

Access Controller

User Manual

V1.0

<u>UD03325</u>

<u>User Manual</u>

COPYRIGHT ©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

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

About this Manual

This Manual is applicable to Master 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

(<u>http://overseas.hikvision.com/en/</u>).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

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

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

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

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

Regulatory Information

FCC statements:

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 interface, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

---Connect the equipment into an outlet on a circuit different from that to which the receiver is

connected.

---Consult the dealer or an experienced radio/TV technician for help

FCC Conditions

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

1. This device may not cause harmful interference.

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

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive

2011/65/EU.



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



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: <u>www.recyclethis.info.</u>

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) 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.



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

A Warnings:

- Please adopt the power adapter from the legitimate factory which can meet the safety extra low voltage (SELV) standard.
- Do not install, wiring, or uninstall when the power is still on.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

ANotice:

- 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 70 $^\circ C$ 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.

0100001061010

Table Of Content

1 Overview	1
1.1 Features	
1.1.1 Master Access Controller Features	1
1.1.2 Distributed Access Controller Feature	1
1.2 Appearance	2
1.2.1 Front Panel and Indicators Description of Master Access Controller	
1.2.2 Rear Panel and Indicators Description of Master Access Controller	
1.2.3 Appearance and Indicators Description of Distributed Access Controller	
1.2.4 Connection Terminal of Distributed Access Controller	6
2 External Device Wiring	19
2.1 Master Access Controller External Device Wiring	
2.1.1 Zone Alarm Input Wiring	19
2.1.2 Fire Alarm Input Wiring	19
2.2 Distributed Access Controller External Device Wiring	
2.2.1 Card Reader Wiring	20
2.2.2 Lock Wiring	21
2.2.3 External Alarm Device Wiring	22
2.2.4 Exit Button Wiring	22
2.2.5 Door Magnetic Sensor Wiring	23
2.2.6 External Power Supply Wiring	24
2.2.7 Zone Alarm Input Wiring	24
2.2.8 Fire Alarm Input Wiring	25
2.2.9 Fire Alarm Linkage Wiring	26
2.3 Master and Distributed Access Controller Wiring	27
3 Hardware Settings	29
3.1 Dial-up Settings	29
3.1.1 Distributed Access Controller Address Settings	29
3.1.2 Dial-up Address Settings	29
3.2 Hardware Initialization Settings	30
4 Activating the Control Panel	31
4.1 Activation via SADP Software	31
4.2 Activation via Client Software	32

5 Overview of Access Control System	35
5.1 Description	
5.2 Configuration Flow	
6 Device Management	
6.1 Controller Management	
6.1.1 Device Management	
6.1.2 Network Settings	
6.1.3 Linked Capture Settings (Do Not Support)	
6.2 Access Control Point Management	
6.2.1 Group Management	
6.2.2 Access Control Point Management	
7 Permission Management	66
7.1 Person Management	
7.1.1 Department Management	
7.1.2 Person Management	
7.2 Card Management	
7.2.1 Empty Card	
7.2.2 Normal Card	72
7.2.3 Lost Card	
7.3 Schedule Template	
7.3.1 Setting Week Plan	74
7.3.2 Setting Holiday Group	75
7.3.3 Setting Schedule Template	
7.4 Door Status Management	
7.5 Interact Configuration	
7.5.1 Event Card Interact	
7.5.2 Client Interact	83
7.6 Access Permission Configuration	
7.6.1 Access Permission Settings	
7.6.2 Access Permission Searching	
7.6.3 Permission Deleting	
7.7 Advanced Functions	
7.7.1 Access Control Type	
7.7.2 Card Reader Authentication	
7.7.3 Multiple Authentication	
7.7.4 First Card	
7.7.5 Anti-Passing Back	

7.7.6 Multi-door Interlocked (Do Not Support)	
7.7.7 White List (Do Not Support)	
7.7.8 Password Authentication	
8 Attendance Management (Do Not Support)	105
8.1 Attendance Configuration	
8.1.1 Shift Group Management	
8.1.2 Shift Management	
8.1.3 Holiday Management	
8.1.4 Shift Schedule Management	
8.1.5 Attendance Check Point Management	
8.1.6 Adjustment Management	
8.1.7 Card Swiping Log Query	
8.1.8 Parameters Configuration	
8.1.9 Data Management	
8.2 Attendance Statistic	
9 Checking Status and Event	122
9.1 Status Monitor	
9.1.1 Access Anti-control	
9.1.2 Access Status	
9.1.3 Real-Time Event	
9.2 Access Control Event	
9.3 Event Search	125
10 System Maintenance	127
10.1 Log Management	127
10.1.1 Searching Configuration Log	
10.1.2 Searching Control Log	
10.2 System Configuration	
10.2.1 Auto Time Synchronization	
10.2.2 Card Dispenser Configuration	
10.2.3 Fingerprint Machine Configuration	
10.2.4 Manual Capture Configuration	

1 Overview

1.1 Features

1.1.1 Master Access Controller Features

- Supports TCP/IP communication and self-adapting network speed and the communication data is more safe with a special encryption method.
- Supports double network interface for uplink communication.
- Supports four RS-485 loops for downlink communication which has functions of dead pixel detection and communication redundancy. It also has a specified network interface to increase the communication bandwidth.
- Up to 64 distributed access controllers can be connected to control maximum 128 doors.
- Supports storing 200 thousand legal cards and 600 thousand records of swiping card.
- Supports opening door with 1000 authentication codes directly.
- Supports functions of anti-passing back, door opening by multi cards, first card, super card or super password, online upgrading and remotely opening door.
- Supports alarm functions of card reader tamper-proof, not-closed door, opening door by force, waiting door open timeout, duress card and code, blacklist and reaching attempts limit of swiping illegal card.
- Supports short circuit attempts alarm and open circuit attempts alarm for zones.
- Supports many kinds of cards including normal card, card for disable person, card in blacklist, patrol card, visitor card, duress card and super card, etc.
- Supports many kinds of status indicators.
- Supports three kinds of time synchronization (NTP, manual or auto).
- Supports offline record keeping and insufficient space alarm for storing records.
- Supports backup batteries, watchdog and tamper-proof functions.
- Supports saving data forever when the master access controller is power off.
- Supports event linkage.
- Supports USB port to upgrade devices (the device will be auto upgraded when restarted), import/export configuration parameters or card parameters and export attendance record.

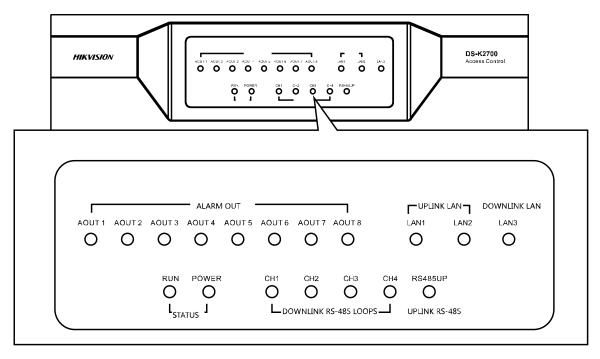
1.1.2 Distributed Access Controller Feature

- Provides high performance and fast speed with 32 bits high speed processer.
- Supports configuring 20 thousand cards via client software, 60 thousand records of swiping card and 20 thousand records of swiping self-learning legal card.
- Provides terminals of door magnetic, door switch and door status detection.
- Supports alarm in and fire alarm in and abnormal circuit (short circuit or open circuit) detection function can be configured.

- Supports alarm functions of card reader tamper-proof, not-closed door, opening door by force, waiting door open timeout, duress card and code, blacklist and reaching attempts limits of swiping illegal card.
- Supports many kinds of cards including normal card, card for disable person, card in blacklist, patrol card, visitor card, duress card and super card, etc.
- Supports event linkage and card linkage functions.
- Supports connecting a card reader via RS-485 or Wiegand interface. For RS-485 interface, it has two interfaces and supports detection of loop power fault and redundant functions. For Wiegand interface, it supports W26 or W34 format to connect a third-party card reader.
- Supports many kinds of status indicators.
- Supports connecting many kinds of card readers including Mifare card reader, ID card reader, CPU card reader, and fingerprint card reader, etc.
- Supports getting status of distributed access controller via remotely operating master access controller in client, including online status, temper-proof status, power supply status, storage battery status and information of whether power storage is in low voltage status, etc.
- Supports offline record keeping and insufficient space alarm for storing records. When the controller is power off, the data can be saved forever.
- Supports backup storage batteries, watchdog and tamper-proof functions.
- Supports many kinds of working mode: online mode, offline mode (configuration mode, self-learning mode and not-support mode).

1.2 Appearance

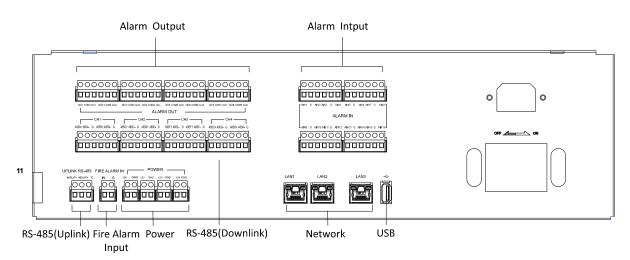
1.2.3 Front Panel and Indicators Description of Master Access Controller



Indicators	Description	Implication
Alarm Out	Display the status of	Off(Red): No alarm out
	alarm out	On(Red) : Alarm out
		Off : Distributed controller network connection exception
Uplink Network	Display the working status of uplink network (LAN1/LAN2)	On : Distributed controller network normally connected
		Flashing: Device has armed via the LAN port
		Off: Network connection exception
Downlink	Display the working	On : Network is normally connected
Network	status of downlink	Rapid Flashing : connected and master access controller can communicates with distributed access controller via LAN3
Run	Display the working status (RUN) and power status (POWER) of master access controller	Flashing: Device is normally working
Downlink	Display the working status of downlink serial	Off : No device in the loop or loop exception
Serial Port	loop (CH1/CH2/CH3/CH4)	On : The loop is normally working with device.
Uplink Serial Port	Display the communication status of uplink RS-485	Off : Distributed controller RS-485 Online On : Distributed controller RS-485 Offline

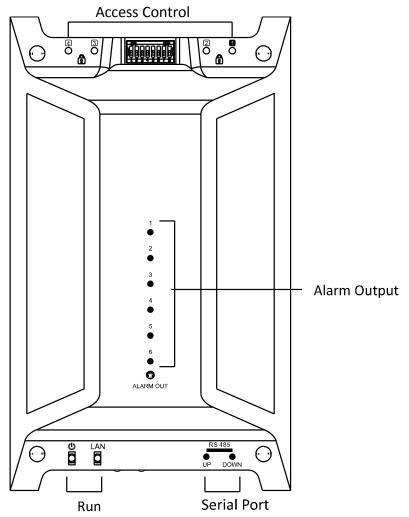
Table 1-1 Indicators Description of Master Access Controller

1.2.4 Rear Panel and Indicators Description of Master Access Controller

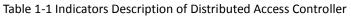


Master Access Controller User Manual

Terminal	Description			
Alarm Out	The connection terminal of alarm out.			
Alarm In	The connection terminal of alarm in.			
RS-485(Uplink)	Connect to the uplink client software (Reserved).			
Fire Alarm In	The alarm input terminal of short circuit attempts and open circuit attempts.			
RS-485 (Downlink)	Downlink RS-485 serial can be used to build a communication loop with distributed access controller.			
Network Interface	LAN1/LAN2 can be used to communicate with the client and LAN3 can be used to communicate with distributed access controller.			
USB	USB port can be used to import or export the data and upgrade the device.			

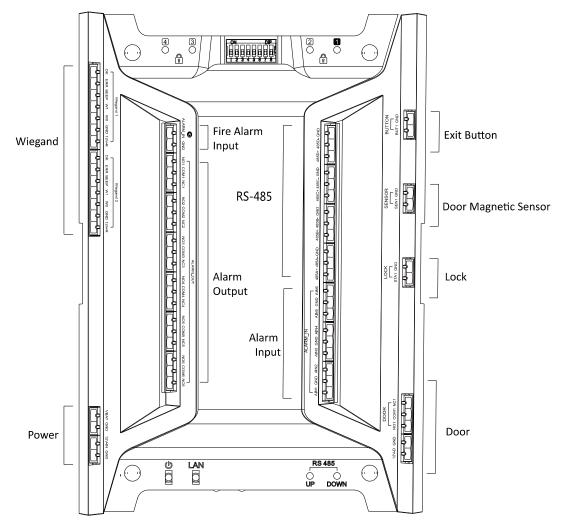


1.2.5 Appearance and Indicators Description of Distributed Access Controller



Indicators	Description		
Access Control	Status of access control.		
Alarm Output	Status of alarm out.		
	U: Status of distributed access controller		
Running Status	LAN: Status of communicating with master controller via LAN	On: Distributed controller and master controller are connected via LAN.Off: Distributed controller and master controller are not connected via LAN.	
Serial Port	UP: Status of communicating with master controller via RS-485	 On: Distributed controller and master controller are connected via RS-485. Off: Distributed controller and master controller are not connected via RS-485. 	
	DOWN: Status of loop On: Loop is connected.		
	connection	OFF: Loop is not connected.	

1.2.6 Connection Terminal of Distributed Access Controller



Connection Terminal of Single-Door Distributed Access Controller

Table 2-1 Description of Connection Terminal

Terminal	Single-Door Distributed Access Controller		
		ОК	Light Control Output (Valid Card)
		ERR	Light Control Output (Invalid Card)
Wiegand Reader 1 Wiegand		BZ	Buzzer Control Output
	-	W1	Wiegand Card Reader Input Data 1
		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
	Wiegand Reader 2	ОК	Light Control Output (Valid Card)
		ERR	Light Control Output (Invalid Card)

Terminal	Single-Door Distributed Access Controller		
		BZ	Buzzer Control Output
		W1	Wiegand Card Reader Input Data 1
		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
	Storage	VBAT	Storage Battery Power In
Dowor	Battery	GND	Grounding
Power	Dowor	12V-IN	Power In
	Power	GND	Grounding
Fire Alarm In	Fire Alarm	ALARM-IN	Fire Alarm In
Fire Alarm in	In	GND	Grounding
		NO1	
	Alarm Out 1	COM1	Relay 1 Alarm Out (Dry Contact)
	-	NC1	
	Alarm Out 2	NO2	
		COM2	Relay 2 Alarm Out (Dry Contact)
		NC2	
	Alarm Out 3	NO3	Relay 3 Alarm Out (Dry Contact)
		СОМ3	
Alerre Out		NC3	
Alarm Out	Alarm Out 4	NO4	Relay 4 Alarm Out (Dry Contact)
		COM4	
		NC4	
		NO5	
	Alarm Out 5	COM5	Relay 5 Alarm Out (Dry Contact)
		NC5	
	Alarm Out 6	NO6	Relay 6 Alarm Out (Dry Contact)
		COM6	
		NC6	

Terminal	Single-Door Distributed Access Controller		
	RS-485D (Uplink)	GND	Grounding
		485D-	Master Access Controller RS-485- Output
		485D+	Master Access Controller RS-485+ Output
		GND	Grounding
	RS-485C (Uplink)	485C-	Master Access Controller RS-485- Output
RS-485	(••••••••	485C+	Master Access Controller RS-485+ Output
		GND	Grounding
	RS-485B (Downlink)	485B-	Card Reader RS-485- Input
		485B+	Card Reader RS-485+ Input
		GND	Grounding
	RS-485A (Downlink)	485A-	Card Reader RS-485- Input
		485A+	Card Reader RS-485+ Input
	ALARM-IN	A6	Alarm In 6
		GND	Grounding
		A5	Alarm In 5
		A4	Alarm In 4
Alarm In		GND	Grounding
		A3	Alarm In 3
		A2	Alarm In 2
		GND	Grounding
		A1	Alarm In 1
Door Switch Input		GND	Grounding
	BUTTON	BUT1	Door Switch Input of Door 1
		GND	Grounding
Door Magnetic Input	SENSOR	SEN1	Door Magnetic Detection Input of Door 1

Terminal	Single-Door Distributed Access Controller		
	GND	Grounding	
Lock Input	LOCK	STA1	Lock Detection Input of Door 1
Relay Output DOOR	DOOR	NC1	Lock Relay Output of Door 1 (Dry Contact)
		COM1	
		NO1	
		GND	Grounding
	12V-D	DC12V Positive Pole Output	

Connection Terminal of Double-Door Distributed Access Controller

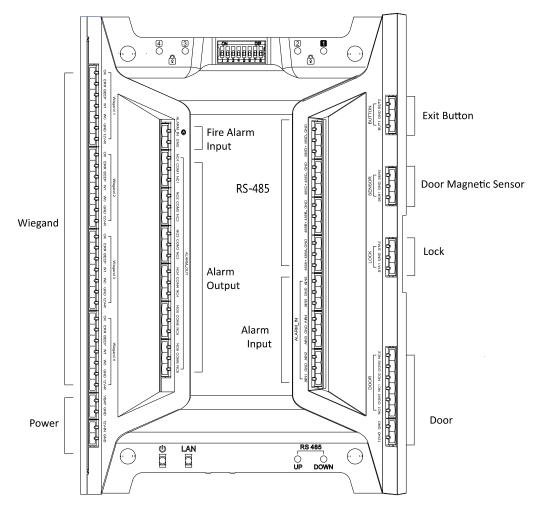


Table 2-2 Description of Connection Terminal

Terminal	Double-Door Distributed Access Controller		
Wiegand	Wiegand	ОК	Light Control Output (Valid Card)
	Reader 1	ERR	Light Control Output (Invalid Card)

Terminal	Double-Door Distributed Access Controller		
		BZ	Buzzer Control Output
		W1	Wiegand Card Reader Input Data 1
		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
		ОК	Light Control Output (Valid Card)
		ERR	Light Control Output (Invalid Card)
		BZ	Buzzer Control Output
	Wiegand Reader 2	W1	Wiegand Card Reader Input Data 1
		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
	Reader 2 Wiegand Reader 3	12V-R	Power Out
		ОК	Light Control Output (Valid Card)
		ERR	Light Control Output (Invalid Card)
		BZ	Buzzer Control Output
	-	W1	Wiegand Card Reader Input Data 1
	Neduer 5	W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
		ОК	Light Control Output (Valid Card)
		ERR	Light Control Output (Invalid Card)
		BZ	Buzzer Control Output
	Wiegand Reader 4	W1	Wiegand Card Reader Input Data 1
		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
	Storage Battery	VBAT	Storage Battery Power In
Power		GND	Grounding
	Power	12V-IN	Power In

Terminal	Double-Door Distributed Access Controller		
		GND	Grounding
Fire Alarm		ALARM-IN	Fire Alarm In
In	Fire Alarm In	GND	Grounding
		NO1	
	Alarm Out 1	COM1	Relay 1 Alarm Out (Dry Contact)
		NC1	
		NO2	
	Alarm Out 2	COM2	Relay 2 Alarm Out (Dry Contact)
		NC2	
		NO3	
	Alarm Out 3	СОМЗ	Relay 3 Alarm Out (Dry Contact)
		NC3	
Alarm Out	Alarm Out 4	NO4	
		COM4	Relay 4 Alarm Out (Dry Contact)
		NC4	
		NO5	
	Alarm Out 5	COM5	Relay 5 Alarm Out (Dry Contact)
		NC5	
		NO6	
	Alarm Out 6	COM6	Relay 6 Alarm Out (Dry Contact)
		NC6	
		GND	Grounding
	RS-485D (Uplink)	485D-	Master Access Controller RS-485- Output
	(0,0,)	485D+	Master Access Controller RS-485+ Output
		GND	Grounding
RS-485	RS-485C (Uplink)	485C-	Master Access Controller RS-485- Output
	<u> </u>	485C+	Master Access Controller RS-485+ Output
	RS-485B (Downlink)	GND	Grounding
		485B-	Card Reader RS-485- Input

Terminal	Double-Door Distributed Access Controller		
		485B+	Card Reader RS-485+ Input
		GND	Grounding
	RS-485A (Downlink)	485A-	Card Reader RS-485- Input
		485A+	Card Reader RS-485+ Input
		A6	Alarm In 6
		GND	Grounding
		A5	Alarm In 5
		A4	Alarm In 4
Alarm In	ALARM-IN	GND	Grounding
		A3	Alarm In 3
		A2	Alarm In 2
		GND	Grounding
		A1	Alarm In 1
Door	BUTTON	BUT2	Door Switch Input of Door 2
Switch		GND	Grounding
Input		BUT1	Door Switch Input of Door 1
Door		SEN2	Door Magnetic Detection Input of Door 2
Magnetic	SENSOR	GND	Grounding
Input		SEN1	Door Magnetic Detection Input of Door 1
		STA2	Lock Detection Input of Door 2
Lock Input	LOCK	GND	Grounding
		STA1	Lock Detection Input of Door 1
		NC2	
		COM2	Lock Relay Output of Door 2 (Dry Contact)
		NO2	
Relay Output	DOOR	NC1	
		COM1	Lock Relay Output of Door 1 (Dry Contact)
		NO1	
		GND	Grounding

Terminal	D	ouble-Door [Distributed Access Controller
		12V-D	DC12V Positive Pole Output

Connection Terminal of Four-Door Distributed Access Controller

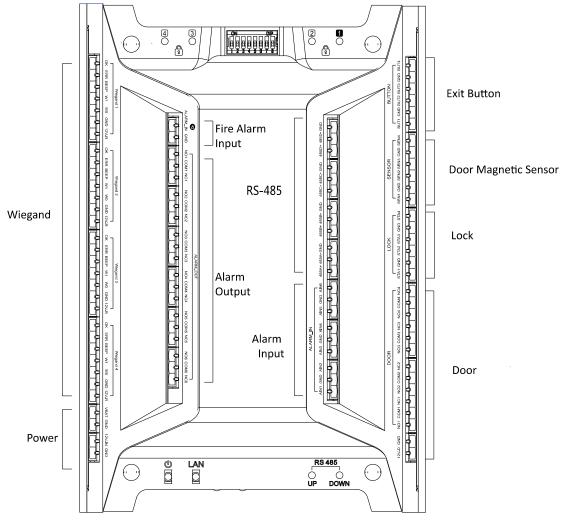


Table 2-3 Description of Connection Terminal

Terminal	Double-Door Distributed Access Controller		
	Wiegand Reader 1	ОК	Light Control Output (Valid Card)
		ERR	Light Control Output (Invalid Card)
		BZ	Buzzer Control Output
		W1	Wiegand Card Reader Input Data 1
Wiegand		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
	Wiegand	ОК	Light Control Output (Valid Card)

Terminal	Double-Door Distributed Access Controller		
	Reader 2	ERR	Light Control Output (Invalid Card)
		BZ	Buzzer Control Output
		W1	Wiegand Card Reader Input Data 1
		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
		ОК	Light Control Output (Valid Card)
		ERR	Light Control Output (Invalid Card)
		BZ	Buzzer Control Output
	Wiegand Reader 3	W1	Wiegand Card Reader Input Data 1
		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
		ОК	Light Control Output (Valid Card)
		ERR	Light Control Output (Invalid Card)
	Wiegand Reader 4	BZ	Buzzer Control Output
		W1	Wiegand Card Reader Input Data 1
		W0	Wiegand Card Reader Input Data 0
		GND	Grounding
		12V-R	Power Out
	Storage Dettery	VBAT	Storage Battery Power In
Devier	Storage Battery	GND	Grounding
Power	Devuer	12V-IN	Power In
	Power	GND	Grounding
Fire	Fire Alarm In	ALARM-IN	Fire Alarm In
Alarm In	Fire Alarm In	GND	Grounding
	Alarm Out 1	NO1	
Alarm Out		COM1	Relay 1 Alarm Out (Dry Contact)
		NC1	

Terminal	Double-Door Distributed Access Controller		
		NO2	
	Alarm Out 2	COM2	Relay 2 Alarm Out (Dry Contact)
		NC2	
		NO3	
	Alarm Out 3	COM3	Relay 3 Alarm Out (Dry Contact)
		NC3	
		NO4	
	Alarm Out 4	COM4	Relay 4 Alarm Out (Dry Contact)
		NC4	
		NO5	
	Alarm Out 5	COM5	Relay 5 Alarm Out (Dry Contact)
		NC5	
		NO6	
	Alarm Out 6	COM6	Relay 6 Alarm Out (Dry Contact)
		NC6	
		GND	Grounding
	RS-485D (Uplink)	485D-	Master Access Controller RS-485- Output
		485D+	Master Access Controller RS-485+ Output
		GND	Grounding
RS-485	RS-485C (Uplink)	485C-	Master Access Controller RS-485- Output
13-485		485C+	Master Access Controller RS-485+ Output
		GND	Grounding
	RS-485B (Downlink)	485B-	Card Reader RS-485- Input
		485B+	Card Reader RS-485+ Input
	RS-485A	GND	Grounding
	(Downlink)	485A-	Card Reader RS-485- Input

Terminal	Double-Door Distributed Access Controller		
		485A+	Card Reader RS-485+ Input
		A6	Alarm In 6
		GND	Grounding
		A5	Alarm In 5
		A4	Alarm In 4
Alarm In	ALARM-IN	GND	Grounding
		A3	Alarm In 3
		A2	Alarm In 2
		GND	Grounding
		A1	Alarm In 1
		BUT4	Door Switch Input of Door 4
		GND	Grounding
Door Switch	BUTTON	BUT3	Door Switch Input of Door 3
Input		BUT2	Door Switch Input of Door 2
		GND	Grounding
		BUT1	Door Switch Input of Door 1
	SENSOR	SEN4	Door Magnetic Detection Input of Door 4
		GND	Grounding
Door		SEN3	Door Magnetic Detection Input of Door 3
Magnetic Input		SEN2	Door Magnetic Detection Input of Door 2
		GND	Grounding
		SEN1	Door Magnetic Detection Input of Door 1
		STA4	Lock Detection Input of Door 4
Lock		GND	Grounding
Input	LOCK	STA3	Lock Detection Input of Door 3
		STA2	Lock Detection Input of Door 2

Terminal	Double-Door Distributed Access Controller		
		GND	Grounding
		STA1	Lock Detection Input of Door 1
		NC4	
		COM4	Lock Relay Output of Door 4 (Dry Contact)
		NO4	
		NC3	
	DOOR	СОМЗ	Lock Relay Output of Door 3 (Dry Contact)
		NO3	
Relay		NC2	
Output		COM2	Lock Relay Output of Door 2 (Dry Contact)
		NO2	
		NC1	
		COM1	Lock Relay Output of Door 1 (Dry Contact)
		NO1	,
		GND	Grounding
		12V-D	DC12V Positive Pole Output

- Please set the ID of RS-485 card readers as 1 to 8. The channel No. of door 1 are 1 (in) and 2 (out). The channel No. of door 2 are 3 (in) and 4 (out). The channel No. of door 3 are 5 (in) and 6 (out). The channel No. of door 4 are 7 (in) and 8 (out).
- For single-door distributed access controller, Wiegand card readers 1/2 correspond to the entering/existing card readers of channel No. 1 respectively.
- For double-door distributed access controller, Wiegand card readers 1/2 correspond to the entering/existing card readers of channel No. 1 respectively and Wiegand card readers 3/4 correspond to the entering/existing card readers of channel No. 2 respectively.
- For four-door distributed access controller, Wiegand card readers 1/2/3/4 correspond to the entering card readers of channel No. 1/2/3/4 respectively.

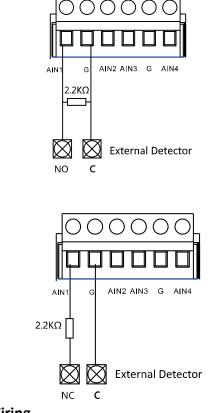
2 External Device Wiring

2.1 Master Access Controller External Device Wiring

2.1.1 Zone Alarm Input Wiring

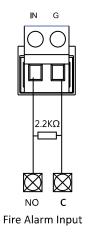
NO Detector Wiring

NC Detector Wiring

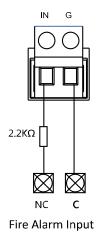


2.1.2 Fire Alarm Input Wiring

NO Alarm Input Wiring



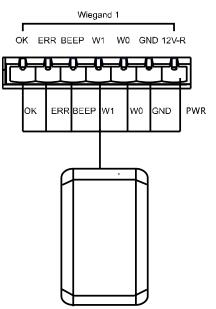
NC Alarm Input Wiring



2.2 Distributed Access Controller External Device Wiring

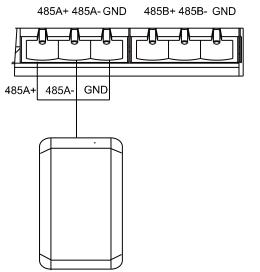
2.2.1 Card Reader Wiring

Wiegand Card Reader Wiring



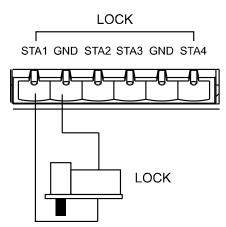
Note: You must connect the OK/ERR/BZ, if using access controller to control the LED and buzzer of the Wiegand card reader.

RS485 Card Reader Wiring

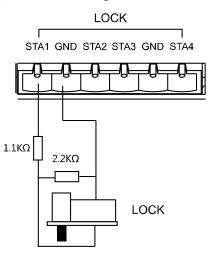


2.2.2 Lock Wiring

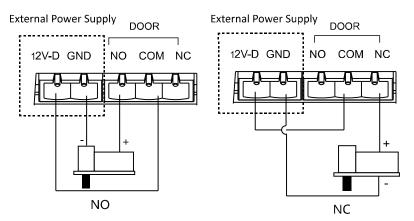
Lock Status Input Wiring



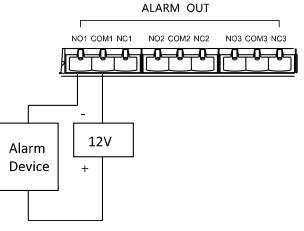
Short/Open Circuit Attempts Alarm Wiring



Lock Relay Output Wiring

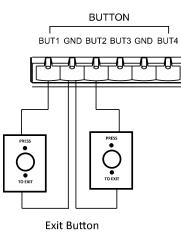


2.2.3 External Alarm Device Wiring

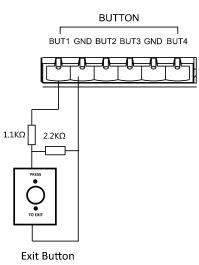


2.2.4 Exit Button Wiring

Exit Button Normal Wiring

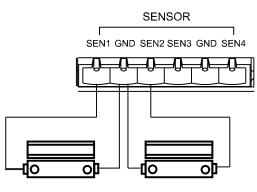


Short/Open Circuit Attempts Alarm Wiring



2.2.5 Door Magnetic Sensor Wiring

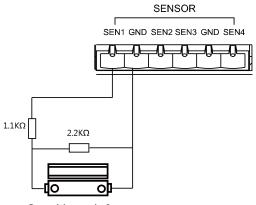
Door Magnetic Sensor Normal Wiring



Door Magnetic Sensor 1

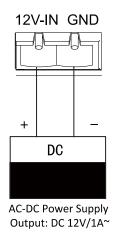
Door Magnetic Sensor 2

Short/Open Circuit Attempts Alarm Wiring



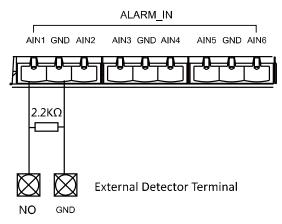
Door Magnetic Sensor

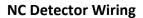
2.2.6 External Power Supply Wiring

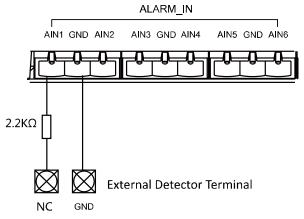


2.2.7 Zone Alarm Input Wiring

NO Detector Wiring

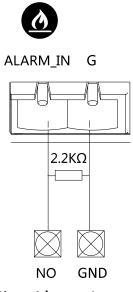






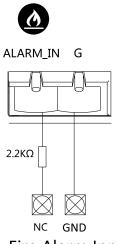
2.2.8 Fire Alarm Input Wiring

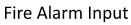
NO Fire Alarm Input Wiring



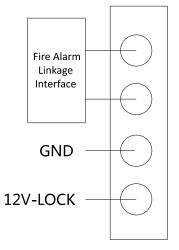
Fire Alarm Input

NC Fire Alarm Input Wiring





2.2.9 Fire Alarm Linkage Wiring

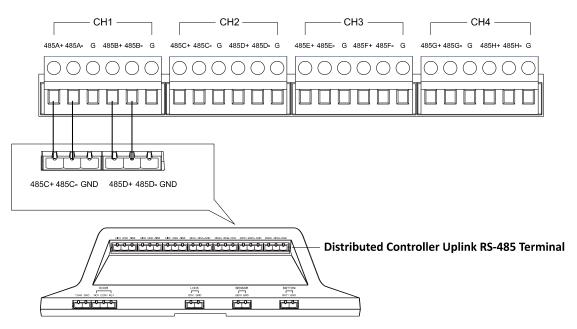


Fire Alarm Linkage Relay

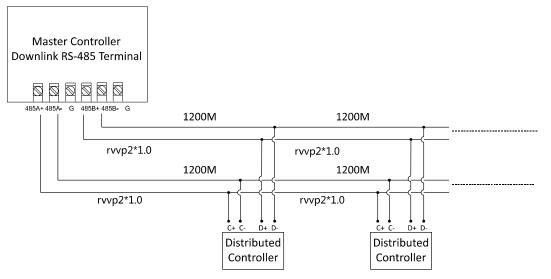
2.3 Master and Distributed Access Controller Wiring

The master access controller connects with the distributed access controller via RS-485. Connect the uplink RS-485C+C-/D+D- terminal of the distributed controller with the downlink RS-485 terminal of the master controller

Max. 64 distributed controllers can be connected to each master controller. For efficient authentication, it should be no more than 16 distributed controllers each loop.



RS-485 Loop 1 Demonstration



Note: It is recommended to use the rvvp2*1.0 cable for wiring. The distance between the master controller and the distributed controller should be less than 1200m.

3 Hardware Settings

3.1 Dial-up Settings

3.1.1 Distributed Access Controller Address Settings

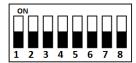
Master access controller can recognize the distributed access controller via dial-up address. The dial-up address can be set to 1 to 224.

The default IP address of distributed access controller is "192.0.0.64".

3.1.2 Dial-up Address Settings

From left to right, the dial-up shows the lowest bit to highest bit, which means 1 to 8.

When the black block is at ON, it means $1(\Box)$, or it means $0(\Box)$.



For example: the dial-up below shows a binary code: 0000 1100. Transform the binary code to decimal to get the dial-up address: Address = 12.

0	N						
	П					П	\square
1	2	3	4	5	6	7	8

Notes:

- The default downlink network interface IP address of master access controller is *192.0.0.254*.
- For uplink network communication, the device needs to be activated via SADP software or 4200 client.
- The distributed access controller has three types: single-door (legal address is 1 to 128), double-door (legal address is 129 to 192 and the dial-up 8 must be up) and four-door (legal address is 193 to 224 and dial-up 7 and 8 must be up). When those kinds of controllers are fully loaded, the total number of doors is 128, or the total number of distributed controller is 64. If the address is beyond the legal address range, adding device to the client will be failed.
- The order of doors.
 - For single-door access controller, the door number is one-to-one corresponding to the address of distributed access control.
 - For double-door access controller, the relationship is: Door Number = (Address of Distributed Access Controller-129)*2+Channel No. of the door.
 - For four-door access controller, the relationship is: Door Number = (Address of Distributed Access Controller-193)*4+Channel No. of the door.

Examples:

 Door 1 can be the single-door distributed access controller with address 1, channel No. 1 of double-door distributed access controller with address 129 or channel No.1 of four-door distributed access controller with address 193.

 Door 5 can be single-door distributed access controller with address 5, channel No.1 of double-door distributed access controller with address 131 or channel No.1 of four-door distributed access controller with address 194.

• The order of card readers.

The number of card readers corresponds to the address of distributed access controller.

3.2 Hardware Initialization Settings

The hardware initialization settings are only supported by the distributed access controller.

Steps:

1. Short connect the JP8 terminal.

2. Cut off the power and restart the device, the buzzer of controller begins continuous beeping.

- 3. After the buzzer stop beeping, disconnect JP8.
- 4. Cut off the power and restart again to finish the initialization.

Note: Hardware initialization will restore all the parameters to default and clear the device events.

4 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.

4.1 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.

SADP									0 <u> </u>
Total numb	er of online devices: 6						Export	Refresh	Activate the Device
ID	▲ Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.	
001		Active		8000	V1.4.0build 1609		80	201	
002		Active		8000	V1.4.2build 1608		80)160	
003		Active		8000	V1.4.0build 1609		80	20	
004		Active		8000	V5.4.0build 1602		80	15	The device is not activated.
005		Active		8000	V2.0.1build 1605		80	'4Pk	
✓ 006	DS-K	Inactive	192.0.0.64	8000	V1.0.0build 1608	0.0.00	80	160	
									You can modify the network parameters after
									the device activation.
									Activate Now
									New Password:
									Confirm Password:
									Activate
4									

3. Create a new password and confirm the password in the password field.

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

4. Click Activate to activate the device.

5. Check the activated device. You can change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

Modify Network	Parameters
Enable DHCP	
Device Serial No.:	
IP Address:	
Port:	8000
Subnet Mask:	
Gateway:	
IPv6 Address:	:
IPv6 Gateway:	::
IPv6 Prefix Length:	0
HTTP Port:	80
S	ecurity Verification
Admin Password:	
	Modify
	Forgot Password

6. Input the password and click the **Modify** button to save the settings.

4.2 Activation via Client Software

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

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

Steps:

- 1. Run the client software and the control panel of the software pops up, as shown in the figure below.
- 2. Click **Switch System**-> **Access Control System** on the menu bar to enter the Access Control System.

ch System	iVMS-420	0 Access Control System	admin 😯 📼 🛗	10:12:53 🔒 🗕
Control Panel				
Access Control				
Status Monitor Display access control status, access control function.	Access Control Ever Display access contro event, and card holde	Search access of		
Access Control Permission Config	uration			
Person Management The adding, deleting an editing of access control and door group.		card. Template The adding, dele editing of duratio plan and holiday	eting and Configur	Duration re the Door State ^{IS.}
Advanced Function Advanced Parameters, including anti-passing b multi-door interlocking.	ack, Interact Configuratio	L. The adding, dele	eting and Lonfigur access and cour	nce Management re attendance rule nt attendance result
Access Control Hardware Configu	ration	System Maintenance		
Controller Managemen The adding, deleting an editing of access control and card reader.	d The adding, deleting a	and Search configura	ation and Configur	Configuration re parameters for system and card ler.

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

to enter the Controller Management interface, as

shown in the figure below.

3.

Click

Add Device	Edit Delete	Bulk Time Adj	Status Re	mote Config	Refresh	Filter	
Name	Туре	Connection M	. IP	Port B	aud Rate Dial-up	Connection St.	Refresh
10.15.6.222	Access Controller_DS-K2700	TCP/IP	10.15.6.222	8000	1	Online	ŵ
10.15.6.248	Access Controller_DS-K2700	TCP/IP	10.15.6.248	8000	1	Online	ø
10.15.6.193	Access Controller_DS-K2700	TCP/IP	10.15.6.193	8000	1	Offline	٩
Online Devices (1)	😵 Refr	esh					
🗘 Add to Client	🗘 Add All Device	Network	Reset P 🥊 Activ	ate		Filter	
Name	Туре		IP	Port	Activated	Added	
44-19-b6-c5-c1-10	Access Contro	ler_DS-K2604-G	10.16.6.248	3 8000	Yes	No	

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

Online Devices (2)	🗞 Refresh					
수 Add to Client 수 /	Add All Device Edit Network	Reset P 🥊 Activate			Filter	
Name	Туре	IP	Port	Activated	Added	
44-19-b6-c5-c1-10	Access Controller		8000	Yes	No	
44-19-b6-ff-17-90	Access Controller	192.0.0.64	8000	No	No	

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

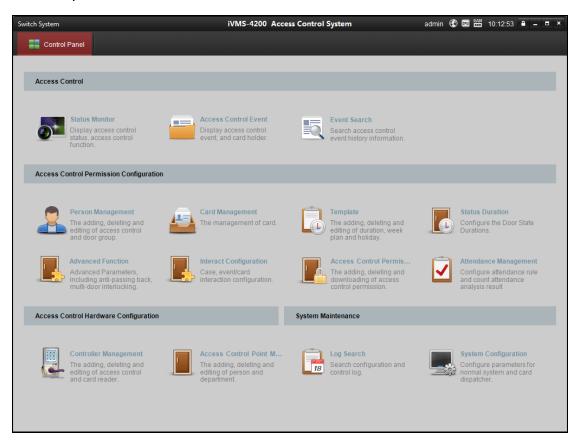
Password:	
	The password (8 to 16 characters) should contain two or more of the following character types: numeric, low.
Confirm Pas	

STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters and maximum of 16 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

- 7. Click ok to start activation.
- 8. Click the **Edit Network**... button to pop up the Network Parameter Modification interface.
- 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. Input the password to activate your IP address modification.

5 Overview of Access Control System

Click **Switch System**-> **Access Control System** on the menu bar to enter the Access Control System.



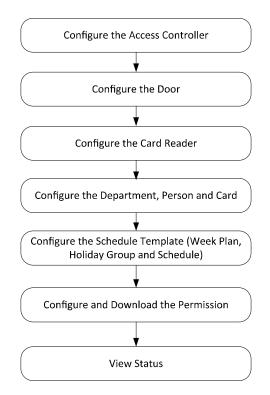
5.1 Description

The Access Control System is a client of configuring permission of door access. It provides multiple functionalities, including access controller management, person/card management, permission configuration, door status management, attendance management, event search, etc.

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

5.2 Configuration Flow

Refer to the following flow chart for the configuration order.



6 Device Management

6.1 Controller Management



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

icon to enter the controller management interface.

Device Managed (3)								
Add Device	Edit Delete	Bulk Time Adj	Status	Remote Config	Refresh	Filter		
Name	Туре	Connection M	IP	Port	Baud Rate Dial-up	Connection St.	Refresh	
10.15.6.222	Access Controller_DS-K2700	TCP/IP	10.15.6.222	8000	1	Online	ŵ	
10.15.6.248	Access Controller_DS-K2700	TCP/IP	10.15.6.248	8000	1	Online	&	
10.15.6.193	Access Controller_DS-K2700	TCP/IP	10.15.6.193	8000	1	Offline	<i>©</i>	
Online Devices (1)		resh						
Add to Client	Add All Device	t Network 🥎 I	Reset P 🌻 Ad	ctivate		Filter		
Name	Туре		IP	Port	Activated	Added		
44-19-b6-c5-c1-10	Access Contro	oller_DS-K2604-G	10.16.6.2	248 800	0 Yes	No		

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.

Note: The control client can manage up to 16 access controllers

6.1.1 Device Management

Adding Controller

Steps:

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

	add the access controller	×
Name:		
Туре:	Access Controller_DS-K2700	~
Connection	TCP/IP	~
Address:		
Port:	8000	
Baud Rate:		×
Dial-up:	1	
Account:		
User Name:		
Password:		
	Add	Cancel

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

6. Click the Add button to finish adding.

Notes:

- Up to 1 access control point and up to 2 card readers can be added to each access control terminal.
- •Add the access control point and the card reader to the DS-K2700 Access Controller after registering the DS-K27M01, DS-K27M02 or DS-K27M04 Distributed Access Controller.
- •Ehome is not supported.

Or you are able to select the detected online device in the Online Devices list and

click Add to Client. Input the device user name and the password to add the

device to the Device Managed list.

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, select a device and click Edit to edit the device information.

		Edit Access Controller		×
Time Settings Network Settings Lin	ked Captur			
3 10.15.6.222	Basic Information			
		[
	Name:	10.15.6.***		
	Connection Method:	TCP/IP	~	
	Address:	10.15.6.***		
	Port:	8000		
	Baud Rate:		~	
	Dial-up:	1		
	Account:			
	User Name:	admin		
	Password:	****		
				Save Cancel

- 2. Edit the basic parameters of the device on your demand, which are the same as the ones when adding the device.
- 3. Click Save to finish editing.

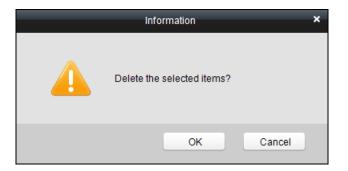
Or in the Online Devices list, select a device and click Lietwork	to edit the
device IP Address, Mask Address, Gateway Address, Port No. Input	the device
password and click ok to finish eliding.	

	Edit Network Parameters	×
Address:		
Address.		
Mask Address:		
Gateway Ad		
Port:		
Password:		
	OK Cancel	

Deleting Device

Steps:

- 1. In the Device Managed 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 Delete the selected device(s).
- 3. Click in the popup confirmation dialog to finish deleting.



Resetting Password

Steps:

- 1. In the Online Devices list, select an online device and click Seset P.....
- 2. Click Export in the pop-up window to export the device security code.
- 3. Send the security code to our technical supporters to get the encrypted security code of the device.
- 4. Click to import the encrypted security code.
- 5. Click \frown to finishing resetting.

	Reset Password	×
Export File:	Export	
Import File:	Import	
Password:]
	The password (8 to 16 characters) should contain two or more of the following character types: numeric, low	
Confirm Pas]
	OK Cancel	

Manually Registering Distributed Access Controller

Steps:

1. In the Device Managed list, double click an online device, or select an online

device and click Edit to enter the Edit Access Controller interface.

- 2. Right click a target access controller in the device list to open the right-click menu.
- 3. Click Add Distributed Access Controller.

		Edit Access Controller	×
Time Settings Network Settings	Linked Captur		
💽 🛃 Distributed Controlle Coll	and All apse All Distributed Access Controller Connection Method: Address: Port: Baud Rate: Dial-up: Account: User Name: Password:	10.15.6.193 TCP/IP 10.15.6.193 8000 1 1 admin	
			Save Cancel

- Select Manual Registration in the Add Distributed Access Controller window, and configure the distributed controller type, the DIP switch and the name.
 If you do not check Enable Network Communication, only configure the type, the DIP switch and the name to add the distributed controller.
- 5. Click Add and click in the pop-up window. The registered

distributed access controller will be displayed in the device list in the Edit Access Controller interface.

6. Click the Hardware Par... (Hardware Parameters Downloading) button to

download information to the device.

	Add Distributed Access Controller ×		
🖲 Manual Registr 🔘 Onlin	e Registra		
Туре:	DS-K27M01 ~]	
DIP Switch:		Enter the integer between 1	
Name:]	
Enable Network Commu			
IP:]	
Port No.:]	
Gateway Address:]	
Mask Address:]	
Offline Work Mode:	Do Not Support 🗸 🗸]	
		Add Cancel	

Registering Distributed Access Controller Online

Steps:

1. In the Registration of Distributed Access Controller window, click Refresh. The

software will search the online distributed access controller. The result will be displayed in the list, including the device No., name, IP address, gateway and subnet mask.

2. Select a distributed access controller and click Add Click OK in the

pop-up window. The distributed access controller will be registered to the access controller.

3. Click the Hardware Par... (Hardware Parameters Downloading) button to download information to the device.

	Add Distribute	ed Access Controller		×
🔵 Manual Registr 🧕 Online	e Registra			
		Searching (0%)	😵 Refresh	
Distributed Name	IP	Port	Gateway	Subnet
			Add	Cancel

Logout Distributed Access Controller

Steps:

- 1. In the Edit Access Controller interface, right click a target distributed assess controller in the device list to open the right-click menu.
- 2. Click Delete Distributed Access Controller.
- 3. Click in the pop-up window to confirm deleting. All related information

of the distributed access controller will be also deleted.

4. Click the Hardware Par... (Hardware Parameters Downloading) button to

download information to the device.

ware Par Reading Hard	Network Settings Linked Cap	tur			
10.15.6.193	Basic Information	Door_1	Door_2	Door_3	Door_4
Distributed Con Expand		Distributed Controlle	_193		
📲 Reader Out_ Delete	Distributed Access Controller	TCP/IP	~		
Teader In_3	Address:	10.15.6.251			
👕 Reader Out_4	Port:	8000			
Teader In_5	Baud Rate:				
Reader Out_6	Dial-up:	193			
Reader In_7 Reader Out_8	Account:				
Teader Out_8	Offline Mode	Do Not Support	`		
	Enable Network Com				
	Enable Network Corr	inunication			

Editing Distributed Access Controller (Door Information)

	Network Settings Linked Captur			
10.15.6.193	Basic Information Door	_1 Door_2	Door_3	Door_4
- 📶 Distributed Controller_193	Items	Options	Value	
Reader In_1 Reader Out_2	Door Magnetic	Remain Closed	~	
Reader In_3	Exit Button Type	Remain Open	¥	
Teader Out_4	Door Locked Time (s)		× 5	
Reader In_5 Reader Out_6	Door Open for Disabled Person		× 15	
Teader In_7	Door Open Timeout (s)		× 30	
Teader Out_8	Lock Door When Door Closed	Yes	¥	
	Duress Code		×	
	Super Password		×	
	Dismiss Code (Max. 8 digits)		×	
	Door Name		×	
	Remaining Open Door by First Card	No	*	
Firs	First Card Mode	Disable First Card Function	¥	
				Restore De

Steps:

- 1. In the editing interface, select a distributed access controller and click **Door_1/Door_2/...** to edit the information of the selected door.
 - 1) **Door Magnetic**: The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
 - 2) **Exit Button Type**: The Exit Button Type is in the status of **Remain Open** (excluding special conditions).
 - 3) Door Locked Time(s): After swiping the normal card and relay action, the

timer for locking the door starts working.

- 4) **Door Open for Disabled Person:** The door magnetic can be enabled with appropriate delay after disabled person swipes the card.
- 5) **Door Open Timeout(s)**: The alarm can be triggered if the door has not been close
- 6) Enable Lock Door when Door Close: This function has not been supported yet.
- 7) **Duress Code**: The door can open by inputting the duress code when there is a duress. At the same time, the access system can report the duress event.
- 8) **Super Password:** The specific person can open the door by inputting the super password.
- 9) **Dismiss Code (Max. 8 digits):** The alarm can be dismissed by entering the configured dismiss code.
- 10) **Door Name:** You are able to edit the door name.
- 11) Remaining Open Door by First Card: Select Yes or No.
- 12) First Card Mode: Select the first card mode, including Disable First Card Function, Remain Open by First Card Mode and First Card Authorization Mode.
- 13) **Remaining Open Duration Time (Minute):** Configure the remaining open duration for the first card.
- 14) **Connected to Distributed Controller:** Connect the door to the distributed access controller or not.
- 15) **Distributed Controller No.:** Configure the distributed access controller No.
- 16) **Distributed Controller Door No.:** Configure the distributed access controller door No.
- 17) **Distributed Controller Network Status:** Configure the distributed access controller status.
- 18) Lock Input Detection: Select enable or disable the function.
- 19) Lock Input Type: Select to remaining open or close the door.
- 20) **Door Control Terminal Work Mode:** Select Open/Short Circuit Attempts Alarm or Normal mode.
- 21) Exit Button: Select to enable or disable the exit button.
- 2. Click the Restore Default Value to restore all parameters into default settings.
- 3. Click the Save button to save parameters.
- 4. Click the Hardware Par... (Hardware Parameters Downloading) button to download information to the device.

Editing Distributed Access Controller (Card Reader Information)

		Edit Access Controller	×
Hardware Par Reading Hard	letwork Settings Linked Cap	tur	
- 🛃 10.15.6.193	Basic Information	Expansion Information	
 Distributed Controller_193 			
Teader In_1	Name:	Reader In_1	
Teader Out_2	Dial-up:	1	
Teader In_3	Account:		
Teader Out_4			
Teader In_5			
Teader Out_6			
Teader In_7			
Teader Out_8			
			Save Cancel

Steps:

- 1. In the device list, select a card reader name to enter into the card reader basic information editing interface.
- 2. Click Basic Information to edit the basic information about the card reader.
- 3. Click **Expansion Information** to edit the expansion information of the card reader.

	Edit Access Controller ×			
Hardware Par Reading Hard Network Settings Linked Captur				
- 🧕 10.15.6.193	Basic Information Expansion Info	rmation		
🖃 🚮 Distributed Controller_193	Items	Options	Value	
Reader In_1	Card Reader Type	~		
Reader In_3	Enable	Yes 🗸		
Reader Out_4	OK LED Polarity	Anode ~		
Reader Out_6	Error LED Polarity	Anode 🗸		
Reader In_7	Buzzer Polarity	Anode ~		
Readel Out_o	Intervals between Card Swiping	×	0	
	Interval (Seconds)	~	10	
	Attempts Limit of Card Reading Failure	No		
	Max. Attempts for Card Swiping Failure	~	5	
	Anti-Tamper Detection	No		
	Detection Time for Card Reader Offline	~	0	
	Mode Switch	Normal 🗸		
			Restore De	
			Save Cancel	

The Expansion Information includes:

- 1) **Card Reader Type:** You cannot select the card reader type. Viewing the card reader type is available.
- 2) Enable: Yes refers to card swiping is available on the card reader. No
- 3) OK LED Polarity: Select the polarity.

- 4) Error LED Polarity: Select the polarity.
- 5) Buzzer Polarity: Select the buzzer polarity.
- 6) Intervals between Card Swiping: It is invalid to swipe the same card again in the configured time duration. Available configured time duration is from 0 to 255s. (If set the time duration to 0, the function is not enabled.)
- 7) **Interval (Seconds):** The maximum interval between entering two characters of the password. After inputting a character, if you do not enter the next character in the configured interval, all characters will be cleared.
- 8) Attempts Limit of Card Reading Failure: If select "Yes", when the operation of card reading failed exceeds the configured attempts, the controller will generate an alarm event.
- 9) Max. Attempts for Card Swiping Failure: The maximum attempts for card swiping failed.
- 10) **Anti-Tamper Detection:** If select "Yes", when the card reader is tampered or removed, the controller will generate an alarm.
- 11) **Detection Time for Card Reader Offline:** If the card reader does not respond to the controller in the configured time duration, the card reader will be in the offline mode.
- 12) **Mode Switch:** Switch the card reader mode. Support the normal mode and the Card Enrollment mode.
- 4. Click the Save button to save parameters.
- 5. Click the Hardware Par... (Hardware Parameters Downloading) button to download information to the device.

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 Adj... button to start time synchronization.

A message box will pop up on the lower-right corner of the screen when the time synchronization is compeleted.

Status

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

	Device Sta	itus	_	×
Host Status	Status Item	Status		
Distributed Controller Status	Storage Battery Power Voltage	0V		
Distributed Controller Status	Whether power storage is in	Yes		
Door Status	Device Power Supply Status	Alternative Cu		
Card Reader Status	Multi-door Interlocking Status	Closed		
Alarm Input Status	Anti-passing Back Status	Closed		
Alaminiput Status	Host Anti-Tamper Status	Closed		
Alarm Output Status	Card Added	1		
Event Sensor Status				
			Refresh	Cancel

1) **Host Status**: The status of the host, including Storage Battery Power Voltage, Whether power storage is in low voltage status, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, Host Anti-Tamper Status and Card Added.

2) **Distributed Controller Status:** Display the distributed access controller status, including the distributed access controller No., offline status, tampering status, device power supply status, fire alarm, storage battery power voltage, Whether power storage is in low voltage status and Serial No.

3) **Door Status**: The status of the connected door. The door status includes Normal Status, Remain Closed and Remain Open.

Note: Normal Status refers to the default value. You are able to configure Remain Closed and Remain Open via the remote open settings and the schedule template setting.

- 4) Card Reader Status: The status of card reader.
- 5) Alarm Input Status: The alarm input status of each port.
- 6) Alarm Output Status: The alarm output status of each port.
- 7) Event Sensor Status: The event status of each port.

Remote Configuration

Purpose:

In this this interface, you can set the access control parameters, remotely reboot device, restore the device parameters, remotely update the access controller and the distributed access controller, remotely configure the alarm zone parameters, remotely configure alarm.

> Checking Device Information

Steps:

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

Editing Device Name

In the Remote Configuration interface, click System -> General to configure the

device name. Click Save to save the settings.

Configuring the General Parameters		
Device Information		
Device Name:	Access Controller	
	Save	

> Editing Time

Steps:

- 1. In the Remote Configuration interface, click **System** -> **Time** to configure the time zone.
- 2. (Optional) Check Enable NTP and configure the NTP server address, the NTP port,

and the synchronization interval.

- 3. (Optional) Check **Enable DST** and configure the DST star time, end time and the bias.
- 4. Click Save to save the settings.

Configuring the Time Settings (e.g., NTP, DST)				
Time Zone				
Select Time Zone:	: (GMT+08:00) Beijing, Hong Kong, Perth, Singa 👻			
Enable NTP				
Server Address:				
NTP Port:	123			
Sync Interval:	0	Minute(s)		
Enable DST				
Start Time:	January 🖌 First Week	Sun 🗸 0 👗 : 00		
End Time:	January 🖌 First Week	Sun 🗸 0 👗 : 00		
DST Bias:	~			
		Save		

System Maintainance Settings

Steps:

- 1. In the Remote Configuration interface, click **System** -> **System Maintenance**.
- 2. Click Reboot to reboot the device.

Or click Restore Default Settings to restore the device settings to the default ones,

excluding the IP address.

Or click Restore All to restore the device parameters to the default

ones. The device should be activated after restoring.

Or click Auto Search External Dev... to search the unlinked alarm output and alarm

input of the distributed access controller. The alarm input and output will be queued after the linked ones.

Or click Auto Register External D... to queue all alarm input and output of the

registered distributed access controller by ID. It will also delete the linked distributed access controller.

Note: You are able to check the queue in **Alarm** -> **Trigger**.

3. In the Remote Upgrade part, select a upgrade file type in the dropdown list. Click

to select the upgrade file. Click Upgrade to start upgrading.

4. You can configure the local controller in the Local Controller Management (Distributed Controller) part. Configure the controller No. Click

Reboot Local Controller or Restore Local Controller to reboot the local controller

(Distributed Controller) or restore the local controller (Distributed Controller) parameters.

System Mainter	nance	
System Manageme	ent	
	Reboot	
	Restore Default Settings	
	Restore All	
	Auto Search External Dev	
	Auto Register External D	
Remote Upgrade		
Controller 🗸		··· Upgrade
		··· Upgrade
Controller Y Progress:	anagement	··· Upgrade
Controller Y Progress:	anagement	Upgrade
Progress: Local Controller Ma	anagement Reboot Local Controller	Upgrade

> Managing User

Steps:

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

Adding, Ed	liting or Deleting	g the User			
🔂 Add	📝 Edit	📅 Delete			
User Name	Priority	IP Address	MAC Address	Password Security	
admin	Administrator	0.0.0	00:00:00:00:00:00	Risky	

2. Click Add to add the user (Do not Support).

to edit the user password, the IP address, the MAC address. Cilck	OK	to
confirm editing.		

User Parameter	-	Patter St.	
User Information			
User Type:	Administrator ~	User Name:	admin
Password:	•••••	Confirm Password:	•••••
IP Address:	0.0.0.0	MAC Address:	00:00:00:00:00:00
User Primission			
 Remote Operation: A Arm 	larm Disarming		Â
 Remote Log Search/S Remote Shutdown / 			
Remote Parameter Se	ettings		
Get Parameters			U
Restore Default Setting Remote Ungrade	igs		
Remote Upgrade			-
		C	Cancel

> Setting Security

Steps:

- 1. Click System -> Security.
- 2. Select the encryption mode in the dropdown list. You are able to select Compatible Mode or Encryption Mode.
- 3. (Optional) You can check **Enable SSH** or **Enable Illegal Login Lock** in the Software part.
- 4. Click Save to save the settings.

Configuring the Security Parameters	
Encryption Mode	
Level: Compatible Mode	
 Enable SSH Enable Illegal Login Lock 	Save

> Configuring Network Parameters

Click **Network** -> **General**. You can configure the network mode, NIC, the NIC type, the IPv4 address, the subnet mask (IPv4), the default gateway (IPv4), MTU, the device

port and the default route. Click	Save	to save the settings.	

Configuring the Networ	k Parameters	
Mode:	Multi-address 🗸	
NIC:	NIC 1	
NIC Type:	10M/100M/1000M Self 🗸	
IPv4 Address:	10.15.6.248	
Subnet Mask (IPv4):	255.255.255.0	
Default Gateway (IPv4):	10.15.6.254	
MAC Address:	44:19:b6:c1:c3:13	
MTU(Byte):	1500	
Device Port:	8000	
Default Route:	NIC 1 ~	
		Save

> Configuring Upload Method

Click **Network** -> **Uploading Method Configuration**. You can configure the cener group parameters. Select the center group in the dropdwon list. Check **Enable** and

enter Group Parameters								
Center Group:	Center Group1		~					
	Enable							
Uploading Method Confi	Main Channel		Backup Chan	n	Backup Chan	n	Backup Channel 3	
	Close	~	Close	~	Close	~	Close	~

configure the uploading method channel. Click Save to save the settings.

Configuring Advanced Network

Click **Network** -> **Advanced Settings**. You can configure the DNS1 IP address, the

DNS2 IP address, the alarm host IP and the alarm host port. Click	Save	to
save the settings.		

Configuring the Advanced Network Settings				
DNS1 IP Address:	0.0.0.0			
DNS2 IP Address:	0.0.0.0			
Alarm Host IP:	0.0.0.0			
Alarm Host Port:	0			
	Save			

> Configuring Alarm Zone Parameters

Steps:

1. In the Remote Configuration interface, click **Alarm** -> **Zone**. You can check the zone parameters.

Туре	Detector Type	Module Status	Module Ad	Module Ch	Module Type	Settings
our Voiced	Passive Infrared	Online	0	1	Local Zone	M
nt Zone	Passive Infrared	Online	0	2	Local Zone	2
nt Zone	Passive Infrared	Online	0	3	Local Zone	2
nt Zone	Passive Infrared	Online	0	4	Local Zone	2
nt Zone	Passive Infrared	Online	0	5	Local Zone	2
nt Zone	Passive Infrared	Online	0	6	Local Zone	2
nt Zone	Passive Infrared	Online	0	7	Local Zone	2
nt Zone	Passive Infrared	Online	0	8	Local Zone	2
nt Zone	Passive Infrared	Online	0	9	Local Zone	2
nt Zone	Passive Infrared	Online	0	10	Local Zone	2
nt Zone	Passive Infrared	Online	0	11	Local Zone	2
nt Zone	Passive Infrared	Online	0	12	Local Zone	2
nt Zone	Passive Infrared	Online	0	13	Local Zone	2
nt Zone	Passive Infrared	Online	0	14	Local Zone	2
nt Zone	Passive Infrared	Online	0	15	Local Zone	2
nt Zone	Passive Infrared	Online	0	16	Local Zone	2

- 2. Click the icon is to enter the Zone Settings window. You can configure the zone name the detector type, the zone type, and the sensitivity.
- 3. Click Save to save the settings.

Zone Settings	×
Zone No.:	2
Name:	
Detector Type:	Passive Infrared Dete 👻
Zone Type:	Instant Zone
Sensitivity:	10ms 🗸
Linked Trigger	
Select All	Â
Trigger 1	U
Trigger 2	
Trigger 3	
Trigger 4	
Trigger 5	
Trigger 6	
Trigger 7	-
	Save Cancel

> Configuring Trigger Parameters

Steps:

1. Click **Alarm** -> **Trigger**. You can check the trigger parameters.

						Refres
Name	Output Delay(s)	Module Status	Module Ad	Module Ch	Module Type	Settings
	0	Online	0	1	Local Trigger	2
	0	Online	0	2	Local Trigger	2
	0	Online	0	3	Local Trigger	2
	0	Online	0	4	Local Trigger	2
	0	Online	0	5	Local Trigger	2
	0	Online	0	6	Local Trigger	2
	0	Online	0	7	Local Trigger	2
	0	Online	0	8	Local Trigger	2
	0	Offline	1	1	Single Door Loc	2
	0	Offline	1	2	Single Door Loc	2
	0	Offline	1	3	Single Door Loc	2
	0	Offline	1	4	Single Door Loc	2
	0	Offline	1	5	Single Door Loc	2
	0	Offline	1	6	Single Door Loc	2
	0	Offline	2	1	Single Door Loc	2
	0	Offline	2	2	Single Door Loc	2
	0	Offline	2	3	Single Door Loc	2
	0	Offline	2	4	Single Door Loc	2
	0	Offline	2	5	Single Deer Les	17/2

Click the icon let to enter the Trigger Parameters Settings window. You can configure the trigger name.

3. Click Save to save the paramters.

Or click Copy to... to copy the trigger information to other triggers.

Trigger Parameters S	ettings
Trigger:	1
Name:	
Output Delay(s):	0
Copy to	Save Cancel

Configuring Access Control

In the Remote Configuration interface, click **Other** -> **Access Control Parameters**.

Check Whether to allow key input card number. Click	Save	to save the
settings.		

Configuring the Access Control	
Whether to allow key input card number	
	Save

> Uploading Background Picture

Click **Other** -> **Picture Upload**. Click 🔲 to select the picture from the local. You can

click Live View to preview the picture. Click Picture Upload to upload the picture.

			Picture	ckgroun	ding Ba	Uploa
					lame:	Picture
ture	Delete Pictu					
w	Live View	•••				
load	Picture Uplo					
le	Picture Upl					

> Operating Zone

Steps:

- 1. Click **Operation** -> **Zone**. You are able to check the zone status.
- 2. Check the zone and click Arm or Disarm to arm/disarm the zone.

Arm Disarm			
Zone No. Name	Status of Gua	ard Status of Alarm	ŕ
1	Disarm	Alarm	
2	Disarm	Normal	
3	Disarm	Normal	
4	Disarm	Normal	
5	Disarm	Normal	
6	Disarm	Normal	
7	Disarm	Normal	
8	Disarm	Normal	
9	Disarm	Normal	
10	Disarm	Normal	
11	Disarm	Normal	
12	Disarm	Normal	
13	Disarm	Normal	
14	Disarm	Normal	
15	Disarm	Normal	
16	Disarm	Normal	
17	Disarm	Normal	
18	Disarm	Normal	
19	Disarm	Normal	
20	Disarm	Normal	

> Operating Trigger

Steps:

- 1. Click **Operation** -> **Trigger**. You can check the trigger status.
- 2. Check the trigger and click Open or Close to open/close the trigger.

Trigger Operation		
Open Close		
Trigger No. Name	Status	
1	Close	
2	Close	
3	Close	
4	Close	
5	Close	
6	Close	
7	Close	
8	Close	
9	Close	
10	Close	
11	Close	
12	Close	
13	Close	
14	Close	
15	Close	
16	Close	
17	Close	
18	Close	
19	Close	
20	Close	

> Operating USB Device

Before you start:

Insert a USB device to the device.

Steps:

1. Click **Operation** -> **USB Device**.

USB Device Operation	
USB Device Status	Refresh
Connection Status: Disconnected	
Device Information:	
Configuration	
Import Export	
Card Parameters	
Import Export	
Attendance Data	
Export	

- 2. You can select the USB connection status in the dropdown list. The USB device information will be displayed in the Device Information box.
- 3. Click Import or Export to import/export the configuration, the card

paramters from/to the USB device.

Or click **Export** to export the attendance data.

Checking Status

Click **Status** -> **Alarm** or **Status** -> **Trigger** to check the zone status and the trigger status.

6.1.2 Network Settings

Purpose:

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

Uploading Mode Settings

	N	etwork Setting	gs	
Upload Mode Settings	Network C	enter Settings	Wireless Commu	inicati
Center Group:	Center Grou	ıp1	~	
	Enable			
Report Type:	Alarm Data		¥	
Upload Mode	Main Ch	Off	~	
	Backup	Off	~	

Steps:

1. In the access controller editing interface, click Network Settings button to enter the network settings interface.

Click Uploading Mode Settings.

- 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.

Note: 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 Setting	gs
Upload Mode Settings	Network Center Settings	Wireless Communicati
Network Center:	Center1	~
IP:		
Port:		
Protocol Type:	Private	~
Account Name:		
		OK

Steps:

- 1. In the access controller editing interface, click Network Settings button to enter the network settings interface.
- 2. Click Network Center Settings.
- 3. Select the network center in the dropdown list.
- 4. Input IP address.
- 5. Input port number.
- Select the protocol type: Private, NAL2300.
 Note: Ehome is not supported.
- 7. Set an account name for the network center. A consistent account should be used in one platform.
- 8. Click the **OK** button to save parameters.

Wireless Communication Center Setting

Steps:

- 1. In the access controller editing interface, click Network Settings button to enter the network settings interface.
- 2. Click **Wireless Communication Center Setting** to configure the report uploading type.
- 3. Configure the APN name, the SIM card center, the IP address, the port, the protocol type and the account name.

Note: The protocol type of DS-K2700 Access Controller, DS-K27M01, DS-K27M02 or DS-K27M04 Distributed Access Controller does not support ehome.

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

Jpload Mode Settings	Network Center Settings	Wireless Communicati
APN Name:	CMNET	~
SIM Card No.:		
Network Center:	Center1	~
IP:		
Port:		
Protocol Type:	Private	~
Account Name:		

6.1.3 Linked Capture Settings (Do Not Support)

Purpose:

Configure the size and the quality of the linked capture picture, the linked capture times, and the capture interval.

Steps:

- 1. In the Edit Access Controller interface, click the button Linked Captur....
- 2. In the pop-up window, configure the capture times and the interval.
- 3. Click the **OK** button to save the parameters.

	Linked Capture Settings	×
Capture Times	1 ~]
Capture Interv		ms
		确定

Note: Getting the linked capturing parameters from the device is available.

6.2 Access Control Point Management



icon on the control panel to enter the door

management interface.

Click the

Add Group 🛛 Delete Gro				
Search 9	Constant Edit	Delete		Filter
	Name	Belong to Controller	Door Camera	Position

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.

6.2.1 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.

Note: 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 <a>Delete Group button.
- Right-click a group and select Delete in the popup menu.
- Move the mouse onto the group and click ³² icon of it.
- And then click the OK button in the popup window.

6.2.2 Access Control Point Management

Purpose:

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

Importing Access Control Point

Steps:

1. Click the <u>mport</u> button to pop up the access control point importing interface.

Select a 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.

Notes:

• You can click 🔄 button on the upper-right corner of the window to create a new

group.

• Up to 64 access control points can be added.

Editing Access Control Point

Steps:

- Click to select a 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.
- 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 ^{SSI} button to delete all access control points under the group.

Note: you can also edit/delete a door on the Import Access Control Point panel.

Import Access Contro	l Point		×
Access Control Point		Group	÷
Search		Search	9
3 10.7.52.106		🗕 🗐 test	/ ×
		10.7.52.106_Door1	
	Import		
	Import All		

Steps:

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

point.

7 Permission Management

7.1 Person Management



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	C Add Person Edit Delete Filter				
🕑 🌲 Default	Person Name	Gender	ID Type	ID No.	Contact Phone No.	

7.1.1 Department Management

Steps:

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

	Add Department	×
Upper Depart	Default	
Department Na		
	OK Cancel	

Notes:

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

upper-level deparment 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 Depa... button to delete it.

Notes:

- 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.

7.1.2 Person Management

Notes:

- In the person management interface, double-click the person name or click the **Edit** button to edit the person informationt
- In the person management interface, click the **Delete** button to delete the person.
- Up to 2000 persons ban be added.

• Inputting General Information

Steps:

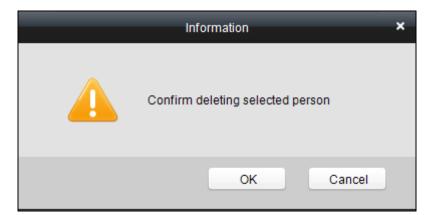
1. Select a department in the list and click the Add Person in the person infoarmation list to pop up the adding person interface.

	Person Information	
General	Fingerprint	
Person No.:	1609221102593185220	
Person Name:		
Gender:	Male O Female	25
ID Type:	ID ~	
ID No.:		Upload Picture
Belong to Dep	Department_1	
Contact No.:		
Contact Address:		
		Save Cancel

2. 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:

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

	Person Information	×
General	Fingerprint	
	Start Re X Delete Fi	Delete All
		Save Cancel

- 2. Click the **Start Register** button, and select the fingerprint to be input. . For details about inputting fingerprint, see *Chapter 11 Appendix: Tips for Scanning Fingerprint*.
- 3. Click the Save button to save the parameter.

Notes:

- Click the **Delete Fingerprint** button to delete the fingerprint.
- Click the **Delete All** button to clear all fingerprints input.
- Editing Person Information

Steps:

- 1. In the Person List in the Person Management interface, select a person.
- 2. Click to enter the Person Information interface.
- 3. Edit the parameters.

If possible, click Fingerprint to enter the fingerprints.

4. Click Save to save the parameters.

7.2 Card Management



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		
0001			Empty Card		
0002			Empty Card		
0003			Empty Card		U
0004			Empty Card		
0005			Empty Card		

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

Empty 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.

7.2.1 Empty Card

• Adding Card

Before you start:

Make sure a card dispenser is connected to the PC and is configured already. Refer to Section *10.2.4 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 🤍 to 🖲 and input 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 🔍 to 🖲 and

input the activation date, expiry date, start card No. and last card No. in the corresponding text fields.

Note: The start card No. and the last card No. should be the with 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 empty card in the list and click Issue Card button to issue the card with a person.

Note: you can double click the empty card in the card list to enter the **Issue Card** Page.

	ls	sue Card		×
Card No.:	001			
Please choos	e responding person for card:			
Search				P
🖃 🚑 Defa	ult			
💄 Le	la			
Please choos	e responding fingerprint for card	l:		
Tip: Pleas	e collect fingerprint data on dev	ice.		
- np. r rous			01	Orașel
			ОК	Cancel

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

Notes:

- The issued card will disappear from the Empty Card list, you can check the card information in the Normal Card list.
- Up to 2000 cards can be added.
- Each card can link up to 10 fingerprints.
- Deleting Card

You can click an added empty card in the list and click Delete button to delete

the selected card.

7.2.2 Normal Card

Purpose:

Click the Normal Card tab in the card managemet 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 Re	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 Card Change button to change the associated card

for card holder. Select another card in the popup window to replace the current card. The old card will turn to the empty card. You should configure the permission to the card again.

• Click to select an issued card and click Return Card to cancel the assotiation of

the card, then the card will disappear from the Normal Card list, which you can find it in the Empty Card list. You should configure the permission to the card again.

- Click to select an issued card and click Report Card L... (Report Card Loss) to set the card as the Lost Card, that is, an invalid card.
- Click to select an issued card and click Password Sett... (Password Settings) 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	

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

7.2.3 Lost Card

Click the Card Reported Loss tab in the card managemet 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											
Card No.	Status	Replace card?	Card Holder Name	Department							
123	Card Reported Lo	oss No	Lela	Default							

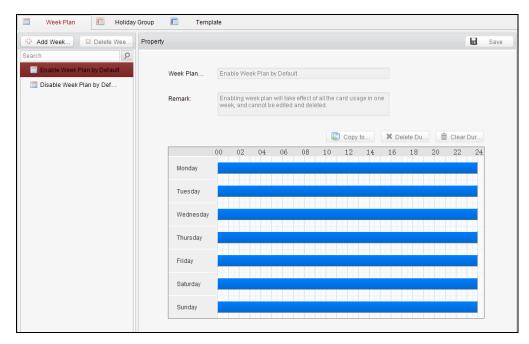
- Click the Cancel Card Loss button to resume the card to the normal card. You should configure the permission to the card again.
- Click the Card Replacement button to issue a new card to the card holder replacing for the lost card. Select another card in the popup window as the new card and the predefined permissions of the lost card will be copied to the new one automatically.

7.3 Schedule Template



on the control panel of the software to enter the schedule

template interface.



There are 3 settings in this interface: Week Plan, Holiday Group, and Template. **7.3.1 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							
	ОК	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 cofigured 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.

Note: Up to 8 time periods can be added in one day.

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.

7.3.2 Setting Holiday Group

• Adding Holiday Group

Steps:

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

Add Holiday Group							
Holiday Group							
	OK Cancel						

- 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.

*Note:*At most 16 holiday periods can be added.

Holiday	list			🗘 Add holiday	Previous	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	× 🖻 ×
2	2014-10-30 🛅	2014-11-01 🐯	00 02 04	06 08 10 12 14	16 18 20 22 24	× 🖞
3	2014-11-05 🛅	2014-11-08 🐯	00 02 04	06 08 10 12 14	16 18 20 22 24	× 🖞
4	2014-11-10 🛅	2014-11-12 🐯	00 02 04	06 08 10 12 14	16 18 20 22 24	× 🖞

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

Note: The holidays cannot be overlapped with each other.

7.3.3 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.

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

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

	Add Template	×
Template Name:		
	OK Cancel	

- 2. Input the name of schedule in the text filed and click the button to add the schedule.
- 3. Select a week plan you want to apply to the schedule.

Click the Week Plan tab and select a plan in the dropdown list.

🔲 Week Plan 🔳 Holiday Group	E Template
Add Template 🛛 Delete Tem Propert	y Save
Search P	
E Default Enable Schedule T	Template Name: Template_1
E DefaultDisable 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
	Friday
	Saturday
	Sunday

Select holiday groups you want to apply to the schedule.
 Note: At most 4 holiday groups can be added.

oliday Group to be Selecte	d		The selected	holiday group	
Search	9		Serial No.	Holiday Group Na	Remark
Holiday_1			1	Holiday_1	
	¢	Add			
	×	Delete			
		Clear			

- Click to select a holiday group in the left-side list and click the Add to add it.
- Click to select an added holiday group in the right-side list and click the

× Delete to delete the it.

- Click the Clear to delete all the added holiday groups.
- 5. Click the Save button to save the settings.

Note: Up to 4 schedule templates can be added.

7.4 Door Status Management

Purpose:

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



icon on the control panel to enter the interface.

sh 9													
10.7.52.106_Door1	Remain Open	Remain C	losed				C	opy to w	/hole w		Celete Celete	dur	Î (
	00 Monday	02	04	06	08	10	12	14	16	18	20	22	24
	Tuesday												
	Wednesday												
	Thur sday												
	Friday												
	Satur day												
	Sunday												

Steps:

- 1. Enter the Door Status Management page.
- 2. Click and select a door from the door list on the left side of the page.
- 3. Draw a schedule map.
 - 1) Select a door status brush <u>Remain Open</u> / 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.



Remain Open	Ren	nain Closed		Co	py to Wh	ole	× (Delete Di	I []	🛱 Clea
	00 02	04 06	08 1) 12	14	16	18	20	22	24
Monday										
Tuesday										
Wednesday										
Thursday										
Friday										
Saturday										
Sunday										

Notes

- The min. segment of the schedule is 30min.
- 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.
- 3. 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 ***** Delete dur... to delete the time period.

• Clear All Durations:

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

- 4. Click on save the settings.
- 5. You can copy the schedule to other doors by clicking on Copy To and select the required doors.

	(Copy to	_	×
1	Please select the access co	ntrol point to copy.		
	Search		9	
	🗕 🗖 📳 Test			
		ок	Cancel	
			Calicer	

6. Click on 🖄 Access Control... to enter the Download Door State page.

Acces	s Control Status	Downloadir	ıg
Please choose acc	ess control point	to downloa	d duration.
Search			9
🖃 🔲 🗐 All Grou	ps		
		ок	Cancel

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

7.5 Interact Configuration

	Interact Configuration
Click	Case, event/card interaction configuration
Click	

on the control panel of the software to enter the interact

configuration interface.

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

7.5.1 Event Card Interact

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

Note: Do not support the Case Trigger function.

• 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 tab to enter the event card interface.
- 2. Select the host to be set from the host list.
- 3. Click Add to start setting the event linkage.

Case Trigger	Event Card Interact	Client In	teract									
Host List 😃	Apply Ev	ent card linkage	detailed informatio	n				🗘 Add		🔀 Delete	E Sa	ave
Search	۶ (Event Li	vent device 👻 I	Device Tampe	ring Al	~	Card	Li				
10.15.6.222	E	vent Source										
10.15.6.248		Device										
- 10.15.6.193		Serial No. Device								1		
		1	10.15.6.193									
		2	Distributed Co									
		nkage target	lot Trigger 🛛 👻				Snapshot No	t Trigger	~			
	C	ard reader b					Alarm out					
		Name	Device	Card reader	b	÷	Name	Enable		Close		•
		Reader In_1	Distributed Co	Not Trigger	~	U	Alarm Output_1	Not Trigger	~	Not Trigger	~	
	1	Reader Out_2	Distributed Co	Not Trigger	*		Alarm Output_2	Not Trigger	*	Not Trigger	~	
		Reader In_3	Distributed Co	Not Trigger	~		Alarm Output_3	Not Trigger	~	Not Trigger	*	
	C	oor					Zone					
		Name	Device	Open	Clo	ose 📩	Name	Arm		Disarm	I	•
		Distributed Co	Distributed Co	Not Trigger	~ Not	t Tr	Alarm In_1	Not Trigger	~	Not Trigger	~	0
		Distributed Co	Distributed Co	Not Trigger	~ Not	t Tr	Alarm In_2	Not Trigger	~	Not Trigger	~	
1		Distributed Co	Distributed Co			1 T.	Alarm In 2	Matting		Net Trianes		

- 4. Click the radio button of the event linkage, and select the event type from the dropdown list.
- 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: Select Trigger in the dropdown list. The connected device real-time capture will be triggered.

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

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

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

Zone: The zone status of arm or disarm.

- 6. Click **Save** to save parameters.
- 7. Click Apply to apply the updated parameters to the local memory of

the device.

Notes:

- The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- The normal access controller can configure up to 50 event linkages and card linkages. The device of DS-K2700 can configure up to 500 event linkages and card linkages.

• 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 tab to enter the event card interact interface.
- 2. Select the host to be set from the host list.
- 3. Click Add to start setting the event linkage.

Host List 🖄 Apply	Event card linkage detailed information	🕂 Add 🛛 🖾 Delete 🗖 Save
Search S	C Event Li Event device V Device Tampering Al V	Card Li
10.15.6.222	Card Source	
10.15.6.193	Card Reader	
	Serial No. Device Name	·
	1 Distributed Co Reader In_1	U
	2 Distributed Co Reader Out_2	
	3 Distributed Co Reader In_3	
	Linkage target	
	Linkage target Controller Not Trigger Snapshot Card reader b Alarm out	
	Controller Not Trigger Snapshot	
	Controller Not Trigger Snapshot Card reader b Alarm out	Enable Close
	Controller Not Trigger Snapshot Card reader b Name Device Card reader b Name Name	Enable Close
	Controller Not Trigger Snapshot Card reader b Name Device Card reader b Name Reader In_1 Distributed Co Not Trigger Alarm Out	Enable Close tput_1 Not Trigger × Not Trigger × Not Trigger Vot Trigger × Not Trigger
	Controller Not Trigger Snapshot Card reader b Name Device Card reader b Name Reader In_1 Distributed Co Not Trigger Alarm Out Alarm Out Alarm Out Alarm Out	Enable Close tput_1 Not Trigger Vot Trigger Vot Trigger Vot Trigger Vot Trigger
	Controller Not Trigger Snapshot Card reader b Name Device Card reader b Name Reader In_1 Distributed Co Not Trigger Alarm Out Reader Out_2 Distributed Co Not Trigger Alarm Out Alarm Out Alarm Out Alarm Out	Enable Close tput_1 Not Trigger Vot Trigger Vot Trigger v Not Trigger v Not Trigger v Not Trigger
	Controller Not Trigger Snapshot Card reader b Alarm out Name Device Card reader b Reader In_1 Distributed Co Not Trigger Reader Out_2 Distributed Co Not Trigger Reader In_3 Distributed Co Not Trigger Door Zone	Enable Close tput_1 Not Trigger V Not Trigger V tput_2 Not Trigger V Not Trigger V tput_3 Not Trigger V Not Trigger V Arm Disarm

- 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.
- 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: Select Trigger in the dropdown list. The connected device real-time capture will be triggered.

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

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

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

Zone: The zone status of arm or disarm.

- 7. Click the save button to save parameters.
- 8. Click Apply to apply the updated parameters to the local memory of

the device.

Notes:

- The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- The normal access controller can configure up to 50 event linkages and card linkages. The device of DS-K2700, can configure up to 500 event linkages and card linkages.

7.5.2 Client Interact

Purpose:

The alarm event will be sent to the client software to trigger other devices operation. *Steps:*

1. Click **Client Interact** to enter the Client Interact tab.

- 2. Click Add
- 3. Select an event linkage main type and the corresponding minor type in the dropdown list.

- Select a host in the Host List dropdown list.
 If you do not select the alarm input event, in the main type dropdown list, you should check an alarm input.
- 5. Configure the Linkage Target parameters. You are able to link the event to the alarm output and the door status. Select Trigger in the Property dropdown list to link the alarm output to the event.

Or click Card Linkage, input the card No., check a card reader and the configure the linkage target.

 Click Save to save the parameters. The saved event will be displayed in the linkage event list.

Or select an event in the Linkage event list and click Delete to delete the event.

7.6 Access Permission Configuration

Access Control Permis



icon on the control panel to enter the interface.

Add Perm Delete Permis	. Start Downloading			
Major Type: By Staff	 Minor Type: 	Access Control Point 👻 Keyword:	Search	Reset
ame	Department	Access Control Point	Template	

7.6.3 Access Permission Settings

Purpose:

You can allocate permission for people/department to enter/exist the control points (doors) and the offline permission of the distributed access controller in this section.

Normal Permission Settings

Steps:

- 1. Enter the Access Control Permission page.
- 2. Click Normal Permission to enter the Normal Permission tab.
- 3. Click Add Permi... (Add Permission) on the upper-left side of the page to enter

the Add Permission window.

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

- 4. Select an adding type in the **Select Type** interface.
 - **By Person:** you can select people from the list to enter/exit the door. The following steps will take By Person as an example.
 - 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.
- 5. Click Next to enter the Permission Settings interface.

	New Access Co	ontrol Permission	×
① Choose Type	Template: Default Enable :	Schedule Template Y	
Permission Settings	Please choose person.	Please choose the access control poir	nt and the
	Search	Search	9
	🖃 🖬 Default	Access Control Point Door O	Group
	🗆 🚨 Lela	- 🗖 Test	
	🗆 💄 Shannar	🗇 📕 Test_Door1	
	🗆 💄 Steve		
		Previous Done	Cancel

Master Access Controller User Manual

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

Template: Default Enable Schedule Template 🗸

Note: The schedule template must be configured before any permission settings. Refer to *Section 7.3 Schedule Template* for detailed configuration guide.

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



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

- 8. Click the **Done** button to complete the permission adding.
- 9. Click Start Downloading to enter the **Download Permission** page.

Download Permission	י א
Download Met 💿 Download All	
Please choose controller to download.:	
Search	9
🖃 🗖 🚮 All Devices	
🗆 🛃 10.7.52.106	
ОК	Cancel

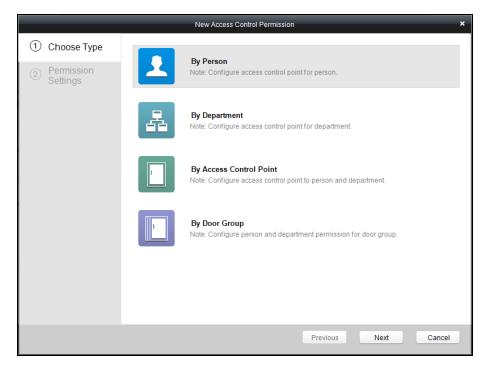
10. Select the control point and click the **OK** button, to enter the download result interface, to download the permission to the device.

	Download Resu	ilt	×
Permission Download P	Downloaded (100	0%)	
Filter			
Device	Progress	sult Remark	
123	100% All	Succee	
			Close

Offline Permission of Distributed Controller Settings

Steps:

- 1. Enter the Access Control Permission page.
- 2. Click Offline Permission of Distributed Controller to enter the Offline Permission of Distributed Controller tab.
- 3. Click Add Permi... (Add Permission) on the upper-left side of the page to enter the Add Permission window.



- 4. Select an adding type in the **Select Type** interface.
 - **By Person:** you can select people from the list to enter/exit the door. The following steps will take By Person as an example.
 - 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.
- 5. Click Next to enter the Permission Settings interface.

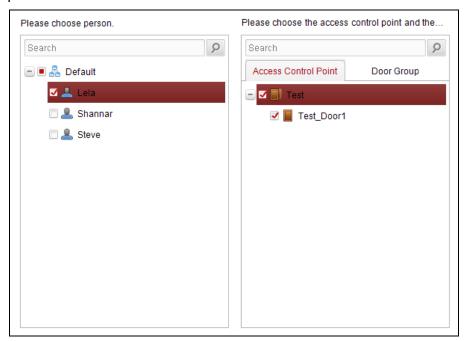
	New Access Control Permiss	sion ×
① Choose Type	Template: Default Enable Schedule Tem	nplate Y
Permission Settings	Please choose person.	Please choose the access control point and the
	Search	Search Access Control Point Door Group
		Previous Done Cancel

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

```
Template: Default Enable Schedule Template 🗸
```

Note: The schedule template must be configured before any permission settings. Refer to *Section 7.3 Schedule Template* for detailed configuration guide.

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



Note: The lower-level of department will also be selected if the highest-level of department is selected.

- 8. Click the **Done** button to complete the permission adding.
- 9. Click Start Downloading to enter the **Download Permission** page.

	Download Permission		×
Downloading	Oownload All		
Please choose co	ontroller to download.		
Search		9	
🖃 🗖 🚮 All De	vices		
🗆 🚮 10.	15.6.222		
- 🗆 📶 10.	15.6.248		
- M			
E 🛃 (
- 🗆 📶 10.			
	Distributed Controller_193		
	ок	Cancel	

10. Select the distributed controller and click the **OK** button, to enter the download result interface, to download the permission to the device.

	Download Result	
Permission Download P	Downloaded (100%)	
Filter		
Device	Progress Result Remark	
123	100% All Succee	
		Close
		0.038

7.6.4 Access Permission Searching

Purpose:

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

Steps:

1. In the Access Control Permission page, select the Normal Permission tab or the Offline Permission of Distributed Controller tab.

Normal Permission Offline Permission o				
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	

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

🗘 Add Perm	Delete Permis	Start Downloa	ding				
Major Type:	By Staff	✓ Minor T	ype: Access Control P	Point Y	Keyword:	Search	Reset

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

Add Perm Delete Permis	Start Downloading		
Major Type: By Staff	 Minor Type: 	Access Control Point 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: You can click **Reset** on the search criteria panel to clear all the displayed search results.

7.6.5 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.

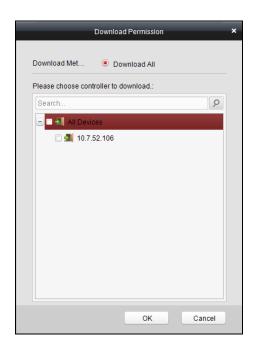
Major Type:	By Staff	Y Minor Type:	Access Control Point 👻 Keyword:	Search Reset
Name		Department	Access Control Point	Template
Lela		Default	Test_Door1	Default Enable Schedule Template

Note: you can press the Ctrl or Shift key on the keyboard,

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



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



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

7.7 Advanced Functions

Purpose:

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

ick the	rameters, -passing back,	e control p	banel to ent	ter the	interface.
Access Control Type Card Reader Aute	Multiple Authentic First Card	Anti-passing Back	Multi-door Interloc	White List	Password Authenti
Controller G 🛃 Apply	Card List				
Search	Add Delete			Filter	
- 10.15.6.222	Card No. Status	Activation Date:	Expiry Date:		
Card for Disabled Person					
Card in Blacklist					
Patrol Card					
Duress Card					
🔄 Super Card					
Visitor Card					
- 🗐 10.15.6.248					
🔯 Normal Card					
Card for Disabled Person					
🔄 Card in Blacklist					
Patrol Card					
Duress Card					
🔄 Super Card					
🔄 Visitor Card					
- 🗐 10.15.6.193					
🔄 Normal Card					
📰 Card for Disabled Person					
🔄 Card in Blacklist					

7.7.6 Access Control Type

Purpose:

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

Steps:

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

ccess Control Type	Card Reader Aute	Multiple Authentic	First Card	Anti-passing Back	Multi-door Interloc	White List	Password Authenti
Controller Group	🖄 Apply	Card List					
learch	9	Add	Delete			Filter	
123		Card No. S	itatus	Activation Date:	Expiry Date:		
Normal C							
	Disabled Person						
Card in B							
Patrol Ca Duress C							
Super Ca							
Visitor Ca							
		Total:0	Page1/1				► ► 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. Double click to edit the

- 2. Click Add and select the available card.
- 3. Click **OK** to confirm assigning the card(s) to the selected card type.
- 4. Click Apply to take effect of the new settings.

Notes:

- You can click **Delete** to remove the card from the card type and the card can be available for being re-assigned.
- Double click the added card in the card list of Visitor Card to edit the maximum card swipe time.

7.7.7 Card Reader Authentication

Purpose:

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

Notes:

- For this authentication mode, the card swiping operation cannot be replaced by entering the card No..
- For password settings, please refer to *Section 21.2.2 Normal Card*. *Steps:*
- 1. Click the 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 and Password: The door can open by both inputting the password and inputting the fingerprint.

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

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

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

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

Access Control Type	Card Reader Aute	Multiple Authenti	tic First Car	d	Anti-pa	assing Ba	ack Mi	ulti-door Ir	terloc	•	White	List	Passw	ord Aut	henti.	
Card Reader List	🕹 Apply	Property											Copy to		۵	Save
	Apply Apply	Property C Card Weel T V T	Card Reade R	eader wipe C			08	~ [] [] []	opy to							
			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.

7.7.8 Multiple Authentication

Purpose:

You can manage the cards by group and set the authentication for multiple cards for one access controller.

Steps:

- 1. Click the Multiple Authentication tab and select a group in the access controller from the list on the left.
- 2. Click Role to enter the Role tab. Select a role in the role list and edit the role name and the expiry date.
- 3. Click Add the group members.

Access Control Type	Card Reader Aute	Multiple Authentic	First Card	Anti-passing Back	Multi-door Interloc	White List	Password Authenti
门禁点列表	🖶 Apply	Role	Certification Grou	IP			
Search	9	🚵 Role_1	Pro	perty			G Save
10.15.6.222		Role_2					
10.15.6.248		Role_3		Role Name:	Role_1		
10.15.6.193		🏰 Role_4		Evelo: Date:	2016-09-20 00:00:00	89	
		😽 Role_5		Expiry Date:	2016-09-20 00.00.00	<u></u>	
		🏰 Role_6			2016-09-20 23:59:59	**	
		🏰 Role_7					
		💒 Role_8		Group Member:	수 Add	🔀 Delete	
		🏰 Role_9		Card No. P	erson Name:		
		🎇 Role_10					
		🎇 Role_11					
		Role_12					
		Sole_13					
		Role_14					
		Role_15					
		Role_16					
		Role_17					
		Role_18					
		Role_19					
		Role_20					
		Role_21					

4. Check the target card No. and click Add to add the selected member with the corresponding card. The added members will be displayed in the group member list.

1 3	Search			Search	
3 Rose 2	- 💶 🚨	Jack			
Rose 2		1			
2		3			
	💄	Rose			
4		2			
		4			

Or select the member in the group member list and click delete the member.

- 5. Click **Save** to save the configuration.
- 6. Click Certification Group to enter the Certification Group tab.
- 7. Select a distributed access controller and click Add

Role Certification	Group	
Distributed C	Group List 🗘 Add 🔯 Delete	🖬 Save
Distributed C	Certification G Template	Certificate Type
Distributed C		
Distributed C		

Configure the template, the certificate type, the offline authentication and the certification group. And click Add in the middle to add the role from

the left list to the right one.

Note: If the certificate type is Local Authentication, you can add up to 8 certificate groups. If the certificate type is not Local Authentication, you can add up to 7 certificate groups.

Or select the target role in the right list and click Belete	to c	delete the
selected role.		
Or select the target role and click Move Up or Move Down	t	to change

the role swiping card order.

Add Certificate ×			
Template:	Default Enable Schedule Template		
Certificate Type:	Local Authentication ~		
Offline Authentication: Enable super password when offline.			
Certification Group:			
Name Card Sw	Name Card Swipi.		
Role_1 0	🕹 Add		
	🔀 Delete		
	Move Up		
	O Move Down		
•	× •		
	Add Cancel		

9. Double click the Card Swiping Times and edit the card swiping times.

10. Click Add			
		×	
	Role Name:	Role_1	
	Card Swiping	0	
		Add Cancel	
11. Click Add at the bottom to add the configured the authentication group			
to the group list. And click 📓 Save to save the configuration.			
Notes:			

- Click Apply on the upper-left to take effect of the new settings.
- The card swiping time should be more then 0.

7.7.9 First Card

Purpose:

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

ccess Control Type Card Reader A	ute Multiple Authentic First Card Anti-passing Back Multi-door Interloc White List	Password Authenti
ontroller 🛃 Apply	Access Control Point First Card Parameters	Save
Gearch	Access Control Point Enable First Card Remain Open Remain Open Duration (Minute)	
10.15.6.222	Distributed Controller_1 Remain Open by First Card v 10	
10.15.6.248	Distributed Controller_1 Disable First Card Function	
10.15.6.193	Distributed Controller_1 Disable First Card Function	
	Distributed Controller_1 Disable First Card Function	
	FirstCard List	
	Add Delete Filter	
	Card No. Status Activation Date: Expiry Date:	

Steps:

- 1. Click the First Card tab and select an access control point.
- 2. Select in **Enable First Card Remain Open**. You are able to select Disable First Card Function, Remain Open by First Card Mode and First Card Authorization Mode.

Remain Open by First Card Mode:	If you select Remain Open by First Card Mode, you should input the time duration for remaining open the door. The door will open for the configured time duration for people accessing the door.
First Card Authorization Mode:	Swipe the authorized first card before other cards swiping. Swipe the first card again to dismiss other cards accessing authorization. After 24:00 every day, you should authorize the first card again.

3. Click Add and select the cards to add as first card for the door and click

the **OK** button.

Click Save and then click the Apply button to take effect of the new settings.

7.7.10 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 the Anti-passing Back tab and select an access control point.

Access Control Type Card Reader Aute	. Multiple Authentic First Card Anti-passing Back Multi-door Interloc White List Password Authenti
Controller 🛃 Apply	Property Save
Controller & Apply Search () 10.15.6.222 () 10.15.6.193 () 10.15.6.193	

- 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.

7.7.11 Multi-door Interlocked (Do Not Support)

Purpose:

You can set the multi-door interlocking between multiple doors of the same access controller. To open one of the doors, other doors must keep closed. That means in

the interlocking combined door group, up to one door can be opened at the same time.

Notes:

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

Steps:

1. Click Multi-door Interlocking tab and select an access controller from the list.

Access Control Type	Card Reader Aute	Multiple Authentic First	t Card Anti-passing Back	Multi-door Interloc	White List	Password Authenti
Controller 🛃	Apply	Multi-door Interlocking List				
Search	9	Add De	elete		Filter	
Search		Add De Serial No. Interlocking		king Combination	Filter	

2. Click Add to pop up the Add Access Control Point window.

	Add Access Control Point to Interlock
Please selec	ct access control point to interlock:
Serial No.	Access Control Name
✓ 1	172.10.18.25_Door1
✓ 2	172.10.18.25_Door2
✓ 3	172.10.18.25_Door3
✓ 4	172.10.18.25_Door4
	OK Cancel

- Select the access control point (door) from the list.
 Note: Up to four doors can be added in one multi-door interlocking combination.
- 4. Click ok to save the adding.
- 5. (Optional) After adding the multi-door interlocking combination, you can

select it from the list and click Delete the combination.

Notes:

- Click Apply button to take effect of the new settings.
- The normal access controller can add up to 4 multi-door interlocks. The device of DS-K2700, DS-K27M01, DS-K27M02 and DS-K27M04 can add up to 8 multi-door interlocks.

7.7.12 White List (Do Not Support)

Steps:

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

Access Control Type	Card Reader Aute	Multiple Authentic	First Card An	i-passing Back	Multi-door Interloc	White List	Password Aut	henti
Controller Lis 😃	Apply	Telephone Whitelist Se	ttings			🗘 Add	🛛 Delete	Save
Search 9	Telephone							
 10.15.6.248 10.15.6.193 	0.10.10.0.240	Door:						
- Sal 10.15.6.193		Name	Open	Close	Normally Open	Normally Close	I	
		Zone: Name A	rm Disarn					
		- Name - P	uni Disani	· ·				

- 2. Select the access control point, and click Add
- 3. Input the mobile number.
- 4. 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).

Zone: The mobile can arm and disarm the arming channels.

- 5. Click Save to save parameters.
- 6. Click Apply to take effect of the new settings.

Notes:

- 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-Normallyopen,021-NormallyClosed,120-Disarm, 121-Arm	
Operation Range	1	1-all objects with permission, 2-single operation	Command#1#

• Each access controller can add up to 8 mobile phone numbers.

Operation	3	Starts from 1 (corresponding Command#2#Operation
Object		to different doors or arming Object#
		regions according to
		commands)

7.7.13 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.

ccess Control Type Card Read	er Aute Multiple Authentic.	First Card	Anti-passing Back	Multi-door Interloc	White List	Password Authenti	
Controller Lis 🛃 Apply	Reader List						
Search	ନ 🕹 Add	Delete			Filter		
- ᆀ 10.15.6.222	Card No.	Password	Activation Date:	Expiry Date:			
- ᆀ 10.15.6.248							
- ᆁ 10.15.6.193							

2. Click Add to enter the Add Card window.

		Filter
Card No.	Status	Password Oper
0001	Normal Card	ß
0002	Normal Card	B
0003	Normal Card	B
0004	Normal Card	ß
0005	Normal Card	ß
	Page1/1	Go to

3. Check the checkbox of the corresponding card, and click the *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 to finish adding the card.
- 6. Click Apply to take effect of the new settings.

Notes:

- The card, which has added the password, will be displayed in the card list.
- You can select the card in the card list, and click Delete to delete the password authentication of the selected card.
- The normal access controller supports up to 500 cards to open door via password. The 500 cards' password should not be duplicated.
- The device of DS-K2700 supports up to 1000 card to open door via password.

8 Attendance Management (Do Not Support)

Purpose:

After adding the device and person, you can set the person shift, set the holiday, manage the person attendance and view the card swiping log.

8.1 Attendance Configuration



icon on the control panel to enter the Attendance

Configuration interface.

8.1.1 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 Shift Group Management tab to enter the following page.

Shift Group Ma S	hiftManagem H	Holiday Manag Shift Schedul	e Attendance Ch Adjustment	Ma Card Swiping L Statistic	Analysis Parameters Co Da	ata Manage
🗘 Add	Edit	Delete				Filter
Serial N	lo.	Shift Group Name	Shift Group No.	People Coun	Remark	
✓ 1	班组1		0001	0		

2. Click Add to pop up the Shift Group window.

			Add Shift	t Group		×
The items	with asteris	sk are required				
*Shift Group	Name:			*Shift Group No.:	0001	
R	emark:					
Person List	t				+ Add	X Delete
Seria	al No.	Name	Gender	Departme	ent	
					ОК	Cancel

3. Enter the shift group name, and click Add on the person list area to pop up the Add Person window.

Add Person	×
Search	9
e 🗹 🛃 Default	
🖃 🗹 🔠 Human Resource Department	
🗹 💶 Wendy	
Cindy	
	OK Cancel

4. Check the checkbox to select the person and click **OK** button and return to the shift group settings interface.

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

Delete

- 5. Click **OK** button to complete the operation.
- 6. You can edit or delete the added shift groups by clicking Edit or

Notes:

- After deleting the shift group, the shift schedule of the shift group will be deleted as well. For details about shift schedule, refer to *Chapter 22.1.4 Shift Schedule Management*.
- If the person has been added to one shift group, he/she cannot be added to

other shift groups.

• No person amount limit when adding the person.

8.1.2 Shift Management

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

Shift Group Ma Shift Managem Holida	y Manag Shift Schedule Attendance Ch Adjustment Ma Card Swipi	ng L Statistic Analysis Parameters Co Data Manage
Shift Man	🗘 Add Edit Delete	Search 9
Normal Shift	Serial No. Rule Name Remark	
Attendance Rule		
Attendance Shift		
Man-Hour Shift		

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

Normal Shift

♦ Setting Attendance Rule

- 1. Click **Attendance Rule** to set the rule for the attendance management.
- 2. Click Add to pop up the Attendance Rule window.

Attendance Rule	×
The items with asterisk 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	
Break Time Minutes 0	
Off-Work Attendance Check Delay Time 0	
Off-Work Early Time Minutes 0	
Absence Threshold (Early-Leave, Unit: 0	
	OK Cancel

- 3. Set a rule name.
- 4. Set detailed parameters for the attendance rule according to actual needs.
- 5. Click to save the rule.
- 6. (Optional) You can edit or delete the rule by clicking Edit or Delete button.

button.

Notes:

- After deleting the rule, the normal attendance shift which has enabled the rule will be deleted as well.
- If the shift which has enabled the rule has already set the shift schedule, the shift will not be deleted.

♦ Setting Attendance Shift

- 1. Click Attendance Shift to set the normal attendance shift.
- 2. Click Add to pop up the attendance shift setting window.

tenda	ance Shift									×
The	e items with aste	erisk are	requir	red.						
*5	Shift Name:				Shi	ift No.:	0001			
	Rem									
Off/(On-Work Period								Clear	
	On-Work Ti	(On-wo	rk Time		Off-wa	ork time	Attendance Rule	I	
	On-Work Ti	Day	~	00 : 00	Day	~	00 : 00		~	
	On-Work Ti	Day	~	00 : 00	Day	~	00 : 00		~	
	On-Work Ti	Day	~	00 : 00	Day	~	00 : 00		~	
								ок	Cancel	

- 3. Set a shift name.
- 4. Set on-work duration for the shift, and select the attendance rule from the dropdown list.
- 5. Click to complete the operation.
- 6. (Optional) You can edit or delete the shift by clicking <u>Edit</u> or <u>Delete</u>.

Note: After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to *Section 8.1.4 Shift Schedule Management*.

Man-Hour Shift

- 1. Click Man-Hour Shift to set the man-hour shift details.
- 2. Click Add to pop up the Man-hour Shift window.

Man-F	lour Shift				×
Th	e items with ast	erisk are required.			
	*Shift Name:		*Shift No.	0001	
*[Daily working	00:00	Latest On-Work	00:00	
	Rem				
Dis	regard Man-Hou	ır Period			Clear
	Time Period	Start Time	End Time	I	1
	Time Period1	00:00	00:00		
	Time Period2	00:00	00:00		
	Time Period3	00:00	00:00		
	Time Period4	00:00	00:00		
				OK	Cancel

- 3. Set a shift name, and daily work duration.
- 4. (Optional) Check the checkbox of latest on-work time, and set the latest on-work time.
- 5. (Optional) Set the durations excluded from man-hour duration.
- 6. Click **OK** button to complete the operation.
- 7. (Optional) You can edit or delete the shift by clicking <u>Edit</u> or <u>Delete</u>.

Note: After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to *Section 8.1.4 Shift Schedule Management*.

8.1.3 Holiday Management

Steps:

1. Click the Holiday Management tab to enter the holiday management interface.

Shift Group Ma Shift Managem Holiday Man	ag Shift Schedule	Attendance Ch Adjustment Ma Card Swipin	g L Statistic Analysis Parameters Co	. Data Manage
🗘 Add Edit Delete			Search	9
🗌 Serial No. Holiday Name	Holiday Days	Remark		

2. Click Add to pop up the Holiday window.

*Holiday N					
Rem					
Date List				🗘 Add	Delete
🗆 🕴 Serial No.	Date		Week		

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

	Select Date	×
The items with asterisk are required		
*Start Date: 3/10/2016	*End Date	: 3/10/2016 🛅
*Select by Week		🗆 All
🗌 Monday 📄 Tuesday 📄 Wed	🗌 Thursday 📄 Friday	Saturday Sunday
		OK Cancel

OK

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

5. Click to save the settings.

8.1.4 Shift Schedule Management

Purpose:

After setting the shift group and the corresponding shift and shift rule, you can set the shift schedule for the shifts.

Steps:

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

hift Grou	Add Delete	Filter
hift Grou		Filter ft No.

- 2. Select the shift group from the list on the left.
- 3. Click Add to pop up the shift schedule settings window.

Add Shift Schedule		_			×
Remark					
Shift Grou Si	hift Group 1	Shift Name		¥	
*Start Date: 20	016-09-22	*End Date	2016-09-22	2	
Add Holiday					
Serial No.	Holiday Name	Holiday Days	Remark		
					-
			ОК	Cancel	

4. Select the shift name from the drop-down list and set the start data and end data.

(Optional) You can check the checkbox of holiday to add the holiday shift.

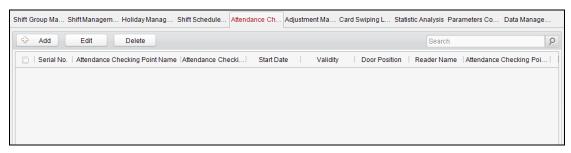
Click to complete the operation.

5. Click to save the settings.

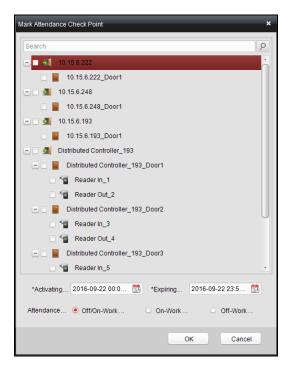
8.1.5 Attendance Check Point Management

Steps:

1. Click the Attendance Check Point Management tab to enter the Attendance Check Point Management interface.



2. Click Add to pop up the Mark Attendance Check Point window.



Check the select the card reader of the access control point and set the start date and end date.

Select the check point type.

Click to save the adding.

The added check points will be displayed in the attendance check point list.

3. You can check the checkbox of a check point, and click Edit to pop up the

attendance check point editing window.

You can edit the attendance check point name, start date, end date, and check point type, controller name, door position, and card reader name.

Click to complete the operation.

Delete to delete the 4. You can check the checkbox of a check point and click

added check point.

8.1.6 Adjustment Management

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

In this module, Reason Management and List Management can be realized.

Reason Management

\diamond Leave

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

Steps:

1. Click Leave to enter the leave interface.

¢ ∧	d Edit Delete	Search	9	
	Serial No. Reason Management			
□ 1	Personal Leave			
2	Sick Leave			
3	3 Marriage Leave			
4	Bereavement Leave			
5	Family Reunion Leave			
6	Annual Leave			
7	Maternity Leave			
8	Paternity Leave			

2. Click Add to pop up the Adjustment Reason adding dialog box.

Ad	Adjustment Reason					
The items with asterisk	are required					
Adjustment Type:	Leave					
*Adjustment Reason:						
	OK Cancel					
	Cancer					

OK 3. Enter the adjustment reason, and click to save the adding.

Notes:

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

Delete to delete the reason. reason, and click

Leave in Lieu

Steps:

1. Click Leave in Lieu to enter the leave-in-lieu interface.

C Add Edit Delete	Search	9
C Serial No. Reason Management		
1 Overtime Exchange Holiday		
2 Business Trip Exchange Holiday		

2. Click Add to pop up the Adjustment Reason adding dialog box.

Adjustment Reason							
The items with asterisk	are required						
Adjustment Type: Leave in Lieu							
*Adjustment Reason:							
	OK Cancel						

3. Enter the adjustment reason, and click

Notes:

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

and click ______ to delete the reason.

♦ Overtime

Steps:

1. Click **Overtime** to enter the overtime interface.

🗘 Add 🛛 Edit	Delete	Search 9
Serial No.	Reason Management	
1	Work Demand	
2	Workday Overtime	
3	Off Day Overtime	
— 4	Holiday Overtime	

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

3. Enter the adjustment reason, and click

Notes:

• 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 Leader to edit the reason,

and click ______ to delete the reason.

♦ Replace Card

Steps:

1. Click **Replace Card** to enter the following interface.

🗘 Add 🛛 Ed	lit Delete	Search	2
🗆 🕴 Serial No.	Reason Management		
1	Forget to Swipe Card		
2	Card Loss		
3	Device Fault		
— 4	Shift Rearrangement		
5	Business Trip		

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

3. Enter the adjustment reason, and click

Notes:

- 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 Edit to edit the reason,

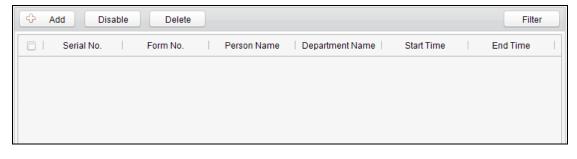
and click Delete the reason.

List Management

♦ Enabled List

Steps:

1. Click **Enabled** to enter the enabled list interface.



2. Click Add to add an attendance management form.

Adjustment Form	● Leave ○ Lea ○ Ove ○ Rep
Adjustme	事假 ~
Staff:	Add Delete
	Serial No. Person Name Gender Depar
Time Period:	2016-09-22 00:00:00 🔀 - 2016-09-22 23:59:59 🔯
	OK Cancel

- 3. Select the adjustment type: leave, leave in lieu, overtime, and card replacement. Leave, Leave in Lieu, and Overtime
 - 1) Select the adjustment reason from the drop-down list.
 - 2) Click Add to pop up the Add Person window.

Add Person	_	_	×
Adding Method:	By Dep	O By Shif	
Search		9	
😑 🗖 🚣 Default			
🖃 🗆 🟯 Depar	tment_1		
🗆 🚨 Jac	:k		
🗆 🚨 Ro:	se		
🗆 🛃 Depar	tment_2		
		ОК	Cancel

- Select the adding type as by department or by shift group. Select the person and click OK
- 4) Set the time duration.

Replace Card

- 1) Select the adjustment reason from the drop-down list.
- 2) Click Add to pop up the Add Person window.



- 3) Select the adding type as by department or by shift group. Select the person and click κ .
- 4) Set the date, attendance shift type, and card replacing time.
- 4. Click $\bigcirc K \bigcirc$ to complete the operation.

♦ Disabled List

Steps:

- 1. In the Enabled List interface, check the checkbox of a piece of enabled list and click Disable button to disable the list.
- 2. Click **Disabled** and the disabled list will be listed on the disabled interface.

	Serial No.	Form No.	Person Name	Department	Start Time	End Time	Adjustment Type	Adjustmen
✓	1	20160310132	Wendy	默认部门/Human	2016-03-10 00:00:00	2016-03-10 23:59:59	Leave	Personal Le
	2	20160310132	Cindy	默认部门/Human	2016-03-10 00:00:00	2016-03-10 23:59:59	Leave	Personal Le

3. You can check the checkbox and click Delete to delete the disabled list.

8.1.7 Card Swiping Log Query

Click **Swiping Log** tab to enter the card swiping log searching and viewing interface.

Query Sc All 💙 Start Date: 2016-09-22 00:00:00 🔀 End Date: 2016-09-22 23:59:59 📆	Reset

You can search the card swiping log by two query types: **By Shift Group**, and **By Department**.

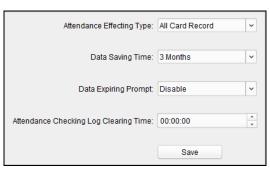
Input other search conditions and click Search to start query the card swiping log.

Or click Reset to reset the search conditions.

8.1.8 Parameters Configuration

Steps:

1. Click the Parameters Configuration tab to enter the parameters configuration interface.



- 2. Select the attendance effecting type, data saving time, data expiring prompt.
- 3. Set the attendance checking log clearing time.
- 4. Click <u>Save</u> to save the parameters.

8.1.9 Data Management

Steps:

1. Click Data Management tab to enter the data management interface.

Calculate Atten	2016-09-22 00:00:00	🖏	2016-09-22 23:59:59	2	🛛 🖉 Calculate Atten
Import/Export	2016-09-22 00:00:00	🔝	2016-09-22 23:59:59	1	
Export Data:					View
Import Data:					View

2. Select the date and time period for calculation and click Calculate Atten...

(Calculate Attendance Data) to start calculating the attendance data.

3. After calculation, you can also export and import the attendance data.

8.2 Attendance Statistic

Click the Attendance Statistics tab to enter the Attendance Statistics interface. On the Attendance Statistics interface, you can search the attendance statistic, attendance result statistics, and attendance rate statistics.

You can input the search condition including shift type, department, start date, and end date, and click Search button to search the attendance data.

You can click Reset to reset the search condition to the default value.

After searching, you can click **Export** to export the searching report to the local PC.

Static Type Attendance Analysis Table Attendance Result Statistic Table	Shift Type: Start Date:	Normal Shift 2016-07-11 00:0	0:00	Department: De End Date: 20	efault 016-07-11 23:59:5		Search Reset
Attendance Rate Statistic Table	Export Attendance Statis	tie Denied	A	Attendance Analys	sis Table		
	Person Name	Department	Attendance Date	Shift Name	Time Period (Dn-Work Attendanc	On-Work Status O
	•						Þ

9 Checking Status and Event

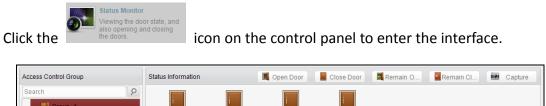
Purpose:

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

9.1 Status Monitor

Purpose:

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



Access Control Group	Status Information	Open Door	Close Door	Remain O	Remain Cl	Capture Capture
Search P Group_1	i	i	i			
	Distributed C Distributed C	Distributed C	Distributed C			
	Live Event					
	Live Event					More
	E	vent Source::				
	c	ard No.:				
	E	vent Type:				
	Т	ime:				

Note: The door status will be displayed according to the door magnetic or the lock. 9.1.1 Access Anti-control

Door Anti-control

Purpose:

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

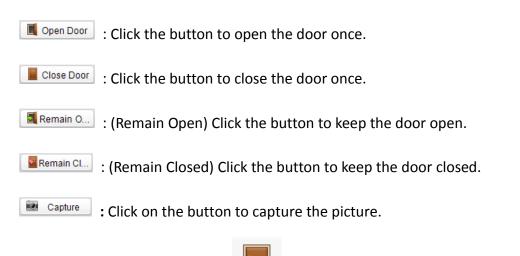
Steps:

1. Enter the status monitor page.

2. Click on the icon

In 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.



4. You can also right click the icon

and to select a status for the door.



Notes:

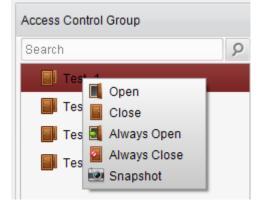
- If the status is selected as **Remain Open/Remain Closed**, the door will keep open/ closed until a new anti-control command being made.
- The function of picture capturing cannot be realized until the storage server is installed.

Group Anti-control

Purpose:

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

- 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.

9.1.2 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.



9.1.3 Real-Time Event

You can check the Real-time 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::		
	Card No.:		
25	Event Type:		
	Time:		

9.2 Access Control Event

Purpose:

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



icon on the control panel to enter the interface.

Access Control Event Information		🔒 Export	Card Holder Information
Seri Event Type Card Holder	Card Type Card No. Event Tin		

Steps:

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

9.3 Event Search

Purpose:

Click the

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 control panel to enter the interface.

Master Access Controller	User Manual
--------------------------	-------------

Event Type:	All	~	Device Name:	All	~	Card Holder:	
Start Time:	2016-09-22 00:00:00	2	Card Type:	All	~	Card No.:	Search
End Time:	2016-09-22 23:59:59	***	Direction:	All	~		
earch Result						Export	Card Holder Information
eri Event Type	Card Holder	Card Type	Card No.	Event Time	Event So	urce Direc	
							Person No.:
							Person No.:
							IC Card No.:

Steps:

- 1. Enter the event search page.
- 2. Enter the search criteria (event type/ person name/ card No/ start &end time).
- 3. Click to get the search results.
- 4. View the event information in the event list.
- 5. Click an event to view the information of the card holder on the **Person Information** panel on the left side of the page.

Or click Export to export the result.

10 System Maintenance

10.1 Log Management

Purpose:

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

	Log Search
18	Search configuration and

icon on the control panel to open the Log Search

page.

Click the

Search Condition	Search Result					Export
Log Type O Configurati 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. *Note:* Please narrow the search condition if there are too many log files.

Control Logs Searching

Purpose:

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

Steps:

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

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

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

10.1.1 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. *Note:* Please narrow the search condition if there are too many log files.

Searching Access Control Configuration Logs

Purpose:

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

- 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. *Note:* 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. *Note:* 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.
- 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.

10.1.2 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.

- 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. *Note:* Please narrow the search condition if there are too many log files.

Log Search

Purpose:

The Log Search of the Access Control System include informations 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. *Note:* Please narrow the search condition if there are too many log files.

10.2 System Configuration

Purpose:

Click the

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



icon on the control panel to open the System

Configuration page.

	System Configuration	×
Card Dispatcher Card Dispatcher Marchine Manual Capture	Basic Parameters Auto Time Synchroniza Everyday 00:00	
	Restore	De Save

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. For now DS-K1F100-D8、 DS-K1F100-M、

DS-K1F100-D8E card reader types are supported.

Fingerprint Machine

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

Manual Capture Configuration

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

10.2.3 Auto Time Synchronization

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

	System Configuration 🗙
Common Card Dispatcher Card Dispatcher Card Dispatcher Card Dispatcher Manual Capture	Basic Parameters ✓ Auto Time Synchroniza Everyday v 00:00
	Restore De Save

- 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 Save to save the settings.

Note: You can click the Restore De... (Restore Default Value) to restore the defaults of

all the local configurations.

10.2.4 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 **Card Dispatcher** on the System Configuration interface to open the Card Dispatcher Configuration page.

	S	ystem Configuration	×
Common Card Dispatcher Fingerprint Machine Manual Capture	S Type: Serial Port Type: Serial Port No.: Baud Rate: Overtime: Buzzing: Card No. Type:	ystem Configuration	▼ ▼ ▼ ▼ ms
			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.

• Configuration Instruction

DS-K1F100-M: select Serial Port Mode as accessing mode (currently only support serial port mode), the serial port No. is the COM port No. of the computer. Set other parameters as default.

DS-K1F100-D8E and **DS-K1F100-D8E**: select USB Mode as accessing mode (currently only support USB mode). Set other parameters as default.

- It is supported using card type as regular and Wiegand.
- When the Buzzing is selected as "YES", the audio will be off when you click

Save . If the Card Reader Configuration is set wrong; the audio will be on

when you click save and when you insert the card reader if the configuration is set correct.

• You can click Restore De... (Restore Default Value) to restore all of the local configuration to the defaults.

10.2.5 Fingerprint Machine Configuration

Steps:

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

	5	system Configuration	×
Common			
Card Dispatcher	Device type:	Optical fingerprint collecting ins 👻	
Fingerprint Machine	Serial Port No.:	COM1 ~	
🚳 Manual Capture	Baud Rate:	19200 ~	
	Device Code:	0	
	Overtime:	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 Save to save the settings.

- It is supported using device type as Optical Fingerprint Collecting Instrument and Capacitive Fingerprint Collecting Instrument.
- The serial port number should correspond to the serial port number of PC.
- The baud rate should be called according to the external fingerprint card dispatcher. The default value is 19200.
- Overtime refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.
- You can click the Restore De... button to restore the defaults of all local settings.

10.2.6 Manual Capture Configuration

Steps:

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

		System Configuration	×
Common			
Card Dispatcher	Size :	UXGA	~
Fingerprint 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.

You can click Restore De... (Restore Default Value) to restore all of the local settings the

defaults.

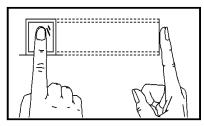
11 Appendix: Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

The figure displayed below is the correct way to scan your finger:



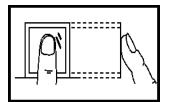
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

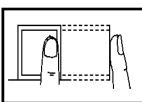
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

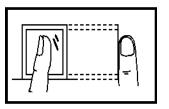
Vertical

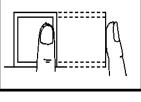
Edge I

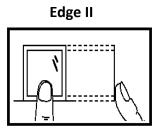












Environment

The scanner should avoid direct high light, high temperature, humid conditions and rain.

When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again after drying the finger.

Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Master Access Controller Licer Manual

