

Wiegand Adapter Board

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the installation of the Wiegand adapter board (hereinafter referred to as the "adapter board"). 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 2025

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 to: 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 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 Issuer.
- 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 adapter board, hazard prevention, and prevention of property damage. Read carefully before using the Issuer, and comply with the guidelines when using it.

Installation Requirements



- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the adapter board.
- Do not connect the adapter board to two or more kinds of power supplies.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.



- Please follow the electrical requirements.
- Use the power supply provided by the manufacturer.

Operation Requirements



Do not use the adapter board under direct sunlight or other heat sources for long durations.



- Make sure that the power supply is correct before use.
- Use the adapter board under allowed humidity and temperature conditions.
- Do not disassemble the adapter board.

Maintenance Requirements



- Power off the adapter board before maintenance.
- Maintenance must be performed by qualified professionals.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Product Overview.....	1
1.1 Introduction.....	1
1.2 Appearance.....	1
2 Wiring and Configuring.....	2
2.1 Wiring Diagram.....	2
2.2 Wiring Interfaces.....	2
2.3 Configuring.....	3
Appendix 1 Security Recommendation.....	4

1 Product Overview

1.1 Introduction

The adapter board is a signal conversion interface device. It is mainly used to convert the data identified by entrance and exit cameras into Wiegand protocol communication format commonly used in access control systems.

1.2 Appearance

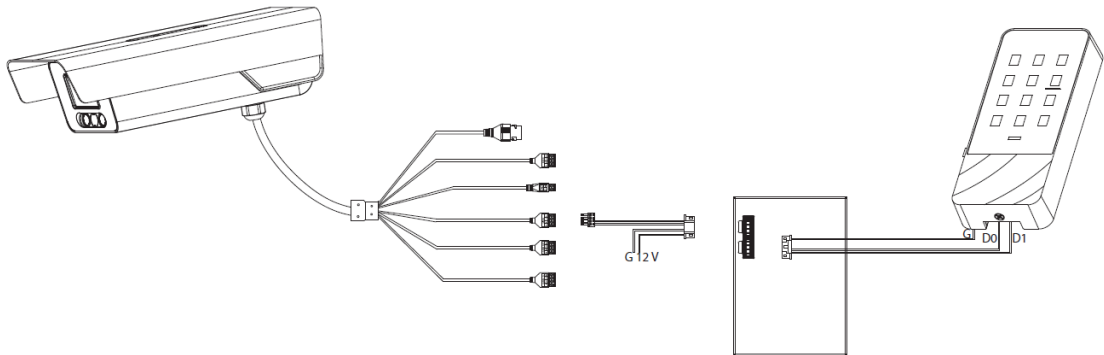
Figure 1-1 Appearance



2 Wiring and Configuring

2.1 Wiring Diagram

Figure 2-1 Wiring



2.2 Wiring Interfaces

The adapter board is connected to the device with two 4-pin terminals.

Figure 2-2 Wiring interfaces

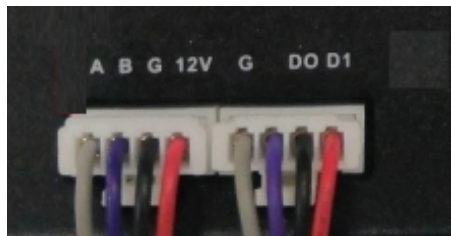


Table 2-1 Description of wiring interfaces

Interface	Description
A	RS-485 ports of the Wiegand module, respectively connecting to A and B interfaces of the camera RS-485.
B	
G	Power supply input of the Wiegand module.
12V	
G	Grounded. Convert the data identified by entrance and exit cameras into Wiegand protocol communication format commonly used in access control systems, connect to G, D0, D1 of access control or receive G, D0, D1 of the signal device (the purple wire is not connected).
D0	
D1	



This Wiegand module outputs the data of Wiegand 26 bit. It is not compatible with Wiegand 34 bit protocol, thereby it cannot work adaptively.

2.3 Configuring

Before using the adapter board, you need to configure it on the camera webpage.

Procedure

- Step 1 On the camera webpage, select **ANPR > RS-485 Settings**.
- Step 2 Click **Added Device > Wiegand**, and then set the baud rate as 9600.
- Step 3 Click **Apply**.

Figure 2-3 Configure the adapter board

The screenshot displays the 'Serial Port' configuration page. At the top, there are two tabs: 'Serial Port1' (selected) and 'Serial Port2'. Below the tabs, there are four configuration fields: 'Protocol' (set to DHRS), 'Baud Rate' (set to 9600), 'Data Bit' (set to 8), and 'Parity' (set to None). Each field has a dropdown arrow. Below these fields is a section titled 'DHRS External Device'. This section contains three items: 'RS-485 Illuminat...' (with an icon of a camera lens and a red dot indicating 'Offline'), 'LED Screen' (with an icon of a screen and a red dot indicating 'Offline'), and 'Wiegand' (with a blue border and the text 'Wiegand' in blue). Below the 'DHRS External Device' section is a 'Wiegand' section with a trash icon. At the bottom of the page are three buttons: 'Apply' (blue), 'Refresh' (white), and 'Default' (white).

Related Operations

Click , and then the Wiegand will be deleted.



If the adapter board connects to the RS-485 illuminator, you need to configure the serial port 1.

If the adapter board connects to the LED Screen, you need to configure the serial port 2.

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 Allowlist**

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

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).