

# DS-K2600 Series Access Controller

User Manual



#### <u>User Manual</u>

©2017 Hangzhou Hikvision Digital Technology Co., Ltd. This manual is applied for Ness Australian Version access controllers..

Product Name	Serials		
Access	DS-K2601 Serials Access Controller		
Access Controller	DS-K2602 Serials Access Controller		
Controller	DS-K2604 Serials Access Controller		

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

#### About this Manual

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

Modifications have been made to this manual by Ness Corporation Australia to suit the Australian market and to assist in Ness customers understanding the product easier.

#### Trademarks

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

#### Disclaimer

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

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

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

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

#### Support

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

#### **Regulatory Information**

#### FCC Information

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

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

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

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

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

#### **FCC Conditions**

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

1. This device may not cause harmful interference.

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

#### **EU Conformity Statement**

**C** This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the R&TTE Directive 1999/5/EC, the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.



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



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated

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

#### Industry Canada ICES-003 Compliance

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

#### **Preventive and Cautionary Tips**

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

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.

Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the manufacturer.



#### **Safety Instruction**



# Please note: There is high voltage (240VAC) inside the housing of the controller. Extreme caution should be taken and only installed and serviced by licensed trained installers.

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

The precaution measure is divided into Warnings and Cautions:

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

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

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

#### 🛆 Warnings

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

# A Cautions

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation. The appropriate operation temperature is 0°C to +45°C, and the storage temperature should be -10°C to +55°C.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do
  not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Warning

Please note: There is high voltage (240VAC) inside the housing of the controller. Extreme caution should be taken and only installed and serviced by licensed trained installers.

DANGE

### **Table of Contents**

Chapter 1	Product Description	.1
1.1	Overview	.1
1.2	Main Features	.1
Chapter 2	Component Description	.3
Chapter 3	Terminal Connection	.4
3.1	Terminal Description	.4
3.1.1	DS-K2601Terminal Description	.4
3.1.2	DS-K2602Terminal Description	.6
3.1.3	DS-K2604 Terminal Description	.9
Chapter 4	Card Reader Installation1	13
4.1	External Terminal1	
4.1.1		13
4.1.2		13
4.1.3	DS-K2604 External Terminals1	13
4.2	Card Reader Installation	L4
4.2.1	The Connection of Wiegand Card Reader1	14
4.2.2		15
4.3	Installing E-Lock1	16
4.3.1		16
4.3.2	Installation of Anode Lock (Power to Lock)1 Connecting the External Alarm Device1	16
4.4	Connecting the External Alarm Device1	L7
4.5	Door Button Wiring Diagram1	L7
4.6	The Connection of Magnetics Detection (Door Monitoring)1	18
4.7	Connecting Power Supply1	18
4.8	Arming Region Input Terminal1	19
4.8.1	Connecting Normally Open Detector1	19
4.8.2	Connecting Normally Closed Detector1	19
4.9	Fire Alarm Module Wiring2	20
Chapter 5	Settings2	21
5.1	Initializing the Hardware	21
5.2	Relay Input NO/NC2	21
5.2.1	Lock Relay Output	21
5.2.2	Alarm Relay Output Status2	22
Chapter 6	Activating the Access Control Terminal2	24

6.2	1	Activating via SADP Software	24
6.2	2	Activating via Client Software	.25
Chap	oter 7	Client Operation	.28
7.	1	Function Module	.28
7.2	2	User Registration and Login	.31
7.3	3	System Configuration	.33
7.4	4	Access Control Management	.33
	7.4.1	Adding Access Control Device	.35
	7.4.2	Viewing Device Status	.39
	7.4.3	Editing Basic Information	.40
	7.4.4		
	7.4.6	5	
	7.4.7		.42
	7.4.8		.42
	7.4.9		.44
7.5	5	Person and Card Management	.48
	7.5.1	5	
	7.5.2		.50
7.6	6	Schedule and Template	64
	7.6.1		
	7.6.2	Holiday Group	.67
	7.6.3	Template	.67
7.7	7	Permission Configuration	. 72
	7.7.1	Adding Permission	.73
	7.7.2	Applying Permission	. 74
7.8	8	Advanced Functions	.75
	7.8.1	Access Control Parameters	.75
	7.8.1	.1 Status Duration Configuration (Auto Unlock of Doors)	.77
7.8	8.2	Card Reader Authentication	.78
	7.8.3	Multiple Authentication	84
	7.8.4	Open Door with First Card	.86
	7.8.5	Anti-Passing Back	.88
	7.8.6	Cross-Controller Anti-passing Back	. 89
	7.8.7	' Multi-door Interlocking	.92
	7.8.8	Authentication Password	.93
	7.8.9	Custom Wiegand	.94

7.9	Sear	rching Access Control Event	97
7.10	Acce	ess Control Event Configuration	98
7.10	0.1	Access Control Event Linkage	99
7.10	0.2	Access Control Alarm Input Linkage	.100
7.10	0.3	Event Card Linkage	.102
7.10	0.4	Cross-Device Linkage	.103
7.11	Doo	r Status Management	.105
7.1	1.1	Access Control Group Management	. 107
7.12	1.2	Anti-control the Access Control Point (Door)	.109
7.12	1.4	Real-time Card Swiping Record	.115
7.12	1.5	Real-time Access Control Alarm	.115
7.12	Arm	ing Control	. 117
Appendi	ix A S	ound Prompt and Indicator	. 118
Appendi	ix B C	ustom Wiegand Rule Descriptions	. 119

# CORPORATION

# **Chapter 1Product Description**

# 1.1 Overview

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

# **1.2 Main Features**

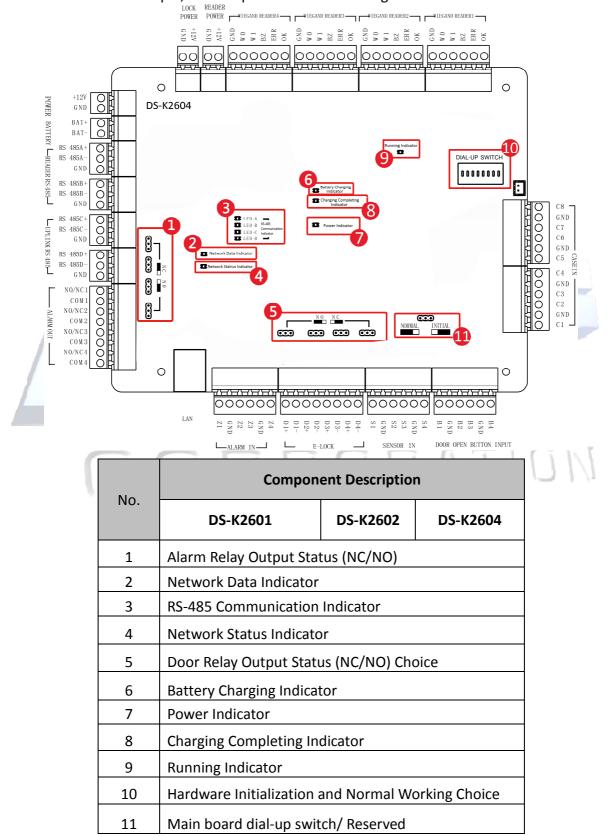
- The access controller is equipped with 32-bit high-speed processor
- Supports TCP/IP network communication. The communication data is specially encrypted to relieve the concern of privacy leak
- Support recognition and storage of card number with maximum length of 20
- The access controller can store 100,000 legal cards (97,000 normal cards and 3,000 visitor cards) and 300,000 card swiping records
- Supports multi-door interlock function, anti-passback function, multi-card function, first card open function, super card and super password function, M1 card encryption, online upgrade function and remote control of the doors
- Supports tamper-proof alarm for card reader, alarm for door not secured, force opening door alarm, alarm for door opening timeout, duress card and code alarm, blacklist alarm and alarm for illegal card swiping attempts reaching the limit
- The alarm input of controller supports short circuit protection function and cut-proof function
- Multiple event upload methods: channel, center group, and listening
- 50 event and card linkages
- IP address conflict detection
- Cross-controller anti-passing back function (For cross-controller anti-passing back based on card, wire the card reader with RS-485. For cross-controller anti-passing back based on network, connect the server and device properly. Up to 5000 cards' swiping records can be stored in the selected server.) and inner-device anti-pass-back function
- Supports RS485 interface and Wiegand interface for accessing card reader. RS485 interface adopts dual-interface design and supports loop breakpoint detection and redundancy function; Wiegand interface supports W26, W34 and is seamlessly compatible with third-party card reader with Wiegand interface
- Supports various card types as normal/ disabled/ blacklist/ patrol/ guest/ duress/ super card, etc.
- Various indicators to show different status
- Supports time synchronization via NTP, manual or automatic method
- Supports record storage function when it is offline and insufficient storage space storage alarm function
- The access controller has backup battery design, watchdog design and tamper-proof function

- Data can be permanently saved after the access controller is powered off.
- Supports I/O linkage, and event linkage
- 500 groups of password under the authentication mode of card and password



# **Chapter 2Component Description**

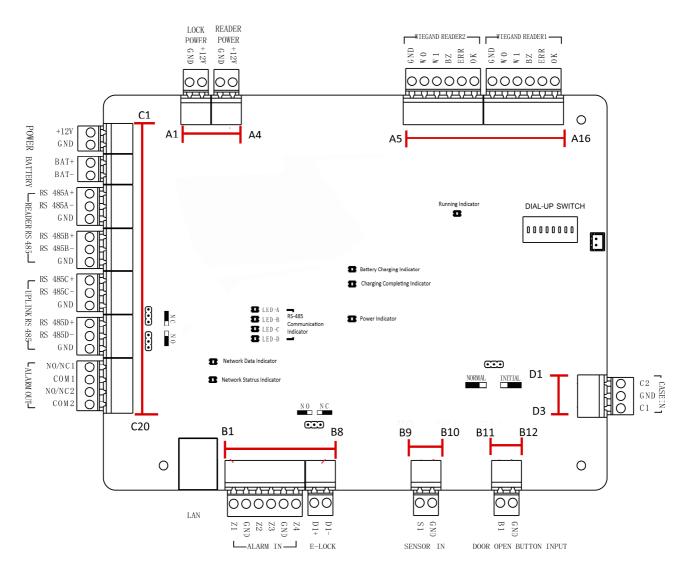
Take DS-K2604 as an example, the component schematic diagram is shown below.



# **Chapter 3Terminal Connection**

## **3.1 Terminal Description**

#### 3.1.1 DS-K2601Terminal Description



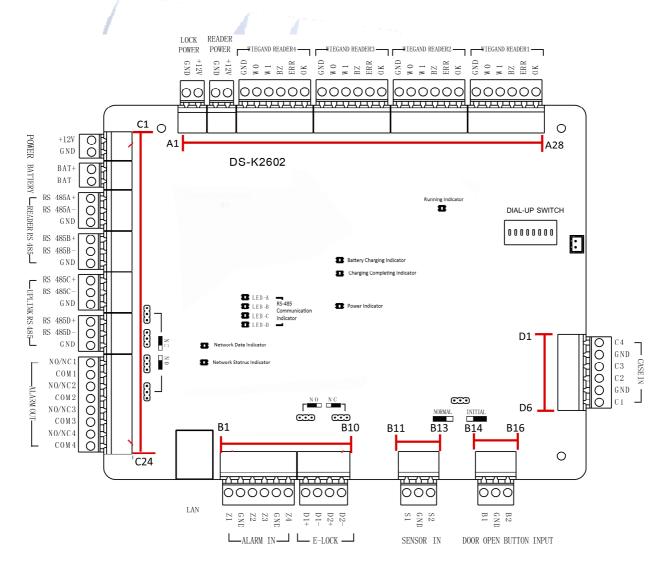
DS-K2601 Terminal descriptions are as follows	s:
---	----

No.	DS-K2601		
A1	Lock Power	GND	Grounding
A2	LUCK POWER	+12V	Power Output of the Lock
A3	Card Reader Power	GND	Grounding
A4	Card Reader Power	+12V	Power Output of the Head Read
A5		GND	Grounding
A6	Wingand Card Boador 2	W0	Wiegand Head Read Data Input Data0
A7	Wiegand Card Reader 2	W1	Wiegand Head Read Data Input Data1
A8		ΒZ	Card Reader Buzzer Control Output

No.	DS-K2601			
4.0			Indicator of Card Reader Control	
A9		ERR	Output (Invalid Card Output)	
A10		OK	Indicator of Card Reader Control	
AIU		OK	Output (Valid Card Output)	
A11		GND	Grounding	
A12		W0	Wiegand Head Read Data Input Data0	
A13		W1	Wiegand Head Read Data Input Data1	
A14	Wiegand Card Reader 1	BZ	Card Reader Buzzer Control Output	
A15	Wieganu Caru Neauer 1	ERR	Indicator of Card Reader Control	
A15		LINN	Output (Invalid Card Output)	
A16		ОК	Indicator of Card Reader Control	
		ÖK	Output (Valid Card Output)	
			Arming Region Access Terminal 1	
B1		Z1	(Only for Linkage of Alarm Relay	
			Output)	
B2		GND	Grounding	
			Arming Region Access Terminal 2	
B3		Z2	(Only for Linkage of Alarm Relay	
	Arming Region Input		Output)	
			Arming Region Access Terminal 3	
B4		Z3	(Only for Linkage of Alarm Relay	
			Output)	
B5		GND	Grounding	
		Z4	Arming Region Access Terminal 4	
B6			(Only for Linkage of Alarm Relay	
			Output)	
B7	E-Lock	D1+	Door 1 Door Relay Input (Dry Contact)	
B8		D1-		
B9	Door Contact Input	S1	Door 1 Door Contact Detector Input	
B10		GND	Grounding	
B11	Door Open Button	B1	Door 1 Door Open Button Input	
B12		GND	Grounding	
C1	Power	+12V	DC12V Cathode	
C2	•.	GND	DC12V Grounding Input	
C3	Battery	BAT+	DC12V Battery Cathode	
C4	,	BAT-	DC12V Battery Anode	
C5		RS 485A+	Card Reader RS485+ Access	
C6		RS 485A-	Card Reader RS485- Access	
C7	485 Card Reader	GND	Grounding	
C8		RS 485B+	Card Reader RS485+	
C9		RS 485B-	Card Reader RS485-	
C10		GND	Grounding	
C11	Access Controller RS485	RS 485C+	Uplink RS485+Communication	
C12	Interface	RS 485C-	Uplink RS485-Communication	
C13		GND	Grounding	

No.	DS-K2601			
C14		RS 485D+		
C15		RS 485D-	Reserved	
C16		GND		
C17		NO/NC1	Alarm Bolay 1 Output (Dry Contact)	
C18	Alarm Output	COM1	Alarm Relay 1 Output (Dry Contact)	
C19	Alarm Output	NO/NC2	Alarm Balay 2 Output (Dry Contact)	
C20		COM2	Alarm Relay 2 Output (Dry Contact)	
D1		C2	Event Alarm Input 2	
D2	Event Input	GND	Grounding	
D3		C1	Event Alarm Input 1	

#### 3.1.2 DS-K2602Terminal Description



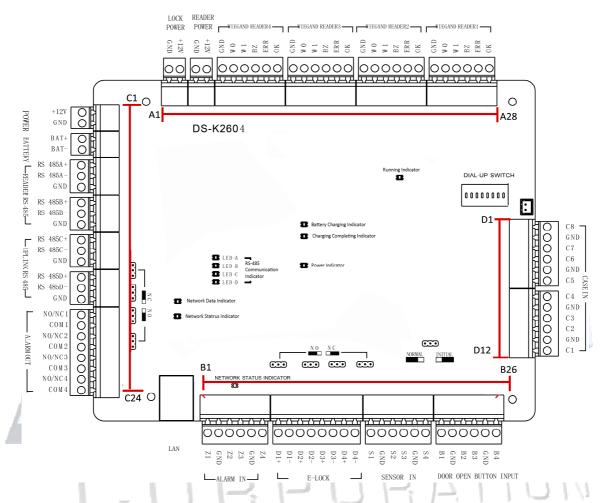
DS-K2602	Terminal	descriptio	ons are a	as follows:
DO NECCE		4696119616		

No.	DS-K2602		
A1	Dower for Elect	GND	Grounding
A2	Power for E-Lock	+12V	Power Output of the Lock

No.			DS-K2602
A3	Devices for Courd Decides	GND	Grounding
A4	Power for Card Reader	+12V	Power Output of the Head Read
A5		GND	Grounding
A6		W0	Wiegand Head Read Data Input Data0
A7		W1	Wiegand Head Read Data Input Data1
A8	Wiegand Card Reader	ΒZ	Card Reader Buzzer Control Output
A9	4	ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A10		ОК	Indicator of Card Reader Control Output (Valid Card Output)
A11		GND	Grounding
A12		W0	Wiegand Head Read Data Input Data0
A13		W1	Wiegand Head Read Data Input Data1
A14	Wiegand Card Reader	BZ	Card Reader Buzzer Control Output
A15	3	ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A16		ОК	Indicator of Card Reader Control Output (Valid Card Output)
A17		GND	Grounding
A18		W0	Wiegand Head Read Data Input Data0
A19		W1	Wiegand Head Read Data Input Data1
A20	Wiegand Card Reader	BZ	Card Reader Buzzer Control Output
A21	2	ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A22		ОК	Indicator of Card Reader Control Output (Valid Card Output)
A23		GND	Grounding
A24		W0	Wiegand Head Read Data Input Data0
		W0 W1	Wiegand Head Read Data Input Data Wiegand Head Read Data Input Data1
A25 A26	Wiegand Card Reader	BZ	Card Reader Buzzer Control Output
			Indicator of Card Reader Control Output (Invalid
A27	-	ERR	Card Output)
A28		ОК	Indicator of Card Reader Control Output (Valid Card Output)
B1		Z1	Arming Region Access Terminal 1 (Only for Linkage of Alarm Relay Output)
B2		GND	Grounding
			Arming Region Access Terminal 2 (Only for
B3		Z2	Linkage of Alarm Relay Output)
B4	Arming Region	Z3	Arming Region Access Terminal 3 (Only for
04		23	Linkage of Alarm Relay Output)
B5		GND	Grounding
B6		Z4	Arming Region Access Terminal 4 (Only for Linkage of Alarm Relay Output)
B7	E-Lock1	D1+	Door 1 Door Relay Input (Dry Contact)
107	L LOCKT	ידס	

No.		C	DS-K2602		
B8		D1-			
B9	51	D2+			
B10	E-Lock2	D2-	Door 2 Door Relay Input (Dry Contact)		
B11	DeerMegneties	S1	Door 1 Magnetic Detector Input		
B12	Door Magnetics	GND	Signal Grounding		
B13	Detector	S2	Door 2 Magnetic Detector Input		
B14		B1	Door 1 Door Button Input		
B15	Door Button	GND	Signal Grounding		
B16		B2	Door 2 Door Button Input		
C1	Dower	+12V	DC12V Cathode		
C2	Power	GND	Grounding		
C3	Dattan	BAT+	DC12V Battery Cathode		
C4	Battery	BAT-	DC12V Battery Anode		
C5		RS 485A+	Card Reader RS485+ Access		
C6		RS 485A-	Card Reader RS485- Access		
C7	Card Reader 485	GND	Grounding		
C8	Interface	RS 485B+	Card Reader RS485+		
C9		RS 485B-	Card Reader RS485-		
C10		GND	Grounding		
C11		RS 485C+	Uplink RS485+Communication		
C12		RS 485C-	Uplink RS485-Communication		
C13	RS-485 Interface	GND	Grounding		
C14	K3-405 IIILEIIALE	RS 485D+			
C15		RS 485D-	Reserved		
C16		GND			
C17		NO/NC1	Alarm Relay 1 Output (Dry Contact)		
C18		COM1	Alarin Kelay I Output (Dry Contact)		
C19		NO/NC2	Alarm Relay 2 Output (Dry Contact)		
C20	Alarm Output	COM2	Alarm Nelay 2 Output (Dry Contact)		
C21	Alarm Output	NO/NC3	Alarm Relay 3 Output (Dry Contact)		
C22		COM3	Alarm Nelay 5 Output (Dry Contact)		
C23		NO/NC4	Alarm Relay 4 Output (Dry Contact)		
C24		COM4	Alarm Nelay 4 Output (Dry Contact)		
D1		C4	Event Alarm Input 4		
D2		GND	Grounding		
D3	Event Input	C3	Event Alarm Input3		
D4	Event input	C2	Event Alarm Input 2		
D5		GND	Grounding		
D6		C1	Event Alarm Input 1		

#### 3.1.3 DS-K2604 Terminal Description



DS-K2604 Terminal descriptions are as follows:

No.	DS-K2604				
A1	Power Supply	GND	Grounding		
A2	of E-Lock	+12V	Power Supply of E-Lock Output		
A3	Power Supply	GND	Grounding		
A4	of Card Reader	+12V	Power Supply of Card Reader Output		
A5		GND	Grounding		
A6		W0	Wiegand Card Reader Data Input Data0		
A7		W1	Wiegand Card Reader Data Input Data1		
A8	Wiegand Card	BZ	Buzzer of Card Reader Control Output		
A9	Reader 4	ERR	Cresset of Card Reader Control Output (Invalid		
A9	-		Card Output)		
A10				ОК	Cresset of Card Reader Control Output (Valid Card
AIU		ŰK	Output)		
A11		GND	Grounding		
A12	Wiegand Card	W0	Wiegand Card Reader Data Input Data0		
A13	Reader 3	W1	Wiegand Card Reader Data Input Data1		
A14		BZ	Buzzer of Card Reader Control Output		

No.			DS-K2604		
A15		ERR	Cresset of Card Reader Control Output (Invalid		
AIS		ENN	Card Output)		
A16		ОК	Cresset of Card Reader Control Output (Valid Card		
A10		ÖK	Output)		
A17		GND	Grounding		
A18		W0	Wiegand Card Reader Data Input Data0		
A19		W1	Wiegand Card Reader Data Input Data1		
A20	Wiegand Card	BZ	Buzzer of Card Reader Control Output		
A21	Reader 2	ERR	Cresset of Card Reader Control Output (Invalid Card Output)		
A22		ОК	Cresset of Card Reader Control Output (Valid Card Output)		
A23		GND	Grounding		
A24	Γ	W0	Wiegand Card Reader Data Input Data0		
A25	[	W1	Wiegand Card Reader Data Input Data1		
A26	Wiegand Card	BZ	Buzzer of Card Reader Control Output		
A27	Reader 1	ERR	Cresset of Card Reader Control Output (Invalid Card Output)		
A28		ОК	Cresset of Card Reader Control Output (Valid Card Output)		
B1			Arming Region Access Terminal 1 (Only for Linkage of Alarm Relay Output)		
B2	Ī	GND	Grounding		
В3	Arming Design	Z2	Arming Region Access Terminal 2 (Only for Linkage of Alarm Relay Output)		
B4	Arming Region - Input	Z3	Arming Region Access Terminal 3 (Only for Linkage of Alarm Relay Output)		
B5		GND	Grounding		
B6		Z4	Arming Region Access Terminal 4 (Only for Linkage of Alarm Relay Output)		
B7		D1+			
B8	E-Lock 1	D1-	Door 1 Door Relay Input (Dry Contact)		
B9		D2+			
B10	E-Lock 2 D2-		Door 2 Door Relay Input (Dry Contact)		
B11		D3+			
B12	E-Lock 3 D3-		Door 3 Door Relay Input (Dry Contact)		
B13		D4+			
B14	E-Lock 4	D4-	Door 4 Door Relay Input (Dry Contact)		
B15		S1	Door 1 Magnetic Detector Input		
B16	[	GND	Signal Grounding		
B17	Door Magnetics	S2	Door 2 Magnetic Detector Input		
B18	Input	<b>S</b> 3	Door 3 Magnetic Detector Input		
B19	] [	GND	Signal Grounding		
B20	Γ	S4	Door 4 Magnetic Detector Input		

No.			DS-K2604			
B21		B1	Door 1 Door Button Input			
B22		GND	Signal Grounding			
B23		B2	Door 2 Door Button Input			
B24	Door Button	B3	Door 3 Door Button Input			
B25		GND	Signal Grounding			
B26		B4	Door 4 Door Button Input			
C1	-	+12V	DC12V Cathode			
C2	Power	GND	Grounding			
C3	<b>B</b>	BAT+	DC12V Battery Cathode			
C4	Battery	BAT-	DC12V Battery Anode			
C5		RS 485A+	Card Reader RS485A+			
C6		RS 485A-	Card Reader RS485A-			
C7	Card Reader	GND	Grounding			
C8	RS485	RS 485B+	Card Reader RS485B+			
C9		RS 485B-	Card Reader RS485B-			
C10		GND	Grounding			
C11		RS 485C+	Uplink RS485+Communication			
C12		RS 485C-	Uplink RS485-Communication			
C13	Access	GND	Grounding			
C14	Controller	RS 485D+				
C15	RS485	RS 485D-	Reserved			
C16		GND				
C17		NO/NC1	Alarma Dalay 1 Outrast (Day Constant)			
C18		COM1	Alarm Relay 1 Output (Dry Contact)			
C19		NO/NC2	Alarm Palay 2 Output (Dry Contact)			
C20	Alarm Output	COM2	Alarm Relay 2 Output (Dry Contact)			
C21	Alarm Output	NO/NC3	Alexan Balay 2 Output (Dry Contact)			
C22		COM3	Alarm Relay 3 Output (Dry Contact)			
C23		NO/NC4	Alarm Relay 4 Output (Dry Contact)			
C24		COM4	Alarin Kelay 4 Output (Dry Contact)			
D1		C8	Event Alarm Input 8			
D2		GND	Grounding			
D3	Event Input	C7	Event Alarm Input 7			
D4		C6	Event Alarm Input 6			
D5		GND	Grounding			
D6		C5	Event Alarm Input 5			
D7		C4	Event Alarm Input 4			
D8		GND	Grounding			
D9	]	C3	Event Alarm Input3			
D10		C2	Event Alarm Input 2			
D11		GND	Grounding			
D12		C1	Event Alarm Input 1			

#### Notes:

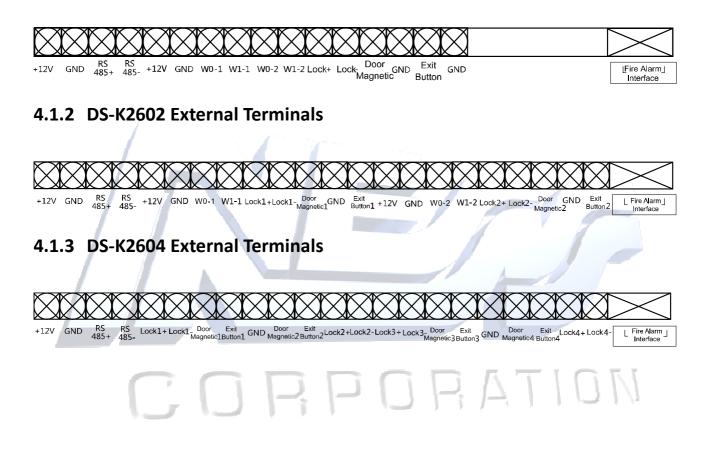
- The Alarm input hardware interface is normally open by default. So only the normally open signal is allowed. It can be linked to the buzzer of the card reader and access controller, and the alarm relay output and open door relay output.
- Arming region alarm input is only for the alarm relay output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

# CORPORATION

# **Chapter 4Card Reader Installation**

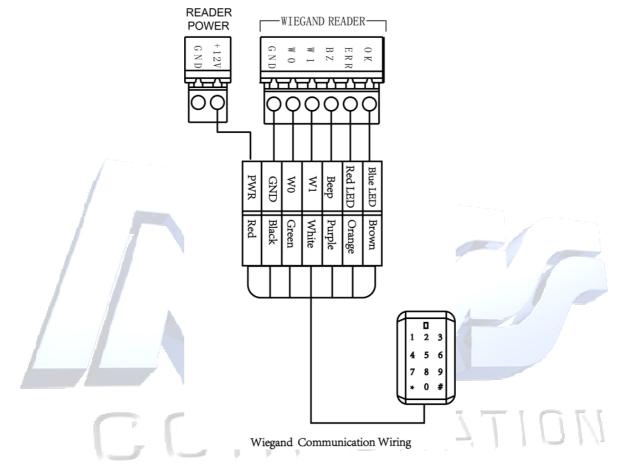
## 4.1 External Terminal

#### 4.1.1 DS-K2601 External Terminals



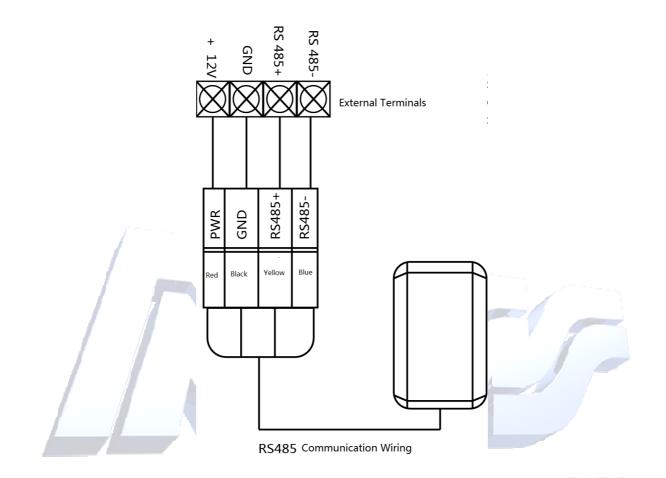
## 4.2 Card Reader Installation

#### 4.2.1 The Connection of Wiegand Card Reader



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

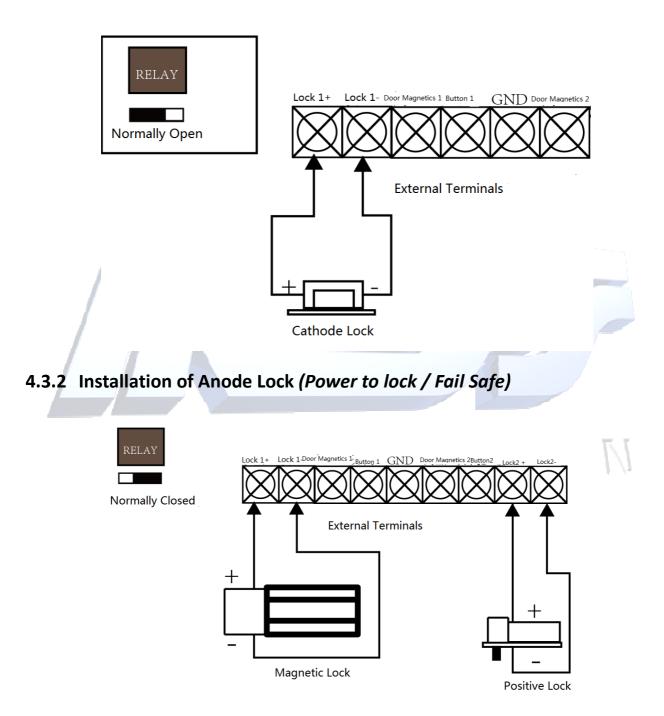


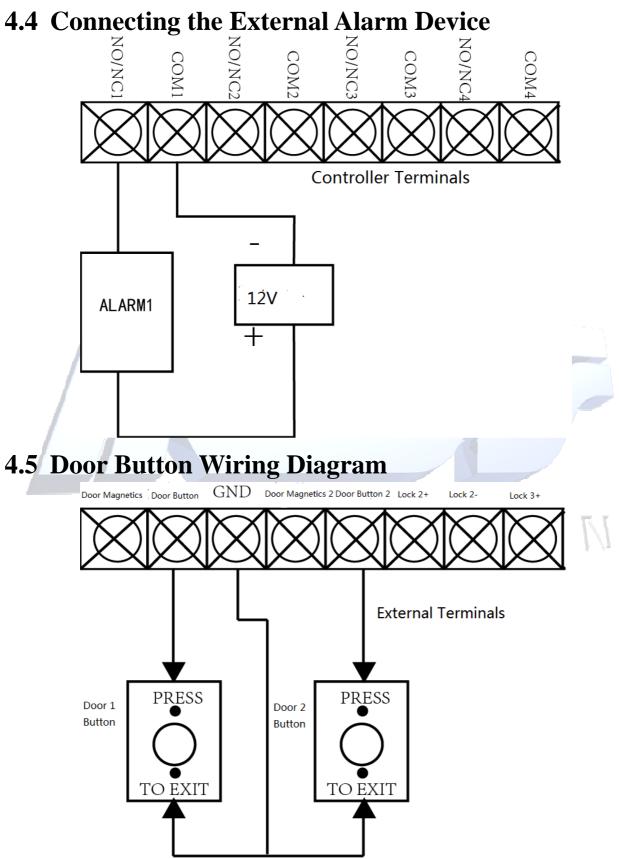


*Note:* If the card reader is installed too far away from the access controller, you can use an external power supply.

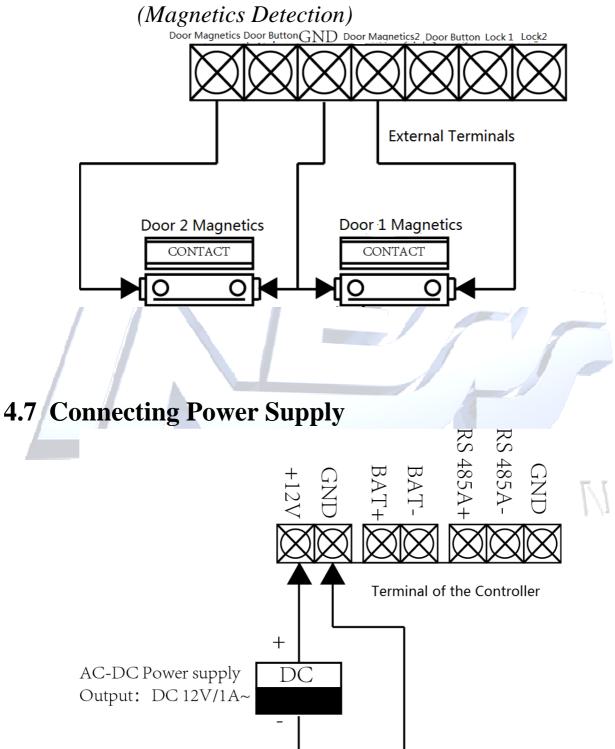
## **4.3 Installing E-Lock**

#### 4.3.1 Installation of Cathode Lock (Power to Unlock / Fail Secure)



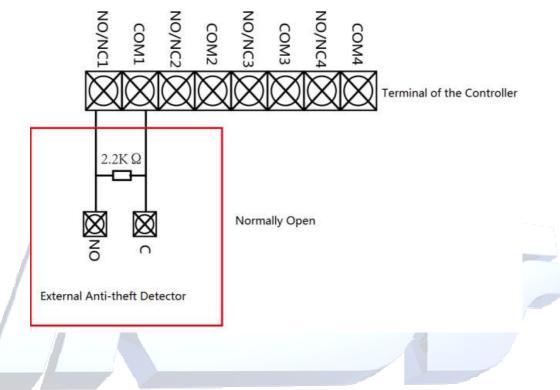


### 4.6 The Connection of Door Monitoring Reed Switches

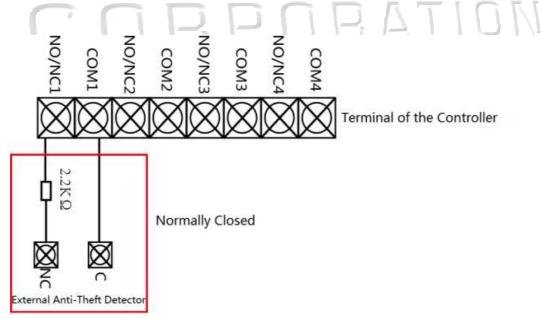


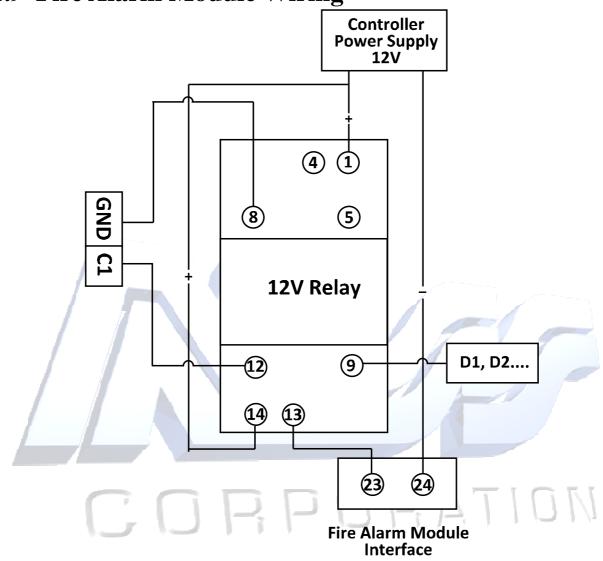
# 4.8 Arming Region Input Terminal

#### 4.8.1 Connecting Normally Open Detector



#### 4.8.2 Connecting Normally Closed Detector





## 4.9 Fire Alarm Module Wiring

# **Chapter 5Settings**

# **5.1 Initializing the Hardware**

#### Option 1:

#### Steps:

- 1. Remove the jumper cap from the Normal terminal.
- 2. Disconnect the power and restart the access controller. The controller buzzer buzzes a long beep.
- 3. When the beeping stops (~10-60 seconds), plug the jumper cap back to Normal.

#### Option 2:

#### Steps:

- 1. Jump the jumper cap from Normal to Initial.
- 2. Disconnect the power and restart the access controller. The controller buzzer buzzes a long beep.
- 3. When the beeping stops (~10-60 seconds), plug the jumper cap back to Normal.

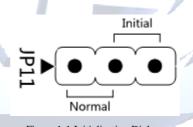


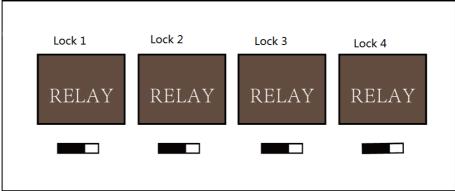
Figure 1-1 Initialization Dial-up

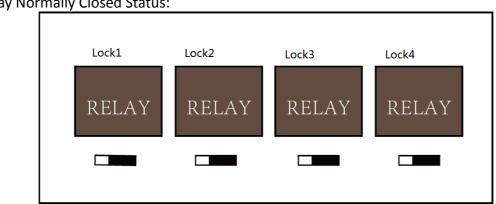
*Note:* The initializing of the hardware will restore all the parameters to the default setting and all the device events are wiping out.

# 5.2 Relay Input NO/NC

#### 5.2.1 Lock Relay Output

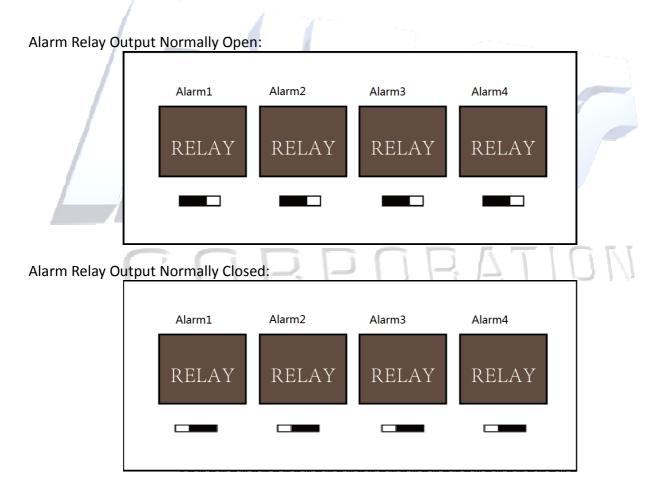
Lock Relay Normally Open Status:





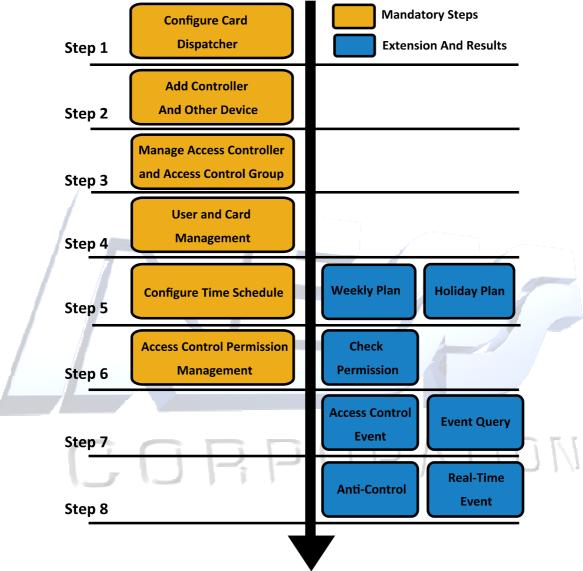
Lock Relay Normally Closed Status:

#### 5.2.2 Alarm Relay Output Status



#### Work Flow of Software

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



# Chapter 6Activating the Access Control Terminal

#### Purpose:

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

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

## 6.1 Activating via SADP Software

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

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

#### Steps:

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

ID	•   Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No	0.
001	10.000	Active		8000	V1.4.0build 1609		80		201
002		Active		8000	V1.4.2build 1608		80		1166
003		Active		8000	V1.4.0build 1609		80		20
004		Active		8000	V5.4.0build 1602		80		The device is not activated.
005	1	Active	10000	8000	V2.0.1build 1605		80		4Pk
006	DS-K	Inactive	192.0.0.64	8000	V1.0.0build 1608	0.0.0.0	80		160
									You can modify the network parameters after the device activation. Activate Now
									New Password:
									Confirm Password:

- 3. Create a password and input the password in the password field, and confirm the password.
  - **STRONG PASSWORD RECOMMENDED** We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
- 4. Click **Activate** to activate the device.
- 5. Check the activated device. You can change the device IP address to the same network segment with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

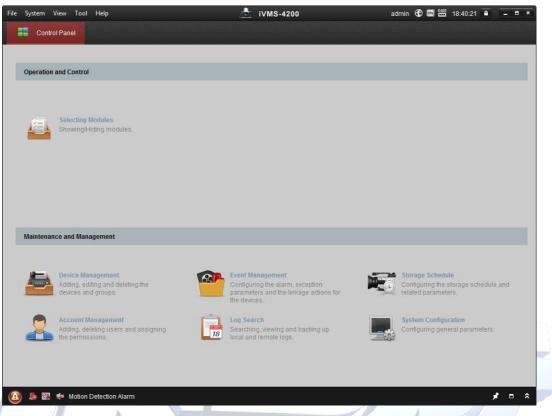
Enable DHCP  Device Serial No.:  IP Address: Port: 8000  Subnet Mask: Gateway: IPv6 Address: IPv6 Gateway: IPv6 Gateway: IPv6 Prefix Length: 0 HTTP Port: 80  Security Verification  Admin Password:	Modify Network	Parameters
IP Address: Port: 8000 Subnet Mask: Gateway: IPv6 Address: :: IPv6 Gateway: ::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

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

## 6.2 Activating via Client Software

The client software is versatile video management software for multiple kinds of devices. Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel. *Steps:* 

1. Run the client software and the control panel of the software pops up, as shown in the figure below.



- 2. Click the **Device Management** to enter the Device Management interface.
- 3. Check the device status from the device list, and select an inactive device.

					1	
 Online Device (	19)				📀 Refresh Every 60s 👋	
 + Add to Clie	nt 🕂 Add All	🗹 Modify Netinfo 🛛 🦘 Reset P	assword 🛛 🌻 Ac	tivate	Filter	
IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.   Start Tir	
192.0.0.64		10.4004000000	Active	8000	. 2017-01	101
192.168.1.64			Inactive	8000	2017-01	
					•	)
4					•	

4. Click the Activate button to pop up the Activation interface.

Ţ

5. In the pop-up window, create a password in the password field, and confirm the password.

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

	Activate Device	×
Password:		1
Confirm Pas	The password ( 8 to 16 characters) should contain two or more of the following character types: numeric, low	
	OK Cancel	J

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



# **Chapter 7 Client Operation**

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

# 7.1 Function Module

Control Panel of iVMS-4200:

Configuring the alarm, exception	Configuring the storage schedule and related parameters.
	related parameters.
	System Configuration Configuring general parameters.
	Compuning general parameters.
「「「「「「「」」」	Event Management Configuring the alarm, exception parameters and the linkage actions for the devices. Log Search Searching, viewing and backing up local and remote logs.

Menu Bar:

Open Image File	Search and view the captured pictures stored on local					
	PC.					
Open Video File	Search and view the video files recorded on local PC.					
Open Log File	View the backup log files.					
Exit	Exit the iVMS-4200 client software.					
Lock	Lock screen operations. Log in the client again to					
LOCK	unlock.					
Switch User	Switch the login user.					
Import System Config	Import client configuration file from your computer.					
File						
Export System Config File	Export client configuration file to your computer.					
	Set the schedule for backing up the database					
Auto Backup	including person, attendance data, and permission					
	data automatically.					
1024*768	Display the window at size of 1024*768 pixels.					
	Open Log File Exit Lock Switch User Import System Config File Export System Config File Auto Backup					

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

For the first time running the software, you can click



on the control

panel to select the modules to display on the Operation and Control area of the control pane. *Steps:* 

1.	Click	æ	to pop up the following	dialog.		
				Selecting Modules	×	
			Video Surveillance			
			🔲 🌄 Main View	🗌 🛅 Remote Playback		
			Access Control, Security Control, Video Inte	rcom		
			Access Control	📄 📕 Status Monitor	🗆 🤮 Time and Attendance	
			Security Control Panel	💷 🧶 Real-time Alarm		
			Extended Module			
		1	Alarm Event	Video Wall	🗌 🖄 E-map	
			Statistics			
			📃 🥑 Heat Map	📄 춢 People Counting	Counting	
			🗆 🚨 Road Traffic	E Face Retrieval	🗌 🔄 License Plate Retrieval	
		/	Behavior Analysis	Face Capture		
		[			OK Cancel	1-

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

#### Notes:

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

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

	The Main View module provides live view of network cameras and video encoders, and supports some basic operations, such as picture capturing, recording, PTZ control, etc.
	The Remote Playback module provides the search, playback, export of video files.
	The Access Control module provides managing the organizations, persons, permissions, and advanced access control functions. Provides video intercom function.
	The Status Monitor module provides monitoring and controlling the door status, viewing the real-time card swiping records and access control events.
¢	The Time and Attendance module provides setting the attendance rule for the employees and generating the reports.
ļ.	The Security Control Panel module provides operations such as arming, disarming, bypass, group bypass, and so on for both the partitions and zones.

	The Real-time Alarm module provides displaying the real-time alarm of security control panel, acknowledging alarms, and searching the history alarms.
	The Alarm Event module displays the alarm and event received by the client software.
	The Video Wall module provides the management of decoding device and video wall and the function of displaying the decoded video on video wall.
	The E-map module provides the displaying and management of E-maps, alarm inputs, hot regions and hot spots.
	The Device Management module provides the adding, modifying and deleting of different devices and the devices can be imported into groups for management.
<b>B</b>	The Event Management module provides the settings of arming schedule, alarm linkage actions and other parameters for different events.
	The Storage Schedule module provides the schedule settings for recording and pictures.
	The Account Management module provides the adding, modifying and deleting of user accounts and different permissions can be assigned for different users.
18	The Log Search module provides the query of system log files and the log files can be filtered by different types.
	The System Configuration module provides the configuration of general parameters, file saving paths, alarm sounds and other system settings.

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

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

# 7.2 User Registration and Login

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

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

R	egister Administator	×
Please create a su	per user before proceeding.	
Super User:		
Password:		
Confirm Password:		
	Enable Auto-login	
	Register Cancel	

- ♦ A user name cannot contain any of the following characters: / \ : \* ? " < > |. And the length of the password cannot be less than 6 characters.
- For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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

#### Steps:

1. Input the user name and password you registered.

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

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

1

1

3. Click Login.

- T	Login	×
<b>.</b>	admin v	
Forgot Passv	vord Login Cancel	

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

# 7.3 System Configuration

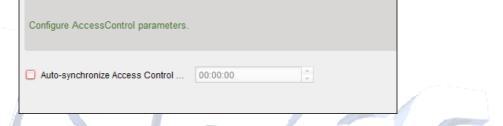
# Purpose:

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

#### Steps:

- 1. Click Tool System Configuration.
- 2. In the System Configuration window, check the **Auto-synchronize Access Control Event** checkbox.
- 3. Set the synchronization time.

The client will auto-synchronize the missed access control event to the client at the set time.



# 7.4 Access Control Management

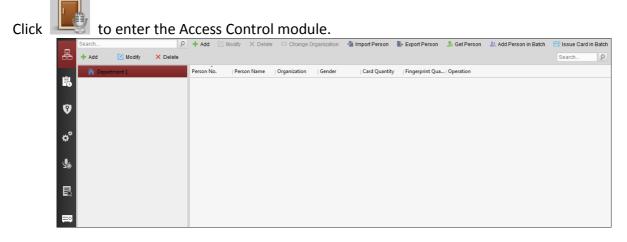
# Purpose:

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

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

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

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



#### Before you start:

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

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



#### Notes:

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

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

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

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

# 7.4.1 Adding Access Control Device

From within the 'Access Control" module, Click in the Access Control module to enter the following interface.

File S	System View Tool	Help						
=	Control Panel	🚔 Device Manager	nent 🚡	Main View	🛅 Remote Playback	Access Control	Statu	
居	Device for Managemer	nt (3)						
	🕂 Add 🗹 Modify	🗙 Delete 🔅 Remote	Configuration	🇱 QR Code 🏾 🌻 A	ctivate 🔤 Device Status	🖞 Upgrade (0)		
R	Device Type	Nickname	Connection	Network Parameters	Device Serial No.		Security	
EQ	Access Controller	Lift Interface	TCP/IP	192.168.0.197:8000	DS-K221020161130V0100008	N123869945	Weak	
	Access Controller	DS-K2804 (S)	TCP/IP	192.168.0.192:8000	DS-K280420160302V0100018	N797637450	Weak	
8	Access Controller	DS-K2604 (L)	TCP/IP	192.168.0.193:8000	DS-K260420171107V0200028	N125840115	Weak	
°° % ₪ ₩	]							

#### Purpose:

The active online devices in the same local subnet will be displayed in the in the **Online Device** area (i.e. bottom section of 'Device management') within the iVMS4200 software. This area is Refreshed every 60 seconds.

Control Panel agem	ent (3)												e
🕂 Add 🛛 Modify	🗙 Delete 🛛 🏶	Remote Configuration	🔠 QR Code   Ac	tivate 🔤 Device Stat	itus 🏦 Upgra	ide (0)						Filter	
Device Type	Nickname	Connection .	. Network Parameters	Device Serial No.		Se	curity	Net Status	Firmware Upgra	Refresh			
Access Controller	Lift Interfac	ice TCP/IP	192.168.0.197:8000	DS-K221020161130V01	10000EN1238699	145 We	eak	0	Not Upgradeable	0			
Access Controller	DS-K2604	TCP/IP	192.168.0.193:8000	DS-K260420171107V02	20002EN1258401	15 We	eak	0	Not Upgradeable	0			
Access Controller	DS-K2804 (	(S) TCP/IP	192.168.0.192:8000	DS-K280420160302V01	10001EN7976374	150 We	eak	0	Not Upgradeable	0			
Online Device (3)													🕢 Refresh Ev
+ Add to Client		Modify Netinfo 🈙 Res										Filter	Refresh Ev
+ Add to Client	vice Type	Firmware Version	Security	Server Port De	evice Serial No.		Added		k   Hik-Connect Stat	us		Filte:	😯 Refresh Ew
Add to Client     De     92.168.0.192     DS	vice Type K2804	Firmware Version V1.0.1 build 160302	Security	Server Port De	S-K280420160	2018-02-27 15:36:16	Yes	N/A	N/A	tus		Filter	🗘 Refresh Ev
Add to Client      Det      192.168.0.192     DS-      192.168.0.193     DS-      DS-	vice Type	Firmware Version	Security Active Active	Server Port         De           8000         DS           8000         DS	S-K280420160 S-K260420171					tus		Filter	€ Refresh Ev

Note: You can click

to hide the **Online Device** area.

# Steps for adding a device to your iVMS4200 Client Software:

*Note:*. Before a device can be added to the software it need to be activated <u>Refer Chapter 6</u> - <u>Activating the Access Control Terminal</u> (Page 24)

1. Select the devices to be added from the list (ie. From Online Device List at the bottom window of the screen.).

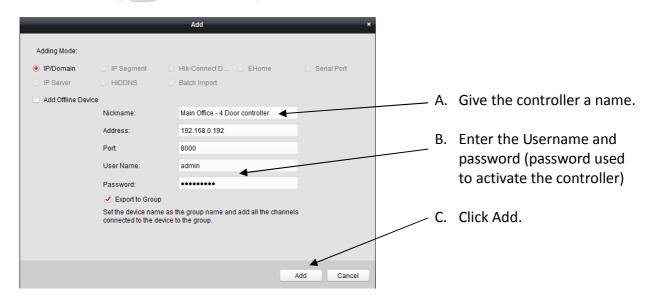
Online Device (	,3)					
🕂 Add to Clie	ent 🕂 Add All	🗹 Modify Netinfo 🛛 🥱 Reset Pa	assword 🛛 🔮 Ac	tivate		
IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.   Start Time	Added
192.168.0.192	DS-K2804	V1.0.1build 160302	Active	8000	DS-K280420160 2018-02-27 16:06:33	No
192,100,0,199	D3-12004	v2.0.200nd 1/110/	Active	0000	D3-N2004201/1 2010-02-2/ 10.00.33	165
192.168.0.197	DS-K2210	V1.0.0build 161130	Active	8000	DS-K221020161 2018-02-27 16:06:33	Yes

2. Click Add to Client to open the device adding dialog box.

Online Device	(3)						
+ Add to Cli	ent 🖶 Add All 🛛	Modify Netinfo 🛛 🦘 Reset Pa	assword 🏾 🔮 Ac	tivate			
IP *	Device Type	Firmware Version	Security	Server Port	Device Serial No.   Start Time	Added	
192.168.0.192	DS-K2804	V1.0.1build 160302	Active	8000	DS-K280420160 2018-02-27 16:06:33	No	
192.168.0.193	DS-K2604	V2.0.2build 171107	Active	8000	DS-K260420171 2018-02-27 16:06:33	Yes	I
192.168.0.197	DS-K2210	V1.0.0build 161130	Active	8000	DS-K221020161 2018-02-27 16:06:33	Yes	I

14

3. Input the required information.



**Nickname:** Edit a name for the device as you want to use for this controller. (Maybe location so it can easily be identified at a later date)

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

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

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

Password: Input the device password. (password used to activate the controller)



The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper and 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.

				<b>T</b> 1	
/ /	_	_	Add		×
	Adding Mode:				
	IP/Domain	<ul> <li>IP Segment</li> </ul>	O Hik-Connect D O EF	lome 📀 Serial Port	
	O IP Server		<ul> <li>Batch Import</li> </ul>		
	Add Offline Devi	се			
		Nickname:	Main Office - 4 Door contr	roller	
		Address:	192.168.0.192		
		Port:	8000		
		User Name:	admin		
	_	Password:	•••••		
		Export to Group Set the device name connected to the device	as the group name and add a ice to the group.	li the channels	
C					101
				Add Cance	4

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

## Adding Multiple Online Device

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

## > Adding All Online Devices

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

*Note:* After adding the device, you should check the device arming status in **Tool** – **Device Arming Control**. If the device is not armed, (i.e. Armed to receive events) you should arm it, or you will not receive the real-time events into the iVMS4200 client software. For details about device arming control, refer *7.11 Arming Control*.

*Note:* After adding the device, you should check the device arming status in **Tool** – **Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, refer *7.11 Arming Control*.

ntrol
ontrol
Arming Status
Ā
A A
A A A

*Note:* After adding the device, you should check the device arming status in **Tool** – **Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, refer *7.11 Arming Control*.

# 7.4.2 Viewing Device Status

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

Control Panel	🔊 Mai	n View	Device I	Management	5	Remote Playback	💾 Access
Device for Managemen	ıt (3)						
🖁 🕂 Add 🗹 Modify	🗙 Delete	🕸 Remote (	Configuration	謎 QR Code	Activa	te 📼 Device Status	1 Upgrade (0)
Device Type	Nickna	ime	Connection	Network Paran	neters   De	evice Serial No.	
Access Controller	Lift Inte	erface	TCP/IP	192.168.0.197:8	000 DS	-K221020161130V010000E	N123869945
Access Controller	DS-K26	i04 (L)	тср/ір	192.168.0.193:8	000 DS	-K260420171107V020002F	N125840115
Access Controller	Main C	office - 4 Doo	TCP/IP	192.168.0.192:8	000 DS	-K280420160302V010001E	EN797637450
Device: Access Controller_2	Dev	ice Status			×	P.A.T	101
Door Status	Door Name	Door Lock Sta	tus  Door Status	Door Magnetic S			
Host Status	1	Close	Normal Status	Close			
Card Reader Status	2	Close	Normal Status	Close	_		
Alarm Input Status Alarm Output Status Event Sensor Status Secure Door Control Unit Status Arming Status							
	4		Refre	sh Cancel			

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

Door Status: The status of the connected door.

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

Card Reader Status: The status of card reader.

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

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

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

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

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

Arming Status: The status of the device.

# 7.4.3 Editing Basic Information

#### Purpose:

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

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

C	Adding Mode: <ul> <li>IP/Domain</li> <li>IP Server</li> </ul>	<ul> <li>IP Segment</li> <li>HiDDNS</li> </ul>	Hik-Connect D O EHome Batch Import	<ul> <li>Serial Port</li> </ul>	T	0
		Nickname:	Access Controller_2	]		
S		Address:	10.15.6.195	]		
		Port:	8000			
		User Name:	admin			
		Password:	•••••			

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

# 7.4.4 Network Settings

#### Purpose:

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

It is recommended to leave these settings as default.

# 7.4.5 RS-485 Settings

#### Purpose:

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

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

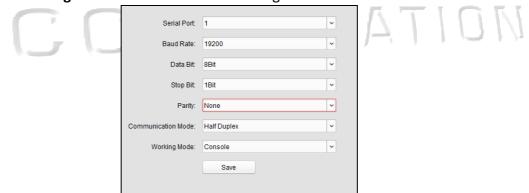
It is recommended to leave these settings as default unless instructed to change by Ness Technical staff.

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

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

#### Steps:

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



It is recommended to leave these settings as default unless instructed to change by Ness Technical staff.

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

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

# 7.4.6 Wiegand Settings

#### Purpose:

You can set the Wiegand channel and the communication mode.

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

# It is recommended to leave these settings as default unless instructed to change by Ness Technical staff.

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

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

#### Steps:

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

~	Wiegand No.:	1	~
	Communication Direction:	Receive	~
		Save	

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

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

# 7.4.7 M1 Card Encryption

# It is recommended to leave these settings as default unless instructed to change by Ness Technical staff.

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

- The function should be supported by the device.
- For details about issuing card, refer to *Adding Person (Card)* in *4 In the* organization list on the left, you should add a top organization as the parent organization of all organizations. Click **Add** button to pop up the adding organization interface.

File System View Tool Help					
📰 Control Panel 🔙 M	ain View 🛅 Rem	ote Playback 🛛 📓	Access Control		
Control Panel	♀ 💠 Add 🕑 × Delete	Modify 🗙 Delete	다 Change Orga	nizal	Add Organization ×
Ness	Person No.	Person Name	Organization	C	
R	1	Greg Kingsley	Ness	Ν	Organization:
	2	Ian Traeger	Ness	N	
8	3	Malcolm Turnbull	Ness	Ν	OK Cancel
	4	Pat Cash	Ness	N	

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

Then the added organization will be the sub-organization of the upper-level organization.

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

## Modifying and Deleting Organization

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

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

Notes:

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

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

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

#### Steps:

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



- 2. Set the sector ID.
- Click Save to save the settings.
   Note: The sector ID ranges from 1 to 100.

# 7.4.8 Remote Configuration

#### Purpose:

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

Device for Managemen		onfiguration 🇱 QR Code 🎈 A	ctivate 📼 Device Status 🏦 Upgrade (0)	
Device Type		Connection Network Parameters		
Access Controller	Lift Interface T	TCP/IP 192.168.0.197:8000	DS-K221020161130V010000EN123869945	
Access Controller	DS-K2604 (L) 1	TCP/ID 102168.0.103-8000	DS-K260420171107\/020002ENI125840115	
Access Controller	Main Office - 4 Doo 1	TCP/IP 192.168.0.192:8000	DS-K280420160302V010001EN797637450	
				F.

# **Checking Device Information**

#### Steps:

1. Click **System** -> **Device Information** to check the device basic information and the device version information.

- a.	Distant Date	1.0		
=) 🚯 System	Displaying the Device	Information		
Device Information	Basic Information			
🎡 General	Device Type:	DS-K2804	Local Trigger Number:	4
🎡 System Maintenance	Electric Lock Number:	4	Local RS-485 Number:	1
Security	Device Serial No.:	DS-K280420160302V	010001EN797637450	
🛨 🚳 Network	Version Information			
🛨 🚳 Alarm	Firmware Version	: V1.0.1 build 160302		
t 🕜 Other	Hardware Version	c 0x20000		
🛨 🚳 Operation 🛨 🏟 Status				

## **Editing Device Name**

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

Configuring the General Parameters							
Device Information							
Device Name:	Access Controller						
Device No.:	0						
	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.

🔞 System	Configuring the Time	oorninga		9., 14.11., 0.	- 17		
Device Information	Time Zone						
🎡 General	Select Time Zone:	(GMT+10:0	00) C	anberra, Gua	m, Me	Melbourne, Syd 👻	
😫 Time	Enable NTP						
System Maintenance Security	Server Address:	au.pool.nt	p.org		1		
🗑 Security	NTP Port	123		Minute(s)			
🖞 🚳 Alarm	Sync Interval:						
🖞 🔞 Other	Enable DST						
🗄 🚳 Operation	Start Time:	October		First Week	~	v Sun v 2 :00	
🖉 🚳 Status	End Time:	April	-	First Week	~		
	DST Bias:	60 min	~				
			-11				

## **Setting System Maintenance**

Steps:

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

Or click **Restore Default Settings** to restore the device settings to the default ones, excluding the IP address.

Or click **Restore All** to restore the device parameters to the default ones. The device should be activated after restoring.

*Note:* The configuration file contains the device parameters.

- 3. You can also remote upgrade the device.
  - 1) In the Remote Upgrade part, select an upgrade file type in the dropdown list. You can select Controller Upgrade File or Card Reader Upgrade in the drop-down list.
  - 2) Click 🔤 to select the upgrade file.
  - 3) Click **Upgrade** to start upgrading.

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

	System Maintenance	
	System Management	
	Reboot	
	Restore Default Settings	
	Restore All	
	Remote Upgrade	
	Select Type: Controller Upgrade 👻	
	Select File: Upgrade	
	Progress:	
Setting Secu	rity	
Steps: 1. Click System	m -> Security.	_
	Configuring the Security Parameters	171
	Encryption Mode	1/1
	Level: Compatible Mode	
	Save	

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

## **Configuring Network Parameters**

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

SCHOLTUN.	Rem	note Configuration	×
System     System     Bevice Information     General     Time     System Maintenance     Security     Security      Network	Configuring the Networ NIC Type: IPv4 Address: Subnet Mask (IPv4): Default Gateway (IPv4):	k Parameters          10M/1000M/1000M Self         192.168.0.215         255.255.255.0	
<ul> <li>General</li> <li>Advanced Settings</li> <li>Control Parameters</li> </ul>	MTU(Byte): Device Port:		

# **Configuring Access Control Parameters**

#### Steps:

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

	Configuring the Access Control		
	Downstream RS485 communication backup		
	Whether to allow key input card number		
_		Save	
G	JRPD		1101

# **Person and Card Management**

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

From the 'Access Control' Module, Click tab to enter the Person and Card Management interface.

File Sy	stem View	Tool Help								olyms-42	00	
==	Control Pane	el 🗾 📷	Face Picture C	omparison Alarm	🔚 Main Vi	ew 🛅	Remote Playback	📕 Acce	ss Control	ᡖ Status	Monitor 📒	Alarm Event 🔁
	trol Panel		9	🕂 Add 🛛 🖄 I	Modify 🗙 Delete	🛱 Change Org	ganization 🛛 📲 Imp	pontreison	Aporti erson	🦾 Get Person	🖳 Add Person i	n Batch 🛛 🗮 Issue Card in E
몲	Add	🔀 Modify	× Delete									
	🟠 Ness			Person No.	Person Name	Orgi	Jender	Card Quantity	Card No.	Fingerprint	Qua   Face Picture	Qu   Operation
R				1	Greg Kingsley	Nes:	/lale	1	0001847010	0	0	2 <b>6</b> 6
				2	Ian Traeger	Ness	/lale	1	0002499605	0	0	🖴 🛱 🖹
9		1		3	Malcolm Turnbull	Ness	Male	1	0002499767	0	0	
		_ <b>_</b>		4	Pat Cash	Ness	Male	1	02812002	0	0	🖴 🛱 🖹
		_		c	02000227	NI	NA-1-	1	02000227	0	0	

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

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

# 7.4.1 Organization Management

# **Adding Organization**

Steps:

4. In the organization list on the left, you should add a top organization as the parent organization of all organizations.

P.AT.

Click Add button to pop up the adding organization interface.

File System View Tool Help						
📰 Co trol Panel 🛛 🔂 Main View	🛅 Remo	te Playback 🛛 📕	Access Contro			
ontri e el 9	🕈 Add 🛛 🖄	Modify X Delete	🛱 Change Orga	nizal		Add Organization ×
Ness.	Person No.	Person Name	Organization	i c	Organization:	
	1	Greg Kingsley	Ness	К	Organization.	
	2	Ian Traeger	Ness	N		
Ø	3	Malcolm Turnbull	Ness	Ν		OK Cancel
	4	Pat Cash	Ness	Ν		

- 5. Input the Organization Name as desired.
- 6. Click **OK** to save the adding.
- 7. You can add multiple levels of organizations according to the actual needs.

To add sub organizations, select the parent organization and click Add.

Repeat *Step 2* and *3* to add the sub organization.

Then the added organization will be the sub-organization of the upper-level organization.

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

# Modifying and Deleting Organization

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

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

#### Notes:

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

# 7.4.2 Person Management

After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting person's information in batch, etc. *Note:* Up to 100,000 persons or cards can be added.

# Adding Person / Card

#### Steps:

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

File System View Tool Help						<u></u>	iVMS-4200		
📲 Control Panel 💭 Main View		Plave 🗸 📕	Access Control	🔥 Statı	is Monitor	l Alarm Event	🚰 Dev	vice Management	
Search Search Search Search	🕂 Add 🖄 Mo	dify 🗙 Delete 1	🕂 Change Organi	ization 📲 Impo	rt Person 📑 E	xport Person  🧏	Get Person 🔔	Add Person in Batch	📴 Issue Card in Batch
👌 Ness	Person No.	Person Name	Organization	Gender	Card Quantity	Card No.	Fingerprint Qua	Face Picture Qu   O	peration
il in the second	1	Greg Kingsley	Ness	Male	1	0001847010	0	0	8 6 8
民	1 2	Greg Kingsley Ian Traeger	Ness Ness	Male Male	1	0001847010 0002499605	0		2 6 6
<b>₽</b>	1 2 3				1 1 1		-	0	

Person No :	2		*:		
Person Name:			*		
	Male		*		
Gender:	Male	- Female	×		
Phone No.:					
Date of Birth:	2017-01-18	<u> </u>			
Place of Birth:					
Email:					
			U	pload Picture	Take Photo
	ID	Country:			
ID Type: ID No.: Job Title: On Board Date: Linked Device: Room No.: Address:				Junior High Sci 10	hool Diploma
ID No.: Job Title: On Board Date: Linked Device: Room No.:		City: Degree:			hool Dipioma

- 1. The Person No. will be generated automatically and is not editable.
- 2. Input the persons information as required. (i.e. Person name, gender, phone No., date of Birth, and email etc to suit the client's actual needs. This is database information for the customer and will work without this information)
- Click Upload Picture to select the person picture from the local PC to upload it to the client.
   Note: The picture should be in \*.jpg format.

(Optional) You can also click Take Phone to take the person's photo with the PC camera.

4. Click **OK** to finish adding.

## Adding Person (Detailed Information)

#### Steps:

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

🔀 Details	🐁 Permission 🛛	💴 Car	d 🧔 Fingerprint 🗄	Attendance Rule	
ID Type:	ID	~	Country:		
ID No.:			City:		
Job Title:			Degree:	Junior High School Diploma	~
On Board Date:	2017-01-18	<b>2</b>	Employment Duration:	10	*
Linked Device:					~
Room No.:					
Address:					
Remark:					

- 2. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.
  - Linked Device: You can bind the Intercom indoor station to the person.
     Note: If you select Analog Indoor Station in the Linked Device, the Door Station field will

display and you are required to select the door station to communicate with the analog indoor station.

- **Room No.:** You can input the room No. of the person, as used with the Apartment Intercom System..
- 3. Click **OK** to save the settings.

# Adding Person (Permission / Access Levels)

*Note:* Before Permissions can be set to a user, they first need to be set. For setting the access control permission, so they can be used, refer to *Chapter 7.6 Permission Configuration*.

Once access permissions are created, you can assign the permissions (ie. What doors the user can access during what times) to the person when adding person.

#### Steps:

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

🛞 Details 🚣 Permission 🧊 Cree	dential 🔚 Attendance Rule	1000
Permission(s) to Select	Selected Permission(s)	
🗆 demo	demo	
Level 5 (management) Doors	Full Access	
Permiter Doors Only	>>	
Full Access	>	
Floors 1-5 Only		
Staff Doors		
Floors 6-16		
	<<	
	<	1
		101/1
	OK Cancel	

 In the 'Permission(s) to Select list', all the configured permissions are displayed. Check the permission(s) checkbox(es) and click > to add to the Selected Permission(s) list. (Optional) You can click >> to add all the displayed permissions to the Selected Permission(s) list.



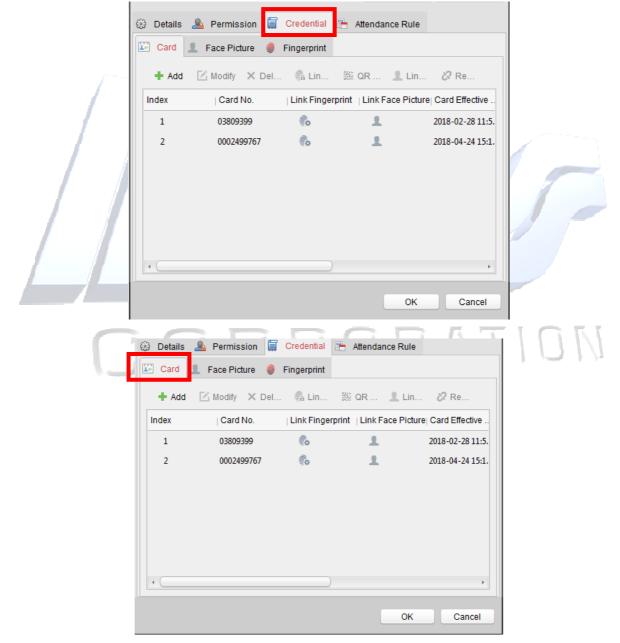
(Optional) In the Selected Permission(s) list, select the selected permission and click < to remove it. You can also click << to remove all the selected permissions.

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

# Adding Person (Card / Credential)

You can add card and issue the card to the person. *Steps:* 

1. In the Add Person interface, click **Credential** tab, then click "Card" tab to add an Access Card.



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

			Add C	ard			×	
:	General Card Smar	t Card						
:	Card Type:	Normal Card					~	
	Remark:							
:	Card Password:	Password					0	
	Effective Period:	From 2018-	04-27 1	3:48:56 📆 1	0 2028-04-2	27 13:4	8:56 📆	
		Access Co	ontro			-	Read	
:	Card Reader Mode:	O Card Enrol	llme	Set Card En	rollment Stati		Read	
		O Manually Ir	nput				Enter	
	Index	ard No.	Card	Туре	Card Class	Ca	ard Effec	
	•						Þ	
					ок	Car	icel	
						1		

- 3. Select the card type according to actual needs.
  - Normal Card
  - **Card for Disabled Person**: The door will remain open for the configured time period for the card holder.
  - **Card in Blacklist**: The card swiping action will be uploaded and the door cannot be opened.
  - **Patrol Card**: The card swiping action can used for checking the working status of the Guard Patrol. The access permission of the Guard Patrol staff is configurable.
  - **Duress Card**: The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.
  - **Super Card**: The card is valid for all the doors of the controller during the configured schedule.
  - Visitor Card: The card is assigned for visitors. For the Visitor Card, you can set the Max. Swipe Times.

#### Notes for Visitor Card:

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

	Add Card	×
General Card Smart	Card	
Card Type:	Visitor Card	~
Max. Card Swipin		
Remark:		

4. Input the password (PIN No) of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

*Note:* The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card**, **Password**, **and Fingerprint**. For details, *Chapter 7.7.2 Card Reader Authentication*.

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

Effective Period: From 201	018-02-28 10:40:21 📆 To	2028-02-28 10:40:21 📆
----------------------------	-------------------------	-----------------------

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

A card can be entered into the system in 3 different ways.

1. Via the Controllers card reader (any reader on the system)

2. Via an Enrollement reader connected via a USB port to the clients PC running iVMS4200 software. (e.g. DS-K1F180-D8E)

3. Manually entering the full card Number (e.g. 8 digits – 3 Digit Site code followed by 5 digit card No.)

• Access Controller Reader: Select "Read" and then place the card on the reader of the Access Controller to get the card No.

**Card Enrollment Station:** Select "Read" and then place the card on the Card Enrollment Station to get the card No.

*Note:* The Card Enrollment Station should connect with the PC running the client. You first need to click **Set Card Enrollment Station** to enter the following dialog to set it up before reading a card.

Card	Enrollment Station	×
Type: Connection Mode:	DS-K1F100-D8	~
Serial Port No.:	Com1	~
Baud Rate:	19200	~
Timeout after:	500	ms
Buzzing:	• Yes	No
Card No. Type:	Normal	~
M1 Card Encryption	Enable	
Sector	Selected Sectors (0/0) M	lodify
	🗆 All	
	Restore Default Value	Save

- 2) Select the Card Enrollment Station type.
- 3) *Note:* Currently, the supported card reader types include DS-K1F100-D8E and DS-K1F180-D8E
- 4) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.
- 5) If using standard 26 Bit Wiegand Cards, then set the Card No. Type to Wiegand.

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

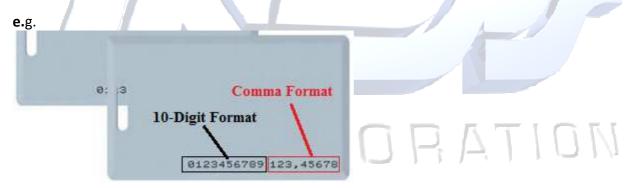
6) Click Save button to save the settings.

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

#### **Understanding Card Markings.**

Depending on the card vendor, there may be a 10 Digit Card No, 8 Digit (with comma after the first 3 digits) or both 10 and 8 Digit numbers on the card.

There are usually two sets of numbers on the 125kHz EM4100 RFID cards. Key fobs usually only have a single 10-digit or Single 8-digit number.



The number on the right, "comma format": (e.g. 123, 45678)

- This is usually the Cards **26 Bit Wiegand Number**. It consists of a 3 Digit Site Code (0-255) and then a 5 Digit Card No (0-65,535).
- According to the Wiegand 26 spec, this is the badge number in this format.

The number on the left, "10-digit format": (e.g. 0123456789)

• If the Card Reader is set to output **34 Bit Wiegand**, then often this is the associated Card No.

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

# **Adding Person (Fingerprint)**

To program Fingerprint into the system, you require a Fingerprint Registration Terminal.



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

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

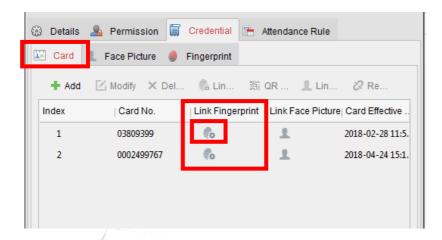
Fi	ngerprint Machine	×
Device Type:	DS-K1F820-F	~
Re	estore Default Value	Save

- 1) Select the device type: DS-K1F820-F
- Click Save button to save the settings.
   You can click Restore Default Value button to restore the default settings.
- 3. Click on the first Finger you with to register,

Details A Permission Credential	Attendance Rule			
🖾 Card 🧘 Face Picture 🧔 Fingerprint				
Collection Mode: <ul> <li>Local Collection</li> </ul>	Remote Collection			
Set Fingerprint Ma Start				
			$T$ $\Lambda$	$I \overline{I} \overline{I} \overline{I} \overline{I}$
		말님	$\Delta \Lambda$	10N
	Delete			
	Clear			
Note: Click Start to start collecting the fingerprint.				
	OK Cancel			

- 4. Click **Start** button, click to select the fingerprint to start collecting.
- 5. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.
- 6. Click **Stop** button can stop collecting.
- After collecting the fingerprint, click 'Card' in the Add Person window to enter the Card tab. You can select the registered fingerprint and click **Delete** to delete it. You can click **Clear** to clear all fingerprints.
- 8. Click **OK** to save the fingerprints.

9. Click Link Fingerprint to link the fingerprint to the card.



Select the Fingerprints you wish to link to the added card and then click "OK".

Select	Fingerprint ×	
	OK Cancel	RATION

# **Adding Person (Attendance Rule)**

You can set the attendance rule for the person.

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

Steps:

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

🛞 Details 💄 Permission 🌘	Credential 👫 Attendance Rule
Time and Attendance	
Schedule Shift by Organiza	tion
Check-in Not Required	Check-out Not Required
Effective for Overtime	Effective for Holiday
More	

2. If the person joins in the time and attendance, check the **Time and Attendance** checkbox to enable this function for the person. Then the person's card swiping records will be recorded and analyzed for time and attendance.

For details about Time and Attendance, click **More** to go to the Time and Attendance module.

- 3. Click **OK** to save the settings.
- 4. Once the person's details have been saved, if the changes affect the access to doors / readers etc, then a 'Data Synchronise' dialog box will open to allow you to download / synchronize the changes into the controller.

Data Synch	nronization ×
Data is changed. Click Apply data to the devices.Or you ca Permission interface.	y Now to apply the updated an apply it to devices later in
Apply Now	Apply Later

5. Click 'apply now' to download the changes to the controller(s)

# **Importing and Exporting Person Information**

The person information can be imported and exported in batch. *Steps:* 

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

Export Person	×
Saving Path o	
Note: The operation will export all the existing persons.	
Person No	Â
✓ Organization	
✓ Name	
✓ Gender	
✓ ID Type	
ID No	
✓ Date of Birth	
Phone No	
✓ Job Title	
✓ Address	
✓ Email	
	-
OK Car	icel

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

- 2. **Importing Person:** You can import the Excel file with persons information in batch from the local PC
  - 1) click Import Person button in the Person and Card tab.

	Import Person	×
Please select the	file to import.	
Import File:		
	Download Template for Importing Person	
	ок с	ancel

- 2) You can click **Download Template for Importing Person** to download the template first.
- 3) Input the person information to the downloaded template.
- 4) Click do select the Excel file with person information.
- 5) Click **OK** to start importing.

To bulk add cards into the system, export the file, modify it with all the card numbers you want to add and then import it into the system.

## **Getting Person Information from Access Control Device**

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

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

#### Steps:

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

	Select Device	×
Nickname	IP	
10.18.146.86	10.18.146.86	
10.16.6.112	10.16.6.112	
10.16.6.111	10.16.6.111	
Note: If the perso from the other de	on has already been added to other department, he/she will be deleted spartment.	1
	OK Cancel	5

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

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

#### Notes:

- The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- Up to 10,000 persons with up to 5 cards each can be imported.

#### **Managing Person**

#### **Modifying and Deleting Person**

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

w	🛅 Remote	Playback	Access Control	Star	tus Monitor	E Time and Attendan	ice 🔂 Face Pic	ture Compan on Alarm	💄 Alarm Ev
9	🕂 Add 🛛 🖾 M	lodify 🗙 Delete	다 Change Organ	ization 📲 Imp	ort Person 🛛 🖹 E	xport Person  🔏 Get P	erson 🛛 🤽 Add Person ir	n Batch 🛛 📑 Issue Card	in Batch
ete									
	Person No.	Person Name	Organization	Gender	Card Quantity	Card No.	Fingerprint Quantity	Face Picture Quantity	Operation
	1	Greg Kingsley	Ness	Male	2	0001847010,03809399	0	0	e é e
	3	Malcolm Turnbull	Ness	Male	1	0002499767	0	0	2 Ë B
	4	Pat Cash	Ness	Male	1	02812002	0	0	e ë E
	7	06409113	Ness	Male	1	06409113	0	0	= 🛱 B

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

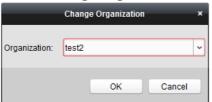
	Card Swiping Reco	ord	×
Serial No.	Event Type Card Holder	Card Type	Card No.
1	Legal Card Authe Greg Kingsle	V Normal Card	03809399
2	Legal Card Authe Greg Kingsle	V Normal Card	03809399
3	Legal Card Authe Greg Kingsle	V Normal Card	03809399
4	Legal Card Authe Greg Kingsle	/ Normal Card	03809399
5	Legal Card Authe Greg Kingsle	/ Normal Card	03809399
6	Legal Card Authe Greg Kingsle	/ Normal Card	03809399

To delete the person, select a person and click **Delete** to delete it. *Note:* If a card is issued to the current person, the linkage will be invalid after the person is deleted.

# **Changing Person to Other Organization**

You can move the person to another organization if needed. *Steps:* 

1. Select the person in the list and click Change Organization button.



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

# **Issuing Card in Batch**

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

- 1. Click **Issue Card in Batch** button to enter the following dialog.
  - All the added person with no card issued will display in the Person(s) with No Card Issued list.

		rd in Batch	×	
Card Type:	Normal Card		~	
Card Password:				
Card Quantity:	1		* *	
Effective Period:	From 2017-01-18 🔂 To 20	27-01-18 📆		
	Access Controller Reader			
Card Reader Mode:	Card Enrollment Station	Set Card Enrollment Station	Read	
	Manually Input		Enter	
Person(s) with No Car	dissued	Person(s) with Card Issued		
Person Name Ge	nder Department	Person Name Card No.	Gender   Departn	
Wendy Fen Cindy Fen	aale Department 1 Nale Department 1/Sub Depar			5
			OK Cancel	

- Select the card type according to actual needs.
   *Note:* For details about the card type, refer to *Adding Person*.
- 3. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

*Note:* The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card**, **Password**, **and Fingerprint**. For details, refer to *Chapter* 7.7.2 Card Reader Authentication.

- 4. Input the card quantity issued for each person.
  - For example, if the Card Quantity is 3, you can read or enter three card No. for each person.
- 5. Click 🖾 to set the effective time and expiry time of the card.
- 6. Select the Card Reader Mode for reading the card No.
  - Access Controller Reader: Place the card on the reader of the Access Controller and click Read to get the card No.
  - **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.

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

Card Enrollment Station ×	
Type: Connection Mode: Timeout after:	DS-K1F100-D8 v USB 500 ms
Buzzing: Card No. Type:	Yes No Normal
Restore	Default Value Save

- 1) Select the Card Enrollment Station type.
- 2) Currently, the supported card reader types include DS-K1F100-D8E and DS-K1F180-D8E
- Set the parameters about the connected card enrollment station. If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check Enable checkbox of M1 Card Encryption and click Modify to select the sector.
- 4) Click Save button to save the settings.You can click Restore Default Value button to restore the defaults.
- Manually Input: Input the card No. and click Enter to input the card No.
- 7. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.
- 8. Click **OK** to save the settings.

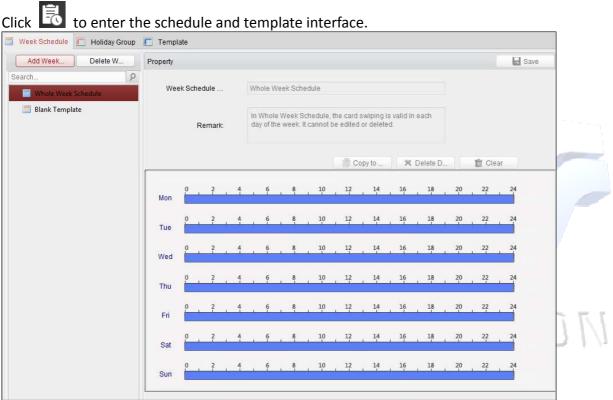
# CORPORATION

## 7.5 Schedule and Template

#### Purpose:

Schedules allow you to set what times and day's events will occur. E.g. Door Auto unlocking, what times card holder can access doors etc.

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



You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, please refer to *Chapter 7.6 Permission Configuration*.

#### 7.5.1 Week Schedule

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

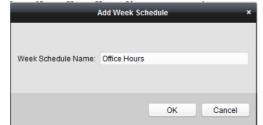
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

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

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

#### Steps:

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



- 2. Input a name of week schedule (e.g. Office Access Hours) and click **OK** button to add the week schedule.
- 3. Select the 'added week schedule' in the schedule list and you can view its property on the right.

You can edit the week schedule name and input the remark / comment information for future reference.

4. On the week schedule, click and drag on a day to draw on the schedule, which means in

that period of time, the configured permission is activated.

	Week Schedule 📄 Holiday Group	Template			
	Add Week Delete W	Property			
	Search 9	Week Schedule Office Hou	rs		
/	Office Hours	Remark	🍵 Copy to 🗶 Delete D 💼 Clear		
		Mon 0, 2, 4, 6,	8         10         12         14         16         18         20         22           8         10         12         14         16         18         20         22           8         10         12         14         16         18         20         22	24	
		Wed		-	
		Thu 0, 2, 4, 6, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,	*         10         12         14         16         18         20         22         .           *         .10         .12         .14         .16         .18         .20         .22         .		TIONT
g.		Sat 0, 2, 4, 6,	\$ , 10 , 12 , 14 , 16 , 18 , 20 , 27 ,		ゲーロル

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

5. When the cursor turns to X, you can move the selected time bar you just edited. You can

also edit the displayed time point to set the accurate time period. When the cursor turns to 😥, you can lengthen or shorten the selected time bar.

- Optionally, you can select the schedule time bar, and then click **Delete Duration** to delete the selected time bar, or click **Clear** to delete all the time bars, or click **Copy to Week** to copy the time bar settings to the whole week.
- 7. Click **Save** to save the settings.

#### 7.5.2 Holiday Group

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

Add Holi Delete H	Property						Save	e
Holiday Group 1		/ Group: Holi Remark:	day Group 1					
	Holiday Lis				+ Add Holiday	Prev Page	▶ Next Page	
	Index 1	Start Date	End Date	Duration	6 8 10 12 14	16 18 20 22 2	Operation	
								F 5

#### Steps:

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

Add Holiday Group 🗙 🖉	
Holiday Group Name: Christmas Period	
OK Cancel	MUHA

- 2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.
- 3. Select the added holiday group and you can edit the holiday group name and input the remark information.
- 4. Click **Add Holiday** icon on the right to add a holiday period to the holiday list and configure the duration of the holiday.

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

Holiday List						+ Add	Holiday		Prev P	age	►	Ne)	t Page
Serial No.	Start Date		End Date		Duration						Opera	ation	
1	3/9/2016	<b>2</b>	3/9/2016	<b>1</b>	0 2 4 6	8 10	12 14	16 18	20	22 24	83	Ô	×
2	3/23/2016	<u></u>	3/31/2016	<u></u>	0 2 4 6	8 10	12 14	16 18	20	22 24	83	Ô	×

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

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

- 2) When the cursor turns to 🕅, you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
- 3) When the cursor turns to 🖼, you can lengthen or shorten the selected time bar.
- 4) Optionally, you can select the schedule time bar, and then click <sup>i</sup>≤ to delete the selected time bar, or click <sup>i</sup>≡ to delete all the time bars of the holiday, or click <sup>i</sup>≤ to delete the holiday directly.
- 5. Click **Save** to save the settings.

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

#### 7.5.3 Template

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

*Note:* The priority of holiday group schedule is higher than the week schedule. Click **Template** tab to enter the Template Management interface.

Add Temp Delete T	Propeny 🛃 Save	
Search P	Template Name: Template 1	1011
Blank Template     Template 1	Remark:	101
	Week Schedule E Holiday Group	
	Week Schedule v + Add Week	
	Mon 0 2 4 6 8 10 12 14 16 18 20 22 24	
	0 2 4 6 8 10 12 14 16 18 20 22 24 Tue	
	Ved 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	
	0 2 4 6 8 10 12 14 16 18 20 22 24 Thu	
	0 2 4 6 8 10 12 14 16 18 20 22 24 Fri	
	0 2 4 6 8 10 12 14 16 18 20 22 24 Sat	
	0 2 4 6 8 10 12 14 16 18 20 22 24 Sun	

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

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

You can define custom templates on your demand.

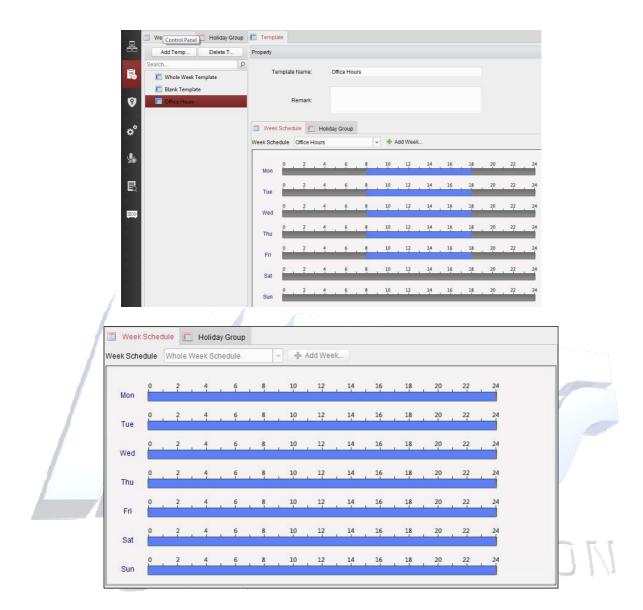
#### Steps:

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

	Control Panel 🔂 Main View	E Remote Playback	Access Control	5 Status Monitor	🧁 Time and A	
-	📃 Week Schedule 🔲 Holiday Group	Template				
몲	Add Temp Delete T	Property				
R	Search 9	Template Name:	Blank Template			
0	Blank Template	Remark:		wiping is invalid in each day of y schedule. It cannot be edited		
°		Week Schedule Ho Week Schedule Blank Templ	late - Add	I Week		
			Add Wool	12 14 16 18	20 22	
		Weeks	Schedule Name: Office Ho			-1-
				ок с	ancel	1
					1	

- 2. Input the template name (for future use that makes easier reference in the future) in the text field and click **OK** button to add the template.
- 3. Select the added template (from the left hand window) and you can edit its property on the right. You can edit the template name and input the remark information.
- Select a week schedule to apply to the schedule.
   Click Week Schedule tab and select a schedule in the dropdown list.

File System View Tool Help		
📰 Control Panel 🛛 👼 Main Vier /	🛅 Remote Playback	Access Control
📕 🗂 Week Schedule 🔳 Holiday Goup	Template	
Add Temp Delete T	Property	
Search	Template Name:	Office Hours
Image: Office Hours	Remark:	
o°	🔲 Week Schedule 🔲 Ho	oliday Group
	Week Schedule Whole Week	K Schedule 🔍 🖡 Add Week
<b>S</b>	0 Mon	late 12



You can also click **+ Add Week Schedule** to add a new week schedule. For details, refer to *Chapter 7.5.1 Week Schedule*.

5. Select holiday groups to apply to the schedule. *Note:* Up to 4 holiday groups can be added.

Control Panel edule 🗾 Holiday Group	Template				
Add Temp Delete T	Property				
Search 9	Template Name:	Office Hours			
Office Hours	Remark:				
•	Week Schedule Holiday Group to Select	loliday Group	Selected Index	Holiday Group   Holiday Group Name	Remark
	Search Christmas Period	2	1	Christmas Period	Covers Xmas Day, Box
		2	1	Christmas Period	Covers Xmas Day, Box
		Add	1	Christmas Period	Covers Xmas Day, Box

Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one from this screen. For details, refer to *Chapter 5 When the* cursor turns to [1, 1], you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period. When the cursor turns to [1, 2], you can lengthen or shorten the selected time bar.

- Optionally, you can select the schedule time bar, and then click **Delete Duration** to delete the selected time bar, or click **Clear** to delete all the time bars, or click **Copy to Week** to copy the time bar settings to the whole week.
- 9. Click **Save** to save the settings.

Holiday Group.

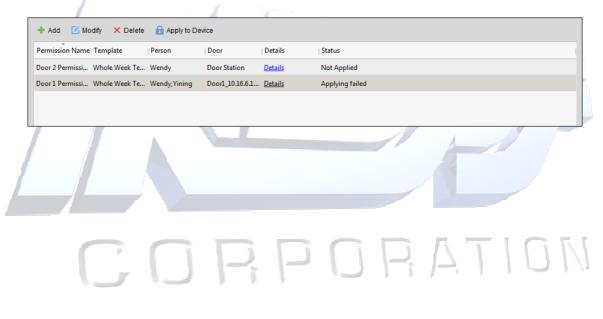
You can click to select an added holiday group in the right-side list and click **Delete** to delete it. You can click **Clear** to delete all the added holiday groups.

6. Click Save button to save the settings.

### 7.6 Permission Configuration

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

Click icon to enter the Access Control Permission interface.



#### 7.6.1 Adding Permission

Purpose:

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

Steps:

1. Click Add icon to enter following interface.

			Add Perm	ssion	*
Permis	nission Name:	Office Doors			
Templ	iplate:	Office Hours	~	Add Template	
/ Persor	on			Selected Personel(1)	
Searc	arch		9	Search	8
	🖲 愶 Ness		Ô	Person Name Organization	
	Carego Ca	olm Turnbull Cash sine Sharp	<	Lorraine Sharp Ness	
Access	ess Control Poin	t/Device		Selected Door/Device(0)	
Searc			9	Search	9
E	<ul> <li>Lift Inter</li> <li>Ness</li> <li>All Acce</li> <li>Main and All Acce</li> </ul>		) ,	Access Contro   Door Group	
	200 000 000 000 000	2_DS-K2604 (L) 3_DS-K2604 (L)	*		
				OK Can	cel
C		iD		NGN	$\pi n T$

- 2. In the Permission Name field, input the name for the permission as desired.
- Click on the dropdown menu to select a template for the permission. (e.g. Office Hours)
   Note: You should configure the Schedule Template before permission settings. You can click
   Add Template button from this screen to add the template. Refer to Chapter 7.5 Schedule and
   Template for details.

In the Person list, all the added persons are displayed. Select the persons for this Permission Group.

*Note:* Once Permissions are added, you can also assign the persons to their permissions from the Add / Modify persons Card section. Refer to *Chapter <u>7.5.2</u> <u>Adding Person (Permission / Access Levels)</u> for details.* 

- 4. Check the checkbox(s) to select person(s) and click > to add to the Selected Person list.(Optional) You can select the person in Selected Person list and click < to cancel the selection.</li>
- 5. In the Access Control Point/Device list, all the added access control points (doors) and door stations will display.

Check the checkbox(s) to select door(s) or door station(s) the person(s) will have access to and click > to add to the selected list.

(Optional) You can select the door or door station in the selected list and click < to cancel the selection.

- 6. Click **OK** button to complete the permission adding. The selected person will have the permission to enter/exit the selected door/door station with their linked card(s).
- 7. (Optional) after adding the permission, you can click **Details** to modify it. Or you can select the permission and click **Modify** to modify.

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

#### 7.6.2 Applying Permission

#### Purpose:

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

#### Steps:

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

ter	ings Progress:	Applie	d (100%)	
-				100%
ilter				
Permission	Progress	Result		
1	100%	Applied		

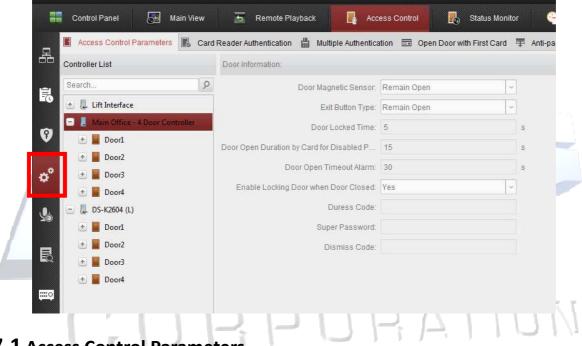
## 7.7 Advanced Functions

#### Purpose:

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

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

## Click click



7.7.1 Access Control Parameters

#### Purpose:

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

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

#### **Door Parameters**

Steps:

1. In the controller list on the left, click  $\blacksquare$  to expand the access control device, select the door

(access control point) and you can edit the information of the selected door on the right.

Access Control Parameters Card F	Reader Authentication 🎽 Multiple Authenticati	on 📰 Open Door with First Card	Anti-Passbac
Controller List	Door Information:		
Search	Door Magnetic Sensor:	Remain Closed	~
🛨 🛃 DS-K2604 (L)	Exit Button Type:	Remain Open	~
Access Demo Case	Door Locked Time:	5	s
Toor1	Door Open Duration by Card for Disabled P	15	s
🖈 📕 Door2	Door Open Timeout Alarm:	30	s
* <b>E</b> Door3	Enable Locking Door when Door Closed:	Yes	~
🔔 📓 Door	Duress Code:		
Alarm Output2	Super Password:		
👃 Alarm Output3	Dismiss Code:		
🍌 Alarm Output4		Status Duration Settings	
🕍 Zone1			
Zone2			
🞽 Zone3			
<ul> <li>Zone4</li> <li>Lift Interface</li> </ul>			

2. You can editing the following parameters:

**Door Magnetic**: (reed switch for monitoring the state (open/close) of the door. When using door monitoring with a N/C Reed Switch, then select '**Remain Closed'**. If not monitoring the state of the door with a N/C Reed switch then have it set to "**Remain Open**" (Normally Open condition).

**Exit Button Type**: Sets the "Request to Exit Button Type" : If the exit button has a Normally Open contact then set this to "**Remain Open**" and if it uses a Normally Closed contact then set this to "**Remain Close**".

**Door Locked Time**: This is the time the door lock Output will stay activated for (Door unlocked for) after a valid Card read.

**Door Open Duration by Card for Disabled Person:** This is the time the door lock Output will stay activated for (Door unlocked for) after a valid Card read by a user assigned as disabled.

**Door Open Timeout Alarm**: The alarm can be triggered if the door has not been closed (i.e. Door open too long). The time set here sets how long the door can remain opened for after a valid card read, or Request to Exit button activation before the door open timeout alarm will activate.

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

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

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

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

#### Notes:

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

#### AUTO UNLOCKING OF DOORS

#### Purpose:

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

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

Access Control Parameters 🔣 Card I	Reader Authentication 📲 Multiple Authenticati	on 📰 Open Door with First Card	ŧ	Anti-Passba
Controller List	Door Information:			
Search	Door Magnetic Sensor:	Remain Closed	~	
🖭 📜 DS-K2604 (L)	Exit Button Type:	Remain Open	~	
😑 📮 Access Demo Case	Door Locked Time:	5		S
Doorl     Entrance Card Reader1	Door Open Duration by Card for Disabled P	15		s
Exit Card Reader2	Door Open Timeout Alarm:	30		s
🖃 📕 Door2	Enable Locking Door when Door Closed:	Yes	~	
📲 Warehouse Entry Door	Duress Code:			
Tait Card Reader4	Super Password:			
🖃 📓 Door3	Dismiss Code:			
* Entrance Card Reader5		Status Duration Settings		1
Tait Card Reader6				•
🖃 📕 Door4				

#### Steps:

- 1. Click to select a door from the access control device list on the left.
- 2. On the Door Status Configuration panel on the right, draw a schedule for the selected door.
  - A. Select a door status brush as Remain Open or Remain Closed.
    - a.**Remain Open**: The door will keep open during the configured time period. The brush is marked as \_\_\_\_\_.
    - b. **Remain Closed**: The door will keep closed during the configured duration. The brush is marked as \_\_\_\_\_.

NOTE: Use "Remain Closed" with caution. During the 'Remain Closed times (if programmed) the door will be in 'lock down' mode and Cards will also not work during this time. Unless 'lock down' operations is required, we recommend only use time in the 'Remain Open' time to Auto Unlock the door and outside these times the door will auto relock.

Remai	n Ope	n	•	Re	mair	n Clo	sed		E) Co	opy to	Who	ole We	ek	×	Delete I	Dura	tion	Û	Cle	ar		H Save
Mon	0	i.	2	x	4	x	6	-i	8	10	),	12	i	14	16	i.	18		20	22	e ,	24
Tue	0	i	2	a	4	Ĵ.	6	i.	8	10	)	12	i	14	16	4	18		20	22		24
Wed	0	i	2	x	4	Ĵ.	6	i.	8	10	) ,	12	i	14	16	a	18		20	22		24
Thu	0	i	2	-i	4	Ĵ.	6	ï.	8	10	) ,	12	i	14	16	-1	18		20	22		24
Fri	0		2	a.	4	÷	6	a.	8	10	) ,	12	i	14	16	ï	18		20	22		24
Sat	0		2	ĩ	4	i	6	x	8	10	)	12		14	16	ī	18		20	22		24
	0		2		4		6		8	10	)	12		14	16		18		20	22		24

B. Click and drag on the timeline to draw a colour bar on the schedule to set the duration.

- C. When the cursor turns to X, you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period. When the cursor turns to X, you can lengthen or shorten the selected time bar.
- 3. Optionally, you can select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
- 4. You can select the time bar and click **Delete Duration** to delete the time period. Or you can click **Clear** to clear all configured durations on the schedule.
- 5. Click Save to save the settings.
- 6. You can click **Copy to** button to copy the schedule to other doors.
- 7. Click Save button to save parameters.

Note: You can also set the auto unlock time to be disabled until the 'First Card' has been used at the premises. This will prevent doors being auto unlocked if no staff member is onsite. Refer 'First Card' feature on page 88.

#### **Card Reader Parameters**

#### Steps:

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

Controller List	Card Reader Information:		
Search P	Basic Information		
🛨 👢 DS-K2604 (L)	Nickname:	Front Door	
😑 📮 Access Demo Case	Enable Card Reader:	Yes	~
😑 📕 Door1	OK LED Polarity:	Anode	~
Entrance Gard Reader1	Error LED Polarity:	Anode	~
The Exit Card Reader2	Buzzer Polarity:	Anode	~
Door2 Warehouse Entry Door	Minimum Card Swiping Interval:	0	
Warehouse Entry Door     Exit Card Reader4	Max. Interval When Inputting Password:	10	
🖃 📕 Door3	Enable Failed Attempts Limit of Card Readi	No	÷
Trance Card Reader5	Max. Times of Card Swiping Failure:	5	
Tit Card Reader6	Enable Tampering Detection:	No	×
🖃 📕 Door4	Detect When Card Reader is Offline for:	0	
📲 Entrance Card Reader7	Buzzing Time:	10	
The Exit Card Reader8	Card Reader Type:		
🎄 Alarm Output1 🏂 Alarm Output2	Card Reader Description:	DS-K1104M/MK build20170428	
🍒 Alarm Output3	Fingerprint	P2 1	
🍰 Alarm Output4	Fingerprint Recognition Level:	Low	~

2. You can editing the following parameters:

Nickname: Edit the card reader name as desired. (e.g. Front Door Entry Reader) Enable Card Reader: Select Yes to enable the card reader. OK LED Polarity: Select the OK LED Polarity of the card reader main board. Error LED Polarity: Select the Error LED Polarity of the card reader main board. Buzzer Polarity: Select the Buzzer LED Polarity of the card reader main board. Minimum Card Swiping Interval: This sets the minimum time between card Reads. If a card is read after another less than this set time, the card swiping is invalid. You can set it as 0 to 255. Max. Interval When Inputting Password: When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

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

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

**Enable Tampering Detection:** Enable the anti-tamper detection for the card reader. (Used with RS485 Readers)

**Detect When Card Reader is Offline for:** When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically. (Used with RS485 Readers).

Fingerprint Recongnition Level: Sets the Fingerprint level for when Fingerprint readers are used.

**Card Reader Type:** If a RS485 reader is used, this filed will automatically be filled by the system showing the type of reader.

Card Reader Description: If a RS485 reader is used, this filed will automatically be filled by the

system showing the description of the reader.

Buzzer Time: sets how long the reader buzzer will pulse for if programmed to pulse.

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

#### 7.7.2 Card Reader Authentication

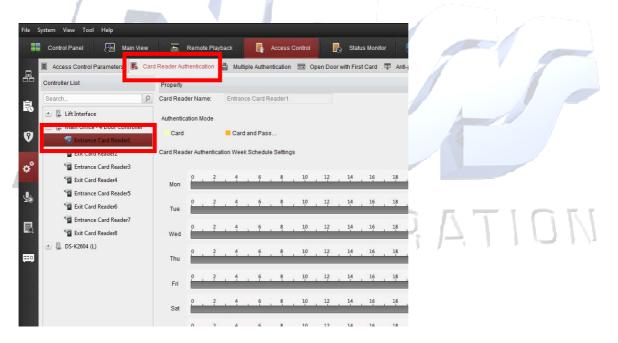
#### Purpose:

You can set what credential is required and during what time for access to be granted.

E.g. Card only during office hours and Card AND Code after hours. This is set for each controller entry point.

Steps:

1. Click Card Reader Authentication tab and select a reader on the left.



2. Select a card reader authentication mode. The available authentication modes depend on the card reader type:

To see what available options you have for the selected Controller and Reader, click on 'Configure' on the top right of the screen.

Control Panel 🛛 👧 Main View	🚡 Remote Playl	back 🔡 Access Control	🛃 Status Monitor	Face Picture Comparison Alarm	Device Management				
Control Panel Control Parameters	d Reader Authentication	Multiple Authentication 📅 Ope	n Door with First Card 🛛 Ŧ	Anti-passing Back 💠 Cross-Controller Ar	ti-passing Back 🍈 Multi-door Interloci	ding IIII Authentication Password 🔃 Re	elay Settings 🗔 Custom Wiegand	🏂 Blacklist	
Controller List	Property							📄 Copy to	B Save
Search P	Card Reader Name:	Entrance Card Reader1							
🐮 🛃 Lift Interface	Authentication Mode	Card and Pass						ß	Configuration
Entrance Card Reader1	Card Reader Authentica	tion Week Schedule Settings					🗐 Copy to Week	X Delete	🂼 Clear
<ul> <li>Entrance Card Readers</li> <li>Exit Card Reader4</li> <li>Entrance Card Reader5</li> </ul>	Mon 2	, 4 , 6 , 8 , 10 ,	12 14 16 1	18 20 22 24					

All available options for your Controller and Reader will be displayed on the left hand window in the 'Selectable Mode' column. Select the option you want to use from the 'Selectable Mode'

column and then select click on the

to add them to the 'Selected Mode'.

Configure Card Re	eader A	uthentication Mode	×
Selectable Mode:		Selected Mode:	
Card		Card	$\uparrow \downarrow$
Card and Password	<b>&gt;</b>	Card and Password	$\uparrow \downarrow$
	<i>«</i>		
		Oł	Cancel

Once selected, you can then set them in the required order they will appear in the settings page by using the up and down arrows options.

thentication Mode										
Selected Mode:							2			
Card	$\uparrow$	$\downarrow$			0		5	 1.0		17
Card and Password	$\uparrow$	$\downarrow$	4	P	U	F	Þ.		U	1/1

Controller List	Property																			
Search 9	Card Rea	der Nar	me:	Er	ntran	ce Ca	ard F	Read	der1											
	Authentic Card	ation M	ode		Card	and	Pas	s												
📲 Exit Card Reader2	Card Read	der Autl	nentica	ation	Weel	k Sch	edu	le S	ettin	gs										
📲 Entrance Card Reader3																				
📲 Exit Card Reader4	Mon	0	2	- d	4		6	1	8	1	10	öl.	12	öl.	14		16		18	
📲 Entrance Card Reader5		_	2				6				10		12		14		16		10	Ī
📲 Exit Card Reader6	Tue	Ě	Ĩ	-	7	a 2	P	1	Ŷ	-	10	24	12	24	14		10	24	10	
👕 Entrance Card Reader7 👕 Exit Card Reader8	Wed	0	2		4		6		8	a	10		12	-	14	-	16		18	
🛨 📜 DS-K2604 (L)	Thu	0	2	a	4		6	j.	8	j.	10	j.	12	à	14		16	j.	18	
	Fri	0	2		4		6	3	8	а	10		12	a	14	3	16	-11	18	

They will then display in the order you selected.

The following possible options are dependent on the Controller and Reader you have.

- Card: The door can be unlocked by presenting a Valid Card only.
- **Card and Password**: The door can open by both inputting the card password and swiping the card.

*Note:* Here the password refers to the password set when issuing the card to the person. *Chapter 4 In the* organization list on the left, you should add a top organization as the parent organization of all organizations.

Click Add button to pop up the adding organization interface.

ile System View Tool Help					
📰 Control Panel 🔝 Main View	🔚 Remo	e Playback 🛛 📕	Access Control		
Control Panel 9	🕂 Add 🛛 🖄	Modify X Delete	Change Organ	izal	Add Organization ×
🙃 🕂 Add 🛛 🗹 Modify 🛛 🗙 Delete					-
ness.	Person No.	Person Name	Organization	( C	Organization:
8	1	Greg Kingsley	Ness	Л	
	2	Ian Traeger	Ness	N	
2	3	Malcolm Turnbull	Ness	N	OK Cancel
	4	Pat Cash	Ness	N	

- 8. Input the Organization Name as desired.
- 9. Click **OK** to save the adding.
- 10. You can add multiple levels of organizations according to the actual needs.

To add sub organizations, select the parent organization and click Add.

Repeat Step 2 and 3 to add the sub organization.

Then the added organization will be the sub-organization of the upper-level organization.

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

#### Modifying and Deleting Organization

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

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

#### Notes:

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

Person Management.

• **Card or Authentication Password**: The door can open by inputting the authentication password (PIN ONLY) or swiping the card.

*Note:* Here the authentication password refers to the password set to open the door. Refer to *Chapter 7.7.8 Authentication Password*.

- **Fingerprint**: The door can open by only inputting the fingerprint.
- **Card or Fingerprint:** The door can open by inputting the fingerprint or swiping the card.
- **Password and Fingerprint**: The door can open by both inputting the card password and inputting the fingerprint.

*Note:* Here the password refers to the card password set when issuing the card to the person. Refer to *Chapter 4 In the* organization list on the left, you should add a top organization as the parent organization of all organizations.

Click Add button to pop up the adding organization interface.

File System View Tool Help Control Panel 🔂 Main View	🛅 Remot	e Playback	Access Control	2	TΑ	10N
Control Panel 9	🕂 Add 🛛	Modify X Delete	Change Orga	ilzal	Ac	ld Organization ×
Ness.	Person No.	Person Name	Organization	C	0	
鼠	1	Greg Kingsley	Ness	Ν	Organization:	J
	2	Ian Traeger	Ness	N		
0	3	Malcolm Turnbull	Ness	А		OK Cancel
	4	Pat Cash	Ness	N		

- 11. Input the Organization Name as desired.
- 12. Click **OK** to save the adding.
- You can add multiple levels of organizations according to the actual needs. To add sub organizations, select the parent organization and click Add.

Repeat Step 2 and 3 to add the sub organization.

Then the added organization will be the sub-organization of the upper-level organization.

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

#### Modifying and Deleting Organization

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

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

#### Notes:

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

Person Management.

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

*Note:* Here the password refers to the card password set when issuing the card to the person. Refer to *Chapter 4 In the* organization list on the left, you should add a top organization as the parent organization of all organizations.

Click Add button to pop up the adding organization interface.

Control Panel	Main View	🚡 Remot	te Playback	Change Orga	1721		
🛉 Add 🛛 🔀 Modify	× Delete		mouly A Delete	- onange orga		Ac	ld Organization
Ness		Person No.	Person Name	Organization	IC	0	1
		1	Greg Kingsley	Ness	K	Organization:	
		2	Ian Traeger	Ness	N		
		3	Malcolm Turnbull	Ness	N		OK Cancel
		4	Pat Cash	Ness	N		

- 14. Input the Organization Name as desired.
- 15. Click **OK** to save the adding.
- 16. You can add multiple levels of organizations according to the actual needs.

To add sub organizations, select the parent organization and click **Add**. Repeat *Step 2* and *3* to add the sub organization.

Then the added organization will be the sub-organization of the upper-level organization.

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

#### Modifying and Deleting Organization

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

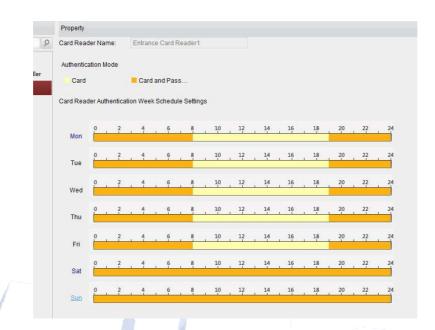
You can select an organization, and click **Delete** button to delete it.

Notes:

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

Person Management.

3. Select the required method for unlocking the door lock and then "click and drag" your mouse on a day to draw a color bar on the schedule. The 'drawn / selected' hours means in that period of time, the card reader authentication is valid. e.g.



Repeat the above step to set other time periods.
 Or you can select a configured day and click **Copy to Week** button (from the top right of the window) to copy the same settings to the whole week.

(Optional) You can click **Delete** button to delete the selected time period or click **Clear** button to delete all the configured time periods.

Property			🛱 Copy to	Save
Card Reader Name:	Entrance Card Reader1			
Authentication Mode			R	Configuration
Card	Card and Pass			
Card Reader Authen	ication Week Schedule Settings		Copy to Week X Delete	💼 Clear
			Copy to Week	
Mon		20 22 24		
Tue	rd and Pa 00:00 0 0 000 000 0000 0000 00000000	20 22 24		
Wed	2 4 6 8 10 12 14 16 18	20 22 24		
Thu 0	2 4 6 8 10 12 14 16 18	20 22 24		
Fri D	2 4 6 8 10 12 14 16 18	20 22 24		

(Optional) You can click **Delete** button to delete the selected time period or click **Clear** button to delete all the configured time periods.

5. (Optional) Click **Copy to** button to copy the settings to other card readers.

			Select Card Reader ×
			Select Card Reader to Copy to:
			Search
	Copy to	Save	- 10.7.39.120
	El cobj to	C Cure	10.7.39.120_Door1
			10.7.39.120_Reader Out2
			- 10.7.39.120_Door2
			10.7.39.120_Reader In3
	2	Configuration	10.7.39.120_Reader Out4
			- 10.7.39.120_Door3
			10.7.39.120_Reader In5
			10.7.39.120_Reader Out6
	V Duluk	- 01	10.7.39.120_Door4
py to Week	× Delete	💼 Clear	10.7.39.120_Reader In7
			10.7.39.120_Reader Out8
			OK Cancel

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

#### 7.7.3 Multiple Authentication

#### Purpose:

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

*Note:* Please set the card permission and apply the permission setting to the access control device first. For details, refer to Chapter 7.6 Permission Configuration.

#### Steps:

earch p	+ Add Card Group Nar Card Group 1		X Delete ive Period 01-09 00:00:00 to 2017-01-09		rd Group Member ing	Details <u>Details</u>
	· · · · · · · · · · · · · · · · · · ·				•	
d 10166111	Card Group 1	2017-0	01-09 00:00:00 to 2017-01-0	9 00:00:00 Yin	ing	<u>Details</u>
	Set Authenticati	on Group	× Delete			
	Linked Door	Template	Authentication Type	Offline Authentication	Authentication Group	Details

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

3. In the Set Card Group panel on the right, click **Add** button to pop up the following dialog:

	Add		×
Card Group Name			
Effective Period	2017-01-12 00:00:00	2017-01-12 23:59:59	
Card Group Member	- Vining		
	12345667		
		OK Cancel	
1) In the Card Group Name field,	input the name	o for the group as	desired
1) In the Card Group Name field,	input the name	e ioi the group as (	Jesireu.

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

P		Add	×
۶l	Access Control Point: D	oor1 ~	
		hole Week Template 🗸 🗸	
	Authentication Type: Lo	ocal Authentication ~	
	Offline Authentication:	Enable Super Password W	
	Group3		Group1 1
		+	Group2 2
		×	
		•	
		•	
		Remark:Follow the configured order to swipe the card to authenticate	
			• •
			OK Cancel

- 1) Select the access control point (door) of the device for multiple authentications.
- 2) Input the time interval for card swiping.

- 3) Select the template of the authentication group from the dropdown list. For details about setting the template, refer to *Chapter 7.5 Schedule and Template*.
- 4) Select the authentication type of the authentication group from the dropdown list.
  - Local Authentication: Authentication by the access control device.
  - Local Authentication and Remotely Open Door: Authentication by the access control device and by the client.

For Local Authentication and Remotely Open Door type, you can check the checkbox to enable the super password authentication when the access control device is disconnected with the client.

- Local Authentication and Super Password: Authentication by the access control device and by the super password.
- 5) In the list on the left, the added card group will display. You can click the card group and click ±/ to add the group to the authentication group.

You can click the added card group and click imes to remove it from the authentication group.

You can also click 🧕 or 🔮 to set the card swiping order.

- Input the Card Swiping Times for the selected card group. Notes:
  - The Card Swiping Times should be larger than 0 and smaller than the added card quantity in the card group.
  - The upper limit of Card Swiping Times is 16.
- 6) Click **OK** to save the settings.
- 5. Click **Save** to save and take effect of the new settings.

#### Notes:

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

#### 7.7.4 Open Door with First Card

#### Purpose:

'Open Door with First Card' has two features associated with it.

- 1. You can use this feature to disable the 'Auto Unlocking' of door from occurring until the First Card is used at that door.
- 2. You can set multiple first cards for one access control point (Door). After the first card is presented to the programmed reader, it allows multiple persons access through this control door point or other authentication actions.

The first card mode contains Remain Open with First Card or Disable Remain Open with First Card.

#### Option 1 – Disabling / Postpone 'auto unlocking' of doors

If you select a Door(s) to 'Remain Open with First Card' but do not assign any Cards (i.e. No card in the 'first Card list', then this feature will be used to 'postpone Auto Unlocking of the door until any user uses their card at the door.

	Access Control Para eters 🖪 Ca	rd Reader Authentication	Multiple Authentication 📴 Ope	n Do	oor with First Card	T Anti-Passback	(串)	Cross-Controller Anti-passin				
롦	Controller List	Door Open by First Ca	Door Open by First Card Parameters									
R	Search	Access Control Point	First Card Mode		Remain Open Dura	tion (mins)						
	Access Demo Case	Door1	Remain Open with First Card	~	10							
9		Door2	Disable Remain Open with	. 👻	10							
V		Door3	Disable Remain Open with	~	10							
		Door4	Disable Remain Open with	.   ~	10							
¢°		First Card List										
		Add × D	Pelete									
\$		Card No.	Person Name Effective Da	ite	Ex	cpiry Date						
EQ												
						1 1	7					

**Example.** If the door is programmed to Auto Unlock 9:00 am – 5:00 pm Mon-Fri (See Door Parameters 'Auto Unlocking of Doors' Page 77), but no one is onsite, i.e has not presented their card first at the door to be Auto Unlocked, then the auto Unlocking will be postponed / disabled until a valid card is first presented to the door to be auto unlocked.

If you wish to cancel / lock an Auto Unlocked door at any time with the above programmed, (e.g. Relock an Auto Unlocked door then a valid user can present their card 3 times within 5 seconds and the door will relock).

Note: the 'Remain Open duration' times are ignored if no cards are added to the 'First Card List'

#### Option 2 – Remain Open by User

**Remain Open with First Card:** When a Card(s) / User is assigned / added to the 'First Card List' (as shown below) the door remains open for the configured time duration after the first card is presented until 'the remain open duration' expires.



**Example.** User arrives in the morning and presents his valid card at the door reader. The door them remains unlocked for the time programmed in the 'Remain Open Duration (Mins)' time. (e.g. 8 hours). At the expiry of this time (or if a card in the 'First Card List' is used again) the door will relock.

#### Notes:

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

#### 7.7.5 Anti-Passing Back

#### Purpose:

You can set anti-passing back for card readers in the same access controller.

Anti-Passback prevents a card from "being passed back" for the same card to be used again at the same reader until it has been used a reader programmed for exiting the area. (e.g. Prevent a card from being used at a car park Entry Reader and then pass the card back to another person to allow them access. The card will be denied access when tried to be used a second time until it is used at an exit reader)

#### Notes:

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

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

#### Steps:

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

Controller List		Property							
Search	9								
👢 Main Office - 4 Do	or Controller	Controller Name:	DS-K2604 (L)						
L DS-K2604 (L)		First Card Read	Disable	~					
<b>\</b>		Index   Card En	rollment Station	Card Reader Afterward					
		1 Entrance	Card Reader1	Entrance Card Reader3					
		2 Exit Card	l Reader2						
I \		3 Entrance	Card Reader3	Entrance Card Reader1					
۱ <i>۱</i>	<b>`</b>	4 Exit Card	l Reader4						
	$\backslash$	5 Entrance	e Card Reader5						
	$\backslash$	6 Exit Card	l Reader6						
		7 Entrance	Card Reader7						
	\	8 Exit Card	Reader8						

- Select an access control device from the device list on the left.
   Note: Not all controllers support Anti-Passback feature. E.g. It is not supported in the DS-K2800 series.
- 3. In the First Card Read... field, leave this as disable.

4. In 'Card Enrolment Station' List, select the reader that will register the person into an Area when their card is first presented (e.g. Into the Car Park). Then in the 'Card Reader Afterward' select from the dialog box the card reader(s) that is required to be used to register the person 'out' of the area (e.g. Out of the Car Park). You will need to also select the same reader from the ''Card Enrolment Station' and select its "matching" reader to toggle out of the area.

**Example**: In the following example when a card is used and granted access at Reader 1 (Entrance Card Reader 1) it will register the card holder 'into' the area and if the same user attempted to present their card to Reader 1 again they will be denied access until they use their card at Reader 3 (Entrance Card Reader 3), and Visa Versa, once they use their card at Reader 3 (Entrance Card Reader 3), they can't use it again until after they use it at Reader 1 (Entrance Card Reader 1).

Controller List	Property		
Search P			
👢 Main Office - 4 Door Controller	Controller Name:	DS-K2604 (L)	
DS-K2604 (L)	First Card Read	Disable	×
	Index Card En	rollment Station	Card Reader Afterward
		e Card Reader1	Entrance Card Reader3
		d Reader2	
		e Card Reader3	Entrance Card Reader1
	4 Exit Car	d Reader4	
	5 Entranc	e Card Reader5	
	6 Exit Car	d Reader6	
	7 Entranc	e Card Reader7	
	8 Exit Car	d Reader8	

#### Notes:

- Up to four afterward card readers can be added for one card reader.
- If a card is programmed as a "Super" Card the card is exempt from Anti-Passback rules.
- 5. (Optional) You can enter the Select Card Reader dialog box again to edit its afterward card readers.
- 6. Click **Save** to save and take effect of the new settings.

#### 7.7.6 Cross-Controller Anti-passing Back

#### Purpose:

It is strongly recommended wherever possible to have Entry and Exit reader for Anti-Passback on one the one controller. However sometimes it is not possible. Therefore you can use the "Cross-Controller Anti-passing Back" feature.

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

For the Cross-Controller Anti-passing Back" feature to operate iVMS4200 software must be running at all times.

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

Enable Cross-Contr	oller Anti-passing Back				Save	
Set Cross-Cont	roller Anti-passing Back					
Mode:	Based on Card 🗸					
Rule:	Route Anti-passing Back 🗸 🗸					
Sector ID:	0					
Access Controll	Select Device					
	Selected Access Controllers (0/0)		×	Delete	🧰 clear	
Set Card Reader:						-
Set Card Reader:						
	Card Enrollment Station	Card Reader Afterward		En	able Anti-passi	
						/
						/
						ו ה ו
			1 1-2 1-	5		SIN

#### Setting Route Anti-passing Back

#### Purpose:

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

#### Steps:

- 3. Check the Enable Cross-Controller Anti-passing Back checkbox to enable the function.
- 4. Set the anti-passing back parameters.
  - Based on Card

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

- 1) Select **Based on Card** as the anti-passing back mode in the drop-down list.
- 2) Select Route Anti-passing Back as the rule.
- 3) Set the sector ID.
- 4) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
- 5) In the Set Card Reader area, click the icon on the left of the card enrollment station

column to select the first card reader. The icon will turn to 送

- 6) Click the card reader afterward input field to select the card readers afterward in the pop-up window.
- 7) Check the checkbox in the Enable Anti-passing Back column to enable the anti-passing back function.

Notes:

- The displayed card readers in the card reader afterward input field should be in authentication order.
- Up to 64 controllers with anti-passing back function can be added.
- Up to 16 card readers afterward can be added for each card reader.
- It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to 7.4.7 M1 Card Encryption.

#### Based on Network

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

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

column to select the first card reader. The icon will turn to 😫

- 6) Click the card reader afterward input field to select the card readers afterward in the pop-up window.
- 7) Check the checkbox in the Enable Anti-passing Back column to enable the anti-passing back function.

Notes:

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

#### Setting Entrance/Exit Anti-passing Back

#### Purpose:

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

#### Steps:

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

#### Based on Card

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

- 1) Select **Based on Card** as the anti-passing back mode in the drop-down list.
- 2) Select Entrance/Exit Anti-passing Back as the rule.
- 3) Set the sector ID.
- 4) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
- 5) In the Set Card Reader area, check the checkboxes in the Enable Anti-passing Back column to select the entrance card reader and the exit card reader.
- 6) Click Save to save the settings.

#### Notes:

- Up to one entrance carder and one exit card reader should be checked.
- Up to 64 controllers with anti-passing back function can be added.
- It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to 7.4.7 M1 Card Encryption.

#### Based on Network

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

- 1) Select Based on Network as the anti-passing back mode in the drop-down list.
- 2) Select Entrance/Exit Anti-passing Back as the rule.
- 3) Select the server in the dropdown list for judging the anti-passing back.
- 4) (Optional) You can click **Delete Record** and select the card in the pop-up window to delete the card swiping information in all devices.
- 5) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
- 6) In the Set Card Reader area, check the checkboxes in the Enable Anti-passing Back column to select the entrance card reader and the exit card reader.
- 7) Click **Save** to save the settings. *Notes:* 
  - Up to one entrance carder and one exit card reader should be checked.
  - Up to 64 controllers with anti-passing back function can be added.
  - Up to 5000 cards' swiping records can be stored in the selected server.

#### 7.7.7 Multi-door Interlocking

#### Purpose:

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

#### Notes:

• The Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).

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

#### Steps:

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

Controller List	Multi-door Ir	nterlocking List				
Search	+ Add	× Delete	- Save		Filter	
. 10.18.146.86	Index	Interlocking Type		Interlocking Combination		I

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

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

#### 7.7.8 Authentication Password

#### Purpose:

You can open the door by inputting the authentication password (PIN) on the card reader keypad. This PIN / Password is different to that entered in the Card Holder profile for the Card and Code option.

#### Notes:

- This authentication password function is only valid during the schedules when the card reader authentication mode for the access control device is set as **Card or Authentication Password**. For details, please refer to *Chapter 7.7.2 Card Reader Authentication*.
- This function should be supported by the access control device.

#### •

#### Steps:

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

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

Once the controller is selected, all the cards and persons which have been applied to the device will be displayed.

#### Note:

- It is important to click on the controller each time you enter the "Authentication Password" field to refresh the list of card applied to that controller.
- For setting and applying the permissions to the device, refer to *Chapter 7.6 Permission Configuration.*
- 2. Click the **Password** field of the card and input the authentication password for the card. *Note:* The authentication password should contain 4 to 8 digits.
- 3. After setting the authentication password, the authentication password function of the card will be enabled.
- 4. (Optional) You can input the keywords of card No., person name, or authentication password to search from the Filter Flield in the top right of the screen.

#### Notes:

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

#### 7.7.9 Custom Wiegand

## Do not attempt to touch these settings unless you have a clear understanding of $3^{rd}$ party integration.

#### Purpose:

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

#### Before you start:

Wire the third party card readers to the controller.

Steps:

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

Custom Wiegand List	Details			Ŀ	Save
Custom Wiegand 1 Custom Wiegand 2 Custom Wiegand 3	Custom Wiega	Select Access Controller			
Custom Wiegand 4 Custom Wiegand 5		Selected Access Controllers (	🗙 Delete 🛛 🎁 d	lear	
	Total Length(bit): Parity Mode:	Odd-Even Parity	×		
	Odd Parity Start Bit: Even Parity Start Bit: Output Transformation	Length: Length: Set Rule			

- 2. Select a custom wiegand on the left of the interface.
- 3. Check Enable checkbox to enable the custom wiegand.
- 4. Set the wiegand name.
- 5. Select device.
  - 1) Click Select Device.
  - 2) Select the device need to use custom wiegand.
  - 3) Click **OK** to save the settings.
- 6. Input the Total Length and select the parity mode in the drop-down list.

If you select Odd-Even Parity, you should set the odd parity start bit, the odd parity length, the even parity start bit and the even parity length.

If you select XOR Parity, you should set the XOR parity start bit, length per group and total length.

If you select None, you are no need to set the parity mode.

- 7. Set output transformation rule.
  - 1) Click Set Rule to pop up the Set Output Transformation Rules window.

electable Rules:	Selected Rules:
Card ID	Manufacturer Code $ op = \downarrow$
Manufacturer Code	Site Code $\uparrow \downarrow$
Site Code	OEM
OEM	

2) Select rules on the left list.

*Note:* Press the *Shift* key to select multiple rules.

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

#### Notes:

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

# CORPORATION

## 7.8 Searching Access Control Event

#### Purpose:

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

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

	Control Panel	5	Main View	1	Remote Playback	ľ	Access (	= Control		Status Mo	nitor		
A A	ccess Control Event	Call Lo	og Unlockin	g Log Not	tice								
ee Er	Event Source: Device:	Main	Office - 4 Doo		Local Event			O	Remote	Event	~		
	Card Holder Name	e:									~		
9	Organization: Start Time:	2018	-03-19 00:00:(	00							~	/	
¢°	Search Result												~
y.	Serial   Event Type	2			Card Hold	er	Card	Туре	Card N	o.   Ev	ent T		
Ð											0		
Access Co	ntrol Event Call Log	Unlockin	g Log Notice			7	-	1	3	K.	ī		1/1 C
Source Device	Client	O De	0.000 to 0.000	Captured Pictu	ire			Card Hol	der Inform:	ation			
Event T	ype: All older Name:		<ul> <li>Start Time</li> <li>End Time</li> </ul>	ə:	2017-05-04 00:00:00		Search						
Card N	o.:		✓ Card Rea	der Type:	All	-							
Search	Result						Export						
Serial	Event Type Caro	l Holder	Card Reader	Card Type	Card No.	t Time	Event S	Person N	lo.:				
								Person N	lame:				
								Gender:					
								ID Type: ID No.:					
								Organiza	tion:			-	
								Phone N					
								Address:					
4							۲						
Total:0	Page:1/1				I I I I Pa	je	Go						

#### Steps:

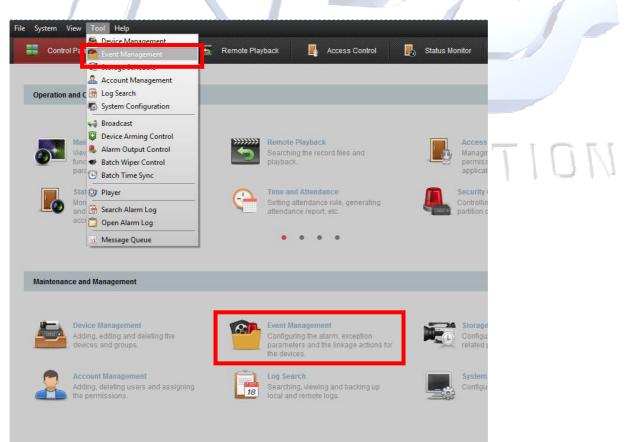
- 1. Select the source. You can select Client or Device.
- 2. Enter the search condition (source, event type/card holder name/card No./capture/start & end time).
- 3. Click **Search** to get the search results.
- 4. View the event information in the event list.
- 5. Click an event to view the information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

## 7.9 Access Control Event Configuration

#### Purpose:

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

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



### 7.9.1 Access Control Event Linkage

### Purpose:

You can assign linkage actions to the access control event by setting up a rule. For example, when the access control event is detected, an audible warning appears or other linkage actions happen. *Note:* The linkage here refers to the linkage of the client software's (iVMS4200) actions.

### Steps:

1. Click the Access Control Event tab.

ess Control Device		
earch		
👢 Lift Interface	Event Type:	Trigger Camera: 🗸
Main Office - 4 Door Contro	I All	✓ Trigger Client
🖃 📕 Doorl	✓ Duress Alarm	Audible Warning Other Alarm Sound 🗸
Entrance Card Read	✓ Card Reader Tampering Alarm	✓ Email Linkage
T Exit Card Reader2	✓ Normal Card Authentication Passed	✓ Alarm Triggere
🕐 🧱 Door2	Card and Password Authentication Passed	
🛨 📕 Door3	✓ Card and Password Authentication Failed	
🛨 📕 Door4	✓ Card Reading Failed Attempts Reach Limit	
& Event1	✓ Card and Password Authentication Attempts Reach Limit	
J Event2	✓ No Permission for Normal Card	
J Event3	✓ Invalid Duration	
🍌 Event4	Z Expired Card	
👃 DS-K2604 (L)	✓ Invalid Card	
	Invalid Anti-Passing Back Authentication	
	Interlocking Door Not Closed	
	Fingerprint Recognition Passed	
	Fingerprint Recognition Failed	
	Card and Fingerprint Passed	
	Card and Fingerprint Authentication Failed	
	Card and Fingerprint Authentication Timeout	
	Card, Fingerprint, and Password Authentication Passed	
	Card, Fingerprint, and Password Authentication Failed	
	Card, Fingerprint, and Password Authentication Timeout	
	Fingerprint and Password Authentication Passed	
	Fingerprint and Password Authentication Failed	
	✓ Fingerprint and Password Authentication Timeout	

- 2. The added access control devices will display in the Access Control Device panel on the left. Select the access control device, or alarm input, or access control point (door), or card reader to configure the event linkage.
- 3. Select the event type to set the linkage. (e.g. Access Granted (Normal Card Authenticated Passed), Invalid card etc)
- 4. Select the triggered camera. The image or video from the triggered camera will pop up when the selected event occurs.
  To capture the picture / record the event of the triggered camera when the selected event

occurs, you must first program and setup a schedule and the storage in 'Storage Schedule'.

5. Check the checkboxes to activate the linkage actions. For details, refer to *Table 14.1 Linkage Actions for Access Control Event*.

- 6. Click **Save** to save the settings.
- 7. You can click Copy to button to copy the access control event to other access control device, alarm input, access control point, or card reader.

Select the parameters for copy, select the target to copy to, and click **OK** to confirm.

Access Control Device	📄 Copy to	Save
	P Event Type: Trigger Camera: ✓	
<ul> <li>Access Controller_01</li> <li>Lent1</li> </ul>	✓ All	
🌽 Event2	✓ Open Door with First Card Started ✓ Audible Warning Other Alarm Sound ×	
J Event3	Open Door with First Card Stopped	
🎄 Event4	✓ Remain Open Started ✓ Alarm Triggere	
🎉 Event5	Remain Open Stopped I Alarm on E-map	
🍰 Eventő	✓ Remain Closed Started	
/€ Event7	Remain Closed Stopped	
🎄 Event8	Unlock Door	
Zonel	Lock Door	
Zone2	Exit Button Pressed	
🔛 Zone3	Exit Button Released	
Zone4	Vormally Open Door	
🛃 🔲 Doorl	Vormally Close Door	
📩 🚪 Door2	Abnormally Open Door	
\pm 📕 Door3	Open Door Timeout	
📩 📓 Door4	Remotely Open Door	
	Remotely Close Door	
	Domain Onen Pomotoke	

	Table 1. 1 Linkage Actions for Access Control Event					
Linkage Actions	Descriptions					
Audible Warning	The client software gives an audible warning when alarm is					
	triggered. You can select the alarm sound for audible warning.					
Send an email notification of the alarm information to one or						
Email Linkage	more email recipients.	1				
	Display the alarm information on the E-map.					
Alarm on E-map	<i>Note:</i> This linkage is only available to access control point and					
	alarm input. (i.e. Events)					
Alarm Triggered	The image with alarm information pops up when alarm is					
Pop-up Image	triggered.					

### 7.9.2 Access Control Alarm Input Linkage

### Purpose:

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

*Note:* The linkage here refers to the linkage of the client software's (iVMS4200) own actions.

Control Panel	out 🗂 Exception 🖬 Zone I	Event 🔳 Access Control Event 🐥 Access	Control Alarm Input 🗮 Event Card Linkage 💷 Cross-Device Linkage 🔳 Pyror
Event	Property		
Search	P Host Buzzer	Disable 💽 Enable	
A Eventi	Card Reader Buzzing	Name   Property	
🏂 Event2		Entrance Card Reader1 Disable Disable	nable
A Event3		Exit Card Reader2 Disable Disable	nable
Los-K2604 (L)		Entrance Card Reader3 Disable Disable	nable
Event1		Exit Card Reader4 Disable Disable	nable
🎄 Event2		Entrance Card Reader5 Disable Disable	nable
🎄 Event3		Exit Card Reader6 Disable O E	nable
Livent5			
🔈 Eventő	Alarm Output	Name	Property
🎄 Event7		Main Office - 4 Door Controller_Alarm Output1	Disable Disable
🎄 Event8		Main Office - 4 Door Controller_Alarm Output2	Disable Disable
		Main Office - 4 Door Controller_Alarm Output3	Disable 💭 Enable
		Main Office - 4 Door Controller_Alarm Output4	Disable Enable
	Access Control Point	Name Open	Close
		Door1 Disable Disable	Disable Disable
		Door2 Disable Disable	Disable 💭 Enable
		Door3 Disable Dable	Disable Disable
		Door4 Disable O Enable	Disable 🕥 Enable

#### Steps:

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

- 2. In the event list on the left, select an alarm / Event input.
- Switch the property from to to enable this action.
   Host Buzzer: The audible warning of controller will be triggered.
   Card Reader Buzzer: The audible warning of card reader will be triggered.
   Alarm Output: The alarm output will be triggered for notification.

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

Access Control Point (Open/Close): The door will be open or closed when the event is triggered.

*Note:* The Door cannot be configured as open or closed at the same time. They need to be different Events. E.g. Event 1 may open / unlock and door and Event 2 may close / lock the door.

4. Click Save button to save the settings.

## 7.9.3 Event Card Linkage

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

- The Event Card Linkage should be supported by the device.
- The linkage here refers to the linkage of the iVMS4200 client software's own actions.

vent Card Linkage	Linkage Details I Add X Delete I Save
Search Access Controller_01	Event Source     Event Linkage: Device Event      Device Tamperin     Card Linkage:
	Linkage Target Host Buzzer Enable Disable Capture Not Trigger Trigger Card Reader Buzzing Alarm Output Zone
	Name         Enable         Disable         Name         Enable         Disable         Name         Arm         Disable           Entrance Card R         Image: Card R
	Exit Card Reader2
	Access Control Point
	Name Open Close Remain Open Remain Closed
	Doorl. No Tri No Tri No Tri NotTrigger Trigger
	Door1         No         Tri         No         Tri         No         Tri         Not Trigger         Trigger           Door2         No         Tri         No         Tri         No         Tri         Not Trigger         Trigger

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

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

### **Event Linkage**

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

Steps:

- 1. Click to select the linkage type as **Event Linkage**, and select the event type from the dropdown list.
  - For Device Event, select the detailed event type from the dropdown list.
  - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
  - For Door Event, select the detailed event type and select the source door from the table.
  - For Card Reader Event, select the detailed event type and select the card reader from the table.
- 2. Set the linkage target, and switch the property from O to C to enable this function.
  - Host Buzzer: The audible warning of controller will be enabled/disabled.
  - **Capture:** The real-time capture will be enabled.

- **Card Reader Buzzer:** The audible warning of card reader will be enabled/disabled.
- Alarm Output: The alarm output will be enabled/disabled for notification.
- **Zone:** Arm or disarm the zone.
- Access Control Point: The door status of open, close, remain open, and remain closed will be enabled.

Notes:

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

### Card Linkage

Steps:

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

**Note:** When you program a Card Linkage event whereby is it is assigned to an Alarm O/P then 1 card swipe will activate the O/P. There is also a 'special' application applied to these Card Linkage events, in that 3 Card swipes of the same card (as programmed in the event linkage) within 5 seconds will deactivate the O/P. This could be used for Arming and Disarming an alarm panel such as the Ness M1 Controller or Ness D8X panels.

Event Card Linkage	Linkage Details
Search	Event Source         Linkage Type:       Event Linkage         Card No.:       0002499767         Card Reader:       Warehouse Entry Door
	Linkage Target Buzzing Recording Alarm Output Zone Access Control Point Audio Play Alarm Output
	Name         Enable         Disable           Alarm Output 1         Image: Control of the second sec
	Alarm Output 2 💿 🐨
	Alarm Output 3
	Alarm Output 4

## 7.9.4 Cross-Device Linkage

### Purpose:

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

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

Access Control Cross-Device Link	Access Control Cross-Device Linkage + Add X Delete Save	
Search 9 Event Linkage_Device Tamperi	Event Source   Event Linkage: Device Event  Device Tamperin Controller List  10.18.146.86	
	Linkage Target Controller List 10.18.146.86  Alarm Output Name Property Alarm Output 1 Not Trigger Trigger	
	Alarm Output 2       Not Trigger       Trigger         Access Control:       Name       Open       Close       Normal Open       Remain Closed         Door1       No       Tri       No       Tri       Not Tri       Not Tri         Door2       No       Tri       No       Tri       Not Tri       Not Tri	i

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

### Event Linkage

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

### Steps:

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

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



### **Card Linkage**

### Steps:

- 1. Click to select the linkage type as Card Linkage.
- 2. Select the card from the dropdown list and select the access control device as event source.
- 3. Select the card reader from the table for triggering.
- Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from 
   to 
   to 
   to 
   to

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

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

## 7.10 Door Status Management

### Note:

• Before use, see section 7.11.1 Access Control Group Management below.

### Purpose:

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

From the 'Control Panel' select



to open 'Status Monitoring'

Select the 'Door Status' tab to open the 'Door Status Management' feature. From the left hand window select the controller / Door Group you wish to monitor.

### Access Controller - User Manual

	учур
	👼 Main View 🚦 Access Control 📙 Status Monitor 📾 License Plate Retrieval 🔄 Vehicle Retrieval 🛓 Road Traffic 🚆
Reco	ord Access Control Alarm
0.001007	Status Information Status Duration 📕 Open Door 📲 Close Door 💐 Remain Open 🧧 Remain Closed
ρ	
2	
	Door1_DS-K26 Door2_DS-K26 Door3_DS-K26 Door4_DS-K26 Door1_DS-K28 Door2_DS-K28 Door3_DS-K28 Door4_DS-K28
	Operating Record
	Serial No. Event Time Door Group Door Operation Operation Result
	5 2018-03-26 15:2 All Access Doors Door3_DS-K260 Open Door Operation com
	4 2018-03-26 15:2 All Access Doors Door2_DS-K280 Remain Closed Operation com
	3 2018-03-26 15:2 All Access Doors Door3_DS-K260 Open Door Operation com
	3         2018-03-26 15:2 All Access Doors         Door3_DS-K260 Open Door         Operation com           2         2018-03-26 15:2 All Access Doors         Door1_DS-K260 Door Remain O Operation com         Operation com

Select the "Card Swiping Record" to view live Card Swiping events as they come in.

oor Status	ard Swiping Record	ess Control Alarm					
Card No.	Person Name	Organization	Event Time	Door Position	Direction	Authentication Result	Operation
03809399	Greg Kingsley	Ness	2018-03-26 15:29:56	Main Office - 4 Door Controller:Entrance Card Reader1	Enter	Legal Card Authentication Passed	ደ 💿 🖾
03809399	Greg Kingsley	Ness	2018-03-26 14:29:58	DS-K2604 (L):Entrance Card Reader5	Enter	Legal Card Authentication Passed	ደ 💿 🔤
14511850	14511850	Ness	2018-03-26 14:29:56	DS-K2604 (L):Entrance Card Reader1	Enter	Invalid Card	ይ 💿 🖂
03809237	Malcolm Turnbull	Ness	2018-03-26 15:29:48	Main Office - 4 Door Controller:Entrance Card Reader5	Enter	Permission Mismatch	2 💿 🖃
03809237	Malcolm Turnbull	Ness	2018-03-26 15:29:42	Main Office - 4 Door Controller:Entrance Card Reader1	Enter	Legal Card Authentication Passed	ይ 💿 🔤
20943500			2018-03-26 15:29:38	Main Office - 4 Door Controller:Entrance Card Reader1	Enter	Invalid Card	ደ ⊙ 🖂
03809237	Malcolm Turnbull	Ness	2018-03-26 14:29:39	DS-K2604 (L):Entrance Card Reader3	Enter	Legal Card Authentication Passed	ይ 💿 🔤
03809399	Greg Kingsley	Ness	2018-03-26 14:29:36	DS-K2604 (L):Entrance Card Reader1	Enter	Legal Card Authentication Passed	<u> 8</u> o 🖂

(Note – When first opening the above screen, previous events may not be visible and only new events will come through as they occur. For past events use the Access Control / Search feature.

System	View Tool I	Help						ivms-4200				
Con	trol Panel	🚮 Main Viev 📲	Access Control	👃 Status Mor	nitor 🔂 Licens	e Plate Retrieval	<b>.</b> v	/ehicle Retrieval	📥 Road Traffic	🍟 Event Management	-	Device Manag
Access	Control Event	Call Log Unlocking Log	Notice									
Eve	int Source:		Local Event		Remote Even	t						
Dev	vice:	Main Office - 4 Door Controlle	er			✓ Eve	nt Type:	All				
Car	rd Holder Name:					✓ Car	1 No.:					
	anization:						d Reader Type:	All				
-	rt Time:	2018-03-26 00:00:00				📆 End		2018-03-26 23:59:5	9			
Sea	irch Result											
Seria	I   Event Type		C	ard Holder	Card Type	Card No.	Event Time	Event Source			Capture	Playbac
1	Door Locked						2018-03-26	15:2 Main Office - 4	Door Controller:Door1			
	Legal Card A	uthentication Passed	G	reg Kingsley	Normal Card	03809399	2018-03-26	15:2 Main Office - 4	Door Controller:Entrance	Card Reader1		0
	Unlock						2018-03-26	15:2 Main Office - 4	Door Controller:Door1			
4	Door Remain	ing Open Status with First Card	l Ended				2018-03-26	15:2 Main Office - 4	Door Controller:Door1			
5	Permission N	lismatch	N	falcolm Turnbull	Normal Card	03809237	2018 03 26	15:2 Main Office 4	Door Controller:Entrance	Card Reader5		
6	Legal Card A	uthentication Passed	N	lalcolm Turnbull	Normal Card	03809237	2018-03-26	15:2 Main Office - 4	Door Controller:Entrance	Card Reader1		0
7	Unlock						2018-03-26	15:2 Main Office - 4	Door Controller:Door1			
8	Door Remain	ing Open Status with First Caro	Started				2018-03-26	15:2 Main Office - 4	Door Controller:Door1			
9	Invalid Card				Normal Card	20943500	2018-03-26	15:2 Main Office - 4	Door Controller:Entrance	Card Reader1		Θ
10	Remote: Clos	e Door					2018-03-26	15:2 Main Office - 4	Door Controller:Door2			
11	Door Locked						2018-03-26	15:2 Main Office - 4	Door Controller:Door2			
12	Remain Close	ed Stopped					2018-03-26	15:2 Main Office - 4	Door Controller:Door2			
13	Door Locked						2018-03-26	15:2 Main Office - 4	Door Controller:Door2			
14	Remain Close	ed Started					2018-03-26	15:2 Main Office - 4	Door Controller:Door2			
15	Remote: Rem	ain Closed					2018-03-26	15:2 Main Office - 4	Door Controller:Door2			
16	Remote: Logi	n					2018-03-26	14:3 Main Office - 4	Door Controller			
17	Remote: Log	out						14:3 Main Office - 4				
18	Remote: Arm	-						10:3 Main Office - 4				
19	Remote: Disa	rming						10:3 Main Office - 4				
20	Remote: Logi	n						09:3 Main Office - 4				
21	Remote: Log	out					2018-03-26	09:3 Main Office - 4	Door Controller			

## 7.10.1 Access Control Group Management

### Purpose:

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

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

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

- FI	ie sysi	tem view 100	і неір						
	==	Control Panel	5	Main Vie	ew	Acce	ss Control		Status Monitor
:::: 0	Devic	e 🖬 Group							
	Device	Туре			Device for	Managem	ent (13)		
		Hikvision Device			🕂 Add	🗹 Modify	🗶 Delete	🌣 Rem	ote Configuration
	- 4	Upgrade Server			Device Typ	e   Nickna	ame	Connect	ion  Network Par
	+	Add New Device	Туре		Access Cor	n Lift Int	erface	TCP/IP	192.168.0.197
					Access Cor	n Main (	Office - 4 Doo.	TCP/IP	192.168.0.192
		/		(***)	1	- DC K24	504 (1)	TCD/ID	102 169 0 103

Resource 🗔 🤤	Access Control Point of Group Access Contro	oller(1)		
Search \$	📲 🕂 Import 🖸 Modify 🗶 Delete 🌣	Remote Configuration	Filter	
🕙 😇 CVR	Nickname	IP	Device Serial No.	
<ul> <li>IO.16.6.112</li> <li>IO.18.146.86</li> <li>IO.18.146.81</li> <li>IO.18.146.81</li> <li>IO.16.6.151</li> <li>IO.16.6.111</li> <li>IO.16.6.104</li> <li>Door Station</li> <li>Access Controller</li> <li>Encoding Channel</li> <li>Alarm Input</li> <li>Zone</li> </ul>	Door1_Access Controller	10.16.6.111		

- 3. Perform the following steps to add the group.
  - 1) Click 🗔 to open the 'Add' Group dialog box.
  - 2) Enter a group name as you want. (e.g. All Access Doors)
  - Click OK to add the new group to the group list.
     You can also check the checkbox Create Group by Device Name to create the new group by the name of the selected device.

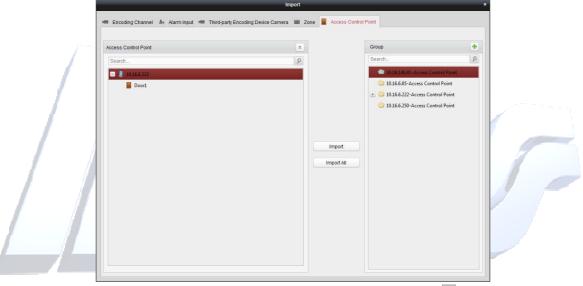
	Add Group	×
Group Name:		
Create Group by De	evice Name	
	ОК	Cancel

4. Perform the following steps to import the access control points to the group:

 Click Import on Group Management interface, and then click the Access Control tab to open the Import Access Control page.

Notes:

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



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

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

### Purpose:

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

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

cess Control Group	Status Information Status Duration 📕 Open Door 📲 Close Door 📓 Remain Open 🧧 Remain Closed 🐱 Capture
earch	
<b>10.18.146.81</b>	
<u>3</u> 10.16.6.85	
10.16.6.222	Door1_10.16.6
	Operating Record
	Serial No.   Event Time   Door Group   Door   Operation   Operation Result   Capture
	3 2017-01-18 20:2 10.16.6.222 Door1_10.16.6.222 Open Door Operation com
	2         2017-01-18 20:2         10:16.6.222         Door1_10:16:6.222         Door1_00:10:00:22         Operation com
	2 2017-01-18 20:2 10.16.6.222 Door1_10.16.6.222 Door Remain O Operation com
	2 2017-01-18 20:2 10.16.6.222 Door Remain O Operation com
	2 2017-01-18 20:2 10.16.6.222 Door1_10.16.6.222 Door Remain O Operation com
	2 2017-01-18 20:2 10.16.6.222 Door1_10.16.6.222 Door Remain O Operation com
	2 2017-01-18 20:2 10.16.6.222 Door1_10.16.6.222 Door Remain O Operation com
	2 2017-01-18 20:2 10.16.6.222 Door1_10.16.6.222 Door Remain O Operation com

#### Steps:

- 1. Select an access control group on the left. For managing the access control group, refer to *Chapter O Purpose:*
- 2. *The door* status of the added access control device will be displayed in real time. You can check the door status and the linked event(s) of the selected door. You can control the status of the door and set the status duration of the doors as well.

From the 'Control Panel' select



to open 'Status Monitoring'

Select the 'Door Status' tab to open the 'Door Status Management' feature. From the left hand window select the controller / Door Group you wish to monitor.

### Access Controller - User Manual

	🕞 Main View 📴 Access Control 🔥 Status Monitor 🔄 License Plate Retrieval 🔄 Vehicle Retrieval 🛓 Road Traffic 🔐
≺eco	rd Access Control Alarm
ρ	Status Information Status Duration 📕 Open Door 📲 Close Door 📓 Remain Open 🧧 Remain Closed
2	Image: Door1_DS-K26       Image: Door3_DS-K26       Image: Door4_DS-K26       Image: Door4_DS-K28       Image: Door3_DS-K28       Image: Door4_DS-K28       Image: Door4_DS-K28
	Operating Record
	Serial No. Event Time Door Group Door Operation Operation Result
	5 2018-03-26 15:2 All Access Doors Door3_DS-K260 Open Door Operation com
	4 2018-03-26 15:2 All Access Doors Door2_DS-K280 Remain Closed Operation com
	4 2018-03-26 15:2 All Access Doors Door2_DS-K280 Remain Closed Operation com

Select the "Card Swiping Record" to view live Card Swiping events as they come in.

Card No.	Person Name	Organization	Event Time	Door Position	Direction	Authentication Result	Operation
03809399	Greg Kingsley	Ness	2018-03-26 15:29:56	Main Office - 4 Door Controller:Entrance Card Reader1	Enter	Legal Card Authentication Passed	ደ 💿 🖂
03809399	Greg Kingsley	Ness	2018-03-26 14:29:58	DS-K2604 (L):Entrance Card Reader5	Enter	Legal Card Authentication Passed	ደ 💿 🔤
14511850	14511850	Ness	2018-03-26 14:29:56	DS-K2604 (L):Entrance Card Reader1	Enter	Invalid Card	ደ 💿 🖂
03809237	Malcolm Turnbull	Ness	2018-03-26 15:29:48	Main Office - 4 Door Controller:Entrance Card Reader5	Enter	Permission Mismatch	ደ 💿 🖬
03809237	Malcolm Turnbull	Ness	2018-03-26 15:29:42	Main Office - 4 Door Controller:Entrance Card Reader1	Enter	Legal Card Authentication Passed	ደ 💿 🔜
20943500			2018-03-26 15:29:38	Main Office - 4 Door Controller:Entrance Card Reader1	Enter	Invalid Card	ደ 💿 🖂
03809237	Malcolm Turnbull	Ness	2018-03-26 14:29:39	DS-K2604 (L):Entrance Card Reader3	Enter	Legal Card Authentication Passed	ደ 💿 🔤
03809399	Greg Kingsley	Ness	2018-03-26 14:29:36	DS-K2604 (L):Entrance Card Reader1	Enter	Legal Card Authentication Passed	ጿ ⊙ 🖂

(Note – When first opening the above screen, previous events may not be visible and only new events will come through as they occur. For past events use the Access Control / Search feature.

Second Control Licent         Cale Licent Device         Licent Device         Licent Device         Licent Device         Device         Licent Device         Device         Licent Device         Device         Licent Device         Device <th>le Sy</th> <th>rstem Vi</th> <th>ew Tool</th> <th>Help</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>📩 iVMS-4:</th> <th>200</th> <th></th> <th></th> <th></th>	le Sy	rstem Vi	ew Tool	Help						📩 iVMS-4:	200			
Image: Second	==	Control	Panel	🔝 Main View	🛃 Access Control	📕 Status Mo	nitor 🔂	License Plate Ret	rieval 💽 V	/ehicle Retrieval	🛓 Road Traffic	🐣 Event Management	2	Device Managem
First Surger     Lacalem     Canada Card       Image: Surger     Image: Surger <t< th=""><th>_ A</th><th>Access Co</th><th>ntrol Event</th><th>Call Log Unlocking Lo</th><th>og Notice</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></t<>	_ A	Access Co	ntrol Event	Call Log Unlocking Lo	og Notice									
Pick:       Man Olice - 4 Door Controler       Pick Hamps       A         Card Factor Falser       Card Read Trype       Card Read Trype       A         Card Factor Falser       Card Read Trype       Card Read Trype       Card Read Trype         Status       Card Read Trype       Card Read Trype       Card Read Trype       Card Read Trype         Status       Card Read Trype       Card Read Trype       Card Read Trype       Card Read Trype         1       Card Read Trype       Card Read Trype       Card Read Trype       Card Read Trype         1       Card Read Trype       Card Read Trype       Card Read Trype       Card Read Trype         1       Card Read Trype       Card Read Trype       Card Read Trype       Card Read Trype         1       Card Read Trype       Card Read Trype       Card Read Trype       Card Read Trype         1       Card Read Trype       Card Read Trype       Card Read Trype       Card Read Trype         1       Card Read Trype         1       Card Read Trype         1       Card Read Trype       Normal Card	iii iii	Event 9	00000		Local Event		O Rem	ote Event						
Card Holder Name       Card Holder Name       Card Holder Name       Card Reader Type       ////////////////////////////////////	_		ource.	Main Office 4 Deer Co			U Keni		Event Tune:	All				
Organization:	0		oldor Nomo:	Main Onice - 4 Door Co	naoner									
Start Time:       2018-032 00 00:00       Description       2018-032 02 03:00       Description         Start Time:       2018-032 00 00:00       Card Holder       Card Type       Card Type       Card Holder       Card Type       Card Holder														
Search Result         Search Result           Seind _ Event Type         Card Holder         Card Type         Card No.         Event Type         Card No.         Card No.         Event Type         Card No.         Card No.         Event Type         Card No.	9	-												
Serial - Event Type       Card Holder       Card Type       Card No.       Event Time       Fore Source       Capture       Playback         1       Door Locked       2018-03-26 152       Main Office - 4 Door Controller/Door1       Image: Source Card Readed       Image: Source C		Start III	me:	2018-03-26 00:00:00					End lime:	2018-03-26 23:	9:59			
1       Door Locked       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader1         2       Legal Card Authentication Passed       Greg Kingsley       Normal Card       03009399       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader1       O         3       Unlock       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader1       O         4       Door Remaining Open Status with First Card Ended       Malcolm Tumbul       Normal Card       03009277       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader5         6       Legal Card Authentication Passed       Malcolm Tumbul       Normal Card       03009277       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader5         7       Unlock       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader1       O         8       Door Isotaning Open Status with First Card Statted       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader1       O         9       Inraild Card       Normal Card       2049300       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader1       O         10       Remain Closed Stopped       2018-03-26 15.2 Main Office - 4 Door Controller.Entrance Card Reader1       O         12       Remain Closed Stopped       2018-03-26 15.2 Main Office - 4 Door Controller.Door2       O <td>¢°</td> <td>Search</td> <td>Result</td> <td></td>	¢°	Search	Result											
1       Uper Locked       Carg Mundberger - 4 Door Controller Journal Card       03093393       2018-03-26 152-2.       Main Offrice - 4 Door Controller Journal Card Readed       ©         2       Legal Card Authennication Passed       Greg Kingsley       Normal Card       03093939       2018-03-26 152-2.       Main Offrice - 4 Door Controller/Doord         4       Door Remaining Open Status with First Card Ended       Malcolm Tumbull       Normal Card       03809237       2018-03-26 152-2.       Main Offrice - 4 Door Controller/Doord         5       Permission Minmatch       Malcolm Tumbull       Normal Card       03809237       2018-03-26 152-2.       Main Offrice - 4 Door Controller/Doord         6       Legal Card Authentication Passed       Malcolm Tumbull       Normal Card       03809237       2018-03-26 152-2.       Main Offrice - 4 Door Controller/Doord       ©         7       Unlock        Door Remaining Open Status with First Card Stated       ©       O       P		Serial	Event Type			Card Holder	Card Type	Card N	o. Event Time	Event Sour	e		Capture	Playback
3       Unlock       200 Permission       Anim Office - 4 Door Controller:Doord         3       Unlock       200 Permission       Mair Office - 4 Door Controller:Doord         4       Door Remaining Open Status with First Card Ended       200 200 201 201 201 201 201 201 201 201	0	1	Door Locked	I					2018-03-26	15:2 Main Office	- 4 Door Controller:Door1			
4       Door Remaining Open Status with First Card Ended       2018-03-26 15:2.       Main Office - 4 Door Controller.Doorl         5       Permission Mismatch       Maleolm Tumbull       Normal Card       03809237       2018 03 26 15:2.       Main Office - 4 Door Controller.Entrance Card ReaderS         6       Legal Card Authentication Passed       Maleolm Tumbull       Normal Card       03809237       2018-03-26 15:2.       Main Office - 4 Door Controller.Entrance Card ReaderL       Image: Card Authentication Passed         7       Unlock       2018-03-26 15:2.       Main Office - 4 Door Controller.Doorl       Image: Card Card Card Card Card Card ReaderL       Image: Card Card Card Card Card Card Card Card		2	Legal Card A	uthentication Passed		Greg Kingsley	Normal Card	038093	99 2018-03-26	15:2 Main Office	- 4 Door Controller:Entranc	e Card Reader1		0
Sol         Permission Mamatch         Malcolm Tumbul         Normal Card         03809237         2018 03 26 15.2 Main Office 4 Door Controller.Entrance Card Readed         Image: Card Authentication Passed         Malcolm Tumbul         Normal Card         03809237         2018 03 26 15.2 Main Office 4 Door Controller.Entrance Card Readed         Image: Card Authentication Passed         Malcolm Tumbul         Normal Card         03809237         2018 03 26 15.2 Main Office 4 Door Controller.Entrance Card Readed         Image: Card Authentication Passed         Image: Card Auth	2	3	Unlock						2018-03-26	15:2 Main Office	- 4 Door Controller:Door1			
6       Legal Card Authentication Passed       Maicolm Tumbull       Normal Card       03809237       2018-03-26 15.2 Main Office - 4 Door ControllerEntrance Card Reader1       Image: Card Card Card Card Card Card Card Card		4	Door Remain	ning Open Status with Firs	t Card Ended				2018-03-26	15:2 Main Office	- 4 Door Controller:Door1			
7       Unlock       2018-03-26 152 Main Office - 4 Door Controller.Door4         8       Door Remaining Open Status with First Card Started       2018-03-26 152 Main Office - 4 Door Controller.Door4         9       Invalid Card       Normal Card       2094300       2018-03-26 152 Main Office - 4 Door Controller.Door4         9       Remote: Close Door       2018-03-26 152 Main Office - 4 Door Controller.Door2       Image: Close Door       2018-03-26 152 Main Office - 4 Door Controller.Door2         10       Remote: Close Door       2018-03-26 152 Main Office - 4 Door Controller.Door2       Image: Close Door         12       Remain Closed Stopped       2018-03-26 152 Main Office - 4 Door Controller.Door2         13       Door Locked       2018-03-26 152 Main Office - 4 Door Controller.Door2         14       Remain Closed Started       2018-03-26 152 Main Office - 4 Door Controller.Door2         15       Remote: Remain Closed       2018-03-26 152 Main Office - 4 Door Controller.Door2         16       Remote: Remain Closed       2018-03-26 152 Main Office - 4 Door Controller.Door2         17       Remote: Remain Closed       2018-03-26 152 Main Office - 4 Door Controller.Door2         18       Remote: Login       2018-03-26 152 Main Office - 4 Door Controller.Door2         19       Remote: Login       2018-03-26 103 Main Office - 4 Door Controller	:0	5	Permission N	Aismatch		Malcolm Turnbull	Normal Card	038092	2018 03 26	15:2 Main Office	4 Door Controller:Entranc	e Card Reader5		
8       Door Remaining Open Status with First Card Stated       2018-03-26 152 Main Office - 4 Door Controller.Doord         9       Invalid Card       Normal Card       2018-03-26 152 Main Office - 4 Door Controller.Entrance Card Reader1       Image: Close Door         10       Remote: Close Door       2018-03-26 152 Main Office - 4 Door Controller.Doord         11       Door Locked       2018-03-26 152 Main Office - 4 Door Controller.Doord         12       Remain Closed Stopped       2018-03-26 152 Main Office - 4 Door Controller.Doord         13       Door Locked       2018-03-26 152 Main Office - 4 Door Controller.Doord         14       Remain Closed Stated       2018-03-26 152 Main Office - 4 Door Controller.Doord         15       Remote: Remain Closed Stated       2018-03-26 152 Main Office - 4 Door Controller.Doord         16       Remote: Login       2018-03-26 152 Main Office - 4 Door Controller.Doord         17       Remote: Login       2018-03-26 152 Main Office - 4 Door Controller.Doord         18       Remote: Login       2018-03-26 152 Main Office - 4 Door Controller.Doord         19       Remote: Login       2018-03-26 152 Main Office - 4 Door Controller.Doord         19       Remote: Login       2018-03-26 103 Main Office - 4 Door Controller.Doord         19       Remote: Disarming       2018-03-26 103 Main Office - 4 Door Cont		6	Legal Card A	uthentication Passed		Malcolm Turnbull	Normal Card	038092	37 2018-03-26	15:2 Main Office	- 4 Door Controller:Entranc	e Card Reader1		o
9       Invalid Card       Normal Card       20943300       2018-03-26 15.2       Main Office - 4 Door Controller.Entrance Card Reader1       Image: Close Door         10       Remote: Close Door       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         11       Door Locked       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         12       Remain Closed Stopped       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         13       Door Locked       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         14       Remain Closed Started       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         15       Remote: Login       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         16       Remote: Login       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         17       Remote: Login       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         17       Remote: Login       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         18       Remote: Login       2018-03-26 15.2       Main Office - 4 Door Controller.Door2         19       Remote: Diarming       2018-03-26 10.3       Main Office - 4 Door Controller         19       Remote: Login       2018-03-26 10.3 </th <th></th> <th>7</th> <th>Unlock</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>2018-03-26</th> <th>15:2 Main Office</th> <th>- 4 Door Controller:Door1</th> <th></th> <th></th> <th></th>		7	Unlock						2018-03-26	15:2 Main Office	- 4 Door Controller:Door1			
10     Remote: Close Door     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       11     Door Locked     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       12     Remain Closed Stopped     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       13     Door Locked     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       14     Remain Closed Started     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       15     Remote: Remain Closed     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       16     Remote: Login     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       17     Remote: Login     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       18     Remote: Login     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       19     Remote: Login     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       19     Remote: Login     2018-03-26 15.3 Main Office - 4 Door Controller:Door2       19     Remote: Disaming     2018-03-26 10.3 Main Office - 4 Door Controller       19     Remote: Login     2018-03-26 10.3 Main Office - 4 Door Controller       20     Remote: Login     2018-03-26 10.3 Main Office - 4 Door Controller       21     Remote: Login     2018-03-26 09.3 Main Office - 4 Door Controller       21     Remote: Login     2018-03-26 09.3 Main Office - 4 Door Controller <td></td> <td>8</td> <td>Door Remain</td> <td>ning Open Status with Firs</td> <td>t Card Started</td> <td></td> <td></td> <td></td> <td>2018-03-26</td> <td>15:2 Main Office</td> <td>- 4 Door Controller:Door1</td> <td></td> <td></td> <td></td>		8	Door Remain	ning Open Status with Firs	t Card Started				2018-03-26	15:2 Main Office	- 4 Door Controller:Door1			
1     Door Locked     2018-03-26 152 Main Offrice - 4 Door Controller:Door2       12     Remain Closed Stopped     2018-03-26 152 Main Offrice - 4 Door Controller:Door2       13     Door Locked     2018-03-26 152 Main Offrice - 4 Door Controller:Door2       14     Remain Closed Started     2018-03-26 152 Main Offrice - 4 Door Controller:Door2       15     Remote Remain Closed     2018-03-26 152 Main Offrice - 4 Door Controller:Door2       16     Remote Login     2018-03-26 152 Main Offrice - 4 Door Controller:Door2       17     Remote Login     2018-03-26 152 Main Offrice - 4 Door Controller:Door2       18     Remote Login     2018-03-26 152 Main Offrice - 4 Door Controller:Door2       19     Remote Login     2018-03-26 143 Main Offrice - 4 Door Controller:Door2       19     Remote Login     2018-03-26 143 Main Offrice - 4 Door Controller:Door2       19     Remote Login     2018-03-26 103 Main Offrice - 4 Door Controller       19     Remote Diarming     2018-03-26 103 Main Offrice - 4 Door Controller       20     Remote Login     2018-03-26 103 Main Offrice - 4 Door Controller       20     Remote Login     2018-03-26 093 Main Offrice - 4 Door Controller       21     Remote Login     2018-03-26 093 Main Offrice - 4 Door Controller       21     Remote Login     2018-03-26 093 Main Offrice - 4 Door Controller		9					Normal Card	209435	2018-03-26	15:2 Main Office	- 4 Door Controller:Entranc	e Card Reader1		0
12     Remain Closed Stopped     2018-03-26 15.2 Main Offrice 4 Door Controller:Door2       13     Door Locked     2018-03-26 15.2 Main Offrice 4 Door Controller:Door2       14     Remain Closed Started     2018-03-26 15.2 Main Offrice 4 Door Controller:Door2       15     Remote: Remain Closed     2018-03-26 15.2 Main Offrice 4 Door Controller:Door2       16     Remote: Login     2018-03-26 14.3 Main Offrice 4 Door Controller:Door2       17     Remote: Logiout     2018-03-26 14.3 Main Offrice 4 Door Controller:Door2       18     Remote: Diarming     2018-03-26 10.3 Main Offrice 4 Door Controller:Door2       19     Remote: Login     2018-03-26 10.3 Main Offrice 4 Door Controller:Door2       20     Remote: Login     2018-03-26 10.3 Main Offrice 4 Door Controller:Door2       21     Remote: Login     2018-03-26 10.3 Main Offrice 4 Door Controller       20     Remote: Login     2018-03-26 09.3 Main Offrice 4 Door Controller       21     Remote: Login     2018-03-26 09.3 Main Offrice 4 Door Controller														
1     Dora Locked     2018-09-26 152 Main Office 4 Door Controller:Door2       14     Remain Closed Started     2018-09-26 152 Main Office 4 Door Controller:Door2       15     Remote Remain Closed     2018-09-26 152 Main Office 4 Door Controller:Door2       16     Remote Login     2018-09-26 143 Main Office 4 Door Controller:Door2       17     Remote Logout     2018-09-26 143 Main Office 4 Door Controller:Door2       18     Remote Logout     2018-09-26 103 Main Office 4 Door Controller       19     Remote: Diarming     2018-09-26 103 Main Office 4 Door Controller       20     Remote: Login     2018-09-26 093 Main Office 4 Door Controller       20     Remote: Login     2018-09-26 093 Main Office 4 Door Controller       20     Remote: Login     2018-09-26 093 Main Office 4 Door Controller       21     Remote: Logout     2018-09-26 093 Main Office 4 Door Controller														
14     Remain Closed Started     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       15     Remote: Remain Closed     2018-03-26 15.2 Main Office - 4 Door Controller:Door2       16     Remote: Login     2018-03-26 14.3 Main Office - 4 Door Controller:Door2       17     Remote: Logiout     2018-03-26 14.3 Main Office - 4 Door Controller:Door2       18     Remote: Diarming     2018-03-26 10.3 Main Office - 4 Door Controller       19     Remote: Login     2018-03-26 10.3 Main Office - 4 Door Controller       20     Remote: Login     2018-03-26 09.3 Main Office - 4 Door Controller       21     Remote: Logiout     2018-03-26 09.3 Main Office - 4 Door Controller														
15     Remote: Remain Closed     2018-03-26 152 Main Office - 4 Door Controller:Door/2       16     Remote: Login     2018-03-26 143 Main Office - 4 Door Controller:       17     Remote: Logout     2018-03-26 143 Main Office - 4 Door Controller       18     Remote: Diarming     2018-03-26 103 Main Office - 4 Door Controller       19     Remote: Login     2018-03-26 103 Main Office - 4 Door Controller       20     Remote: Login     2018-03-26 093 Main Office - 4 Door Controller       21     Remote: Logout     2018-03-26 093 Main Office - 4 Door Controller														
16     Remote: Login     2018-03-26 14:3 Main Office - 4 Door Controller       17     Remote: Logout     2018-03-26 14:3 Main Office - 4 Door Controller       18     Remote: Diarming     2018-03-26 10:3 Main Office - 4 Door Controller       19     Remote: Login     2018-03-26 10:3 Main Office - 4 Door Controller       20     Remote: Login     2018-03-26 09:3 Main Office - 4 Door Controller       21     Remote: Logout     2018-03-26 09:3 Main Office - 4 Door Controller														
17     Remote Logout     2018-03-26 14-3 Main Office - 4 Door Controller       18     Remote Arming     2018-03-26 10-3 Main Office - 4 Door Controller       19     Remote Disarming     2018-03-26 10-3 Main Office - 4 Door Controller       20     Remote: Login     2018-03-26 09-3 Main Office - 4 Door Controller       21     Remote: Logout     2018-03-26 09-3 Main Office - 4 Door Controller														
18     Remote: Aming     2018-03-26 10:3 Main Office - 4 Door Controller       19     Remote: Disaming     2018-03-26 10:3 Main Office - 4 Door Controller       20     Remote: Login     2018-03-26 09:3 Main Office - 4 Door Controller       21     Remote: Logout     2018-03-26 09:3 Main Office - 4 Door Controller			-											
19     Remote: Disarming     2018-03-26 10:3 Main Office - 4 Door Controller       20     Remote: Login     2018-03-26 09:3 Main Office - 4 Door Controller       21     Remote: Logout     2018-03-26 09:3 Main Office - 4 Door Controller			-											
20     Remote: Login     2018-03-26 09:3 Main Office - 4 Door Controller       21     Remote: Logout     2018-03-26 09:3 Main Office - 4 Door Controller				-										
21 Remote: Logout 2018-03-26 09:3 Main Office - 4 Door Controller				-										
		22							2018-03-26	09:3 Main Office	- 4 Door Controller			

## 3. Access Control Group Management.

4. The access control points of the selected access control group will be displayed on the right.

Click icon

on the Status Information panel to select a door.

- 5. Click the following button listed on the **Status Information** panel to control the door.
  - Open Door : Click to open the door once.
  - Close Door : Click to close the door once.
  - Remain Open: Click to keep the door open.
  - Remain Closed: Click to keep the door closed.
  - Capture : Click to capture the picture manually.
- 6. You can view the anti-control operation result in the Operation Log panel.

### Notes:

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

## 7.10.3 Real-time Card Swiping Record

r Status C	ard Swiping Record	Access Control Al	arm					
rd No.	Person Name	Organization	Event Time	Door Position	Direction	Operation	Card Holder Information	
							Person No.: Person Name:	
							Gender:	
							ID No.: Organization:	
							Phone No.: Address: Email:	
							Enten.	

Click Card Swiping Record tab to enter the following interface.

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

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

### 7.10.4 Real-time Access Control Alarm

### Purpose:

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

Click Access Control Alarm tab to enter the following interface.

Subscribe						
Alarm Type	Alarm Time	Alarm Location	Alarm Content	Opera	tion	
Remote: Disarm	2016-12-16 13:5	Access Controller	Remote: Disarm	2	$\odot$	
Remote: Arming	2016-12-16 13:5	Access Controller	Remote: Arming	2	0	
Remote: Login	2016-12-16 13:5	Access Controller	Remote: Login	2	0	
Remote: Disarm	2016-12-16 13:5	Access Controller	Remote: Disarm	2	0	
Remote: Logout	2016-12-16 13:5	Access Controller	Remote: Logout	2	$\odot$	
Remote: Login	2016-12-16 13:5	Access Controller	Remote: Login	2	0	
Remote: Arming	2016-12-16 13:4	Access Controller	Remote: Arming	2	$\odot$	
Remote: Login	2016-12-16 13:4	Access Controller	Remote: Login	2	0	
Remote: Disarm	2016-12-16 13:4	Access Controller	Remote: Disarm	2	$\odot$	
Door Locked	2016-12-16 13:4	Door1	Door Locked	ደ	0	
Unlock	2016-12-16 13:4	Door1	Unlock	ደ	0	
Remote: Arming	2016-12-16 13:4	Access Controller	Remote: Arming	2	0	
Remote: Login	2016-12-16 13:4	Access Controller	Remote: Login			
Remote: Disarm	2016-12-16 13:4	Access Controller	Remote: Disarm	2	0	

### Steps:

- All access control alarms will display in the list in real time. You can view the alarm type, alarm time, location, etc.
- 2. Click  $\stackrel{2}{\sim}$  to view the alarm on E-map.
- 3. You can click or to view the live view or the captured picture of the triggered camera when the alarm is trigged.

*Note:* For setting the triggered camera, refer to *Chapter 7.9.1 Access Control Event Linkage*.

4. Click **Subscribe** to select the alarm that the client can receive when the alarm is triggered.

Subscribe ×	T	INT
 Device Exception Door Event Card Reader Event Alarm Input	. ).	101
All		
✓ Device Tampering Alarm		
✓ No Memory Alarm		
✓ Network Disconnected		
Vetwork Recovered		
Low Battery Voltage		
Low Battery Voltage Recovered		
AC Power Off		
OK Cancel		

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

3)

## 7.11 Arming Control

### Purpose:

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

Steps:

- 1. Click **Tool->Device Arming Control** to pop up the Device Arming Control window.
- 2. Arm the device by checking the corresponding checkbox.

Then the alarm information will be auto uploaded to the client software when alarm occurs.

	Device Arming Control	¢ _
Hikvision Device		
 ✓ All	Arming Status	
✓ 10.16.6.250		
✓ 10.16.6.171	8	
10.18.146.81		
10.17.137.250	le .	
✓ 10.16.6.111	<b>₽</b>	
) P.	POP	Z T I O N

# **Appendix A Sound Prompt and Indicator**

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

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

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

Table 7-1	Description	of Dromot	- Sound
	DESCHOUOH		

/	Table 7-2 Description of LED Indicator						
1	LED Indicator Status	Description					
	Green and blinking	Card reader is working normally.					
	Solid green	The operation of pressing keys or swiping card is valid.					
	Solid red	The operation of pressing keys or swiping card is invalid.					
		For RS-485 protocol: Registering failed or card reader is					
	Red and blinking	offline. Failed to get key files of PSAM card; Failed to					
		detect the PSAM card.					
	Red and Keeping	Available for reading file mode of CPU card: PSAM is not					
	rapidly blinking	inserted or undetected.	Π.Τ.				
		חואאחחאא	1/1				

# Appendix B Custom Wiegand Rule Descriptions

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

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

Wiegand Data = Valid Data + Parity Data

Total Length: Wiegand data length.

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

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

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

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

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

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

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

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

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

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

0200001071120





This manual has been modified by Ness Corporation for our valued customers.



www.nesscorporation.com

www.hikvision.com