HIKVISION

DS-K3BC430LX Series Swing Gate

Legal Information

About this Manual

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

Trademarks

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

Disclaimer

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

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

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

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:

- Stainless steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- 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.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

Available Models

Product Name	Model
Swing Gate	DS-K3BC430LX

Contents

Chapter 1 Overview

1.1 Introduction

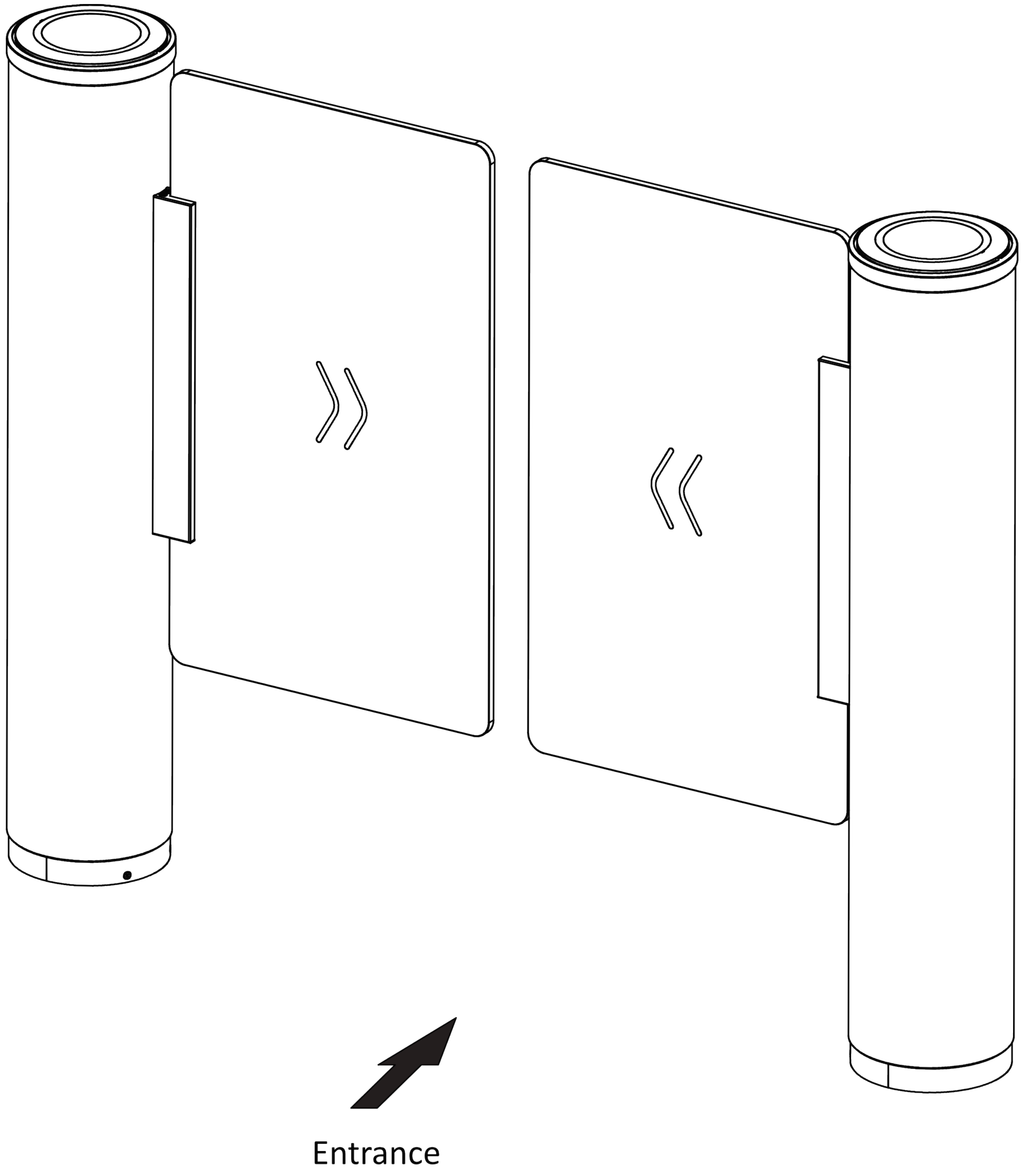


Figure 1-1 Appearance

1.2 Main Features

- Supports control mode, remain open mode and remain closed mode in both entrance and exit direction.
- Self-detection, self-diagnostics, and automatic alarm
- Fire alarm passing
  When the fire alarm is triggered, the barrier will be open automatically for emergency evacuation.
- Valid passing duration settings
  System will cancel the passing permission if a person does not pass through the lane within the valid passing duration.
- Bidirectional (Entrance/Exit) lane
  The barrier opening and closing speed can be configured according to the visitor flow.
- TCP/IP network communication
  The communication data is specially encrypted to relieve the concern of privacy leak.
- Remote barrier opening via keyfob and broadcasting via loudspeaker (custom broadcasting context is supported when installed with access control board).

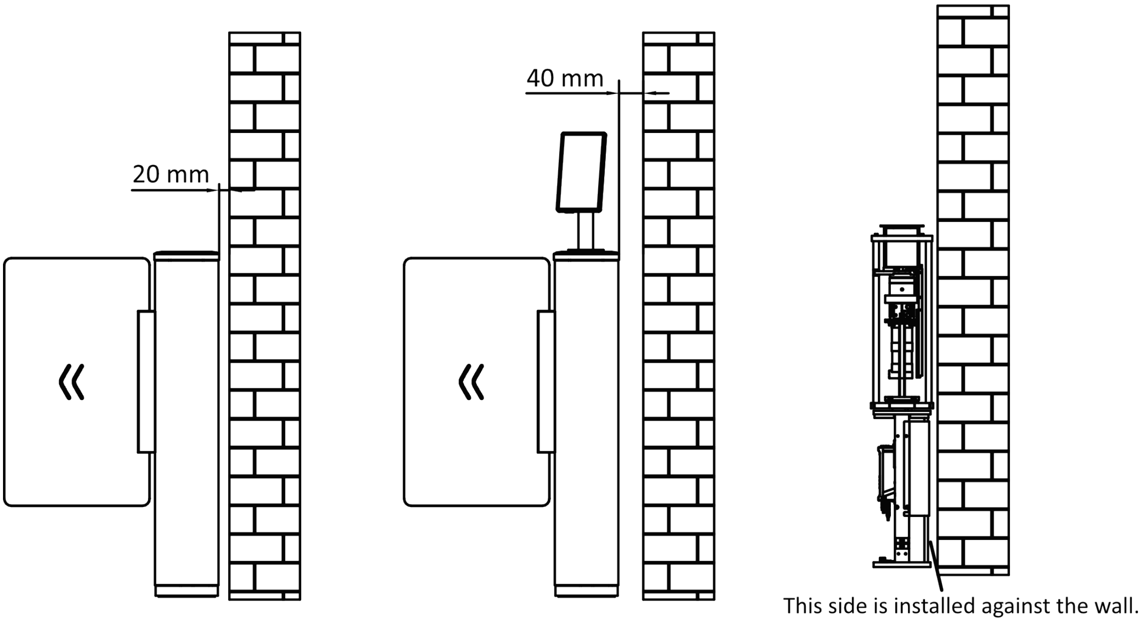
Chapter 2 System Wiring

The preparation before installation and general wiring.

Steps

Note

- The device should be installed concrete surface or other flat non-flammable surface.
- If the installation area is too close to the wall, make sure the distance between the pedestal and the wall should be no less than 20 mm (40 mm if with face recognition terminals), or you cannot open the pedestal's top panel or might cause damage to devices.



- The dimension is as follows.

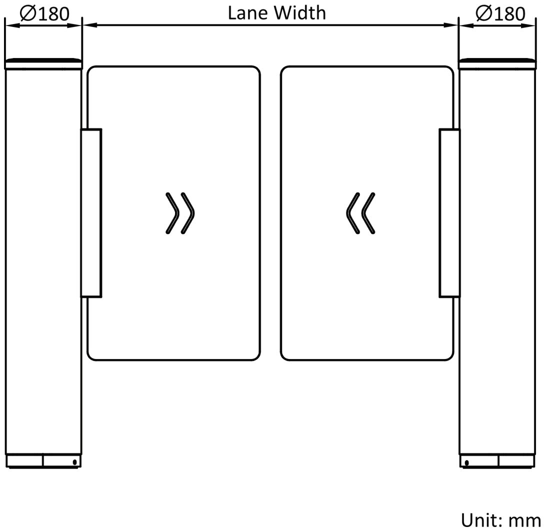


Figure 2-1 Dimension

1. Draw a central line on the installation surface of the left or right pedestal.
2. Draw other parallel lines for installing the other pedestals.

Note

The distance between the nearest two line is L + 180 mm. L represents the lane width.

3. Slot on the installation surface and dig installation holes. Put 3 expansion bolts of M12*150 for each pedestal.

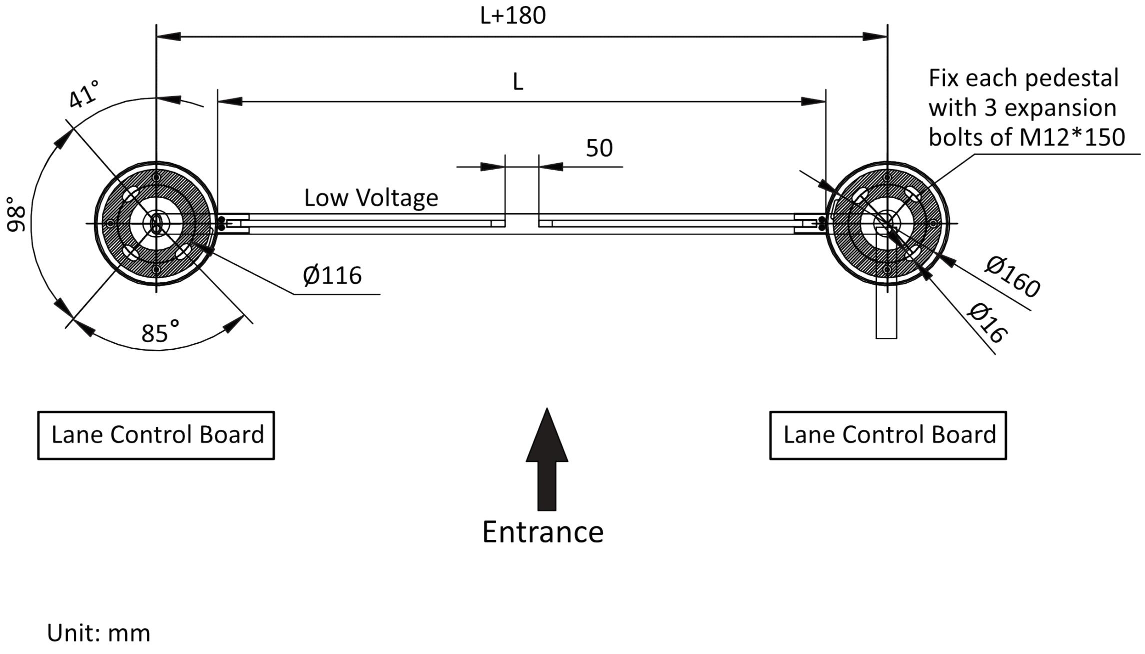


Figure 2-2 Hole Position and System Wiring

4. Bury cables.

Note

- Interconnecting cable (available for two pedestals and above): The recommended length is L +1.5 m.

  Network communication cable: It is recommended to use CAT5e or the network cable has better performance.
- The suggested external diameter of the low voltage conduit is 30 mm.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.
- Before digging holes, evaluate the thickness of the installation surface to avoid puncturing.
- When slotting on the installation surface, pay attention to the position and width of the slot to avoid misalignment of the barrier.
- One distribution cabinet supplies one pedestal.

  The maximum allowable diameter of the power cable is 12 AWG (UL1015), and the transmission distance is 100 m.

  One distribution cabinet supplies two pedestals.

  The maximum allowable diameter of the power cable is 16 AWG (UL1015), and the transmission distance is 25 m.

Chapter 3 Install Pedestals

Before You Start

Prepare for the installation tools, check the device and the accessories, and clear the installation base.

Steps

Note

- The installation diagram is for illustration. For details, please refer to ***Wiring*** for video guide.
- The device should be installed on the concrete surface or other flat non-flammable surfaces.
- Make sure the device is powered off during installation and other operations.
- The installation tools are put inside the package of the pedestal.
- To prevent stainless steel from rusting due to dirt during construction, it is recommended that the protective film be removed after the installation is completed. There may be residual adhesive at the film cutting position. It is recommended to use WD-40 protective liquid to wipe after tearing the film.
- It is recommended that at least two people collaborate to install the sleeve. You'd better wear gloves throughout the entire process, handle with care, and pay attention to preventing crushing or pinching injuries.

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Seal the bottom of the pedestal with sealing materials to prevent water accumulation.
3. Remove the protective panel on the top of the device, and determine the barrier direction and the pedestal installation position according to the default barrier opening direction mark.

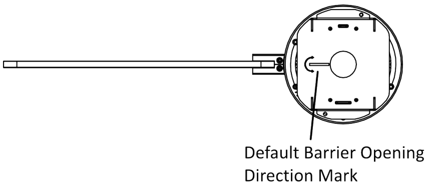


Figure 3-1 Default Barrier Opening Direction Mark

Note

Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 150 mm. The bottom circuit board can't be immersed.

4. Use a cross screwdriver to remove screws of the decorative ring and cable protection panel, and complete wiring.

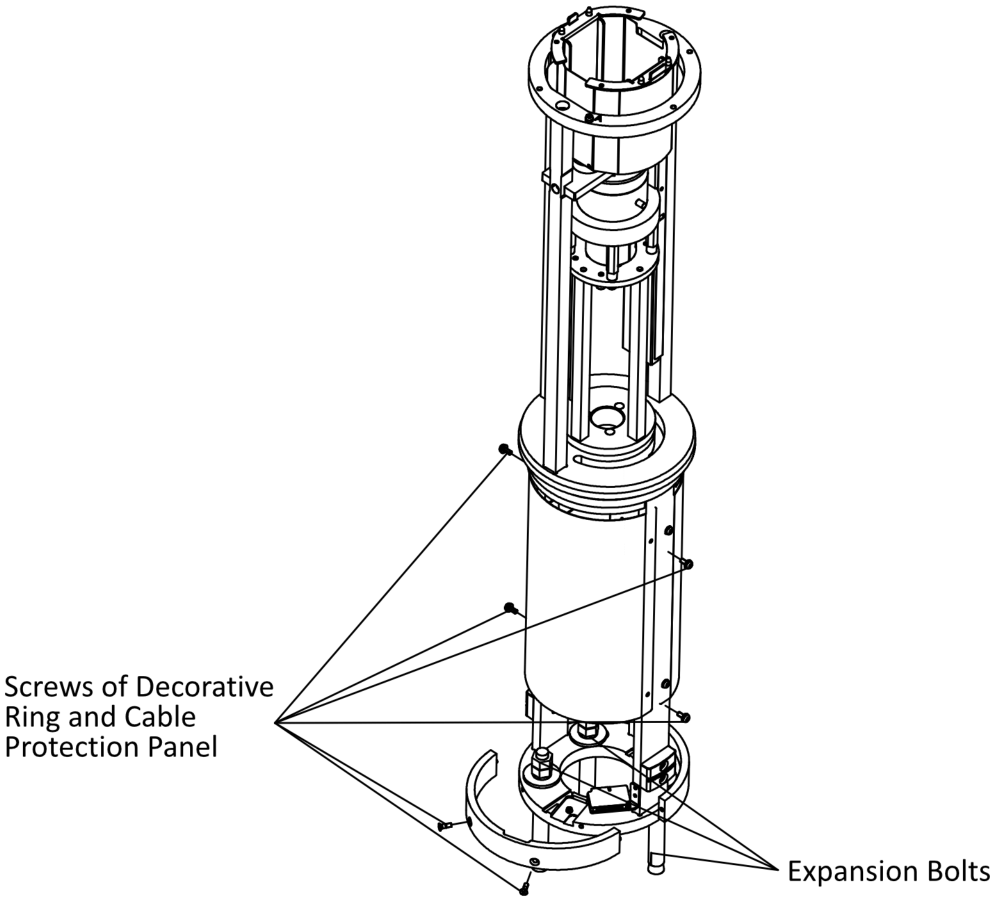


Figure 3-2 Remove Decorative Ring and Cable Protection Panel

5. Use a cross screwdriver to fix the top plastic part, and use a hexagon wrench to fix the rotary tube.

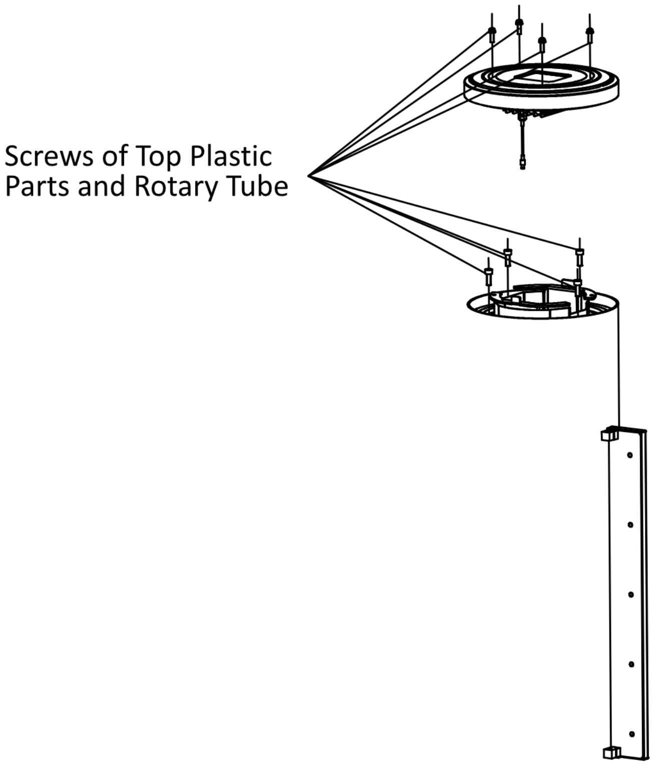


Figure 3-3 Fix Top Plastic Part and Rotary Tube

6. Fix the barrier and decorative parts.

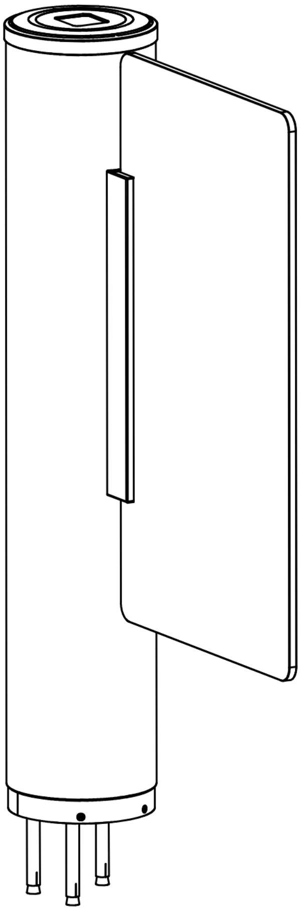


Figure 3-4 Fix Barrier

Chapter 4 General Wiring

Note

- The supplied interconnecting cables need connecting on-site: CAT5e Communication cable. The cable is 3 m in length and put inside the package.

4.1 Components Introduction

By default, basic components of the turnstile are connected well. The pedestals can communicate by wiring the interconnecting cables. And the turnstile supports wiring the AC electric supply for the whole system' s power supply.

Note

Power supply: 24 V DC
Power supply voltage fluctuation range: ± 5%

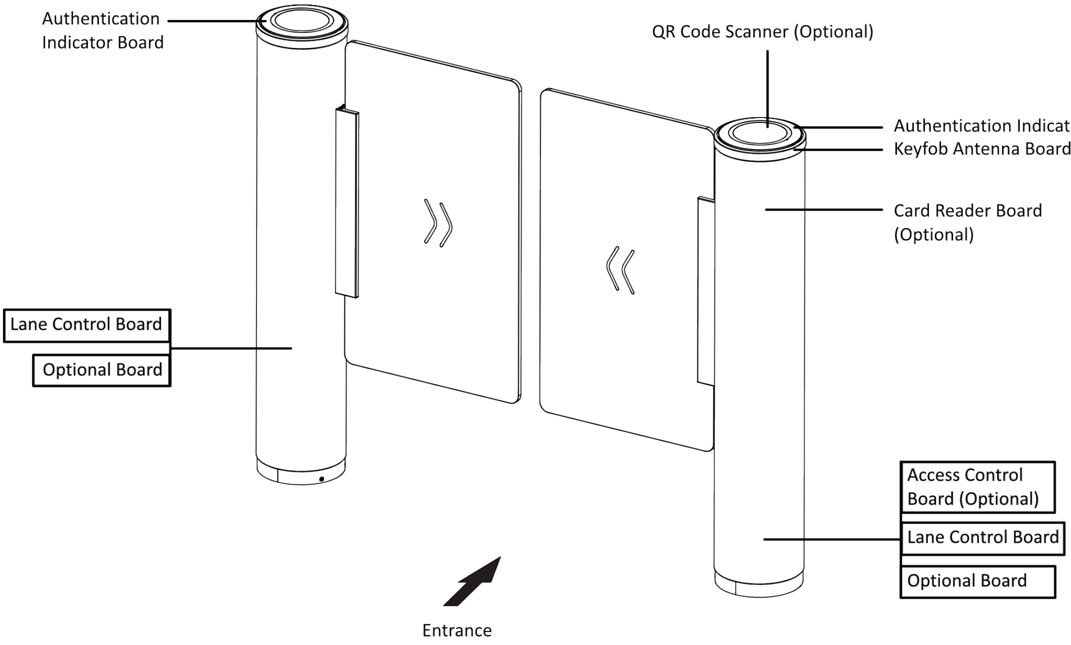

Authentication Indicator Board
QR Code Scanner (Optional)
Authentication Indicator Board
Keyfob Antenna Board
Card Reader Board (Optional)
Lane Control Board
Optional Board
Access Control Board (Optional)
Lane Control Board
Optional Board
Entrance

Figure 4-1 Components Introduction

4.2 Wiring

Scan the QR code to view the wiring guide video.

4.3 Terminal Description

4.3.1 General Wiring

The general wiring of lane control board, access control board and optional board.

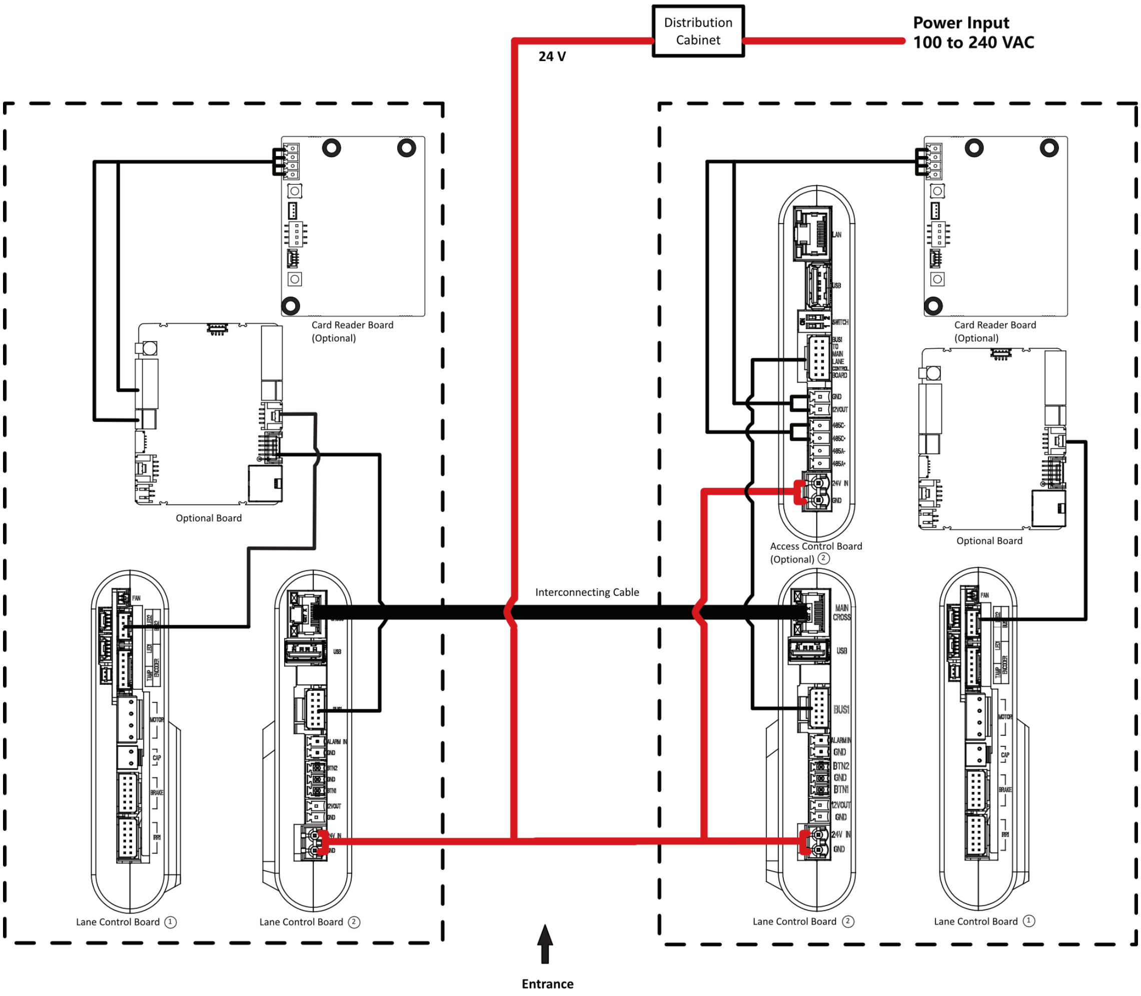


Figure 4-2 General Wiring

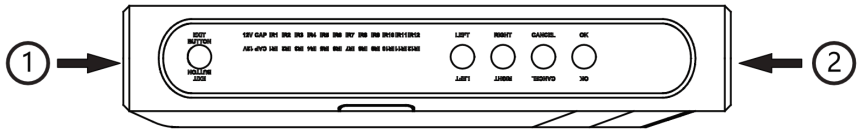
Note

- It is recommended to use Hikvision matched distribution cabinet (sold separately) to covert the AC mains power to 24 V.
- The ① and ② refer to the two sides of a same board.
- Barrier opens at the entrance/exit: connect to BTN1/BTN2 and GND.

4.3.2 Lane Control Board Terminal Description

The lane control board contains indicator board interface, interconnecting interface, access control board interface, fire input interface, exit button interface, 12 VDC output interface, 24 VDC input interface, communication interface, encoder interface, power supply interface for motor, supercapacitor interface, brake interface, and tamper interface.

The picture displayed below is the lane control board diagram.



Lane Control Board

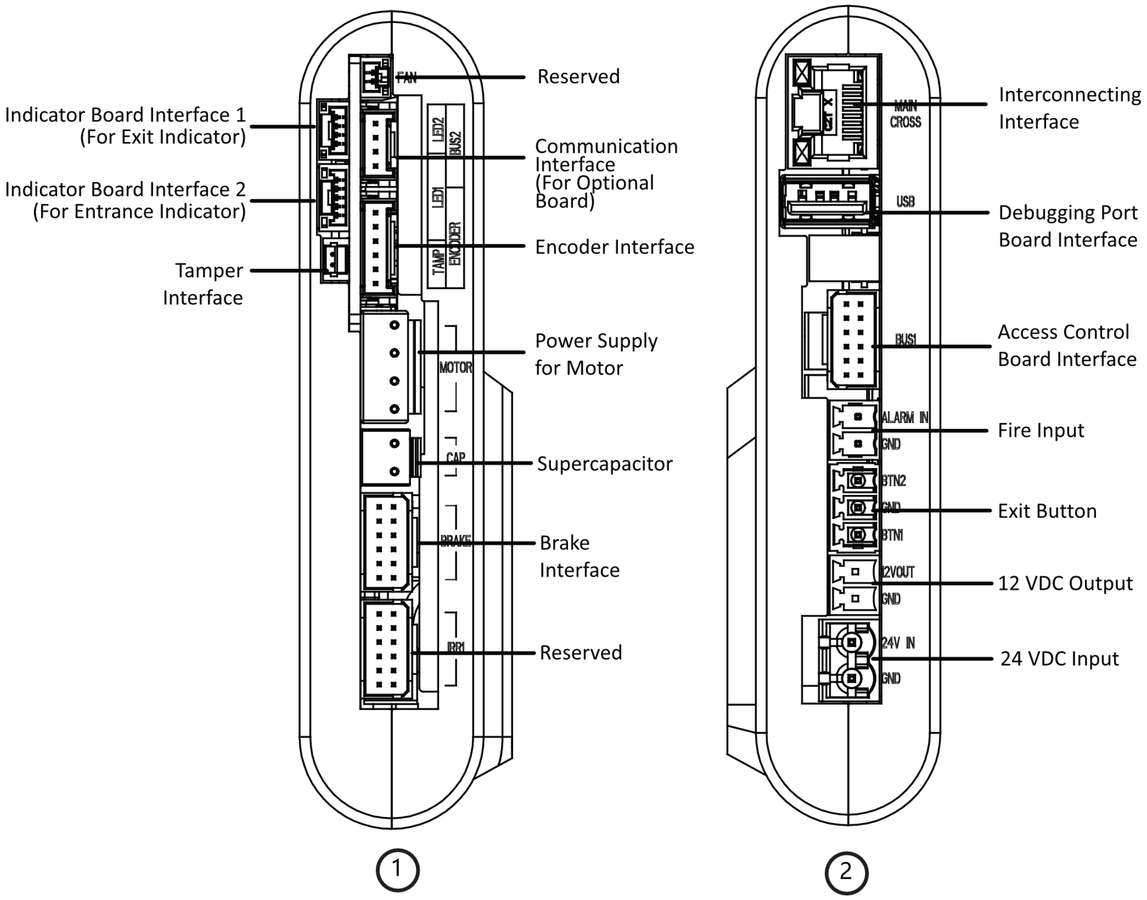


Figure 4-3 Lane Control Board

4.3.3 Access Control Board Terminal Description (Optional)

Access control board is mainly used for authority identification in places with high security levels such as public security or judicial place, external device accessing, and communication with the upper platform and lane controller.

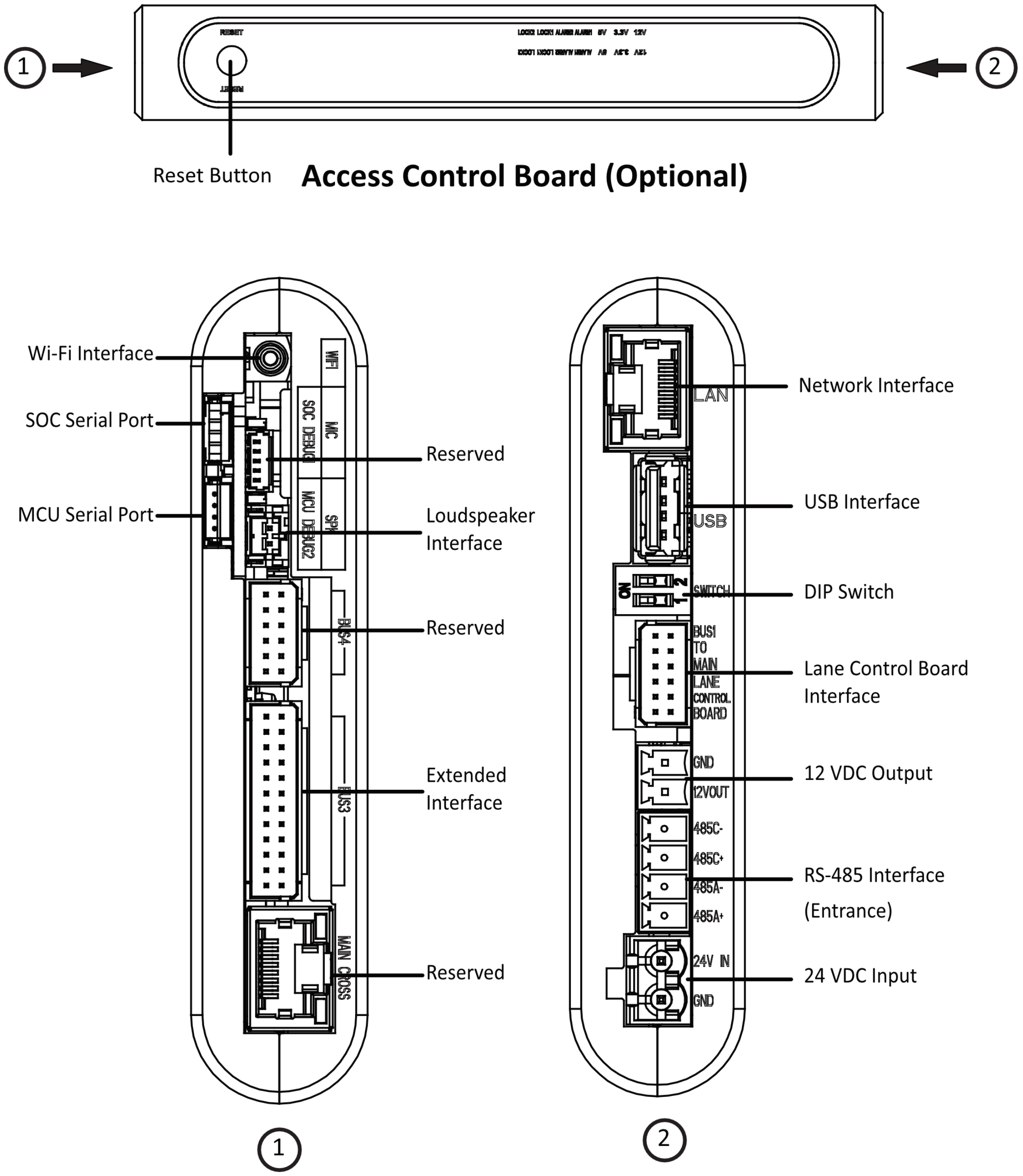


Figure 4-4 Access Control Board

Note

- RS-485A corresponds to UART 5 on web and is for QR code scanner connection at entrance by default; RS-485C corresponds to UART 7 on web and is for card reader connection at entrance by default.
- The SOC and MCU serial port are for maintenance and debugging use only.

- Press the Reset button for 5 s and the device will start to restore to factory settings.
- The DIP switch is for study mode setting and keyfob paring. For detailed information about the DIP switch, see *DIP Switch Description*.

The wiring diagram of extended interface of access control board is shown as follows.

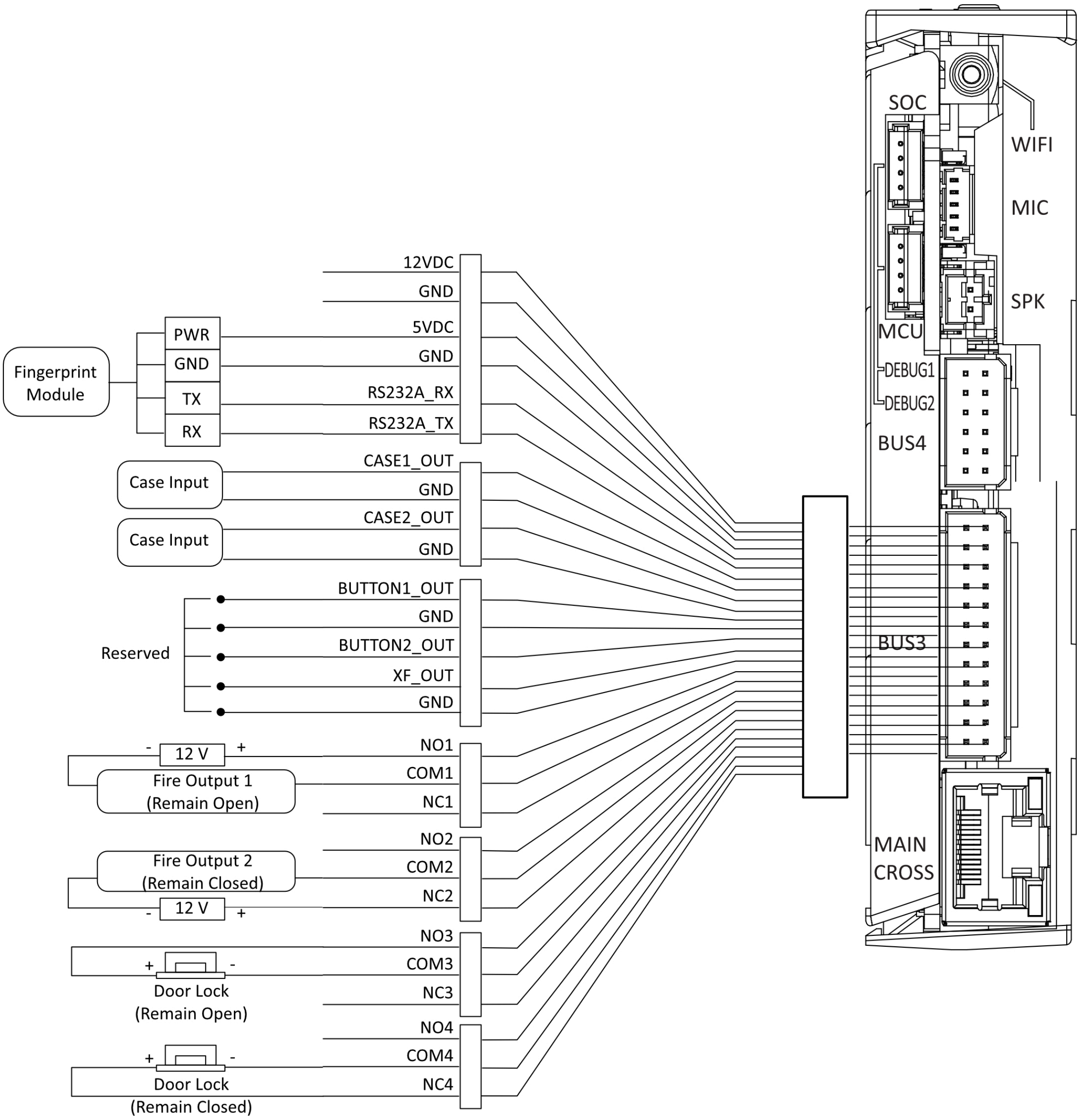


Figure 4-5 Wring Diagram of BUS3 Interface

Note

RS-232A corresponds to UART 1 on web.

4.3.4 Optional Board Terminal Description

The optional board contains the sub-1G antenna interface, 485/232 interface, 12 V output interface, loudspeaker interface, debugging port, Wiegand/exit button interface, BUS interface, 5 VDC output and communication interface.

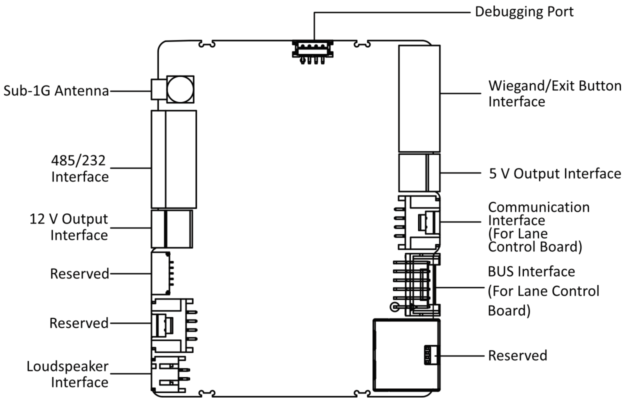


Figure 4-6 Optional Board Terminal

4.3.5 Card Reader Board Terminal Description

The card reader board can be connected to the access control board via RS-485 interface.

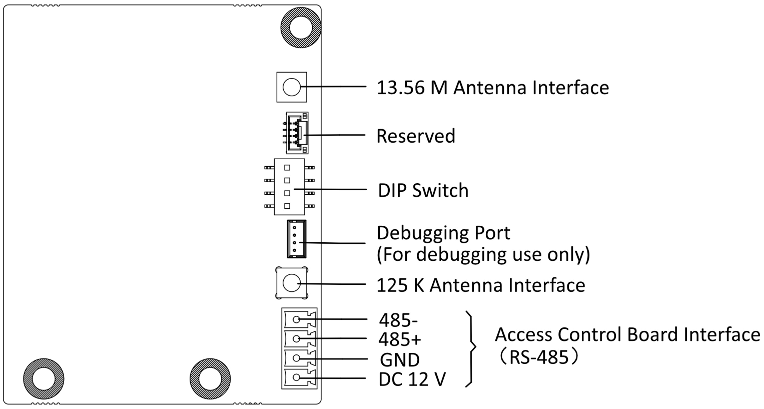

13.56 M Antenna Interface
Reserved
DIP Switch
Debugging Port (For debugging use only)
125 K Antenna Interface
485-
485+
GND
DC 12 V
Access Control Board Interface （RS-485）

Figure 4-7 Card Reader Board

4.3.6 RS-485 Wiring

The RS-485 interfaces on the access control board and optional board are suggested to connect with the face recognition module or the card reader. Here takes connecting with a card reader as an example.

Note

- There are 2 RS-485 interfaces on the access control board for entrance. Refer to ***Access Control Board Terminal Description (Optional)*** for details.
  There are 2 RS-485 interfaces on the optional board for exit. Refer to for details.
- If there are other RS-485 devices connecting, the ID of the RS-485 cannot be conflicted.
- The connected 12 V power interface for the face recognition terminal cannot be connected with other 12 V devices.

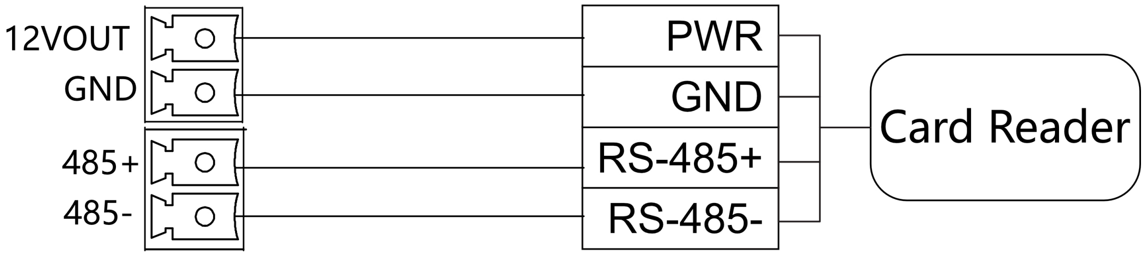


Figure 4-8 Wiring RS-485

4.3.7 RS-232 Wiring

Note

- There are 1 RS-232 interface on the extended interface of access control board, see ***Access Control Board Terminal Description (Optional)*** . The RS-232A corresponds to UART 1 on web.
- There is 1 RS-232 interface on the optional board, see . The RS-232B corresponds to UART 2 on web.
  The RS-232C interface is reserved.

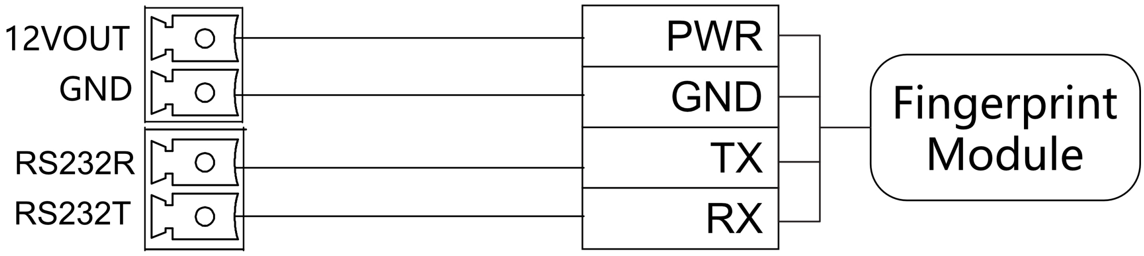


Figure 4-9 RS-232 Wiring

4.3.8 Alarm Input Wiring

On the main lane control board, you can wire the fire alarm input interface.

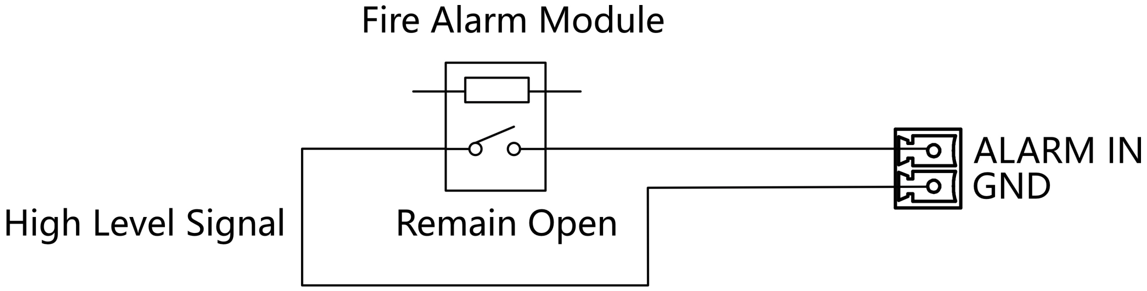


Figure 4-10 Remaining Open

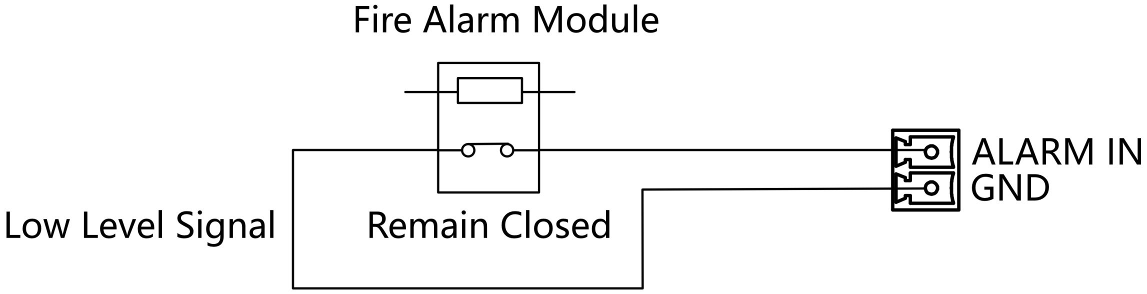


Figure 4-11 Remaining Closed

4.3.9 Exit Button Wiring

The main and sub lane control board each has 1 button interface, which can be connected to exit button or face recognition device.

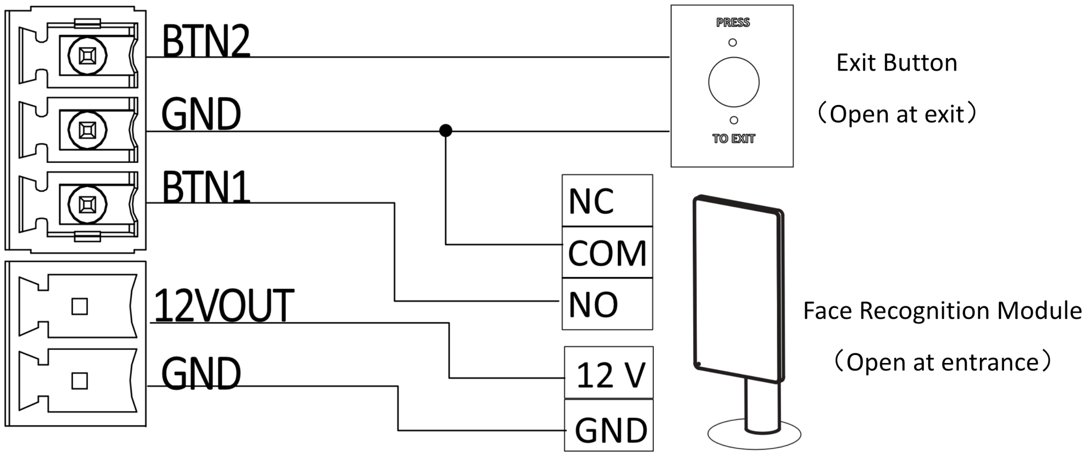


Figure 4-12 Exit Button Wiring

Note

- The face recognition devices are powered via 12 VDC power output interface of the main and sub lane control board.
- Barrier open at the entrance: connect to BTN1 and GND.
- Barrier open at the exit: connect to BTN2 and GND.

4.4 Device Settings via Button

You can configure the device via button on the lane control board.

Note

- Refer to ***Button Configuration Description*** for detailed information.
- If the optional board is not installed, the error code of "59" will appear but the device functions normally.
- For the main lane, "99" is displayed on the screen by default. For the sub lane, "00" is displayed on the screen by default.

4.4.1 Configuration via Button

Button Description

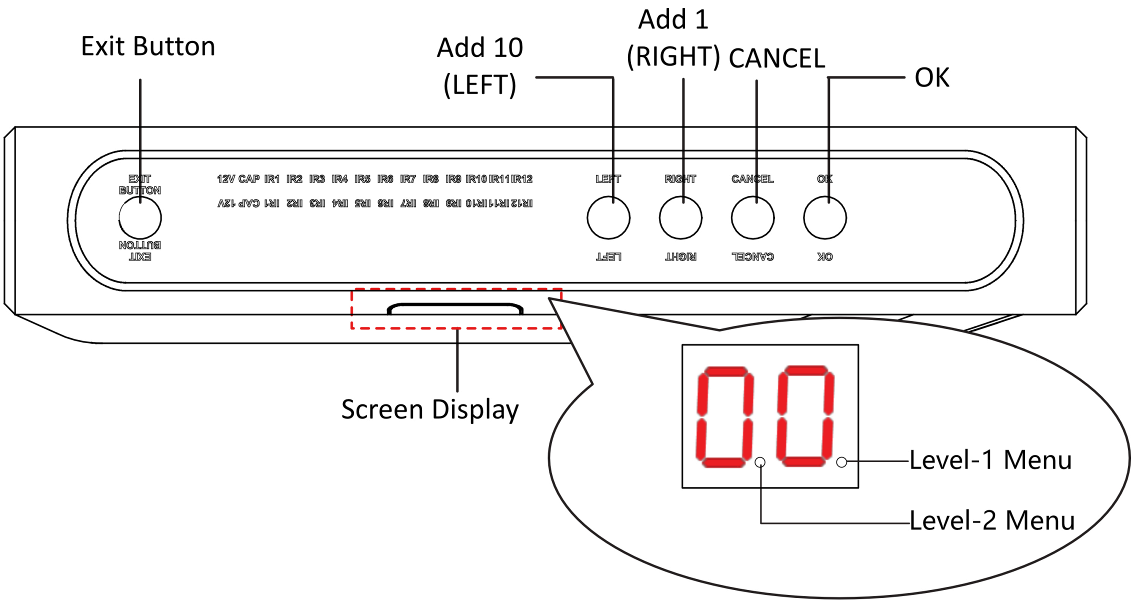


Figure 4-13 Button

Exit Button

- Press to open the barrier from the entrance position.
- Double press to open the barrier from the exit position.

Parameter Configuration Button

- LEFT: Press to add 10 to configuration data.
- RIGHT: Press to add 1 configuration data.
- CANCEL: Return to the Level-1 menu, or exit Level-1 menu.
- OK: Confirm the settings, or enter configuration mode, or enter the Level-2 menu.

Note

- Configuration No. is displayed by two digital tubes.
- Level-1 Menu: If the decimal point on the right is on, it indicates the Level-1 menu. The number represents the configuration No.
- Level-2 Menu: If the decimal point in the middle is on, it indicates the level-2 menu. The number represents the configuration No.

Button Configuration Procedure

Here takes setting intrusion duration to 12 s as example:

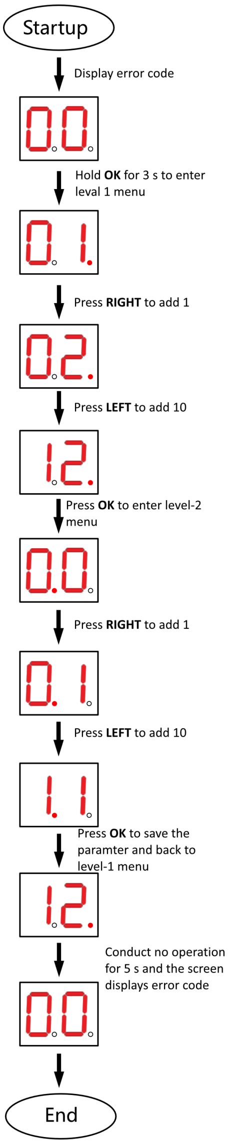

Startup
Display error code
0.0.
Hold OK for 3 s to enter leval 1 menu
0.1.
Press RIGHT to add 1
0.2.
Press LEFT to add 10
1.2.
Press OK to enter level-2 menu
0.0.
Press RIGHT to add 1
0.1.
Press LEFT to add 10
1.1.
Press OK to save the paramter and back to level-1 menu
1.2.
Conduct no operation for 5 s and the screen displays error code
0.0.
End

Figure 4-14 Procedure

Steps:

1. Hold **OK** button for 3 s until one beep occurs. The device enter the configuration mode. Level 1 menu lights up. The display screen displays the configuration No. **1**.
2. In the Level-1 menu, press **LEFT** (plus 10) once and press **RIGHT** (plus 1) twice to set the configuration No. to 12. Press **OK** to save settings and the enter the level-2 menu. Or you can press **CANCEL** to exit the current menu, or conduct no operation for 5 s to cancel configuration and exit the current menu.
3. After enter the level 2 menu, press **LEFT** (plus 10) once and **RIGHT** (plus 1) twice to set the configuration No. to 12. Press **OK** to save the settings. Or you can press **CANCEL** to exit the current menu, or conduct no operation for 5 s to cancel configuration and exit the current menu.

Note

- The configuration No. will display in a cycle.
- Each configuration No. refers to a function. For details about the configuration No. and its related function, see ***Button Configuration Description*** .

4.4.2 Set Study Mode via Button

Enter the study mode through button configuration to set the closed position of the device barrier.

Steps

Note

- For details about button's operation, see ***Configuration via Button*** .
- For details about the configuration No. and its related function, see ***Button Configuration Description*** .

1. Enter the study mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **1**. The device will enter the study mode.
   3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the study mode.
2. Power off the device and swing the barrier until it is vertical to the pedestal.
3. Power on the device.
   The device will remember the current position automatically.
4. Reboot the device when you hear **Study accomplished. Please reboot.**

4.4.3 Pair Keyfob via Button

Pair the keyfob to the device via button to open/close the barrier remotely.

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

Note

- For details about button's operation, see ***Configuration via Button*** .
- For details about the configuration No. and its related function, see ***Button Configuration Description*** .
- For details about the keyfob operation instructions, see the keyfob's user manual.

1. Enter the keyfob pairing mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **2**. The device will enter the keyfob pairing mode.

   3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the keyfob pairing mode.

2. Hold the **Close** button for more than 10 seconds.

   The keyfob's indicator will flash if the pairing is completed.

3. Exit the keyfob pairing mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **2**. The device will enter the keyfob pairing mode.
   3) Set the configuration No. in the Level-2 menu to **1**. The device will exit the keyfob pairing mode.

4. Reboot the device to take effect.

4.4.4 Initialize Device

Steps

1. Hold the initialization button on the access control board for 5 s.

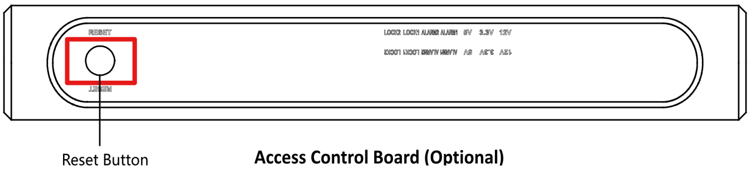

RESET
LOCK2 LOCK1 ALARM2 ALARM1 5V 3.3V 12V
Reset Button
Access Control Board (Optional)

Figure 4-15 Initialization Button Position

2. The device will start restoring to factory settings.
3. When the process is finished, the device will beep for 3 s.

Caution

The initialization of the device will restore all the parameters to the default setting and all the device events are deleted.

Note

Make sure no persons are in the lane when powering on the device.

Chapter 5 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.: 80
- The default user name: admin

5.1 Activate via SADP

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

Before You Start

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

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

Steps

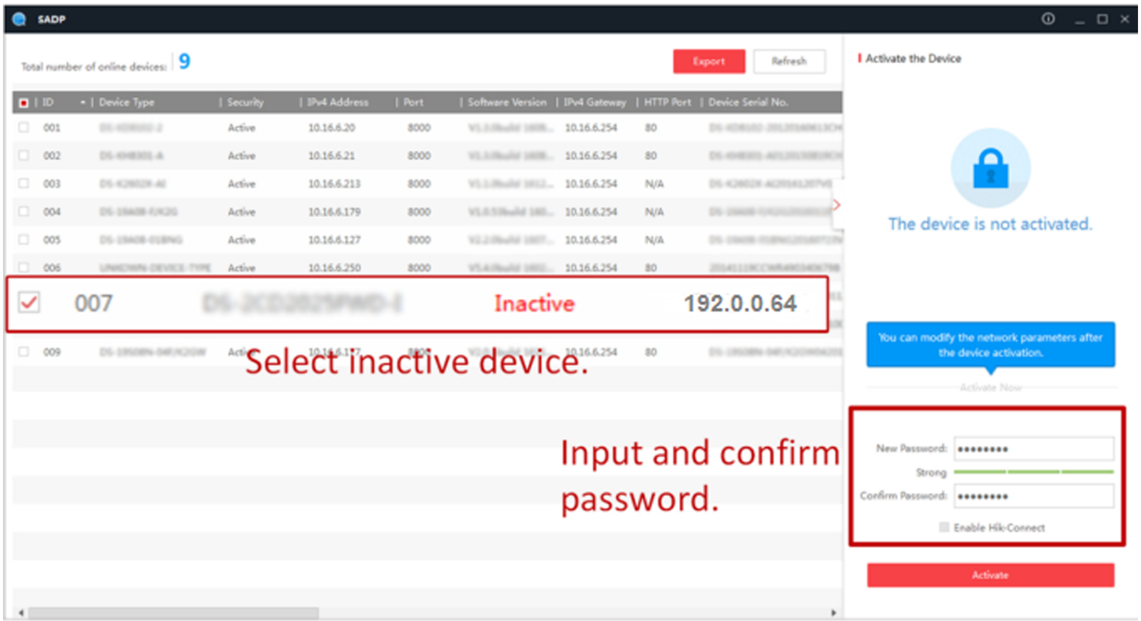
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

   Caution

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

   Note

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



Total number of online devices: 9

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	[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.

5.2 Activate Device via iVMS-4200 Client Software

For some devices, you are required to create the password to activate them before they can be added to the iVMS-4200 software and work properly.

Steps

Note

This function should be supported by the device.

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

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

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you 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 installer and/or end-user.

Note

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

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

5.3 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.

Chapter 6 Quick Operation via Web Browser

6.1 Time Settings

Click ◅ in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** 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.

DST

Enable DST. Set the DST start time, end time and bias time.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

6.2 Administrator Settings

Steps

1. Click ◅ in the top right of the web page to enter the wizard page. After setting time, you can click **Next** to enter the **Administrator Settings** page. Or you can click **Skip** to enter the **Administrator Settings** page directly.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

   Note

   You should select at least one credential.

   1) Click **Add Card** to enter the Card No. and select the property of the card.

   Note

   Up to 50 cards can be supported.
4. Click **Complete** to complete the settings.

Chapter 7 Operation via Web Browser

7.1 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*** .

Login via Web Browser

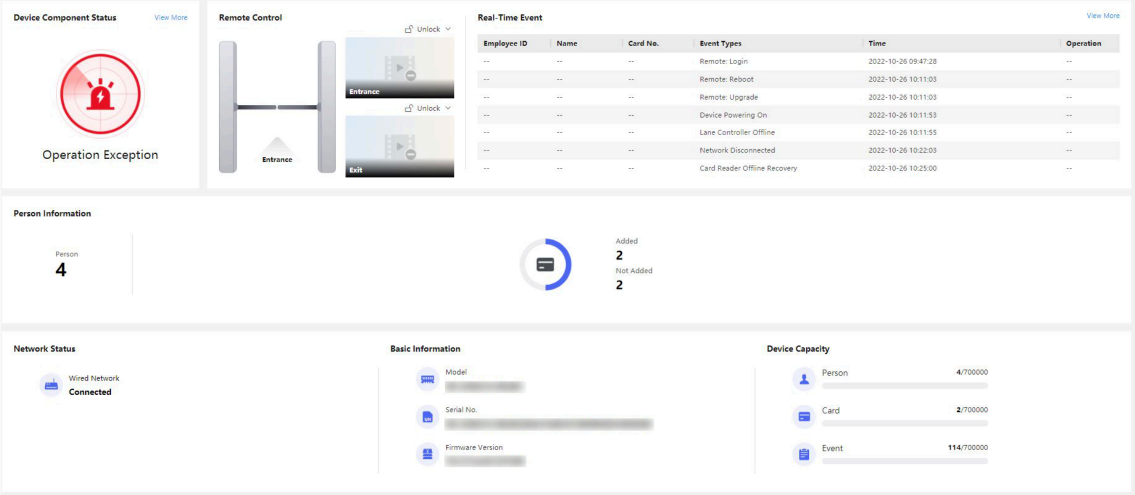
Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

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

7.2 Overview

You can view the device component status, real-time event, person information, network status, basic information, and device capacity. You can also control the barrier remotely.



Real-Time Event

Employee ID	Name	Card No.	Event Types	Time	Operation
--	--	--	Remote: Login	2022-10-26 09:47:28	--
--	--	--	Remote: Reboot	2022-10-26 10:11:03	--
--	--	--	Remote: Upgrade	2022-10-26 10:11:03	--
--	--	--	Device Powering On	2022-10-26 10:11:53	--
--	--	--	Lane Controller Offline	2022-10-26 10:11:55	--
--	--	--	Network Disconnected	2022-10-26 10:22:03	--
--	--	--	Card Reader Offline Recovery	2022-10-26 10:25:00	--

Person Information

Person 4

Added 2

Not Added 2

Network Status

Wired Network
Connected

Basic Information

Model [redacted]

Serial No. [redacted]

Firmware Version [redacted]

Device Capacity

Person	4/700000
Card	2/700000
Event	114/700000

Figure 7-1 Overview

Function Descriptions:

Device Component Status

You can check if the device is working properly. Click **View More** to view the detailed component status.

Remote Control

🔓 / 🔒 / ▣ / ▣

The door is opened/closed/remaining open/remaining closed.

Real-Time 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.

Person Information

You can view the added and not added information of person and card.

Network Status

You can view the network connection status.

Basic Information

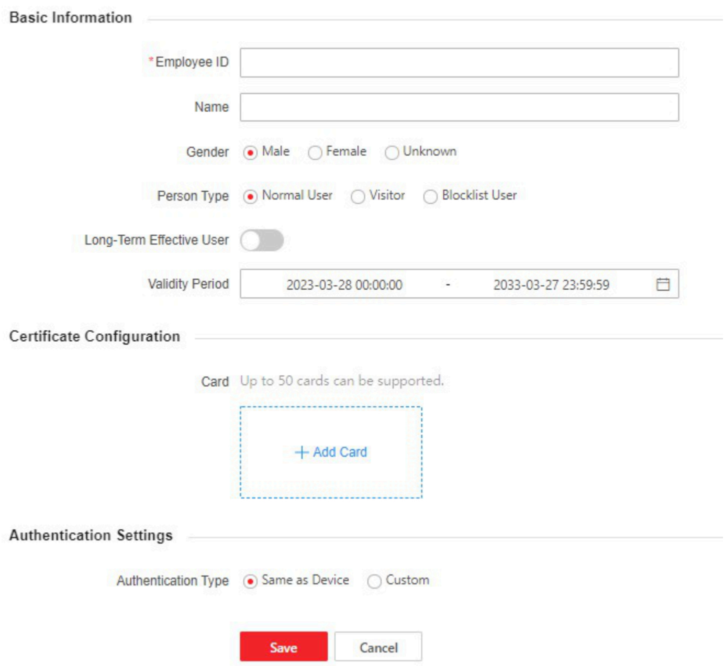
You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, card and event capacity.

7.3 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.



Basic Information

*Employee ID

Name

Gender ● Male ○ Female ○ Unknown

Person Type ● Normal User ○ Visitor ○ Blocklist User

Long-Term Effective User

Validity Period 2023-03-28 00:00:00 - 2033-03-27 23:59:59

Certificate Configuration

Card Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type ● Same as Device ○ Custom

Save Cancel

Figure 7-2 Add Person

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.

If you select **Visitor** as the person type, you can set the visit times.

Click **Save** to save the settings.

Set Permission Time

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

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

Click **Save** to save the settings.

Add Card

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

Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.

Note

Up to 50 cards can be added.

Click **Save** to save the settings.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set **Authentication Type** as **Same as Device** or **Custom**.
Click **Save** to save the settings.

Import/Export Person Data

Export Person Data

You can export added person data for back-up or importing to other devices.

Click **Export Person Data**, set an encryption password and confirm it. Click **OK**.

Note

- The person data will be downloaded to your PC.
- The password you set will be required for importing the data file.

Importing Person Data

Click **Importing Person Data** and select the file. Click **Import**.

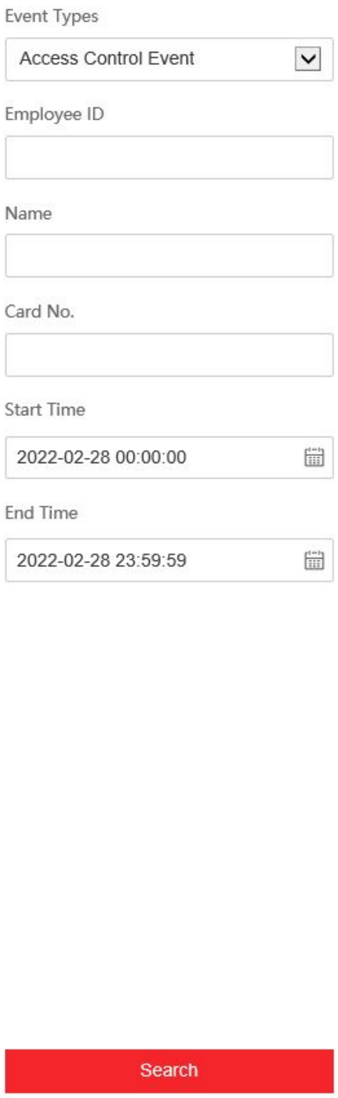
Enter the encryption password to import and synchronize the person data to devices.

Note

- Please ensure the name of the imported file is "UserDataFile".

7.4 Search Event

Click **Event Search** to enter the Search page.



Event Types

Access Control Event

Employee ID

Name

Card No.

Start Time

2022-02-28 00:00:00

End Time

2022-02-28 23:59:59

Figure 7-3 Search Event

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**.

The event types contain access control event and ID card event. If you choose to search for ID card event, you will not need to enter the employee ID, the name, or the card No.

The results will be displayed on the right panel.

7.5 Configuration

7.5.1 View Device Information

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view the device name, language, model, serial No., version, IO input, IO output, and local RS-485 number.

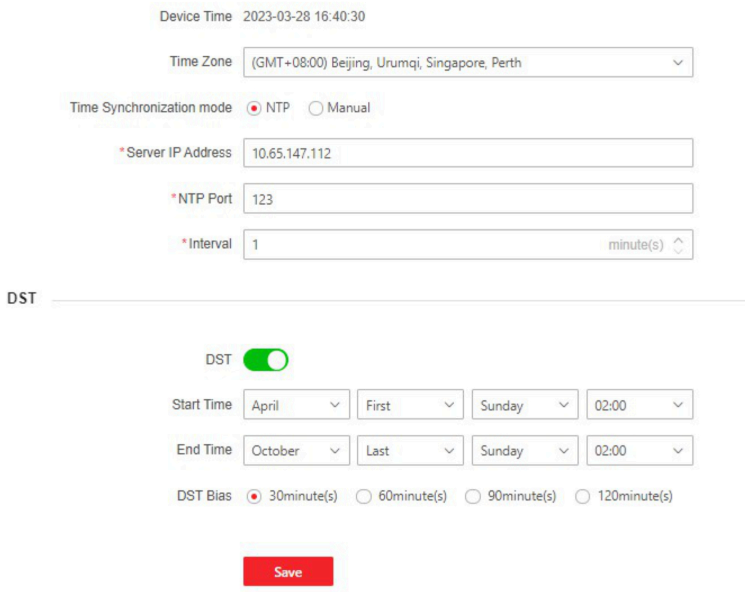
You can change **Device Name** and click **Save**.

You can view the device capacity, including person, card and event.

7.5.2 Set Time

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

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



Device Time	2023-03-28 16:40:30
Time Zone	(GMT+08:00) Beijing, Urumqi, Singapore, Perth
Time Synchronization mode	● NTP ○ Manual
*Server IP Address	10.65.147.112
*NTP Port	123
*Interval	1 minute(s)

DST

DST	On			
Start Time	April	First	Sunday	02:00
End Time	October	Last	Sunday	02:00
DST Bias	● 30minute(s)	○ 60minute(s)	○ 90minute(s)	○ 120minute(s)

Figure 7-4 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 Sync.

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.

7.5.3 Set DST

Steps

1. Click **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.

7.5.4 Change Administrator's Password

Steps

1. Click **Configuration → User Management** .
2. Click ✎ .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **OK**.

⚠ **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 installer and/or end-user.

7.5.5 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

7.5.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

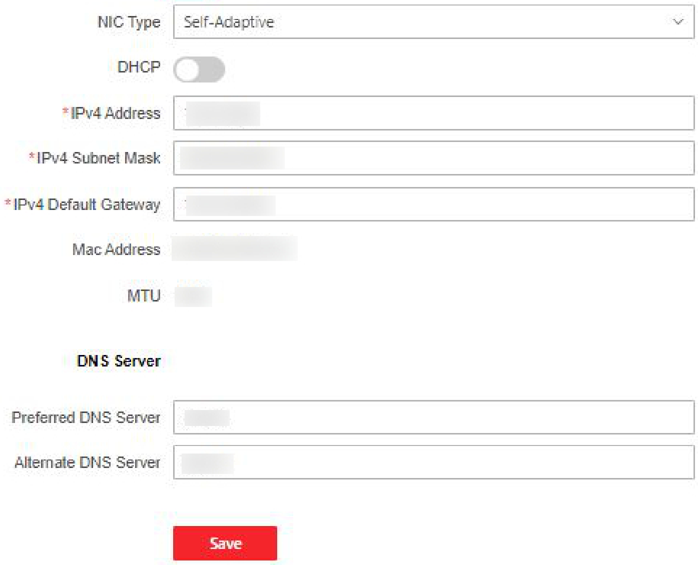
Go to **Configuration → User Management → Arming/Disarming Information** .
You can view the device arming/disarming information. Click **Refresh** to refresh the page.

7.5.7 Network Settings

Set TCP/IP and HTTP(S).

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .



NIC Type: Self-Adaptive

DHCP: ○

*IPv4 Address

*IPv4 Subnet Mask

*IPv4 Default Gateway

Mac Address

MTU

DNS Server

Preferred DNS Server

Alternate DNS Server

Save

Figure 7-5 TCP/IP Settings Page

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

NIC Type

Select a NIC type from the drop-down list. By default, it is **Auto**.

DHCP

If you 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.

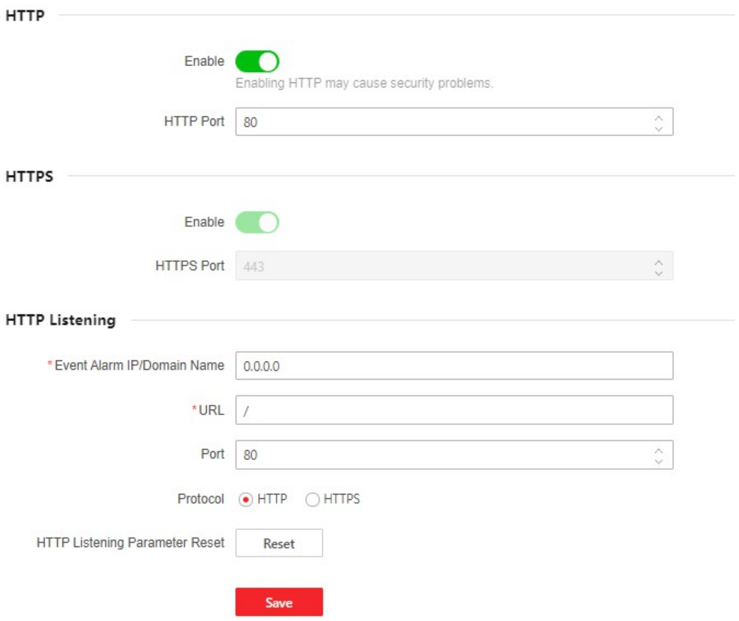
DNS Server

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

Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening parameters.

Click **Configuration → Network → Network Service → HTTP(S)** .



HTTP

Enable

Enabling HTTP may cause security problems.

HTTP Port: 80

HTTPS

Enable

HTTPS Port: 443

HTTP Listening

*Event Alarm IP/Domain Name: 0.0.0.0

*URL: /

Port: 80

Protocol: ● HTTP ○ HTTPS

HTTP Listening Parameter Reset

Figure 7-6 Network Service

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

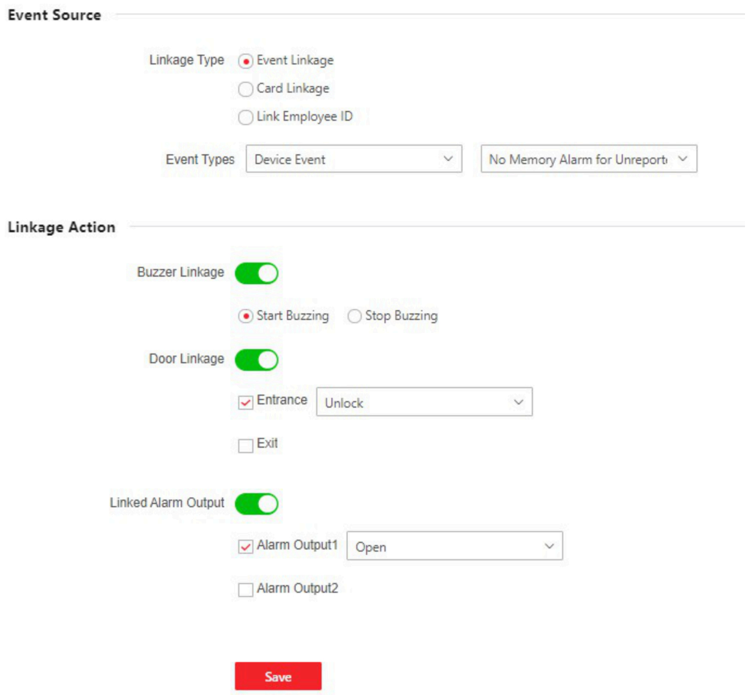
The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

7.5.8 Event Linkage

Set linked actions for events.

Steps

1. Click **Configuration → Event → Basic Event → Event Linkage** to enter the page.



Event Source

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

Event Types: Device Event; No Memory Alarm for Unreport

Linkage Action

Buzzer Linkage: on — ● Start Buzzing ○ Stop Buzzing

Door Linkage: on — ☑ Entrance: Unlock; □ Exit

Linked Alarm Output: on — ☑ Alarm Output1: Open; □ Alarm Output2

Figure 7-7 Event Linkage

2. 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.
3. Set linked action.

   Buzzer Linkage

   Enable **Buzzer Linkage** and select **Start Buzzing** or **Stop Buzzing** for the target event.

   Door Linkage

   Enable **Door Linkage**, check **Entrance** or **Exit**, and set the door status for the target event.

   Linked Alarm Output

Enable **Linked Alarm Output**, check **Alarm Output 1** or **Alarm Output 2**, and set the alarm output status for the target event.

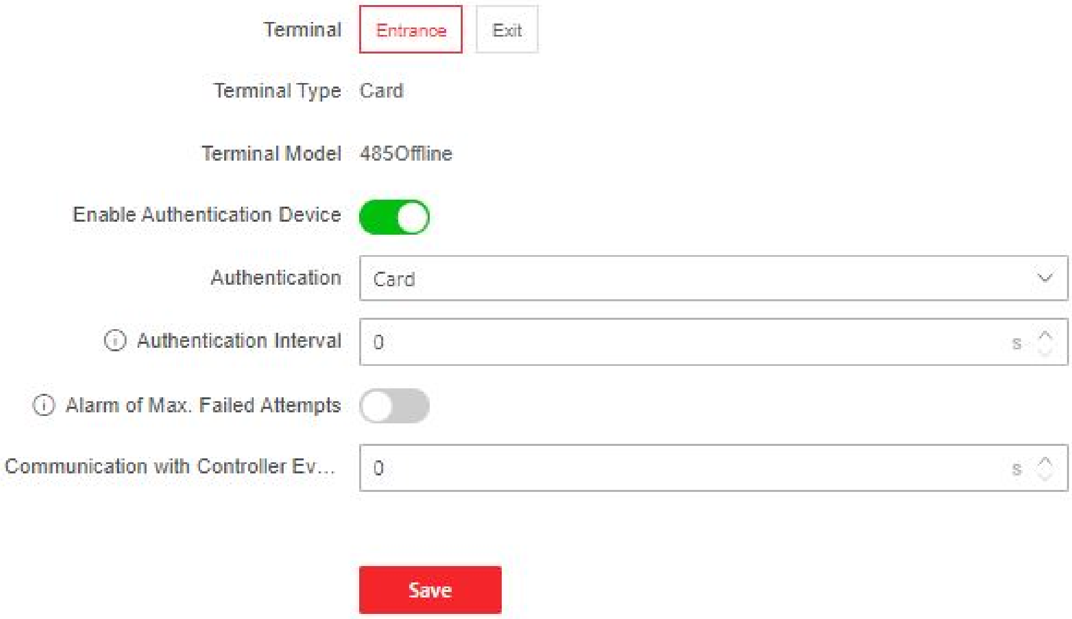
7.5.9 Access Control Settings

Set Authentication Parameters

Click **Configuration → Access Control → Authentication Settings** .

Note

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



Terminal: Entrance | Exit

Terminal Type: Card

Terminal Model: 485Offline

Enable Authentication Device: On

Authentication: Card

Authentication Interval: 0 s

Alarm of Max. Failed Attempts: Off

Communication with Controller Ev...: 0 s

Figure 7-8 Set Authentication Parameters

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

Terminal

Choose **Entrance** or **Exit** for settings.

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

Select an authentication mode according to your actual needs from the drop-down list.

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

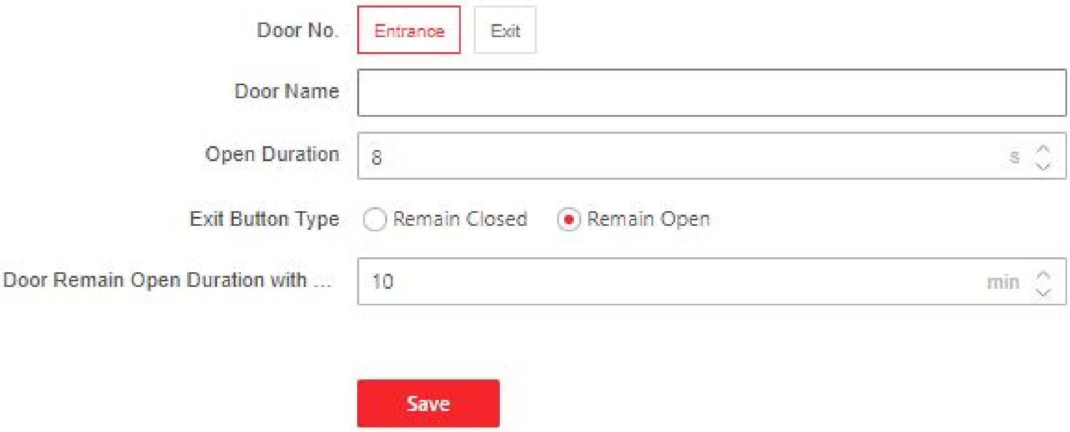
When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Note

The authentication interval value ranges from 2 s to 255 s.

Set Door Parameters

Click **Configuration → Access Control → Door Parameters** .



Door No. Entrance / Exit

Door Name

Open Duration 8 s

Exit Button Type ○ Remain Closed ● Remain Open

Door Remain Open Duration with ... 10 min

Figure 7-9 Door Parameters Settings Page

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

Door No.

Select **Entrance** or **Exit** for settings.

Door Name

You can create a name 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.

Note

The open duration ranges from 5 s to 60 s.

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**.

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.

Note

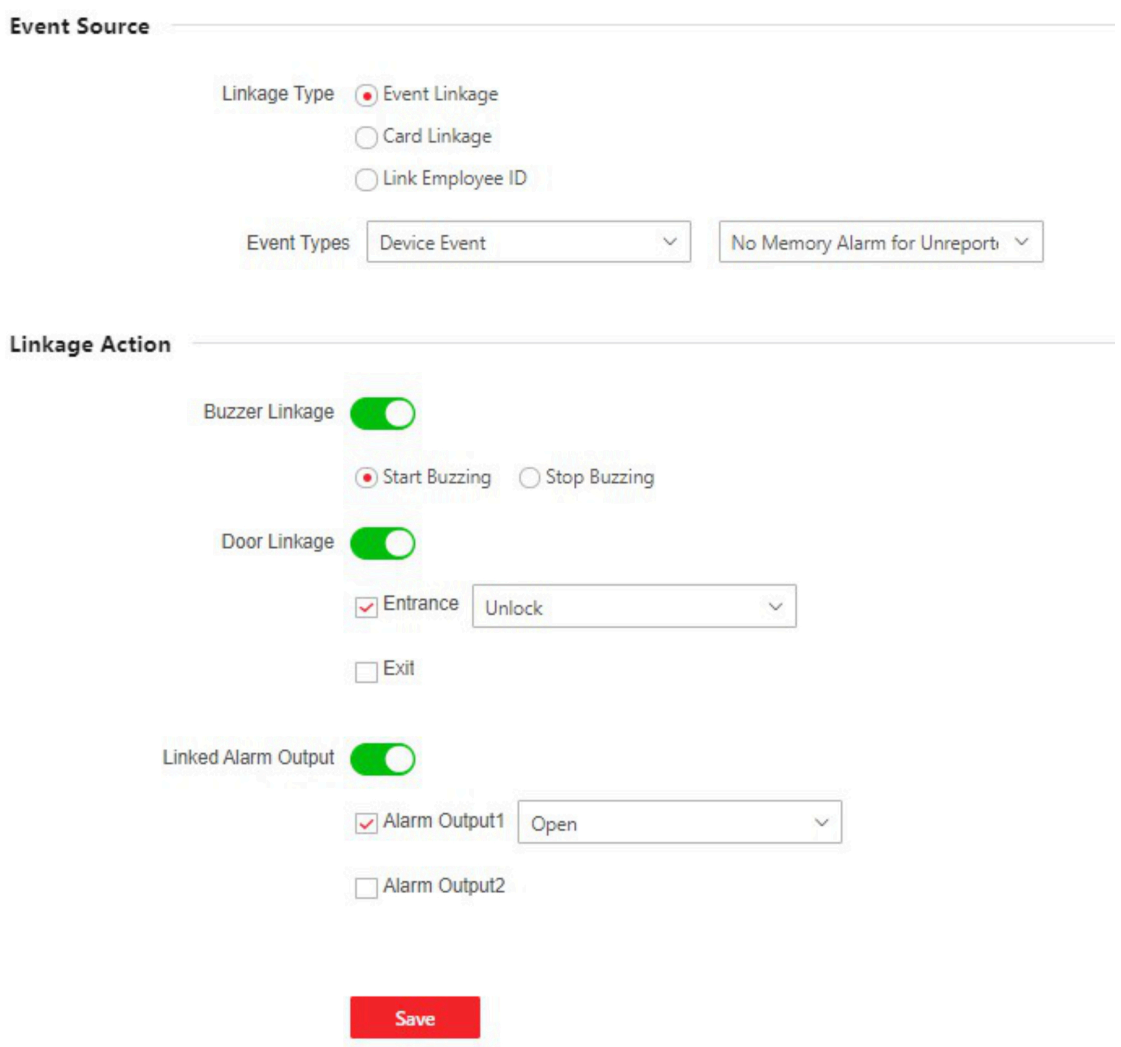
The duration ranges from 1 s to 1440 s.

Serial Port Settings

Set serial port parameters.

Steps

1. Click **Configuration → Access Control → Serial Port Settings** .



Event Source

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

Event Types: Device Event; No Memory Alarm for Unreport

Linkage Action

Buzzer Linkage: on — ● Start Buzzing ○ Stop Buzzing

Door Linkage: on — ☑ Entrance: Unlock; □ Exit

Linked Alarm Output: on — ☑ Alarm Output1: Open; □ Alarm Output2

Figure 7-10 Serial Port Settings

2. Set the **No.**, **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.
3. Set the **Peripheral Type** as **Card Reader**, **Card Receiver**, **QR Code Scanner** or **Disable**.
4. Set the **Peripheral Position** as **Entrance** or **Exit**.
5. You can view the serial port type, external device model and peripheral software version.
6. Click **Save**.

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 **Configuration → Access Control → Wiegand Settings** .
2. Select **Entrance** or **Exit**.
3. Enable **Wiegand** function.
4. The wiegand transmission direction is set **Input** by default.

   Note

   Input: the device can connect a Wiegand card reader.
5. Select **Wiegand Mode**.
6. Click **Save** to save the settings.

   Note

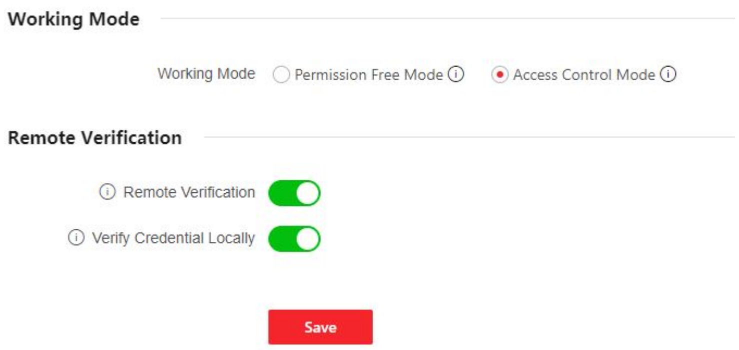
   If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Set Terminal Parameters

Set the working mode and remote verification.

Steps

1. Click **Configuration → Access Control → Terminal Parameters** to enter the page.



Working Mode

Working Mode ○ Permission Free Mode ⓘ ● Access Control Mode ⓘ

Remote Verification

ⓘ Remote Verification: on

ⓘ Verify Credential Locally: on

Figure 7-11 Terminal Parameters

2. Set the device working mode.

   Permission Free Mode

   The device will not verify the person's permission, but only the person's validity period. If the person is in the validity period, the barrier will open.

You can enable **Verify Credential Locally**. After enabling the function, the device will only verify the person's permission without the schedule template, etc.

Access Control Mode

The device works normally and will verify the person's permission to open the barrier.

3. Set remote verification.
   1) Enable **Remote Verification**.

   Note

   The device will upload the person's authentication information to the platform. The platform will judge to open the barrier or not.

   2) **Optional:** Enable **Verify Credential Locally**.

   Note

   After enabling the function, the device will only verify the person's permission without the schedule template, etc.

4. Click **Save** to complete terminal parameter settings.

7.5.10 Turnstile

Basic Parameters

Set turnstile basic parameters.

Steps

1. Click **Configuration → Turnstile → Basic Settings** to enter the page.
2. View the **Device Type**, **Device Model** and **Working Status**.
3. Set **Barrier Material**, **Lane Width**, **Barrier Height**, **Barrier Opening Speed** and **Barrier Closing Speed**.
4. Set the passing mode.
   - If you choose **General Passing**, you can select the barrier status for the entrance and exit from the drop-down list.

     Note

     If you set barrier-free mode, the barrier remains open and will close when authentication fails.

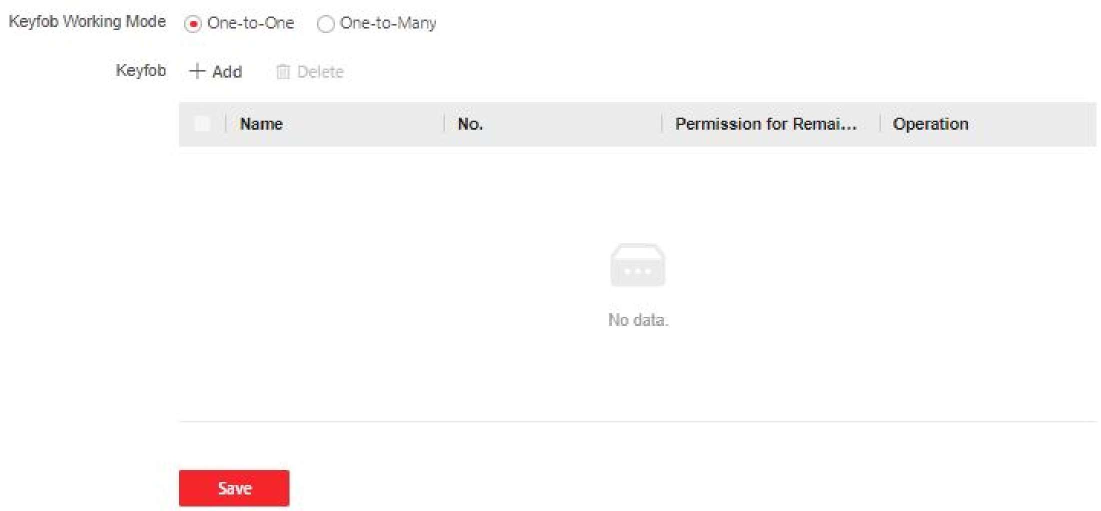
   - If you choose **Weekly Schedule**, you can set a weekly schedule for entrance and exit barriers.
5. Click **Save**.

keyfob

Set keyfob patameters.

Steps

1. Click **Configuration → Turnstile → Keyfob** to enter the page.



Keyfob Working Mode ● One-to-One ○ One-to-Many

Keyfob + Add Delete

□	Name	No.	Permission for Remai...	Operation

No data.

Save

Figure 7-12 keyfob

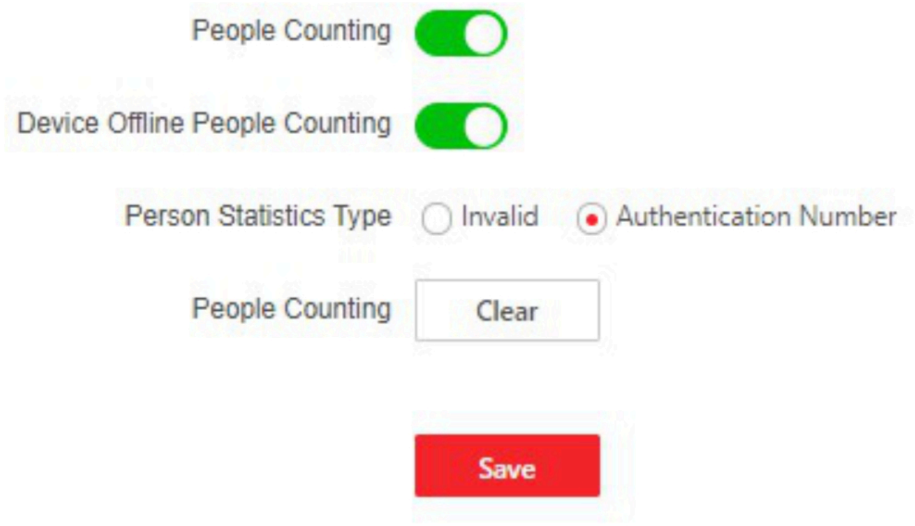
2. Set **Working Mode** as **One-to-One** or **One-to-Many**.
3. Add keyfob.
   1) Click **Add** and the keyfob adding window will pop up.
   2) Enter the **Name** and **Serial No.**.
   3) Check to enable **Remain Open Permission** at your actual needs.
   4) Click **OK** to add the keyfob.
4. **Optional:** Select a keyfob and click **Delete** to delete the keyfob.
5. Click **Save**.

People Counting

Set people counting .

Steps

1. Click **Configuration → Turnstile → People Counting** to enter the page.



People Counting

Device Offline People Counting

Person Statistics Type ○ Invalid ● Authentication Number

People Counting

Figure 7-13 People Counting

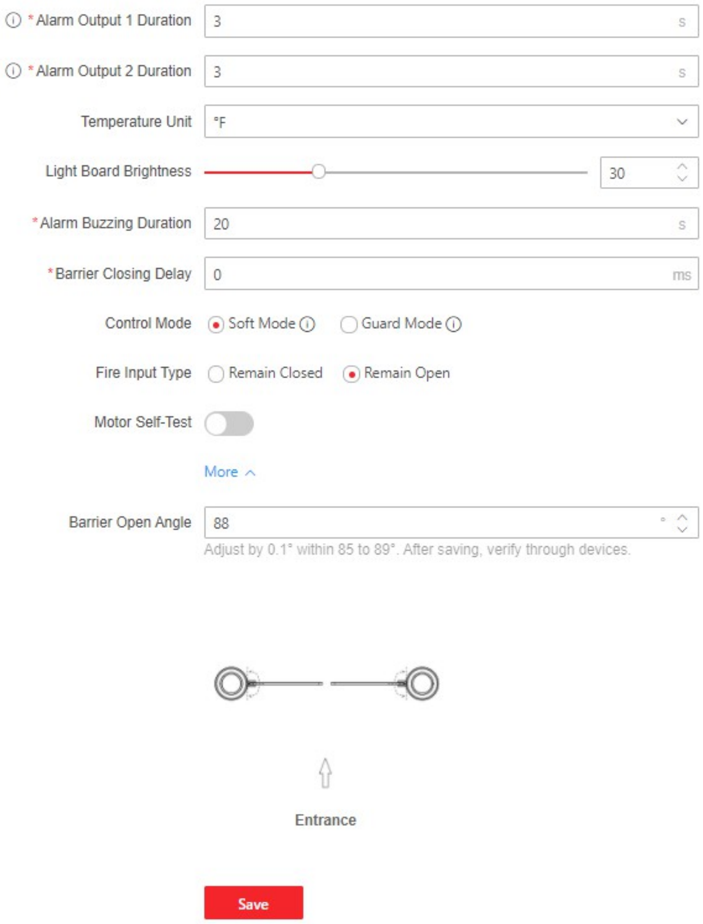
2. Enable **People Counting**.
3. Enable**Device Offline People Counting** at your actual needs.
4. Select **Person Statistics Type** as **Invalid** or **Authentication Number**.
5. **Optional:** Click **Clear** to clear all the people counting information.

Other Settings

Set other parameters.

Steps

1. Click **Configuration → Turnstile → Other Settings** to enter the page.



*Alarm Output 1 Duration	3 s
*Alarm Output 2 Duration	3 s
Temperature Unit	°F
Light Board Brightness	30
*Alarm Buzzing Duration	20 s
*Barrier Closing Delay	0 ms
Control Mode	● Soft Mode ○ Guard Mode
Fire Input Type	○ Remain Closed ● Remain Open
Motor Self-Test	
Barrier Open Angle	88 °

Adjust by 0.1° within 85 to 89°. After saving, verify through devices.

2. Set **Alarm Output Duration**.

Note

The alarm output duration ranges from 0 s to 3599 s.

3. Set **Temperature Unit**.
4. Drag the block or enter the value to adjust the light board brightness.
5. Set the alarm buzzer beeping duration, door closing delay time.
6. Choose the control mode.

   Soft Mode

   The barrier will be closed after the person has passed through the barrier.

   Guard Mode

   The barrier will be closed immediately.
7. Set the fire input type.
8. Click to enable **Motor Self-Test** and choose the main lane or sub lane to start motor self-testing.
9. Click **Save**.
10. Click **More** to adjust **Barrier Open Angle**.

7.5.11 Card Settings

Set Card Security

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

Set the parameters and click **Save**.

Enable NFC Card

Reserved.

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

After enable the DESFire card content reading function, 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 Authentication Parameters

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

Go to **Configuration → Card Settings → Card NO. Authentication Settings** .

Select a card authentication mode and enable reversed card No. at your actual needs. Click **Save**.

7.5.12 Set Privacy Parameters

Set the event storage type.

Go to **Configuration → Security → Privacy Settings**

The event storage type is overwriting by default. The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

7.5.13 Upgrade and Maintenance

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

Reboot Device

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

Upgrade

Click **Maintenance and Security → 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.

Note

Do not power off during the upgrading.

Restore Parameters

Click **Maintenance and Security → 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 network parameters and the user information.

Import and Export Parameters

Click **Maintenance and Security → 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.

7.5.14 Device Debugging

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security → 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.

7.5.15 Overview

You can view the main lane and sub lane status.

Main Lane Status

Device Component

You can view the status of the access control board, lane control board and user extended interface board.

Peripheral

You can view the status of the RS-485 card reader and RS-232 card receiver.

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Sub Lane Status

Device Component

You can view the status of the lane control board.

Peripheral

You can view the status of the RS-485 card reader and RS-232 card receiver.

Movement

You can view the working status of motor encoder.

Others

Passing Mode

You can view the entrance and exit mode.

Input and Output Status

You can view the status of the event input/output, alarm input/output and fire alarm.

Other Status

You can view the status of the barrier and the keyfob receiving module.

7.5.16 Log Query

You can search and view the device logs.

Go to **Maintenance and Security → 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.

7.5.17 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 Self-signed Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.

6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Key** area, and select a certificate from the local, and click **Import**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. 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 **Import CA Certificate** 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 8 Client Software Configuration

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

8.1 Configuration Flow of Client Software

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

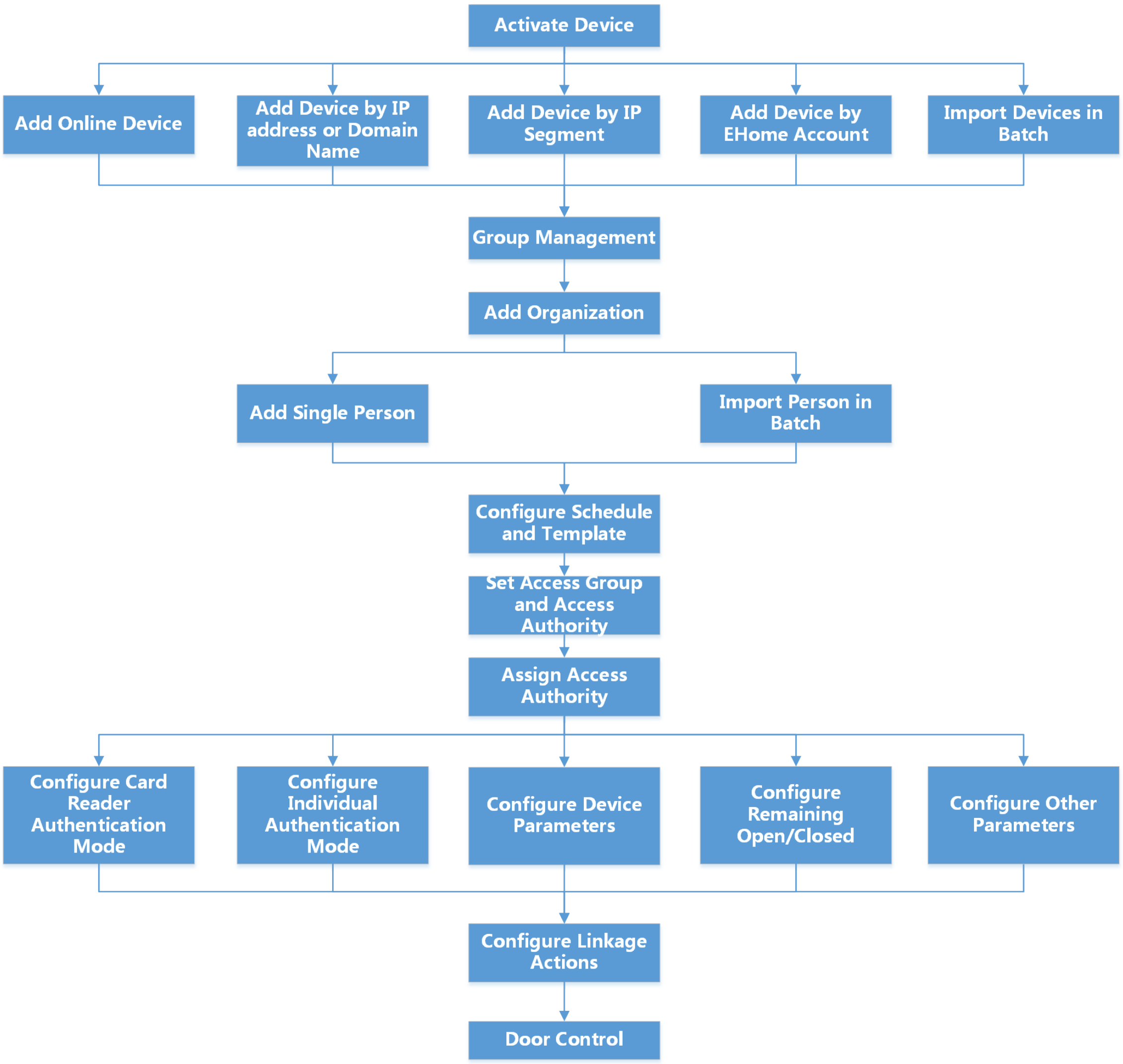

Activate Device
Add Online Device
Add Device by IP address or Domain Name
Add Device by IP Segment
Add Device by EHome Account
Import Devices in Batch
Group Management
Add Organization
Add Single Person
Import Person in Batch
Configure Schedule and Template
Set Access Group and Access Authority
Assign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

Figure 8-1 Flow Diagram of Configuration on Client Software

8.2 Device Management

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

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

8.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and ISUP protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.

   The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

   Name

   Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

   Address

   The IP address or domain name of the device.

   Port

   The devices to add share the same port number. The default value is ***8000***.

   Note

   For some device types, you can enter ***80*** as the port No. This function should be supported by the device.

   User Name

   Enter the device user name. By default, the user name is ***admin***.

   Password

Enter the device password.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you 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 installer and/or end-user.

5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See for details about enabling certificate verification.
- You can log into the device to get the certificate file by web browser.

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

Example

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.

Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.

5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

Note

For detailed description of the required fields, refer to the introductions in the template.

Adding Mode

Enter ***0*** or ***1*** or ***2***.

Address

Edit the address of the device.

Port

Enter the device port number. The default port number is ***8000***.

User Name

Enter the device user name. By default, the user name is ***admin***.

Password

Enter the device password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you 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 installer and/or end-user.

Import to Group

Enter ***1*** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter ***0*** to disable this function.

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

8.2.2 Reset Device Password

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

Steps

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

All the online devices sharing the same subnet will be displayed in the list.

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

Note

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

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you 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 installer and/or end-user.

8.2.3 Manage Added Devices

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

Table 8-1 Manage Added Devices

Edit Device	Click ✎ to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click **Delete** to delete the selected devices.
Remote Configuration	Click ⚙ to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click ▤ to view device status, including door No., door status, etc. **Note** For different devices, you will view different information about device status.

View Online User	Click 👤 to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click ↻ to refresh and get the latest device information.

8.3 Group Management

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

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

8.3.1 Add Group

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

Steps

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

   Note

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

8.3.2 Import Resources to Group

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

Before You Start
Add a group for managing devices. Refer to ***Add Group*** .

Steps

1. Enter the Device Management module.

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

Note

You can click ⊞ or ☰ to switch the resource display mode to thumbnail view or to list view.

6. Click **Import** to import the selected resources to the group.

8.4 Person Management

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

8.4.1 Add Organization

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

Steps

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

Note

Up to 10 levels of organizations can be added.

4. **Optional:** Perform the following operation(s).

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

Delete Organization
Hover the mouse on an added organization and click ✕ to delete it.

Note

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

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

8.4.2 Import and Export Person Identify Information

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

Import Person Information

You can enter the information of multiple persons in a predefined template (CSV/Excel file) to import the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.

Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

7. Click ... to select the CSV/Excel file with person information from local PC.
8. Click **Import** to start importing.

Note

- If a person No. already exists in the client's database, delete the existing information before importing.
- You can import information of no more than 2,000 persons.

Export Person Information

You can export the added persons' information to local PC as a CSV/Excel file.

Before You Start

- Make sure you have added persons to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button.

Steps

1. Enter the Person module.

2. **Optional:** Select an organization in the list.

   Note

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

3. Click **Export**.
4. Enter the super user name and password for verification.

   The Export panel is displayed.
5. Check **Person Information** as the content to export.
6. Check desired items to export.
7. Click **Export** to save the exported file in CSV/Excel file on your PC.

8.4.3 Get Person Information from Access Control Device

If the access control device has been configured with person information, you can get the person information from the added device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.

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

   Note

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

   Note

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

   Note

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

The person information, and the linked cards (if configured), will be imported to the selected organization.

8.4.4 Issue Cards to Persons in Batch

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

Steps

1. Enter **Person** module.
2. **Optional:** Select a person group, and select the persons with no card issued.
   - The selected persons with no card issued in the person group will be displayed in the right panel.
   - If you do not select the persons with no card issued in a person group, all the added persons with no card issued will be displayed in the right panel.
3. Click **Batch Issue Cards**.
4. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
5. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to *Issue a Card by Local Mode*.
6. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
7. Click the **Card No.** column and enter the card number.
   - Place the card on the card enrollment station.
   - Swipe the card on the card reader.
   - Manually enter the card number and press the **Enter** key.

   The person(s) in the list will be issued with card(s).

8.4.5 Report Card Loss

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

Steps

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

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

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

apply the changes to the device. After applying to device, these changes can take effect on the device.

8.4.6 Set Card Issuing Parameters

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

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

Local Mode: Issue Card by Card Enrollment Station

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

Card Enrollment Station

Select the model of the connected card enrollment station

Note

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

Card Type

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

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

Serial Port

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

Select the COM the card enrollment station connects to.

Buzzing

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

Card No. Type

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

M1 Card Encryption

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

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

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

8.5 Configure Schedule and Template

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

Note

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

8.5.1 Add Holiday

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

Steps

Note

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

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

   Note

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

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

      Note

      Up to 8 time durations can be set to one holiday period.
   3) **Optional:** Perform the following operations to edit the time durations.

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

4) **Optional:** Select the time duration(s) that need to be deleted, and then click ⊗ in the Operation column to delete the selected time duration(s).

5) **Optional:** Click 🗑 in the Operation column to clear all the time duration(s) in the time bar.

6) **Optional:** Click ☒ in the Operation column to delete this added holiday period from the holiday list.

6. Click **Save**.

8.5.2 Add Template

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

Steps

Note

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

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

   Note

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

   All-Day Authorized

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

   All-Day Denied

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

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

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

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

   Note

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

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

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

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

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

Note

Up to 4 holidays can be added to one template.

1) Click **Holiday** tab.
2) Select a holiday in the left list and it will be added to the selected list on the right panel.
3) **Optional:** Click **Add** to add a new holiday.

Note

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

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

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

8.6 Set Access Group to Assign Access Authorization to Persons

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

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to ***Group Management*** .
- Add template.

Steps

When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details.

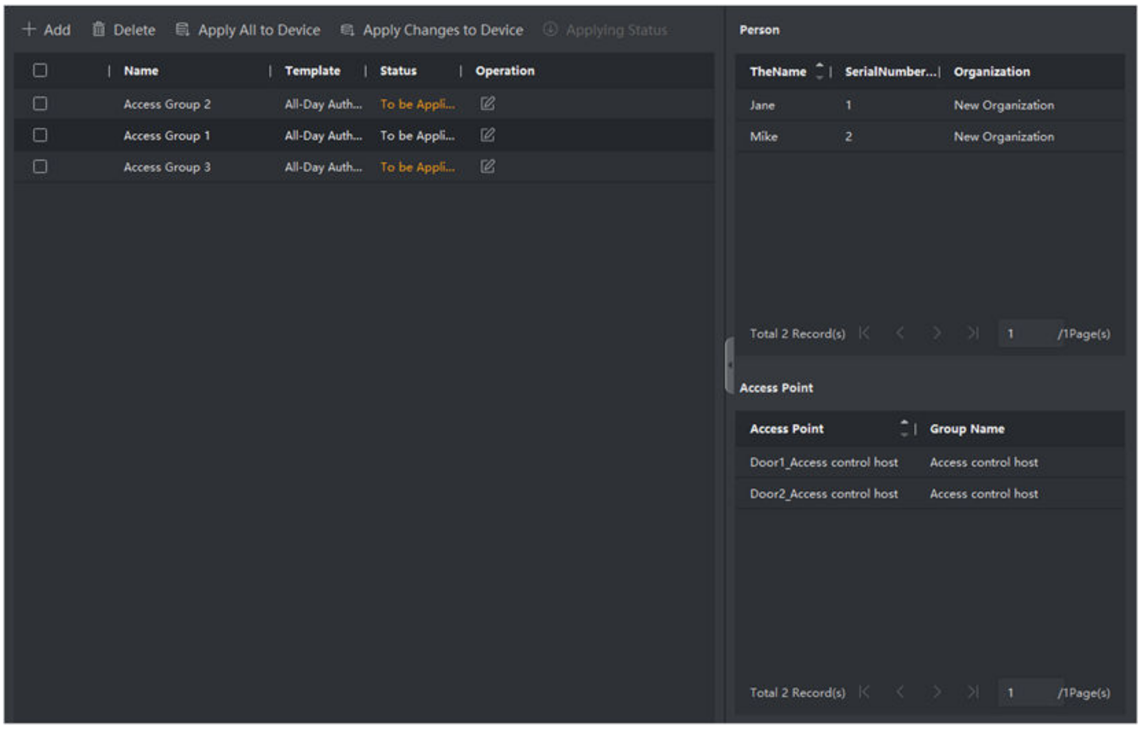
1. Click **Access Control → Authorization → Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

Note

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

5. In the left list of the Select Person field, select person(s) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

   You can view the selected person(s) and the selected access point(s) on the right side of the interface.



□	Name	Template	Status	Operation
□	Access Group 2	All-Day Auth...	To be Appli...	✎
□	Access Group 1	All-Day Auth...	To be Appli...	✎
□	Access Group 3	All-Day Auth...	To be Appli...	✎

Person

TheName	SerialNumber...	Organization
Jane	1	New Organization
Mike	2	New Organization

Total 2 Record(s) 1 /1Page(s)

Access Point

Access Point	Group Name
Door1_Access control host	Access control host
Door2_Access control host	Access control host

Total 2 Record(s) 1 /1Page(s)

Figure 8-2 Display the Selected Person(s) and Access Point(s)

8. After adding the access groups, you need to apply them to the access control device to take effect.
   1) Select the access group(s) to apply to the access control device.
   2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
   3) Click **Apply All to Devices** or **Apply Changes to Devices**.

   Apply All to Devices

   This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

   Apply Changes to Devices

This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).

4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

Note

You can check **Display Failure Only** to filter the applying results.

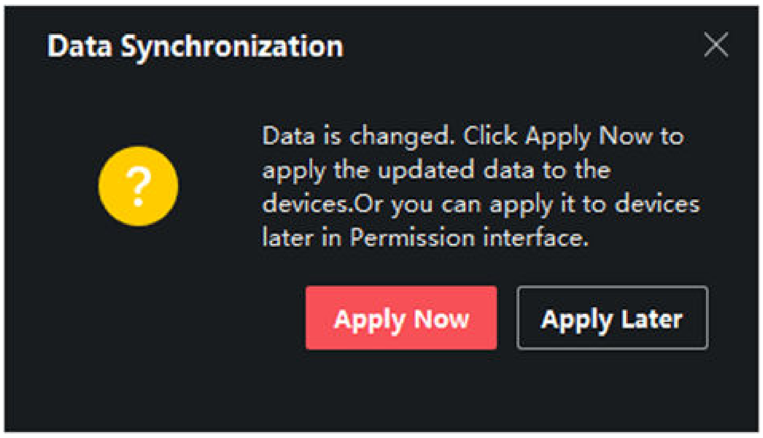
The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s).

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

Note

If you change the persons' access information or other related information, you will view the prompt **Access Group to Be Applied** on the right corner of the client.

You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.



Data Synchronization

Data is changed. Click Apply Now to apply the updated data to the devices.Or you can apply it to devices later in Permission interface.

Figure 8-3 Data Synchronization

8.7 Configure Advanced Functions

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

Note

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

8.7.1 Configure Device Parameters

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

Configure Parameters for Access Control Device

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

Before You Start

Add access control device to the client.

Steps

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

   Note

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

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

   Note

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

Enable NFC

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

Enable M1 Card

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

Enable EM Card

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

Enable CPU Card

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

Enable ID Card

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

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

Configure Parameters for Door/Elevator

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

Before You Start

Add access control device to the client.

Steps

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

   Note

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

   Name

   Edit the card reader name as desired.

   Exit Button Type

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

   Open Duration

   The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.
5. Click **OK**.
6. **Optional:** Click **Copy to** , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).

   Note

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

Configure Parameters for Card Reader

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

Before You Start

Add access control device to the client.

Steps

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

   Note

   - The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
   - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

   Name

   Edit the card reader name as desired.

   Card Authentication Interval

   The time interval between two continuous card recognitions when authenticating.

   Repeated Authentication Interval

   Within the specified interval, repeated authentication of the same card number (uploaded by different devices) is invalid, and only one authentication is performed.

   Enable Failed Attempts Limit of Authentication/Max. Failed Attempts for Authentication

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

   Card Reader Type/Card Reader Description

   Get card reader type and description. They are read-only.
4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Output

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

Before You Start

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

Steps

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

   Name

   Edit the card reader name as desired.

   Alarm Output Active Time

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

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Before You Start

Add access control device to the client.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

   Passing Mode

   Select the controller which will control the barrier status of the device.

   Opening/Closing Barrier Speed

   Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.

   Note

   The recommended value is 6.

   Alarm Voice Prompt Time Duration

   Set how long the audio will last, which is played when an alarm is triggered .

   Note

   0 refers to the alarm audio will be played until the alarm is ended.

Temperature Unit

Select the temperature unit that displayed in the device status.

Lightboard Brightness

Adjust the brightness of the device light.

Barrier Material

Select the material of the barrier gate. You can select the barrier material from the drop-down list.

Note

The barrier material may affect the device working. Select a correct barrier material or the barrier may not open.

Lane Length

The width of the lane. You can set the lane width.

Note

The lane width may affect the device working. Set a correct lane width or the barrier may not open.

4. Click **OK**.

8.7.2 Configure Device Parameters

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

Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Before You Start

Add access control device to the client, and make sure the device supports RS-485 interface.

Steps

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, and connection mode in the drop-down list.
6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - When you change the connection mode, the device will reboot automatically.

Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

Before You Start

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

Steps

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
4. Set the switch to on to enable the Wiegand function for the device.
5. Select the Wiegand channel No. and the communication mode from the drop-down list.

   Note

   If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.
6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - After changing the communication direction, the device will reboot automatically.

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

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

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

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

8.8 Door/Elevator Control

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

Note

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

8.8.1 Control Door Status

You can control the status for the door(s), including unlock door, locking door, remaining the door unlock, remaining the door locked, remain all unlocked, etc.

Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (doors). For details, refer to ***Person Management*** and ***Set Access Group to Assign Access Authorization to Persons*** .
- Make sure the operation user has the permission of the access points (doors).

Steps

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

   Note

   For managing the access point group, refer to ***Group Management*** .

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

   Note

   For **Remain All Unlocked** and **Remain All Locked**, ignore this step.
4. Click the following buttons to control the door.

   Unlock Door

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

   Lock Door

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

Remain Unlocked

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

Remain Locked

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

Remain All Unlocked

All doors in the group will be unlocked (no matter closed or open). All the persons can access the doors with no credentials required.

Remain All Locked

All doors in the group will be closed and locked. No person can access the doors even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client.

Remotely Unlocking Door Station

When the group includes door stations, you can check **Lock1** or **Lock2**, then click **Unlock Door** to unlock the door station.

Note

By default, **Lock1** is checked for door stations.

Refresh Status

Click **Refresh Status** to get the door's newest status.

Result

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

8.8.2 Check Real-Time Access Records

The real-time access records can be displayed in the client. Also, you can view the person information.

Before You Start

You have added person(s) and access control device(s) to the client. For details, refer to ***Person Management*** and ***Add Device*** .

Steps

1. Click **Monitoring** to enter monitoring module.

   Real-time access records are displayed on the bottom of the page. You can view record details

   Note

   You can right click the column name of access event table to show or hide the column according to actual needs.

2. **Optional:** Select an access point group from the drop-down list in the upper-right corner to show the real time access records of the selected group.
3. **Optional:** Check the event type and event status.

   The detected events of checked type and status will be displayed in the list below.

4. **Optional:** Check **Show Latest Event** to view the latest access record.

   The record list will be listed reverse chronologically.

5. **Optional:** Click ⧉ to view details.

   Note

   In the pop-up window, you can click □ to view details in full screen.

Appendix A. DIP Switch

A.1 DIP Switch Description

The DIP switch is on the access control board. No.1 and No 2 is from the low bit to the high bit.

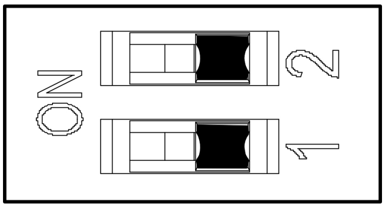


Figure A-1 DIP Switch

When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off.

Appendix B. Button Configuration Description

Refer to the table below for device configuration via button on the lane control board.

Level-1 Configuration No.	Description	Level-2 Configuration No. and Functions	Notes
1	Study Mode	1-Exit Study Mode/ Normal Mode 2-Study Mode **Note** By default, 1 will be displayed on the display screen.	
2	keyfob Pairing Mode	1-Normal Mode 2-Pairing Mode **Note** By default, 1 will be displayed on the display screen.	
3	Passing Mode	1-Both sides under control **Note** By default, 1 will be displayed on the display screen. 2-Entrance under control; exit prohibited 7-Both sides prohibited 8-Entrance prohibited; exit under control 10-Entrance under control; exit remaining open	

Level-1 Configuration No.	Description	Level-2 Configuration No. and Functions	Notes
		14-Entrance prohibited; exit remaining open 16-Entrance remaining open; exit under control 18-Entrance remaining open; exit remaining open 20-Entrance remaining open; exit prohibited	
4	Memory Mode	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	
5	keyfob Remote Control	1-one to one 2-one to multiple **Note** By default, 2 will be displayed on the display screen.	
6	Barrier Opening Speed	1-1, 2-2, …10-10 **Note** By default, 5 will be displayed on the display screen.	
7	Barrier Closing Speed	1-1, 2-2, …10-10	

Level-1 Configuration No.	Description	Level-2 Configuration No. and Functions	Notes
		Note By default, 5 will be displayed on the display screen.	
8	Card Reading on the Alarm Area	1-Do not open 2-Open **Note** By default, 2 will be displayed on the display screen.	
9	Enter Duration	5-5s，6-6s，7-7s, ..., 60-60s **Note** By default, 5 will be displayed on the display screen.	
10	Exit Duration	5-5s，6-6s，7-7s, ..., 60-60s **Note** By default, 5 will be displayed on the display screen.	
21	Volume	1-0， 2-1， 3-2， 4-3， 5-4 **Note** By default, 2 will be displayed on the display screen.	The device will be muted when set to "1".
36	Barrier Material	1-Acrylic 2-Glass	

Level-1 Configuration No.	Description	Level-2 Configuration No. and Functions	Notes
		Note By default, 1 will be displayed on the display screen.	
37	Barrier Length	1-550 2-600 3-650 4-700 5-750 6-800 7-850 8-900 9-950 10-1000 11-1100 12-1200 13-1300 14-1400 **Note** By default, 8 will be displayed on the display screen.	
38	Motor Inspection	1-Disable 2-Enable on Main Lane 3-Enable on Sub Lane **Note** By default, 1 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-2 Configuration No. and Functions	Notes
39	Brightness of Light	0-0， 1-1， 2-2, … , 10-10 **Note** By default, 3 will be displayed on the display screen.	The higher the value is, the brighter the light will be.
40	Self-check Voice Prompt	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	
41	Study Mode Voice Prompt	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.	
43	Application Mode	1-Wind-proof 2-Indoor **Note** By default, 1 will be displayed on the display screen.	
44	Barrier Recover Duration	1-Normal Speed 2-Fast Recover **Note** By default, 1 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-2 Configuration No. and Functions	Notes
45	Brake	1-Disable 2-Barrier Position Exception 3-Intrusion **Note** By default, 2 will be displayed on the display screen.	
46	Brake Angle	1-5° 2-10° 3-15° **Note** By default, 1 will be displayed on the display screen.	
48	Fan	1-Disabled 2-Enabled **Note** By default, 2 will be displayed on the display screen.	
49	Barrier Height	1-700 2-1200 3-1400 4-1600 5-1800 **Note** By default, 5 will be displayed on the display screen.	

Level-1 Configuration No.	Description	Level-2 Configuration No. and Functions	Notes
50	Main Lane or Sub Lane	1-Main Lane 2-Sub Lane **Note** By default, 1 will be displayed on the display screen.	
51	Combination Mode	1-Main and Sub Lane 2-Single Main Lane **Note** By default, 1 will be displayed on the display screen.	
52	Barrier Open Mode	1-Normal 2-Reverse Barrier Opening **Note** By default, 1 will be displayed on the display screen.	
53	Mechanical Anti-Pinch Recover Duration	1-1 s 2-2 s 3-3 s 4-4 s 5-5 s **Note** By default, 3 will be displayed on the display screen.	
99	Restore to Default	1-Default 2-Start	

Level-1 Configuration No.	Description	Level-2 Configuration No. and Functions	Notes
		Note By default, 1 will be displayed on the display screen.	

Note

- When the Configuration No. 50 and 51 are adjusted, you need to reboot the device manually.

Appendix C. Event and Alarm Type

Event	Alarm Type
Passing Timeout	None
Barrier Obstructed	None

Appendix D. Table of Audio Index Related Content

Index	Content
1	Authenticated.
2	Card No. does not exist.
3	Passing timeout.
4	No permissions.
5	Authentication time out.
6	Authentication failed.
7	Expired card.

Appendix E. Error Code Description

The swing gate will display the error code on the seven-segment display if error occurred. Refer to the table below to find the description of each number.

Error Reason	Code	Error Reason	Code
Interconnecting Exception	53	Not Studying	54
Obstruction	55	Exceeding Studying Range	56
Encoder Exception	57	Motor Exception	58
Optional Board Offline (If the board is not installed, the error code of "59" will appear but the device functions normally)	59		

See Far, Go Further