

Access Reader

User's Manual



V1.0.3

Foreword

General

This manual introduces the functions and operations of the Access 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.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.3	Added wiring requirements.	September 2024
V1.0.2	Updated the manual.	April 2023
V1.0.1	Updated the manual.	January 2023
V1.0.0	First release.	December 2019

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 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

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Product Overview.....	1
1.1 Introduction.....	1
1.2 Dimensions.....	2
2 Wiring and Installation.....	3
2.1 Wiring Requirements.....	3
2.2 Installation Procedure.....	3
3 Updating the System.....	5
3.1 Updating through SmartPSS Lite.....	5
3.2 Updating through Config Tool.....	5
Appendix 1 Security Recommendation.....	6

1 Product Overview

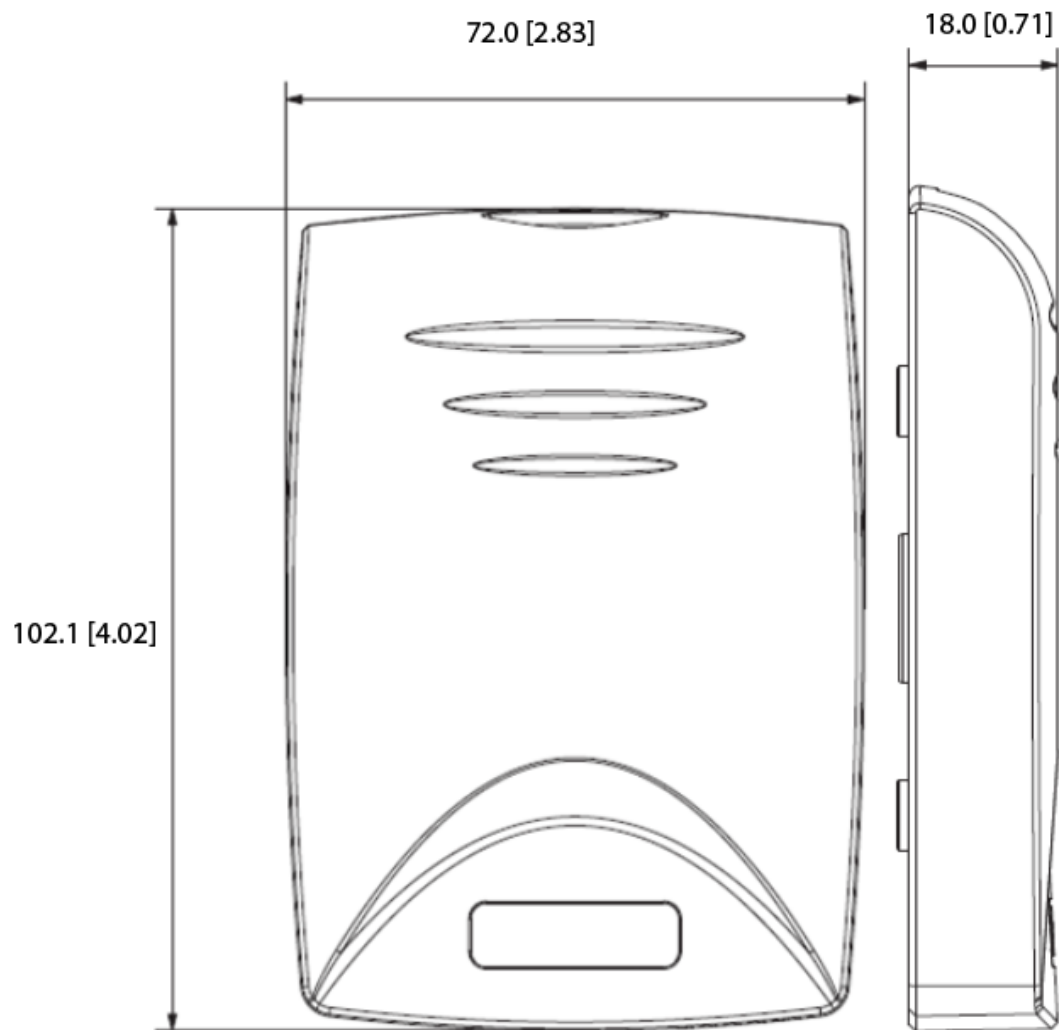
1.1 Introduction

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.

- Non-contact reader (read-only), card reading distance is 3 cm-5 cm, and response time is < 0.3 s.
- Supports Wiegand Protocol and RS-485 protocol. RS-485 baud rate is 9600 bps.
- Supports watch dog.
- Supports over-current and overload protection.
- Work temperature is: -30 °C to +60 °C; working humidity is ≤95%.
- Buzzer and indicator prompts.
- Supports online update.
- Advanced key management service to reduce the risk of data leakage and or card duplication.

1.2 Dimensions

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



2 Wiring and Installation

2.1 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 2-1 Ports overview

Color	Port	Description
Red	12 V	Power supply
Black	GND	
Blue	ALARM_OUT	Alarm output signals(for Wiegand card reader)
White	D1	Wiegands transmission signals (for Wiegand card reader)
Green	D0	
Brown	LED/BELL_CTRL	Wiegand responsive signals (for Wiegand card reader)
Yellow	RS-485_B	RS-485 card reader
Purple	RS-485_A	

Table 2-2 Wiring requirements of card reader

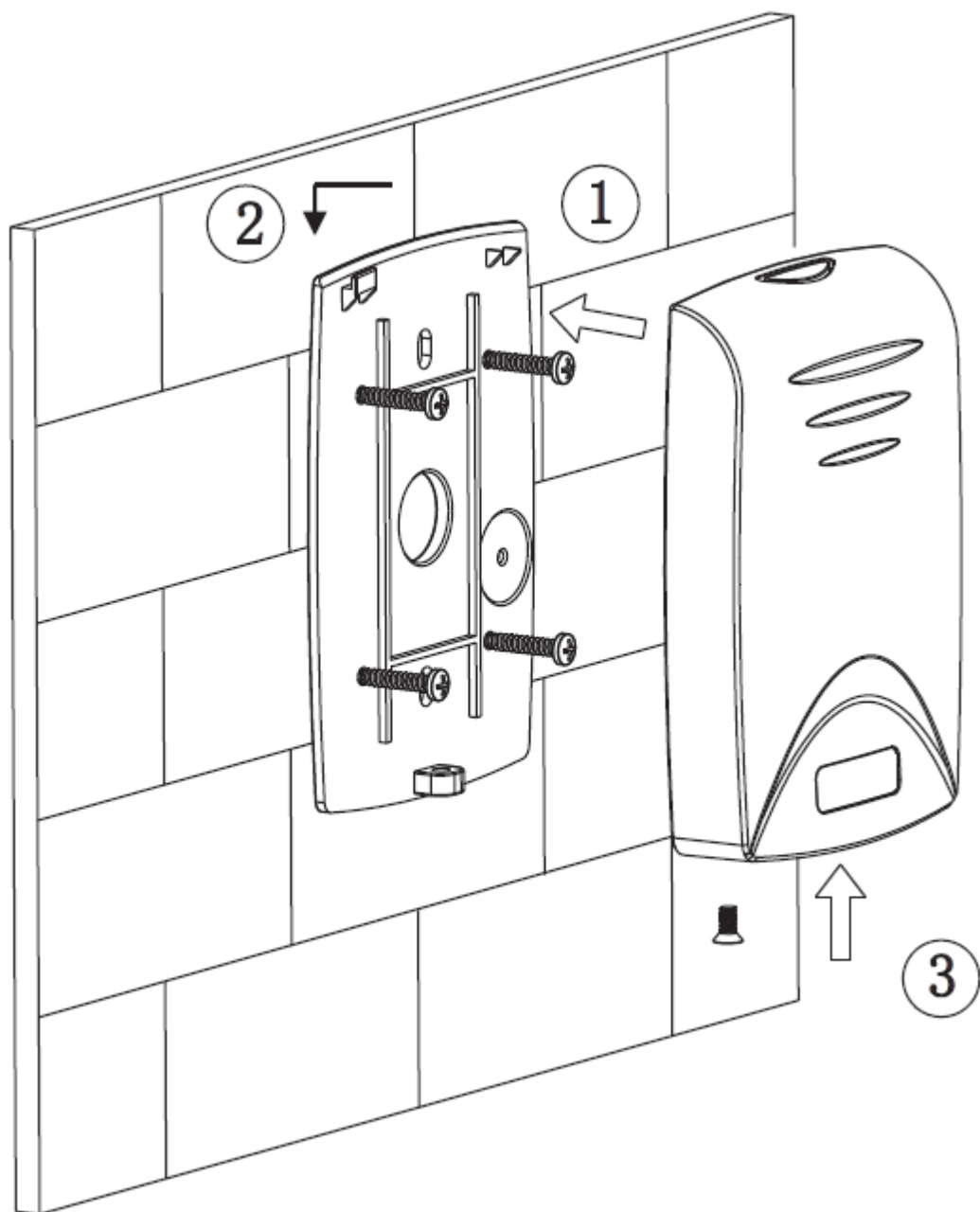
Type	Impedance Requirements	Length Requirements
RS485 card reader	Connects RS-485 wires, and the impedance of a single wire must $\leq 10 \Omega$.	≤ 100 m. Above UL1061 24AWG shielded wires are recommended.
Wiegand card reader	Connects Wiegand wires, and the impedance of a single wire must $\leq 2 \Omega$.	≤ 80 m. Above UL1061 18AWG shielded wires are recommended.

2.2 Installation Procedure

Procedure

- Step 1 Mount the back cover to the wall by screwing in 2 self-tapping screws.
- Step 2 Attach the front cover to the back cover.
- Step 3 Screw in a screw at the bottom to secure the device.

Figure 2-1 Drill holes (unit:mm[inch])



Step 4 Apply silica gel to the gap between the device and the wall to prevent water leakage.

3 Updating the System

3.1 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 3-1 Select the access controller

☒	No.	Name	IP	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
☒	1	Device01	172.16.101.80	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.

3.2 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 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 logout function

The account logout 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;
- Establish 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).