



**Two Door Access Controller Panel  
Board TCP/IP Wiegand with Software  
and Power Supply Included 100,000  
Users**



**VS-AXESS-2DLX  
Installation Manual**

## **User Manual**

COPYRIGHT © Visionis Technology.  
ALL RIGHTS RESERVED.


Any and all information, including, among others, wordings, pictures, graphs are the properties of Visionis Technology or its subsidiaries (hereinafter referred to be "Visionis"). 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 Visionis. Unless otherwise stipulated, Visionis 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://www.visionistech.com>).

Please use this user manual under the guidance of professionals.

## **Trademarks Acknowledgement**

 **VISIONIS** and other Visionis' trademarks and logos are the properties of Visionis 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 VISIONIS 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 VISIONIS, 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 VISIONIS 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. VISIONIS 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, VISIONIS 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. VISIONIS 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.

## Regulatory Information

### FCC Information

**FCC compliance:** This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

### 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 EMC Directive 2004/108/EC, 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.recyclethis.info](http://www.recyclethis.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](http://www.recyclethis.info).

### Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.




## Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the manufacturer.



### Safety Information

Signs	Description
 <b>Warning</b>	Follow these safeguards to prevent serious injury or death.
 <b>Note</b>	Follow these precautions to prevent potential injury or material damage.
 <b>Tips</b>	The additional information as a complimentary of the contents.



### Warnings

Please adopt the power adapter from the legitimate factory which can meet the safety extra low voltage (SELV) standard.

Do not install, wiring, or uninstall when the power is still on.

To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.

This installation should be made by a qualified service person and should conform to all the local codes.

If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the product yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



### Note

Please do not drop the objects on hard surface, and keep the equipment from the magnetic field. Avoid install the equipment to the vibrated or vulnerable places.

Please do not install the device in the extreme temperature (higher than 65°C or lower than -20°C)

Keep ventilation.

Do not operate in humid environment.

Do not operate in explosive environment.

Keep the device clean and dry.

Avoid bare electrical wire.

# Content

<b>CHAPTER 1</b>	<b>PRODUCT DESCRIPTION</b>	<b>6</b>
1.1	OVERVIEW	6
1.2	PRODUCT FUNCTION	6
<b>CHAPTER 2</b>	<b>APPEARANCE</b>	<b>7</b>
2.1	COMPONENT DESCRIPTION	7
<b>CHAPTER 3</b>	<b>TERMINAL CONNECTION</b>	<b>9</b>
3.1	TERMINALS DESCRIPTION	9
<b>CHAPTER 4</b>	<b>CARD READER INSTALLATION</b>	<b>12</b>
4.1	EXTERNAL TERMINAL	12
4.2	CARD READER INSTALLATION	13
4.2.1	The Connection of Wiegand Card Reader	13
4.2.2	RS485 Card Reader Connection	14
4.3	INSTALLING E-LOCK	15
4.3.1	Installation of Cathode Lock	15
4.3.2	Installation of Anode Lock	15
4.4	CONNECTING THE EXTERNAL ALARM DEVICE	16
4.5	DOOR BUTTON WIRING DIAGRAM	16
4.6	THE CONNECTION OF MAGNETICS DETECTION	17
4.7	CONNECTING POWER SUPPLY	17
4.8	ARMING REGION INPUT TERMINAL	18
4.8.1	Connecting Normally Open Detector	18
4.8.2	Connecting Normally Closed Detector	18
<b>CHAPTER 5</b>	<b>SETTINGS</b>	<b>19</b>
5.1	INITIALIZING THE HARDWARE	19
5.2	RELAY INPUT NO/NC	19
5.2.1	Lock Relay Output	19
5.2.2	Alarm Relay Output Status	20
<b>CHAPTER 6</b>	<b>ACTIVATING THE CONTROL PANEL</b>	<b>22</b>
6.1	ACTIVATION VIA SADP SOFTWARE	22
6.2	ACTIVATION VIA CLIENT SOFTWARE	24
	<b>SPECIFICATION</b>	<b>26</b>

# Chapter 1. Product Description

## 1.1 Overview

VS-AXESS-2DLX is a powerful and stable access controller, using the logical architecture design.

VS-AXESS-2DLX is designed with TCP/IP network interface and its signal processed with special encryption and can be run offline. Anti-tampering function is also supported.

## 1.2 Product Function

- The access controller is equipped with 32-bit high-speed processor;
- Supports TCP/IP network communication, with self-adaptive network interface. The communication data is specially encrypted to relieve the concern of privacy leak;
- Support recognition and storage of card number with maximum length of 20;
- The access controller can store 100 thousand legal cards and 300 thousand card swiping records;
- Supports multi-door interlock function, anti-passback function, multi-card function, first card open function, super card and super password function, online upgrade function and remote control of the doors;
- Supports tamper-proof alarm for card reader, alarm for door not secured, force opening door alarm, alarm for door opening timeout, duress card and code alarm, blacklist alarm and alarm for illegal card swiping attempts reaching the limit.;
- The alarm input of controller supports short circuit protection function and cut-proof function;
- Supports RS485 interface and Wiegand interface for accessing card reader. RS485 interface adopts dual-interface design and supports loop breakpoint detection and redundancy function; Wiegand interface supports W26, W34 and is seamlessly compatible with third-party card reader with Wiegand interface;
- Supports various card types as normal/ disabled/ blacklist/ patrol/ guest/ duress/super card, etc.;
- Various indicators to show different status;
- Supports time synchronization via NTP, manual or automatic method;
- Supports record storage function when it is offline and insufficient storage space storage alarm function;
- The access controller has backup battery design, watchdog design and tamper-proof function;
- Data can be permanently saved after the access controller is powered off.
- Supports I/O linkage, and event linkage;
- Supports Ehome protocol, and inter-network communication.
- 500 groups of password under the authentication mode of card and password;

# Chapter 2. Appearance

## 2.1 Component Description

### Access Controller Component Schematic Diagram

Take VS-AXESS-2DLX as an example, the component schematic diagram is shown below.

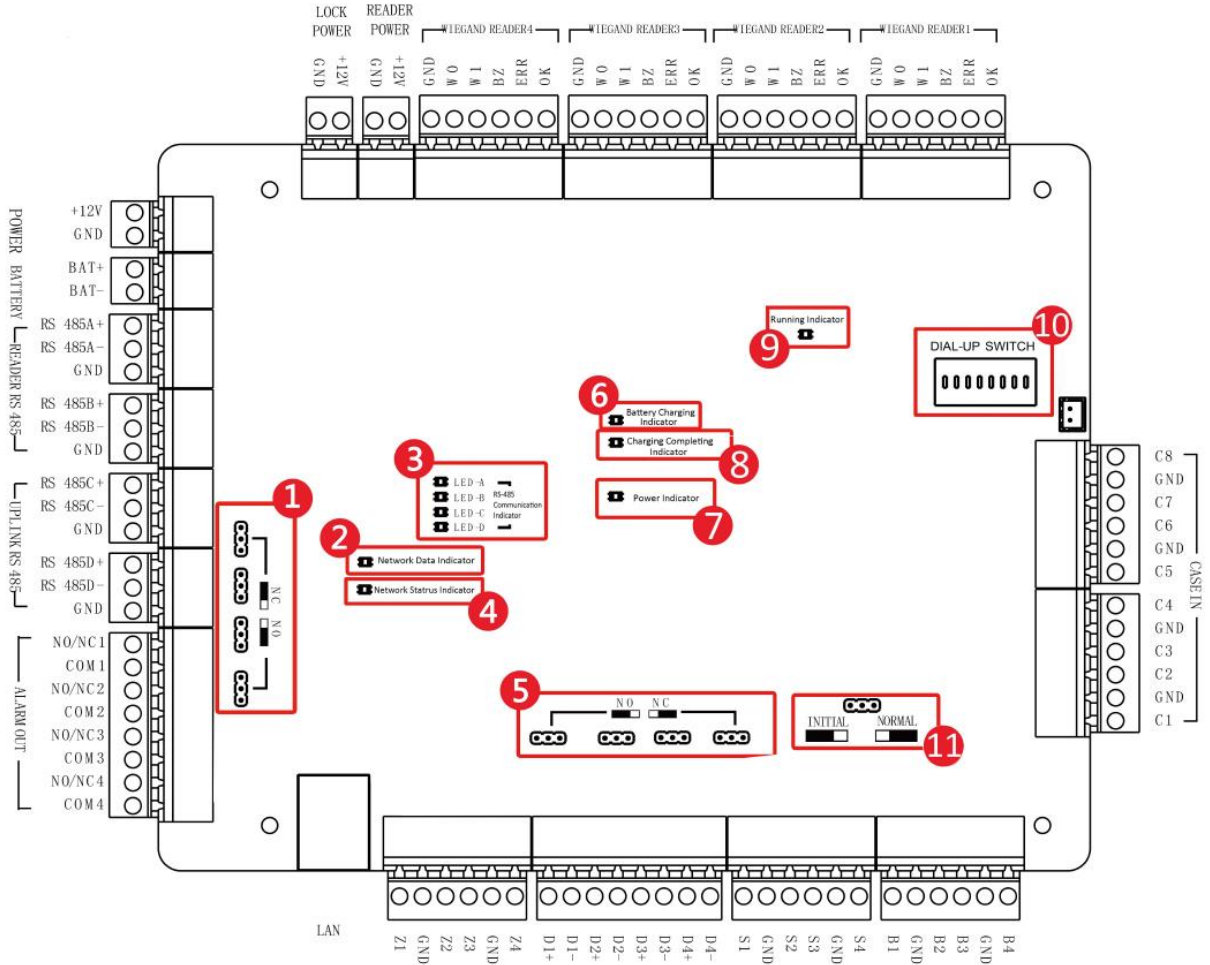


Figure 2-VS-AXESS-2DLX Component Schematic Diagram

Table 2-1 VS-AXESS-2DLX Component Description

No.	Component Description
	VS-AXESS-2DLX
1	Alarm Relay Output Status (NC/NO)
2	Network Data Indicator
3	RS-485 Communication Indicator
4	Network Status Indicator
5	Door Relay Output Status (NC/NO) Choice
6	Battery Charging Indicator
7	Power Indicator
8	Charging Completing Indicator
9	Running Indicator
10	Hardware Initialization and Normal Working Choice
11	Main board dial-up switch/ Reserved

# Chapter 3 Terminal Connection

## 3.1 Terminals Description

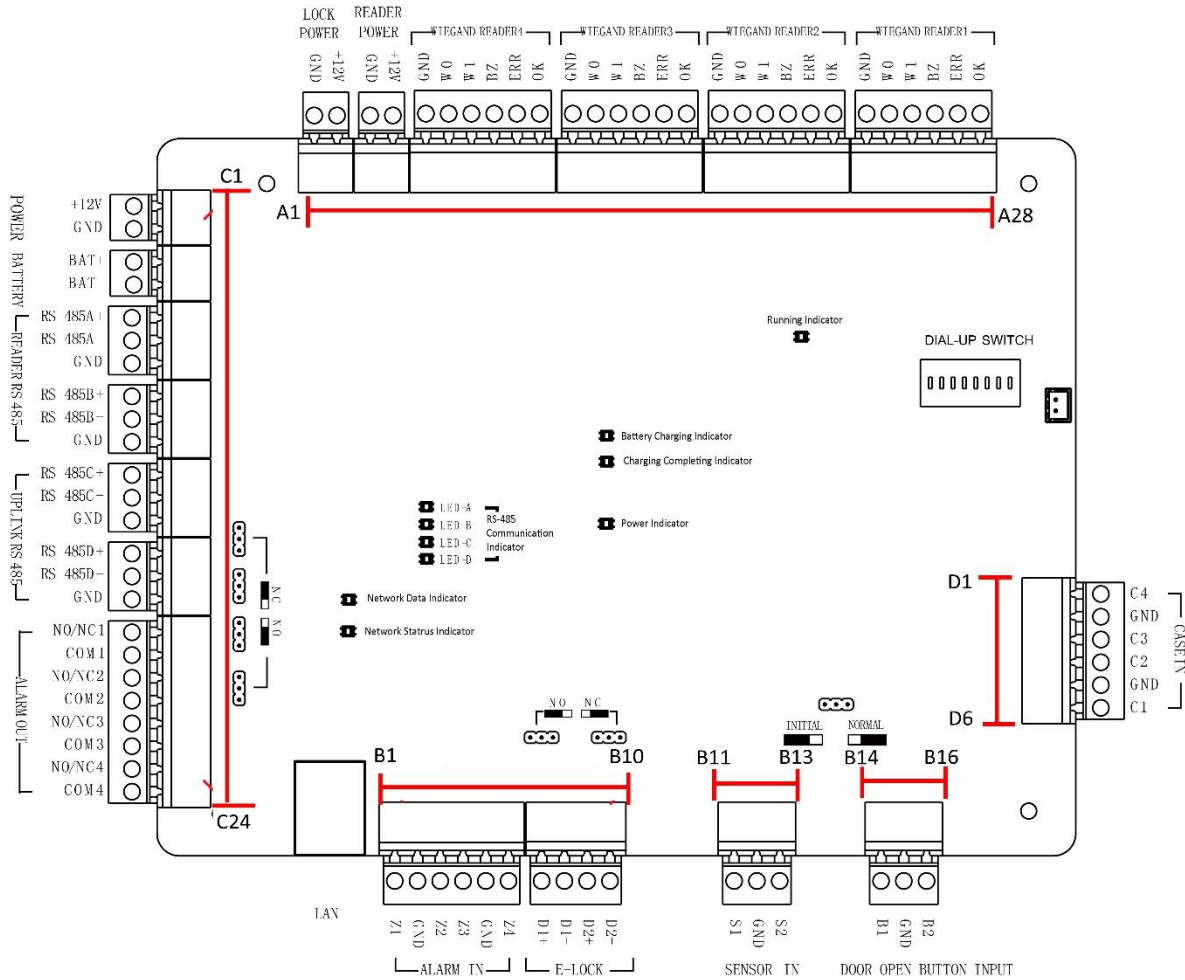


Figure 3-1 VS-AXESS-2DLX Terminal Description

Table-3-1 VS-AXESS-2DLX Terminal Description

No.	VS-AXESS-2DLX		
A1	Power for E-Lock	GND	Grounding
A2		+12V	Power Output of the Lock
A3	Power for Card Reader	GND	Grounding
A4		+12V	Power Output of the Head Read
A5	Wiegand Card Reader 4	GND	Grounding
A6		W0	Wiegand Head Read Data Input Data0
A7		W1	Wiegand Head Read Data Input Data1
A8		BZ	Card Reader Buzzer Control Output
A9		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A10		OK	Indicator of Card Reader Control Output (Valid Card Output)
A11	Wiegand Card Reader 3	GND	Grounding
A12		W0	Wiegand Head Read Data Input Data0
A13		W1	Wiegand Head Read Data Input Data1
A14		BZ	Card Reader Buzzer Control Output
A15		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A16		OK	Indicator of Card Reader Control Output (Valid Card Output)
A17	Wiegand Card Reader 2	GND	Grounding
A18		W0	Wiegand Head Read Data Input Data0
A19		W1	Wiegand Head Read Data Input Data1
A20		BZ	Card Reader Buzzer Control Output
A21		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A22		OK	Indicator of Card Reader Control Output (Valid Card Output)
A23	Wiegand Card Reader 1	GND	Grounding
A24		W0	Wiegand Head Read Data Input Data0
A25		W1	Wiegand Head Read Data Input Data1
A26		BZ	Card Reader Buzzer Control Output
A27		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A28		OK	Indicator of Card Reader Control Output (Valid Card Output)
B1	Arming Region	Z1	Arming Region Access Terminal 1 (Only for Linkage of Alarm Relay Output)
B2		GND	Grounding
B3		Z2	Arming Region Access Terminal 2 (Only for Linkage of Alarm Relay Output)
B4		Z3	Arming Region Access Terminal 3 (Only for Linkage of Alarm Relay Output)
B5		GND	Grounding

B6		Z4	Arming Region Access Terminal 4 (Only for Linkage of Alarm Relay Output)
B7	E-Lock1	D1+	Door 1 Door Relay Input (Dry Contact)
B8		D1-	
B9	E-Lock2	D2+	Door 2 Door Relay Input (Dry Contact)
B10		D2-	
B11	Door Magnetics Detector	S1	Door 1 Magnetic Detector Input
B12		GND	Signal Grounding
B13		S2	Door 2 Magnetic Detector Input
B14	Door Button	B1	Door 1 Door Button Input
B15		GND	Signal Grounding
B16		B2	Door 2 Door Button Input
C1	Power	+12V	DC12V Cathode
C2		GND	Grounding
C3	Battery	BAT+	DC12V Battery Cathode
C4		BAT-	DC12V Battery Anode
C5	Card Reader 485 Interface	RS 485A+	Card Reader RS485+ Access
C6		RS 485A-	Card Reader RS485- Access
C7		GND	Grounding
C8		RS 485B+	Card Reader RS485+
C9		RS 485B-	Card Reader RS485-
C10		GND	Grounding
C11	RS-485 Interface	RS 485C+	Reserved
C12		RS 485C-	
C13		GND	
C14		RS 485D+	
C15		RS 485D	
C16		GND	
C17	Alarm Output	NO/NC1	Alarm Relay 1 Output (Dry Contact)
C18		COM1	
C19		NO/NC2	Alarm Relay 2 Output (Dry Contact)
C20		COM2	
C21		NO/NC3	Alarm Relay 3 Output (Dry Contact)
C22		COM3	
C23		NO/NC4	Alarm Relay 4 Output (Dry Contact)
C24		COM4	
D1	Event Input	C4	Event Alarm Input 4
D2		GND	Grounding
D3		C3	Event Alarm Input3
D4		C2	Event Alarm Input 2
D5		GND	Grounding
D6		C1	Event Alarm Input 1



**Note:**

- The Alarm input hardware interface is normally open by default. So only the normally open signal is allowed. It can be linked to the buzzer of the card reader and access controller, and the alarm relay output and open door relay output.
- Arming region alarm input is only for the alarm relay output linkage.
- RS485 card ID should be set as 1 to 8. For example, the ID of door 1 is 1 and 2 standing for in and out respectively.

## Chapter 4 Card Reader Installation

### 4.1 External Terminal

#### VS-AXESS-2DLX External Terminals



Figure 4-1 VS-AXESS-2DLX External Terminals

## 4.2 Card Reader Installation

### 4.2.1 The Connection of Wiegand Card Reader

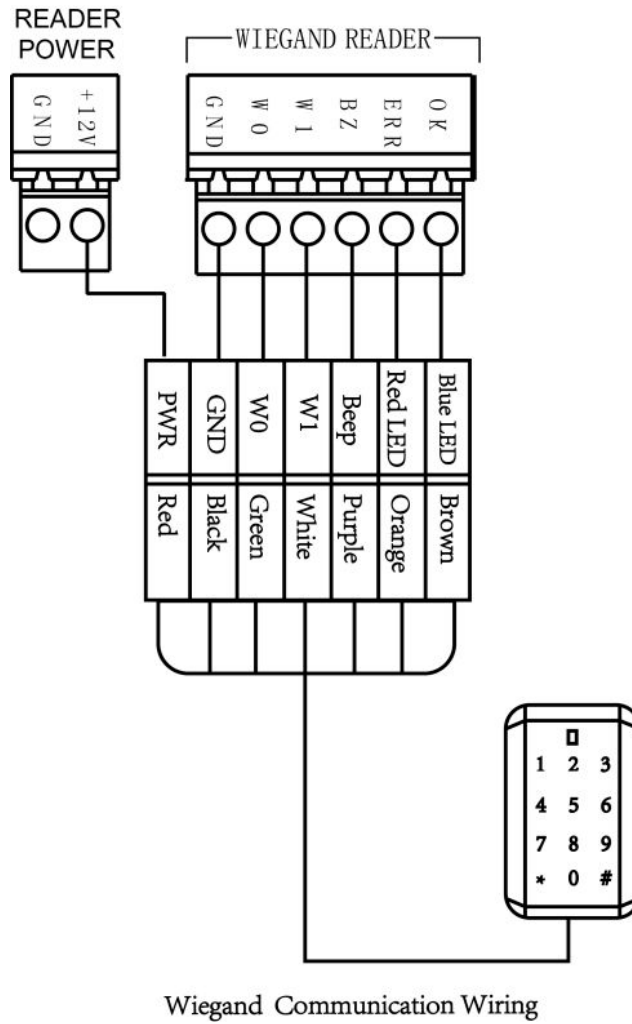


Figure 4-2 Wiring diagram of Wiegand card reader



**Note:**

You must connect the OK/ERR/BZ, if using access controller to control the LED and buzzer of the Wiegand card reader.

### 4.2.2 RS485 Card Reader Connection

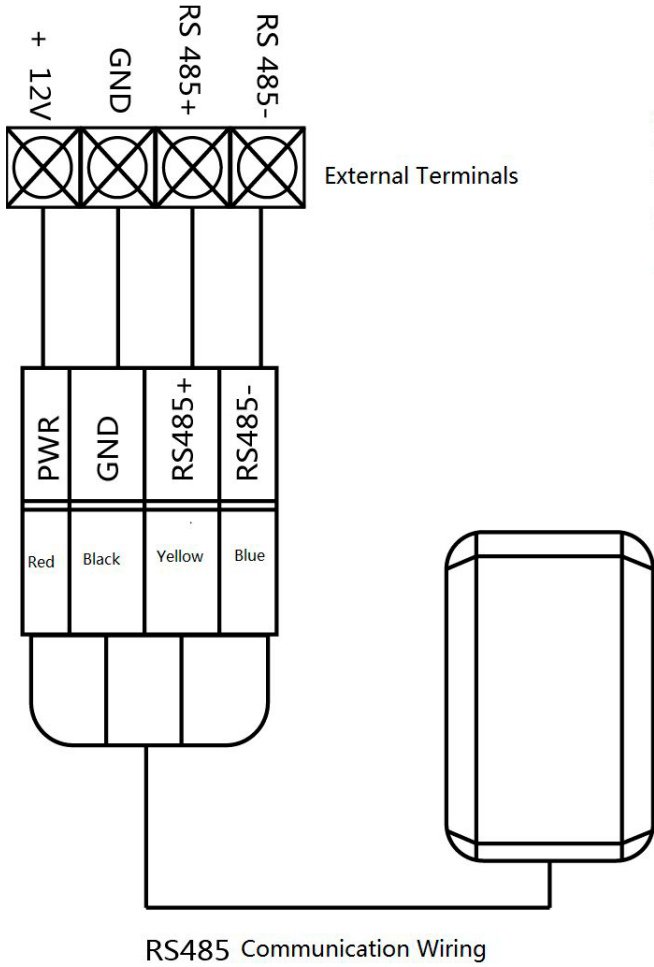


Figure 4-3 Wiring diagram of RS485

## 4.3 Installing E-Lock

### 4.3.1 Installation of Cathode Lock

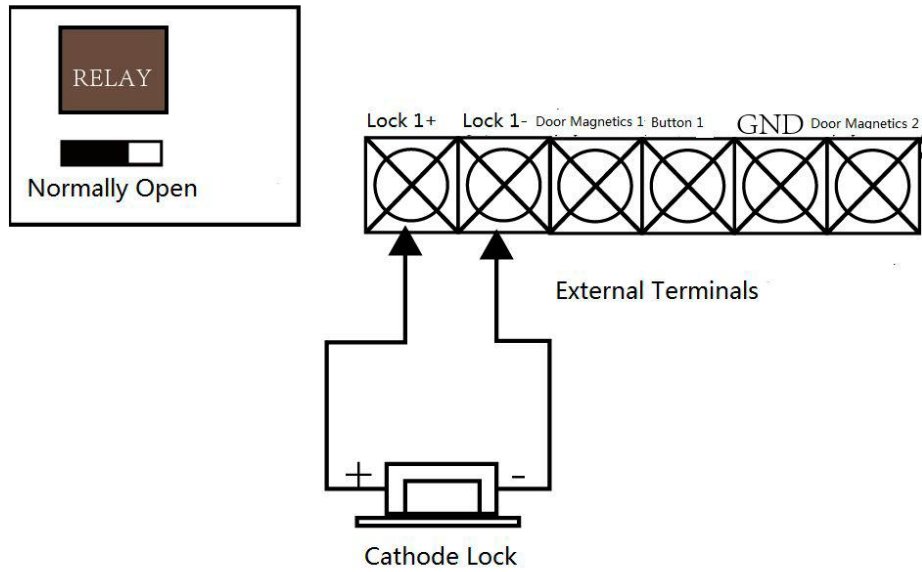


Figure 4-4 Wiring diagram of cathode lock

### 4.3.2 Installation of Anode Lock

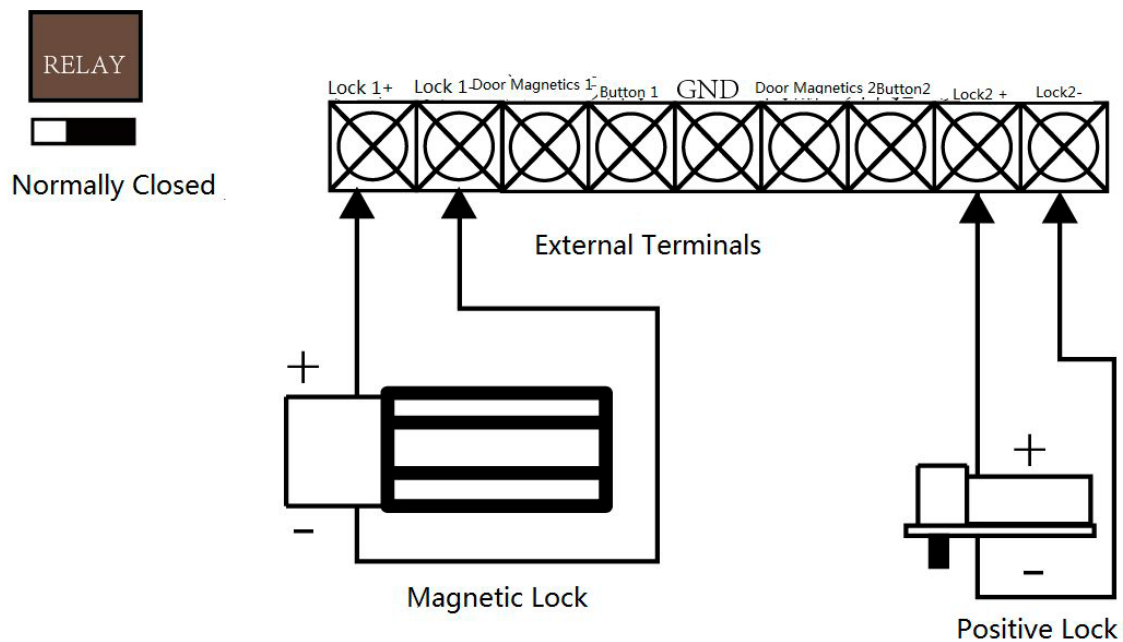


Figure 4-5 Wiring diagram of anode lock

### 4.4 Connecting the External Alarm Device

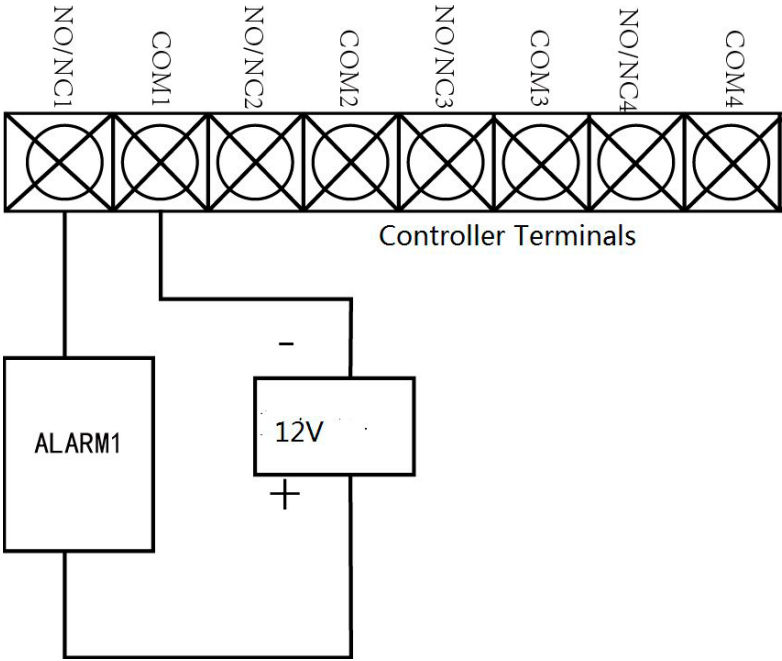


Figure 4-6 External Alarm Device Connection

### 4.5 Door Button Wiring Diagram

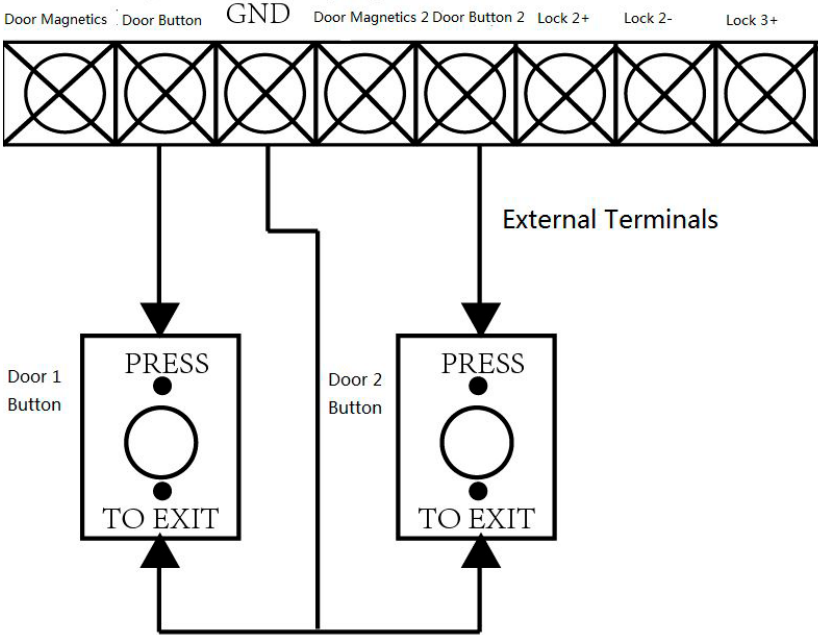


Figure 4-7 Power Button Connection

### 4.6 The Connection of Magnetics Detection

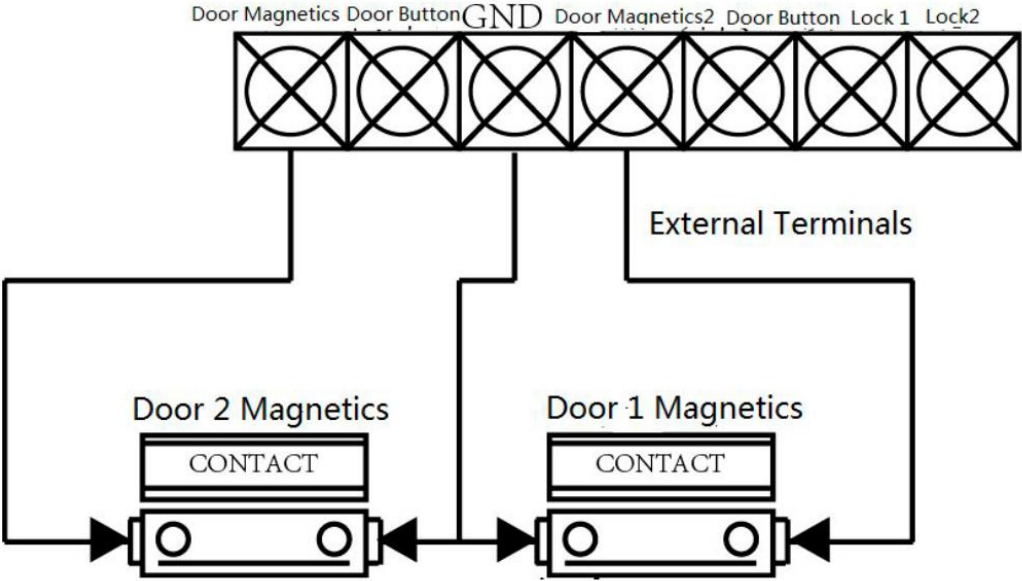


Figure 4-8 Magnetics Connection

### 4.7 Connecting Power Supply

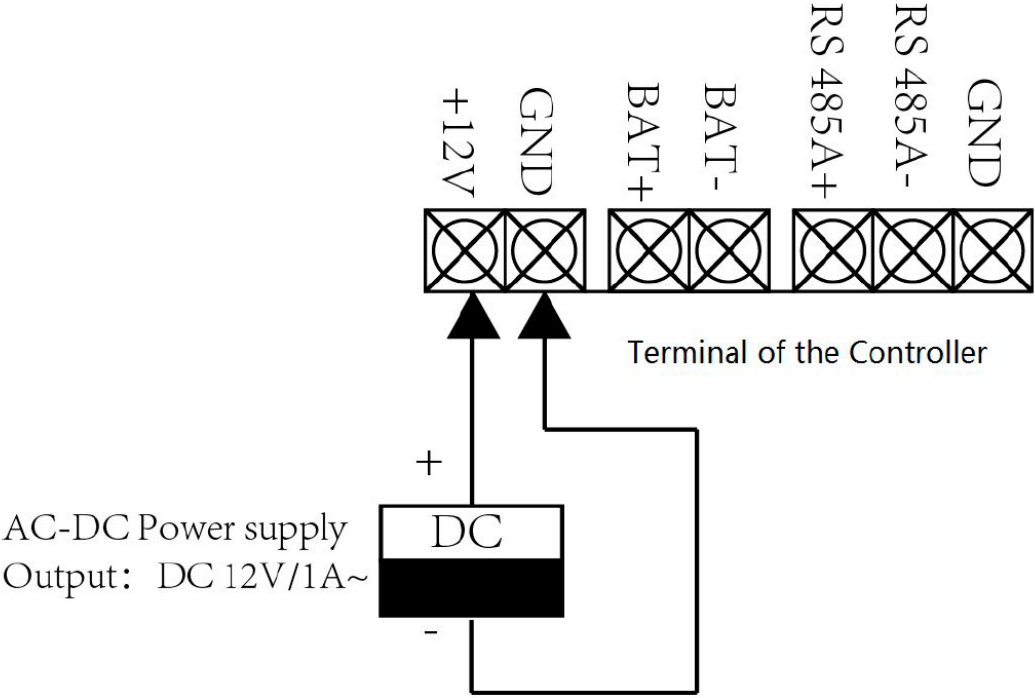


Figure 4-9 Power Supply Connection

## 4.8 Arming Region Input Terminal

### 4.8.1 Connecting Normally Open Detector

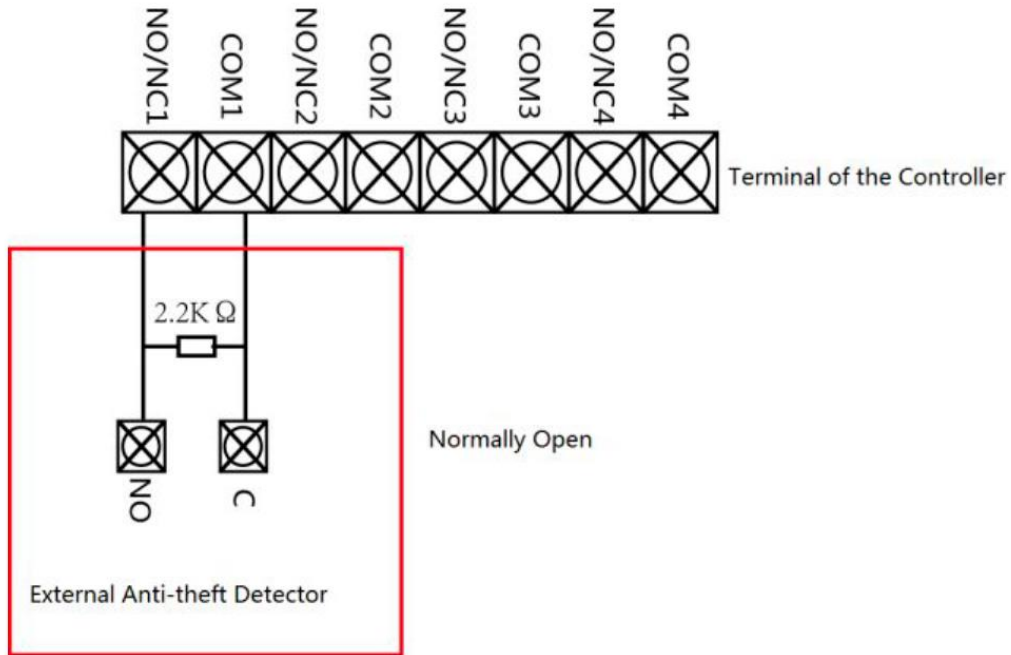


Figure 4-10 Normally Open Status

### 4.8.2 Connecting Normally Closed Detector

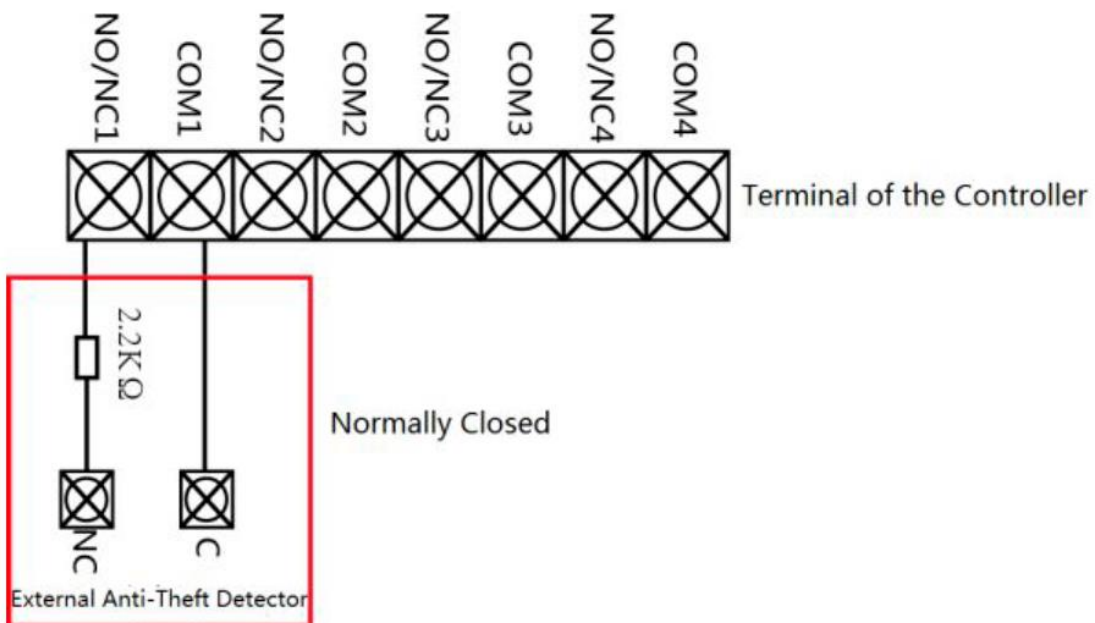


Figure 4-14 Normally Closed Status

# Chapter 5 Settings

## 5.1 Initializing the Hardware

**Steps:**

1. The jumper cap jumps from Normal to Initial.
2. Disconnect the power and restart the access controller, the controller buzzer buzzes a long warning.
3. After the buzzer stops, jump the jumper cap back to Normal.
4. Disconnect the power and restart the access controller.

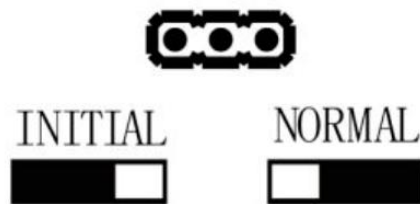


Figure 5-1 Initialization Dial-up



**Note:**

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

## 5.2 Relay Input NO/NC

### 5.2.1 Lock Relay Output

Lock Relay Normally Open Status

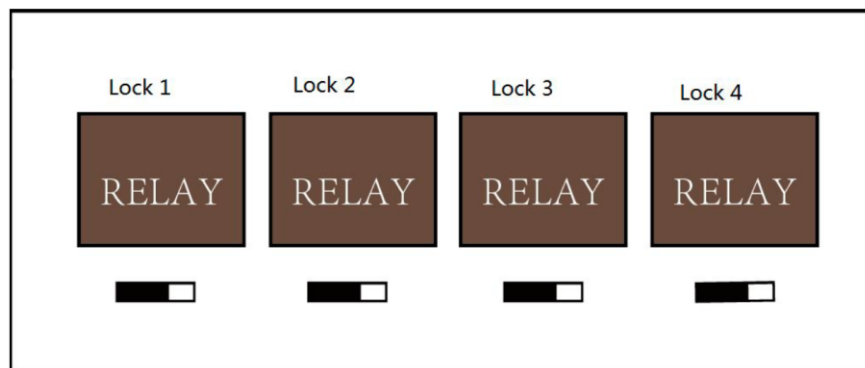


Figure 5-2 Normally Open Status

### Lock Relay Normally Closed Status

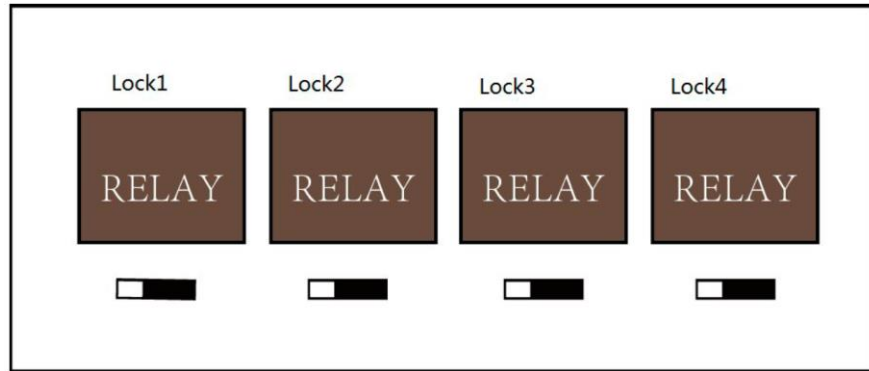


Figure 5-3 Normally Closed Status

## 5.2.2 Alarm Relay Output Status

### Alarm Relay Output Normally Open

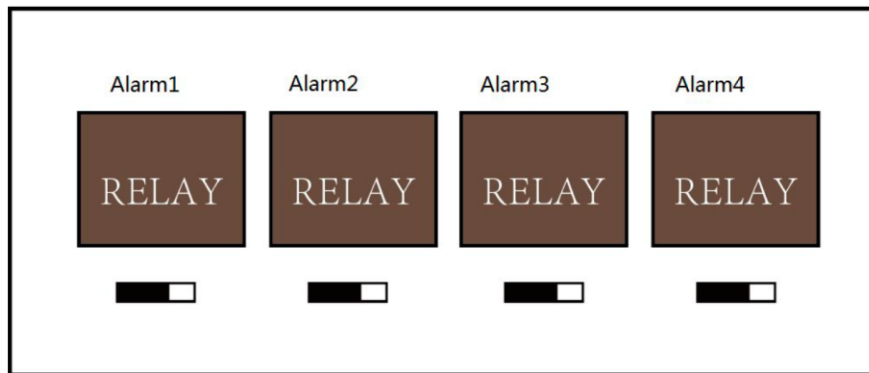


Figure 5-4 Alarm Relay Output Normally Open

### Alarm Relay Output Normally Closed

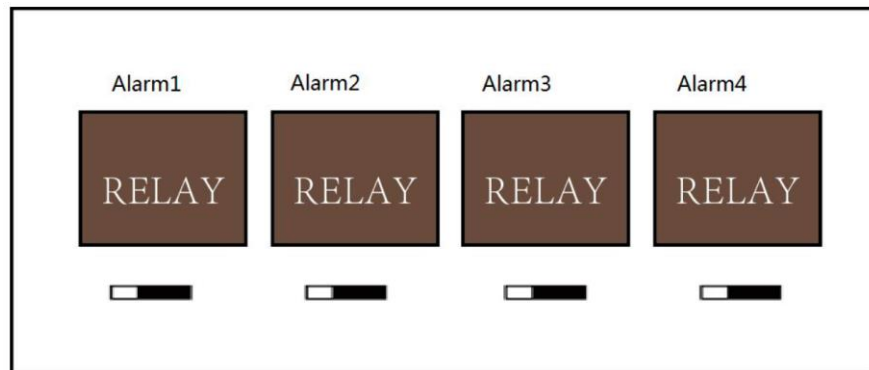


Figure 5-5 Normally Closed Status

## Work Flow of Software

For detailed information, please see the user manual of the client software.

Refer to the following work flow:

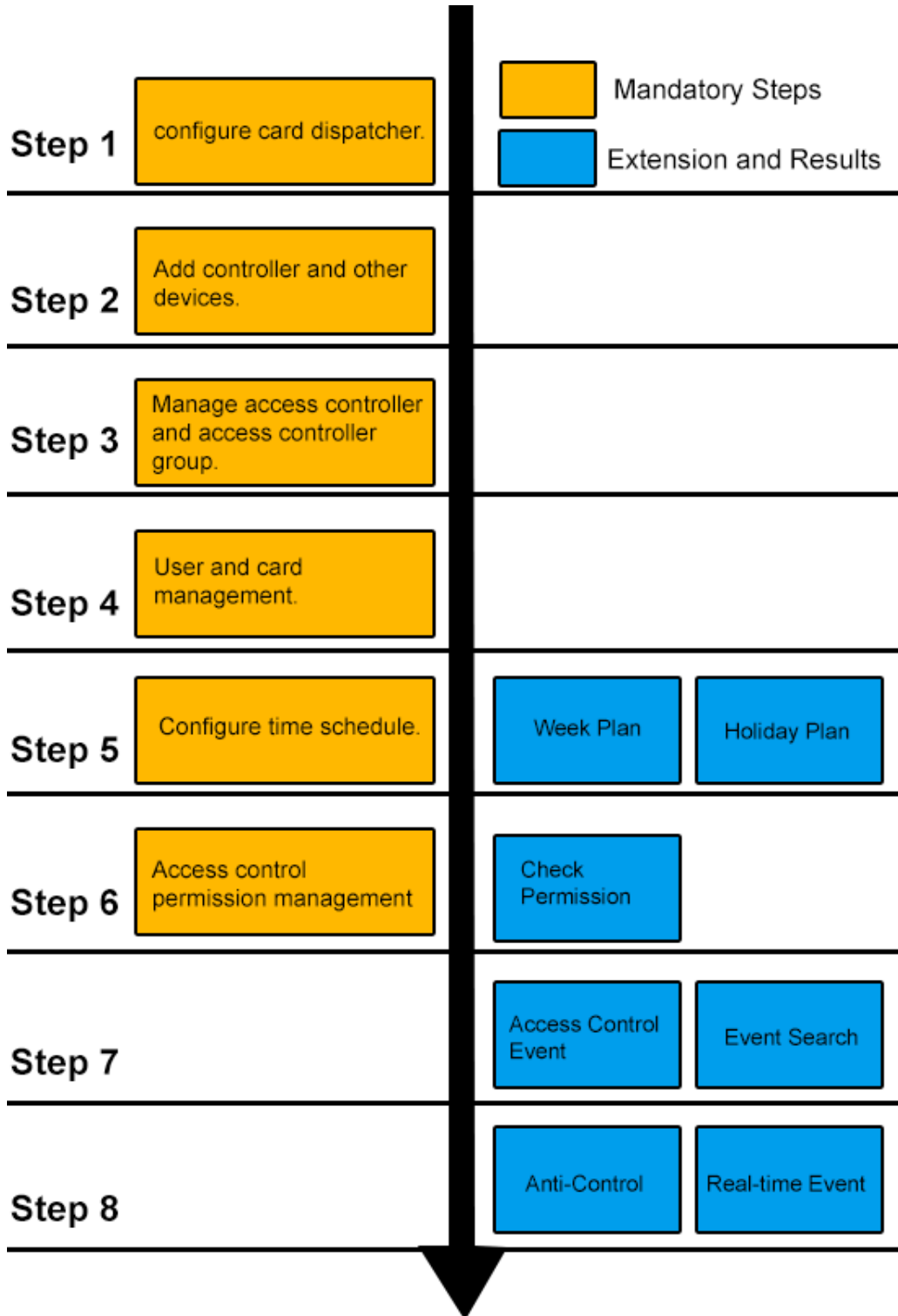


Figure 6-1 Software Client Work Flow

# Chapter 6     Activating the Control Panel

## **Purpose:**

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.

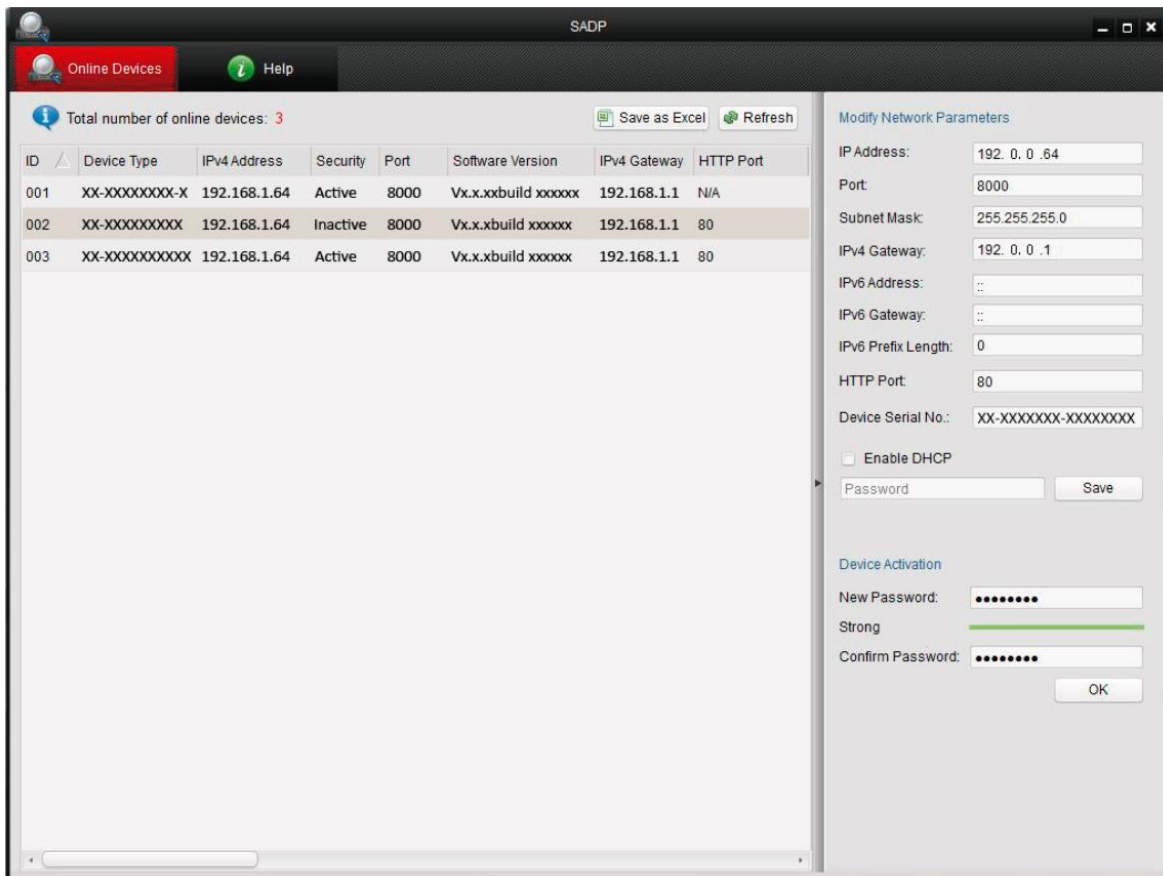
## **6.1 Activation via SADP Software**

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the control panel.

## **Steps:**

1. Run the SADP software to search the online devices.
2. Check the device status from the device list, and select an inactive device.



3. Create a password and input the password in the password field, and confirm the password.



## **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.*

4. Click **OK** to save the password.

You can check whether the activation is completed on the pop-up window.

If activation failed, please make sure that the password meets the requirement and then try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

**Modify Network Parameters**

IP Address: 192.0.0.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.0.0.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXX-XXXXXXX

Enable DHCP

Password  Save

6. Input the password and click the **Save** button to activate your IP address modification.

## 6.2 Activation via Client Software

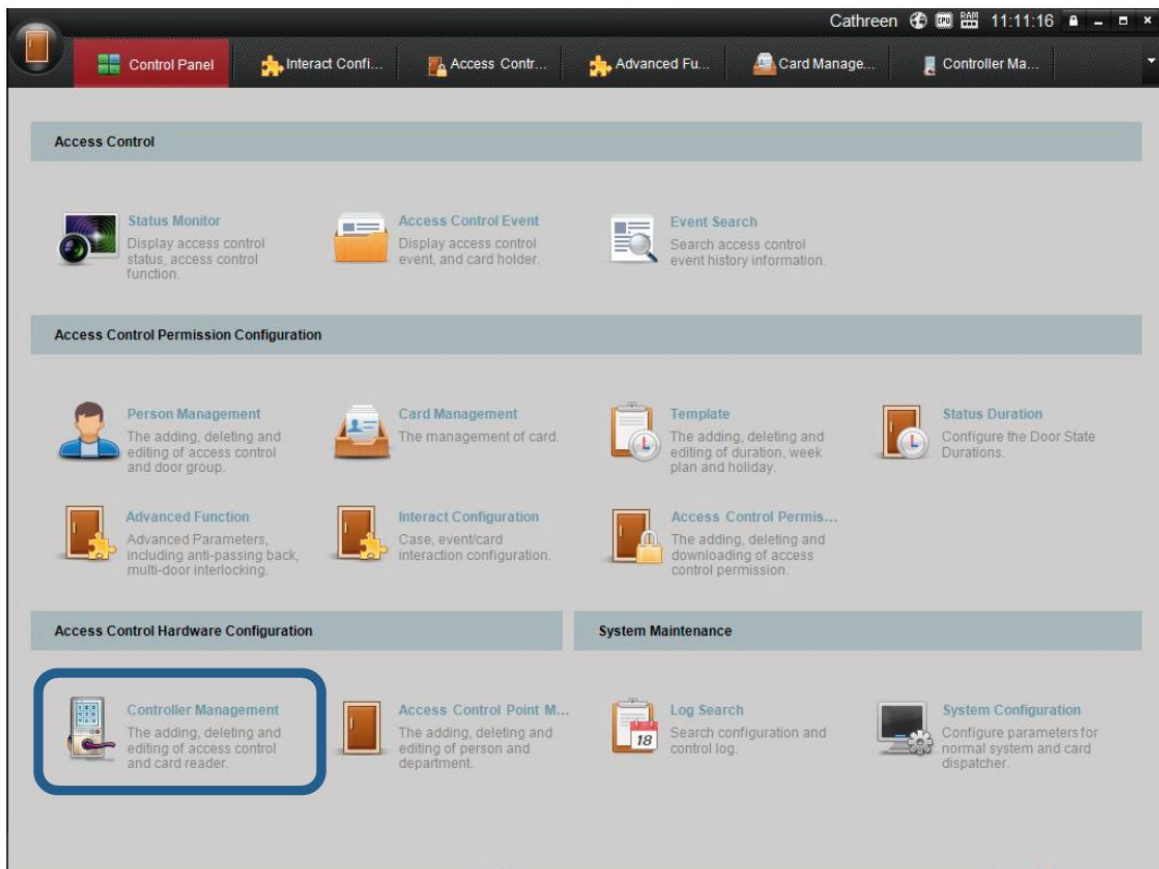
The client software is versatile video management software for multiple kinds of devices. Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

### Steps:

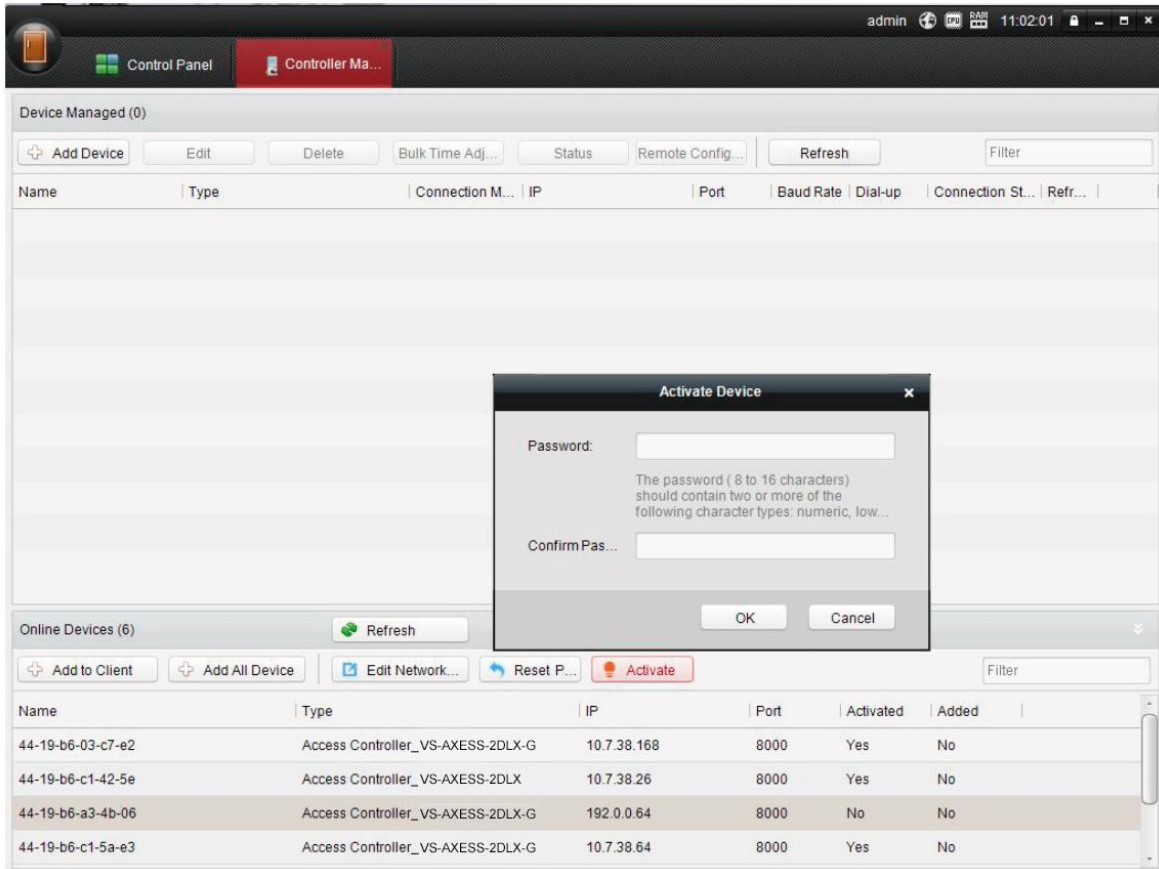
1. Run the client software and the control panel of the software pops up, as shown in the figure below.



2. Click the icon on the upper-left side of the page, select **Access Control** to enter the control panel.




3. Click the **Controller Management** icon to enter the Controller Management interface, as shown in the figure below.



4. Check the device status from the device list, and select an inactive device.
5. Click the **Activate** button to pop up the Activation interface.



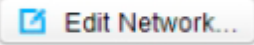
6. Create a password and input the password in the password field, and confirm the password. Click OK button to start activation.



**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.*



7. Click **OK** button to start activation.

8. Click the  button to pop up the Network Parameter Modification interface.

9. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

10. Input the password to activate your IP address modification.

## Specification

Model	VS-AXESS-2DLX
Power	DC 12V/1A
Processor	32bit
Capacity	16M
Uplink Communication Interface	TCP/IP Interface, and RS-485 Interface
Downlink Communication Interface	RS-485 and Wiegand
Normal Card/Event Log	100,000 normal card and 300,000 card wiping logs
LED Indicators	Power Status, Communication Status, Exception Status
Embedded Timer	Yes
Card Readers	4* RS485 Card Reader and 4*Wiegand Card Reader
Input Port	Alarm Input*4, Door Contact *2, Door Button*2, Case Input*4, Anti-Tamper*1
Output Port	Door Relay * 2, Alarm Relay * 4
Working Temperature	-20°C -- +65°C
Working Humidity	10%--90% (noncondensing)
Dimension	370mm(L)*345mm(w)*90mm(H)

Table 6-1 VS-AXESS-2DLX Specification