Access Controller

User Manual

Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Available Model

Product Name	Model
Access Controller	DS-K2601T Series Access Controller
	DS-K2602T Series Access Controller
	DS-K2604T Series Access Controller
	DS-K2601-G Access Controller
	DS-K2602-G Access Controller
	DS-K2604-G Access Controller

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
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
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

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, RE Directive 2014/53/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 (B)/NMB-3(B) standards requirements.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.
Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- An appropriate disconnect device shall be provided as part of installation.

  Note

  External disconnect devices will not necessarily be supplied with the equipment.
- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The 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.

Contents

Chapter 1 Preventive and Cautionary Tips 1

Chapter 2 Product Description 2

Chapter 3 Main Board Description 3

3.1 Single-Door Access Controller Main Board Description 3

3.2 Two-Door Access Controller Main Board Description 4

3.3 Four-Door Access Controller Main Board Description 5

3.4 Component Description 5

Chapter 4 Terminal Description 8

4.1 Single-Door Access Controller Terminal Description 8

4.2 Two-Door Access Controller Terminal Description 12

4.3 Four-Door Access Controller Terminal Description 17

Chapter 5 Terminal Wiring 24

5.1 External Terminal 24

5.1.1 Single-Door Access Controller Terminal Description 24

5.1.2 Two-Door Access Controller Terminal Description 25

5.1.3 Four-Door Access Controller Terminal Description 25

5.2 Wiegand Card Reader Wiring 25

5.3 RS-485 Card Reader Wiring 27

5.4 Cathode Lock Wiring 28

5.5 Anode Lock Wiring 28

5.6 External Alarm Device Wiring 29

5.7 Exit Button Wiring 30

5.8 Door Contact Wiring 31

5.9 Power Supply Wiring 32

5.10 Arming Region Input Wiring 33

5.10.1 NO Wiring of Arming Region Input 33

5.10.2 NC Wiring of Arming Region Input 34
5.11 Fire Alarm Module Wiring 35
Chapter 6 Settings 37
6.1 Initialization (Option 1) 37
6.2 Initialization (Option 2) 37
6.3 Relay Output NO/NC Settings 38
6.3.1 Lock Relay Output Settings 38
6.3.2 Alarm Relay Output Settings 39
Chapter 7 Activation 41
7.1 Activate via SADP 41
7.2 Activate Device via Client Software 42
Chapter 8 Client Software Configuration 44
8.1 Operation on Client Software 44
8.1.1 Add Device 44
8.1.2 Select Application Scenario 53
8.1.3 Configure Other Parameters 54
8.1.4 Manage Organization 56
8.1.5 Manage Person Information 57
8.1.6 Configure Schedule and Template 70
8.1.7 Manage Permission 73
8.1.8 Configure Advanced Functions 75
8.1.9 Search Access Control Event 92
8.1.10 Configure Access Control Alarm Linkage 93
8.1.11 Manage Access Control Point Status 101
8.1.12 Control Door during Live View 103
8.1.13 Display Access Control Point on E-map 104
8.2 Remote Configuration (Web) 105
8.2.1 Time Management 105

8.2.2 Network Parameters Settings 106
8.2.3 Report Strategy Settings 106
8.2.4 Network Center Parameters Settings 107
8.2.5 Change Device Password 107
8.2.6 Security Mode Settings 108
8.2.7 Optimize Event Name 108
8.2.8 Set Event Mode 109
8.2.9 System Maintenance 109
8.3 Time and Attendance 110
8.3.1 Manage Shift Schedule 110
8.3.2 Manually Correct Check-in/out Record 115
8.3.3 Add Leave and Business Trip 115
8.3.4 Calculate Attendance Data 116
8.3.5 Configure Advanced Settings 117
8.3.6 View Attendance Report 123
Appendix A. Tips for Scanning Fingerprint 130
Appendix B. DIP Switch Description 132
Appendix C. Custom Wiegand Rule Descriptions 133

Chapter 1 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.

Chapter 2 Product Description

- 32-bit high-speed processor
- Supports TCP/IP communication, EHome 5.0 accessing, ISAPI protocol, and OSDP protocol. The communication data is specially encrypted to relieve the concern of privacy leak
- Supports recognition and storage of card No. with maximum length of 20
- Supports up to 100,000 cards and 300,000 card presenting records
- Supports multi-door interlock function, anti-passback function, multiple authentications function, open door with first card function, super card and super password function, M1 card encryption, online upgrade function and remote control of the doors
- Supports tampering alarm for the card reader, alarm for door not secured, force opening door alarm, alarm for door opening timeout, duress card and code alarm, blocklist alarm and alarm for illegal card swiping attempts reaching the limit
- Short circuit attempts alarm and open circuit attempts alarm
- IP address conflict detection
- Cross-controller anti-passback function (For cross-controller anti-passback based on card, wire the card reader with RS-485. For cross-controller anti-passback based on network, make sure the server and device communicate with each other properly. Up to 5000 card swiping records can be stored in the selected server.) and inner-device anti-passback function
- Supports RS-485 interface and Wiegand interface for accessing card reader. Wiegand interface supports W26, W34 and is compatible with the third-party card reader with Wiegand interface
- Supports adding various person types: normal person, visitor, and person in blocklist.
- Supports various card types: normal/disabled/blocklist/patrol/visitor/duress/super card, etc.
- Various indicators to show different status
- Supports automatically and manually time synchronization
- Supports record storage function when the device is offline and insufficient storage space storage alarm function
- Backup battery design, watchdog design and tamper-proof function
- Data can be permanently saved after the access controller is powered off
- Supports I/O linkage and event linkage
- Supports EHome protocol to connect with public network
- 500 groups of password under the authentication mode of card or password
- Supports time zone settings

Chapter 3 Main Board Description

3.1 Single-Door Access Controller Main Board Description

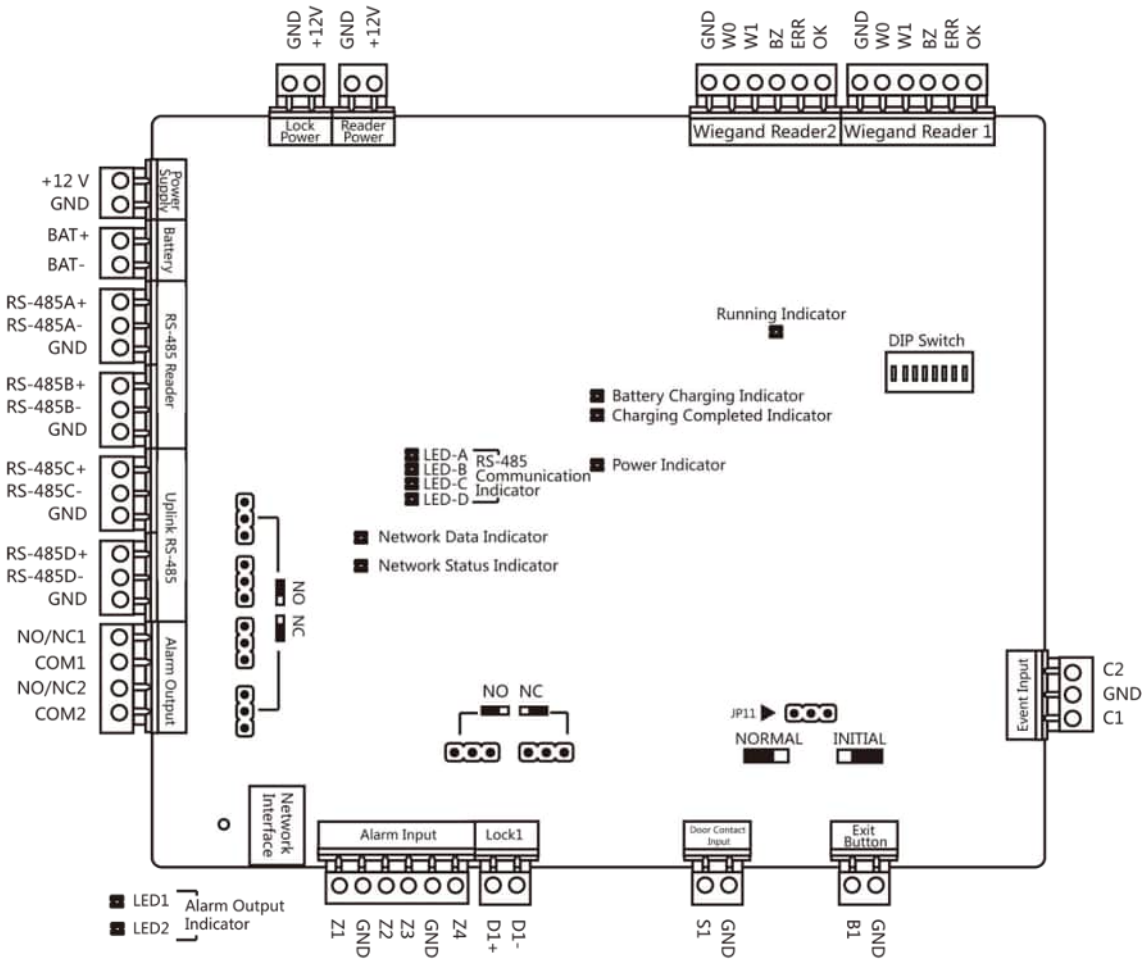


Figure 3-1 Single-Door Access Controller Main Board

3.2 Two-Door Access Controller Main Board Description

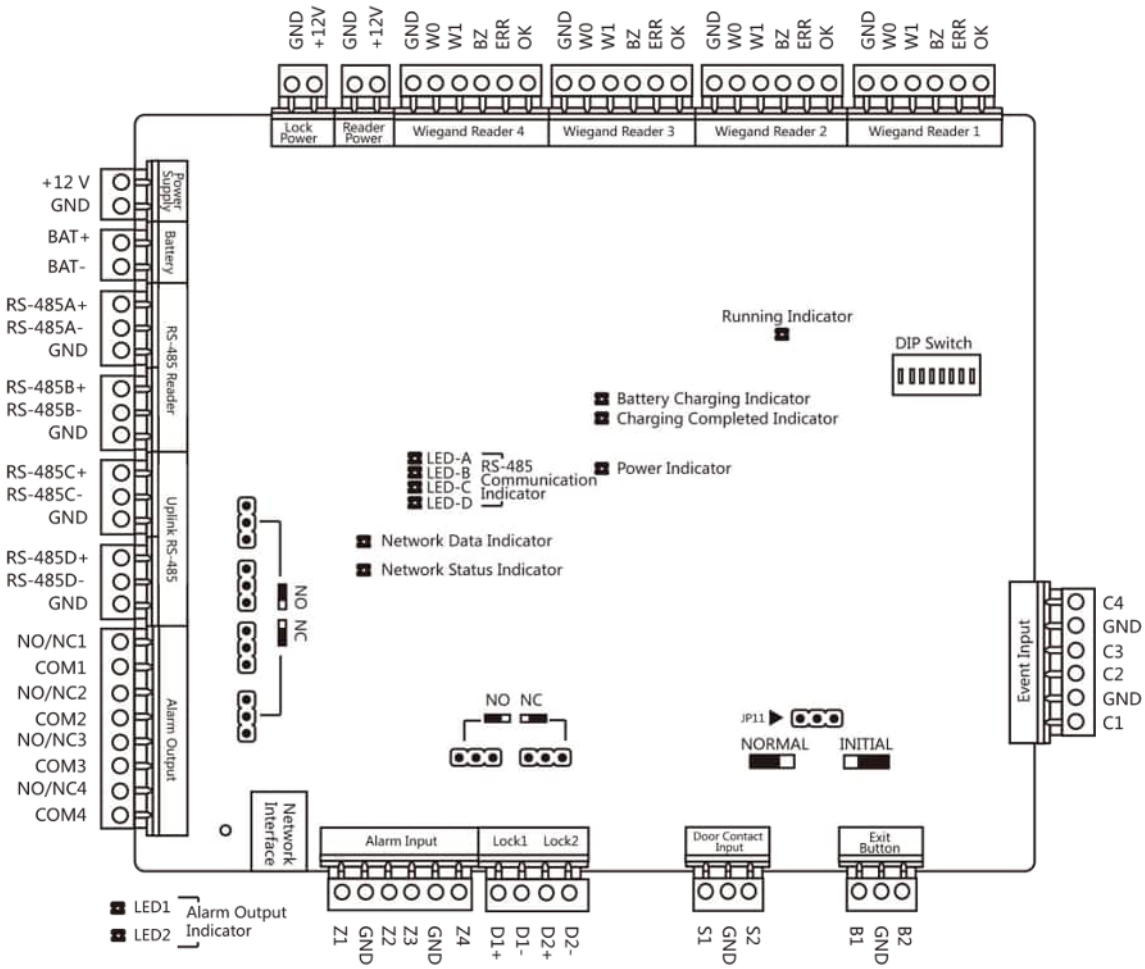


Figure 3-2 Two-Door Access Controller Main Board

3.3 Four-Door Access Controller Main Board Description

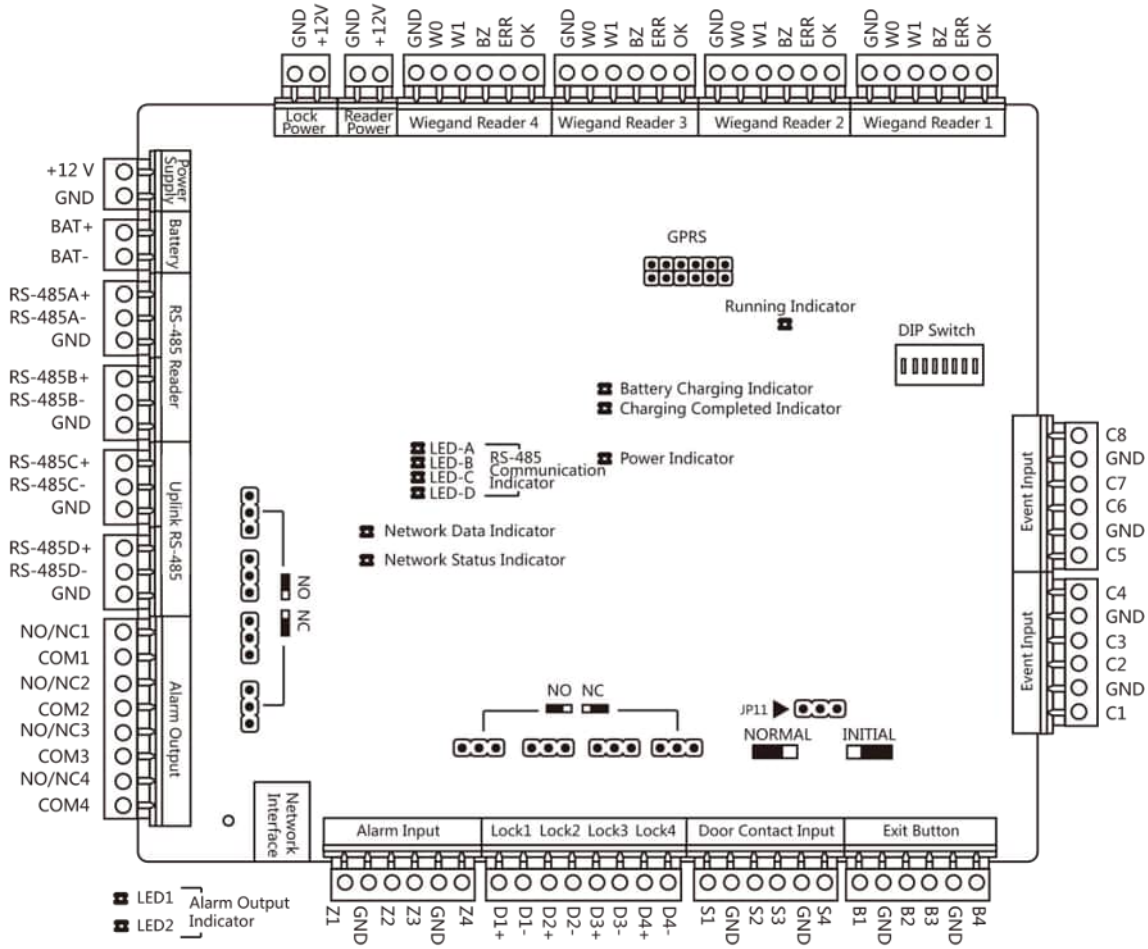


Figure 3-3 Four-Door Access Controller Main Board

3.4 Component Description

You can view the device's components and their descriptions.

Take four-door access controller as an example, the component diagram is shown below.

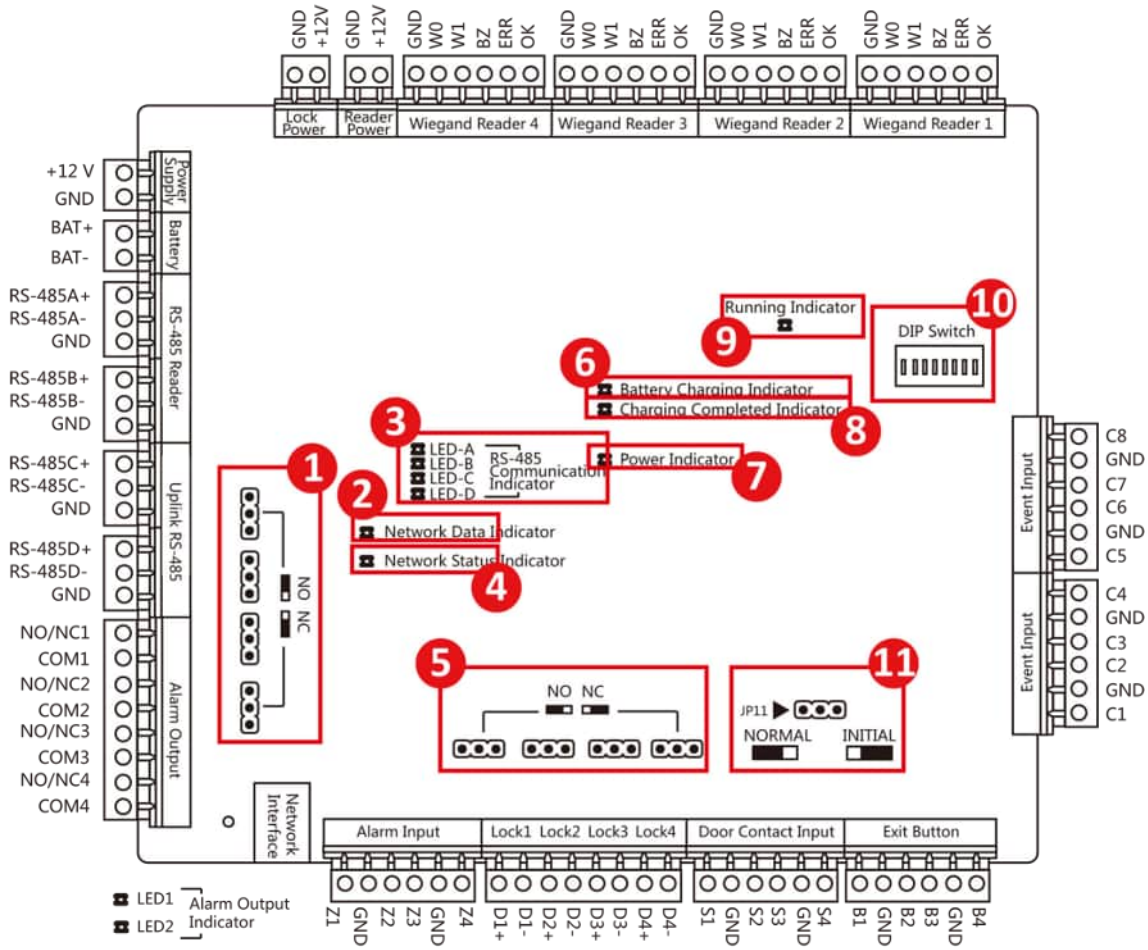


Figure 3-4 Four-Door Access Controller Component Diagram

Table 3-1 Four-Door Access Controller Component Description

No.	Component Description		
	Single-Door Access Controller	Two-Door Access Controller	Four-Door Access Controller
1	Alarm Relay Output Status (NC/NO)		
2	Network Data Indicator		
3	RS-485 Communication Indicator		
4	Network Status Indicator		
5	Door Relay Output Status (NC/NO) Choice		
6	Battery Charging Indicator		

7	Power Indicator
8	Charging Completing Indicator
9	Running Indicator
10	Main Board DIP Switch Set the DIP address for the access controller. Available range: 1 to 63. Example: If the DIP address is 24, switch Bit 4 and Bit 5 to ON. **Note** • The settings will be valid after the device reboot. • For details about the DIP settings, see *Appendix A DIP Switch Description*.
11	Hardware Initialization and Normal Working Choice

Chapter 4 Terminal Description

Note

- 2602 and 2604 series: The rated power for door lock is 12 V/2 A, and for card reader power supply is 12 V/0.67 A.
- 2601 series: The rated power for door lock is 12 V/0.5 A, and for card reader power supply is 12 V/0.3 A.

4.1 Single-Door Access Controller Terminal Description

You can view the single-door access controller's terminal description.

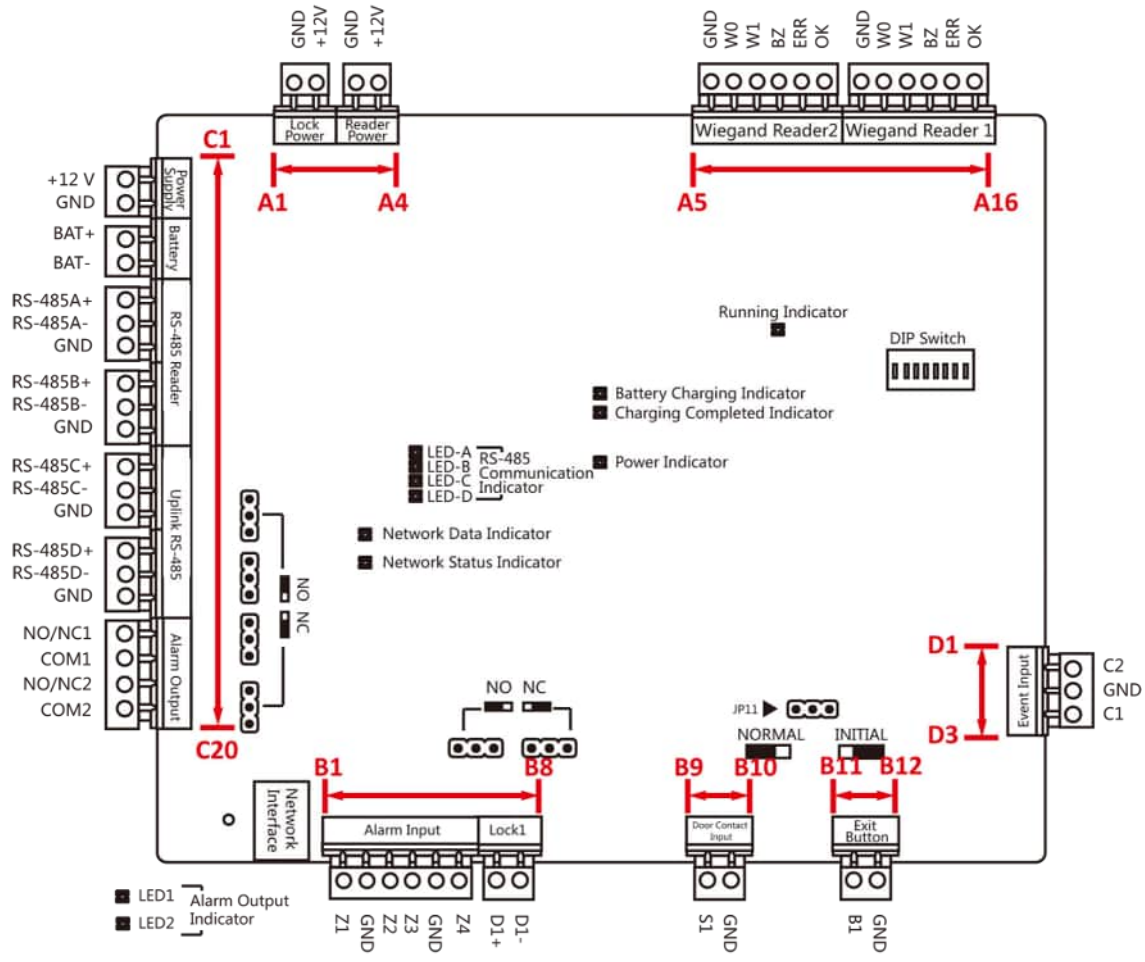


Figure 4-1 Single-Door Access Controller Main Board

Table 4-1 Single-Door Access Controller Terminal Description

No.	Single-Door Access Controller		
A1	Power Supply of E-Lock	GND	Grounding
A2		+12 V	Power Supply of E-Lock Output
A3	Power Supply of Card Reader	GND	Grounding
A4		+12 V	Power Supply of Card Reader Output
A5	Wiegand Card Reader 2	GND	Grounding
A6		W0	Wiegand Card Reader Data Input Data0
A7		W1	Wiegand Card Reader Data Input Data1
A8		BZ	Card Reader Buzzer Control Output
A9		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A10		OK	Indicator of Card Reader Control Output (Valid Card Output)
A11	Wiegand Card Reader 1	GND	Grounding
A12		W0	Wiegand Card Reader Data Input Data0
A13		W1	Wiegand Card Reader Data Input Data1
A14		BZ	Card Reader Buzzer Control Output
A15		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A16		OK	Indicator of Card Reader Control Output (Valid Card Output)

No.	Single-Door Access Controller		
B1	Arming Region Input	Z1	Arming Region Access Terminal 1
B2		GND	Grounding
B3		Z2	Arming Region Access Terminal 2
B4		Z3	Arming Region Access Terminal 3
B5		GND	Grounding
B6		Z4	Arming Region Access Terminal 4
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	+12 V	12 VDC Cathode
C2		GND	Grounding
C3	Battery	BAT+	12 VDC Battery Cathode
C4		BAT-	12 VDC Battery Anode
C5	RS-485 Card Reader Interface	RS485A+	Card Reader RS485A+ Access
C6		RS485A-	Card Reader RS485A- Access
C7		GND	Grounding
C8		RS485B+	Card Reader RS485B+
C9		RS485B-	Card Reader RS485B-
C10		GND	Grounding

No.	Single-Door Access Controller		
C11	Access Controller RS485 Interface	RS485C+	Uplink RS485+Communication
C12		RS485C-	Uplink RS485-Communication
C13		GND	Grounding
C14		RS 485D+	Reserved
C15		RS 485D-	
C16		GND	
C17	Alarm Output	NO/NC1	Alarm Relay 1 Output (Dry Contact)
C18		COM1	
C19		NO/NC2	Alarm Relay 2 Output (Dry Contact)
C20		COM2	
D1	Event Input	C2	Event Alarm Input 2
D2		GND	Grounding
D3		C1	Event Alarm Input 1

Note

- The Alarm input hardware interface is normally open by default. Only the normally open signal is allowed. It can be linked to the buzzer of the card reader and access controller, the alarm relay output, and door relay open and close.
- Arming region alarm input linkage is only for the alarm relay output linkage.
- RS-485 card reader ID should be set as 1to 2. The table displayed below shows the relationship between the door No. and the ID.

Door No.	RS-485 Card Reader ID	Description
Door 1	1	Enter
	2	Exit

- For single-door access controller, the Wiegand card reader and door's relationship is as follows.

Door No.	Wiegand Card Reader	Description
Door 1	1	Enter
	2	Exit

4.2 Two-Door Access Controller Terminal Description

You can view the two-door access controller's terminal description.

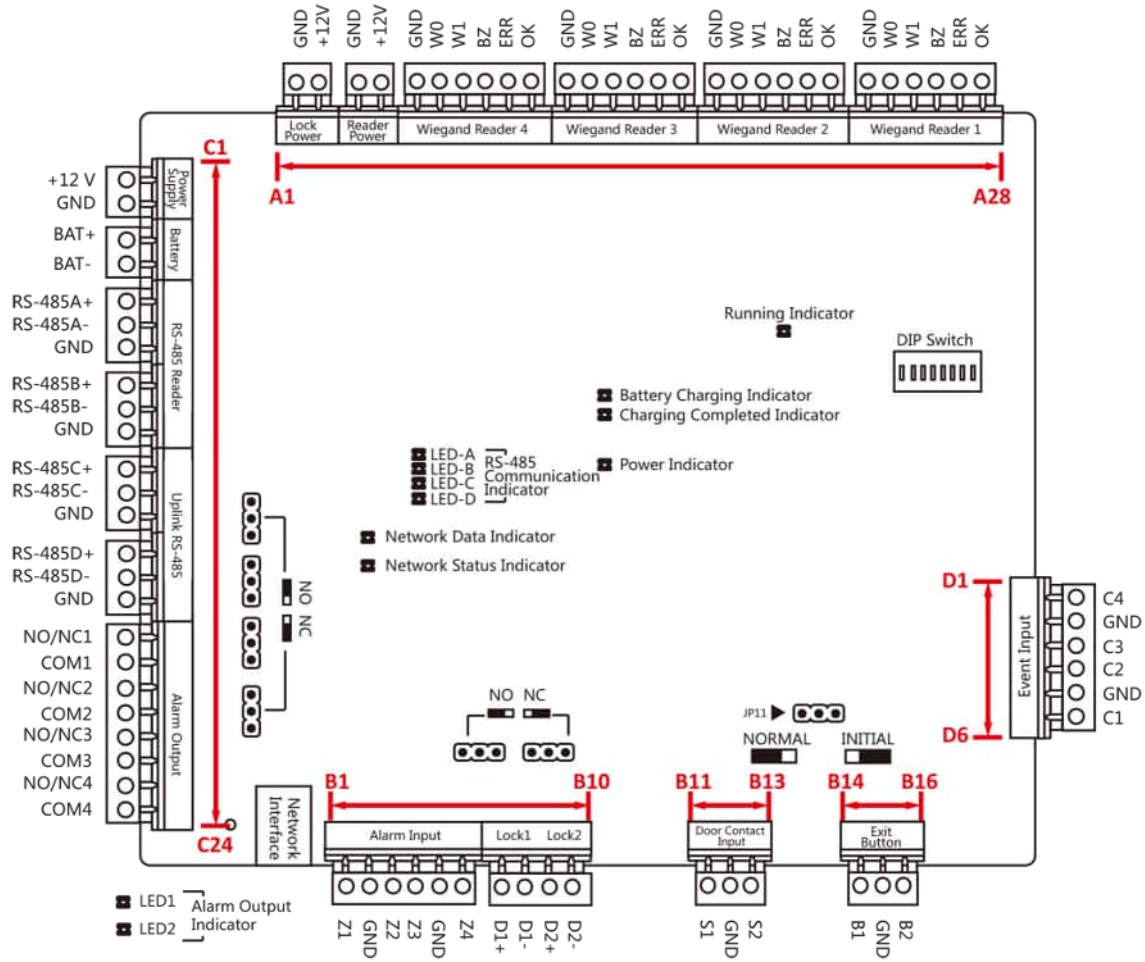


Figure 4-2 Two-Door Access Controller Main Board

Table 4-2 Two-Door Access Controller Terminal Description

No.	Two-Door Access Controller		
A1	Power Supply of E-Lock	GND	Grounding
A2		+12 V	Power Supply of E-Lock Output
A3	Power Supply of Card Reader	GND	Grounding
A4		+12 V	Power Supply of Card Reader Output
A5	Wiegand Card Reader 4	GND	Grounding
A6		W0	Wiegand Card Reader Data Input Data0
A7		W1	Wiegand Card Reader Data Input Data1
A8		BZ	Card Reader Buzzer Control Output
A9		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A10		OK	Indicator of Card Reader Control Output (Valid Card Output)
A11	Wiegand Card Reader 3	GND	Grounding
A12		W0	Wiegand Card Reader Data Input Data0
A13		W1	Wiegand Card Reader Data Input Data1
A14		BZ	Card Reader Buzzer Control Output
A15		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A16		OK	Indicator of Card Reader Control Output (Valid Card Output)

No.	Two-Door Access Controller		
A17	Wiegand Card Reader 2	GND	Grounding
A18		W0	Wiegand Card Reader Data Input Data0
A19		W1	Wiegand Card Reader Data Input Data1
A20		BZ	Card Reader Buzzer Control Output
A21		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A22		OK	Indicator of Card Reader Control Output (Valid Card Output)
A23	Wiegand Card Reader 1	GND	Grounding
A24		W0	Wiegand Card Reader Data Input Data0
A25		W1	Wiegand Card Reader Data Input Data1
A26		BZ	Card Reader Buzzer Control Output
A27		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A28		OK	Indicator of Card Reader Control Output (Valid Card Output)
B1	Arming Region Input	Z1	Arming Region Access Terminal 1
B2		GND	Grounding
B3		Z2	Arming Region Access Terminal 2
B4		Z3	Arming Region Access Terminal 3

No.	Two-Door Access Controller		
B5		GND	Grounding
B6		Z4	Arming Region Access Terminal 4
B7	E-Lock1	D1+	Door 1 Door Relay Input (Dry Contact)
B8		D1-	
B9	E-Lock2	D2+	Door 2 Door Relay Input (Dry Contact)
B10		D2-	
B11	Door Magnetic Detector	S1	Door 1 Magnetic Detector Input
B12		GND	Grounding
B13		S2	Door 2 Magnetic Detector Input
B14	Door Button	B1	Door 1 Door Button Input
B15		GND	Grounding
B16		B2	Door 2 Door Button Input
C1	Power	+12 V	12 VDC Cathode
C2		GND	Grounding
C3	Battery	BAT+	12 VDC Battery Cathode
C4		BAT-	12 VDC Battery Anode
C5	RS485 Card Reader Interface	RS485A+	Card Reader RS485A+ Access
C6		RS485A-	Card Reader RS485A- Access
C7		GND	Grounding
C8		RS485B+	Card Reader RS485B+
C9		RS485B-	Card Reader RS485B-
C10		GND	Grounding

No.	Two-Door Access Controller		
C11	Access Controller RS485 Interface	RS485C+	Uplink RS485+Communication
C12		RS485C-	Uplink RS485-Communication
C13		GND	Grounding
C14		RS 485D+	Reserved
C15		RS 485D-	
C16		GND	
C17	Alarm Output	NO/NC1	Alarm Relay 1 Output (Dry Contact)
C18		COM1	
C19		NO/NC2	Alarm Relay 2 Output (Dry Contact)
C20		COM2	
C21		NO/NC3	Alarm Relay 3 Output (Dry Contact)
C22		COM3	
C23		NO/NC4	Alarm Relay 4 Output (Dry Contact)
C24		COM4	
D1	Event Input	C4	Event Alarm Input 4
D2		GND	Grounding
D3		C3	Event Alarm Input 3
D4		C2	Event Alarm Input 2
D5		GND	Grounding
D6		C1	Event Alarm Input 1

Note

- 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, the alarm relay output, and door relay open and close.
- Arming region alarm input linkage is only for the alarm relay output linkage.
- RS-485 card reader ID should be set as 1 to 8.

Door No.	RS-485 Card Reader ID	Description
Door 1	1	Enter
	2	Exit
Door 2	3	Enter
	4	Exit

- For two-door access controller, the Wiegand card reader and door's relationship is as follows.

Door No.	Wiegand Card Reader	Description
Door 1	1	Enter
	2	Exit
Door 2	3	Enter
	4	Exit

4.3 Four-Door Access Controller Terminal Description

You can view the four-door access controller's terminal description.

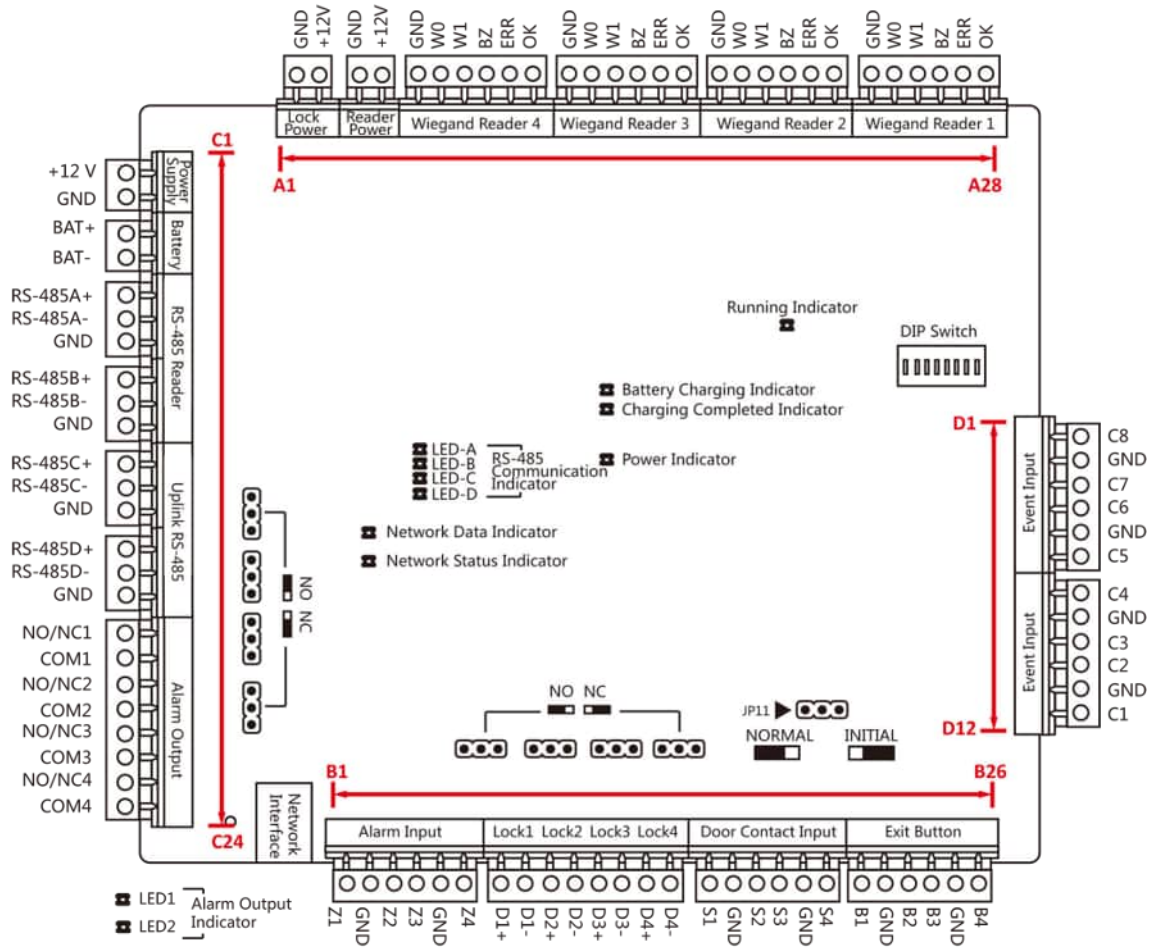


Figure 4-3 Four-Door Access Controller Main Board

Table 4-3 Four-Door Access Controller Terminal Description

No.	Four-Door Access Controller		
A1	Power Supply of E-Lock	GND	Grounding
A2		+12 V	Power Supply of E-Lock Output
A3	Power Supply of Card Reader	GND	Grounding
A4		+12 V	Power Supply of Card Reader Output
A5	Wiegand Card Reader 4	GND	Grounding
A6		W0	Wiegand Card Reader Data Input Data0

No.	Four-Door Access Controller		
A7		W1	Wiegand Card Reader Data Input Data1
A8		BZ	Card Reader Buzzer Control Output
A9		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A10		OK	Indicator of Card Reader Control Output (Valid Card Output)
A11	Wiegand Card Reader 3	GND	Grounding
A12		W0	Wiegand Card Reader Data Input Data0
A13		W1	Wiegand Card Reader Data Input Data1
A14		BZ	Card Reader Buzzer Control Output
A15		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A16		OK	Indicator of Card Reader Control Output (Valid Card Output)
A17	Wiegand Card Reader 2	GND	Grounding
A18		W0	Wiegand Card Reader Data Input Data0
A19		W1	Wiegand Card Reader Data Input Data1
A20		BZ	Card Reader Buzzer Control Output
A21		ERR	Indicator of Card Reader Control Output (Invalid Card Output)

No.	Four-Door Access Controller		
A22		OK	Indicator of Card Reader Control Output (Valid Card Output)
A23	Wiegand Card Reader 1	GND	Grounding
A24		W0	Wiegand Card Reader Data Input Data0
A25		W1	Wiegand Card Reader Data Input Data1
A26		BZ	Card Reader Buzzer Control Output
A27		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
A28		OK	Indicator of Card Reader Control Output (Valid Card Output)
B1	Arming Region Input	Z1	Arming Region Access Terminal 1
B2		GND	Grounding
B3		Z2	Arming Region Access Terminal 2
B4		Z3	Arming Region Access Terminal 3
B5		GND	Grounding
B6		Z4	Arming Region Access Terminal 4
B7	E-Lock1	D1+	Door 1 Door Relay Input (Dry Contact)
B8		D1-	
B9	E-Lock2	D2+	Door 2 Door Relay Input (Dry Contact)
B10		D2-	
B11	E-Lock3	D3+	Door 3 Door Relay Input (Dry Contact)
B12		D3-	

No.	Four-Door Access Controller		
B13	E-Lock4	D4+	Door 4 Door Relay Input (Dry Contact)
B14		D4-	
B15	Door Magnetic Detector	S1	Door 1 Magnetic Detector Input
B16		GND	Grounding
B17		S2	Door 2 Magnetic Detector Input
B18		S3	Door 3 Magnetic Detector Input
B19		GND	Grounding
B20		S4	Door 4 Magnetic Detector Input
B21	Door Button	B1	Door 1 Door Button Input
B22		GND	Grounding
B23		B2	Door 2 Door Button Input
B24		B3	Door 3 Door Button Input
B25		GND	Grounding
B26		B4	Door 4 Door Button Input
C1	Power	+12 V	12 VDC Cathode
C2		GND	Grounding
C3	Battery	BAT+	12 VDC Battery Cathode
C4		BAT-	12 VDC Battery Anode
C5	RS485 Card Reader Interface	RS485A+	Card Reader RS485A+ Access
C6		RS485A-	Card Reader RS485A- Access
C7		GND	Grounding

No.	Four-Door Access Controller		
C8		RS485B+	Card Reader RS485B+
C9		RS485B-	Card Reader RS485B-
C10		GND	Grounding
C11	Access Controller RS485 Interface	RS485C+	Uplink RS485+Communication
C12		RS485C-	Uplink RS485-Communication
C13		GND	Grounding
C14		RS 485D+	Reserved
C15		RS 485D-	
C16		GND	
C17	Alarm Output	NO/NC1	Alarm Relay 1 Output (Dry Contact)
C18		COM1	
C19		NO/NC2	Alarm Relay 2 Output (Dry Contact)
C20		COM2	
C21		NO/NC3	Alarm Relay 3 Output (Dry Contact)
C22		COM3	
C23		NO/NC4	Alarm Relay 4 Output (Dry Contact)
C24		COM4	
D1	Event Input	C8	Event Alarm Input 8
D2		GND	Grounding
D3		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 Input 3
D10		C2	Event Alarm Input 2

No.	Four-Door Access Controller		
D11		GND	Grounding
D12		C1	Event Alarm Input 1

Note

- 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 door relay open and close.
- Arming region alarm input linkage is only for the alarm relay output linkage.
- RS-485 card ID should be set as 1to 8.

Door No.	RS-485 Card Reader ID	Description
Door 1	1	Enter
	2	Exit
Door 2	3	Enter
	4	Exit
Door 3	5	Enter
	6	Exit
Door4	7	Enter
	8	Exit

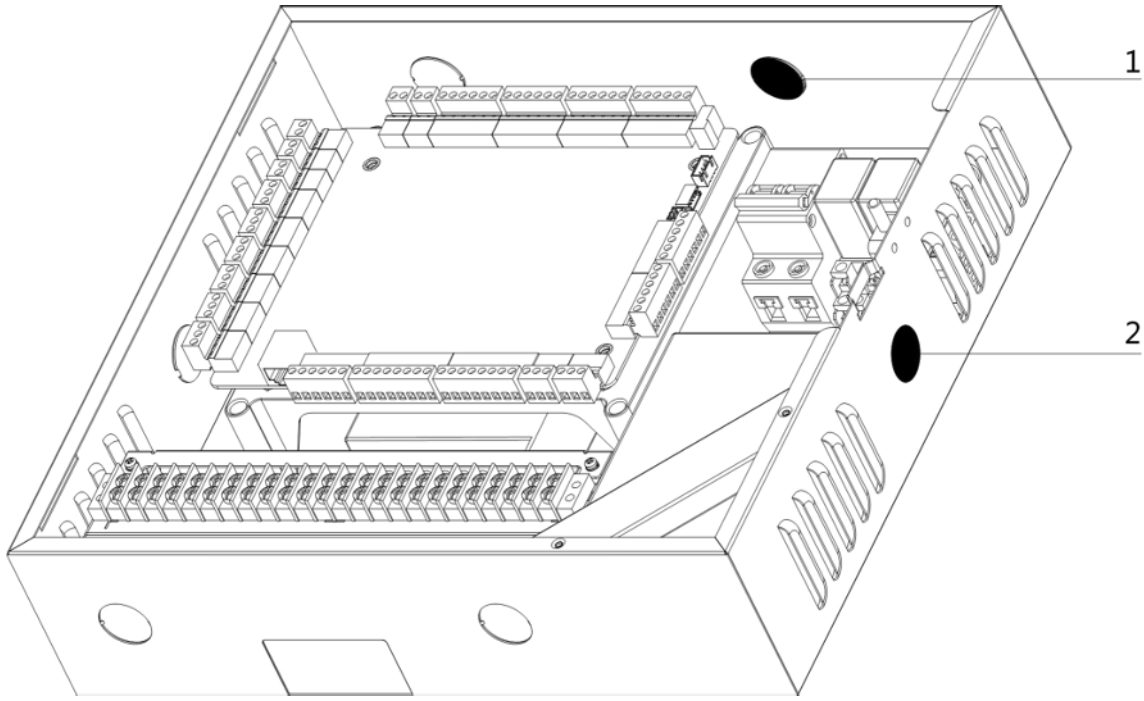
- For four-door access controller, the Wiegand card reader and door's relationship is as follows.

Door No.	Wiegand Card Reader	Description
Door 1	1	Enter
	/	Exit
Door 2	2	Enter
	/	Exit
Door 3	3	Enter
	/	Exit
Door 4	4	Enter
	/	Exit

Chapter 5 Terminal Wiring

Warning

The high voltage cable should be threaded through the Hole 1 and Hole 2. The Hole 1 and Hole 2 should be installed with rubber ring to avoid the sharp edge cutting the cable and avoid electric shock.



5.1 External Terminal

5.1.1 Single-Door Access Controller Terminal Description

You can view the single-door access controller's terminals diagram.

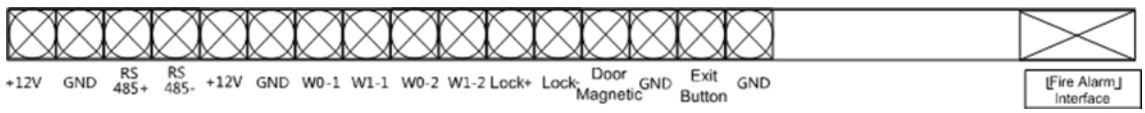


Figure 5-1 Single-Door Access Controller Terminals

5.1.2 Two-Door Access Controller Terminal Description

You can view the two-door access controller's terminals diagram.

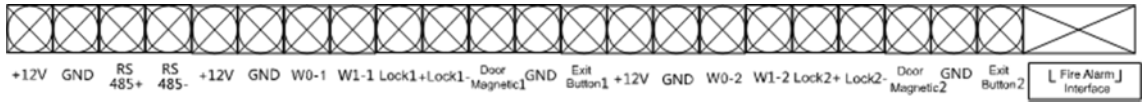


Figure 5-2 Two-Door Access Controller Terminals

5.1.3 Four-Door Access Controller Terminal Description

You can view the four-door access controller's terminals diagram.

Figure 5-3 Four-Door Access Controller Terminal

5.2 Wiegand Card Reader Wiring

You can view the Wiegand card reader wiring diagram.

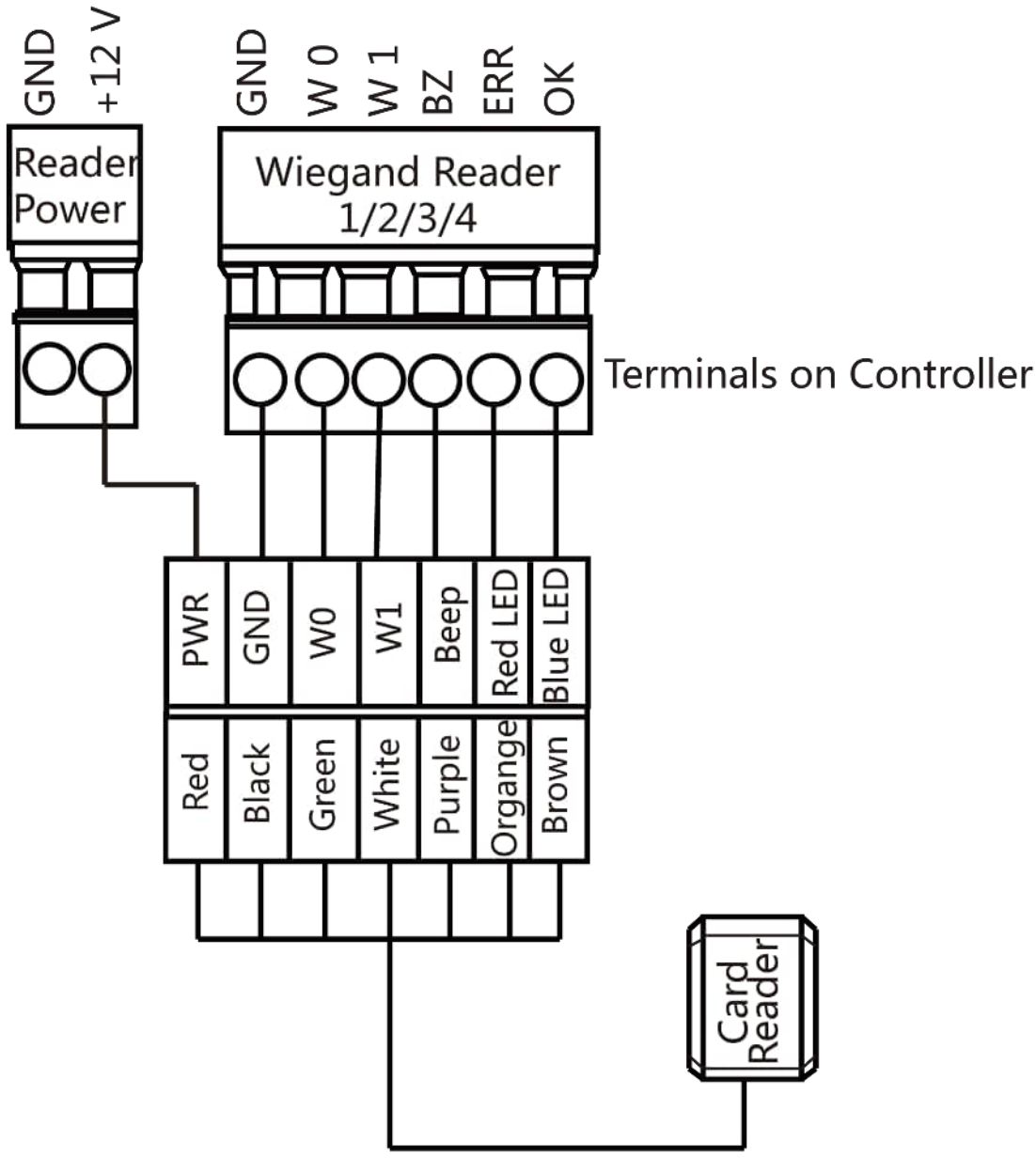


Figure 5-4 Wiegand Card Reader Wiring Diagram

Note

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

5.3 RS-485 Card Reader Wiring

You can view the RS-485 card reader wiring diagram.

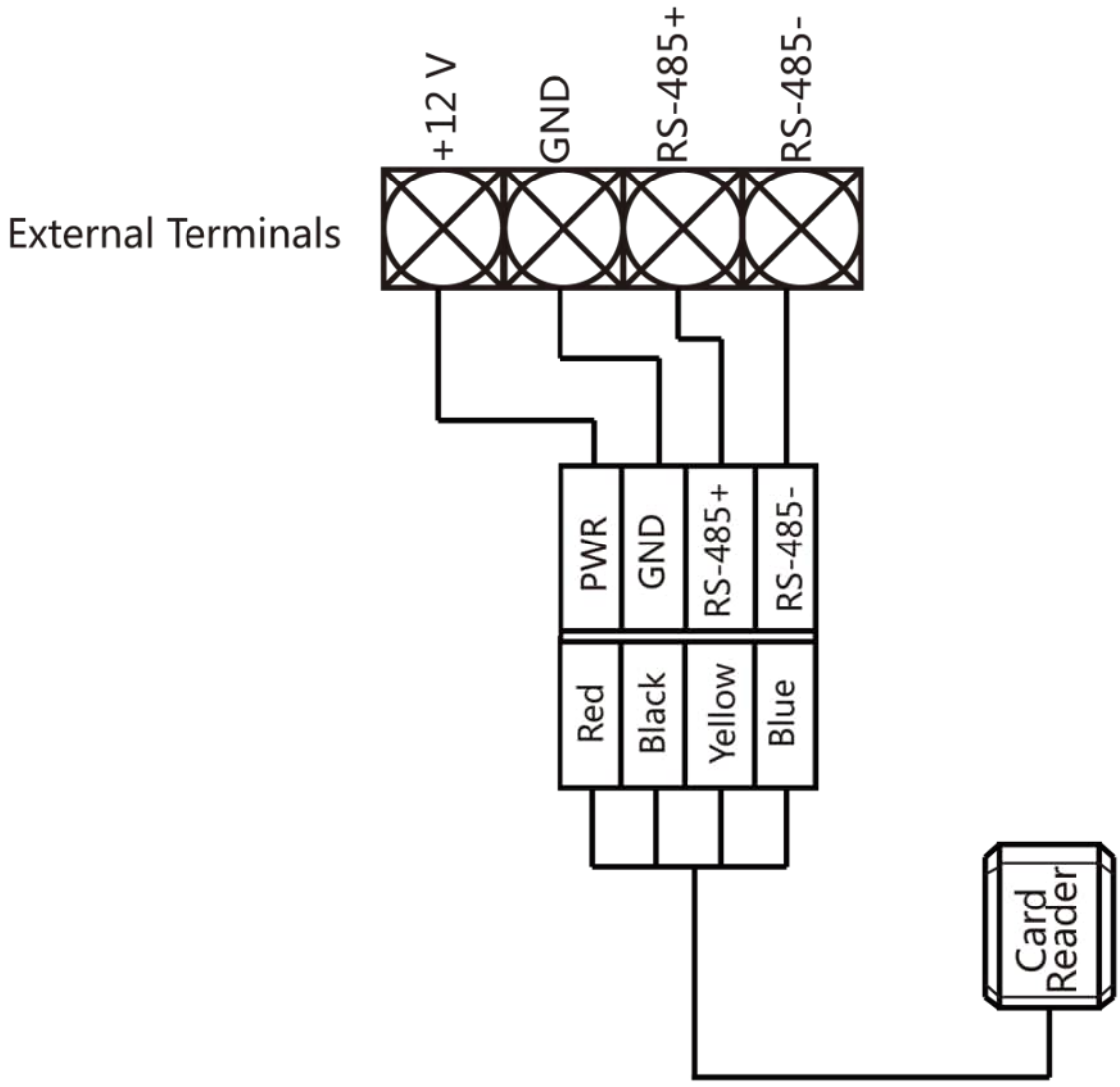


Figure 5-5 RS-485 Card Reader Wiring Diagram

Note

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

5.4 Cathode Lock Wiring

You can view the cathode lock wiring diagram.

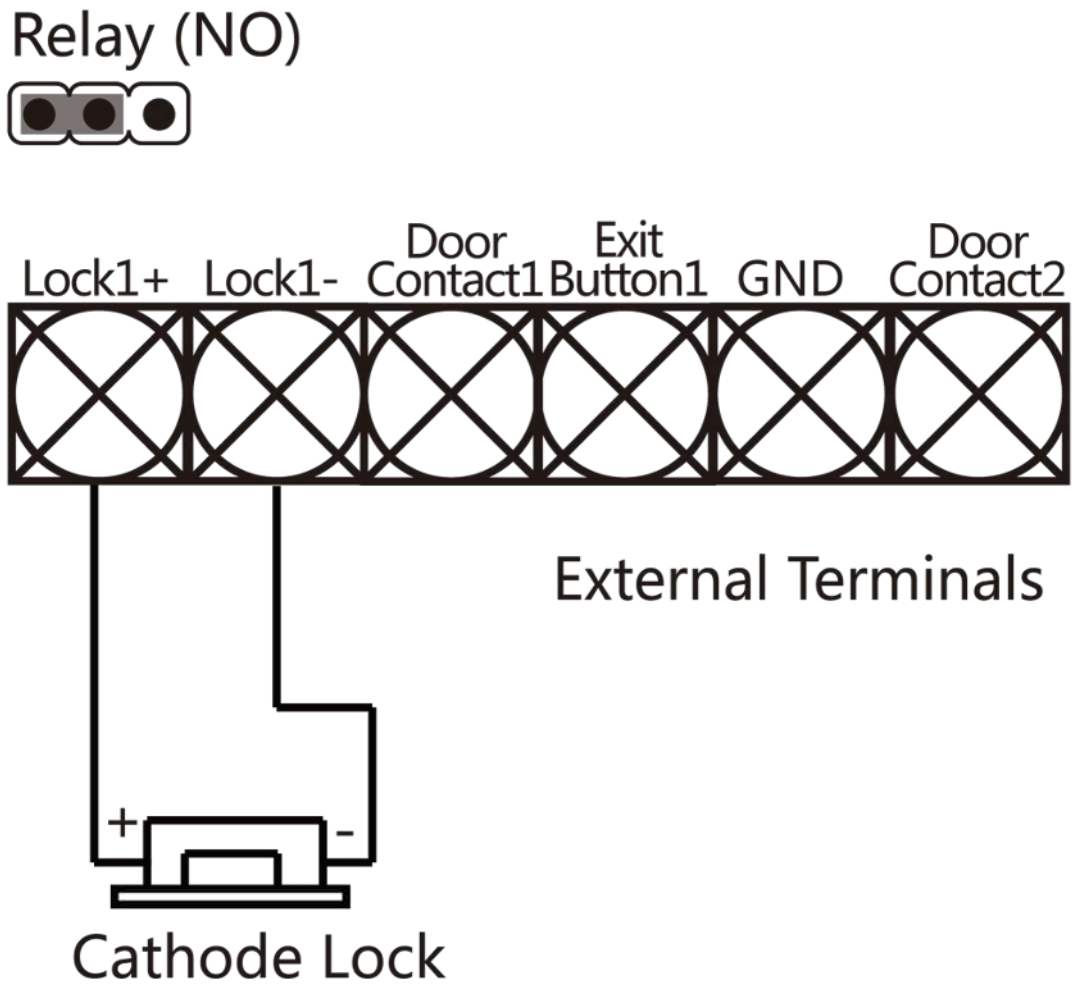


Figure 5-6 Wiring Diagram of Cathode Lock

5.5 Anode Lock Wiring

You can view the anode lock wiring diagram.

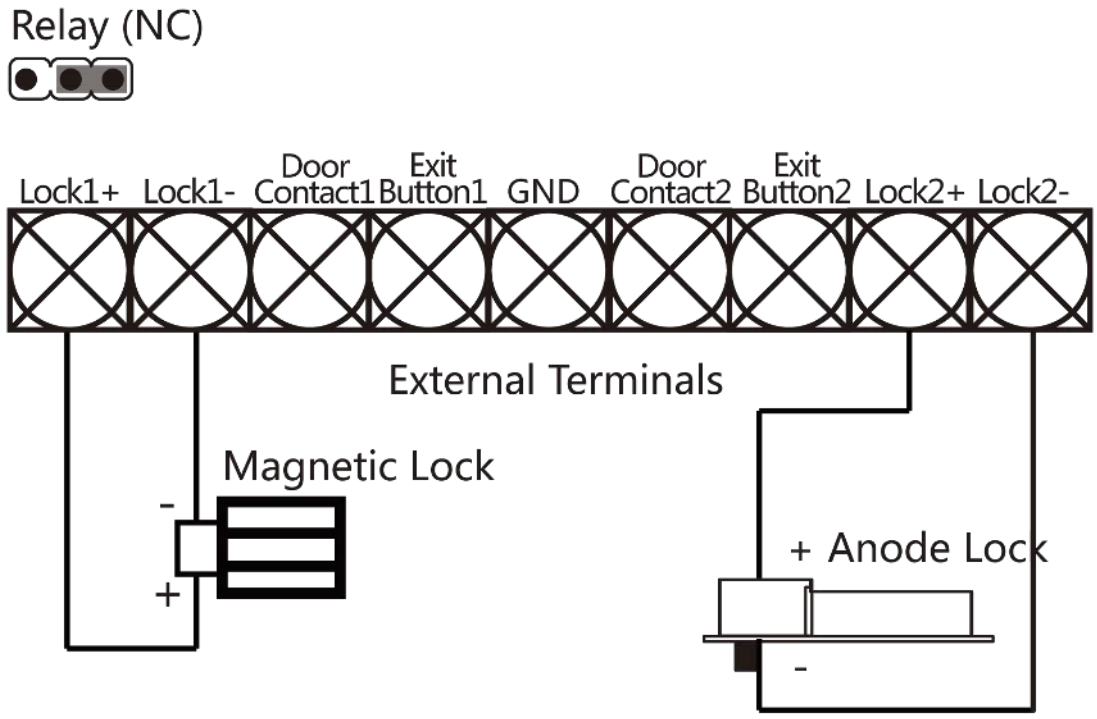


Figure 5-7 Wiring Diagram of Anode Lock

5.6 External Alarm Device Wiring

You can view the external alarm device wiring diagram.

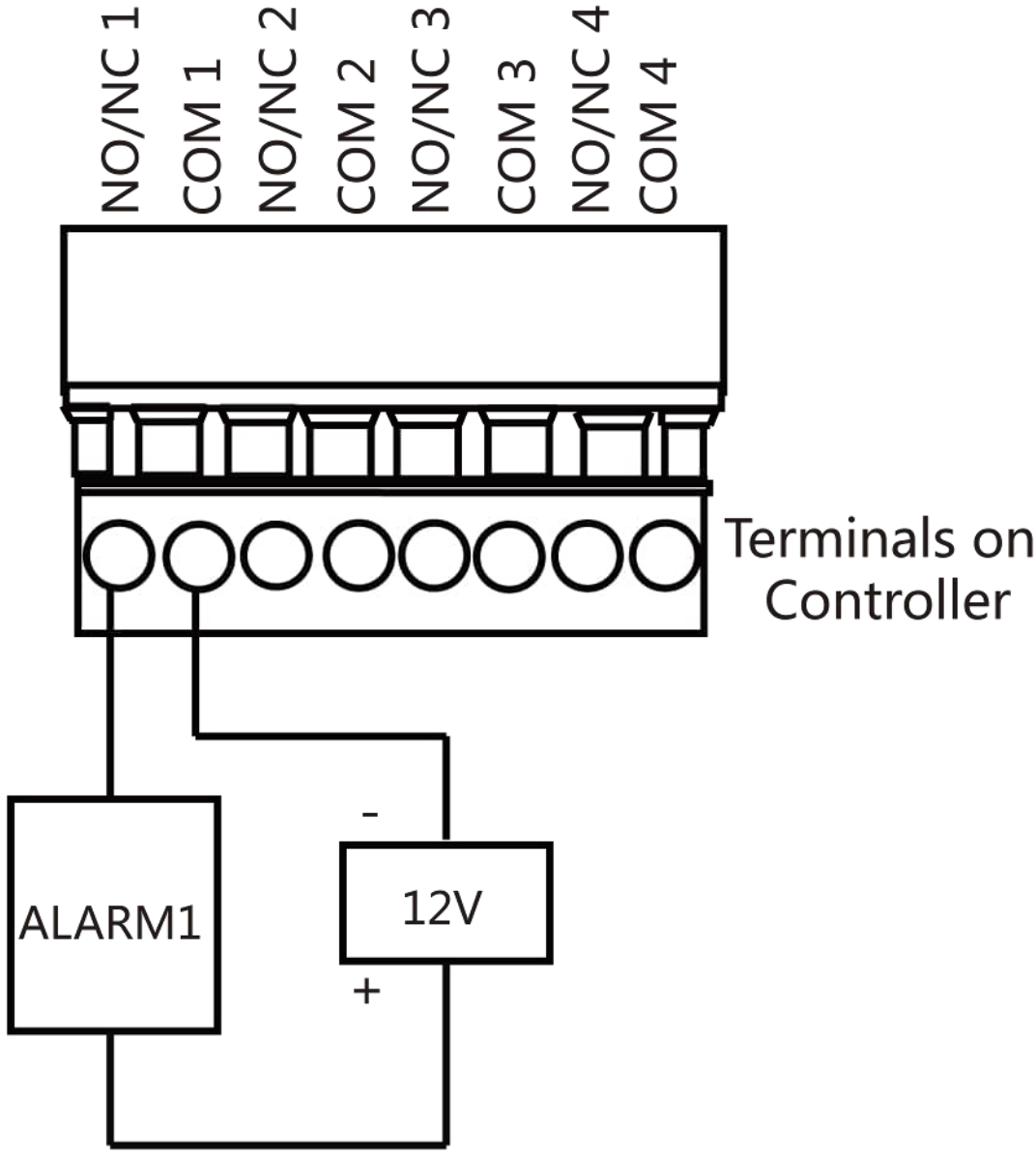


Figure 5-8 External Alarm Device Wiring

5.7 Exit Button Wiring

You can view the exit button wiring diagram

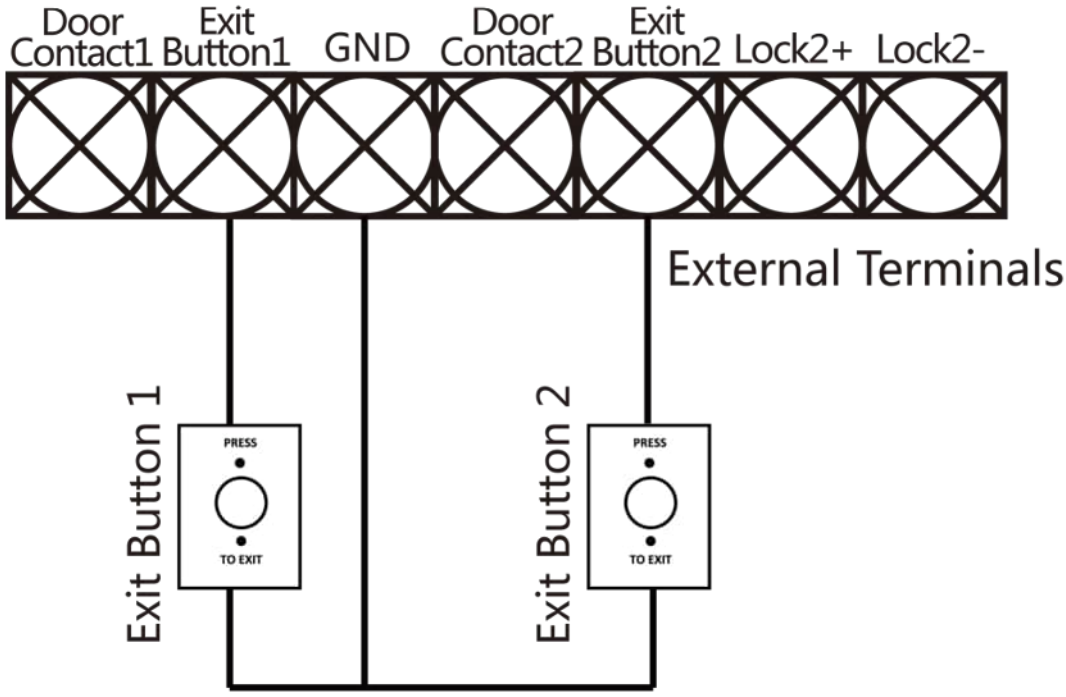


Figure 5-9 Exit Button Wiring

5.8 Door Contact Wiring

You can view the door contact wiring diagram.

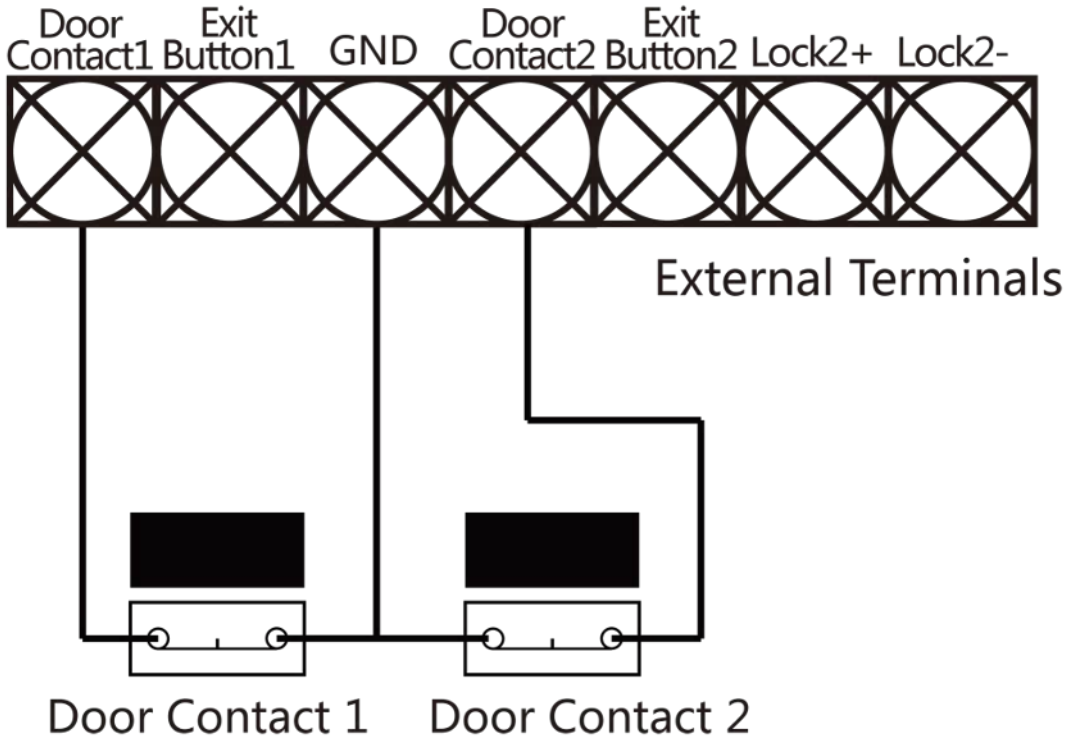


Figure 5-10 Door Contact Wiring

5.9 Power Supply Wiring

You can view the power supply wiring diagram.

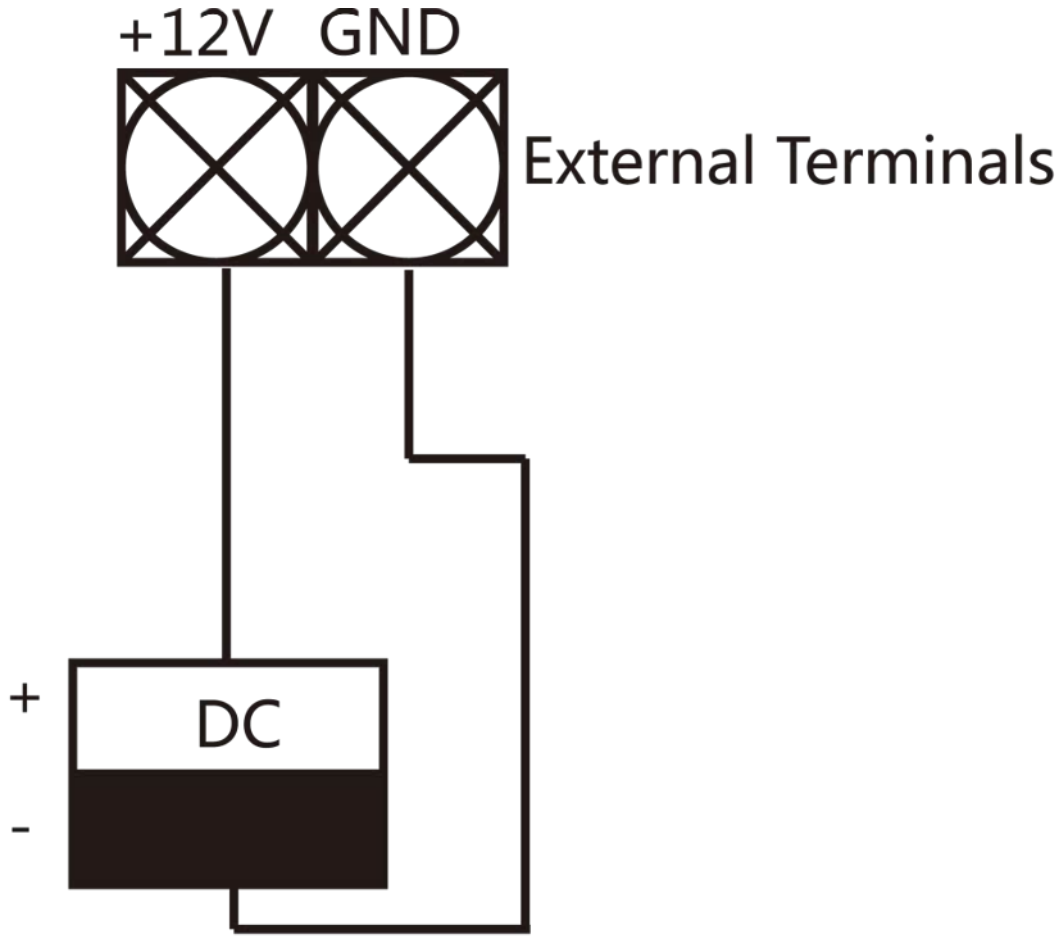


Figure 5-11 Power Supply Wiring

5.10 Arming Region Input Wiring

5.10.1 NO Wiring of Arming Region Input

You can view the arming region input of NO wiring.

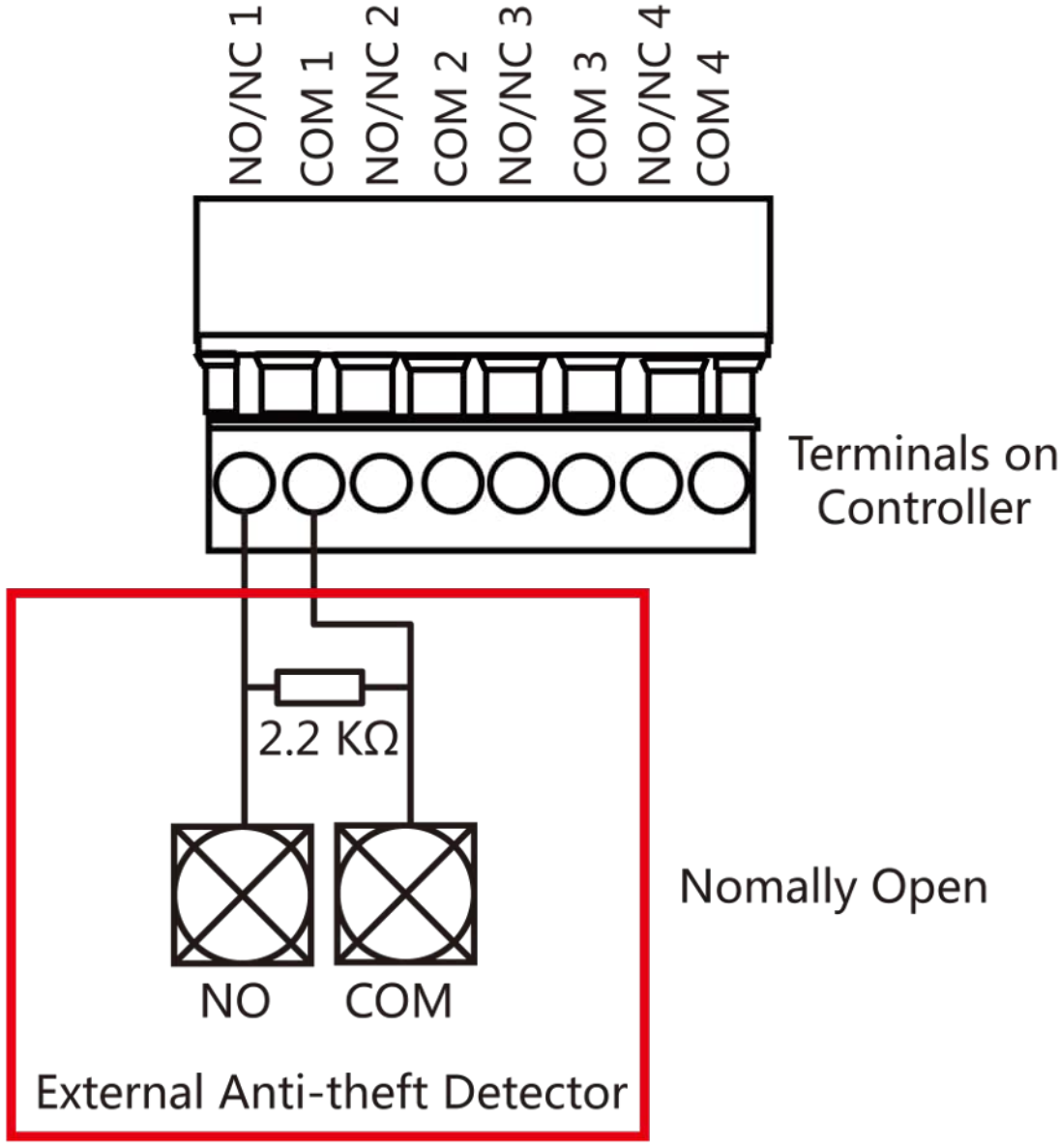


Figure 5-12 NO Wiring

5.10.2 NC Wiring of Arming Region Input

You can view the arming region input of NC wiring.

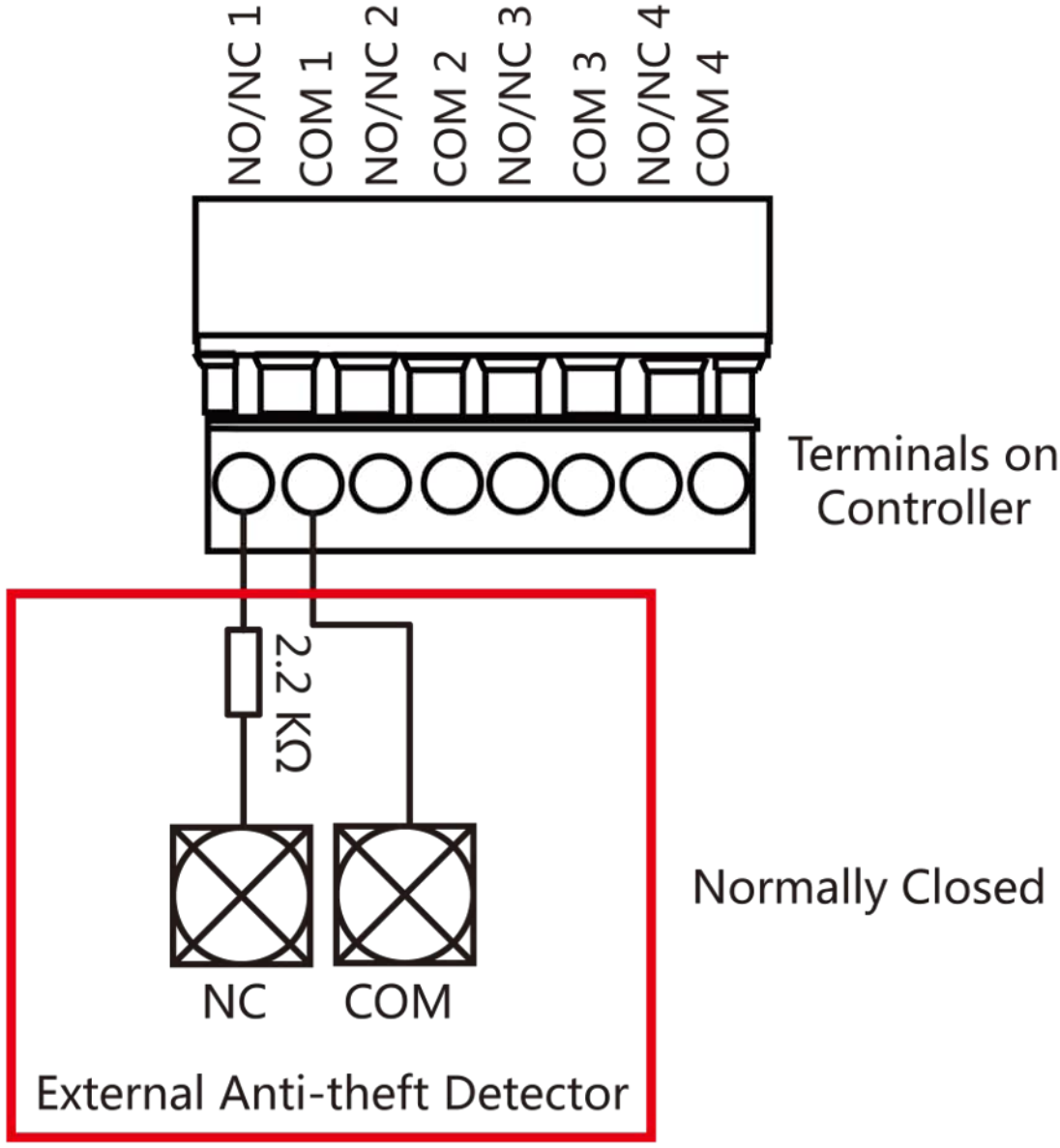


Figure 5-13 Normally Closed Wiring

5.11 Fire Alarm Module Wiring

You can view the fire alarm module wiring diagram.

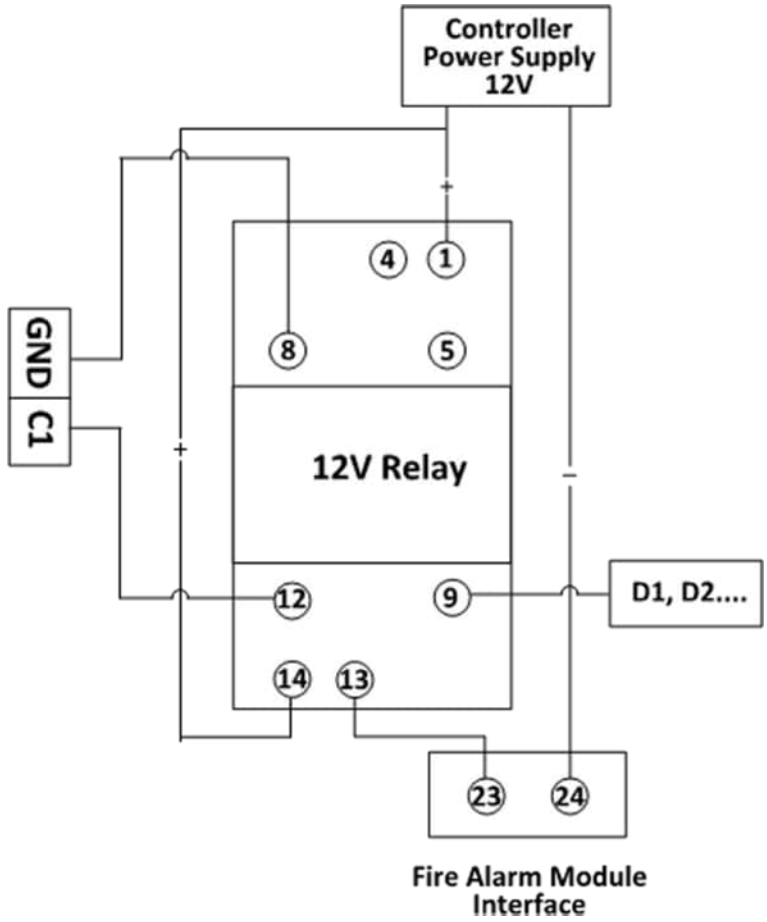


Figure 5-14 Fire Alarm Module Wiring

Chapter 6 Settings

6.1 Initialization (Option 1)

You can initialize the device with the jumper cap.

Steps

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

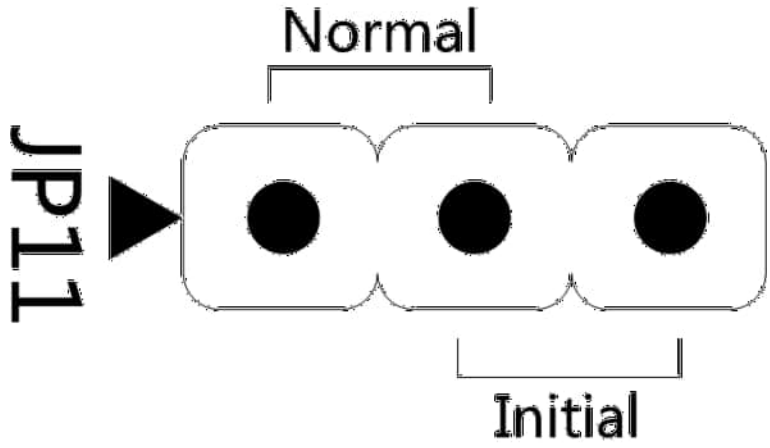


Figure 6-1 Initialization Jumper

Note

The device initialization will restore all the parameters to the default settings and all the device event logs will be deleted.

6.2 Initialization (Option 2)

You can initialize the device with the jumper cap.

Steps

1. Move the jumper cap from Normal to Initial.
2. Cut off the power and restart the access controller.
   The controller buzzer buzzes a long beep.
3. When the beep stopped, move the jumper cap back to Normal.
4. Cut off the power and restart the access controller.

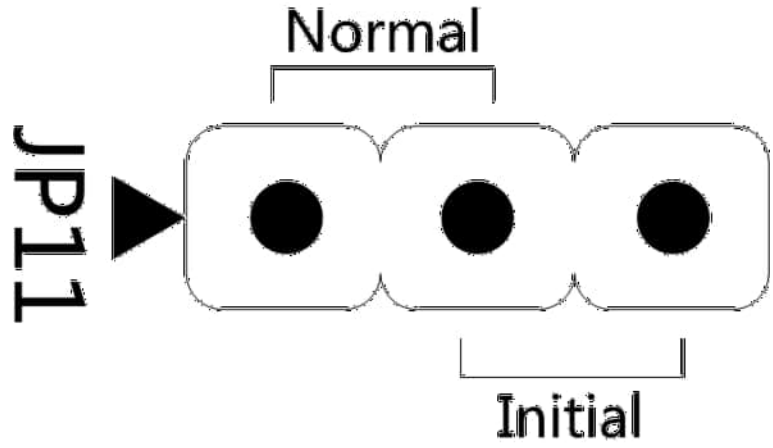


Figure 6-2 Initialization Jumper

Note

The device initialization will restore all the parameters to the default settings and all the device event logs will be deleted.

6.3 Relay Output NO/NC Settings

6.3.1 Lock Relay Output Settings

You can view the NO/NC status of the lock relay.

Lock Relay NO Status

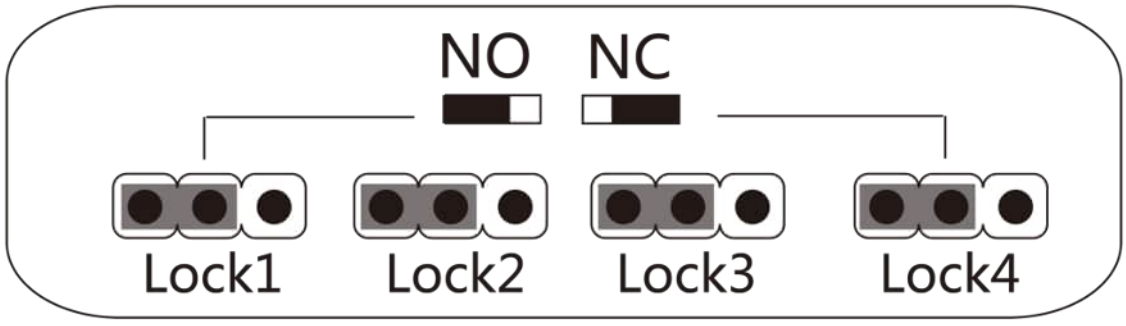


Figure 6-3 NO Status

Lock Relay NC Status

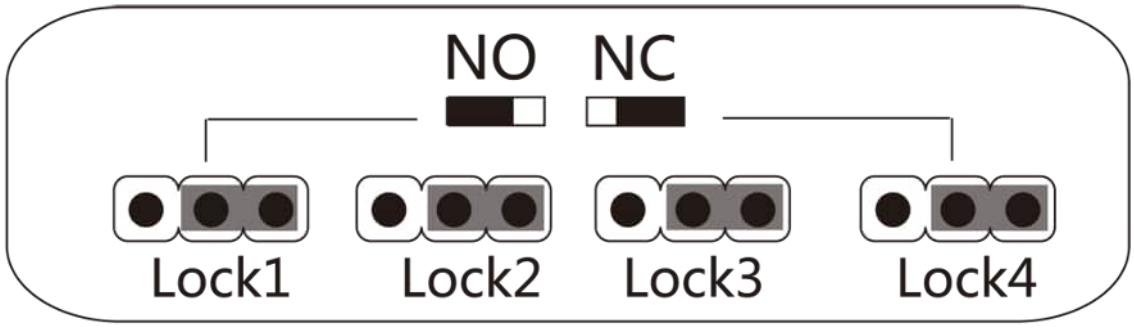


Figure 6-4 NC Status

6.3.2 Alarm Relay Output Settings

You can view the NO/NC status of the alarm relay.

Alarm Relay Output NO Status

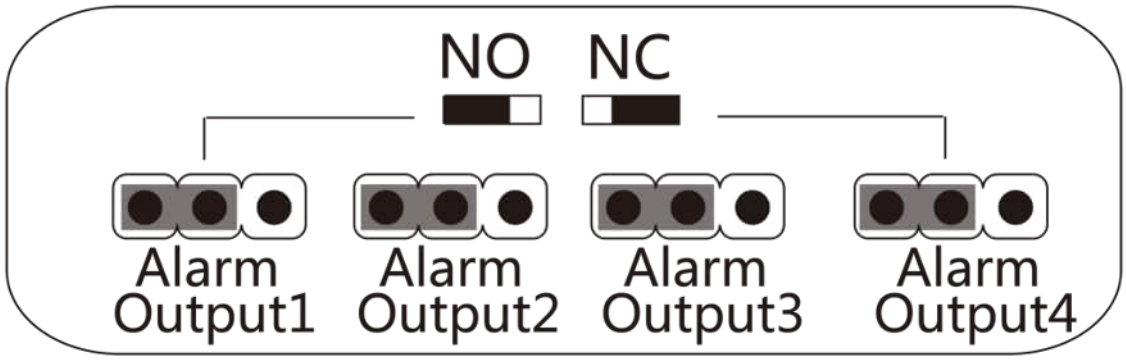


Figure 6-5 NO Status

Alarm Relay Output NC Status

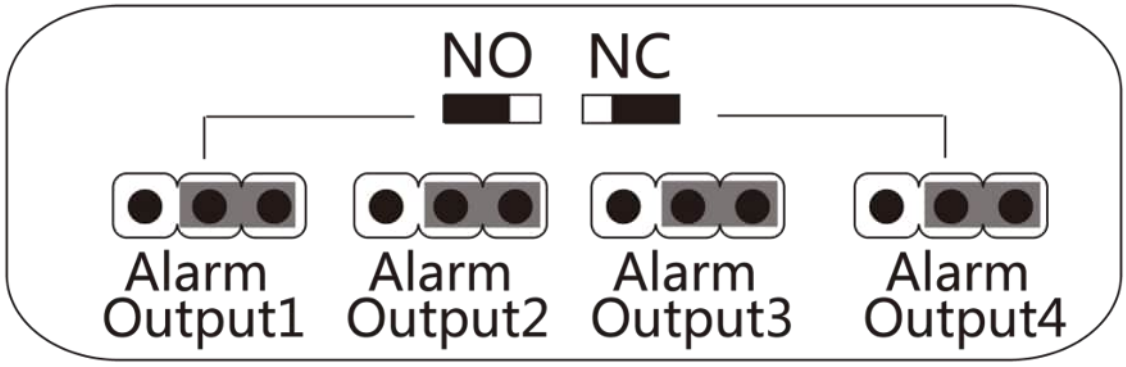


Figure 6-6 NC Status

Chapter 7 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

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

7.1 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

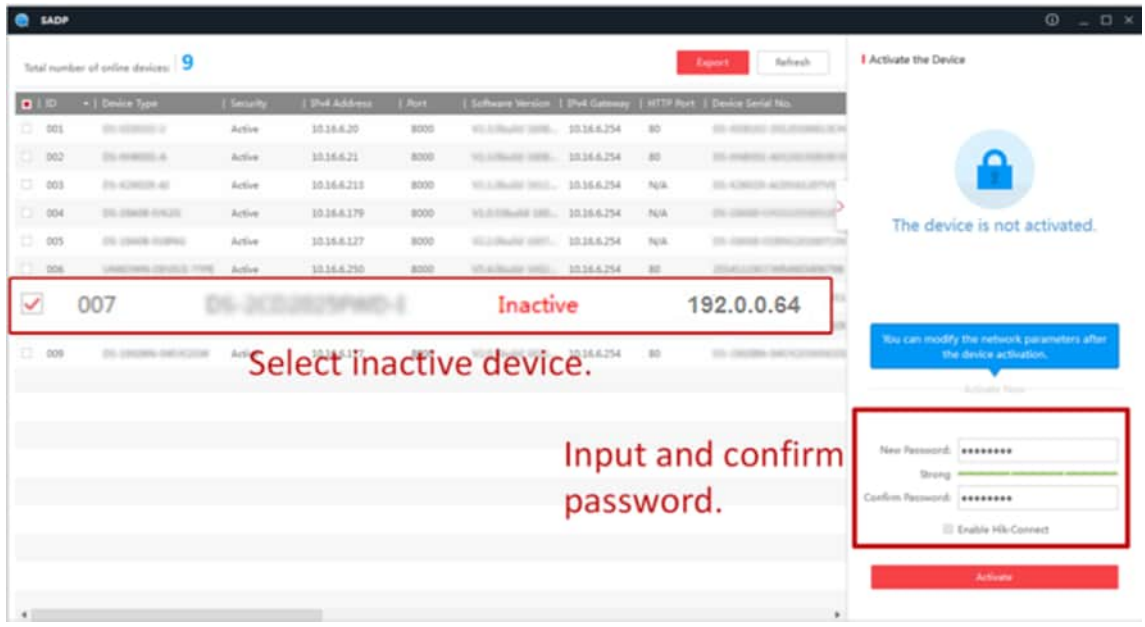
The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

   Caution

   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 start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

7.2 Activate Device via Client Software

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

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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

Chapter 8 Client Software Configuration

8.1 Operation on Client Software

The Access Control module provides multiple functionalities, including person and card management, permission configuration, and other advanced functions.

Note

For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings. For setting the user permission of Access Control module, refer to *Account Management* in *User Manual of iVMS-4200 Client Software*.

8.1.1 Add Device

After running the client, devices should be added to the client for the remote configuration and management.

After adding device(s), you can select a device and click **Remote Configuration** to configure further parameters of the selected device if needed. You can also

Note

For some models of devices, you can open its general or advanced parameters configuration window. To open the original remote configuration window, press **CTRL** and click **Remote Configuration**.

After adding access control devices, you can select access control device from the list and click **Device Status** to view the device status.

Add Online Device

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

Add Single Online Device

You can add single online device to the client software.

Perform this task to add single online device to the client software.

Steps

1. Enter the Device Management module.

2. Click **Device** tab and select **Hikvision Device** as the device type to display the **Online Device** area.

Figure 8-1 Online Device

3. Select an online device from the **Online Device** area.

Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activation*** .

4. Click **Add to Client** to open the device adding window.
5. Input the required information.

Address

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

Port

The default value is 8000.

User Name

By default, the user name is admin.

Password

Input the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.

7. **Optional:** Check **Export to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

8. **Optional:** Add the offline devices.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
9. Click **Add** to add the device.

Add Multiple Online Devices

You can add multiple online devices to the client software.

Perform this task if you need to add multiple online devices to the client software.

Steps

1. Enter the Device Management module.
2. Click **Device** tab and select **Hikvision Device** as the device type to display the **Online Device** area.
3. Click and hold **Ctrl** key to select multiple devices.

Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activation*** .

4. Click **Add to Client** to open the device adding window.
5. Input the required information.

   User Name

   By default, the user name is admin.

   Password

   Input the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Check **Synchronize Device Time** to synchronize the time of the devices with the PC running the client after adding the devices to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

8. Click **Add** to add the devices.

Add All Online Devices

You can add all online devices to the client software.

Perform this task if you need to add all online devices to the client software.

Steps

1. Enter the Device Management page.
2. Click **Device** tab and select **Hikvision Device** as the device type to display the **Online Device** area.
3. Click **Add All** to open the device adding window.

Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activation*** .

4. Input the user name and password.

User Name

By default, the user name is admin.

Password

Input the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Check **Synchronize Device Time** to synchronize the time of the devices with the PC running the client after adding the devices to the client.

6. **Optional:** Check **Export to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

7. Click **Add** to add the devices.

Add Device by IP Address or Domain Name

You can add device by IP address or domain name.

Perform this task if you need to add device by IP address or domain name.

Steps

1. Open the Device Management module.
2. Click **Device** tab and select **Hikvision Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **IP/Domain** as the adding mode.
5. Input the required information, including nickname, IP address, port number, user name, and password.

   Address

   Input the device IP addresss or domain name.

   Port

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

   User Name

   Input the device user name. By default, the user name is admin.

   Password

   Input the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

8. **Optional:** Add the offline devices.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
9. Click **Add** to add the device.

Add Devices by IP Segment

If you want to add devices of which the IP addresses are within an IP segment, you can specify the start IP address and end IP address, user name, password, and other parameters to add them.

Perform this task when you need to add devices to the client by IP segment.

Steps

1. Enter the Device Management module.
2. Click **Device** tab and select **Hikvision Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **IP Segment** as the adding mode.
5. Input the required information.

   Start IP

   Input a start IP address.

   End IP

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

   Port

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

   User Name

   By default, the user name is admin.

   Password

   Input the device password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.

Note

You can import all the channels of the device to the corresponding group by default.

8. **Optional:** Add offline devices to the client.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
9. Click **Add** to add the device.

Add Device by EHome Account

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

Before You Start

Set the network center parameter first. For details, refer to ***Set Network Parameters*** .

Perform this task if you need to add devices by EHome account.

Steps

1. Enter the Device Management module.
2. Click **Device** tab and select **Hikvision Device** as the device type.
3. Click **Add** to open the Add window.
4. Select **EHome** as the adding mode.
5. Input the required information.

   Account

   Input the account name registered on EHome protocol.
6. **Optional:** Check **Synchronize Device Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Export to Group** to create a group by the device name.
8. **Optional:** Add the offline devices.
   1) Check **Add Offline Device**.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

Note

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

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

Import Devices in a Batch

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

Perform this task to import devices in a batch.

Steps

1. Enter the Device Management page
2. Click **Device → Hikvision Device → Add** to open the adding device window.
3. Select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and input the required information of the devices to be added on the corresponding column.

Adding Mode

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

Address

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

Port

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

Device Information

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

User Name

Input the device user name. By default, the user name is admin.

Password

Input the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Add Offline Device

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

Export to Group

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

Channel Number

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

Alarm Input Number

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

Serial Port No.

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

Baud Rate

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

DIP

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

Hik-Connect Account

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

Hik-Connect Password

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

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

8.1.2 Select Application Scenario

For the first time entering the Access Control module, you are required to select the access control's application scenario as residence or non-residence according to the actual needs.

Perform this task if you need to select the access control's application scenario when entering the Access Control module for the first time.

Steps

Note

Once the scene is configured, you cannot change it.

1. Enter the Access Control module.

   The Select Scene window will pop up.

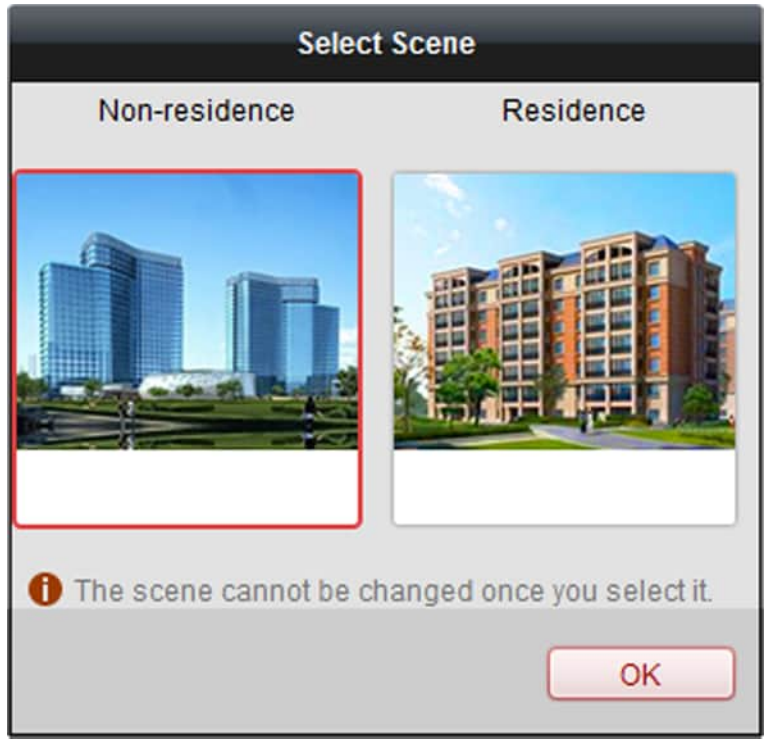


Figure 8-2 Select Access Control Application Scenario

2. Select the scene as residence or non-residence according to the actual needs.

   Note

   If you select **Residence** mode, you cannot configure person's attendance rule when adding person.

3. Click **OK**.

8.1.3 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

Set Network Parameters

After adding the access control device, you can set the device log uploading mode, and create EHome account via wired or wireless network.

Set Log Uploading Mode

You can set the mode for uploading logs via EHome protocol.

Perform this task when you need to set the access control device's log uploading mode.

Steps

1. Click **Access Control → Device Management** to enter the Device Management page.
2. Select the device in the device list and click **Modify**.
3. Click **Network Settings → Uploading Mode** to enter the Uploading Mode page.
4. Select the center group from the drop-down list.
5. Check **Enable** to enable to set the oploading mode.
6. Select the uploading mode from the drop-down list.
   - Enable **N1** or **G1** for the main channel and the backup channel.
   - Select **Close** to disable the main channel or the backup channel

Note

- The main channel and the backup channel cannot enable N1 or G1 at the same time.
- N1 refers to wired network and G1 refers to GPRS.
- Only device with 3G/4G function supports setting the channel as G1.
- For wired network settings, see ***Create EHome Account in Wire Communication Mode*** .
- For wireless network settings, see ***Create EHome Account in Wireless Communication Mode*** .

7. Click **Save**.

Create EHome Account in Wire Communication Mode

You can set the account for EHome protocol in wire communication mode. Then you can add devices via EHome protocol.

Perform this task when you need to create EHome account in wire communication mode for access control device.

Steps

Note

This function should be supported by the device

1. Click **Access Control → Device Management** to enter the Device Management page.
2. Select the device in the device list and click **Modify**.
3. Click **Network Settings → Network Center** to enter the Network Center page.
4. Select the center group from the drop-down list.
5. Select the **Address Type** as **IP Address** or **Domain Name**.
6. Input IP address or domain name according to the address type.
7. Input the port number for the protocol.

   Note

   The port number of the wireless network and wired network should be consistent with the port number of EHome.
8. Select the **Protocol Type** as **EHome** and select EHome version.

   Note

   If set the EHome version as **5.0**, you should create an EHome key for the EHome account.
9. Set an account name for the network center.
10. Click **Save**.

Create EHome Account in Wireless Communication Mode

You can set the account for EHome protocol in wireless communication mode. Then you can add devices via EHome protocol.

Perform this task when you need to create EHome account in wireless communication mode for access control device.

Steps

Note

This function should be supported by the device

1. Click **Access Control → Device Management** to enter the Device Management page.
2. Select the device in the device list and click **Modify**.
3. Click **Network Settings → Wireless Communication Center** to enter the Wireless Communication Center page.
4. Select the center group from the drop-down list.
5. Input the IP address and port number.

Note

- By default, the port number for EHome is 7660.
- The port number of the wireless network and wired network should be consistent with the port number of EHome.

6. Select the **Protocol Type** as **EHome**.
7. Set an account name for the network center.
8. Click **Save**.

Authenticate M1 Card Encryption

M1 card encryption can improve the authentication security level. After issuing the card, you can enable the M1 card encryption function in the client software.

Before You Start

Use the specified card enrollment station to issue card. See ***Issue a General Card to Person*** for details.

Perform this task when you need to enable M1 card encryption function.

Note

The function should be supported by the access control device and the card reader.

Steps

1. Click **Access Control → Device Management** to enter the access control device management page.
2. Select the device in the device list, and click **Modify** to pop up Modify window.
3. Click **M1 Card Encryption** tab to enter the M1 Card Encryption page.
4. Check **Enable** to enable the M1 card encryption function.
5. Set the sector ID.

   The sector ID ranges from 1 to 100.
6. Click **Save** to save the settings.

Note

After enabling the M1 card encryption function, you should set the added card's sector ID as the configured sector ID here.

8.1.4 Manage Organization

You can manage the organization as desired, such as adding, editing, or deleting the organization.

Perform this task when you need to manage organization.

Steps

1. Click **Access Control → Person and Card** to enter the person and card management page.

2. Click **Add** to pop up Add Organization window.
3. Create a name for the organization.
4. Click **OK**.

Note

Up to 10 levels of organizations can be added.

5. **Optional:** After adding the organization, you can do one or more of the following operations.

Edit Organization	Select the added organization and click **Modify** to modify its name.
Delete Organization	Select the added organization and click **Delete** to delete it. **Note** • 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.

8.1.5 Manage Person Information

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 information in batch, etc.

Note

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

Add Single Person

You can add person to the client software one by one and input the person information such as basic information, detailed information, access control permission, linked card, linked face picture, linked fingerprint, and attendance rule.

Configure Person's Basic Information

You can add person to the client software one by one and configure the person's basic information such as name, phone number, etc.

Perform this task when you need to configure the person's basic information when adding person.

Steps

1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person.

3. Click **Add** to open the adding person window.

   The Person No. will be generated automatically and is not editable.
4. Input the basic information including person name, valid time duration, password.
5. Set person type and privilege.

   Normal

   You can set privilege for the normal person, including **Manage Device Backend** and **Close Delay Enabled**.

   Visitor

   If the person is a visitor, you should set the maximum times for the visitor to open the door. After the configured value, the visitor cannot open the door again.

   Blocklist

   Add the person in the blocklist. If the person authenticates on the device, the device will upload an event to the client software.

   Manage Device Backend

   Set the person as an administrator. After the permission is applied to the device, the person can log in the device and configure parameters on the device.

   Close Delay Enabled

   If enabled the function, the door opening time duration will be extended. You can set the Extended Open Duration in *Configure Door Parameters*.
6. **Optional:** Set the person's picture.
   - Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
   - Click **Take Photo** to take the person's photo with the PC camera.
7. Confirm adding the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Configure Detailed Information

When adding person, you can configure the detailed information for the person, such as person's ID type, ID No., country, etc., according to actual needs.

Perform this task when you need to configure the person's detailed information.

Steps

1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Input the person's basic iformation first. For details about configuring person's basic information, refer to ***Configure Person's Basic Information*** .
3. Click **Details** tab.

4. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.

   Linked Device

   bind the indoor station to the person.

   Note

   If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

5. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Assign Permission to Person

When adding person, you can assign the permissions (including operation permissions of access control device and access control permissions) to the person.

Perform this task when you need to assign access control permission to the person.

Steps

Note

For setting the access control permission, refer to ***Assign Permission to Person*** .

1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person.
3. Click **Add**.
4. Input person's basic information.

   Note

   For details about configuring person's basic information, refer to ***Configure Person's Basic Information*** .

5. Click **Permission** tab.
6. In the Permission(s) to Select list, check the permission(s) checkbox(es) and click **>** to add to the Selected Permission(s) list.
7. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Issue a General Card to Person

When adding person, you can issue a general card with a unique card number to the person.

Perform this task when you need to issue a general card to the person.

Steps

1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.

Note

Input the person's basic information first. For details about configuring person's basic information, refer to *Configure Basic Information*.

3. Click **Credential → Card** tab to enter the card credential settings page.
4. Click **Add** and select **General Card** tab to enter the general card configuration page.
5. Set card parameters.
   1) Select a card type for the general card.

      Normal Card

      By default, the card is normal card, which has no additional functions.

      Patrol Card

      The card swiping action can used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.

      Duress Card

      The 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.

   2) **Optional:** In the Remark field, input the remark information for the card if needed.

      Note

      Up to 32 characters are allowed in the Remark field.

   3) Set the effective time and expiry time of the card.
6. Select the reading card mode and input the card number.
   - Access Controller Reader
     1. Place the card on the reader of the Access Controller.
     2. Click **Read** to get the card number.
   - Card Enrollment Station
     1. Connect the card enrollment station with the PC running the client.
     2. Click **Set Card Enrollment Station** to set the card enrollment station's parameters.
     3. Select the Card Enrollment Station type.

        Note

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

4. Set the serial port number, the baud rate, the timeout value, the buzzing, or the card number type.

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

Note

The M1 Card Encryption function is supported by DS-K1F100-D8, DS-K1F100-D8E, and DS-K1F180-D8E.

6. Click **Save**.

7. Place the card on the card enrollment station.

8. Click **Read**to get the card No.

- Manually Input

1. Input the card number manually.

2. Click **Enter** to input the card number.

7. Click **OK**.

The card(s) will be issued to the person.

8. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Collect Person's Fingerprint Locally

When adding person, you can collect the person's fingerprint information via the fingerprint recorder connected to the PC running the client.

Perform this task when you need to collect the person's fingerprint via the fingerprint recorder connected to the PC running the client.

Steps

1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.

Note

Input the person's basic information first. For details about configuring person's basic information, refer to *Configure Person's Basic Information*.

3. Click **Credential → Fingerprint** tab to enter the card credential settings page.
4. Select the collection mode as **Local Collection**.
5. Connect the fingerprint recorder to the PC and set its parameters.
   1) Click **Set Fingerprint Machine** to open the setting fingerprint machine window.
   2) Select the device type.

Note

Currently, the supported fingerprint recorder types include DS-K1F800-F, DS-K1F300-F, DS-K1F810-F, and DS-K1F820-F.

3) **Optional:** For fingerprint recorder type DS-K1F800-F, you can set the serial port number, baud rate, and overtime parameters of the fingerprint recorder.

Note

- The serial port number should correspond to the serial port number of PC.
- The baud rate should be set according to the external fingerprint card reader. The default value is 19200.
- **Timeout after** field refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collection is over.

4) Click **Save**.

6. Collect the fingerprint.

1) Click **Start**.
2) Select a fingerprint on the hand picture to start collecting.
3) Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint.
1) Select a fingerprint type.

Note

When the same fingerprints of one person are collected, the prompt with repeat ID appears. When the similar fingerprints are collected for different person, the prompt with repeat ID and person name appears.

7. Confirm adding the person.

- Click **OK** to add the person and close the Add Person window.
- Click **Save and Continue** to add the person and continue to add other persons.

Collect Person's Fingerprint Remotely

When adding person, you can collect the person's fingerprint information via the remote access control device's fingerprint module.

Perform this task when you need to collect the person's fingerprint via the fingerprint module of the access control device.

Steps

1. Enter **Access Control → Person and Card** .

2. Select an organization in the organization list to add the person and click **Add**.

Note

Input the person's basic information first. For details about configuring person's basic information, refer to *Configure Person's Basic Information*.

3. Click **Credential → Fingerprint** tab to enter the card credential settings page.
4. Select the collection mode as **Remote Collection**.
5. Click **Start** and select an access control device to collect the fingerprint.

Note

The function should be supported by the device.

6. Collect the fingerprint.
   1) Select a fingerprint on the hand picture to start collecting.
   2) Lift and rest the corresponding fingerprint on the device's fingerprint module to collect the fingerprint.
   3) Select a fingerprint type.
   4) Click **Stop**.
7. Confirm adding the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons.

Configure Attendance Rule

When adding person, you can configure the person's attendance rule if the application scenario is non-residence mode and the person joins in the time and attendance.

Perform this task when you need to configure the person's attendance rule when adding person.

Steps

Note

For details about attendance settings and application, refer to ***Time and Attendance*** .

1. Enter **Access Control → Person and Card** .
2. Select an organization in the organization list to add the person and click **Add**.
3. Enter person's basic information.

Note

For details about configuring person's basic information, refer to ***Configure Person's Basic Information*** .

4. Click **Attendance Rule** tab.

Note

This tab page will display when you select **Non-Residence** mode as the application scene when running the software for the first time. For details, refer to ***Select Application Scenario*** .

5. If the person joins in the time and attendance, check **Time and Attendance** to enable this function for the person.

   The person's card swiping records will be recorded and analyzed for time and attendance.
6. Set attendance rule for the person.

   Note

   For details about Time and Attendance, click **More** to go to the Time and Attendance module.
7. Confirm to add the person.
   - Click **OK** to add the person and close the Add Person window.
   - Click **Save and Continue** to add the person and continue to add other persons .

Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

Import Person Information

You can import the information of multiple persons (including identity information, fingerprint data, and fingerprint linked card number) to the client software in a batch by importing an Excel file from the local PC.

Perform this task when you need to import the person information to the client in a batch.

Steps

1. Enter **Access Control → Person and Card** .
2. Click **Import Persons** and select **Person Information** as the content to import.
3. In the pop-up window, click **Download Template for Importing Person** to download the template first.
4. Input the person information in the downloaded template.

   f1 to f10

   The person's fingerprint data.

   f1card to f10card

   The fingerprint's linked card number. If it links to no card, leave it empty.

   Note

   If the person has multiple cards, separate the card No. with semicolon.
5. Enter **Access Control → Person and Card** , click **Import Person** and select the Excel file with person information.
6. Click **OK** to start importing.

Note

If the person No. already exists in the client software's database, it will replace the person information automatically after importing.

Export Person Information

You can export the added persons' information to the local PC in an Excel file.

Perform this task when you need to export the added person information in a batch.

Steps

1. Enter **Access Control → Person and Card** module.
2. Click **Export Person** and select **Person Information** as the content to export.
3. Select the path for saving the exported Excel file.
4. Select the items of person information to export.
5. Click **OK** to start exporting.

f1 to f10

The person's fingerprint data.

f1card to f10card

The fingerprint's linked card number. If it links to no card, leave it empty.

Get 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.

Perform this task when you need to get the configured person informatio from the access control device.

Steps

Note

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

1. Enter **Access Control → Person and Card** .
2. Select an organization to import the persons.
3. Click **Get Person** to open the selecting device window.

   The added access control device will be displayed.

4. Start getting the person information.
   - Select the device and then click **OK** to start getting the person information from the device.
   - Double click the device name to start getting the person information.

   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.

Issue Cards to Person in Batch

You can issue multiple cards to one person in batch.

Perform this task when you need to issue multiple cards to one person.

Steps

1. Enter **Access Control → Person and Card** .
2. Click **Issue Card in Batch**.

   All the added person with no card issued will display in the Person(s) with No Card Issued list.
3. Set the parameters for the cards.
   1) Select the card type according to actual needs.

   Note

   For details about the card type, refer to *Issue a General Card to Person*..

   2) In the Card Password field, create a password (4 to 8 digits) for the card itself.

   Note

   The password will be required when the card holder swiping the card to enter or exit the door if the card reader authentication mode requires password. For details, refer to *Configure Card Reader Authentication Mode and Schedule*.

   3) Input the card quantity issued for each person.

   Example

   If the card quantity is 3, you can read or enter three card numbers for each person.

   4) Set the effective time and expiry time of the card.
4. In the Person(s) with No Card Issued list on the left, select the person to issue cards.
5. Select the reading card mode and input the card number.

   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 set the card enrollment station's parameters. For details, refer to *Issue a General Card to Person*.

Manually Input

Input the card No. manually and click **Enter** to input the card No.

After issuing the cards to the person, the person and card information will display in the Person(s) with Card Issued list.

6. Click **OK**.

Search Person Information

After adding the person information to the client, you can search the person by setting the search conditions.

It provides normal search and advanced search to search the person.

Normal Search

After adding the person information to the client, you can search the person by person name or card number.

Perform this task if you want to search the person information by person name or card number.

Steps

1. Enter **Access Control → Person and Card** module.
2. Set the search condition.
   - To search the person by person name, input the keyword of the person name in the search field.
   - To search the person by card number, input the keyword of the card number in the search field manually, or click **Read** to read the card number from certain card by card enrollment station.

   Note

   Before reading by card enrollment station, you need to connect the card enrollment station with the PC running the client first. You can click **Read → Set Card Enrollment Station** to set its parameters. For details, refer to ***Issue a General Card to Person*** .
3. Click **Search**.

   The search results will display in the person list.

Advanced Search

After adding the person information to the client, you can search the target person by setting more accurate search conditions, including card number, person name, person number.

Perform this task if you need to search the target person with more accurate search conditions.

Steps

1. Enter **Access Control → Person and Card** module.
2. Click **Advanced Search** to display the search conditions.
3. Set the search condition.

   Card No.

   Input the keyword of the card number, or click **Read** to read the card number from certain card by card enrollment station.

   Note

   Before reading by card enrollment station, you need to connect the card enrollment station with the PC running the client first. You can click **Read → Set Card Enrollment Station** to set its parameters. For details, refer to ***Issue a General Card to Person*** .

   Person No.

   Input the keyword of the person number.

   Person Name

   Input the keyword of the person name.

   Note

   The person name is case sensitive.
4. Click **Search**.

   The search results will display in the person list.
5. **Optional:** Click **Reset** to clear the search conditions.

Report Card Loss

If the person lost his/her card, you can report the card loss so that the related access control permission will be deleted.

Perform this task if you need to report the card loss for the person who lost his/her card.

Steps

1. Enter **Access Control → Person and Card** module.
2. **Optional:** Search the person you want to report card loss for.

Note

For searching the person, refer to ***Search Person Information*** .

3. Select the person and click **Modify** to open the Edit Person window.
4. Click **Credential → Card** tab to show the person's card information
5. Select the lost card and click **Report Card Loss**.

   The card status will turn to lost.
6. **Optional:** If the lost card is found, you can select the card and click **Cancel Card Loss** to cancel the loss.

   The card status will turn to normal.
7. **Optional:** If you have assigned access permission to the person, a window will pop up to notify you to apply the permission to the device again to take effect. You can click **Apply Now** or **Apply Later** to apply the permission changes to the device.

Set Card Enrollment Station

The card enrollment station can read the number of the card placed on it and show the card number on the client. After connecting a card enrollment station to the PC running the client by USB interface or COM, you need to set the card enrollment station parameters before using it to reading the card number.

When adding a card to one person, click **Set Card Enrollment Station** to open the Card Enrollment Station window.

The following parameters are available:

Type

Select the model of the connected card enrollment station

Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

If the card contains both EM and IC chips, you can also select **All** to read the numbers of both EM and IC chips.

Serial Port No. and Baud Rate

These two fields are only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to and set the baud rate.

Timeout after

Specify the milliseconds after which the read card number will be timeout.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

The type of the card number.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

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

8.1.6 Configure Schedule and Template

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

Note

For access control permission settings, refer to ***Assign Permission to Person*** .

Add Week Schedule

You can add custom week schedule to make the access control permission valid or invalid in the configured schedule of the week.

Perform this task when you want to add custom week schedule.

Steps

1. Click **Access Control → Schedule and Template → Week Schedule** to enter the Week Schedule Management page.

   Note

   There are two default week schedules: Whole Week Schedule and Blank Schedule, and they cannot be edited or deleted.

   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.

2. Add a week schedule.
   1) Click **Add Week Schedule** to open the Add Week Schedule dialog.
   2) Input a desired name in the **Week Schedule Name** field.

3) Click **OK** to add the week schedule.

3. Click the added week schedule in the left list to show its property on the right.
4. Select a day of the week and draw time periods on the timeline bar.

Note

Up to 8 time periods can be set for each day in the week schedule.

5. **Optional:** Perform one of the following operations to edit the drawn time periods.
   - Move the cursor to the time period and drag the time period on the timeline bar to the desired position when the cursor turns to .
   - Click the time period and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the ends of time period and drag to lengthen or shorten the time period when the cursor turns to .
6. **Optional:** After setting the time schedule, you can do one or more of the following operations.

Delete Day Schedule	Select a day and click **Delete Duration** to delete the schedule of the selected day.
Clear Week Schedule	Click **Clear** to delete the whole week schedule.
Copy to Whole Week	Click **Copy to Week** to copy the schedule of this day to the whole week.

7. Click **Save** to saving the settings and finishing adding the week schedule.

Add Holiday Schdule

You can create a schedule for holidays and set the days in the holiday schedule, including start date, end date, and holiday duration in one day.

Perform this task when you need to add a holiday schedule to pre-define the holidays.

Steps

1. Click **Access Control → Schedule and Template → Week Schedule** to enter the Holiday Group Management page.
2. Add a holiday group.
   1) Click **Add Holiday Group** on the left to open the adding holiday group window.
   2) Create a name for the holiday group.
   3) Click **OK**.
3. Add a holiday period to the holiday group and configure the holiday duration.

Note

Up to 16 holiday periods can be added to one holiday group.

   1) Click **Add Holiday**.
   2) 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 to one holiday period.

3) **Optional:** 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.
4) **Optional:** When the cursor turns to , you can lengthen or shorten the selected time bar.

4. Click **Save**.

Add Template

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

Perform this task if you want to add and configure template.

Steps

1. Click **Access Control → Schedule and Template → Template** to enter the Template Management page.

Note

There are two default templates: Whole Week Template and Blank Template, and they cannot be edited or deleted.

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.

2. Add a template.
   1) Click **Add Template** to open Add Template window.
   2) Input a name in the **Template Name** filed.
   3) Click **OK** to add the template.
3. Click the added template in the left list to show its property on the right.
4. Add a week schedule to apply to the template.
   1) Click **Week Schedule** tab on the right.
   2) In the Week Schedule field, select a configured week schedule.
   3) **Optional:** Click **Add Week Schedule** to add a new week schedule.

Note

For details about adding a week schedule, refer to ***Add Week Schedule*** .

5. Add a holiday group schedule to apply to the template.

Note

Up to four holiday groups can be added to one template.

1) Click **Holiday Group** tab.
2) Select a holiday group in the list.
3) **Optional:** Click **Add Holiday Group** to add a new holiday group schedule.

Note

For details about adding a holiday group, refer to ***Add Holiday Schdule*** .

4) Click **Add** to add the selected holiday group schedule to the right list.
5) **Optional:** Select a selected holiday group on the right list and click **Delete** to remove the selected one.

6. Click **Save** to save the settings and finish adding the template.

8.1.7 Manage Permission

After adding the person and configuring the person's credentials, you can create the access permissions to define the access level of which person(s) can get access to which door(s).

Assign Permission to Person

You can assign permission to persons so that person can enter or exist the access control points (doors) according to the assigned permission.

Perform this task if you need to assign access permissions to persons.

Steps

- You can add up to 4 permissions to one access control point of one device.
- You can add up to 128 permissions in total.
- When the permission settings are changed, you need to apply the permissions to the devices again to take effect. The permission changes include changes of schedule and template, permission settings, person's permission settings, and related person details (including card number, fingerprint, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control → Permission** to enter the Permission Management interface.
2. Click **Add** to open the adding permission window.
3. In the **Permission Name** text field, create a name for the permission as you want.
4. Select a schedule template for the permission.

Note

You should configure the template before permission settings. You can click **Add Template** to add the template. Refer to *Configure Schedule and Template* for details.

5. In the Person list, select person(s) to assign the permission and click **>** to add to the Selected Person list.
6. In the Access Control Point/Device list, select door(s) or door station(s) for the selected persons to access and click **>** to add to the selected list.

7. Click **OK**.

   The selected persons will have the permission to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.
8. After adding the access permissions, you need to apply them to the access control device to take effect.
   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 All** to start applying all the selected permission(s) to the access control device or door station.

   Note

   You can also click **Apply Changes** to apply the changed part of the selected permission(s) to the device(s).

Search Assigned Permission

After adding the access permissions, you can search the existing permissions by setting the search conditions.

Perform this task if you need to search the assigned access permission.

Steps

1. Click **Access Control → Permission** to enter the Permission Management interface.
2. Click **Advanced Search** to open the search window.
3. Set the search condition.

   Person No.

   Input the keyword of the person number.

   Person Name

   Input the keyword of the person name.

   Note

   The person name is case sensitive.

   Card No.

   Input the keyword of the card number.

   Permission Name

   The permission name is case sensitive.
4. Click **Search**.

   The search results will display below.
5. Click **Reset** to clear the search conditions.

8.1.8 Configure Advanced Functions

After configuring the person, template, and access 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-passback, etc.

By default, three functions are displayed in the advanced functions: access control parameters, card reader authentication, and multiple authentications. You can click **Add** in the tab bar to select the functions you want to display.

Note

The advanced functions should be supported by the device.

Configure Access Control Parameters

After adding the access control device, you can configure the parameters of access control points (door or floor), alarm inputs, alarm outputs, and card readers.

Configure Access Control Device Parameters

After adding the access control device, you can configure its parameters,.

Perform this task when you want to configure device parameters for the access control device.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select an access controller to show its parameters on the right.
3. Check the checkbox to enable the corresponding functions.

   Note

   The displayed parameters may vary for different access control devices.

   RS-485 Card Reader Communication Redundancy

   You should check the checkbox if you wire the RS-485 card reader to the access control device redundantly.

   Press Key to Input Card No.

   If you check the checkbox, you can input the card No. by pressing the key.
4. Click **Save**.
5. **Optional:** Click **Copy to** and select the access control device to copy the parameters to other devices.

Configure Door Parameters

After adding the access control device, you can configure its access control point (door) parameters.

Perform this task when you want to configure door (floor) parameters for the access control device.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select an access controller and click + to show the doors or floors of the selected access control device.
3. Select a door or floor to show its parameters on the right.
4. Edit the door or floor parameters.

Door Magnetic Sensor

Select the door contact status of Remain Closed or Remain Open.

Exit Button Type

Select the exit button status of Remain Closed or Remain Open.

Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

Extended Open Duration

The door magnetic can be enabled with appropriate delay after the person swipes the card.

Door Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period.

Duress Code

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

Super Password

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

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Note

- The duress code, super code, 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.

5. Click **Status Duration Settings** to set the door status duration. For details, see *Configure Duration Schedule for Door Status*.
6. Click **Save**.
7. **Optional:** Click **Copy to** and select the door/floor(s) to copy the parameters to other doors/floors.

Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

Configure Duration Schedule for Door Status

You can configure the weekly duration schedule for access control device's access control point (door) to remain open or remain closed.

Perform this task when you need to configure the door status duration schedule.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select a door to show its parameters on the right.
3. Click **Status Duration Settings** to open the Status Duration window.
4. Select a door status brush as **Remain Open** or **Remain Closed**.
   - **Remain Open:** The door will keep unlocked during the configured time period. The brush is marked as .
   - **Remain Closed:** The door will keep locked during the configured duration. The brush is marked as .
5. Drag on the time line to draw a color bar on the schedule to set the duration.
6. **Optional:** Select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
7. Click **Save** to save the status duration schedule.
8. Click **Save** to save the door parameters.

Configure Card Reader Parameters

After adding the access control device, you can configure its card reader parameters.

Perform this task when you want to configure card reader parameters for the access control device.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select an access controller and click to show the card readers of the selected access controller.

3. Select a card reader to show its parameters on the right.
4. Edit the card reader parameters.

Note

The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.

Nickname

Edit the card reader name as desired.

Enable Card Reader

Select **Yes** to enable the card reader for card swiping.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Max. Interval When Inputting Password

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

Enable Failed Attempts Limit of Card Reading

Enable to report alarm when the card reading attempts reach the set value.

Max. Times of Card Swiping Failure

Set the max. failure attempts of reading card.

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Detect When Card Reader is Offline for

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Default Card Reader Authentication Mode

You can view the default card reader authentication mode in this part.

5. Click **Save**.
6. **Optional:** Click **Copy to** and select the card reader(s) to copy the parameters to other card readers.

Configure Alarm Input Parameters

After adding the access control device, you can configure the parameters for its alarm inputs.

Perform this task if you need to set the alarm input parameters of the access control device.

Steps

Note

If the alarm input is armed, you cannot edit its parameters. Disarm it first.

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select a device and click + to show the alarm inputs of the selected access control device.
3. Set the alarm input parameters.

   Nickname

   Edit the alarm input name as desired.

   Detector Type

   The detector type of the alarm input.

   Zone Type

   Set the zone type for the alarm input.

   Sensitivity

   Only when the duration of signal detected by the detector reaches the setting time, the alarm input is triggered. For example, you have set the sensitivity as 10ms, only when the duration of signal detected by the detector reach 10ms, this alarm input is triggered.

   Trigger Alarm Output

   Select the alarm output(s) to be triggered.
4. Click **Save**.
5. **Optional:** Click the switch on the upper-right corner to arm or disarm the alarm input.

Configure Alarm Output Parameters

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Perform this task if you need to set the alarm input parameters of the access control device.

Steps

1. Click **Access Control → Advanced Function → Access Control Parameters** to enter Parameter Settings page.
2. Select a device and click + to show the alarm outputs of the selected access control device.
3. Set the alarm output parameters.

   Output Delay

   The delay time for the alarm output to be triggered.
4. Click **Save**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Individual Authentication

Set individual's authentication mode.

Before You Start

Add person and apply the person to the device. For details, see *Manage Person Information* and *Manage Permission*.

Steps

1. Click **Access Control → Advanced Function → Card Reader Authentication** to enter the card reader authentication configuration page.
2. Click a device name to enter the Individual Advanced Authentication page.
3. Click **Add** and select persons and their authentication mode.
4. Click **OK** to save the settings.

   Note

   The configured individual authentication has higher priority than other authentication modes.

   The individual application mode will be applied to the device automatically.
5. **Optional:** Select a person in the Individual Authentication page, and click **Modify** to change the person's individual authentication mode.
6. **Optional:** If applying individual authentication mode failed, click **Failed Application** to view details. Select an applying status from the list and click **Apply Again** to apply the person's authentication mode again to the device.

Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Perform this task if you need to configure the card reader's authentication mode and schedule.

Steps

1. Click **Access Control → Advanced Function → Card Reader Authentication** to enter the card reader authentication configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
   1) Click **Configuration**.

   Note

   - Password refers to the card password set when issuing the card to the person. For details, refer to *Add Single Person*.
   - Authentication password refers to the password set to open the door. Refer to Configure Authentication Password.
   - The supported card reader authentication mode varies according to different devices. For details, refer to the actual product.

   2) Select the modes and click » to add to the selected modes list.
   3) **Optional:** Click ↑ or ↓ to adjust the display order.
   4) Click **OK**.

   After selecting the modes, the selected modes will display as icons.
4. Click the icon to select a card reader authentication mode, and drag on the day to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.
5. Repeat the above step to set other time periods.
6. **Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. **Optional:** Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

Configure Multiple Authentication

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

Before You Start

Set the card permission and apply the permission settings to the access control device. For details, refer to ***Assign Permission to Person*** .

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control → Advanced Function → Multiple Authentication** to enter the Multiple Authentication page.
2. Select an access control device in the list of Controller List panel.
3. Add a card group for the access control device.
   1) Click **Add** on the Set Card Group panel.

2) Create a name for the group as desired.
3) Specify the start time and end time of the effective period for the card group.
4) Select card(s) to add to the card group.
5) Click **OK**.

4. Select an access control point (door) of selected device on the Set Authentication Group panel.
5. Input the time interval for card swiping.
6. Add an authentication group for the selected access control point.
   1) Click **Add** on the Set Authentication Group panel.
   2) Select a configured template for the authentication group from the drop-down list.

Note

For setting the template, refer to ***Configure Schedule and Template*** .

3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down 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. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.

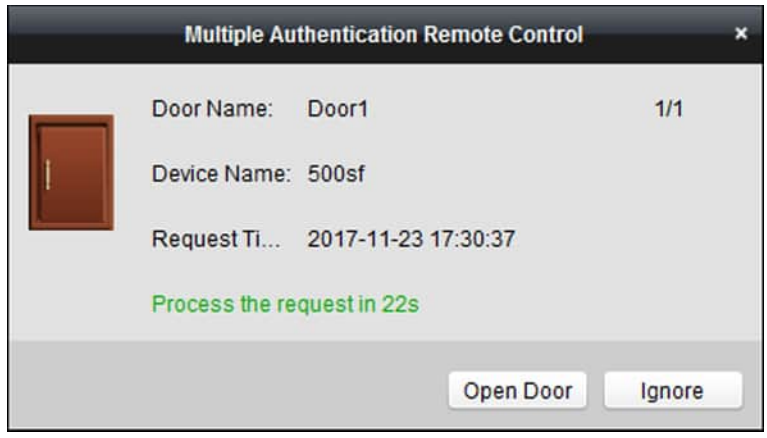


Figure 8-3 Remotely Open Door

Note

You can check **Offline Authentication** 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.

4) Select the added card group in the left list below and click + to add the selected card group to the right list as the authentication group.

5) **Optional:** Click or to set the card swiping order.
6) Click the added authentication group in the right list to set card swiping times.

Note

- The card swiping times should be larger than 0 and smaller than the added card quantity in the card group.
- The maximum value of card swiping times is 16.

7) Click **OK**.

Note

- For each access control point (door), up to four authentication groups can be added.
- For the authentication group of which authentication type is **Local Authentication**, up to 8 card groups can be added to the authentication group.
- For the authentication group of which authentication 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. Click **Save**.

Configure Opening Door with First Card

You can set multiple first cards for one access control point. After the first card swiping, it allows multiple persons access the door or other authentication actions.

Before You Start
Set the card permission and apply the permission setting to the access control device. For details, refer to ***Assign Permission to Person*** .

Perform this task when you want to configure opening door with first card.

Steps
1. Click **Access Control → Advanced Function → Open Door with First Card** to enter the Open Door with First Card page.
2. Select an access control device in the list of Controller List panel.
3. Select the first card mode as **Remain Open with First Card**, **Disable Remain Open with First Card**, or **First Card Authorization** from the drop-down list for each access control point of the selected device.

   Remain Open with First Card

   The door remains open for the configured time duration after the first card swiping until the remain open duration ends. If you select this mode, you should set the remain open duration.

   Note

   The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

Disable Remain Open with First Card

Disable the function of remaining open with first card.

First Card Authorization

All authentications (except for the authentications of super card, super password, super fingerprint, duress card, duress code, and duress fingerprint) are allowed only after the first card authorization.

Note

The **First Card Authorization** is effective only on the current day. The authorization will be expired after 24:00 on the current day.

Note

You can swipe the first card again to disable the first card mode.

4. Click **Add** on the First Card List panel.
5. Select a card in the list and click **OK** to add the selected card as the first card of the doors.

   The added first card will list on the First Card List panel.
6. **Optional:** Select a first card from the list and click **Delete** to remove the card from the first card list.
7. Click **Save**.

Configure Anti-Passback

You can set to only pass the access control point according to the specified path and only one person could pass the access control point after swiping the card.

Before You Start

Enable the anti-passing back function of the access control device.

Perform this task when you want to configure the anti-passing back for the access control device.

Steps

Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to ***Configure Multi-door Interlocking*** .

1. Click **Access Control → Advanced Function → Anti-Passback** to enter the anti-passing back configuration page.
2. Select an access control device in the list.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.
4. Click the text field of the selected first card reader in the **Card Reader Afterward** column to open Select Card Reader dialog.

5. Select the afterward card readers for the first card reader.

Note

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

6. Click **OK** in the dialog to save the selections.
7. Click **Save** at the upper-right corner of Anti-Passback page to save the settings and take effect.

Note

Super credentials, such as super card, super password, super fingerprint, and so on, have the privilege of not following the anti-passback rules.

Example

Set Card Swiping Path

If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

Configure Cross-Controller Anti-passing Back

You can set anti-passing back for card readers in multiple access control devices. 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.

Note

It should be supported by the device.

Configure Route Anti-passing Back Based on Card

The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards. It will judge the anti-passing back according to the entrance and exit records on the card.

Perform this task if you need to configure route anti-passing back and judge the anti-passing back according to the entrance and exit records on the card.

Steps

Note

It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to ***Authenticate M1 Card Encryption*** .

1. Click **Access Control → Advanced Function → Cross-Controller Anti-passing Back** to enter the cross-controller anti-passing back configuration page.
2. Check **Enable Cross-Controller Anti-passing Back** to enable the function.

3. Select **Based on Card** as the anti-passing back mode.
4. Select **Route Anti-passing Back** as the rule.
5. Set the sector ID.
6. Click **Select Access Controller** to select a device for anti-passing back.

Note

Up to 64 devices with anti-passing back function can be added.

7. Set the first card reader and after card readers.
   1) In the Card Reader area, click the icon on the left of the card reader column to set it as the first card reader.

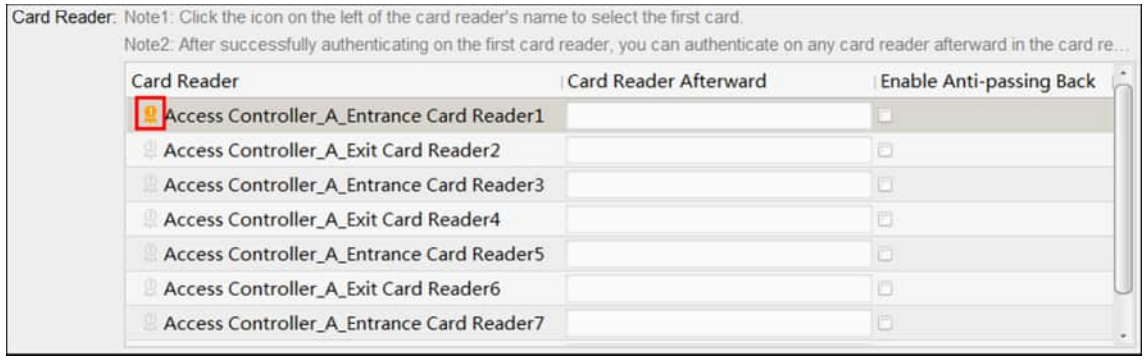


Figure 8-4 Select First Card

   The icon will turn to .
   2) Click the card reader afterward input field to select the card readers afterward in the pop-up window.

Note

- Up to 16 card readers afterward can be added for each card reader.
- The displayed card readers in the card reader afterward input field should be in authentication order.

   3) Check the checkbox in the **Enable Anti-passing Back** column to enable the anti-passing back function.
8. Click **Save**.

Configure Route Anti-passing Back Based on Network

The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards. It will authenticate the anti-passing back according to the entrance and exit information stored on the card reader.

Perform this task if you need to configure route anti-passing back and authentice the anti-passing back recsult according to the entrance and exit information stored on the card reader.

Steps

1. Click **Access Control → Advanced Function → Cross-Controller Anti-passing Back** to enter the cross-controller anti-passing back configuration page.
2. Check **Enable Cross-Controller Anti-passing Back** to enable the function.
3. Select **Based on Network** as the anti-passing back mode.
4. Select **Route Anti-passing Back** as the rule.
5. Select a server in the drop-down list for judging the anti-passing back.

Note

- You can click **Delete Card Swiping Record** and select the card in the pop-up window to delete the card swiping information in all devices.
- Up to 5000 cards' swiping records can be stored in the selected server.

6. Click **Select Access Controller** to select a device for anti-passing back.

Note

Up to 64 devices with anti-passing back function can be added.

7. Set the first card reader and after card readers.
   1) In the Card Reader area, click the icon on the left of the card reader column to set it as the first card reader.

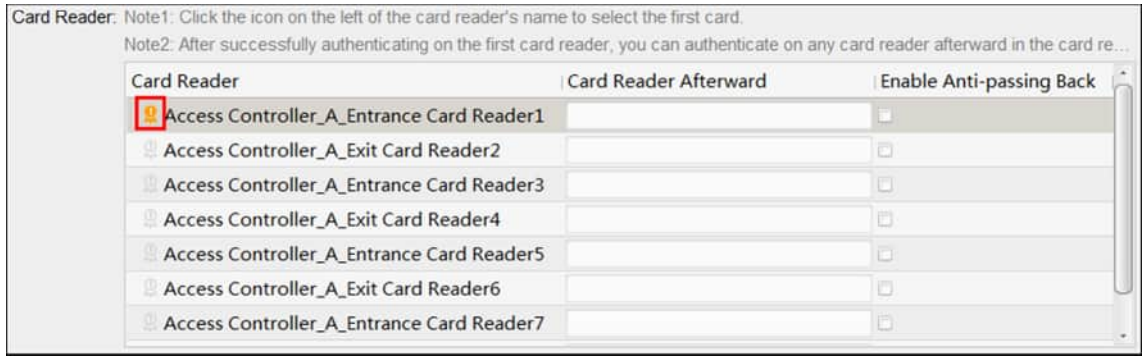


Figure 8-5 Select First Card

   The icon will turn to .
   2) Click the card reader afterward input field to select the card readers afterward in the pop-up window.

Note

- Up to 16 card readers afterward can be added for each card reader.
- The displayed card readers in the card reader afterward input field should be in authentication order.

   3) Check the checkbox in the **Enable Anti-passing Back** column to enable the anti-passing back function.
8. Click **Save**.

Configure Entrance/Exit Anti-Passback Based on Card

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. It will judge the anti-passing back according to the entrance and exit records on the card.

Perform this task if you need to configure entrance/exit anti-passing back and judge the anti-passing back according to the entrance and exit records on the card.

Steps

Note

It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to ***Authenticate M1 Card Encryption*** .

1. Click **Access Control → Advanced Function → Cross-Controller Anti-passing Back** to enter the cross-controller anti-passing back configuration page.
2. Check **Enable Cross-Controller Anti-passing Back** to enable the function.
3. Select **Based on Card** as the anti-passing back mode.
4. Select **Entrance/Exit Anti-passing Back** as the rule.
5. Set the sector ID.
6. Click **Select Access Controller** to select a device for anti-passing back.

   Note

   Up to 64 devices with anti-passing back function can be added.
7. In the Card Reader area, check the checkboxes in the **Enable Anti-passing Back** column to select the entrance card reader and the exit card reader.

   Note

   Up to one entrance carder and one exit card reader should be checked.
8. Click **Save**.

Configure Entrance/Exit Anti-Passback Based on Network

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. It will authenticate the anti-passing back according to the entrance and exit information on the card reader.

Perform this task if you need to configure entrance/exit anti-passing back and judge the anti-passing back according to the entrance and exit information stored on the card reader.

Steps

1. Click **Access Control → Advanced Function → Cross-Controller Anti-passing Back** to enter the cross-controller anti-passing back configuration page.

2. Check **Enable Cross-Controller Anti-passing Back** to enable the function.
3. Select **Based on Network** as the anti-passing back mode.
4. Select **Entrance/Exit Anti-passing Back** as the rule.
5. Select a server in the drop-down list for judging the anti-passing back.

Note

- You can click **Delete Card Swiping Record** and select the card in the pop-up window to delete the card swiping information in all devices.
- Up to 5000 cards' swiping records can be stored in the selected server.

6. Click **Select Access Controller** to select a device for anti-passing back.

Note

Up to 64 devices with anti-passing back function can be added.

7. In the Card Reader area, check the checkboxes in the **Enable Anti-passing Back** column to select the entrance card reader and the exit card reader.

Note

Up to one entrance carder and one exit card reader should be checked.

8. Click **Save**.

Configure Multi-door Interlocking

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.

Perform this task when you want to realize interlocking between multiple doors.

Steps

Note

- 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. For the configuration of anti-passing back function, refer to ***Configure Anti-Passback*** .

1. Click **Access Control → Advanced Function → Multi-door Interlocking** to enter the Multi-door Interlocking page.
2. Select an access control device in the list of Controller List panel.
3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to Interlock window.
4. Select access control point (s) from the list.

Note

Up to four doors can be added in one multi-door interlocking combination.

5. Click **OK** to add the selected access control point(s) for interlocking.

   The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.
6. **Optional:** Select an added multi-door interlocking combination from the list and click **Delete** to delete the combination.
7. Click **Save**.

Configure Authentication Password

You can input the authentication password on the card reader keypad to open the door after setting the authentication password.

Perform this task when you want to configure authentication password to open door.

Note

- The authentication password function should be supported by the access control device.
- Up to 500 cards with authentication password can be added to one access control device. The password should be unique and cannot be same with each other.

Steps

1. Click **Access Control → Advanced Function → Authentication Password** to enter the authentication password configuration page.
2. Select an access control device in the list of Controller List panel.

   All the applied cards and persons will display on the Card List panel.

   Note

   For setting and applying the permissions to the device, refer to ***Assign Permission to Person*** .
3. Click the field of each card in the Password column to input the authentication password.

   Note

   The authentication password should contain 4 to 8 digits.
4. Click **Save** at the upper-right corner of Authentication Password page to save the settings.

   The authentication password function of the card will be enabled automatically. And you can set the card reader authentication mode of access control device as **Card or Authentication Password**. Refer to ***Configure Card Reader Authentication Mode and Schedule*** for details.

Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start

Wire the third party card readers to the device.

Perform this task to configure the custom Wiegand rule for the third party card readers.

Steps

Note

- 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.
- For details about the custom Wiegand, see ***Custom Wiegand Rule Descriptions*** .

1. Click **Access Control → Advanced Function → Custom Wiegand** to enter the custom Wiegand configuration page.
2. Select a custom Wiegand on the left.
3. Check **Enable** to enable the custom Wiegand.
4. Create a Wiegand name.

   Note

   Up to 32 characters are allowed in the custom Wiegand name.
5. Click **Select Device** to select the access control device for setting the custom wiegand.
6. Set the parity according to the property of the third party card reader.

   Note

   - Up to 80 bits are allowed 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.
7. Set output transformation rule.
   1) Click **Set Rule** to open the Set Output Transformation Rules window.

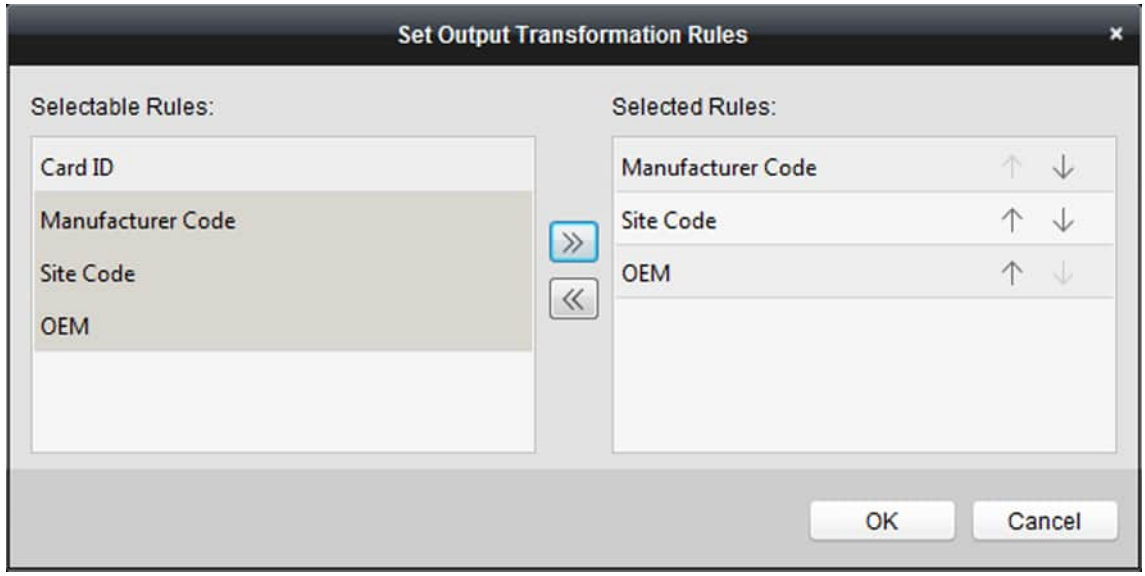


Figure 8-6 Set Output Transformation Rule

2) Select rules on the left list.
3) Click » to move the selected rules to the right list.
4) **Optional:** Click ↓ or ↑ to change the rule order.
5) Click **OK**.
6) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

8. Click **Save**.

8.1.9 Search Access Control Event

You can search the access control history events including remote event and local event via the client.

Search Access Control Events Stored in Local Client

You can search the history access records and events from the database of the current client and export the records to local PC.

Steps

Note

You can search the access control events within three months.

1. Click **Access Control → Search → Access Control Event** to enter the searching access control event page.
2. Select the event source as **Local Event**.
3. Set the search conditions, such as device(s), event type, occurred time, and so on.

4. Click **Search** to start searching the access control events.

   The matched access control events will display.
5. **Optional:** After searching the events, you can do one or more of the followings.

View Person Details	For the access control event which is triggered by person, click the event to view the person details, including person No., person name, organization, phone number, contact address and photo.
View Linked Video	For events contain linked video, click **Playback** column to view the recorded video file of the triggered camera when the alarm is triggered. **Note** For setting the triggered camera, refer to ***Configure Client Actions for Access Event*** .
Export Event Information	Click **Export** to export the search results to the local PC in CSV file.

Search Remote Access Control Event

You can search the access control event records stored on the access control device.

Perform this task when you need to search the access control events stored on the access control device.

Steps

1. Click **Access Control → Search → Access Control Event** to enter the searching remote access control event page.
2. Select the event source as **Remote Event**.
3. Set the search conditions as desired.
4. Click **Search**.

   The matched access control events will display.
5. **Optional:** Click **Export** to export the search results to the local PC in CSV file.

8.1.10 Configure Access Control Alarm Linkage

For the added access control device, you can configure the linkage actions such as client linkage, device linkage, or cross-device linkage.

Configure Client Actions for Access Event

You can assign client linkage actions to the event by setting up a rule. For example, when the event is detected, an audible warning appears to notify the security personnel.

Steps

Note

The linkage actions here refer to the linkage of the client software's own actions such as audible warning, email linkage, etc.

1. Click **Event Management → Access Control Event** .

   The added access control devices will display in the device list.
2. Select a resource from the device list.

   The event types which the selected resource supports will display.
3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.
4. Set the linkage actions of the event.

   1) Select the event(s) and click **Edit Linkage** to set the client actions when the events triggered.

   Audible Warning

   The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.

   Note

   For setting the alarm sound, please refer to *Set Alarm Sound* in the user manual of the client software.

   Email Linkage

   Send an email notification of the alarm information to one or more receivers.

   2) Click **OK**.
5. Enable the event so that when the event is detected, en event will be sent to the client and the linkage actions will be triggered.
6. **Optional:** Click **Copy to...** to copy the event settings to other access control device, alarm input, door, or card reader.

Configure Device Linkage for Access Control Alarm

You can set the access control device's linkage actions for the access control device's triggered alarm. When the alarm is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

Perform this task when you need to configure the access control device linkage for the device's access control alarm.

Steps

Note

It should be supported by the device.

1. Click **Event Management → Event Card Linkage** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Event Linkage**.
5. select the alarm type and detailed alarm to set the linkage.
6. In the Linkage Target panel, set the property switch to on to enable this action.

   Host Buzzer

   The audible warning of access control device will be triggered.

   Capture

   The real-time capture will be triggered.

   Recording

   The recording will be triggered.

   Note

   The device should support recording.

   Card Reader Buzzer

   The audible warning of card reader will be triggered.

   Alarm Output

   The alarm output will be triggered for notification.

   Zone

   Arm or disarm the zone.

   Note

   The device should support zone function.

   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.
   - The target door and the source door cannot be the same one.

   Audio Play

   The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.
7. Click **Save**.
8. **Optional:** After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

Configure Device Linked Actions for Card Swiping

You can set the access control device's linkage actions for the specified card swiping. When you swipe the specified card, it can trigger the alarm output, host buzzer, and other actions on the same device.

Perform this task when you need to configure the access control device linkage for the card swiping action.

Steps

Note

It should be supported by the device.

1. Click **Event Management → Event Card Linkage** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Card Linkage**.
5. Input the card number or select the card from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target panel, set the property switch to on to enable this action.

Host Buzzer

The audible warning of access control device will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

Note

The device should support recording.

Card Reader Buzzer

The audible warning of card reader will be triggered.

Alarm Output

The alarm output will be triggered for notification.

Zone

Arm or disarm the zone.

Note

The device should support zone function.

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.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.

When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. **Optional:** After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

Configure Employee ID Linkage

When person enter the employee ID on the specified card reader, it can trigger linkage actions of other devices, such as alarm output, opening door, etc.

Before You Start

Add person. For details, see *Manage Person Information*.

Steps

1. Click **Event Management → Event Card Linkage** to enter the Event Card Linkage page.
2. Select an access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select the event source as **Employee ID Linkage**.
5. Select an employee ID from the drop-down list.
6. In the Linkage Target panel, set the property switch to On to enable the linkage action.

Host Buzzer

The audible warning of access control device will be triggered.

Capture

The real-time capture will be triggered.

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.

7. Click **Save**.

When the employee ID has entered on the selected card reader, it can trigger the linked actions (configured in step 7).

8. After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

Configure Cross-Device Linkage

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

Note

It should be supported by the device.

Configure Cross-Device Linkage for Access Control Event

When the access control event is triggered and detected, it can trigger linkage actions of other access control device, such as alarm output, opening door, etc. The event can be divided into four types: device event, alarm input, door event, and card reader event.

Perform this task when you need to configure other access control device's linkage actions for access control event.

Steps

Note

The devices should support this function.

1. Click **Event Management → Cross-Device Linkage** to enter the cross-device linkage configuration interface.

2. Click **Add** to add a new cross-device linkage.
3. Select the linkage type as **Event Linkage**.
4. Set the event source.
   1) Select the access control device as event source device.
   2) Select the access control event type.

   Device Event

   Select the detailed event type from the dropdown list.

   Alarm Input

   Select the detailed event type as zone event or alarm input event and select the zone name or alarm input name from the dropdown list.

   Door Event

   Select the detailed event type and select the access control point from the dropdown list.

   Card Reader Event

   Select the detailed event type and select the card reader from the dropdown list.
5. Set the target access control device as linkage target.
   1) Select the access control device from the dropdown list as the linkage target.
   2) Set the switch to on to enable the linkage action.

   Alarm Output

   The alarm output pf the target device 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.
6. Click **Save**.

Configure Cross-Device Linkage for Card Swiping

When person swipes the specified card on the specified card reader, it can trigger linkage actions of other access control device, such as alarm output, opening door, etc.

Perform this task when you need to configure other access control device's linkage actions for card swiping.

Steps

1. Click **Event Management → Cross-Device Linkage** to enter the cross-device linkage configuration interface.
2. Click **Add** to add a new cross-device linkage.
3. Select the linkage type as **Card Linkage**.
4. Set the event source.

1) Select the card from the dropdown list.
2) Select the access control device as event source device.
3) Select the card reader for triggering.

5. Set the target access control device as linkage target.
   1) Select the access control device from the dropdown list as the linkage target.
   2) Set the switch to on to enable the linkage action.

   Alarm Output

   The alarm output pf the target device 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.

6. Click **Save**.

Configure Cross-Device Linkage for Employee ID

When person enter the employee ID on the specified card reader, it can trigger linkage actions of other access control device, such as alarm output, opening door, etc.

Perform this task when you need to configure other access control device's linkage actions for entering employee ID.

Steps

1. Click **Event Management → Cross-Device Linkage** to enter the cross-device linkage configuration interface.
2. Click **Add** to add a new cross-device linkage.
3. Select the linkage type as **Employee ID Linkage**.
4. Set the employee ID.
   1) Select the access control device as event source device.
   2) Select the card reader for triggering.
5. Set the target access control device as linkage target.
   1) Select the access control device from the dropdown list as the linkage target.
   2) Set the switch to on to enable the linkage action.

   Alarm Output

   The alarm output pf the target device 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.

6. Click **Save**.

8.1.11 Manage Access Control Point Status

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

Group Access Control Points

Before controlling the doors status and setting the status duration, you should organize the access control device's access control points into groups for convenient management.

Perform this task when you need to group the access control points for convenient management.

Steps

Note

- You can also import the access control device's alarm inputs into groups.
- For video access control terminal, you can import its camera into groups.
- For other detailed operations, refer to *Group Management*.

1. Click **Device Management → Group** to enter the group management page.
2. Add a new group.
   1) Click to open the Add Group window.
   2) Create a group name.
   3) **Optional:** Check **Create Group by Device Name** to create the new group by the name of the selected device.
   4) Click **OK**.
3. Import the access control points to the group.
   1) Click **Import**.
   2) Click **Access Control Point** tab.
   3) Select the access control points in the list.
   4) Select a group from the group list.
   5) Click **Import** to import the selected access control points to the group.

Control Door Status

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

Perform this task when you need to control the door's status.

Steps

1. Click **Status Monitor → Door Status** to door status monitoring page.
2. Select an access control group on the left.

   Note

   For managing the access control group, refer to *Group Access Control Points*..

   The access control points of the selected access control group will be displayed on the right.
3. Click on the Status Information panel to select a door.
4. Click the following buttons listed on the Status Information panel to control the door.

   Open Door

   Open the door once.

   Close Door

   Close the door once.

   Remain Open

   Keep the door open.

   Remain Closed

   Keep the door closed.

   Note

   - Make sure the door has linked to a door contact, or the door status cannot be displayed in the operation log.
   - Make sure the access control point cannot be armed by other client software, or you may not view the changes of door status. Only one client software can arm the device, and then view the changes of the door status, receive the alarm messages from the access control point.

Check Real-time Access Records

The access records of all access control devices will display in real time, including card swiping records, face recognitions records, fingerprint comparison records, etc.

Steps

1. Click **Status Monitor** and you can view the real-time access records.

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

2. **Optional:** Check **Show Latest Access Record** and the latest access record will be selected and displayed at the top of the record list.
3. **Optional:** Click the event to view the person details, including captured person pictures (captured picture and profile) person No., person name, organization, phone, contact address, etc.

   Authentication Result

   Access results such as card No. not registered, succeeded, etc.

Check Real-time Access Control Alarm

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

Perform this task when you need to check the real-time access control alarms.

Steps

1. Click **Status Monitor → Access Control Alarm** to enter the real-time access control alarm page.

   All access control alarms will display in the list in real time.You can view the alarm type, alarm time, location, etc.
2. Click to view the alarm on E-map.

   Note

   For configuring the access control point on E-map, refer to ***Display Access Control Point on E-map*** .
3. **Optional:** 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 ***Configure Client Actions for Access Event*** .
4. **Optional:** Select the alarm that the client can receive when the alarm is triggered.
   1) Click **Subscribe**.
   2) Check the checkbox(es) to select the alarm(s), including device exception alarm, door event alarm, card reader alarm, and alarm input.
   3) Click **OK** to save the settings.

8.1.12 Control Door during Live View

During live view, you can control the camera's linked access control point (door) such as opening door, closing door, etc.

Perform this task when you need to control the camera's linked door to open or close during live view.

Steps

1. Enter **Live View** module and start live view of one camera.

   Note

   For details about starting live view, refer to for details.

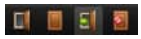
2. Link the camera with an access control point.
   1) Right click on the live view window and select **Link to Access Control Point** to open the Set Linked Access Control Point window.
   2) Check **Enable** to enable the linkage.
   3) Select access control point from the drop-down list.
   4) Click **OK**.

   Note

   One camera can be linked to only one access control point; Different cameras can be linked to the same access control point.

3. Start the camera's live view again to make the settings effective.

   Four door control buttons will appear on the toolbar during live view.

4. Click  to control the door to open, close, remain open, or remain closed.

8.1.13 Display Access Control Point on E-map

You can add the access control point on the E-map. When the alarm of the access control point is triggered, you can view the alarm notification on the E-map, check the alarm details, and control the door.

Perform this task when you need to display the access control point on the e-map as hot spot.

Steps

Note

- For Video Access Control Terminal, you can also add its camera to the E-map to view the live view of the camera.
- For detailed operations of E-map, refer to .

1. Enter **E-map** module.
2. Click **Edit** on the E-map toolbar to enter the map editing mode.
3. Click on the toolbar to open the Add Hot Spot window.
4. Select the access control point to be added as hot spot.
5. **Optional:** Edit hot spot name, select the name color, and select the hot spot icon by double-clicking the corresponding field.
6. Click **OK**.

The door icons are added on the map as hot spots and the icons of added access control points change from to in the group list. You can click-and-drag the access control point icons to move the hot spots to the desired locations.

7. After adding the access control point on the map as hot spot, you can control the access control point and view triggered alarm.
   1) Click **Exit Editing Mode** on the E-map toolbar to enter the map preview mode.
   2) To control the access control point, you can right click the access control point icon on the map, and click **Open Door**, **Close Door**, **Remain Open**, and **Remain Closed** to control the door.

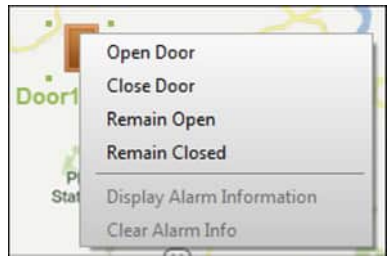


Figure 8-7 Control Access Control Point on Map

   3) **Optional:** If there is any alarm triggered, an icon will appear and twinkle near the hot spot (it will twinkle for 10s). Click the alarm icon to check the alarm information, including alarm type and triggering time.

Note

To display the alarm information on the map, you should set display on e-map as the alarm linkage action. For details, refer to ***Configure Client Actions for Access Event*** .

8.2 Remote Configuration (Web)

Configure device parameters remotely.

8.2.1 Time Management

Manage device's time zone, time synchronization, and DST parameters.

Time Zone and Time Synchronization

On the Device for Management page, select a device and click **Remote Configuration → System → Time** to enter the Time tab.
You can select a time zone, set NTP parameters, or manually synchronize time.

Time Zone

Select a time zone from the drop-down list.

NTP

The device will synchronize time with NTP automatically. After you enable **NTP**, you should set the NTP server address, NTP port, and synchronization interval.

Manual Time Synchronization

After you enable **Manual Time Synchronization**, you can manually set the device time.

If you check **Synchronize with Computer Time**, the **Set Time** will display the current computer's time. At this time, uncheck **Synchronize with Computer Time**, and click , you can edit the device time manually.

Click **Save** to save the settings.

DST

On the Device for Management page, click **Remote Configuration → System → Time → DST** to enter the DST tab.
Enable DST and you can edit the DST bias time, the DST start time, and end time.
Click **Save**.

8.2.2 Network Parameters Settings

Set device network parameters, including the NIC type, DHCP, and HTTP.

On the Device for Management page, click **Remote Configuration → Network → Network Parameters** to enter the Network Parameters Settings tab.

NIC Type

Select a NIC type from the drop-down list. You can select either Self-adaptive, 10M, or 100M.

DHCP

If you disable the function, you should manually set the device's IPv4 address, IPv4 subnet mask, IPv4 default gateway, MTU, and port.

If you enable the function, the system will automatically assign IPv4 address, IPv4 subnet mask, IPv4 default gateway for the device.

HTTP

Set the HTTP port, DNS1 server address, and DNS2 server address.

8.2.3 Report Strategy Settings

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

On the Device for Management page, click **Remote Configuration → Network → Report Strategy** to enter the Report Strategy Settings tab.

You can set the center group and the system will transfer logs via EHome protocol. Click **Save** to save the settings.

Center Group

Select a center group from the drop-down list.

Main Channel/Backup Channel

The device will communicate with the center via the main channel. When exception occurs in the main channel, the device and the center will communicate with each other via the backup channel.

Note

- N1 refers to wired network and G1 refers to GPRS.
- Only device with 3G/4G function supports setting the channel as G1.

8.2.4 Network Center Parameters Settings

You can set the notify security center, center's IP address, the port No., the protocol (EHome), the EHome account user name,etc. to transmit data via EHome protocol.

On the Device for Management page, click **Remote Configuration → Network → Network Center Parameters** to enter the Network Center Parameters Settings tab.

Select a center from the drop-down list.

After enabling the function, you can set the center's address type, IP address/domain name, and port No., create EHome user name, etc.

Note

If set the EHome type as EHome5.0, you should create an EHome key as well.

Click **Save**.

After creating the EHome information, you can add the device via EHome protocol.

8.2.5 Change Device Password

You can change the device password.

Before You Start

Make sure the device is activated. For details, see *Activation*.

Steps

1. On the Device for Management page, click **Remote Configuration → System → User** to enter the User tab.
2. Select a user and click **Edit** to enter the Edit page.
3. Input the old password, create a new password, and confirm the new password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: 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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Click **OK**.

Result

The device password is changed. You should enter the new password on the Device for Management page to reconnect the device.

8.2.6 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **Remote Configuration → System → Security** to enter the Security Mode tab.

Select a security mode from the drop-down list, and click **Save**.

Security Mode

High security level for user information verification when logging in the client software.

Compatible Mode

The user informaiton verification is compatible with the old client software version when logging in.

8.2.7 Optimize Event Name

The system will upload the optimized event name to the client software after enabling the function.

On the Device for Management page, click **Remote Configuration → Settings → Event → Optimize Event Name** .

Enable **Optimize Event Name**, and click **Save**.

The system can upload the optimized event name to the client software.

8.2.8 Set Event Mode

According to the employee ID length, you can set different event mode. Different event modes supports different event capacities.

On the Device for Management page, click **Remote Configuration → Settings → Event → Event Mode** .

Select an event mode from the drop-down list and click **Save**.

Mode A

250,000 events storage of the device. Supports employee ID of 32 characters (combination among digits and lowercase letters) or 16 characters (combination among uppercase letters, lowercase letters, digits and special characters).

Mode B

300,000 events storage of the device. Supports employee ID of 24 characters (combination among digits and lowercase letters) or 12 characters (combination among uppercase letters, lowercase letters, digits and special characters).

8.2.9 System Maintenance

You can reboot the device, restore the device to the default settings, and upgrade the device.

Reboot

On the Device for Management page, click **Remote Configuration → System → System Maintenance** to enter the System Maintenance tab.
Click **Reboot** and the device starts rebooting.

Restore Default Settings

On the Device for Management page, click **Remote Configuration → System → System Maintenance** to enter the System Maintenance tab.

Restore Default

The parameters will be restored the default ones, excluding the IP address.

Restore All

All device parameters will be restored to the default ones. The device should be activated after restoring.

Upgrade

On the Device for Management page, click **Remote Configuration → System → System Maintenance** to enter the System Maintenance tab.
Select a device type from the drop-down list, click **Browse** and select an upgrade file from the local computer, and click **Upgrade**.

Note

- If you select Card reader as the device type, you should also select a card reader No. from the drop-down list.
- The upgrade will lasts for about 2 min. Do not power off during the upgrading. After upgrading, the device will reboot automatically.

8.3 Time and Attendance

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.

Note

In this section, we introduce the configurations before you can getting the attendance reports. The access records recorded after these configurations will be calculated in the statistics.

8.3.1 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.

You can set department schedule, person schedule, and temporary schedule.

Add Time Period

You can add the time period for the shift schedule.

Perform this task when you need to add time period.

Steps

1. Enter Time and Attendance module and click **Shift Schedule Management** tab.
2. Click **Shift Settings → Time Period Settings** to enter Time Period Settings window.
3. Click **Add** to enter Add Time Period page.
4. Set the time period related parameters.

   Attend at Least

   Set the minimum attendance time.

Note

If you have configured the different card readers as start-work and end-work check points, you can check **Absence time is not included in effective work hours** to exclude the absence time from the work hours.

Check-in / Check-out Required

Check the checkboxes and set the valid period for check-in or check-out.

Mark as Late/Mark as Early Leave

Set the time period for late or early leave.

Exclude Break Period from Work Duration

Check the checkbox and set the break period excluded.

Note

Up to 3 break periods can be set.

Set as Pay-per-Time Period

Check the checkbox and set the pay rate and minimum time unit.

5. Click **Save**.

The added time period lists on the left panel of the window.

Add Shift

You can add the shift for the shift schedule.

Before You Start

Add a time period first. See ***Add Time Period*** for details.

Perform this task when you need to add shift.

Steps

1. Enter Time and Attendance module.
2. Click **Shift Schedule Management → Shift Settings → Shift** to enter Shift Settings window.
3. Click **Add** to enter Add Shift page.
4. Input the name for shift.
5. Select the shift period from the drop-down list.
6. Select the added time period and click on the time bar to apply the time period.
7. Click **Save**.

The added shift lists on the left panel of the window.

Set Department Schedule

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Before You Start

In Time and Attendance module, the department list is the same with the organization in Access Control module. You should add departments and persons in Access Control module first. See ***Manage Organization*** and ***Manage Person Information*** for details.

Perform this task when you need to set department schedule.

Steps

1. Click **Time and Attendance → Shift Schedule Management** to enter the Shift Schedule Management page..
2. Select a department and click **Department Schedule** to pop up Department Schedule window.
3. Check **Time and Attendance** .

   All persons in the department expect those excluded from attendance will apply the attendance schedule.
4. Select the shift from the drop-down list.
5. Set the start date and end date.
6. Set other parameters for the schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, or Effective for Multiple Shift Schedules.

   Note

   After checking the **Effective for Multiple Shift Schedules**, you can select the effective time period(s) from the added time periods for the persons in the department.

   Multiple Shift Schedules

   It contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.
   If the multiple shift schedules contains three time periods: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three time periods. If the person checks in at 07:50, it will apply the nearest time period 08:00 to 15:00 to the person's attendance.
7. **Optional:** Check **Set as Default for All Persons in Department**.

   All persons in the department will use this shift schedule by default.
8. **Optional:** If the selected department contains sub department(s), you can check **Set as Shift Schedule for All Sub Departments** to apply the department schedule to its sub departments.
9. Click **Save**.

Set Person Schedule

You can assign the shift schedule to one person. You can also view and export the person schedule details.

Before You Start

Add department and person in Access Control module. See ***Manage Organization*** and ***Manage Person Information*** for details.

Perform this task when you need to set person schedule.

Steps

1. Enter Time and Attendance module.
2. Click **Shift Schedule Management** to enter the Shift Schedule Management page.
3. Select the department and select one person.
4. Click **Person Schedule** to pop up Person Schedule window.
5. Check **Time and Attendance**.

   The configured person will apply the attendance schedule.
6. Select the shift from the drop-down list.
7. Set the start date and end date.
8. Set other parameters for the schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, and Effective for Multiple Shift Schedules.

   Note

   After checking the **Effective for Multiple Shift Schedules**, you can select the effective time period(s) from the added time periods for the persons in the department.

   Multiple Shift Schedules

   It contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.
   If the multiple shift schedules contains three time periods: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three time periods. If the person checks in at 07:50, it will apply the nearest time period 08:00 to 15:00 to the person's attendance.
9. Click **Save**.

Set Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and export the temporary schedule details.

Before You Start

Add department and person in Access Control module, and set the attendance rule for the person. See ***Manage Organization*** and ***Manage Person Information*** for details.

Perform this task when you need to set temporary schedule.

Steps

Note

The temporary schedule has higher priority than department schedule and person schedule.

1. Enter Time and Attendance module.
2. Click **Shift Schedule Management** tab to enter the Shift Schedule Management page.
3. Select the department and select one person.
4. Click **Temporary Schedule** to pop up Temporary Schedule window.
5. Click to set the shift date.
6. Select the time period.
7. Click the time bar to apply the time period for the select date.
8. **Optional:** Click **Advanced Settings** and select advanced attendance rules for the temporary schedule.
9. Click **Add**.

Check and Edit Shift Schedule

You can check the shift schedule details and edit the schedule.

Perform this task when you need to check and edit shift schedule.

Steps

1. Enter Time and Attendance module.
2. Click **Shift Schedule Management** tab to enter the Shift Schedule Management page.
3. Select the department and corresponding person(s).
4. Click **View** to open Shift Schedule Details window.

   The shift schedule details display.
5. Edit the normal schedule details.
   1) Click **Normal Schedule** tab.
   2) Select a shift from the drop-down list.
   3) Click **Attendance Rule Settings** to open Attendance Rule Settings window.
   4) Select the attendance rules as desired and click **OK**.
   5) Click to set the effective date.
   6) Click **Save**.
6. **Optional:** Click **Temporary Schedule** and perform one of the following operations.

Add	Add the temporary schedule for the selected person.
	Edit the time period.
	Delete the temporary schedule.

8.3.2 Manually Correct Check-in/out Record

If the attendance status is not correct, you can manually correct the check-in or check out record. You can also edit, delete, search, or export the check-in or check-out record.

Before You Start

- You should add organizations and persons in Access Control module. For details, refer to ***Manage Organization*** and ***Manage Person Information*** .
- The person's attendance status is incorrect.

Perform the following steps to correct the check-in or check-out record.

Steps

1. Enter Time and Attendance module.
2. Click **Attendance Handling → Check-in/out Correction** to enter the Check-in/out Correction page.
3. Click **Add** to enter the Add Check-in/out Correction window.
4. Set the check-in/out correction parameters.
   - Check **Check-in** and set the actual start-work time.
   - Check **Check-out** and set the actual end-work time.
5. Click **Employee Name** field and select the person for correction.
6. **Optional:** Input the remark information as desired.
7. Click **Add**.
8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

Search	Set the search conditions and search the correction.
Modify	Edit the selected check-in/out correction.
Delete	Delete the selected check-in/out correction.
Report	Generate and view the check-in/out correction report.
Export	Export the check-in/out correction details to local PC.

Note

The exported details are saved in CSV format.

8.3.3 Add Leave and Business Trip

You can add leave and business trip application when the employee want to ask for leave or go on a business trip.

Before You Start

You should add organizations and persons in the Access Control module. For details, refer to ***Manage Organization*** and ***Manage Person Information*** .

Perform the following steps when you want to add a leave or business trip application.

Steps

1. Enter Time and Attendance module.
2. Click **Attendance Handling → Leave and Business Trip** to enter the Leave and Business Trip page.
3. Click **Add** to open the Add Leave and Business Trip Application window.
4. Select the leave and business trip type from the drop-down list.

   Note

   You can set the leave type in Advanced Settings. For details, refer to ***Configure Leave Type*** .
5. Click and set the time period for your leave or business trip.
6. Click **Employee Name** filed and select the person for the application in the pop-up Add Person window.
7. **Optional:** Input the remark information as desired.
8. Click **Add**.

   The added leave and business trip displays on the Leave and Business Trip page.
9. **Optional:** After adding the leave and business trip application, perform one of the following operations.

   Modify Select the leave and business trip and click **Modify** to edit the leave or business application.

   Delete Select the leave and business trip and click **Delete** to delete the leave or business trip application.

   Report Click **Report** to generate the leave or business trip report.

   Export Click **Export** to export the leave or business trip details to local PC.

   Note

   The exported details are saved in CSV format.

8.3.4 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

Automatically Calculate Attendance Data

You can set a schedule so that the client can calculate the attendance data automatically at the time you configured every day.

Perform this task if you need to set the time to make the client calculate attendance data automatically.

Steps

Note

It will calculate the attendance data till the previous day.

1. Enter the Time and Attendance module.
2. Click **Attendance Handling → Attendance Calculation** to enter the attendance record calculation page.
3. In the Auto-Calculate Attendance panel, set the time that you want the client to calculate the data every day.
4. Click **Save**.

Manually Calculate Attendance Data

You can calculate the attendance data manually by setting the data range.

Perform the following steps to manually calculate the attendance data.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Handling → Attendance Calculation** to enter the attendance record calculation page.
3. In the Manually Calculate Attendance panel, set the start time and end time to define the attendance data range.
4. Click **Calculate**.

Note

It can only calculate the attendance data within three months.

8.3.5 Configure Advanced Settings

You can configure the advanced settings for the attendance, including the attendance basic settings, attendance rule settings, attendance check point settings, holiday settings, and leave type settings.

Configure Basic Parameters

You can configure the attendance basic parameters, including the start day of each week, the start date of each month, and the non-work day.

Perform the following steps to configure the attendance basic parameters.

Steps

1. Enter Time and Attendance module.
2. Click **Advanced Settings → Basic Settings** to enter the Basic Settings page.
3. Set the start day of each week and the start date of each month from the drop-down list.
4. Set the non-work day settings.

   Set as Non-Work Day

   Check the checkboxes to set the dates as non-work days.

   Set Non-Work Day's Color in Report

   Select the color from the Select Color window. The non-work days in the report will mark as the configured color.

   Set Non-Work Day's Mark in Report

   Input the mark and the non-work day field in the report will display with the mark.
5. Set the authentication type, which means the client will calculate the attendance data recorded based on the selected authentication type.
6. Click **Save**.

Configure Attendance Rule

You can configure the attendance rule for all shifts before setting shift. You can configure the rule for attendance/absence, check-in/out, and overtime.

Perform the following steps to configure the attendance rule.

Steps

Note

The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

1. Enter Time and Attendance module.
2. Click **Advanced Settings → Attendance Rule Settings** to enter the Attendance Rule Settings page.
3. Set rule parameters, including attendance/absence parameters, check-in/out parameters, and overtime parameters.
4. **Optional:** Check **Non-scheduled Work Day** and set the overtime rule for non-work day.
5. Click **Save**.

Configure Attendance Check Point

You can set the card reader(s) of the access control point as the attendance check point, so that the card swiping on the card reader(s) will be valid for attendance.

Before You Start

You should add access control device before configuring attendance check point. For details, refer to ***Add Device*** .

Perform the following steps to set the card reader of the access control point as the attendance check point.

Steps

Note

By default, all card readers of the added access control devices are set as attendance checkpoint.

1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Attendance Check Point Settings** to enter the Attendance Check Point Settings page.
3. **Optional:** Uncheck **Set All Card Readers as Check Points**.

   Only the card readers in the list will be set as the attendance check points.
4. Click + to enter the Add Attendance Check Point window.
5. Set the related parameters.

   Check Point Name

   Customize a name for the check point.

   Card Reader

   Select the card reader from the drop-down list as the attendance check point.

   Check Point Function

   Select the check point function from the drop-down list. You can set the check point as Start/End-Work check point, Start-Work check point, or End-Work check point.

   Door Location

   Input the door location's name.

   Check Point Description

   Input the check point's descriptions as desired.
6. Click **Add**.

   The added attendance check point displays on the list.
7. **Optional:** After adding the attendance check point, perform one of the following operations.

   Edit the attendance check point information.

   Delete the attendance check point in the list.

Configure Holiday

You can add the holiday during which the check-in or check-out will not be recorded.

Add Holiday with Fixed Date

You can configure a holiday which will take effect for only once.

Perform this task if you want to configure a holiday with fixed date.

Steps

1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Holiday Settings** to enter the Holiday Settings page.
3. Click + to pop up the Add Holiday window.
4. Click **Fixed Date** tab.

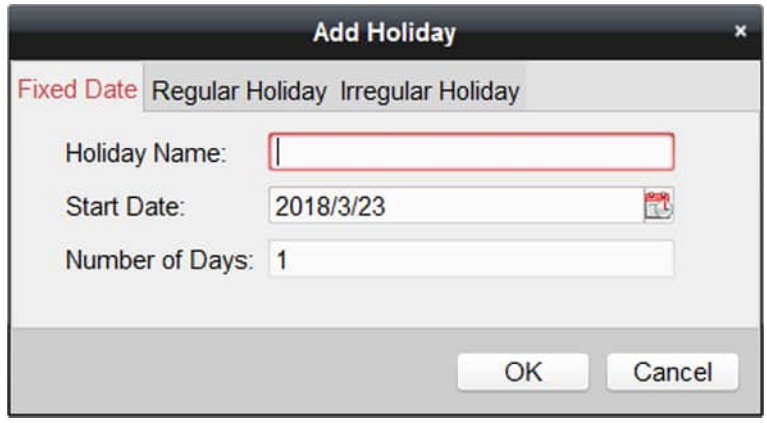


Figure 8-8 Add Holiday with Fixed Date

5. Customize a name for the holiday.
6. Set the start date as the first day of the holiday.
7. Set the number of days in the holiday.
8. **Optional:** After adding the holiday, perform one of the following operations.

   Edit the holiday information.

   Delete the holiday from the holiday list.

Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.

Perform this task if you need to add a regular holiday.

Steps

1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Holiday Settings** to enter the Holiday Settings page.
3. Click + to pop up the Add Holiday window.
4. Click **Regular Holiday** tab.

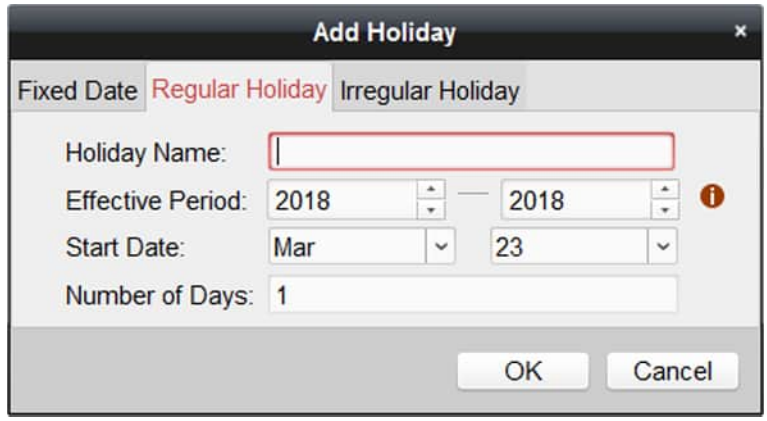


Figure 8-9 Add Regular Holiday

5. Set the holiday parameters.

   Start Date

   The first day of the holiday.

   Effective Period

   The years during which the holiday's start date will take effect. For example, if the holiday's effective period is set as 2018 to 2019, and the start date is set as December 31st, and the numbers of days is 3, then the holiday will be 2018/12/31 to 2019/01/02, 2019/12/31 to 2020/01/02.
6. Click **OK**.
7. **Optional:** After adding the holiday, perform one of the following operations.

   Edit the holiday information.

   Delete the holiday from the holiday list.

Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

Perform this task if you want to add an irregular holiday.

Steps

1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Holiday Settings** to enter the Holiday Settings page.
3. Click to pop up the Add Holiday window.
4. Click **Irregular Holiday** tab.

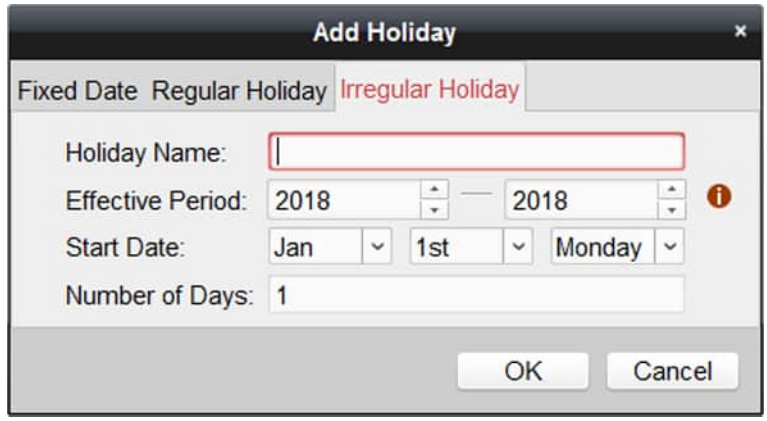


Figure 8-10 Add Irregular Holiday

5. Set the holiday parameters.

Start Date

The first day of the holiday.

Effective Period

The years during which the holiday's start date will take effect. For example, if the holiday's effective period is set as 2018 to 2019, and the start date is set as December 31st, and the numbers of days is 3, then the holiday will be 2018/12/31 to 2019/01/02, 2019/12/31 to 2020/01/02.

Note

If one holiday crosses two years and the effective period

6. Click **OK**.
7. **Optional:** After adding the holiday, perform one of the following operations.

Edit the holiday information.

Delete the holiday from the holiday list.

Configure Leave Type

You can customize the leave type according to actual needs. By default, there are three major leave types: Leave, Day Off in Lieu, and Go Out on Business.

Perform the following steps to add, edit, or delete the leave type.

Steps

1. Enter the Time and Attendance module.
2. Click **Advanced Settings → Leave Type Settings** to enter the Leave Type Settings page.
3. Click + to add a major leave type on the left panel.
4. **Optional:** Perform one of the following operations for major leave type.

Edit the major leave type.

Delete the major leave type.

5. Click to add a minor leave type on the right panel.
6. **Optional:** Perform one of the following operations for major leave type.

Edit the minor leave type.

Delete the minor leave type.

8.3.6 View Attendance Report

After calculating attendance data, you can check the attendance summary, attendance details, abnormal attendance, overtime, card swiping logs and reports based on the calculated attendance data.

Get an Overview of Employees' Attendance Data

You can search the employee's required attendance times, actual attendance times, late times, early leave times, absent times, overwork times, leave times, etc. in a time period to get an overview of the employees' attendance data.

Before You Start

- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to ***Manage Organization*** and ***Manage Person Information*** .
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Perform the following steps to search the employees' all attendance data in a time period.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Attendance Summary** to enter the Attendance Summary page.
3. Select a department from the drop-down list.
4. **Optional:** Input the person name for search.
5. Select the attendance start date and end date that you want to search from.
6. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.

The result displays on the page. You can view the employee's required attendance times, actual attendance times, late times, early leave times, absent times, overwork times, leave times, etc.

8. **Optional:** After searching the result, perform one of the following operations.

   Report Generate the attendance report.

   Export Export the results to the local PC.

Search Employees' Detailed Attendance Data

You can search the employee's every attendance data with details, including the attendance date, the person belonged shift, time period, start-work status, end-work status, check-in time, check-out time, late period, early leave period, attendance period, absence period, leave period, and overwork period.

Before You Start

- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to ***Manage Organization*** and ***Manage Person Information*** .
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Perform the following steps to search the employee's detailed attendance data.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Attendance Details** to enter the Attendance Details page.
3. Select a department from the drop-down list.
4. **Optional:** Input the person name for search.
5. Select the attendance start date and end date that you want to search from.
6. **Optional:** Check the attendance status that you want to search.
7. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
8. Click **Search**.

   The detailed information of the attendance details displays below. You can view the attendance date, the person belonged shift, time period, start-work status, end-work status, check-in time, check-out time, late period, early leave period, attendance period, absence period, leave period, and overwork period.

9. **Optional:** After searching the result, perform one of the following operations.

   Report Generate the attendance report.

Export Export the results to the local PC.

Search Employees' Abnormal Attendance Data

You can search and get the statistics of the employee's abnormal attendance data, including No., name and department of the employees, abnormal type, start/end time and date of attendance.

Before You Start

- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to ***Manage Organization*** and ***Manage Person Information***
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Perform the following steps to search the employee's abnormal attendance data.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Abnormal Attendance** to enter the Abnormal Attendance page.
3. Select a department from the drop-down list.
4. **Optional:** Input the person name for search.
5. Select the attendance start date and end date that you want to search from.
6. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.

   The result displays below. You can view the employee No., the person name, the person belonged department, the abnormal type, the abnormal start time, the abnormal end time, and the abnormal date.
8. **Optional:** After searching the result, perform one of the following operations.

   Report Generate the attendance report.

   Export Export the results to the local PC.

Search Employees' Overtime Working Data

You can search and get the overtime status statistics of the selected employee in the specified time period. And you can check the detailed overtime information, including No., name and department of the employees, attendance date, overtime duration and overtime type.

Before You Start

- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to ***Manage Organization*** and ***Manage Person Information*** .
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Perform the following steps to search the overtime working data.

Steps

1. Enter the Time and Attendance module
2. Click **Attendance Statistics → Overtime Search** to enter the Overtime Search page.
3. Select a department from the drop-down list.
4. **Optional:** Input the person name for search.
5. Select the attendance start date and end date that you want to search from.
6. **Optional:** Click **Reset** to reset all search conditions and edit the search conditions again.
7. Click **Search**.

   The detailed information of the overtime work result displays below. You can view the employee No., the person name, the person belonged department, the overtime work's date, the overtime duration, and the overtime type.
8. **Optional:** After searching the result, perform one of the following operations.

   Report Generate the attendance report.

   Export Export the results to the local PC.

Check Employees' Card Swiping Logs

You can search and view the employees' card swiping logs when you want to check the employees' card swiping details.

Before You Start

- You should add organizations and persons in Access Control module and the persons has swiped card. For details, refer to ***Manage Organization*** and ***Manage Person Information*** .
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Perform the following steps to searching and the view card swiping log.

Steps

1. Enter the Time and attendance module.
2. Click **Attendance Statistics → Card Swiping Log** to enter the Card Swiping Log page.
3. Configure the search conditions, including the employee department, employee name, or attendance date.
4. **Optional:** Click **Reset** to reset all search conditions.
5. Click **Search**.

   The search result lists on this page.

   You can view the result details, including the employee No., employee name, department, time, authentication mode, and card No.
6. **Optional:** After searching and view the card swiping log, perform one of the following operations.

   Report Generate the attendance report.

   Export Export the results to the local PC.

Generate Attendance Report

After the attendance data is calculated, you can generate reports which show the attendance status of the employees in the specific time period.

Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start

Calculate the attendance data.

Note

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

Perform the following steps to generate the attendance report instantly.

Steps

1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Report** to enter the Report page.
3. In the Instant Report panel, select a report type from the drop-down list.
4. Select a person or department.
5. Set the time period during which the attendance data will be displayed in the report.
6. Click **Generate**.

Configure Scheduled Report

It supports 5 report types and you can pre-define the report content and it will send the report automatically to the email address you configured.

Perform this task if you want to configure a scheduled report.

Steps

Note

Set the email parameters before you want to enable auto-sending email functions. For details, refer to *Set Email Parameters*.

1. Enter the Time and Attendance module.
2. Click **Attendance Statistics → Report** to enter the Report page.
3. In the Scheduled Report panel, click **Add** to pre-define a report and set the report content.
4. Set the report content.

   Person

   Select the added person(s) and click > to add the person.
5. **Optional:** Set the schedule to send the report to the email address(es) automatically.
   1) Set the **Auto-Sending Email** switch to ON to enable this function.
   2) Set the effective period during which the client will send the report on the selected sending date(s).
   3) Select the date(s) on which the client will send the report.
   4) Set the time at which the client will send the report.

      Example

      If you set the effective period as ***2018/3/10 to 2018/4/10***, select ***Friday*** as the sending date, and set the sending time as ***20:00:00***, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.

      Note

      Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .
   5) Input the receiver email address(es).

Note

You can click + to add a new email address. Up to 5 email addresses are allowed.

6. Click **Save**.
7. **Optional:** After adding the scheduled report, you can do one or more of the followings:

Modify Report	Select one added report and click **Modify** to edit its settings.
Delete Report	Select one added report and click **Remove** to delete it.
Generate Report	Select one added report and click **Generate** to generate the report instantly and you can view the report details.

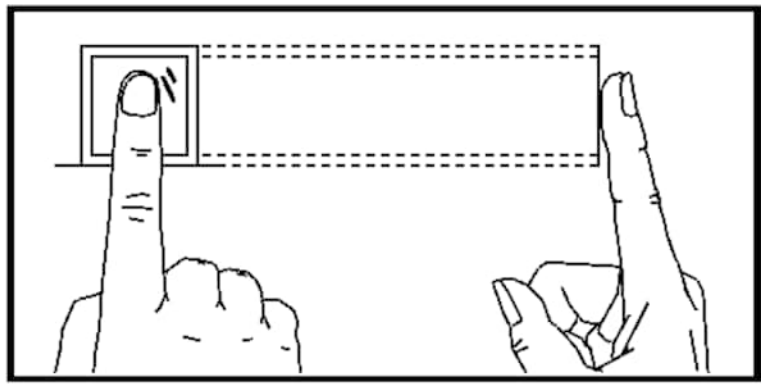
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

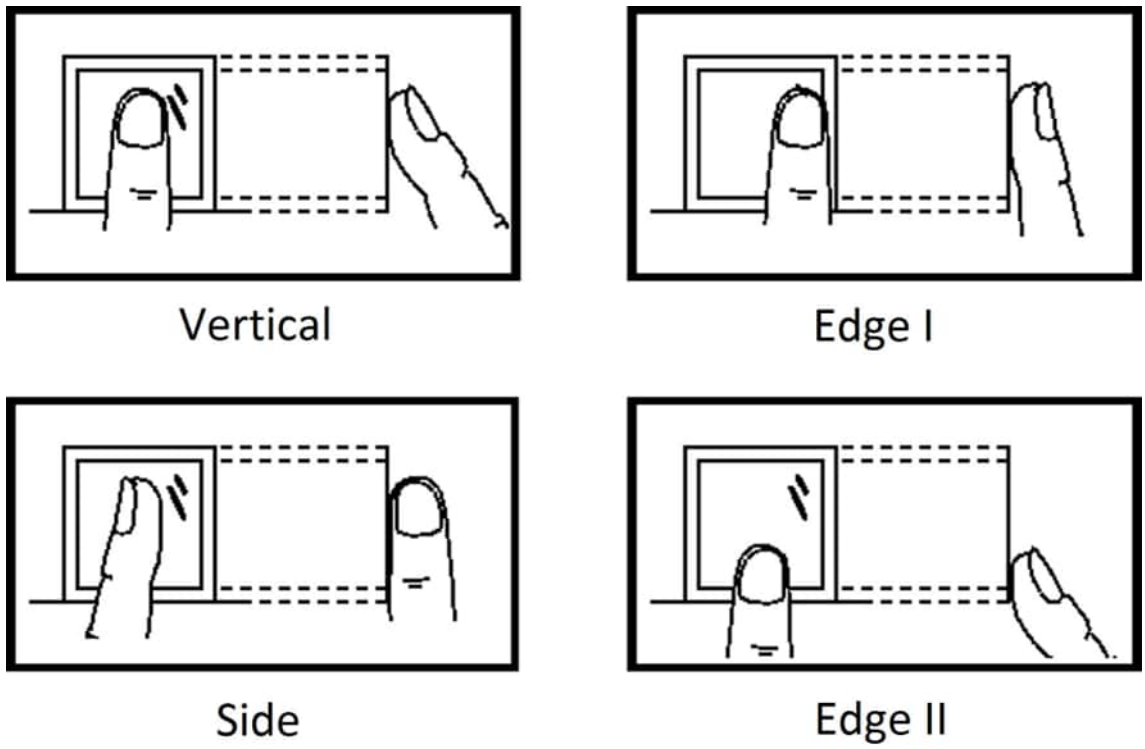
The figure displayed below is the correct way to scan your finger:



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

Incorrect Scanning

The figures of scanning fingerprint displayed below are incorrect:



Environment

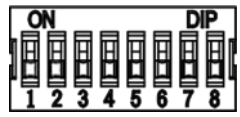
The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

Others

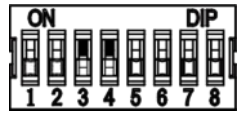
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.
If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix B. DIP Switch Description

No.1 to No 8 is from the low bit to the high bit.



When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off. If you set the DIP switch like the figure displayed below, its binary value is 00001100, and its decimal value is 12.



Appendix C. Custom Wiegand Rule Descriptions

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

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

Wiegand Data

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.

See Far, Go Further