

Wiring of Four-Door Access Controller



Access Controller

Quick Start Guide

UD17322B-A

Scan the QR code to get the user manual for detailed information. Note that mobile data charges may apply if Wi-Fi is unavailable.



COPYRIGHT © 2019 Hangzhou Hikvision Digital Technology Co., Ltd. ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual
The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (<http://overseas.hikvision.com/en/>).

Please use this user manual under the guidance of professionals.
Trademarks Acknowledgement
HIKVISION and other Hikvision' s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

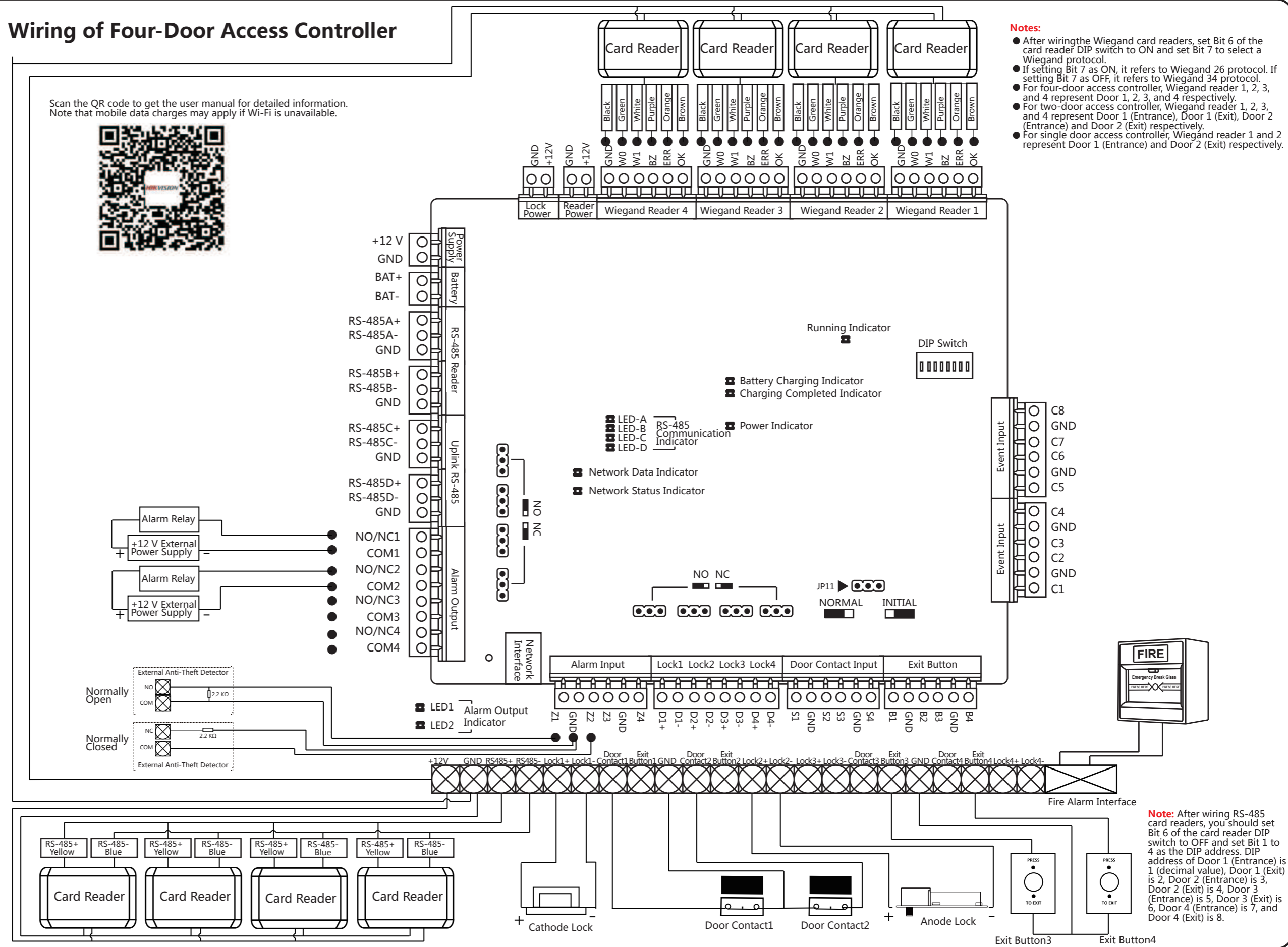
REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Data Protection
During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

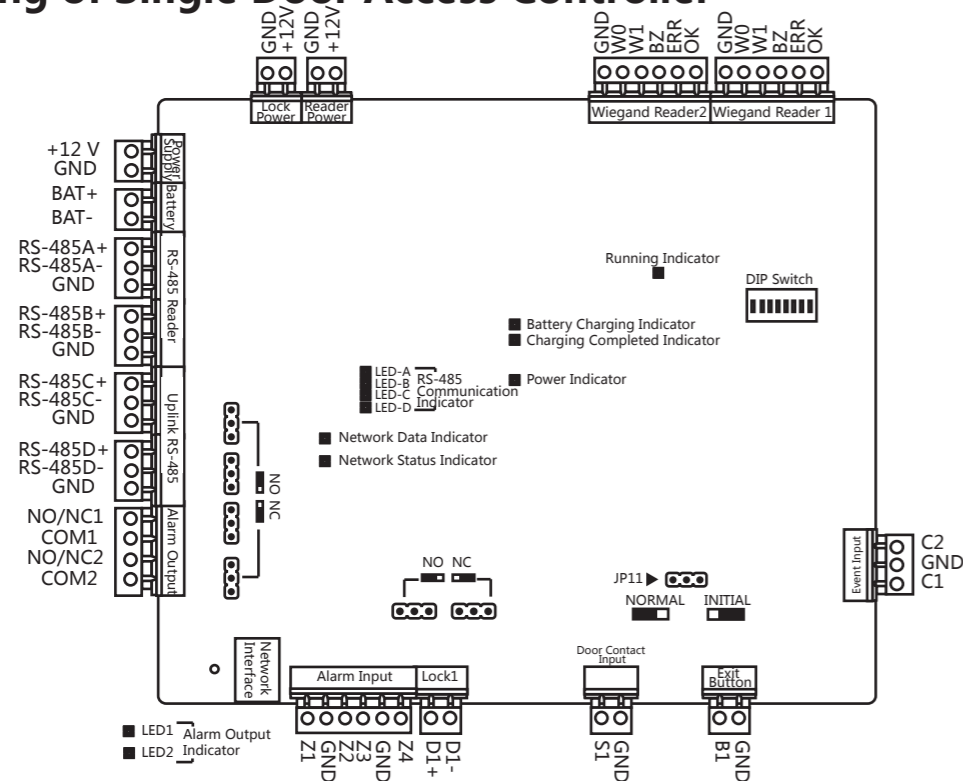


- Notes:**
- After wiring the Wiegand card readers, set Bit 6 of the card reader DIP switch to ON and set Bit 7 to select a Wiegand protocol.
 - If setting Bit 7 as ON, it refers to Wiegand 26 protocol. If setting Bit 7 as OFF, it refers to Wiegand 34 protocol.
 - For four-door access controller, Wiegand reader 1, 2, 3, and 4 represent Door 1, 2, 3, and 4 respectively.
 - For two-door access controller, Wiegand reader 1, 2, 3, and 4 represent Door 1 (Entrance), Door 1 (Exit), Door 2 (Entrance) and Door 2 (Exit) respectively.
 - For single door access controller, Wiegand reader 1 and 2 represent Door 1 (Entrance) and Door 2 (Exit) respectively.

Note: After wiring RS-485 card readers, you should set Bit 6 of the card reader DIP switch to OFF and set Bit 1 to 4 as the DIP address. DIP address of Door 1 (Entrance) is 1 (decimal value), Door 1 (Exit) is 2, Door 2 (Entrance) is 3, Door 2 (Exit) is 4, Door 3 (Entrance) is 5, Door 3 (Exit) is 6, Door 4 (Entrance) is 7, and Door 4 (Exit) is 8.

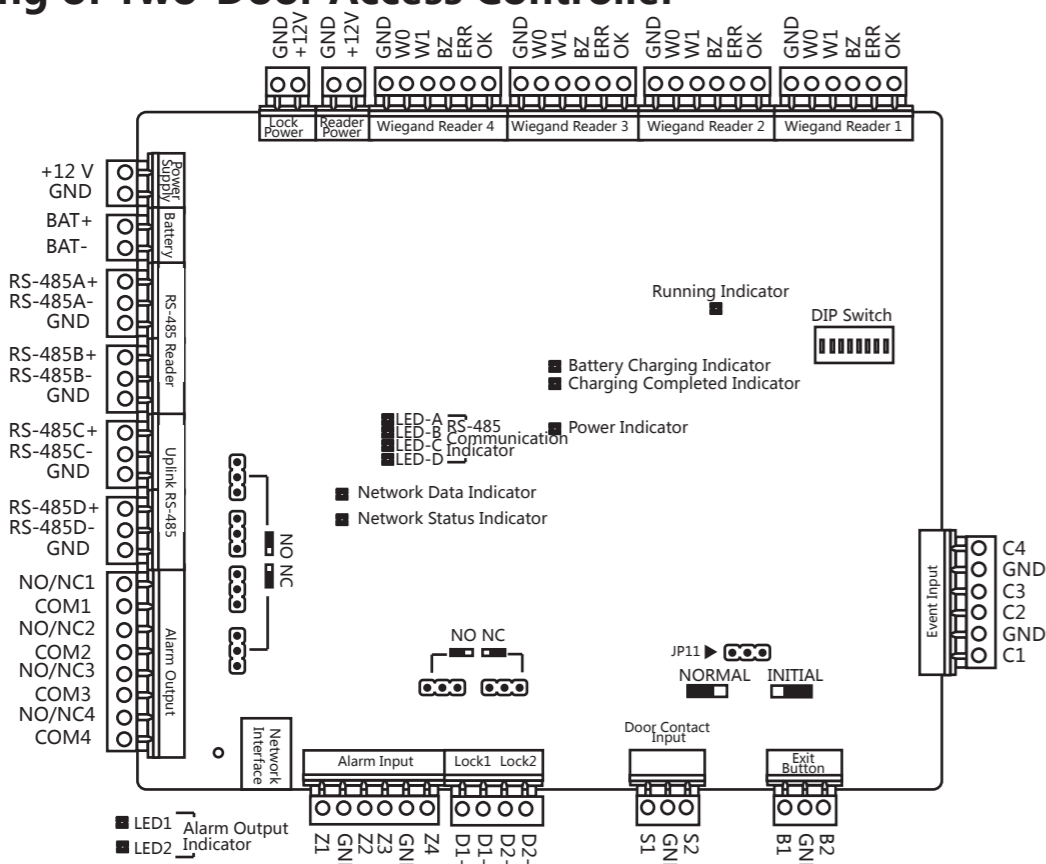
2

Wiring of Single Door Access Controller



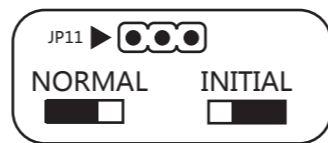
3

Wiring of Two-Door Access Controller



4

Hardware Initialization



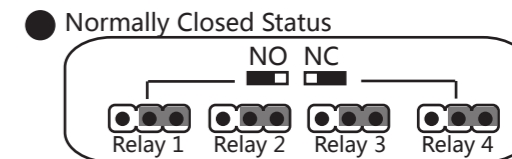
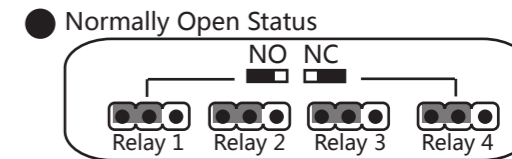
Note: The initializing of the hardware will restore all the parameters to the default setting and all the device events are wiping out.

- Choice 1**
 - Step 1: Remove the jumper cap from the Normal terminal.
 - Step 2: Disconnect the power and restart the access controller. The controller buzzer buzzes a long beep.
 - Step 3: When the beep stopped, plug the jumper cap back to Normal.
 - Step 4: Disconnect the power and restart the access controller.
- Choice 2**
 - Step 1: Jump the jumper cap from Normal to Initial.
 - Step 2: Disconnect the power and reboot the access controller. The controller buzzer buzzes a long beep.
 - Step 3: When the beep stopped, jump the jumper cap back to Normal.
 - Step 4: Disconnect the power and reboot the access controller.

5

Relay NO/NC Settings

Set the relay NO/NC status when setting the lock output and alarm output. The position of the jumper cap position and the related NO/NC status are as follows:

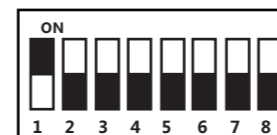


6

DIP Switch Settings of Card Reader

DIP Switch Settings of RS-485 Card Reader

Set Bit 6 of the card reader DIP switch to OFF and set Bit 1 to 4 as the DIP address.
Note: DIP address of Door 1 (Entrance) is 1 (decimal value), Door 1 (Exit) is 2, Door 2 (Entrance) is 3, Door 2 (Exit) is 4, Door 3 (Entrance) is 5, Door 3 (Exit) is 6, Door 4 (Entrance) is 7, and Door 4 (Exit) is 8.



DIP Switch of Door 1 (Entrance)

DIP Switch Settings of Wiegand Card Reader

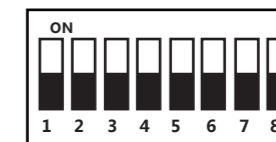
Set Bit 6 of the card reader DIP switch to ON and set Bit 7 to select a Wiegand protocol.
Note: If setting Bit 7 as ON, it refers to Wiegand 26 protocol. If setting Bit 7 as OFF, it refers to Wiegand 34 protocol.



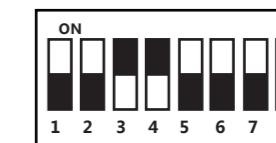
DIP Switch of Wiegand 26 Protocol

DIP Switch Description

Take the 8-bit DIP switch as an example; No.1 to No 8 is from the low bit to the high bit.



When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off. If you set the DIP switch like the figure displayed below, its binary value is 00001100, and its decimal value is 12.



7

Activation

You are required to activate the control panel first before you can use the control panel.

Activation via SADP, and activation via client software are supported.

The default values of the terminal are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

Activate Device via Client Software

- Get the client software from the official website. Install and run the client software.
- Enter the Device Management page.
- Click **Device** on the top of the right panel.
- Click **Online Device** to show the online device area at the bottom of the page.
- Check the device status (shown on Security Level column) and select an inactive device.
- Click **Activate**.
- Create a password in the password field, and confirm the password.
- Click **OK** to activate the device.
- Select an activated device in Online Device area, click on the Operation column to open the Modify Network Parameter window. Change the device IP address to the same subnet with your computer if you need to add the device to the client.

Activate Device via SADP Tool

- Get the SADP tool from the supplied disk. Install and run the SADP tool.
- Check the device status from the device list, and select an inactive device.
- Create a password in the password field, and confirm the password.
- Click **Activate** to activate the device.
- Check the activated device. You can change the device IP address to the same IP segment with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.
- Input the password and click **Modify** to complete the configuration.



STRONG PASSWORD RECOMMENDED—We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Regulatory Information

FCC Information
 Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
 1. This device may not cause harmful interference.
 2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the R&TTE Directive 1999/5/EC, the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recycle-this.info.

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance
 This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.