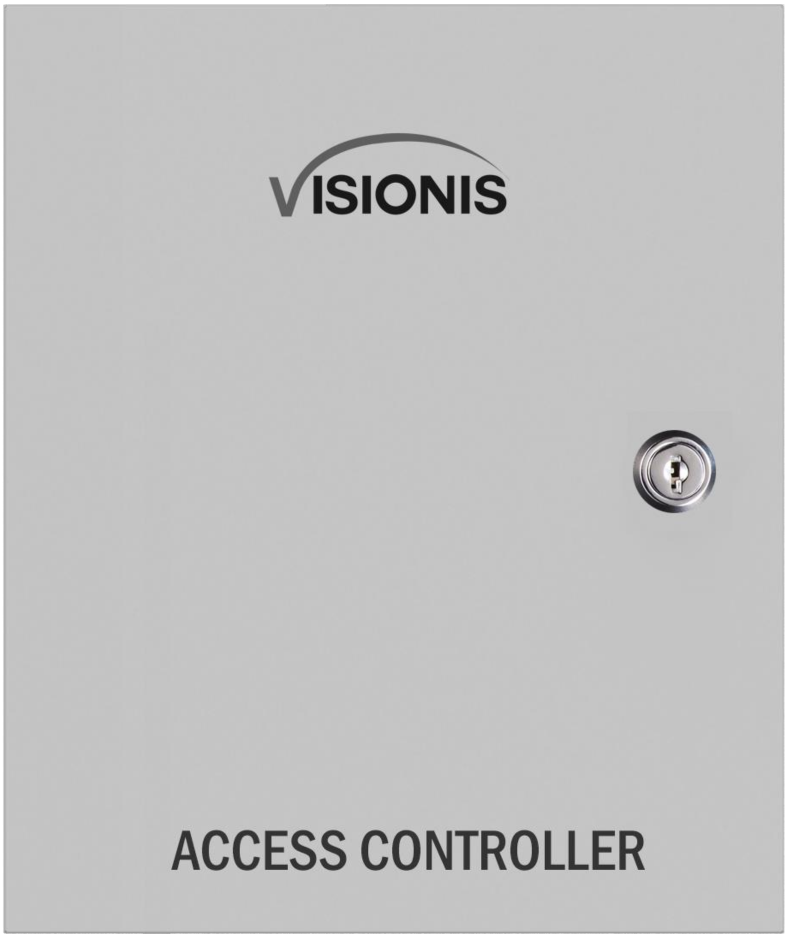
Two Door Access Controller Panel Board TCP/IP Wiegand with Software and Power Supply Included 10,000 Users



VS-AXESS-2ETL Installation Manual

User Manual

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 RESPONSIBILITES 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 USEDWITH 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.

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 (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
⚠ **Warning**	Follow these safeguards to prevent serious injury or death.
⚠ **Note**	Follow these precautions to prevent potential injury or material damage.
📝 **Tips**	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

Chapter 1. Product Description

1.1 Overview

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

VS-AXESS-2ETL 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
- Supports recognition and storage of card number with maximum length of 20
- The access controller can store 10 thousand legal cards and 50 thousand card swiping records
- Supports first card open function, super card and super password function, online upgrade function and remote control of the doors
- Supports Wiegand interface for accessing card reader. 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 watchdog design
- Data can be permanently saved after the access controller is powered off.
- Supports I/O linkage, and event linkage
- Supports alarm of offline event exceeding 90%

Chapter 2. Appearance

2.1 Component Description

Access Controller Component Schematic Diagram

The component schematic diagram is shown below.

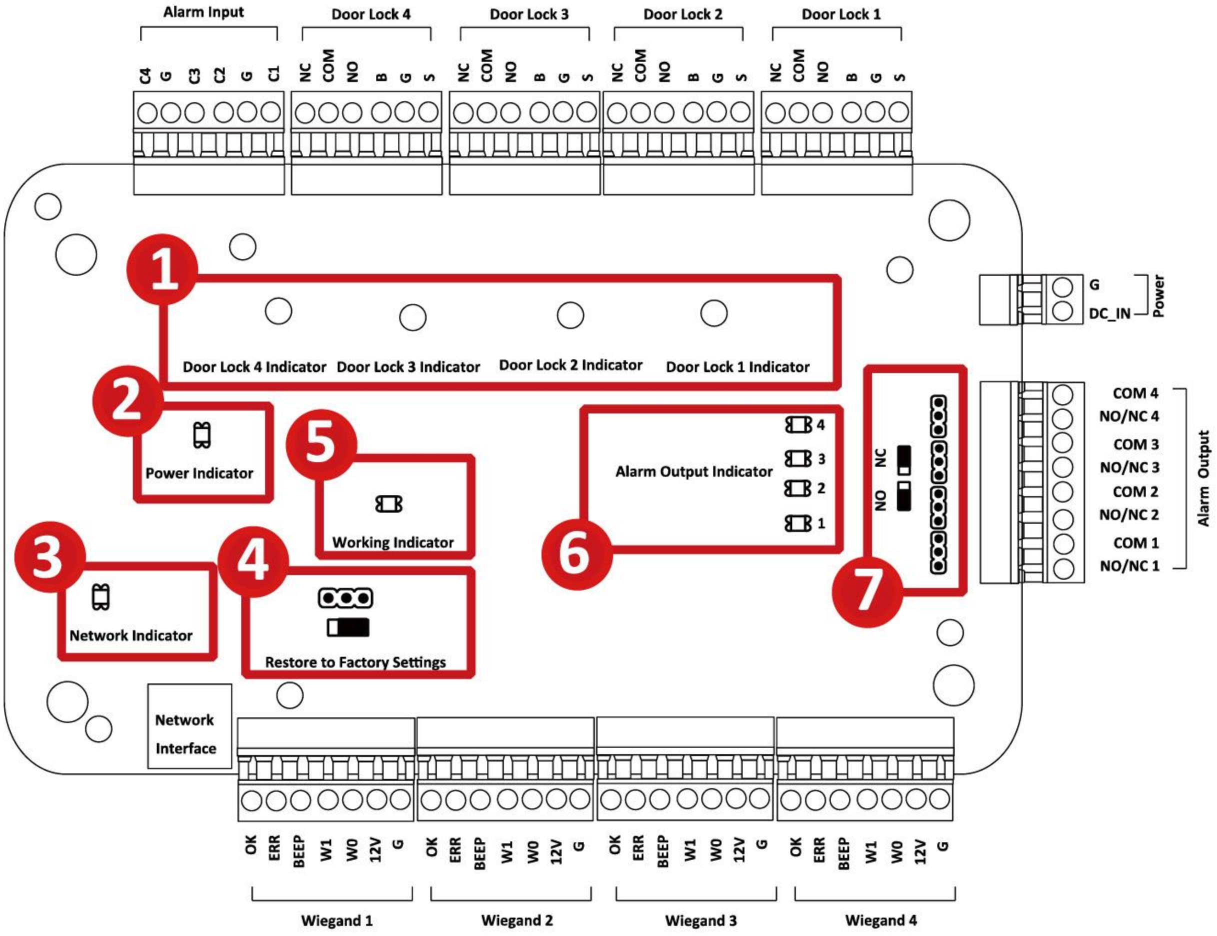


Figure 2-1 VS-AXESS-4ETL Component Schematic Diagram

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

No.	Component Description
	VS-AXESS-2ETL
1	Door Lock 1/2 Indicator
2	Power Indicator
3	Network Indicator
4	Jumper Cap for Restoring Factory Settings
5	Working Indicator
6	Alarm Output Indicator
7	Alarm Output (NO/NC) Jumper Cap

Chapter 3 Terminal Connection

3.1 Terminals Description

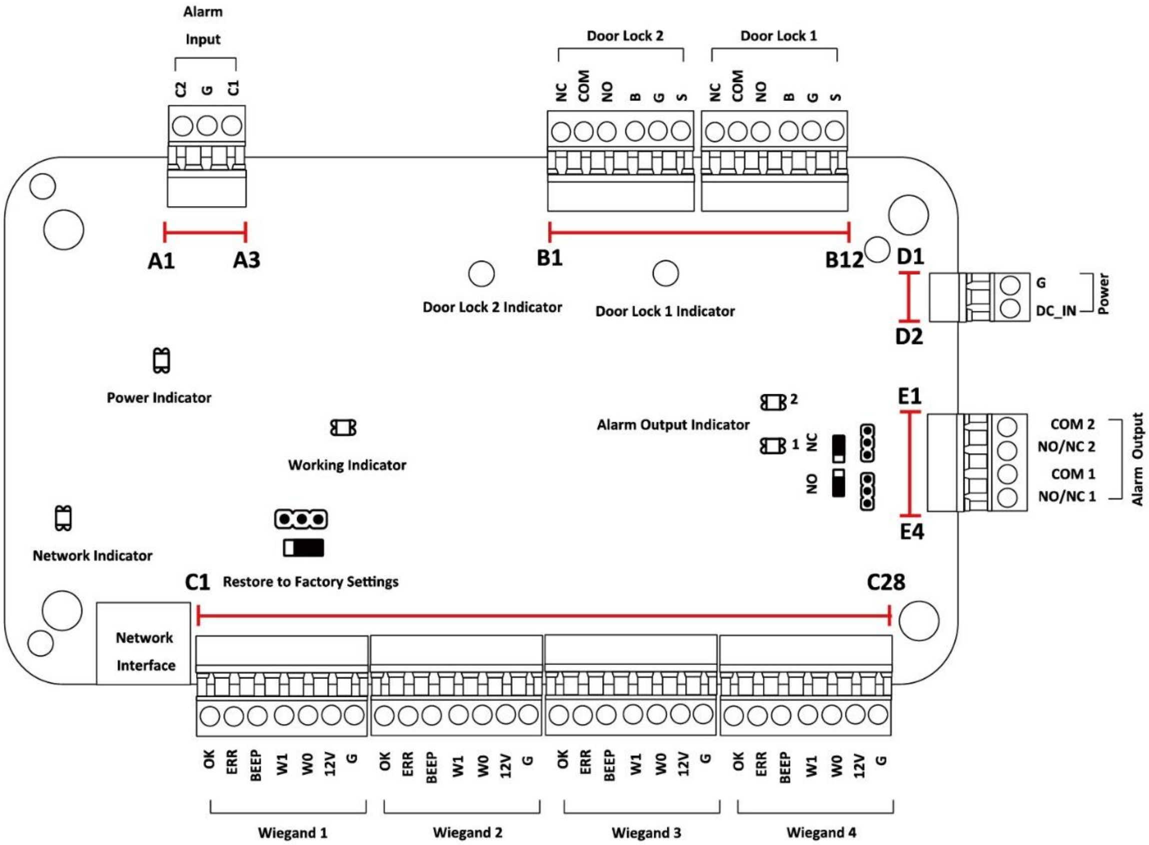


Figure 3-1 VS-AXESS-2ETL Terminal Description

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

No.	VS-AXESS-2ETL		
A1	Alarm Input	IN2	Alarm Input 2
A2		GND	Grounding
A3		IN1	Alarm Input 1
B1	Door 2	NC	Door Lock Relay Output (Dry Contact)
B2		COM	
B3		NO	
B4		BUTTON	Door Button Input
B5		GND	Grounding
B6		SENSOR	Door Magnetic detector

B7	Door 1	NC	Door Lock Relay Output (Dry Contact)
B8		COM	
B9		NO	
B10		BUTTON	Door Button Input
B11		GND	Grounding
B12		SENSOR	Door Magnetic detector
D1	Power	GND	DC12V Grounding
D2		+12V	DC12V Input
E1	Alarm Output 2	COM2	Alarm Relay Output 2 (Dry Contact)
E2	Alarm Output 1	NO/NC2	
C1	Wiegand Card Reader 1	OK	Indicator of Card Reader Control Output (Valid Card Output)
C2		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
C3		BZ	Card Reader Buzzer Control Output
C4		W1	Wiegand Head Read Data Input Data1
C5		W0	Wiegand Head Read Data Input Data0
C6		PWR	Card Reader Power Output
C7		GND	
C8	Wiegand Card Reader 2	OK	Indicator of Card Reader Control Output (Valid Card Output)
C9		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
C10		BZ	Card Reader Buzzer Control Output
C11		W1	Wiegand Head Read Data Input Data1
C12		W0	Wiegand Head Read Data Input Data0
C13		PWR	Card Reader Power Output
C14		GND	
C15	Wiegand Card Reader 3	OK	Indicator of Card Reader Control Output (Valid Card Output)
C16		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
C17		BZ	Card Reader Buzzer Control Output
C18		W1	Wiegand Head Read Data Input Data1
C19		W0	Wiegand Head Read Data Input Data0
C20		PWR	Card Reader Power Output
C21		OK	
C22	Wiegand Card Reader 4	OK	Indicator of Card Reader Control Output (Valid Card Output)

C23		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
C24		BZ	Card Reader Buzzer Control Output
C25		W1	Wiegand Head Read Data Input Data1
C26		W0	Wiegand Head Read Data Input Data0
C27		PWR	Card Reader Power Output
C28		OK	

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.

- For single-door access controller, the Wiegand card reader 1 and 2respectivelycorrespond to the entering and exiting card readers of door 1. For two-door access controller, the Wiegand card reader 1 and 2respectivelycorrespond to the entering and exiting card readers of door 1 , and the Wiegand card reader 3 and 4respectivelycorrespond to the entering and exiting card readers of door 2. For single-door access controller, the Wiegand card reader 1, 2, 3 and 4respectivelycorrespond to the entering card readers of door 1, 2, 3, and 4.

Chapter 4 External Device Wiring

4.1 Card Reader Wiring

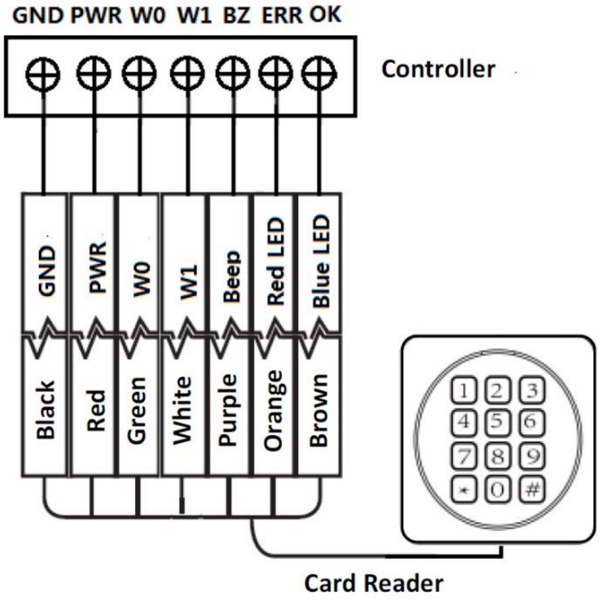


Figure 4-1 Wiring diagram of Wiegand card reader

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 Installing Door Lock

4.2.1 Installation of Cathode Lock

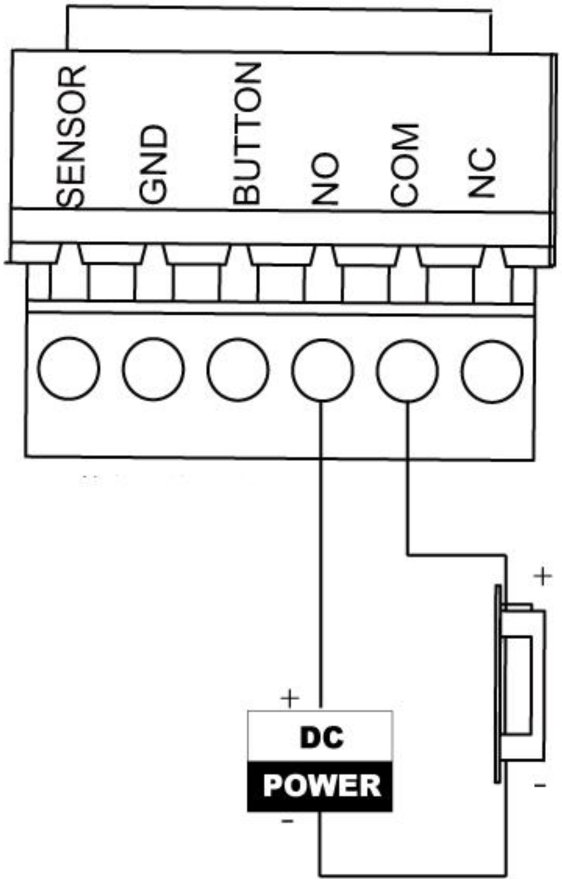


Figure 4-2 Wiring diagram of cathode lock

4.2.2 Installation of Anode Lock

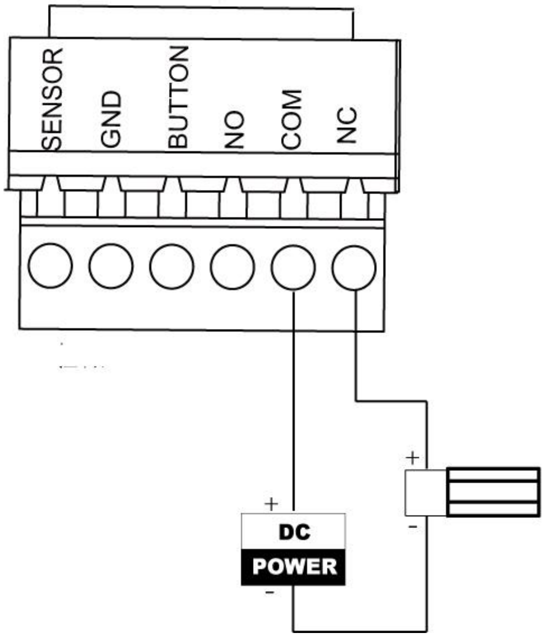


Figure 4-3 Wiring diagram of anode lock

4.3 Connecting the External Alarm Device

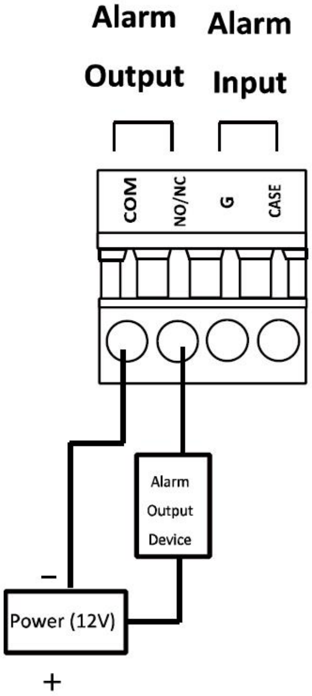


Figure 4-4 External Alarm Device Connection

4.4 Door Button Wiring Diagram

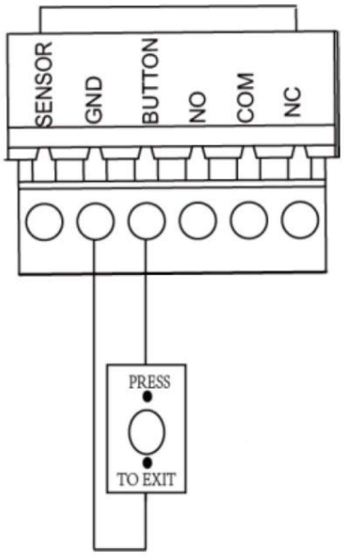


Figure 4-5 Power Button Connection

4.5 The Connection of Magnetics Detection

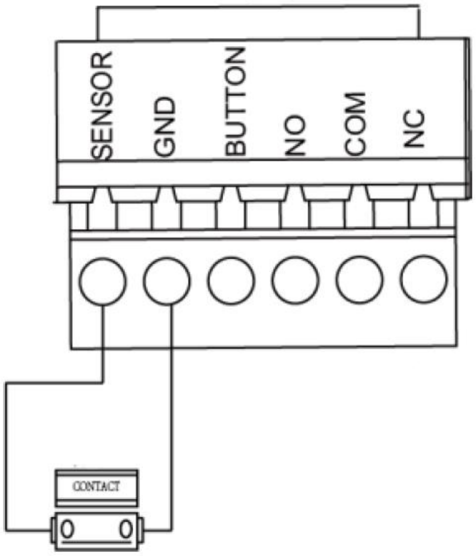


Figure 4-6 Magnetics Connection

4.6 Connecting Power Supply

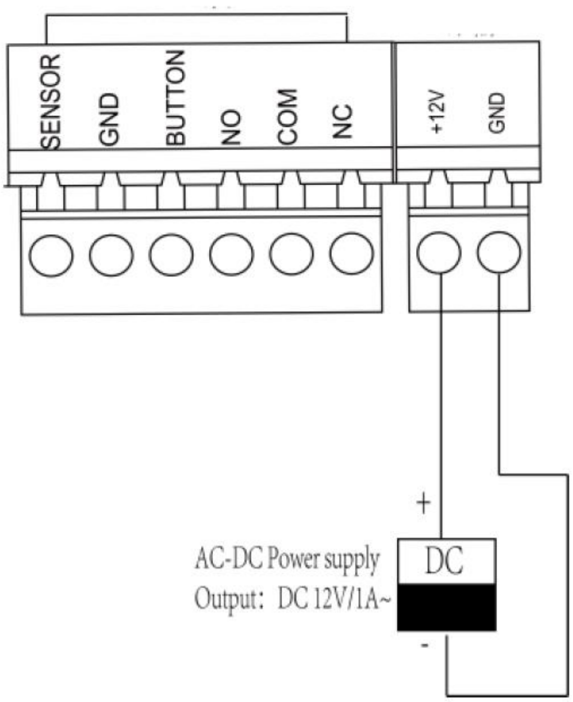


Figure 4-7 Power Supply Connection

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.

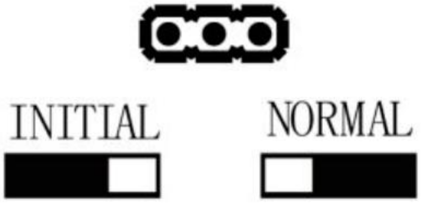


Figure 5-1 Initialization Dial-up

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

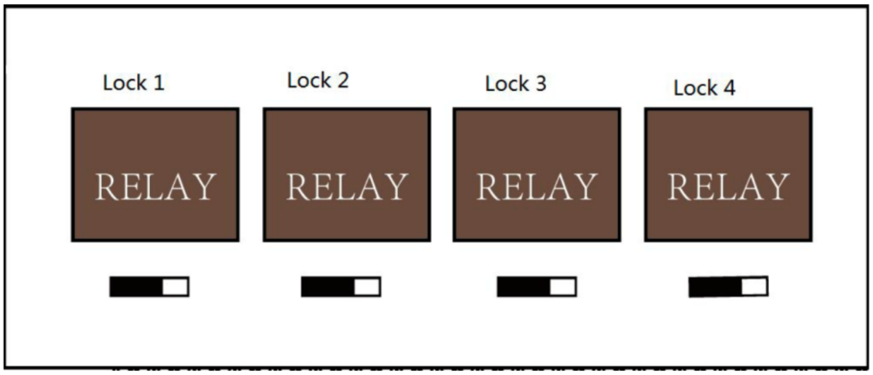


Figure 5-2 Normally Open Status

Lock Relay Normally Closed Status

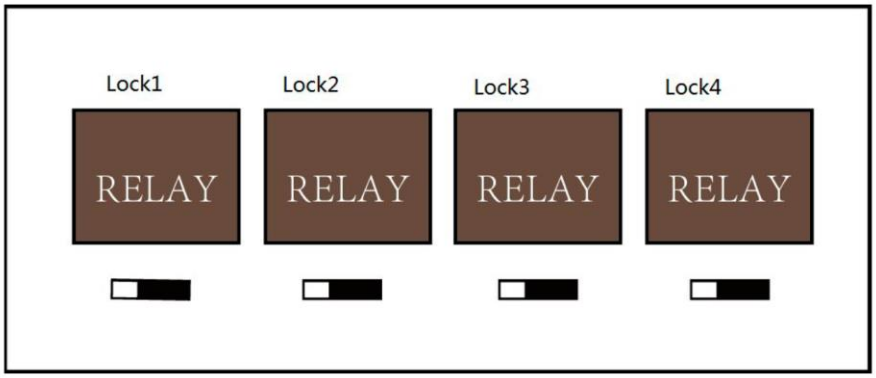


Figure 5-3 Normally Closed Status

5.2.2 Alarm Relay Output Status

Alarm Relay Output Normally Open

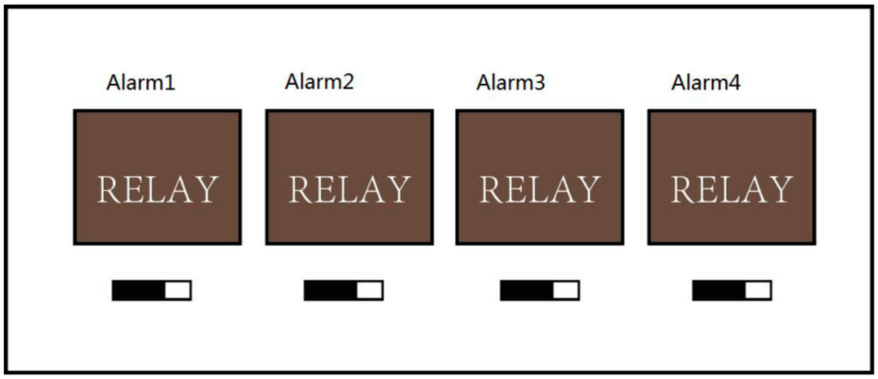


Figure 5-4 Alarm Relay Output Normally Open

Alarm Relay Output Normally Closed

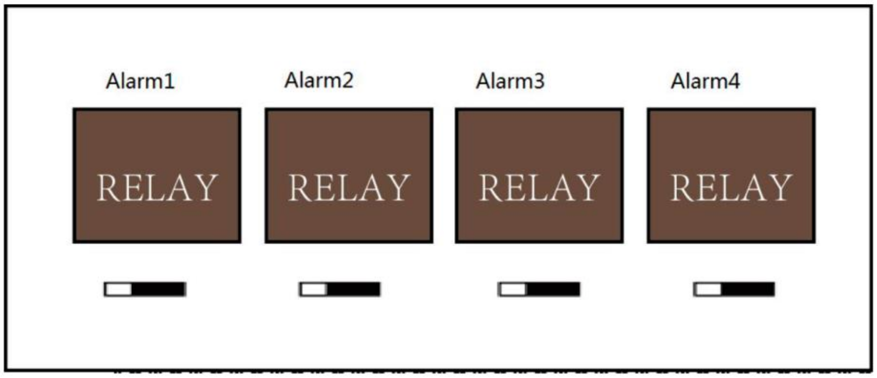


Figure 5-5 Normally Closed Status

Work Flow of Software

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

Refer to the following work flow:

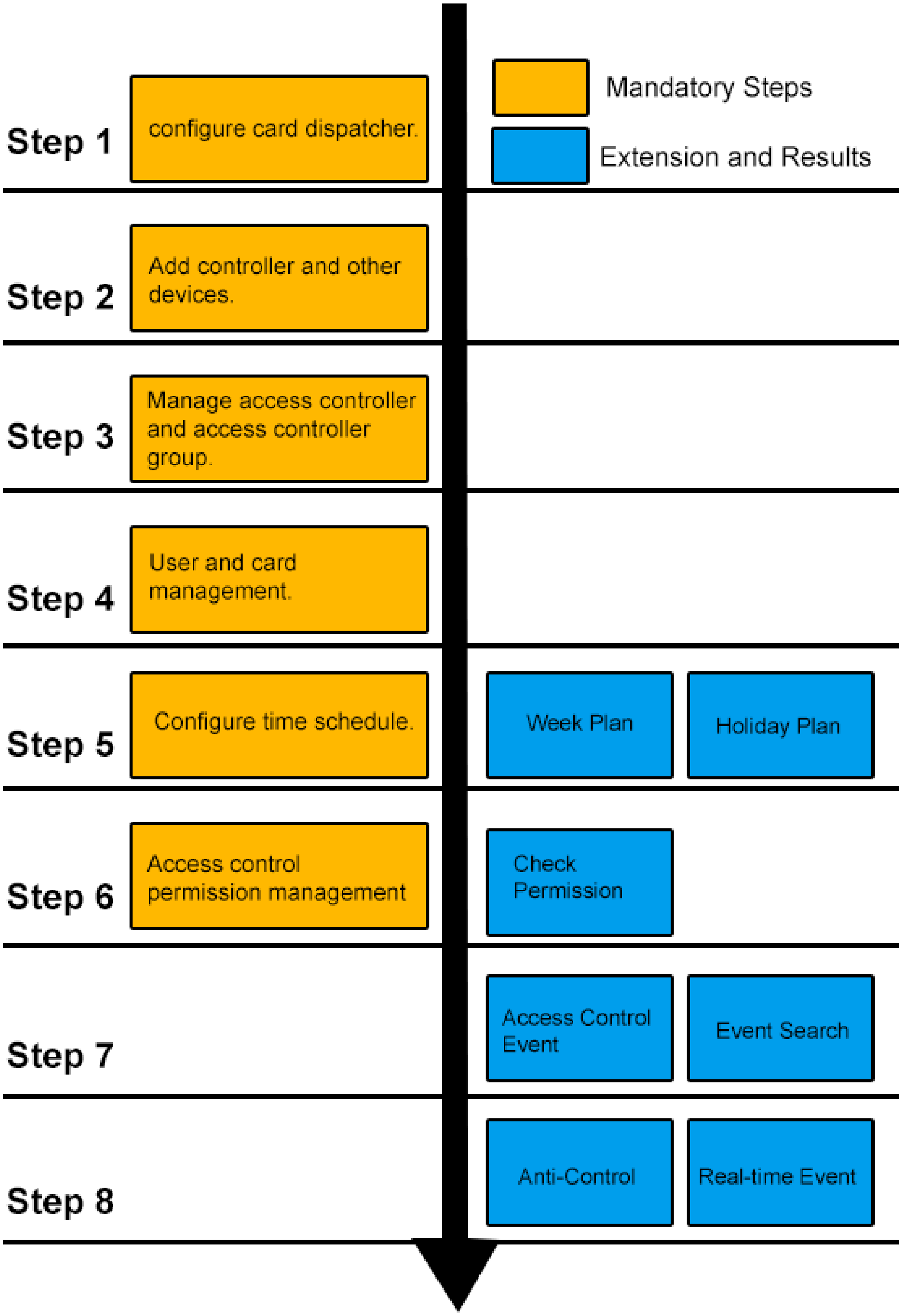


Figure 6-1 Software Client Work Flow

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

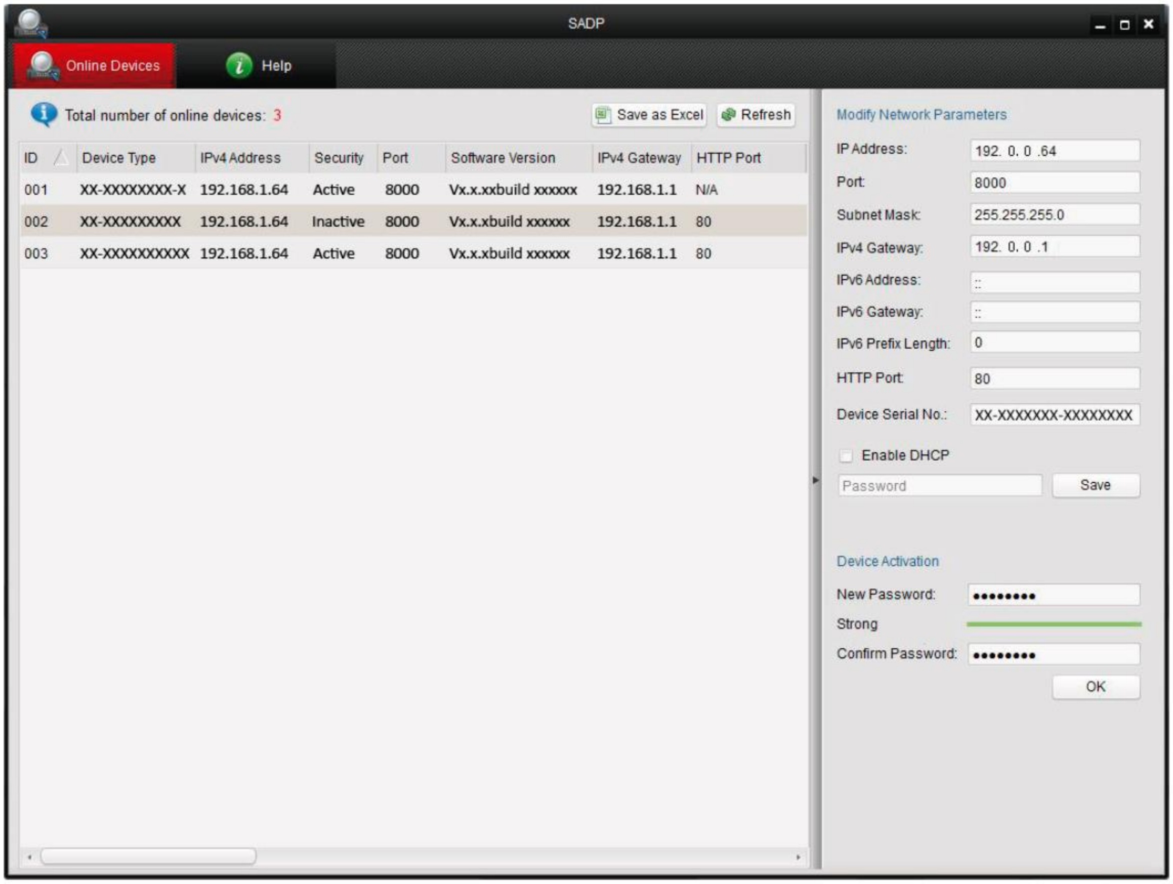
SADP software is used for detecting the online device, activating the device, and resetting the password.

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.



Total number of online devices: 3

ID	Device Type	IPv4 Address	Security	Port	Software Version	IPv4 Gateway	HTTP Port
001	XX-XXXXXXXX-X	192.168.1.64	Active	8000	Vx.x.xxbuild xxxxxx	192.168.1.1	N/A
002	XX-XXXXXXXXX	192.168.1.64	Inactive	8000	Vx.x.xbuild xxxxxx	192.168.1.1	80
003	XX-XXXXXXXXXX	192.168.1.64	Active	8000	Vx.x.xbuild xxxxxx	192.168.1.1	80

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-XXXXXXXX

□ Enable DHCP

Password Save

Device Activation

New Password:	••••••••
Strong	
Confirm Password:	••••••••

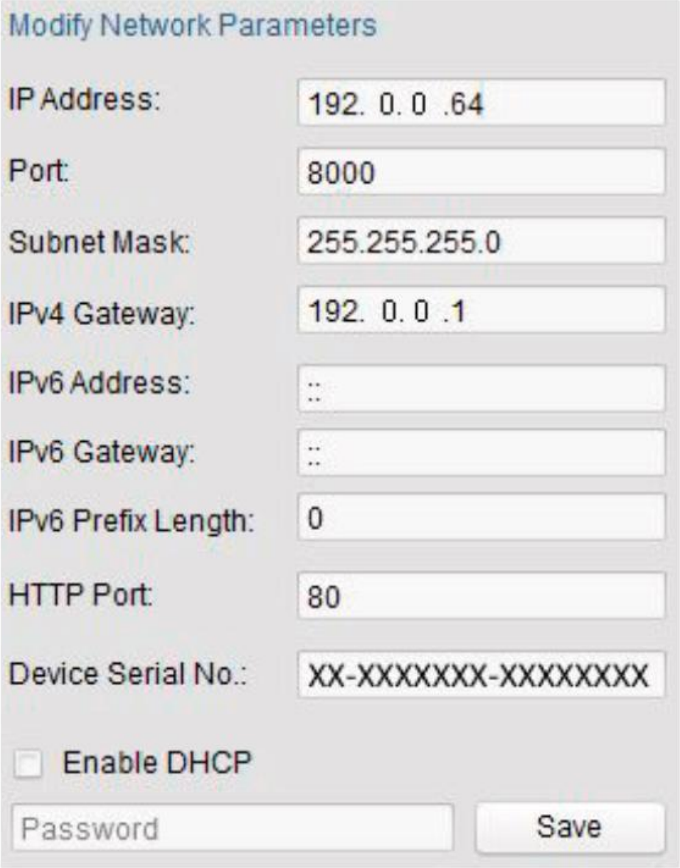
OK

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-XXXXXXXX

□ Enable DHCP

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

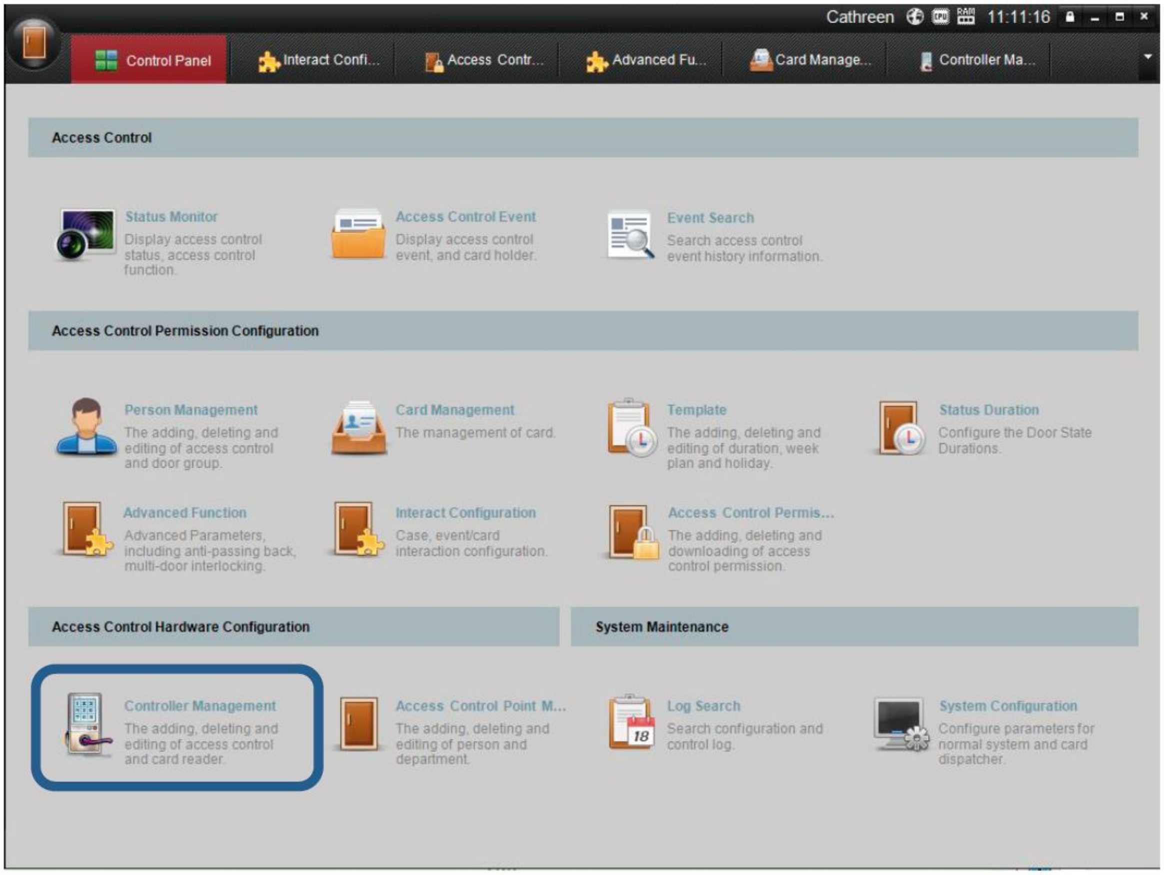
6.2 Activation via Client Software

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.



Access Control

Status Monitor
Display access control status, access control function.

Access Control Event
Display access control event, and card holder.

Event Search
Search access control event history information.

Access Control Permission Configuration

Person Management
The adding, deleting and editing of access control and door group.

Card Management
The management of card.

Template
The adding, deleting and editing of duration, week plan and holiday.

Status Duration
Configure the Door State Durations.

Advanced Function
Advanced Parameters, including anti-passing back, multi-door interlocking.

Interact Configuration
Case, event/card interaction configuration.

Access Control Permis...
The adding, deleting and downloading of access control permission.

Access Control Hardware Configuration

Controller Management
The adding, deleting and editing of access control and card reader.

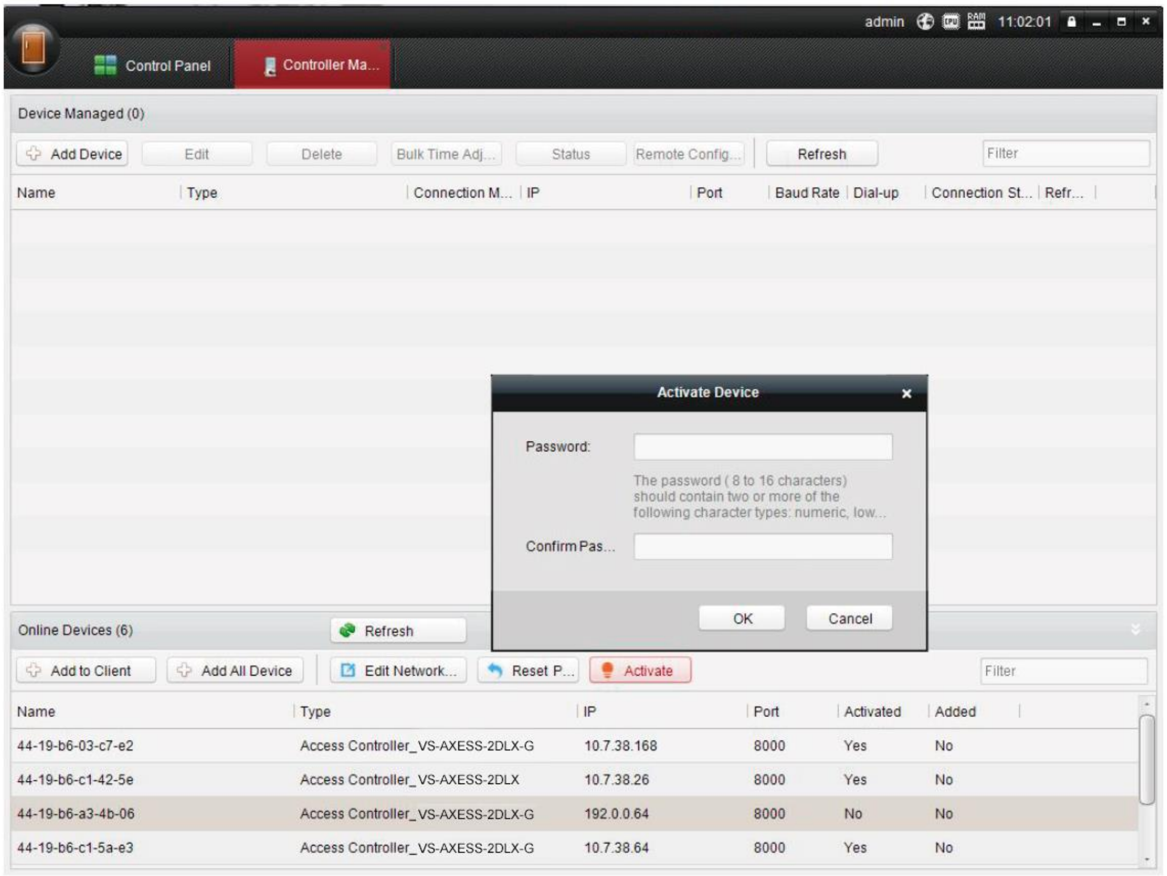
Access Control Point M...
The adding, deleting and editing of person and department.

System Maintenance

Log Search
Search configuration and control log.

System Configuration
Configure parameters for normal system and card dispatcher.

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



Password:

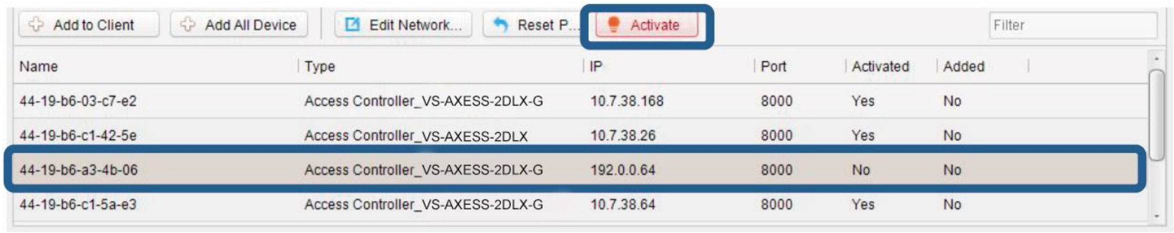
The password (8 to 16 characters) should contain two or more of the following character types: numeric, low...

Confirm Pas...

Name	Type	IP	Port	Activated	Added
44-19-b6-03-c7-e2	Access Controller_VS-AXESS-2DLX-G	10.7.38.168	8000	Yes	No
44-19-b6-c1-42-5e	Access Controller_VS-AXESS-2DLX	10.7.38.26	8000	Yes	No
44-19-b6-a3-4b-06	Access Controller_VS-AXESS-2DLX-G	192.0.0.64	8000	No	No
44-19-b6-c1-5a-e3	Access Controller_VS-AXESS-2DLX-G	10.7.38.64	8000	Yes	No

4. Check the device status from the device list, and select an inactive device.

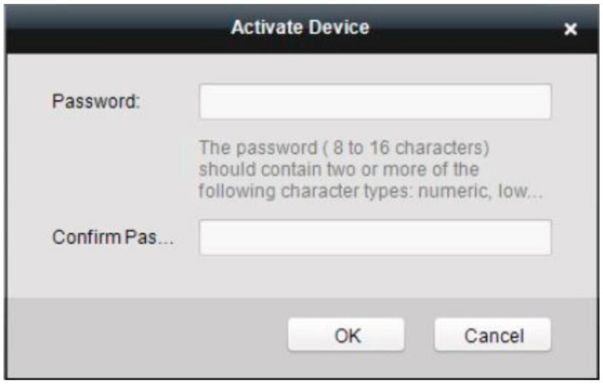
5. Click the **Activate** button to pop up the Activation interface.



Name	Type	IP	Port	Activated	Added
44-19-b6-03-c7-e2	Access Controller_VS-AXESS-2DLX-G	10.7.38.168	8000	Yes	No
44-19-b6-c1-42-5e	Access Controller_VS-AXESS-2DLX	10.7.38.26	8000	Yes	No
44-19-b6-a3-4b-06	Access Controller_VS-AXESS-2DLX-G	192.0.0.64	8000	No	No
44-19-b6-c1-5a-e3	Access Controller_VS-AXESS-2DLX-G	10.7.38.64	8000	Yes	No

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.*



The password (8 to 16 characters) should contain two or more of the following character types: numeric, low...

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

8. Click the Edit Network... 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.