



DS-K3B220X Series Swing Barrier

User Manual

Legal Information

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

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

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

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

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

Data Protection

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

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

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.

If the top caps should be open and the device should be powered on for maintenance, make sure:

1. Power off the fan to prevent the operator from getting injured accidentally.
 2. Do not touch bare high-voltage components.
 3. Make sure the switch's wiring sequence is correct after maintenance.
- 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 100% 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	Description
Swing Barrier	DS-K3B220X-L	Left Pedestal
	DS-K3B220X-M	Middle Pedestal
	DS-K3B220X-R	Right Pedestal

Contents

Chapter 1 Overview	1
1.1 Introduction	1
1.2 Main Features	1
Chapter 2 System Wiring	3
Chapter 3 Installation	6
Chapter 4 General Wiring	10
4.1 Components Introduction	10
4.2 Wiring	11
4.3 Terminal Description	12
4.3.1 Main Lane Control Board Terminal Description	12
4.3.2 Sub Lane Control Board Terminal Description	13
4.3.3 Access Control Board Terminal Description	14
4.3.4 Sub Optional Board Terminal Description (Optional)	16
4.3.5 Card Reader Board Terminal Description	16
4.3.6 Main Optional Board Terminal Description (Optional)	17
4.3.7 General Wiring	18
4.3.8 RS-485 Wiring	19
4.3.9 RS-232 Wiring	20
4.3.10 Alarm Input Wiring	21
4.3.11 Exit Button Wiring	21
4.4 Device Settings	22
4.4.1 Configuration via Button	23
4.4.2 Normal/Study Mode Settings	26
4.4.3 Keyfob Pairing	28
4.4.4 Initialize Device	30
Chapter 5 Activation	32

5.1 Activate via SADP	32
5.2 Activate Device via iVMS-4200 Client Software	33
Chapter 6 Operation via Web Browser	35
6.1 Login	35
6.2 Live View	35
6.3 Person Management	37
6.4 Search Event	38
6.5 Configuration	40
6.5.1 View Device Information	40
6.5.2 Set Time	40
6.5.3 Set DST	41
6.5.4 Change Administrator's Password	41
6.5.5 Online Users	41
6.5.6 View Device Arming/Disarming Information	42
6.5.7 Network Settings	42
6.5.8 Event Linkage	44
6.5.9 Access Control Settings	45
6.5.10 Turnstile	49
6.5.11 Card Settings	53
6.5.12 Set Privacy Parameters	55
6.5.13 Upgrade and Maintenance	55
6.5.14 Device Debugging	56
6.5.15 Component Status	56
6.5.16 Log Query	58
6.5.17 Certificate Management	59
Chapter 7 Client Software Configuration	61
7.1 Configuration Flow of Client Software	61
7.2 Device Management	62

7.2.1 Add Device	62
7.2.2 Reset Device Password	64
7.2.3 Manage Added Devices	65
7.3 Group Management	66
7.3.1 Add Group	66
7.3.2 Import Resources to Group	66
7.4 Person Management	67
7.4.1 Add Organization	67
7.4.2 Import and Export Person Identify Information	68
7.4.3 Get Person Information from Access Control Device	70
7.4.4 Issue Cards to Persons in Batch	71
7.4.5 Report Card Loss	72
7.4.6 Set Card Issuing Parameters	72
7.5 Configure Schedule and Template	73
7.5.1 Add Holiday	73
7.5.2 Add Template	74
7.6 Set Access Group to Assign Access Authorization to Persons	76
7.7 Configure Advanced Functions	78
7.7.1 Configure Device Parameters	78
7.7.2 Configure Other Parameters	85
7.8 Door/Elevator Control	88
7.8.1 Control Door Status	88
7.8.2 Check Real-Time Access Records	90
Appendix A. DIP Switch	92
A.1 DIP Switch Description	92
A.2 DIP Switch Corresponded Functions	92
Appendix B. Button Configuration Description	93
Appendix C. Event and Alarm Type	99

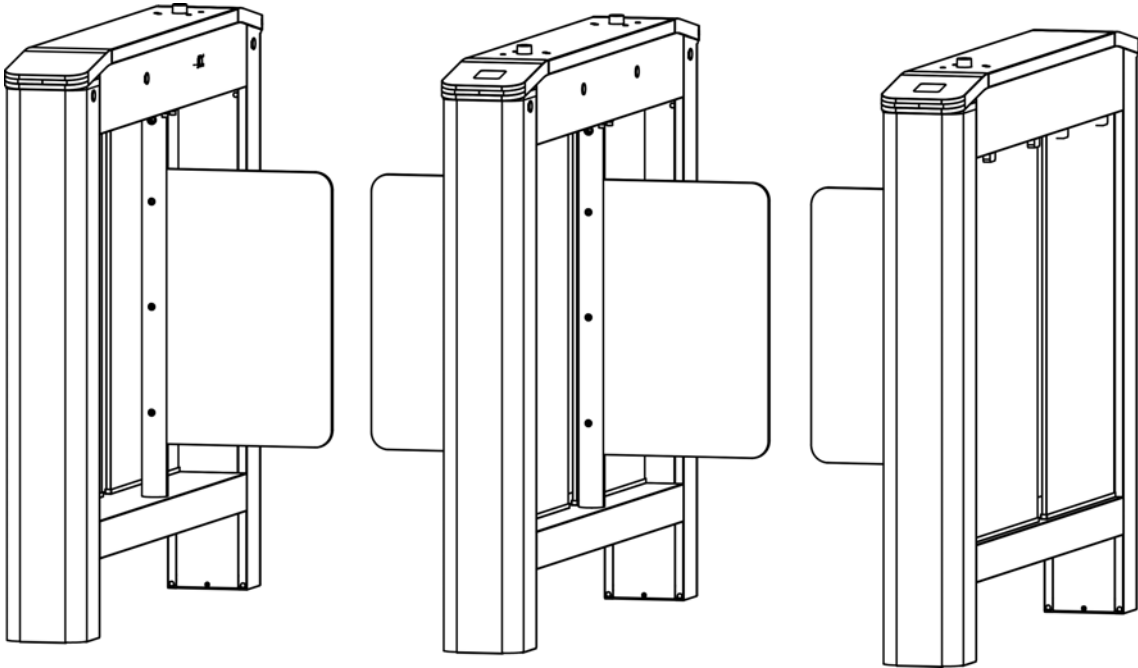
Appendix D. Table of Audio Index Related Content 100

Appendix E. Error Code Description 101

Appendix F. Communication Matrix and Device Command 102

Chapter 1 Overview

1.1 Introduction



The flap barrier with two barriers and 12 IR lights is designed to detect unauthorized entrance or exit. By adopting the flap barrier integratedly with the access control system, person should authenticate to pass through the lane via swiping IC or ID card, scanning QR code, etc. It is widely used in attractions, stadiums, construction sites, residences, etc.

1.2 Main Features

- Control mode, free passing mode and prohibition mode selectable on both entering and exiting direction.
- The barrier will be locked or stop working when people are nipped
- Anti-forced-accessing
The barrier will be locked automatically without open-barrier signal.
- Self-detection, Self-diagnostics, and automatic alarm
- Audible and visual alarm will be triggered when detecting intrusion, tailgating, reverse passing, and climbing over barrier
- LED indicates the entrance/exit and passing status
- Barrier is in free status when powered down; If the device is installed with lithium battery (optional), the barrier remains open when powered down

- 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
- Adjustable indicator brightness
- Bidirectional (Entering/Exiting) 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
- Permissions validation and anti-tailgating
- Remote barrier opening via keyfob and broadcasting via loudspeaker when the keyfob kit (optional) is installed.

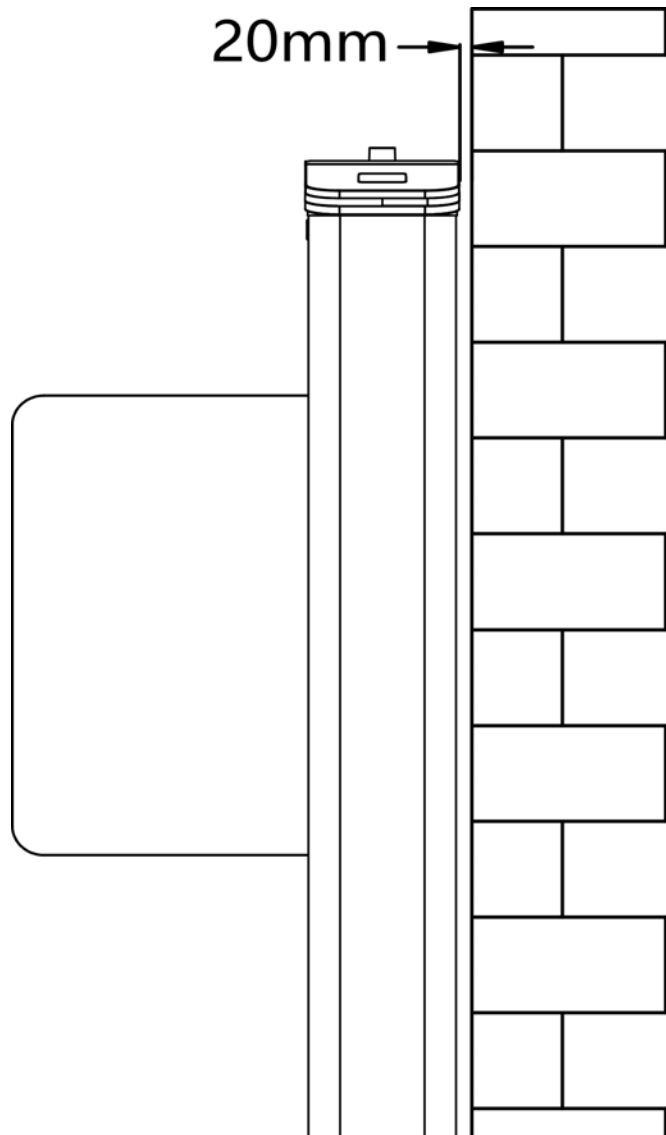
Chapter 2 System Wiring

The preparation before installation and general wiring.

Steps

Note

- The device should be installed on the concrete surface or other non-flammable surfaces.
- 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, or you cannot open the pedestal's top panel.



- The dimension is as follows.

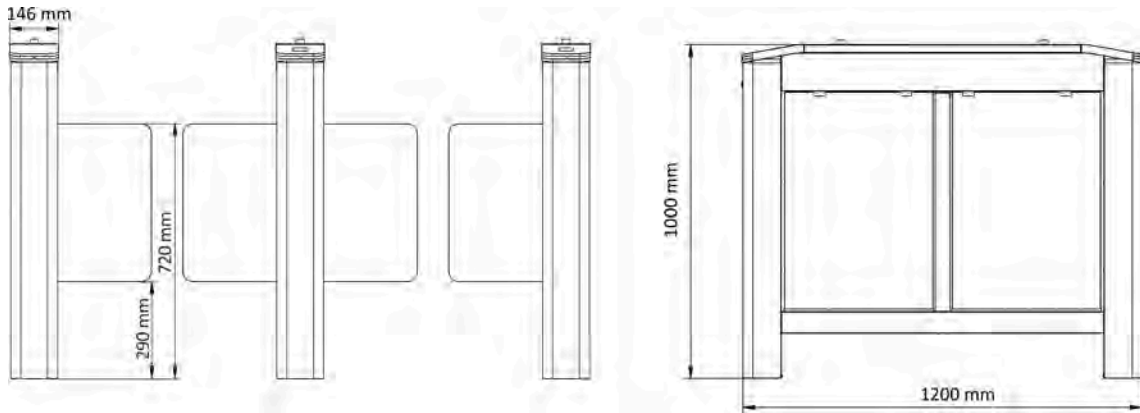


Figure 2-1 Dimension

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 $L + 146$ mm. L represents the lane width.

3. Slot on the installation surface and dig installation holes. Put 4 expansion bolts of M12*120 for each pedestal.

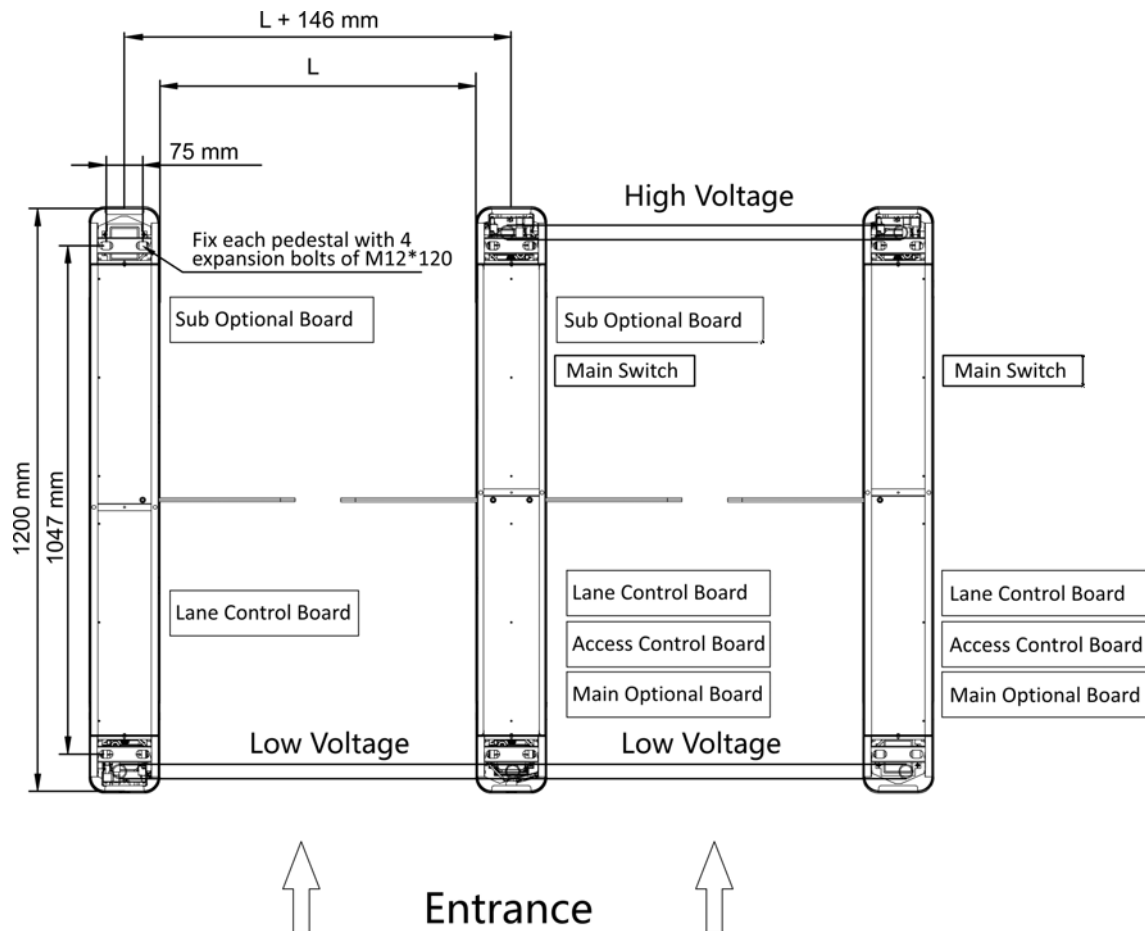


Figure 2-2 Hole Position and System Wiring

4. Bury cables. Each lane buries 1 high voltage cable and 1 low voltage cable. For details, see the system wiring diagram of step 3.

 Note

- High voltage: AC power input
Low voltage: interconnecting cable (communication cable and 24 V power cable) and network communication cable
- The supplied 24 V power cable length is 2.5 m and the communication cable length is 3 m.
- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- If you want to bury both of the AC power cord and the low voltage cable, the two cables should be in separated conduits to avoid interference.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.
- The external AC power cord should be double-insulated.
- The network cable must be CAT5e or the network cable has better performance.

Chapter 3 Installation

1. Before installation, you should unscrew and disassemble the pedestal.

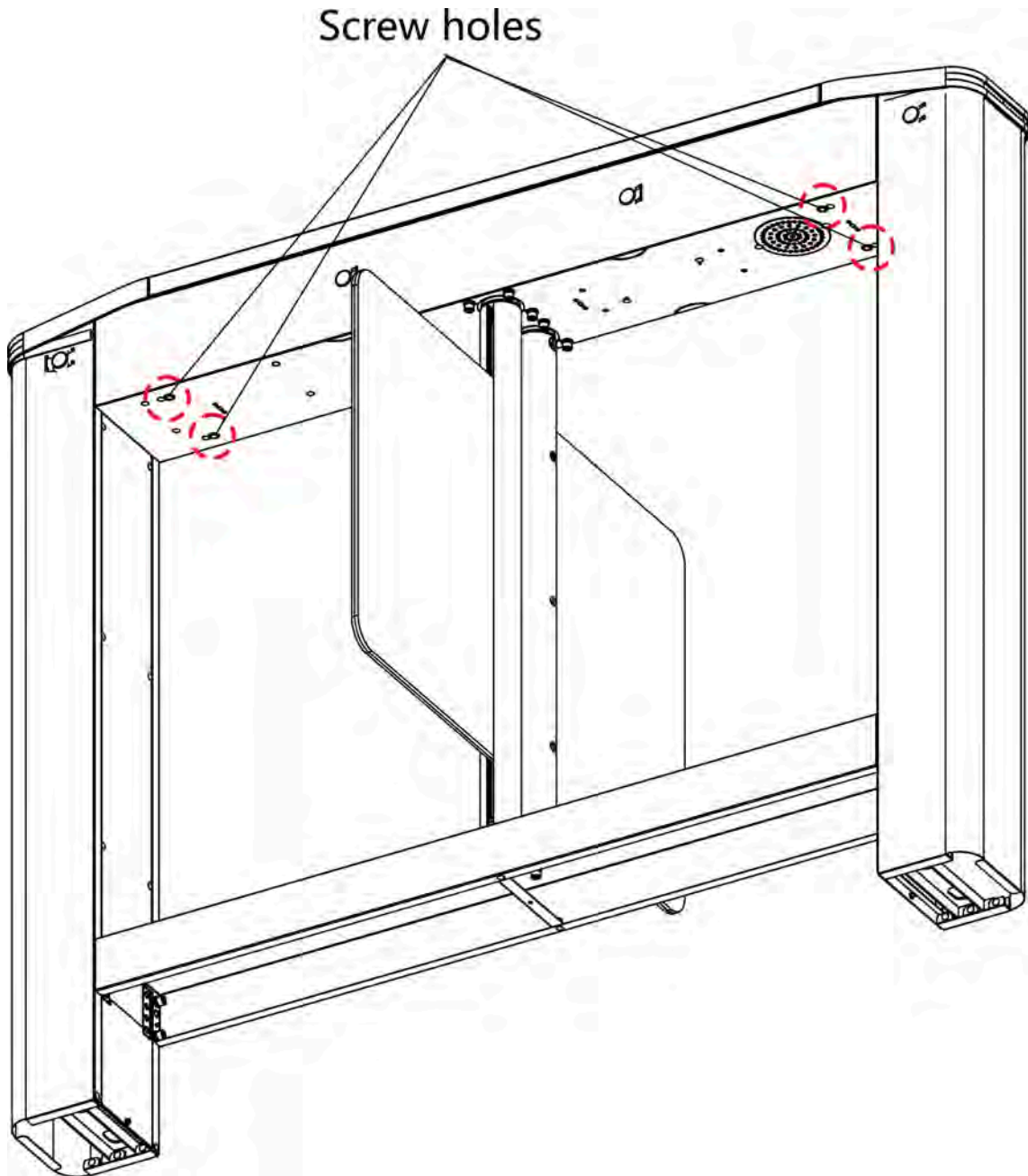


Figure 3-1 Screw Hole

2. Keep the disassembled components and make sure the accessories are intact.
3. Prepare for system wiring and installation. For details, see **System Wiring**.

4. Place the pedestal above the embedded expansion bolt. Unscrew and remove the maintenance door.

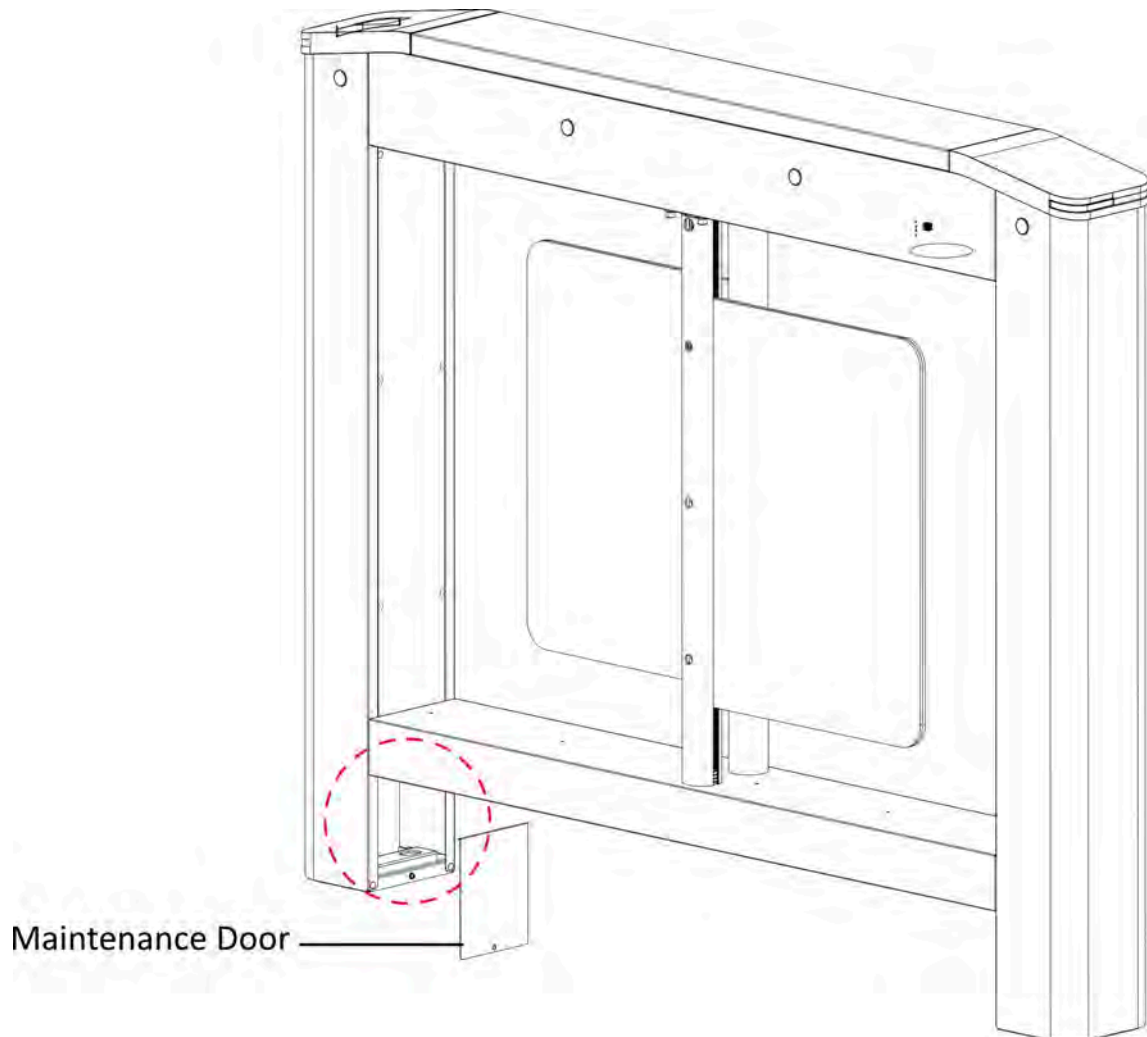


Figure 3-2 Maintenance Door

5. Place the platen on the expansion bolt and adjust the position of the pedestal to make sure the platen fits well to the bottom of the pedestal.

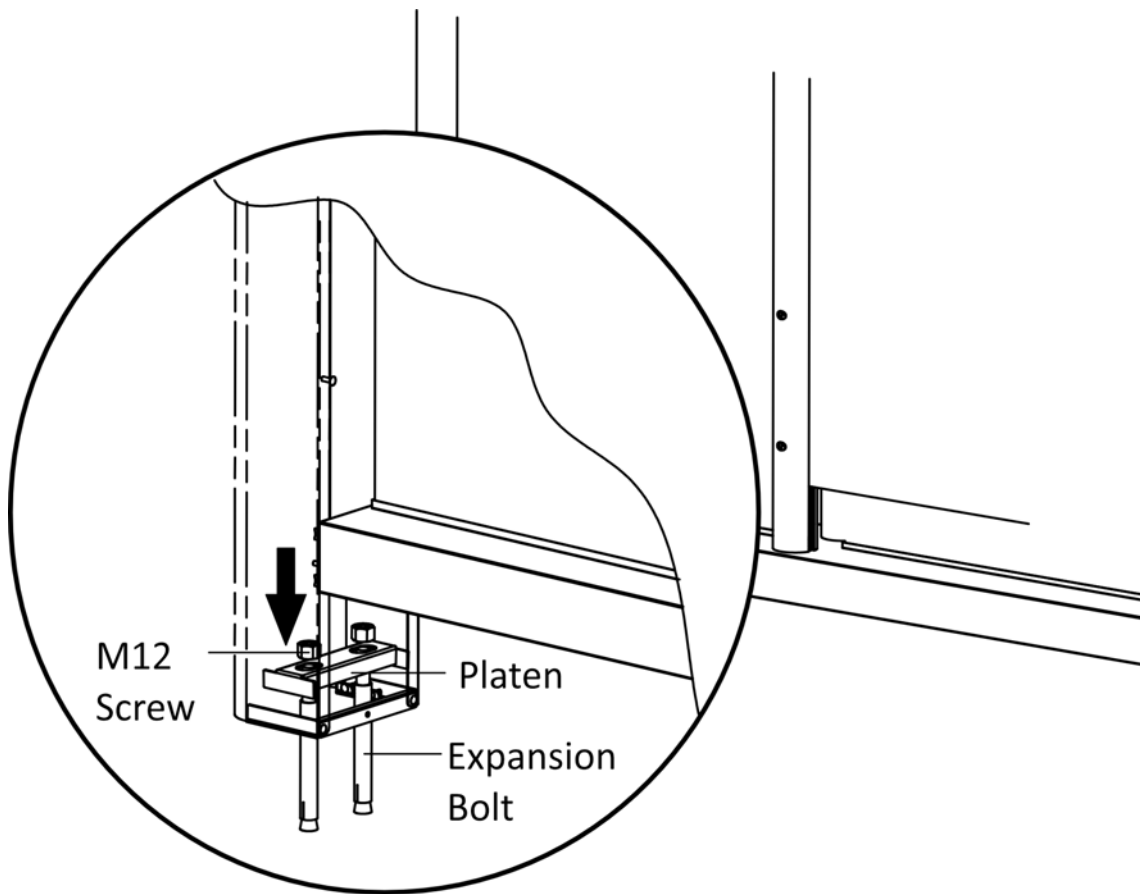


Figure 3-3 Platen

6. Fasten the nuts of the expansion bolts with a screwdriver (shank length more than 120 mm) and reinstall the maintenance door.

Scan the QR Code to view the side board installation guide video.



Chapter 4 General Wiring

Note

- When you should maintain or disassemble the high voltage modules, you should remove the entire high voltage modules and maintain it outside the turnstile. You should unplug the cables that connected to the peripherals before maintenance to avoid destroy of the device.
- When disassembling the high voltage module, you should disconnect the power to avoid injury.

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

The voltage fluctuation of the electric supply is between 100 VAC and 260 VAC, 50 to 60 Hz.

The picture displayed below describes the serial port on the entrance and exit direction.

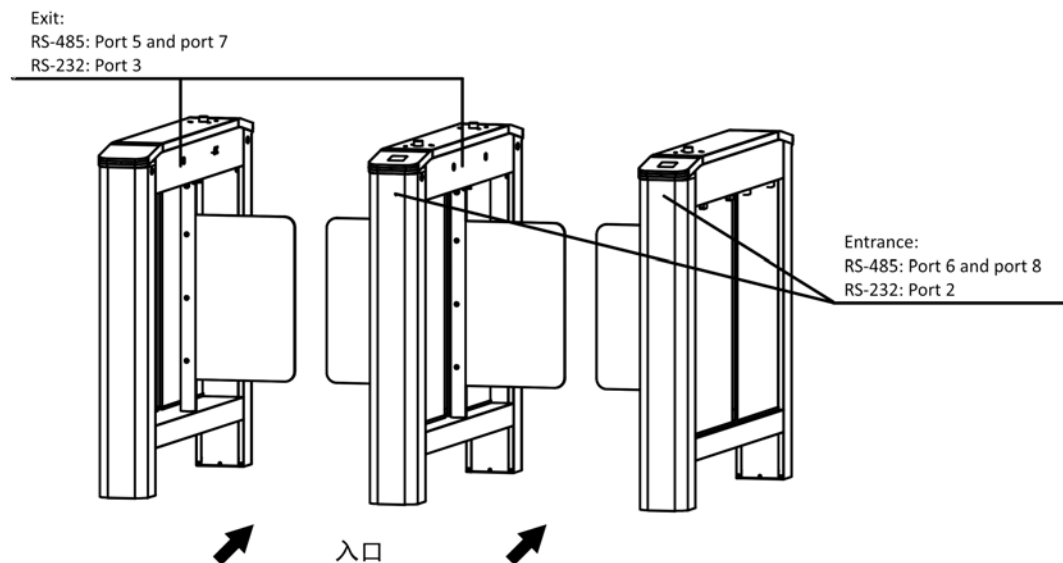


Figure 4-1 Serial Port

The picture displayed below describes the IR sending/receiving module and their corresponding number on the pedestal.

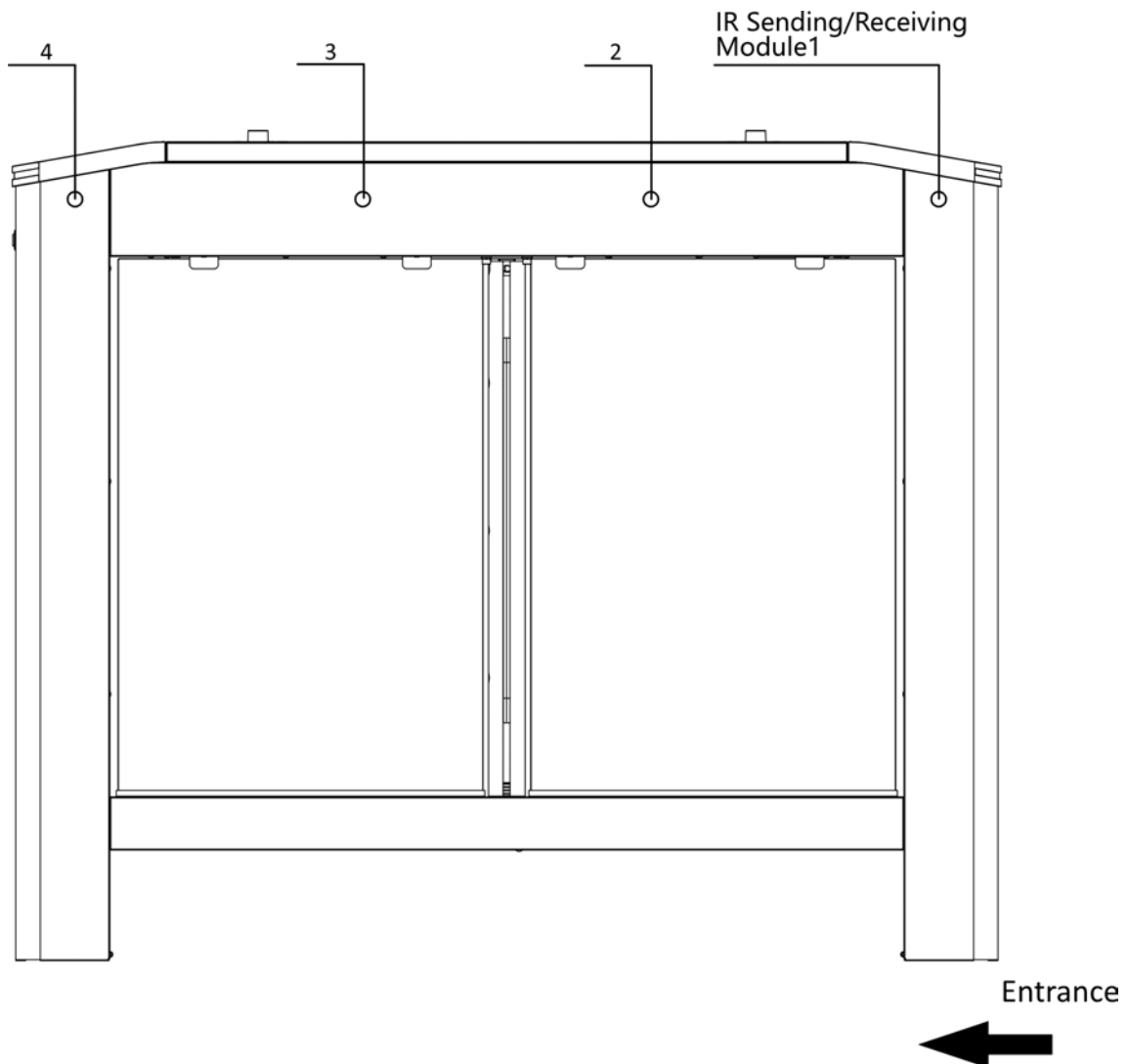


Figure 4-2 IR Sending/Receiving Module Position

Note

If the turnstile contains two lanes, standing at the entrance position, the IR modules on the left pedestal are the IR sending modules. The IR modules on the right pedestal are the IR receiving modules. The IR modules on the left side of the middle pedestal are the IR receiving modules, while the IR modules on the right side of the middle pedestal are the IR sending modules.

4.2 Wiring

Scan the QR code to view the wiring guide video of peripheral devices.



4.3 Terminal Description

The lane controller contains main lane controller and sub lane controller, which controls the IR beams, motor, and other components' work.

4.3.1 Main Lane Control Board Terminal Description

The main lane control board contains interconnecting interface, USB flash drive interface (reserved), access control board interface, fire input interface, exit button interface, 12 VDC output interface (reserved), 24 VDC input interface, fan interface, communication interface, encoder interface, power supply interface for motor, supercapacitor interface, IR adaptor interface and light bar interface.

The picture displayed below is the main lane control board diagram.

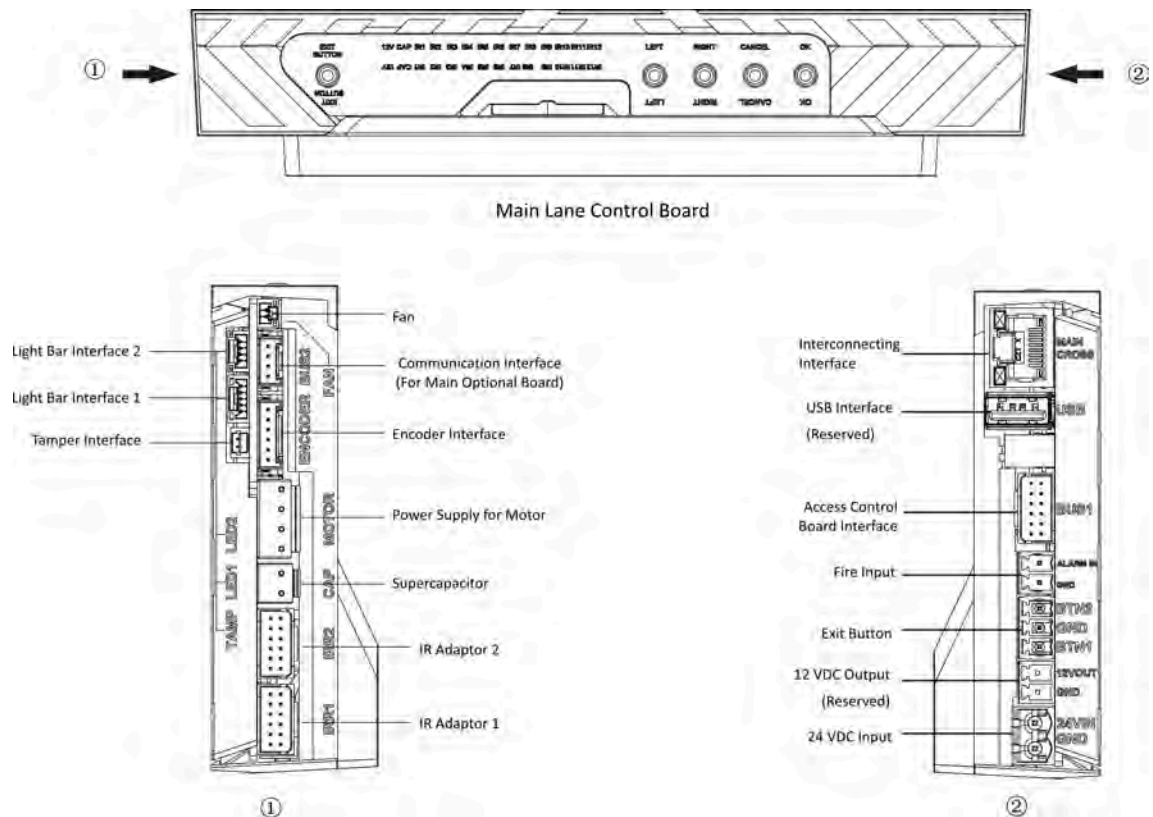


Figure 4-3 Main Lane Control Board Terminals

4.3.2 Sub Lane Control Board Terminal Description

The sub lane control board contains interconnecting interface, USB flash drive interface (reserved), access control board interface, exit button interface, 12 VDC power output interface (reserved), 24 VDC power input interface, fan interface, communication interface, encoder interface, power supply interface for motor, supercapacitor interface, IR adaptor interface and light bar interface.

The picture displayed below is the sub lane control board diagram.

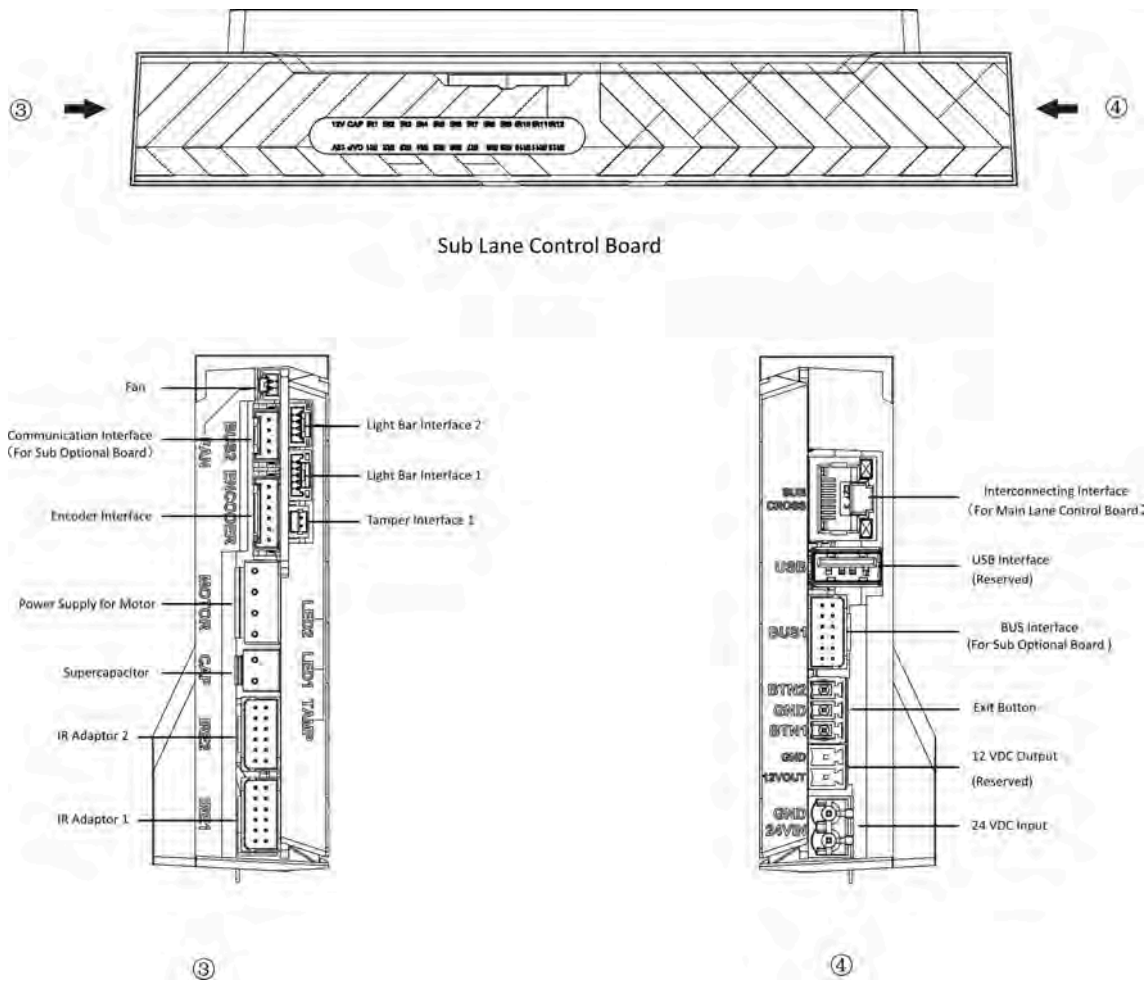
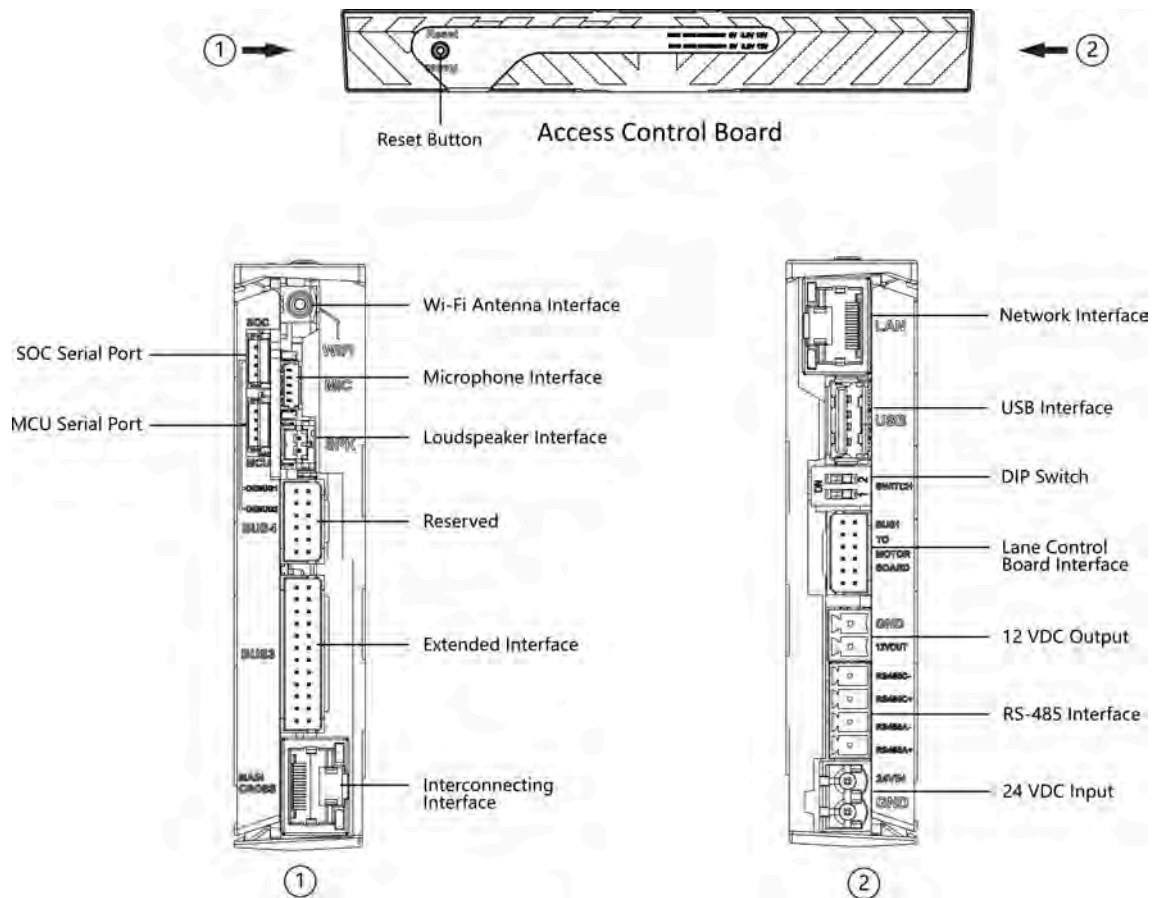


Figure 4-4 Sub Lane Control Board Terminals

4.3.3 Access Control Board Terminal Description

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.



Note

- RS-485A corresponds to serial port 6, connecting to QR code scanner by default. RS-485C corresponds to serial port 8, connecting to card reader 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*.

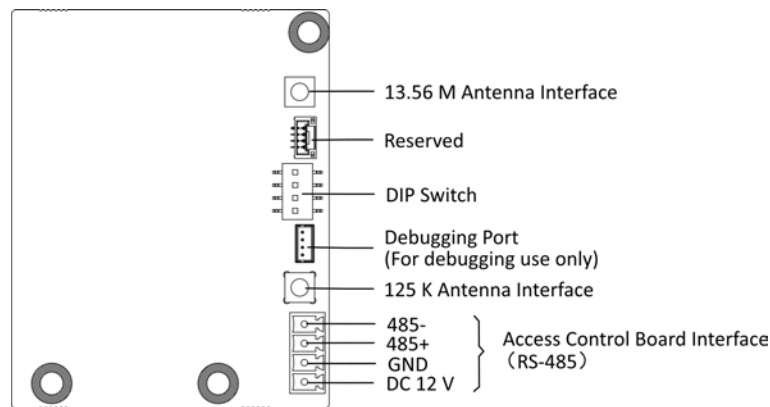


Figure 4-6 Card Reader Board (RS-485)

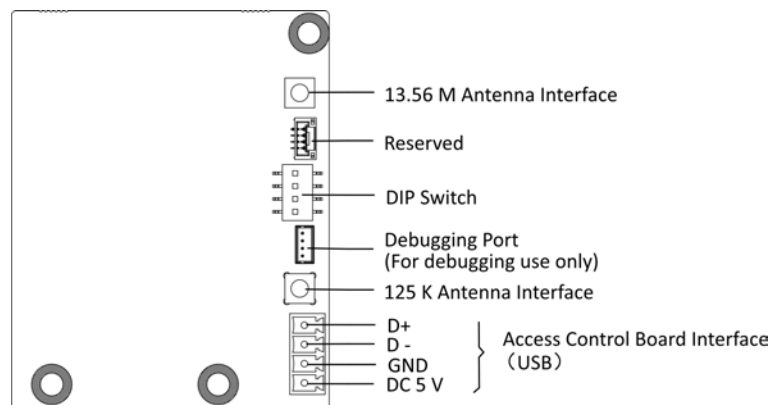


Figure 4-7 Card Reader Board (USB)

4.3.6 Main Optional Board Terminal Description (Optional)

The loudspeaker board contains the sub-1G antenna interface, lane control board interface, loudspeaker interface, debugging port, wiegand/exit button interface, 5 VDC output and communication interface.

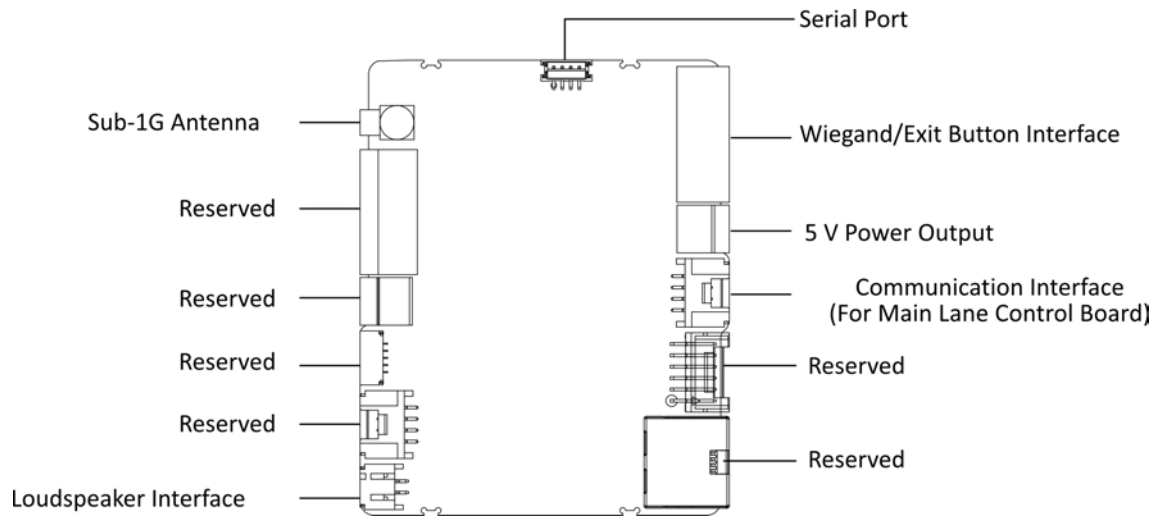


Figure 4-8 Loudspeaker Board Terminal

4.3.7 General Wiring

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

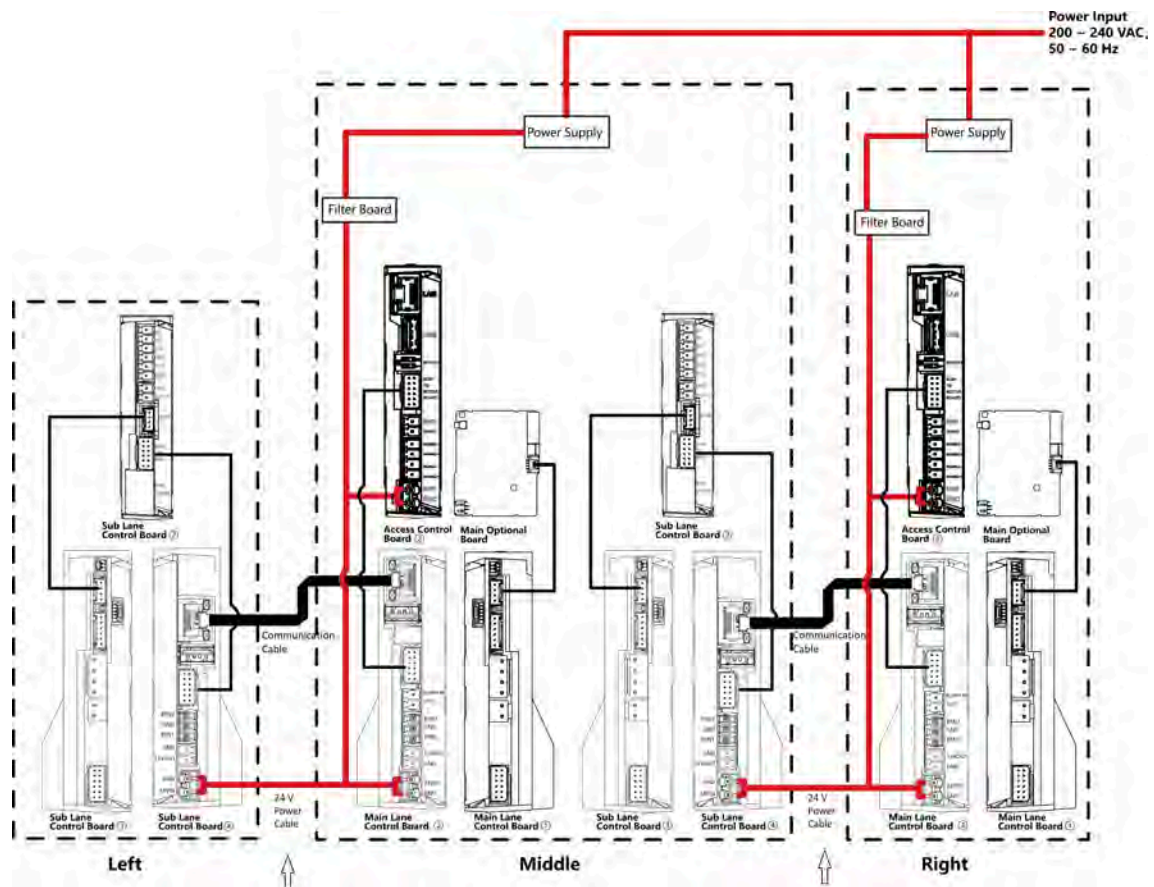


Figure 4-9 General Wiring

Note

- The power cable from power supply to the main lane control board has been connected. You will need to prepare the 14AWG power cable to connect the AC power input to power supply.
- The supplied 2 interconnecting cables need connecting on-site:
 1. 24 V power cable of 14 AWG. The cable is 2.5 m in length and put inside the right/middle pedestal at the exit.
 2. UTP-5e Communication cable. The cable is 3 m in length and put inside the package of the right/middle pedestal.
- The ① and ② or ③ and ④ refer to the two sides of a same board.
- Barrier opens at the entrance/exit: connect to BTN1/BTN2 and GND.

4.3.8 RS-485 Wiring

The RS-485 interfaces on the access control 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

- If connecting the RS-485 with a card reader, by default, the DIP switch of the card reader is: 1 for entrance, and 4 for exit.
- 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.

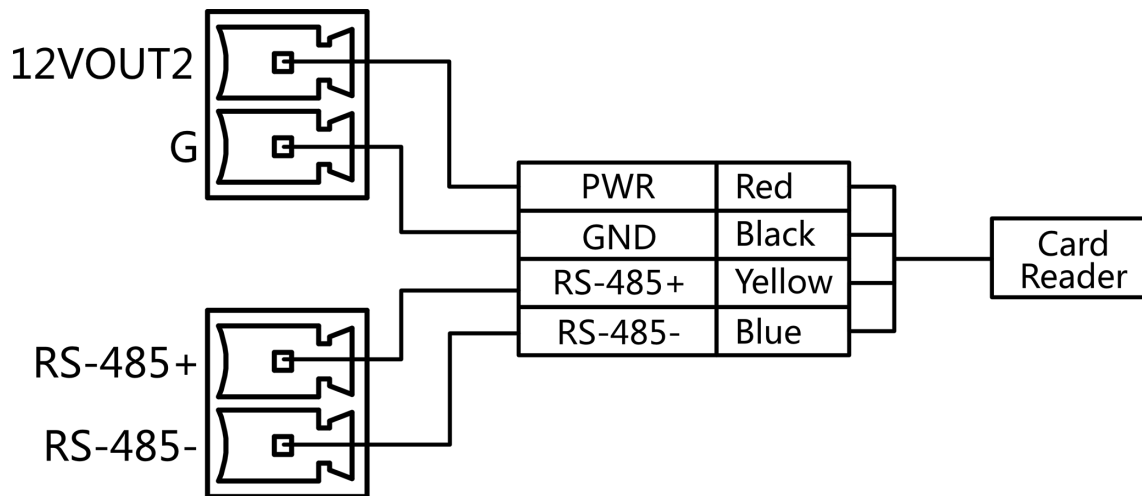


Figure 4-10 Wiring RS-485

4.3.9 RS-232 Wiring

Note

The RS-232 interface is on the extended interface of access control board.
The RS-232A corresponds to serial port 2, connecting to fingerprint scanner by default.

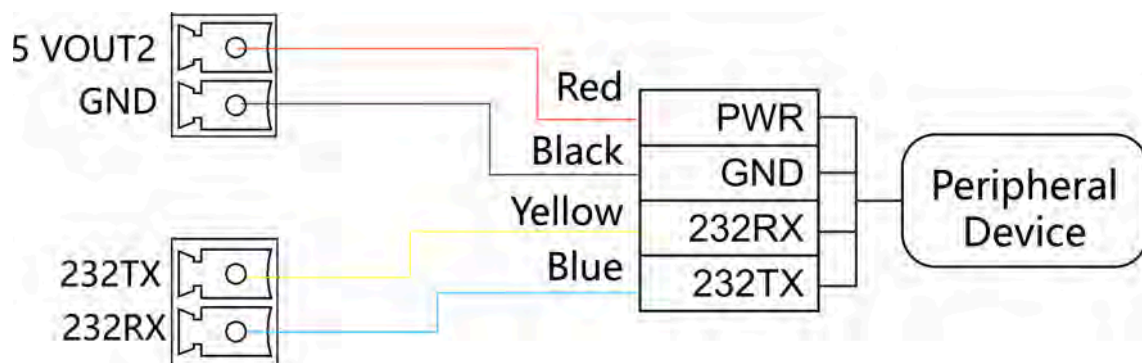


Figure 4-11 RS-232 Wiring

4.3.10 Alarm Input Wiring

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

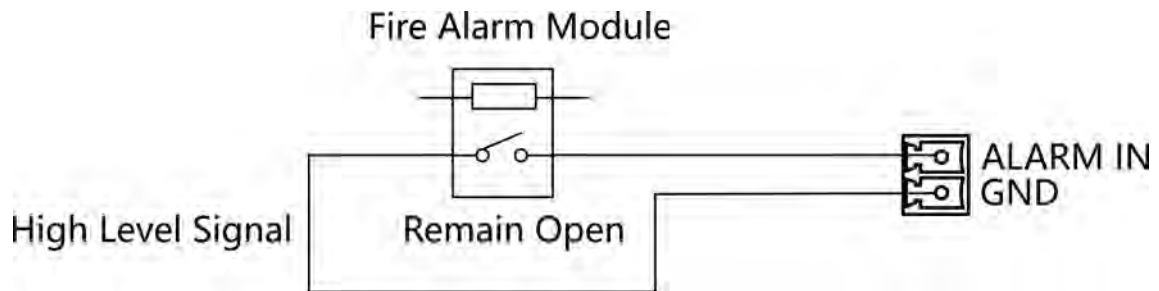


Figure 4-12 Remaining Open

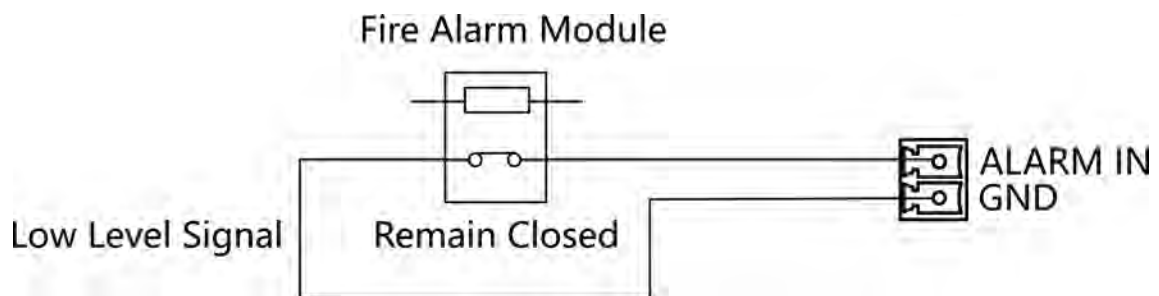


Figure 4-13 Remaining Closed

4.3.11 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.

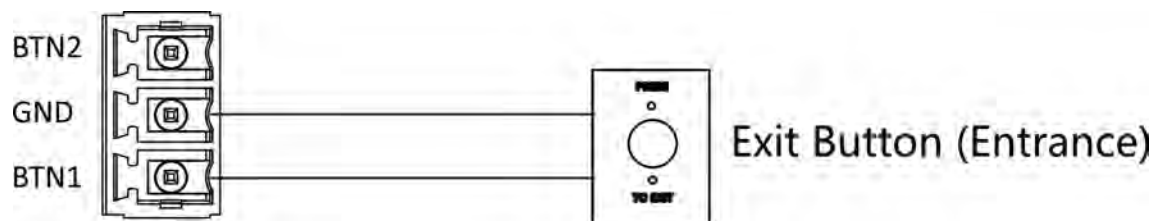


Figure 4-14 Exit Button Wiring (Entrance)

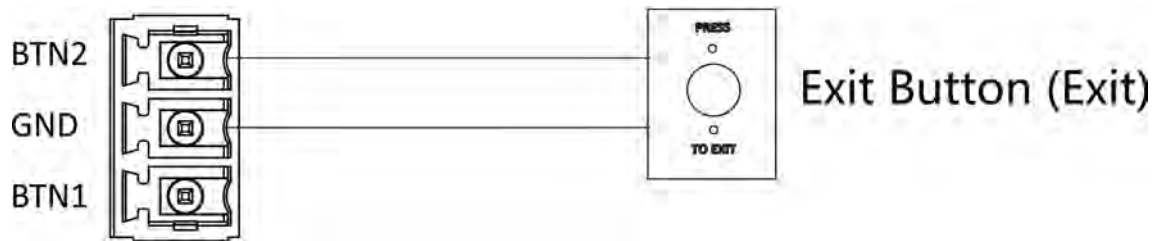


Figure 4-15 Exit Button Wiring (Exit)

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

You can configure the device via button on the main lane control board or the DIP switch on the access control board.

Function	Main Lane Control Board & Access Control Board & Loudspeaker (Optional)
Working Mode	
Normal/Study Mode	Configure via button (refer to <u>Set Study Mode via Button</u>) Configure via DIP switch (refer to <u>Set Study Mode</u>) Voice prompt (can be disabled)
keyfob Pairing	Configure via button (refer to <u>Pair Keyfob via Button</u>) Configure via button (refer to <u>Pair Keyfob</u>)
Passing Mode	Configure via button/web
Memory Mode	Configure via button/web
Parameter Settings	
Barrier Opening Speed	Configure via button/web
Barrier Closing Speed	Configure via button/web

Function	Main Lane Control Board & Access Control Board & Loudspeaker (Optional)
Card Reading on the Alarm Area	Configure via button/web
Enter Duration	Configure via button/web
Exit Duration	Configure via button/web
IR Sensing Duration	Configure via button/web
Intrusion Duration	Configure via button/web
Overstay Duration	Configure via button/web
Delay Time for Barrier Closing	Configure via button/web
Authentication on Free Passing	Not support
Volume Adjustment	Configure via button
Barrier Material	Configure via button/web
Barrier Length	Configure via button/web
Light Brightness	Configure via button/web
Restore to Default	Configure via button/web
Voice Prompt	
Climbing over Barrier	Enable or disable via button
Reverse Passing	Enable or disable via button
Exceeding Passing Duration	Enable or disable via button
Intrusion Alarm	Enable or disable via button
Tailgating Alarm	Enable or disable via button
Overstaying Alarm	Enable or disable via button
Motor Inspection	Enable or disable via button
Self-check Voice Prompt	Enable or disable via button
Study Mode Voice Prompt	Enable or disable via button

Refer to **Button Configuration Description** for detailed information.

4.4.1 Configuration via Button

Button Description

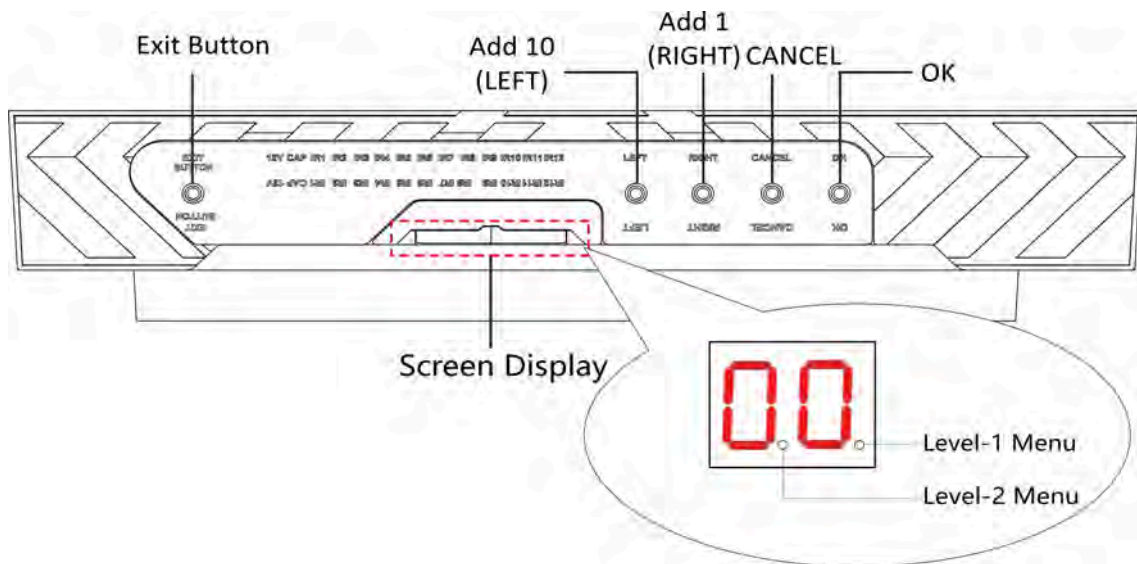


Figure 4-16 Button

Exit Button

- Single 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 ten to configuration data
- RIGHT: Press to add one configuration data
- CANCEL: Return to the level-1 menu, or exit the configuration from the level-1 menu
- OK: Confirm the data, or enter configuration mode, or enter the submenu



Note

- Configuration data 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 item number.
 - Level-2 Menu: if the decimal point in the middle is on, it indicates the level -2 menu. The number represents the parameters of a configuration item.
-

Button Configuration Procedure



Figure 4-17 Procedure

Steps:

1. Enter the configuration mode. The number of 1 will show up on the right side of the screen and the device is ready for configuration.
2. Press **LEFT** and **RIGHT** to set the configuration No. Press **OK** to enter the level-2 menu and view the parameters. Press **CANCEL**, or conduct no operation for 5 s to cancel configuration.
3. Press **LEFT** and **RIGHT** to set the parameters at your needs. Press **OK** to save the changes or press **CANCEL** back to configuration No. setting without saving changes. Conduct no operations for 5 s to cancel configuration.

4.4.2 Normal/Study Mode Settings

Set normal mode or study mode for device via button or DIP switch.

Set Study Mode via Button

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

Steps

1. Set the configuration No. to "1" and the parameter to "2".
The device enters 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."

Set Study Mode

Enter the study mode through DIP switching to set the closed position of the device barrier.

Steps

1. Set The No.1 of the 2-digit DIP Switch on the access control board to ON by referring the following figure to enter the study mode.

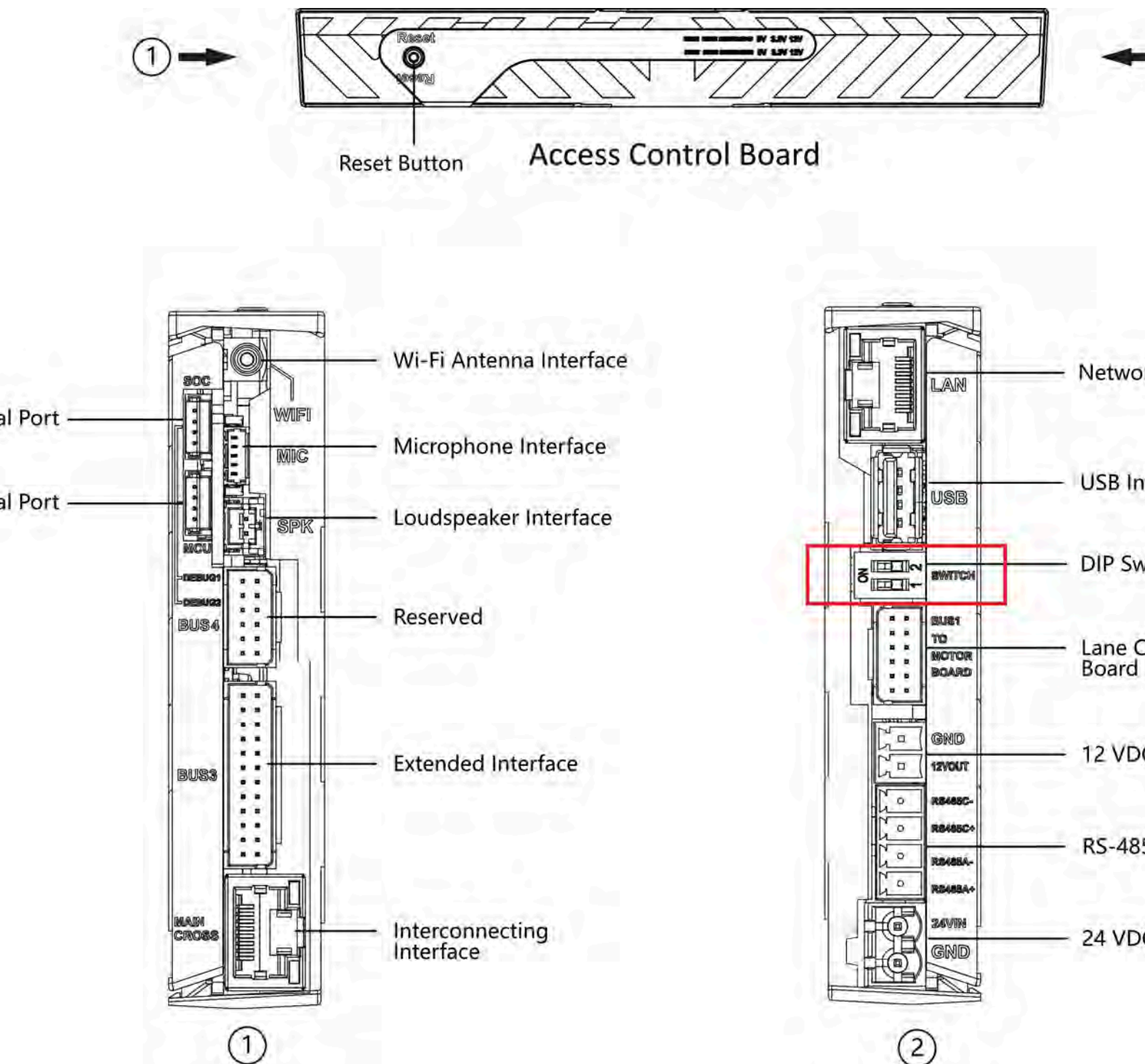


Figure 4-18 DIP Switch Location

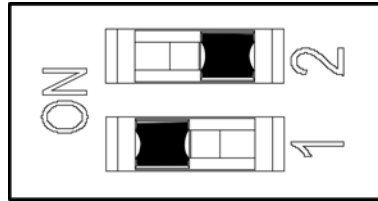


Figure 4-19 Study Mode

2. Adjust the closed position of the barrier.
3. Power on the device.
The device will remember the current position (closed position) automatically.
4. Power off the device.
5. Set the No.1 switches of the 2-digit DIP Switch on the main user extended interface board by referring to the following figure.

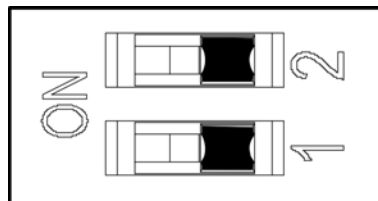


Figure 4-20 Normal Mode

6. Power on the device again.



Note

For details about the DIP switch value and meaning, see *DIP Switch Description*.

The barrier will open automatically and turns back to the closed position. At this circumstance, the device enters the normal mode.

4.4.3 Keyfob Pairing

Pair keyfob via button or DIP switch.

Pair Keyfob via Button

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

Steps

1. Set the configuration No. to "2" and the parameter to "2".
The device enters the keyfob pairing mode.
2. Hold the **Close** button for more than 10 seconds.
The keyfob's indicator of the will flash twice if the pairing is completed.

3. Set the configuration No. to "2" and the parameter to "1".
The device enters the normal mode.
4. Reboot the device to take effect.

Pair Keyfob

Pair the remote control to the device through DIP switch to open/close the barrier remotely.

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

1. Power off the turnstile.
2. Set the No.2 switch of the DIP Switch on the access control board to the ON side.

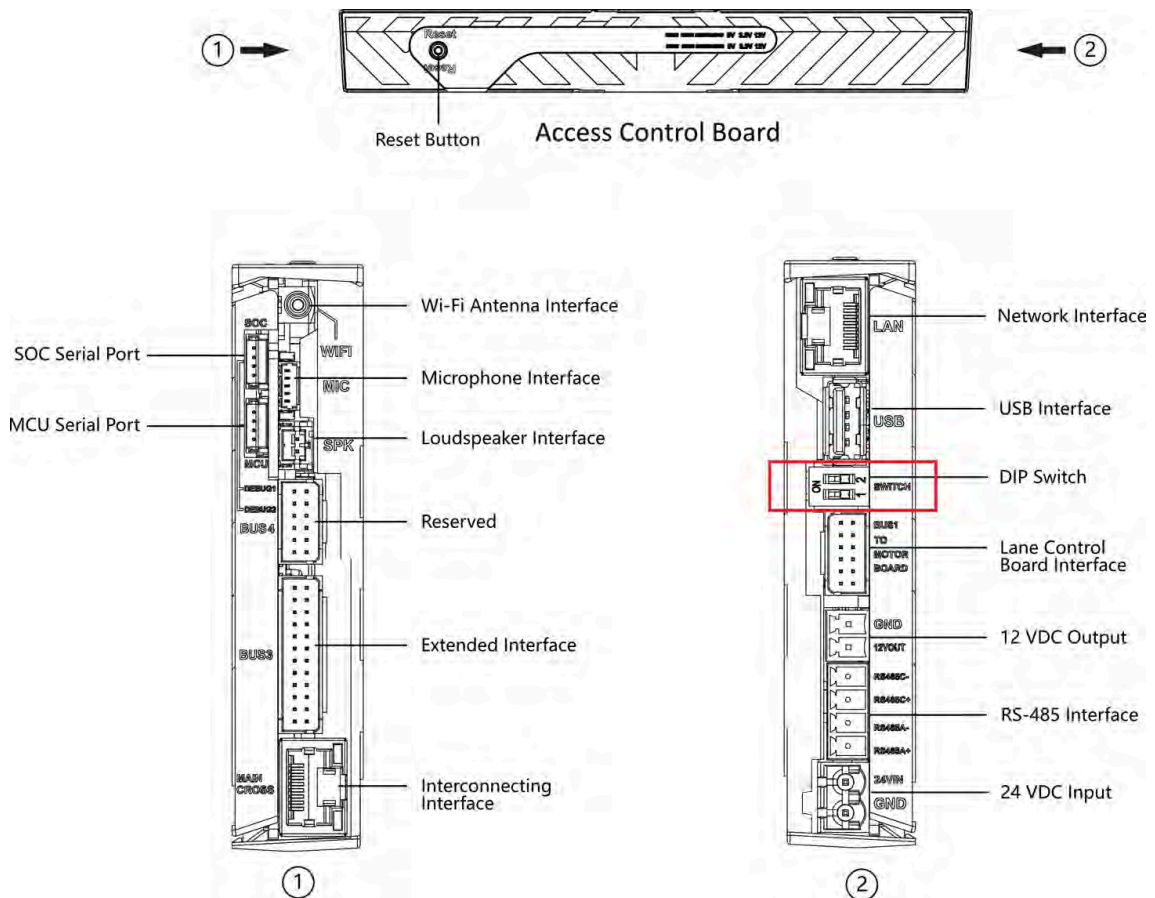


Figure 4-21 DIP Switch Location

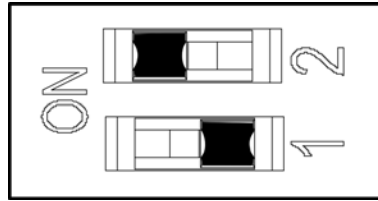


Figure 4-22 Enable Keyfob Pairing Mode

3. Power on the turnstile and it will enter the keyfob pairing mode.
4. Hold the **Close** button for more than 10 seconds.
The keyfob's indicator will flash twice if the pairing is completed.
5. Set the No.2 switch to the OFF side, and reboot the turnstile to take effect.

 Note

- Only one turnstile can pair the keyfob. If multiple turnstiles are in the pairing mode, the keyfob will select only one of them to pair.
 - For details about DIP switch value and meaning, see [DIP Switch Description](#).
-
6. **Optional:** Go to **System → User → Keyfob User** on the remote control page of the client software to delete the keyfob.

4.4.4 Initialize Device

Steps

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

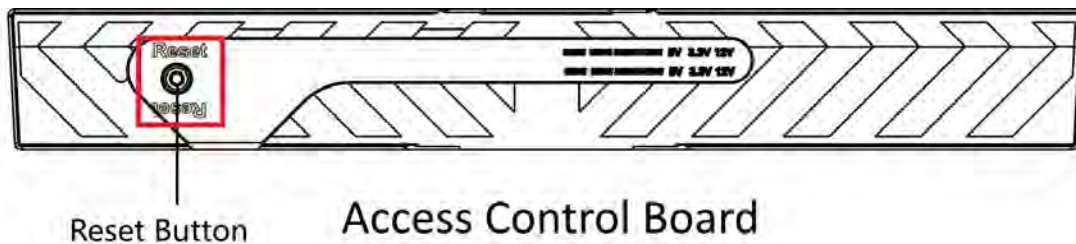


Figure 4-23 Initialization Button Position

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.: 8000
- 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

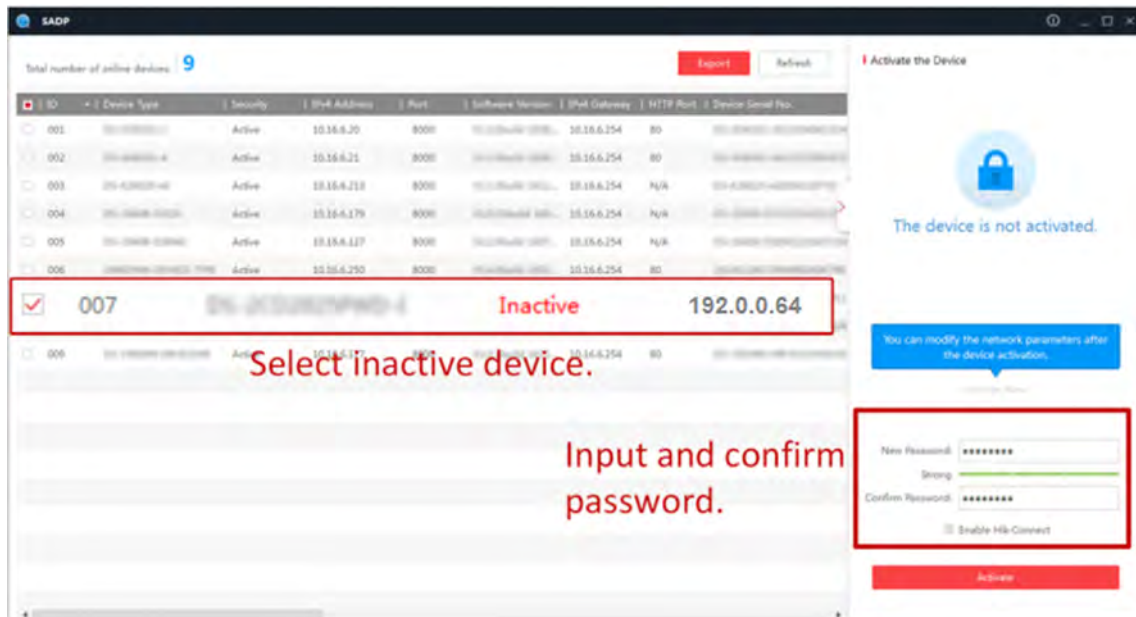
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.



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.

4. Click **Activate** to start activation.



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

5. Modify IP address of the device.

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

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.

Chapter 6 Operation via Web Browser

6.1 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.

6.2 Live View

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

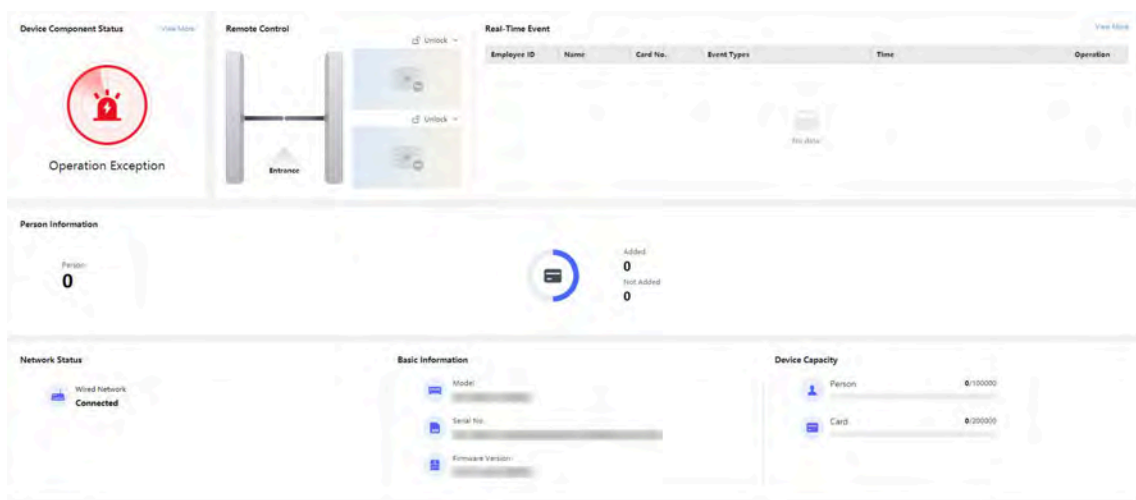


Figure 6-1 Live View Page

Function Descriptions:

Device Component Status

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

Door Status

Click  to view the device live view.



Set the volume when starting live view.



Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.



You can capture image when starting live view.



Select the streaming type when starting live view. You can select from the main stream and the sub stream.



Full screen view.



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

Controlled Status

You can select open/closed/remaining open/remaining closed status according to your actual needs.

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 face, card, and fingerprint.

Network Status

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

Basic Information

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

Device Capacity

You can view the person and card capacity.

6.3 Person Management

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

The screenshot displays a web-based form for adding a new person. It is divided into three main sections: Basic Information, Certificate Configuration, and Authentication Settings. The Basic Information section includes fields for Employee ID, Name, Gender (Male, Female, Unknown), Person Type (Normal User, Visitor, Person in Blocklist), Long-Term Effective User (toggle), Validity Period (date range), and Administrator (toggle). The Certificate Configuration section shows a card slot with a '+ Add Card' button and a note that up to 50 cards can be supported. The Authentication Settings section includes an Authentication Type (Same as Device, Custom) and a Save/Cancel button at the bottom.

Basic Information

* Employee ID

Name

Gender ☒ Male ☐ Female ☐ Unknown

Person Type ☒ Normal User ☐ Visitor ☐ Person in Blocklist

Long-Term Effective User ☐

Validity Period 2022-08-22 00:00:00 - 2032-08-21 23:59:59

Administrator ☐

Certificate Configuration

Card ⓘ Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type ☒ Same as Device ☐ Custom

Save Cancel

Figure 6-2 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, the gender, 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.

Authentication Settings

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

Set the authentication type.

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

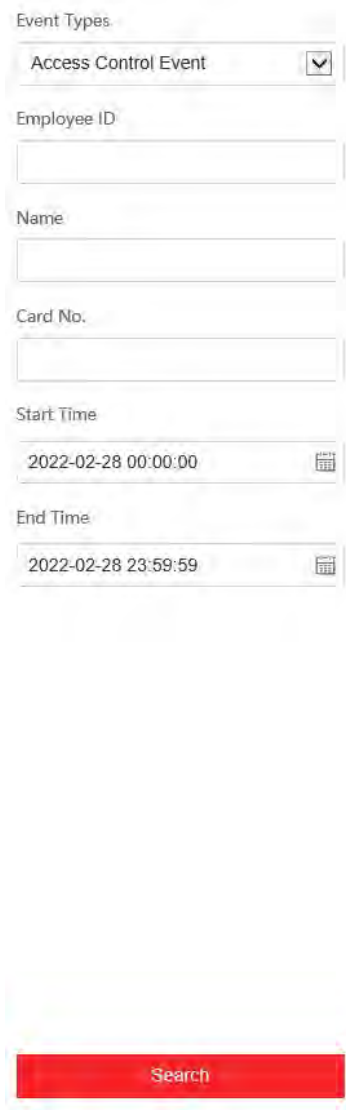
Click **Person Management** → **Add** to enter the Add Person page.

Set **Authentication Type** as **Same as Device** or **Custom**.

Click **Save** to save the settings.

6.4 Search Event

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



The image shows a search form for events. It includes a dropdown menu for 'Event Types' with 'Access Control Event' selected. Below this are text input fields for 'Employee ID', 'Name', and 'Card No.'. There are also date and time pickers for 'Start Time' (set to 2022-02-28 00:00:00) and 'End Time' (set to 2022-02-28 23:59:59). A red 'Search' button is at the bottom.

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
Search

Figure 6-3 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 results will be displayed on the right panel.

6.5 Configuration

6.5.1 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, local RS-485, alarm input, alarm output, and device capacity, etc.

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

6.5.2 Set Time

Set the device's time.

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

Device Time: 2015-01-01 00:37:18

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

Time Synchronization mode: ☐ NTP ☒ Manual

Set Time: 2015-01-01 00:36:49

DST

DST: ☒

Start Time: April, First, Sunday, 02

End Time: October, Last, Sunday, 02

DST Bias: 30minute(s)

Figure 6-4 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.

NTP

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

Manual

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

Server Address Type/Server Address/NTP Port/Interval

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

6.5.3 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.

6.5.4 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.

6.5.5 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.

6.5.6 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.

6.5.7 Network Settings

Set TCP/IP and port.

Set Basic Network Parameters

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

The screenshot displays the TCP/IP Settings page. At the top, there is a 'NIC Type' dropdown menu set to 'Self-Adaptive'. Below it is a 'DHCP' toggle switch, which is currently turned off. The next section contains three input fields: '*IPv4 Address', '*IPv4 Subnet Mask', and '*IPv4 Default Gateway'. Below these are 'Mac Address' and 'MTU' fields. The 'DNS Server' section includes 'Preferred DNS Server' and 'Alternate DNS Server' input fields. At the bottom of the form is a prominent red 'Save' button.

Figure 6-5 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 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, and HTTP Listening parameters.

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

The screenshot displays the 'Network Service' configuration page. It is divided into three main sections: HTTP, HTTPS, and HTTP Listening. The HTTP section has an 'Enable' toggle switch turned on, with a warning message 'Enabling HTTP may cause security problems' below it, and an 'HTTP Port' input field. The HTTPS section also has an 'Enable' toggle switch turned on and an 'HTTPS Port' input field. The HTTP Listening section contains four input fields: '*Event Alarm IP Address/Domain ...', '*URL', 'Port', and 'Protocol' (which is a dropdown menu currently set to 'HTTP'). At the bottom of the form are two buttons: a red 'Save' button and a white 'Reset' button.

Figure 6-6 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.

6.5.8 Event Linkage

Set linked actions for events.

Steps

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

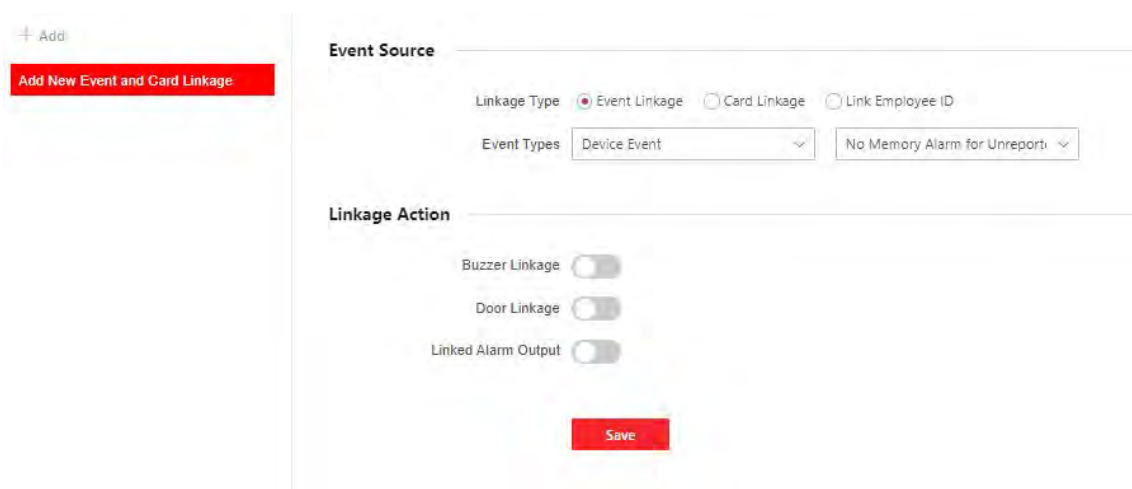


Figure 6-7 Event Linkage

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 **Employee ID Linkage**, you need to enter the employee ID and select the card reader.

3. Set linked action.

Linked Buzzer

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

Linked Door

Enable **Linked Door**, check **Door 1** or **Door 2**, 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.

6.5.9 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.

The screenshot shows the 'Set Authentication Parameters' configuration page. At the top, there are three buttons: 'Terminal', 'Entrance' (highlighted with a red border), and 'Exit'. Below these are three labels: 'Terminal Type' with the value 'Card', 'Terminal Model' with the value '485Offline', and 'Enable Authentication Device' with a green toggle switch. The 'Authentication' section has a dropdown menu set to 'Card'. Below this is the 'Authentication Interval' set to '0' with a reset icon. The 'Alarm of Max. Failed Attempts' is a toggle switch that is currently off. The 'Communication with Controller Ev...' is set to '0' with a reset icon. At the bottom is a red 'Save' button.

Figure 6-8 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 0 to 255.

Set Door Parameters

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

Door No. Entrance Exit

Door Name

Open Duration s

Exit Button Type ☐ Remain Closed ☒ Remain Open

Save

Figure 6-9 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

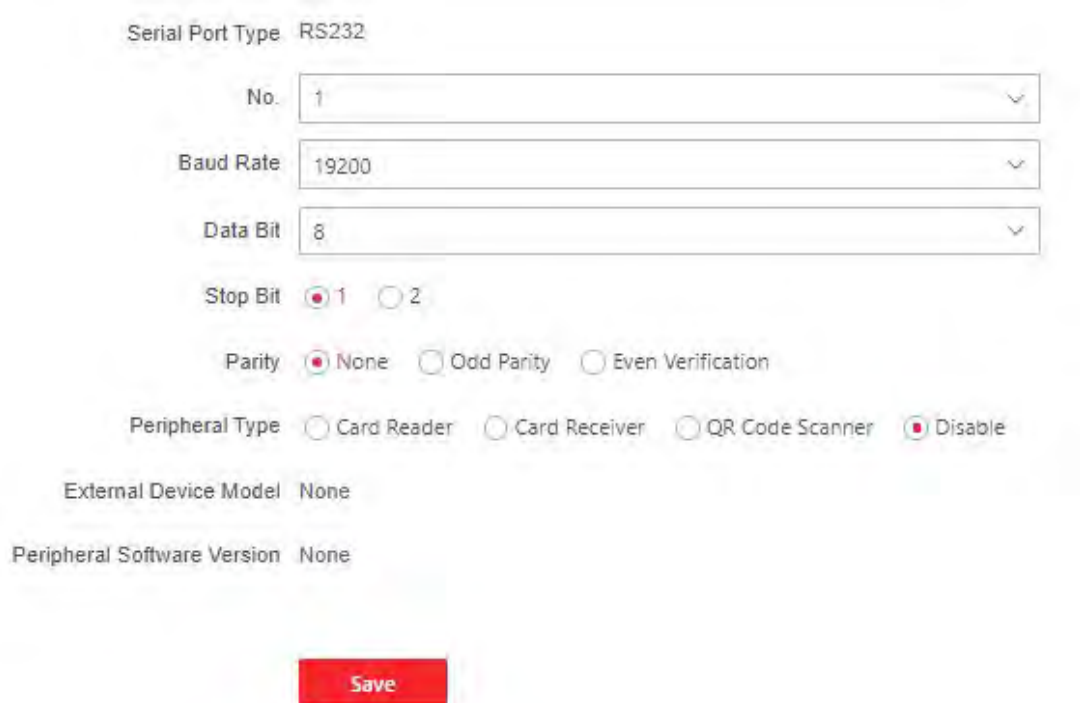
You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Serial Port Settings

Set serial port parameters.

Steps

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



The image shows a 'Serial Port Settings' form. At the top, 'Serial Port Type' is set to 'RS232'. Below this are four dropdown menus: 'No.' with '1', 'Baud Rate' with '19200', 'Data Bit' with '8', and 'Stop Bit' with '1'. The 'Parity' section has three radio buttons: 'None' (selected), 'Odd Parity', and 'Even Verification'. The 'Peripheral Type' section has four radio buttons: 'Card Reader', 'Card Receiver', 'QR Code Scanner', and 'Disable' (selected). Below these are two text fields: 'External Device Model' with 'None' and 'Peripheral Software Version' with 'None'. At the bottom center is a red 'Save' button.

Figure 6-10 Serial Port Settings

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

Host Parameters

Set door contact settings and RS-485 protocol.

Steps

1. Click **Configuration** → **Access Control** → **Host Parameter** to enter the page.
2. Set door contact.



Note

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

-
3. Set RS-485 protocol.
 4. Click **Save**.

Set Terminal Parameters

Set the working mode.

Steps

1. Set the device working mode.

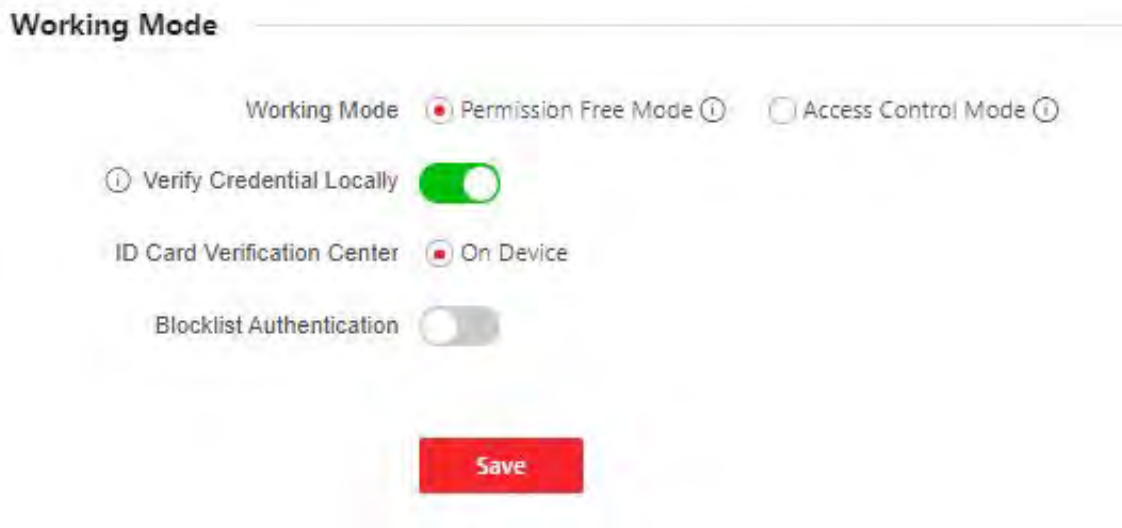


Figure 6-11 Working Mode

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.

2. **Optional:** Enable **Blocklist Authentication**.
3. Click **Save** to complete terminal parameter settings.

6.5.10 Turnstile

Basic Parameters

Set turnstile basic parameters.

Steps

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

The screenshot displays a configuration window for a swing barrier. The parameters are as follows:

Parameter	Value
Channel Type	Swing Barrier
Channel Model	[Blurred]
Barrier Material	Acrylic
Lane Width	900
Barrier Opening Speed	5
Barrier Closing Speed	4
Working Status	Normal
Passing Mode	General Passing (selected)
Entrance	Controlled
Exit	Controlled

A red **Save** button is located at the bottom center of the configuration area.

Figure 6-12 Basic Parameters

2. View the **Device Type**, **Device Model** and **Working Status**.
3. Set **Barrier Material**, **Lane Width**, **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.
 - If you choose **Weekly Schedule**, you can set a weekly schedule for entrance and exit barriers.
5. Click **Save**.

keyfob

Set keyfob parameters.

Steps

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

Working Status: Normal

Working Mode: ☐ One-to-One ☒ One-to-Many

Keyfob: + Add

Name	Serial No.	Remain Open Permission	Operation
------	------------	------------------------	-----------

Save

Figure 6-13 keyfob

2. View the keyfob working status.
3. Set **Working Mode** as **One-to-One** or **One-to-Many**.
4. 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.
5. **Optional:** Select a keyfob and click **Delete** to delete the keyfob.
6. Click **Save**.

IR Detector

Set IR detector.

Steps

1. Click **Configuration** → **Turnstile** → **IR Detector** to enter the page.

Inductive Mode (Entrance): ☒ Single Triggered ☐ Triggered Simultaneously

Inductive Mode (Exit): ☒ Single Triggered ☐ Triggered Simultaneously

Custom IR Detector: ☐ Enable IR Emergency Mode ⓘ ☐ Enable Custom Anti-pinch for Door Closing ⓘ

Save

Figure 6-14 IR Detector

2. Set the entrance and exit inductive mode as **Single Triggered** or **Triggered Simultaneously**.
3. Set custom IR detector mode.

Enable IR Emergency Mode

If some IR beams do not work properly, you can shield those IR beams to restore the lane. But this action may hit person and cause injury.

Enable Custom Anti-pinch for Door Closing

Anti-pinch for door closing refers that the barrier will not close if the device has detected person in the lane. Only after the person walks out of the lane, the barrier will close. If you enable the function, you can shield parts of the IR beams for closing barrier in advance. But this action may hit person and cause injury.

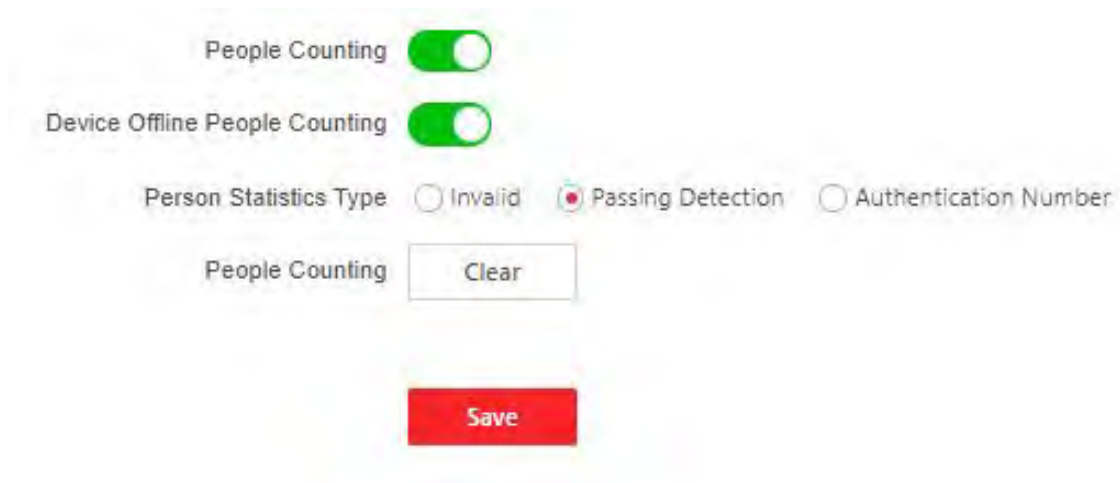
4. Click **Save**.

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 ☒ Passing Detection ☐ Authentication Number

People Counting

Figure 6-15 People Counting

2. Check to enable **People Counting**.
3. Enable **Device Offline People Counting** at your actual needs.
4. Select **People Counting Type** as **Invalid**, **Passing Detection** 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.
2. Set **Alarm Output Duration**.



Note

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

3. Set **Temperature Unit**.
 4. Check to enable **Do Not Open Barrier When Lane is Not Clear**.
 5. Drag the block or enter the value to adjust the light board brightness.
 6. Set the alarm buzzer beeping duration, door closing delay time, max. intrusion duration, overstaying duration and max. IR obstructed duration.
 7. Check to enable **Memory Mode** at your actual needs.
-



Note

Multiple cards presenting for multiple person passing is allowable when enabling the memory mode. When the passing person's number exceeds the card presenting number, or after the latest person passing with no other person passing within the door open duration, the door will close automatically.

8. Choose the control mode.

Soft Mode

The barrier will be closed after the person has passed through the barrier when there are tailing, forced accessing, etc.

Guard Mode

The barrier will be closed immediately when there are tailgating, forced accessing, etc.

9. Set the fire input type.
10. Click to enable **Motor Self-Test** and choose the main lane or sub lane to start motor self-testing.
11. Click **Save**.

6.5.11 Card Settings

Set Card Security

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

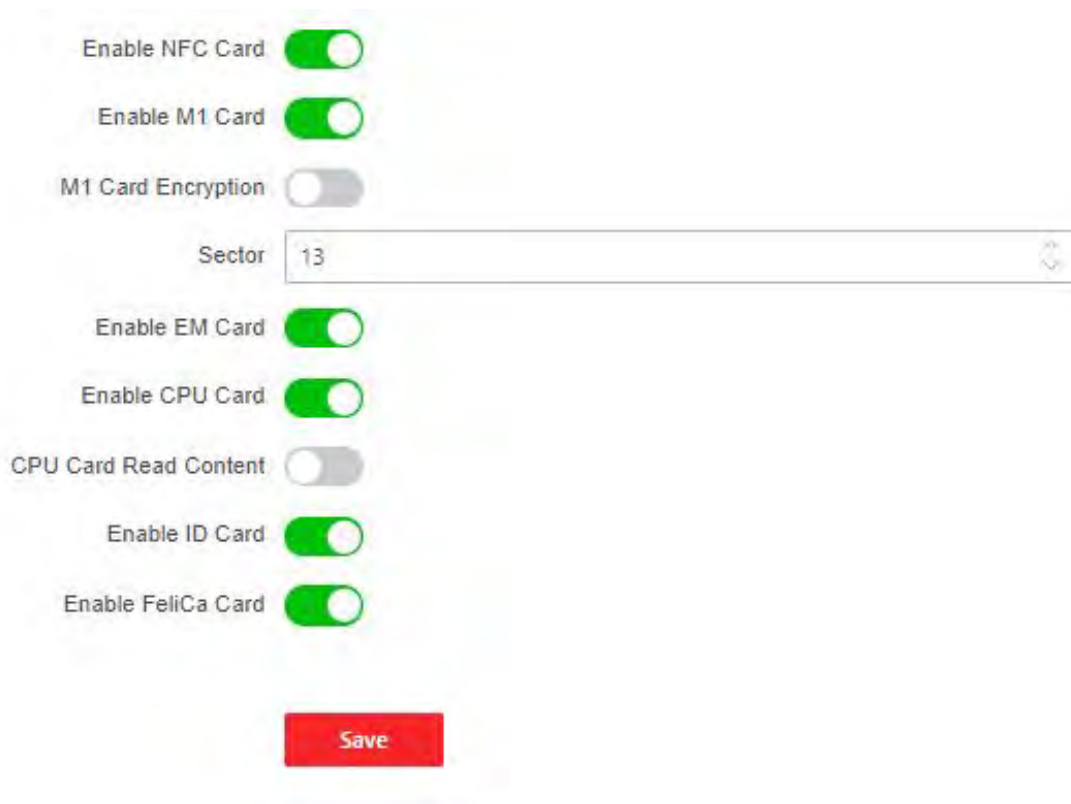


Figure 6-16 Card Type

Set the parameters and click **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

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

Enable EM Card

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



Note

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

Enable CPU Card

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

CPU Card Read Content

After enable the CPU card content reading function, the device can read the CPU card content.

Enable ID Card

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

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**.

6.5.12 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.

6.5.13 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.

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.



Note

Do not power off during the upgrading.

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 device IP address 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.

6.5.14 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.

6.5.15 Component Status

You can view the main lane and sub lane status.

Main Lane Status

Main Lane Status		
Device Component		
Access Control Board	✓ Online	
Lane Control Board	✓ Online	
User Extended Interf...	✓ Online	
Arrow Light Board (E...	✓ Online	
Peripheral Device		
RS-485 Card Reader	✓ Online	
Temperature		
Pedestal Temperature	39°C	
Movement		
Motor Encoder	✓ Normal	

Figure 6-17 Main Lane Status

Device Component

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

Peripheral

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

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Sub Lane Status

Sub Lane Status		
Device Component		
Lane Control Board	✓ Online	
Arrow Light Board (E...	✓ Online	
Peripheral Device		
RS-485 Card Reader	✓ Online	
Movement		
Motor Encoder	✓ Normal	

Figure 6-18 Sub Lane Status

Device Component

You can view the status of the access control board and arrow light board.

Peripheral

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

Movement

You can view the working status of motor encoder.

Others

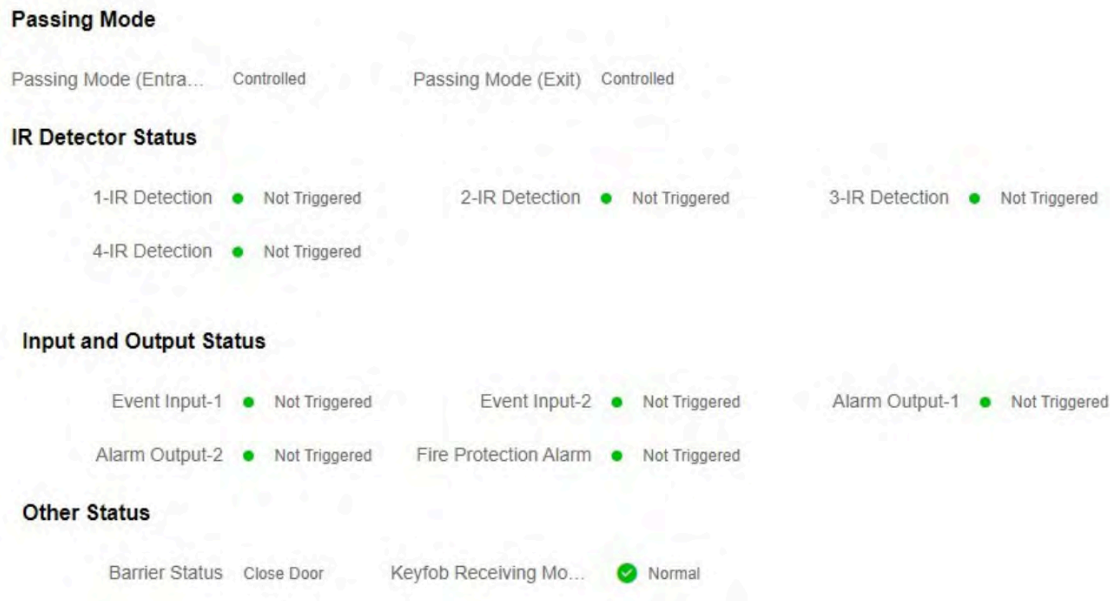


Figure 6-19 Other Status

Passing Mode

You can view the entrance and exit mode.

IR Detector Status

You can view the status of each pair of the 4 IR beam sensors.

Input and Output Status

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

Other Status

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

6.5.16 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.

6.5.17 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 Install 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 Passwords** area, and select a certificate from the local, and click **Install**.
 - 2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Install**.

Install 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 Passwords** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Install**.

Install 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 **Install**.

Chapter 7 Client Software Configuration

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

7.1 Configuration Flow of Client Software

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

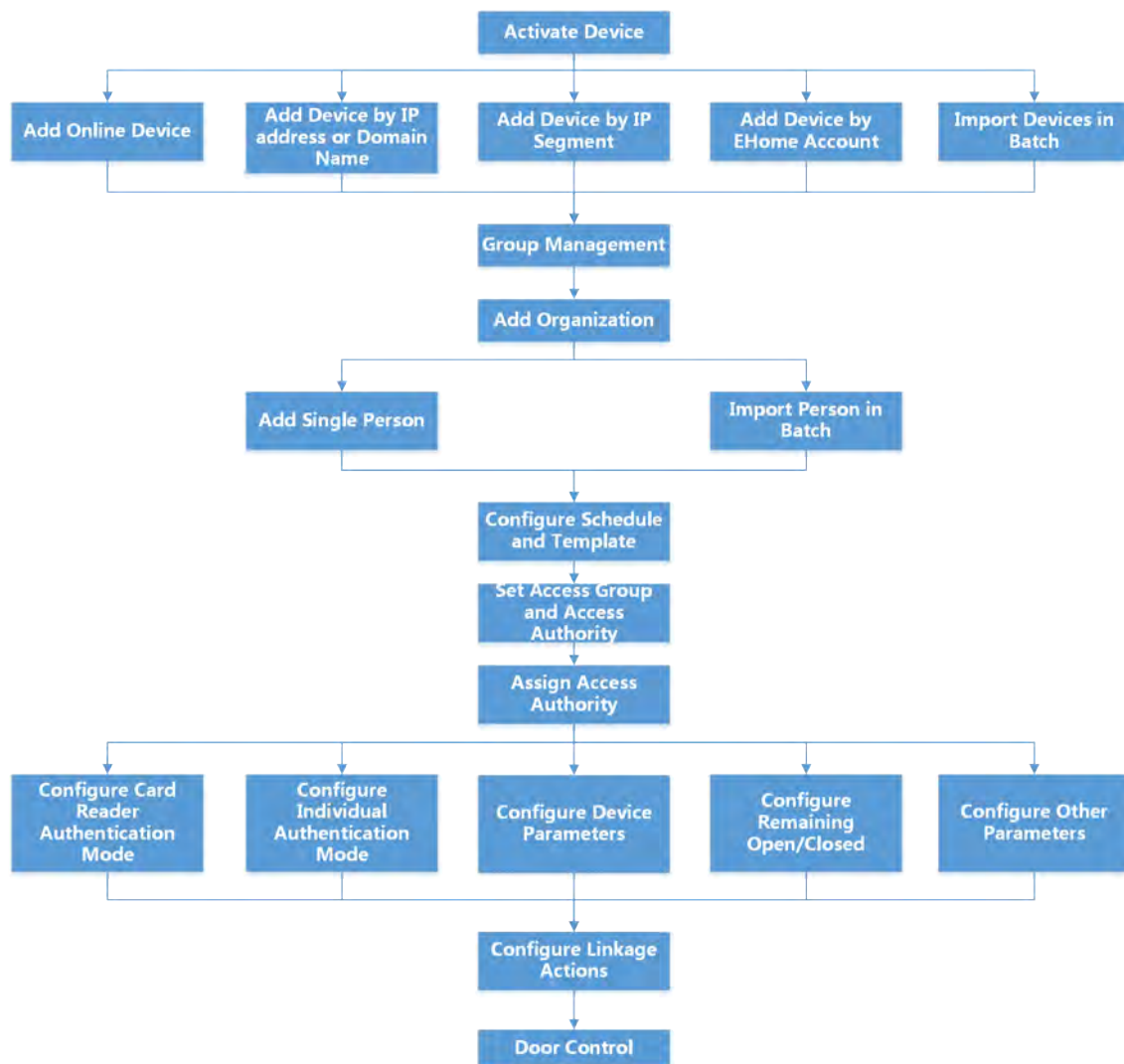


Figure 7-1 Flow Diagram of Configuration on Client Software

7.2 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.

7.2.1 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.

7.2.2 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.

7.2.3 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 7-1 Manage Added Devices

Edit Device	Click  to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click Delete to delete the selected devices.
Remote Configuration	On the device list page, click  in the Operation column to perform remote configuration for a device. The  is in the rightmost column of the Device page. For details, refer to the user manual of device.
View Device Status	Click  to view device status, including door No., door status, etc.  Note For different devices, you will view different information about device status.
View Online User	Click  to view the details of online user who access the device, including user name, user type, IP address and login time.

Refresh Device Information	Click  to refresh and get the latest device information.
Upgrade Device	View device status in the Firmware Upgrade column, check one or more upgradable devices, and click Upgrade Device Firmware to upgrade the selected devices. For details, refer to .
Get Events from Device	Check one device, and click Get Events from Device to synchronize events. For details, refer to .

7.3 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.

7.3.1 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.

7.3.2 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.

7.4 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.

7.4.1 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 subordinate 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.

7.4.2 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.
-

Import Person Pictures

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

Before You Start

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

Steps

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



Note

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

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

The importing progress and result will be displayed.

Export Person Information

You can export the added persons' information to 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. See for details.

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.

Export Person Pictures

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

Before You Start

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

Steps

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



Note

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

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

The Export panel is displayed.

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



Note

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

7.4.3 Get Person Information from Access Control Device

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

Steps

Note

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

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

Note

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

5. Select the **Getting Mode**.
-

Note

The getting mode varies according to different devices. The access control device supports getting the person information by employee ID. Up to 5 employee IDs can be specified each time.

6. Click **Import** to start importing the person information to the client.
-

Note

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

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

7.4.4 Issue Cards to Persons in Batch

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

Steps

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

All the added persons with no card issued will be displayed in the right panel.
3. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to .

5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. 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).

7.4.5 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.

7.4.6 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.

7.5 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***](#) .

7.5.1 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**.
-

7.5.2 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.
-

7.6 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 (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control** → **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.

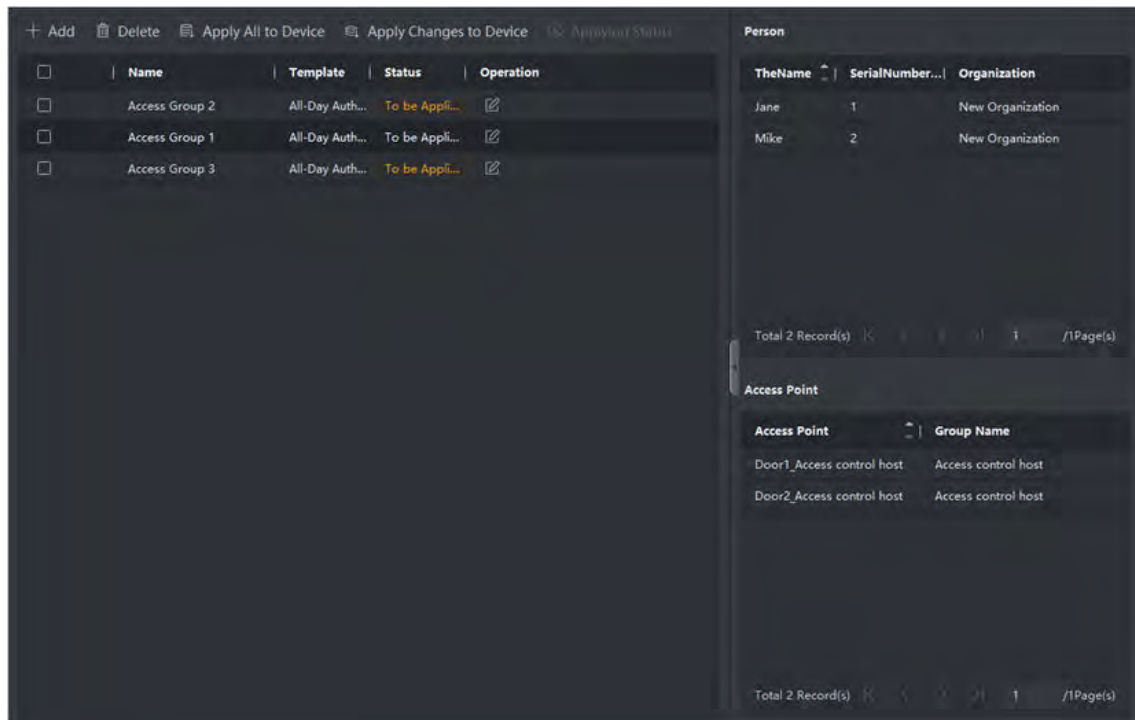


Figure 7-2 Display the Selected Person(s) and Access Point(s)

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) or fingerprints.

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**.

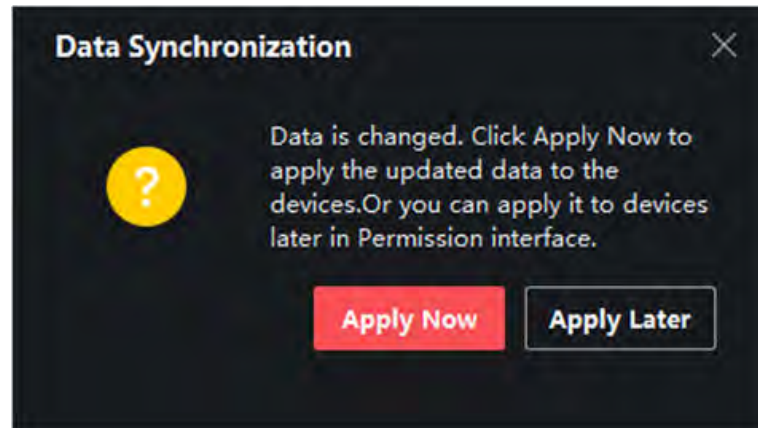


Figure 7-3 Data Synchronization

7.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene, such as multi-factor authentication, anti-passback, etc.

Note

- For the card related functions(the type of access control card/multi-factor authentication), 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.

7.7.1 Configure Device Parameters

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

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 Parameter** .



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.

RS-485 Comm. Redundancy

You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

Display Detected Face

Display face picture when authenticating.

Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

Upload the pictures captured by linked camera to the system automatically.

Save Pic. After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

NFC An i-Cloning

If you enable this function, you cannot use the cloned card for authentication and further enhance security.

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.

Door Contact

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

Exit Button Type

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

Door Locked Time

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

Extended Open Duration

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

Door Left Open Timeout Alarm

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

Lock Door when Door Closed

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

Duress Code

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

Super Password

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

Dismiss Code

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



Note

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

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.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

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

Minimum Card Swiping Interval

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

Max. Interval When Entering PWD

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

Alarm of Max. Failed Attempts

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

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

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

Buzzing Time

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

Card Reader Type/Card Reader Description

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

Fingerprint Recognition Level

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

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Security Level

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

Live Face Detection

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same

user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

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.

- If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.
- If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

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.

Audible Prompt 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.

4. Click **OK**.

7.7.2 Configure Other Parameters

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

Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps



Note

This function should be supported by the device.

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 **Face Recognition Terminal**.
4. Set the parameters.



Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blocklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blocklist.

If matched (the person is in the blocklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blocklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

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, communication mode, working mode, and connection mode in the drop-down list.



Note

When the connection mode is **Connect Access Control Device**, you can select **Card No.** or **Person ID** as the output type.

6. Click **Save**.
 - The configured parameters will be applied to the device automatically.
 - When you change the working mode or 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.

7.8 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 .

7.8.1 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). For details, refer to .

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

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

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. For setting the saving path, refer to .

Result

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

7.8.2 Check Real-Time Access Records

The real-time access records can be displayed in the client, including card swiping records, face recognition records, skin-surface temperature information, etc. Also, you can view the person information and view the picture captured during access.

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, including card No., person name, event time, door location, temperature, authentication type etc.

Card No.	Person Name	Event Time	Door Location	Temperature	Abnormal Temperature	Authentication Type	Person	Linked Capture Picture
00000001	Tom	2020-05-15 17:03:44	Door1	36.6°C	No	Card/Face		
00000002	Tom	2020-05-15 17:03:41	Door1	36.6°C	No	Card/Face		
00000003	Tom	2020-05-15 17:03:39	Door1	36.6°C	No	Card/Face		
00000004	Tom	2020-05-15 17:03:39	101:Door1	-	-	-		

Figure 7-4 Real-time Access Records



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:** Check **Enable Abnormal Temperature Prompt** to enable abnormal skin-surface temperature prompt.



Note

When enabled, if there is abnormal temperature information, an Abnormal Temperature window pops up when you enter Monitoring module, displaying person's picture, skin-surface temperature, card No., person name, etc.

6. **Optional:** Click an event to view person pictures (including captured picture and profile).



Note

In **Linked Capture Picture** field, you can double click the captured picture to view an enlarged picture.

-
7. **Optional:** Click  to view surveillance details (including person's detailed information and the captured picture).
-



Note

In the pop-up window, you can click  to view surveillance 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.

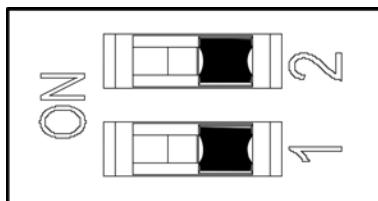


Figure A-1 DIP Switch

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

A.2 DIP Switch Corresponded Functions



Note

After setting the DIP switch, you should reboot the device, or the function cannot take effect.

The 2-bit DIP switch corresponded functions on the access control board are as follows:

Bit	Device Mode	Function	Decimal Value	DIP Switch Address Diagram
1	Work Mode	Normal Mode	0	
		Study Mode	1	
2	Keyfob Paring Mode	Disable Keyfob Paring Mode	0	
		Enable Keyfob Paring Mode	1	

Appendix B. Button Configuration Description

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

No.	Description	Default Value	Parameters	Notes
1	Normal/Study Mode	1	1-Normal Mode 2-Study Mode	
2	keyfob Pairing	1	1-Normal Mode 2-Pairing Mode	
3	Passing Mode	1	1-Both sides under control 2-Entrance under control; exit prohibited 3-Entrance under control; exit on inductive mode 4-Both sides on inductive mode 5-Entrance on inductive mode; exit under control 6-Entrance on inductive mode; exit prohibited 7-Both sides prohibited 8-Entrance prohibited; exit under control 9-Entrance prohibited; exit on inductive mode 10-Entrance under control; exit remaining open	

No.	Description	Default Value	Parameters	Notes
			11-Entrance under control; exit on free mode 12-Entrance on inductive mode; exit remaining open 13-Entrance on inductive mode; exit on free mode 14-Entrance prohibited; exit remaining open 15-Entrance prohibited; exit on free mode 16-Entrance remaining open; exit under control 17-Entrance remaining open; exit on inductive mode 18-Entrance remaining open; exit remaining open 19-Entrance remaining open; exit on free mode 20-Entrance remaining open; exit prohibited 21-Entrance on free mode; exit under control	

No.	Description	Default Value	Parameters	Notes
			22-Entrance on free mode; exit on inductive mode 23-Entrance on free mode; exit remaining open 24-Entrance on free mode; exit on free mode 25-Entrance on free mode; exit prohibited	
4	Memory Mode	2	1-Disable 2-Enable	
5	keyfob Remote Control	2	1-one to one 1-one to multiple	
6	Barrier Opening Speed	5	1-1, 2-2, ...10-10	
7	Barrier Closing Speed	5	1-1, 2-2, ...10-10	
8	Card Reading on the Alarm Area	2	1-Do not open 2-Open	
9	Enter Duration	5	5-5s, 6-6s, 7-7s, ..., 60-60s	
10	Exit Duration	5	5-5s, 6-6s, 7-7s, ..., 60-60s	
11	IR Sensing Duration	0	0-0s, 1-1s, 2-2s,..., 25-25s	
12	Intrusion Duration	0	0-0s, 1-1s, 2-2s,..., 20-20s	
13	Overstay Duration	0	0-0s, 1-1s, 2-2s,..., 20-20s	
14	Delay Time for Barrier Closing	0	0-0s, 1-1s, 2-2s, 3-3s, 4-4s, 5-5s	

No.	Description	Default Value	Parameters	Notes
15	Control Mode	1	1-Button Configuration 2-DIP Switch on Access Control Board	
16	Authentication on Free Passing	1	1-Disable 2-Enable	Unable to change
17	IR Configuration for Closing in Advance	1	1-1, 2-2, ..., N-N	
18	Swing Barrier Quantity	1	1-Dual Lanes 2-Single Lane	Unable to change
19	Motor Rotation	1	1-Clockwise 2-Anticlockwise	Unable to change
20	Motor Type	1	1-Dunker Motor 2-Control Motor	Unable to change
21	Volume	2	1-0, 2-1, 3-2, 4-3, 5-4	The device will be muted when set to "1".
22	Authenticated Passing	1	1-Disable 2-Enable	Unable to change
23	Invalid Card No.	1	1-Disable 2-Enable	Unable to change
24	Fingerprint Unmatched	1	1-Disable 2-Enable	Unable to change
25	Climbing over Barrier	1	1-Disable 2-Enable	
26	Reverse Passing	1	1-Disable 2-Enable	
27	Exceeding Passing Duration	1	1-Disable 2-Enable	
28	Intrusion Alarm	1	1-Disable	

No.	Description	Default Value	Parameters	Notes
			2-Enable	
29	Forced Passing	1	1-Disable 2-Enable	Unable to change
30	Tailgating Alarm	1	1-Disable 2-Enable	
31	Unauthorized Passing	1	1-Disable 2-Enable	Unable to change
32	Exceeding Authentication Duration	1	1-Disable 2-Enable	Unable to change
33	Failed Authentication	1	1-Disable 2-Enable	Unable to change
34	Expired Certificate	1	1-Disable 2-Enable	Unable to change
35	Overstaying Alarm	1	1-Disable 2-Enable	
36	Barrier Material	1	Acrylic	
37	Barrier Length	8	1-550 2-600 3-650 4-700 5-750 6-800 7-850 8-900	
38	Motor Inspection	1	1-Disable 2-Enable on Main Lane 3-Enable on Sub Lane	
39	Brightness of Light	3	0-0, 1-1, 2-2, ... , 10-10	The higher the value is, the

No.	Description	Default Value	Parameters	Notes
				brighter the light will be.
40	Self-check Voice Prompt	2	1-Disable 2-Enable	Voice prompt of self-check at startup and motor inspection
41	Study Mode Voice Prompt	2	1-Disable 2-Enable	Voice prompt of study mode
42	IR Detector Quantity	4	4-4, 6-6, 8-8,	Unable to change
99	Restore to Default	1	1- Default 2- Start	The device will reboot.

Appendix C. Event and Alarm Type

Event	Alarm Type
Tailgating	Visual and Audible
Reverse Passing	Visual and Audible
Force Accessing	None
Climb over Barrier	Visual and Audible
Overstay	Visual and Audible
Passing Timeout	None
Intrusion	Visual and Audible
Free Passing Authentication Failed	Visual and Audible
Barrier Obstructed	None

Appendix D. Table of Audio Index Related Content

Index	Content
1	Climbing over the barrier.
2	Reverse passing.
3	Passing timeout.
4	Intrusion.
5	Tailgating.
6	Overstay.

Appendix E. Error Code Description

The swing barrier 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
The First IR Beam Triggered	01	Not Studying	54
The Second IR Beam Triggered	02	Obstruction	55
The Third IR Beam Triggered	03	Exceeding Studying Range	56
The Fourth IR Beam Triggered	04	Encoder Exception	57
Loudspeaker Offline (If the kit is not installed, the error code of "49" will appear but the device functions normally)	49	Motor Exception	58
Interconnecting Exception	53		

Appendix F. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.

Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.



Figure F-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.

Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.



Figure F-2 Device Command



See Far, Go Further