

DS-K2600 Series Access Controller User Manual

UD.6L0206D1189A02

User Manual

About this Manual

This Manual is applicable to 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. Please use this user manual under the guidance of professionals.

Legal Disclaimer

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED. SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

0101001051112

Regulatory Information

FCC Information

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

FCC Conditions

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



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



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

collection points. For more information see: www.recyclethis.info.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol,

which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

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

Preventive and Cautionary Tips

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

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



Safety Information

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



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 $^\circ\!C$ or lower than -20 $^\circ\!C$)

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

1 Product Description	3
1.1 Overview	3
1.2 Main Feature	3
2 Appearance	5
2.1 Component Description	5
2.1.1 Access Controller Component Schematic Diagram	5
3 Terminal Connection	7
3.1 Terminals Description	7
3.1.1 DS-K2601Terminal Description	7
3.1.2 DS-K2602Terminal Description	11
3.1.3 DS-K2604 Terminal Description	16
4 Card Reader Installation	22
4.1 External Terminal	22
4.1 External Terminal 4.1.1 DS-K2601 External Terminals	22
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals 4.1.2 DS-K2602 External Terminals 	22 22 22
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals 4.1.2 DS-K2602 External Terminals 4.1.3 DS-K2604 External Terminals 	
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals 4.1.2 DS-K2602 External Terminals 4.1.3 DS-K2604 External Terminals 4.2 Card Reader Installation	
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals 4.1.2 DS-K2602 External Terminals 4.1.3 DS-K2604 External Terminals 4.2 Card Reader Installation 4.2.1 The Connection of Wiegand Card Reader 	22 22 22 22 22 22 23 23 23
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals	22 22 22 22 22 23 23 23 23 24
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals	22 22 22 22 23 23 23 23 24 24
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals	22 22 22 22 23 23 23 23 24 24 24 24
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals	22 22 22 23 23 23 23 24 24 24 24 24 25
 4.1 External Terminal	22 22 22 22 23 23 23 23 24 24 24 24 24 25 25
 4.1 External Terminal 4.1.1 DS-K2601 External Terminals	22 22 22 23 23 23 24 24 24 24 24 24 25 25 25 26
 4.1 External Terminal	22 22 22 22 23 23 23 24 24 24 24 24 25 25 25 26 26

4.8 Arming Region Input Terminal	27
4.8.5 Connecting Normally Open Detector	27
4.8.6 Connecting Normally Closed Detector	28
4.9 Fire Alarm Module Wiring	28
5 Settings	29
5.1 Initializing the Hardware	29
5.2 Relay Input NO/NC	29
5.2.1 Lock Relay Output	29
5.2.2 Alarm Relay Output Status	30
6 Activating the Control Panel	32
6.1 Activation via SADP Software	32
6.2 Activation via Client Software	34

1 Product Description

1.1 Overview

DS-K2600 is a powerful and stable access controller, using the logical architecture design. DS-K2600 is designed with TCP/IP network interface and its signal processed with special encryption and can be run offline. Anti-tampering function is also supported.

1.2 Main Feature

- The access controller is equipped with 32-bit high-speed processor;
- Supports TCP/IP network communication, with self-adaptive network interface. The communication data is specially encrypted to relieve the concern of privacy leak;
- Support recognition and storage of card number with maximum length of 20;
- The access controller can store 100 thousand legal cards and 300 thousand card swiping records;
- Supports multi-door interlock function, anti-passback function, multi-card function, first card open function, super card and super password function, online upgrade function and remote control of the doors;
- Supports tamper-proof alarm for card reader, alarm for door not secured, force opening door alarm, alarm for door opening timeout, duress card and code alarm, blacklist alarm and alarm for illegal card swiping attempts reaching the limit.;
- The alarm input of controller supports short circuit protection function and cut-proof function;
- Supports RS485 interface and Wiegand interface for accessing card reader. RS485 interface adopts dual-interface design and supports loop breakpoint detection and redundancy function; Wiegand interface supports W26, W34 and is seamlessly compatible with third-party card reader with Wiegand interface;
- Supports various card types as normal/ disabled/ blacklist/ patrol/ guest/ duress/ super card, etc.;
- Various indicators to show different status;

- Supports time synchronization via NTP, manual or automatic method;
- Supports record storage function when it is offline and insufficient storage space storage alarm function;
- The access controller has backup battery design, watchdog design and tamper-proof function;
- Data can be permanently saved after the access controller is powered off.
- Supports I/O linkage, and event linkage;
- Supports Ehome protocol, DNS domainn name analysis, and inter-network communication.
- 500 groups of password under the authentication mode of card and password;

2 Appearance

2.1 Component Description

2.1.1 Access Controller Component Schematic Diagram

Take DS-K2604 as an example, the component schematic diagram is shown below.



Figure 2-1 DS-K2604 Component Schematic Diagram

Ne	Component Description			
NO.	DS-K2601	DS-K2602	DS-K2604	
1	Alarm Relay O	utput Status (NC/	NO)	
2	Network Data	Indicator		
3	RS-485 Comm	unication Indicato	or	
4	Network Status Indicator			
5	Door Relay Output Status (NC/NO) Choice			
6	Battery Charging Indicator			
7	Power Indicator			
8	Charging Completing Indicator			
9	Running Indicator			
10	Hardware Initialization and Normal Working Choice			
11	Main board di	al-up switch/ Rese	erved	

Table 2-1 DS-I	(2600 Component	Description
----------------	-----------------	-------------

3 Terminal Connection

3.1 Terminals Description

3.1.1 DS-K2601Terminal Description



Figure 3-1 DS-K2601 Terminals

No.	DS-K2601		
A1	Lask Davies	GND	Grounding
A2	LOCK POWER	+12V	Power Output of the Lock
A3	Card Reader	GND	Grounding
A4	Power	+12V	Power Output of the Head Read
A5		GND	Grounding
A6		W0	Wiegand Head Read Data Input Data0
Α7	Wiegond	W1	Wiegand Head Read Data Input Data1
A8	Card Reader	BZ	Card Reader Buzzer Control Output
A9	2	ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A10		ОК	Indicator of Card Reader Control Output (Valid Card Output)
A11		GND	Grounding
A12		W0	Wiegand Head Read Data Input Data0
A13	Wiegond	W1	Wiegand Head Read Data Input Data1
A14	Card Reader	BZ	Card Reader Buzzer Control Output
A15	1	ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A16		ОК	Indicator of Card Reader Control Output (Valid Card Output)
B1	Arming Region	Z1	Arming Region Access Terminal 1 (Only for Linkage of Alarm Relay Output)
B2	Input GND		Grounding

Table 3-1 DS-K2601 Terminal Description

No.	DS-K2601		
B3		Z2	Arming Region Access Terminal 2 (Only for Linkage of Alarm Relay Output)
B4		Z3	Arming Region Access Terminal 3 (Only for Linkage of Alarm Relay Output)
B5		GND	Grounding
B6		Z4	Arming Region Access Terminal 4 (Only for Linkage of Alarm Relay Output)
B7	E Look	D1+	
B8	E-LOCK	D1-	Door 1 Door Relay Input (Dry Contact)
В9	Door	S1	Door 1 Door Contact Detector Input
B10	Contact Input	GND	Grounding
B11	Door Open	B1	Door 1 Door Open Button Input
B12	Button	GND	Grounding
C1	Dowor	+12V	DC12V Cathode
C2	Power	GND	DC12V Grounding Input
C3	Patton	BAT+	DC12V Battery Cathode
C4	Ballery	BAT-	DC12V Battery Anode
C5		RS 485A+	Card Reader RS485+ Access
C6		RS 485A-	Card Reader RS485- Access
C7	485 Card Reader	GND	Grounding
C8	incauci	RS 485B+	Card Reader RS485+
C9		RS 485B-	Card Reader RS485-

No.	DS-K2601			
C10		GND	Grounding	
C11		RS 485C+		
C12	Access	RS 485C-		
C13	Controller	GND	Percented	
C14	RS485 Interface	RS 485D+	keserveu	
C15		RS 485D-		
C16		GND		
C17		NO/NC1	Alarm Polay 1 Output (Dry Contact)	
C18	Alarm	COM1		
C19	Output	NO/NC2	Alarm Palay 2 Output (Dry Contact)	
C20		COM2	Aldriff Kelay 2 Output (Dry Contact)	
D1		C2	Event Alarm Input 2	
D2	Event Input	GND	Grounding	
D3		C1	Event Alarm Input 1	



3.1.2 DS-K2602Terminal Description

Figure 3-2 DS-K2602 Terminal Description

No.	DS-K2602		
A1	Power for	GND	Grounding
A2	E-Lock	+12V	Power Output of the Lock
A3	Power for	GND	Grounding
A4	Card Reader	+12V	Power Output of the Head Read
A5		GND	Grounding
A6		W0	Wiegand Head Read Data Input Data0
A7	Wingond	W1	Wiegand Head Read Data Input Data1
A8	Card Reader	ΒZ	Card Reader Buzzer Control Output
A9	4	ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A10		ОК	Indicator of Card Reader Control Output (Valid Card Output)
A11		GND	Grounding
A12		W0	Wiegand Head Read Data Input Data0
A13	Wiegond	W1	Wiegand Head Read Data Input Data1
A14	Card Reader	ΒZ	Card Reader Buzzer Control Output
A15	3	ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A16		ОК	Indicator of Card Reader Control Output (Valid Card Output)
A17	Wiegand	GND	Grounding
A18	Card Reader	W0	Wiegand Head Read Data Input Data0

Table 3-2 DS-K2602	. Terminal	Description
--------------------	------------	-------------

No.	DS-K2602		
A19	2	W1	Wiegand Head Read Data Input Data1
A20		BZ	Card Reader Buzzer Control Output
A21		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A22		ОК	Indicator of Card Reader Control Output (Valid Card Output)
A23		GND	Grounding
A24		W0	Wiegand Head Read Data Input Data0
A25	M/in more d	W1	Wiegand Head Read Data Input Data1
A26	Card Reader	BZ	Card Reader Buzzer Control Output
A27	1	ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A28		ОК	Indicator of Card Reader Control Output (Valid Card Output)
B1		Z1	Arming Region Access Terminal 1 (Only for Linkage of Alarm Relay Output)
B2		GND	Grounding
В3	Arming Region	Z2	Arming Region Access Terminal 2 (Only for Linkage of Alarm Relay Output)
B4		Z3	Arming Region Access Terminal 3 (Only for Linkage of Alarm Relay Output)
B5		GND	Grounding
В6		Z4	Arming Region Access Terminal 4 (Only for Linkage of Alarm Relay Output)
B7	E-Lock1	D1+	Door 1 Door Relay Input (Dry Contact)

No.	DS-K2602		
B8		D1-	
B9		D2+	
B10	E-LOCKZ	D2-	Door 2 Door Kelay Input (Dry Contact)
B11	Door	S1	Door 1 Magnetic Detector Input
B12	Magnetics	GND	Signal Grounding
B13	Detector	S2	Door 2 Magnetic Detector Input
B14		B1	Door 1 Door Button Input
B15	Door Button	GND	Signal Grounding
B16	Button	B2	Door 2 Door Button Input
C1	Dowor	+12V	DC12V Cathode
C2	Power	GND	Grounding
C3	Battery	BAT+	DC12V Battery Cathode
C4		BAT-	DC12V Battery Anode
C5		RS 485A+	Card Reader RS485+ Access
C6		RS 485A-	Card Reader RS485- Access
C7	Card Reader	GND	Grounding
C8	485 Interface	RS 485B+	Card Reader RS485+
C9		RS 485B-	Card Reader RS485-
C10		GND	Grounding
C11	RS-485	RS 485C+	Reserved
C12	Interface	RS 485C-	

No.		DS-K2602	
C13		GND	
C14		RS 485D+	
C15		RS 485D-	
C16		GND	
C17	Alarm	NO/NC1	Alarm Relay 1 Output (Dry Contact)
C18		COM1	
C19		NO/NC2	Alarra Balau 2 Outrout (Dr. Cantart)
C20		COM2	Alarm Relay 2 Output (Dry Contact)
C21	Output	NO/NC3	Alarm Balay 2 Output (Dry Contact)
C22		COM3	Alarm Relay 3 Output (Dry Contact)
C23		NO/NC4	Alarm Balay & Output (Dry Contact)
C24		COM4	Alarm Relay 4 Output (Dry Contact)
D1		C4	Event Alarm Input 4
D2	Event Input	GND	Grounding
D3		C3	Event Alarm Input3
D4		C2	Event Alarm Input 2
D5		GND	Grounding
D6		C1	Event Alarm Input 1

No

A3

Power



3.1.3 DS-K2604 Terminal Description

Figure 3-3 DS-K2604 Access Controller Terminals

No.	DS-K2604		
A1	Power	GND	Grounding
A2	Supply of	+12V	Power Supply of E-Lock Output

GND

Table 3-3 DS-K2604 Port Description

Grounding

No.	DS-K2604		
A4	Supply of Card Reader	+12V	Power Supply of Card Reader Output
A5		GND	Grounding
A6		W0	Wiegand Card Reader Data Input Data0
A7)A/is sound	W1	Wiegand Card Reader Data Input Data1
A8	Card Reader	BZ	Buzzer of Card Reader Control Output
A9	4	ERR	Cresset of Card Reader Control Output (Invalid Card Output)
A10		ОК	Cresset of Card Reader Control Output (Valid Card Output)
A11		GND	Grounding
A12		W0	Wiegand Card Reader Data Input Data0
A13		W1	Wiegand Card Reader Data Input Data1
A14	Card Reader	BZ	Buzzer of Card Reader Control Output
A15	3	ERR	Cresset of Card Reader Control Output (Invalid Card Output)
A16		ОК	Cresset of Card Reader Control Output (Valid Card Output)
A17	Wiegand Card Reader 2	GND	Grounding
A18		W0	Wiegand Card Reader Data Input Data0
A19		W1	Wiegand Card Reader Data Input Data1
A20		BZ	Buzzer of Card Reader Control Output
A21		ERR	Cresset of Card Reader Control Output (Invalid Card Output)

No.	DS-K2604		
A22		ОК	Cresset of Card Reader Control Output (Valid Card Output)
A23		GND	Grounding
A24		W0	Wiegand Card Reader Data Input Data0
A25		W1	Wiegand Card Reader Data Input Data1
A26	Wiegand	BZ	Buzzer of Card Reader Control Output
A27	Card Reader 1	ERR	Cresset of Card Reader Control Output (Invalid Card Output)
A28		ОК	Cresset of Card Reader Control Output (Valid Card Output)
B1	Arming Region Input	Z1	Arming Region Access Terminal 1 (Only for Linkage of Alarm Relay Output)
B2		GND	Grounding
B3		Z2	Arming Region Access Terminal 2 (Only for Linkage of Alarm Relay Output)
B4		Z3	Arming Region Access Terminal 3 (Only for Linkage of Alarm Relay Output)
B5		GND	Grounding
B6		Z4	Arming Region Access Terminal 4 (Only for Linkage of Alarm Relay Output)
B7	- E-Lock 1	D1+	
B8		D1-	Door 1 Door Relay Input (Dry Contact)
В9	E-Lock 2	D2+	Door 2 Door Relay Input (Dry Contact)

No.			DS-K2604
B10		D2-	
B11	E-Lock 3	D3+	
B12		D3-	Door 3 Door keiay input (Dry Contact)
B13		D4+	Door 4 Door Relay Input (Dry Contact)
B14	E-LOCK 4	D4-	
B15		S1	Door 1 Magnetic Detector Input
B16		GND	Signal Grounding
B17	Door	S2	Door 2 Magnetic Detector Input
B18	Input	\$3	Door 3 Magnetic Detector Input
B19		GND	Signal Grounding
B20		S4	Door 4 Magnetic Detector Input
B21		B1	Door 1 Door Button Input
B22		GND	Signal Grounding
B23	Door Button	B2	Door 2 Door Button Input
B24	DOOF BULLON	B3	Door 3 Door Button Input
B25		GND	Signal Grounding
B26		B4	Door 4 Door Button Input
C1	Daviar	+12V	DC12V Cathode
C2	Power	GND	Grounding
C3	Detter	BAT+	DC12V Battery Cathode
C4	Battery	BAT-	DC12V Battery Anode
C5	Card Reader RS485	RS 485A+	Card Reader RS485A+

No.	DS-K2604		
C6		RS 485A-	Card Reader RS485A-
C7		GND	Grounding
C8		RS 485B+	Card Reader RS485B+
C9		RS 485B-	Card Reader RS485B-
C10		GND	Grounding
C11		RS 485C+	
C12		RS 485C-	
C13	Access	GND	
C14	Controller	RS	Reserved
	RS485	485D+	
C15		RS 485D-	
C16		GND	
C17		NO/NC1	Alarm Polou 1 Output (Dry Contact)
C18		COM1	Alarin Kelay I Output (Dry Contact)
C19		NO/NC2	Alarm Polou 2 Output (Dry Contact)
C20	Alarm	COM2	Alarm Relay 2 Output (Dry Contact)
C21	Output	NO/NC3	Alexan Deley 2 Output (Day Content)
C22	-	COM3	Alarm Kelay 5 Output (Dry Contact)
C23		NO/NC4	Alexan Delevi 4 Output (Day Content)
C24		COM4	Alarm Relay 4 Output (Dry Contact)
D1		C8	Event Alarm Input 8
D2	Event Input	GND	Grounding
D3		C7	Event Alarm Input 7

No.	DS-K2604		
D4		C6	Event Alarm Input 6
D5		GND	Grounding
D6		C5	Event Alarm Input 5
D7		C4	Event Alarm Input 4
D8		GND	Grounding
D9		C3	Event Alarm Input3
D10		C2	Event Alarm Input 2
D11		GND	Grounding
D12		C1	Event Alarm Input 1



- The Alarm input hardware interface is normally open by default. So only the normally open signal is allowed. It can be linked to the buzzer of the card reader and access controller, and the alarm relay output and open door relay output.
- Arming region alarm input is only for the alarm relay output linkage.
- RS485 card ID should be set as 1to 8. For example, the ID of door 1 is 1 and 2 standing for in and out respectively.
- 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 reader 1, 2, 3 and 4 respectively correspond to the entering card reader 1, 2, 3 and 4 respectively correspond to the entering card readers of door 1, 2, 3, and 4.

4 Card Reader Installation

4.1 External Terminal

4.1.1 DS-K2601 External Terminals



Figure 4-1 DS-K2601 External Terminals

4.1.2 DS-K2602 External Terminals



Figure 4-2 DS-K2602 External Terminals

4.1.3 DS-K2604 External Terminals



Figure 4-3 DS-K2604 External Terminals

4.2 Card Reader Installation

4.2.1 The Connection of Wiegand Card Reader



Wiegand Communication Wiring

Figure 4-4 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.

4.2.2 RS485 Card Reader Connection



RS485 Communication Wiring

Figure 4-5 Wiring diagram of RS485

4.3 Installing E-Lock

4.3.3 Installation of Cathode Lock



Figure 4-6 Wiring diagram of cathode lock

4.3.4 Installation of Anode Lock



Figure 4-7 Wiring diagram of anode lock

4.4 Connecting the External Alarm Device



Figure 4-8 External Alarm Device Connection

4.5 Door Button Wiring Diagram



Figure 4-9 Power Button Connection

4.6 The Connection of Magnetics Detection



Figure 4-10 Magnetics Connection

4.7 Connecting Power Supply



Figure 4-11 Power Supply Connection

4.8 Arming Region Input Terminal

4.8.5 Connecting Normally Open Detector



Figure 4-12 Normally Open Status

4.8.6 Connecting Normally Closed Detector







4.9 Fire Alarm Module Wiring

Figure 4-14 Fire Alarm Module Wiring

5 Settings

5.1 Initializing the Hardware

Steps:

- **1.** The jumper cap jumps from Normal to Initial.
- 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 setting and all the device events are wiping out.

5.2 Relay Input NO/NC

5.2.1 Lock Relay Output

Lock Relay Normally Open Status



Figure 5-2 Normally Open Status

Lock Relay Normally Closed Status



Figure 5-3 Normally Closed Status

5.2.2 Alarm Relay Output Status

Alarm Relay Output Normally Open



Figure 5-4 Alarm Relay Output Normally Open

Alarm Relay Output Normally Closed



Figure 5-5 Normally Closed Status
Work Flow of Software

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

Refer to the following work flow:



Figure 5-6 Software Client Work Flow

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.

				SA	DP			- o ×
Online Devices	🕜 Help							
Total number of onli	ne devices: 3				E Save as Ex	el @ Refresh	Modify Network Para	imeters
Total number of end Dexics Type XX-30000000-X XX-3000000000X XX-3000000000X	ne devices: 3 IP-4 Address 192.168.1.64 192.168.1.64 192.168.1.64	Security Active Inactive Active	Port 8000 8000 8000	Software Version Vicx.sobuild zooxex Vicx.sobuild zooxex Vicx.sobuild zooxex	 Bave as Exi IPv4 Gateway 192.168.1.1 192.168.1.1 192.168.1.1 192.168.1.1 	In Press	Modify Network Para IP Address: Port: Subnet Mask: IPv6 Gateway: IPv6 Gateway: IPv6 Gateway: IPv6 Perfst.Length: HTTP Port: Device Sensi No: Device Sensi No: Device Adhuston New Password: Strong Contimn Password:	meters 192.0.0.46. 000 255.255.55 192.0.0.1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	Citine Devices	Other Devices P Help Total number of artifica devices: 3 3 Devices Total number of artifica devices: 3 2 Vice Notation of Artification of Artificatio Artificatio of Artificatio Artificatio Artificatio	Other Device Peter Mathematical Teal number of anline devices: 3 Device Type PP4-Address Security XXXXXXXXXXXX 192-168-1.64 Active XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Others Devices Point Tead number of online devices: 3 Device PrivAddress: Becarity XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Other Devices Holp Total number of anima devices: 3	Cited Devices Port Bite as Elia Devices // Port Borkar Markov Port Borkar Markov Devices // Status X Arcon Port Borkar Markov Port definition VX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Charles Portes Participation Total number of enline devices:	Total model Image: Control Devices Image: Contr

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

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

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

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

 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 Para	meters
IP Address:	192. 0. 0 .64
Port:	8000
Subnet Mask:	255.255.255.0
IPv4 Gateway:	192. 0.0 .1
IPv6 Address:	:
IPv6 Gateway:	:
IPv6 Prefix Length:	0
HTTP Port	80
Device Serial No.:	XX-XXXXXXX-XXXXXXXX
Enable DHCP	
Password	Save

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.
- Click the control panel.
 Click the control panel.



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

		iVM	IS-4200 Access	Control System	admin	仓 🖬 譜 11:02:01 🔒 -	
🧾 📰 Con	trol Panel 🛛 💂 C	ontroller Ma		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
Device Managed (0)							
Add Device	Edit	Delete Bulk Time Adj	Status	Remote Config	Refresh	Filter	
Name	Туре	Connection M.	. IP	Port	Baud Rate Dial-up	Connection St Refr	
		_				_	
			_	Activate Device	,		
			Password:				
				The password (8 to 16 should contain two or following character by	i characters) nore of the		
			Confirm Pas				
				_	_		
Online Devices (6)		Refresh		OK	Cancel		
Add to Client	🔶 Add All Device	Edit Network	Reset P	Activate		Filter	
Name		Туре	IP.	Po	t Activated	Added	ć
44-19-b6-03-c7-e2		Access Controller_DS-K2604-G	10.7.3	8.168 80	00 Yes	No	
44-19-b6-c1-42-5e		Access Controller_DS-K2604	10.7.3	8.26 80	00 Yes	No	
44-19-b6-a3-4b-06		Access Controller_DS-K2604-G	192.0.	0.64 80	00 No	No	
44-19-b6-c1-5a-e3		Access Controller_DS-K1T200EF	MF/CF 10.7.3	8.64 80	00 Yes	No	

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

🗘 Add to Client 🛛 🗘 A	dd All Device 🛛 🖸 Edit Network 🔦 Reset P.	P Activate			Filter	
Name	Туре	IP	Port	Activated	Added	·
44-19-b6-03-c7-e2	Access Controller_DS-K2604-G	10.7.38.168	8000	Yes	No	
44-19-b6-c1-42-5e	Access Controller_DS-K2604	10.7.38.26	8000	Yes	No	
44-19-b6-a3-4b-06	Access Controller_DS-K2604-G	192.0.0.64	8000	No	No	
44-19-b6-c1-5a-e3	Access Controller_DS-K1T200EF/MF/CF	10.7.38.64	8000	Yes	No	

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		

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

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

7.2.3 Controller Management

Interface Introduction



icon to enter the controller management

interface.

Click the

Add Device	Edit Del	ete Bulk Time	Adj	tus Remote Con	fig	Refresh	Filter	
łame	Туре	Connection Mode	IP .	Port Baud Rate	Dial-up	Connection Status	Refresh	
23	Access Controller_DS-K2601	TCP/IP	10.16.38.164	8000	1	Offline	ø	
Online Devices (C	0)	Refresh						
Inline Devices (C	9) It. Q: Add All Device	Refresh	Reset P.	• Activate			Filter	
Inline Devices (C Add to Clien lame	0) It 🕀 Add All Device Typ	 Refresh Edit Network 	Reset P.	Activate	Port	Activated Activ	Filter	

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:

	ado	d the access controller	_
Name:			
Type:		Access Controller_DS-K2601	~
Connection N	Method:	TCP/IP	~
Address:			
Port:		8000	
Baud Rate:			~
Dial-up:		1	
Account:			
User Name:			
Password:			

- 2. Input the device name.
- 3. Select the access controller type in the dropdown list.
- 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.



6. Click the Add 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.

		Edit Access Controller	×
Hardware Par Reading Hard	Time Settings Network Settin	Linked Captur	
- 123	Basic Information	Door_1	
Teader In_1			
Teader Out_2	Name:	123	
	Connection Method:	TCP/IP	
	Address:	10.17.138.232	
	Port:	8000	
	Baud Rate:	×	
	Dial-up:	1	
	Account:		
	User Name:	admin	
	Password:	10100	
	Enable Holiday		
		Edit Cance	4

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)

	Edit Access	Controller	×
Hardware Par Reading Hard	Time Settings Network Settings Linked C	Captur	
- 📶 123	Basic Information Door_1		
Teader In_1	Items	Options	Value
Teader Out_2	Door Magnetic	Remain Closed 🗸	
	Exit Button Type	Remain Open 🗸 🗸	
	Door Locked Time (s)		5
	Door Open for Disabled Person		15
	Door Open Timeout (s)	· · ·	30
	Enable Lock Door when Door Close	Yes	
	Duress Code		
	Super Password		
	Dismiss Code (Max. 8 digits)		
			Restore De
			Edit Cancel

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

		Edit Access Controller ×
Hardware Par Reading Hard	Time Settings Network S	Settings Linked Captur
- 123	Basic Information	Expansion Information
Reader Out_2	Name:	Reader In_1
	Dial-up:	1
	Account:	
	User Name:	
	Password:	
		Edit Cancel

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 Delete 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.

Steps:

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, Multi-door Interlocking Status, Anti-passing Back Status, 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 this interface, you can set the access parameters, enable the face detection function, and so on.

🛚 🚳 System	Configure Acs Paramters.	
Device Infor		
General	Downstream RS485 communication backup	
System Mai	Display face detection picture	
@ RS485	Display card	
Security Network	Display user information	
Alarm	Superimposed user information	
Others Acs Parame	Enable voice prompts	
Acs Picture	Upload pictures to capture whether the linkage	
Face Detect	Save interact capture picture	
Status	Enable manually entering card no	
	Apply	
	·	

Network Settings

Purpose:

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

Uploading Mode Settings

	N	etwork Sett	ings	×
Upload Mode Setting	Network C	enter Setting	is Wireless Commu	unicati
Center Group:	Center Grou	up1	~	
	Enable			
Report Type:	Alarm Data		~	
Upload Mode	Main Ch	Off	~	
	Backup	Off	×	
				ок

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

	Network Settin	ys ×		Network Settin	gs
oload Mode Settings	Network Center Settings	Wireless Communicati	Upload Mode Settings	Network Center Settings	Wireless Communicati
Network Center:	Center1	~	Network Center:	Center1	×
Address Type:	IP	 Image: A start of the start of	Address Type:	Domain Name	~
IP:			Domain Name:		
Port:			Port:		
Protocol Type:	Private	~	Protocol Type:	Private	¥
Account Name:			Account Name:		
		04			

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. Select the address type in the dropdown list: IP, or Domain Name.

IP: Input the IP address, and port No..

Domain Name: Input the domain name, and port No..

- 5. Select the protocol type: Ehome.
- 6. Set an account name for the network center. A consistent account should be used in one platform.
- 7. 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 No. of the wireless network and wired network should be consistent with the port No. of Ehome.

7.2.4 Access Control Point Management

Interface Introduction

		Access Control Point
	Ľ	The adding, deleting and editing of person and
Click the		department.

icon on the control panel to enter the door

management interface.

😔 Add Group 🛛 😂 Delete Gro	Access Control Point under Group	Test_1		
Search P	🔶 Import 🛛 Edit	Delete		Filter
Test_1	Name	Belong to Controller	Door Camera	Position
Test_2	123_Door1	123	1	
Test_3				
Test_4				

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 Add Group button to pop up the Add Group dialog.



Input the group name in the text field and click the OK 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 ²³ Delete Group button.
- Right-click a group and select Delete in the popup menu.
- ◆ Move the mouse onto the group and click ²²³ 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:

- Click the Import 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 Import button to import the selected access control points or click

Import All 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:

- Click to select an access control point in the list and click the Edit button to edit the access control point.
- 2. Edit the Door Name and Position.
- 3. Click OK button to finish editing.

NOTE 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

Delete button.

51

Click to select a group in the group list, and click
 Delete
 button to delete all

access control points under the group.

Move the mouse onto a group in the group list, and click ³²³ button to delete all access control points under the group.

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

	Import Access Control	Point		×
Access Control Point			Group	
Search	9		Search	9
10.7.52.106			- 🗾 test	🥖 ×
			10.7.52.106_Door1	
		Import		
		Invest All		
		Import All		

Steps:

- 1. Select a control point on the Group panel.
- 2. Click the Keiner the Edit Access Control Point panel or to delete the

control point.

7.3 Permission Management

7.3.5 Person Management

Interface Introduction



icon on the control panel of the software.

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

Add Depart 🛛 😂 Delete Dep	Person List				
Search 9	🗘 Add Person	Edit	Delete	FI	lter
🖻 🚣 Default	Name	Gender	ID Type	ID No.	Contact Phone No.
	Fiona	Female	ID	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	xx
	Cathreen	Female	Social Security Card	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
	Lela	Female	ID	000000000000000000000000000000000000000	
	Shanna	Female	Driver's License	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
	Olivia	Female	ID	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
	Steave	Male	ID	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
	Mike	Male	Passport	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
	John	Male	Officer ID	000000000000000000000000000000000000000	
	Jack	Male	Student ID	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
	Sunny	Female	Student ID	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
,	Total:10	Page1/1		M	Go to

Department Management

Steps:

1. In the department list, click

🗘 Add Depart...

button to pop up the adding

department interface.

	Add Department	×
Upper Depart	Default	
Department Na		
	OK Cancel	



• Multi-level department system can be created. Click a department as the

upper-level department and click Add Depart... 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 Delete Depa... 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 ban be added.
- Inputting General Information

Steps:

1. Select a department in the list and click the Add Person in the person information

list to pop up the adding person interface.

Conoral	Figaemist	
General	Fingerprint	
Person No.:	1511111439040367470	
Person Name:		
Gender:	Male C Female	
ID Type:	ID ~	
ID No.:		Upload Picture
Belong to Dep	Default	
Contact No.:		
Contact Address:		

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



NOTE 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 Delete 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:

- Person Information
 X

 General
 Fingerprint

 Image: The contract of the contract
- 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.
- The fingerprint associated functions are only supported by device with fingerprint recognition module.
- The fingerprint associated functions are only supported by device with fingerprint recognition module.

7.3.6 Card Management Interface Introduction



on the control panel of the software to enter the card

management interface.

Empty Card	Normal Card	Card Reported Loss			
Empty Card List					
Add Card Is	sue Card Delete			Filter	
Card No.			Status		Ċ
0001			Empty Card		
0002			Empty Card		
0003			Empty Card		U
0004			Empty Card		
0005			Empty Card		

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. Refer to Section 0 Card Dispenser Configuration for details.

Steps:

- 1. Click the Add Card 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 Start Date, Expiring Date and Card No. in the text field.

	Add Card	×
Adding Meth	Add One O Bulk Adding	
Activation Da	2015-07-29 00:00:00	
Expiry Date:	2036-12-31 00:00:00	
Enter card No.:		
	OK Cancel	

Batch Adding Cards

Choose the Bulking Adding as the adding mode by clicking the Section 1 to Section 1 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

	Add Card	×
Adding Meth	Add One	
Activation Da	2015-07-31 00:00:00	
Expiry Date:	2036-12-31 00:00:00	
Start card No.:		
End Card No.:		
	OK Cancel]

- 3. Click the OK button to finish adding.
- 4. Click an added blank card in the list and click **Issue Card** 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.

Issue Card X
Card No.: 001 Please choose responding person for card:
Search
- 🏯 Default
🚨 Fiona
A Office 1
Please choose responding fingerprint for card:
Tip: Please collect fingerprint data on device.
OK Cancel

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





- 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.
- The fingerprint associated functions are only supported by device with fingerprint

recognition module.

Deleting Card

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

Normal Card

Click the Normal Card 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.

Empty Card	Normal Card	Card Reported Loss			
Normal Card List					
Card Change R	eturn Card Report Card	L Password Sett		Filter	
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.

Password Settings		
Card No.:	123	
Card Password:		
	OK Cancel	



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.

7.3.7 Schedule Template Interface Introduction

	Ê	Template The adding, deleting and	
Click		editing of duration, week plan and holiday.	on the control panel of the software to enter the schedule

template interface.

Add Week 23 Delete Wee	Property		🖬 Sar
arch P			
Enable Week Plan by Default	Week Plan	Enable Week Plan by Default	
Disable Week Plan by Def			
	Remark:	Enabling week plan will take effect of all the card usage in one week, and cannot be edited and deleted.	
		🐻 Copy to 🗱 Delete Du 🛍	Clear Dur
		00 02 04 06 08 10 12 14 16 18 20	22 24
	Monday		
	-		
	Tuesday		
	wednesda	ay and a second s	
	wednesda		
	Thursday		
	Thursday		
	Thursday Friday		
	Weanesda Thursday Friday Saturday		

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.

	Add Week Plan	×
Week Plan Na]
	OK Cancel	

- 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.

Holiday Group OK Cancel		Add Holiday Group	×
OK Cancel	Holiday Group		
		ОК Са	incel

2. Input the name of holiday group in the text filed, and click the OK button to

add the holiday group.

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

duration of the holiday.

- The second sec			
NOTE	At most 16	holiday periods	can be added.

Holiday list		🗘 Add holiday	Next			
Seria	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	X 🗄 X
2	2014-10-30 🛗	2014-11-01 🔯	00 02 04	06 08 10 12 14	16 18 20 22 24	X 🖞 X
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.



Steps:

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

	Add Template	×
Template Name:		
	ОК	Cancel

- Input the name of schedule in the text filed, and click the OK 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.

Add Template 🛛 😂 Delete Tem 🛛 F	operty	🖬 Sa
rch P		
Default Enable Schedule T	Template Name: Template_1	
Default Disable Schedule		
Template_1	Remark:	
	🔟 Week Plan 🔳 Holiday Group	
	Week P Enable Week Plan by Default Y	
	00 02 04 06 08 10 12 14 16	18 20 22 24
	Monday	
	Tuesday	
	Wednesday	
	Thursday	
	muisday	
	Friday	
	Saturday	

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

NOTE At most 4 holiday groups can be added.

oliday Group to be Se	elected		The selected	l holiday group	
Search	9		Serial No.	Holiday Group Na	Remark
Holiday_1			1	Holiday_1	
	4	Add			
	×	Delete			
	Ē	Clear			

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

🗘 Add

to add it.


7.3.8 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.





icon on the control panel to enter the interface.

arch	Door Status Configuratio	VII		EP Copy To	Sav
10.7.52.106_Door1	Remain Open	Remain Closed	Copy to whole w	X Delete dur	💼 Clea
	Monday	00 02 04 06 0	16 10 12 14 16	18 20 22	24
	Tuesday				
	Wednesday				
	Thursday				
	Friday				
	Sunday				

- 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 Remain Open / Remain Closed 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.





- 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 Copy to whole w... 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 **Click** to delete the time period.

• Clear All Durations:

Click Clear to clear all configured durations on the schedule map.

- 5. Click on Save to save the settings.
- You can copy the schedule to other doors by clicking on Copy To 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.

7.3.9 Interact Configuration



on the control panel of the software to enter the interact

configuration interface.

Case T	rigger	Event Card	Interact	Client Interact				
Case List	B	Apply	Property					Save
Search - 123 Case Case	_1 _2			Host Buzzer:	Name	Property		
				Alarm Output:	Name	Property		
				Door(Open / Close);	Name	Remain Open	Remain Closed	

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 Case Trigger button to enter the case trigger interface, and select a

case.

and the second sec									
se List 🏼 🕹	Apply	Property						E	San
arch	9	Host Buzzer	Not Trigger						
123		and How Duller.	Teor myyer						
Case_1		Reader Buzzer:	Name	Property					
Case_2			Reader In_1	Not Trigger	~				
			Reader Out_2	Not Trigger	~				
		Alarm Output:	Name	Property					
			Alarm Output_1	Not Trigger	~				
			Alarm Output_2	Not Trigger	~				
		Door(Open / Close):	Name	Remain Open		Remain Closed	1		
			123_Door1	Not Trigger	-	Not Trigger	~		

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.



NOTE 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 CAdd button to start setting the event linkage.

Case Ingge	Event Car	1 interac	Client Int	eract					
Host List	🕭 Apply	E	Event card linkage o	letailed inform	nation				Add 🛛 Delete 🖬 Save
3earch		9	Event Li Ev	ent device	~ Device	e Tamp	ering Alarm	~	O Card Li
123			Linkage target						
			Controller	Not Trigger	~				Snapshot Not Trigger 💙
			Name	e Name I					Name Name I
			Reader In_1	Not Trigger	~				Alarm Output_1 Not Trigger ~
			Reader Out_2	Not Trigger	~				
			Door						
			Name		Open		Close		Normally Open Normally Close
			123_Door1		Not Trigg	er 🗸	Not Trigger	~	V Not Trigger V Not Trigger V

- 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.

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



NOTE 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
- Event Card Interact
 - button to enter the event card interface
- 2. Select the host to be set from the host list.
- 3. Click the CAdd

button to start setting the event linkage.

Case Trigger	Event Card Inte	eract Client Interact				
Host List	Apply	Event card linkage detailed info	rmation		Add 🔀 Delete	Bave Save
Search	9	O Event Li Event device	~ Device Tamp	ering Alarm \vee	Card Li	
- 123		Card Source Card Reader Card Reader 0 Reader 1 Reader Linkage target	n_1 Dut_2			I
		Controller Not Trigger	~		Snapshot Not Trigger Y	
		Name Name			Name Name	
		Reader In_1 Not Trigge	r Y		Alarm Output_1 Not Trigger	
		Reader Out_2 Not Trigge	r Y			
		Door				
		Name	Open	Close	Normally Open Normally Close	
		123_Door1	Not Trigger 🛛 👻	Not Trigger 🛛 👻	Not Trigger Y Not Trigger Y	

- 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.

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



 ${f I\!I\!I\!I}$ The door status of open, close, normally open, and normally close cannot be

triggered at the same time.

Click the

7.3.10 Access Permission Configuration



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 Click on contexperient side of the page to enter the Add

Permission page.

		New Access Control Permission X
Choose Type Permission Settings	1	By Person Hote: Configure access control point for person.
	A	By Department Note: Configure access control point for department.
	-	By Access Control Point Note: Configure access control point to person and department.
		By Door Group Note: Configure person and department permission for door group.
		Previous Next Cancel

- 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.

		New Access Co	ntrol Permission		×
① Choose Type	Template:	Default Enable S	ichedule Templati	e Y	
Permission Settings	Please choose	person.		Please choose the access of	control point and the
	Search		8	Search	9
	😑 🗖 🏯 Det	ault		Access Control Point	Door Group
	E 🚨 F	Fiona		- 🔤 🔄 group 1	
				Previous	e Cancel

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

Template:	Default Enable Schedule Template	~

The schedule template must be configured before any permission settings. Refer to Section

7.3.7 Schedule Template for detailed configuration guide.

NOT

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



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.

Download Permiss	sion
Downloading 💿 Download A	.11
Please choose controller to download.	
Search	9
- 🗆 🎦 All Devices	
🗆 🛃 123	

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

	Downloa	d Result	_	
Permission Download P	Downloade	ed (100%)		
Filter				
Device	Progress	Result	Remark	
123	100%	All Succe	e	
				01
				Close

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.

Add Perm Delete Permis	Start Downloading]		
Major Type: By Staff	Y Minor Type:	Access Control Point Y Keyword:		Search Rese
Name	Department	Access Control Point	Template	

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

🗘 Add Perm	Delete Permis	Star	t Downloading						
Major Type:	By Staff	~	Minor Type:	Access Control Point	~	Keyword:		Search	Reset

3. Click Search to get the search results.

🗘 Add Perm	Delete Permis	Start Downloading]		
Major Type:	By Staff	Y Minor Type:	Access Control Point Y Keyword:	Search	Reset
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	

NOTE

NOTE 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.

🗢 Add Perm.	Delete Permis	Start Downloading			
Major Type:	By Staff	Y Minor Type:	Access Control Point * Keyword:	Search	Reset
Name		Department	Access Control Point	Template	
Fiona		Default	123_Door1	Default Enable Schedule Templa	ite

NOTE

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

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

Information	×
Delete the selected access control permission?	
OK Cancel	

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.

7.3.11 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.



icon on the control panel to enter the

interface.

Add Edit	Delete				Filter
Serial No.	Shift Group Name	Shift Group No.	People Coun	Remark	

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

Add

button to pop up the shift group formation window.



2. Enter the shift group name, and click the Add 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 _____OK ____ button and

return to the shift group settings interface.

*Shift G	ro Shift Group 1	Shif	t Gro 0001	
erson Lis	ıt		¢.,	Add Delete
	Serial No. Fiona	Name	Gender De ale Defau	partment Name
2	Cathree	n Fem	ale Defau	ult
3	Lela	Fem	ale Defau	ılt
4	Shanna	Fem	ale Defau	ılt
5	Olivia	Fem	ale Defau	itt

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

Delete button.

4. Click the OK button to complete the operation.

Serial N	o. Shift Group Name	Shift Group No.	People Coun	Remark		
1	Shift Group 1	0001	5			
2	Shift Group 2	0002	5			
Total 2	Page1/1 Item per Pag	je: 50 v		14 4	N	Go
				And Arts	Colore Sheet - L	
-						
You can	edit and dele	te the added	shift groups b	y clicking the	Edi	t
			0 1	, 0		

Shift Management

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

No. 2020 Mills				
- Normal Shift	🖂 Serial I	No. Rule Name	Remark	
Attendance Rule	1	Attendance Rule 1	For technical staff	
Attendance Shift	2	Attendance Rule 2	For Cleaning Staff	
Man-Hour Shift	3	Attendance Rule 3	For administration staff	

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

Normal Shift

• Setting Attendance Rule

Steps:

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

The items with aster	sk are required.	
*Rule Name		
Rem		
Detailed Parameters		
On-Work Attendance	Check Advanced 0	
On-Work	Late Time (Minutes) 0	
Absence Threshold	(Late, Unit: Minutes) 0	
E	Break Time (Minutes) 0	
Off-Work Attendance	Check Delay Time 0	
Off-Work	Early Time (Minutes) 0	
Absence Threshold	(Early-Leave, Unit 0	

- 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).
- Click the OK button to complete the operation. 4.
- **Setting Attendance Shift**

Steps:

1.

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

				_				
*5	Shift Name:			Sh	ft No.:	0001		
	Rem							
f/4	On-Work Period	i.						Clear
	On-Work Ti		On-work Time	E.	Off-worl	time	Attendance Rule	ï
	On-Work Ti	Day	-	Day	~			~
	On-Work Ti	Day	~	Day	~			~
		Day	~	Day	~			~
3	On-Work Ti							

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



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

• Setting Man-Hour Shift

Steps:

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

*Shift Name:		*Shift No.:	0002	
aily working		Latest On-Work		
Rem				
egard Man-Hour Pe	riod			Clear
Time Period	Start Time	End Time		
Time Period1				
Time Period2				
Time Period3				
Time Period4				
	*Shift Name: ally working Rem Time Period Time Period Time Period2 Time Period3 Time Period4	*Shift Name: ally working Rem egard Man-Hour Period Time Period Time Period1 Time Period2 Time Period3 Time Period3	*Shift Name: *Shift No: ally working Rem egard Man-Hour Period Time Period Start Time End Time Time Period1 Time Period2 Time Period3 Time Period4	*Shift Name: *Shift No.: 0002

- 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 OK 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.

Rem					
ate List				🕀 Add	Delete
Serial N	lo. Da	ate	Week		
3 1	2016-01-01	Friday			
2	2016-01-02	Saturd	lay		
3	2016-01-03	Sunda	iy		

2.

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

Start Date	2015-11-12	1	*End [Date 201	5-11-12	2
ect by Week						✓ Sel
🛃 Mondaj	y 🕑 Tues	✓ Wed…	🕑 Thur	🕑 Friday	Satur	🕑 Sunday

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

button.

Shift Schedule Management

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

Shift Group Ma., Shift Managem.	HolidayMan	ag Shi	t Schedul	e Atter	ndance Ch Ad	ljustment Ma	. Card Swiping L.	Statistic Analysi	s Parameters Co	. Data Manage
Shift Grou		Add	De	lete						Filter
San Orop 1 San Orop 2	2) Si	Devia No.		Wonling Date		Shift Name		Shift No.	1
	Te	rtal 0	Ра	201/1	ltern per P	age: 50		н	4 F F	et oD

Steps:

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

Shift Grou.	group1		Shift Name:	Normal Shift1	~
*Start Date	2015-11-12	1	*End Date:	2015-11-12	1
dd Holiday					
Serial N	o. 🕴 Holiday Nam	ie Ho	iday Days	Remark	
1	Holiday 1	3			

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

Attendance Check Point Management

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

Add	Edit	Delete						Search	3
Serial No.	Attendance Chec	king Point Name	Attendance Checki	Start Date	Validity	Door Position	Reader Name	Attendance Checkin	g Point Description
1	123_Door1_Che	king Point_1	On/Off Work Che	2015-11-12	2015-11-12		Reader In_1		
2	123_Door1_Che	cking Point_2	On/Off Work Che	2015-11-12	2015-11-12		Reader Out_2		
3	456_Door1_Cher	king Point_3	On/Off Work Che	2015-11-12	2015-11-12		Reader In_1		
4	456_Door1_Che	king Point_4	On/Off Work Che	2015-11-12	2015-11-12		Reader Out_2		

• Adding Attendance Check Point

Steps:

v A00	Edit Delete					obaren.	
🗌 Seria	I No. Attendance Checking Point Na	me (Attendance Checki)	Start Date Va	lidity Door Position	Reader Name	Attendance Che	cking Point Descripti
8 1	123_Door1_Checking Point_1	On/Off Work Che	2015-11-12 2015	5-11-12	Reader In_1		
2	123_Door1_Checking Point_2	On/Off Work Che	2015-11-12 2015	5-11-12	Reader Out_2		
3	456_Door1_Checking Point_3	On/Off Work Che	2015-11-12 2015	5-11-12	Reader In_1		
4	456_Door1_Checking Point_4	On/Off Work Che	2015-11-12 2015	i-11-12	Reader Out_2		

- 1. Check the checkbox of a checking point, and click the **Edit** 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 OK button to complete the operation.
- Adding Attendance Check Point

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

Adjustment Management

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

djustment Management	Add Edit Delete	Search	
Reason Management	🗇 🕴 Serial No. 🕴 Reason Management		
Leave	1 Leave for Personal Affairs		
Leave in Lieu	2 Sick Leave		
Overtime	3 Marriage Leave		
Replace Card	🗇 4 Funeral Leave		
List Management	🗂 5 Home Leave		
Disabled	🗇 6 Annual Leave		
Disabled	7 Maternity Leave		
	B Paternity Leave		

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.



Add

2. Click the

button to pop up the adjustment reason adding dialog box.

The items with ast	erisk are re	equired.	
Adjustmen	Leave		
*Adjustmen	12		

3. Enter the adjustment reason, and click the _____OK ____ 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 <u>Edit</u> button to edit the reason, and click the <u>Delete</u> button to delete the reason.

Leave in Lieu

Steps:

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

Add	Edit	Delete		Search	P
🖂 🗌 Ser	ial No.	Reason Manag	ement		
0 1	Overti	me			
2	Busin	ess Trip			
Total:2	Page1/1	Item per Page:	50 4		Go to
	• •	Total:2 Page1/1	Image: Senal No. Reason Manage Image: Senal No. Reason Manage Image: Senal No. Senal No. Image: Senal No. Reason Manage Image: Senal No. Senal No. Image: Senal No. Reason Manage Image: Senal No. Senal No. Image: Senal No. Senal No. </td <td>Total2 Page1/1 Rem per Page: 50 Y</td> <td>Setial No Reason Management 1 Overtime 2 Business Trip Total:2 Page1/1 Total:2 Page1/1 1 Nem per Page: 50</td>	Total2 Page1/1 Rem per Page: 50 Y	Setial No Reason Management 1 Overtime 2 Business Trip Total:2 Page1/1 Total:2 Page1/1 1 Nem per Page: 50

2.

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

Adjustmen Leave	The items with aste	erisk are required.	
*Adjustmen	Adjustmen	Leave	
	*Adjustmen		

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



- The default adjustment reasons for leave in lieu include overtime, and business trip. •
- You can check the checkbox of a reason and click the Edit button to edit the ٠ reason, and click the Delete button to delete the reason.
- Overtime

Steps:

- Shift Group Ma., Shift Managem., Holiday Manag., Shift Schedule., Attendance Ch., Adjustment Ma., Card Swiping L., Statistic Analysis Parameters Co., Data Manage. Adjustment Management 😔 Add Edit Delete - Reason Management E Serial No. | Reason Management 1 Work Requirement Leave Leave in Lieu 2 Working Day Overtime
 3 Rest Day Overtime Overtime Rest Day Overtime Replace Card 0 4 Holiday Overtime - List Management Enabled Disabled Total:4 Page1 / 1 Item per Page: 50 👻 H 🚽 🕨 Go to
- 1. Press the overtime tab to enter the overtime interface.

2. Click the Add

button to pop up the adjustment reason adding dialog box.

The	items wit	h asteri:	sk are i	equired	i.		
	Adjustm	en L	eave				
	*Adjustm	en					
				ок		Cancel	

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 Edit button to edit

the reason, and click the	Delete	button to delete the reason.
---------------------------	--------	------------------------------

Replace Card

Steps:

1. Press the replace card tab to enter.

Add



2. Click the

button to pop up the adjustment reason adding dialog box.

Adjustmen Leave	
*Adjustmen	

3. 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 <u>Edit</u> button to edit the reason, and click the <u>Delete</u> button to delete the reason.

List Management

Enabling

Steps:

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

Readon Management Leve Leve Leve Leve Lave Lave Lave Serial No. Form No. Person Name Department Name Start Time End Time Adjustment Type Adju Low Form Replace Card J 2 201511 Shanna Default 2015-11 2015-11 Leave in Like Bas Overtime Replace Card Disabled	Pitter							elete		Disable	Add	0	djustment Management
Lave in Lieu Leve in Lieu Leve in Lieu 2 2 201511. Shanna Default 2015-11. Leve in Lieu Bus Overtime Replace Card Lat Management Enable Disabled	djustment Rea	ype Ad	stment Typ	Adj	End Time	Start Time	rtment Name	Name	Perso	Form No.	Serial No.		Reason Management
Lazer di Lieu Detrime Card Card Clat Management Eabled Disabled	lick Leave	Si		Leave	2015-11	2015-11	it	5	Fiona	201511	1		Leave
Overtime 3 201511 Lela Default 201511 201511 Overtime Work Usabled Disabled Image: State of the state of th	Jusiness Trip	BL	in Lieu	Leave	2015-11	2015-11	it.		Shan	201511	2		Leave in Lieu
Replace Card _: Lat Management Enabled Disabled	Vorking Day O	W	ne	Overt	2015-11	2015-11	t.)	Lela	201511	3		Overtime
Lut Mangement Esabled Desabled													Replace Card
Enabled													List Management
Disabled													Enabled
													Disabled
												4.1.	

2. Click the Add button.

Serial No.		Name	Gende	r C)epa
)	7.6
5 <mark>-11-1</mark> 2 00:00:00	1 - 1	2015-11-12 23:	59:59 📆		
	5-11-12 00:00:00	5-11-12 00:00:00 🔯 - 🛛	5-11-12 00:00:00 🔃 - 2015-11-12 23:5	5-11-12 00:00:00 🔀 - 2015-11-12 23:59:59 🔯	5-11-12 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 Add button to pop up the person adding window.

	OK	Of	

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

Replace Card

1) Select the radio button of replace card.
| Staff: | | | | | | 🗘 Add | Dele | te |
|---------------------------|--|-----------|-------|-------|----------|------------|------|------|
| | I I S | erial No. | Ť | Name | Î | Gender | [| Depa |
| | | | | | | | | |
| | | | | | | | | |
| | 4 (| | | | | | | |
| Select Date: | 2015-11-12 | | | Atten | Normal S |)
Shift | ~ | |
| Select Date:
Card Repl | 2015-11-12 Time | On | Off- | Atten | Normal S |)
Shift | ~ | |
| Select Date:
Card Repl | 2015-11-12
Time
Time | On | Coff- | Atten | Normal S | Shift | ~ | |

- 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 OK button.
- 5) Set the date, attendance shift, and card replacing time.
- 4. Click the OK 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.

Shift Group Ma Shift Managem	Holiday Manag S	hift Schedule /	Attendance Ch	Adjustment Ma Ca	rd Swiping L	Statistic Ar	nalysis Parameters C	o Data Manage
Adjustment Management	😔 Add	Disable	Delete					Filter
E Reason Management	🖸 Seri	al No. Form No.	Person Name	Department Name	Start Time	End Time	Adjustment Type	Adjustment Reason
Leave	. 1	201511	Fiona	Default	2015-11	2015-11	Leave	Sick Leave
Leave in Lieu Overtime								
Replace Card								
🔄 List Management								
Enabled								
Disabled								
	10					_) •
	Total:1	Page1/	1 litem pe	er Page: 50 🐂			H 4 P H	Go to

Card Swiping Log Query

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

Query Ty	By Department		~	Department	Default		~	Name:			Search
Query Sc.	All		*	Start Date:	2015-11	-12 00:00:00	1	End Date:	2015-11-12 23:59:59		Reset
earch Result											
Serial	Person Name	Card	No.	Swiping	Time	Department		Card Reader	Reader Name	Door Name	Controller Na
1	P1	05092661	31	2015-11-12 2	3:01:06	Default	260	4_Door4_Chec	ki Reader In_7	2604_Door4	2604
2	P1	05092661	31	2015-11-12 2	3:01:05	Default	260	4_Door4_Chec	ki Reader In_7	2604_Door4	2604
з	P1	05092661	31	2015-11-12	18:05:26	Default	260	4_Door4_Chec	N Reader In_7	2604_Door4	2604
4	P1	05092661	31	2015-11-12	8:30:52	Default	260	4_Door4_Chec	ki Reader In_7	2604_Door4	2604
5	P1	05092661	31	2015-11-12 0	18:30:51	Default	260	4_Door4_Chec	ki Reader In_7	2604_Door4	2604
6	P1	05092661	31	2015-11-12 0	8:30:49	Default	260	4_Door4_Ched	N Reader In_7	2604_Door4	2604
7	P1	05092661	31	2015-11-12 0	18:30:48	Default	260	4_Door4_Chec	ki Reader In_7	2604_Door4	2604



- 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.

100		(accession accession)			General		
ndance Analysis Table	Shift Type:	Normal Shift	v	Department:	Default	·	Search
ndance Result Statistic Table	Start Date:	2015-11-12 00:00:	00 🔯	End Date:	2015-11-12 23:59	59 📆	Reset
ndance Rate Statistic Table	🔒 Export				2015-11-12 23:59:59 (Analysis Table Jame Time Period On-Work		
				Attendance Ana	lysis Table		
	Attendance Stat	istic Period				i9 💽 Reset	
	Name	Department	Date	Shift Nam	e Time Period	On-Work Attendar	c On-Work Status

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.

	01/07							
endance Analysis Table	Shift Type:	Normal Shift	v	Department:	Default	~	Search	
endance Result Statistic Table	Start Date:	2015-11-12 00	00:00	End Date:	2015-11-12 23:59	59 📆	Reset	
endance Rate Statistic Table	Export							
				Attendance Ana	alysis Table			
	Attendance Stat	istic Period 2015-	11-12 00:00:00 -	2015-11-12 23:59	:59			
	Name	Department	Date	Shift Nam	e Time Period	On-Work Atte	ndance Checking Time	
	P1	Default	2015-11-12	Normal Shift1	1	2015-11-12 08	30:48	1
							Search Reset endance Checking Time 3 30.48	



- 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.

tatic Type							
Attendance Analysis Table	Shift Type:	Normal Shift	♥ De	epartment: Default		Search	
Attendance Result Statistic Table	ex Analysis Table Export Start Date: 2015-11-12 00:000 End Date: 2015-11-12 23:95.9 Export Attendance Result Statistic Table Attendance Result Statistic Table Attendance Result Statistic Table International Statistic Period 2015-11-12 23:95.99 Name Department Required Attend_Actual Attendance Rate P1 Default 1 1 1 000000 0	Reset					
Attendance Rate Statistic Table	Export						
			Attenda	nce Result Statistic	Table		
Abendance Rate Statistic Table	Attendance Stati	istic Period 2015-11-1	2 00:00:00 - 2015-1	1-12 23:59:59			
	Name	Department	Required Attend	Actual Attendanc	Attendance Rate	Late Times	Early-Leave
Adendance Ravis Statsto: Table Start Date: 2015-11-12 0.000.0 Start Date: 2015-11-12 0.000.0			0				



- 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.

ic Type											
Attendance Analysis Table	Shift Type.	Normal Shift	v	Department	Default	Searc	<u>n</u>				
Attendance Result Statistic Table	Start Date:	2015-11-12 00:00:0	0 📅	End Date:	2015-11-12 23:59:59	Rese	e				
Mendance Rate Statistic Table	C. Faut										
	Les Export		Atte	ndance Rate S	tatistic Table						
	Attendance Statistic Period 2015-11-12 00:00:00 - 2015-11-12 23:59:59										
	Name	Department	Date	Shift Na	me Day Required At.	Day Actual Atten	Day Attendar				
	P1	Default	2015-11-12	Normal Shi	R1 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.

nift Group Ma Shift Managem.	. Holiday Manag Shit	t Schedule	Attendance Ch	Adjustment Ma	. Card Swiping L	Statistic Analysis	Parameters Co	Data Manage
Attendance Effecting Type:	Valid Card Record	~						
Data Saving Time:	3 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.

Calculate Atten	2015-11-12 00:00:00	100	-	2015-11-12 23:59:59	12	Calculate Atten
Import/Export	2015-11-12 00:00:00	1 3	-	2015-11-12 23:59:59		
Export Data:						View
Import Data:						View

Click the Calculate Atten...

button to calculate the attendance date.

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

7.3.12 Advanced Functions

Purpose:

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



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.

Access Control Type	Card Reader Aute	Multiple Authentic	First Card	Anti-passing Back	Multi-door Interloc	White List	Password Authenti
Controller Group	🕹 Apply	Card List					
Search	9	Add	Delete			Filter	
- 🗐 123		Card No.	Status	Activation Date:	Expiry Date:		
Normal C	Card						
Card for	Disabled Person						
🔄 Card in E	Blacklist						
Patrol Ca	ard						
🔄 Duress C	ard						
🔝 Super Ca	ard						
Visitor Ca	ard						
		Total:0	Page1/1			M 4	Go to

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 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 16.2.3 Normal Card.

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.



The fingerprint associated functions are only supported by device with fingerprint recognition module.

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.

ccess Control Type	Card Reader Aute	Multiple Ar	uthentic First	Card	Anti-p	assing B	ack M	ulti-doo	r Interio	D	White	List	Passw	ord Aut	nenti	
Card Reader List	🕭 Apply	Property											Copyte			s
Bearch	5	>														
123			Card Reade	Reader	In_1											
Reader I	n_1 Dut 2		Card Reader Aut	Swipe C	ard & Pa	ssword										
			Weekly Schedule Se	ettings					Copy to	.	×	Delete		Clea	r	
			00 • Monday	02	04	06	08	10	12	14	16	18	20	22	2.	
			Tuesday													
		Wednesday														
			Thursday													
			Friday													
			Saturday													
			Sunday													

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.

Controller 🖄 Apply	Access Control Point First Card Parameters	Save
Search 9	Access Control Point Enable First Card Rem Remain Ope	Duration
1 23	456_Door1 🖌 10	
456		

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.

NOTE

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.

oller 👌 Apply	Property	E s
ch P		
123	Controller Name: 123	
456	First Card Baadeer Dirable	
	Prist Calu Reader. Disable	
	Seria Card Reader Card Reader Afterward	Enable Anti-p
	1 Reader In_1	
	2 Reader Out_2	

- 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.

White List

Steps:

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

Controller Lis 🖄 Apply		Telephone Whitel	ist Settings						🗘 Add		😂 Delete	E Save
Bearch	9	Telephone										
- 🛋 123		Permission										
456		Pennission										
		Door:										
		Name		Op	en	Close	Normally O	pen	Normally Cle	ose		
		456_Door1		For	bidden 👻	Forbidden ~	Forbidden	~	Forbidden	~		
		Zone:			100							
		Zone:	1.0		-							
		Alarm In 1	Earbidden	v	Eorbidden							
		Alarm In 2	Forbidden	~	Forbidden	~						
		Alarm In_3	Forbidden	~	Forbidden	~						
		Alarm In_4	Forbidden	~	Forbidden	~						
		Alarm In_4	Forbidden	~	Forbidden	•						
		Alarm In_4	Forbidden	~	Forbidden							
		Alarm In_4	Forbidden	~	Forbidden	×						
		Alarm In_4	Forbidden	~	Forbidden	~						
		Alarm In_4	Forbidden	~	Forbidden	•						
		Alarm In_4	Forbidden	~	Forbidden	•						

- 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 commands)	Command#2#Operation Object#

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.

Controller List 🙁 Apply	Reader List				
Search P	Add Delete			Filter	
- 📶 123	Card No. Password	Activation Date:	Expiry Date:		
	0001	2015-07-31	2036-12-31		

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

_	_	Add Card
Please select card t	o add.	
		Filter
Card No.	Status	Password Oper
0001	Normal Card	ß
0002	Normal Card	ß
0003	Normal Card	ß
0004	Normal Card	ß
0005	Normal Card	ß
Total:5	Page1/1	Go to
		OK Cancel

3. Check the checkbox of the corresponding card, and click the \square button to pop up the

password setting dialogue box.

	Password Settings	×
Card No.:	0001	
Card Password:		
	OK Cancel	

- 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.

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.

7.4.13 Status Monitor

Purpose:

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



icon on the control panel to enter the interface.

Access Control Group	Status Information	📕 Open Door	Close Door	Remain O	Remain Cl	Capture
Search 9	123_Door1					
	Live Event					More
		Event Source::				
		Card No.:				
		Event Type:				
		Time:				

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.

Always Open : Click on the button to keep the door open.

Always Close : Click on the button to keep the door closed.

- Capture : Click on the button to capture the picture.
- 4. You can also right click the icon



NOTE 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.

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::	test001_Door1	
	Card No.:		
	Event Type:	Normally Open Started	
	Time:	2014-09-12 19:07:56	

7.4.14 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.

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

icon on the control panel to enter the interface.

Access Con	trol Event Information	n					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: Name: Gender: ID Type: ID No: Belong to Contact No: Contact Ad

Steps:

Click the

- 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.

7.4.15 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.

			Icon on	the cont	roi panei to enter the in
Event Type: Card Holder:	All	Start Time: End Time:	2015-07-31 00:00:00 🔯 2015-07-31 23:59:59 🔯	Search	Card Holder Information
Card No.: Search Result Serial No. Even	Type Card Holder Card N	lo. Event Time	Event Source V Direction	Export Capture images	
					Person No:
					Person No.:
					Person No.:

Steps:

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

Event Type:	All	~	Start Time:	2014-09-18 00:00:00		
Card Holder:			End Time:	2014-09-18 23:59:59	**	Search
Card No.:						

- 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

7.5.16 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.



icon on the control panel to open the Log Search

Click the page.

Search Condition	Search Result					Export
Log Type Configurat Control Log	Serial No.	Operation Type	Occurrence Time	Content		
Operation Type:						
Start Time: 2015-07-31 00:00:00						
End Time: 2015-07-31 23:59:59						
Q. Search						
	Total:0	Page1/1				Go to

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.



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.

NOTE 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.



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.



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.

7.5.17 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.

System Configuration ×					
Common Card Dispatcher Fingerprint Machine Manual Capture	Basic Parameters ✓ Auto Time Synchroniza Everyday v 00:00				
	Restore De Sa	ve			

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.



The fingerprint associated functions are only supported by device with fingerprint recognition module

Manual Capture Configuration

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

Auto Time Synchronization

Steps:

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

System Configuration			
Card Dispatcher	Basic Parameters ✓ Auto Time Synchroniza Everyday ✓ 00:00]	

- 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.

NOTE

 \blacksquare 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.

Card Dispatcher

	S	system Configuration		×
Common	Туре:	D8E-U-A-III	~	
Bingerprint Machine	Serial Port Type:	USB	~	
📸 Manual Capture	Serial Port No.:		~	
	Baud Rate:		~	
	Overtime:	200		ms
	Buzzing:	● Yes 🔘 No		
	Card No. Type:	General	~	
				Restore De 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

Reprint Machine

icon on the System Configuration interface to open

the Fingerprint Machine Configuration page.

		System Configuration ×
Common Card Dispatcher Card Dispatcher	Device type: Serial Port No.: Baud Rate: Device Code: Overtime:	System Configuration × Optical fingerprint collecting ins COM1 19200 0 5000 ms
		Restore De Save

- 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.



- The fingerprint associated functions are only supported by device with fingerprint recognition module
- 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:

Click the

1.

ญ Manual Capture

icon on the System Configuration interface to

open the Manual Capture Configuration page.

	Syste	m Configuration	×
Common			
Card Dispatcher	Size:	CIF ~	
Bingerprint Machine	Quality:	High ~	
Manual Capture 🔹 🕨			
			Restore De Save

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



• 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.