DS-K27XX Series Access Controller

User Manual

Legal Information

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- 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.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT 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 DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

Available Model

Product Name	Model
Access Controller	DS-K2701X Series Access Controller
	DS-K2702X Series Access Controller
	DS-K2702WX-E1 Series Access Controller
	DS-K2704X Series Access Controller
	DS-K2708X Series Access Controller
Access Module	DS-K2M002X Access Module

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 Features

- The access controller and access module are cascaded by RS-485. The 4-door access controller can control up to 128 doors, the 2-door access controller can control up to 126 doors, and the 1-door access controller can control up to 125 doors.
- Supports access control application.
- Supports management via Web client.
- Supports RS-485 to achieve hand-in-hand cascade.
- Supports backup battery charging and discharging.

  Note

  Only partial models support this function.
- Uplink supports wired network or Wi-Fi; Downlink supports Wiegand (customizable) and OSDP.

  Note

  Only partial models support Wi-Fi function.
- In addition to the conventional DC 12 V power supply, device can also be powered via POE.

  Note

  Only partial models support this function.
- The main board sells separately and supports rail mounting.

Chapter 2 Appearance

2.1 Appearance and Interfaces of 1-Door/2-Door/4-Door/8-Door Access Controller

The appearance and interfaces of 1-door/2-door/4-door/8-door access controller are as follows.

Appearance and Interfaces of 1-Door Access Controller

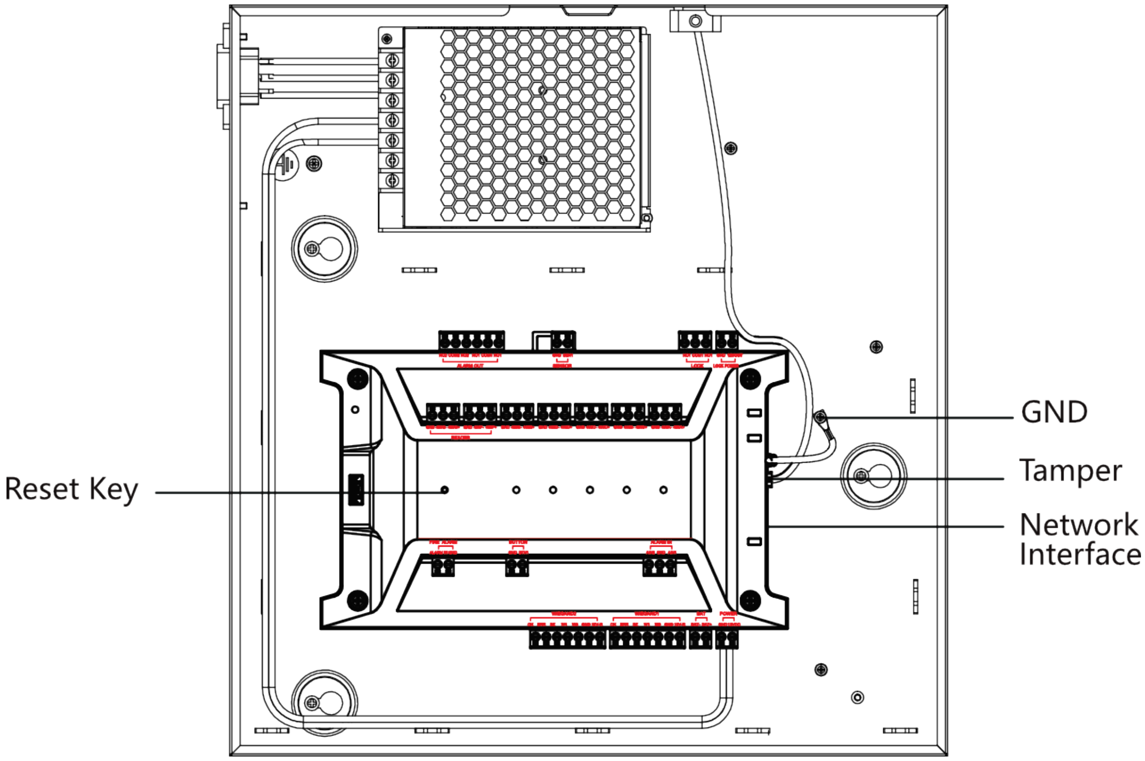


Figure 2-1 Appearance and Interfaces of 1-Door Access Controller

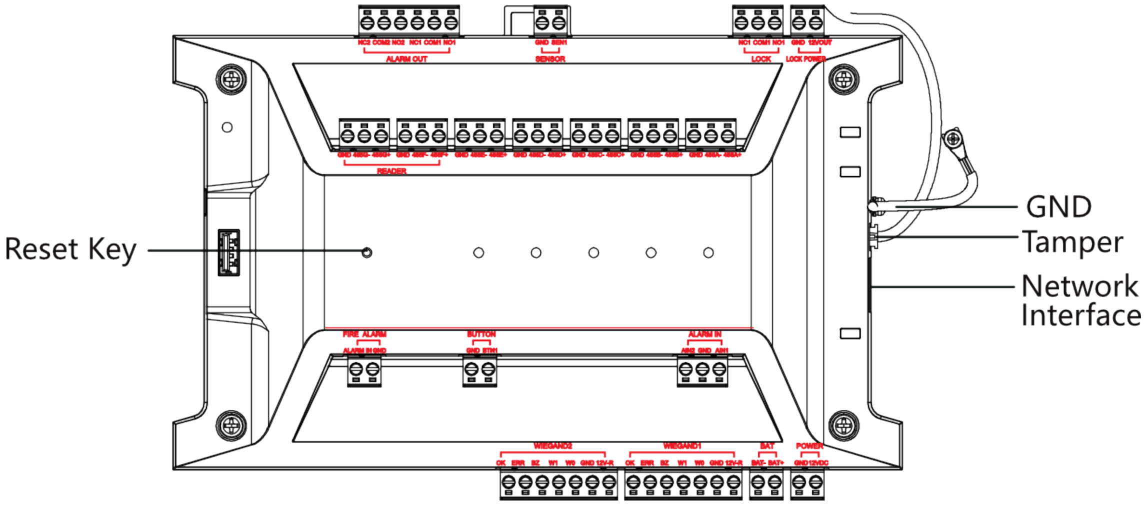


Figure 2-2 Appearance and Interfaces of 1-Door Access Controller Main Board

Appearance and Interfaces of 2-Door Access Controller

Note

- Only partial models support Wi-Fi and POE function.
- PoE model devices need to be aware of the following:

  1. The switch specification is 30 W.
  2. PoE and Wi-Fi function cannot be used at the same time.
  3. If the total power of the incoming locks exceeds 10 W, an additional separate power supply is required for one of the locks.
  4. Supports access to up to 4 card readers.

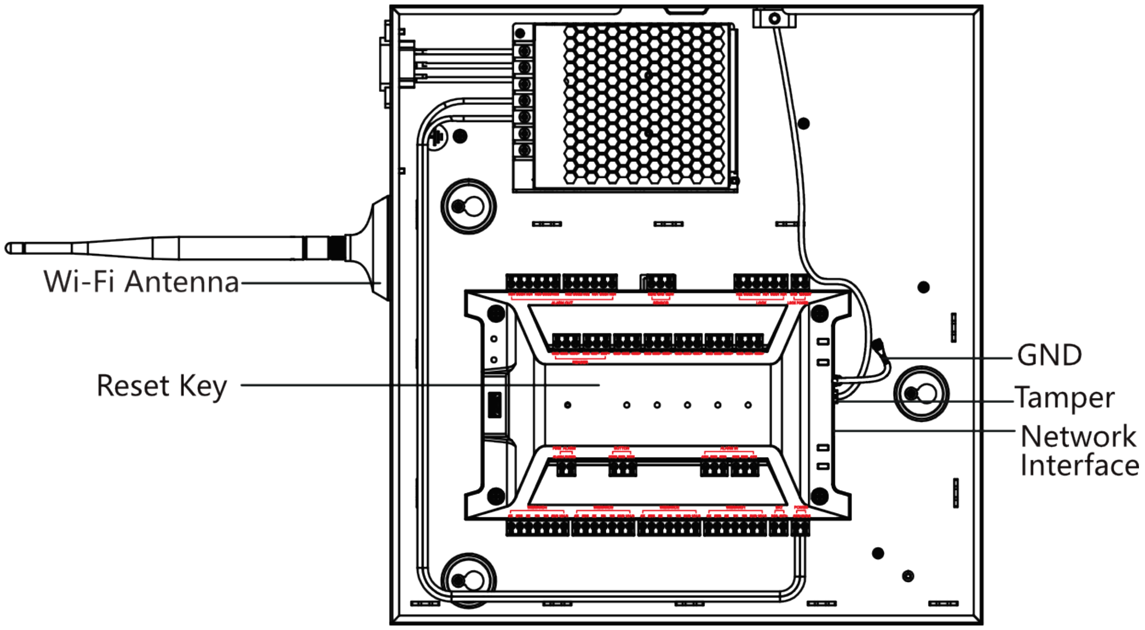


Figure 2-3 Appearance and Interfaces of 2-Door Access Controller

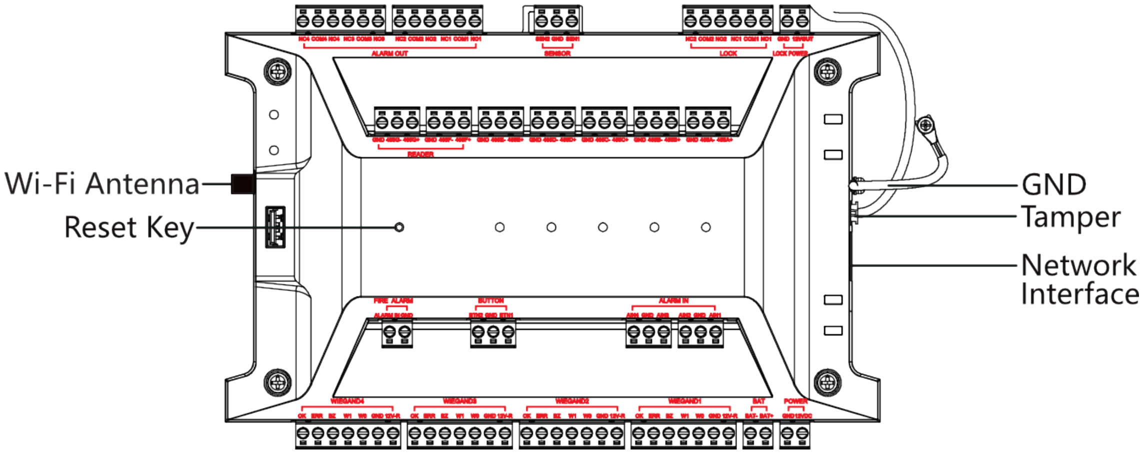

NC4 COM4 NO4 NC3 COM3 NO3 NC2 COM2 NO2 NC1 COM1 NO1
ALARM OUT
SEN2 GND SEN1
SENSOR
NC2 COM2 NO2 NC1 COM1 NO1
LOCK
GND 12VOUT
LOCK POWER
GND 485G- 485G+ GND 485F- 485F+ GND 485E- 485E+ GND 485D- 485D+ GND 485C- 485C+ GND 485B- 485B+ GND 485A- 485A+
READER
Wi-Fi Antenna
Reset Key
GND
Tamper
Network Interface
FIRE ALARM
ALARM IN GND
BUTTON
BTN2 GND BTN1
ALARM IN
AIN4 GND AIN3 AIN2 GND AIN1
WIEGAND4
WIEGAND3
WIEGAND2
WIEGAND1
OK ERR BZ W1 W0 GND 12V-R
BAT
BAT- BAT+
POWER
GND 12VDC

Figure 2-4 Appearance and Interfaces of 2-Door Access Controller Main Board

Appearance and Interfaces of 4-Door Access Controller

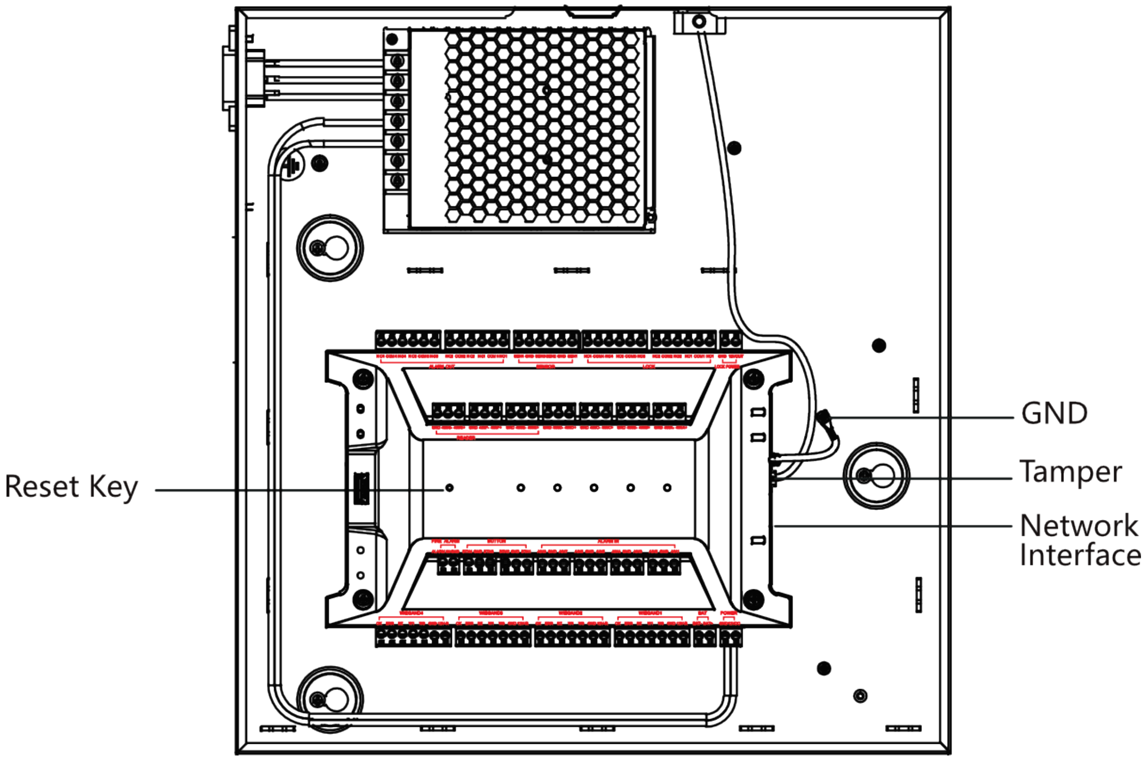


Figure 2-5 Appearance and Interfaces of 4-Door Access Controller

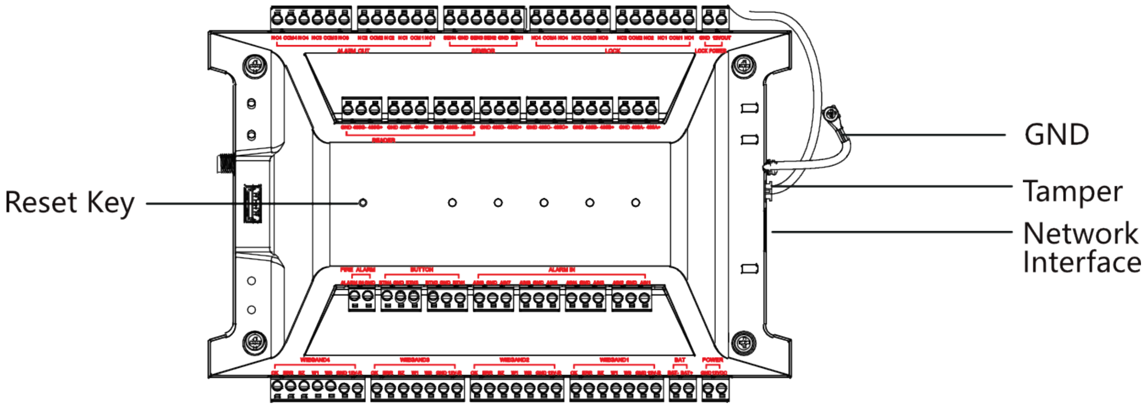


Figure 2-6 Appearance and Interfaces of 4-Door Access Controller Main Board

Appearance and Interfaces of 8-Door Access Controller

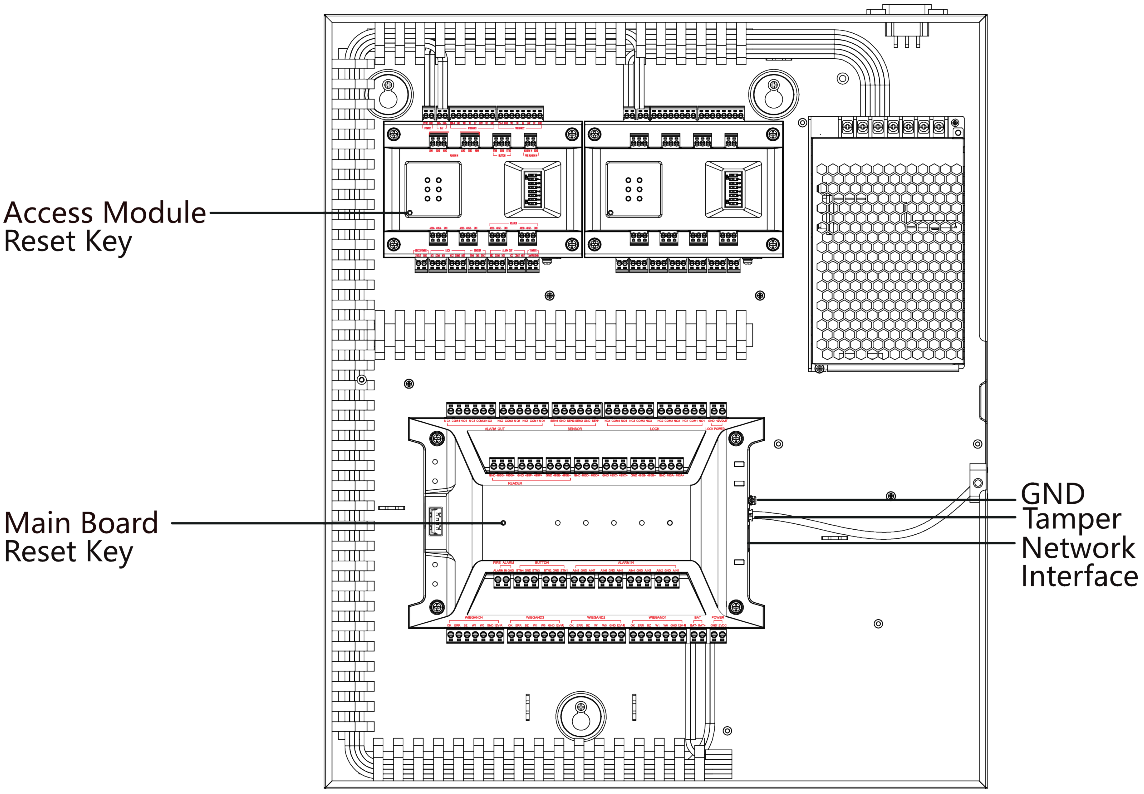


Figure 2-7 Appearance and Interfaces of 8-Door Access Controller

2.2 Access Module Appearance

View the access module appearance.

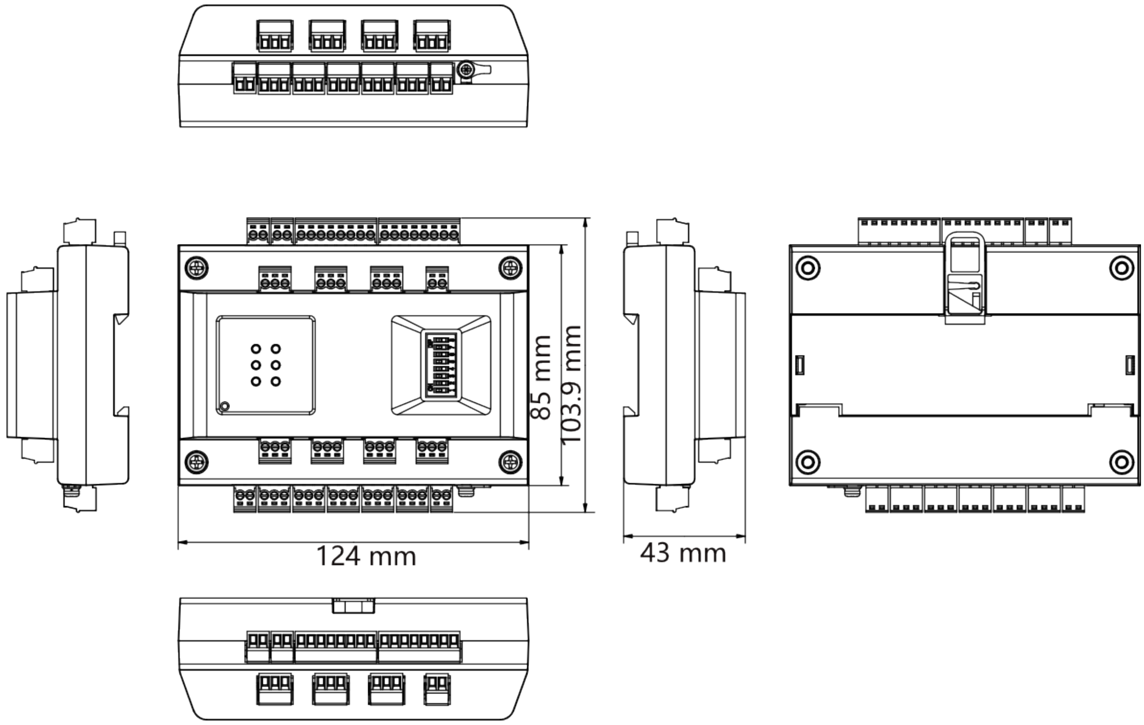


Figure 2-8 Access Module Appearance

2.3 Indicator Description

The indicator description of 1-door/2-door/4-door/8-door access controller and access module is as follows.

Device Name	Description
1-Door Access Controller	There are a total of 9 indicators: a power supply indicator, a working status indicator, a network indicator, a door status and 5 RS-485 status indicators.
2-Door Access Controller	There are a total of 11 indicators: a power supply indicator, a working status indicator, a network indicator, a Wi-Fi indicator, 5 RS-485 status indicators and 2 door status indicators.

	Note Some models do not support Wi-Fi indicators.
4-Door Access Controller	There are a total of 12 indicators: a power supply indicator, a working status indicator, a network indicator, 5 RS-485 status indicators and 4 door status indicators.
8-Door Access Controller	Access Controller: There are a total of 12 indicators: a power supply indicator, a working status indicator, a network indicator, 5 RS-485 status indicators and 4 door status indicators. Access module: There are a total of 6 indicators: a power supply indicator, a working status indicator, 2 communication status indicators, and 2 door status indicators.
Access Module	There are a total of 6 indicators: a power supply indicator, a working status indicator, 2 communication status indicators, and 2 door status indicators.

Note

When the working status indicator is red, it means that the device is powered on; When the working status indicator is flashing green, it means that the device is added to the platform. When the door status indicator is on, it means that the door is open, and the light is off means that the door is closed. When the other status indicators are on, it means connecting, and the light off means that it is not connected.

Chapter 3 Terminal Wiring

Terminal Wiring Description of the Access Controller.

3.1 Wiring Description

The wiring of 1-door/2-door/4-door/8-door access controller are as follows.

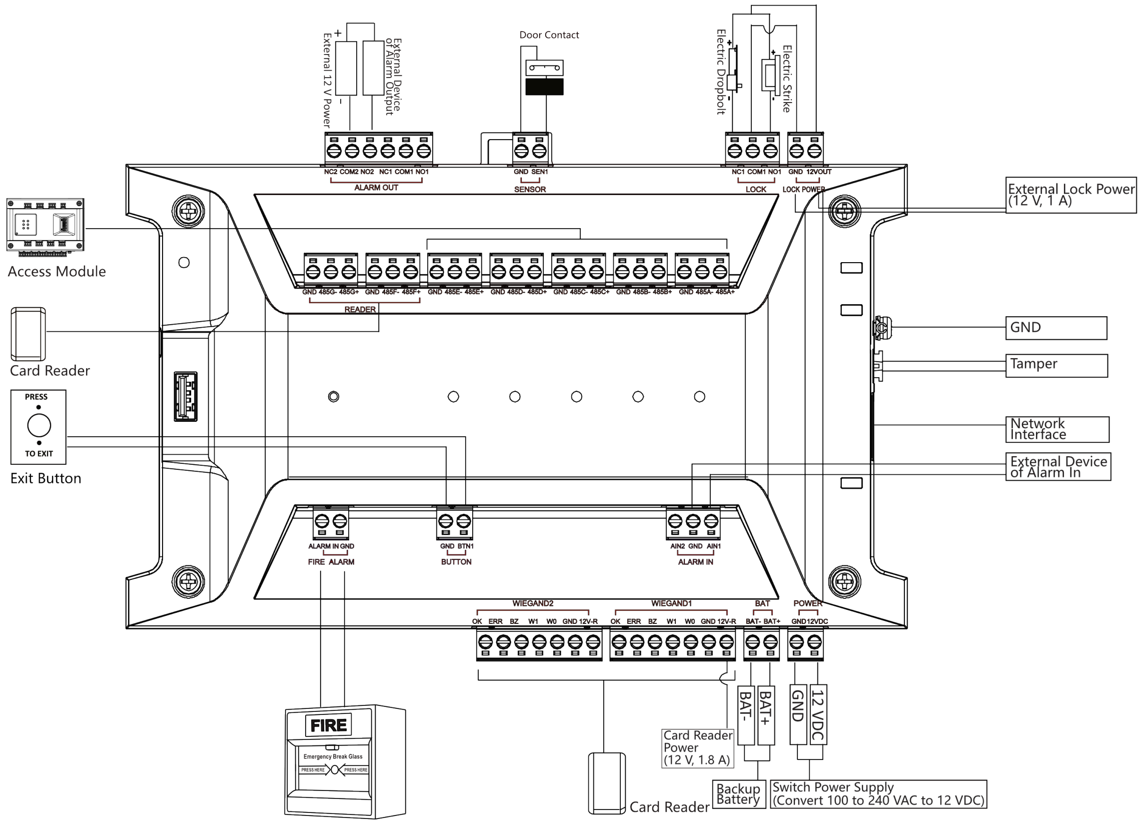


Figure 3-1 The Wiring of 1-Door Access Controller

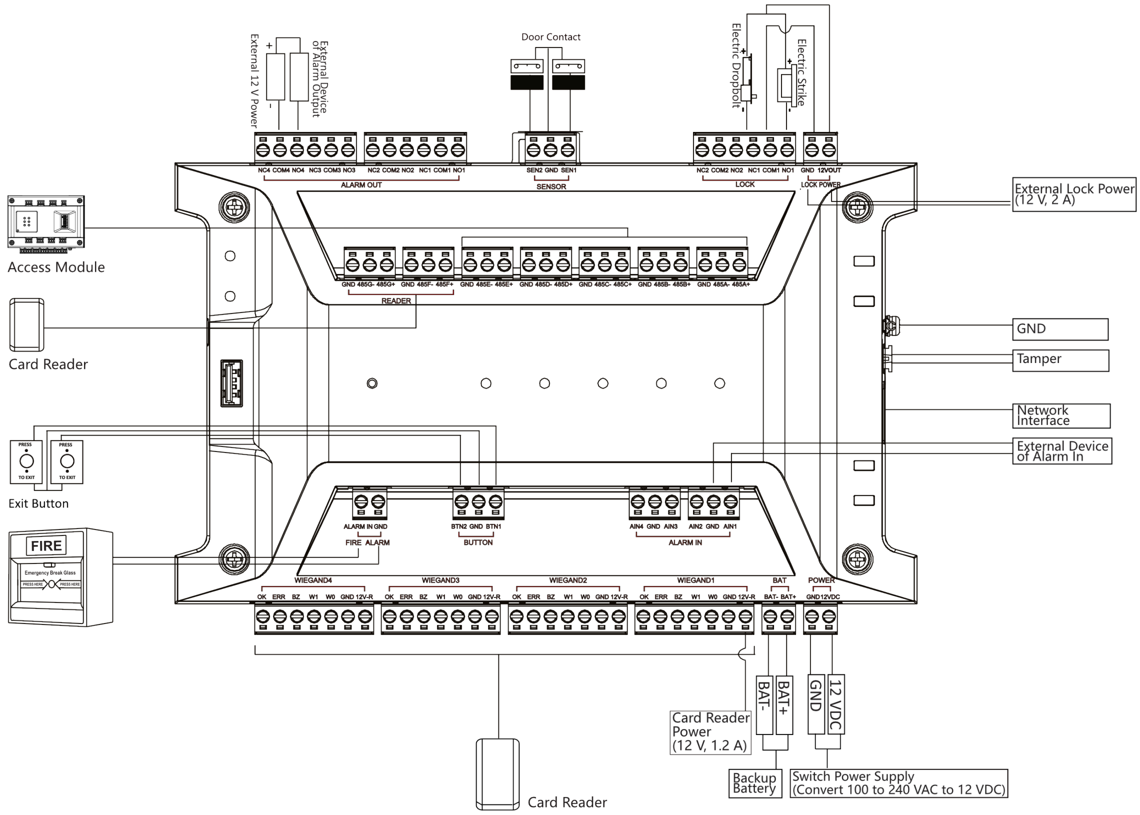

External 12 V Power
+
-
External Device of Alarm Output
Door Contact
Electric Dropbolt
Electric Strike
NC4 COM4 NO4 NC3 COM3 NO3 NC2 COM2 NO2 NC1 COM1 NO1
ALARM OUT
SEN2 GND SEN1
SENSOR
NC2 COM2 NO2 NC1 COM1 NO1
LOCK
GND 12VOUT
LOCK POWER
External Lock Power (12 V, 2 A)
Access Module
GND 485G- 485G+ GND 485F- 485F+ GND 485E- 485E+ GND 485D- 485D+ GND 485C- 485C+ GND 485B- 485B+ GND 485A- 485A+
READER
Card Reader
GND
Tamper
Network Interface
External Device of Alarm In
PRESS
TO EXIT
Exit Button
FIRE
Emergency Break Glass
ALARM IN GND
FIRE ALARM
BTN2 GND BTN1
BUTTON
AIN4 GND AIN3 AIN2 GND AIN1
ALARM IN
WIEGAND4
WIEGAND3
WIEGAND2
WIEGAND1
OK ERR BZ W1 W0 GND 12V-R
BAT
BAT- BAT+
POWER
GND 12VDC
BAT-
BAT+
GND
12 VDC
Card Reader Power (12 V, 1.2 A)
Backup Battery
Switch Power Supply (Convert 100 to 240 VAC to 12 VDC)
Card Reader

Figure 3-2 The Wiring of 2-Door Access Controller

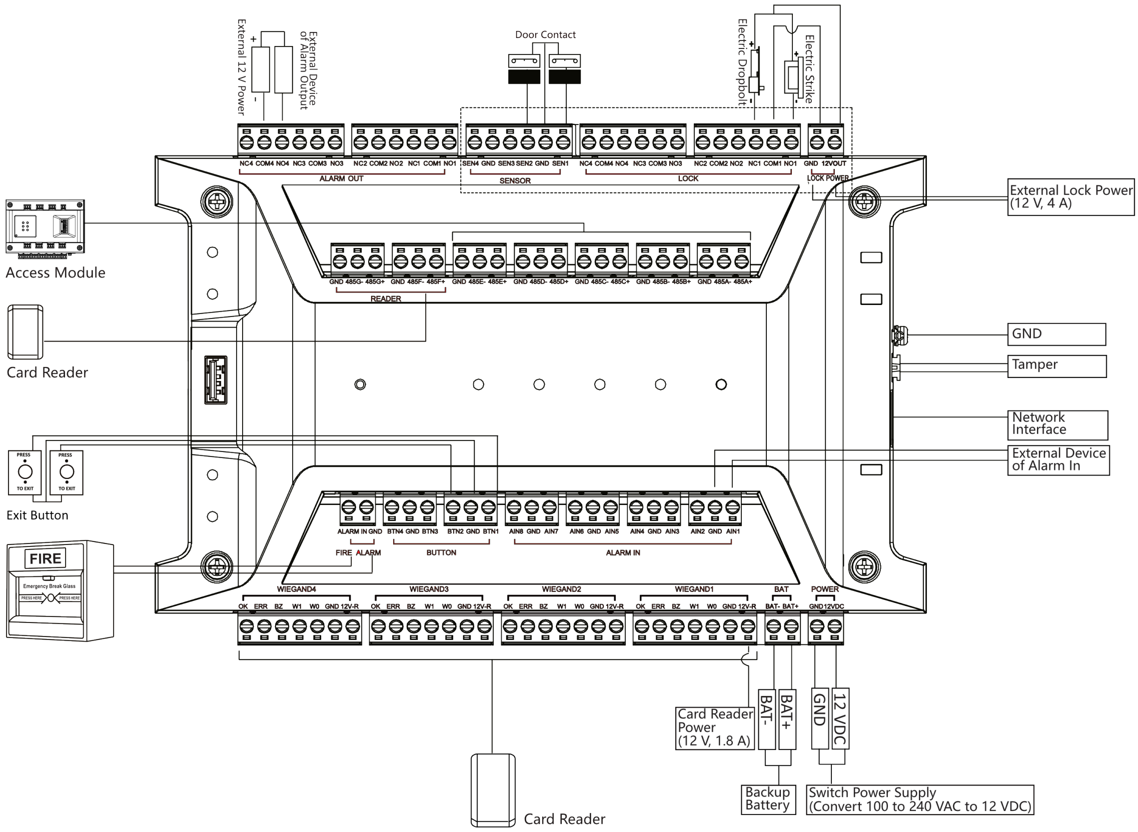

External 12 V Power
+
-
External Device of Alarm Output
Door Contact
Electric Dropbolt
Electric Strike
NC4 COM4 NO4 NC3 COM3 NO3 NC2 COM2 NO2 NC1 COM1 NO1
ALARM OUT
SEN4 GND SEN3 SEN2 GND SEN1
SENSOR
NC4 COM4 NO4 NC3 COM3 NO3 NC2 COM2 NO2 NC1 COM1 NO1
LOCK
GND 12VOUT
LOCK POWER
External Lock Power (12 V, 4 A)
Access Module
GND 485G- 485G+ GND 485F- 485F+ GND 485E- 485E+ GND 485D- 485D+ GND 485C- 485C+ GND 485B- 485B+ GND 485A- 485A+
READER
Card Reader
GND
Tamper
Network Interface
External Device of Alarm In
PRESS
TO EXIT
Exit Button
ALARM IN GND
FIRE ALARM
BTN4 GND BTN3 BTN2 GND BTN1
BUTTON
AIN8 GND AIN7 AIN6 GND AIN5 AIN4 GND AIN3 AIN2 GND AIN1
ALARM IN
FIRE
Emergency Break Glass
WIEGAND4
WIEGAND3
WIEGAND2
WIEGAND1
OK ERR BZ W1 W0 GND 12V-R
BAT
BAT- BAT+
POWER
GND 12VDC
Card Reader Power (12 V, 1.8 A)
BAT-
BAT+
GND
12 VDC
Backup Battery
Switch Power Supply (Convert 100 to 240 VAC to 12 VDC)
Card Reader

Figure 3-3 The Wiring of 4-Door Access Controller

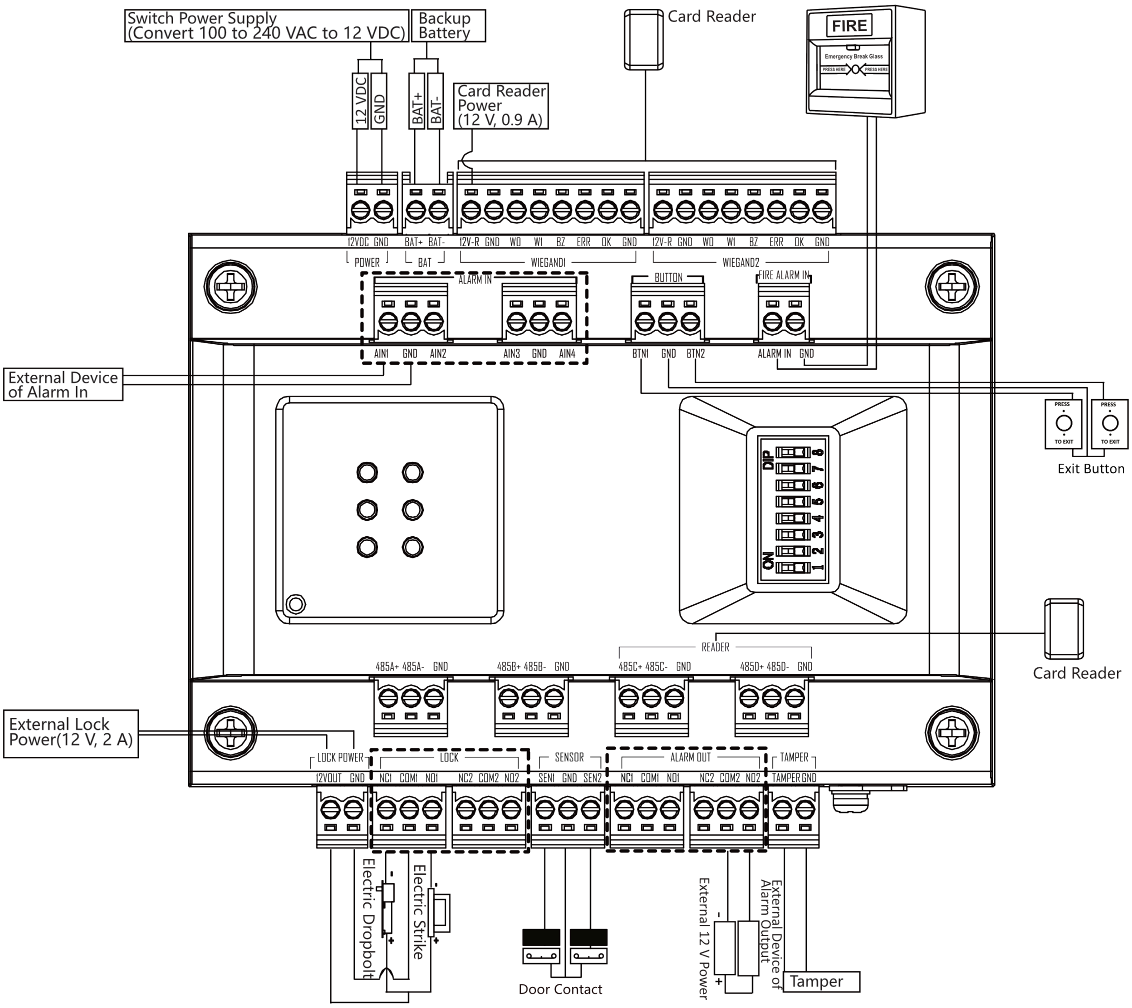


Figure 3-4 The Wiring of Access Module

3.2 Wiegand Card Reader Wiring

You can view the Wiegand card reader wiring diagram.

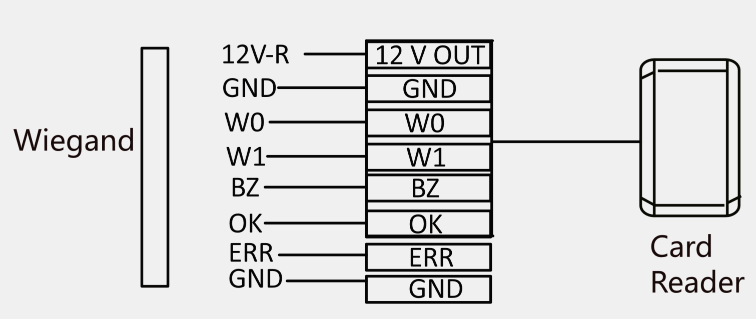


Figure 3-5 Wiegand Card Reader Wiring Diagram

Note

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

3.3 RS-485 Card Reader Wiring

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

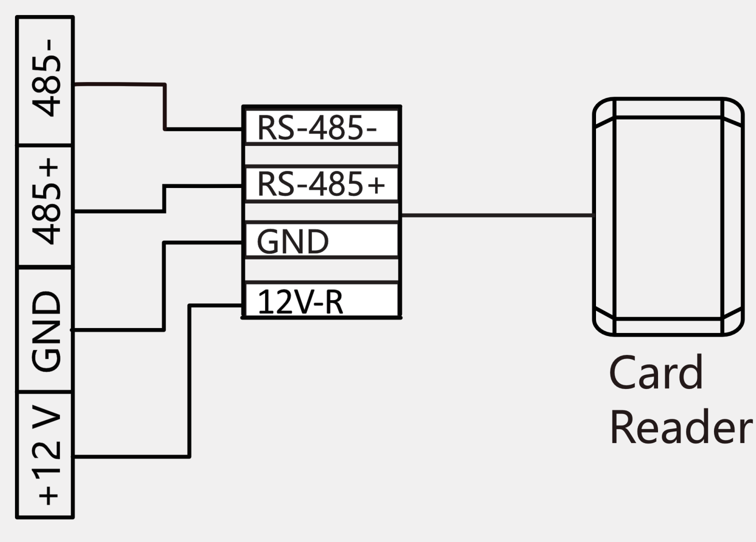


Figure 3-6 RS-485 Card Reader Wiring Diagram

Note

- If the card reader is installed too far away from the access controller, you can use an external power supply.
- It is recommended to use hand-in-hand wiring to connect the RS-485 card reader.

3.4 Door Lock Wiring

You can view the door lock wiring diagram.

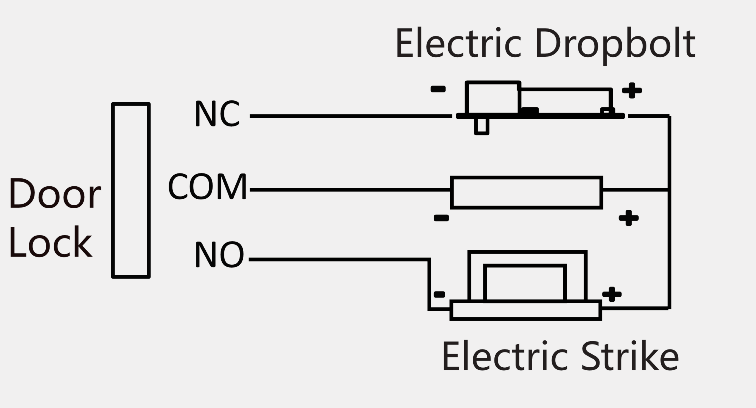


Figure 3-7 Wiring Diagram of Door Lock

3.5 Alarm Wiring

You can view the alarm wiring diagram.

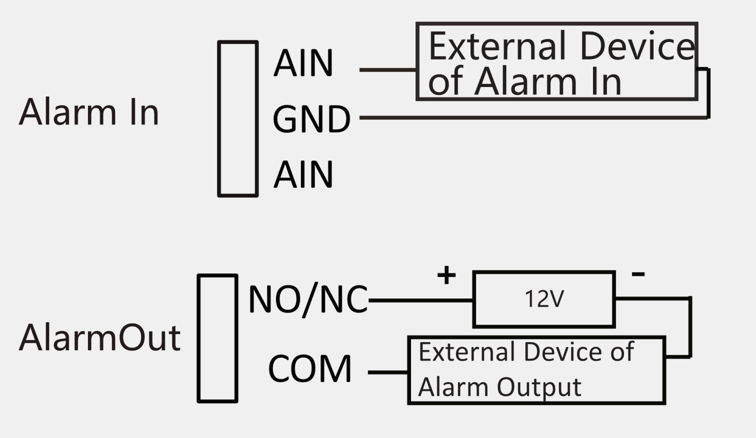


Figure 3-8 Alarm Wiring

3.6 Exit Button Wiring

You can view the exit button wiring diagram

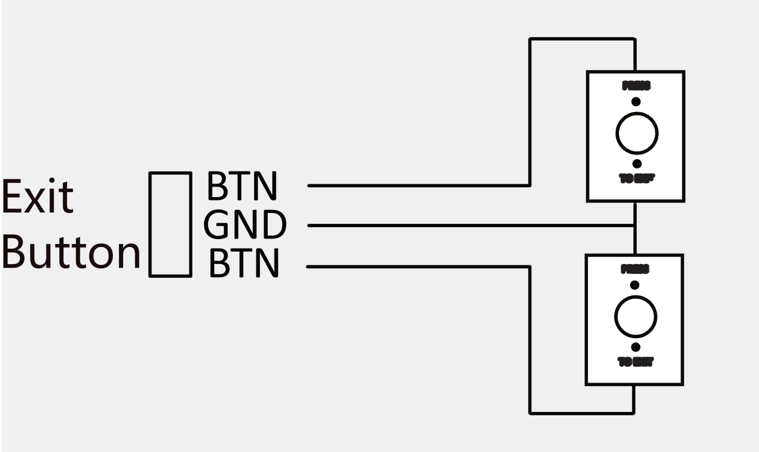


Figure 3-9 Exit Button Wiring

3.7 Door Contact Wiring

You can view the door contact wiring diagram.

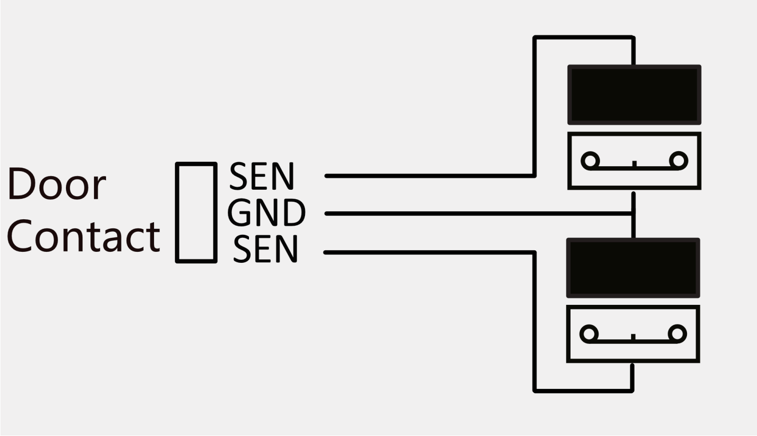


Figure 3-10 Door Contact Wiring

3.8 Fire Alarm Module Wiring

You can view the fire alarm module wiring diagram.

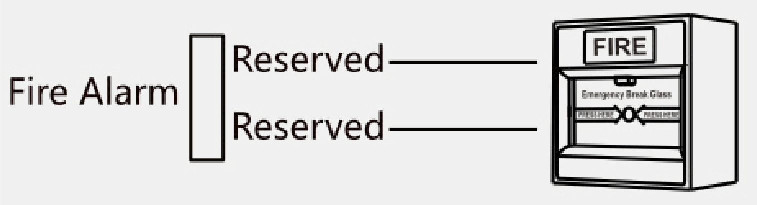


Figure 3-11 Fire Alarm Module Wiring

Chapter 4 Installation

4.1 Install Access Controller

The access controller chassis can be wall-mounted.

Steps

Note

- Indoor use only.
- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.
- Here we take 1-door access controller as example.

1. Fix 3 SC-KA4X45 screws to the wall, and 3 to 5 mm thread should be reserved on the top of the screw (to facilitate subsequent hanging of the chassis).

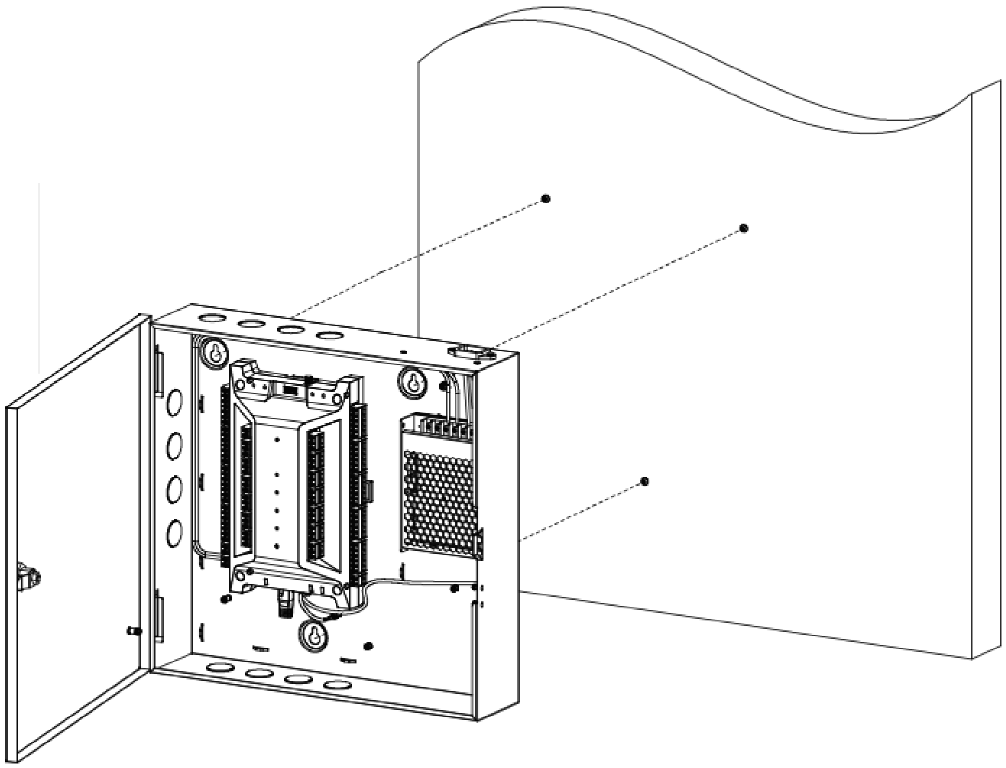


Figure 4-1 Fix Chassis

2. Open the chassis cover and press the holes on the chassis body with the screws reserved on the wall. Then attach the chassis from top to bottom onto the screws.

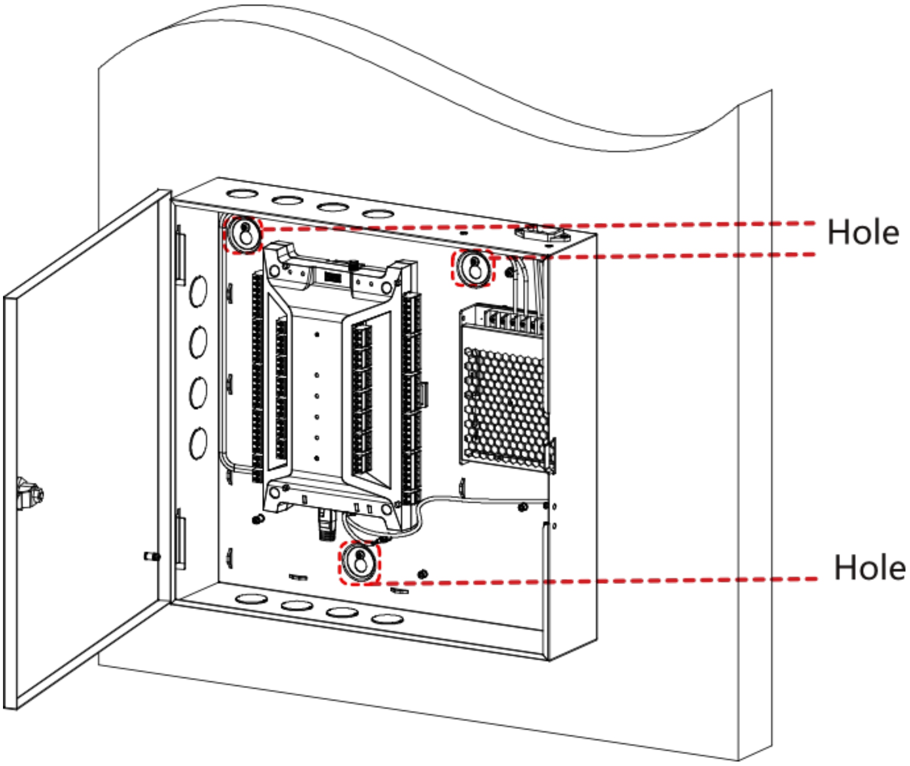


Figure 4-2 Hang Chassis

3. Close the chassis cover to complete the installation.

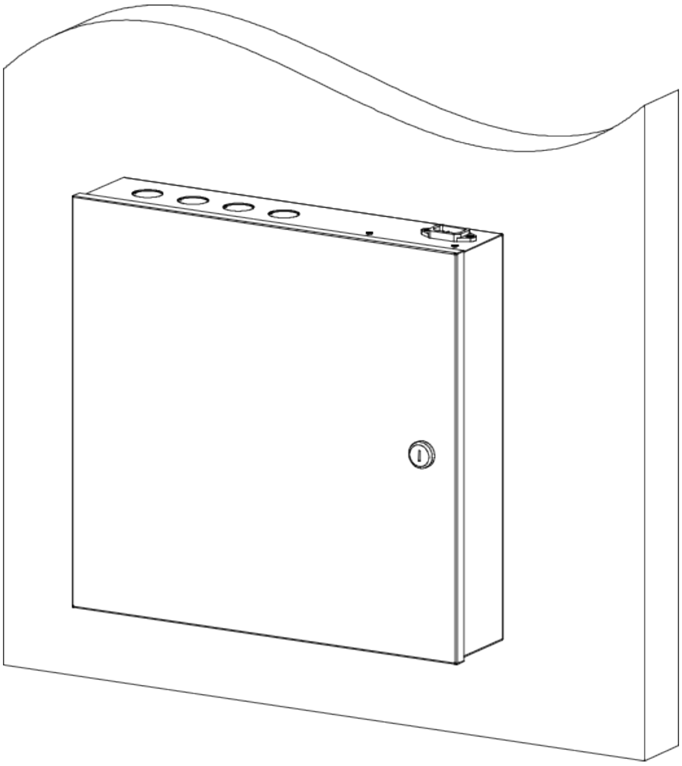


Figure 4-3 Complete Installation

4.2 Install Access Controller Main Board

The access controller main board can be wall-mounted.

Steps

Note

- Indoor use only.
- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.
- Here we take 1-door access controller main board as example.

1. Use 2 SC-KA4X25 screws to secure the rail to the wall.

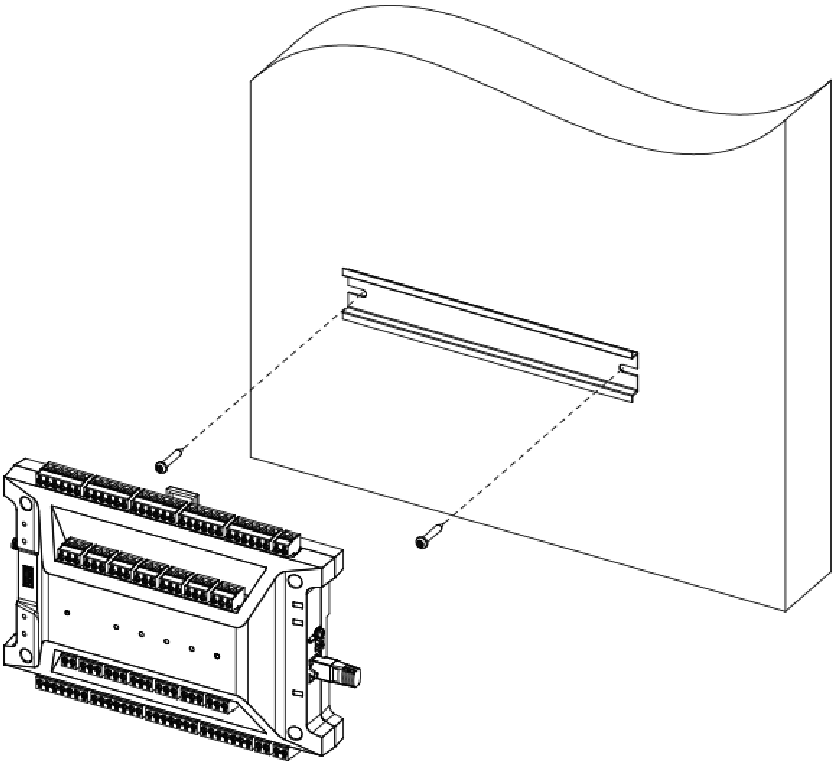


Figure 4-4 Secure Rail

2. Align the rail groove on the bottom of the device with the rail, press the device, and snap the device to the rail with the tabs on the bottom.

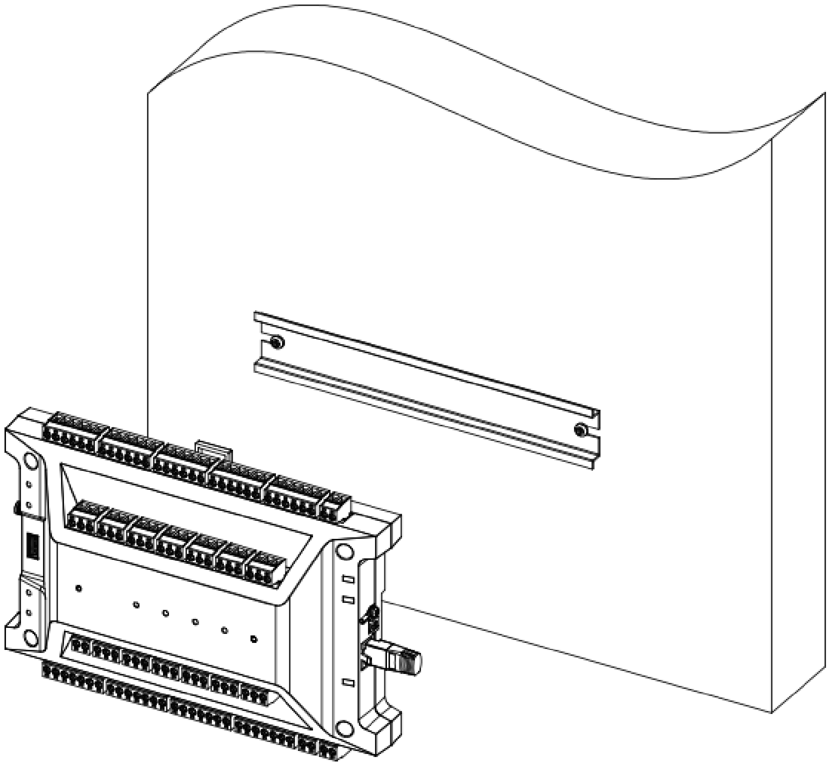


Figure 4-5 Fix Device

3. Installation completed.

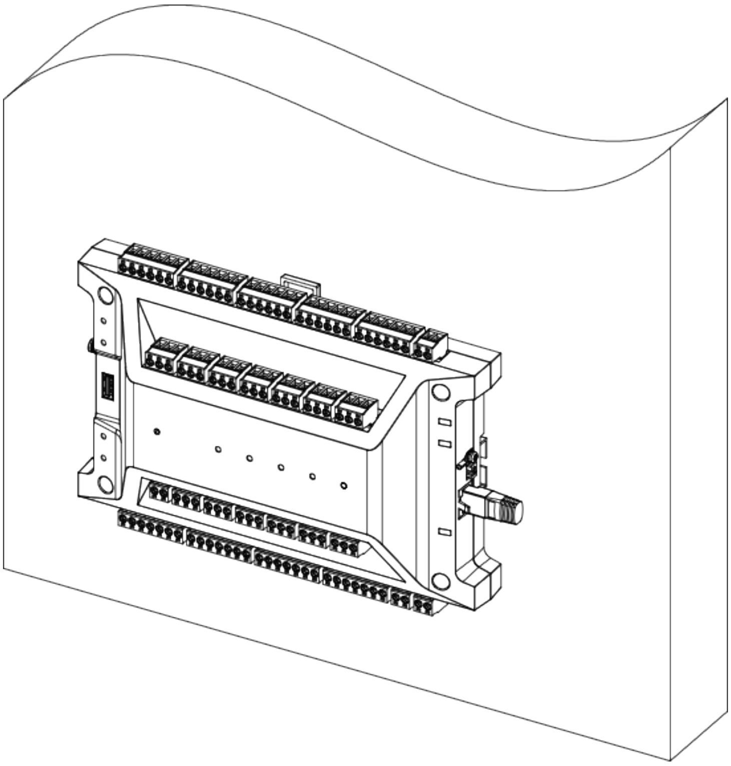


Figure 4-6 Complete Installation

Chapter 5 Settings

Hardware Initialization

Hold the restore button for 5s to initialize the hardware.

Fire Relay NO/NC

The position of the fire jumper cap position and the related NO/NC status are as follows:

Note

This operation requires disassembling the upper and lower shells of the device, which is recommended by a professional.

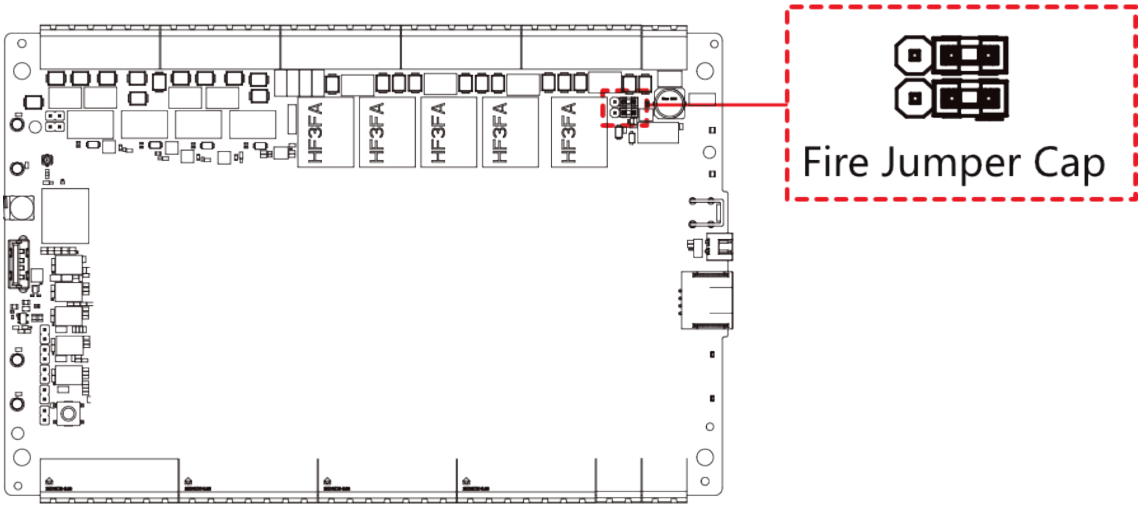
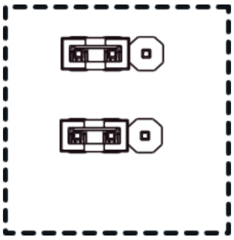
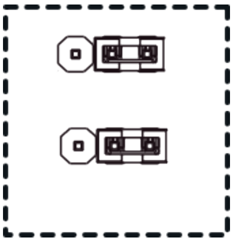


Figure 5-1 Fire Jumper Cap Position Description

Normally Closed Status	Normally Open Status
	

Chapter 6 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

6.1 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

   Note

   Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a 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.

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

6.2 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.

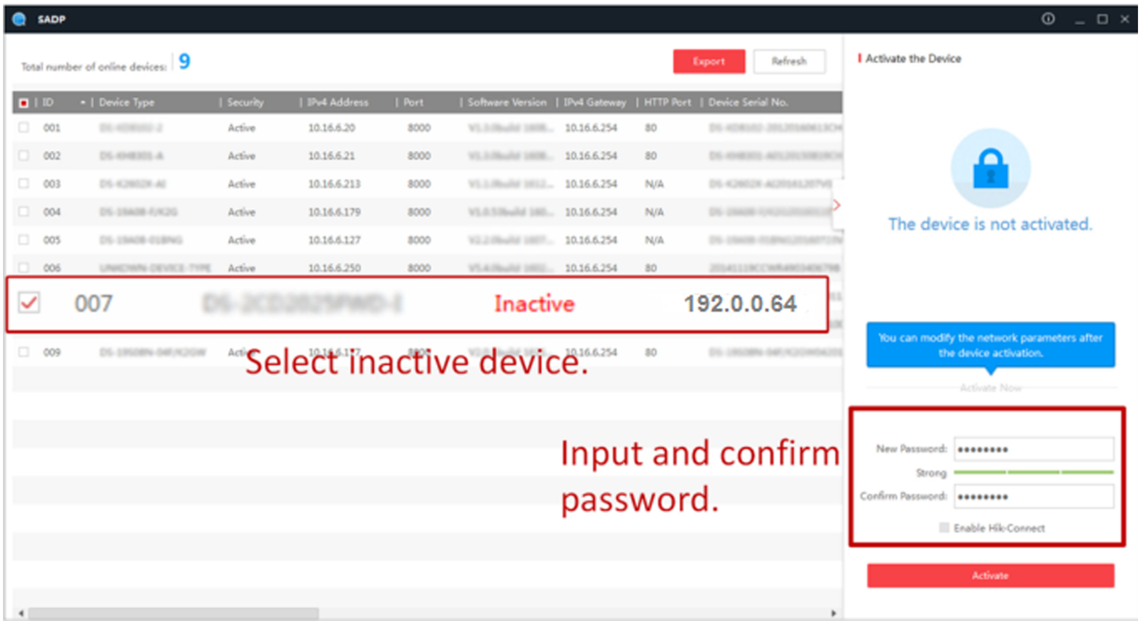
Caution

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	UNKNOWN-DEVICE-TYPE	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑	007	[illegible]	Inactive	192.0.0.64					
☐	009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ●●●●●●●●

Strong

Confirm Password: ●●●●●●●●

☐ Enable Hik-Connect

Input and confirm password.

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.

Chapter 7 Typical Application

The typical application for access controller, access module, lock and platform is as follows.

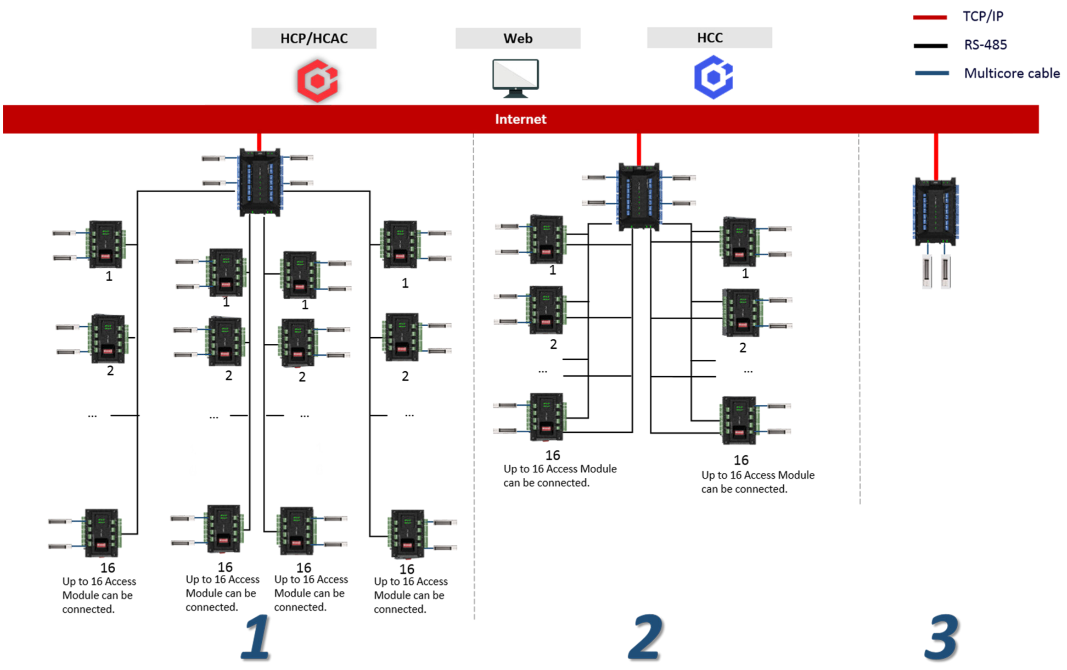

TCP/IP
RS-485
Multicore cable
HCP/HCAC
Web
HCC
Internet
1
2
...
16
Up to 16 Access Module can be connected.
Up to 16 Access Module can be connected.
1
2
3

Figure 7-1 Typical Application

1	No RS-485 redundant protection max. 128 doors. **Note** The DS-K2704X series support up to 128 doors; K2702X series support up to 126 doors; K2701x series support up to 125 doors.
2	With RS-485 redundant protection max. 64 doors.
3	Max. 4 doors.

Chapter 8 Quick Operation via Web Browser

8.1 Set Security Question

If you forget the device activation password, you can change the password via security questions. Set the security questions before configuration.

Click in the top right of the web page to enter the **Change Password** page. You can click **Skip** to skip the step. Or select three questions to answer and click **Next**.

8.2 Select Language

You can select a language for the device system.

Click in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

After you change the system language, the device will reboot automatically.

8.3 Time Settings

Click in the top right of the web page to enter the wizard page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

Chapter 9 Operation via Web Browser

9.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

- Make sure the device is activated. For detailed information about activation, see Activation Chapter.
- It is recommended to log in through the Chrome browser.

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click ⚙ to enter the Configuration page.

9.2 Forget Password

If you forget the password when logging in, you can change the password by security questions.

On the login page, click **Forget Password**.

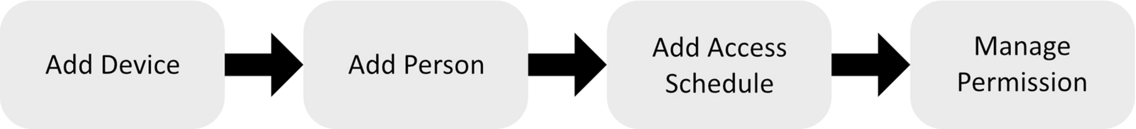
Answer the security questions.

Click **Next**, create a new password and confirm it.

9.3 Module Description

You can set Person management, device management, access control, system and maintenance parameters.

Click on the right side to open the module description page and view the description of each module. Click each hyperlink to jump to the corresponding settings page.
Configuration process is as follows:



Add Device → Add Person → Add Access Schedule → Manage Permission

9.4 Access Control Management

9.4.1 Overview

You can select the area and control the door status, view the device status, view the event, view the person information, network status, basic information, and device capacity. You can also enter the page from quick start part.

Login the web browser and enter the **Access Control → Overview** .

Door Status

Click **View More** to view and control all doors' status.

🔓 / 🔒 / ▣ / ▣

Set the door status as unlock, closed, remain open, or remain closed.

Quick Start

Click **Add Person**, **Add Device**, **System Settings**, or **System and Maintenance** on the upper-right of the page to quick enter the page to configure parameters.

Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation.

You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Device Status

View the other linked devices' status.

Person Information

View the person number, card number, fingerprint No.

Network Status

You can view the connected and registered status of wired network, wireless network, ISUP and cloud service.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, card, fingerprint, and event capacity.

9.4.2 Search Event

Click **Access Control → Event Search** to enter the Search page.

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

Note

The searched name should be up to 32 bits.

The results will be displayed on the right panel.

9.4.3 Access Point Management

Click **Access Control → Access Point Management**, you can view the doors associated with the access controller and the card readers associated with the doors.

Hover the mouse over the door or card reader on the right side of the interface, and you can click to configure the door parameters and the card reader authentication parameters.

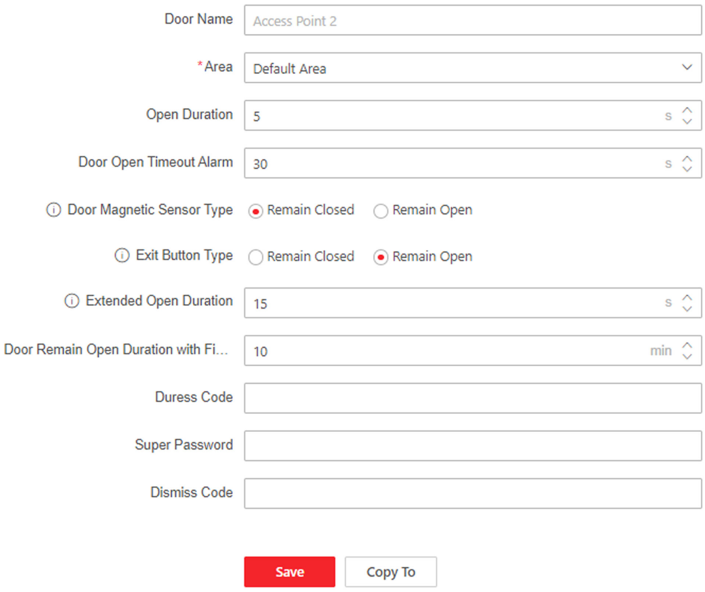
Set Door Parameters

Set the door parameters.

You can enter the door parameters page from the following 2 methods:

1. Click **Access Control → Access Point Management** . Hover the mouse on the door and click ⚙ to enter the door parameters page.
2. Click **Access Control → Configuration → Door Parameters** .

Click **Save** to save the settings after the configuration. Click **Copy to** to copy the door's parameters to other doors.



Door Name	Access Point 2
*Area	Default Area
Open Duration	5 s
Door Open Timeout Alarm	30 s
ⓘ Door Magnetic Sensor Type	● Remain Closed ○ Remain Open
ⓘ Exit Button Type	○ Remain Closed ● Remain Open
ⓘ Extended Open Duration	15 s
Door Remain Open Duration with Fi...	10 min
Duress Code	
Super Password	
Dismiss Code	

Figure 9-1 Set Door Parameters

Door Name

You can create a name for the door.

Area

Select an added area or click **Add Area** to add a new area for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Door Open Timeout Alarm

An alarm will be triggered if the door has not been closed within the configured time duration.

Door Contact Type

You can set the door contact as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Closed**.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Extended Open Duration

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

Door Remain Open Duration with First Person

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Duress Code

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

Super Password

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

Dismiss Code

When the alarm is triggered, you can enter the dismiss code to dismiss the alarm.

Note

The duress code and the super password should be different.

Set Authentication Parameters

You can enter the authentication parameters page from the following 2 methods:

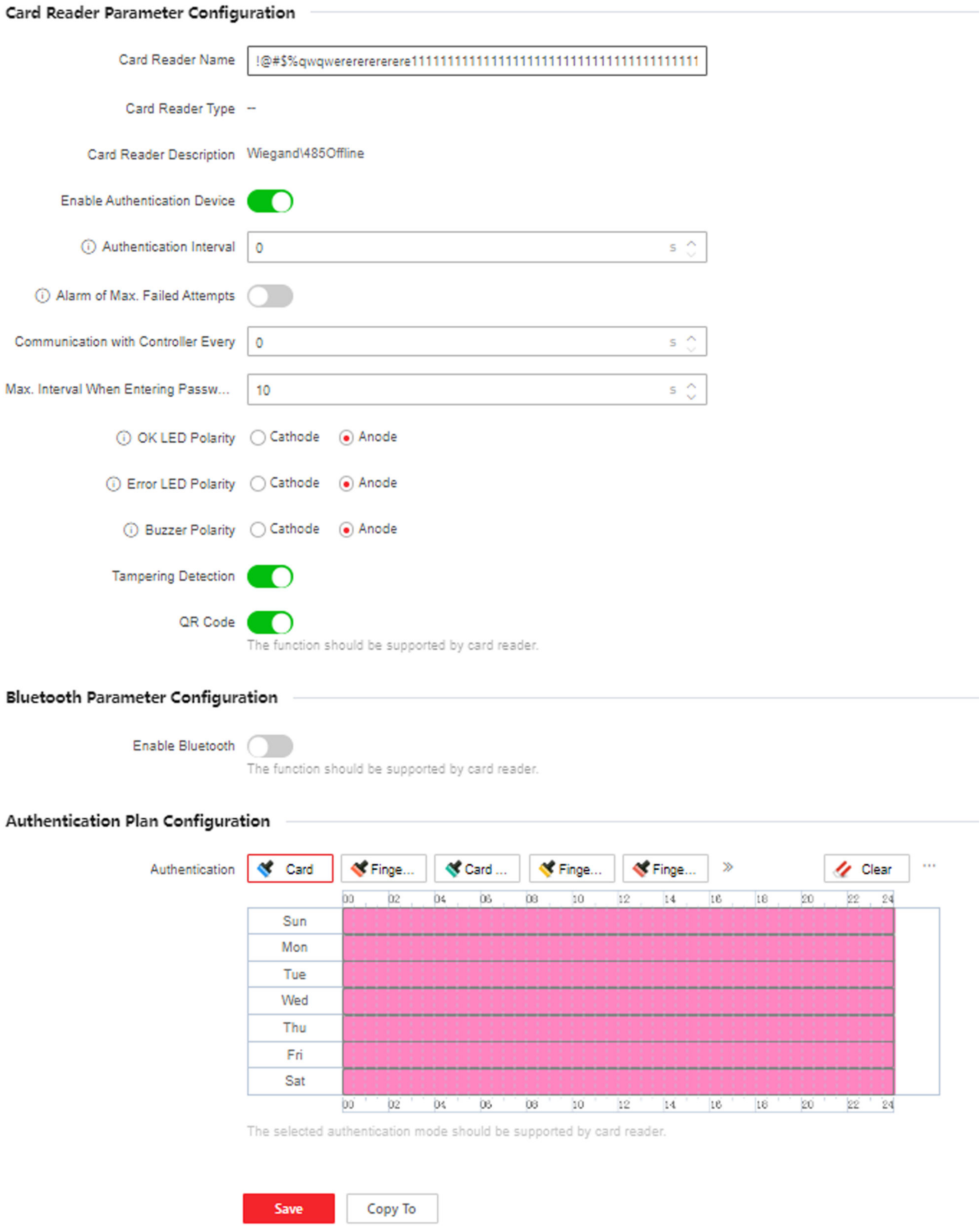
1. Click **Access Control → Access Point Management** . Hover the mouse on the card reader and click ⚙ to enter the authentication parameters page.

2. Click **Access Control → Configuration → Authentication Parameters** .

Click **Save** to save the settings after the configuration. Click **Copy to** to copy the card reader's parameters to other card readers.

Note

The functions vary according to different models. Refers to the actual device for details.



Card Reader Parameter Configuration

Card Reader Name: !@#$%qwqwererererere1111111111111111111111111111111111111111

Card Reader Type: --

Card Reader Description: Wiegand\485Offline

Enable Authentication Device: on

Authentication Interval: 0 s

Alarm of Max. Failed Attempts: off

Communication with Controller Every: 0 s

Max. Interval When Entering Passw...: 10 s

OK LED Polarity: ○ Cathode ● Anode

Error LED Polarity: ○ Cathode ● Anode

Buzzer Polarity: ○ Cathode ● Anode

Tampering Detection: on

QR Code: on

The function should be supported by card reader.

Bluetooth Parameter Configuration

Enable Bluetooth: off

The function should be supported by card reader.

Authentication Plan Configuration

Authentication: Card | Finge... | Card ... | Finge... | Finge... | » | Clear

The selected authentication mode should be supported by card reader.

Figure 9-2 Set Authentication Parameters

Card Reader Parameter Configuration

Card Reader Name

Create a name for the card reader.

Card Reader Type/Card Reader Description

View the card reader's type and description.

Enable Authentication Device

Enable the authentication function.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

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

Max. Authentication Failed Attempts

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

Communication 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.

Max. Interval When Entering Password

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

OK LED Polarity/Error LED Polarity/Buzzer Polarity

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

Tampering Detection

Enable the anti-tamper detection for the card reader.

QR Code

Enable the function and the card reader can recognize the QR code for authentication.

Note

The function should be supported by the card reader.

Bluetooth Parameter Configuration

Enable Bluetooth

Enable the bluetooth function and the you can use the bluetooth function (e.g. opening door) on the card reader.

Device Name/Transmitting Power

Edit the card reader's name and its transmitting power.

Open Door via Bluetooth

Enable the function and you can open the door via bluetooth through App. You should add the device to the App before use the function.

Authentication Plan Configuration

Set the authentication schedule for the card reader.

Select an authentication type and drag the time duration on the time schedule table to draw the authentication duration.

Click **Clear** and drag a time duration to delete, or click ··· → **Clear All** to delete all time durations.

Set Smart Parameters

Click **Access Control → Configuration → Smart → Smart** .

Note

- The functions vary according to different models. Refers to the actual device for details.
- After configuring the general parameters, all card readers will take effect.

Click **Save** to save the settings after the configuration.

Fingerprint Recognition

The device support recognition fingerprint after the function is enabled.

Fingerprint Security Level

Select the fingerprint security level.

The higher is the security level, the lower is the false acceptance rate (FAR).

9.4.4 Permission Management

You can set access permission schedule template, holiday schedule template, and set access permission.

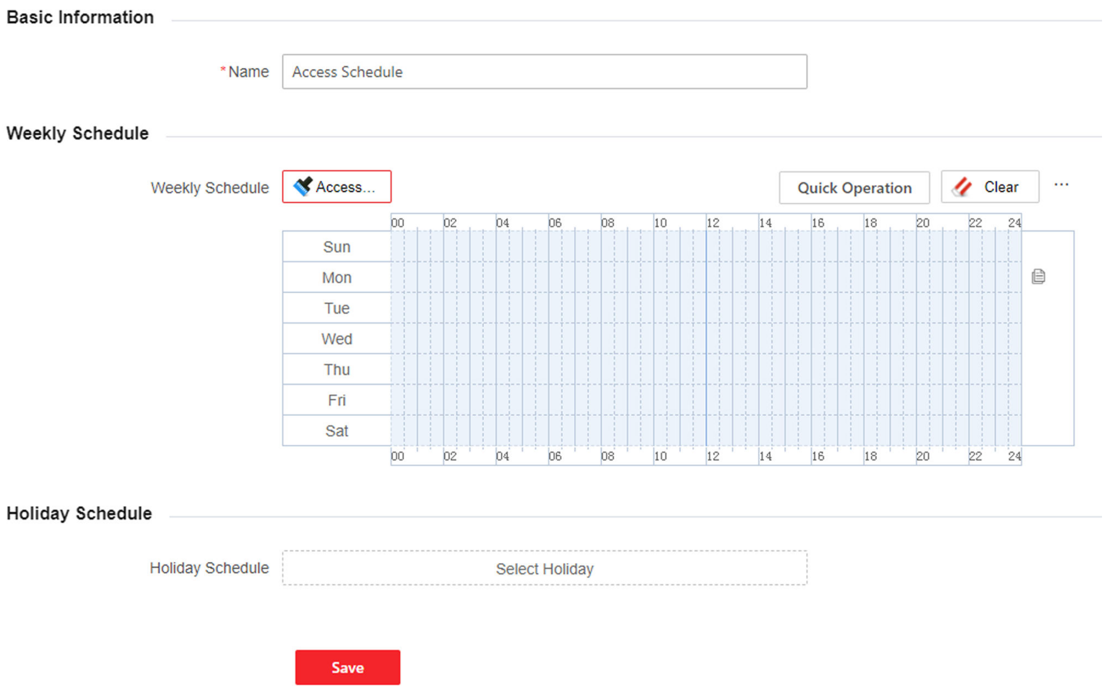
Configure Schedule Template

Set Access Schedule Template

Access schedule templates are used to set authorized passing time for people. The device provides three default access schedule templates: all-day template, workday template, and weekend template. You can also add custom templates according to actual needs.

Steps

1. Click **Access Control → Permission Management → Access Plan Management → + Add**.



*Name: Access Schedule

Figure 9-3 Set Access Schedule Template

2. Set the template.

   Name

   Set the template name.

3. On the weekly schedule template, drag the cursor to draw on the time bar.

Note

You can set up to 8 access periods per day.

4. **Optional:** Click **Clear**, and drag on the time bar to delete the corresponding time period.
5. **Optional:** Select Holiday Schedule.

Note

If the holiday schedule and weekly schedule conflict, the holiday schedule will be in priority.

1) Click **Select Holiday**.
2) Select holiday, and set holiday name and date.
3) Click **Add**.
4) Click and drag on the corresponding time bar to draw the valid access permission period.

Note

You can set up to 8 access periods per day.

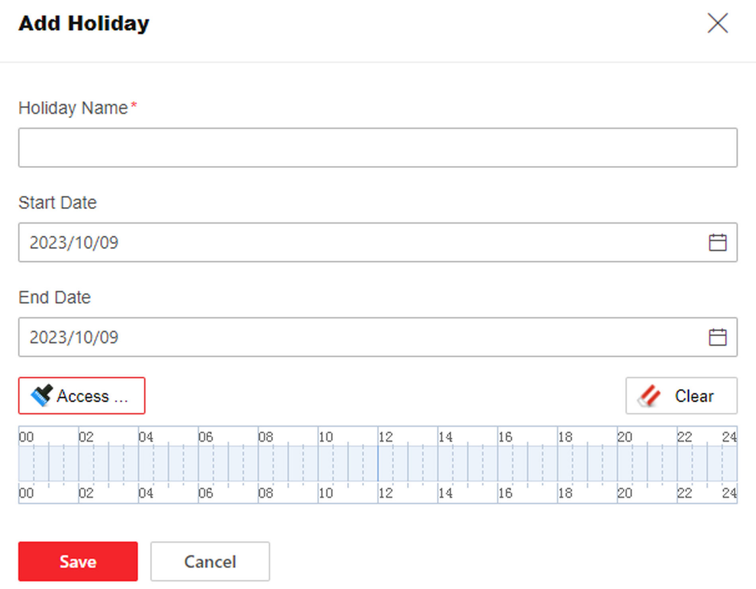
6. Click **Save.**

Set Holiday Schedule Template

You can set a legal holiday or a specified date as a holiday. The access permission of holiday is higher than other basic access permission.

Steps

1. Click **Access Control → Permission Management → Holiday Schedule Management → + Add**.



Add Holiday

Holiday Name*

Start Date: 2023/10/09

End Date: 2023/10/09

Figure 9-4 Set Holiday Schedule Template

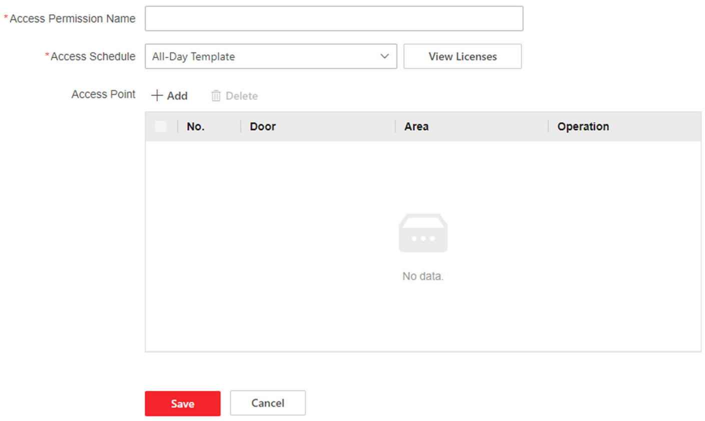
2. Enter holiday name.
3. Set the start date and end date of holiday.
4. Click and drag on the corresponding time bar to draw the valid access permission period.
5. **Optional:** Move the cursor or click **Clear** to adjust the time period that has been drawn.
6. Click **Save**.

Set Access Permission

Access permission can be defined, and it can be convenient to group according to access points and manage uniformly.

Steps

1. Click **Access Control → Permission Management → Manage Access Permission → +Add**.



*Access Permission Name

*Access Schedule: All-Day Template

Figure 9-5 Set Access Permission

2. Enter **Access Permission Name**.
3. Select Access Schedule. You can click **View** on the right side to view the access period of different template.
4. Click **+ Add** to check the access point, and click **Save**.
5. Click **Save**.

9.4.5 Access Control Application

Open Door with First Person

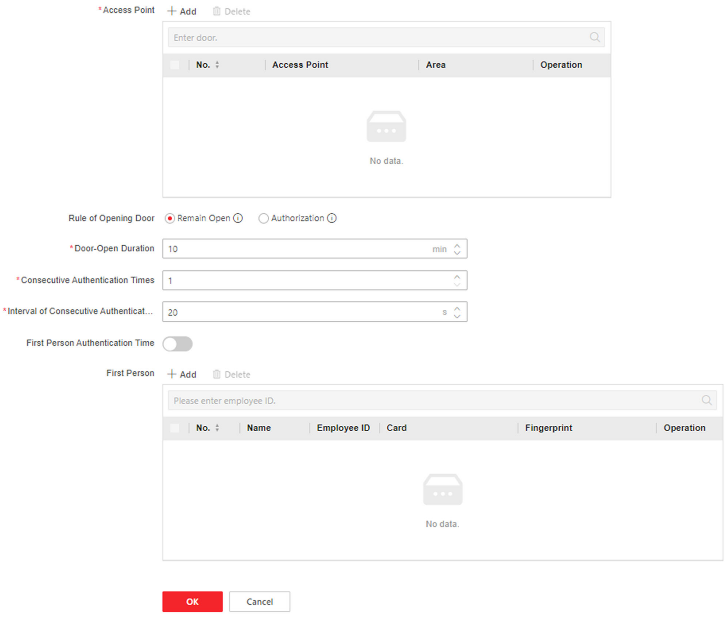
The first person can be set to open the door, that is, after a specific person (the first person) uses credentials (such as cards, fingerprints, and faces) to authenticate, other personnel can pass directly, or use credentials to pass, which is often used in scenarios where a large number of people pass.

Before You Start

The device is added. For more information about how to add a device, see ***Device Management*** .

Steps

1. Click **Access Control → Access Control Application → Open Door with First Person → +Add**.



*Access Point

Rule of Opening Door: ● Remain Open ○ Authorization

*Door-Open Duration: 10 min

*Consecutive Authentication Times: 1

*Interval of Consecutive Authenticat...: 20 s

First Person Authentication Time: ○ (off)

First Person

Figure 9-6 Open Door with First Person

2. Click **+ Add**, and select the access point.
3. Set the parameters of first person.

Rule of Opening Door

Remain Open

After the first person is authenticated, the door opening status will last for a period of time, and other personnel can pass without authentication during this time period. This function is often used in scenarios where a large number of people pass, such as group visitors entering tourist attractions. The door-open duration can be configured.

Authorization

The mode is applicable to places with high security requirements. Only after the person configured with access permission passes through, other persons can pass through after authenticating with credentials.

Consecutive Authentication Times

The number of times that authentication is valid during consecutive authentication periods.

Interval of Consecutive Authentication

The interval between which the same person can repeat authentication. Repeated authentication by the same person at the configured interval is considered invalid.

First Person Authentication Time

You can set the start time and effective time periods of the first person.

4. Add the first person. Click **+ Add**, and select the first person.
   1) Click **+ Add**.
   2) Select the first person.

3) Click **OK**.

5. Click **OK**.
6. **Optional:** Select multiple first personnel and click **Delete** to delete related settings.

Multi-Factor Authentication Settings

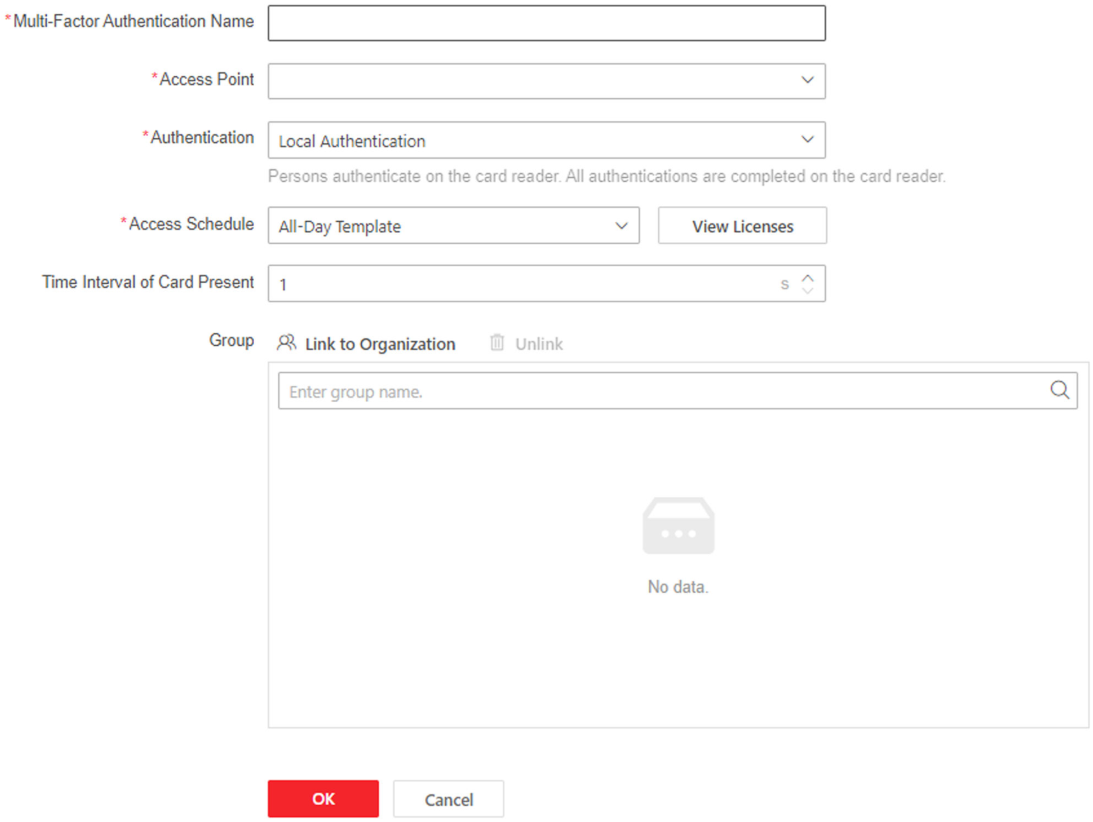
Only after authenticating according to the multi-factor authentication rule, can persons in multi-factor authentication groups open the door.

Before You Start

- The device is added. For more details, see ***Device Management*** .
- The access point is added. For more details, see ***Access Point Management*** .
- The access schedule is set. For more details, see ***Permission Management*** .

Steps

1. Click **Access Control → Access Control Application → Multi-Factor Authentication**.



*Multi-Factor Authentication Name

*Access Point

*Authentication: Local Authentication

Persons authenticate on the card reader. All authentications are completed on the card reader.

*Access Schedule: All-Day Template

Time Interval of Card Present: 1 s

Group

Figure 9-7 Multi-Factor Authentication Settings

2. Click **Group Management**.
   1) Click **+**, and enter the group name.
   2) Click **+ Add**, select person, and click **OK**.

3) Click **OK**. The added group will show in the list on the left side of the page. When you select a group, the information about the people in the group will show on the right side of the page.
4) **Optional:** Select a group, click **+ Add**, and you can add more group members. Select and click **OK**.

3. Add multi-factor authentication rule.
   1) Click **+ Add**.
   2) Set multi-factor authentication parameters.

Multi-Factor Authentication Name

Create the multi-factor authentication name.

Access Point

In the drop-down box, select the access point that needs to be applied in the relevant multi-factor authentication.

Authentication Mode

Local Authentication

Personnel can only open the door after authenticating locally on the device in accordance with the authentication rules.

Local Authentication + Remotely Opening Door

Personnel can only open the door after after authenticating locally on the device in accordance with the authentication rules and authenticating via platform remotely.

Local Authentication + Super Credential

Personnel can only open the door after after authenticating locally on the device in accordance with the authentication rules and authenticating via super credential.

Access Schedule

Select the access schedule. Click **View** to see the template details.

Time Interval of Card Present

Configure the time interval between authentication for different authenticating personnel.

Group

Click **Link to Organization**, and select the group. In the added group, you can drag ☰ in the operation bar to adjust the order, or configure the Number of Persons for Authentication. It needs to be authenticated according to the order in the list and the **Number of Persons for Authentication** when authenticating.

   3) Click **OK**.

4. **Optional:** Select the unnecessary multi-factor authentication, and click **Delete**.
5. Click 🗎 to view the access schedule details.

Multi-Door Interlocking Settings

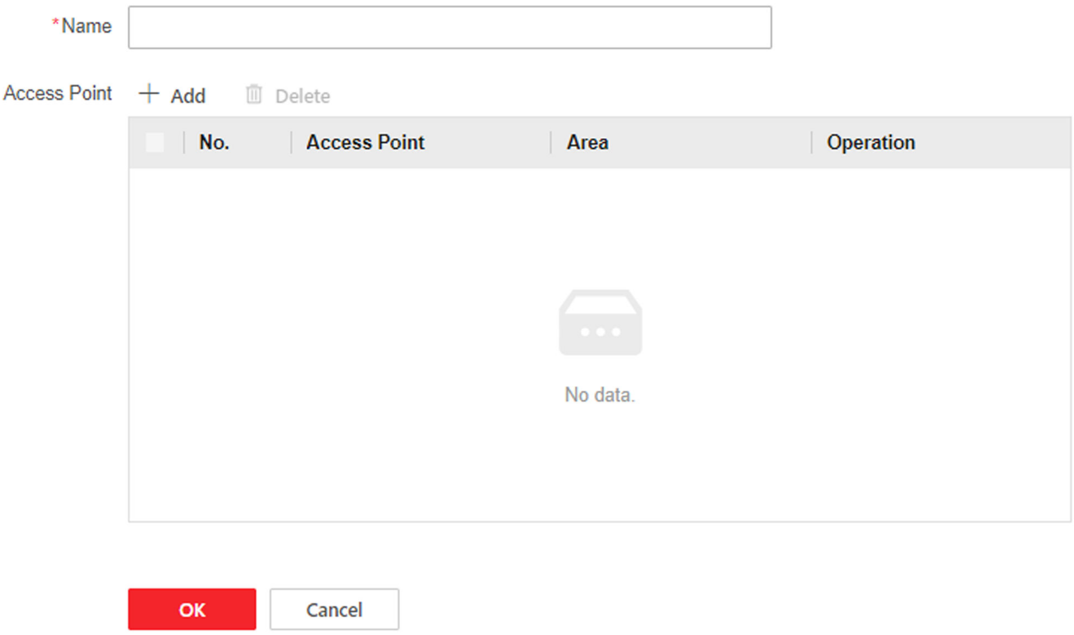
Multi-door interlocking refers to multiple doors forming an interlocking combination, in which one door can only be opened at most at the same time, and the other doors must be closed.

Before You Start

- The device is added. For more details, see ***Device Management*** .
- The access point is added. For more details, see ***Access Point Management*** .

Steps

1. Click **Access Control → Access Control Application → Multi-Door Interlocking → + Add**.



*Name

Access Point

□	No.	Access Point	Area	Operation

Figure 9-8 Multi-Door Interlocking Settings

2. Create the name.
3. Click **+ Add**, and select the access points.
4. Delete unnecessary access points.
   - Select unnecessary access points in the list and click **Delete** to delete access points in batch.
   - Click 🗑 to delete the single access point.
5. Click **OK**.
6. You can edit and delete the created multi-door interlocking.
   - Select the multi-door interlocking, and click ✎ to edit.
   - Select the multi-door interlocking, and click 🗑 to delete.
   - Select the multi-door interlocking, and click **Delete** to delete in batch.

Anti-Passback Settings

Personnel must follow the set route for one-way passing. If you do not follow this route for authentication, the door will not open. If a person does not enter the door after swiping the card, the door will not open when swiping the card again, and the same will apply when going out.

Before You Start
The device is added. For more details, see ***Device Management*** .

Steps

1. Click **Access Control → Access Control Application → Anti-Passback**.

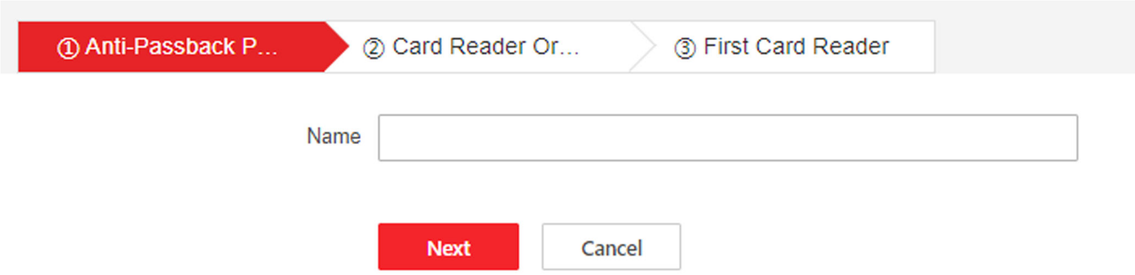


Figure 9-9 Anti-Passback Settings

2. Add anti-passback route.
   1) Enter name and click **Next**.
   2) Set card reader order. Click **Add** and select the card reader.
   3) Click ⊕ to add another card reader.
   4) Repeat substep 3 to add multiple card readers.
   5) **Optional:** Click a card reader to replace or remove the card reader.
   6) Click **Next**.
   7) Set first card reader.

   Disable

   - If the passed card reader of last person recorded by the device is not set anti-passback or the person is a new user, the anti-passback is authenticated to pass.
   - If the passed card reader of last person recorded by the device has set anti-passback, it is necessary to check whether the current card reader is in the sequent anti-passback card reader after the last passed card reader, if so, the anti-passback is authenticated to pass; if not, the anti-passback authenticating failed.

   Select One Card Reader as First Card Reader

   - In any case, the personnel swipe the first card reader and the anti-passback will be authenticated to pass.
   - If the passed card reader of last person recorded by the device has set anti-passback, it is necessary to check whether the current card reader is in the sequent anti-passback card reader after the last passed card reader, if so, the anti-passback is authenticated to pass;

If not, the anti-passback authenticating failed. And the anti-passback authenticating failed in any other cases.

Note

- If you violated the anti-passback rule, you should swipe the card again from the first card reader.
- Superusers do not follow the above rules.
- Up to 64 doors can be applied in anti-passback.

3. **Optional:** Set anti-passback parameter.
   1) Click **Anti-Passback Parameter**.
   2) You can enable **Forgive Anti-Passback**, and set the Forgive Anti-Passback schedule.

      Forgiving Mode

      Forgive Anti-Passback Regularly

      Set the time of Forgive Anti-Passback, the system will clear the anti-passback at the set time. After clearing, the personnel need to follow the anti-passback rules again, starting from the first card reader to authenticate.

      Delay Forgiving Anti-Passback

      Set the time of **Forgiving Anti-Passback**. The system starts timing after the person swipes the card, and after the set delay time, the anti-passback will be cleared. After clearing, the personnel need to follow the anti-passback rules again, starting from the first card reader to authenticate.

      Non Anti-Passback Period

      After selecting the effective time, drag to draw the non anti-passback period on the time bar, and the anti-passback will not take effect within the configured time period.

      Click **Clear**, and drag on the time bar to delete related time period.

      Click ··· → **Clear All** to delete all time periods.
   3) Click **Save**.
4. You can edit, delete and view the created anti-passback.
   - Select the anti-passback, and click ✎ to edit.
   - Select the anti-passback, and click 🗑 to delete.
   - Select multiple anti-passback, and click **Delete** to delete in batch.
   - Select the anti-passback, and click 🗎 to view the anti-passback route.

Remain Open or Closed Settings

Set the time period by week during which the door(s) remains locked/unlocked.

Before You Start

- The device is added. For more details, see ***Device Management*** .
- The access point is added. For more details, see ***Access Point Management*** .

Steps

1. Click **Access Control → Access Control Application → Remain Open or Closed**.

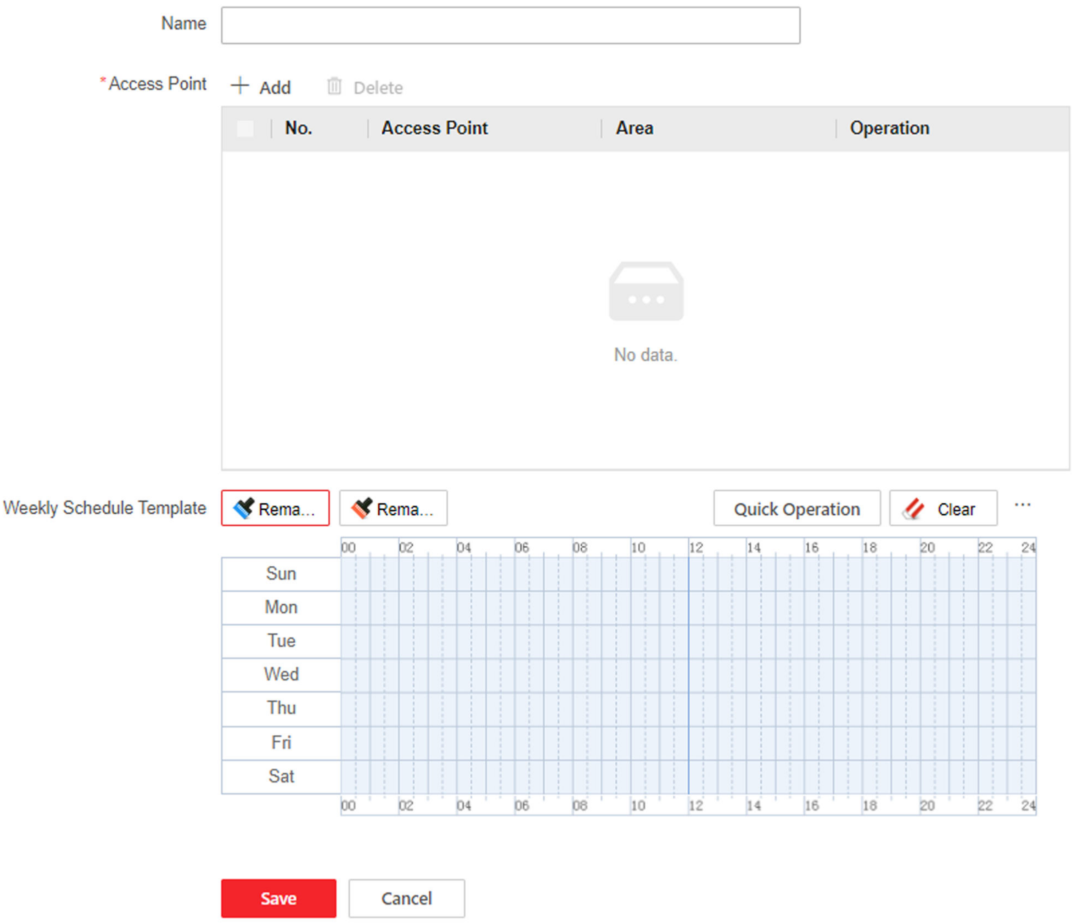


Figure 9-10 Remain Open or Closed Settings

2. Click **+ Add**.
3. Add the access point.
   1) Click **+ Add**.
   2) Select the access point, and click **OK**.
   3) You can click 🗑 to delete single access point or click **Delete** to delete in batch.
4. Set weekly schedule template.
   1) Draw time periods of Remain Open or Closed.
   - Click **Remain Open** or **Remain Closed**, and drag over the time bar of the periods that need to be remain open or closed.
   - Select **Remain Open** or **Remain Closed**, click **Quick Operation**, and click **All-Day Schedule**, **Work Schedule**, **Weekend Schedule** and the time period will be drawn automatically.

   1) **Optional:** Click **Clear**, and drag on the time bar to delete the corresponding time period. Click ··· **→ Clear All** to delete all time periods.
5. Click **Save**.

9.5 Person Management

9.5.1 Add Organization

After you add an organization, you can add people to the corresponding organization.

Steps

1. Click **Person Management** to enter the settings page.
2. Click **+** on the left side of the page and select the parent organization.
3. Create the organization name.
4. Click **Save**.

   The added organization will be listed in the selected parent organization.
5. **Optional:** Edit / Delete
   - Click an organization, and then click ✎ to edit the organization information.

     Select people and click **Delete** to delete the information in batch.

     Click **Clear All**, and all person information will be deleted.
   - Click an organization and click 🗑 to delete that organization information.

9.5.2 Add Person

Add the person's information, including the basic information, certificate, authentication and settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.

Add the person's basic information, including the employee ID, the person's name, and person type.

Note

- If you select **Visitor** as the person type, you can set the visit times.
- Letters are allowed in the employee ID. Up to 32 bits are allowed.
- Up to 128 bits are allowed in the name.

Click **Add** to save the settings.

Click **Save and Configure** to save the settings and continue to add next person.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.

Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.

Click **Add** to save the settings.

Click **Save and Configure** to save the settings and continue to add next person.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Configuration**. If select the Collection Device as **Card Enrollment Station**, you should select the device model, card type, set buzzing, M1 card encryption, and sector. Click **OK** to save.

Note

If select the Collection Device as **Card Enrollment Station**, click **Download** to download the plug-in to view the device status. During the installation, you should close the web page.

If select the Collection Device as **Card Reader**, you should select the card reader from the drop-down list. Click **OK** to save.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.
Click **Add** to save the settings.
Click **Save and Configure** to save the settings and continue to add next person.

Add Fingerprint

Note

Only devices supporting the fingerprint function can add the fingerprint.

Click **Person Management → Add** to enter the Add Person page.
Click **Configuration**. If you select**USB Fingerprint Recorder**, you can click **Download**to download the plug-in and view the status. Or select **Fingerprint and Card Reader** and select a card reader from the drop-down list. Click **OK** to save.

Note

During the installation, you should close the web page.

Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.
Click **Add** to save the settings.
Click **Save and Configure** to save the settings and continue to add next person.

Note

The plugin for adding card or fingerprint via USB is only available in Windows.

Add PIN

Before configuring PIN, it is necessary to clarify whether the PIN is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

Make sure you have already set the PIN mode as **Device-Set Personal PIN** in ***Set Password Mode*** .
Click **PIN Mode** on the page to go to configure.
Click **Person Management → Add** to enter the Add Person page.
Set the PIN. Or click **Auto Generate** to generate a PIN automatically.
Click **Add** to save the settings.
Click **Save and Configure** to save the settings and continue to add next person.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
Click **Add** to save the settings.
Click **Save and Configure** to save the settings and continue to add next person.

Permission Management

Before you start:

- You have already add the device. For details, see ***Device Management*** .
- You have already complete access point management. For details, see ***Access Point Management*** .
- You have already complete the access permission management. For details, see ***Permission Management*** .

Click **Person Management → Add** to enter the Add Person page.
Set the permission parameters.

Permission Type

By Permission Group

Click **Allocate** and select an added access permission. The person will contain the checked access permission. If you have not added the access permission in advance, you can click **Add Access Permission** to add. For details, see ***Permission Management*** . Click **OK**.

By Access Point

Click **Allocate** and select the access schedule. Click**Add** to add the access points. The person will contain the permissions of the access point within the access schedule. Click **OK**.

Extend Door Opening

The person related door will close after the configured time duration. You should go to ***Set Door Parameters*** to set the **Extended Open Duration**. Click **Door Parameters** to go to the configuration page.

Click **Add** to save the settings.
Click **Save and Configure** to save the settings and continue to add next person.

Edit/Delete/Search Person

Click **Person Management** to enter the page.
Select a person and click ✎ to edit the person's information.
Select a person and click 🗑 to delete the person information.

Select multiple person, click **Delete** can delete person in batch.
Click **Clear All** to delete all person information.
Click ⊞ or ☰ to switch the viewing method.
Enter the person's employee ID and select the credential status and click **Filter** to search. Click **Reset** to reset all conditions.
Check **Show Sub Organization**, all persons in the sub organizations will be displayed.

9.6 Device Management

9.6.1 Search Not Added Device

The system can automatically search for not added access modules that have been connected to the access controller.

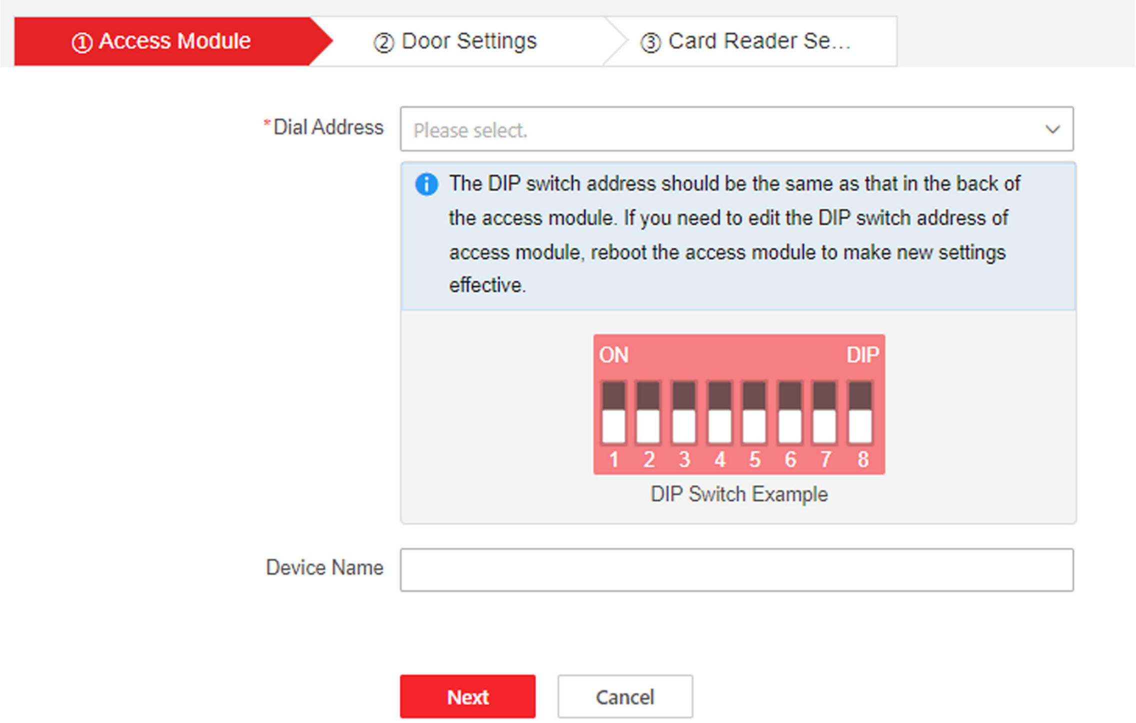
Click **Device Management → Search Not Added Device**. The searched not added access modules will be displayed in the list of the page.
Click + in the action bar to add an access module to the access controller.

9.6.2 Add Access Module

Add access module manually.

Before You Start
Make sure that the area has been added. For more details, see ***Area Management*** .

Steps
1. Click **Device Management** to enter the settings page.



*Dial Address: Please select.

The DIP switch address should be the same as that in the back of the access module. If you need to edit the DIP switch address of access module, reboot the access module to make new settings effective.

Device Name:

Figure 9-11 Add Access Module

2. Select the dial address of the access module, and set the DIP switch of the access module to be consistent with the one shown in the picture.

Note

After adding or modifying the dialing address of the access module, you need to reboot the access module to take it effect.

3. Set the door parameters, and click **Next**.

Select Door of Access Module

According to the door actually controlled by the access module, select **1** or **2**.

Door Name

Create the door name associated with the access module.

Area

Choose the area from the drop-down list. If you have not created an associated area in advance, click **Add Area** to create.

Open Duration

Set the action time after the associated door is unlocked. If the door is not opened within the set time, the door will lock automatically. The range can be set from 1 to 255 s.

Door Magnetic Sensor Type

The door magnetic sensor can be controlled as Remain Closed or Remain Open. Under normal circumstances, it is Remain Closed (except for special needs).

Exit Button Type

Under normal circumstances, it is Remain Open (except for special needs).

Extended Open Duration

For the elderly or children with reduced mobility, by set Extended Open Duration, the door magnetic sensor opening time after swiping card can be appropriately delayed.

4. Set the card reader parameters associated with the access module.

Select Door of Access Module

According to the door actually controlled by the access module, select **1** or **2**.

Select Card Reader

Select Enter or Exit according to the actual card reader location.

Card Reader Name

Create the card reader name.

Card Reader Description

View the card reader description. Read Only

QR Code

If the card reader supports the QR code authentication function, this function can be enabled, then on the card reader, it can be carried out through the QR code authentication.

Enable Bluetooth

If the card reader supports the Open Door via Bluetooth function, this function can be enabled, then on the card reader, the door can be opened via bluetooth.

Authentication Plan Configuration

Set the authentication plan of different authentication type. You can set different authentication type in different time periods.

Select the authentication type (you can select more than one), and draw the required time period in the time bar below, during which you can perform the selected authentication type.

Click **Clear** and select the time period that has been drawn in the time bar to clear the plan.

Click ··· → **Clear All** to clear all time periods.

5. Click **OK**.
6. **Optional:** Other Operations

Icon	Description
✎	You can edit the access module.
🗑	You can delete the access module.
⟳	You can restart the access module.
©	You can restore the access module to the factory settings.

⇧ You can upgrade the access module. Select a local upgrade package to upgrade.

9.6.3 Area Management

After you create an area, you can add access control points to the area to manage them in a partition.

Steps

1. Click **Device Management → Area Management**.
2. Click **+** on the left side of the page, select a parent area, and create the area name.
3. Click **Save**.

   The added area will be listed in the selected parent area.
4. **Optional:** Edit / Delete
   - Select the area and click ✎ to edit the information.

     Select multiple personnel, and click **Delete** to delete the information of person in batch.

     Click **Clear All** to delete information of all personnel.
   - Select the area, and click 🗑 to delete the information of area.

9.7 System and Maintenance

9.7.1 View Device Information

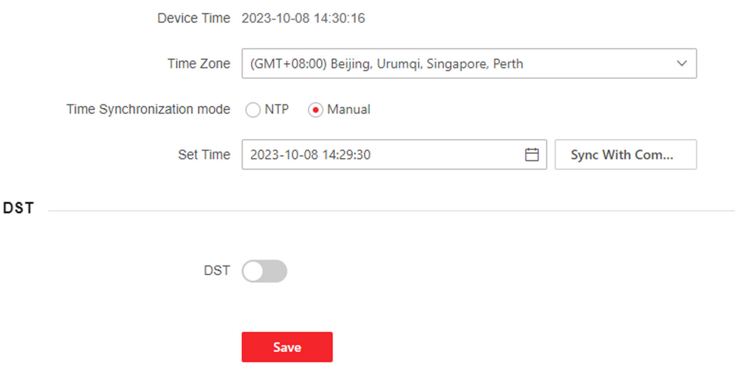
View the device name, language, model, serial No., version, number of channels, IO input, IO output, RS-485, alarm output, and device capacity, etc.

Click **System and Maintenance → System Configuration → System → System Settings → Basic Information** to enter the configuration page.
You can the device name, language, model, serial No., version, number of channels, IO input, IO output, RS-485, alarm output, and device capacity, etc.

9.7.2 Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

Click **System and Maintenance → System Configuration → System → System Settings → Time Settings** .



Device Time 2023-10-08 14:30:16

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Synchronization mode ○ NTP ● Manual

Set Time 2023-10-08 14:29:30

Figure 9-12 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Synchronization Mode

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server IP Address/NTP Port/Interval

You can set the server IP address, NTP port, and interval.

9.7.3 Set DST

Steps

1. Click **System and Maintenance → System Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

9.7.4 Change Administrator's Password

Steps

1. Click **System and Maintenance → System Configuration → System → User Management** .
2. Click ✎ .

3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

⚠ **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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

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

9.7.5 Account Security Settings

You can change the security questions and answers, or the email address for the device. After change the settings, once you forgot the device password, you should answer the new questions or use the new email address to reset the device password.

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → Account Security Settings** .
2. Change the security questions or email address according your actual needs.
3. Enter the device password and click **OK** to confirm changing.

9.7.6 View Online User

You can view online users.

Click **System and Maintenance → System Configuration → System → User Management → Online Users** .

You can view online users' information including name, type, IP Address and operation time. Click **Refresh** to refresh the page.

9.7.7 View Open Source Software License on PC Web

On the main page of the device PC Web, click ⓘ **→ Open Source Software Statement** , to view the device license.

9.7.8 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **System and Maintenance → System Configuration → System → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

9.7.9 Network Settings

Set Basic Network Parameters

Click **System and Maintenance → System Configuration → Network → Network Settings → TCP/IP** .

Set the parameters and click **Save** to save the settings.

NIC Type

Select a NIC type from the drop-down list.

DHCP

If uncheck the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, Mac address, and MTU.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Network Settings → Wi-Fi** .
2. Check **Wi-Fi**.
3. Select a Wi-Fi
   - Click 🔗 of a Wi-Fi in the list and enter the Wi-Fi password.

- Click **Add** and enter a Wi-Fi's name, password, and encryption type. Click **Connect**. When the Wi-Fi is connected, click **OK**.

4. **Optional:** Set the WLAN parameters.
   1) Set the IP address, subnet mask, and default gateway. Or enable **DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.
5. Click **Save**.

Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening, RTSP and Server port parameters.

Click **System and Maintenance → System Configuration → Network → Network Service → HTTP(S)** .

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.

Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

Click **System and Maintenance → System Configuration → Network → Network Service → WebSocket(s)** .

View WebSocket and WebSockets port.

Set ISUP Parameters

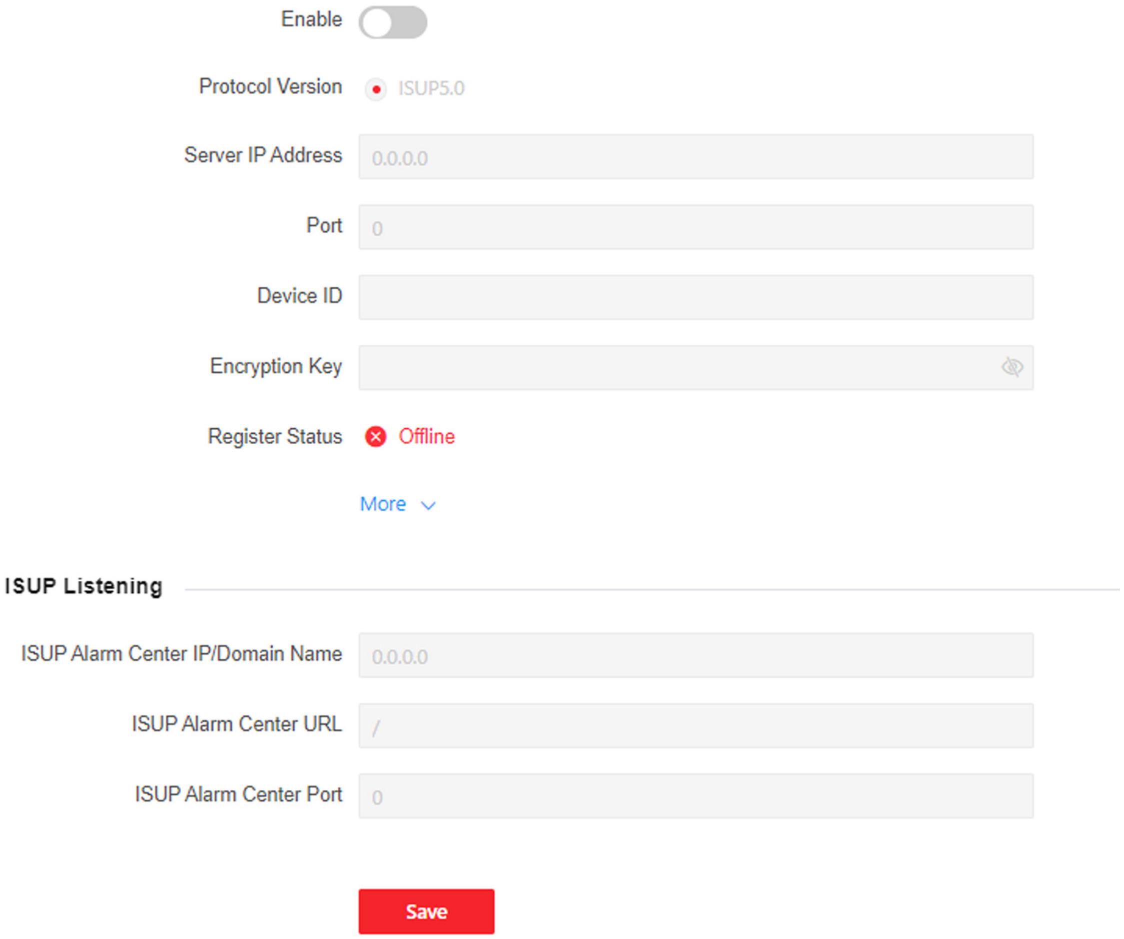
Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Device Access → ISUP** .



Enable

Protocol Version ● ISUP5.0

Server IP Address 0.0.0.0

Port 0

Device ID

Encryption Key

Register Status ⊗ Offline

ISUP Listening

ISUP Alarm Center IP/Domain Name 0.0.0.0

ISUP Alarm Center URL /

ISUP Alarm Center Port 0

Figure 9-13 Set ISUP Parameters

2. Check **Enable**.
3. View the ISUP version, set server IP address, port, device ID, encryption key and view the ISUP status.
4. **Optional:** Click **More** to set the network connection priority.
   1) Enable **WLAN** or **Wired Network** according to your actual needs.
   1) Hold and drag ☰ to adjust the access priority.
5. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
6. Click **Save**.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **System and Maintenance → System Configuration → Network → Device Access → Hik-Connect** to enter the settings page.

   Note

   Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. **Optional:** View the register status. Click **Refresh** to refresh the status.
6. **Optional:** Click **More** to set the network connection priority.

   1) Enable **WLAN** or **Wired Network** according to your actual needs.

   1) Hold and drag ☰ to adjust the access priority.

7. Click **View** to view device QR code. Scan the QR code to bind the account.

   Note

   8 to 32 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

8. Click **Save** to enable the settings.
9. **Optional:** Click **Refresh** to refresh the binding status.
10. Click **Save**.

9.7.10 Event Settings

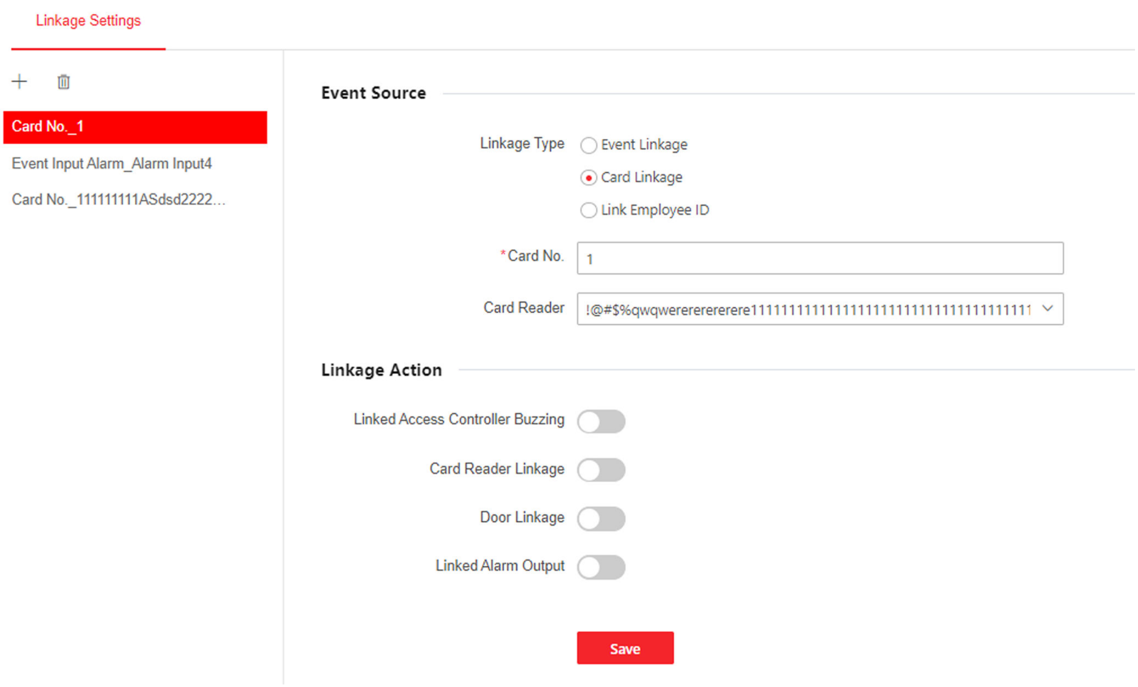
Set the event linkage and the alarm output paramters.

Event Linkage

Set linked actions for events.

Steps

1. Click **System and Maintenance → System Configuration → Event → Event Detection → Linkage Settings** to enter the page.



Linkage Settings

+ 🗑

Card No._1

Event Input Alarm_Alarm Input4

Card No._111111111ASdsd2222...

Event Source

Linkage Type ○ Event Linkage ● Card Linkage ○ Link Employee ID

*Card No. 1

Card Reader !@#$%qwqwerererererere111111111111111111111111111111111111

Linkage Action

Linked Access Controller Buzzing

Card Reader Linkage

Door Linkage

Linked Alarm Output

Save

Figure 9-14 Event Linkage

2. Click +
3. Set event source.
   - If you choose **Linkage Type** as **Event Linkage**, you need to select event types from the drop-down list.
   - If you choose **Linkage Type** as **Card Linkage**, you need to enter the card No. and select the card reader.
   - If you choose **Linkage Type** as **Link Employee ID**, you need to enter the employee ID and select the card reader.
4. Set linked action.

Linked Access Controller Buzzing

Enable **Linked Access Controller Buzzing** and select **Start Buzzing** or **Stop Buzzing** for the target event.

Card Reader Linkage

Enable **Card Reader Linkage** and click **Add** can check the card reader that will buzz. Click **Save**.

Set the card reader's buzzing action.

Click 🗑 to delete single card reader. Check the card readers and click **Delete** to delete in batch. Click **Batch Configure** to configure all card readers in the list.

Door Linkage

Enable **Door Linkage** and click **Add** can check the card reader that will buzz. Click **Save**.

Set the access point's action.

Click 🗑 to delete single card reader. Check the card readers and click **Delete** to delete in batch.

Linked Alarm Output

If the Linkage Type in the Event Source is **Card Linkage**, when enable **Linked Alarm Output**, you can set **Triggering Times Configuration**, **Triggering Times (Enable)**, and **Triggering Times (Disable)**.

If set **Triggering Times (Enable)** as 3, and **Triggering Times (Disable)** as 3, you can present the card that configured in the Event Source for 3 time to stop alarm when the following alarm output in the list is in open status. If the alarm output is in the disabled status, you can present the card for 3 times to trigger alarm.

Set the alarm output. Click **Add** and check the alarm outputs in the list and click **Save**.

Click ⚙ to set the alarm duration. Click **Save**.

Note

After the configuration is completed, the configuration of the same output linked to other actions will also be changed.

Continuous Alarm

The alarm output device will continuously in the alarm status.

Custom Alarm Duration

You should set the custom duration. The alarm output device will be in the alarm status for the configured time duration.

Note

Range: from 0 to 5999s.

5. Click **Save**.

Alarm Settings

Set the device's alarm output parameters.

Click **System and Maintenance → System Configuration → Event → Alarm Settings → Alarm Output** .

Select an access point from the list on the left. Select a alarm output device No. Create a name for the alarm output device and set the alarm duration. Click **Save**.

Continuous Alarm

The alarm output device will continuously in the alarm status.

Custom Alarm Duration

You should set the custom duration. The alarm output device will be in the alarm status for the configured time duration.

Note

Range: from 1 to 5999s.

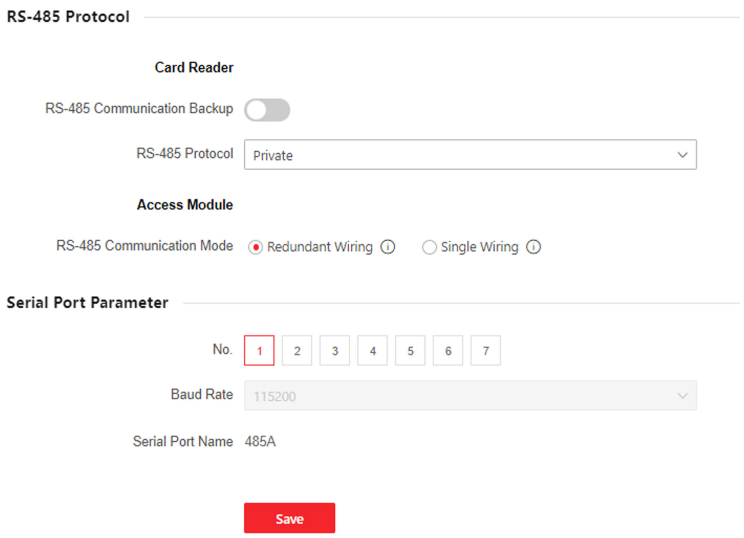
9.7.11 Access Configuration

You can set RS-485, Wiegand and host parameters.

Set RS-485 Parameters

You can set the RS-485 parameters including the peripheral, address, baud rate, etc.

Click **System and Maintenance → System Configuration → Access Configuration → RS-485** .



RS-485 Protocol

Card Reader

RS-485 Communication Backup: ○

RS-485 Protocol: Private

Access Module

RS-485 Communication Mode: ● Redundant Wiring ○ Single Wiring

Serial Port Parameter

No.: 1 2 3 4 5 6 7

Baud Rate: 115200

Serial Port Name: 485A

Figure 9-15 Set RS-485 Parameters

Click **Save** to save the settings after the configuration.

RS-485 Communication Backup

The controller and the access module can communicate via redundant wiring mode.

RS-485 Protocol

Select the RS-485 protocol from the drop-down list.

RS-485 Communication Mode

Redundant Wiring

When the access controller connects to the terminal (RS-485A/RS-485B/RS-485C/RS-485D) of the access module, RS-485A and RS-485B are a pair using redundancy wiring, and RS-485C and RS-485D are another pair. When one of the channels is disconnected, the access controller can communicate with another channel. No more than 32 access module(s) can be connected to the access controller.

Single Wiring

RS-485A to RS-485D are communication terminals of the access module. The RS-485E terminal on the access controller can be connected to RS-485A to RS-485D terminals via single wiring for data transmission. No more than 62 access module(s) can be connected to the access controller.

No.

Select the RS-485 No.

Baud Rate

The baud rate when the devices are communicating via the RS-485 protocol.

Serial Port Name

View the serial port name.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **System and Maintenance → System Configuration → Access Configuration → Wiegand Settings** .
2. Select a access point from the list on the left.
3. Set Wiegand parameters.

   No.

   Select Wiegand No. for parameters settings.

   Wiegand

   select to enable the card reader's Wiegand function.

   Wiegand Direction

   By default, the direction is **Input**.

   Wiegand Mode

   Select the Wiegand mode and the card reader can communicate with the controller by Wiegand 26/34 or other protocol.

Click **Auto Recognize**, enter card No. to recognize the Wiegand mode. Enter the Card No., and click **Start to Recognize**. Present the card on the related card reader. The system will show the Wiegand mode. Click **OK**.

If select **Custom**, you should set custom Wiegand parameters. Click **Custom Wiegand Settings**, and set the name, parity type, total length and Wiegand rule. Click **OK**.

Wiegand Mapping Card Reader

Select the Wiegand card reader related door and card reader direction.

4. Click **Save** to save the settings.

Note

If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Door Magnetic Contact Settings

Set the opening and closing door status of the door magnetic contact to match the actual wiring method.

Before You Start

The access controller has connected to the door magnetic contact.

Steps

1. Click **System and Maintenance → Maintenance → Device Access → Host Parameter** to enter the settings page.
2. Select the door magnetic contact status.

Barrier Open Status (Default)

The door magnetic contact is in open status in default. Access controller is connected to the door magnet contact through NO.

Door Closed Status

The door magnetic contact is in closed status in default. Access controller is connected to the door magnet contact through NC.

9.7.12 Card Settings

Set Card Security

Click **System and Maintenance → System Configuration → Card Settings → Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can enable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption Sector

M1 card encryption can improve the security level of authentication.

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

DESFire Card Read Content

The device can read the DESFire card content.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Set Card No. Authentication Parameters

Set the card reading content when authenticate via card on the device.

Go to **System and Maintenance → System Configuration → Card Settings → Card No. Auth. Settings** .

Select a card authentication mode and set the reversed card No. and click **Save**.

Full Card No.

All card No. will be read.

3 bytes

The device will read card via Wiegand 26 protocol (read 3 bytes).

4 bytes

The device will read card via Wiegand 34 protocol (read 4 bytes).

Enable Reversed Card No.

The read card No. will be in reverse sequence after enabling the function.

9.7.13 Maintenance and Security

Set Privacy Parameters

Set the event storage type, picture upload and storage parameters, and the picture clearing parameters.

Go to **System and Maintenance → System Configuration → Security → Privacy Settings**

Select a method to delete the event. You can select from **Delete Old Events Periodically**, **Delete Old Events by Specified Time**, or **Overwriting**. Click **Save** after configuration.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Set Password Mode

Before configuring passwords, it is necessary to clarify whether the password is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

Steps

1. Click **System and Maintenance → System Configuration → Security → PIN Mode**

   Device-Set Personal PIN

   It can be created or edited on the device or on the web, and cannot be set on other platforms.

   Platform-Applied Personal PIN

   It can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

2. Click **Save**.

Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **System and Maintenance → Maintenance → Restart** .
Click **Restart** to reboot the device.

Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click 🗀 and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.
If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

Note

Do not power off during the upgrading.

Sub Device Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .
Set Upgrade Settings as **RS-485 Card Reader**, and select a card reader.
Select an upgrade type from the drop-down list. Click 🗀 and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Restore Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the device IP address and the user information.

Import and Export Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note

You can import the exported device parameters to another device.

Import

Click 🗀 and select the file to import. Click **Import** to start import configuration file.

Device Debugging

You can set device debugging parameters.

Steps

1. Click **System and Maintenance → Maintenance → Device Debugging** .
2. You can set the following parameters.

   Enable SSH

   To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

   Print Log

   You can click **Export** to export log.

   Capture Network Packet

   You can set the **Capture Packet Duration**, **Capture Packet Size**, and click **Start** to capture.

Log Query

You can search and view the device logs.

Go to **System and Maintenance → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

9.7.14 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **HTTPS Certificate** area, click **Create Certificate Request**.

3. Input certificate information and click **Save**.
   - Click **View** and the created certificate will be displayed.
   - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
   1) In the **Import Key** area, select a certificate from the local, and click **Import**.
   2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Create and Import SYSLOG Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **SYSLOG Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.
   - Click **View** and the created certificate will be displayed.
   - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
   1) In the **Import Key** area, select a certificate from the local, and click **Import**.
   2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **CA Certificate ID** area.

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Upload a certificate file from the local.
4. Click **Import**.

Chapter 10 Other Platforms to Configure

You can also configure the device via HikCentral Access Control. For details, see the platforms' user manual.

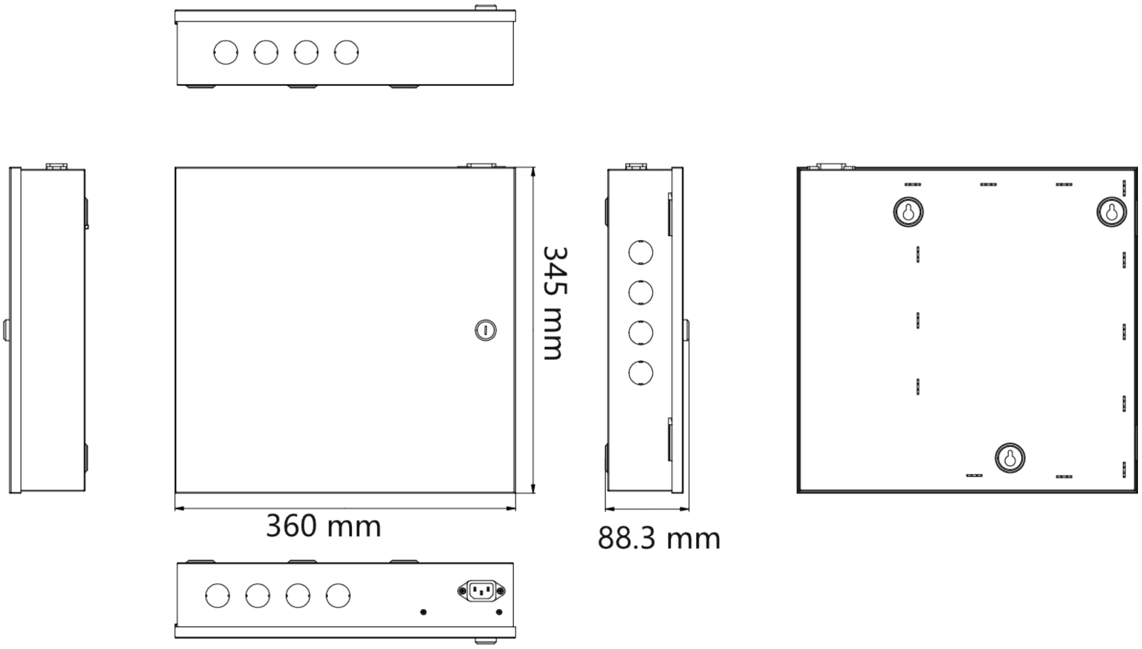
HikCentral Access Control (HCAC)

Click/tap the link to view the HCAC's user manual.

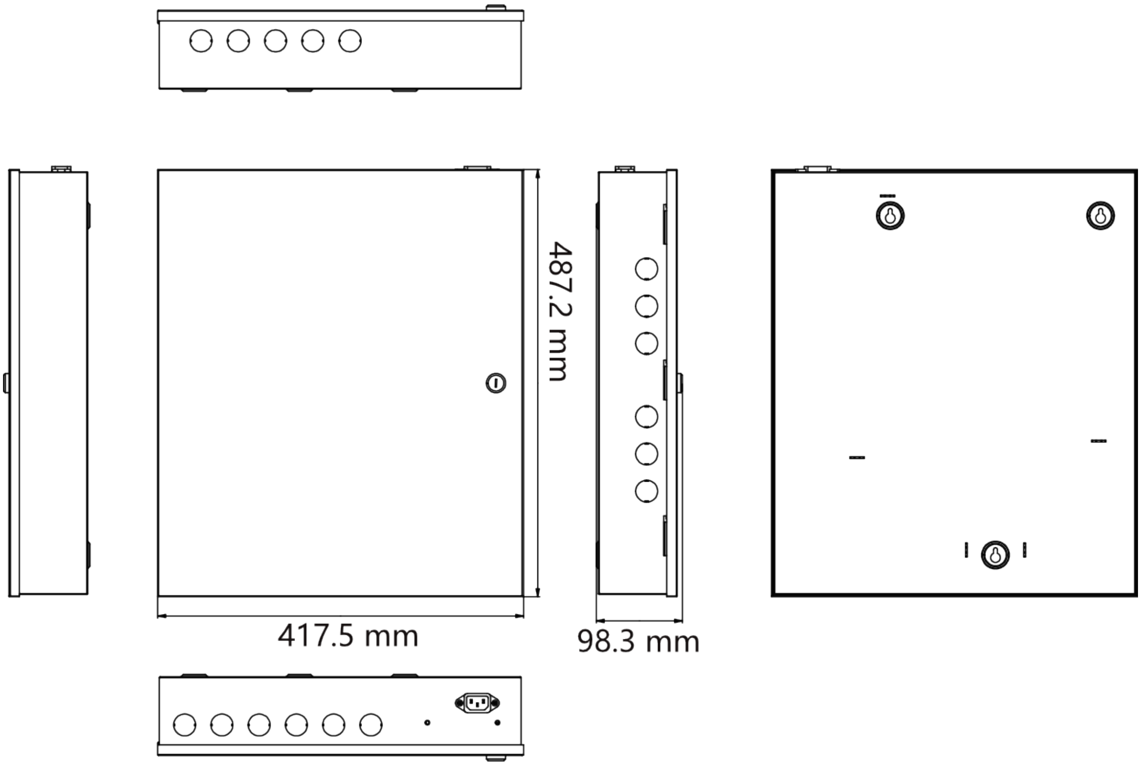
http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

Appendix A. Dimension

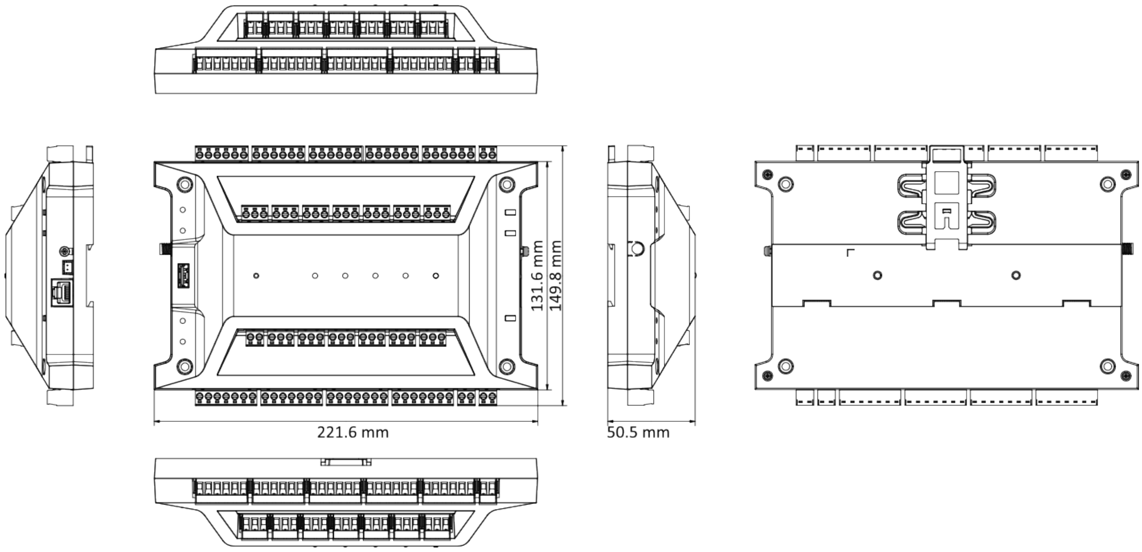
Dimension of 1-Door/2-Door/4-Door Access Controller



Dimension of 8-Door Access Controller



Dimension of Access Controller Main Board



See Far, Go Further