DS-K281X Series Access Controller

User Manual

Legal Information

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.

Available Model

Product Name	Model
Access Controller	DS-K2811
	DS-K2812
	DS-K2814

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

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:

- 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:

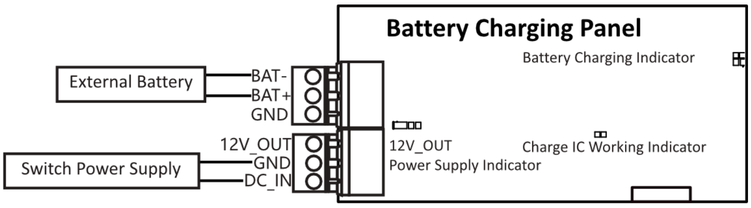
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification 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

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.
- It is recommended to choose a 12 V 7 AH lead-acid battery that meets the IEC 60896 standard. The battery wiring method is shown in the following figure.



Chapter 2 Product Description

- 32-bit high-speed processor
- Supports TCP/IP communication. 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 10,000 cards and 50,000 card presenting records
- Supports multi-door interlock function, inner-device anti-passback function, multiple authentications function, open door with first card function, super password function, M1 card encryption, online upgrade function and remote control of the doors
- IP address conflict detection
- 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
- Various indicators to show different status
- Supports record storage function when the device is offline and insufficient storage space storage alarm function
- Data can be permanently saved after the access controller is powered off
- Supports I/O linkage and event linkage

Chapter 3 Main Board Description

3.1 Single-Door Access Controller Main Board Description

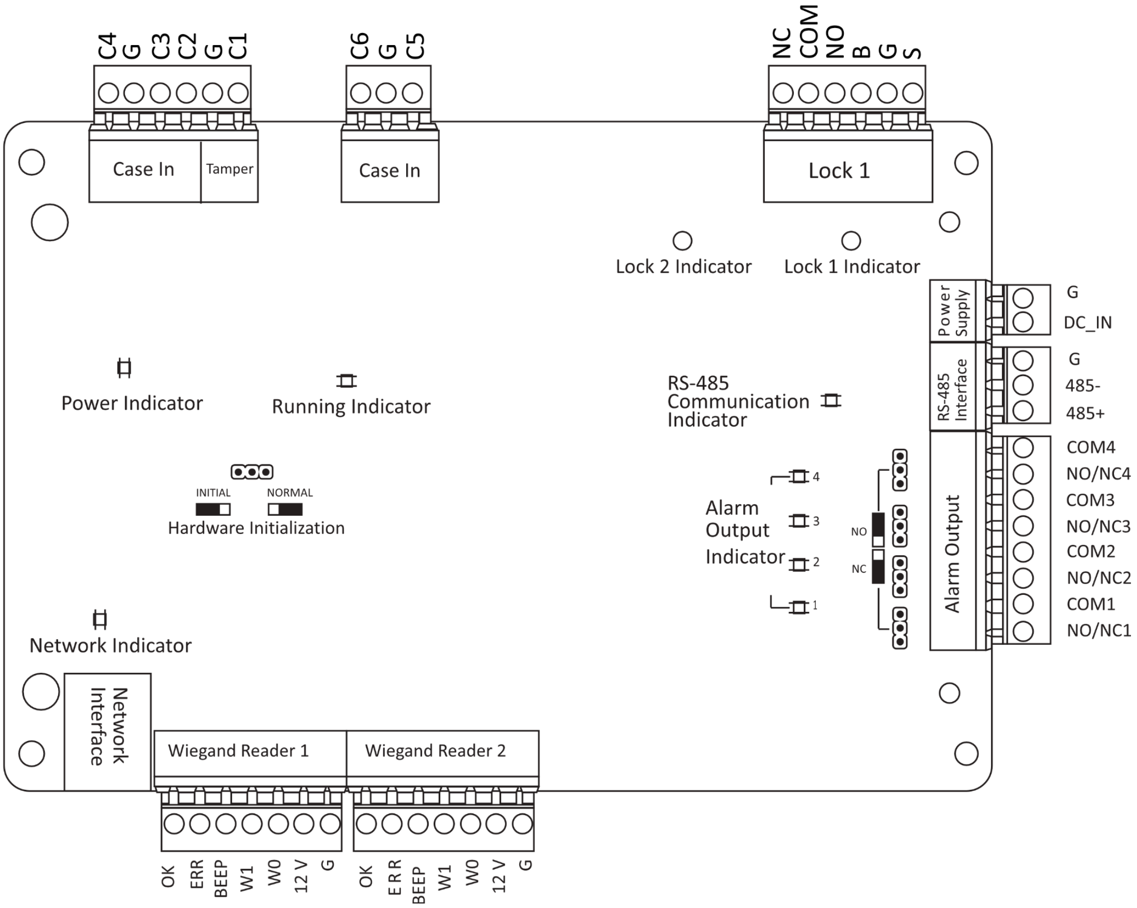


Figure 3-1 Single-Door Access Controller Main Board

3.2 Two-Door Access Controller Main Board Description

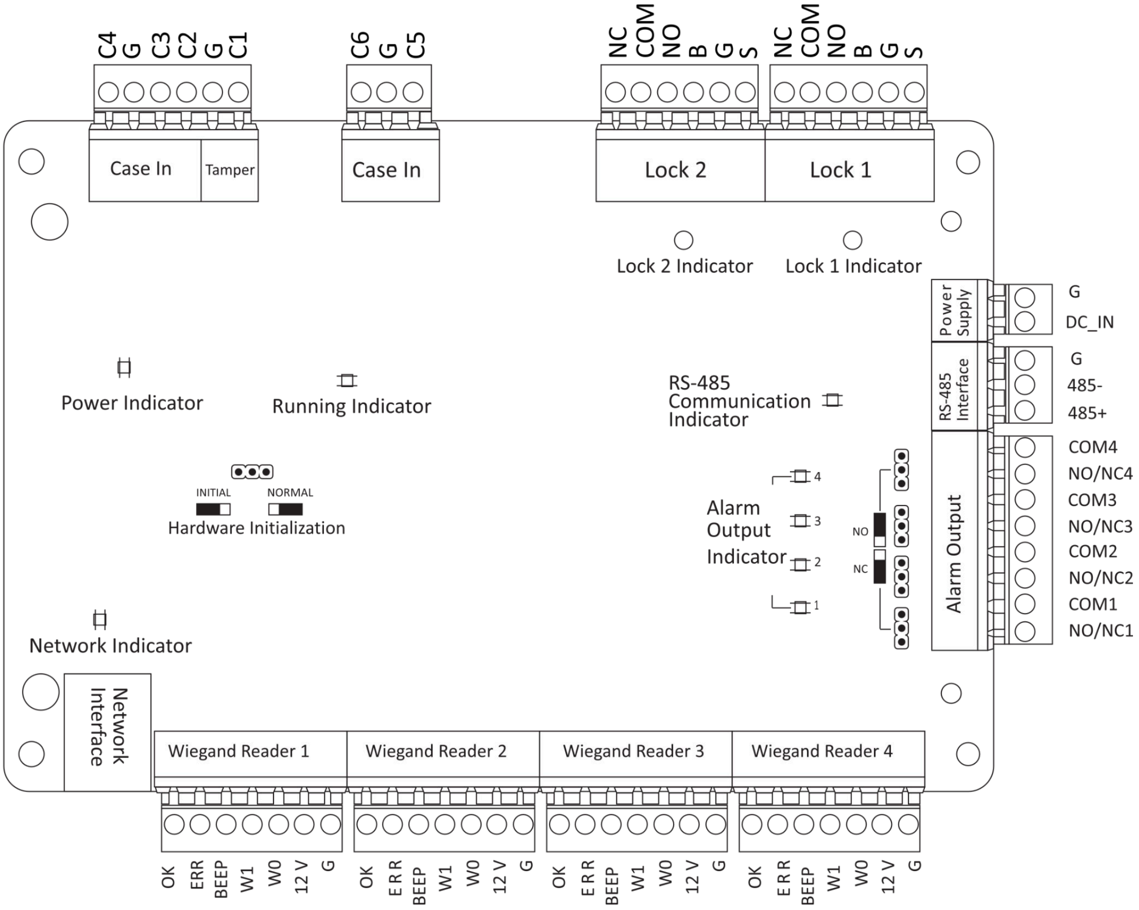


Figure 3-2 Two-Door Access Controller Main Board

3.2.1 Four-Door Access Controller Main Board Description

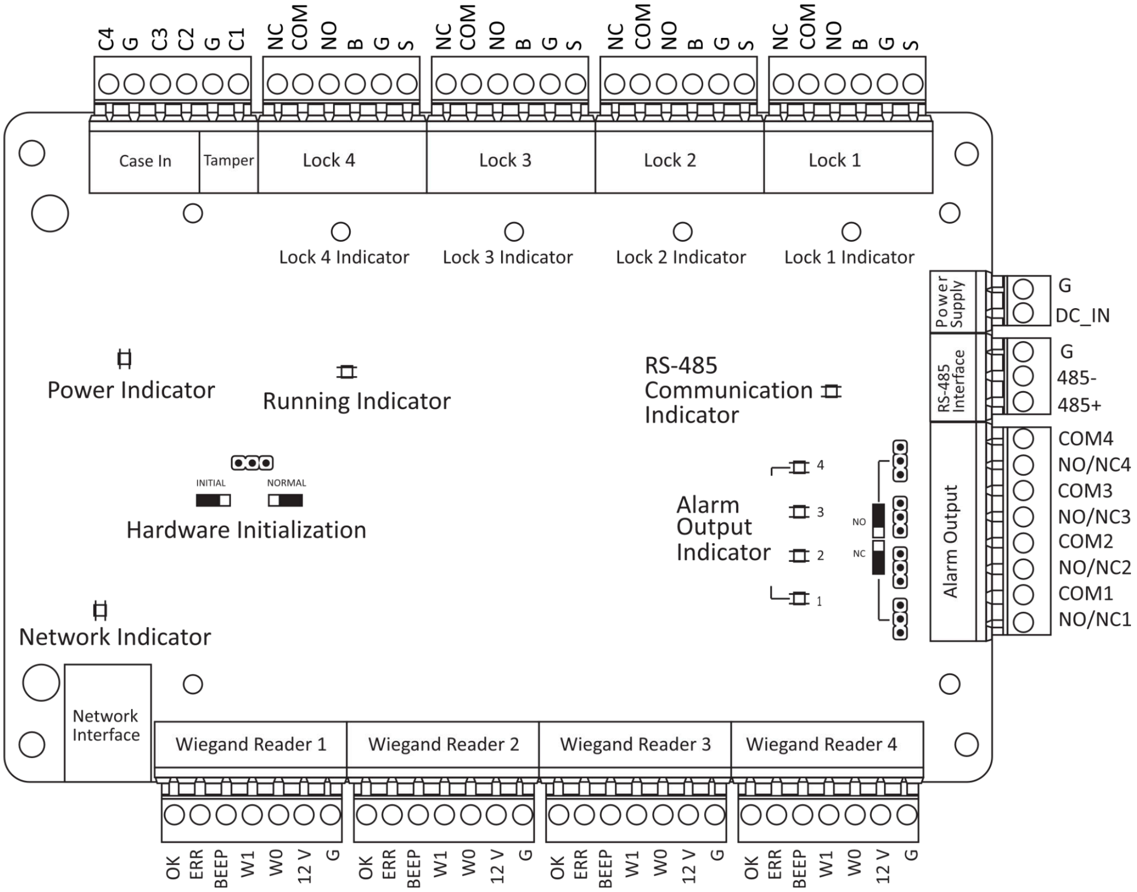


Figure 3-3 Four-Door Access Controller Main Board

3.3 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.

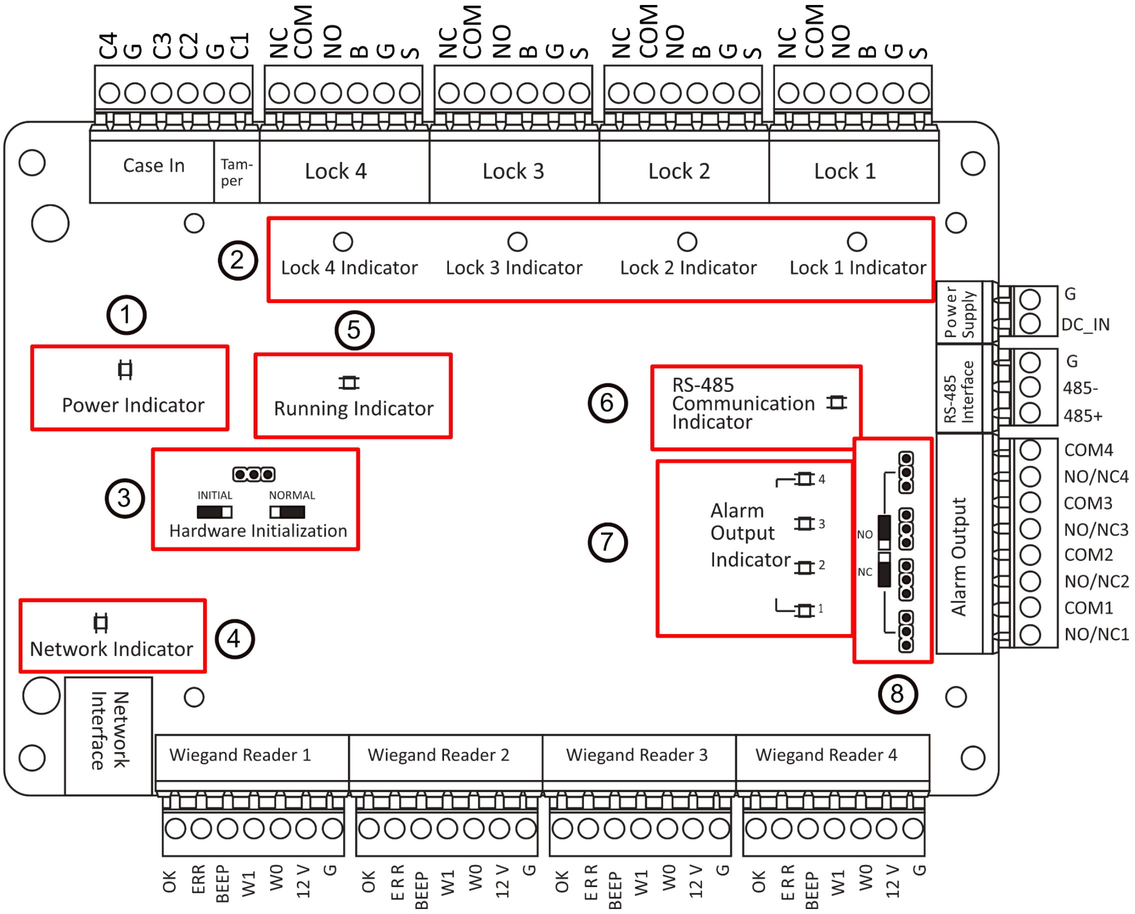


Figure 3-4 Four-Door Access Controller Component Diagram

Table 3-1 Four-Door Access Controller Component Description

No.	Component Description
1	Power Indicator
2	Lock Indicator
3	Hardware Initialization and Normal Working Choice
4	Network Indicator
5	Running Indicator
6	RS-485 Communication Indicator
7	Alarm Output Indicator
8	Door Relay Output Status (NC/NO) Choice

3.4 Battery Charging Board

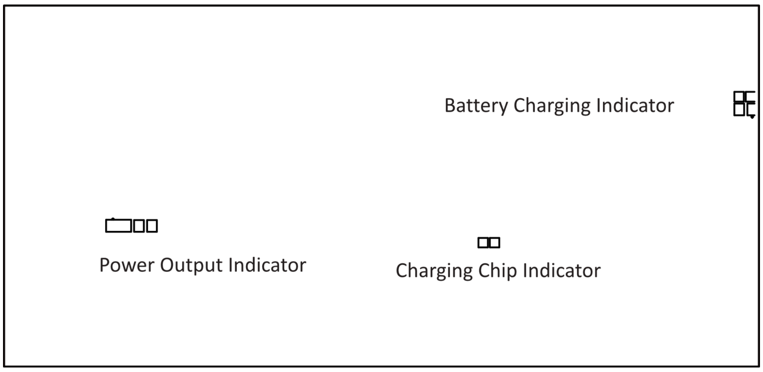


Figure 3-5 Battery Charging Board

Note

The battery charging boards are only for devices that support battery.

Chapter 4 Terminal Description

4.1 Single-Door Access Controller Terminal Description

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

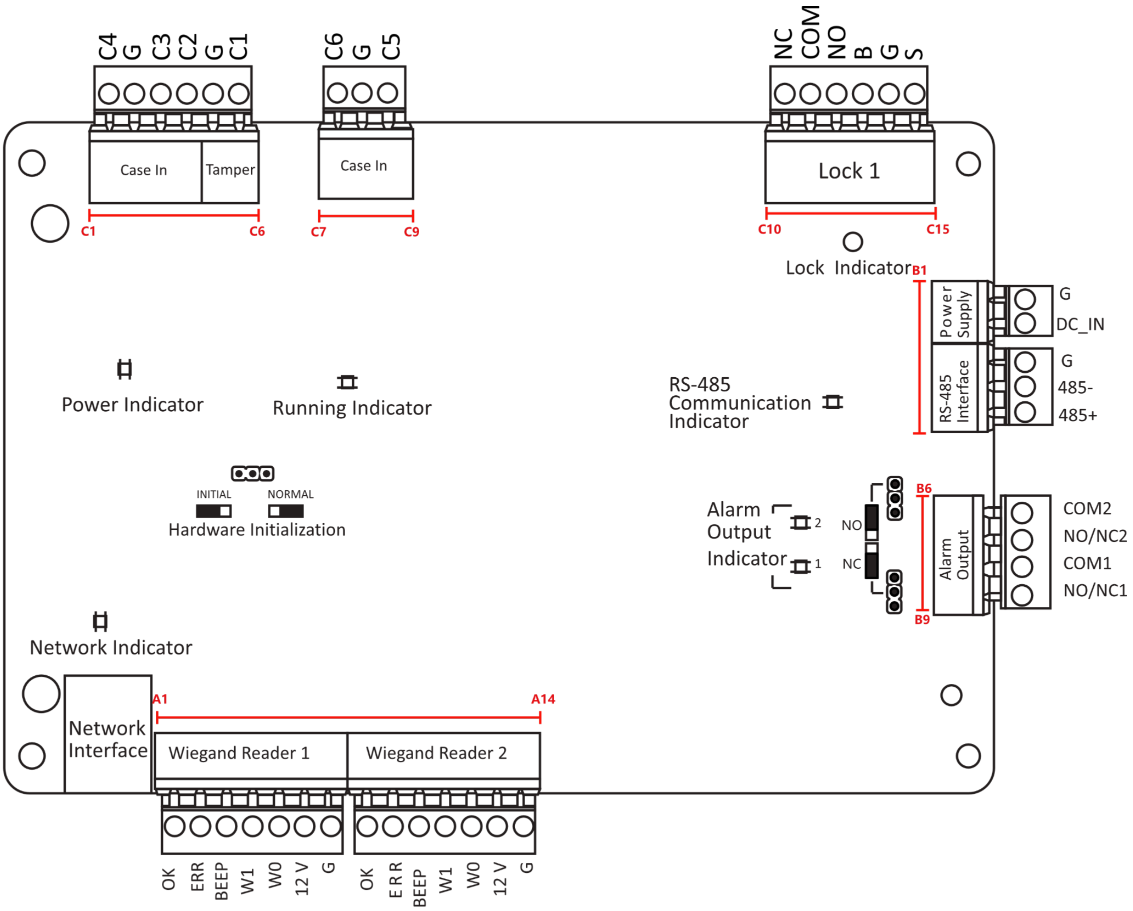


Figure 4-1 Single-Door Access Controller Main Board

Table 4-1 Single-Door Access Controller Terminal Description

No.	Four-Door Access Controller		
A1~A28	Wiegand Reader 1~4	OK	Indicator of Card Reader Control Output (Valid Card Output)
		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
		BEEP	Card Reader Buzzer Control Output
		W1	Wiegand Card Reader Data Input Data1
		W0	Wiegand Card Reader Data Input Data0
		12 V	Wiegand Card Reader Data Input Data0
		G	Grounding
B1	Power Supply	G	Grounding
B2		DC_IN	Power In
B3	RS-485 Interface	G	Grounding
B4		485-	Card Reader 485-
B5		485+	Card Reader 485+
B6~B13	Alarm Output	COM4	Alarm Relay 4Output (Dry Contact)
		NO/NC4	
		COM3	Alarm Relay 3 Output (Dry Contact)
		NO/NC3	
		COM2	Alarm Relay 2 Output (Dry Contact)
		NO/NC2	
		COM1	Alarm Relay 1 Output (Dry Contact)
		NO/NC1	
C1	Event In	C4	Event In 4
C2		G	Grounding

No.	Four-Door Access Controller		
C3		C3	Event In 3
C4	Tamper	C2	Reserved
C5		G	Grounding
C6		C1	Tamper
C7	Event In	C6	Event In 6
C8		G	Grounding
C9		C5	Event In 5
C10~C15	Lock 1	NC	Lock Relay Output (Dry Contact)
		COM	
		NO	
		B	Exit Button In
		G	Grounding
		S	Door Contact

Note

- 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 by default.

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.

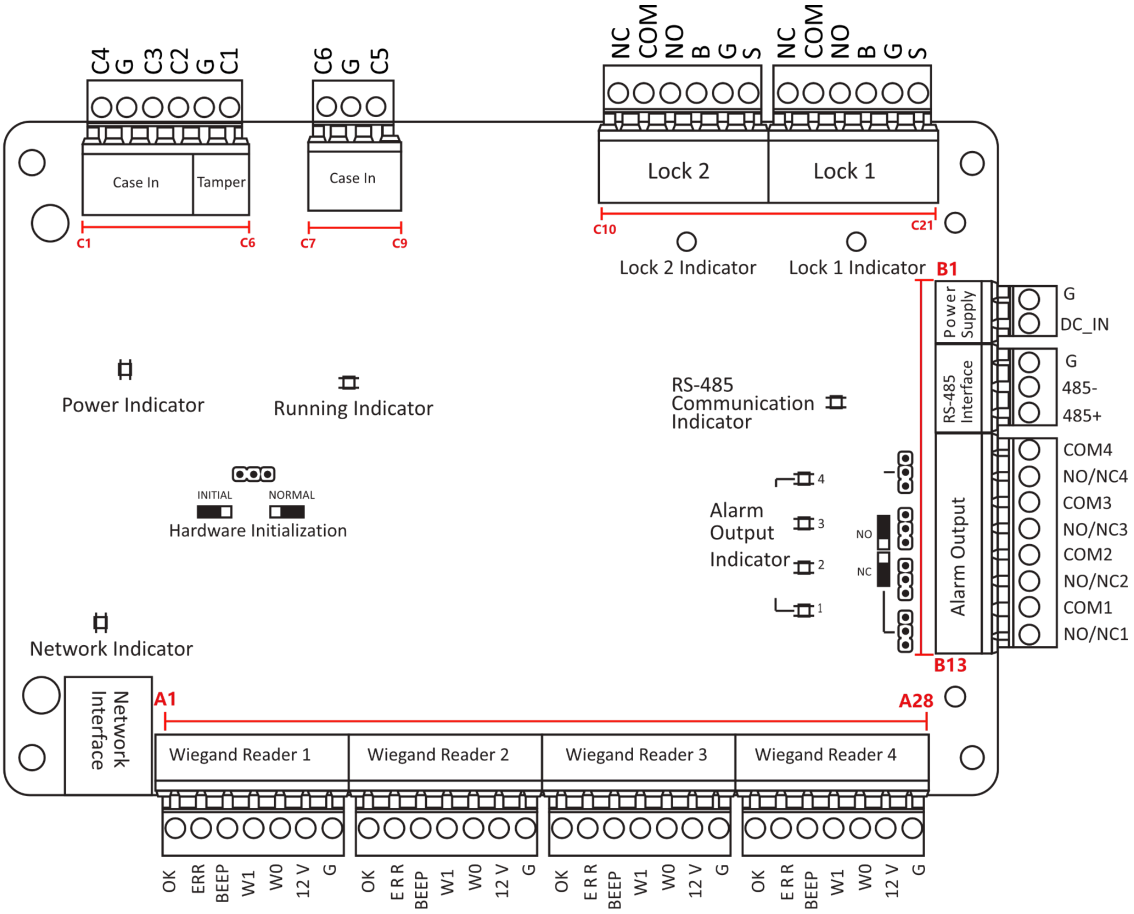


Figure 4-2 Two-Door Access Controller Main Board

Table 4-2 Two-Door Access Controller Terminal Description

No.	Four-Door Access Controller		
A1~A28	Wiegand Reader 1~4	OK	Indicator of Card Reader Control Output (Valid Card Output)
		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
		BEEP	Card Reader Buzzer Control Output
		W1	Wiegand Card Reader Data Input Data1

No.	Four-Door Access Controller		
		W0	Wiegand Card Reader Data Input Data0
		12 V	Wiegand Card Reader Data Input Data0
		G	Grounding
B1	Power Supply	G	Grounding
B2		DC_IN	Power In
B3	RS-485 Interface	G	Grounding
B4		485-	Card Reader 485-
B5		485+	Card Reader 485+
B6~B13	Alarm Output	COM4	Alarm Relay 4Output (Dry Contact)
		NO/NC4	
		COM3	Alarm Relay 3 Output (Dry Contact)
		NO/NC3	
		COM2	Alarm Relay 2 Output (Dry Contact)
		NO/NC2	
		COM1	Alarm Relay 1 Output (Dry Contact)
		NO/NC1	
C1	Event In	C4	Event In 4
C2		G	Grounding
C3		C3	Event In 3
C4	Tamper	C2	Reserved
C5		G	Grounding
C6		C1	Tamper
C7	Event In	C6	Event In 6
C8		G	Grounding
C9		C5	Event In 5
C10~C21	Lock 1~Lock 2	NC	Lock Relay Output (Dry Contact)
		COM	

No.	Four-Door Access Controller		
		NO	
		B	Exit Button In
		G	Grounding
		S	Door Contact

Note

- 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 by default.

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.

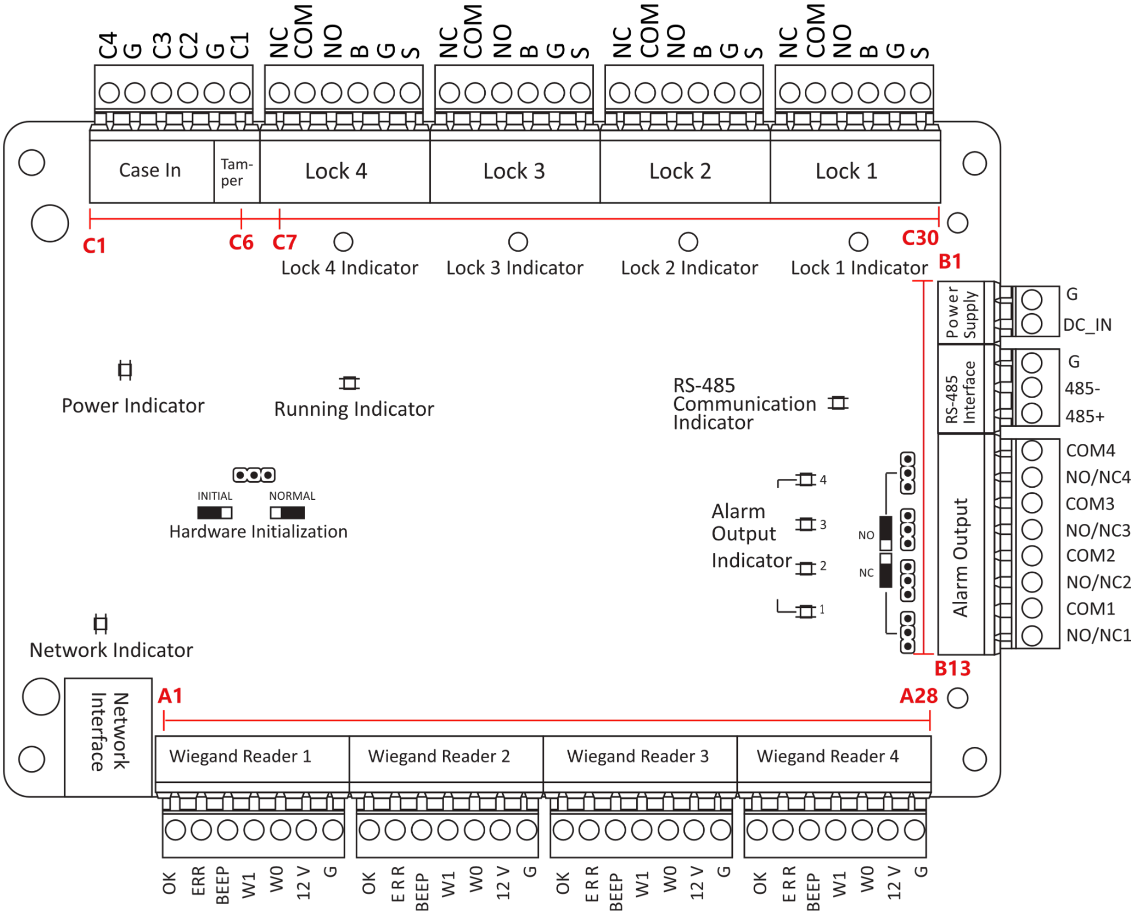


Figure 4-3 Four-Door Access Controller Main Board

Table 4-3 Four-Door Access Controller Terminal Description

No.	Four-Door Access Controller		
A1~A28	Wiegand Reader 1~4	OK	Indicator of Card Reader Control Output (Valid Card Output)
		ERR	Indicator of Card Reader Control Output (Invalid Card Output)
		BEEP	Card Reader Buzzer Control Output
		W1	Wiegand Card Reader Data Input Data1

No.	Four-Door Access Controller		
		W0	Wiegand Card Reader Data Input Data0
		12 V	Wiegand Card Reader Data Input Data0
		G	Grounding
B1	Power Supply	G	Grounding
B2		DC_IN	Power In
B3	RS-485 Interface	G	Grounding
B4		485-	Card Reader 485-
B5		485+	Card Reader 485+
B6~B13	Alarm Output	COM4	Alarm Relay 4Output (Dry Contact)
		NO/NC4	
		COM3	Alarm Relay 3 Output (Dry Contact)
		NO/NC3	
		COM2	Alarm Relay 2 Output (Dry Contact)
		NO/NC2	
		COM1	Alarm Relay 1 Output (Dry Contact)
		NO/NC1	
C1	Event In	C4	Event In 4
C2		G	Grounding
C3		C3	Event In 3
C4	Tamper	C2	Reserved
C5		G	Grounding
C6		C1	Tamper
C7~C30	Lock 1~4	NC	Lock Relay Output (Dry Contact)
		COM	
		NO	
		B	Exit Button In

No.	Four-Door Access Controller		
		G	Grounding
		S	Door Contact

Note

- RS-485 card 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
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 by default.

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 Installation

5.1 Wall Mounting

The access controller can be installed on the wall.

Steps

1. **Note**

   In the process of installing, after routing the cable through the knockout, the knockout should be sealed with flame-retardant clay or a plug that achieves the rating of V-1.

   Open and take off the case door.

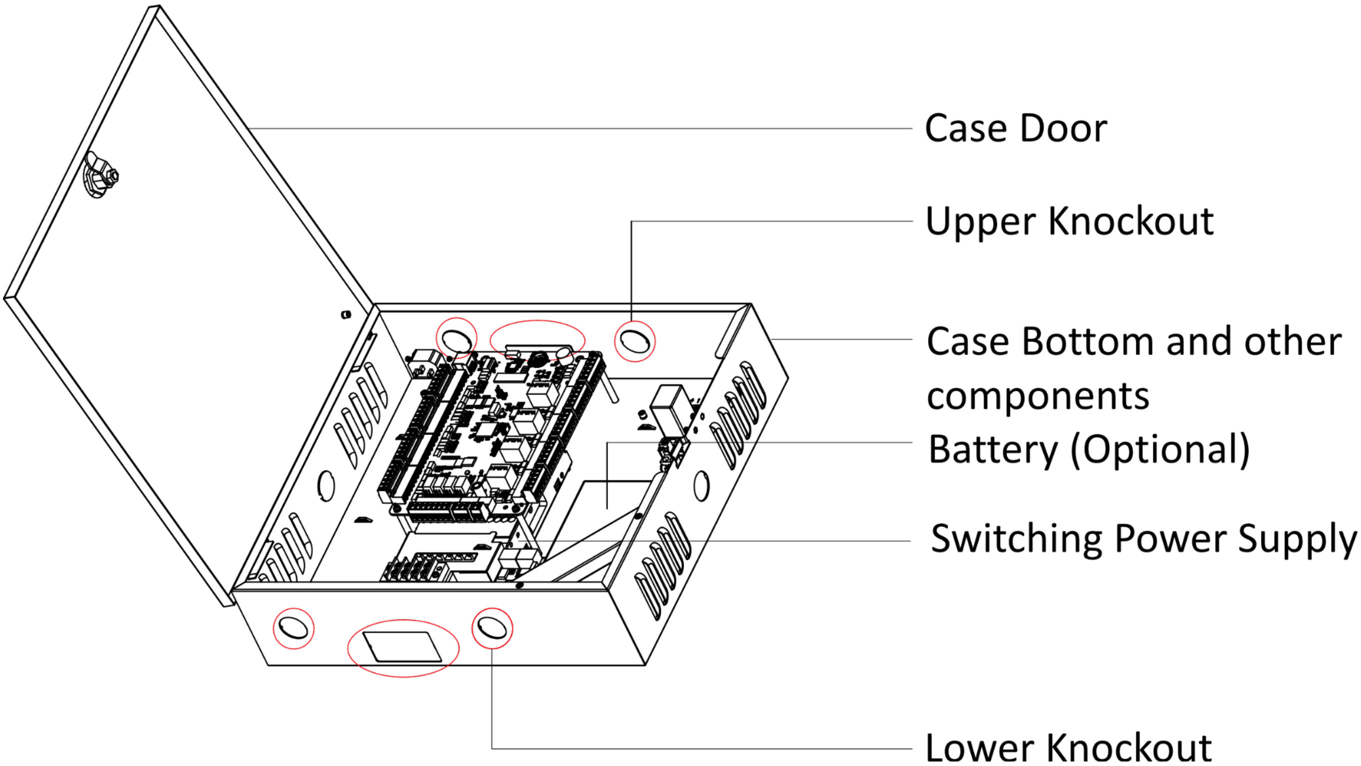


Figure 5-1 Open the case door

2. Secure the device on the wall with expansion screws.

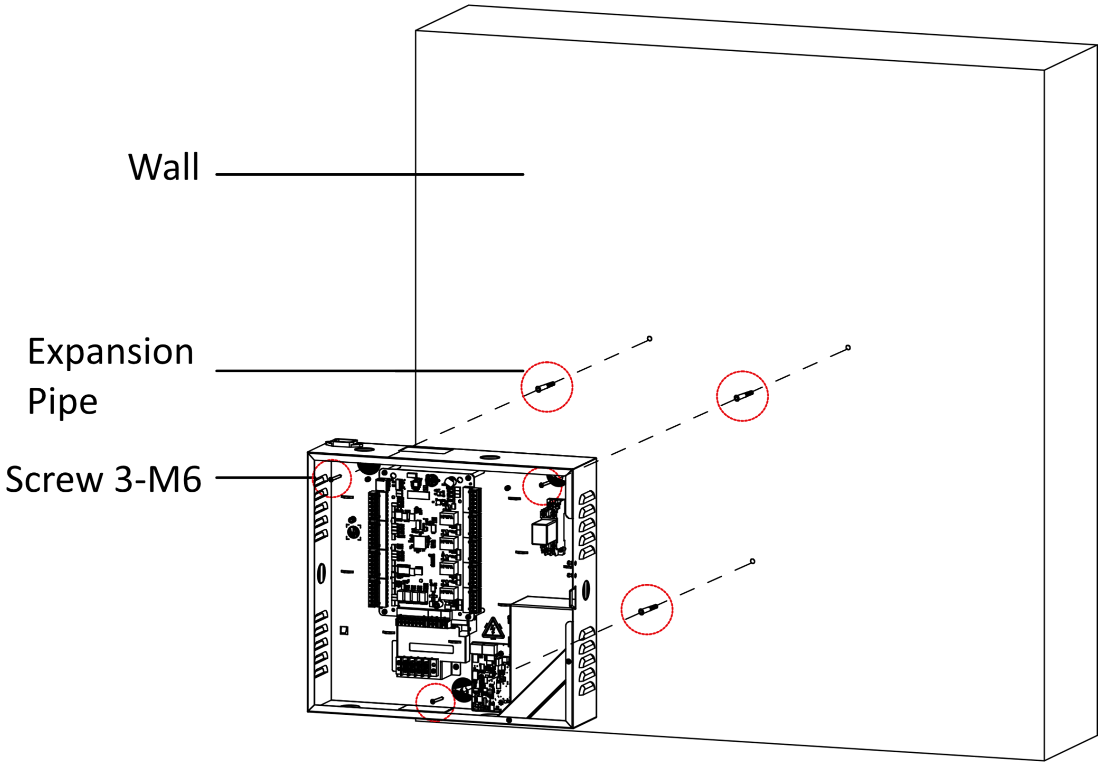


Figure 5-2 Secure the device

3. After wiring, recover the case door and bottom.

Note

When wiring, you can open knockouts to your actual needs.

Chapter 6 Terminal Wiring

Terminal Wiring Description of the Access Controller.

6.1 Main Board Wiring

You can view the main board wiring diagram.

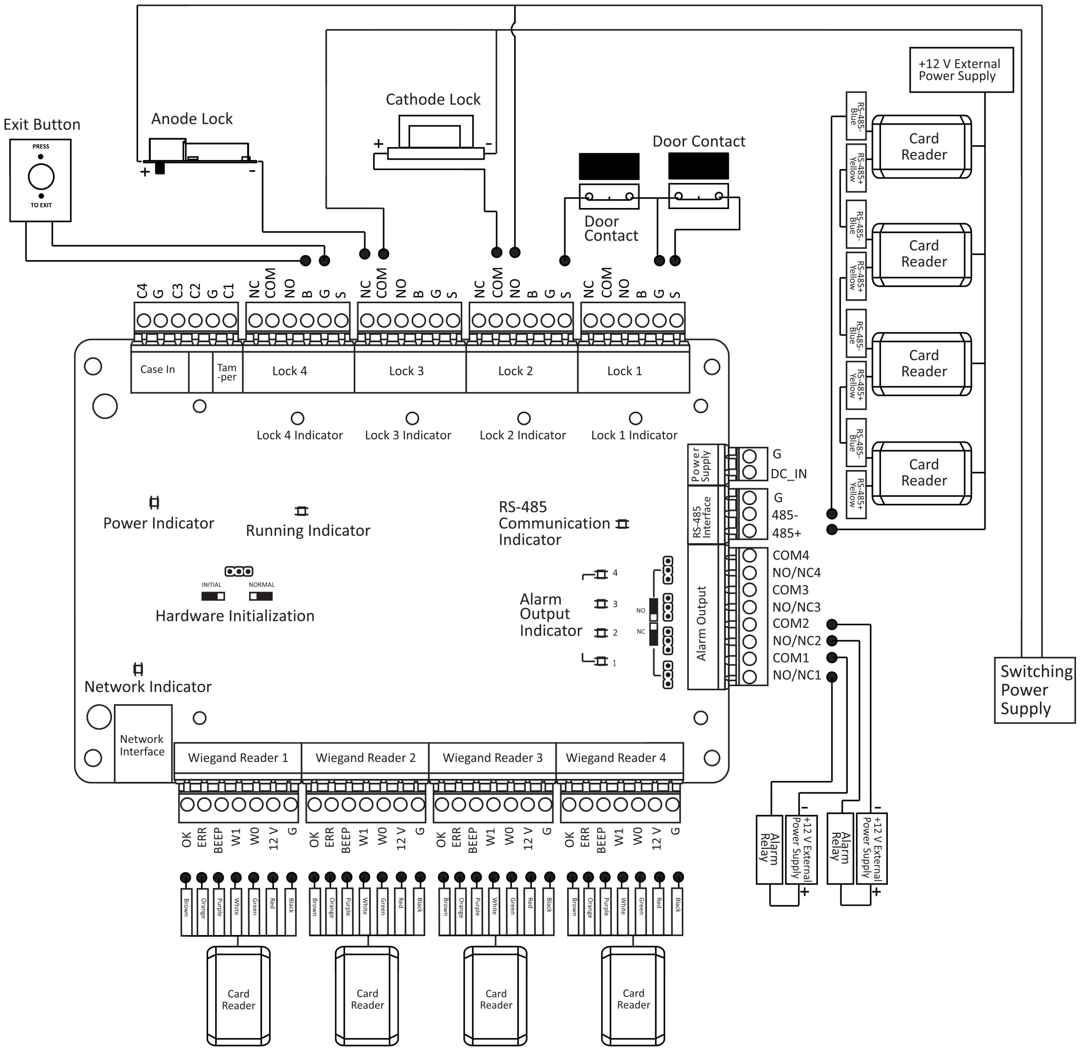


Figure 6-1 Access Controller Main Board Wiring

6.2 Wiegand Card Reader Wiring

You can view the Wiegand card reader wiring diagram.

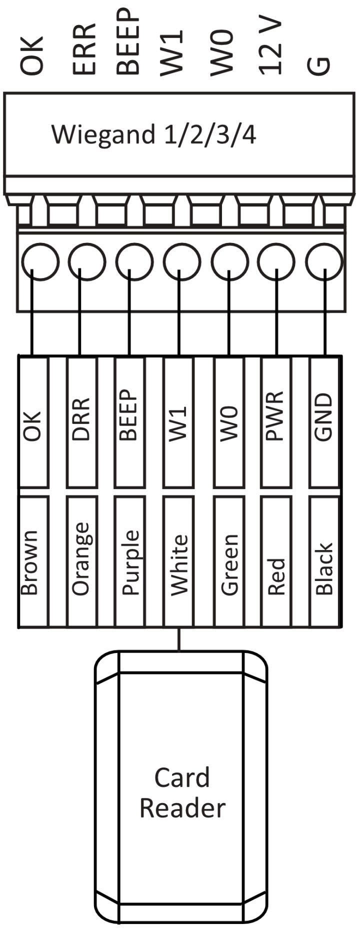


Figure 6-2 Wiegand Card Reader Wiring Diagram

Note

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

6.3 RS-485 Card Reader Wiring

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

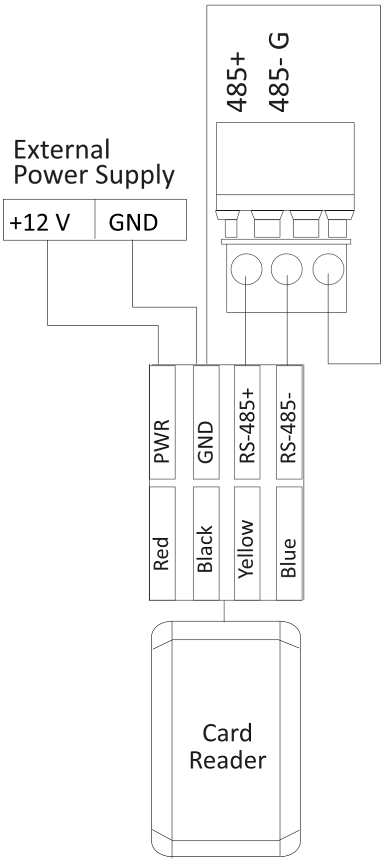


Figure 6-3 RS-485 Card Reader Wiring Diagram

Note

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

6.4 Cathode Lock Wiring

You can view the cathode lock wiring diagram.

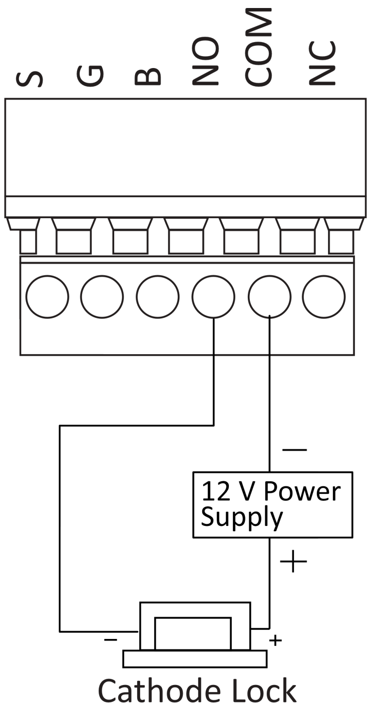


Figure 6-4 Wiring Diagram of Cathode Lock

6.5 Anode Lock Wiring

You can view the anode lock wiring diagram.

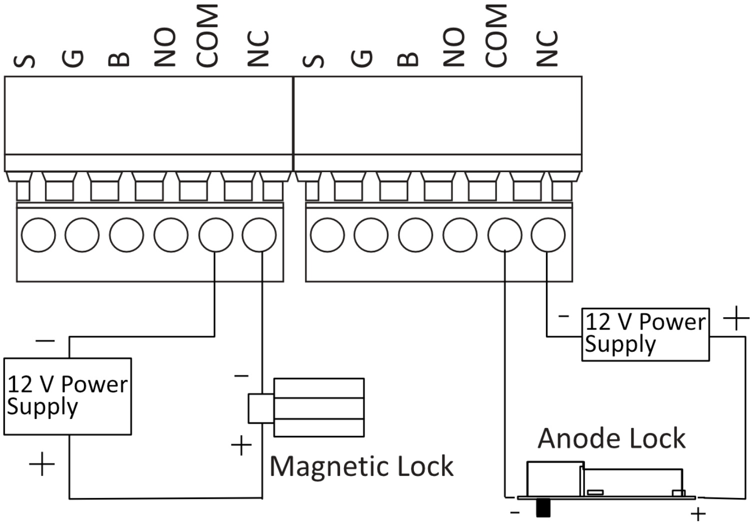


Figure 6-5 Wiring Diagram of Anode Lock

6.6 Alarm Output Wiring

You can view the Alarm Output Wiring diagram.

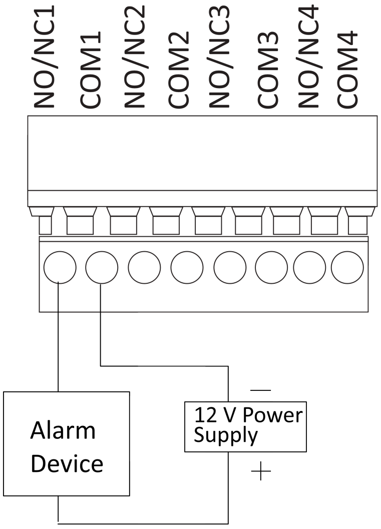


Figure 6-6 Alarm Output Wiring

6.7 Exit Button Wiring

You can view the exit button wiring diagram

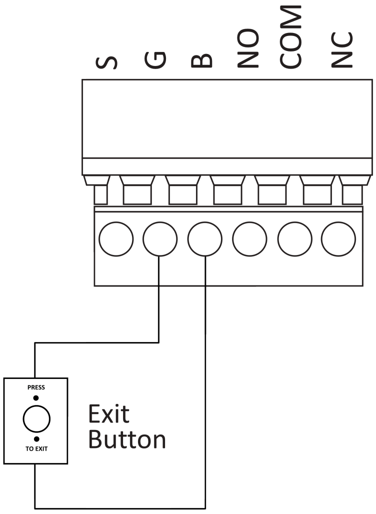


Figure 6-7 Exit Button Wiring

6.8 Door Contact Wiring

You can view the door contact wiring diagram.

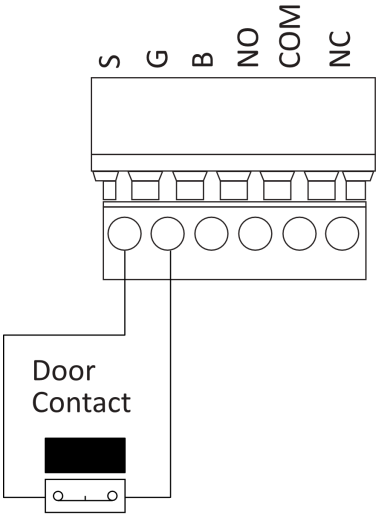


Figure 6-8 Door Contact Wiring

6.9 Power Supply Wiring

You can view the power supply wiring diagram.

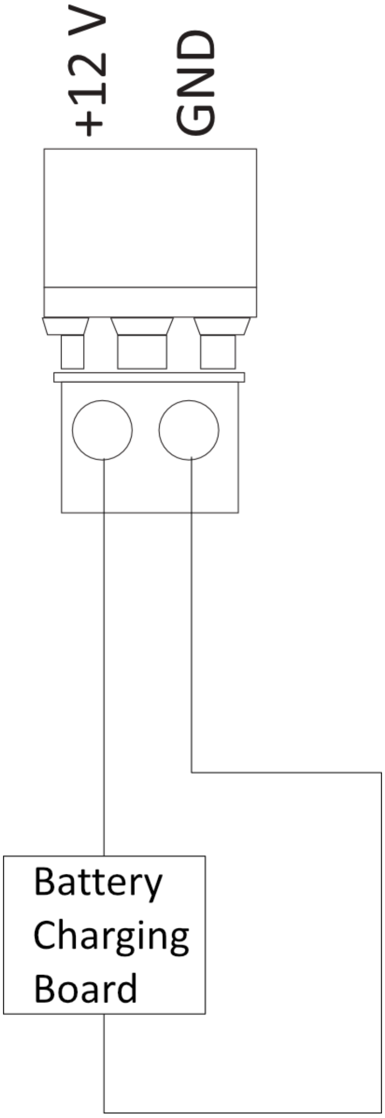


Figure 6-9 Power Supply Wiring

Chapter 7 Settings

7.1 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.

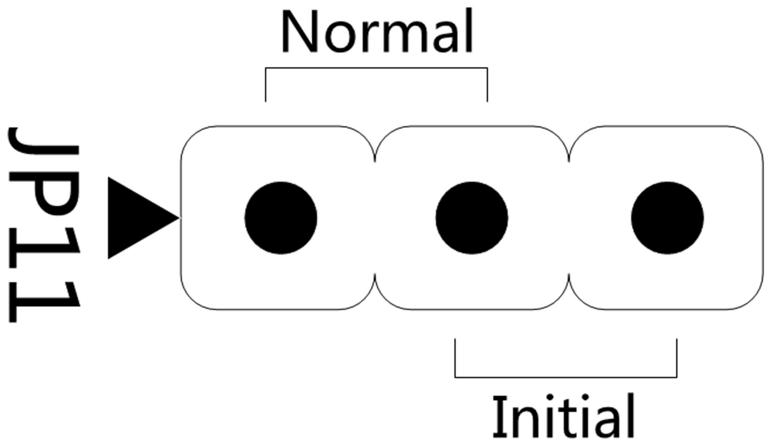


Figure 7-1 Initialization Jumper

Note

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

7.2 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.

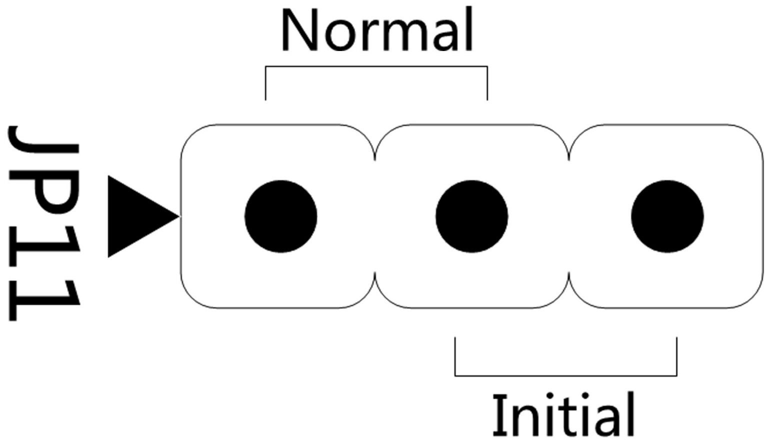


Figure 7-2 Initialization Jumper

Note

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

7.3 Relay Output NO/NC Settings

7.3.1 Lock Relay Output Settings

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

Lock Relay NO Status

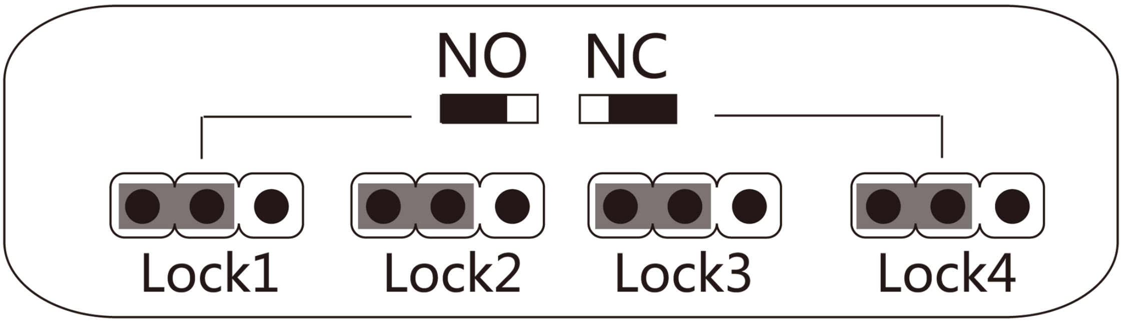


Figure 7-3 NO Status

Lock Relay NC Status

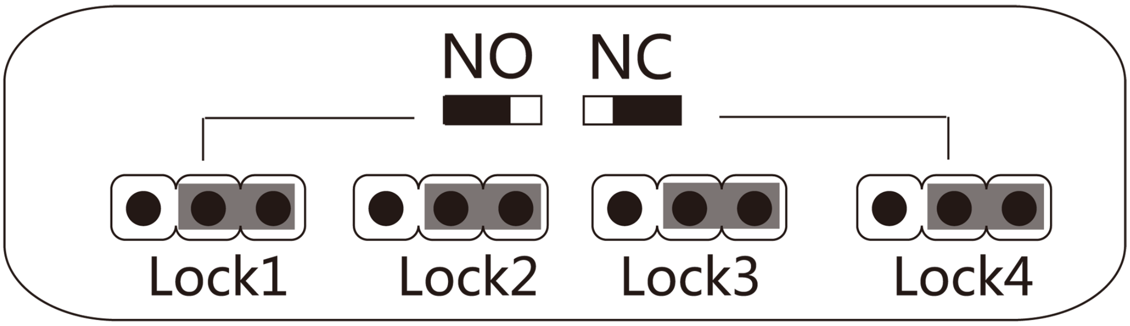


Figure 7-4 NC Status

7.3.2 Alarm Relay Output Settings

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

Alarm Relay Output NO Status

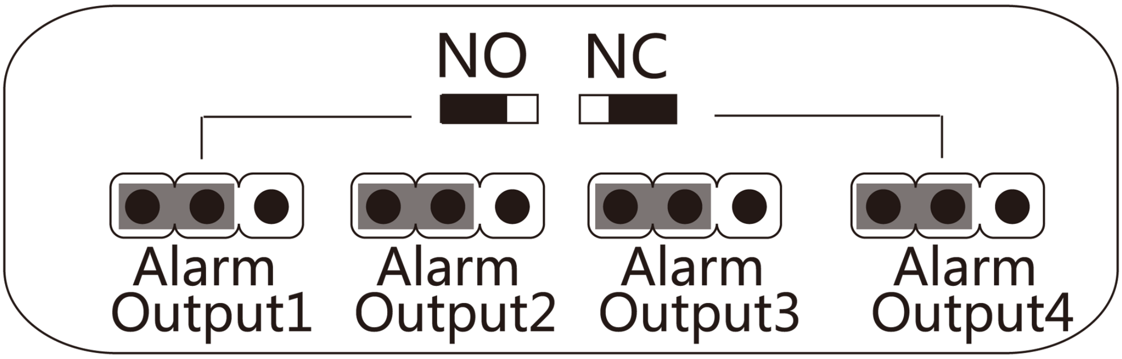


Figure 7-5 NO Status

Alarm Relay Output NC Status

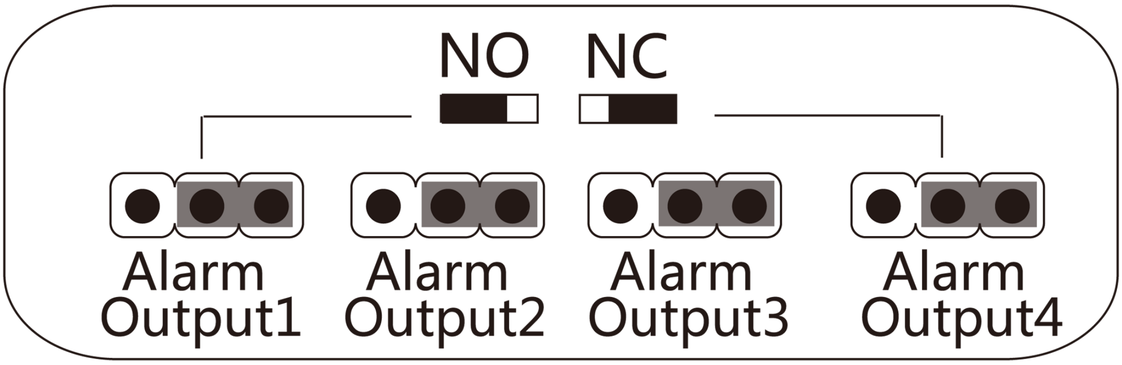


Figure 7-6 NC Status

Chapter 8 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

8.1 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

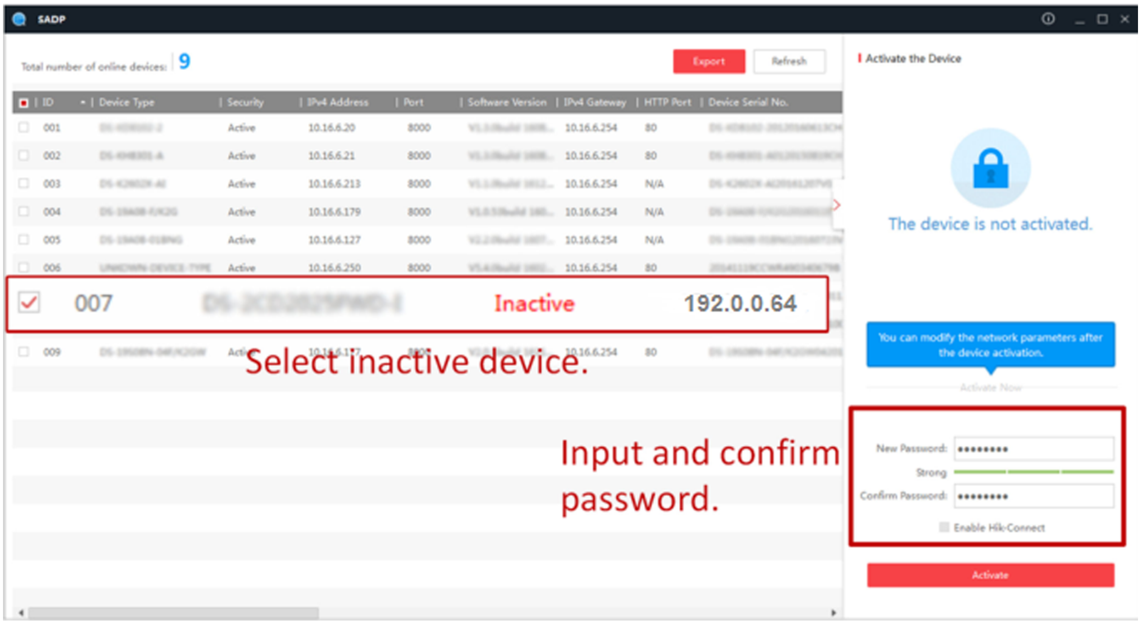
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

   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.

   Note

   Characters containing admin and nimda are not supported to be set as activation password.
4. Click **Activate** to start activation.



Total number of online devices: 9

☐ ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐ 001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
☐ 002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
☐ 003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	DS-2CD2025FWD-I	Inactive	192.0.0.64					
☐ 009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

Activate

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.

8.2 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.

Note

Characters containing admin and nimda are not supported to be set as activation password.

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

Chapter 9 Client Software Configuration

You can call the hotline to get the iVMS-4200 client software installation package.

9.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

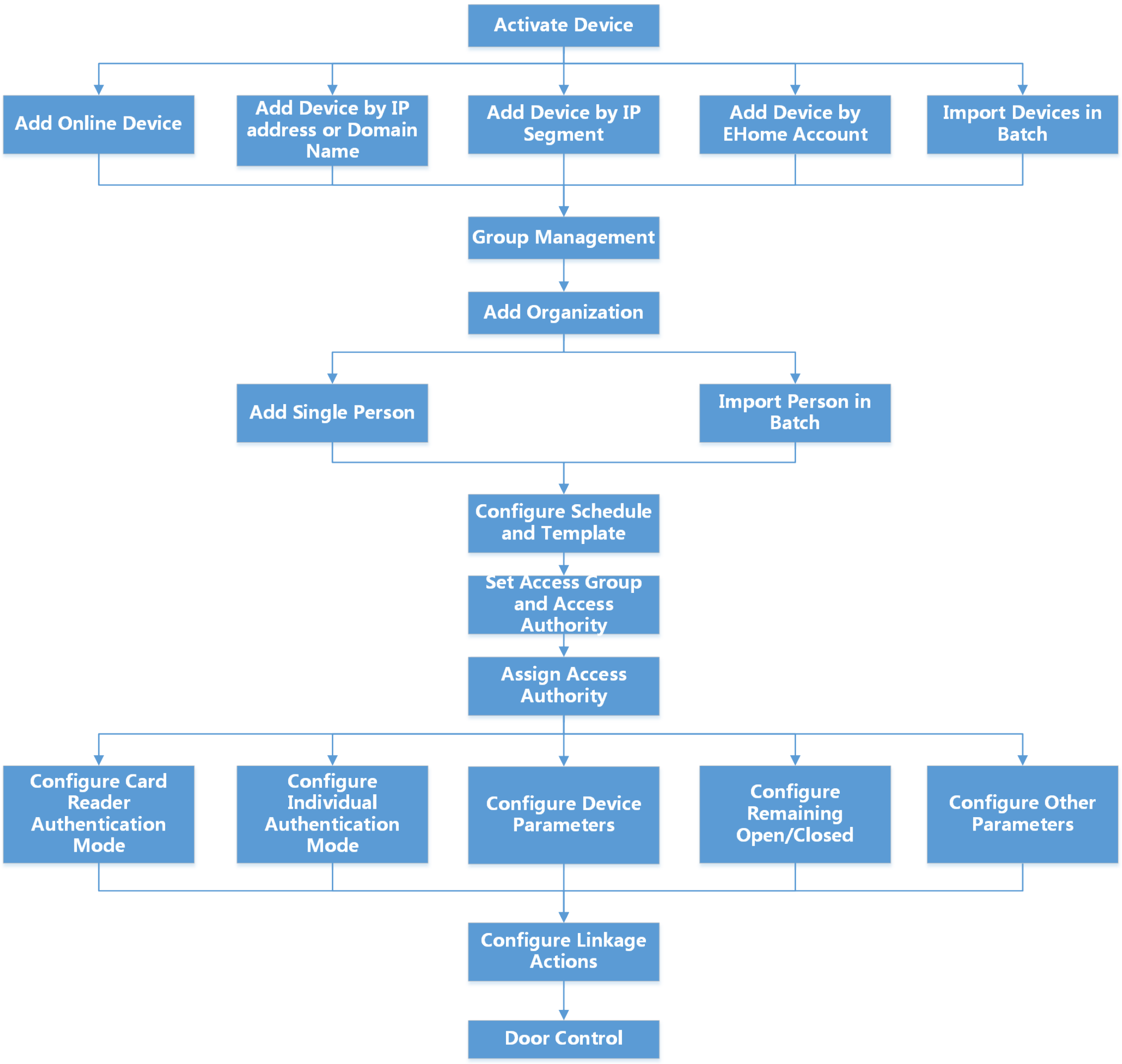

Activate Device
Add Online Device
Add Device by IP address or Domain Name
Add Device by IP Segment
Add Device by EHome Account
Import Devices in Batch
Group Management
Add Organization
Add Single Person
Import Person in Batch
Configure Schedule and Template
Set Access Group and Access Authority
Assign Access Authority
Configure Card Reader Authentication Mode
Configure Individual Authentication Mode
Configure Device Parameters
Configure Remaining Open/Closed
Configure Other Parameters
Configure Linkage Actions
Door Control

Figure 9-1 Flow Diagram of Configuration on Client Software

9.2 Device Management

The client supports managing access control devices and video intercom devices.

Example
You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

9.2.1 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 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.

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.

9.2.2 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.

   All the online devices sharing the same subnet will be displayed in the list.
3. Select the device from the list and click 🔑 on the Operation column.
4. Reset the device password.
   - Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.

     Note

     For the following operations for resetting the password, contact our technical support.

⚠ **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.

9.2.3 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device parameters, remote configuration, viewing device status, etc.

Table 9-1 Manage Added Devices

Edit Device	Click ✎ to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click **Delete** to delete the selected devices.
Remote Configuration	On the device list page, click ⚙ in the Operation column to perform remote configuration for a device. The ⚙ is in the rightmost column of the Device page. For details, refer to the user manual of device.
View Device Status	Click ▤ to view device status, including door No., door status, etc. ℹ **Note** For different devices, you will view different information about device status.
View Online User	Click 👤 to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click ↻ to refresh and get the latest device information.
Upgrade Device	View device status in the Firmware Upgrade column, check one or more upgradable devices, and click **Upgrade Device Firmware** to upgrade the selected devices. For details, refer to .

Get Events from Device	Check one device, and click **Get Events from Device** to synchronize events. For details, refer to .
Export Device	Click **Export Device**, set the saving path and select device type to export the device details (such as device type, IP address, and port No.) to your local PC. **Note** The super user can enable **Password Protection** and enter the password, then the exported file of device information will be encrypted.

9.3 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

Example
For example, on the 1st floor, there mounted 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can control door status, and do some other operations of the devices after managing the resources by groups.

9.3.1 Add Group

You can add group to organize the added device for convenient management.

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Create a group.
   - Click **Add Group** and enter a group name as you want.
   - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.

   Note

   The resources (such as alarm inputs/outputs, access points, etc.) of this device will be imported to the group by default.

9.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, access points, etc.) to the added group in a batch.

Before You Start

Add a group for managing devices. Refer to ***Add Group*** .

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.

   Note

   You can click ⊞ or ☰ to switch the resource display mode to thumbnail view or to list view.
6. Click **Import** to import the selected resources to the group.

9.4 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

9.4.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a surbodinate organization for the added one.

Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.

   Note

   Up to 10 levels of organizations can be added.
4. **Optional:** Perform the following operation(s).

   Edit Organization Hover the mouse on an added organization and click ✎ to edit its name.

Delete Organization

Hover the mouse on an added organization and click ☒ 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.

Show Persons in Sub Organization

Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

9.4.2 Import and Export Person Identify Information

You can import the information of multiple persons to the client software in a batch. Meanwhile, you can also export the person information 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.

Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click ⋯ to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
- Each picture file should be in JPG format and should be no larger than 200 KB.
- Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

6. Click **Import** to start importing.

   The importing progress and result will be displayed.

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.

Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start

- Make sure you have added persons and their face pictures to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button. See for details.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

Note

All persons' face pictures will be exported if you do not select any organization.

3. Click **Export** on the top menu bar.
4. Enter the super user name and password for verification.

   The Export panel is displayed.
5. Check **Face** as the content to export.
6. Click **Export** and set an encryption key to encrypt the exported file.

Note

- The exported file is in ZIP format.
- The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).

9.4.3 Get Person Information from Access Control Device

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

Steps

Note

- 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.
- If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select an added access control device or the enrollment station from the drop-down list.

   Note

   If you select the enrollment station, you should click **Login**, and enter IP address, port No., user name and password of the device.
5. Select the **Getting Mode**.

   Note

   The getting mode varies according to different devices. The access control device supports getting the person information by employee ID. Up to 5 employee IDs can be specified each time.
6. Click **Import** to start importing the person information to the client.

   Note

   Up to 2,000 persons and 5,000 cards can be imported.

   The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

9.4.4 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

Steps

1. Enter **Person** module.
2. Click **Batch Issue Cards**.

   All the added persons with no card issued will display.
3. Set the card issuing parameters. For details, refer to ***Set Card Issuing Parameters*** .
4. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
5. Click the card number column and enter the card number.
   - Place the card on the card enrollment station.

- Swipe the card on the card reader.
- Enter the card number manually and press **Enter** key on your keyboard.

The card number will be read automatically and the card will be issued to the person in the list.

6. Repeat the above step to issue the cards to the persons in the list in sequence.

9.4.5 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click on the added card to set this card as lost card.

   After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click to cancel the loss.

   After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

9.4.6 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station ℹ **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.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

Buzzing

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

Card No. Type

Select the type of the card number according to actual needs.

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 enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

9.5 Configure Schedule and Template

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

ℹ **Note**

For access group settings, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

9.5.1 Add Holiday

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

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control → Schedule → Holiday** to enter the Holiday page.
2. Click **Add** on the left panel.
3. Create a name for the holiday.
4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
5. Add a holiday period to the holiday list and configure the holiday duration.

   Note

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

   1) Click **Add** in the Holiday List field.
   2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

      Note

      Up to 8 time durations can be set to one holiday period.
   3) **Optional:** Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .
   4) **Optional:** Select the time duration(s) that need to be deleted, and then click ⊗ in the Operation column to delete the selected time duration(s).
   5) **Optional:** Click 🗑 in the Operation column to clear all the time duration(s) in the time bar.
   6) **Optional:** Click ☒ in the Operation column to delete this added holiday period from the holiday list.
6. Click **Save**.

9.5.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

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

   Note

   There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

   All-Day Authorized

   The access authorization is valid in each day of the week and it has no holiday.

   All-Day Denied

   The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.
3. Create a name for the template.
4. Enter the descriptions or some notification of this template in the Remark box.
5. Edit the week schedule to apply it to the template.

   1) Click **Week Schedule** tab on the lower panel.

   2) Select a day of the week and draw time duration(s) on the timeline bar.

   Note

   Up to 8 time duration(s) can be set for each day in the week schedule.

   3) **Optional:** Perform the following operations to edit the time durations.

   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .

   4) Repeat the two steps above to draw more time durations on the other days of the week.

6. Add a holiday to apply it to the template.

   Note

   Up to 4 holidays can be added to one template.

   1) Click **Holiday** tab.

   2) Select a holiday in the left list and it will be added to the selected list on the right panel.

   3) **Optional:** Click **Add** to add a new holiday.

   Note

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

   4) **Optional:** Select a selected holiday in the right list and click ✕ to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.

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

9.6 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Steps

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

1. Click **Access Control → Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

   Note

   You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.

5. In the left list of the Select Person field, select person(s) and the person(s) will be added to the selected list .
6. In the left list of the Select Door field, select door(s) or door station(s) for the selected persons to access, and the selected door(s) or door station(s) will be added to the selected list.
7. Click **OK**.
8. After adding the access groups, you need to apply them to the access control device to take effect.
   1) Select the access group(s) to apply to the access control device.

      To select multiple access groups, you can hold the **Ctrl** or **Shift** key and select access groups.
   2) Click **Apply All to Devices** to start applying all the selected access group(s) to the access control device or door station.

      Caution

      - Be careful to click **Apply All to Devices**, since this operation will clear all the access groups of the selected devices and then apply the new access group, which may brings risk to the devices.
      - You can click **Apply Changes to Devices** to only apply the changed part of the selected access group(s) to the device(s).
   3) View the apply status in the Status column or click **Applying Status**to view all the applied access group(s).

The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.

9. **Optional:** Click ✎ to edit the access group if necessary.

9.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene.

Note

- For the card related functions(the type of access control card), only the card(s) with access group applied will be listed when adding cards.
- The advanced functions should be supported by the device.
- Hover the cursor on the Advanced Function, and then Click ⚙ to customize the advanced function(s) to be displayed.

9.7.1 Configure Remaining Unlocked/Locked

You can set the status of the door as unlocked or locked and set the elevator controller as free and controlled. For example, you can set the door remaining locked in the holiday, and set the door remaining unlocked in the specified period of the work day.

Before You Start
Add the access control devices to the system.

Steps

1. Click **Access Control → Advanced Function → Remain Locked/Unlocked** to enter the Remain Locked/Unlocked page.
2. Select the door or elevator controller that need to be configured on the left panel.
3. To set the door or elevator controller status during the work day, click the **Week Schedule** and perform the following operations.
   1) For door, click **Remain Unlocked** or **Remain Locked**.
   2) For elevator controller, click **Free** or **Controlled**.
   3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

   Note

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

   4) **Optional:** Perform the following operations to edit the time durations.

- Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
- Click the time duration and directly edit the start/end time in the appeared dialog.
- Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .

5) Click **Save**.

Related Operations

Copy to Whole Week Select one duration on the time bar, click **Copy to Whole Week** to copy all the duration settings on this time bar to other week days.

Delete Selected Select one duration on the time bar, click **Delete Selected** to delete this duration.

Clear Click **Clear** to clear all the duration settings in the week schedule.

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.

1) Click **Remain Unlocked** or **Remain Locked**.
2) Click **Add**.
3) Enter the start date and end date.
4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to one holiday period.

5) Perform the following operations to edit the time durations.
- Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
- Click the time duration and directly edit the start/end time in the appeared dialog.
- Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .

6) **Optional:** Select the time duration(s) that need to be deleted, and then click ⊗ in the Operation column to delete the selected time duration(s).
7) **Optional:** Click 🗑 in the Operation column to clear all the time duration(s) in the time bar.
8) **Optional:** Click ☒ in the Operation column to delete this added holiday period from the holiday list.
9) Click **Save**.

5. **Optional:** Click **Copy to** to copy the door status settings of this door to other door(s).

9.7.2 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-Passpack Settings page.
2. Select an access control device on the left panel.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.
4. Click ✎ of the selected first card reader in the **Card Reader Afterward** column to open the 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 as afterward card readers for one card reader.
6. Click **OK** in the dialog to save the selections.
7. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

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.

9.7.3 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.

Before You Start

Add access control device to the client, and make sure the device supports the multi-door interlocking function.

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** .
2. Select an access control device on the left panel.
3. Click **Add** on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
4. Select at least two access control points(doors) 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 **Apply** to apply the settings to the access control device.

9.7.4 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

- Add access control device to the client, and make sure the device supports the first person in function.
- Add person and assign access authorization to designed person. For details, refer to ***Person Management*** and ***Set Access Group to Assign Access Authorization to Persons*** .

Steps

1. Click **Access Control → Advanced Function → First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.
3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

   Enable Remaining Open after First Person

The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the consecutive authentication times and interval of consecutive authentication.

Note

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

Disable Remaining Open after First Person

Disable the function of first person in, namely normal authentication.

Authorization by First Person

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

Note

You can authenticate by the first person again to disable the first person mode.

4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.

   The added first person(s) will list in the First Person List
6. **Optional:** Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

9.7.5 Configure Multi-Factor Authentication

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

Before You Start

Set access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

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 → Multi-Factor Auth** .
2. Select an access control device in device list on the left panel.
3. Add a person/card group for the access control device.
   1) Click **Add** on the right panel.
   2) Create a name for the group as desired.
   3) Specify the start time and end time of the effective period for the person/card group.

4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

Note

Make sure you have issue card to the person.
Make sure you have set access group and apply the access group to the access control device successfully.

5) Click **Save**.
6) **Optional:** Select the person/card group(s), and then click **Delete** to delete it(them).
7) **Optional:** Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.

4. Select an access control point (door) of selected device on the left panel.

5. Enter the maximum interval when entering password.

6. Add an authentication group for the selected access control point.

1) Click **Add** on the Authentication Groups panel.
2) Select a configured template as the authentication template from the drop-down list.

Note

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

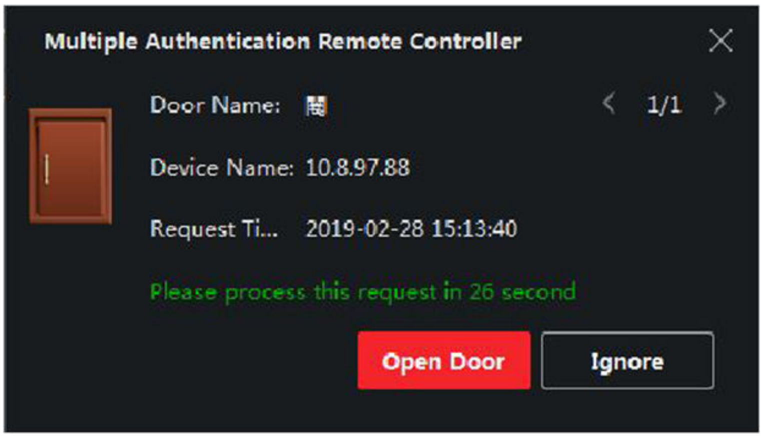
3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

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.



Multiple Authentication Remote Controller

Door Name: [illegible]

Device Name: 10.8.97.88

Request Ti... 2019-02-28 15:13:40

Please process this request in 26 second

Figure 9-2 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 person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.
5) Click the added authentication group in the right list to set authentication times in the Auth Times column.

Note

The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.

6) Click **Save**.

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 person/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 person/card groups can be added to the authentication group.

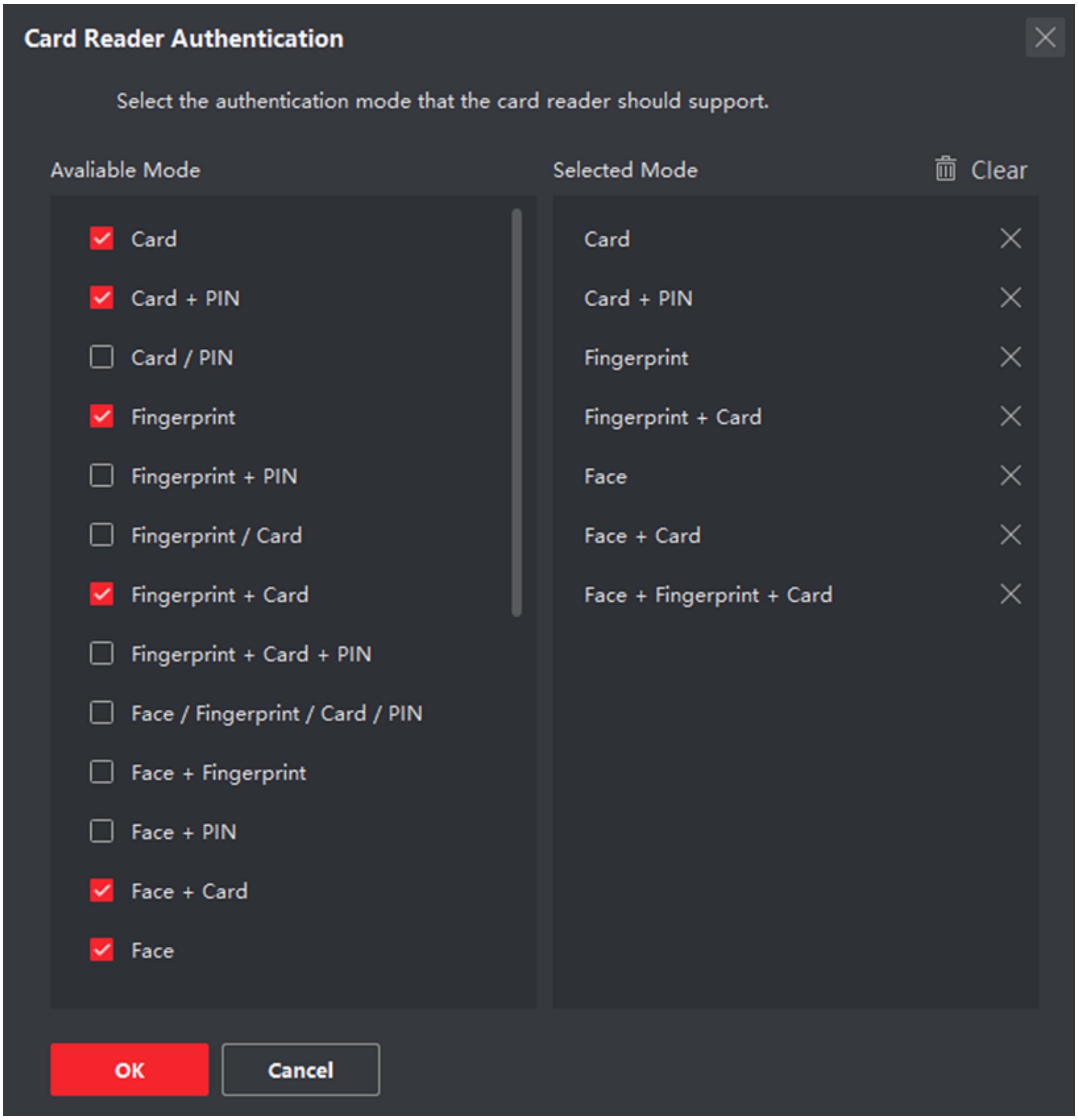
7. Click **Save**.

9.7.6 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.

Steps

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



Card Reader Authentication

Select the authentication mode that the card reader should support.

Avaliable Mode

- ☑ Card
- ☑ Card + PIN
- □ Card / PIN
- ☑ Fingerprint
- □ Fingerprint + PIN
- □ Fingerprint / Card
- ☑ Fingerprint + Card
- □ Fingerprint + Card + PIN
- □ Face / Fingerprint / Card / PIN
- □ Face + Fingerprint
- □ Face + PIN
- ☑ Face + Card
- ☑ Face

Selected Mode

- Card
- Card + PIN
- Fingerprint
- Fingerprint + Card
- Face
- Face + Card
- Face + Fingerprint + Card

Figure 9-3 Select Card Reader Authentication Mode

2) Check the modes in the Available Mode list and they will be added to the selected modes list.

3) Click **OK**.

After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor 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**.

9.7.7 Configure Device Parameters

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

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control → Advanced Function → Device Parameters** .

   Note

   If you can not find Device Parameter in the Advanced Function list, hover the cursor on the Advanced Function, and then Click ⚙ to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

   Note

   - The displayed parameters may vary for different access control devices.
   - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Enable NFC

If enable the function, the device can recognize the NFC card. You can present NFC card on the device.

Enable M1 Card

If enable the function, the device can recognize the M1 card. You can present M1 card on the device.

Enable EM Card

If enable the function, the device can recognize the EM card. You can present EM card on the device.

Enable CPU Card

Reserved. If enable the function, the device can recognize the CPU card. You can present CPU card on the device.

Enable ID Card

Reserved. If enable the function, the device can recognize the ID card. You can present ID card on the device.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door

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

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. Select an access control device on the left panel, and then click ▸ to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.

Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Open Duration

The door contact can be enabled with appropriate delay after person with extended accesss needs swipes her/his card.

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Super Password

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

5. Click **Advanced** to configure advanced parameters.

Extended Open Duration

The door contact can be enabled with appropriate delay after person with extended accesss needs swipes her/his card.

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.

Enable Locking Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

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 and super password should be different.
- The duress code and super password should be different from the authentication password.
- The length of duress code and super password is according the device, usually it should contains 4 to 8 digits.

6. Click **OK**.
7. **Optional:** Click **Copy to** , and then select the door to copy the parameters in the page to the selected doors.

Note

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

Configure Parameters for Card Reader

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

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. In the device list on the left, click ▸ to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.

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.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

Card Authentication 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.

Enable Failed Attempts Limit of Authentication

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

Card Reader Type/Card Reader Description

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

4. Click **Advanced** and you can configure more parameters.

Enable Card Reader

Enable the function and you can operate the functions below on the card reader.

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.

Buzzer Polarity

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

Buzzing Time

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

Max. Interval When Entering PWD

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.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

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

Fingerprint Recognition Level

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

5. Click **OK**.
6. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Output

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

Before You Start

Add access control device to the client, and make sure the device supports alarm output.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click ▸ to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

   Name

   Edit the card reader name as desired.

   Alarm Output Active Time

   How long the alarm output will last after triggered.
4. Click **OK**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

9.7.8 Configure Device Parameters

After adding the access control device, you can set its parameters such as network parameters.

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

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

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **M1 Card Encryption** to enter the M1 Card Encryption page.
4. Set the switch to on 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.

9.8 Door Control

In Monitoring module, you can view the real-time status of the doors managed by the added access control device. You can also control the doors such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door control permission, the user can enter the Monitoring module and control the door. Or the icons used for control will not show. For setting the user permission, refer to ***Person Management*** .

9.8.1 Control Door Status

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

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   For managing the access point group, refer to *Group Management* in the user manual of the client software.

   The doors in the selected access control group will display.
3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.
4. Click the following buttons to control the door.

   Open Door

   When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

   Close Door

   When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

   Remain Open

   The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

   Remain Closed

   The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to *Set File Saving Path* in the user manual of the client software.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

9.8.2 Check Real-Time Access Records

The access records will display in real time, including card swiping records, fingerprint comparison records, etc. You can view the person information and view the picture captured during access.

Steps

1. Click **Monitoring** and select a group from the drop-down list on the upper-right corner.

   The access records triggered at the doors in the selected group 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 the event type and event status so that these events will show in the list if the events are detected. The events of unchecked type or status will not be displayed in the list.
3. **Optional:** Check **Show Latest Event** and the latest access record will be selected and displayed at the top of the record list.
4. **Optional:** Click the event to view the accessed person details, including person pictures (captured picture and profile), person No., person name, organization, phone, contact address, etc.

   Note

   You can double click the captured picture to enlarge it to view the details.
5. **Optional:** Right click on the column name of the access event table to show or hide the column according to actual needs.

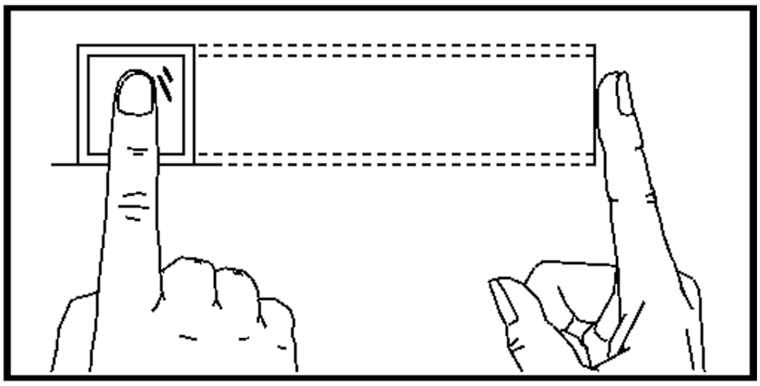
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

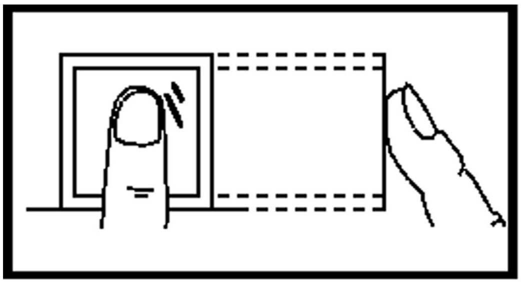
The figure displayed below is the correct way to scan your finger:



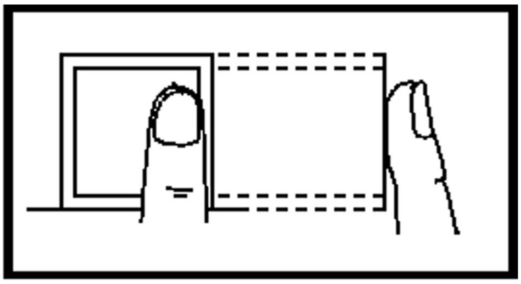
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

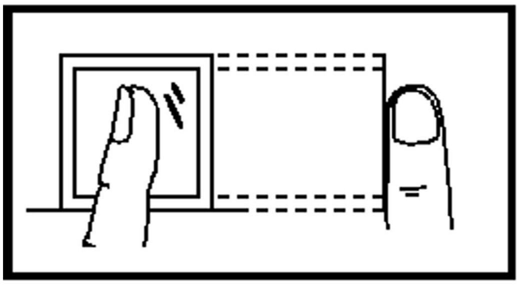
The figures of scanning fingerprint displayed below are incorrect:



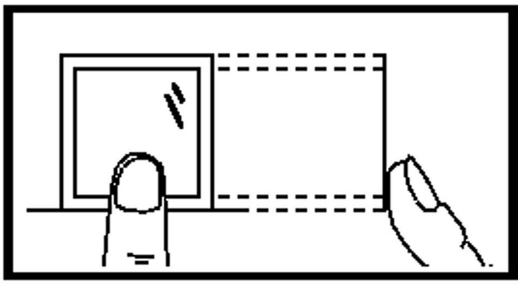
Vertical



Edge I



Side



Edge II

Environment

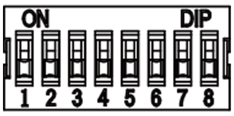
The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

Others

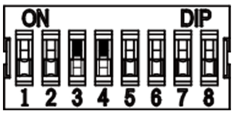
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.
If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

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.

Appendix D. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.
Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

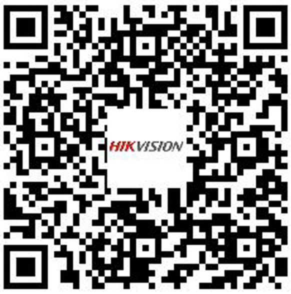


Figure D-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.
Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

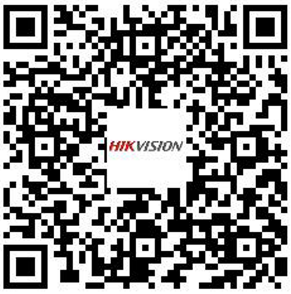


Figure D-2 Device Command

See Far, Go Further