



**HIKVISION**

**DS-K2800 Series**  
**Access Controller**  
**User Manual**

**UD.6L0206D1131A0**

1

## User Manual

COPYRIGHT ©2015 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

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

### About this Manual

This Manual is applicable to Access Controller

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

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

Please use this user manual under the guidance of professionals.

### Trademarks Acknowledgement

**HIKVISION** and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

### Legal Disclaimer

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

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

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

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

0100001051101

## Regulatory Information

### FCC Information

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

### FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

### EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.



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

[www.recyclethis.info](http://www.recyclethis.info).



2006/66/EC (battery directive): This product contains a battery that

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

Industry Canada ICES-003 Compliance

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

### Preventive and Cautionary Tips

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

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



#### Safety Information

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



#### Warnings:

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

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

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

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

local codes.

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



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

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

Keep ventilation.

Do not operate in humid environment.

Do not operate in explosive environment.

Keep the device clean and dry.

Avoid bare electrical wire.

# Table of Contents

<b>CHAPTER 1</b>	<b>PRODUCT DESCRIPTION</b>	<b>3</b>
1.1	OVERVIEW	3
1.2	PRODUCT FUNCTION	3
<b>CHAPTER 2</b>	<b>APPEARANCE</b>	<b>5</b>
<b>CHAPTER 3</b>	<b>TERMINAL CONNECTION</b>	<b>7</b>
3.1	DS-K2801 TERMINAL DESCRIPTION	7
3.2	DS-K2802 TERMINAL DESCRIPTION	9
3.3	DS-K2804 TERMINAL DESCRIPTION	12
<b>CHAPTER 4</b>	<b>EXTERNAL DEVICE WIRING</b>	<b>16</b>
4.1	CARD READER WIRING	16
4.2	INSTALLING DOOR LOCK	17
4.2.1	<i>Installation of Cathode Lock</i>	17
4.2.2	<i>Installation of Anode Lock</i>	17
4.3	CONNECTING THE EXTERNAL ALARM DEVICE	18
4.4	DOOR BUTTON WIRING DIAGRAM	18
4.5	THE CONNECTION OF MAGNETICS DETECTION	19
4.6	CONNECTING POWER SUPPLY	19
<b>CHAPTER 5</b>	<b>SETTINGS</b>	<b>20</b>
5.1	INITIALIZING THE HARDWARE	20
5.2	RELAY INPUT NO/NC	20
5.2.1	<i>Lock Relay Output</i>	20
5.2.2	<i>Alarm Relay Output Status</i>	21
<b>CHAPTER 6</b>	<b>ACTIVATING THE CONTROL PANEL</b>	<b>24</b>
6.1	ACTIVATION VIA SADP SOFTWARE	24
6.2	ACTIVATION VIA CLIENT SOFTWARE	26

- CHAPTER 7 CLIENT OPERATION ..... 30**
- 7.1 OVERVIEW OF ACCESS CONTROL SYSTEM .....30
  - 7.1.1 *Description*.....30
  - 7.1.2 *Configuration Flow* .....30
- 7.2 DEVICE MANAGEMENT .....32
  - 7.2.1 *Controller Management* .....32
  - 7.2.2 *Access Control Point Management*.....44
- 7.3 PERMISSION MANAGEMENT .....49
  - 7.3.1 *Person Management* .....49
  - 7.3.2 *Card Management*.....56
  - 7.3.3 *Schedule Template* .....62
  - 7.3.4 *Door Status Management* .....68
  - 7.3.5 *Interact Configuration* .....73
  - 7.3.6 *Access Permission Configuration* .....79
  - 7.3.7 *Attendance Management*.....88
  - 7.3.8 *Advanced Functions*.....120
- 7.4 CHECKING STATUS AND EVENT.....131
  - 7.4.1 *Status Monitor*.....131
  - 7.4.2 *Access Control Event*.....135
  - 7.4.3 *Event Search* .....136
- 7.5 SYSTEM MAINTENANCE .....139
  - 7.5.1 *Log Management* .....139
  - 7.5.2 *System Configuration*.....144

# Chapter 1 Product Description

## 1.1 Overview

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

## 1.2 Product Function

- The access controller is equipped with 32-bit high-speed processor
- Supports TCP/IP network communication, with self-adaptive network interface. The communication data is specially encrypted to relieve the concern of privacy leak
- Supports recognition and storage of card number with maximum length of 20
- The access controller can store 10 thousand legal cards and 50 thousand card swiping records
- Supports first card open function, super card and super password function, online upgrade function and remote control of the doors
- Supports Wiegand interface for accessing card reader. Wiegand interface supports W26, W34 and is seamlessly compatible with third-party card reader with Wiegand interface
- Supports various card types as normal/ disabled/ blacklist/ patrol/ guest/ duress/ super card, etc.
- Various indicators to show different status
- Supports time synchronization via NTP, manual or automatic method
- Supports record storage function when it is offline and insufficient storage space storage alarm function
- The access controller has watchdog design

- Data can be permanently saved after the access controller is powered off
- Supports I/O linkage, and event linkage
- Supports alarm of offline event exceeding 90%

# Chapter 2 Appearance

## Component Description

### Access Controller Component Schematic Diagram

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

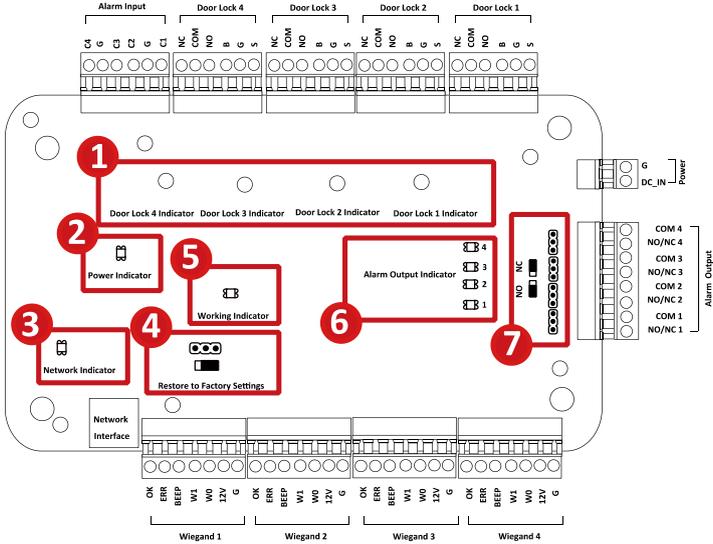


Figure 2-1 DS-K2804 Component Schematic Diagram

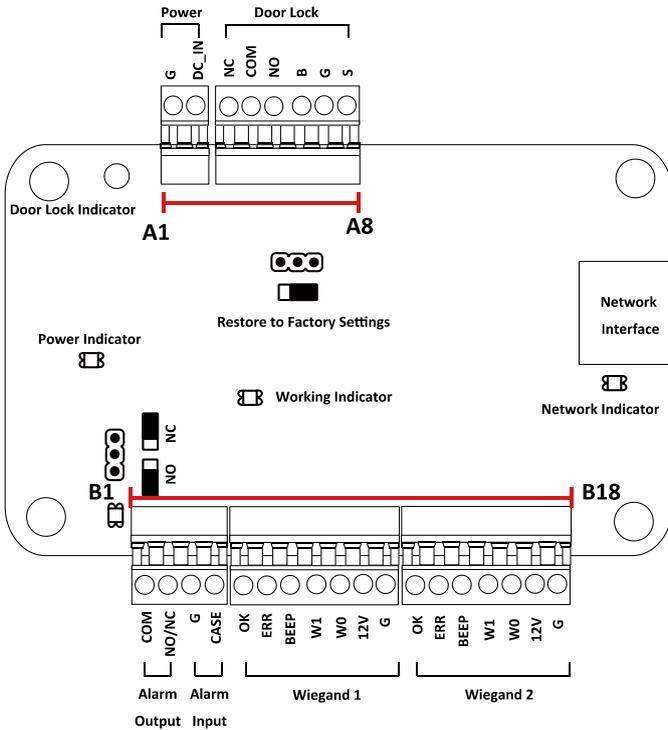
Table 2-1 DS-K2800 Component Description

No.	Component Description		
	DS-K2801	DS-K2802	DS-K2804
1	Door Lock 1 Indicator	Door Lock 1/2 Indicator	Door Lock 1/2/3/4 Indicator
2	Power Indicator		
3	Network Indicator		
4	Jumper Cap for Restoring Factory Settings		

No.	Component Description
5	Working Indicator
6	Alarm Output Indicator
7	Alarm Output (NO/NC) Jumper Cap

# Chapter 3 Terminal Connection

## 3.1 DS-K2801 Terminal Description



1

Figure 3-1 DS-K2801 Terminals

Table 3-1 DS-K2801 Terminal Description

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

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

### 3.2 DS-K2802 Terminal Description

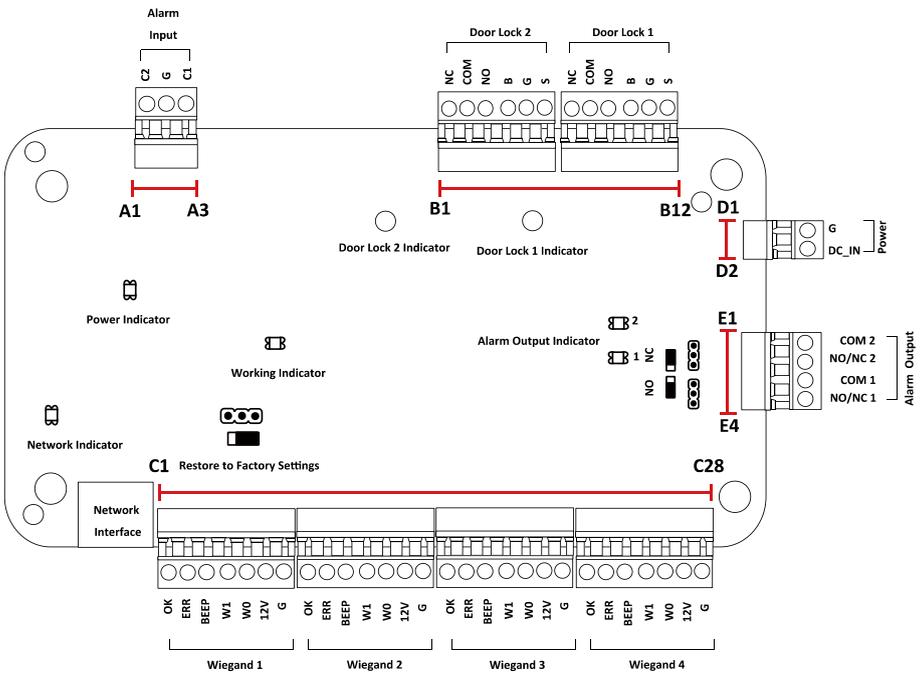


Figure 3-2 DS-K2802 Terminal Description

Table 3-2 DS-K2802 Port Description

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

No.	DS-K2802		
A3		IN1	Alarm Input 1
B1	Door 2	NC	Door Lock Relay Output (Dry Contact)
B2		COM	
B3		NO	
B4		BUTTON	Door Button Input
B5		GND	Grounding
B6		SENSOR	Door Magnetic detector
B7	Door 1	NC	Door Lock Relay Output (Dry Contact)
B8		COM	
B9		NO	
B10		BUTTON	Door Button Input
B11		GND	Grounding
B12		SENSOR	Door Magnetic detector
D1	Power	GND	DC12V Grounding
D2		+12V	DC12V Input
E1	Alarm Output 2	COM2	Alarm Relay Output 2 (Dry Contact)
E2		NO/NC2	
E3	Alarm Output 1	COM1	Alarm Relay Output 1 (Dry Contact)
E4		NO/NC1	
C1	Wiegand Card Reader 1	OK	Indicator of Card Reader Control Output (Valid Card Output)
C2		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
C3		BZ	Card Reader Buzzer Control Output
C4		W1	Wiegand Head Read Data Input Data1
C5		W0	Wiegand Head Read Data Input Data0
C6		PWR	Card Reader Power Output
C7		GND	
C8	Wiegand Card Reader 2	OK	Indicator of Card Reader Control

No.	DS-K2802		
			Output (Valid Card Output)
C9		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
C10		BZ	Card Reader Buzzer Control Output
C11		W1	Wiegand Head Read Data Input Data1
C12		W0	Wiegand Head Read Data Input Data0
C13		PWR	Card Reader Power Output
C14		GND	
C15		Wiegand Card Reader 3	OK
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
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

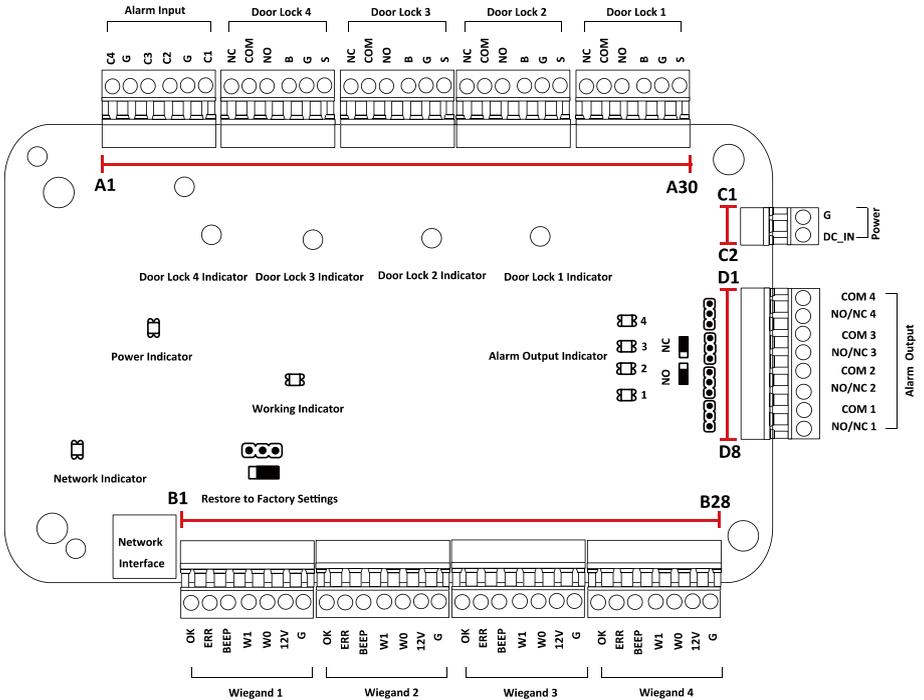


Figure 3-3 DS-K2804 Access Controller Terminals

Table 3-3 DS-K2804 Port Description

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

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

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

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



- The Alarm input hardware interface is normally open by default. So only the normally open signal is allowed. It can be linked to the buzzer of the card reader and access controller, and the alarm relay output and open door relay output.
- For single-door access controller, the Wiegand card reader 1 and 2 respectively correspond to the entering and exiting card readers of door 1. For two-door access controller, the Wiegand card reader 1 and 2 respectively correspond to the entering and exiting card readers of door 1, and the Wiegand card reader 3 and 4 respectively correspond to the entering and exiting card readers of door 2. For single-door access controller, the Wiegand card reader 1, 2, 3 and 4 respectively correspond to the entering card readers of door 1, 2, 3, and 4.

# Chapter 4 External Device Wiring

## 4.1 Card Reader Wiring

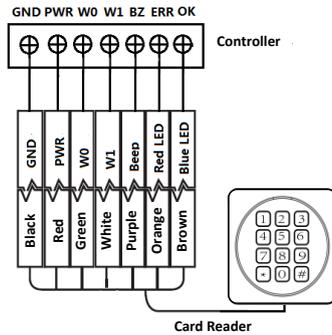


Figure 4-1 Wiring diagram of Wiegand card reader



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

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

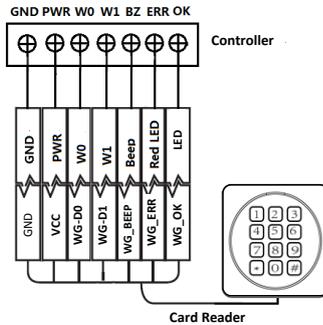


Figure 4-2 Wiring diagram of 1800 series card reader

## 4.2 Installing Door Lock

### 4.2.1 Installation of Cathode Lock

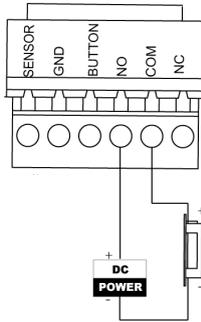


Figure 4-3 Wiring diagram of cathode lock

### 4.2.2 Installation of Anode Lock

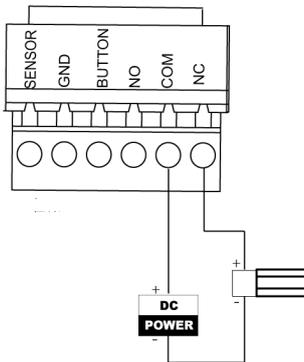


Figure 4-4 Wiring diagram of anode lock

### 4.3 Connecting the External Alarm Device

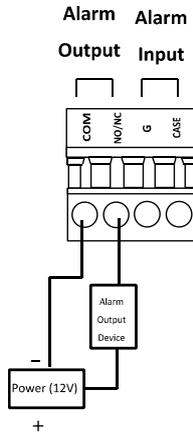


Figure 4-5 External Alarm Device Connection

### 4.4 Door Button Wiring Diagram

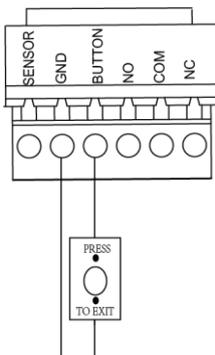


Figure 4-6 Power Button Connection

## 4.5 The Connection of Magnetics Detection

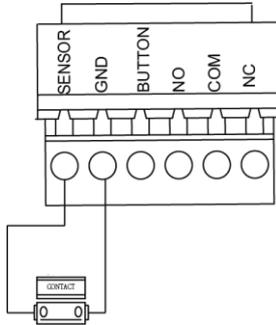


Figure 4-7 Magnetics Connection

## 4.6 Connecting Power Supply

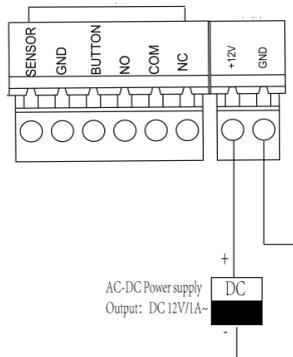


Figure 4-8 Power Supply Connection

# Chapter 5 Settings

## 5.1 Initializing the Hardware

**Steps:**

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

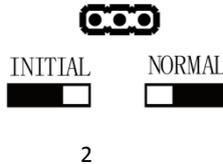


Figure 5-1 Initialization Dial-up



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

## 5.2 Relay Input NO/NC

### 5.2.1 Lock Relay Output

Lock Relay Normally Open Status

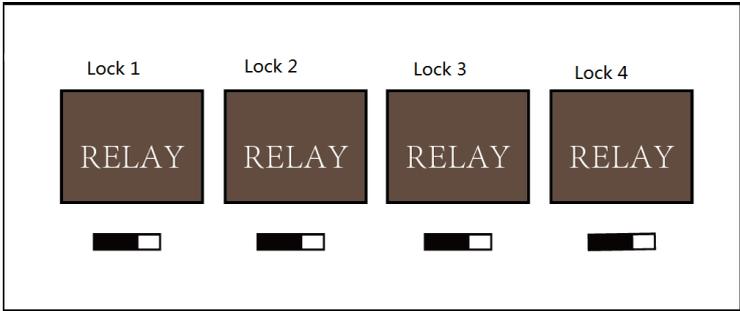


Figure 5-2 Normally Open Status

Lock Relay Normally Closed Status

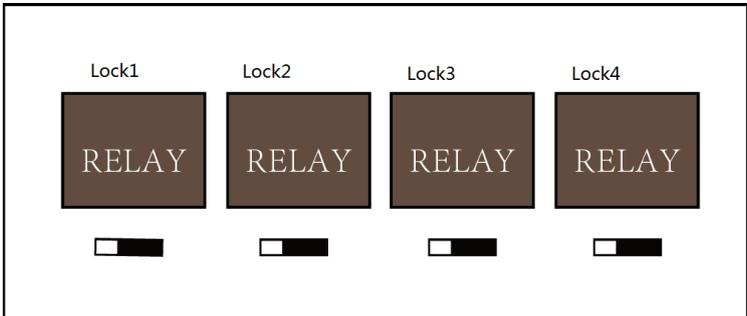


Figure 5-3 Normally Closed Status

## 5.2.2 Alarm Relay Output Status

Alarm Relay Output Normally Open

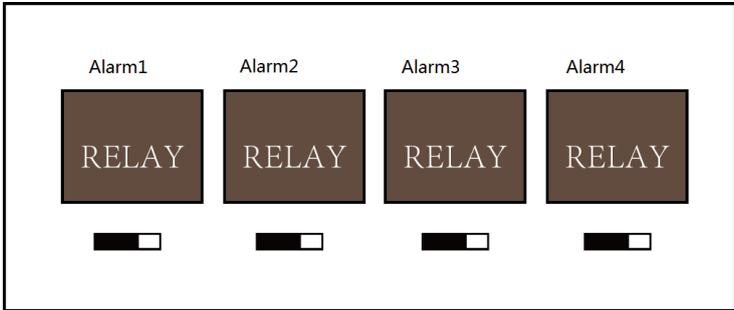


Figure 5-4 Alarm Relay Output Normally Open

Alarm Relay Output Normally Closed

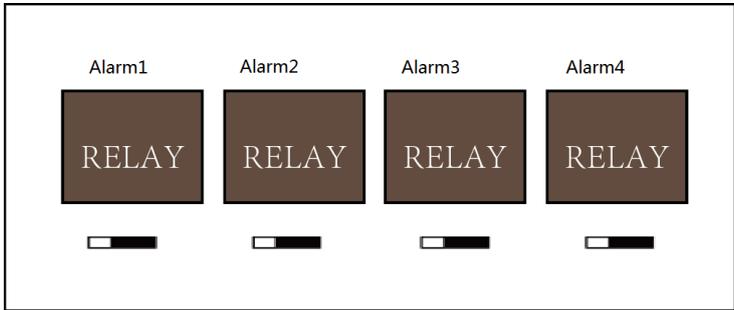
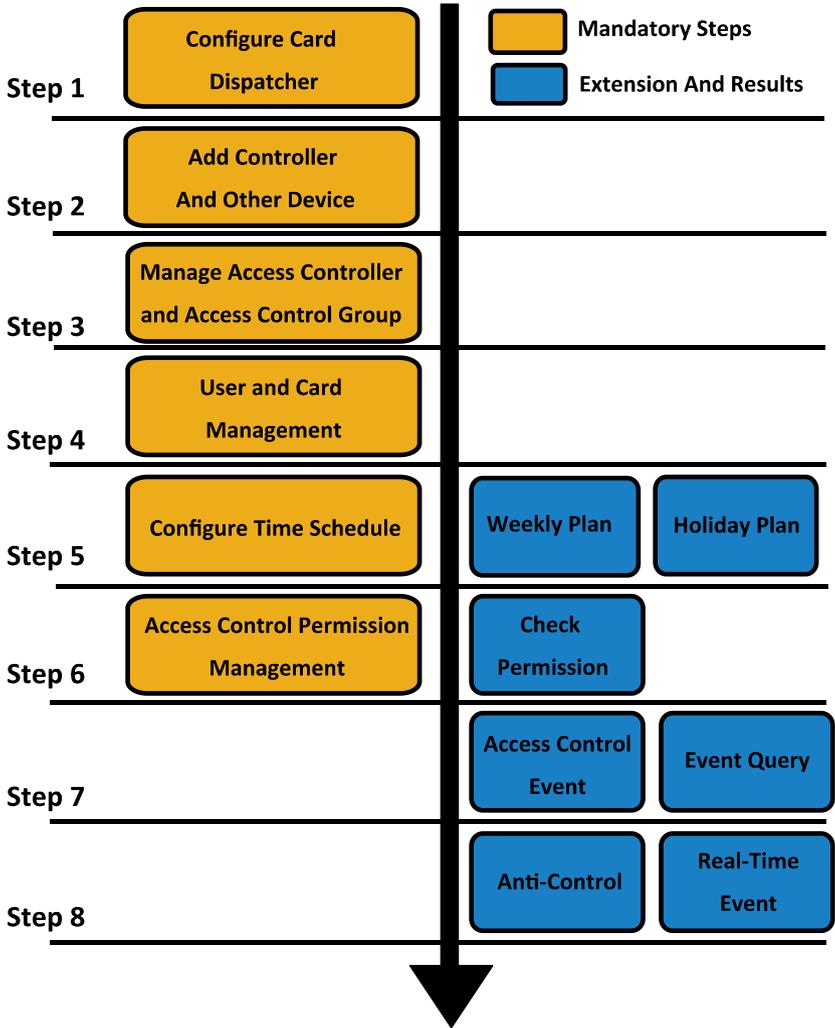


Figure 5-5 Normally Closed Status

Work Flow of Software

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

Refer to the following work flow:



3

Figure 5-6 Software Client Work Flow

# Chapter 6 Activating the Control Panel

**Purpose:**

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

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

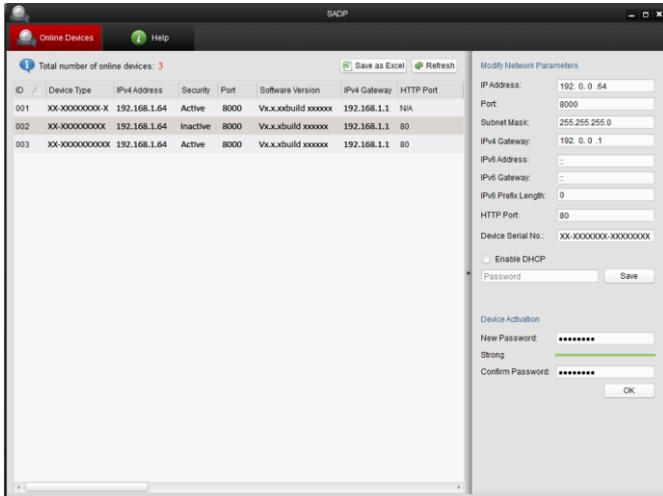
## 6.1 Activation via SADP Software

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

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

**Steps:**

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



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



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

4. Click OK to save the password.

You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and then try again.

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

Modify Network Parameters

IP Address: 192.0.0.64

Port: 8000

Subnet Mask: 255.255.255.0

IPv4 Gateway: 192.0.0.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Device Serial No.: XX-XXXXXXX-XXXXXXX

Enable DHCP

Password  Save

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

## 6.2 Activation via Client Software

The client software is versatile video management software for multiple kinds of devices.

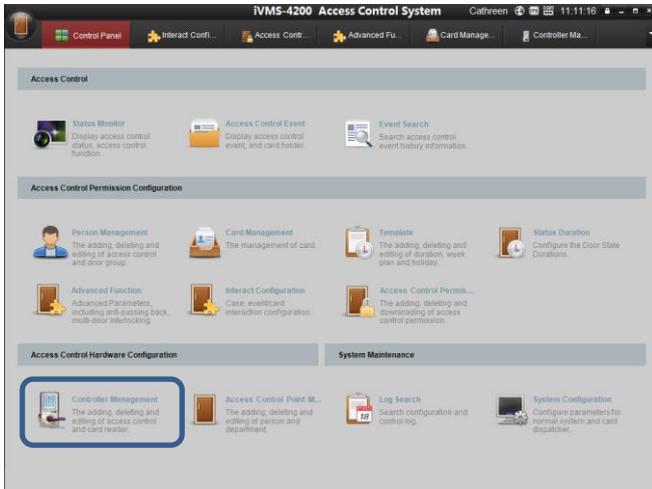
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

### **Steps:**

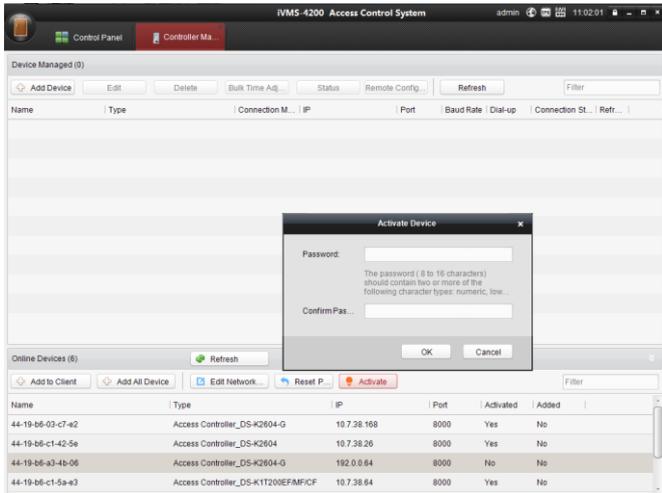
1. Run the client software and the control panel of the software pops up, as

shown in the figure below.

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



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



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



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



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.

Activate Device

Password:

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

Confirm Pas...

OK Cancel

7. Click OK button to start activation.
8. Click the  button to pop up the Network Parameter Modification interface.
9. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.
10. Input the password to activate your IP address modification.

# Chapter 7 Client Operation

## 7.1 Overview of Access Control System

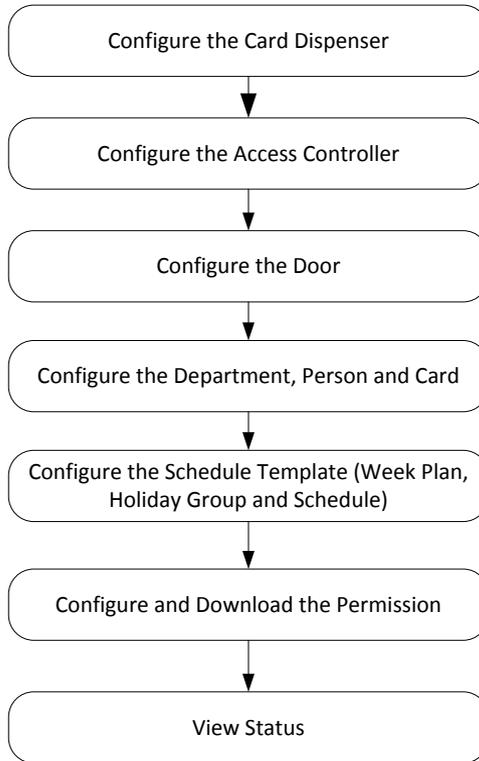
### 7.1.1 Description

The access control system is a system of configuring permission of door access. It provides multiple functionalities, including access controller management, people/card management, permission configuration, door status management, event search, etc.

This user manual describes the function, configuration and operation steps of Access Control System. To ensure the properness of usage and stability of the system, please refer to the contents below and read the manual carefully before installation and operation.

### 7.1.2 Configuration Flow

Refer to the following flow chart for the configuration order.



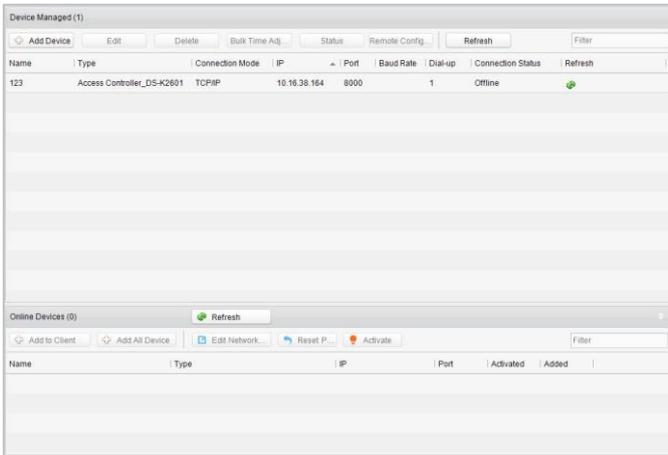
## 7.2 Device Management

### 7.2.1 Controller Management

#### Interface Introduction



Click the icon to enter the controller management interface.



The interface is divided into 2 parts: device management and online device detection.

**Device Management:**

Manage the access control devices, including adding, editing, deleting, and batch time synchronizing functions.

**Online Device Detection:**

Automatically detect online devices in the same subnet with the access control server, and the detected devices can be added to the server in an easy way.



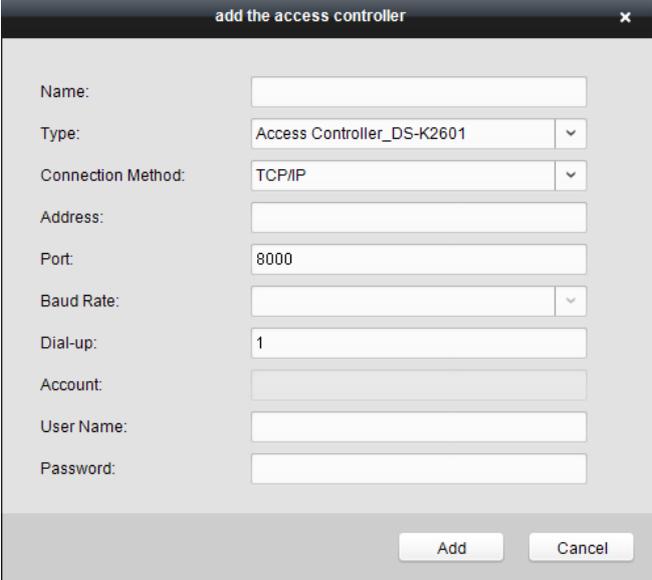
The control client can manage 100 access controllers at most.

## Device Management

### Adding Controller

#### Steps:

1. Click the  to enter the add access controller interface.



The screenshot shows a dialog box titled "add the access controller" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Name:
- Type:  (dropdown)
- Connection Method:  (dropdown)
- Address:
- Port:
- Baud Rate:  (dropdown)
- Dial-up:
- Account:
- User Name:
- Password:

At the bottom of the dialog are two buttons: "Add" and "Cancel".

2. Input the device name.
3. Select the access controller type in the dropdown list.
4. Select the connection mode in the dropdown list: TCP/IP, or COM port, or Ehome.

**TCP/IP:** Connect the device via the network.

**Ehome:** Connect the device via the Ehome protocol.

5. Set the parameters of connecting the device.

If you choose to connect the device via network, you should input the IP address and port No. of the device, and set the Dial-up value to 1.

If you choose to connect the device via Ehome protocol, you should input an account.



For the detailed information about the account, refer to 15.1.3.

6. Click the  button to finish adding.

You can click **Status** to check the detailed status of the controller, and click **Remote Configuration** to configure the settings of the controller.

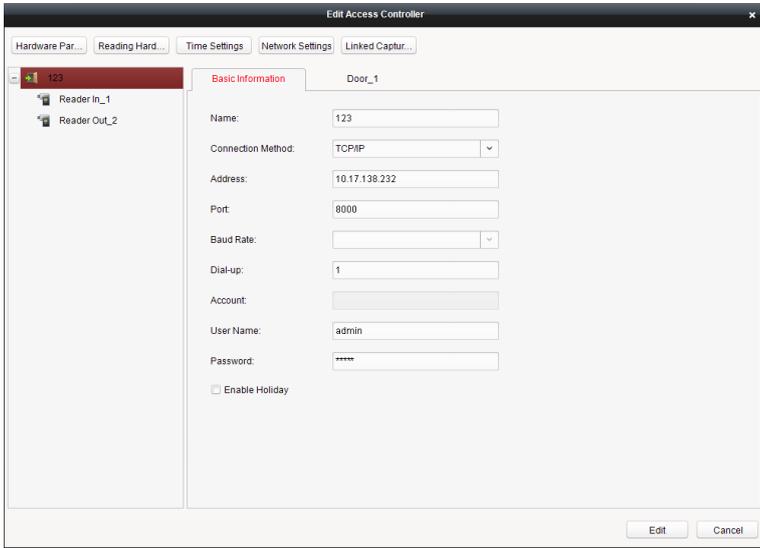
### Editing Device (Basic Information)

#### **Purpose:**

After adding the device, some advanced parameters can be configured in the editing device interface, e.g. downloading hardware parameters, reading hardware parameters, time synchronizing, configuring access point, etc.

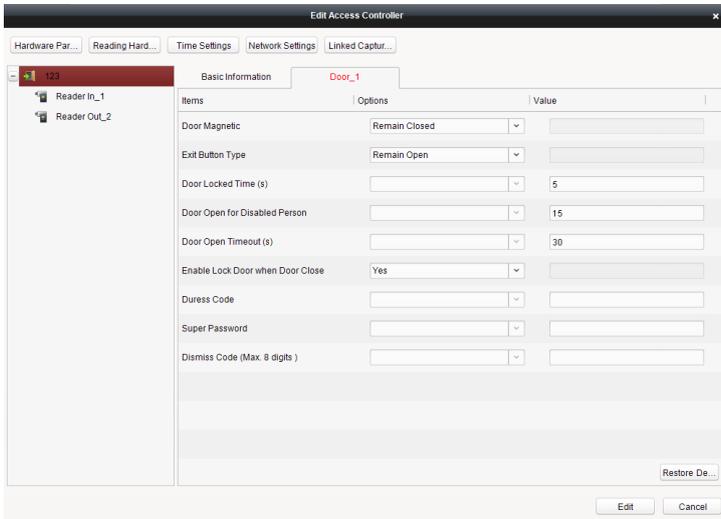
#### **Steps:**

1. In the device list, click Edit button to edit the information of the selected added device.



2. Edit the basic parameters of the device on your demand, which are the same as the ones when adding the device.
3. (Optional) Check the checkbox of **Enable Holiday** to enable the holiday parameters when downloading permissions.
4. Click the **Edit** button to finish editing.
5. Click the **Hardware Parameters Downloading** button to download the updated parameters to the local memory of the device.

### Editing Device (Door Information)

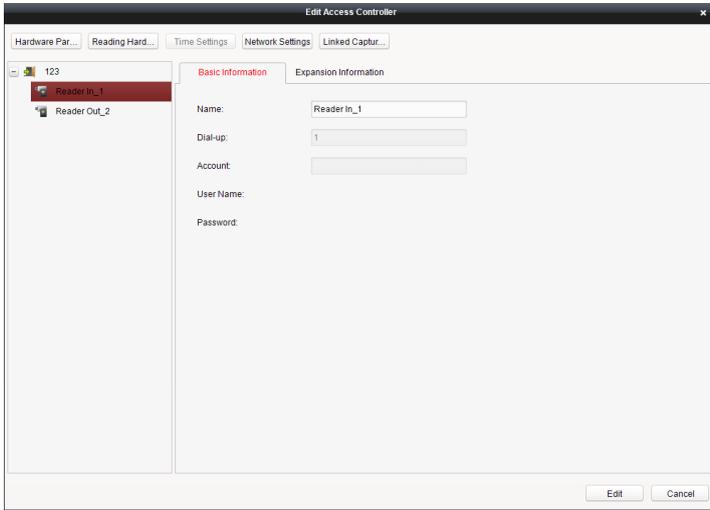


**Steps:**

1. In the editing interface, click the **Door\_1** button to edit the information of the selected door.
  - 1) **Door Magnetic:** The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
  - 2) **Exit Button Type:** The Exit Button Type is in the status of Remain Open (excluding special conditions).
  - 3) **Door Locked Time(s):** After swiping the normal card and relay action, the timer for locking the door starts working.
  - 4) **Door Open for Disabled Person:** The door magnetic can be enabled with appropriate delay after disabled person swipes the card.
  - 5) **Door Open Timeout(s):** The alarm can be triggered if the door has not been close

- 6) **Enable Lock Door when Door Close:** This function has not been supported yet.
  - 7) **Duress Code:** The door can open by inputting the duress code when there is a duress. At the same time, the access system can report the duress event.
  - 8) **Super Password:** The specific person can open the door by inputting the super password.
2. Click the **Restore Default Value** to restore all parameters into default settings.
  3. Click the **Edit** button to save parameters.
  4. Click the **Hardware Parameters Downloading** button to download the updated parameters to the local memory of the device.

### **Editing Device (Card Reader Information)**



### **Steps:**

1. In the device list, select a card reader name to enter into the card reader information editing interface.
2. Click the **Basic Information** button to edit the basic information about the card reader.
3. Click the **Expansion Information** button to edit the expansion information about the card reader.
4. Click the **Edit** button to save parameters.
5. Click the **Hardware Parameters Downloading** button to download the updated parameters to the local memory of the device.

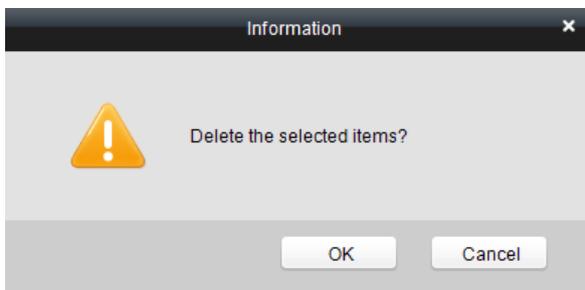
### **Deleting Device**

#### **Steps:**

1. In the device list, select a device by clicking it, or select multiple devices

by pressing Ctrl button on your keyboard and clicking them one by one.

2. Click the  button to delete the selected device(s).
3. Click **OK** button in the popup confirmation dialog to finish deleting.



### **Bulk Time Synchronization**

#### **Steps:**

1. In the device list, select a device by clicking it, or select multiple devices by pressing Ctrl button on your keyboard and clicking them one by one.
2. Click the **Bulk Time Adjustment** button to start time synchronization.  
A message box will pop up on the lower-right corner of the screen when the time synchronization is completed.

#### **Status**

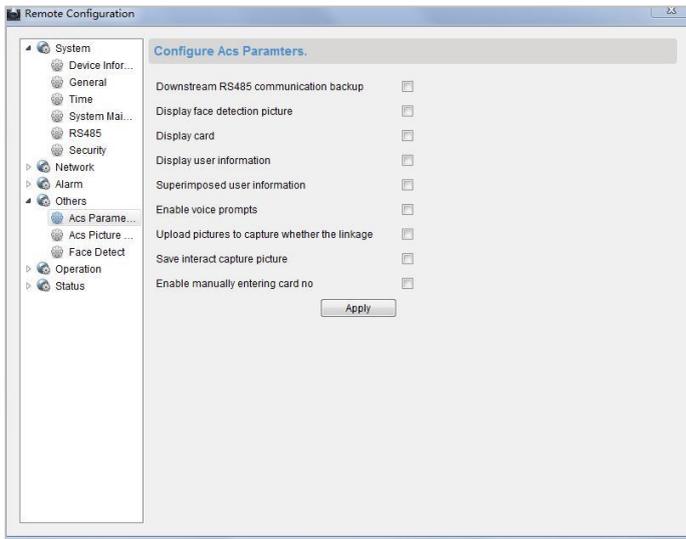
In the device list, you can click **Status** button to enter view the status.

- 1) **Door Status:** The status of the connected door.
- 2) **Host Status:** The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, and Host Anti-Tamper Status.
- 3) **Card Reader Status:** The status of card reader.
- 4) **Alarm Input Status:** The alarm input status of each port.

- 5) **Alarm Output Status:** The alarm output status of each port.
- 6) **Event Sensor Status:** The event status of each port.

### Remote Configuration

In the device list, you can click **Remote Configuration** button to enter the remote configuration interface. On this interface, you can set the access parameters, enable the face detection function, and so on.

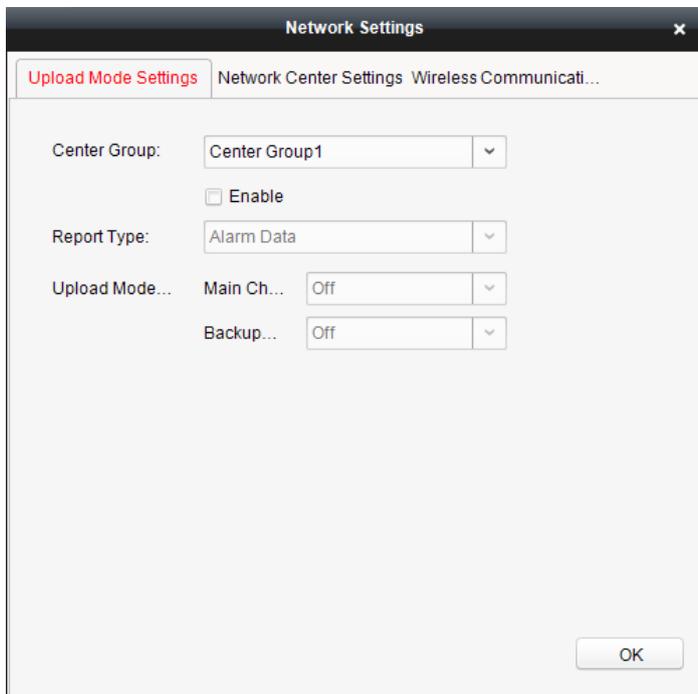


### Network Settings

#### **Purpose:**

In the network settings interface, the network settings of the device can be uploaded and reported.

#### **Uploading Mode Settings**



**Steps:**

1. In the access controller editing interface, click **Network Settings** button to enter the network settings interface.
2. Click the **Uploading Mode Settings** button.
3. Select the center group in the dropdown list.
4. Tick the **Enable** to enable the selected center group.
5. Select the report type in the dropdown list.
6. Select the uploading mode in the dropdown list. You can enable N1/G1 for the main channel and the backup channel, or select off to disable the

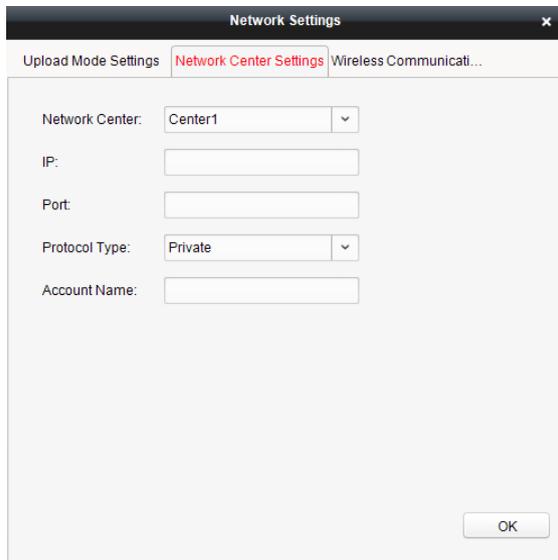
main channel or the backup channel.



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

7. Click the **OK** button to save parameters.

### Network Center Settings

A screenshot of a "Network Settings" dialog box. The dialog has a title bar with "Network Settings" and a close button. Below the title bar are three tabs: "Upload Mode Settings", "Network Center Settings" (which is selected and highlighted in red), and "Wireless Communicati...". The main area contains several fields: "Network Center:" with a dropdown menu showing "Center1"; "IP:" with an empty text box; "Port:" with an empty text box; "Protocol Type:" with a dropdown menu showing "Private"; and "Account Name:" with an empty text box. An "OK" button is located in the bottom right corner.

#### Steps:

1. In the access controller editing interface, click **Network Settings** button to enter the network settings interface.
2. Click the **Network Center Settings** button.
3. Select the network center in the dropdown list.

4. Input IP address.
5. Input port number.
6. Select the protocol type.
7. Set an account name for the network center. A consistent account should be used in one platform.
8. Click the **OK** button to save parameters.



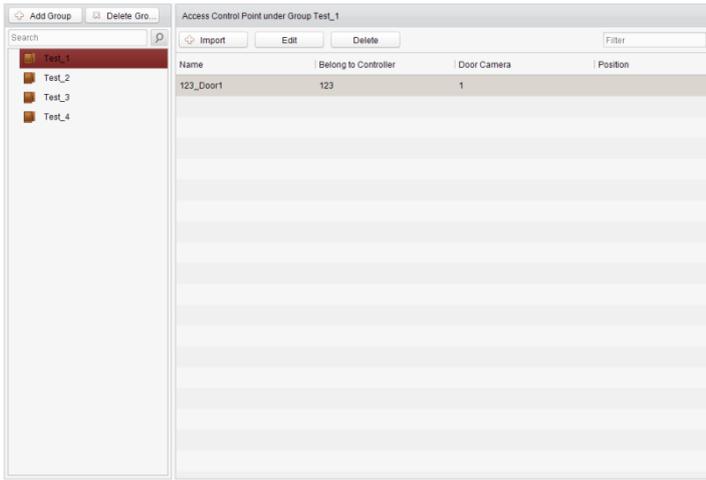
- In the Ehome protocol, the default port number is 7661, and the port type should be UDP port. Related settings files need modifying if the port type does not match.
- The port number of the wireless network and wired network should be consistent with the port number of Ehome.

## 7.2.2 Access Control Point Management

### Interface Introduction



Click the icon on the control panel to enter the door management interface.



### Group Management

The doors can be added to different groups to realize the centralized management.

### Door Management

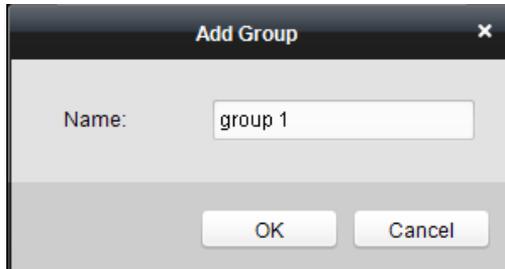
Manage the specific door under the door group, including importing, editing and deleting door.

### Group Management

#### ● Adding Group

#### Steps:

1. Click the  button to pop up the Add Group dialog.



2. Input the group name in the text field and click the  button to finish adding.



Multi-level groups are not supported yet.

- **Editing Group**

**Steps:**

Double-click the group or right-click the group and select Edit in the right-click menu.

- **Deleting Group**

To delete a group, three ways are supported.

- ◆ Click to select a group and click the  button.
- ◆ Right-click a group and select Delete in the popup menu.
- ◆ Move the mouse onto the group and click  icon of it. And then click the OK button in the popup window.

## Access Control Point Management

Access control points under the group can also be edited, refer to the following instructions.

- **Importing Access Control Point**

**Steps:**

1. Click the  button to pop up the access control point importing interface.
2. Select an access control point to import by clicking it.
3. Click to select a group in the right side bar to import to.
4. Click  button to import the selected access control points or click  to import all the available access control points.



- You can click  button on the upper-right corner of the window to create a new group.
- The control client can manage 100 access control points at most.

- **Editing Access Control Point**

**Steps:**

1. Click to select an access control point in the list and click the



button to edit the access control point.

2. Edit the Door Name and Position.



button to finish editing.



You can also enter the Edit interface by double clicking the door from the list.

- **Deleting Access Control Point**

Several ways are supported to delete the access control point, as shown below.

- ◆ Click to select a group in the group list, select door(s) under it, and click



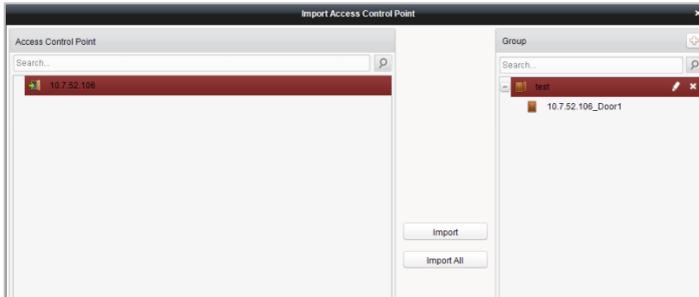
button.

- ◆ Click to select a group in the group list, and click  button to delete all access control points under the group.

- ◆ Move the mouse onto a group in the group list, and click  button to delete all access control points under the group.



You can also edit/delete a door on the Import Access Control Point panel.



**Steps:**

1. Select a control point on the **Group** panel.
2. Click the  /  icon to enter the **Edit Access Control Point** panel or to delete the control point.

## 7.3 Permission Management

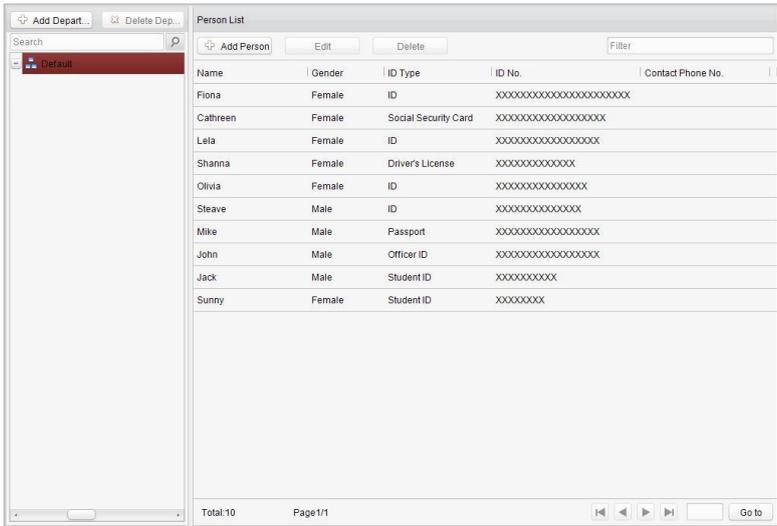
### 7.3.1 Person Management

#### Interface Introduction



Click the  icon on the control panel of the software.

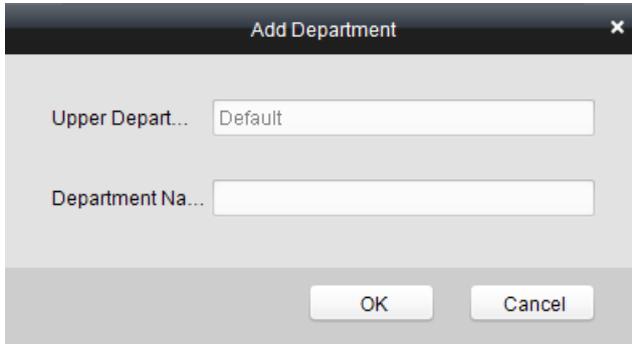
Adding, editing, deleting and filtering of the department and person are supported in this interface.



## Department Management

### Steps:

1. In the department list, click  button to pop up the adding department interface.



- ◆ Multi-level department system can be created. Click a department as the upper-level department and click  button, and then the added department will be the sub-department of it.
  - ◆ Up to 10 levels can be created.
2. You can double-click an added department to edit its name.
  3. You can click to select a department, and click the  button to delete it.



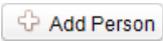
- ◆ The lower-level departments will be deleted as well if you delete a department.
- ◆ Make sure there is no person added under the department, or the department cannot be deleted.

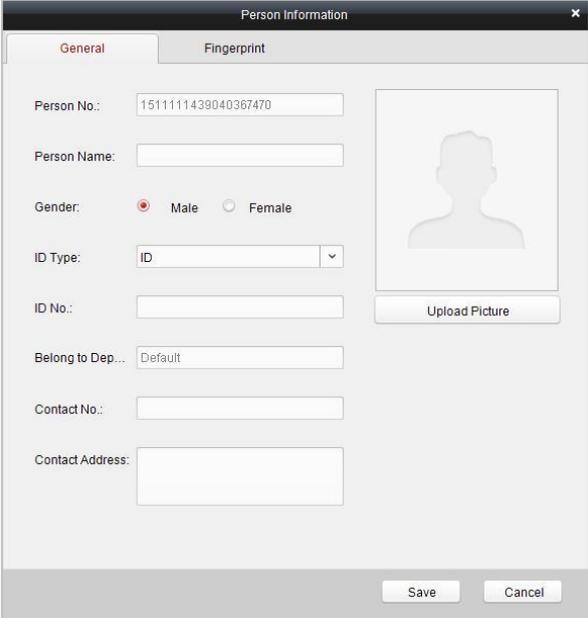
## Person Management



- ◆ In the person management interface, double-click the person name or click the Edit button to edit the person information.
- ◆ In the person management interface, click the Delete button to delete the person.
- ◆ Up to 2000 persons can be added.
- **Inputting General Information**

### **Steps:**

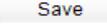
1. Select a department in the list and click the  in the person information list to pop up the adding person interface.



The image shows a 'Person Information' dialog box with two tabs: 'General' and 'Fingerprint'. The 'General' tab is active. It contains the following fields and controls:

- Person No.: Text box containing '1511111439040367470'
- Person Name: Empty text box
- Gender: Radio buttons for 'Male' (selected) and 'Female'
- ID Type: Dropdown menu showing 'ID'
- ID No.: Empty text box
- Belong to Dep...: Text box containing 'Default'
- Contact No.: Empty text box
- Contact Address: Empty text box

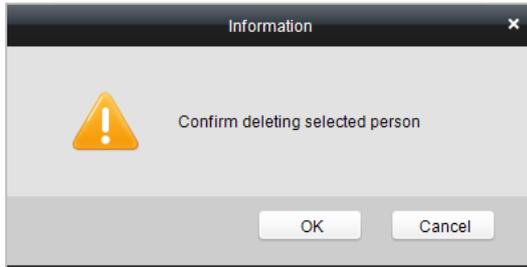
On the right side, there is a placeholder for a person's photo and an 'Upload Picture' button. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

2. Input the Person Name (required), Gender, ID Card, etc., upload the photo of the person and click the  icon to finish adding.



The format of the photo should be .jpg, or .jpeg.

3. You can double-click an added person to edit its information.
4. You can click to select a person, and click the  button to delete it.

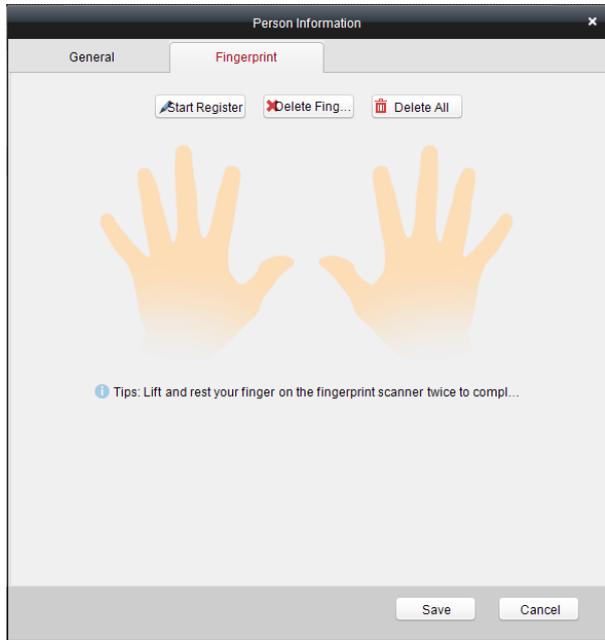


If a card is associated with the current person, the association will be invalid after the person is deleted.

- **Inputting Fingerprint**

**Steps:**

1. In the personal information interface, click the **Fingerprint** button.



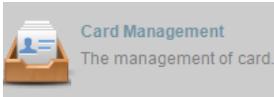
2. Click the **Start Register** button, and select the fingerprint to be input.
3. Click the **Save** button to save the parameter.

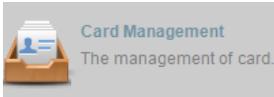


- Click the **Delete Fingerprint** button to delete the fingerprint.
- Click the **Delete All** button to clear all fingerprints input.
- Models DS-K2801, DS-K2802, and DS-K2804 do not support the fingerprint function.

## 7.3.2 Card Management

### Interface Introduction



Click  on the control panel of the software to enter the card management interface.



The cards are divided into 3 types: Blank Card, Normal Card, and Lost Card.

**Blank Card:** A card has not been issued with a person.

**Normal Card:** A card is issued with a person and is under normal using.

**Lost Card:** A card is issued with a person and is reported as lost.

### Blank Card

#### ● Adding Card

#### *Before you start:*

Make sure a card dispenser is connected to the PC and is configured already.

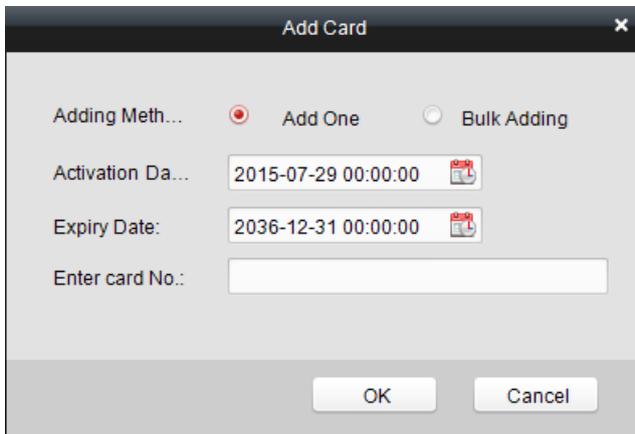
#### *Steps:*

1. Click the  button to add cards.

2. Two modes of adding cards are supported.

### Adding Single Card

Choose the Single Add as the adding mode by clicking the  to  and input the Start Date, Expiring Date and Card No. in the text field.



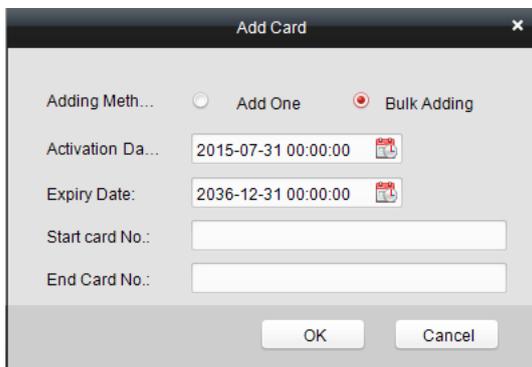
The screenshot shows a dialog box titled "Add Card". It features two radio buttons under the label "Adding Meth...". The "Add One" radio button is selected, while "Bulk Adding" is unselected. Below this, there are three input fields: "Activation Da..." containing "2015-07-29 00:00:00", "Expiry Date:" containing "2036-12-31 00:00:00", and "Enter card No.:" which is an empty text box. At the bottom of the dialog are "OK" and "Cancel" buttons.

### Batch Adding Cards

Choose the Bulking Adding as the adding mode by clicking the  to  and input the activation date, expiry date, start card No. and last card No. in the corresponding text fields.



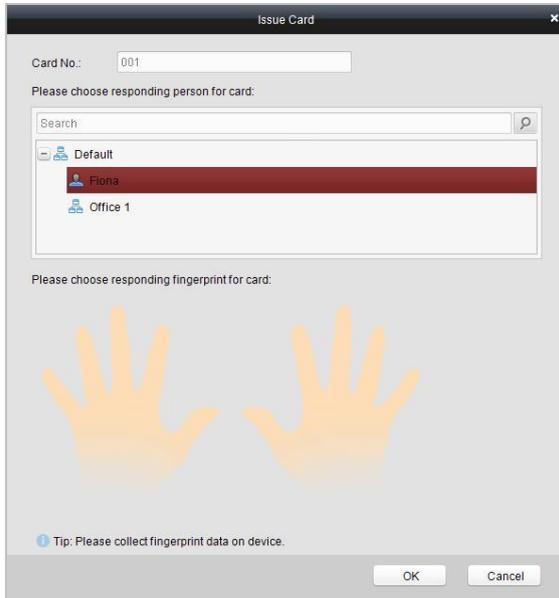
The start card No. and the last card No. should be in the same length. E.g., the last card No. is 234, then the start card No. should be like 028



3. Click the  button to finish adding.
4. Click an added blank card in the list and click  button to issue the card with a person.



You can double click the blank card in the card list to enter the **Issue Card** Page.



5. Click to choose a person on your demand in the popup dialog box, select a fingerprint, and click  to finish.

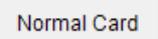


- The issued card will disappear from the Blank Card list, you can check the card information in the Normal Card list.
- Up to 2000 cards can be added.
- Models DS-K2801, DS-K2802, and DS-K2804 do not support the fingerprint function.

- **Deleting Card**

You can click an added blank card in the list and click  button to delete the selected card.

## Normal Card

Click the  tab in the card management interface to show the Normal Card list. You can view all the issued card information, including card No., card holder, and the department of the card holder.



Card No.	Status	Card Holder Name	Department
0001	Normal Card	Lela	Market Department
0002	Normal Card	Olivia	Market Department
0003	Normal Card	Shanna	Market Department
0004	Normal Card	Sam	Market Department
0005	Normal Card	Lemon	Market Department

- ◆ Click to select a card and click the **Card Change** button to change the associated card for card holder. Select another card in the popup window to replace the current card.
- ◆ Click to select an issued card and click the **Return Card** button to cancel the association of the card, and then the card will disappear from the Normal Card list, which you can find it in the Blank Card list.
- ◆ Click to select an issued card and click the **Report Card Loss** button to set the card as the Lost Card, that is, an invalid card.
- ◆ Click to select an issued card and click the **Password Settings** button to

set the password for the card, set the password in the text filed and click the **OK** button to finish setting.



The password will be required when the card holder swiping the card to enter to or exit from the door if you enable the card&password authentication on the advanced configuration page.

## Lost Card

Click the **Card Reported Loss** tab in the card management interface to show the Lost Card list. You can view all the lost card information, including card No., card holder, and the department of the card holder.

Empty Card	Normal Card	Card Reported Loss		
Card Loss List				
Cancel Card L...	Card Replace...			Filter
Card No.	Status	Replace card?	Card Holder Name	Department
123	Card Reported Loss	No	Lela	Default

- ◆ Click the **Cancel Card Loss** button to resume the card to the normal card.

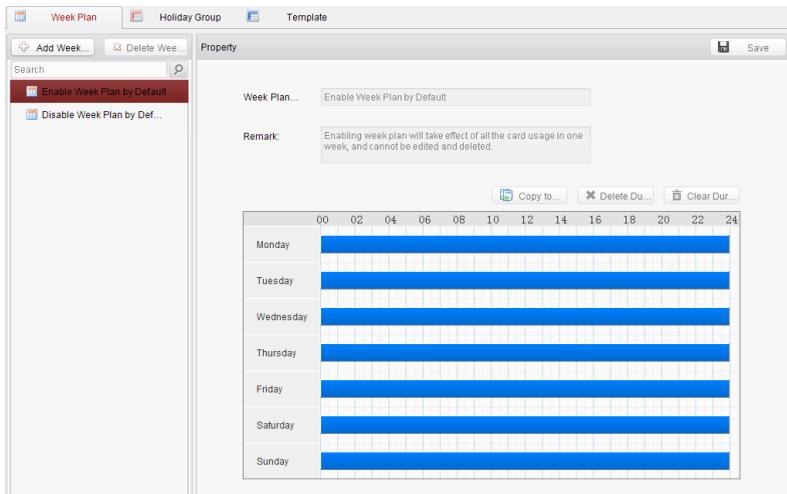
- ◆ Click the **Card Replacement** button to issue a new card to the card holder replacing for the lost card. Select another card in the popup window as the new card and the predefined permissions of the lost card will be copied to the new one automatically.

## 7.3.3 Schedule Template

### Interface Introduction



Click on the control panel of the software to enter the schedule template interface.



There are 3 settings in this interface: Week Plan, Holiday Plan, and Template.

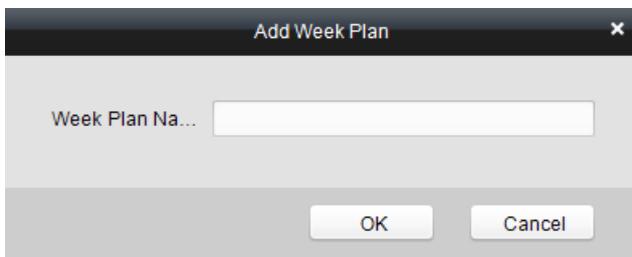
## Setting Week Plan

### ● Adding Week Plan

System defines 2 kinds of week plan by default, Enable Week Plan by Default and Disable Week Plan by Default. You can define custom plans on your demand.

#### **Steps:**

1. Click the **Add Week Plan** button to pop up the adding plan interface.



2. Input the name of week plan and click the **OK** button to add the week plan.
3. Select a week plan in the plan list on the left-side of the window to edit.
4. Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that period of time, the configured permission is activated.
5. Repeat the above step to configure other time periods.

Or you can select a configured day and click the **Copy to Week** button to copy the same settings to the whole week.

### ● Deleting Week Plan

- ◆ Click to select a configured duration and click the **Delete Duration**

button to delete it.

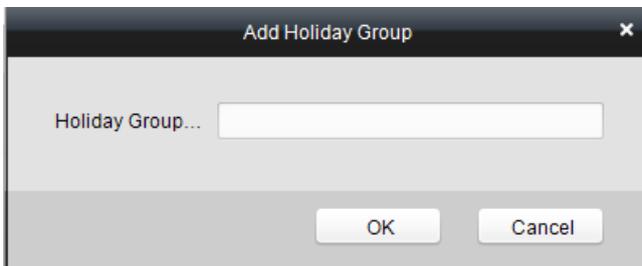
- ◆ Click the **Clear Duration** button to clear all the configured durations, while the week plan still exists.
- ◆ Click the **Delete Week Plan** button to delete the week plan directly.

## Setting Holiday Group

### ● Adding Holiday Group

#### **Steps:**

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



2. Input the name of holiday group in the text field, and click the  button to add the holiday group.

3. Click the  icon to add a holiday in the holiday list and configure the duration of the holiday.



At most 16 holiday periods can be added.

Holiday list					Add holiday	Previous	Next
Serial...	Start Time	End Time	Duration	Opera...			
1	2014-10-28	2014-10-29	00 02 04 06 08 10 12 14 16 18 20 22 24 				
2	2014-10-30	2014-11-01	00 02 04 06 08 10 12 14 16 18 20 22 24 				
3	2014-11-05	2014-11-08	00 02 04 06 08 10 12 14 16 18 20 22 24 				
4	2014-11-10	2014-11-12	00 02 04 06 08 10 12 14 16 18 20 22 24 				

- 1) Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that duration, the configured permission is activated.
  - 2) Click to select a configured duration and click the to delete it.
  - 3) Click the to clear all the configured durations, while the holiday still exists.
  - 4) Click the to delete the holiday directly.
4. Click the Save button to save the settings.



The holidays cannot be overlapped with each other.

## Setting Schedule Template

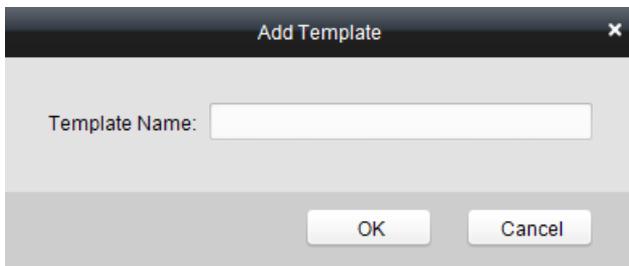
The schedule consists of week plan and holiday group; you can only choose which plan and group to enable in the schedule template configuration interface. Configure the week plan and holiday group before configuring the schedule template.



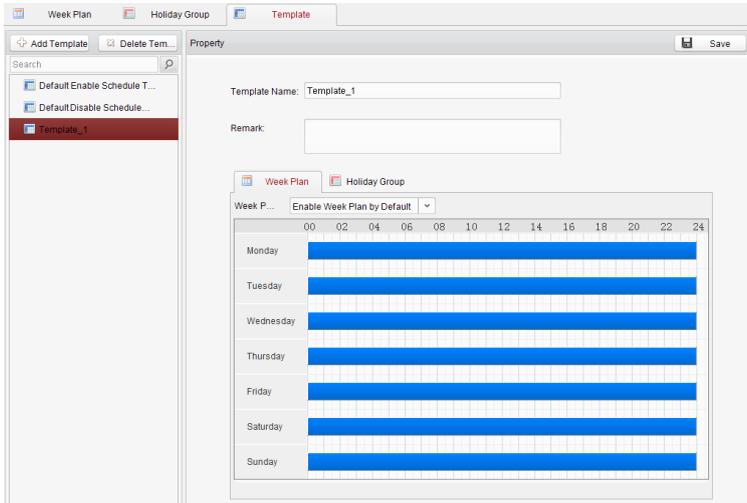
The priority of holiday group schedule is higher than the week plan.

### Steps:

1. Click the  to pop up the adding schedule interface.



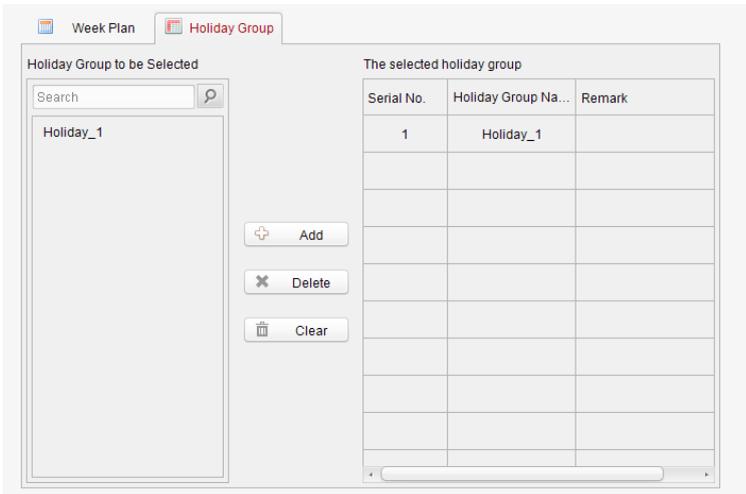
2. Input the name of schedule in the text field, and click the  button to add the schedule.
3. Select a week plan you want to apply to the schedule.  
Click the Week Plan tab and select a plan in the dropdown list.



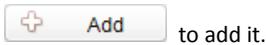
4. Select holiday groups you want to apply to the schedule.



At most 4 holiday groups can be added.



- ◆ Click to select a holiday group in the left-side list and click the



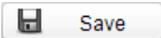
to add it.

- ◆ Click to select an added holiday group in the right-side list and click



the to delete it.

- ◆ Click the  to delete all the added holiday groups.

5. Click the  button to save the settings.

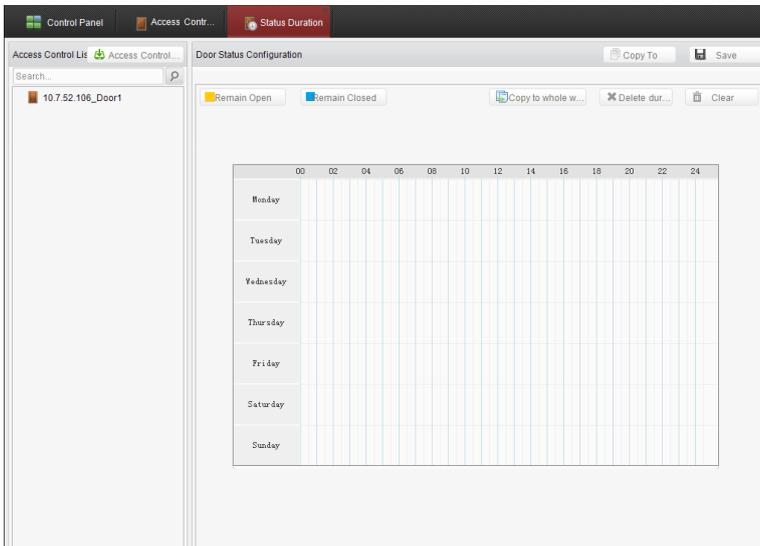
## 7.3.4 Door Status Management

### **Purpose:**

The function of **Door Status Management** allows you to schedule weekly time periods for a door to remain open or closed.



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



### **Steps:**

1. Enter the Door Status Management page.
2. Click and select a door from the door list on the left side of the page.
3. Draw a schedule map.

- 1) Select a door status brush

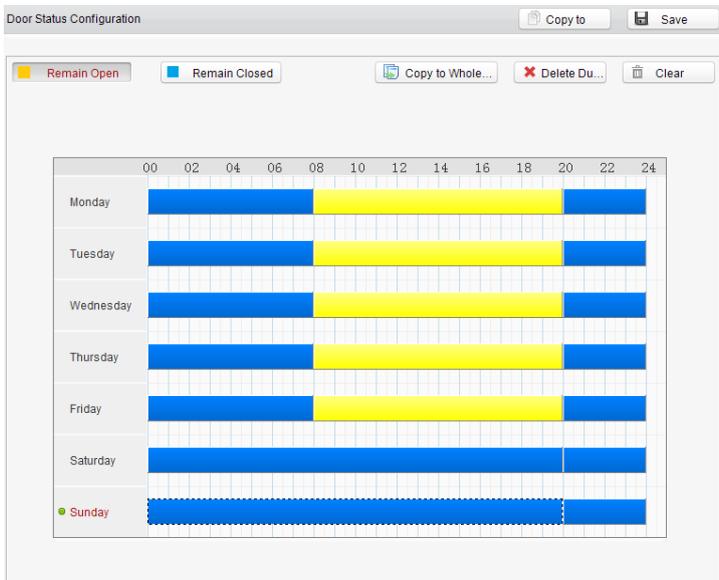


on the upper-left side of the **Door Status Settings** panel.

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

**Remain Closed:** the door will keep closed during the configured duration. The brush is marked as blue.

- 2) Click and drag the mouse to draw a color bar on the schedule map to set the duration.

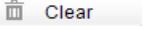


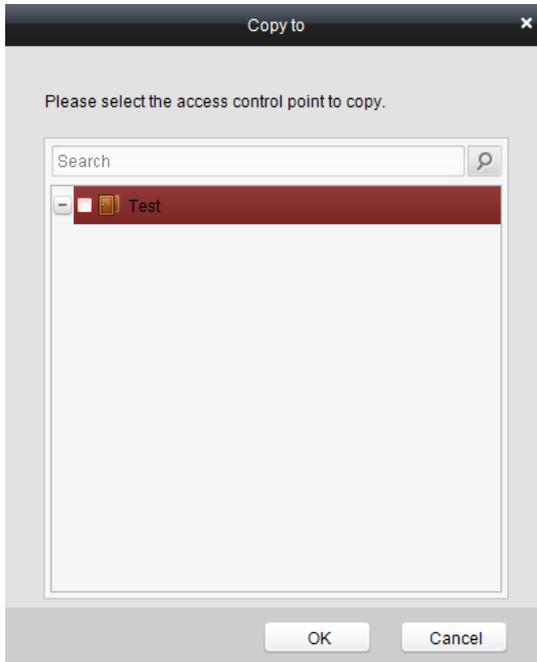
### Notes

- The min. segment of the schedule is 30 mins.
- You can copy the configured time periods of a day to the

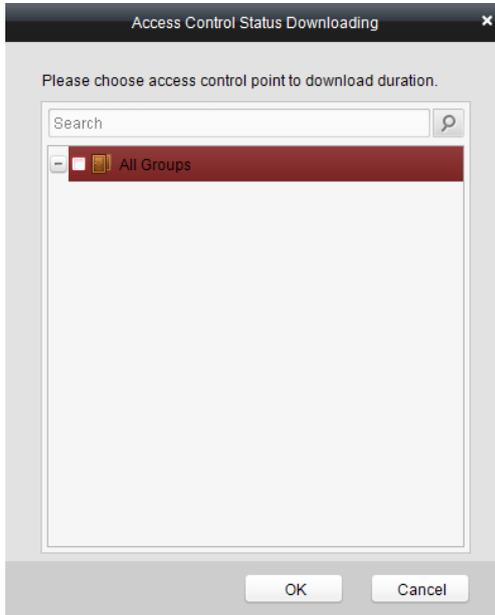
whole week.

**Steps:**

1. Select a day which has already been configured.
  2. Click on  to copy the time periods to the whole week.
4. Edit the schedule map.
- **Edit Duration:**  
Click and drag the color bar on the schedule map and you can move the bar on the time track.  
Click and drag the mouse on the ends of the color bar and you can adjust the length of the bar.
  - **Delete a Duration:**  
Click and select a color bar and click  to delete the time period.
  - **Clear All Durations:**  
Click  to clear all configured durations on the schedule map.
5. Click on  to save the settings.
6. You can copy the schedule to other doors by clicking on  and select the required doors.



7. Click on  **Access Control...** to enter the Download Door State page.

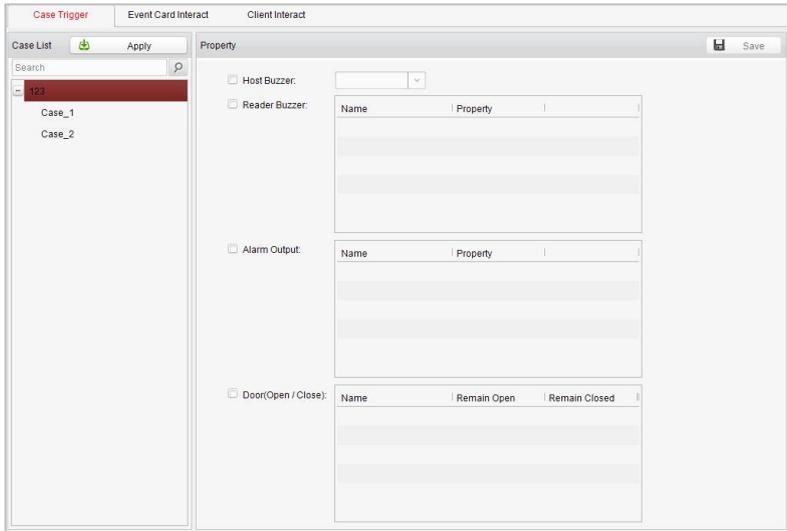


8. Select a control point and click **OK** to download the settings to the system.

### 7.3.5 Interact Configuration



Click  on the control panel of the software to enter the interact configuration interface.



In this interface, you can set alarm linkage modes of the access host, including case trigger, event card interact, and client interact.

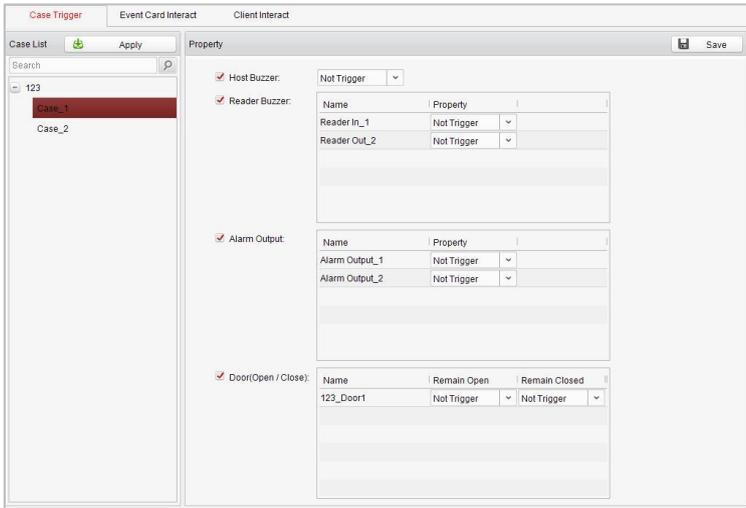
## Case Trigger

### ***Purpose:***

The case (refer to the triggers of the controller) can be linked to some actions (e.g., alarm output, host buzzer) when it is triggered.

### ***Steps:***

1. Click the  button to enter the case trigger interface, and select a case.



2. Check the checkbox of the corresponding linkage actions and set the property as **Trigger** to enable this function.

**Host Buzzer:** The audible warning of controller will be triggered.

**Reader Buzzer:** The audible warning of card reader will be triggered.

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

**Door (Open/Close):** The door will be open or closed when the case is triggered.

3. Click the **Save** button.
4. Click the **Apply** button to take effect of the new settings.



The Door cannot be configured as open or closed at the same time.

### Event Card Interact

In the Interact Configuration interface, click the **Event Card Interact** button to

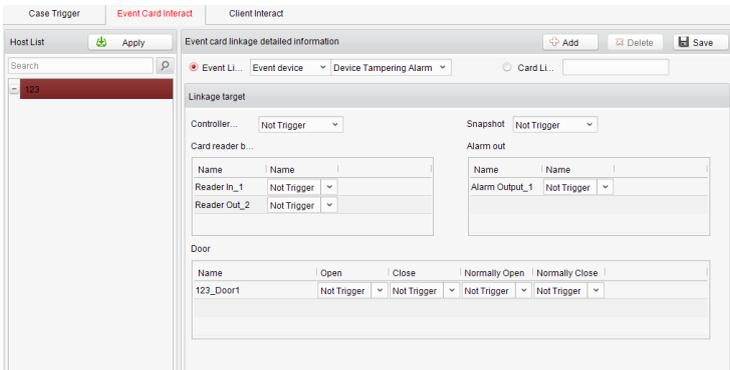
enter the settings interface.

- **Event Linkage**

In the Event Interact interface, the linkage alarm action, after triggering alarm event, can be set. The alarm event can be divided into four types: event device, event input alarm, door event, and card reader event.

**Steps:**

1. Click the **Event Card Interact** button to enter the event card interface
2. Select the host to be set from the host list.
3. Click the **+ Add** button to start setting the event linkage.



4. Click the radio button of the event linkage, and select the event type from the dropdown list.
5. Set the linkage target, and set the property as **Trigger** to enable this function.

**Host Buzzer:** The audible warning of controller will be triggered.

**Snapshot:** The real-time capture will be triggered.

**Reader Buzzer:** The audible warning of card reader will be triggered.

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

**Door:** The door status of open, close, normally open, and normally close will be triggered.



Models DS-K2801, DS-K2802, and DS-K2804 do not support the snapshot function.

6. Click the  button to save parameters.
7. Click the **Apply** button to download the updated parameters to the local memory of the device.

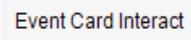


The door status of open, close, normally open, and normally close cannot be triggered at the same time.

- **Card Linkage**

In the Event Interact interface, the linkage alarm action, after triggering the card number, can be set.

**Steps:**

1. Click the  button to enter the event card interface
2. Select the host to be set from the host list.
3. Click the  button to start setting the event linkage.

4. Click the radio button of card linkage, and input the card number.
5. Select the event source, and check the checkbox of the card reader's serial number.
6. Set the linkage target, and set the property as **Trigger** to enable this function.

**Controller Buzzer:** The audible warning of controller will be triggered.

**Snapshot:** The real-time capture will be triggered.

**Reader Buzzer:** The audible warning of card reader will be triggered.

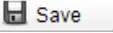
**Alarm Output:** The alarm output will be triggered for notification.

**Door:** The door status of open, close, normally open, and normally close will be triggered.



Models DS-K2801, DS-K2802, and DS-K2804 do not support the snapshot

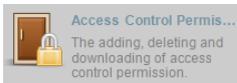
function.

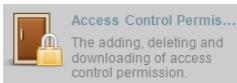
7. Click the  button to save parameters.
8. Click the **Apply** button to download the updated parameters to the local memory of the device.

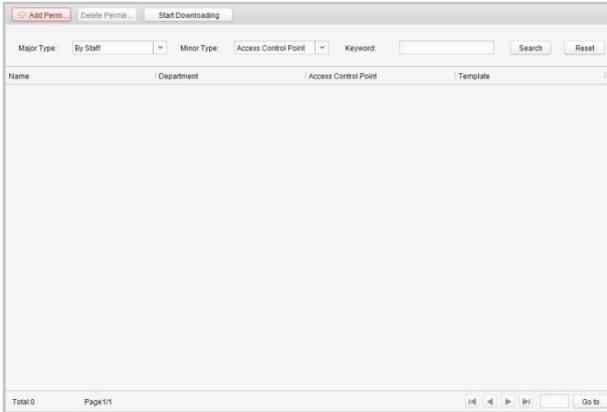


The door status of open, close, normally open, and normally close cannot be triggered at the same time.

## 7.3.6 Access Permission Configuration



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

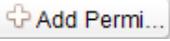


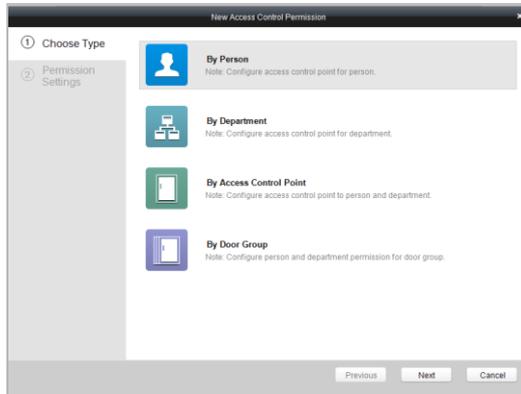
## Access Permission Settings

### ***Purpose:***

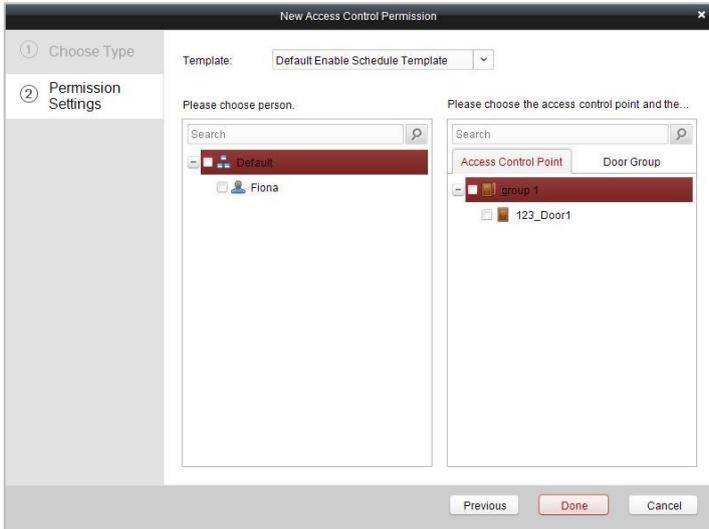
You can allocate permission for people/department to enter/exist the control points (doors) in this section.

### ***Steps:***

1. Enter the **Permission** page.
2. Click on  icon on the upper-left side of the page to enter the **Add Permission** page.



3. Select an adding type in the **Select Type** interface.
  - ◆ **By Person**: you can select people from the list to enter/exit the door.
  - ◆ **By Department**: You can select departments from the list to enter/exit the door. Once the permission is allocated, all the people in this department will have the permission to access the door.
  - ◆ **By Access Control Point**: You can select doors from the door list for people to enter/exit.
  - ◆ **By Door Group**: You can select groups from the door list for people to enter/exit. The permission will take effect on the door in this group.
4. Click Next to enter the Permission Settings interface.



5. Click on the dropdown menu to select a schedule template for the permission.



The schedule template must be configured before any permission settings. Refer to Section 7.3.3 Schedule Template for detailed configuration guide.

6. Select people/ department and corresponding doors/door groups from the appropriate lists.

Please choose person.

Search

 Default

 Lela

 Shannar

 Steve

Please choose the access control point and the...

Search

**Access Control Point** Door Group

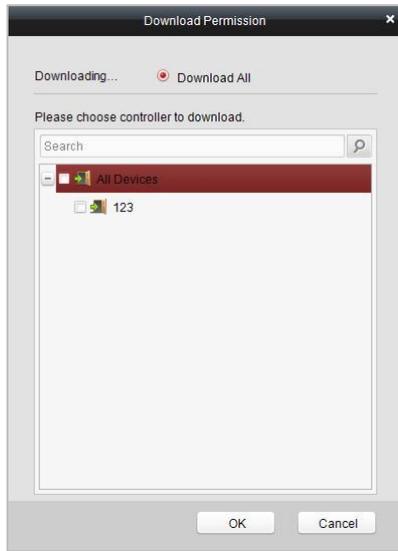
 Test

 Test\_Door1

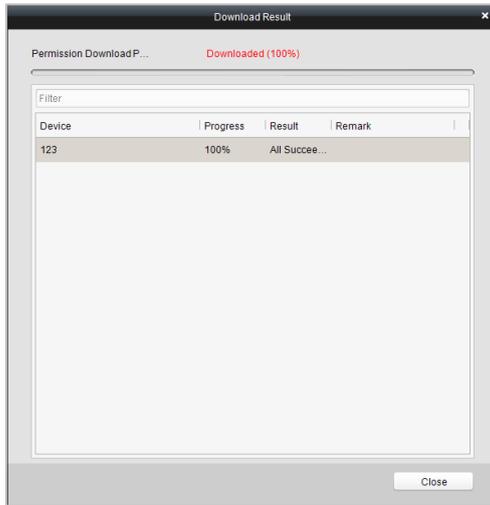


The lower-level of department will also be selected if the highest-level of department is selected,

7. Click the **Done** button to complete the permission adding.
8. Click [Start Downloading](#) to enter the **Download Permission** page.



9. Select a control point and click the **OK** button, to enter the download result interface, to download the permission to the device.



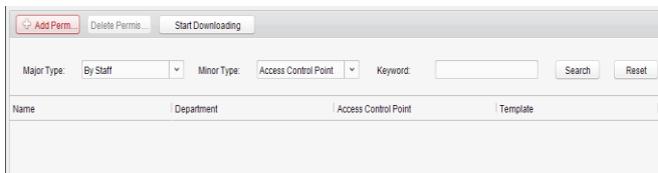
## Access Permission Searching

### **Purpose:**

After the permission settings being completed, you can search and view permission assigning condition on the searching interface.

### **Steps:**

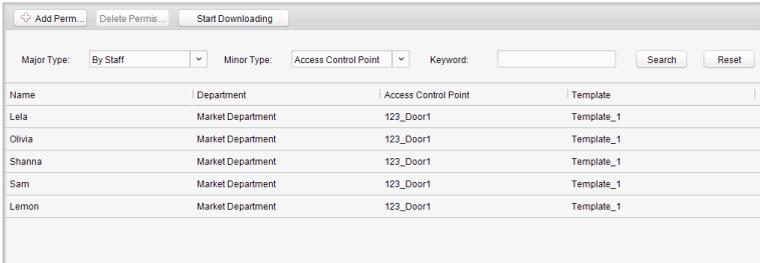
1. Enter the **Permission** page.



2. Enter the search criteria (main type/minor type/Keyword).



3. Click **Search** to get the search results.



Name	Department	Access Control Point	Template
Lela	Market Department	123_Door1	Template_1
Olivia	Market Department	123_Door1	Template_1
Shanna	Market Department	123_Door1	Template_1
Sam	Market Department	123_Door1	Template_1
Lemon	Market Department	123_Door1	Template_1

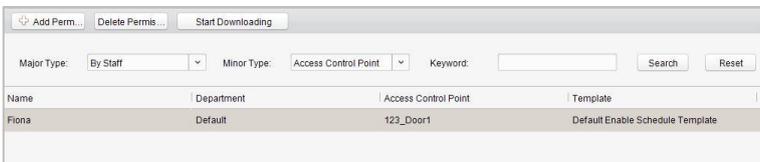


You can click **Reset** on the search criteria panel to clear all the displayed search results.

## Permission Deleting

### Steps:

1. Follow steps 1-3 in the Permission Searching section to search for the permission needs to be deleted.
2. Select the permission from the results list.

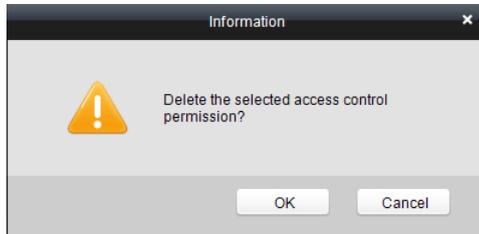


Name	Department	Access Control Point	Template
Fiona	Default	123_Door1	Default Enable Schedule Template

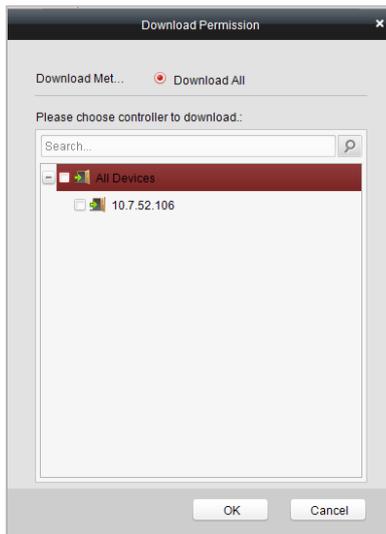


You can press the Ctrl or Shift key on the keyboard,

3. Click the **Delete Permission** button to delete the permission.



4. Click **Start Downloading** to enter the **Download Permission** page.

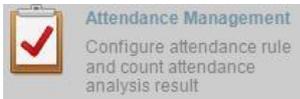


5. Select a control point and click the **OK** button to download the deletion operation to the device.

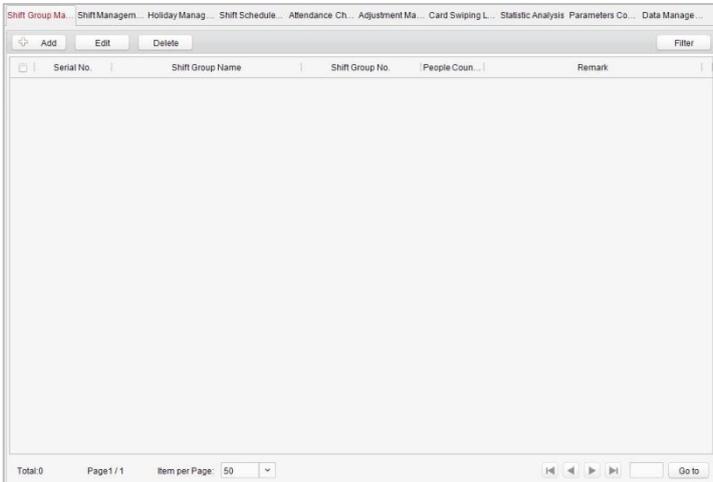
## 7.3.7 Attendance Management

**Purpose:**

On the attendance management interface, various functions can be implemented such as shift group management, shift management, holiday management, shift schedule, and so on.



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



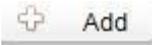
### Shift Group Management

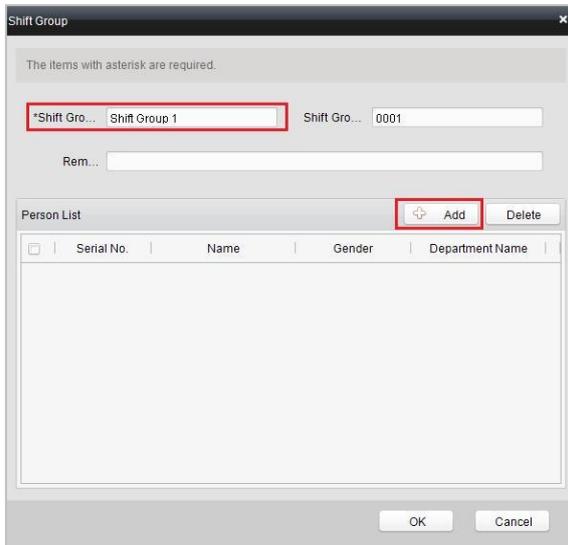
**Purpose:**

On the shift group management interface, you can add, edit, and delete shift

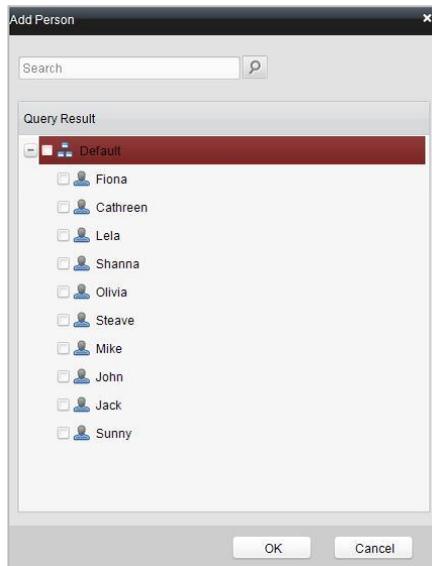
groups for attendance management.

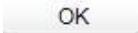
**Steps:**

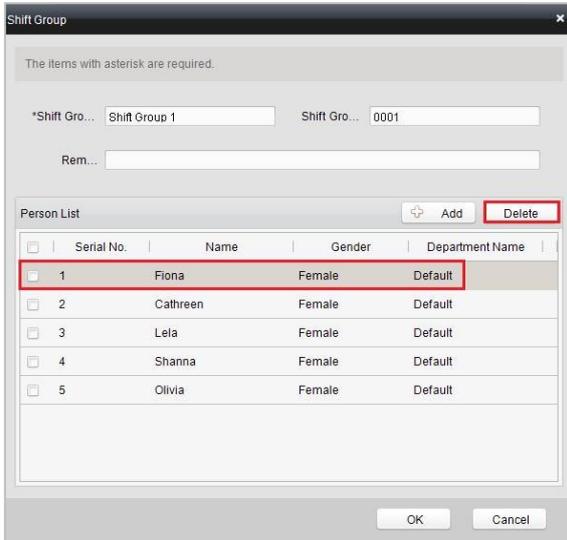
1. Click the  button to pop up the shift group formation window.



2. Enter the shift group name, and click the  button on the person list area to pop up the person adding window.

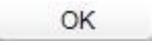


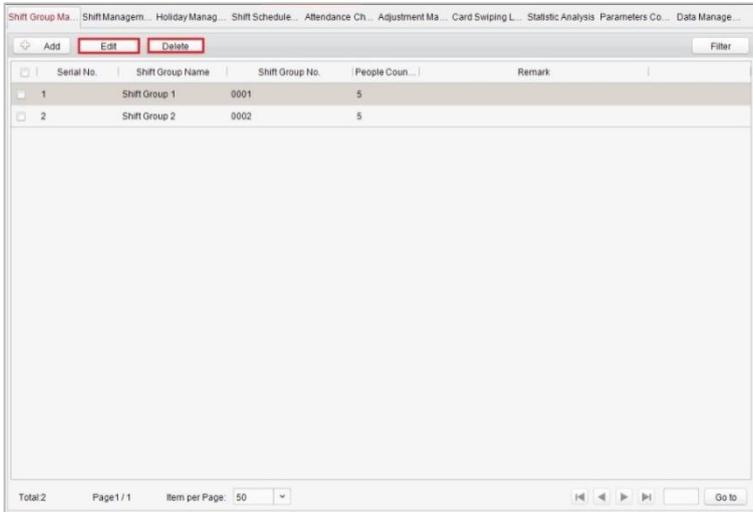
3. Check the checkbox(es) of persons to be added and click the  button and return to the shift group settings interface.



To delete the added person, check the person from the person list, and

click the  button.

4. Click the  button to complete the operation.



You can edit and delete the added shift groups by clicking the

Edit

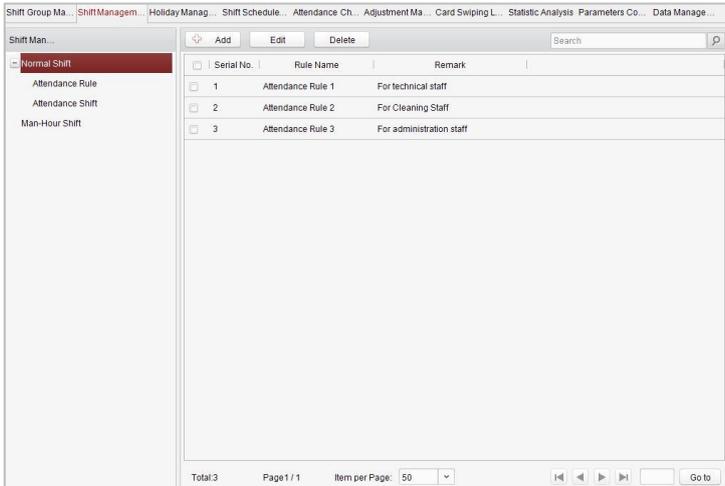
and

Delete

buttons.

## Shift Management

Press the Shift Management tab to enter the shift management interface.

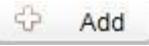


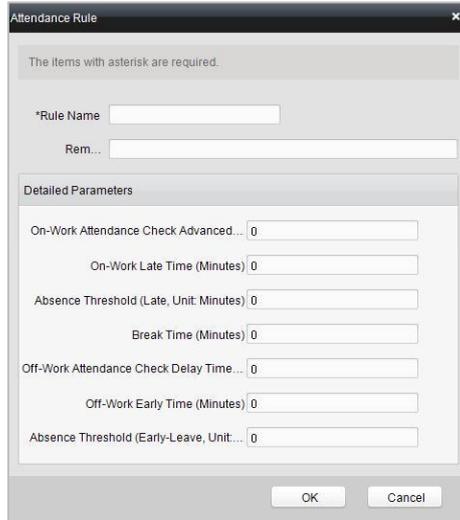
There are two kinds of shifts in this interface: **Normal Shift**, and **Man-Hour Shift**.

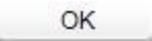
## Normal Shift

- **Setting Attendance Rule**

### *Steps:*

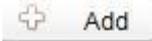
1. Click the  button to pop up the attendance rule setting window.



2. Set a rule name.
3. Set detailed parameters for the attendance rule: on-work attendance check advance time, on-work late time, absence threshold, break time, off-work attendance check delay time, off-work early time, and absence threshold (early leave).
4. Click the  button to complete the operation.

● **Setting Attendance Shift**

**Steps:**

1. Click the  button to pop up the attendance shift setting window.

The items with asterisk are required.

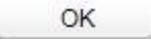
\*Shift Name:  Shift No.: 0001

Rem...

Off/On-Work Period Clear

	On-Work Time	Off-work time	Attendance Rule
<input type="checkbox"/> On-Work Ti...	Day <input type="text"/>	Day <input type="text"/>	<input type="text"/>
<input type="checkbox"/> On-Work Ti...	Day <input type="text"/>	Day <input type="text"/>	<input type="text"/>
<input type="checkbox"/> On-Work Ti...	Day <input type="text"/>	Day <input type="text"/>	<input type="text"/>

OK Cancel

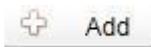
2. Set a shift name.
3. Set on-work duration for the shift, and select the attendance rule.
4. Click the  button to complete the operation.



The format of on-work time and off-work time should be 00:00 to 23:59.

### Man-Hour Shift

#### Steps:

1. Click the  button to pop up the man-hour shift setting window.

The items with asterisk are required.

\*Shift Name:  \*Shift No.: 0002

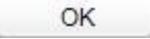
\*Daily working...   Latest On-Work...

Rem...

Disregard Man-Hour Period Clear

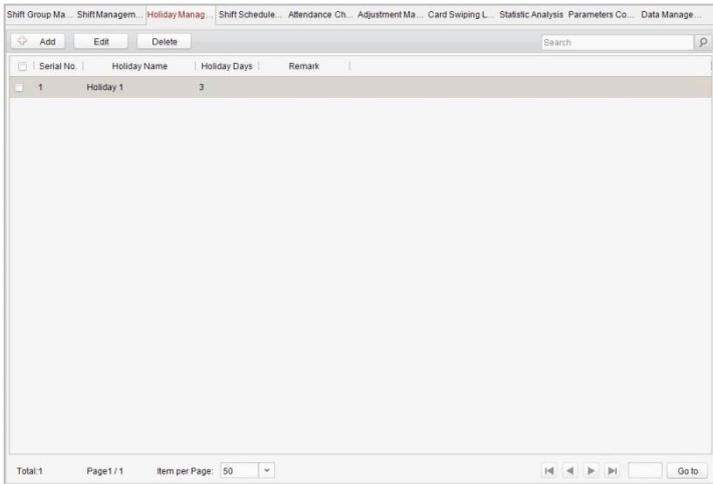
	Time Period	Start Time	End Time
<input type="checkbox"/>	Time Period1	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Time Period2	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Time Period3	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Time Period4	<input type="text"/>	<input type="text"/>

OK Cancel

2. Set a shift name, and daily working duration.
3. (Optional) Check the checkbox of latest on-work time, and set the latest on-work time.
4. (Optional) Set the disregard man-hour period.
5. Click the  button to complete the operation.

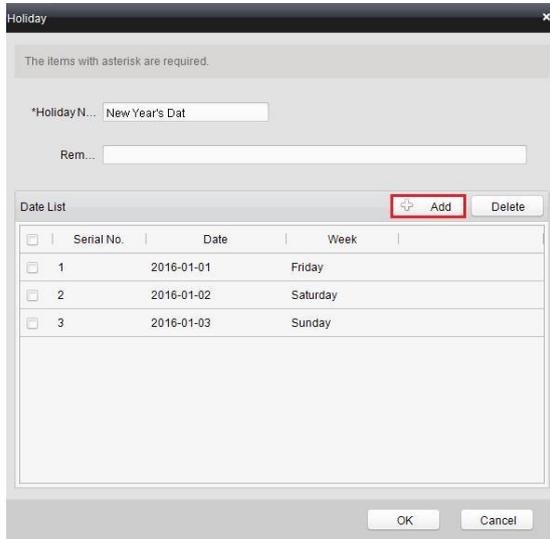
## Holiday Management

Press the **Holiday Management** tab to enter the holiday management interface.

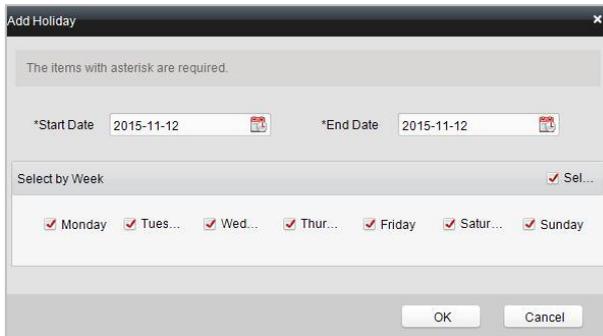


### Steps:

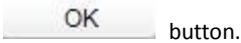
1. Click the  **Add** button to pop up the holiday setting window.



2. Click the  **Add** button to pop-up holiday adding window.



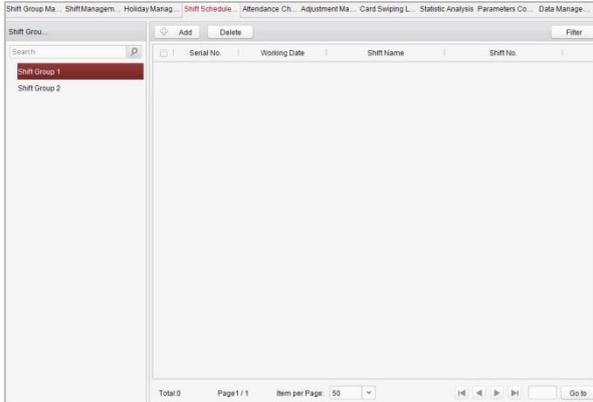
3. Set the start date and end date, select the date of week, and click the



button.

## Shift Schedule Management

Press the **Shift Schedule Management** tab to enter the shift schedule management interface.



### Steps:

1. Press a tab of shift group on the shift group list.
2. Click the  button to pop up the shift schedule settings window.

Remark

Shift Group: group1      Shift Name: Normal Shift1

\*Start Date: 2015-11-12      \*End Date: 2015-11-12

Add Holiday

<input type="checkbox"/>	Serial No.	Holiday Name	Holiday Days	Remark
<input checked="" type="checkbox"/>	1	Holiday 1	3	
<input type="checkbox"/>				

OK      Cancel

3. Select the shift name from the drop-down list.
4. Set the start data and end data.
5. (Optional) Check the checkbox of holiday to add the holiday shift.
6. Click the  button to complete the operation.

### Attendance Check Point Management

Press the **Attendance Check Point Management** tab to enter the attendance check point management interface.

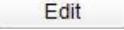
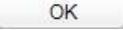
## DS-K2800 Series Access Controller

Serial No.	Attendance Checking Point Name	Attendance Check...	Start Date	Validity	Door Position	Reader Name	Attendance Checking Point Description
1	123_Door1_Checking Point_1	On/Off Work Che...	2015-11-12	2015-11-12		Reader In_1	
2	123_Door1_Checking Point_2	On/Off Work Che...	2015-11-12	2015-11-12		Reader Out_2	
3	456_Door1_Checking Point_3	On/Off Work Che...	2015-11-12	2015-11-12		Reader In_1	
4	456_Door1_Checking Point_4	On/Off Work Che...	2015-11-12	2015-11-12		Reader Out_2	

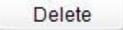
### ● Adding Attendance Check Point

#### Steps:

Serial No.	Attendance Checking Point Name	Attendance Check...	Start Date	Validity	Door Position	Reader Name	Attendance Checking Point Description
1	123_Door1_Checking Point_1	On/Off Work Che...	2015-11-12	2015-11-12		Reader In_1	
2	123_Door1_Checking Point_2	On/Off Work Che...	2015-11-12	2015-11-12		Reader Out_2	
3	456_Door1_Checking Point_3	On/Off Work Che...	2015-11-12	2015-11-12		Reader In_1	
4	456_Door1_Checking Point_4	On/Off Work Che...	2015-11-12	2015-11-12		Reader Out_2	

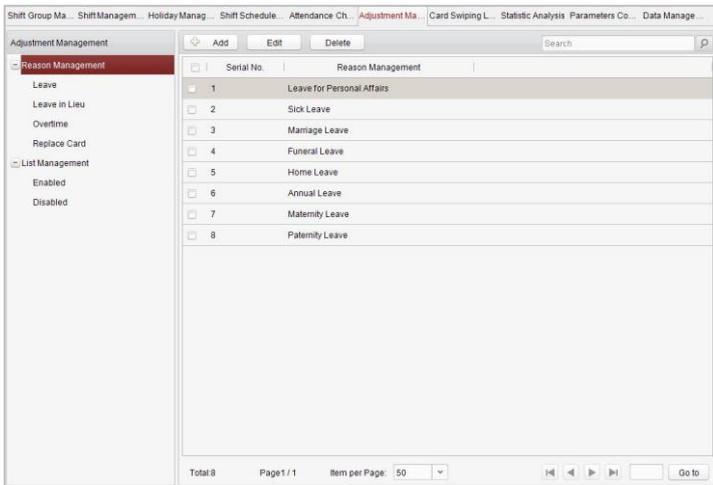
1. Check the checkbox of a checking point, and click the  button to pop up the attendance checking point editing window.
2. Edit the attendance checking point name, start date, validity, and attendance checking point type, controller name, door position, and reader name.
3. Click the  button to complete the operation.

● **Adding Attendance Check Point**

Check the checkbox of a checking point and click the  button to delete the added checking point.

### Adjustment Management

Press the **Adjustment Management** tab to enter the adjustment management interface.



On this interface, **Reason Management** and **List Management** can be realized.

### Reason Management

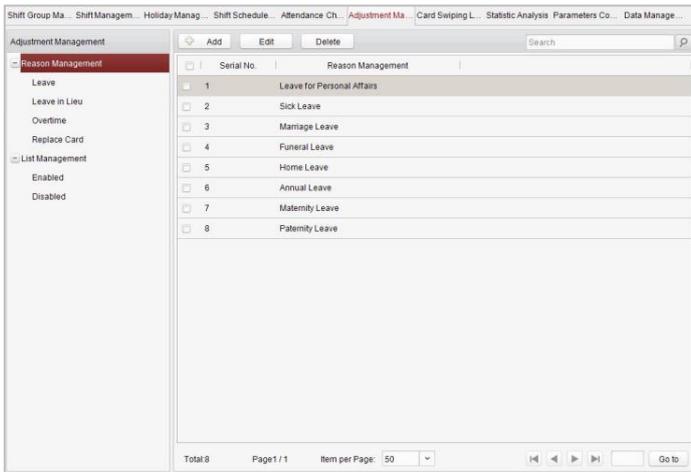
- **Leave**

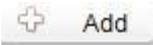
**Purpose:**

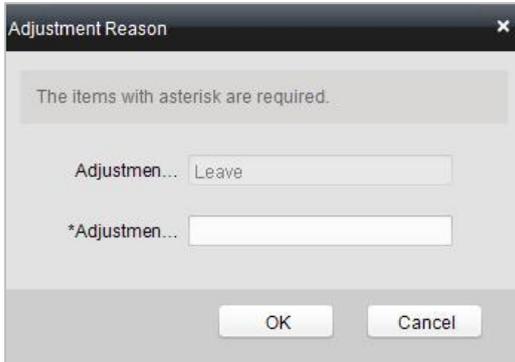
You can add, edit, and delete reasons for leave on the leave interface.

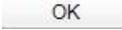
**Steps:**

1. Press the leave tab to enter the leave interface.

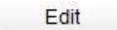


2. Click the  **Add** button to pop up the adjustment reason adding dialog box.



3. Enter the adjustment reason, and click the  button.

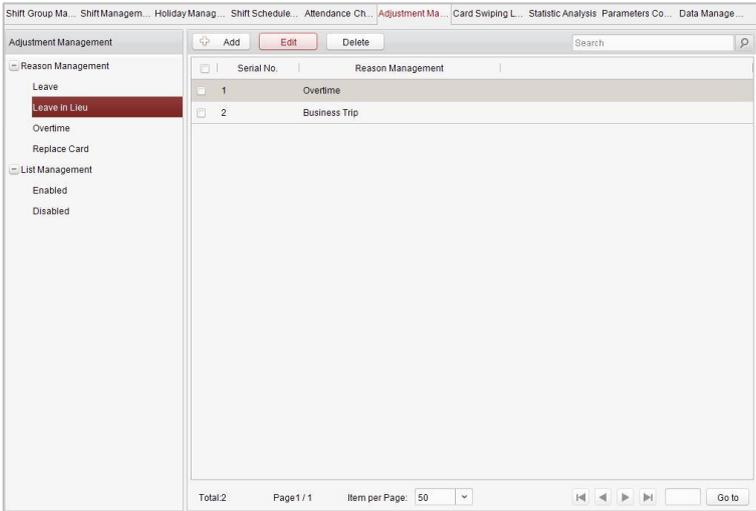


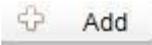
- The default adjustment reasons include leave for personal affairs, sick leave, marriage leave, funeral leave, home leave, annual leave, maternity leave, and paternity leave.
- You can check the checkbox of a reason and click the  button to edit the reason, and click the  button to delete the reason.

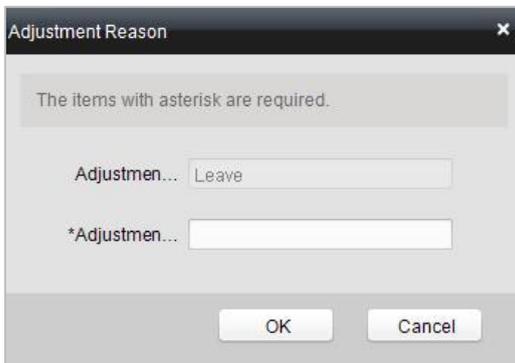
- **Leave in Lieu**

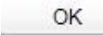
**Steps:**

1. Press the leave in lieu tab to enter the leave-in-lieu interface.

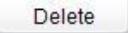


2. Click the  **Add** button to pop up the adjustment reason adding dialog box.



3. Enter the adjustment reason, and click the  **OK** button.

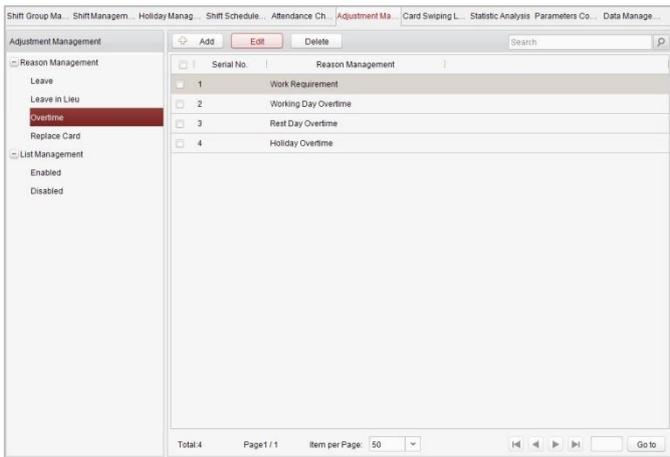


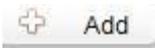
- The default adjustment reasons for leave in lieu include overtime, and business trip.
- You can check the checkbox of a reason and click the  button to edit the reason, and click the  button to delete the reason.

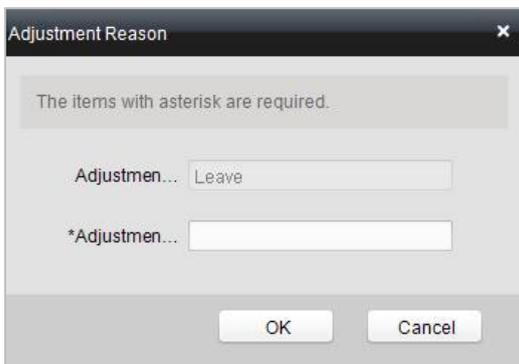
● **Overtime**

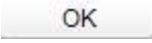
**Steps:**

1. Press the overtime tab to enter the overtime interface.



2. Click the  button to pop up the adjustment reason adding dialog box.



3. Enter the adjustment reason, and click the  button.



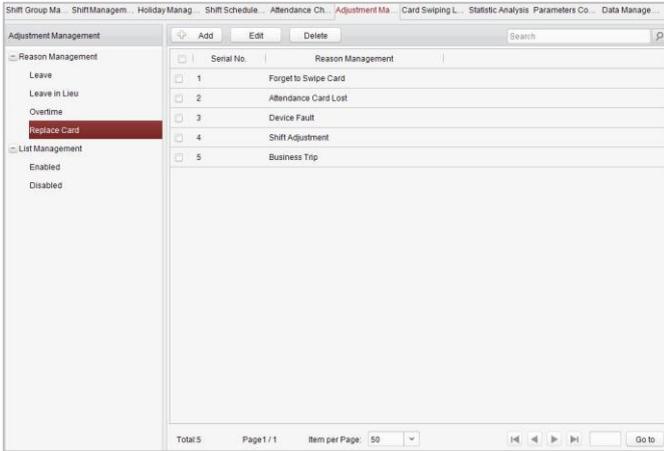
- The default adjustment reasons for overtime include work requirement, working day overtime, rest day overtime, and holiday overtime.

- You can check the checkbox of a reason and click the  button to edit the reason, and click the  button to delete the reason.

- **Replace Card**

**Steps:**

1. Press the replace card tab to enter.



- Click the  **Add** button to pop up the adjustment reason adding dialog box.

The dialog box is titled 'Adjustment Reason' and contains the following text and fields:

The items with asterisk are required.

Adjustmen...

\*Adjustmen...

At the bottom of the dialog box, there are two buttons: **OK** and **Cancel**.

- Enter the adjustment reason, and click the  **OK** button.



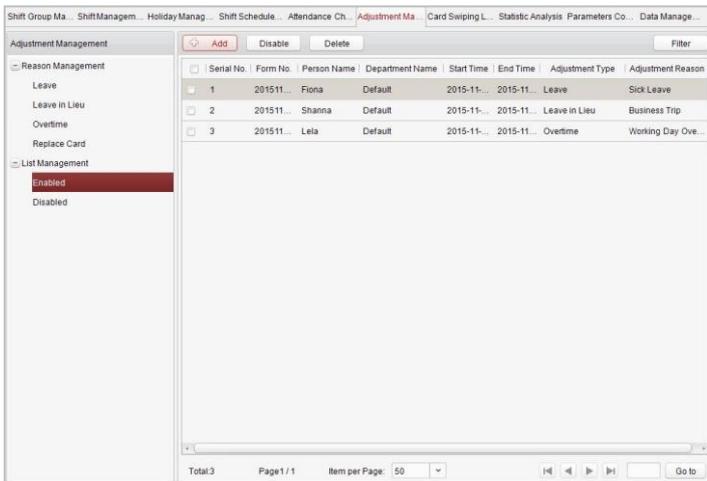
- The default adjustment reasons for card replacing include forget to swipe card, attendance card lost, device fault, shift adjustment, and business trip.
- You can check the checkbox of a reason and click the  button to edit the reason, and click the  button to delete the reason.

## List Management

### ● Enabling

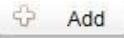
#### Steps:

1. Press the **Enabled** tab to enter the enabled list interface.



The screenshot shows the 'Adjustment Management' interface. The left sidebar has 'List Management' expanded with 'Enabled' selected. The main area displays a table with columns: Serial No., Form No., Person Name, Department Name, Start Time, End Time, Adjustment Type, and Adjustment Reason. There are three rows of data. Below the table, it shows 'Total: 3', 'Page 1 / 1', and 'Item per Page: 50'.

Serial No.	Form No.	Person Name	Department Name	Start Time	End Time	Adjustment Type	Adjustment Reason
1	201511...	Fiona	Default	2015-11-...	2015-11-...	Leave	Sick Leave
2	201511...	Shanna	Default	2015-11-...	2015-11-...	Leave in Lieu	Business Trip
3	201511...	Lela	Default	2015-11-...	2015-11-...	Overtime	Working Day Ove...

2. Click the  button.

Adjustment Form

Adjustme...  Leave  Lea...  Ove...  Rep...

Adjustme... Leave for Personal Aff... ▼

Staff:

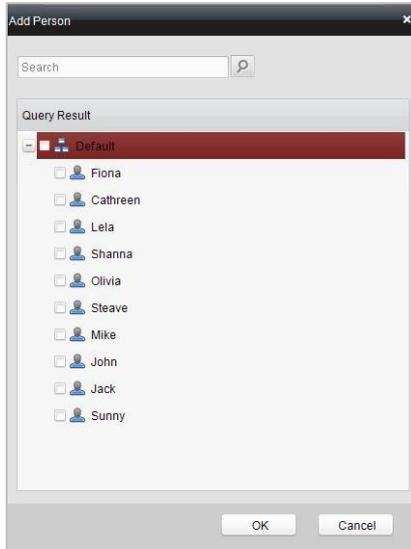
<input type="checkbox"/>	Serial No.	Name	Gender	Depart
--------------------------	------------	------	--------	--------

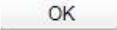
Time Period: 2015-11-12 00:00:00  -- 2015-11-12 23:59:59

3. Select the radio button of adjustment type: leave, leave in lieu, overtime, and replace card.

**Leave, Leave in Lieu, and Overtime**

- 1) Select the adjustment reason from the drop-down list.
- 2) Click the  button to pop up the person adding window.



- 3) Select the person and click the  button.
- 4) Set the time period.

**Replace Card**

- 1) Select the radio button of replace card.

Adjustment Form

Adjustme...  Leave  Lea...  Ove...  Rep...

Adjustme... Forget to Swipe Card

Staff:

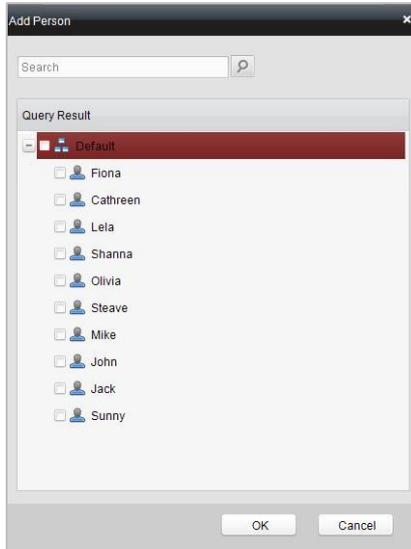
<input type="checkbox"/>	Serial No.	Name	Gender	Depart...
--------------------------	------------	------	--------	-----------

Select Date: 2015-11-12 Atten... Normal Shift

Card Repl...  Time...  On-...  Off-...  
 Time...  On-...  Off-...  
 Time...  On-...  Off-...

OK Cancel

- 2) Select the adjustment reason from the drop-down list.
- 3) Click the  **Add** button to pop up the person adding window.

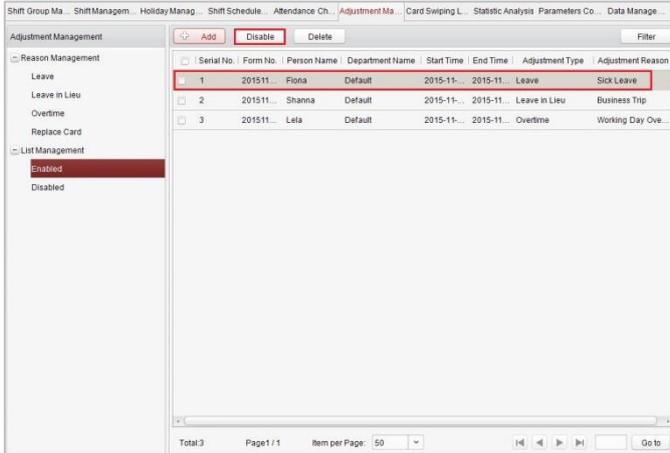


- 4) Select the person and click the  button.
  - 5) Set the date, attendance shift, and card replacing time.
4. Click the  button to complete the operation

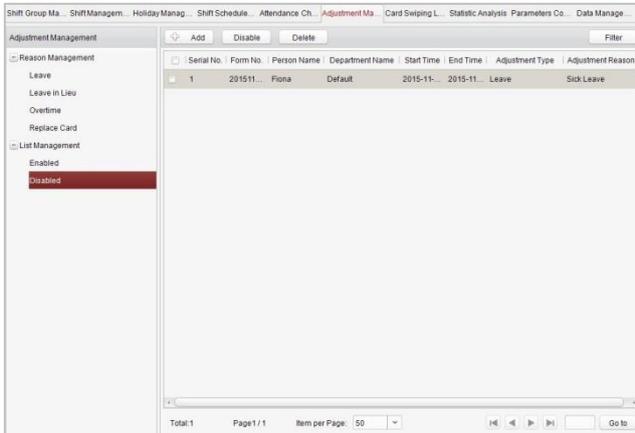
● **Disabling**

**Steps:**

1. Check the checkbox of a piece of enabled information.

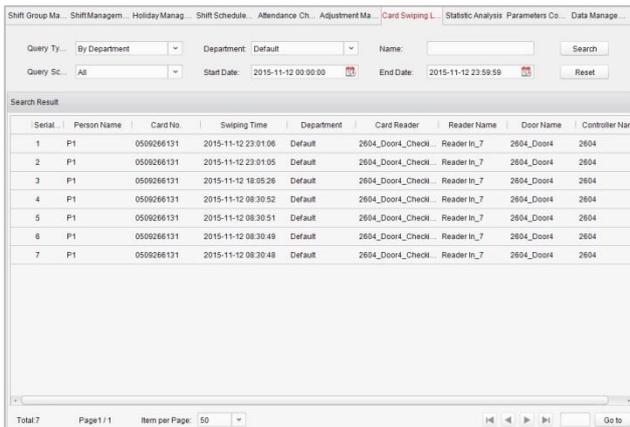


2. Click the **Disable** button to disable the information.
3. Press the **Disabled** tab and the disabled information will be listed on the disabled interface.



## Card Swiping Log Query

Press the **Card Swiping Log Query** tab to enter the card swiping log searching and viewing interface.





- You can search the card swiping log by two query types: **By Shift Group**, and **By Department**.
- You can search the card swiping log by group name.
- You can search the card swiping log by start date and end date.
- You can restrict the query scope: **All**, **First**, or **Last**.

## Statistic Analysis

Press the **Statistic Analysis** tab to enter the statistic analysis interface.

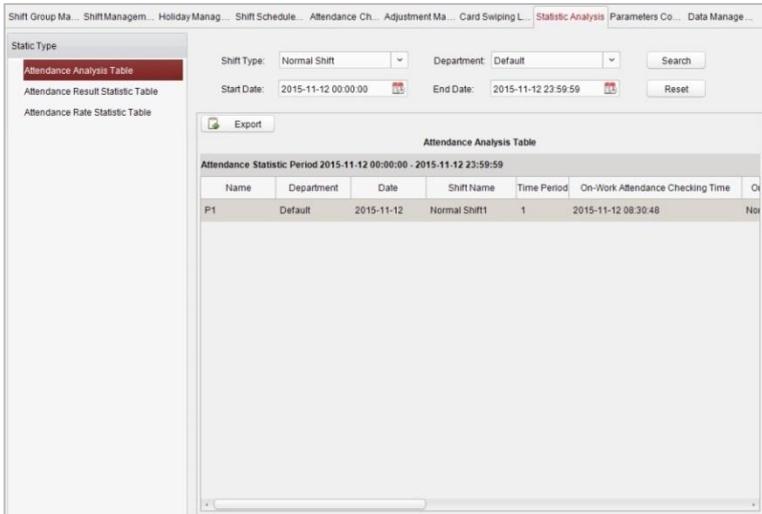
The screenshot shows the 'Statistic Analysis' interface. At the top, there are navigation tabs: 'Shift Group Ma...', 'Shift Managem...', 'Holiday Manag...', 'Shift Schedule...', 'Attendance Ch...', 'Adjustment Ma...', 'Card Swiping L...', 'Statistic Analysis' (selected), 'Parameters Co...', and 'Data Manage...'. Below the tabs, there are search filters: 'Shift Type' (Normal Shift), 'Department' (Default), 'Start Date' (2015-11-12 00:00:00), and 'End Date' (2015-11-12 23:59:59). There are 'Search' and 'Reset' buttons. An 'Export' button is also present. The main area is titled 'Attendance Analysis Table' and contains a table with the following columns: 'Name', 'Department', 'Date', 'Shift Name', 'Time Period', 'On-Work/Attendanc...', 'On-Work Status', and 'O'. The table is currently empty.

On the statistic analysis interface, you can search the attendance analysis table, attendance result statistic table, and attendance rate statistic table.

### Attendance Analysis Table

Press the **Attendance Analysis Table** tab to enter the attendance analysis

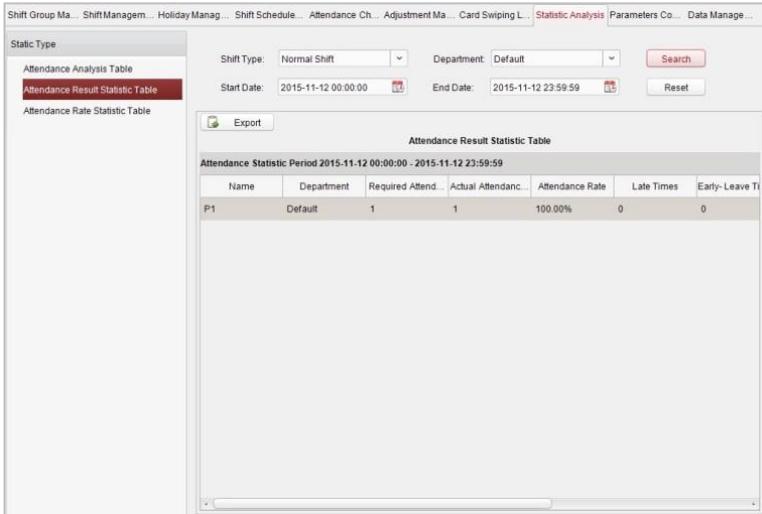
interface.



- You can search the attendance statistics by different shift type: **Normal Shift**, or **Man-Hour Shift**.
- You can search the attendance statistics by department.
- You can search the attendance statistics by start date and end date.

#### Attendance Result Statistic Table

Press the **Attendance Result Statistic Table** tab to enter the attendance result analysis interface.



- You can search the attendance result statistics by different shift type: **Normal Shift**, or **Man-Hour Shift**.
- You can search the attendance result statistics by department.
- You can search the attendance result statistics by start date and end date.

#### Attendance Rate Statistic Table

Press the **Attendance Rate Statistic Table** tab to enter the attendance rate analysis interface.

The screenshot displays the 'Statistic Analysis' tab of the DS-K2800 Series Access Controller software. The interface includes a navigation menu on the left with options like 'Attendance Analysis Table', 'Attendance Result Statistic Table', and 'Attendance Rate Statistic Table'. The main area shows search filters for 'Shift Type' (Normal Shift), 'Department' (Default), 'Start Date' (2015-11-12 00:00:00), and 'End Date' (2015-11-12 23:59:59). An 'Export' button is visible above the table. The table itself is titled 'Attendance Rate Statistic Table' and shows data for the period '2015-11-12 00:00:00 - 2015-11-12 23:59:59'. The table has columns for Name, Department, Date, Shift Name, Day Required At., Day Actual Atten., and Day Attendance. A single row is displayed for 'P1' in the 'Default' department on '2015-11-12' for 'Normal Shift1', with 1 day required, 1 day actual, and 100.00% attendance.

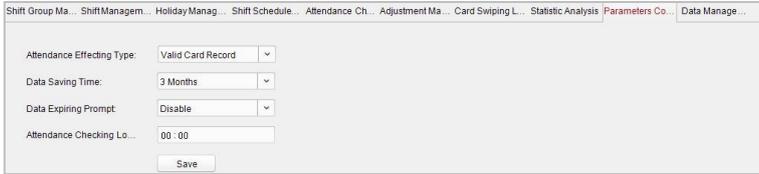
Name	Department	Date	Shift Name	Day Required At.	Day Actual Atten.	Day Attendance
P1	Default	2015-11-12	Normal Shift1	1	1	100.00%



- You can search the attendance rate statistics by different shift type: **Normal Shift**, or **Man-Hour Shift**.
- You can search the attendance rate statistics by department.
- You can search the attendance rate statistics by start date and end date.

### Parameters Configuration

Press the **Parameters Configuration** tab to enter the parameters configuration interface.



Shift Group Ma... ShiftManagem... Holiday Manag... Shift Schedule... Attendance Ch... Adjustment Ma... Card Swiping L... Statistic Analysis Parameters Co... Data Manage...

Attendance Effecting Type: Valid Card Record

Data Saving Time: 9 Months

Data Expiring Prompt: Disable

Attendance Checking Lo...: 00:00

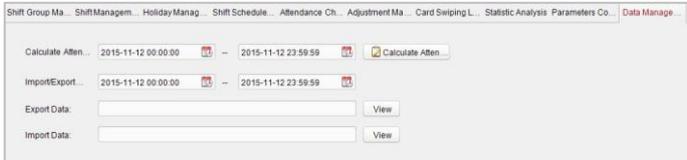
Save

### **Steps:**

1. Select the attendance effecting type (Valid Card Record, or Invalid Card Record), data saving time, data expiring prompt.
2. Set the attendance checking log clearing time.

### **Data Management**

Press the **Data Management** tab to enter the data management interface.



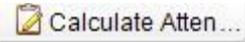
Shift Group Ma... ShiftManagem... Holiday Manag... Shift Schedule... Attendance Ch... Adjustment Ma... Card Swiping L... Statistic Analysis Parameters Co... Data Manage...

Calculate Atten... 2015-11-12 00:00:00 - 2015-11-12 23:59:59 Calculate Atten...

Import/Export... 2015-11-12 00:00:00 - 2015-11-12 23:59:59

Export Data: View

Import Data: View

Click the  button to calculate the attendance date.

On this interface, you can export and import attendance data.

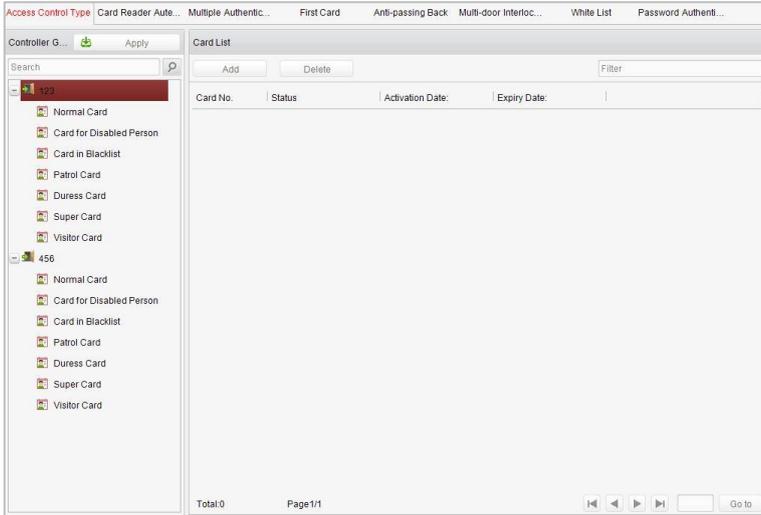
## 7.3.8 Advanced Functions

### **Purpose:**

The advanced functions of the access control system can be configured, such as access control type, password authentication and first card.



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



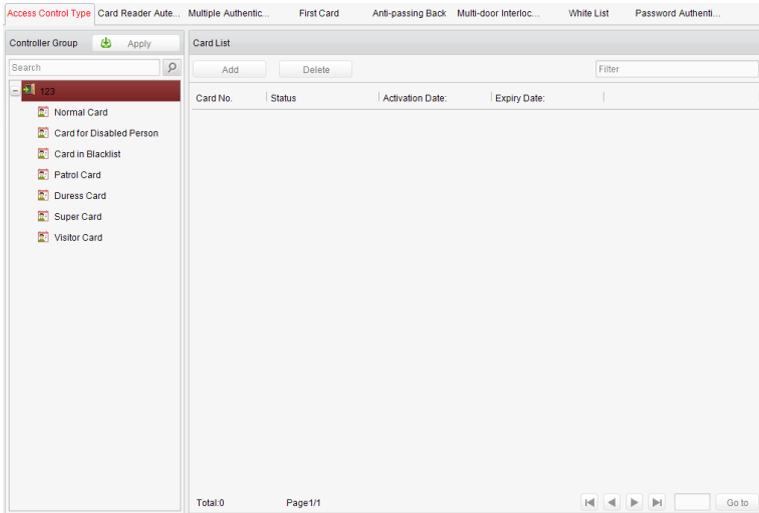
### Access Control Type

#### **Purpose:**

The added cards can be assigned with different card type for the corresponding usage.

#### **Steps:**

1. Click **Access Control Type** tab and select a card type.



**Normal Card:** By default, the card is set as normal card.

**Card for Disabled Person:** The door will remain open for the configured time period for the cardholder.

**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 card swiping action will be uploaded.

**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.

2. Click **Add** and select the available card.

3. Click **OK** to confirm assigning the card(s) to the selected card type.
4. Click the **Apply** button to take effect of the new settings.



You can click **Delete** to remove the card from the card type and the card can be available for being re-assigned.

## Card Reader Authentication

### *Purpose:*

You can only open the door by both swiping card and entering the password during the set time periods.



- For this authentication mode, the card swiping operation cannot be replaced by entering the card No..
- For password settings, please refer to Section 7.3.2 Normal Card.
- For models DS-K2801, DS-K2802, and DS-K2804, only two kinds of card reader authentication are supported: **Swipe Card**, and **Swipe Card Password**.

### *Steps:*

1. Click **Card Reader Authentication** tab and select a card reader.
2. Select a card reader authentication type from the dropdown list.

**Fingerprint:** The door can open by only inputting the fingerprint.

**Swipe Card:** The door can open by only swiping the card.

**Fingerprint/Swipe Card:** The door can open by inputting the fingerprint or swiping the card.

**Swipe Card/Password:** The door can open by inputting the password or swiping the card.

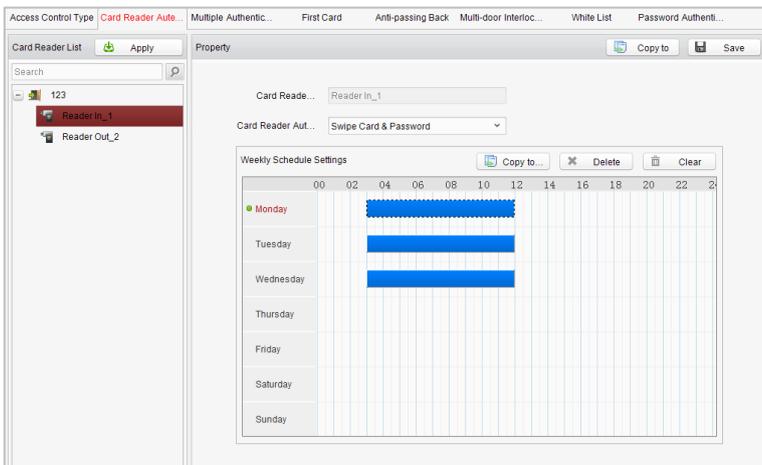
**Fingerprint Password:** The door can open by both inputting the password and inputting the fingerprint.

**Swipe Card Password:** The door can open by both inputting the password and swiping the card.

**Fingerprint Swipe Card:** The door can open by both inputting the fingerprint and swiping the card.

**Fingerprint Swipe Card Password:** The door can open by inputting the fingerprint, inputting the password, and swiping the card.

3. Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that period of time, the password authentication is valid.



4. Repeat the above step to set other time periods.  
Or you can select a configured day and click the **Copy to Week** button to copy the same settings to the whole week.  
You can click the **Delete** button to delete the selected time period or

click the **Clear** button to delete all the configured time periods.

5. (Optional) Click the **Copy to** button to copy the settings to other card readers.
6. Click the **Save** button to save parameters.
7. Click the **Apply** button to take effect of the new settings.

## First Card

### **Purpose:**

The door remains open for the configured time duration after the first card swiping.



### **Steps:**

1. Click **First Card** and select an access control point.
2. Check the checkbox of **Enable First Card Remain Open** to enable this function.
3. In the **Remain Open Duration** (min), input the time duration for remaining open the door.
4. Click **Add** and select the cards to add as first card for the door and click the **OK** button.
5. Click **Save** and then click the **Apply** button to take effect of the new settings.

## Anti-Passing Back

### **Purpose:**

In this mode, you can only pass the access control system according to the specified path.

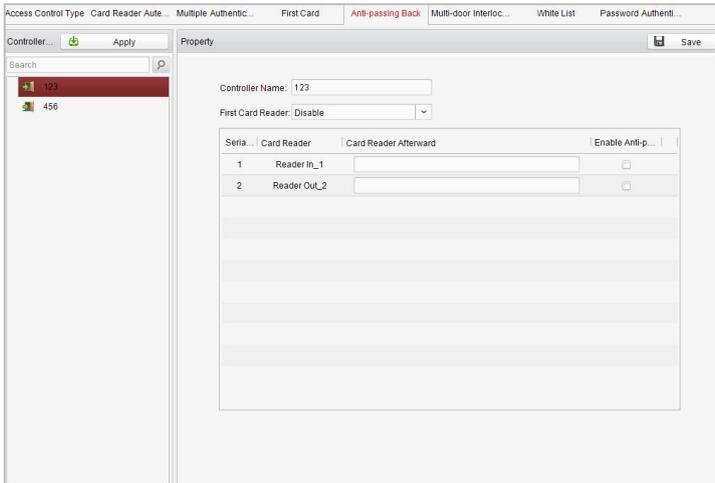


Either the anti-passing back or multi-door interlocking can be configured for an access controller at the same time.

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

#### Steps:

1. Click **Anti-passing Back** and select an access control point.



2. You can set the name for the controller and select the card reader as the beginning of the path.
3. 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 system by swiping the card in the order as Reader In\_01, Reader In\_02 and Reader Out\_04.

4. Check the checkbox of Enable Anti-Passing back.
5. Click Save and then click the Apply button to take effect of the new settings.

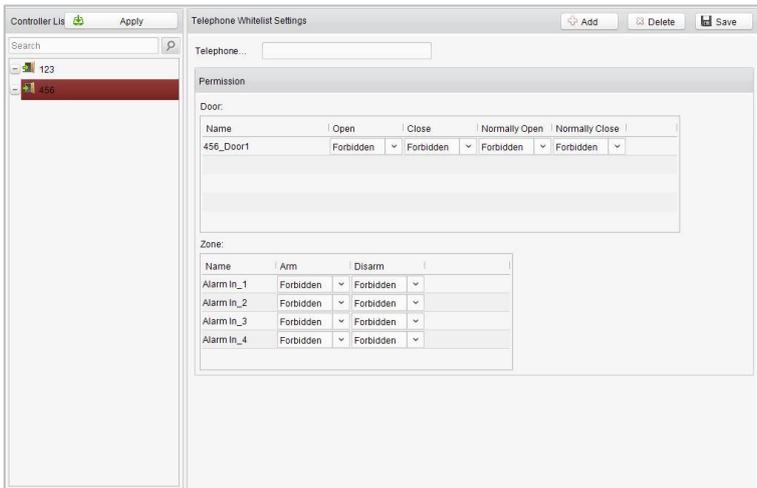


Models DS-K2801, DS-K2802, and DS-K2804 do not support the anti-passing back function.

## White List

### Steps:

1. Click the **White List** button to enter into the white list interface.



2. Select the access control point, and click the **Add** button. **Multi-door Interlocking** and select an access control point.
3. Select the access control points and click **Add** button.
4. Input the mobile number.

5. Select the settings of control permission, and set the property as **Allow** to enable this function.

Door: The mobile can control the door (open, closed, normally open, or normally closed).

Arming Region: The mobile can arm and disarm the arming channels

6. Click the **Save** button to save parameters.
7. Click the **Apply** button to take effect of the new settings.



The mobile can control the door and the arming region by sending SMS control instructions.

The SMS control instruction is composed of Command, Operation Range, and Operation Object.

Instruction Content	Digit	Description	Format
Command	3	010-Open, 011-Closed, 020-Normally open, 021-Normally Closed, 120-Disarm, 121-Arm	
Operation Range	1	1-all objects with permission, 2-single operation	Command#1#
Operation Object	3	Starts from 1 (corresponding to different doors or arming regions according to	Command#2#Operation Object#

Instruction Content	Digit	Description	Format
		commands)	



Models DS-K2801, DS-K2802, and DS-K2804 do not support the white list function.

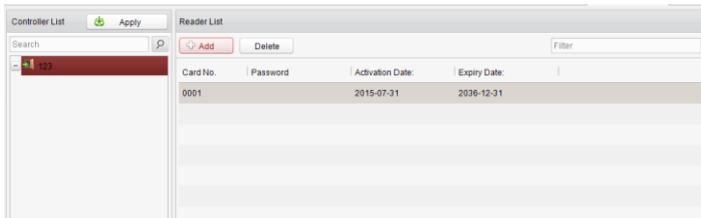
## Password Authentication

### *Purpose:*

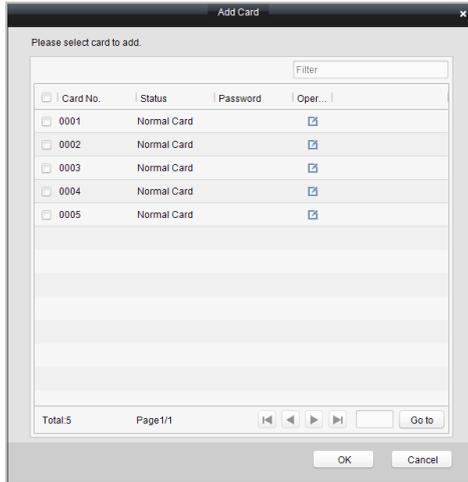
You can open the door by inputting the password only after finishing the operation of password authentication.

### *Steps:*

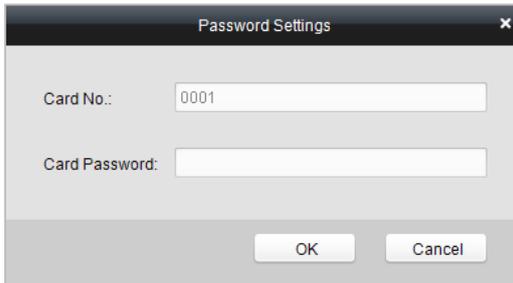
1. Click **Password Authentication** tab and select a host.



2. Click the **Add** button to enter card adding interface.



3. Check the checkbox of the corresponding card, and click the  button to pop up the password setting dialogue box.



4. Input the card password.
5. Click the Ok button to finish adding the card.



- The card, having added the password, will display in the card list.
- You can select the card in the card list, and click the Delete button to delete the password authentication of the selected card.
- Models DS-K2801, DS-K2802, and DS-K2804 do not support the password authentication function.

## 7.4 Checking Status and Event

### ***Purpose:***

In this section, you are able to anti-control the status of the door and to check the event report of the control point.

### 7.4.1 Status Monitor

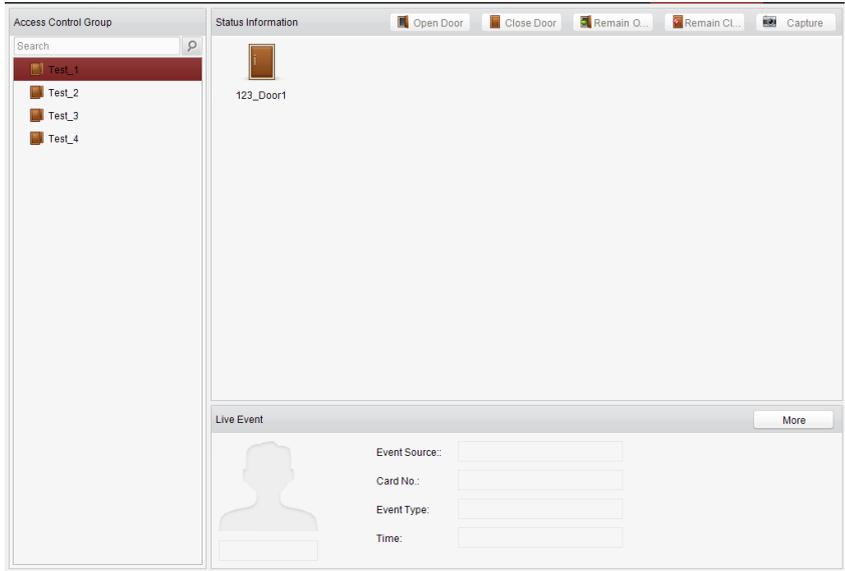
#### ***Purpose:***

You can anti-control the door status and check the real-time access event information for the control point.



Click the

icon on the control panel to enter the interface.



### Access Anti-control

#### Door Anti-control

##### ***Purpose:***

You can control the status for a single control point (a door) in this section.

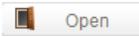
##### ***Steps:***

1. Enter the status monitor page.

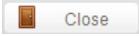


2. Click on the icon  on the **Status Information** panel to select a door.
3. Click on the button listed on the upper-left side of the **Status Information**

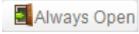
panel to select a door status for the door.



: Click on the button to open the door once.



: Click on the button to close the door once.



: Click on the button to keep the door open.



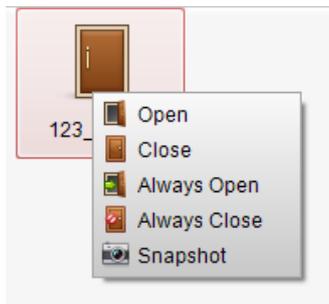
: Click on the button to keep the door closed.



: Click on the button to capture the picture.



4. You can also right click the icon and to select a status for the door.



- If the status is selected as **Remain Open/Remain Closed**, the door will keep open/ closed until a new anti-control command being made.
- The function of picture capturing cannot be realized until the storage server is installed.
- Models DS-K2801, DS-K2802, and DS-K2804 do not support the capture function.

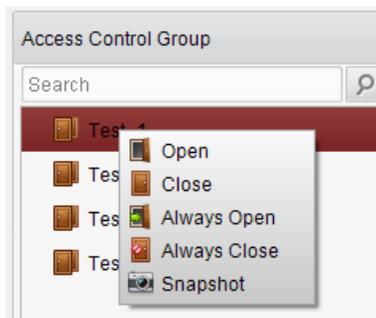
## Group Anti-control

### ***Purpose:***

You can control the status for a group of control points (doors) in this section.

### ***Steps:***

1. Enter the status monitor page.
2. Right click on a group in the **Group** list and to select a door status for the group.



If the status is selected as **Remain Open/Remain Closed**, all the doors in the group will keep open/ closed until a new anti-control command being made.

The function of picture capturing cannot be realized until the storage server is installed.

### **Access Status**

The door status will be represented instantly by the change of icon on the **Access Information** panel if the access event is triggered or an anti-control command is made.



### Live Event

You can check the live information of the access event on this panel. Click **More** to enter the Access Event page to view more event information.

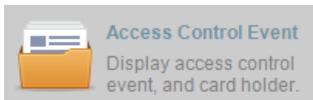
Live Event More

	Event Source:: <input type="text" value="test001_Door1"/>
	Card No.: <input type="text"/>
	Event Type: <input type="text" value="Normally Open Started"/>
	Time: <input type="text" value="2014-09-12 19:07:56"/>

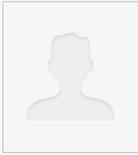
## 7.4.2 Access Control Event

### **Purpose:**

You can view real-time access event (such as swiping to open the door, unrecognized card number, duration group error, etc.) information in this section.



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

Access Control Event Information							Card Holder Information
Serial No.	Event Type	Card Holder	Card No.	Event Time	Event Source	Direction	
7	Remotely Arming			2015-07-31 16:50:24	123		
6	Remotely Disarm...			2015-07-31 16:50:24	123		
5	Remotely Logout			2015-07-31 16:48:42	123		
4	Remotely Login			2015-07-31 16:41:20	123		
3	Remotely Logout			2015-07-31 16:41:13	123		
2	Remotely Login			2015-07-31 16:39:43	123		
1	Remotely Clear...			2015-07-31 16:07:53	123		

Person No.:	<input type="text"/>
Name:	<input type="text"/>
Gender:	<input type="text"/>
ID Type:	<input type="text"/>
ID No.:	<input type="text"/>
Belong to...:	<input type="text"/>
Contact No.:	<input type="text"/>
Contact Ad.:	<input type="text"/>

### **Steps:**

1. Enter the access event page.
2. View the event information in the event list.
3. Click on an event to view the information of the card holder on the **Person Information** panel on the left side of the page.

## 7.4.3 Event Search

### **Purpose:**

You can search historical access event according to the search criteria (such as event type, name of the person, card No. or start/end time) in this section.



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

A screenshot of the Event Search web interface. The top section contains search filters: "Event Type" (dropdown menu set to "All"), "Start Time" (calendar icon, date "2015-07-31 00:00:00"), "Card Holder" (text input), "End Time" (calendar icon, date "2015-07-31 23:59:59"), and "Card No." (text input). A "Search" button is to the right. Below the filters is a "Search Result" section with an "Export" button. A table with columns "Serial No.", "Event Type", "Card Holder", "Card No.", "Event Time", "Event Source", "Direction", and "Capture Images" is shown, but it is currently empty. At the bottom of the table area, it says "Total:0 Page:1/1" and has navigation buttons. On the right side, there is a "Card Holder Information" panel with a placeholder for a person's photo and several text input fields for "Person No.", "Name", "Gender", "ID Type", "ID No.", "Belong to...", "Contact No.", and "Contact Ad...".

**Steps:**

1. Enter the event search page.
2. Enter the search criteria (event type/ person name/ card No/ start &end time).

A close-up view of the search criteria input fields from the interface. It shows "Event Type" (dropdown menu set to "All"), "Start Time" (calendar icon, date "2014-09-18 00:00:00"), "Card Holder" (text input), "End Time" (calendar icon, date "2014-09-18 23:59:59"), and "Card No." (text input). A "Search" button is located to the right of the "End Time" field.

3. Click **Search** to get the search results.

4. View the event information in the event list.
5. Click on an event to view the information of the card holder on the **Person Information** panel on the left side of the page.

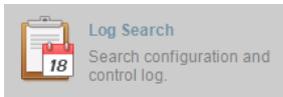
## 7.5 System Maintenance

### 7.5.1 Log Management

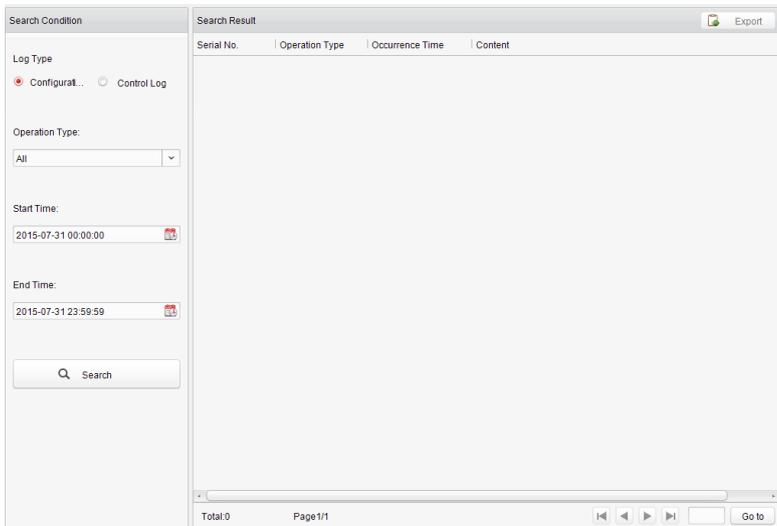
#### Interface Introduction

**Purpose:**

The log files of the Access Control System and the devices that connected to the Access Control System can be searched for checking.



Click the icon on the control panel to open the Log Search page.



## Configuration Logs Searching

### **Purpose:**

The Configuration Log files of the Access Control System can be searched by time, including One-Card Configuration, Access Control Configuration, Downloading Permission and System Configuration.

### **Steps:**

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the Operation Type of log files.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.



Please narrow the search condition if there are too many log files.

## Control Logs Searching

### **Purpose:**

The Control Log files of the Access Control System can be searched by time, including Access Control and Log Search.

### **Steps:**

1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the Operation Type of log files.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the

logs.



Please narrow the search condition if there are too many log files.

## Searching Configuration Log

### Searching One-card Configuration Logs

#### ***Purpose:***

The One-card Configuration Log files include departments, persons and cards log files. One-card Configuration of the Access Control System can be operated as adding, modifying and deleting logs.

#### ***Steps:***

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as One-card Configuration.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.



Please narrow the search condition if there are too many log files.

### Searching Access Control Configuration Logs

#### ***Purpose:***

The Access Control Configuration Log files include Access Control devices log files. Access Control Configuration of the Access Control System can be operated as adding, modifying and deleting door groups or doors and access control device permission operations.

#### ***Steps:***

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as Access Control Configuration.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.



Please narrow the search condition if there are too many log files.

### Searching Downloading Permission Logs

#### ***Purpose:***

The Downloading Permission Log files include downloading permission log files, and no record for downloading permission failure log files.

#### ***Steps:***

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as Downloading Permission.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.



Please narrow the search condition if there are too many log files.

### Searching System Configuration Logs

#### ***Purpose:***

The System Configuration Log files of the Access Control System can be searched as system configuration interface log files.

**Steps:**

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as System Configuration Logs.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.



Please narrow the search condition if there are too many log files.

## Searching Control Log

### Searching Access Control Logs

**Purpose:**

The Access Control Log files of the Access Control System include door groups and doors access control logs and door on/off control log files.

**Steps:**

1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the operation type as Access Control Logs.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.



Please narrow the search condition if there are too many log files.

## Log Search

### ***Purpose:***

The Log Search of the Access Control System includes information for configuration log files and control log files.

### ***Steps:***

1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the operation type as Log Search.
4. Click the icon  to specify the start time and end time.
5. Click **Search**. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.



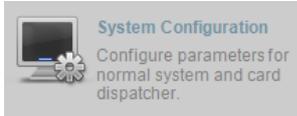
Please narrow the search condition if there are too many log files.

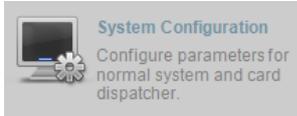
## 7.5.2 System Configuration

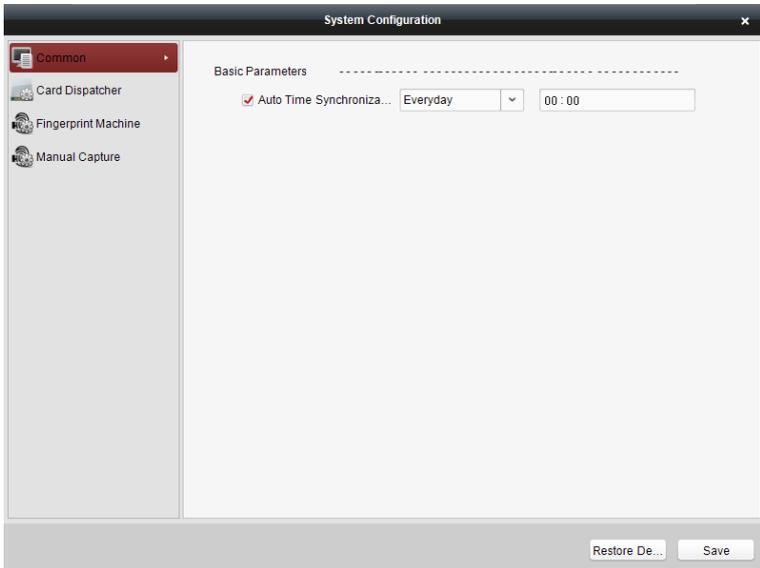
### Interface Introduction

#### ***Purpose:***

The general parameters, Auto Time Adjustment and Card Reader of the Access Control System can be configured.



Click the  icon on the control panel to open the System Configuration page.



### **Auto Time Synchronization**

The Auto Time Synchronization of the Access Control System can operate auto time adjustment to all access control devices of the Access Control System according to specified period and time.

### **Card Reader Configuration**

The Card Reader Configuration is for Access Control System to read the card by setting Card Reader parameters.

## Fingerprint Machine

The Fingerprint Machine is for Access Control system to collect fingerprints.



Models DS-K2801, DS-K2802, and DS-K2804 do not support the fingerprint machine function.

## Manual Capture Configuration

The Manual Capture Configuration is for Access Control system to take photos remotely.

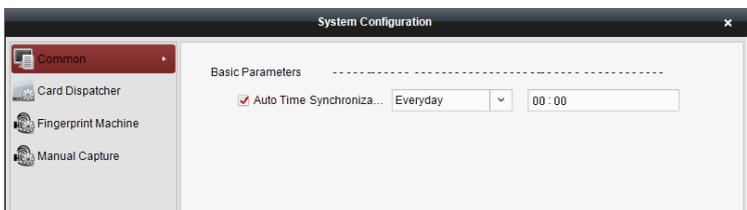


Models DS-K2801, DS-K2802, and DS-K2804 do not support the manual capture configuration.

## Auto Time Synchronization

### Steps:

1. Open the System Configuration page.
2. Click the **Common** tab to enter the Common Settings interface.



3. Tick the checkbox to enable Auto Time Synchronization.
4. Select the matched day and input the time to operate the time adjustment.

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



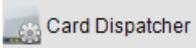
You can click the **Restore Default Value** button to restore the defaults of all the local configurations.

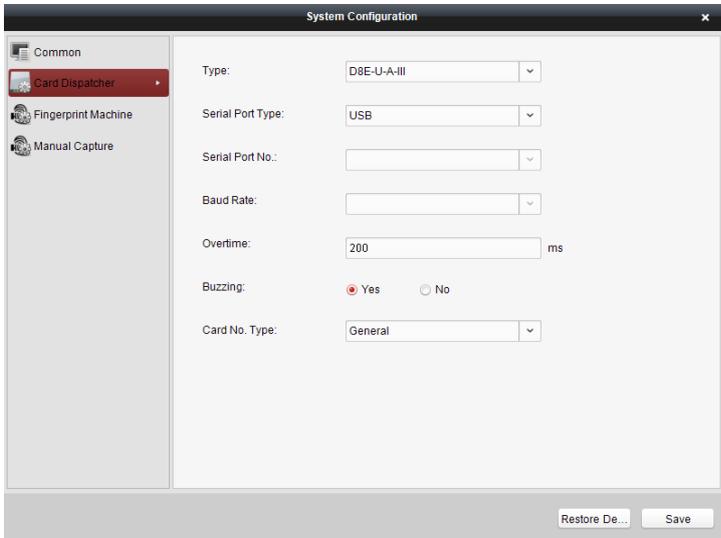
## Card Dispenser Configuration

### ***Purpose:***

The Card Reader Configuration of the Access Control System can configure device type, connection mode, serial port, baud rate and other parameters of the Card Reader Configuration.

### ***Steps:***

1. Click the  icon on the System Configuration interface to open the Card Dispatcher Configuration page.



The screenshot shows a window titled "System Configuration" with a sidebar on the left containing "Common", "Card Dispatcher" (selected), "Fingerprint Machine", and "Manual Capture". The main area contains the following configuration options:

Type:	D8E-U-A-III
Serial Port Type:	USB
Serial Port No.:	
Baud Rate:	
Overtime:	200 ms
Buzzing:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Card No. Type:	General

At the bottom right, there are two buttons: "Restore De..." and "Save".

2. Select the device type, serial port type, serial port, baud rate, and other parameters of the Card Dispatcher.
3. Click the save button to save the settings.

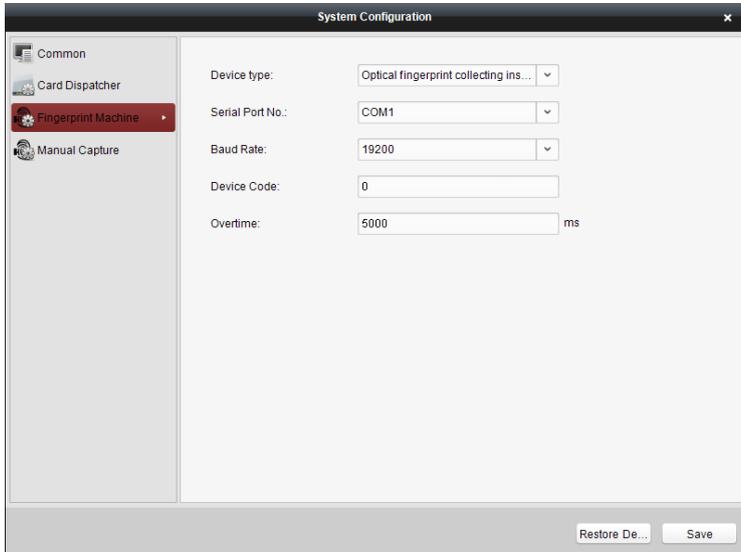


- It is supported using card type as regular and Wiegand.
- When the BEEP is selected as "YES", the audio will be off when you click the "SAVE" if the Card Reader Configuration is set wrong; the audio will be on when you click the "Save" and when you insert the card reader if the configuration is set correct.
- You can click the **Restore Default Value** button to restore the defaults of the entire local configuration.

## Fingerprint Machine Configuration

### *Steps:*

1. Click the  **Fingerprint Machine** icon on the System Configuration interface to open the Fingerprint Machine Configuration page.



2. Select the device type, serial port number, baud rate, device code, and overtime parameters of the fingerprint machine.
3. Click the **Save** button to save the settings.



- Models DS-K2801, DS-K2802, and DS-K2804 do not support the fingerprint machine function.
- It is supported using device type as Optical Fingerprint Collecting Instrument and Capacitive Fingerprint Collecting Instrument.
- The serial port number should correspond to the serial port number of PC.
- The baud rate should be called according to the external fingerprint card

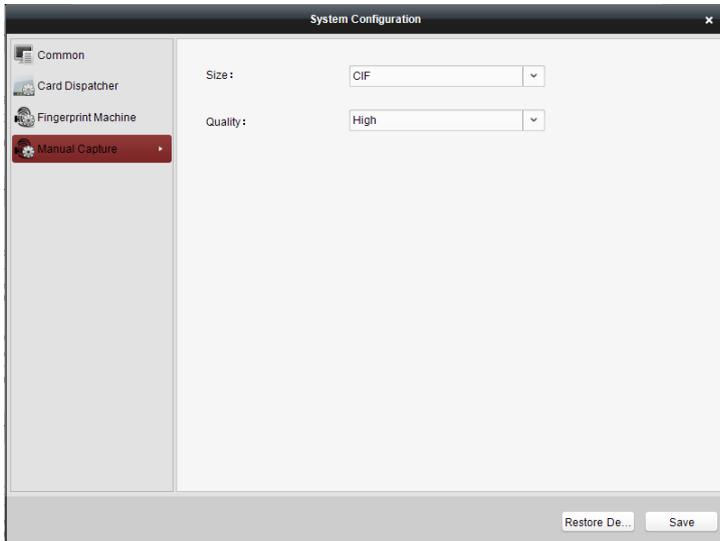
dispatcher. The default value is 19200.

- Overtime 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.
- You can click the **Restore Default Value** button to restore the defaults of all local settings.

## Manual Capture Configuration

### Steps:

1. Click the  icon on the System Configuration interface to open the Manual Capture Configuration page.



2. Select the picture size from the dropdown list
3. Select the picture quality from the dropdown list.



- Models DS-K2801, DS-K2802, and DS-K2804 do not support the manual capture configuration.
- It is supported using the picture size as CIF, QCIF, 4CIF/D1, SVGA, HD720P, VGA, WD1, and AUTO.
- It is supported using the picture quality as High, Medium, and Low.

**First Choice for Security Professionals**