Access Controller

Quick Start Guide

V1.0.0

Foreward

General

This manual introduces the installation, functions and operations of the Access Controller (hereinafter referred to as the "Device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
ELECTRIC SHOCK	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	October 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Access Controller, hazard prevention, and prevention of property damage. Read carefully before using the Access Controller, and comply with the guidelines when using it.

Transportation Requirement

Transport, use and store the Access Controller under allowed humidity and temperature conditions.

Storage Requirement

Store the Access Controller under allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the Access Controller while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Access Controller.
- Do not connect the Access Controller to two or more kinds of power supplies, to avoid damage to the Access Controller.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Access Controller in a place exposed to sunlight or near heat sources.
- Keep the Access Controller away from dampness, dust, and soot.
- Install the Access Controller on a stable surface to prevent it from falling.
- Install the Access Controller in a well-ventilated place, and do not block its ventilation.

- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Access Controller is a class I electrical appliance. Make sure that the power supply of the Access Controller is connected to a power socket with protective earthing.

Operation Requirements

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Access Controller while the adapter is powered on.
- Operate the Access Controller within the rated range of power input and output.
- Use the Access Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Controller, and make sure that there is no object filled with liquid on the Access Controller to prevent liquid from flowing into it.
- Do not disassemble the Access Controller without professional instruction.
- This product is professional equipment.
- The Access Controller is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Structure

Figure 1-1 Access controller for single door (unit: mm [inch])

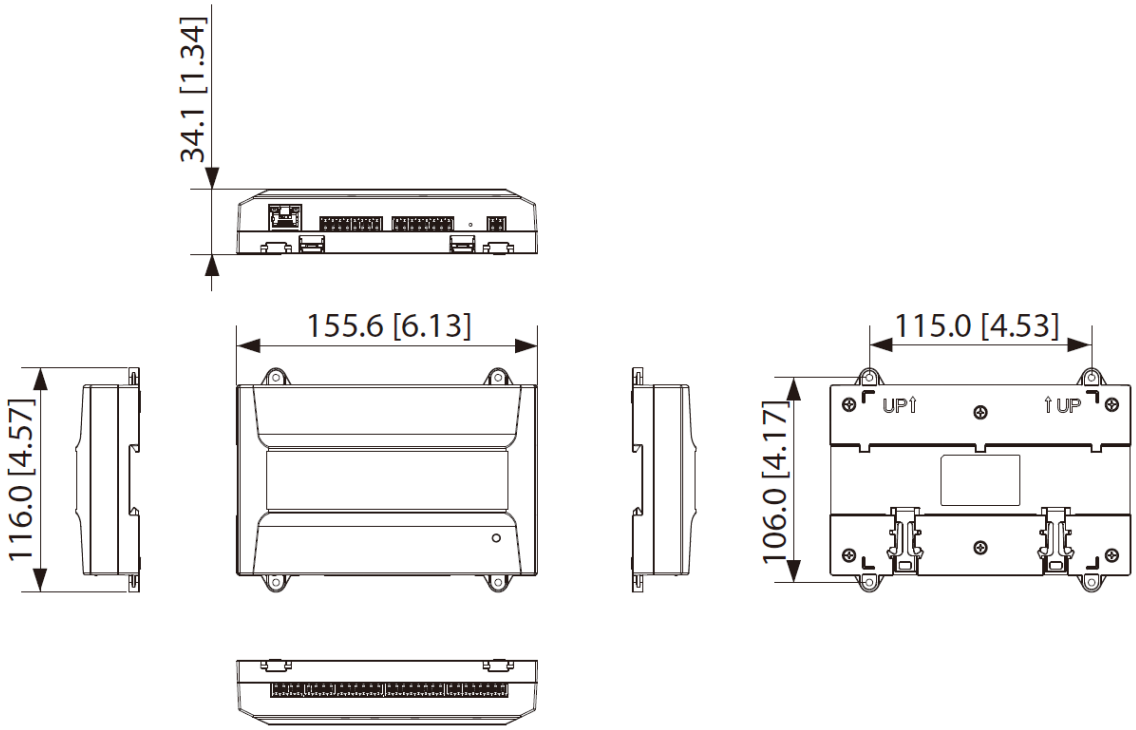


Figure 1-2 Access controller for 2 and 4 doors (unit: mm [inch])

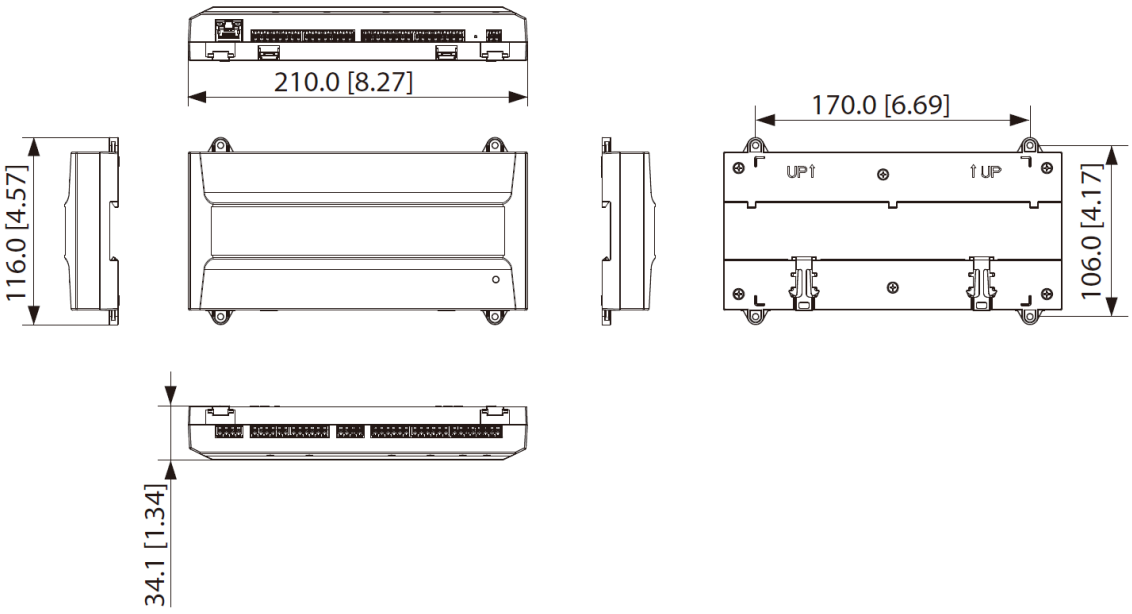
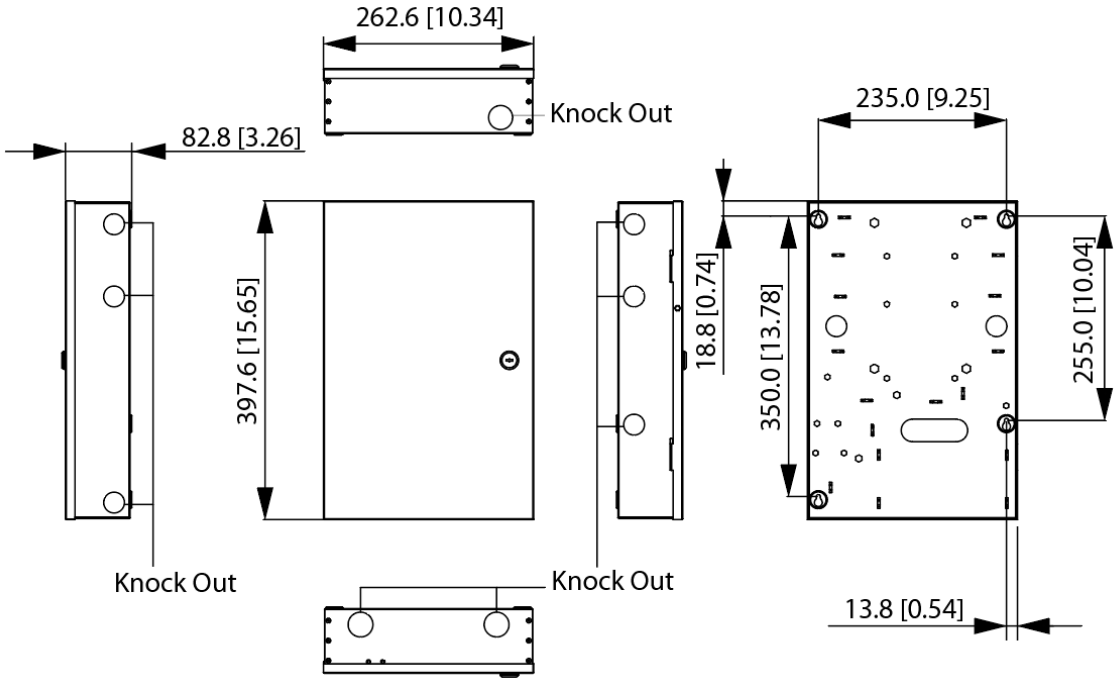


Figure 1-3 Access controller with battery (unit: mm [inch])



2 Wiring and Installation

2.1 Installation Procedure

2.1.1 Wall Mount (Linux B)

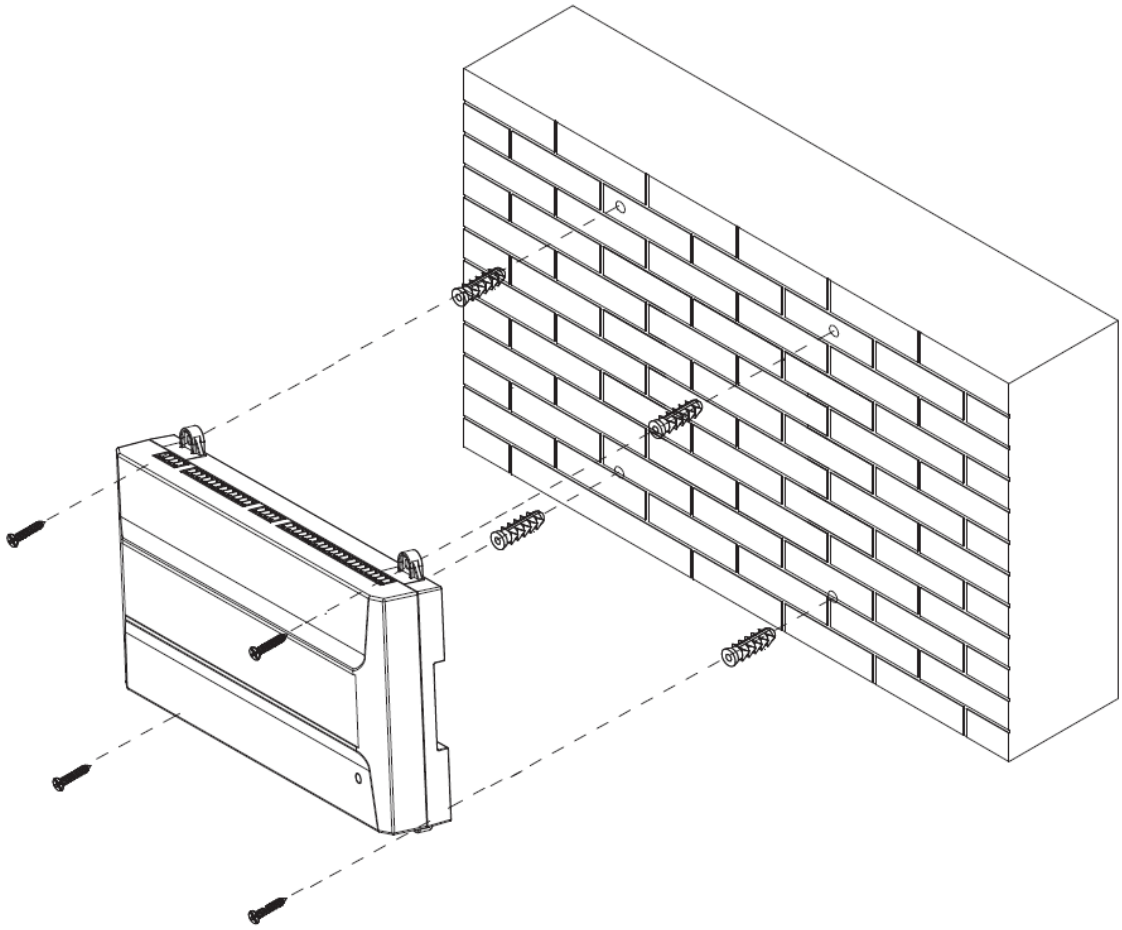
Procedure

Step 1 According the holes' position of the bracket, drill 4 holes in the wall, and then insert the expansion bolts in the holes.

Step 2 Use 4 screws to fix the Device to the wall.

Step 3 Wire the Access Controller. For details, see "2.2 Wiring (Linux B)".

Figure 2-1 Wall mount



2.1.2 Slide Rail Installation (Linux B)

Procedure

Step 1 Use screws to fix the U-shaped guide rail to the wall.

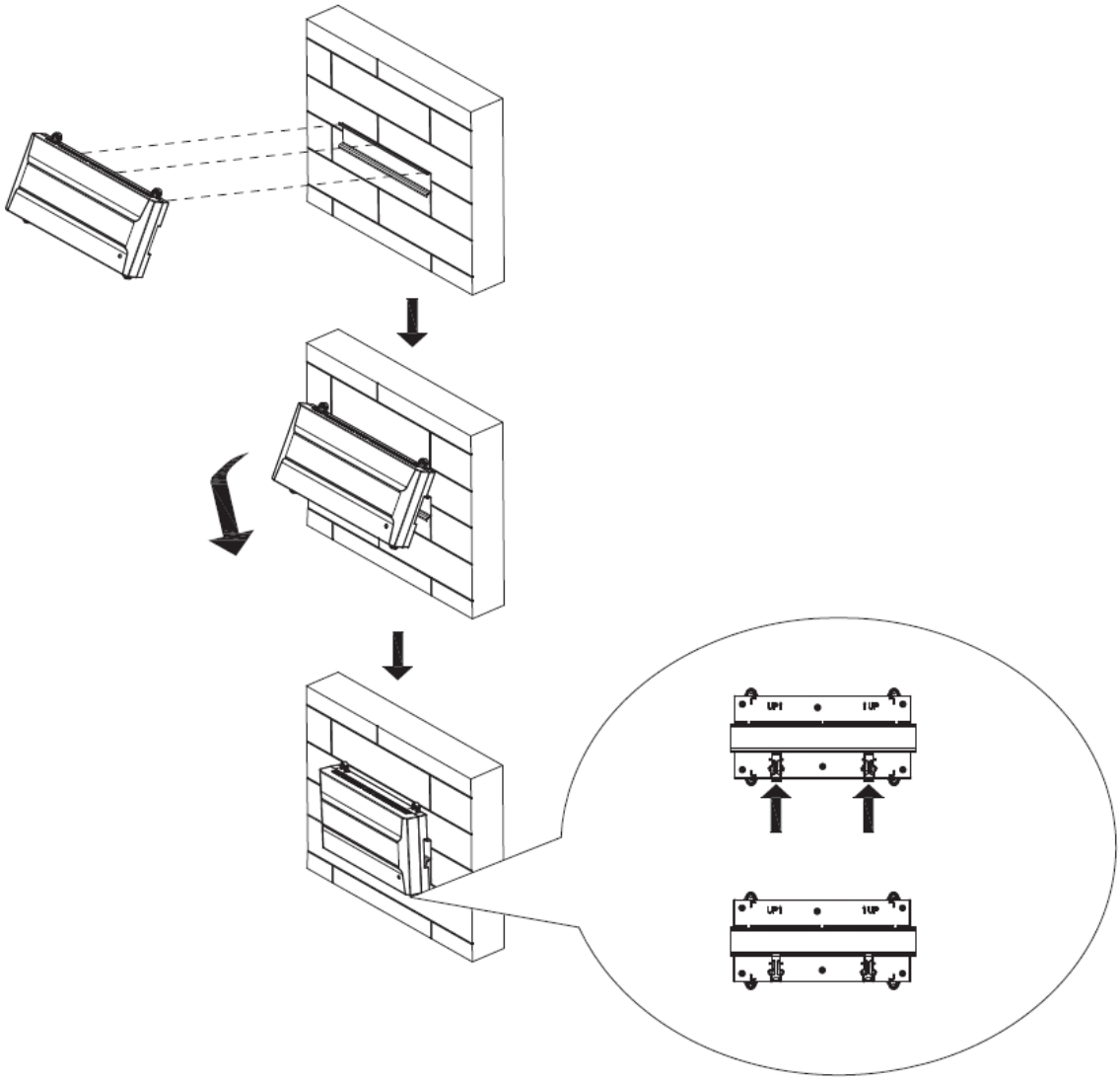
Step 2 Insert the device into the U-shaped rail slot.

Step 3 Push the clip at the bottom of the Device upwards.

After hearing a clicking sound, the installation is complete.

Step 4 Wire the Access Controller. For details, see "2.3.1 Components".

Figure 2-2 Slide rail installation



2.1.3 Wall Mount (Linux C)

Procedure

Step 1 According the holes' position of the bracket, drill 4 holes in the wall, and then insert the expansion bolts in the holes.

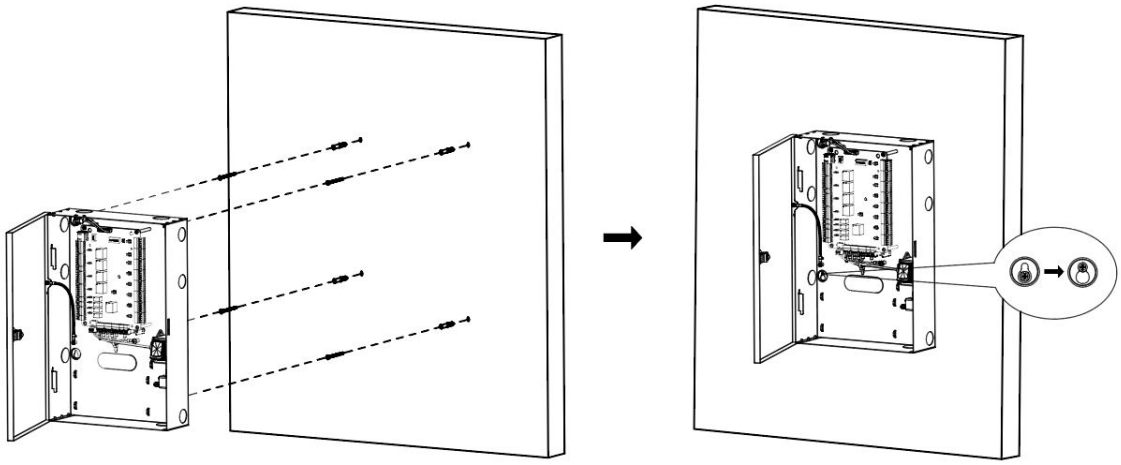
Step 2 Hammer in 4 screws, and then attach the Device to the wall.

Step 3 Remove the metal sheet according to the actual wiring situation.

Step 4 Wire the Access Controller. For details, see "2.3.1 Components".

Step 5 (Optional) Use the key to lock the cover of the controller.

Figure 2-3 Wall mount



2.2 Wiring (Linux B)

2.2.1 Components

Figure 2-4 Access controller (single door)

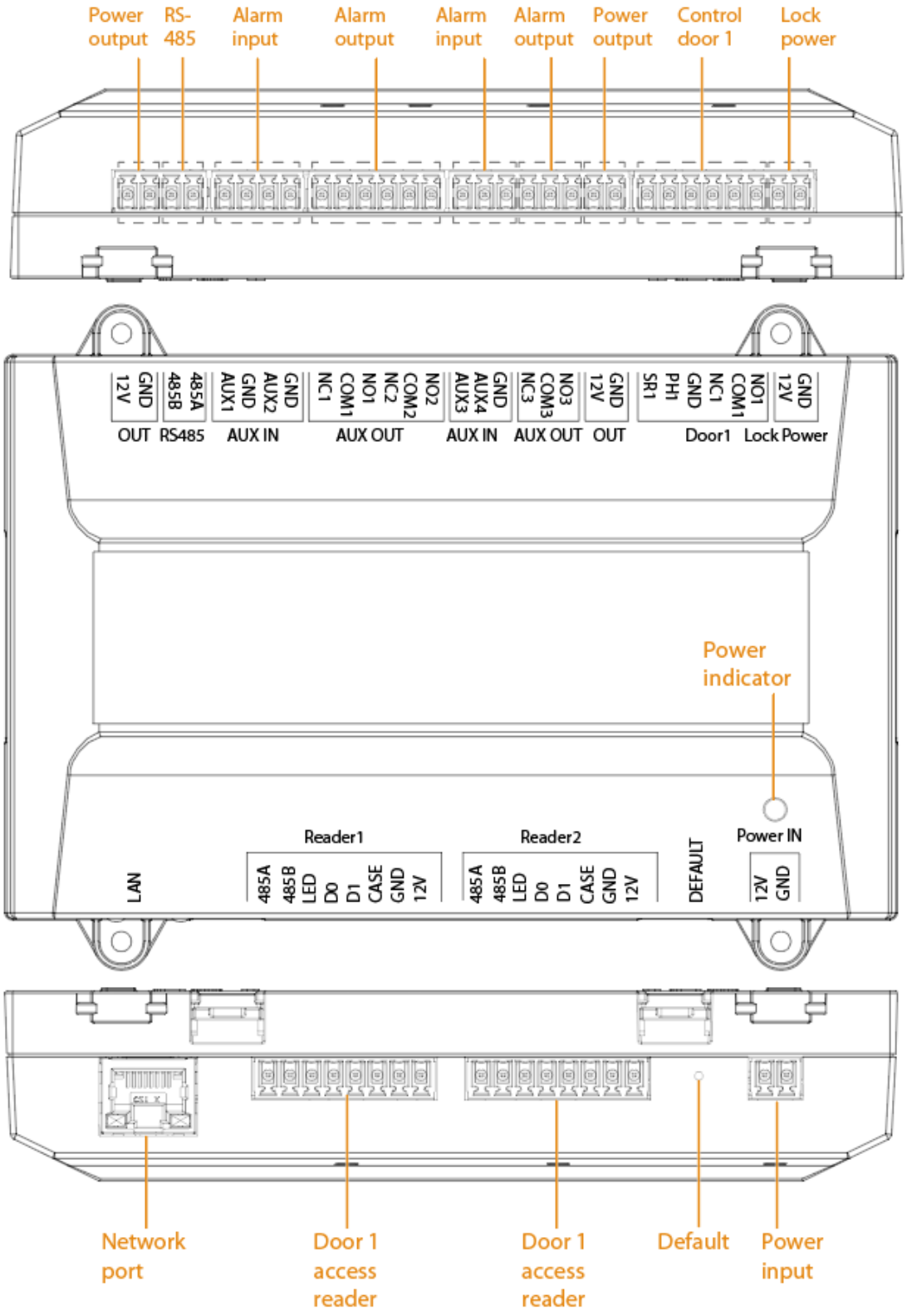


Figure 2-5 Access controller (2 doors)

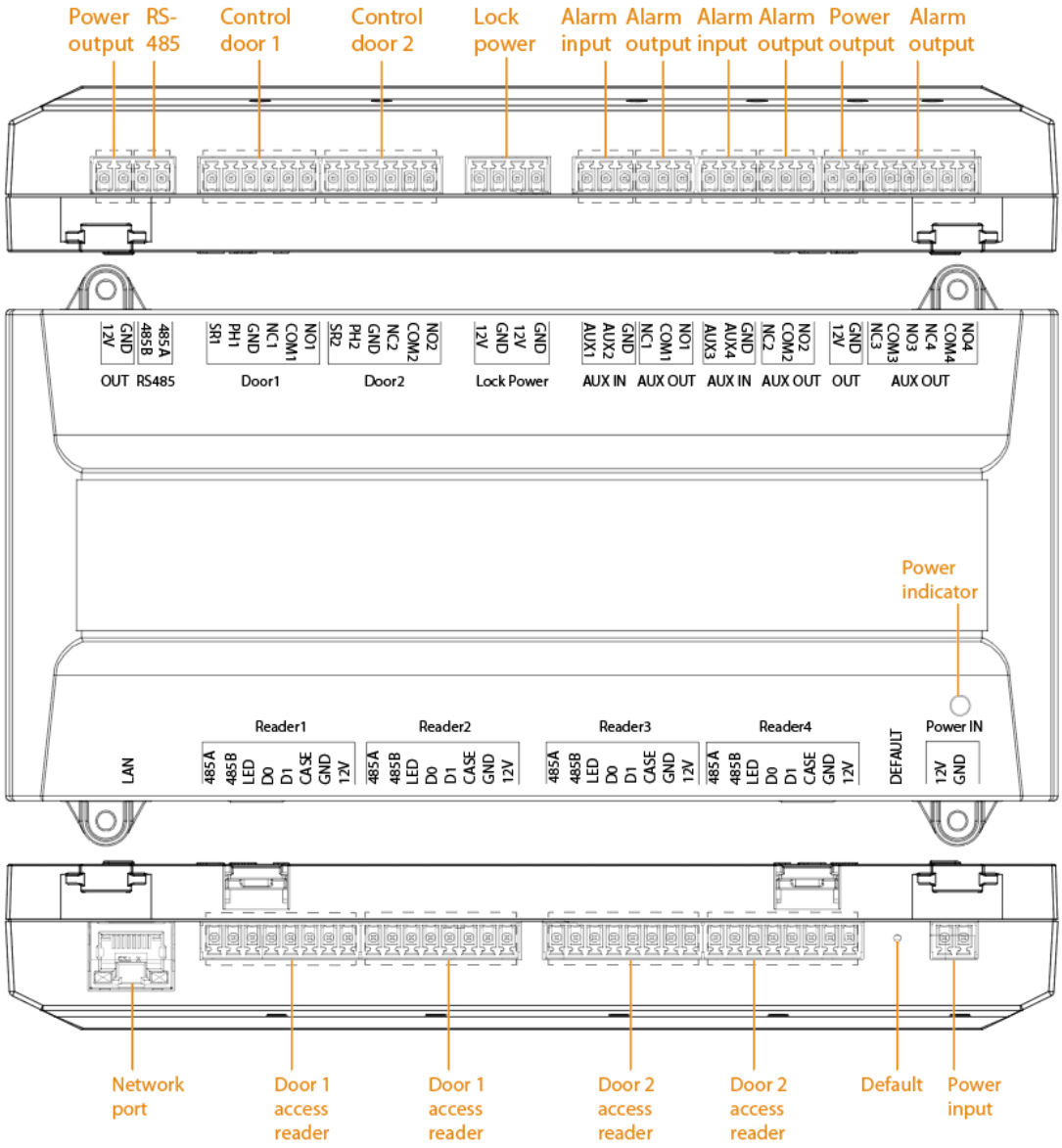
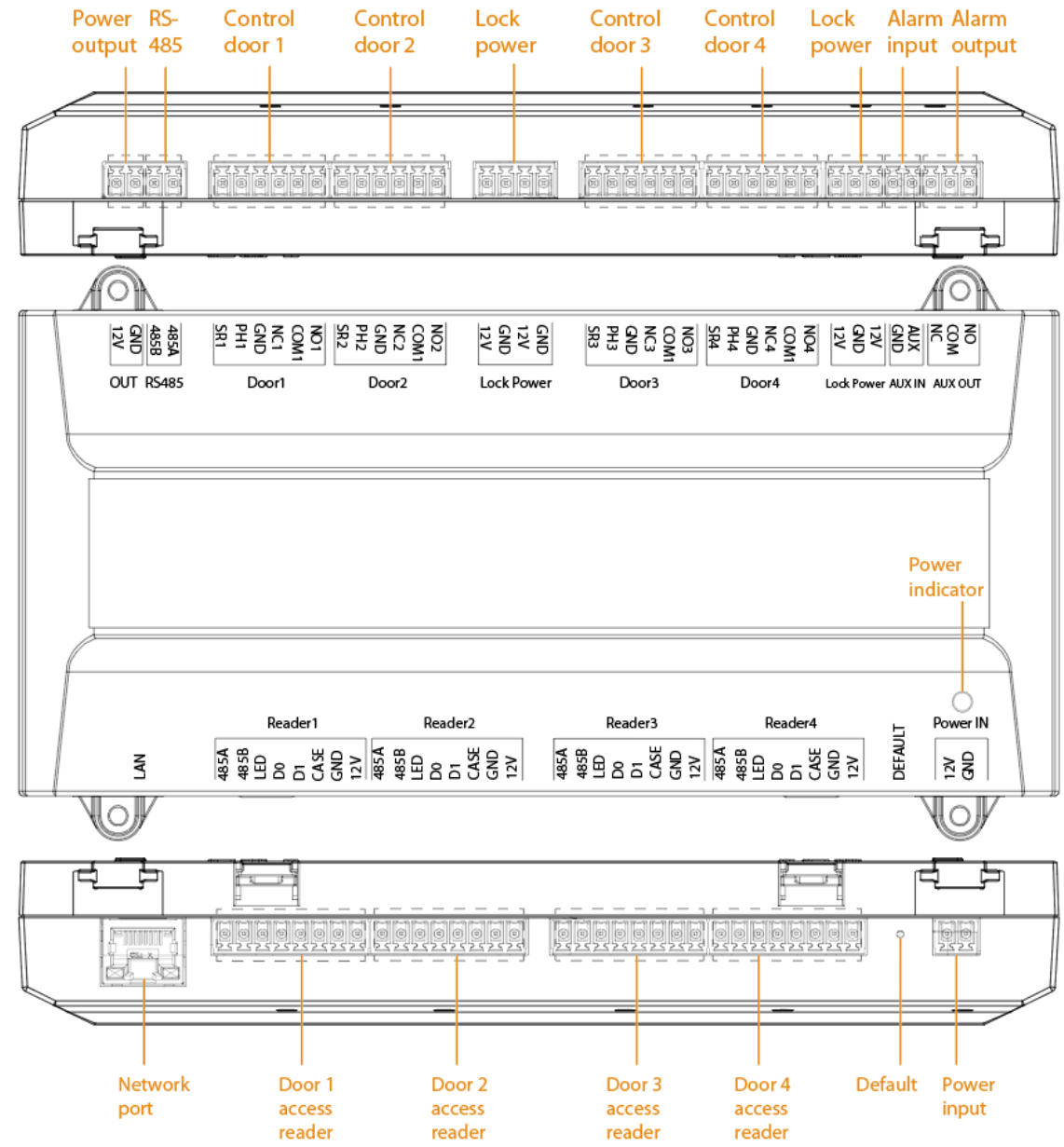


Figure 2-6 Access controller (4 doors)



When powered by PoE, the total power consumption must be less than 20 W.

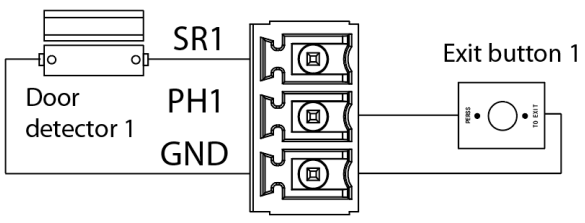
Table 2-1 Components description

Component	Description
OUT	Power output port. ● Access controller (single door or two doors): The OUT port next to RS-485 port supports the maximum current of 500 mA. Other OUT ports support the maximum current of 1 A. ● Access controller (four doors): The OUT port next to RS-485 port supports the maximum current of 500 mA.

Component	Description
RS485	Connects to external alarm module to expand 8-channel alarm input or 8-channel alarm output.
Door1 – Door4	Door control port. The connection method for the 4 ports is the same. • Access controller (single door): Connects to Door1 port. • Access controller (two doors): Connects to Door1 and Door2 ports. • Access controller (four doors): Connects to ports from Door1 to Door4.
Lock Power	The port for lock power output (12 VDC, 1.2 A).
AUX IN	Alarm input port. Connects to smoke detector and IR detector.
AUX OUT	Alarm output port. When there is external alarm signal input, you can configure alarm linkage output. The output channel and duration can be configured on the webpage of the Device.
Power Indicator	• Red: The system starts. • Green: The device is working normally.
LAN	Network port.
Reader1–Reader4	Access reader port. The connection method for the 4 ports is the same. The power of the reader supports 12 VDC and the current of 1 A.
DEFAULT	Restore the Device to default settings. • Restore to default settings (remain user information and logs): Press the DEFAULT key for 500 ms, and the Device beeps once. During the restoring process, the Device beeps all the time. If the Device stops beeping, it is restored to the default settings and automatically restarts. • Restore to factory settings: Press and hold the DEFAULT key for more than 5 seconds, and the Device beeps for 3 seconds. During the restoring process, the Device beeps all the time. If the Device stops beeping, it is restored to the factory settings and automatically restarts. Operate the restoring function within 5 minutes after the Device is powered on.
Power IN	Power input port (12 VDC).

2.2.2 Exit Button or Door Detector

Figure 2-7 Wiring of exit button or door detector



2.2.3 Cables Specification

Access controller supplies power for the access reader and the lock (select a power supply adapter with sufficient power based on the external load to supply power to the access control controller).

Figure 2-8 Power wiring

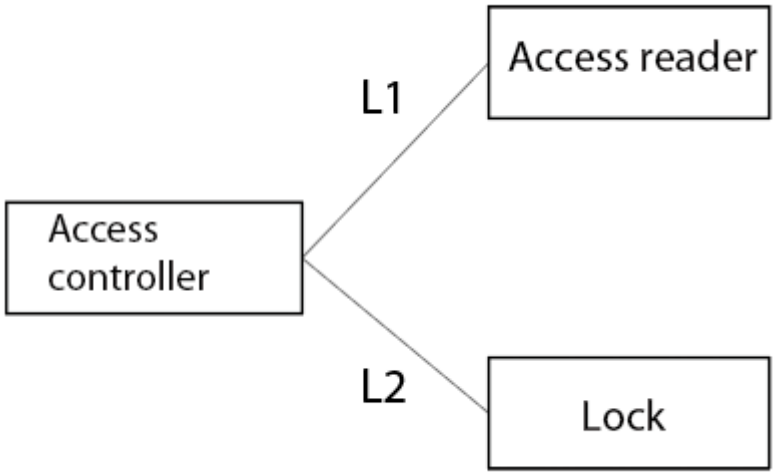


Table 2-2 Cable specification description

No.	Name	Recommended Model and Specification	Recommended Max Power Supply Distance
L1	Access Reader Cable	RVV2 × 1.0, RVV4 × 1.0 or CAT5E network cable ● RVV0.5 (DC resistance of a single conductor ≤ 39.0 Ω/km) ● RVV1.0 (DC resistance of a single conductor ≤ 19.5 Ω/km) ● RVV1.5 (DC resistance of a single conductor ≤ 13.3 Ω/km) ● CAT5E network cable (impedance within 100 m ≤ 9 Ω)	● RVV0.5 ◇ Less than 200 m for RS-485 access reader. ◇ Less than 120 m for Wiegand access reader. ● CAT5E (single cable) ◇ Less than 120 m for RS-485 access reader. ◇ Less than 50 m for Wiegand access reader.

No.	Name	Recommended Model and Specification	Recommended Max Power Supply Distance
L2	Lock Cable		• RVV0.5 ◇ Less than 20 m for 2 doors electromagnetic lock (280 kg). ◇ Less than 55 m for single door electromagnetic lock (280 kg). ◇ Less than 15 m for 2 doors electromagnetic lock (500 kg). ◇ Less than 45 m for single door electromagnetic lock (500 kg). • RVV1.0 ◇ Less than 35 m for 2 doors electromagnetic lock (280 kg). ◇ Less than 95 m for single door electromagnetic lock (280 kg). ◇ Less than 35 m for 2 doors electromagnetic lock (500 kg). ◇ Less than 95 m for single door electromagnetic lock (500 kg). • RVV1.5 ◇ Less than 75 m for 2 doors electromagnetic lock (280 kg). ◇ Less than 135 m for single door electromagnetic lock (280 kg). ◇ Less than 55 m for 2 doors electromagnetic lock (500 kg). ◇ Less than 135 m for single door electromagnetic lock (500 kg).

⚠

- If the access reader is powered by the access controller, it is recommended to select an access reader with a maximum current not exceeding 200 mA. The selected access reader should support wide voltage operation, with the lowest operating voltage not exceeding 9 V.
- If the lock is powered by the access controller, it is recommended to select a lock with a maximum current not exceeding 1,200 mA. The selected lock should support wide voltage operation, with the lowest operating voltage not exceeding 10 V.
- The wiring distance of L1 and L2 is affected by the voltage of the power supply and the power supply cable specification. During actual construction, the power supply voltage should be ensured not to be lower than the lowest operating voltage of the access standalone, access reader, and lock. Additionally, L1 and L2 should not use the same wire.
- When using CAT5E (impedance within 100 m ≤ 9 Ω) for the power supply of locks or access readers, it is recommended to allocate the extra wires, apart from the necessary signal wires, evenly for the power supply of locks or access readers in order to minimize power supply loss.
- The above data is measured under laboratory conditions and might differ from actual working conditions. It is for reference only.

2.2.4 Lock

Select the wiring method according to the lock type. The lock can be powered by access controller (connect to the **12V** and **GND** on **LOCK POWER** port of the access controller) or the external power supply.

Figure 2-9 Wiring of motor lock

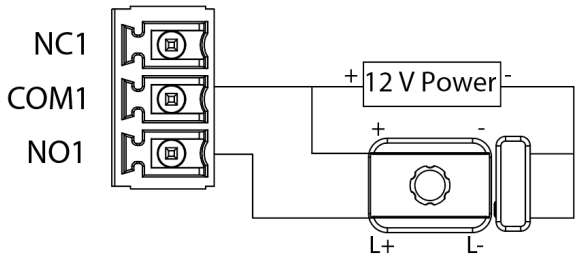


Figure 2-10 Wiring of electromagnetic lock

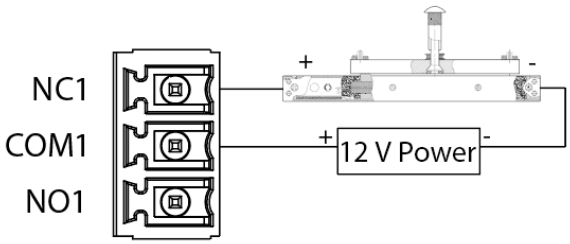


Figure 2-11 Wiring of electric bolt lock (open when powered off)

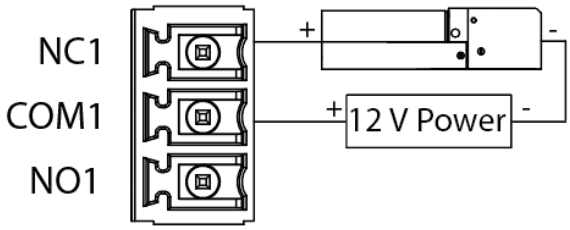
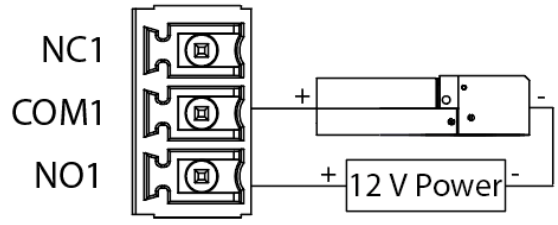


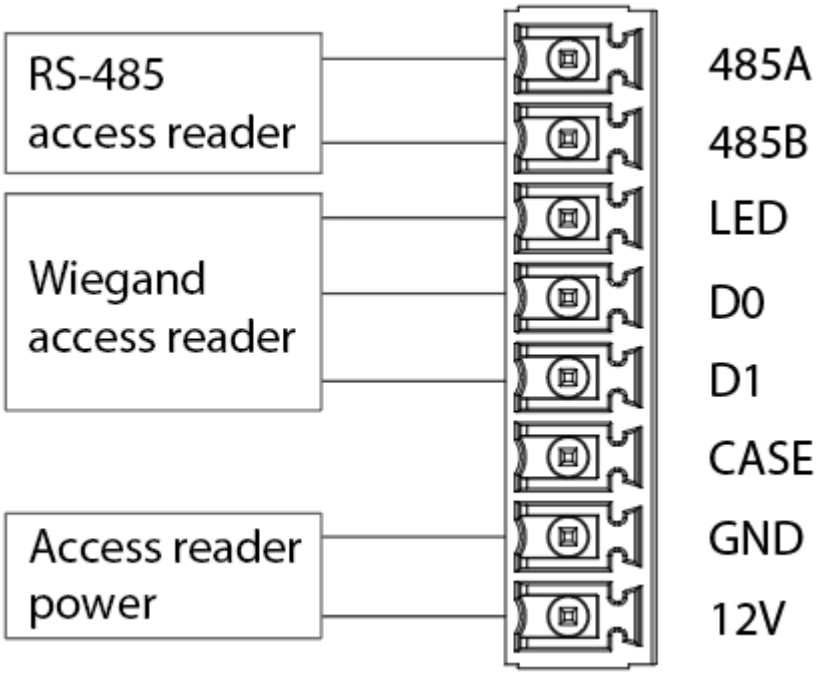
Figure 2-12 Wiring of electric bolt lock (close when powered off)



2.2.5 Access Reader

One access reader port can only connect to the access readers of the same type. Select from RS-485 access reader and Wiegand access reader.

Figure 2-13 Wiring of access reader



2.3 Wiring (Linux C)

2.3.1 Components

Wiring Instruction

- The door lock jumper cap connects to 1 and 2 by default.
  - Connecting 1 and 2 means COM is not powered, and the lock uses external power supply. COM serves as the common terminal. Wiring distribution should be done according to the actual type of lock used.
  - Connecting 2 and 3 means COM serves as a 12 V output terminal, supplying power to the lock from the COM terminal. Wiring distribution should be done according to the actual type of lock used.
- The alarm output jumper cap connects to 1 and 2 by default.
  - Connecting 1 and 2 means NO is the output terminal (dry contact), used for connecting normally open alarm devices.
  - Connecting 2 and 3 means NC is the output terminal (dry contact), used for connecting normally closed alarm devices.
- The fire alarm input port supports switching through dip switches to connect normally open or normally closed alarm devices.

Figure 2-14 Access controller (single door)

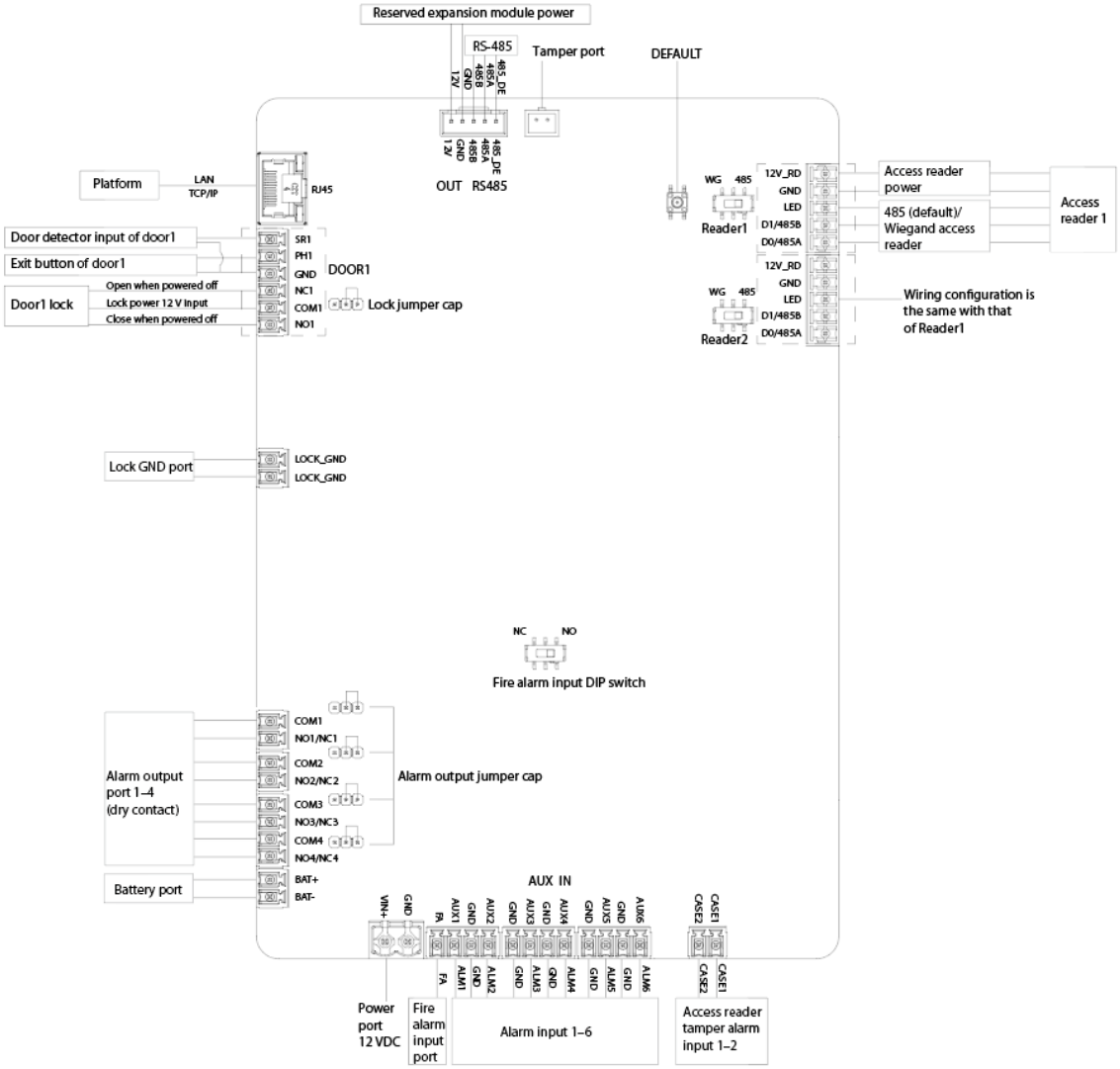


Figure 2-15 Access controller (2 doors)

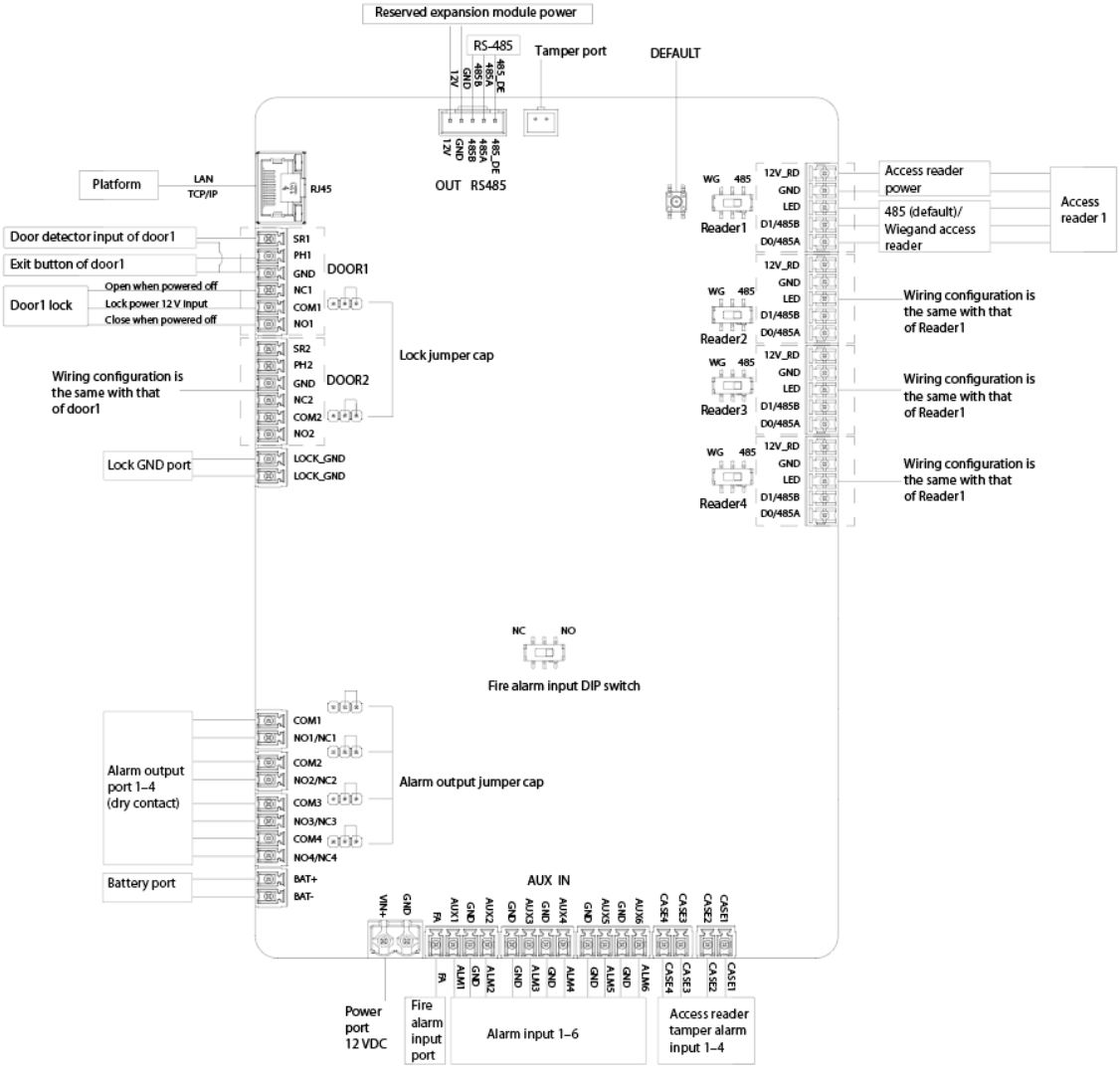


Figure 2-16 Access controller (4 doors)

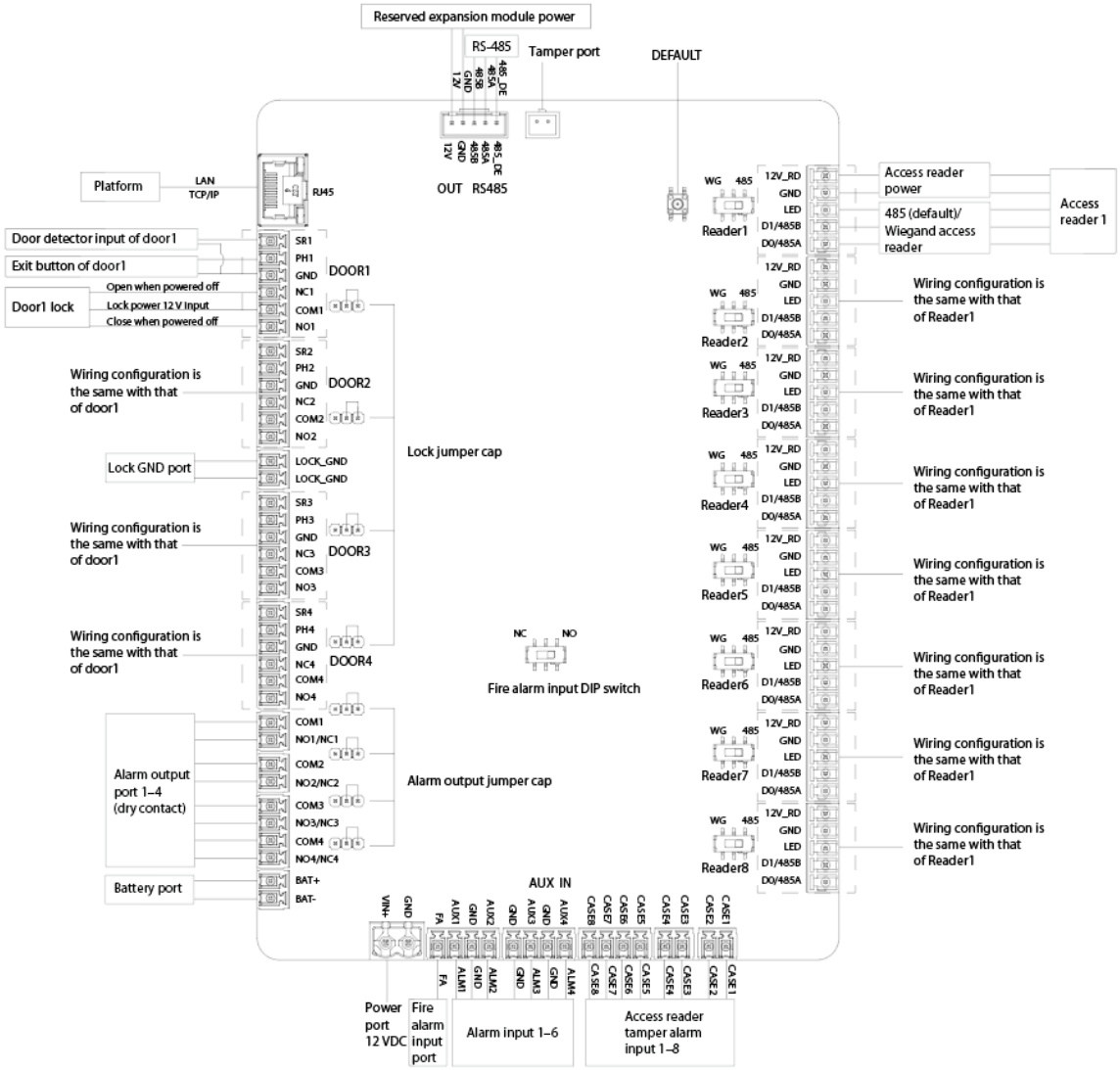


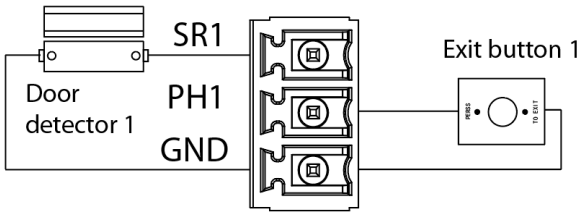
Table 2-3 Components description

Component	Description
OUT	Power output port. The OUT port next to RS-485 port supports the maximum current of 500 mA.
RS485	Connects to external alarm module to expand 8-channel alarm input or 8-channel alarm output.
Tamper Port	Used for tamper alarm.

Component	Description
DEFAULT	Restore the Device to default settings. • Restore to default settings (remain user information and logs): Press the DEFAULT key for 500 ms, and the Device beeps once. During the restoring process, the Device beeps all the time. If the Device stops beeping, it is restored to the default settings and automatically restarts. • Restore to factory settings: Press and hold the DEFAULT key for more than 5 seconds, and the Device beeps for 3 seconds. During the restoring process, the Device beeps all the time. If the Device stops beeping, it is restored to the factory settings and automatically restarts.  Operate the restoring function within 5 minutes after the Device is powered on.
Reader1–Reader8	Access reader port. The connection method for the 4 ports is the same. The power of the reader supports 12 VDC and the current of 1 A.
AUX IN	Alarm input port. Connects to smoke detector and IR detector.
Power	Power input port. Converts the input power to 12 VDC.
Battery Port	Connects to the battery.
Alarm Output Jumper Cap	The alarm output jumper cap connects to 1 and 2 by default. • Connecting 1 and 2 means NO is the output terminal (dry contact), used for connecting normally open alarm devices. • Connecting 2 and 3 means NC is the output terminal (dry contact), used for connecting normally closed alarm devices.
Lock Power	Power port for the lock (12 VDC, 1.2 A).
Fire Alarm Input DIP Switch	The fire alarm input port supports switching through dip switches to connect normally open or normally closed alarm devices.
Door1 – Door4	Door control port. The connection method for the 4 ports is the same. The door lock jumper cap connects to 1 and 2 by default. • Connecting 1 and 2 means COM is not powered, and the lock uses external power supply. COM serves as the common terminal. Wiring distribution should be done according to the actual type of lock used. • Connecting 2 and 3 means COM serves as a 12 V (1 A) output terminal, supplying power to the lock from the COM terminal. Wiring distribution should be done according to the actual type of lock used.
RJ45	Network port.

2.3.2 Exit Button or Door Detector

Figure 2-17 Wiring of exit button or door detector



2.3.3 Cables Specification

Access controller supplies power for the access reader and the lock.

Figure 2-18 Power wiring

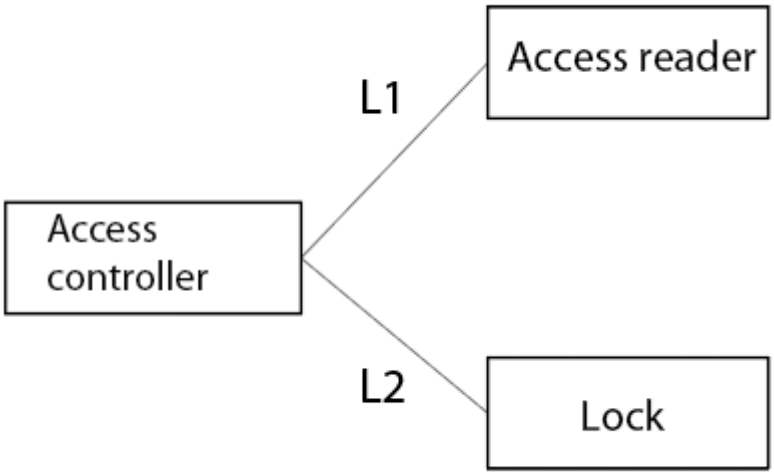


Table 2-4 Cable specification description

No.	Name	Recommended Model and Specification	Recommended Max Power Supply Distance
L1	Access Reader Cable	RVV2 × 1.0, RVV4 × 1.0 or CAT5E network cable ● RVV0.5 (DC resistance of a single conductor ≤ 39.0 Ω/km) ● RVV1.0 (DC resistance of a single conductor ≤ 19.5 Ω/km) ● RVV1.5 (DC resistance of a single conductor ≤ 13.3 Ω/km) ● CAT5E network cable (impedance within 100 m ≤ 9 Ω)	● RVV0.5 ◇ Less than 200 m for RS-485 access reader. ◇ Less than 120 m for Wiegand access reader. ● CAT5E (single cable) ◇ Less than 120 m for RS-485 access reader. ◇ Less than 50 m for Wiegand access reader.
L2	Lock Cable		● RVV0.5 ◇ Less than 25 m for 2 doors electromagnetic lock (280 kg). ◇ Less than 60 m for single door electromagnetic lock (280 kg). ◇ Less than 20 m for 2 doors electromagnetic lock (500 kg). ◇ Less than 50 m for single door electromagnetic lock (500 kg). ● RVV1.0 ◇ Less than 40 m for 2 doors electromagnetic lock (280 kg). ◇ Less than 100 m for single door electromagnetic lock (280 kg). ◇ Less than 40 m for 2 doors electromagnetic lock (500 kg). ◇ Less than 100 m for single door electromagnetic lock (500 kg). ● RVV1.5 ◇ Less than 80 m for 2 doors electromagnetic lock (280 kg). ◇ Less than 140 m for single door electromagnetic lock (280 kg). ◇ Less than 60 m for 2 doors electromagnetic lock (500 kg). ◇ Less than 140 m for single door electromagnetic lock (500 kg).

- If the access reader is powered by the access controller, it is recommended to select an access reader with a maximum current not exceeding 200 mA. The selected access reader should support wide voltage operation, with the lowest operating voltage not exceeding 9 V.

- If the lock is powered by the access controller, it is recommended to select a lock with a maximum current not exceeding 1,200 mA. The selected lock should support wide voltage operation, with the lowest operating voltage not exceeding 10 V.
- The wiring distance of L1 and L2 is affected by the voltage of the power supply and the power supply cable specification. During actual construction, the power supply voltage should be ensured not to be lower than the lowest operating voltage of the access standalone, access reader, and lock. Additionally, L1 and L2 should not use the same wire.
- When using CAT5E (impedance within 100 m ≤ 9 Ω) for the power supply of locks or access readers, it is recommended to allocate the extra wires, apart from the necessary signal wires, evenly for the power supply of locks or access readers in order to minimize power supply loss.
- The above data is measured under laboratory conditions and might differ from actual working conditions. It is for reference only.

2.3.4 Lock

Select the wiring method according to the lock type. The lock can be powered by access controller (COM port of the access controller) or the external power supply.

Powered by External Power Supply

Figure 2-19 Wiring of motor lock

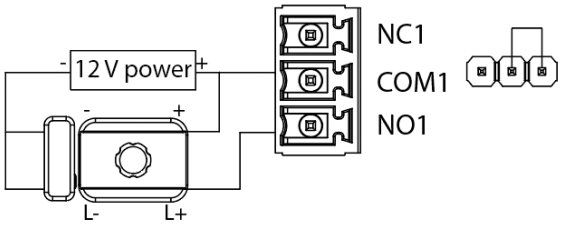


Figure 2-20 Wiring of electromagnetic lock

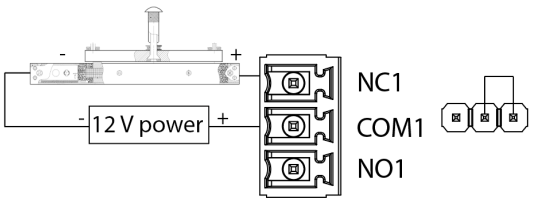


Figure 2-21 Wiring of electric bolt lock (open when powered off)

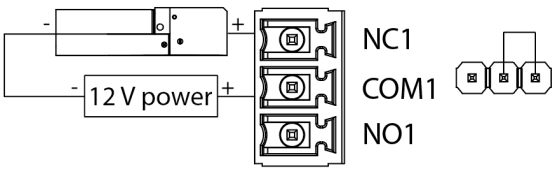
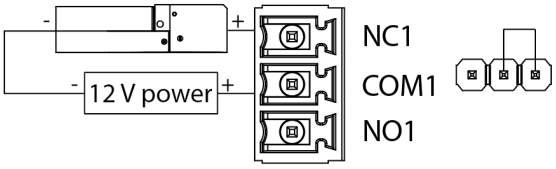


Figure 2-22 Wiring of electric bolt lock (close when powered off)



Powered by Access Controller

Connecting 2 and 3 means COM serves as a 12 V output terminal.

Figure 2-23 Wiring of motor lock

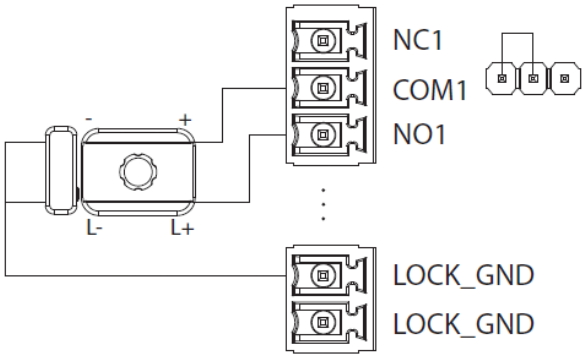


Figure 2-24 Wiring of electromagnetic lock

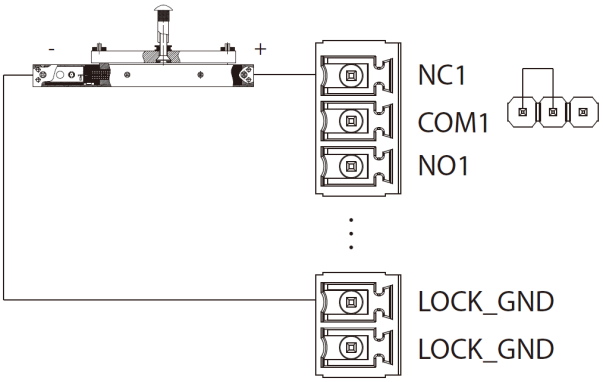


Figure 2-25 Wiring of electric bolt lock (open when powered off)

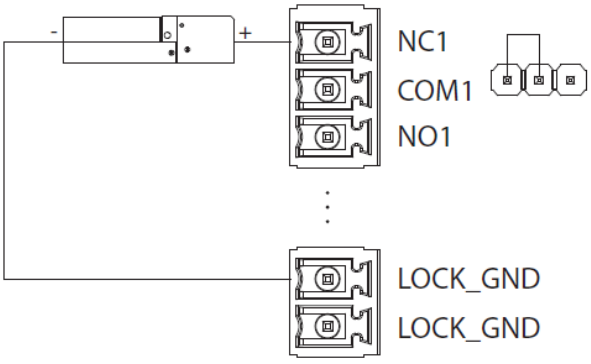
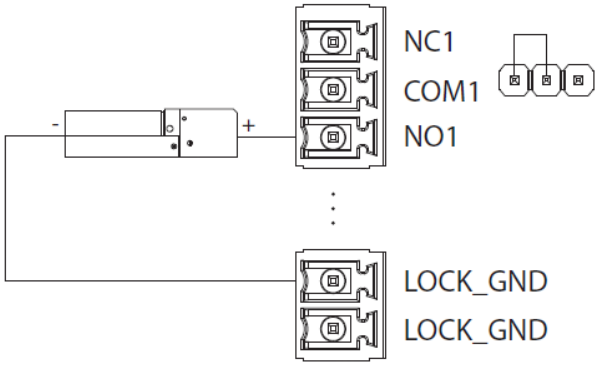


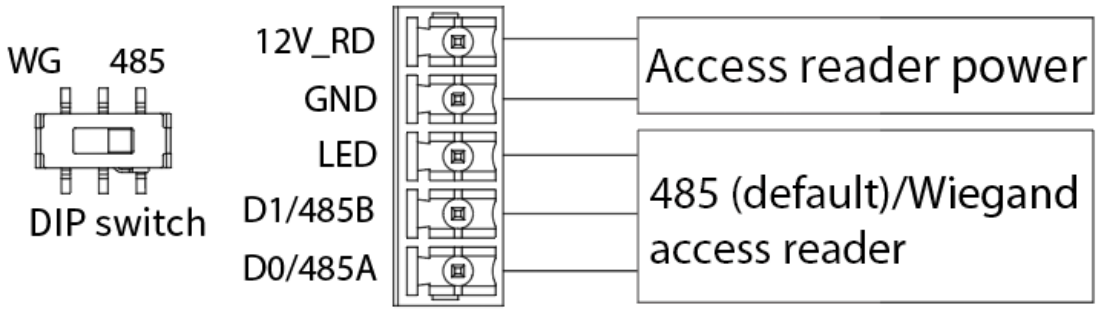
Figure 2-26 Wiring of electric bolt lock (close when powered off)



2.3.5 Access Reader

One access reader port can only connect to the access readers of the same type. The DIP switch is in the 485 position by default. If you connect to external Wiegand access reader, turn the DIP switch to the WG position.

Figure 2-27 Wiring of access reader



3 Web Operations

You can configure the network parameters, access control parameters on the webpage of the Device. This chapter only introduces login operations. For details on other operations and functions, see the user's manual.

Prerequisites

Make sure that the computer used to log in to the webpage is on the same LAN as the Device.

Procedure

Step 1 Open a browser, go to the IP address of the Device.

Step 2 Enter the username and password, and then click **Login**.

- The default username of the administrator is admin, and the password is configured during initialization. Keep the password safe after initialization and change the password regularly to improve security.
- If you forget the login password, click **Forgot Password** to reset the password. For details, see the user's manual.

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).