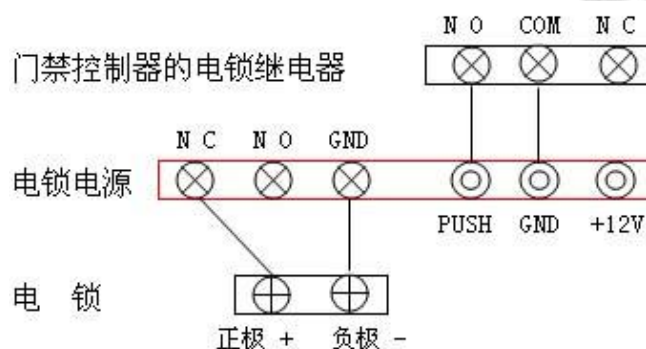
Different types of electric locks require different wiring methods. Electric locks are generally classified into Normally Open (NO) and Normally Closed (NC) types. The unlocking and locking operations are controlled by the electric lock relay of the access control controller.

- 1) Connection with Dedicated Access Control Power Supply

It is recommended to connect the normally open contact (NO) of the access control controller's electric lock relay to the PUSH or HANDLE terminal of the power supply, and connect the common terminal (COM) to the power supply negative terminal (GND).

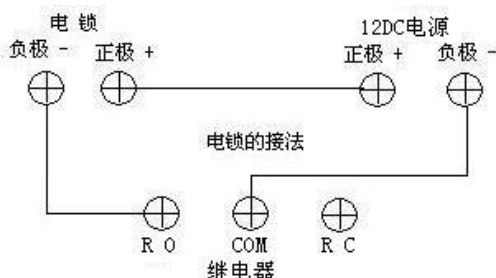
Direct Connection of Electric Lock to Power Supply:

- For normally closed locks, such as electric drop bolt locks, connect the positive terminal (+) of the lock to the power supply NC (Normally Closed) terminal, and connect the negative terminal (-) to the COM terminal.
- For normally open locks, such as electric strike locks, connect the positive terminal (+) of the lock to the power supply NO (Normally Open) terminal, and connect the negative terminal (-) to the COM terminal.



2) The wiring diagram for connection with a 12V DC power supply is shown below (the power supply is integrated inside the access control controller):

- For normally open locks, such as electric strike locks and electronic locks, connect them as shown below:



- For normally closed locks, such as electric drop bolt locks and magnetic locks, connect them as shown below:

3. Operation Instructions

3.1. Device Startup

After completing the device installation according to Section 2.3, connect the device to the power supply. The device will automatically power on and start up.

3.2. Device Web Interface Overview

3.2.1. Web Login

First, ensure that the computer and the device are on the same network segment. The default IP address of the access control controller is 192.168.131.200. Open the Internet Explorer (IE) browser, enter the IP address in the address bar, and press Enter. The following login interface will appear:

The username is 'admin', and the default password is blank.



3.2.2. Operating Status Display

The Operating Status Display page allows users to conveniently view device information, operating parameters, and door status information. It helps monitor device connectivity and operating conditions during system commissioning and setup.

The following figure shows the I240 Access Control Controller interface as an example:

- 运行状态
- 网络参数设置
- 控制参数设置
- 恢复出厂设置
- 测试界面
- 退出登陆

控制器信息					
设备类型	硬件版本	软件版本	终端编号	终端日期	终端时间
一控四门禁控制器	1.01	2.00A	AD54DE28	2013-12-05	16:02:44
MAC地址	IP地址	默认网关	子网掩码	未上传记录	运行时间
00-AD-54-DE-E8-4F	192.168.131.201	192.168.131.254	255.255.255.0	7	0小时51分
采集IP地址	采集端口	是否联机	代理IP地址	代理端口	代理是否启用
192.168.131.44	5035	未连接	192.168.131.44	5033	未启用

控制参数信息					
关门延时	超时未关延时	多卡开门延时	多卡开门数量	假日授权	假日开始日期
3s	3s	0s	0张	0	2012-01-01
假日名单个数	非法卡报警	内外校验	单双门设置	平时空闲模式	假日空闲模式
0	不允许	不启用	四门单向	刷卡开门	禁用

门1信息							
授权个数	门状态	工作模式	周计划版本	防潜回组	互锁组	联动控制	报警输出
0	关	刷卡开门	0000000000	无	无	禁止	禁止

门2信息							
授权个数	门状态	工作模式	周计划版本	防潜回组	互锁组	联动控制	报警输出
0	关	刷卡开门	0000000000	无	无	禁止	禁止

门3信息							
授权个数	门状态	工作模式	周计划版本	防潜回组	互锁组	联动控制	报警输出
0	关	刷卡开门	0000000000	无	无	禁止	禁止

门4信息							
授权个数	门状态	工作模式	周计划版本	防潜回组	互锁组	联动控制	报警输出
0	关	刷卡开门	0000000000	无	无	禁止	禁止

3.2.3. Network Parameter Settings

The Network Parameter Settings page allows users to modify the device IP parameters, acquisition server IP address, port parameters, and proxy server-related settings. After completing the modifications, click Submit to save the changes. Click Reset to reload and display the parameters saved on the device.

Note: After submitting changes to the IP parameters, the device must be accessed using the new IP address.

- 运行状态
- 网络参数设置
- 控制参数设置
- 恢复出厂设置
- 安全设置
- 测试界面
- 退出登陆

- 基础设置

IP地址: 192.168.131.202
默认网关: 192.168.131.254
子网掩码: 255.255.255.0

- 采集服务器设置

采集服务IP地址: 192.168.131.31
采集服务器端口: 5033

- 代理服务器设置

是否启用: ☒ 不启用 ☐ 启用
代理服务IP地址: 192.168.131.44
代理服务器端口: 5033
用户名: 888888
密码: 888888

提交 重置

3.2.4. Control Parameters

The Control Parameters page allows users to configure the connected platform, record storage method, single-door/double-door mode settings, and door operation mode during idle periods. The parameters are described as follows:

- 1) **Connected Platform:** Select the platform according to actual application requirements. In network mode, the access control controller needs to connect to the Access Control Management System (hereinafter referred to as the "platform") for operation. In network mode, the authorized user list is issued by the platform, and access permissions are managed by the platform. For system installation and commissioning details, please refer to the "Access Control Management System Commissioning Manual".
- 2) **Record Storage Method:** The default setting is "Do not save records when storage is full." It can be configured as "Do not save records" or "Overwrite records when storage is full." The latter two modes are suitable for devices that frequently operate offline.
- 3) **Single-Door / Double-Door Mode Settings:** The two-door controller supports single-door two-way control and two-door one-way control modes. The four-door controller supports four-door one-way control and two-door two-way control modes.
- 4) **Record Storage Type Settings:** Users can configure the types of access records to be stored.

运行状态

网络参数设置

控制参数设置

恢复出厂设置

安全设置

测试界面

退出登陆

门禁参数设置

对接平台: **老系统**

提示: 选择老系统支持接入V4.0.80TB.20131127之前版本的门禁管理系统, 及支持ARM门禁的一卡通平台, 新增功能(多卡、首卡、假日、扩展功能)不能使用。

选择新系统支持接入V4.0.80TB.20131127及更新版本的门禁管理系统, 多卡、首卡、假日等功能可以使用。

记录覆盖: **记录清不再保存**

单门设置: **四门单向**

平时空闲时段: **刷卡开门**

假日空闲时段: **禁用**

记录保存类型设置

☒ 正常刷卡记录 ☒ 试图开锁记录 ☒ 异常开锁记录 ☒ 按键开锁记录 ☒ 复位记录 ☒ 火警记录 ☒ 盗警记录

☒ 密码开门记录 ☒ 胁迫密码开门记录 ☒ 防拆报警记录 ☒ 强行开门记录 ☒ 身份证认证不通过记录

☒ 门禁开放时间未绑定 ☒ 用户开放时间未绑定 ☒ 未授权假日加班名单 ☒ 多卡开门记录

☒ 首卡开门记录 ☒ 互锁试图开门记录 ☒ 防潜回试图开门记录 ☒ 普通密码开门记录 **全选** **清空**

提示: 选中需要更改的功能后, 点击“提交”按钮可更改参数。点击“全选”按钮, 全选记录类型, 点击“清空”, 取消全选记录类型。

提交 **重置** **刷新** 提示: 控制器进入测试模式时, 按钮有效。

3.2.5. Factory Reset

The Control Parameters page allows users to clear the device's first card information, multi-card information, holiday information, user records, door access passwords, and system parameter information.

These operations require the device to be operating in Test Mode. The buttons are disabled when the device is not in Test Mode. The last button, "Exit Test Mode", can be used to exit Test Mode. The interface is shown below.

Restoring factory settings will reset the IP parameters to the default IP address and clear the device communication key.



3.2.6. Security Settings

This page is used to modify the Web login password. The interface is shown below:

Note: After the I220 and I240 access control controllers are connected to the platform, the Web login password will be automatically configured by the platform after the device is successfully activated. The default password is 888888, and it can be modified through the platform.



3.2.7. Test Interface

- Unlock Door: All relays on the mainboard will be activated.
- Lock Door: All relays on the mainboard will be deactivated.

- Time Synchronization: Synchronizes the time on the mainboard. If a card reader is connected (with the time synchronization cable connected), the card reader time can also be synchronized simultaneously. This function is used to verify whether the mainboard time synchronization function operates normally.
- Note: Test items not specifically described in this section are unreleased functions. Please do not operate them.



4. Precautions / Daily Maintenance

- Avoid exposure to rain and direct sunlight. The device must be protected from water and dust, and should be cleaned regularly.
- Avoid installing the product in extreme environments, such as prolonged exposure to sunlight, rain, sand, dust, or strong vibration.
- If any malfunction occurs during use, please refer to the User Manual or contact Newcapec for assistance.
- Avoid frequently powering the device on and off within a short period of time.