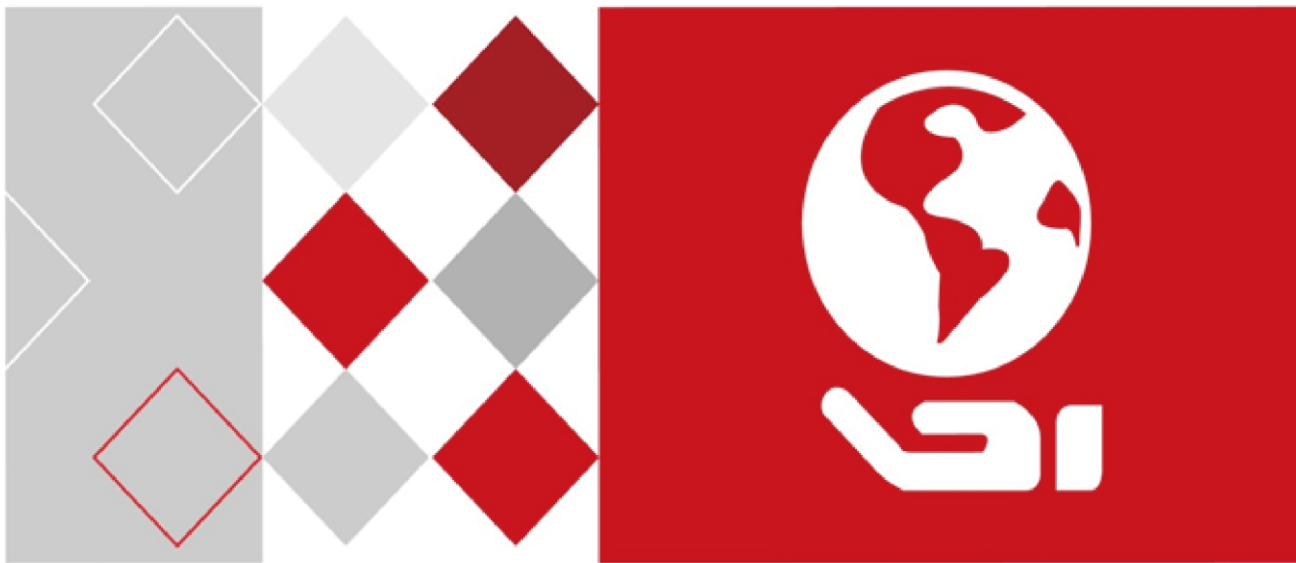


**HIKVISION**



# DS-K2800 Series Access Controller

User Manual

## User Manual

©2017 Hangzhou Hikvision Digital Technology Co., Ltd.

This manual is applied for access controller.

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

It includes instructions on how to use the Product. The software embodied in the Product is governed by the user license agreement covering that Product.

## About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. (“Hikvision”) reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

## Trademarks

**HIKVISION** and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

## Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY 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, OUR COMPANY 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. OUR COMPANY 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.

## Support

Should you have any questions, please do not hesitate to contact your local dealer.

## 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.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 Instruction**

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into **Warnings** and **Cautions**:

**Warnings:** Neglecting any of the warnings may cause serious injury or death.

**Cautions:** Neglecting any of the cautions may cause injury or equipment damage.

	
<b>Warnings</b> Follow these safeguards to prevent serious injury or death.	<b>Cautions</b> Follow these precautions to prevent potential injury or material damage.



**Warnings**

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



**Cautions**

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation. The appropriate operation temperature is 0°C to +45°C, and the storage temperature should be -10°C to +55°C.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.

- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- 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 battery manufacturer.

## Table of Contents

<b>Chapter 1</b>	<b>Product Description</b> .....	<b>1</b>
1.1	Overview .....	1
1.2	Main Features .....	1
<b>Chapter 2</b>	<b>Component Description</b> .....	<b>2</b>
<b>Chapter 3</b>	<b>Terminal Connection</b> .....	<b>3</b>
3.1	DS-K2801 Terminal Description.....	3
3.2	DS-K2802 Terminal Description.....	5
3.3	DS-K2804 Terminal Description.....	7
<b>Chapter 4</b>	<b>External Device Wiring</b> .....	<b>10</b>
4.1	Card Reader Wiring .....	10
4.1.1	Wiegand Card Reader Wiring .....	10
4.1.2	DS-K1800 Series Card Reader Wiring.....	10
4.2	DS-K2801 External Terminals .....	10
4.2.1	Installation of Cathode Lock.....	11
4.2.2	Installation of Anode Lock.....	11
4.3	Connecting the External Alarm Device .....	12
4.4	Door Button Wiring Diagram .....	12
4.5	The Connection of Magnetics Detection .....	13
4.6	Connecting Power Supply .....	13
<b>Chapter 5</b>	<b>Settings</b> .....	<b>14</b>
5.1	Initializing the Hardware .....	14
5.2	Relay Input NO/NC .....	14
5.2.1	Lock Relay Output .....	14
5.2.2	Alarm Relay Output Status .....	15
<b>Chapter 6</b>	<b>Activating the Access Control Terminal</b> .....	<b>17</b>
6.1	Activating via SADP Software .....	17
6.2	Activating via Client Software .....	18
<b>Chapter 7</b>	<b>Client Operation</b> .....	<b>21</b>
7.1	Function Module .....	21
7.2	User Registration and Login .....	24
7.3	System Configuration .....	25
7.4	Access Control Management .....	26
7.4.1	Adding Access Control Device .....	27
7.4.2	Viewing Device Status.....	41

7.4.3	Editing Basic Information .....	42
7.4.4	Network Settings .....	43
7.4.5	Capture Settings .....	45
7.4.6	RS-485 Settings .....	46
7.4.7	Wiegand Settings .....	47
7.4.8	M1 Card Encryption .....	47
7.4.9	Remote Configuration .....	48
7.5	Person and Card Management .....	55
7.5.1	Organization Management .....	56
7.5.2	Person Management .....	57
7.6	Schedule and Template .....	66
7.6.1	Week Schedule .....	67
7.6.2	Holiday Group .....	68
7.6.3	Template .....	69
7.7	Permission Configuration .....	71
7.7.1	Adding Permission .....	72
7.7.2	Applying Permission .....	73
7.8	Advanced Functions .....	73
7.8.1	Access Control Parameters .....	74
7.8.2	Card Reader Authentication .....	76
7.8.3	Multiple Authentication .....	78
7.8.4	Open Door with First Card .....	81
7.8.5	Anti-Passing Back .....	82
7.8.6	Cross-Controller Anti-passing Back .....	83
7.8.7	Multi-door Interlocking .....	86
7.8.8	Authentication Password .....	87
7.8.9	Custom Wiegand .....	88
7.9	Searching Access Control Event .....	90
7.10	Access Control Event Configuration .....	91
7.10.1	Access Control Event Linkage .....	91
7.10.2	Access Control Alarm Input Linkage .....	93
7.10.3	Event Card Linkage .....	93
7.10.4	Cross-Device Linkage .....	95
7.11	Door Status Management .....	97
7.11.1	Access Control Group Management .....	97
7.11.2	Anti-control the Access Control Point (Door) .....	98



7.11.3	Status Duration Configuration .....	100
7.11.4	Real-time Card Swiping Record .....	101
7.11.5	Real-time Access Control Alarm .....	102
7.12	Arming Control .....	103
<b>Appendix A Sound Prompt and Indicator .....</b>		<b>105</b>
<b>Appendix B Custom Wiegand Rule Descriptions.....</b>		<b>106</b>

# Chapter 1 Product Description

## 1.1 Overview

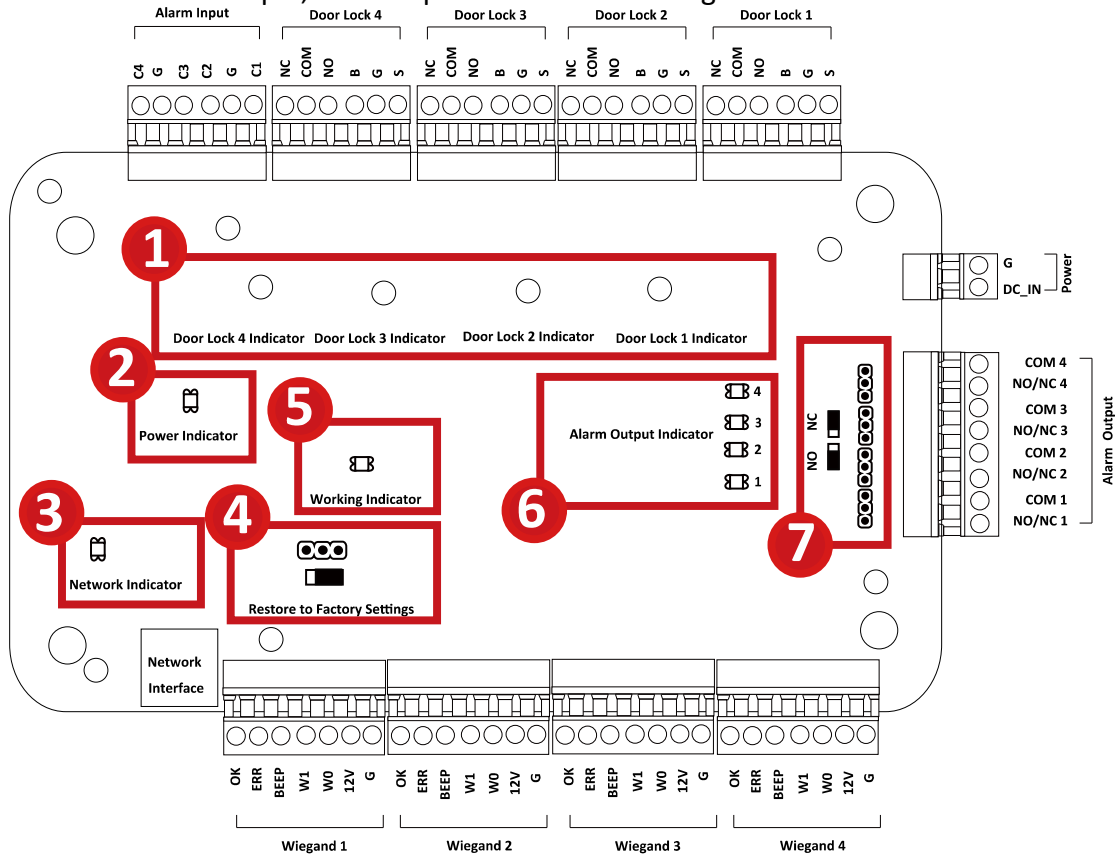
DS-K2800 is a powerful and stable access controller, using the logical architecture design. DS-K2800 is designed with TCP/IP network interface and its signal processed with special encryption and can be run offline. Anti-tampering function is also supported.

## 1.2 Main Features

- 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-door and first card authorization 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.
- 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%
- Multiple event upload methods: channel, center group, and listening
- 500 groups of authentication code
- Anti-pass-back function.

# Chapter 2 Component Description

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

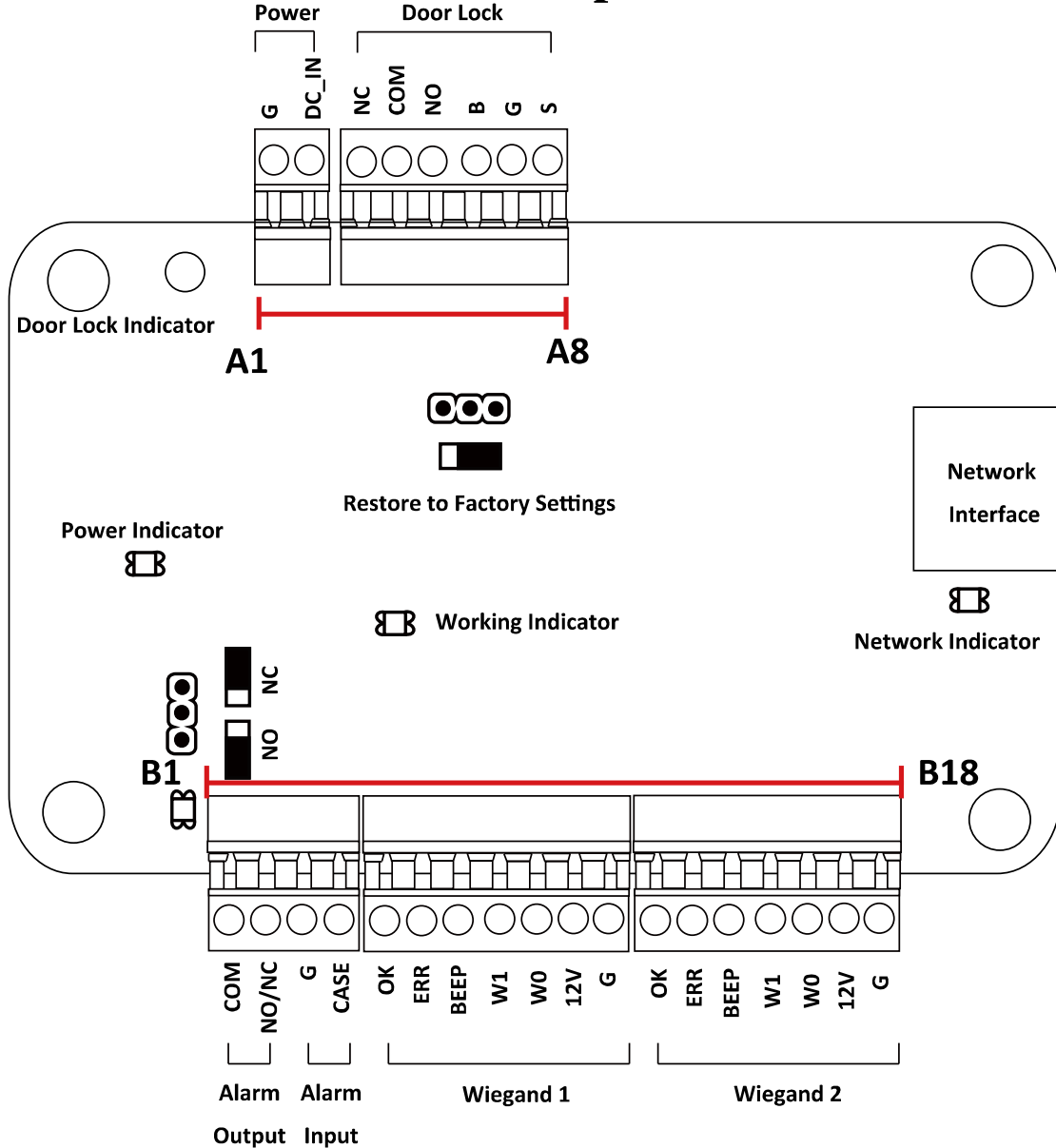


DS-K2800 component descriptions are as follows:

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		
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-K2801 Terminal Description

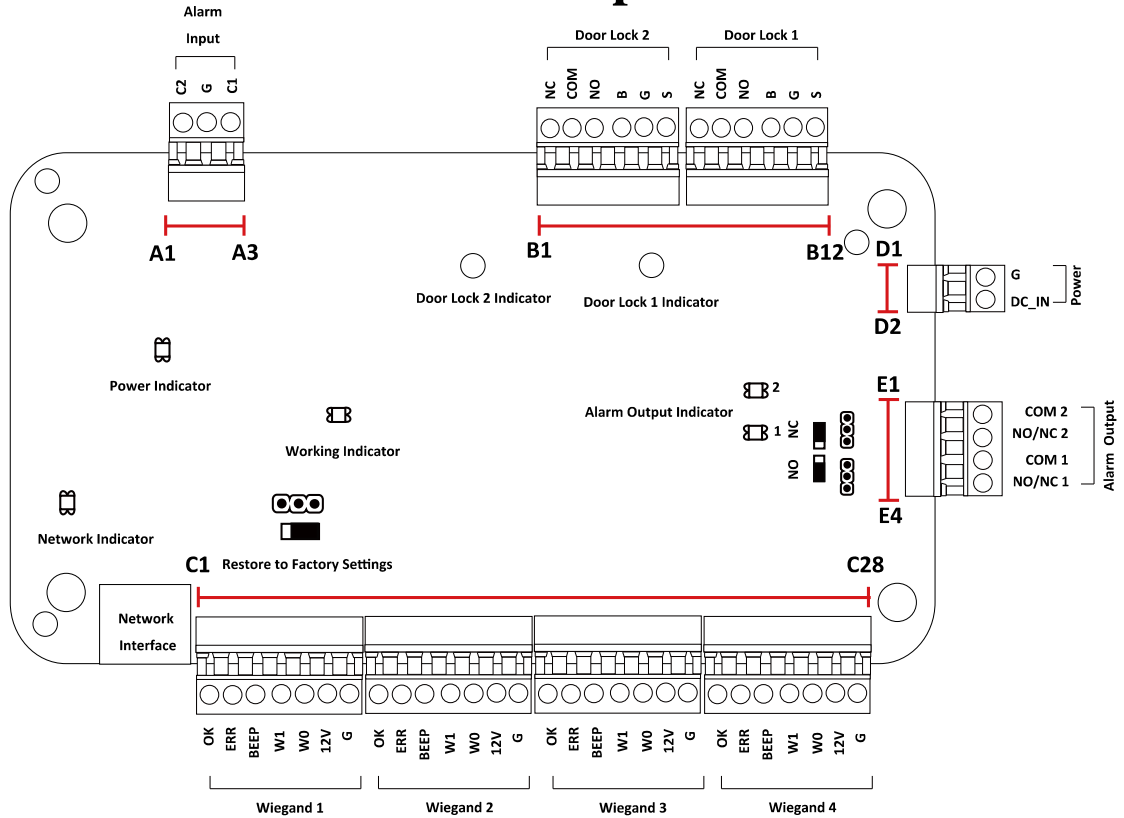


DS-K2801 Terminal descriptions are as follows:

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

No.	DS-K2801		
A8		SENSOR	Door Magnetic detector
B1	Alarm Output	COM	Alarm Relay Output (Dry Contact)
B2		NO/NC	
B3	Alarm Input	GND	Grounding
B4		IN	Event 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
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
B16	W0		Wiegand Head Read Data Input Data0
B17	PWR		Card Reader Power Output
B18	GND		

### 3.2 DS-K2802 Terminal Description

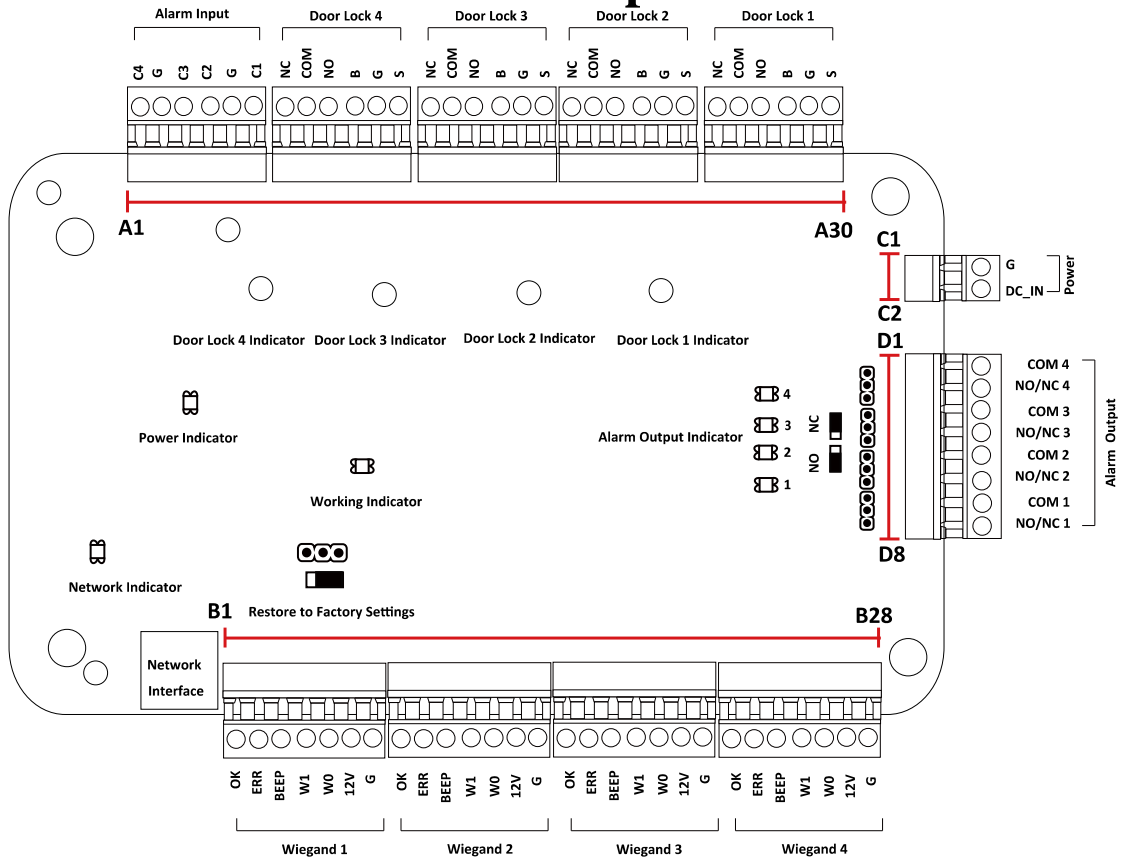


DS-K2802 Terminal descriptions are as follows:

No.	DS-K2802		
A1	Alarm Input	IN2	Event Input 2
A2		GND	Grounding
A3		IN1	Event 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	

No.	DS-K2802		
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 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		GND	
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		GND	

### 3.3 DS-K2804 Terminal Description



DS-K2804 Terminal descriptions are as follows:

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



No.	DS-K2804		
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
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)

No.	DS-K2804		
B24		BZ	Card Reader Buzzer Control Output
B25		W1	Wiegand Head Read Data Input Data1
B26		W0	Wiegand Head Read Data Input Data0
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	

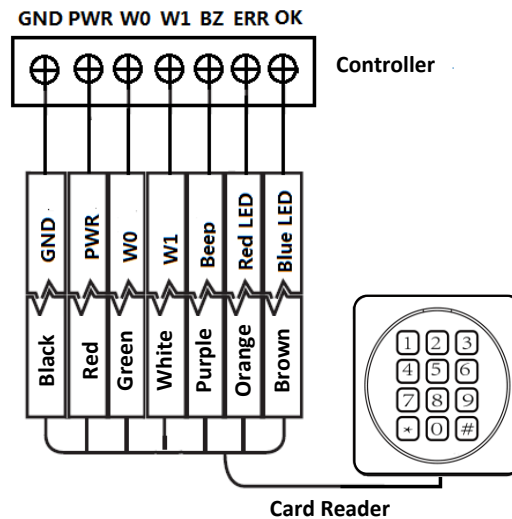
**Notes:**

- 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

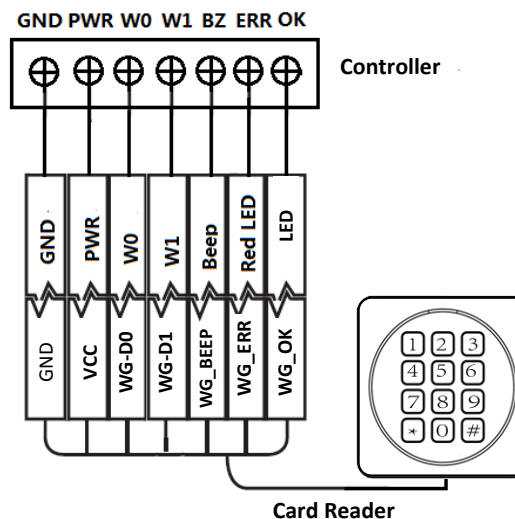
## 4.1 Card Reader Wiring

### 4.1.1 Wiegand Card Reader Wiring



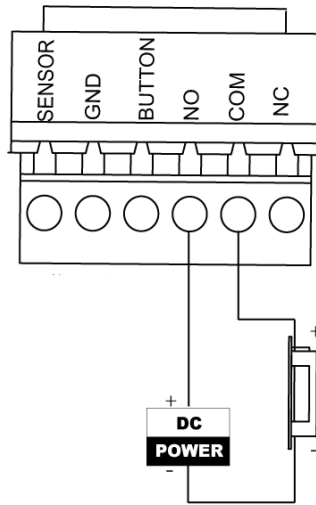
**Note:** You must connect the OK/ERR/BZ, if using access controller to control the LED and buzzer of the Wiegand card reader.

### 4.1.2 DS-K1800 Series Card Reader Wiring

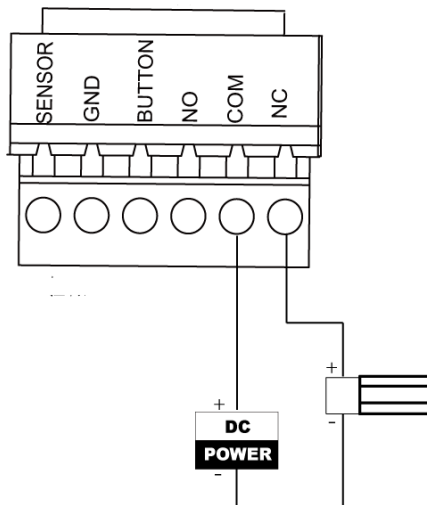


## 4.2 DS-K2801 External Terminals

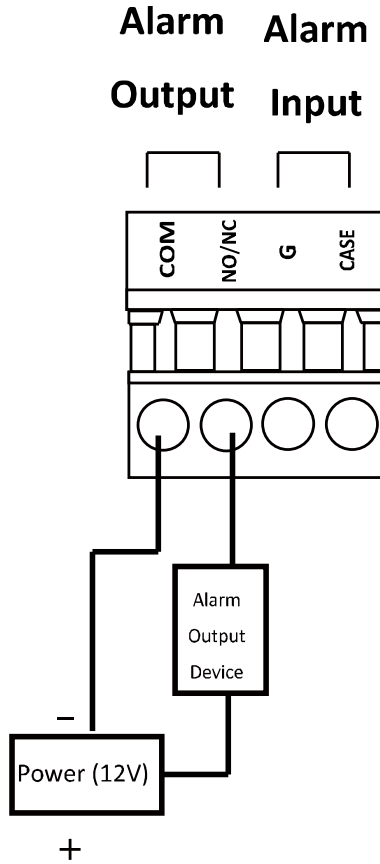
### 4.2.1 Installation of Cathode Lock



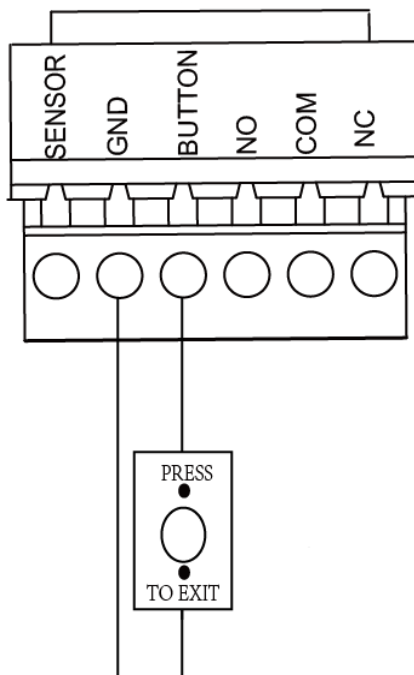
### 4.2.2 Installation of Anode Lock



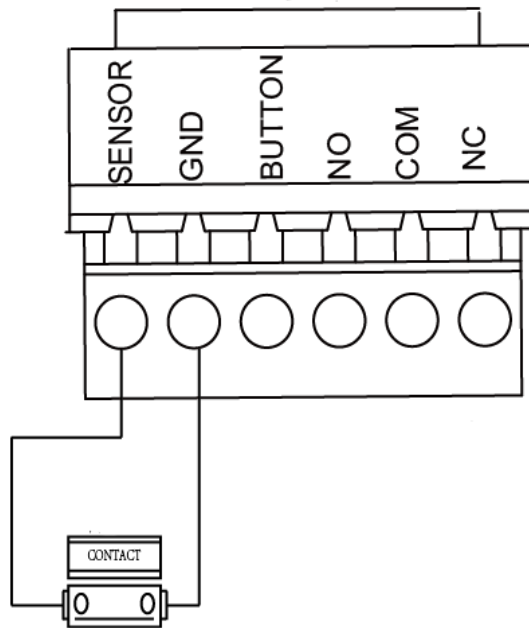
### 4.3 Connecting the External Alarm Device



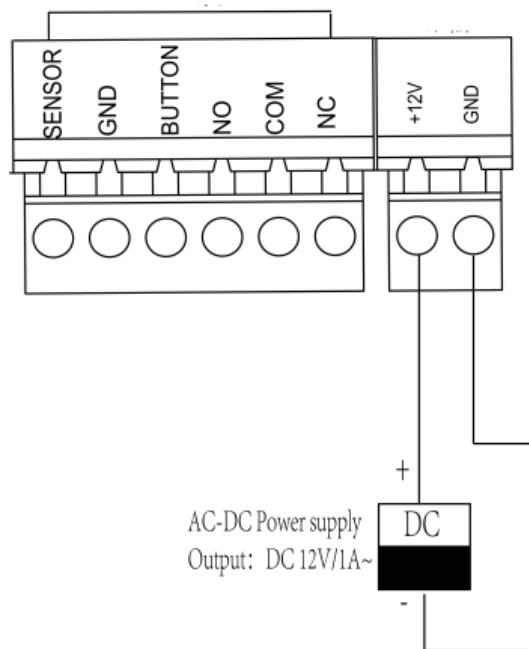
### 4.4 Door Button Wiring Diagram



## 4.5 The Connection of Magnetics Detection



## 4.6 Connecting Power Supply



# Chapter 5 Settings

## 5.1 Initializing the Hardware

**Option 1:**

**Steps:**

1. Remove the jumper cap from the Normal terminal.
2. Disconnect the power and restart the access controller. The controller buzzer buzzes a long beep.
3. When the beep stopped, plug the jumper cap back to Normal.

**Option 2:**

**Steps:**

1. Jump the jumper cap from Normal to Initial.
2. Disconnect the power and restart the access controller. The controller buzzer buzzes a long beep.
3. When the beep stopped, jump the jumper cap back to Normal.

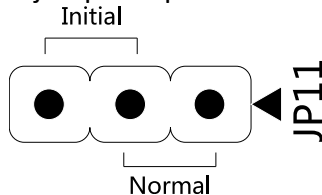


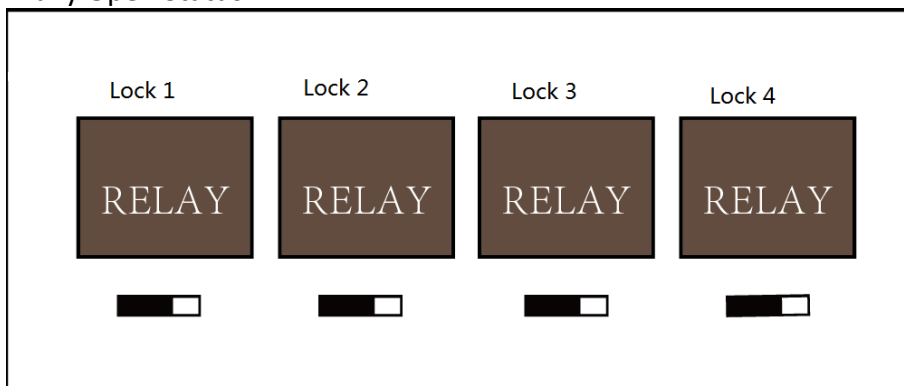
Figure 1-1 Initialization Dial-up

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

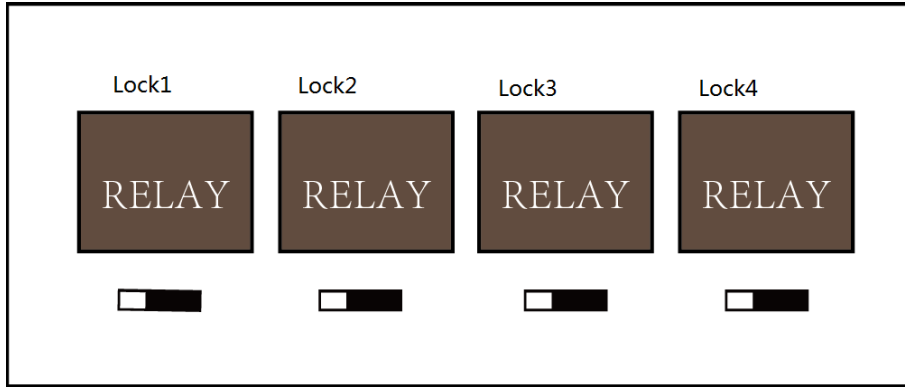
## 5.2 Relay Input NO/NC

### 5.2.1 Lock Relay Output

Lock Relay Normally Open Status:

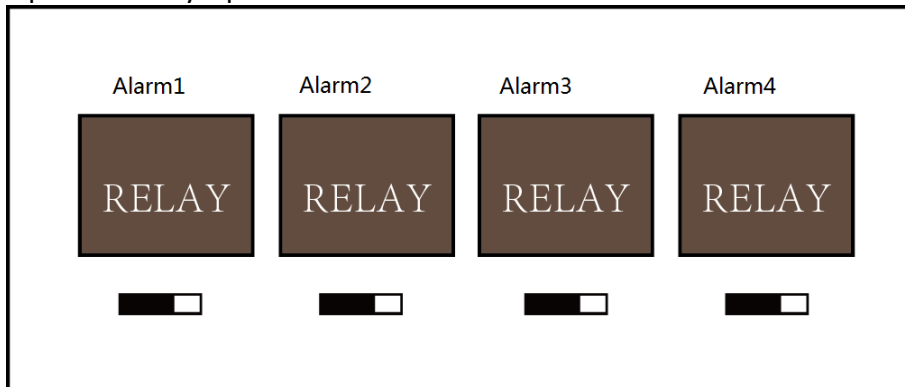


Lock Relay Normally Closed Status:

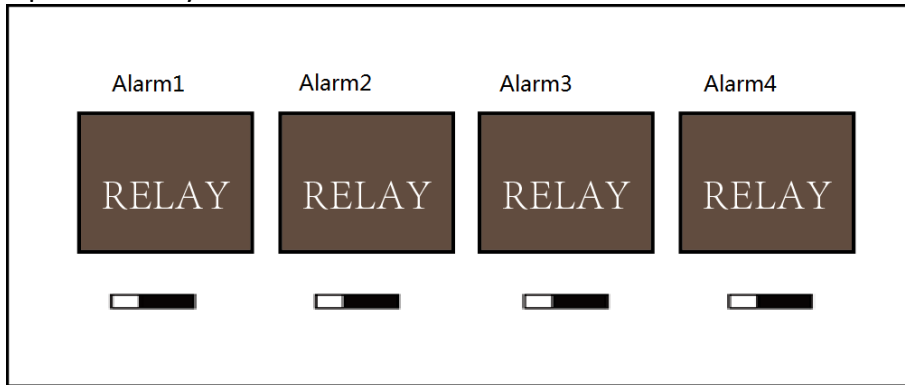


### 5.2.2 Alarm Relay Output Status

Alarm Relay Output Normally Open:



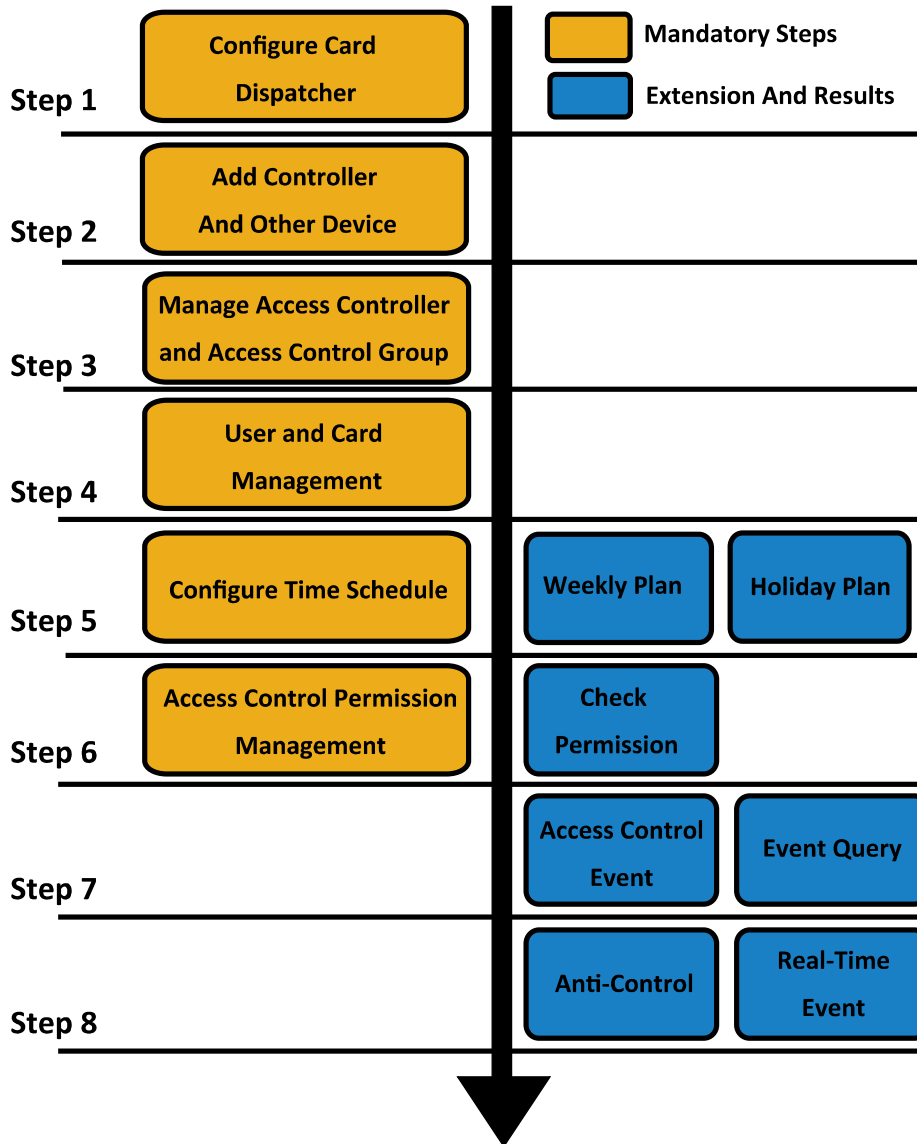
Alarm Relay Output Normally Closed:



### Work Flow of Software

For detailed information, please see the user manual of the client software.  
Refer to the following work flow:





# Chapter 6 Activating the Access Control Terminal

**Purpose:**

You are required to activate the terminal first before using it. Activation via SADP, and Activation via client software are supported. The default values of the control terminal are as follows.

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

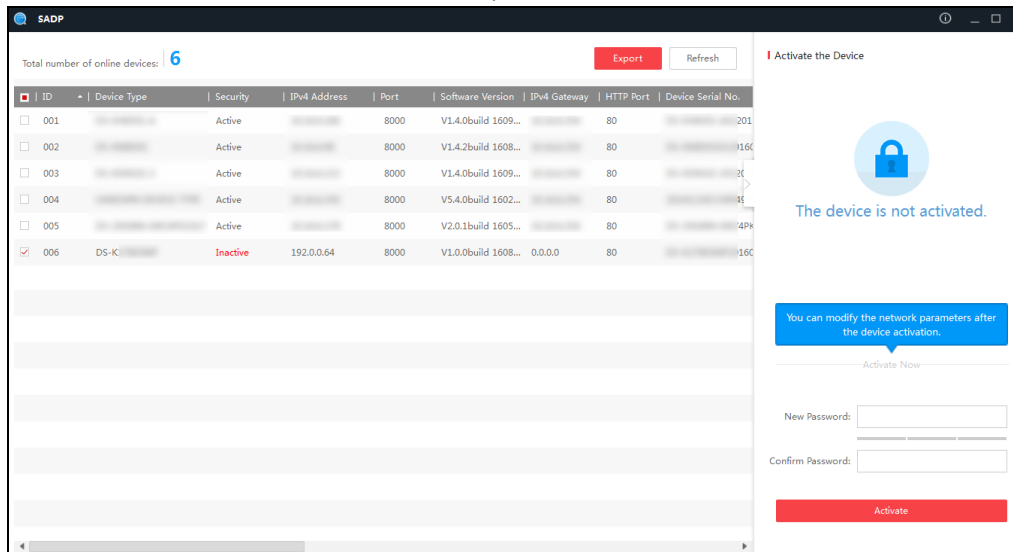
## 6.1 Activating via SADP Software

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 **Activate** to activate the device.
5. Check the activated device. You can change the device IP address to the same network

segment with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

Modify Network Parameters

Enable DHCP

Device Serial No.:

IP Address:

Port:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port:

Security Verification

Admin Password:

[Forgot Password](#)

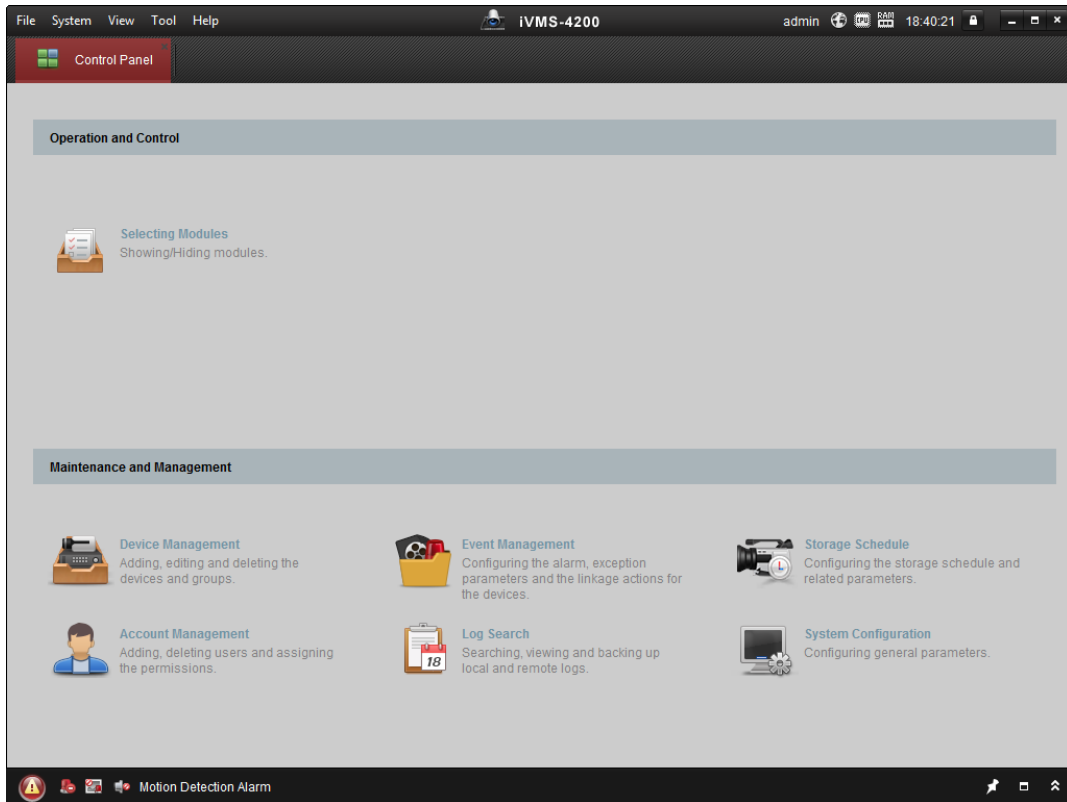
6. Input the password and click the **Modify** button to activate your IP address modification.

## 6.2 Activating 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 **Device Management** to enter the Device Management interface.
3. Check the device status from the device list, and select an inactive device.

IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Time
192.0.0.64			Active	8000		2017-01
192.168.1.64			Inactive	8000		2017-01

4. Click the **Activate** button to pop up the Activation interface.
5. In the pop-up window, create a 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.



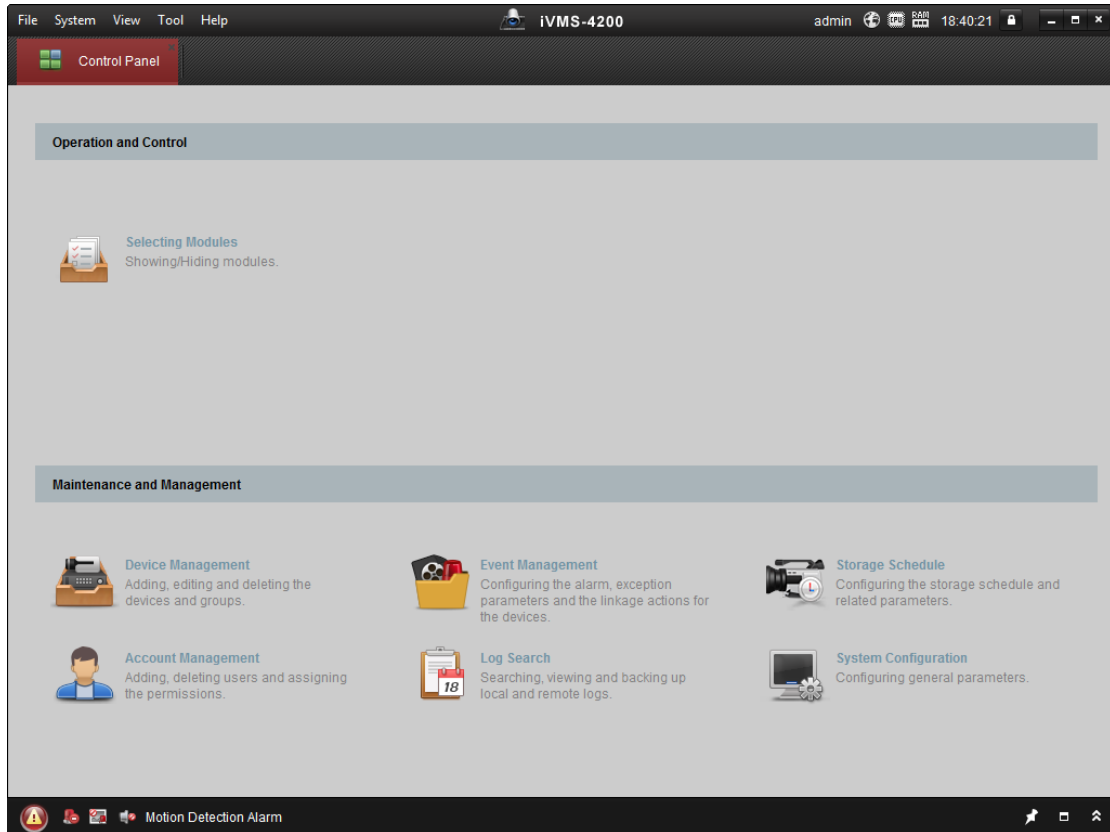
6. Click **OK** button to start activation.
7. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.
8. Change the device IP address to the same network segment with your computer by either modifying the IP address manually.
9. Input the password and click the **OK** button to save the settings.

# Chapter 7 Client Operation

You can set and operate the access control devices via the client software. This chapter will introduce the access control device related operations in the client software. For integrated operations, refer to *User Manual of iVMS-4200 Client Software*.

## 7.1 Function Module

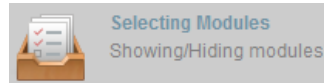
### Control Panel of iVMS-4200:



### Menu Bar:

<b>File</b>	<b>Open Image File</b>	Search and view the captured pictures stored on local PC.
	<b>Open Video File</b>	Search and view the video files recorded on local PC.
	<b>Open Log File</b>	View the backup log files.
	<b>Exit</b>	Exit the iVMS-4200 client software.
<b>System</b>	<b>Lock</b>	Lock screen operations. Log in the client again to unlock.
	<b>Switch User</b>	Switch the login user.
	<b>Import System Config File</b>	Import client configuration file from your computer.
	<b>Export System Config File</b>	Export client configuration file to your computer.
	<b>Auto Backup</b>	Set the schedule for backing up the database including person, attendance data, and permission data automatically.

View	<b>1024*768</b>	Display the window at size of 1024*768 pixels.
	<b>1280*1024</b>	Display the window at size of 1280*1024 pixels.
	<b>1440*900</b>	Display the window at size of 1440*900 pixels.
	<b>1680*1050</b>	Display the window at size of 1680*1050 pixels.
	<b>Maximize</b>	Display the window in maximum mode.
	<b>Control Panel</b>	Enter Control Panel interface.
	<b>Main View</b>	Open Main View page.
	<b>Remote Playback</b>	Open Remote Playback page.
	<b>Access Control</b>	Enter the Access Control Module.
	<b>Status Monitor</b>	Enter the Status Monitor Module.
	<b>Time and Attendance</b>	Enter the Time and Attendance Module.
	<b>Security Control Panel</b>	Enter the Security Control Panel Module.
	<b>Real-time Alarm</b>	Enter the Real-time Alarm Module.
	<b>Video Wall</b>	Open Video Wall page.
	<b>E-map</b>	Open E-map page.
<b>Auxiliary Screen Preview</b>	Open Auxiliary Screen Preview window.	
Tool	<b>Device Management</b>	Open the Device Management page.
	<b>Event Management</b>	Open the Event Management page.
	<b>Storage Schedule</b>	Open the Storage Schedule page.
	<b>Account Management</b>	Open the Account Management page.
	<b>Log Search</b>	Open the Log Search page.
	<b>System Configuration</b>	Open the System Configuration page.
	<b>Broadcast</b>	Select camera to start broadcasting.
	<b>Device Arming Control</b>	Set the arming status of devices.
	<b>Alarm Output Control</b>	Turn on/off the alarm output.
	<b>Batch Wiper Control</b>	Batch starting or stopping the wipers of the devices.
	<b>Batch Time Sync</b>	Batch time synchronization of the devices.
	<b>Player</b>	Open the player to play the video files.
<b>Message Queue</b>	Display the information of Email message to be sent.	
Help	<b>Open Video Wizard</b>	Open the video guide for the video surveillance configuration.
	<b>Open Video Wall Wizard</b>	Open the guide for the video wall configuration.
	<b>Open Security Control Panel Wizard</b>	Open the guide for the security control panel configuration.
	<b>Open Access Control and Video Intercom Wizard</b>	Open the guide for the access control and video intercom configuration.
	<b>Open Attendance Wizard</b>	Open the guide for the time and attendance configuration.
	<b>User Manual (F1)</b>	Click to open the User Manual; you can also open the User Manual by pressing <b>F1</b> on your keyboard.
	<b>About</b>	View the basic information of the client software.
<b>Language</b>	Select the language for the client software and reboot the software to activate the settings.	

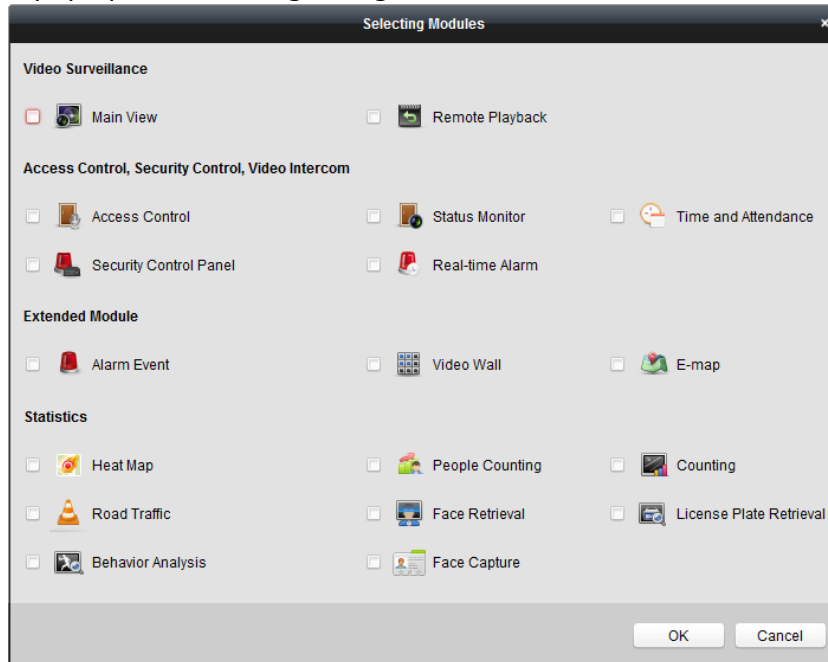


For the first time running the software, you can click on the control panel to select the modules to display on the Operation and Control area of the control pane.

**Steps:**



1. Click to pop up the following dialog.



2. Check the module checkboxes to display them on the control panel according to the actual needs.
3. Click **OK** to save the settings.













**Notes:**

- After adding the access control device in Device Management module, the Access Control, Status, and Time and Attendance module will be displayed on the control panel automatically.
- After adding the security control panel in Device Management module, the Security Control Panel and Real-time Alarm modules will be displayed on the control panel automatically.

The iVMS-4200 client software is composed of the following function modules:

	The Main View module provides live view of network cameras and video encoders, and supports some basic operations, such as picture capturing, recording, PTZ control, etc.
	The Remote Playback module provides the search, playback, export of video files.
	The Access Control module provides managing the organizations, persons, permissions, and advanced access control functions. Provides video intercom function.
	The Status Monitor module provides monitoring and controlling the door status, viewing the real-time card swiping records and access control events.



	The Time and Attendance module provides setting the attendance rule for the employees and generating the reports.
	The Security Control Panel module provides operations such as arming, disarming, bypass, group bypass, and so on for both the partitions and zones.
	The Real-time Alarm module provides displaying the real-time alarm of security control panel, acknowledging alarms, and searching the history alarms.
	The Alarm Event module displays the alarm and event received by the client software.
	The Video Wall module provides the management of decoding device and video wall and the function of displaying the decoded video on video wall.
	The E-map module provides the displaying and management of E-maps, alarm inputs, hot regions and hot spots.
	The Device Management module provides the adding, modifying and deleting of different devices and the devices can be imported into groups for management.
	The Event Management module provides the settings of arming schedule, alarm linkage actions and other parameters for different events.
	The Storage Schedule module provides the schedule settings for recording and pictures.
	The Account Management module provides the adding, modifying and deleting of user accounts and different permissions can be assigned for different users.
	The Log Search module provides the query of system log files and the log files can be filtered by different types.
	The System Configuration module provides the configuration of general parameters, file saving paths, alarm sounds and other system settings.

The function modules are easily accessed by clicking the navigation buttons on the control panel or by selecting the function module from the **View** or **Tool** menu.

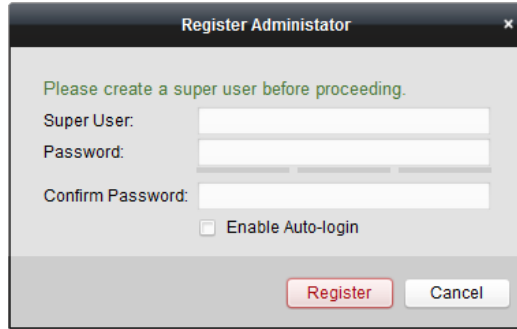
You can check the information, including current user, network usage, CPU usage, memory usage and time, in the upper-right corner of the main page.

## 7.2 User Registration and Login

For the first time to use iVMS-4200 client software, you need to register a super user for login.

### Steps:

1. Input the super user name and password. The software will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.
2. Confirm the password.
3. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
4. Click **Register**. Then, you can log into the software as the super user.



- ◆ A user name cannot contain any of the following characters: / \ : \* ? " < > |. And the length of the password cannot be less than 6 characters.
- ◆ For your privacy, we strongly recommend changing the password to something 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.
- ◆ Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

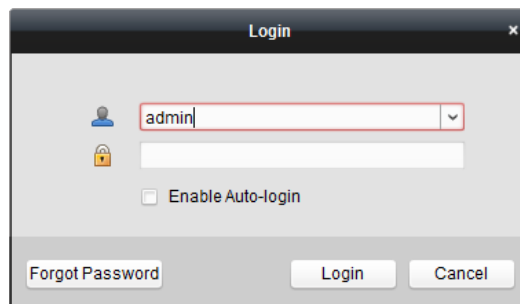
When opening iVMS-4200 after registration, you can log into the client software with the registered user name and password.

**Steps:**

1. Input the user name and password you registered.

**Note:** If you forget your password, please click **Forgot Password** and remember the encrypted string in the pop-up window. Contact your dealer and send the encrypted string to him to reset your password.

2. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
3. Click **Login**.



After running the client software, you can open the wizards (including video wizard, video wall wizard, security control panel wizard, access control and video intercom wizard, and attendance wizard), to guide you to add the device and do other settings and operations. For detailed configuration about the wizards, please refer to the *Quick Start Guide of iVMS-4200*.

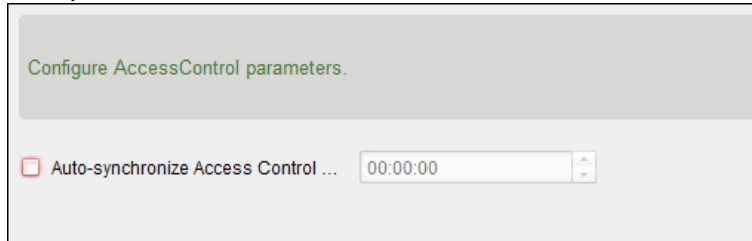
## 7.3 System Configuration

**Purpose:**

You can synchronize the missed access control events to the client.

**Steps:**

1. Click **Tool – System Configuration**.
2. In the System Configuration window, check the **Auto-synchronize Access Control Event** checkbox.
3. Set the synchronization time.  
The client will auto-synchronize the missed access control event to the client at the set time.



## 7.4 Access Control Management

**Purpose:**

The Access Control module is applicable to access control devices and video intercom. It provides multiple functionalities, including person and card management, permission configuration, access control status management, video intercom, and other advanced functions.


You can also set the event configuration for access control and display access control points and zones on E-map.

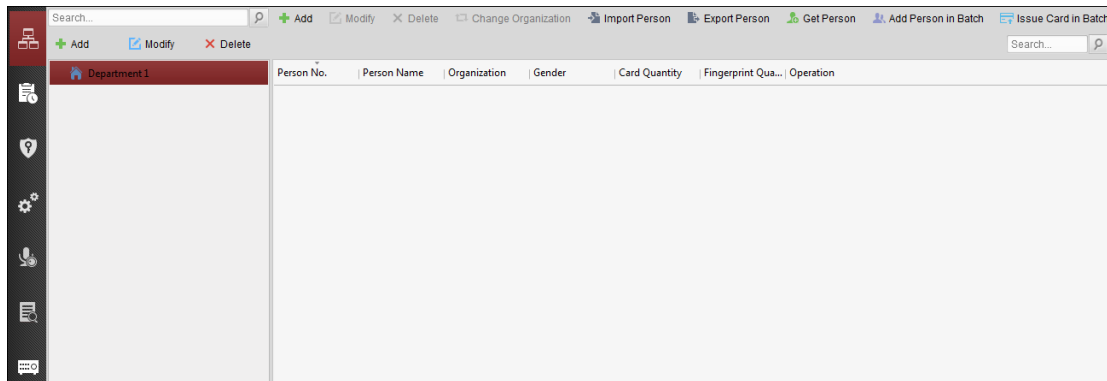
**Note:** For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings.



Click  in the control panel, and check **Access Control** to add the Access Control module to the control panel.



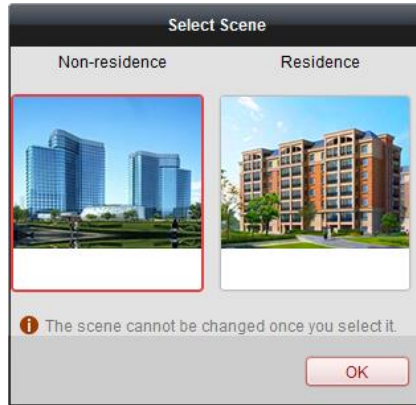
Click  to enter the Access Control module.



**Before you start:**

For the first time opening the Access Control module, the following dialog will pop up and you are required to select the scene according to the actual needs.

You can select the scene as **Non-residence** and **Residence**.



**Notes:**

- Once the scene is configured, you cannot change it later.
- When you select **Non-Residence** mode, you cannot configure the Attendance Rule when adding person.

The Access Control module is composed of the following sub modules.

	<b>Person and Card</b>	Managing the organizations, persons, and assigning cards to persons.
	<b>Schedule and Template</b>	Configuring the week schedule, holiday group, and setting the template.
	<b>Permission</b>	Assigning access control permissions to persons and applying to the devices.
	<b>Advanced Function</b>	Providing advanced functions including access control parameters settings, card reader authentication, opening door with first card, anti-passing back, multi-door interlocking, and authentication password.
	<b>Video Intercom</b>	Video intercom between client and resident, searching the dial log, and releasing notice.
	<b>Search</b>	Searching history events of access control; Searching call logs, unlocking logs, and released notices.
	<b>Device Management</b>	Managing the access control devices and video intercom devices.

**Note:** In this chapter, we only introduce the operations about access control.

### 7.4.1 Adding Access Control Device

Click in the Access Control module to enter the following interface.

Device Type	Nickname	Connection ...	Network Parameters	Device Serial No.
Access Controller	Access Controller	TCP/IP	10.18.146.86:8000	DS- [REDACTED] 6
Encoding Device	10.33.3.159	TCP/IP	10.33.3.159:8000	DS- [REDACTED] 3
Encoding Device	10.16.6.250	TCP/IP	10.16.6.250:8000	2014- [REDACTED]
Encoding Device	10.20.132.215	TCP/IP	10.20.132.215:8000	DS- [REDACTED] 7
Encoding Device	10.66.76.193	TCP/IP	10.66.76.193:8005	DS- [REDACTED] J
Indoor Station	Indoor Station	TCP/IP	10.16.6.104:8000	DS- [REDACTED] J
Security Control Panel	Security Control Pa...	TCP/IP	10.18.146.81:8000	DS- [REDACTED] U
Security Control Panel	10.16.6.92	TCP/IP	10.16.6.92:8000	DS- [REDACTED] 7

**Note:** After adding the device, you should check the device arming status in **Tool – Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, refer *7.12 Arming Control*.

### Creating Password

**Purpose:**

For some devices, you are required to create the password to activate them before they can be added to the software and work properly.

**Note:** This function should be supported by the device.

**Steps:**

1. Enter the Device Management page.
2. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.

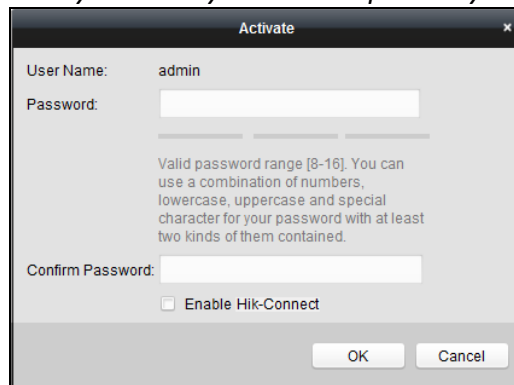
IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Time
192.0.0.64	[REDACTED]	[REDACTED]	Active	8000	[REDACTED]	2017-01
192.168.1.64	[REDACTED]	[REDACTED]	Inactive	8000	[REDACTED]	2017-01

3. Click the **Activate** button to pop up the Activation interface.
4. Create a password in the password field, and confirm the password.



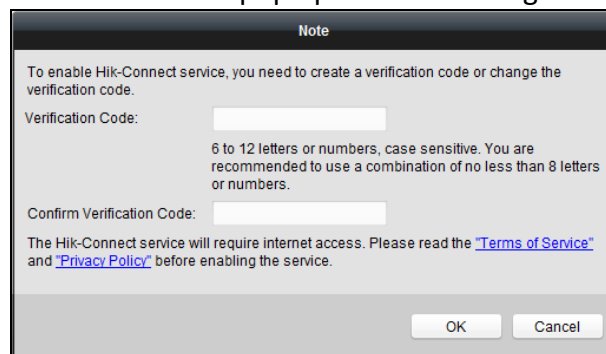
**STRONG PASSWORD RECOMMENDED**– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your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

resetting the password monthly or weekly can better protect your product.



5. (Optional) Enable Hik-Connect service when activating the device if the device supports.

- 1) Check **Enable Hik-Connect** checkbox to pop up the Note dialog.



- 2) Create a verification code.
- 3) Confirm the verification code.
- 4) Click **Terms of Service** and **Privacy Policy** to read the requirements.
- 5) Click **OK** to enable the Hik-Connect service.

6. Click **OK** to activate the device.

A "The device is activated." window pops up when the password is set successfully.

7. Click **Modify Netinfo** to pop up the Modify Network Parameter interface.


**Note:** This function is only available on the **Online Device** area. You can change the device IP address to the same subnet with your computer if you need to add the device to the software.

8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of DHCP.
9. Input the password set in step 4 and click **OK** to complete the network settings.

## Adding Online Device

### Purpose:

The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area. You can click the **Refresh Every 60s** button to refresh the information of the online devices.

**Note:** You can click  to hide the **Online Device** area.

IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Time
10.16.6.236	D		Active	8000		2017-01
10.16.6.92	D		Active	8000		2017-01
192.0.0.64	D		Active	8000		2017-01

### Steps:

1. Select the devices to be added from the list.

**Note:** For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, please refer to *Chapter 6 Activating the Access Control Terminal*.

2. Click **Add to Client** to open the device adding dialog box.
3. Input the required information.

**Nickname:** Edit a name for the device as you want.

**Address:** Input the device's IP address. The IP address of the device is obtained automatically in this adding mode.

**Port:** Input the device port No. The default value is *8000*.

**User Name:** Input the device user name. By default, the user name is *admin*.

**Password:** Input the device password.



*The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

**Note:** iVMS-4200 also provides a method to add the offline devices.

- 1) Check the **Add Offline Device** checkbox.
- 2) Input the required information, including the device channel number and alarm input number.
- 3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

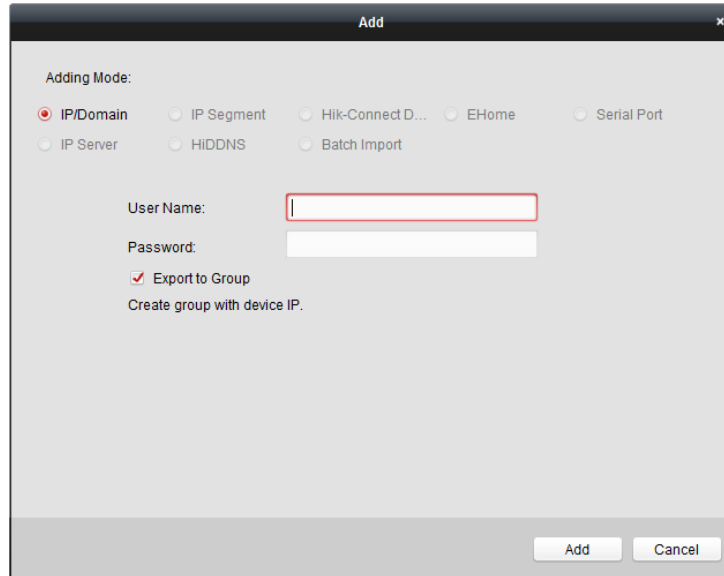
### ➤ Adding Multiple Online Device

If you want to add multiple online devices to the client software, click and hold *Ctrl* key to select multiple devices, and click **Add to Client** to open the device adding dialog box. In the pop-up message box, enter the user name and password for the devices to be added.

### ➤ Adding All Online Devices

If you want to add all the online devices to the client software, click **Add All** and click **OK** in the pop-up message box. Then enter the user name and password for the devices to be added.





## Adding Devices by IP or Domain Name

### Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP/Domain** as the adding mode.
3. Input the required information.

**Nickname:** Edit a name for the device as you want.

**Address:** Input the device's IP address or domain name.

**Port:** Input the device port No.. The default value is *8000*.

**User Name:** Input the device user name. By default, the user name is *admin*.

**Password:** Input the device password.



*The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

**Note:** iVMS-4200 also provides a method to add the offline devices.

- 1) Check the **Add Offline Device** checkbox.
- 2) Input the required information, including the device channel number and alarm input number.
- 3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

## Adding Devices by IP Segment

### Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP Segment** as the adding mode.
3. Input the required information.

**Start IP:** Input a start IP address.

**End IP:** Input an end IP address in the same network segment with the start IP.

**Port:** Input the device port No.. The default value is *8000*.

**User Name:** Input the device user name. By default, the user name is *admin*.

**Password:** Input the device password.



*The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

**Note:** iVMS-4200 also provides a method to add the offline devices.

- 1) Check the **Add Offline Device** checkbox.
- 2) Input the required information, including the device channel number and alarm input number.
- 3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add**.

You can add the device which the IP address is between the start IP and end IP to the device

list.

## Adding Devices by Hik-Connect Domain

### **Purpose:**

You can add the devices connected via Hik-Connect by inputting the Hik-Connect account and password.

**Before you start:** Add the devices to Hik-Connect account via iVMS-4200, iVMS-4500 Mobile Client, or Hik-Connect first. For details about adding the devices to Hik-Connect account via iVMS-4200, refer to *the User Manual of iVMS-4200 Client Software*.

### ➤ **Add Single Device**

#### **Steps:**

1. Click **Add** to open the device adding dialog.
2. Select **Hik-Connect Domain** as the adding mode.
3. Select **Single Adding**.
4. Input the required information.

**Nickname:** Edit a name for the device as you want.

**Device Serial No.:** Input the device serial No.

**User Name:** Input the device user name. By default, the user name is *admin*.

**Password:** Input the device password.



*The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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.*

**Hik-Connect Account:** Input the Hik-Connect account.

**Hik-Connect Password:** Input the Hik-Connect password.

- Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
- Click **Add** to add the device.

The screenshot shows the 'Add' dialog box with the following configuration:

- Adding Mode:**
  - IP/Domain
  - IP Segment
  - Hik-Connect D...
  - EHome
  - Serial Port
  - IP Server
  - HIDDNS
  - Batch Import
- Adding Mode:**
  - Batch Adding
  - Single Adding
- Nickname:** [Empty text box]
- Device Serial No.:** [Empty text box]
- User Name:** [Empty text box]
- Password:** [Empty text box]
- Hik-Connect Account:** [Empty text box]
- Hik-Connect Password:** [Empty text box]
- Export to Group**  
Set the device name as the group name and add all the channels connected to the device to the group.

Buttons: Add, Cancel

## Add Devices in Batch

### Steps:

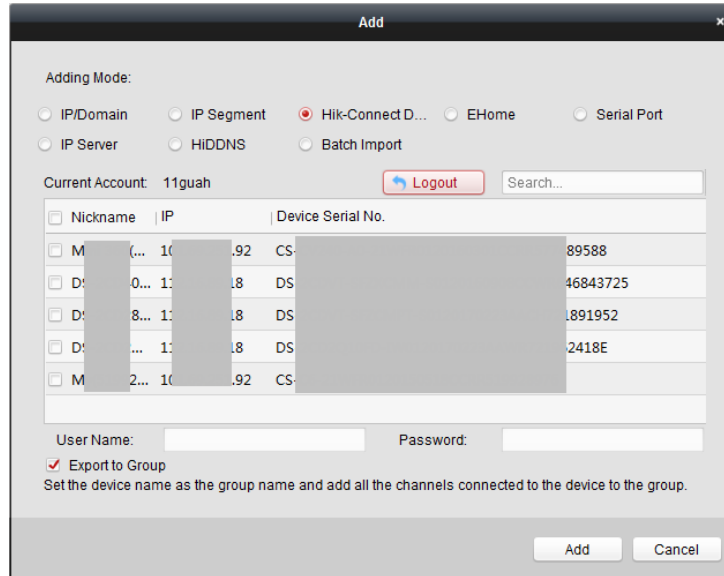
- Click **Add** to open the device adding dialog.

The screenshot shows the 'Add' dialog box with the following configuration:

- Adding Mode:**
  - IP/Domain
  - IP Segment
  - Hik-Connect D...
  - EHome
  - Serial Port
  - IP Server
  - HIDDNS
  - Batch Import
- Adding Mode:**
  - Batch Adding
  - Single Adding
- Hik-Connect Account:** [Empty text box]
- Hik-Connect Password:** [Empty text box]
- 

Buttons: Add, Cancel

- Select **Hik-Connect Domain** as the adding mode.
- Select **Batch Adding**.
- Input the required information.
  - Hik-Connect Account:** Input the Hik-Connect account.
  - Hik-Connect Password:** Input the Hik-Connect password.
- Click **Get Device List** to show the devices added to Hik-Connect account.



6. Check the checkbox(es) to select the device as desired.
7. Input the user name and password for the devices to be added.
8. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
9. Click **Add** to add the devices.

### Adding Devices by EHome Account

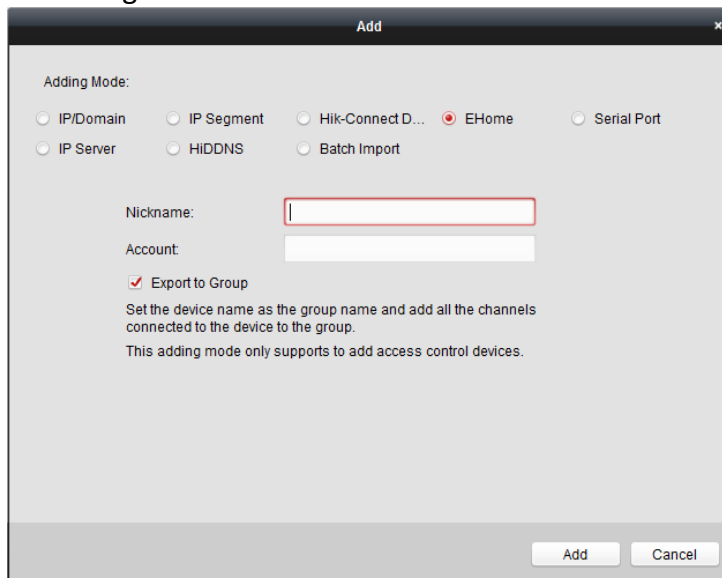
**Purpose:**

You can add access control device connected via EHome protocol by inputting the EHome account.

**Before you start:** Set the network center parameter first. For details, refer to *Chapter 7.4.4 Network Settings*.

**Steps:**

1. Click **Add** to open the device adding dialog box.
2. Select **EHome** as the adding mode.



3. Input the required information.

**Nickname:** Edit a name for the device as you want.

**Account:** Input the account name registered on EHome protocol.

- Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

**Note:** iVMS-4200 also provides a method to add the offline devices.

- Check the **Add Offline Device** checkbox.
- Input the required information, including the device channel number and alarm input number.
- Click **Add**.

When the offline device comes online, the software will connect it automatically.

- Click **Add** to add the device.

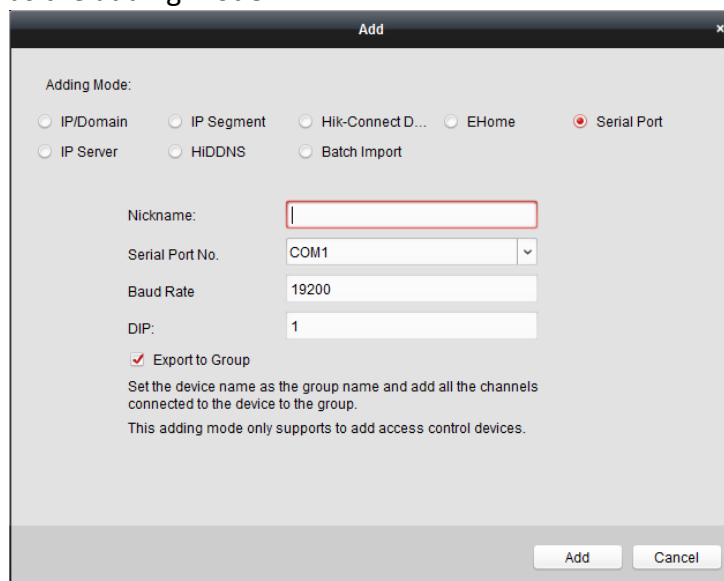
### Adding Devices by Serial Port

**Purpose:**

You can add access control device connected via serial port.

**Steps:**

- Click **Add** to open the device adding dialog box.
- Select **Serial Port** as the adding mode.



- Input the required information.

**Nickname:** Edit a name for the device as you want.

**Serial Port No.:** Select the device's connected serial port No.

**Baud Rate:** Input the baud rate of the access control device.

**DIP:** Input the DIP address of the device.

- Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

**Note:** iVMS-4200 also provides a method to add the offline devices.

- Check the **Add Offline Device** checkbox.
- Input the required information, including the device channel number and alarm input number.

3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

## Adding Devices by IP Server

### Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP Server** as the adding mode.

3. Input the required information.

**Nickname:** Edit a name for the device as you want.

**Server Address:** Input the IP address of the PC that installs the IP Server.

**Device ID:** Input the device ID registered on the IP Server.

**User Name:** Input the device user name. By default, the user name is *admin*.

**Password:** Input the device password.



*The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

**Note:** iVMS-4200 also provides a method to add the offline devices.

- 1) Check the **Add Offline Device** checkbox.
- 2) Input the required information, including the device channel number and alarm input number.
- 3) Click **Add**.

When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

## Adding Devices by HiDDNS

### Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **HiDDNS** as the adding mode.

3. Input the required information.

**Nickname:** Edit a name for the device as you want.

**Server Address:** [www.hik-online.com](http://www.hik-online.com).

**Device Domain Name:** Input the device domain name registered on HiDDNS server.

**User Name:** Input the device user name. By default, the user name is *admin*.

**Password:** Input the device password.



*The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

**Note:** iVMS-4200 also provides a method to add the offline devices.

- 1) Check the **Add Offline Device** checkbox.
- 2) Input the required information, including the device channel number and alarm input number.
- 3) Click **Add**.

When the offline device comes online, the software will connect it automatically.



- Click **Add** to add the device.

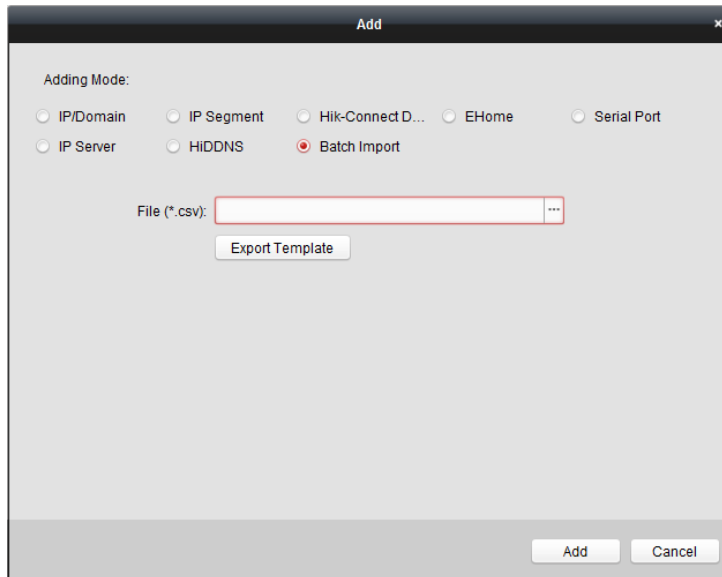
## Importing Devices in Batch

### **Purpose:**

The devices can be added to the software in batch by inputting the device information in the pre-defined CSV file.

### **Steps:**

- Click **Add** to open the device adding dialog box.
- Select **Batch Import** as the adding mode.



- Click **Export Template** and save the pre-defined template (CSV file) on your PC.
- Open the exported template file and input the required information of the devices to be added on the corresponding column.

**Nickname:** Edit a name for the device as you want.

**Adding Mode:** You can input 0, 2, 3, 4, 5, or 6 which indicated different adding modes. 0 indicates that the device is added by IP address or domain name; 2 indicates that the device is added via IP server; 3 indicates that the device is added via HiDDNS; 4 indicates that the device is added via EHome protocol; 5 indicates that the device is added by serial port; 6 indicates that the device is added via Hik-Connect Domain.

**Address:** Edit the address of the device. If you set 0 as the adding mode, you should input the IP address or domain name of the device; if you set 2 as the adding mode, you should input the IP address of the PC that installs the IP Server; if you set 3 as the adding mode, you should input *www.hik-online.com*.

**Port:** Input the device port No.. The default value is 8000.

**Device Information:** If you set 0 as the adding mode, this field is not required; if you set 2 as the adding mode, input the device ID registered on the IP Server; if you set 3 as the adding mode, input the device domain name registered on HiDDNS server; if you set 4 as the adding mode, input the EHome account; if you set 6 as the adding mode, input the device serial No.

**User Name:** Input the device user name. By default, the user name is *admin*.

**Password:** Input the device password.



*The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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.*

**Add Offline Device:** You can input 1 to enable adding the offline device, and then the software will automatically connect it when the offline device comes online. 0 indicates disabling this function.

**Export to Group:** You can input 1 to create a group by the device name (nickname). All the channels of the device will be imported to the corresponding group by default. 0 indicates disabling this function.

**Channel Number:** If you set 1 for Add Offline Device, input the channel number of the device. If you set 0 for Add Offline Device, this field is not required.

**Alarm Input Number:** If you set 1 for Add Offline Device, input the alarm input number of the device. If you set 0 for Add Offline Device, this field is not required.


**Serial Port No.:** If you set 5 as the adding mode, input the serial port No. for the access control device.

**Baud Rate:** If you set 5 as the adding mode, input the baud rate of the access control device.

**DIP:** If you set 5 as the adding mode, input the DIP address of the access control device.

**Hik-Connect Account:** If you set 6 as the adding mode, input the Hik-Connect account.

**Hik-Connect Password:** If you set 6 as the adding mode, input the Hik-Connect password.

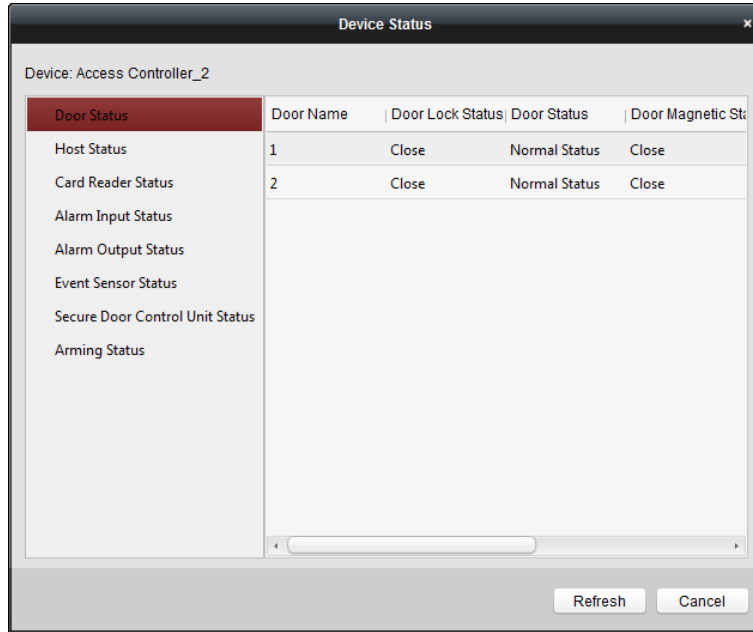
5. Click  and select the template file.
6. Click **Add** to import the devices.

The devices will be displayed on the device list for management after added successfully. You can check the resource usage, HDD status, recording status, and other information of the added devices on the list.

Click **Refresh All** to refresh the information of all added devices. You can also input the device name in the filter field for search.

## 7.4.2 Viewing Device Status

In the device list, you can select the device and then click **Device Status** button to view its status.



**Note:** The interface may differ from the picture displayed above. Refer to the actual interface when adopting this function.

**Door Status:** The status of the connected door.

**Host Status:** The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, and Host Anti-Tamper Status.

**Card Reader Status:** The status of card reader.

**Note:** If you use the card reader with RS-485 connection, you can view the status of online or offline. If you use the card reader with Wiegand connection, you can view the status of offline.

**Alarm Input Status:** The alarm input status of each port.

**Alarm Output Status:** The alarm output status of each port.

**Event Sensor Status:** The event sensor status of each port.

**Secure Door Control Unit Status:** The online status and tamper status of the Secure Door Control Unit.

**Arming Status:** The status of the device.

### 7.4.3 Editing Basic Information

**Purpose:**

After adding the access control device, you can edit the device basic information.

**Steps:**

1. Select the device in the device list.
2. Click **Modify** to pop up the modifying device information window.
3. Click **Basic Information** tab to enter the Basic Information interface.

4. Edit the device information, including the adding mode, the device name, the device IP address, port No., user name, and the password.

### 7.4.4 Network Settings

**Purpose:**

After adding the access control device, you can set the uploading mode, and set the network center and wireless communication center.

Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **Network Settings** tab to enter the network settings interface.

#### Uploading Mode Settings

**Purpose :**

You can set the center group for uploading the log via the EHome protocol.

**Steps:**

1. Click the **Uploading Mode** tab.

2. Select the center group in the dropdown list.
3. Check the **Enable** checkbox to enable the selected center group.
4. Select the uploading mode in the dropdown list. You can enable **N1/G1** for the main channel and the backup channel, or select **Close** to disable the main channel or the backup channel.

**Note:** The main channel and the backup channel cannot enable N1 or G1 at the same time.

5. Click **Save** button to save parameters.

## Network Center Settings

You can set the account for EHome protocol in Network Settings page. Then you can add devices via EHome protocol.

### Steps:

1. Click the **Network Center** tab.

The screenshot shows a configuration window with three tabs: 'Uploading Mode', 'Network Center', and 'Wireless Communication Center'. The 'Network Center' tab is active. It contains the following fields: 'Center Group' (dropdown menu with 'Center1' selected), 'Address Type' (dropdown menu with 'Domain Name' selected), 'Domain Name' (text input field), 'Port' (text input field), 'Protocol Type' (dropdown menu), and 'Account' (text input field). A 'Save' button is located at the bottom center of the form.

2. Select the center group in the dropdown list.
3. Select the address type.
4. Set the IP address/domain name.
5. Set the port No. for EHome protocol. By default, the port No. is 7660.
6. Select the protocol type as EHome.
7. Set an account name for the network center.
8. Click **Save** button to save parameters.

### Notes:

- The account should contain 1 to 32 characters and only letters and numbers are allowed.
- The port No. of the wireless network and wired network should be consistent with the port No. of EHome.
- You can set the domain name in Enable NTP area *Time* section in Remote Configuration. For details, refer to *Time* in 7.4.9 Remote Configuration.

## Wireless Communication Center Settings

### Steps:

1. Click the **Wireless Communication Center** tab.

The screenshot shows a configuration window with three tabs: 'Uploading Mode', 'Network Center', and 'Wireless Communication Center'. The 'Wireless Communication Center' tab is active. It contains the following fields: 'APN Name' (dropdown menu), 'SIM Card No.' (text input field), 'Center Group' (dropdown menu with 'Center1' selected), 'IP Address' (text input field with '0.0.0.0' entered), 'Port' (text input field), 'Protocol Type' (dropdown menu), and 'Account' (text input field). A 'Save' button is located at the bottom center of the form.

2. Select the APN name as CMNET or UNINET.
3. Input the SIM Card No.
4. Select the center group in the dropdown list.
5. Input the IP address and port No.
6. Select the protocol type as EHome. By default, the port No. for EHome is 7660.
7. Set an account name for the network center. A consistent account should be used in one platform.
8. Click **Save** button to save parameters.

**Note:** The port No. of the wireless network and wired network should be consistent with the port No. of EHome.

### 7.4.5 Capture Settings

You can set the parameters of capture linkage and manual capture.

Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **Capture Settings** tab to enter the capture settings interface.

**Notes:**

- The **Capture Settings** should be supported by the device.
- Before setting the capture setting, you should configure the storage server for picture storage.

#### Linked Capture

**Steps:**

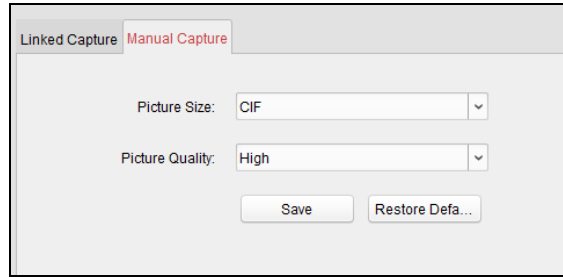
1. Select the **Linked Capture** tab.

2. Set the linked capture times once triggered.  
Set the capture interval according to the capture times.
3. Click **Save** to save the settings.

#### Manual Capture

**Steps:**

1. Select the **Manual Capture** tab.



2. Select the resolution of the captured pictures from the dropdown list.  
**Note:** The supported resolution types are CIF, QCIF, 4CIF/D1, SVGA, HD720P, VGA, WD1, and AUTO.
3. Select the picture quality as High, Medium, or Low.
4. Click **Save** to save the settings.
5. You can click **Restore Default Value** to restore the parameters to default settings.

### 7.4.6 RS-485 Settings

**Purpose:**

You can set the RS-485 parameters including the serial port, the baud rate, the data bit, the stop bit, the parity type, the communication mode, and the working mode.

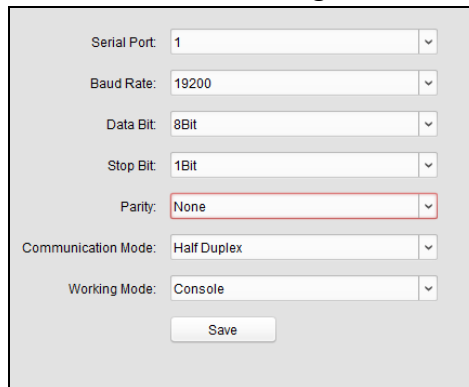
Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **RS-485 Settings** tab to enter the RS-485 settings interface.

**Note:** The RS-485 Settings should be supported by the device.

**Steps:**

1. Click **RS-485 Settings** tab to enter the RS-485 settings interface.



2. Select the serial No. of the port from the dropdown list to set the RS-485 parameters.
3. Set the baud rate, data bit, the stop bit, parity type, communication mode, and work mode in the dropdown list.
4. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

**Note:** After changing the working mode, the device will be rebooted. A prompt will be popped up after changing the working mode.

## 7.4.7 Wiegand Settings

### **Purpose:**

You can set the Wiegand channel and the communication mode.

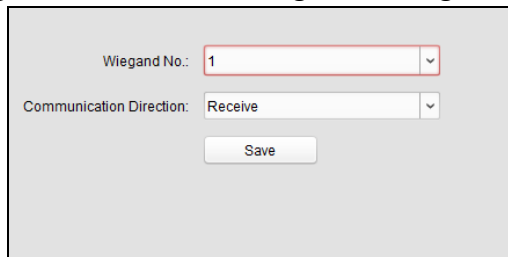
Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **Wiegand-485 Settings** tab to enter the Wiegand settings interface.

**Note:** The Wiegand Settings should be supported by the device.

### **Steps:**

1. Click the **Wiegand Settings** tab to enter the Wiegand Settings interface.



The screenshot shows a settings window with a light gray background. At the top, there is a label 'Wiegand No.' followed by a dropdown menu containing the number '1'. Below this is another label 'Communication Direction' followed by a dropdown menu containing the word 'Receive'. At the bottom center of the window is a rectangular button labeled 'Save'.

2. Select the Wiegand channel No. and the communication mode in the dropdown list.  
If you set the **Communication Direction** as **Send**, you are required to set the Wiegand Mode as Wiegand 26 or Wiegand 34.
3. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

**Note:** After changing the communication direction, the device will be rebooted. A prompt will be popped up after changing the communication direction.

## 7.4.8 M1 Card Encryption

The M1 Card Encryption function increases the authentication security level, which should be applied together with the card enrollment station of our company via the client software or the web client. After issuing the card, you can set the M1 card encryption function on the controller.

### **Notes:**

- The function should be supported by the device.
- For details about issuing card, refer to *Adding Person (Card)* in 7.5.2 *Person Management*.

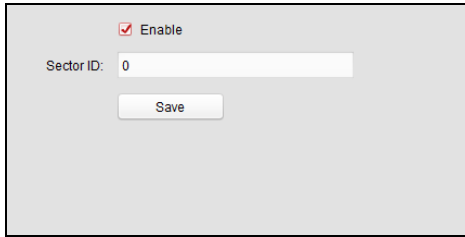
Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **M1 Card Encryption** tab to enter the M1 Card Encryption interface.

### **Steps:**

1. In the M1 Card Encryption interface, check **Enable** checkbox to enable the M1 card encryption function.





2. Set the sector ID.
3. Click **Save** to save the settings.

**Note:** The sector ID ranges from 1 to 100.

## 7.4.9 Remote Configuration

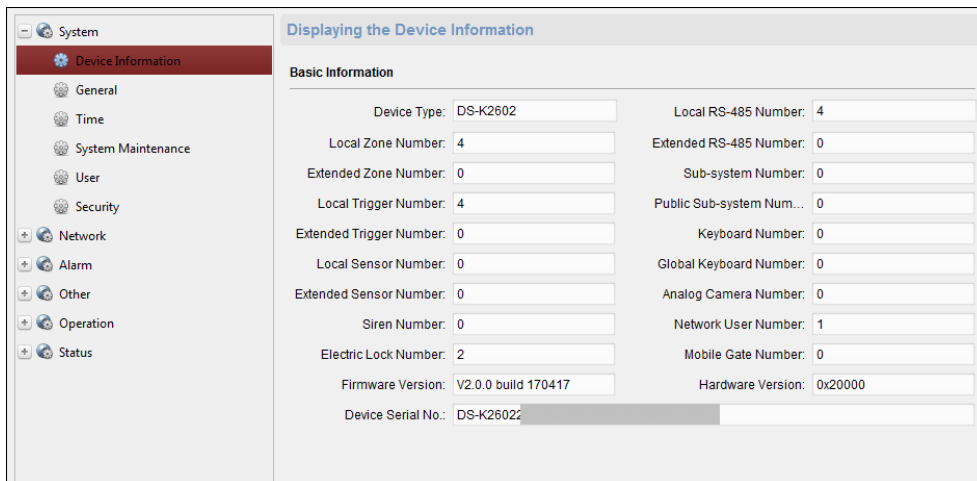
### **Purpose:**

In the device list, select the device and click **Remote Configuration** button to enter the remote configuration interface. You can set the detailed parameters of the selected device.

### **Checking Device Information**

#### **Steps:**

1. In the device list, you can click **Remote Configuration** to enter the remote configuration interface.
2. Click **System** -> **Device Information** to check the device basic information and the device version information.



### **Editing Device Name**

In the Remote Configuration interface, click **System** -> **General** to configure the device name and overwrite record files parameter. Click **Save** to save the settings.

**Configuring the General Parameters**

**Device Information**

Device Name:

## Editing Time

### Steps:

1. In the Remote Configuration interface, click **System** -> **Time** to configure the time zone.
2. (Optional) Check **Enable NTP** and configure the NTP server address, the NTP port, and the synchronization interval.
3. (Optional) Check **Enable DST** and configure the DST star time, end time and the bias.
4. Click **Save** to save the settings.

**Configuring the Time Settings (e.g., NTP, DST)**

**Time Zone**

Select Time Zone:

**Enable NTP**

Server Address:

NTP Port:

Sync Interval:  Minute(s)

**Enable DST**

Start Time:     : 00


End Time:     : 00

DST Bias:

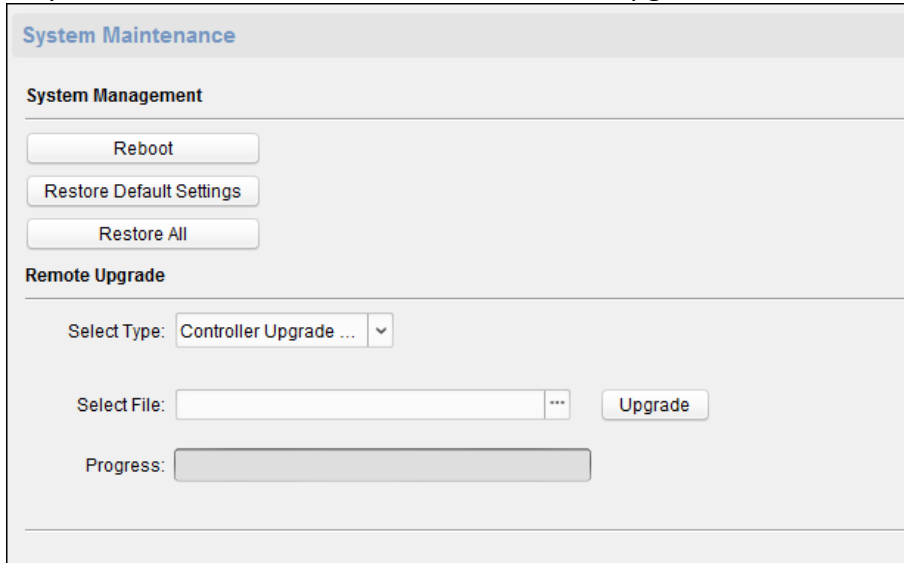
## Setting System Maintenance

### Steps:

1. In the Remote Configuration interface, click **System** -> **System Maintenance**.
  2. Click **Reboot** to reboot the device.  
 Or click **Restore Default Settings** to restore the device settings to the default ones, excluding the IP address.  
 Or click **Restore All** to restore the device parameters to the default ones. The device should be activated after restoring.
- Note:** The configuration file contains the device parameters.
3. You can also remote upgrade the device.
    - 1) In the Remote Upgrade part, select an upgrade file type in the dropdown list.  
 You can select Controller Upgrade File or Card Reader Upgrade in the drop-down list.

- 2) Click  to select the upgrade file.
- 3) Click **Upgrade** to start upgrading.

**Note:** Only card readers connected via RS-485 can be upgraded.

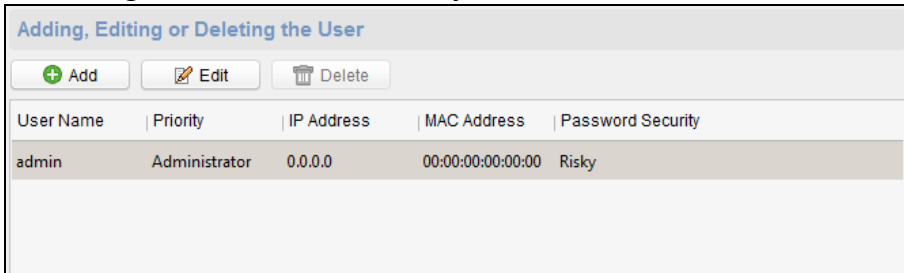


The screenshot shows the 'System Maintenance' interface. Under 'System Management', there are three buttons: 'Reboot', 'Restore Default Settings', and 'Restore All'. Under 'Remote Upgrade', there is a 'Select Type' dropdown menu currently set to 'Controller Upgrade ...'. Below that is a 'Select File' field with a file selection icon and an 'Upgrade' button. At the bottom, there is a 'Progress' bar.

## Managing User

### Steps:

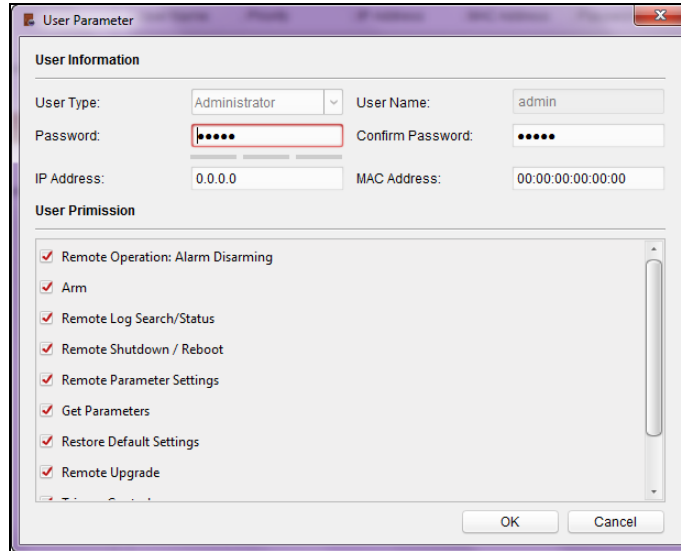
1. In the Remote Configuration interface, click **System** -> **User**.



The screenshot shows the 'Adding, Editing or Deleting the User' interface. At the top, there are three buttons: '+ Add', 'Edit', and 'Delete'. Below these is a table with the following columns: 'User Name', 'Priority', 'IP Address', 'MAC Address', and 'Password Security'. The table contains one row with the following data:

User Name	Priority	IP Address	MAC Address	Password Security
admin	Administrator	0.0.0.0	00:00:00:00:00:00	Risky

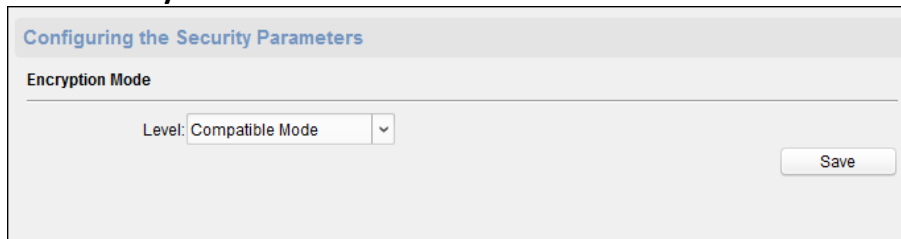
2. Click **Add** to add the user (Do not support by the elevator controller.).  
Or select a user in the user list and click **Edit** to edit the user. You are able to edit the user password, the IP address, the MAC address and the user permission. Click **OK** to confirm editing.



## Setting Security

### Steps:

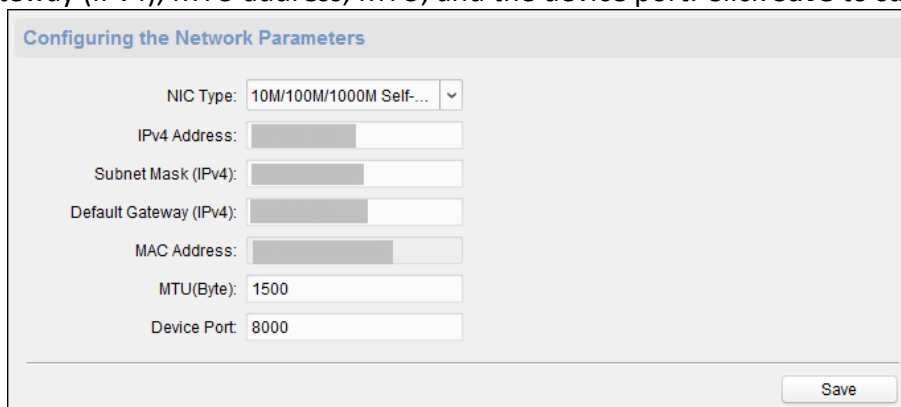
1. Click **System** -> **Security**.



2. Select the encryption mode in the dropdown list.  
You can select **Compatible Mode** or **Encryption Mode**.
3. Click **Save** to save the settings.

## Configuring Network Parameters

Click **Network** -> **General**. You can configure the NIC type, the IPv4 address, the subnet mask (IPv4), the default gateway (IPv4), MTU address, MTU, and the device port. Click **Save** to save the settings.



## Configuring Upload Method

### Purpose :

You can set the center group for uploading the log via the EHome protocol.

**Steps:**

1. Click **Network** -> **Report Strategy**.

2. Select a Center Group from the drop-down list.
3. Check the **Enable** check box.
4. Set the uploading method.  
You can set the main channel and the backup channel.
5. Click **Settings** on the right of the channel field to set the detailed information.
6. Click **Save** to save the settings.

**Configuring Advanced Network**

Click **Network** -> **Advanced Settings**. You can configure the DNS address 1, the DNS address 2, the alarm host IP and the alarm host port. Click **Save** to save the settings.

**Configuring Zone Parameters**

**Step:**

1. Click **Alarm** -> **Zone** to enter the Zone interface.

Configuring the Zone Parameters				
Zone	Name	Zone Type	Sensitivity	Settings
1		24-hour Voiced ...	250ms	
2		24-hour Voiced ...	250ms	
3		24-hour Voiced ...	250ms	
4		24-hour Voiced ...	250ms	

- Click to pop up the Zone Settings window.

**Zone Settings** [X]

Zone No.:

Name:

Detector Type:  ▾

Zone Type:  ▾

Sensitivity:  ▾

- Set the zone name, the detector type, the zone type and the sensitivity.
- Click **Save** to save the settings.  
Or click **Copy to...** to copy the parameters to other zones.

### Configuring Relay Parameters

**Steps:**

- Click **Alarm -> Relay**.  
You can view the relay parameters.

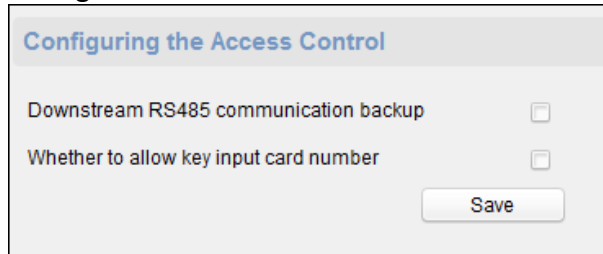
Configuring Relay Parameters				
Relay	Name	Output Delay(s)	Zone Linkage	Settings
1		0	None	
2		0	None	
3		0	None	
4		0	None	

- Click the to pop up the Relay Parameters Settings window.
- Set the relay name and the output delay.
- Click **Save** to save the paramters.  
Or click **Copy to...** to copy the relay information to other relays.


### Configuring Access Control Parameters

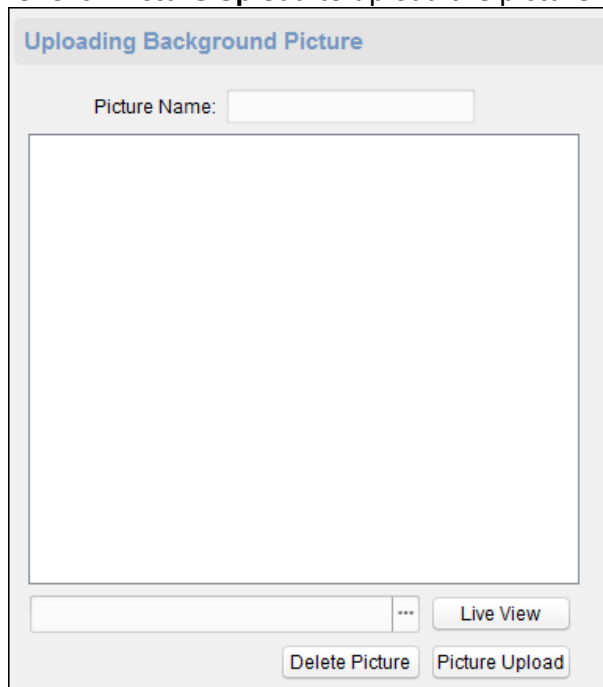
**Steps:**

1. In the Remote Configuration interface, click **Other** -> **Access Control Parameters**.
2. Select and check the **Downstream RS-485 Communication Backup** checkbox or the **Press Key to Input Card No.** checkbox.
3. Click **Save** to save the settings.



### Uploading Background Picture

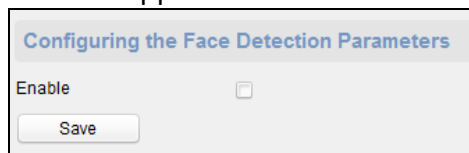
Click **Other** -> **Picture Upload**. Click  to select the picture from the local. You can also click **Live View** to preview the picture. Click **Picture Upload** to upload the picture.



### Configuring Face Detection Parameters

Click **Other** -> **Face Detection**. You can check the **Enable** checkbox to enable the device face detection function.

**Note:** Only devices with video function support this function.

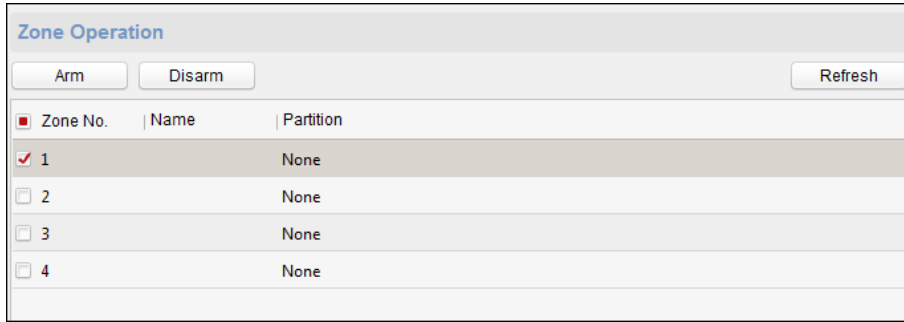


### Operating Zone

**Steps:**

1. Click **Operation** -> **Zone**.

You can view the zone information.

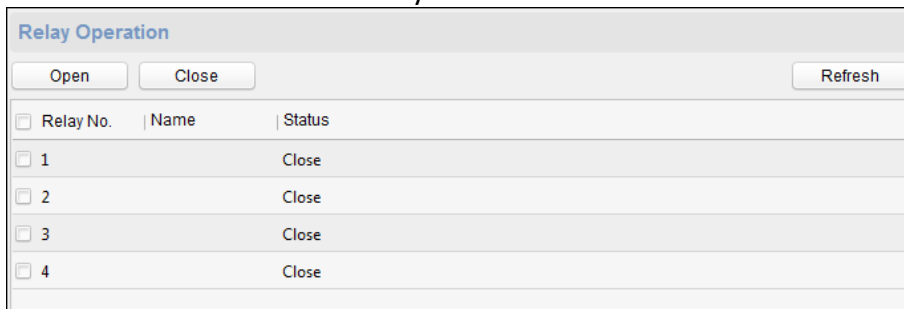


2. Check the zone checkbox.
3. Click **Arm** or **Disarm** to arm or disarm the zone.
4. (Optional) click **Refresh** to refresh the zone status.

### Operating Relay

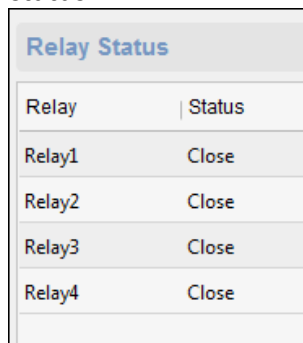
**Steps:**

1. Click **Operation** -> **Relay**.  
You can view the relay status.
2. Check the relay checkbox
3. Click **Open** or **Close** to open/close the relay.
4. (Optional) Click **Refresh** to refresh the relay status.



### Viewing Relay Status


Click **Status** -> **Relay** to view the relay status.

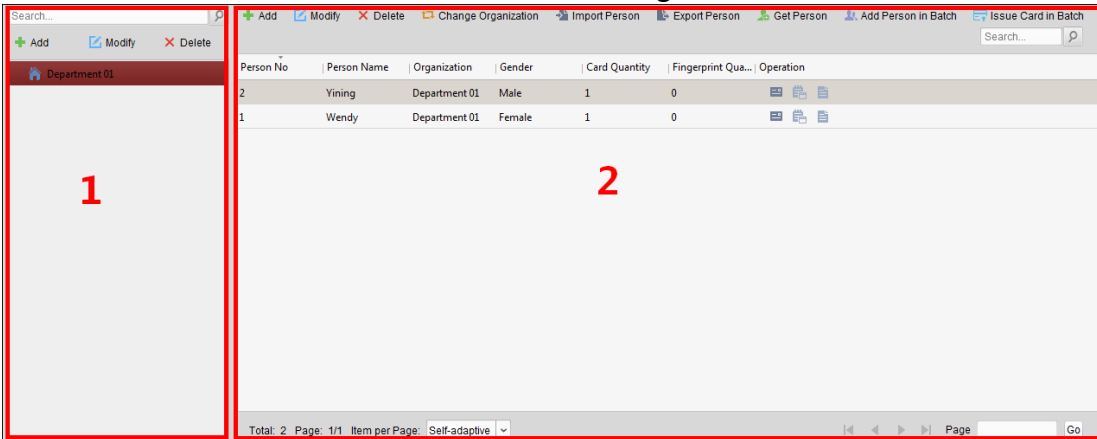


## 7.5 Person and Card Management

You can add, edit, and delete the organization and person in Person and Card Management module.



Click  tab to enter the Person and Card Management interface.



The interface

is divided into two parts: Organization Management and Person Management.

<b>1</b>	<b>Organization Management</b>	You can add, edit, or delete the organization as desired.
<b>2</b>	<b>Person Management</b>	After adding the organization, you can add the person to the organization and issue card to persons for further management.

## 7.5.1 Organization Management

### Adding Organization

#### Steps:

- In the organization list on the left, you should add a top organization as the parent organization of all organizations.  
Click **Add** button to pop up the adding organization interface.

- Input the Organization Name as desired.
- Click **OK** to save the adding.
- You can add multiple levels of organizations according to the actual needs.  
To add sub organizations, select the parent organization and click **Add**.  
Repeat *Step 2* and 3 to add the sub organization.  
Then the added organization will be the sub-organization of the upper-level organization.

**Note:** Up to 10 levels of organizations can be created.

### Modifying and Deleting Organization

You can select the added organization and click **Modify** to modify its name.

You can select an organization, and click **Delete** button to delete it.

**Notes:**

- The lower-level organizations will be deleted as well if you delete an organization.
- Make sure there is no person added under the organization, or the organization cannot be deleted.

## 7.5.2 Person Management

After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting persons information in batch, etc.

**Note:** Up to 10,000 persons or cards can be added.

### Adding Person

#### Adding Person (Basic Information)

##### Steps:

1. Select an organization in the organization list and click **Add** button on the Person panel to pop up the adding person dialog.

2. The Person No. will be generated automatically and is not editable.
3. Input the basic information including person name, gender, phone No., birthday details, and email address.
4. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.  
**Note:** The picture should be in \*.jpg format.
5. (Optional) You can also click **Take Photo** to take the person's photo with the PC camera.
6. Click **OK** to finish adding.

#### Adding Person (Detailed Information)

##### Steps:

1. In the Add Person interface, click **Details** tab.

2. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.
  - **Linked Device:** You can bind the indoor station to the person.
    - Note:** If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.
  - **Room No.:** You can input the room No. of the person.
3. Click **OK** to save the settings.

### Adding Person (Permission)

You can assign the permissions (including operation permissions of access control device and access control permissions) to the person when adding person.

**Note:** For setting the access control permission, refer to *Chapter 7.7 Permission Configuration*.

#### Steps:

1. In the Add Person interface, click **Permission** tab.

2. In the Device Operation Role field, select the role of operating the access control device.
  - Normal User:** The person has the permission to check-in/out on the device, pass the access control point, etc.
  - Administrator:** The person has the normal user permission, as well as permission to configure the device, including adding normal user, etc.
3. In the Permission(s) to Select list, all the configured permissions display. Check the permission(s) checkbox(es) and click > to add to the Selected Permission(s) list. (Optional) You can click >> to add all the displayed permissions to the Selected Permission(s) list. (Optional) In the Selected Permission(s) list, select the selected permission and click < to

remove it. You can also click << to remove all the selected permissions.

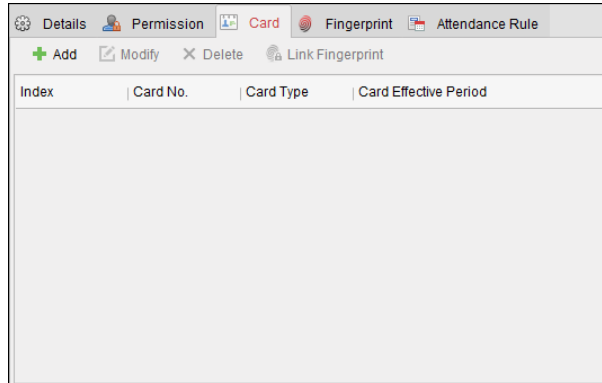
4. Click **OK** to save the settings.

### Adding Person (Card)

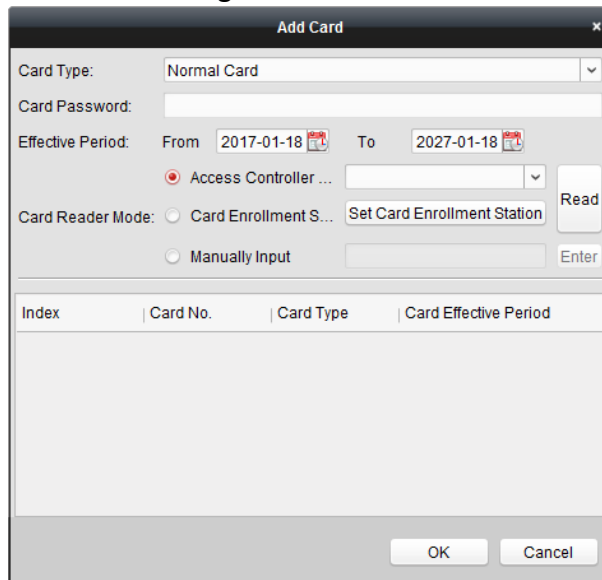
You can add card and issue the card to the person.

#### Steps:

1. In the Add Person interface, click **Card** tab.



2. Click **Add** to pop up the Add Card dialog.



3. Select the card type according to actual needs.

- **Normal Card**
- **Card for Disabled Person:** The door will remain open for the configured time period for the card holder.
- **Card in Blacklist:** The card swiping action will be uploaded and the door cannot be opened.
- **Patrol Card:** The card swiping action can be used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
- **Duress Card:** The door can be opened by swiping the duress card when there is duress. At the same time, the client can report the duress event.
- **Super Card:** The card is valid for all the doors of the controller during the configured schedule.


- **Visitor Card:** The card is assigned for visitors. For the Visitor Card, you can set the **Max. Swipe Times**.

**Notes:**

- The Max. Swipe Times should be between 0 and 255. When your swiping card times is more than the configured times, card swiping will be invalid.
- When set the times as 0, it means the card swiping is unlimited.

4. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

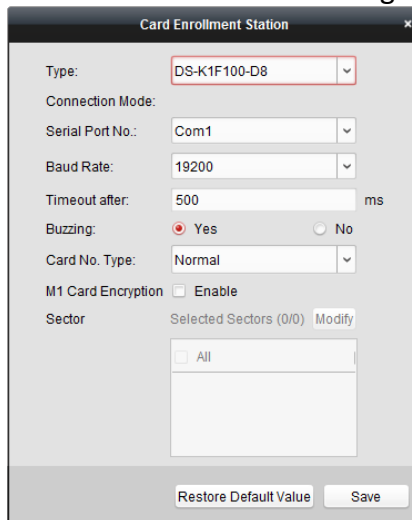
**Note:** The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, *Chapter 7.8.2 Card Reader Authentication*.

5. Click  to set the effective time and expiry time of the card.

6. Select the Card Reader Mode for reading the card No.

- **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
- **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.

**Note:** The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



- 2) Select the Card Enrollment Station type.

**Note:** Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

- 3) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.

- 4) Click **Save** button to save the settings.

You can click **Restore Default Value** button to restore the defaults.

- **Manually Input:** Input the card No. and click **Enter** to input the card No.
- 7. Click **OK** and the card(s) will be issued to the person.
- 8. (Optional) You can select the added card and click **Edit** or **Delete** to edit or delete the card.
- 9. (Optional) You can click **Link Fingerprint** to link the card with the person's fingerprint, so that the person can place the finger on the scanner instead of swiping card when passing the door.
- 10. Click **OK** to save the settings.

### Adding Person (Fingerprint)

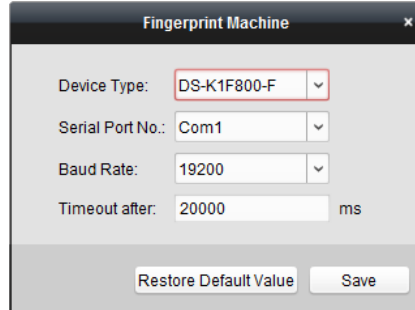
**Steps:**

1. In the Add Person interface, click **Fingerprint** tab.



2. Before inputting the fingerprint, you should connect the fingerprint machine to the PC and set its parameters first.

Click **Set Fingerprint Machine** to enter the following dialog box.



- 1) Select the device type.  
Currently, the supported fingerprint machine types include DS-K1F800-F, DS-K1F300-F, and DS-K1F810-F.
- 2) For fingerprint machine type DS-K1F800-F, you can set the serial port number, baud rate, and overtime parameters of the fingerprint machine.
- 3) Click **Save** button to save the settings.  
You can click **Restore Default Value** button to restore the default settings.

**Notes:**

- The serial port number should correspond to the serial port number of PC. You can check the serial port number in Device Manager in your PC.
- The baud rate should be set according to the external fingerprint card reader. The default value is 19200.
- **Timeout after** field refers to the valid fingerprint collecting time. If the user does not input

a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.

3. Click **Start** button, click to select the fingerprint to start collecting.
4. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.
5. Click **Stop** button can stop collecting.  
You can also click **Collect from Device** button and select the device to collect fingerprint. (The function should be supported by the device).
6. After collecting the fingerprint, click Card in the Add Person window to enter the Card tab.
7. Click **Link Fingerprint** to link the fingerprint to the card.  
You can select the registered fingerprint and click **Delete** to delete it.  
You can click **Clear** to clear all fingerprints.
8. Click **OK** to save the fingerprints.

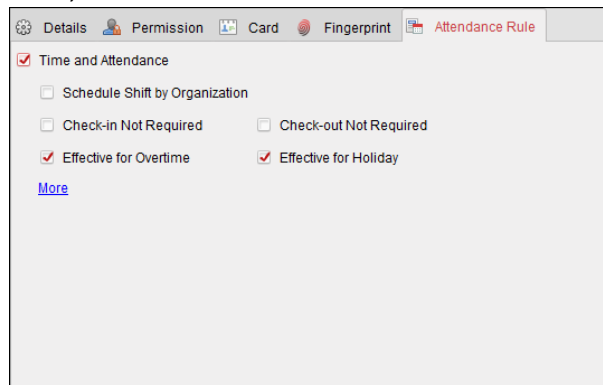
### Adding Person (Attendance Rule)

You can set the attendance rule for the person.

**Note:** This tab page will display when you select **Non-Residence** mode in the application scene when running the software for the first time.

#### Steps:

1. In the Add Person interface, click **Attendance Rule** tab.




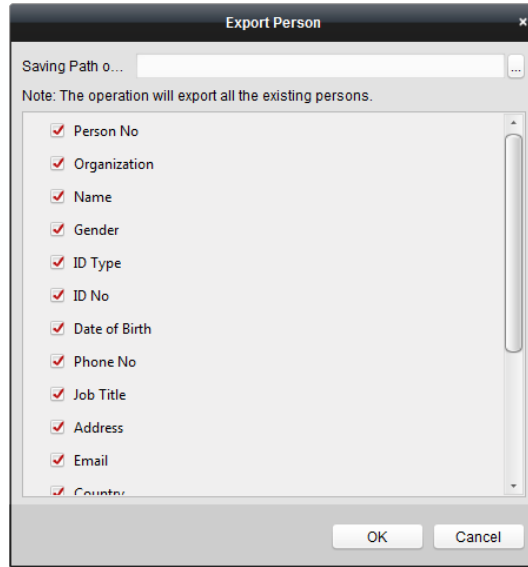
2. If the person joins in the time and attendance, check the **Time and Attendance** checkbox to enable this function for the person. Then the person's card swiping records will be recorded and analyzed for time and attendance.  
For details about Time and Attendance, click **More** to go to the Time and Attendance module.
3. Click **OK** to save the settings.

### Importing and Exporting Person Information

The person information can be imported and exported in batch.

#### Steps:

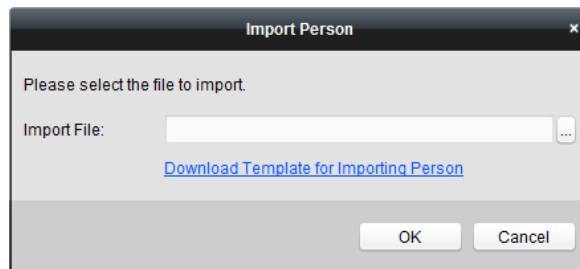
1. **Exporting Person:** You can export the added persons' information in Excel format to the local PC.
  - 1) After adding the person, you can click **Export Person** button in the Person and Card tab to pop up the following dialog.
  - 2) Click  to select the path of saving the exported Excel file.
  - 3) Check the checkboxes to select the person information to export.



4) Click **OK** to start exporting.

2. **Importing Person:** You can import the Excel file with persons information in batch from the local PC

1) click **Import Person** button in the Person and Card tab.



2) You can click **Download Template for Importing Person** to download the template first.

3) Input the person information to the downloaded template.

4) Click  to select the Excel file with person information.

5) Click **OK** to start importing.

### Getting Person Information from Access Control Device

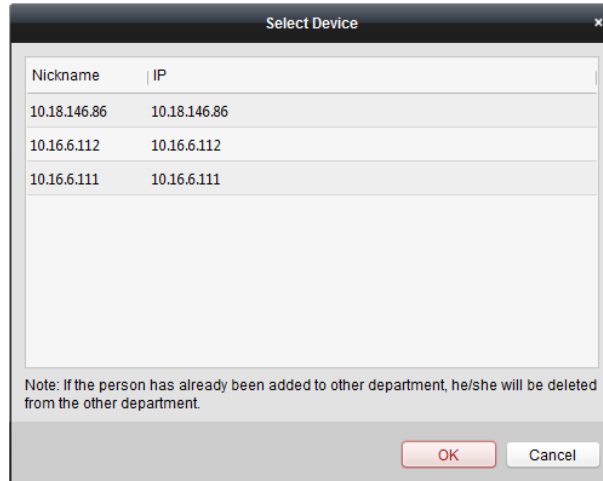
If the added access control device has been configured with person information (including person details, fingerprint, issued card information), you can get the person information from the device and import to the client for further operation.

**Note:** This function is only supported by the device the connection method of which is TCP/IP when adding the device.

**Steps:**

1. In the organization list on the left, click to select an organization to import the persons.
2. Click **Get Person** button to pop up the following dialog box.





- The added access control device will be displayed.
- Click to select the device and then click **OK** to start getting the person information from the device.

You can also double click the device name to start getting the person information.

**Notes:**

- The person information, including person details, person’s fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- Up to 10000 persons with up to 5 cards each can be imported.

**Managing Person**

**Modifying and Deleting Person**

To modify the person information and attendance rule, click or in the Operation column, or select the person and click **Modify** to open the editing person dialog.

You can click to view the person’s card swiping records.

To delete the person, select a person and click **Delete** to delete it.

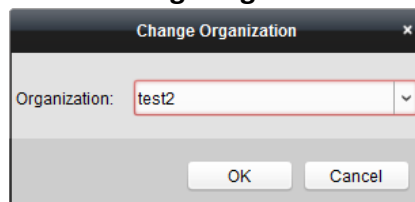
**Note:** If a card is issued to the current person, the linkage will be invalid after the person is deleted.

**Changing Person to Other Organization**

You can move the person to another organization if needed.

**Steps:**

- Select the person in the list and click **Change Organization** button.



- Select the organization to move the person to.
- Click **OK** to save the settings.

## Issuing Card in Batch

You can issue multiple cards for the person with no card issued in batch.

### Steps:

1. Click **Issue Card in Batch** button to enter the following dialog.

All the added person with no card issued will display in the Person(s) with No Card Issued list.

Person(s) with No Card Issued			Person(s) with Card Issued			
Person Name	Gender	Department	Person Name	Card No.	Gender	Departn
Wendy	Female	Department 1				
Cindy	Female	Department 1/Sub Depar...				

2. Select the card type according to actual needs.

**Note:** For details about the card type, refer to *Adding Person*.

3. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

**Note:** The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to *Chapter 7.8.2 Card Reader Authentication*.

4. Input the card quantity issued for each person.

For example, if the Card Quantity is 3, you can read or enter three card No. for each person.

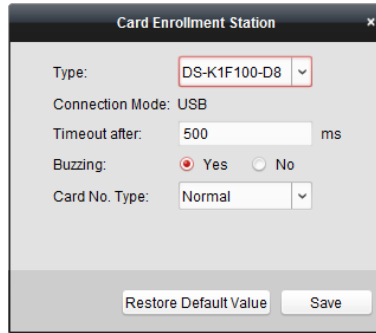
5. Click to set the effective time and expiry time of the card.

6. Select the Card Reader Mode for reading the card No.

- **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.

- **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.

**Note:** The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



- 1) Select the Card Enrollment Station type.

**Note:** Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

- 2) Set the parameters about the connected card enrollment station.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.

- 3) Click **Save** button to save the settings.

You can click **Restore Default Value** button to restore the defaults.

- **Manually Input:** Input the card No. and click **Enter** to input the card No.

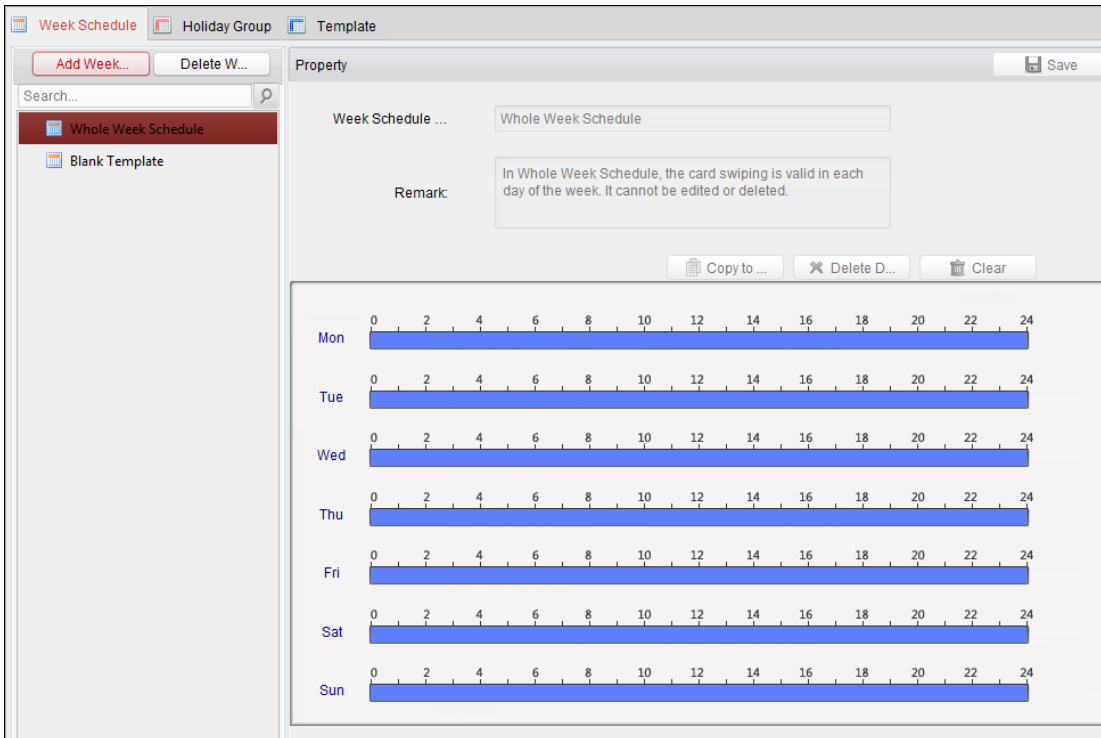
7. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.
8. Click **OK** to save the settings.

## 7.6 Schedule and Template

### **Purpose:**

You can configure the template including week schedule and holiday schedule. After setting the templates, you can adopt the configured templates to access control permissions when setting the permission, so that the access control permission will take effect in the time durations of the template.

Click  to enter the schedule and template interface.



You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, please refer to *Chapter 7.7 Permission Configuration*.

### 7.6.1 Week Schedule

Click **Week Schedule** tab to enter the Week Schedule Management interface.

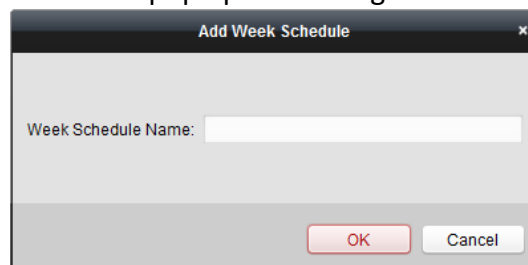
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

- **Whole Week Schedule:** Card swiping is valid on each day of the week.
- **Blank Schedule:** Card swiping is invalid on each day of the week.

You can perform the following steps to define custom schedules on your demand.

**Steps:**



1. Click **Add Week Schedule** button to pop up the adding schedule interface.



2. Input the name of week schedule and click **OK** button to add the week schedule.
3. Select the added week schedule in the schedule list and you can view its property on the right. You can edit the week schedule name and input the remark information.
4. On the week schedule, click and drag on a day to draw on the schedule, which means in that

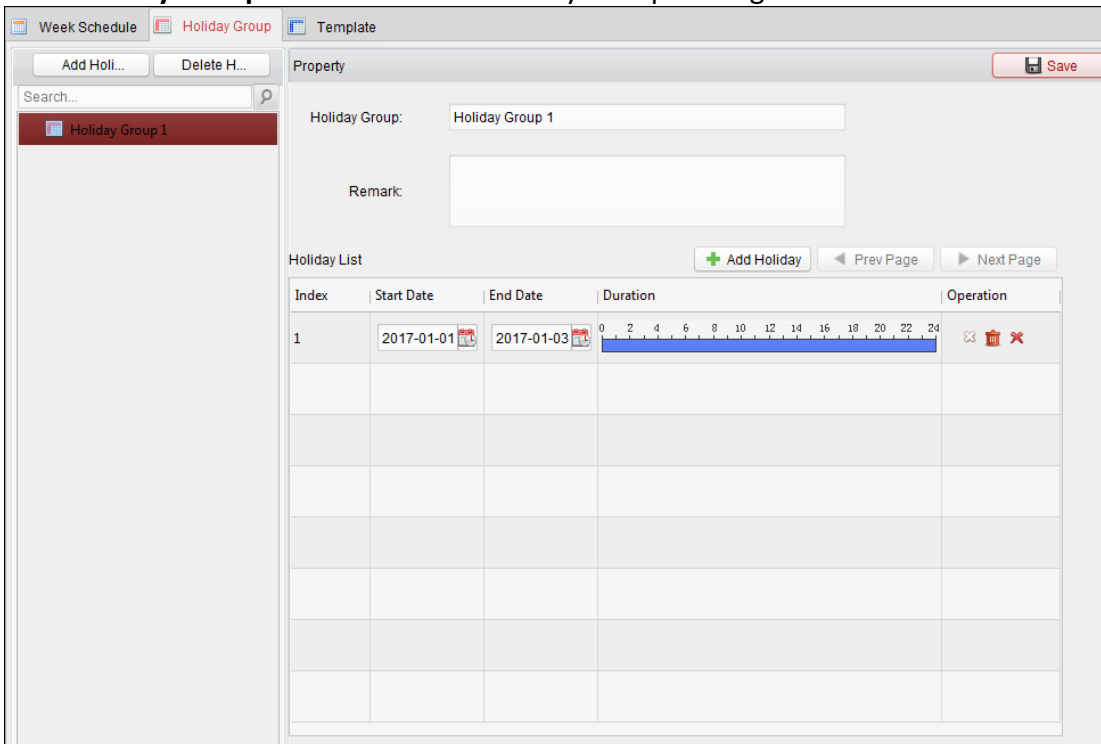
period of time, the configured permission is activated.

**Note:** Up to 8 time periods can be set for each day in the schedule.

5. When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.  
When the cursor turns to , you can lengthen or shorten the selected time bar.
6. Optionally, you can select the schedule time bar, and then click **Delete Duration** to delete the selected time bar, or click **Clear** to delete all the time bars, or click **Copy to Week** to copy the time bar settings to the whole week.
7. Click **Save** to save the settings.

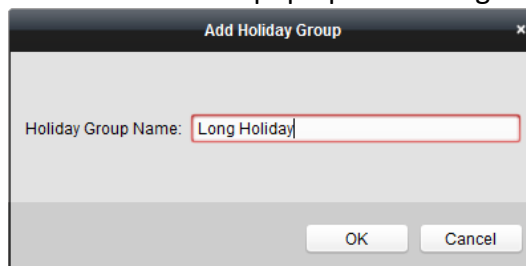
## 7.6.2 Holiday Group

Click **Holiday Group** tab to enter the Holiday Group Management interface.



### Steps:

1. Click **Add Holiday Group** button on the left to pop up the adding holiday group interface.

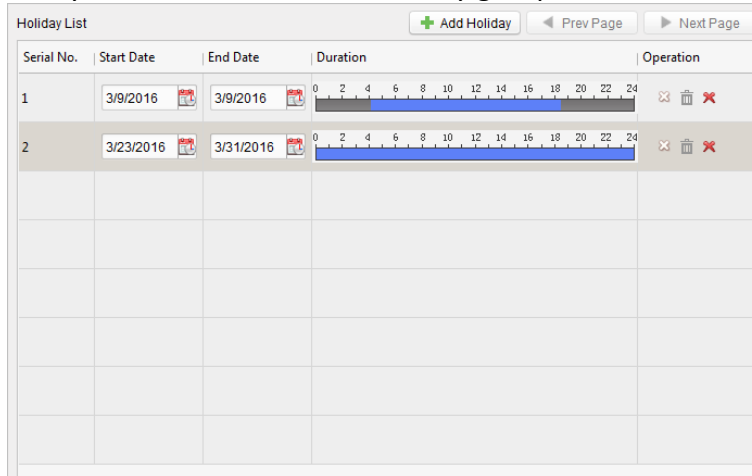


2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.
3. Select the added holiday group and you can edit the holiday group name and input the remark

information.






- Click **Add Holiday** icon on the right to add a holiday period to the holiday list and configure the duration of the holiday.

**Note:** Up to 16 holidays can be added to one holiday group.



- On the period schedule, click and drag to draw the period, which means in that period of time, the configured permission is activated.

**Note:** Up to 8 time durations can be set for each period in the schedule.

- When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
- When the cursor turns to , you can lengthen or shorten the selected time bar.
- Optionally, you can select the schedule time bar, and then click  to delete the selected time bar, or click  to delete all the time bars of the holiday, or click  to delete the holiday directly.

- Click **Save** to save the settings.

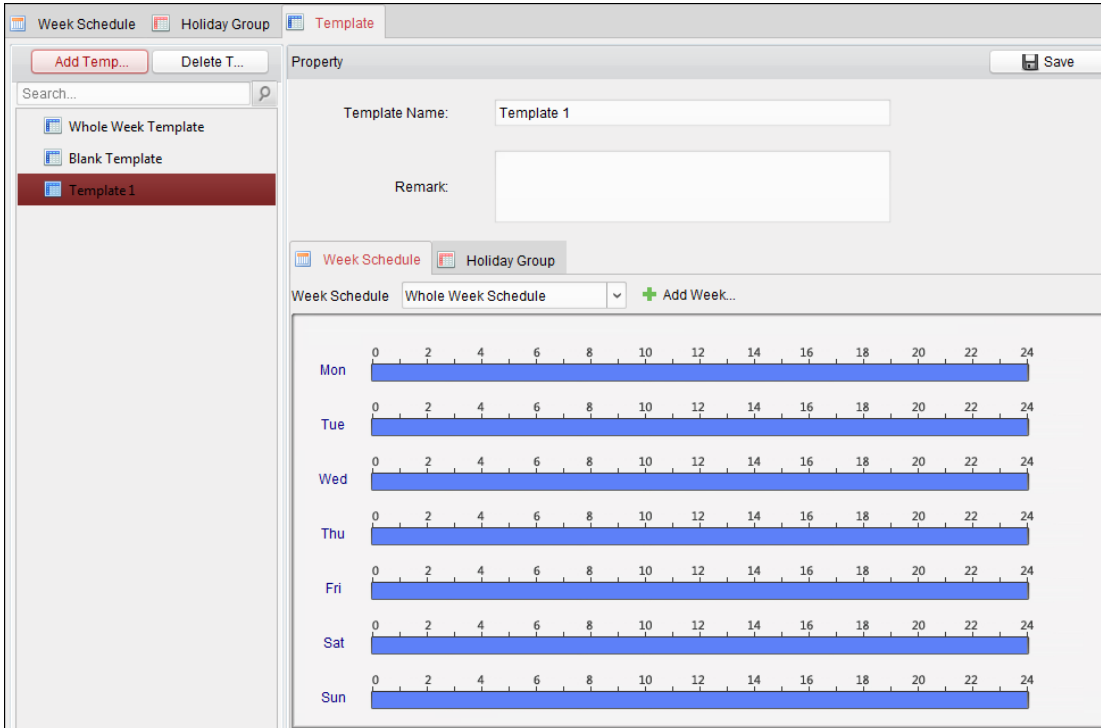
**Note:** The holidays cannot be overlapped with each other.

### 7.6.3 Template

After setting the week schedule and holiday group, you can configure the template which contains week schedule and holiday group schedule.

**Note:** The priority of holiday group schedule is higher than the week schedule.

Click **Template** tab to enter the Template Management interface.



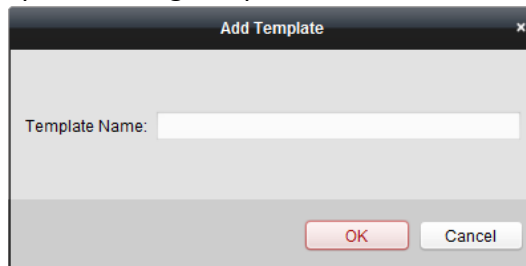
There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

- **Whole Week Template:** The card swiping is valid on each day of the week and it has no holiday group schedule.
- **Blank Template:** The card swiping is invalid on each day of the week and it has no holiday group schedule.

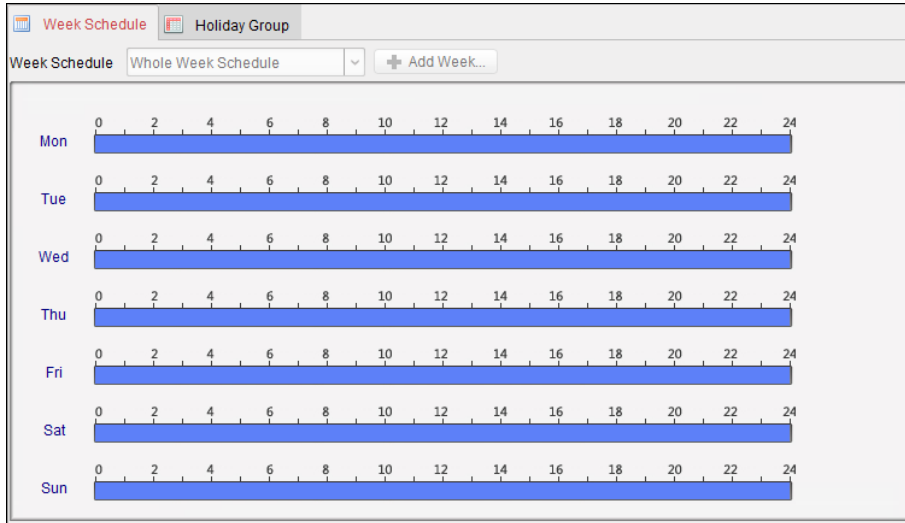
You can define custom templates on your demand.

**Steps:**

1. Click **Add Template** to pop up the adding template interface.

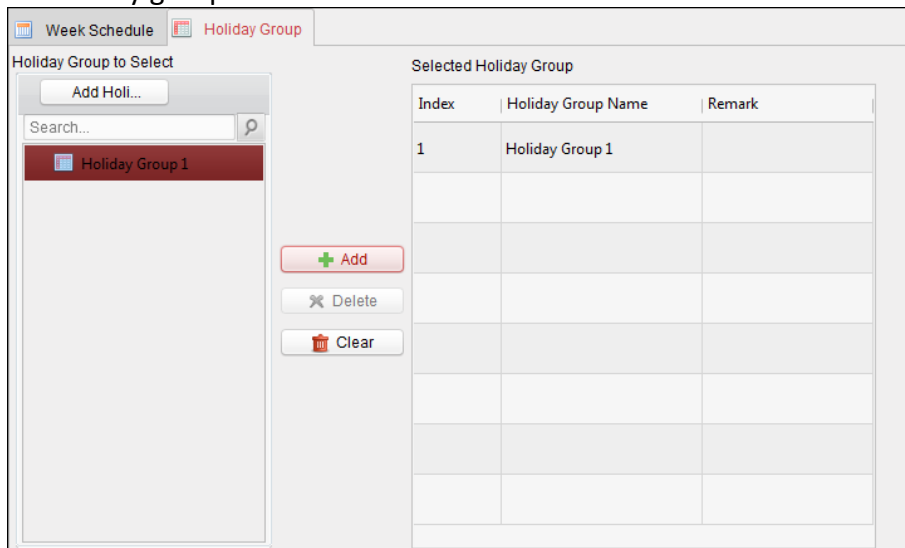


2. Input the template name in the text field and click **OK** button to add the template.
3. Select the added template and you can edit its property on the right. You can edit the template name and input the remark information.
4. Select a week schedule to apply to the schedule.  
Click **Week Schedule** tab and select a schedule in the dropdown list.  
You can also click **Add Week Schedule** to add a new week schedule. For details, refer to *Chapter 7.6.1 Week Schedule*.



5. Select holiday groups to apply to the schedule.

**Note:** Up to 4 holiday groups can be added.




Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one. For details, refer to *Chapter 7.6.2 Holiday Group*. You can click to select an added holiday group in the right-side list and click **Delete** to delete it. You can click **Clear** to delete all the added holiday groups.

6. Click **Save** button to save the settings.

## 7.7 Permission Configuration

In Permission Configuration module, you can add, edit, and delete the access control permission, and then apply the permission settings to the device to take effect.

Click  icon to enter the Access Control Permission interface.



Permission Name	Template	Person	Door	Details	Status
Door 2 Permissi...	Whole Week Te...	Wendy	Door Station	<a href="#">Details</a>	Not Applied
Door 1 Permissi...	Whole Week Te...	Wendy,Yining	Door1_10.16.6.1...	<a href="#">Details</a>	Applying failed

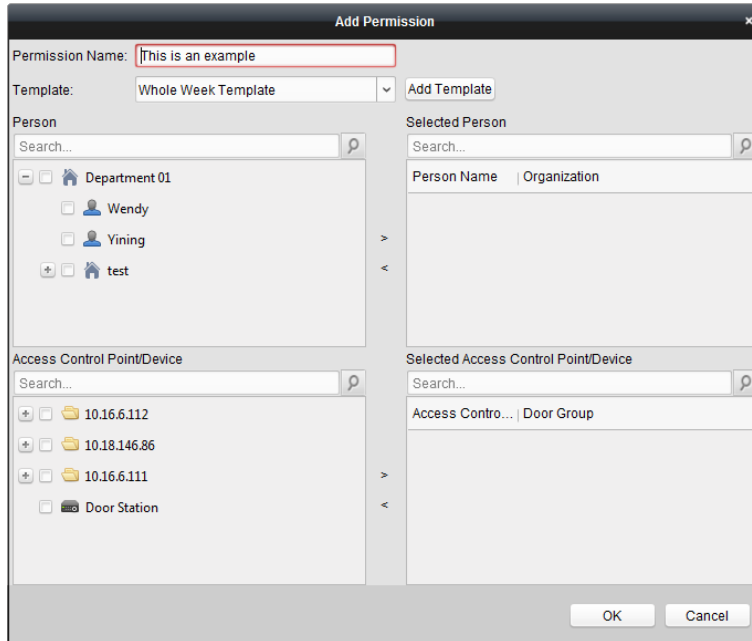
### 7.7.1 Adding Permission

**Purpose:**

You can assign permission for persons to enter/exist the access control points (doors) in this section.

**Steps:**

1. Click **Add** icon to enter following interface.



2. In the Permission Name field, input the name for the permission as desired.
3. Click on the dropdown menu to select a template for the permission.
 

**Note:** You should configure the template before permission settings. You can click **Add Template** button to add the template. Refer to *Chapter 7.6 Schedule and Template* for details.
4. In the Person list, all the added persons display. Check the checkbox(es) to select person(s) and click > to add to the Selected Person list. (Optional) You can select the person in Selected Person list and click < to cancel the selection.
5. In the Access Control Point/Device list, all the added access control points (doors) and door stations will display. Check the checkbox(es) to select door(s) or door station(s) and click > to add to the selected list. (Optional) You can select the door or door station in the selected list and click < to cancel the selection.
6. Click **OK** button to complete the permission adding. The selected person will have the

permission to enter/exit the selected door/door station with their linked card(s) or fingerprints.

- (Optional) after adding the permission, you can click **Details** to modify it. Or you can select the permission and click **Modify** to modify.

You can select the added permission in the list and click **Delete** to delete it.

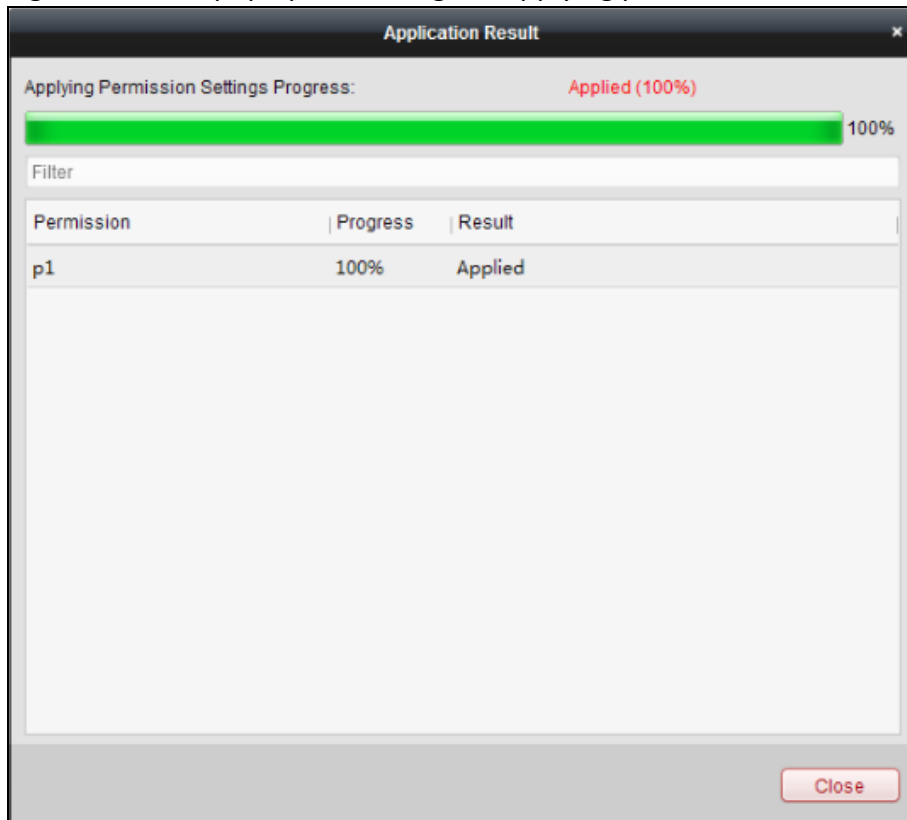
### 7.7.2 Applying Permission

**Purpose:**

After configuring the permissions, you should apply the added permission to the access control device to take effect.

**Steps:**

- Select the permission(s) to apply to the access control device. To select multiple permissions, you can hold the *Ctrl* or *Shift* key and select permissions.
- Click **Apply to Device** to start applying the selected permission(s) to the access control device or door station.
- The following window will pop up, indicating the applying permission result.




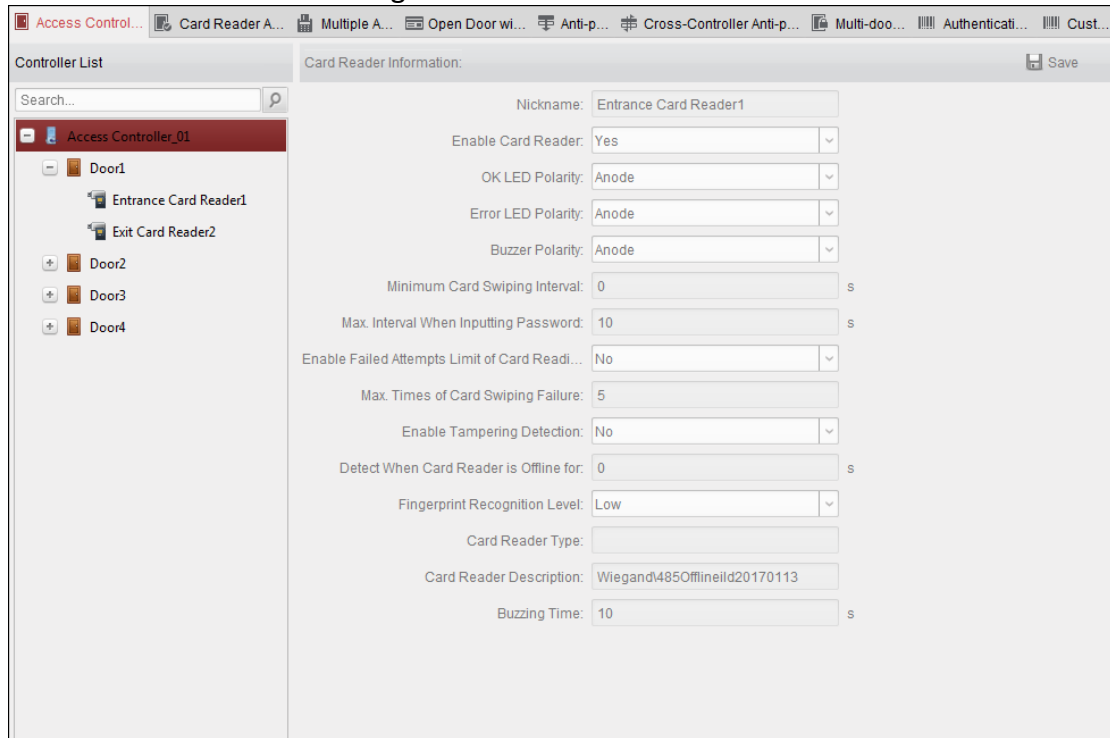
## 7.8 Advanced Functions

**Purpose:**

After configuring the person, template, and access control permission, you can configure the advanced functions of access control application, such as access control parameters, authentication password, and opening door with first card, anti-passing back, etc.

**Note:** The advanced functions should be supported by the device.

Click  icon to enter the following interface.



## 7.8.1 Access Control Parameters


### **Purpose:**

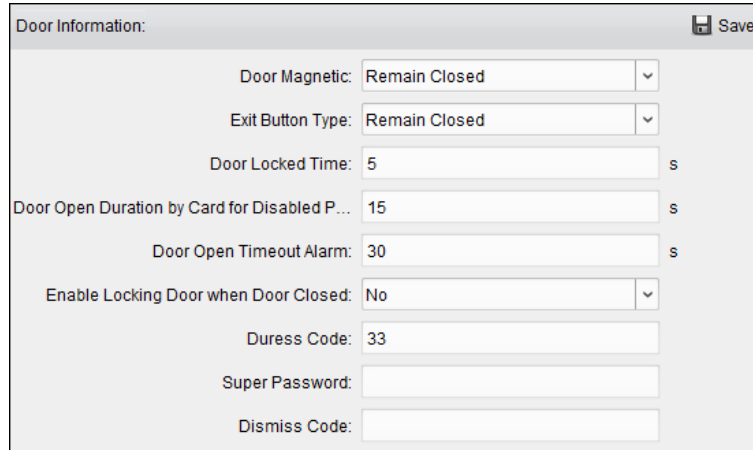
After adding the access control device, you can configure its access control point (door)'s parameters, and its card readers' parameters.

Click **Access Control Parameters** tab to enter the parameters settings interface.

### **Door Parameters**

#### **Steps:**

1. In the controller list on the left, click  to expand the access control device, select the door (access control point) and you can edit the information of the selected door on the right.



2. You can editing the following parameters:

**Door Magnetic:** The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).

**Exit Button Type:** The Exit Button Type is in the status of **Remain Open** (excluding special conditions).

**Door Locked Time:** After swiping the normal card and relay action, the timer for locking the door starts working.

**Door Open Duration by Card for Disabled Person:** The door magnetic can be enabled with appropriate delay after disabled person swipes the card.

**Door Open Timeout Alarm:** The alarm can be triggered if the door has not been close

**Enable Locking Door when Door Closed:** The door can be locked once it is closed even if the Door Locked Time is not reached.

**Duress Code:** The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

**Super Password:** The specific person can open the door by inputting the super password.

**Dismiss Code:** Input the dismiss code to stop the buzzer of the card reader.


**Notes:**

- The duress code, Super password, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The duress code, super password, and the dismiss code should contain 4 to 8 numerics.

3. Click **Save** button to save parameters.

### Card Reader Parameters

**Steps:**

1. In the device list on the left, click  to expand the door, select the card reader name and you can edit the card reader parameters on the right.

2. You can editing the following parameters:

**Nickname:** Edit the card reader name as desired.

**Enable Card Reader:** Select **Yes** to enable the card reader.

**OK LED Polarity:** Select the OK LED Polarity of the card reader mainboard.

**Error LED Polarity:** Select the Error LED Polarity of the card reader mainboard.

**Buzzer Polarity:** Select the Buzzer LED Polarity of the card reader mainboard.

**Minimum Card Swiping Interval:** If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

**Max. Interval When Inputting Password:** When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

**Enable Failed Attempts Limit of Card Reading:** Enable to report alarm when the card reading attempts reach the set value.

**Max. Times of Card Swiping Failure:** Set the max. failure attempts of reading card.

**Enable Tampering Detection:** Enable the anti-tamper detection for the card reader.

**Detect When Card Reader is Offline for:** When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

**Fingerprint Recognition Level:** Select the fingerprint recognition level in the dropdown list. By default, the level is Low.

**Card Reader Type:** Read the card reader's type.

**Card Reader Description:** Read the card reader description.

**Buzzing Time:** Set the card reader buzzing time. The available time ranges from 0 to 5999s. 0 represents continuous buzzing.

3. Click the **Save** button to save parameters.

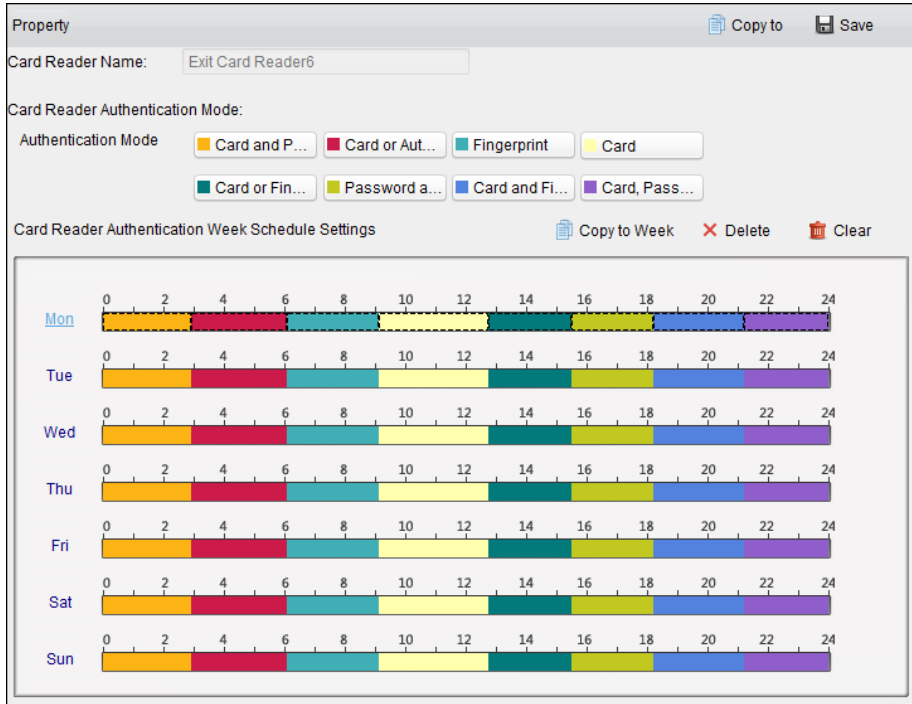
## 7.8.2 Card Reader Authentication

### **Purpose:**

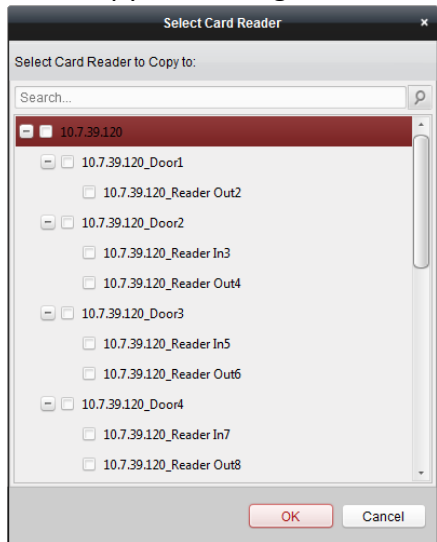
You can set the passing rules for the card reader of the access control device.

### **Steps:**

1. Click **Card Reader Authentication** tab and select a card reader on the left.
2. Select a card reader authentication mode. The available authentication modes depend on the card reader type:
  - **Card and Password:** The door can open by both inputting the card password and swiping the card.  
*Note:* Here the password refers to the password set when issuing the card to the person. Refer to *Chapter 7.5.2 Person Management*.
  - **Card or Authentication Password:** The door can open by inputting the authentication password or swiping the card.  
*Note:* Here the authentication password refers to the password set to open the door. Refer to *Chapter 7.8.8 Authentication Password*.
  - **Fingerprint:** The door can open by only inputting the fingerprint.
  - **Card:** The door can open by only swiping the card.
  - **Card or Fingerprint:** The door can open by inputting the fingerprint or swiping the card.
  - **Password and Fingerprint:** The door can open by both inputting the card password and inputting the fingerprint.  
*Note:* Here the password refers to the card password set when issuing the card to the person. Refer to *Chapter 7.5.2 Person Management*.
  - **Card and Fingerprint:** The door can open by both inputting the fingerprint and swiping the card.
  - **Card, Password and Fingerprint:** The door can open by both inputting the fingerprint, inputting the card password, and swiping the card.  
*Note:* Here the password refers to the card password set when issuing the card to the person. Refer to *Chapter 7.5.2 Person Management*.
3. Click and drag your mouse on a day to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.



4. Repeat the above step to set other time periods.  
 Or you can select a configured day and click **Copy to Week** button to copy the same settings to the whole week.  
 (Optional) You can click **Delete** button to delete the selected time period or click **Clear** button to delete all the configured time periods.
5. (Optional) Click **Copy to** button to copy the settings to other card readers.



6. Click **Save** button to save parameters.

### 7.8.3 Multiple Authentication

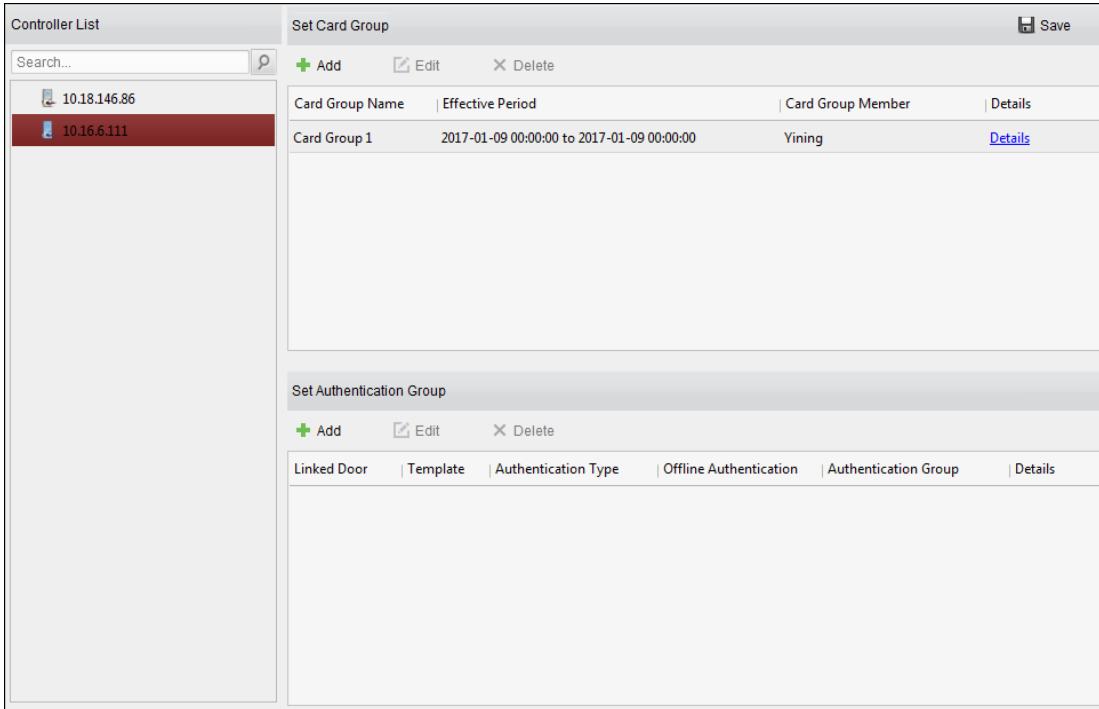
**Purpose:**

You can manage the cards by group and set the authentication for multiple cards for one access control point (door).

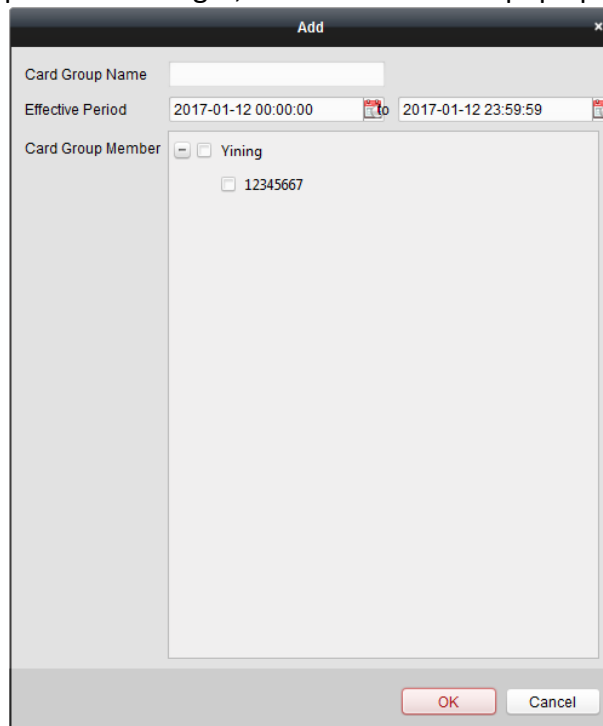
**Note:** Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration*.

**Steps:**


1. Click **Multiple Authentication** tab to enter the following interface.

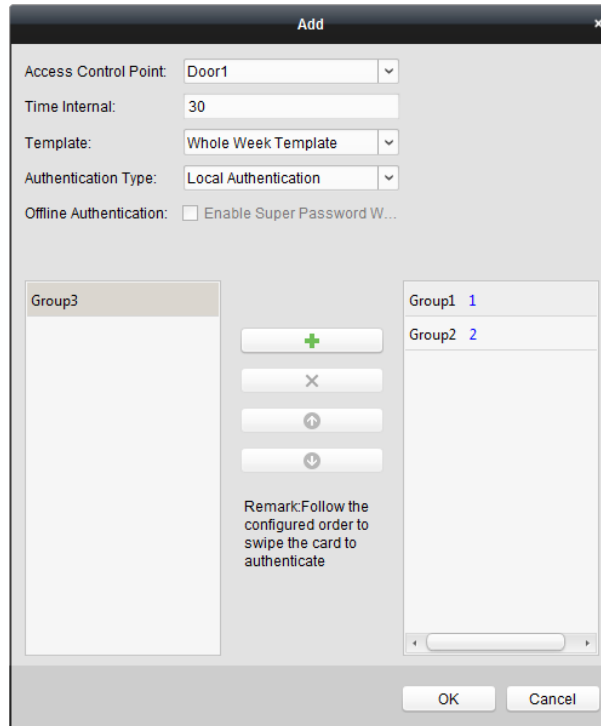






2. Select access control device from the list on the left.
3. In the Set Card Group panel on the right, click **Add** button to pop up the following dialog:





- 1) In the Card Group Name field, input the name for the group as desired.
  - 2) Click  to set the effective time and expiry time of the card group.
  - 3) Check the checkbox(es) to select the card(s) to add the card group.
  - 4) Click **OK** to save the card group.
4. In the Set Authentication Group panel on the left, click **Add** to pop up the following dialog.



- 1) Select the access control point (door) of the device for multiple authentication.
- 2) Input the time interval for card swiping.
- 3) Select the template of the authentication group from the dropdown list. For details about setting the template, refer to *Chapter 7.6 Schedule and Template*.
- 4) Select the authentication type of the authentication group from the dropdown list.
  - **Local Authentication:** Authentication by the access control device.
  - **Local Authentication and Remotely Open Door:** Authentication by the access control device and by the client.  
For Local Authentication and Remotely Open Door type, you can check the checkbox to enable the super password authentication when the access control device is disconnected with the client.
  - **Local Authentication and Super Password:** Authentication by the access control device and by the super password.
- 5) In the list on the left, the added card group will display. You can click the card group and click  to add the group to the authentication group.  
You can click the added card group and click  to remove it from the authentication group.  
You can also click  or  to set the card swiping order.
- 5) Input the **Card Swiping Times** for the selected card group.

**Notes:**

- The Card Swiping Times should be larger than 0 and smaller than the added card quantity in the card group.
- The upper limit of Card Swiping Times is 16.

6) Click **OK** to save the settings.

5. Click **Save** to save and take effect of the new settings.

**Notes:**

- For each access control point (door), up to four authentication groups can be added.
- For the authentication group which certificate type is **Local Authentication**, up to 8 card groups can be added to the authentication group.
- For the authentication group which certificate type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 card groups can be added to the authentication group.

### 7.8.4 Open Door with First Card

**Purpose:**

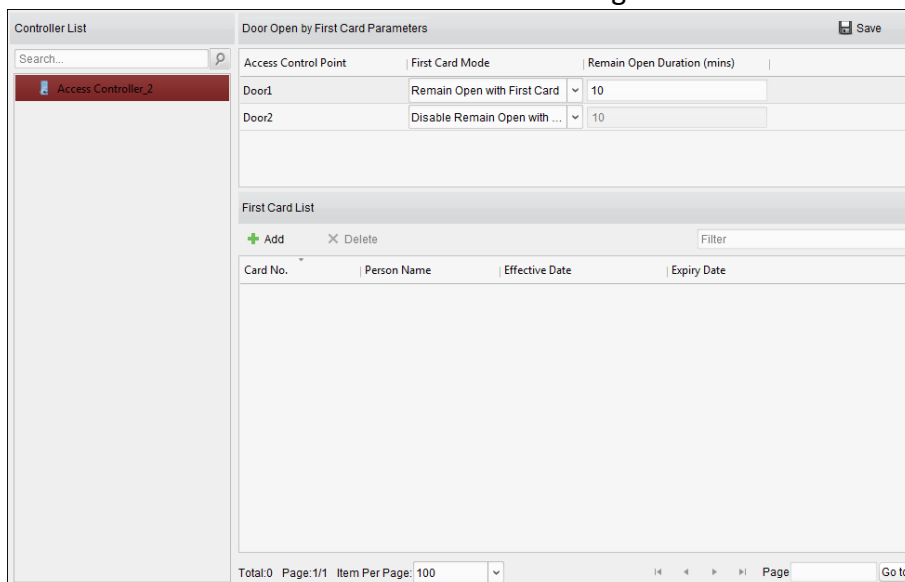
You can set multiple first cards for one access control point. After the first card swiping, it allows multiple persons access the door or other authentication actions. The first card mode contains Remain Open with First Card, Disable Remain Open with First Card, and First Card Authorization.

**Remain Open with First Card:** The door remains open for the configured time duration after the first card swiping until the remain open duration ends.

**First Card Authorization:** All authentications, except for the authentications of super card, duress card, and duress code, are allowed only after the first card authorization.

**Steps:**

1. Click **Open Door with First Card** tab to enter the following interface.

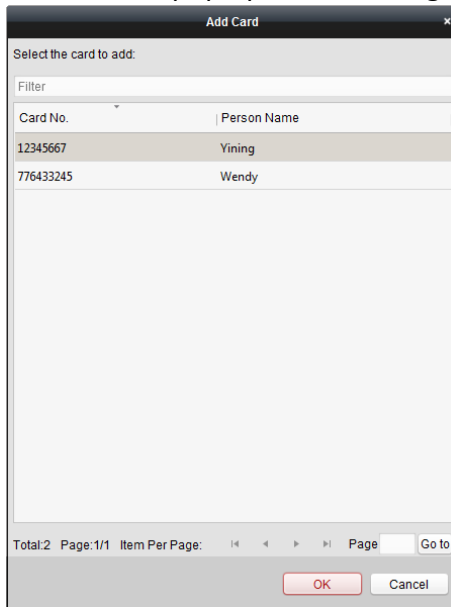


2. Select an access control device from the list on the left.
3. Select the first card mode in the drop-down list for the access control point.
4. (Optional) If you select Remain Open with First Card, you should set remain open duration.

**Notes:**

- The Remain Open Duration should be between 0 and 1440 minutes. By default, it is 10 minutes.
- In the First Card Authorization mode, you can access the door when swiping the super card, the duress card or input the duress code without swiping the first card.
- You can swipe the first card again to disable the first card mode.
- The first card authorization is effective only on the current day. The authorization will be expired after 24:00 on the current day.

5. In the First Card list, Click **Add** button to pop up the following dialog box.



1) Select the cards to add as first card for the door

**Note:** Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration*.

2) Click **OK** button to save adding the card.

6. You can click **Delete** button to remove the card from the first card list.

7. Click **Save** to save and take effect of the new settings.

### 7.8.5 Anti-Passing Back

**Purpose:**

You can set anti-passing back for card readers in the same access controller. You should swipe the card according to the configured swiping card route. And only one person could pass the access control point after swiping the card.

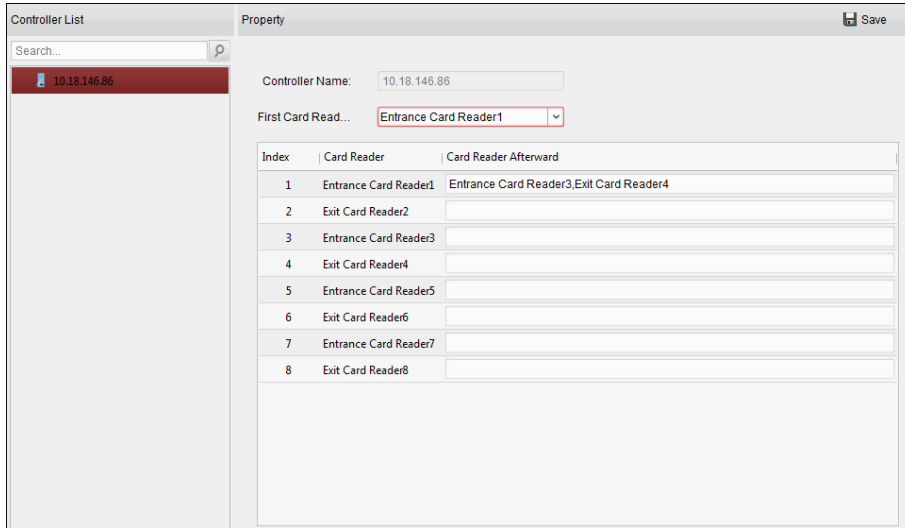
**Notes:**

- Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time.
- You should enable the anti-passing back function on the access control device first.

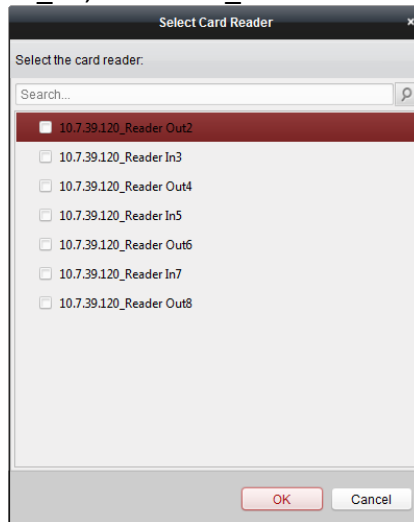
### Setting the Path of Swiping Card (Card Reader Order)

**Steps:**

1. Click **Anti-passing Back** tab to enter the following interface.



2. Select an access control device from the device list on the left.
3. In the First Card Reader field, select the card reader as the beginning of the path.
4. In the list, click the text filed of **Card Reader Afterward** and select the linked card readers.  
**Example:** If you select Reader In\_01 as the beginning, and select Reader In\_02, Reader Out\_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In\_01, Reader In\_02 and Reader Out\_04.



**Note:** Up to four afterward card readers can be added for one card reader.

5. (Optional) You can enter the Select Card Reader dialog box again to edit its afterward card readers.
6. Click **Save** to save and take effect of the new settings.

### 7.8.6 Cross-Controller Anti-passing Back

**Purpose:**

You can set anti-passing back for card readers in multiple access controllers. You should swipe the

card according to the configured swiping card route. And only one person could pass the access control point after swiping the card.

Click **Cross-Controller Anti-passing Back** to enter the Cross-Controller Anti-passing Back tab.

## Setting Route Anti-passing Back

### **Purpose:**


The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards.

### **Steps:**

1. Check the **Enable Cross-Controller Anti-passing Back** checkbox to enable the function.
2. Set the anti-passing back parameters.

#### ➤ **Based on Card**

**Note:** The system will judge the anti-passing back according to the entrance and exit records on the card.


- 1) Select **Based on Card** as the anti-passing back mode in the drop-down list.
- 2) Select Route Anti-passing Back as the rule.
- 3) Set the sector ID.
- 4) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
- 5) In the Set Card Reader area, click the icon on the left of the card enrollment station column to select the first card reader. The icon will turn to .
- 6) Click the card reader afterward input field to select the card readers afterward in the pop-up window.
- 7) Check the checkbox in the Enable Anti-passing Back column to enable the anti-passing back function.

**Notes:**

- The displayed card readers in the card reader afterward input field should be in authentication order.
- Up to 64 controllers with anti-passing back function can be added.
- Up to 16 card readers afterward can be added for each card reader.
- It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to *7.4.8 M1 Card Encryption*.

➤ **Based on Network**

**Note:** Authenticate the anti-passing back according to the entrance and exit information on the card reader.

- 1) Select **Based on Network** as the anti-passing back mode in the drop-down list.
- 2) Select Route Anti-passing Back as the rule.
- 3) Select a server in the drop-down list for judging the anti-passing back.
- 4) (Optional) You can click **Delete Anti-passing Back Record** and select the card in the pop-up window to delete the card swiping information in all devices. The user should be start swiping card again from the first card reader.
- 5) In the Set Card Reader area, click the icon on the left of the card enrollment station column to select the first card reader. The icon will turn to .
- 6) Click the card reader afterward input field to select the card readers afterward in the pop-up window.
- 7) Check the checkbox in the Enable Anti-passing Back column to enable the anti-passing back function.

**Notes:**

- The displayed card readers in the card reader afterward input field should be in authentication order.
- Up to 64 controllers with anti-passing back function can be added.
- Up to 16 card readers afterward can be added for each card reader.
- Up to 5000 cards' swiping records can be stored in the selected server.

## Setting Entrance/Exit Anti-passing Back

**Purpose:**

You can set the entrance card reader and the exit card readers only for entering and exiting, without setting the first card reader and the card readers afterwards.

**Steps:**

1. In the Cross-Controller Anti-passing Back tab, check the **Enable Cross-Controller Anti-passing Back** checkbox to enable the function.
2. Set the anti-passing back parameters.

➤ **Based on Card**

**Note:** The system will judge the anti-passing back according to the entrance and exit records on the card.

- 1) Select **Based on Card** as the anti-passing back mode in the drop-down list.
- 2) Select Entrance/Exit Anti-passing Back as the rule.

- 3) Set the sector ID.
- 4) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
- 5) In the Set Card Reader area, check the checkboxes in the Enable Anti-passing Back column to select the entrance card reader and the exit card reader.
- 6) Click **Save** to save the settings.

**Notes:**

- Up to one entrance carder and one exit card reader should be checked.
- Up to 64 controllers with anti-passing back function can be added.
- It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to *7.4.8 M1 Card Encryption*.

➤ **Based on Network**

**Note:** Authenticate the anti-passing back according to the entrance and exit information on the card reader.

- 1) Select **Based on Network** as the anti-passing back mode in the drop-down list.
- 2) Select Entrance/Exit Anti-passing Back as the rule.
- 3) Select the server in the dropdown list for judging the anti-passing back.
- 4) (Optional) You can click **Delete Record** and select the card in the pop-up window to delete the card swiping information in all devices.
- 5) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
- 6) In the Set Card Reader area, check the checkboxes in the Enable Anti-passing Back column to select the entrance card reader and the exit card reader.
- 7) Click **Save** to save the settings.

**Notes:**

- Up to one entrance carder and one exit card reader should be checked.
- Up to 64 controllers with anti-passing back function can be added.
- Up to 5000 cards' swiping records can be stored in the selected server.

## 7.8.7 Multi-door Interlocking

**Purpose:**

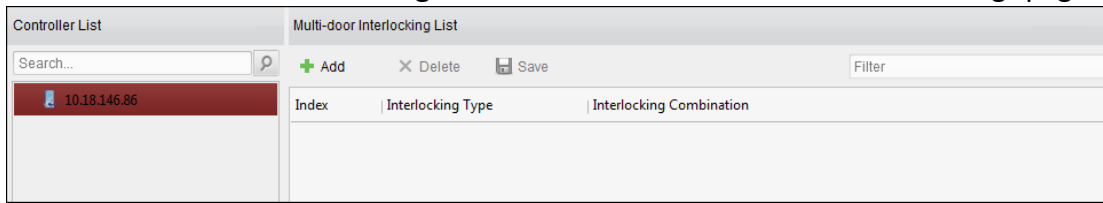
You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

**Notes:**

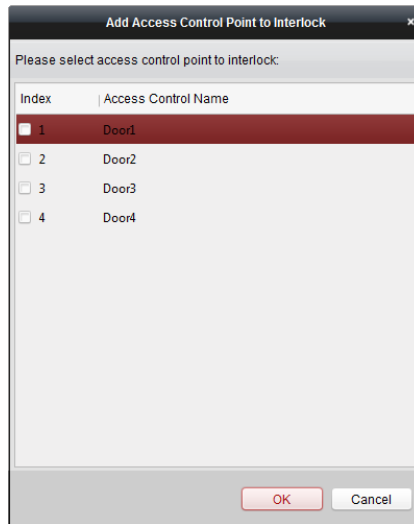
- The Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time.

**Steps:**

1. Click **Multi-door Interlocking** tab to enter the multi-door interlock settings page.



2. Select an access controller from the Controller List.
3. Click **Add** to pop up the Add Access Control Point to Interlock interface.



4. Select the access control point (door) from the list.
 

**Note:** Up to four doors can be added in one multi-door interlocking combination.
5. Click **OK** to save the adding.
6. (Optional) After adding the multi-door interlocking combination, you can select it from the list and click **Delete** to delete the combination.
7. Click **Save** button to save and take effect.

### 7.8.8 Authentication Password

**Purpose:**

You can open the door by inputting the authentication password on the card reader keypad after finishing the operation of setting authentication password.

**Notes:**

- This authentication password function is only valid during the schedules when the card reader authentication mode for the access control device is set as **Card or Authentication Password**. For details, please refer to *Chapter 7.8.2 Card Reader Authentication*.
- This function should be supported by the access control device.

**Steps:**

1. Click **Authentication Password** tab and select an access control device from the list.



Controller List	Card List		Save
Search...			Filter
10.18.146.86	Card No.	Person Name	Password
	999	999	Please input the authentication password.
	776433245	Wendy	9638
	12345667	Yining	8527

All the cards and persons which have been applied to the device will be displayed.

**Note:** For setting and applying the permissions to the device, refer to *Chapter 7.7 Permission Configuration*.

2. Click the **Password** field of the card and input the authentication password for the card.

**Note:** The authentication password should contain 4 to 8 digits.

3. After setting the authentication password, the authentication password function of the card will be enabled by default.
4. (Optional) You can input the keywords of card No., person name, or authentication password to search.

**Notes:**

- Up to 500 cards with authentication password can be added to one access control device.
- The password should be unique and cannot be the same with super password, duress code, and dismiss code in the access control parameters.

### 7.8.9 Custom Wiegand

**Purpose:**

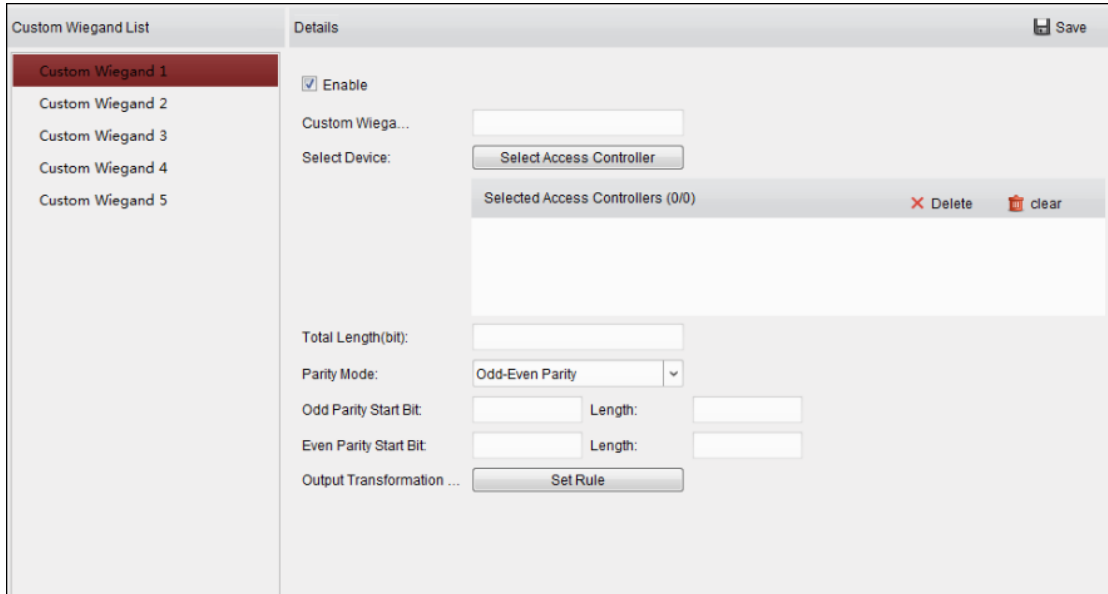
Based on the knowledge of uploading rule for the third party wiegand, you can set multiple customized wiegand protocols to communicate between the controller and the third party card readers.

**Before you start:**

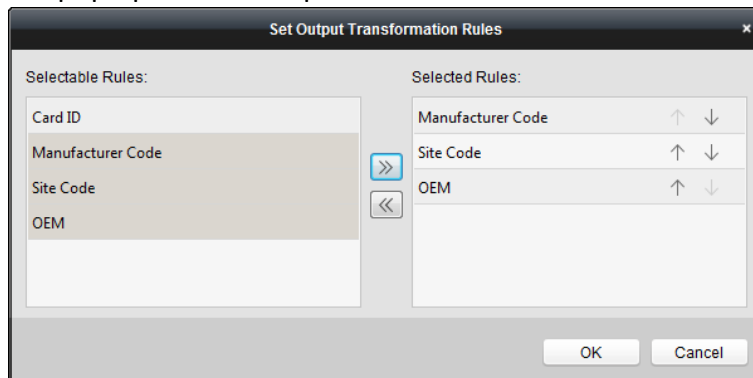
Wire the third party card readers to the controller.


**Steps:**




1. Click **Custom Wiegand** to enter the Custom Wiegand tab.



2. Select a custom wiegand on the left of the interface.
3. Check **Enable** checkbox to enable the custom wiegand.
4. Set the wiegand name.
5. Select device.
  - 1) Click **Select Device**.
  - 2) Select the device need to use custom wiegand.
  - 3) Click **OK** to save the settings.
6. Input the Total Length and select the parity mode in the drop-down list.  
 If you select Odd-Even Parity, you should set the odd parity start bit, the odd parity length, the even parity start bit and the even parity length.  
 If you select XOR Parity, you should set the XOR parity start bit, length per group and total length.  
 If you select None, you are no need to set the parity mode.
7. Set output transformation rule.
  - 1) Click **Set Rule** to pop up the Set Output Transformation Rules window.



- 2) Select rules on the left list.  
**Note:** Press the *Shift* key to select multiple rules.
- 3) Click  to move the selected rules to the right list.

- 4) (Optional) Click  or  to change the rule order.
  - 5) (Optional) Select the rules in the Selected Rule list and click  to remove the rule from the list on the right.
  - 6) Click **OK** to save the settings.
  - 7) In the Custom Wiegand tab, set the rule start bit, length, and the decimal digit.
8. Click **Save** at the upper right corner of the interface to save the settings.


**Notes:**

- By default, the device disables the custom wiegand function.
- If the device enables the custom wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom wiegands can be set.
- Up to 32 characters are allowed in the custom wiegand name.
- Up to 80 bits are available in the total length.
- The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
- The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
- For details about the custom wiegand, see Appendix.

## 7.9 Searching Access Control Event

**Purpose:**

You can search the access control history events including device exception event, door event, alarm input, and card reader event.

Click  icon and click Access Control Event tab to enter the following interface.

The screenshot shows a web-based interface for searching access control events. At the top, there are tabs for 'Access Control Event', 'Call Log', 'Unlocking Log', and 'Notice'. Below the tabs, there are search filters: 'Source' (radio buttons for Client and Device), 'Device' (dropdown), 'Event Type' (dropdown), 'Card Holder Name' (dropdown), 'Card No.' (dropdown), 'Card Reader Type' (dropdown), 'Start Time' (datetime picker), and 'End Time' (datetime picker). A 'Search' button is positioned to the right of the time pickers. To the right of the search filters is a 'Card Holder Information' panel with a placeholder for a photo and several input fields for personal details. Below the search filters is a 'Search Result' section with an 'Export' button and a table with columns for Serial No., Event Type, Card Holder, Card Reader, Card Type, Card No., Event Time, and Event S. At the bottom, there is a pagination bar showing 'Total:0 Page:1/1' and navigation buttons.

**Steps:**


1. Select the source.  
You can select Client or Device.
2. Enter the search condition (source, event type/card holder name/card No./capture/start & end time).
3. Click **Search** to get the search results.
4. View the event information in the event list.
5. Click an event to view the information of the card holder on the **Card Holder Information** panel on the left side of the page.
6. You can click **Export** button to export the search results to the local PC.

## 7.10 Access Control Event Configuration

**Purpose:**

For the added access control device, you can configure its access control linkage including access control event linkage, access control alarm input linkage, event card linkage, and cross-device linkage.



Click the  icon on the control panel, or click **Tool->Event Management** to open the Event Management page.

### 7.10.1 Access Control Event Linkage

**Purpose:**

You can assign linkage actions to the access control event by setting up a rule. For example, when the access control event is detected, an audible warning appears or other linkage actions happen.

**Note:** The linkage here refers to the linkage of the client software’s own actions.

**Steps:**

1. Click the **Access Control Event** tab.
2. The added access control devices will display in the Access Control Device panel on the left. Select the access control device, or alarm input, or access control point (door), or card reader to configure the event linkage.
3. Select the event type to set the linkage.
4. Select the triggered camera. The image or video from the triggered camera will pop up when the selected event occurs.  
To capture the picture of the triggered camera when the selected event occurs, you can also set the capture schedule and the storage in Storage Schedule.
5. Check the checkboxes to activate the linkage actions. For details, refer to *Table 14.1 Linkage Actions for Access Control Event*.
6. Click **Save** to save the settings.
7. You can click Copy to button to copy the access control event to other access control device, alarm input, access control point, or card reader.  
Select the parameters for copy, select the target to copy to, and click **OK** to confirm.

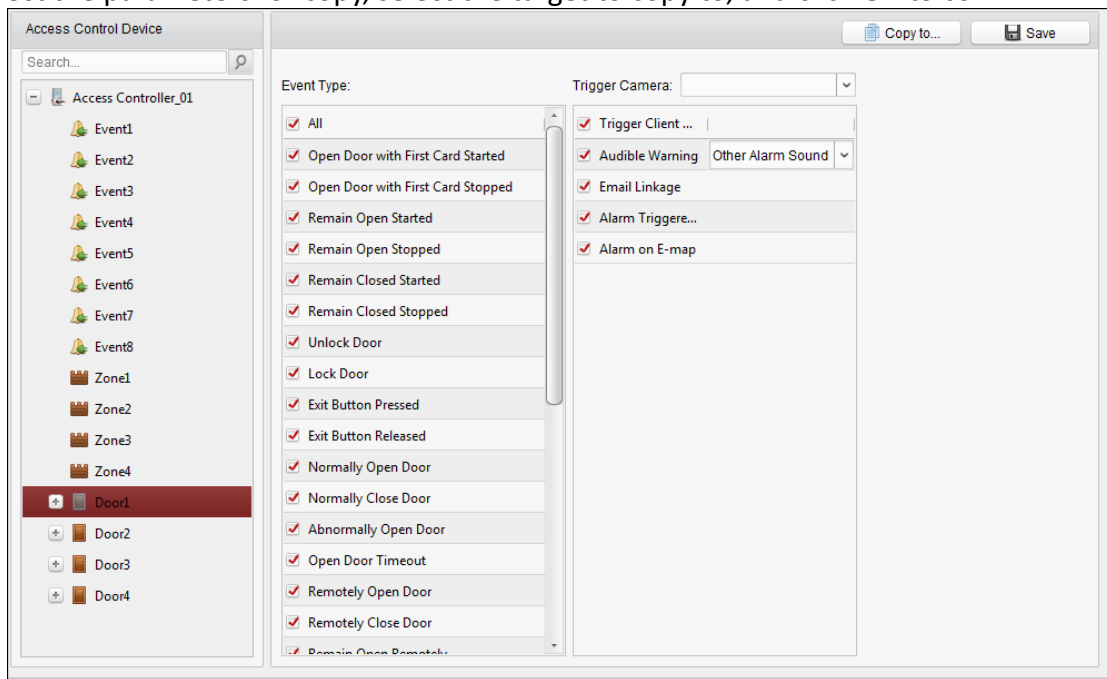


Table 1. 1 Linkage Actions for Access Control Event

Linkage Actions	Descriptions
<b>Audible Warning</b>	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.
<b>Email Linkage</b>	Send an email notification of the alarm information to one or more receivers.
<b>Alarm on E-map</b>	Display the alarm information on the E-map. <b>Note:</b> This linkage is only available to access control point and alarm input.

<b>Alarm Triggered Pop-up Image</b>	The image with alarm information pops up when alarm is triggered.
-------------------------------------	---

### 7.10.2 Access Control Alarm Input Linkage

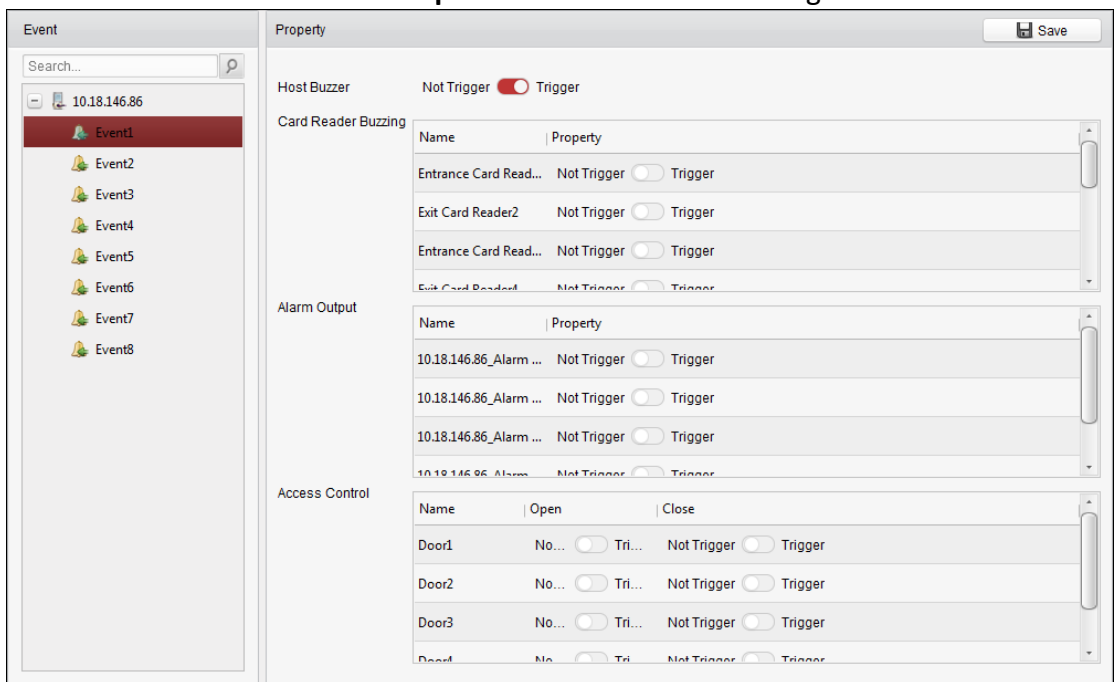
**Purpose:**

The access control alarm inputs can be linked to some actions (e.g., alarm output, host buzzer) when it is triggered.

**Note:** The linkage here refers to the linkage of the client software’s own actions.

**Steps:**

1. Click **Access Control Alarm Input** tab to enter the following interface.



2. In the event list on the left, select an alarm input.
3. Switch the property from  to  to enable this action.
  - Host Buzzer:** The audible warning of controller will be triggered.
  - Card Reader Buzzer:** The audible warning of card reader will be triggered.
  - Alarm Output:** The alarm output will be triggered for notification.
  - Access Control Point (Open/Close):** The door will be open or closed when the case is triggered.
- Note:** The Door cannot be configured as open or closed at the same time.
4. Click **Save** button to save the settings.

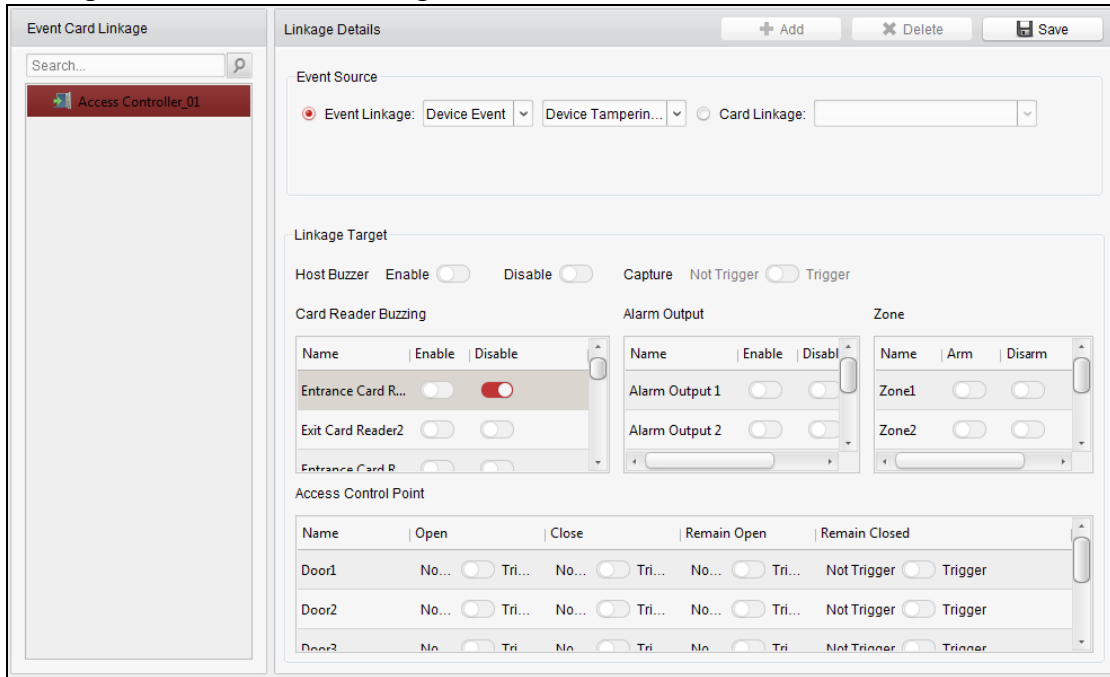
### 7.10.3 Event Card Linkage

Click **Event Card Linkage** tab to enter the following interface.

**Notes:**

- The Event Card Linkage should be supported by the device.

- The linkage here refers to the linkage of the client software's own actions.



Select the access control device from the list on the left.

Click **Add** button to add a new linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

## Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, and card reader event.

### Steps:

1. Click to select the linkage type as **Event Linkage**, and select the event type from the dropdown list.
  - For Device Event, select the detailed event type from the dropdown list.
  - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
  - For Door Event, select the detailed event type and select the source door from the table.
  - For Card Reader Event, select the detailed event type and select the card reader from the table.
2. Set the linkage target, and switch the property from  to  to enable this function.
  - **Host Buzzer:** The audible warning of controller will be enabled/disabled.
  - **Capture:** The real-time capture will be enabled.
  - **Card Reader Buzzer:** The audible warning of card reader will be enabled/disabled.
  - **Alarm Output:** The alarm output will be enabled/disabled for notification.
  - **Zone:** Arm or disarm the zone.
  - **Access Control Point:** The door status of open, close, remain open, and remain closed will be enabled.

### Notes:

- The door status of open, close, remain open, and remain close cannot be triggered at the same time.
  - The target door and the source door cannot be the same one.
3. Click **Save** button to save and take effect of the parameters.

## Card Linkage

### *Steps:*

1. Click to select the linkage type as **Card Linkage**.
2. Input the card No. or select the card from the dropdown list.
3. Select the card reader from the table for triggering.
4. Set the linkage target, and switch the property from  to  to enable this function.
  - **Host Buzzer:** The audible warning of controller will be enabled/disabled.
  - **Capture:** The real-time capture will be enabled.
  - **Card Reader Buzzer:** The audible warning of card reader will be enabled/disabled.
  - **Alarm Output:** The alarm output will be enabled/disabled for notification.
  - **Zone:** Arm or disarm the zone.
  - **Access Control Point:** The door status of open, close, remain open, and remain closed will be enabled.
5. Click **Save** button to save and take effect of the parameters.

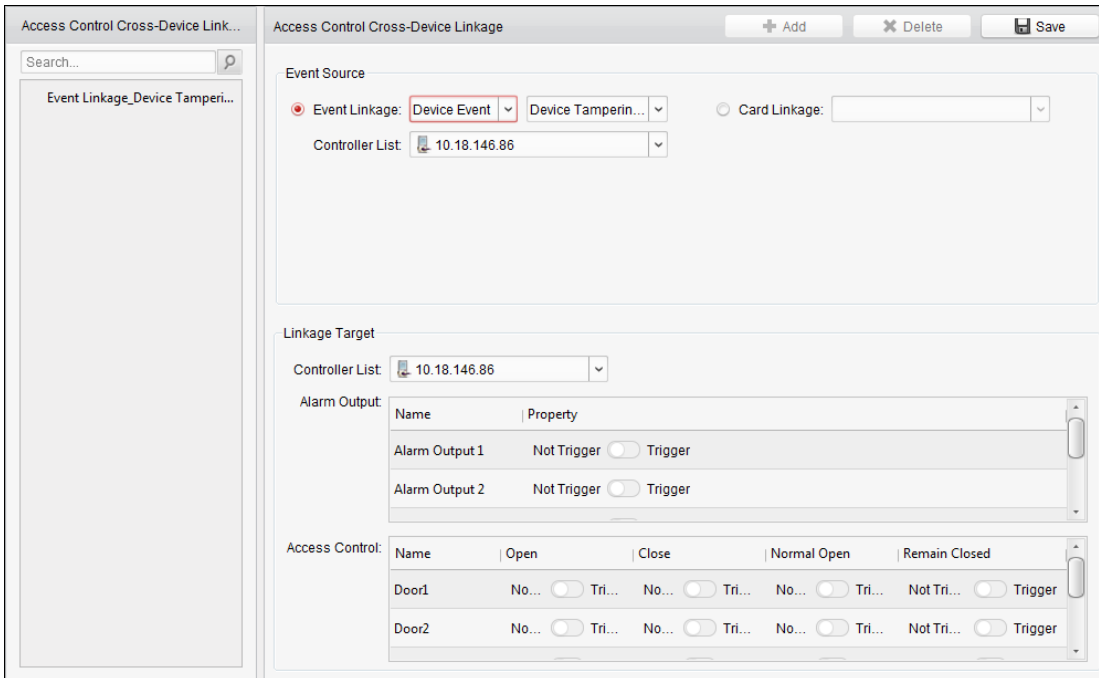
## 7.10.4 Cross-Device Linkage

### *Purpose:*

You can assign to trigger other access control device's action by setting up a rule when the access control event is triggered.

Click **Cross-Device Linkage** tab to enter the following interface.





Click **Add** button to add a new client linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

## Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, and card reader event.



### Steps:

1. Click to select the linkage type as **Event Linkage**, select the access control device as event source, and select the event type from the dropdown list.
  - For Device Event, select the detailed event type from the dropdown list.
  - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
  - For Door Event, select the detailed event type and select the door from the table.
  - For Card Reader Event, select the detailed event type and select the card reader from the table.
2. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from  to  to enable this function.
  - **Alarm Output:** The alarm output will be triggered for notification.
  - **Access Control Point:** The door status of open, close, remain open, and remain close will be triggered. **Note:** The door status of open, close, remain open, and remain close cannot be triggered at the same time.
3. Click **Save** button to save parameters.

## Card Linkage

### Steps:

1. Click to select the linkage type as **Card Linkage**.

2. Select the card from the dropdown list and select the access control device as event source.
3. Select the card reader from the table for triggering.
4. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from  to  to enable this function.

**Alarm Output:** The alarm output will be triggered for notification.

5. Click **Save** button to save parameters.

## 7.11 Door Status Management

### **Purpose:**

The door status of the added access control device will be displayed in real time. You can check the door status and the linked event(s) of the selected door. You can control the status of the door and set the status duration of the doors as well.


### 7.11.1 Access Control Group Management

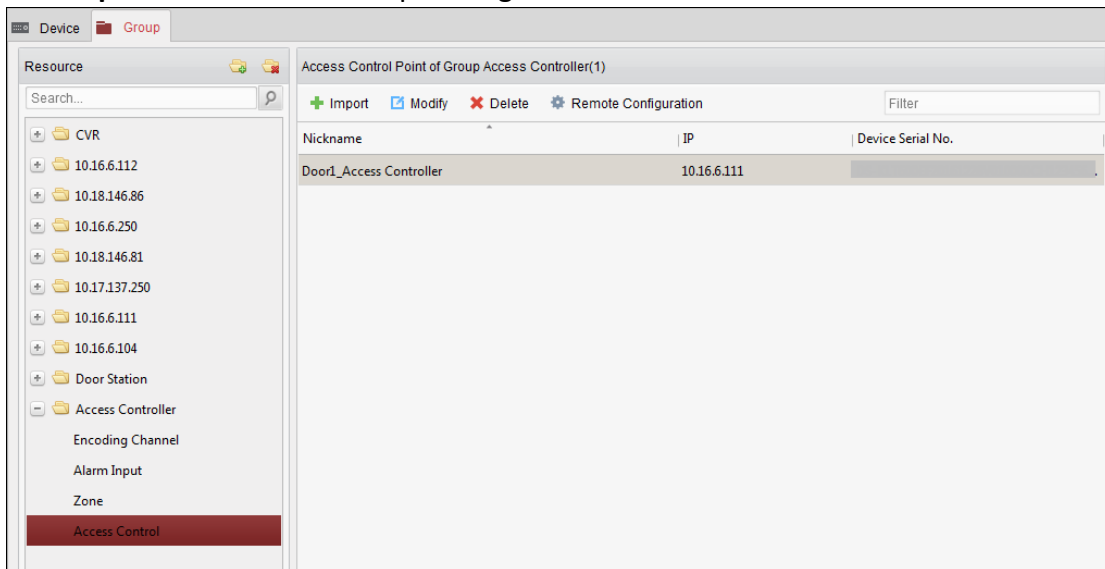
#### **Purpose:**


Before controlling the door status and setting the status duration, you are required to organize it into group for convenient management.

Perform the following steps to create the group for the access control device:

#### **Steps:**

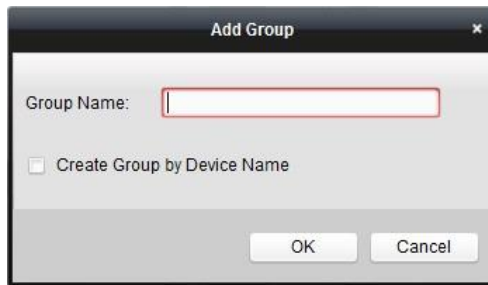
1. Click  on the control panel to open the Device Management page.
2. Click **Group** tab to enter the Group Management interface.



3. Perform the following steps to add the group.
  - 1) Click  to open the Add Group dialog box.
  - 2) Input a group name as you want.
  - 3) Click **OK** to add the new group to the group list.

You can also check the checkbox **Create Group by Device Name** to create the new group by

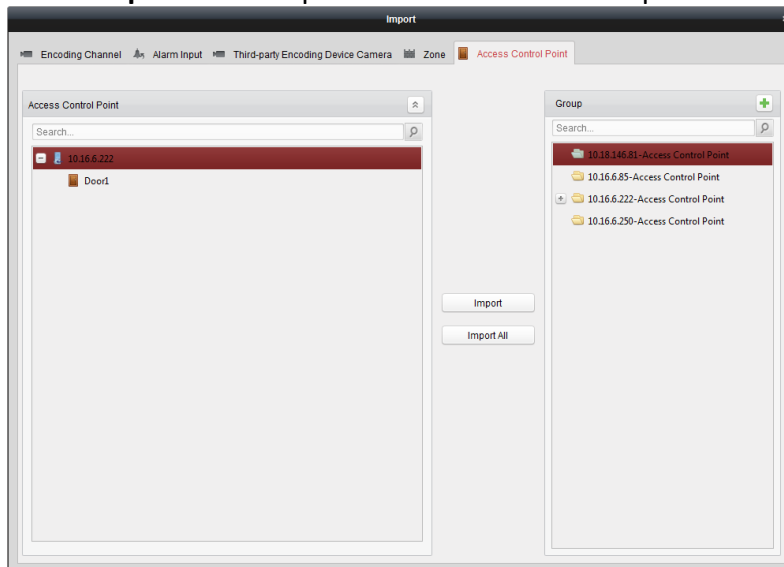
the name of the selected device.




4. Perform the following steps to import the access control points to the group:
  - 1) Click **Import** on Group Management interface, and then click the **Access Control** tab to open the Import Access Control page.

**Notes:**

- You can also select **Alarm Input** tab and import the alarm inputs to group.
  - For the Video Access Control Terminal, you can add the cameras as encoding channel to the group.
- 2) Select the names of the access control points in the list.
  - 3) Select a group from the group list.
  - 4) Click **Import** to import the selected access control points to the group.  
You can also click **Import All** to import all the access control points to a selected group.



5. After importing the access control points to the group, you can click , or double-click the group/access control point name to modify it.

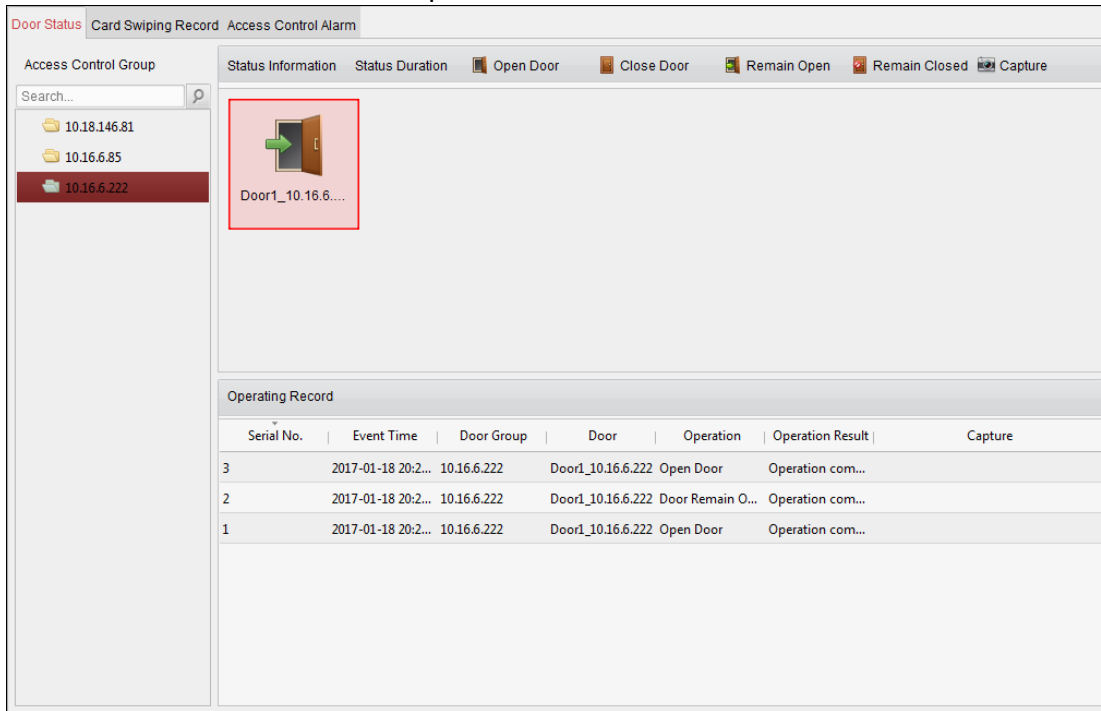
## 7.11.2 Anti-control the Access Control Point (Door)

**Purpose:**

You can control the status for a single access control point (a door), including opening door, closing door, remaining open, and remaining closed.



Click icon on the control panel to enter the Status Monitor interface.



**Steps:**

1. Select an access control group on the left. For managing the access control group, refer to *Chapter 7.11.1 Access Control Group Management*.
2. The access control points of the selected access control group will be displayed on the right.



Click icon on the Status Information panel to select a door.

3. Click the following button listed on the **Status Information** panel to control the door.

- Open Door** : Click to open the door once.
- Close Door** : Click to close the door once.
- Remain Open** : Click to keep the door open.
- Remain Closed** : Click to keep the door closed.
- Capture** : Click to capture the picture manually.

4. You can view the anti-control operation result in the Operation Log panel.

**Notes:**

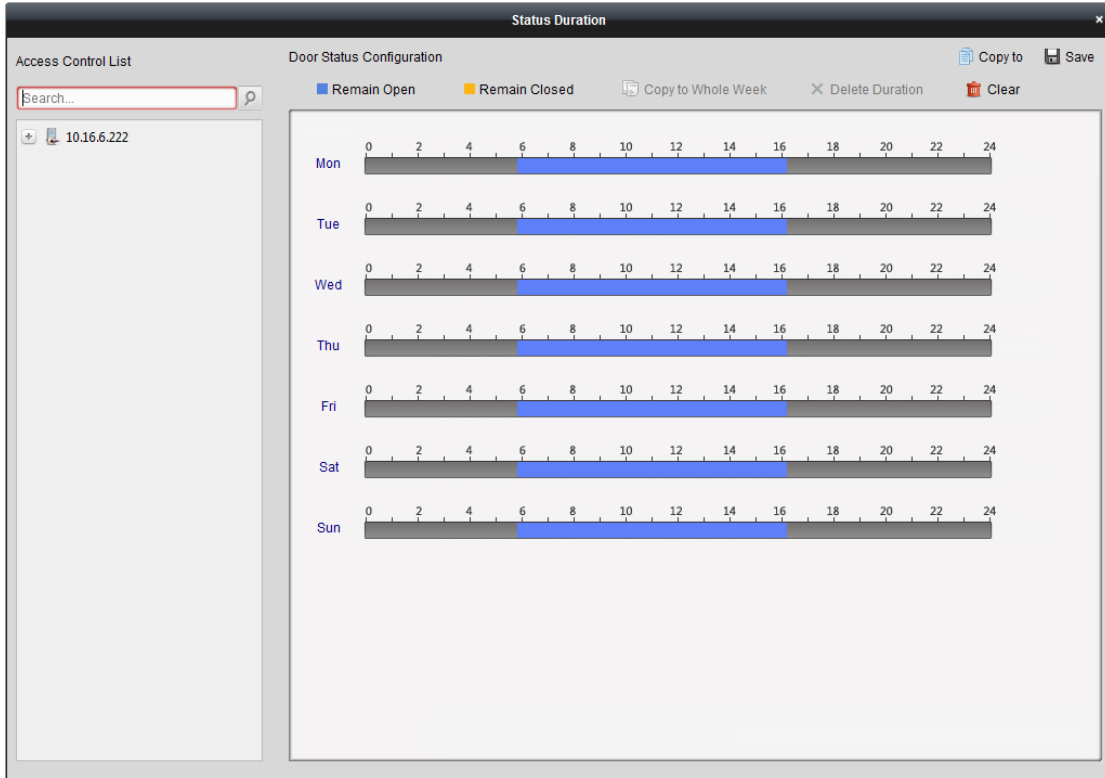
- If you select the status as **Remain Open/Remain Closed**, the door will keep open/closed until a new anti-control command being made.
- The **Capture** button is available when the device supports capture function. And it cannot be realized until the storage server is configured.
- If the door is in remain closed status, only super card can open the door or open door via the client software.

### 7.11.3 Status Duration Configuration

**Purpose:**

You can schedule weekly time periods for an access control point (door) to remain open or remain closed.

In the Door Status module, click **Status Duration** button to enter the Status Duration interface.




**Steps:**


1. Click to select a door from the access control device list on the left.
2. On the Door Status Configuration panel on the right, draw a schedule for the selected door.
  - 1) Select a door status brush as  Remain Open or  Remain Closed .
 

**Remain Open:** The door will keep open during the configured time period. The brush is marked as ■.

**Remain Closed:** The door will keep closed during the configured duration. The brush is marked as ■.
  - 2) Click and drag on the timeline to draw a color bar on the schedule to set the duration.



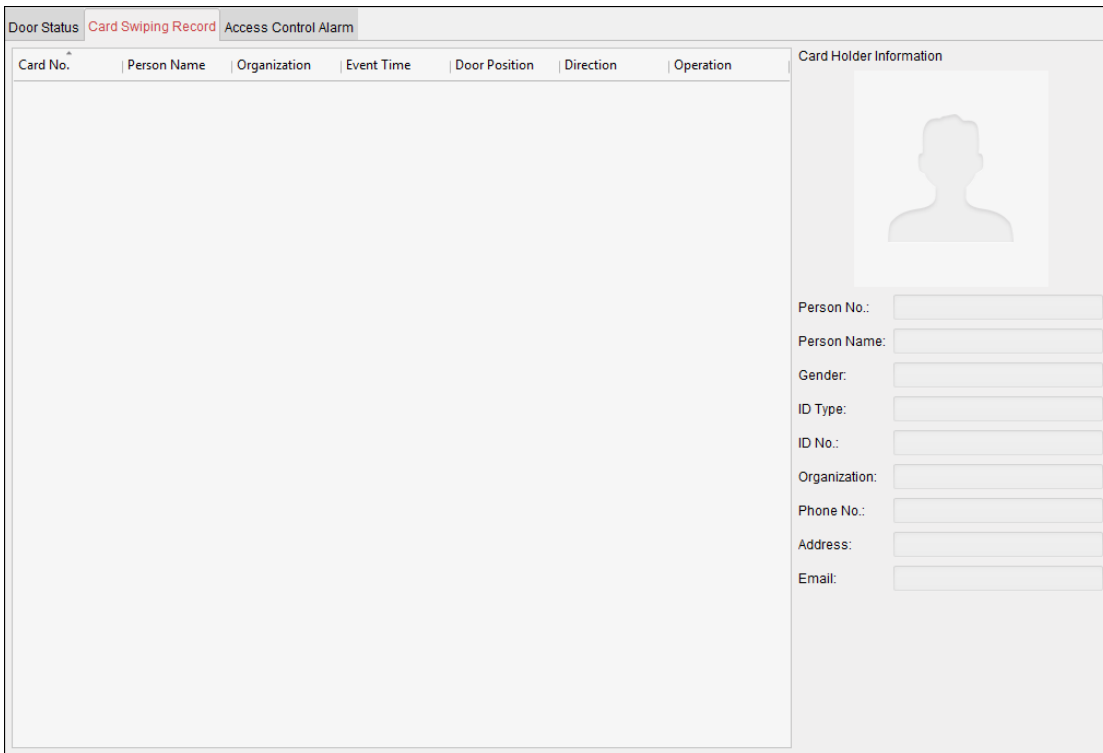
3) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.

When the cursor turns to , you can lengthen or shorten the selected time bar.

3. Optionally, you can select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
4. You can select the time bar and click **Delete Duration** to delete the time period.  
Or you can click **Clear** to clear all configured durations on the schedule.
5. Click **Save** to save the settings.
6. You can click **Copy to** button to copy the schedule to other doors.

### 7.11.4 Real-time Card Swiping Record

Click **Card Swiping Record** tab to enter the following interface.



The logs of card swiping records of all access control devices will display in real time. You can view the details of the card swiping event, including card No., person name, organization, event time, etc.

You can also click the event to view the card holder details, including person No., person name, organization, phone, contact address, etc.

## 7.11.5 Real-time Access Control Alarm

**Purpose:**

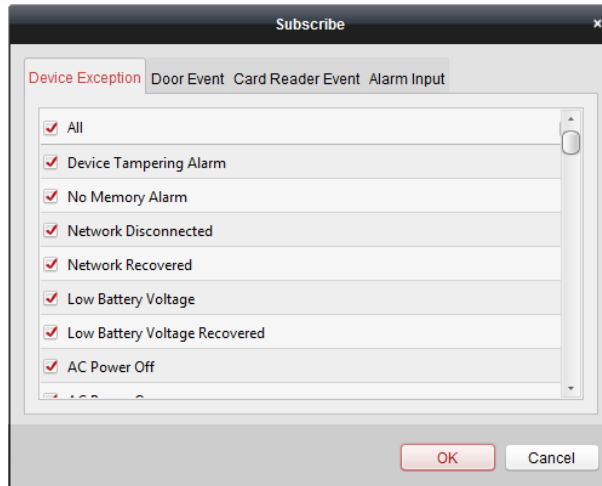
The logs of access control events will be displayed in real time, including device exception, door event, card reader event, and alarm input.

Click **Access Control Alarm** tab to enter the following interface.

Alarm Type	Alarm Time	Alarm Location	Alarm Content	Operation
Remote: Disarm...	2016-12-16 13:5...	Access Controller	Remote: Disarm...	
Remote: Arming	2016-12-16 13:5...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:5...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:5...	Access Controller	Remote: Disarm...	
Remote: Logout	2016-12-16 13:5...	Access Controller	Remote: Logout	
Remote: Login	2016-12-16 13:5...	Access Controller	Remote: Login	
Remote: Arming	2016-12-16 13:4...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:4...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:4...	Access Controller	Remote: Disarm...	
Door Locked	2016-12-16 13:4...	Door1	Door Locked	
Unlock	2016-12-16 13:4...	Door1	Unlock	
Remote: Arming	2016-12-16 13:4...	Access Controller	Remote: Arming	
Remote: Login	2016-12-16 13:4...	Access Controller	Remote: Login	
Remote: Disarm...	2016-12-16 13:4...	Access Controller	Remote: Disarm...	

**Steps:**

1. All access control alarms will display in the list in real time.  
You can view the alarm type, alarm time, location, etc.
  2. Click to view the alarm on E-map.
  3. You can click or to view the live view or the captured picture of the triggered camera when the alarm is triggered.
- Note:** For setting the triggered camera, refer to *Chapter 7.10.1 Access Control Event Linkage*.
4. Click **Subscribe** to select the alarm that the client can receive when the alarm is triggered.



- 1) Check the checkbox(es) to select the alarm(s), including device exception alarm, door event alarm, card reader alarm, and alarm input.
- 2) Click **OK** to save the settings.

## 7.12 Arming Control

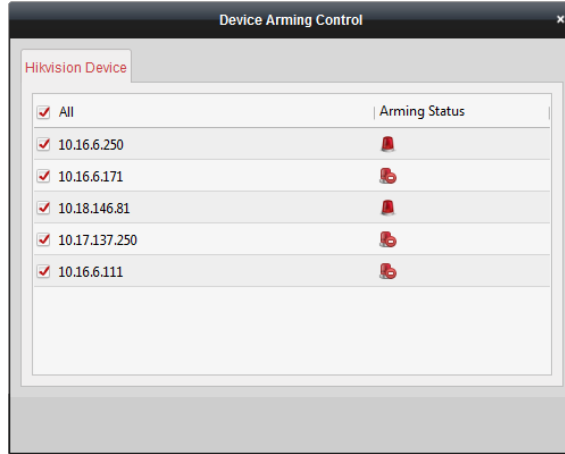
**Purpose:**



You can arm or disarm the device. After arming the device , the client can receive the alarm information from the device.

**Steps:**

1. Click **Tool->Device Arming Control** to pop up the Device Arming Control window.
2. Arm the device by checking the corresponding checkbox.  
Then the alarm information will be auto uploaded to the client software when alarm occurs.



## Appendix A Sound Prompt and Indicator

After the card reader is powered on, LED status indicator will turn blue and blink for 1 time. Then it will turn red and blink for 3 times. At last the buzzer will send out a beep sound indicating the starting up process is completed.

During using the card reader, it will send out different sounds prompt and the LED indicator on it have different statuses. You can refer to tables below for detailed information.

Table 7-1 Description of Prompt Sound

Sound Prompt	Description
One beep	RS-485 protocol: Pressing keys prompt; Swiping card prompt; Time out prompt for pressing keys or swiping card. Wiegand protocol: Pressing keys prompt; Swiping card prompt.
Two rapid beeps	The operation of pressing keys or swiping card is valid.
Three slow beeps	The operation of pressing keys or swiping card is invalid.
Rapidly continuous beeps	Alarm of tamper-proof.
Slowly continuous beeps	The card reader is unencrypted.

Table 7-2 Description of LED Indicator

LED Indicator Status	Description
Green and blinking	Card reader is working normally.
Solid green	The operation of pressing keys or swiping card is valid.
Solid red	The operation of pressing keys or swiping card is invalid.
Red and blinking	For RS-485 protocol: Registering failed or card reader is offline. Failed to get key files of PSAM card; Failed to detect the PSAM card.
Red and Keeping rapidly blinking	Available for reading file mode of CPU card: PSAM is not inserted or undetected.

# Appendix B Custom Wiegand Rule Descriptions

Take Wiegand 44 as an example, the setting values in the Custom Wiegand tab are as follows:

Custom Wiegand Name:	Wiegand 44				
Total Length	44				
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]				
Parity Mode	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Wiegand Data = Valid Data + Parity Data

**Total Length:** Wiegand data length.

**Transportation Rule:** 4 bytes. Display the combination types of valid data. The example displays the combination of Card ID and Manufacturer Code. The valid data can be single rule, or combination of multiple rules.

**Parity Mode:** Valid parity for wiegand data. You can select either odd parity or even parity.

**Odd Parity Start Bit, and Length:** If you select Odd Parity, these items are available. If the odd parity start bit is 1, and the length is 12, then the system will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0. (Bit 0 is the first bit.)

**Even Parity Start Bit, and Length:** If you select Even Parity, these items are available. If the even parity start bit is 12, and the length is 12, then the system will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

**XOR Parity Start Bit, Length per Group, and Total Length:** If you select XOR Parity, these items are available. Depending on the table displayed above, the start bit is 0, the length per group is 4, and the total length is 40. It means that the system will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits. (The result length is the same as the length per group.)

**Card ID Start Bit, Length, and Decimal Digit:** If you use the transformation rule, these items are available. Depending on the table displayed above, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

**Site Code Start Bit, Length, and Decimal Digit:** If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

**OEM Start Bit, Length, and Decimal Digit:** If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

**Manufacturer Code Start Bit, Length, and Decimal Digit:** If you use the transformation rule, these items are

available. Depending on the table displayed above, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

0200001070507



First Choice for Security Professionals