DS-K2800 Series

Access Controller

Quick Start Guide

UD.6L0206D1184A01

User Manual

About this Manual

This Manual is applicable to Access Controller

Product Name	Serials
Access Controller	DS-K2801 Serials Access Controller
	DS-K2802 Serials Access Controller
	DS-K2804 Serials Access Controller

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 RESPONSIBILITES 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.

0100001060303

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

CE 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 camera 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℃ or lower than -20℃)

Keep ventilation.

Do not operate in humid environment.

Do not operate in explosive environment.

Keep the device clean and dry.

Avoid bare electrical wire.

Table of Contents

Chapter 1 Product Description

1.1 Overview

DS-K2800 is a powerful and stable access controller, using the logical architecture design. DS-K2800 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, Private 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

Component Description

Access Controller Component Schematic Diagram

Take DS-K2804 as an example, the component schematic diagram is shown below.

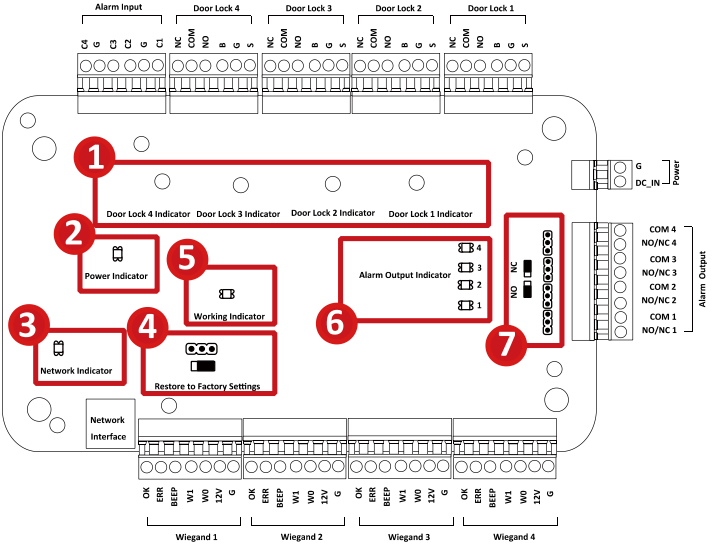


Figure 2-1 DS-K2804 Component Schematic Diagram

Table 2-1 DS-K2800 Component Description

No.	Component Description		
	DS-K2801	**DS-K2802**	**DS-K2804**
1	Door Lock 1 Indicator	Door Lock 1/2 Indicator	Door Lock 1/2/3/4 Indicator
2	Power Indicator		
3	Network Indicator		

No.	**Component Description**
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 DS-K2801Terminal Description

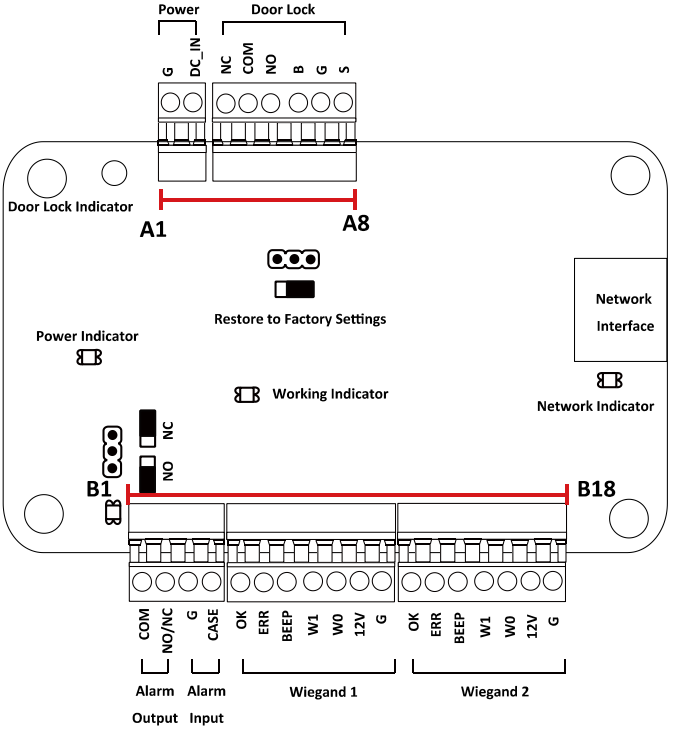


Figure 3-1 DS-K2801 Terminals

Table 3-1 DS-K2801 Terminal Description

No.	DS-K2801		
A1	Power	GND	DC12V Grounding
A2		+12V	DC12V Input
A3	Door	NC	Door Lock Relay Output
A4		COM	
A5		NO	
A6		BUTTON	Door Button Input
A7		GND	Grounding
A8		SENSOR	Door Magnetic detector
B1	Alarm Output	COM	Alarm Relay Output (Dry Contact)
B2		NO/NC	
B3	Alarm Input	GND	Grounding
B4		IN	Alarm Input
B5	Wiegand Card Reader 1	OK	Indicator of Card Reader Control Output (Valid Card Output)
B6		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
B7		BZ	Card Reader Buzzer Control Output
B8		W1	Wiegand Head Read Data Input Data1
B9		W0	Wiegand Head Read Data Input Data0
B10		PWR	Card Reader Power Output
B11		GND	
B12	Wiegand Card Reader 2	OK	Indicator of Card Reader Control Output (Valid Card Output)
B13		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
B14		BZ	Card Reader Buzzer Control Output
B15		W1	Wiegand Head Read Data Input Data1

No.	DS-K2801		
B16		W0	Wiegand Head Read Data Input Data0
B17		PWR	Card Reader Power Output
B18		GND	

3.2 DS-K2802Terminal Description

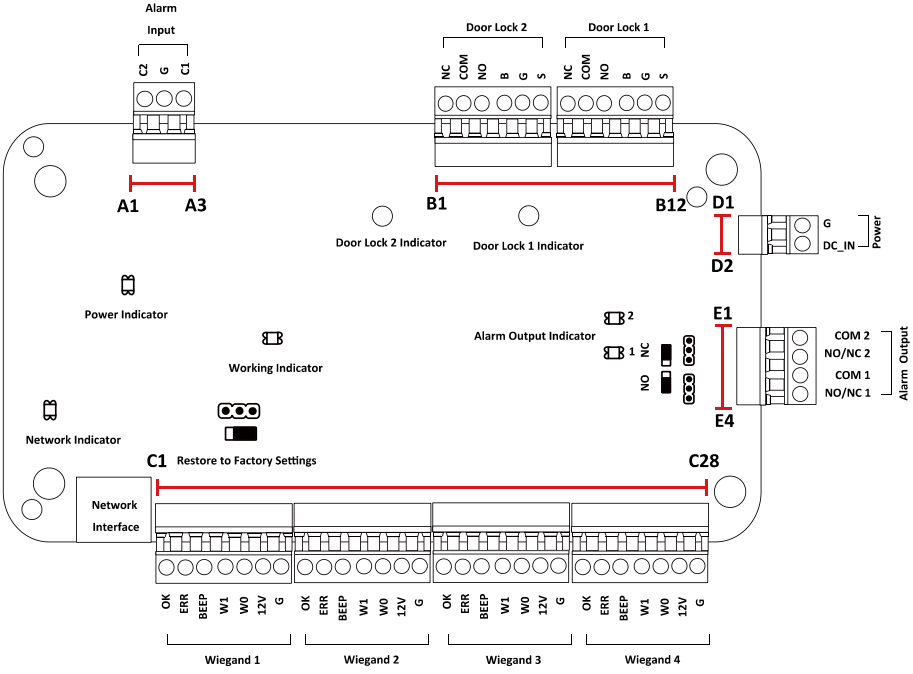


Figure 3-2 DS-K2802 Terminal Description

Table 3-2 DS-K2802 Port Description

No.	DS-K2802		
A1	Alarm Input	IN2	Alarm Input 2
A2		GND	Grounding

No.	DS-K2802		
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		NO/NC2	
E3	Alarm Output 1	COM1	Alarm Relay Output 1 (Dry Contact)
E4		NO/NC1	
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

No.	DS-K2802		
			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		OK	Indicator of Card Reader Control Output (Valid Card Output)
C16		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
C17	Wiegand Card Reader 3	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		GND	
C22		OK	Indicator of Card Reader Control Output (Valid Card Output)
C23		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
C24	Wiegand Card Reader 4	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		GND	

3.3 DS-K2804 Terminal Description

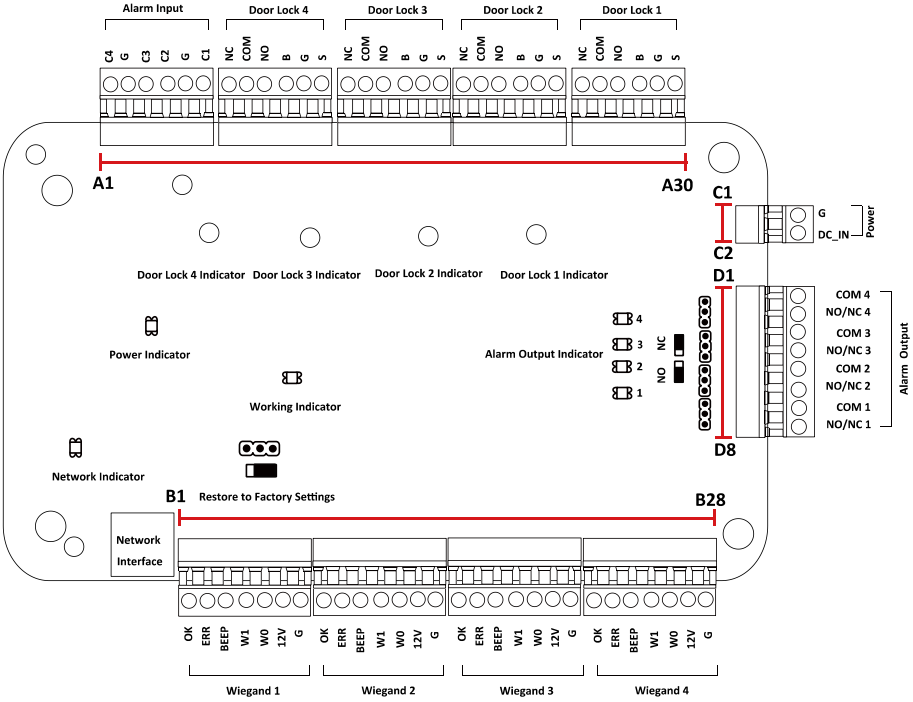


Figure 3-3 DS-K2804 Access Controller Terminals

Table 3-3 DS-K2804 Port Description

No.	DS-K2804		
A1	Alarm Input	IN4	Alarm Input 4
A2		GND	Grounding
A3		IN3	Alarm Input 3
A4		IN2	Alarm Input 2
A5		GND	Grounding
A6		IN1	Alarm Input 1

No.	DS-K2804		
A7	Door 4	NC	Door Lock Relay Output (Dry Contact)
A8		COM	
A9		NO	
A10		BUTTON	Door Button Input
A11		GND	Grounding
A12		SENSOR	Door Magnetic detector
A13	Door 3	NC	Door Lock Relay Output (Dry Contact)
A14		COM	
A15		NO	
A16		BUTTON	Door Button Input
A17		GND	Grounding
A18		SENSOR	Door Magnetic detector
A19	Door 2	NC	Door Lock Relay Output (Dry Contact)
A20		COM	
A21		NO	
A22		BUTTON	Door Button Input
A23		GND	Grounding
A24		SENSOR	Door Magnetic detector
A25	Door 1	NC	Door Lock Relay Output (Dry Contact)
A26		COM	
A27		NO	
A28		BUTTON	Door Button Input
A29		GND	Grounding
A30		SENSOR	Door Magnetic detector
B1	Wiegand Card Reader 1	OK	Indicator of Card Reader Control Output (Valid Card Output)
B2		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
B3		BZ	Card Reader Buzzer Control Output

No.	DS-K2804		
B4		W1	Wiegand Head Read Data Input Data1
B5		W0	Wiegand Head Read Data Input Data0
B6		PWR	Card Reader Power Output
B7		GND	
B8	Wiegand Card Reader 2	OK	Indicator of Card Reader Control Output (Valid Card Output)
B9		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
B10		BZ	Card Reader Buzzer Control Output
B11		W1	Wiegand Head Read Data Input Data1
B12		W0	Wiegand Head Read Data Input Data0
B13		PWR	Card Reader Power Output
B14		GND	
B15	Wiegand Card Reader 3	OK	Indicator of Card Reader Control Output (Valid Card Output)
B16		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
B17		BZ	Card Reader Buzzer Control Output
B18		W1	Wiegand Head Read Data Input Data1
B19		W0	Wiegand Head Read Data Input Data0
B20		PWR	Card Reader Power Output
B21		GND	
B22	Wiegand Card Reader 4	OK	Indicator of Card Reader Control Output (Valid Card Output)
B23		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
B24		BZ	Card Reader Buzzer Control Output
B25		W1	Wiegand Head Read Data Input Data1
B26		W0	Wiegand Head Read Data Input Data0

No.	DS-K2804		
B27		PWR	Card Reader Power Output
B28		GND	
C1	Power	GND	DC12V Grounding
C2		+12V	DC12V Input
D1	Alarm Output 4	COM4	Alarm Relay Output 4 (Dry Contact)
D2		NO/NC4	
D3	Alarm Output 3	COM3	Alarm Relay Output 3 (Dry Contact)
D4		NO/NC3	
D5	Alarm Output 2	COM2	Alarm Relay Output 2 (Dry Contact)
D6		NO/NC2	
D7	Alarm Output 1	COM1	Alarm Relay Output 1 (Dry Contact)
D8		NO/NC1	

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

Chapter 4 External Device Wiring

4.1 Card Reader Wiring

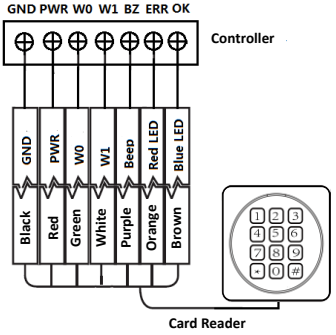


Figure 4-1 Wiring diagram of Wiegand card reader

Note:

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

For 1800 series card reader, the wiring diagram is shown below.

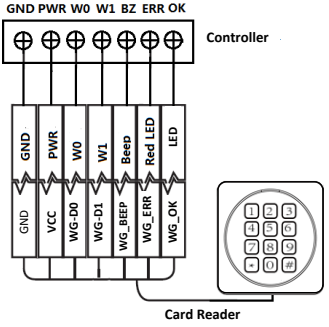


Figure 4-2 Wiring diagram of 1800 series card reader

4.2 Installing Door Lock

4.2.1 Installation of Cathode Lock

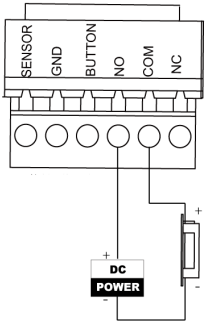


Figure 4-3 Wiring diagram of cathode lock

4.2.2 Installation of Anode Lock

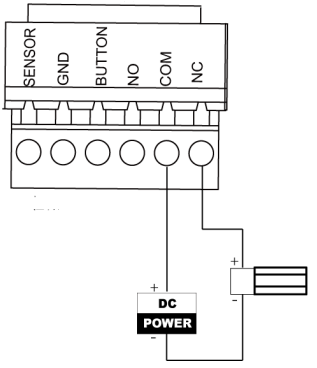


Figure 4-4 Wiring diagram of anode lock

4.3 Connecting the External Alarm Device

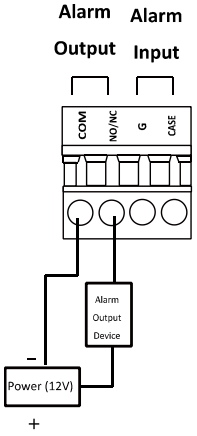


Figure 4-5 External Alarm Device Connection

4.4 Door Button Wiring Diagram

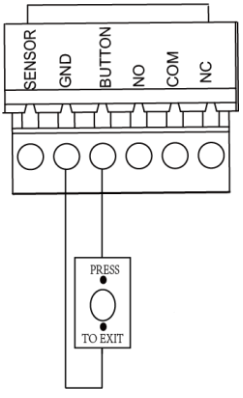


Figure 4-6 Power Button Connection

4.5 The Connection of Magnetics Detection

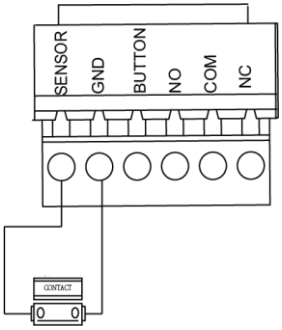


Figure 4-7 Magnetics Connection

4.6 Connecting Power Supply

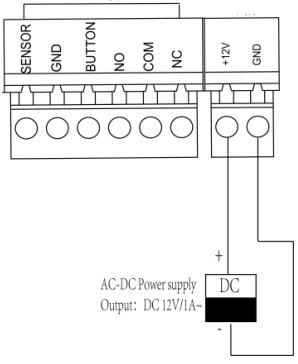


Figure 4-8 Power Supply Connection

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.

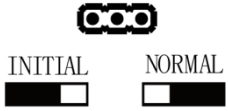


Figure 5-1 Initialization Dial-up

Note*:*

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

5.2 Relay Input NO/NC

5.2.1 Lock Relay Output

Lock Relay Normally Open Status

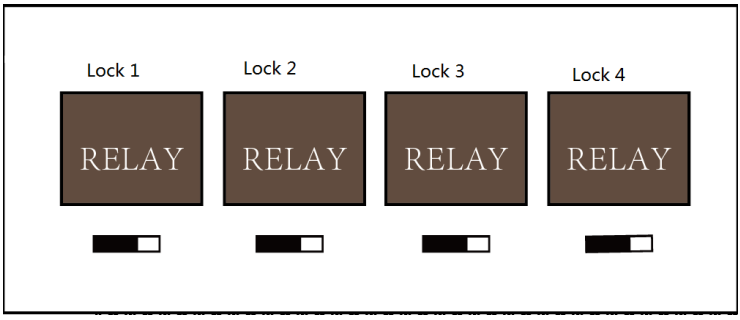


Figure 5-2 Normally Open Status

Lock Relay Normally Closed Status

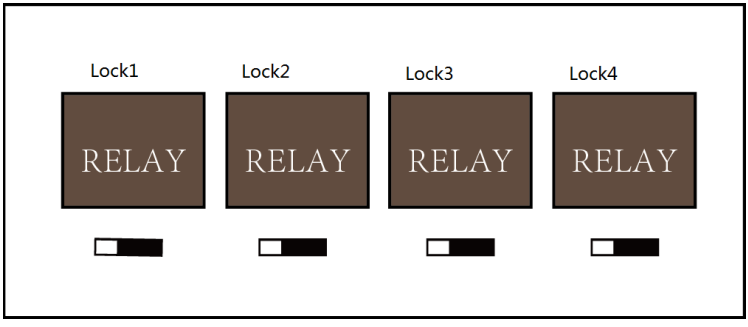


Figure 5-3 Normally Closed Status

5.2.2 Alarm Relay Output Status

Alarm Relay Output Normally Open

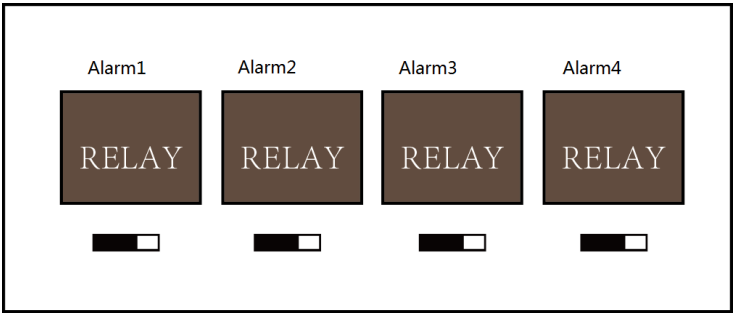


Figure 5-4 Alarm Relay Output Normally Open

Alarm Relay Output Normally Closed

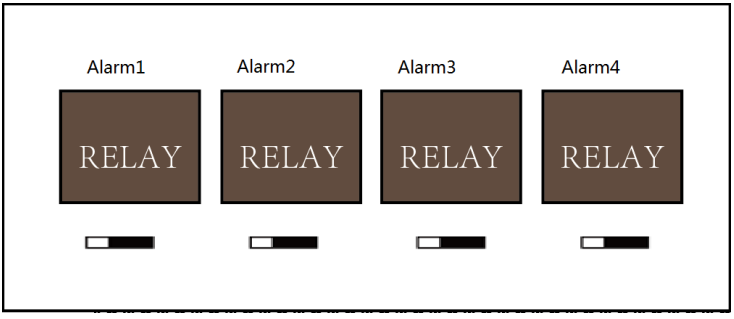


Figure 5-5 Normally Closed Status

Work Flow of Software

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

Refer to the following work flow:

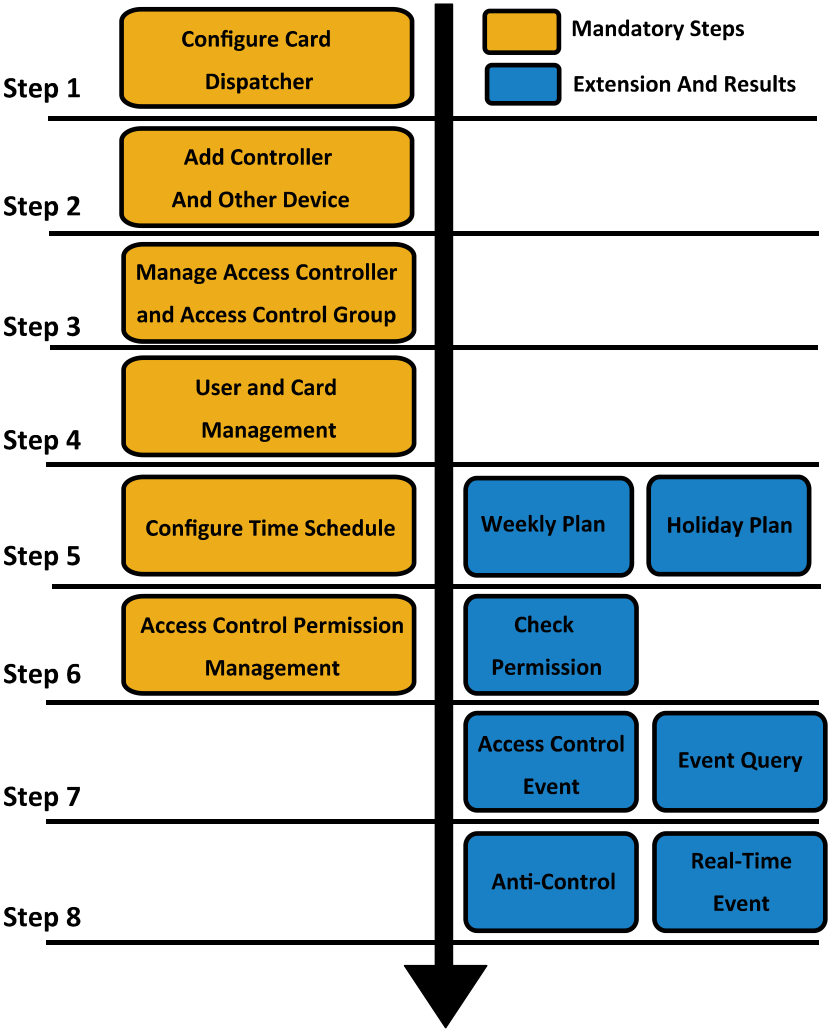


Figure 5-6 Software Client Work Flow

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.

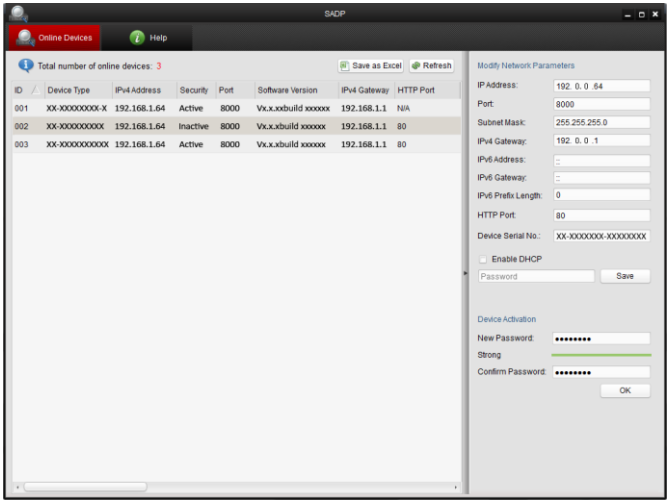
6.1 Activation via SADP Software

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.



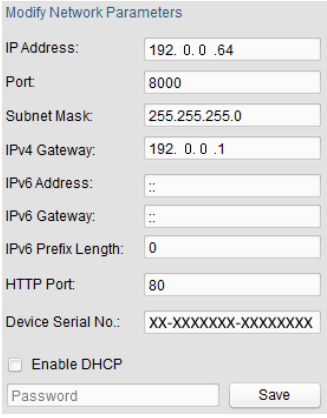
3. Create a password and input the password in the password field, and confirm the password.

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 popup 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.



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.

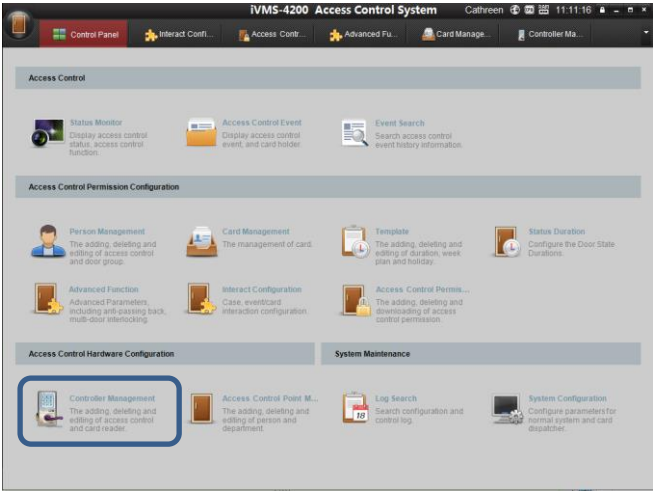
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

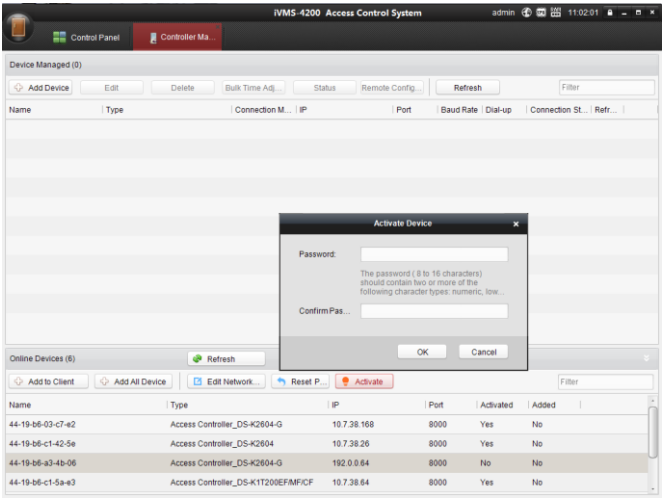
1. Run the client software and the control panel of the software pops up, as

shown in the figure below.

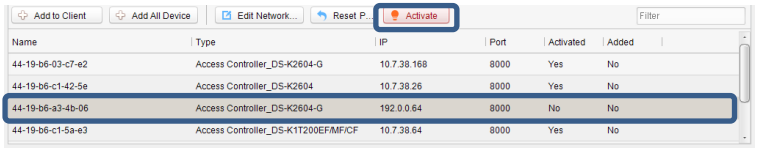
2. Click the  icon on the upper-left side of the page, select **Access Control** to enter the control panel.



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.

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 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.

First Choice for Security Professionals