Access Reader

User's Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of the Access Reader (hereinafter referred to as the "Card Reader "). 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.
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.	November 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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 Card Reader, hazard prevention, and prevention of property damage. Read carefully before using the Card Reader, and comply with the guidelines when using it.

Transportation Requirement

⚠

Transport, use and store the Card Reader under allowed humidity and temperature conditions.

Storage Requirement

⚠

Store the Card Reader under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Card Reader 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 Card Reader to two or more kinds of power supplies, to avoid damage to the Card Reader.
- Improper use of the battery might result in a fire or explosion.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Card Reader in a place exposed to sunlight or near heat sources.
- Keep the Card Reader away from dampness, dust, and soot.
- Install the Card Reader on a stable surface to prevent it from falling.
- Install the Card Reader 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 power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Card Reader label.
- The Card Reader is a class I electrical appliance. Make sure that the power supply of the Card Reader is connected to a power socket with protective earthing.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Card Reader while the adapter is powered on.

- Operate the Card Reader within the rated range of power input and output.
- Use the Card Reader under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Card Reader, and make sure that there is no object filled with liquid on the Card Reader to prevent liquid from flowing into it.
- Do not disassemble the Card Reader without professional instruction.

Table of Contents

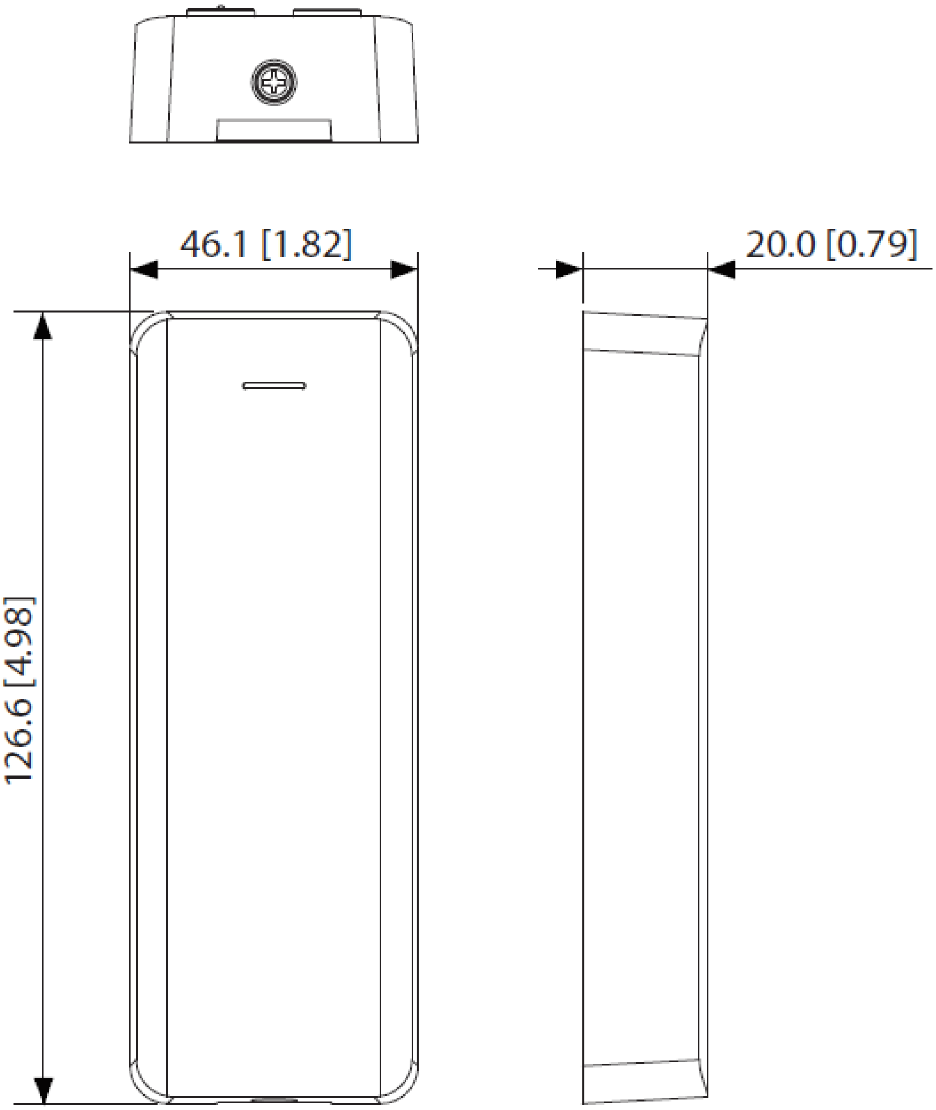
1 Product Overview

1.1 Introduction

In most access control systems, an access control card reader is a security system that requires a swipe of a credential card to verify the person entering the room/space is cleared. It is suitable for a wide variety of scenes such as office buildings, schools, compounds, communities, factories, public venues, business centers and government buildings.

1.2 Dimensions

Figure 1-1 Dimensions of card reader (unit: mm[inch])



2 Wiring and Installation

2.1 Ports Overview

Table 2-1 Ports overview

Color	Port	Description
Red	RD+	PWR (12 VDC)
Black	RD−	GND
Blue	CASE	Anti-tampering alarm signal
White	D1	Wiegands transmission signal (effective only when using Wiegand protocol)
Green	D0	
Brown	LED	Wiegand responsive signal (effective only when using Wiegand protocol)
Yellow	RS−485_B	
Purple	RS−485_A	

2.2 Wiring Requirements

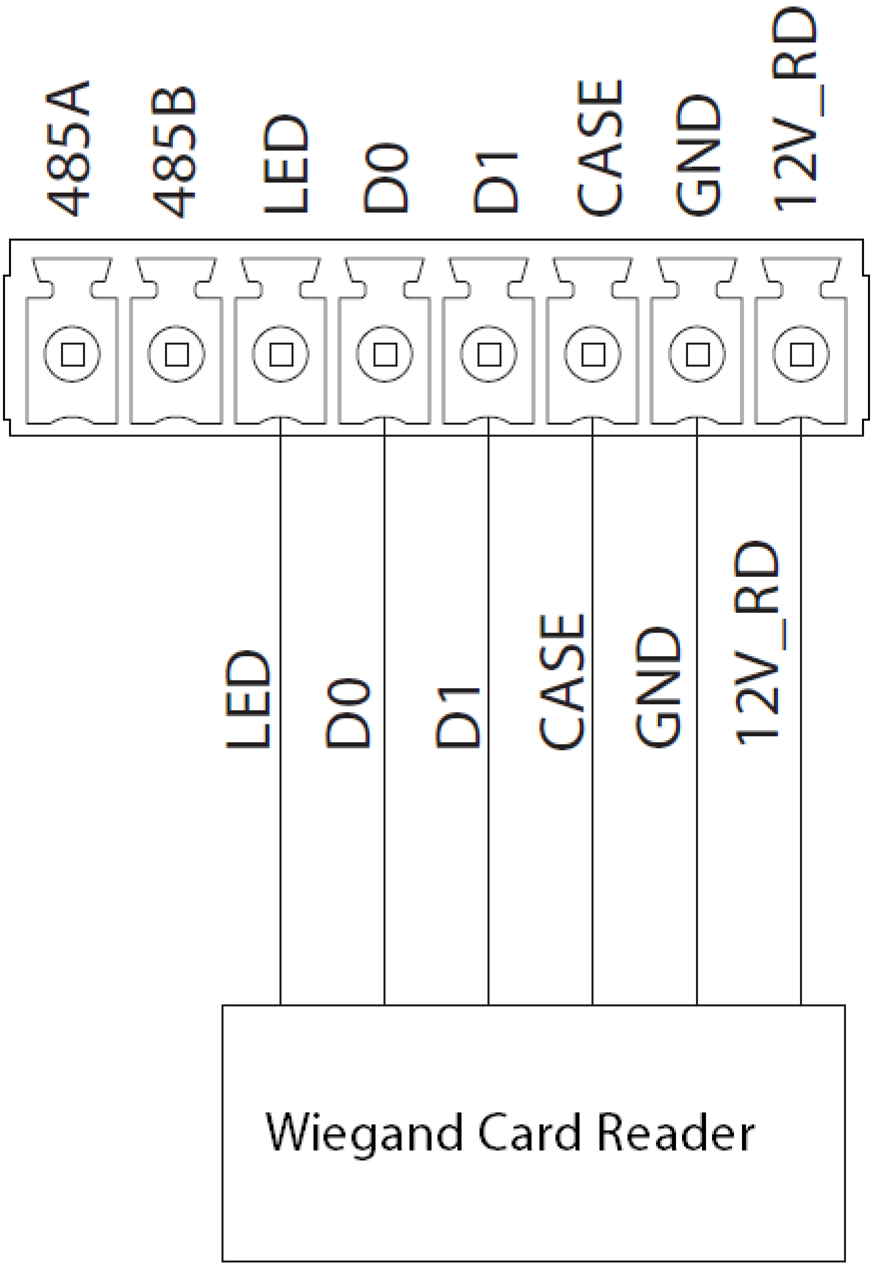
- Connect the card reader to the Wiegand ports or the RS-485 ports according to the type of the card reader.
- Select proper wires according to the requirements on wires.

Table 2-2 Wiring requirements of card reader

Type	Impedance Requirements	Length Requirements
RS-485 card reader	Connects RS-485 wires, and the impedance of a single wire must≤ 10 Ω.	≤ 100 m. Above UL1061 24AWG shielded wires are recommended.
Wiegand card reader	Connects Wiegand wires, and the impedance of a single wire must≤ 2 Ω.	≤ 80 m. Above UL1061 18AWG shielded wires are recommended.

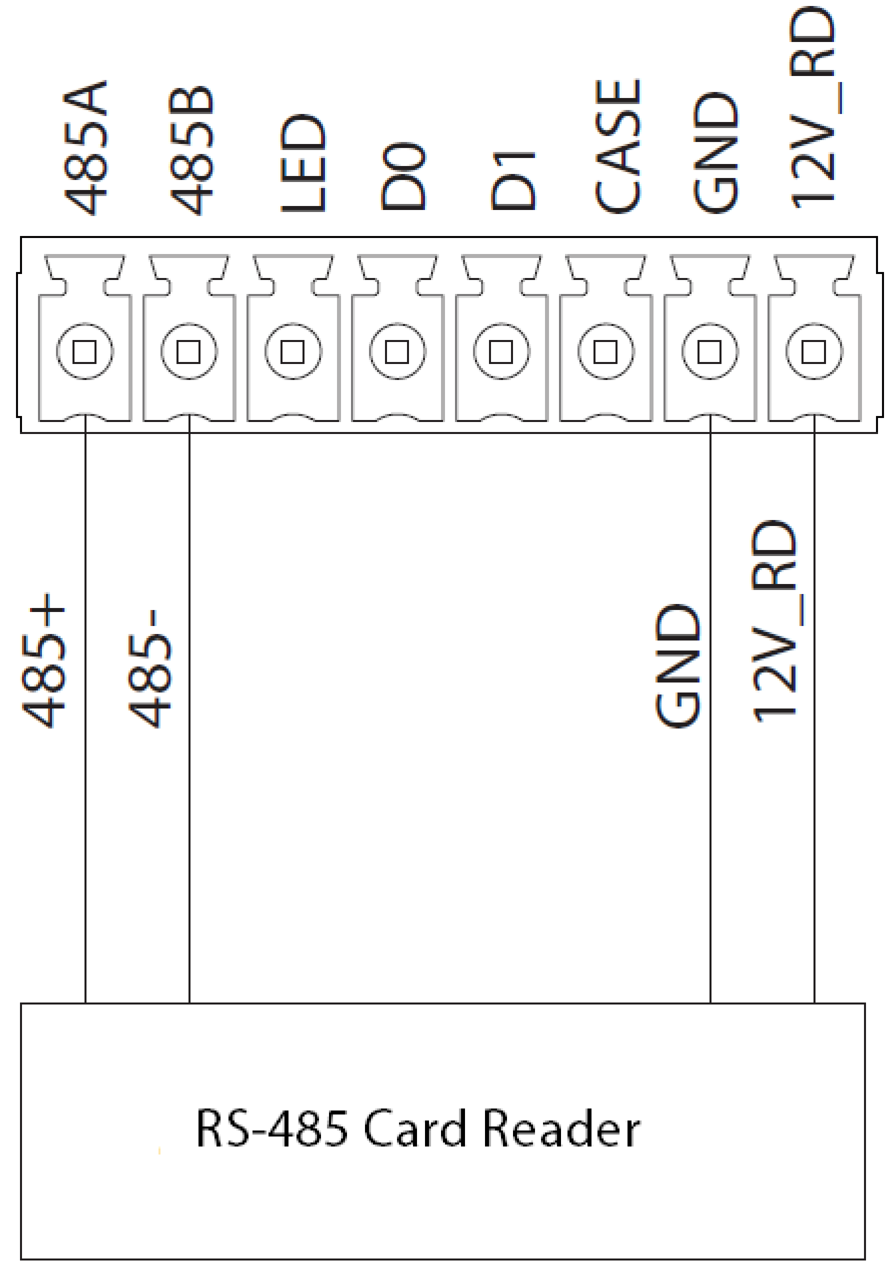
2.3 Wiring

Figure 2-1 Wiring of Wiegand card reader



- For Wiegand card reader without keypad, Wiegand 34 is supported by default and Wiegand 26 is customizable.
- For Wiegand card reader with keypad, tap ****0034**** to switch to the Wiegand 34 format,and tap ****0026**** to switch to the Wiegand 26 format.

Figure 2-2 Wiring of RS-485 card reader



2.4 Installation Procedure

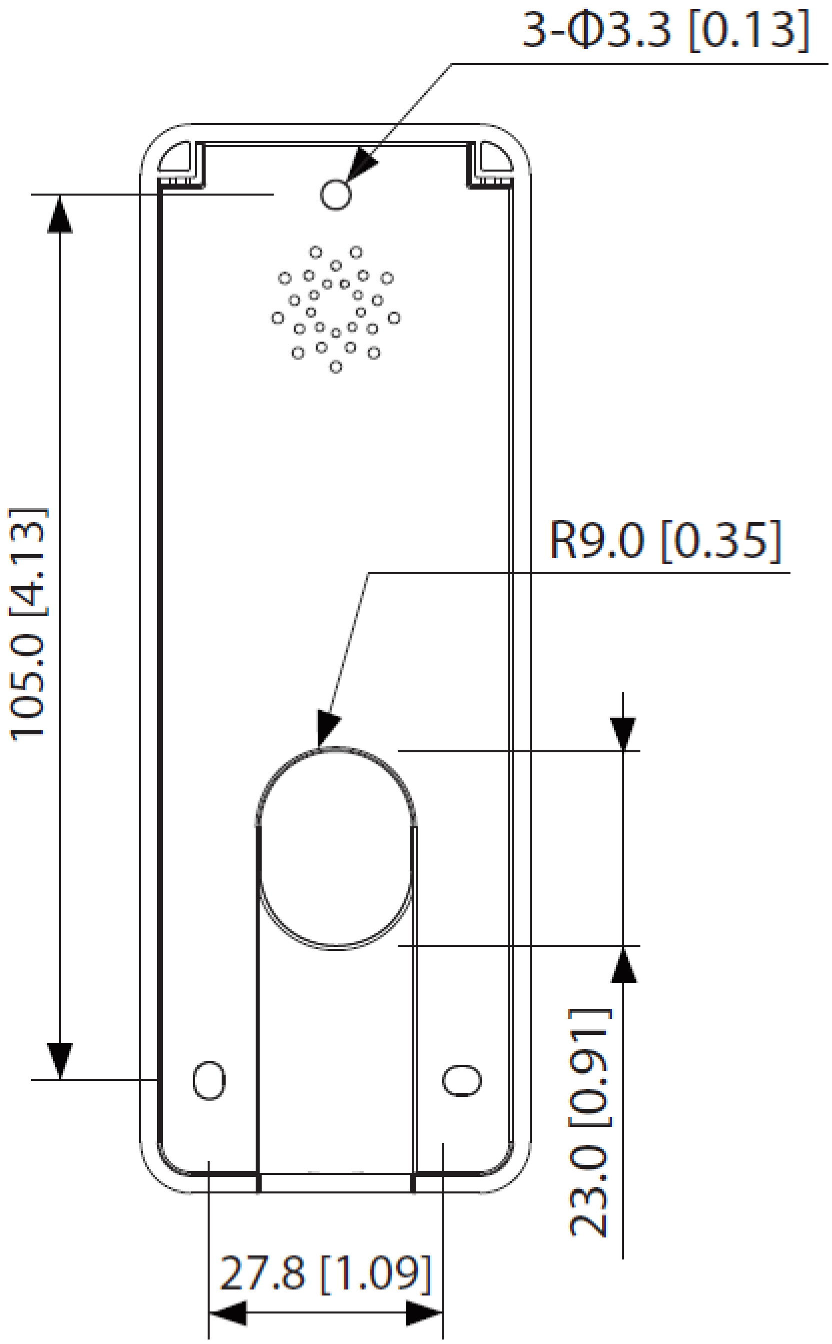
The recommend installation height is 1.3 m–1.5 m (from the center of the device to the ground) and not more than 2 m.

Procedure

Step 1 Drill 3 installation holes on the wall according to the hole's position of the bracket.

Step 2 Put 3 expansion bolts into the holes.

Figure 2-3 Drill holes (unit:mm[inch])



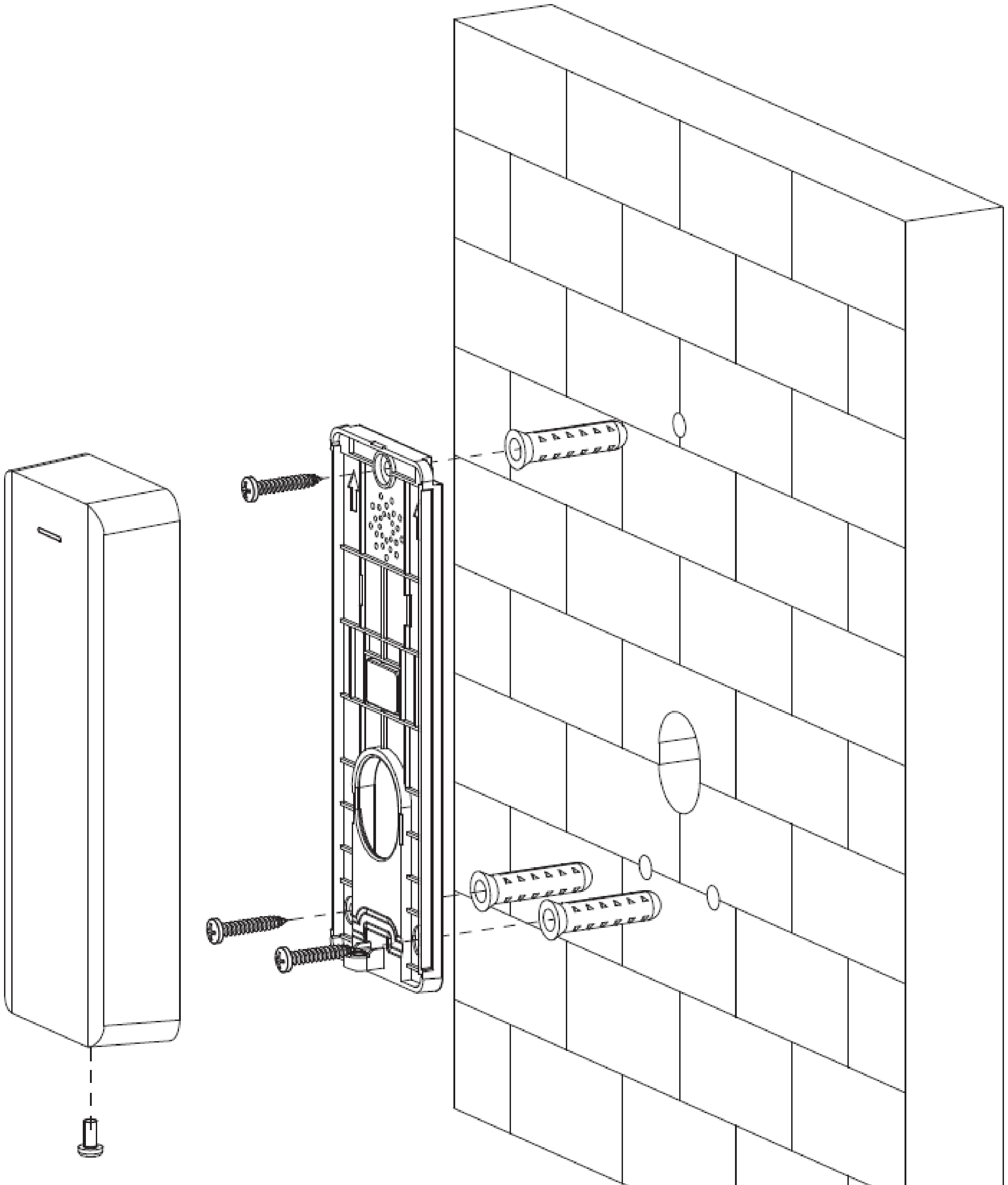
Step 3 Pass the wires of the Card Reader through the slot of the bracket.

Step 4 Use 3 screws to fix the bracket on the wall.

Step 5 Attach the Card Reader to the bracket from bottom to top.

Step 6 Screw in 1 screw at the bottom to secure the Card Reader.

Figure 2-4 Drill holes (unit:mm[inch])



3 Unlocking the Door

Swipe card on the card reader to open the door. For card reader with keypad, you can also unlock the door by entering the password.

- Unlock the door through public password: Enter the public password, and then tap **#**.
- Unlock the door through user password: Enter the user ID and tap **#**, and then enter the user password and tap **#**.
- Unlock the door through card + password: Swipe card, enter the password, and then tap **#**.

If the password is correct, the indicator is green and the buzzer sound once. If the password is incorrect, the indicator is red, and the buzzer sounds 4 times (RS-485 communication) or sounds 3 times (Wiegand communication or no signal line is connected).

4 Light and Voice Prompt

After the Card Reader is powered on, it beeps and the LED is solid blue, which means it is successfully started.

Only swipe one card at one time. Do not swipe multiple cards at the same time.

Table 4-1 Light and Voice Prompts

Function	Prompts
The card reader is powered on.	Beeps once, and the indicator is solid blue.
Anti-tamper	Beeps once and lasts for 15 seconds.
Keypad sound	Beeps once.
Alarm linkage	Beeps once and lasts for 15 seconds.
Swipe the authenticated card (RS-485 communication).	Beeps once and the indicator lights green.
Swipe the unauthenticated card (RS-485 communication)	Beeps 4 times and the indicator lights red.
RS-485 communication error and swipe the authenticated /unauthenticated card.	Beeps 3 times and the indicator lights red.
Swipe the authenticated card (Wiegand communication).	Beeps once and the indicator lights green.
Swipe the unauthenticated card (Wiegand communication)	Beeps once and the indicator lights red.
The main program is updating or in the BOOT status for updating.	The indicator flashed in blue until the updating completes.

5 Updating the System

5.1 Updating through SmartPSS Lite

Prerequisites

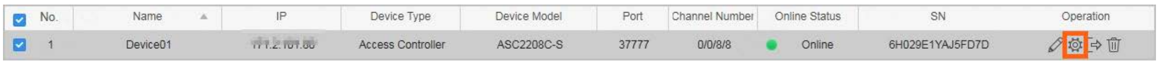
- The Card Reader was added to the access controller through RS-485 wires.
- The access controller and Card Reader are powered on.

Procedure

Step 1 Install and log in to SmartPSS Lite, and then select **Device Manager**.

Step 2 Click ⚙.

Figure 5-1 Select the access controller



☑ No.	Name ▲	IP	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
☑ 1	Device01	[redacted]	Access Controller	ASC2208C-S	37777	0/0/8/8	● Online	6H029E1YAJ5FD7D	✎ ⚙ ⇨ 🗑

Step 3 Click ☁ and 📁 to select the update file.

Step 4 Click **Upgrade.**

The indicator of the Card Reader flashes blue until the update is completed, and then the Card Reader automatically restarts.

5.2 Updating through Config Tool

Prerequisites

- The Card Reader was added to the access controller through RS-485 wires.
- The access controller and Card Reader are powered on.

Procedure

Step 1 Install and open the Configtool, and then select **Device upgrade**.

Step 2 Click 🗋 of an access controller, and then click ⇧.

Step 3 Click **Upgrade**.

The indicator of the Card Reader flashes blue until update is completed, and then the Card Reader automatically restarts.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the“auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.