DS-K3Y411X Series Flap Barrier

User Manual

Legal Information

About this Manual

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

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

Trademarks

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

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

Disclaimer

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

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

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

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

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The equipment must be connected to an earthed mains socket-outlet.
- Shock hazard! Disconnect all power sources before maintenance.
- Do not touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- ϟ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- Keep body parts away from fan blades. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.
- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- 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:**

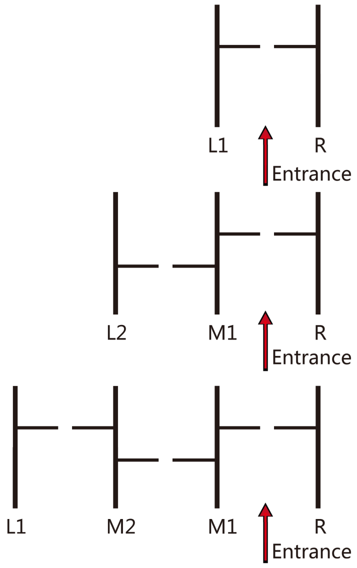
- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- Ensure correct wiring of the terminals for connection to an AC mains supply.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- This equipment is suitable for mounting on concrete or other non-combustible surface only.
- Install the equipment according to the instructions in this manual.
- To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- Stainless steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.

- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

Available Models

Product Name	Model	Description	Example
Flap Barrier	DS-K3Y411X-L1	Left Pedestal 1	DS-K3Y411X-L1/Dp60 DS-K3Y411X-L1/Dp60-S12
	DS-K3Y411X-L2	Left Pedestal 2	DS-K3Y411X-L2/Dp60 DS-K3Y411X-L2/Dp60-S12
	DS-K3Y411X-M1	Middle Pedestal 1	DS-K3Y411X-M1/M-Dp60 DS-K3Y411X-M1/M-Dp60-S12
	DS-K3Y411X-M2	Middle Pedestal 2	DS-K3Y411X-M2/M-Dp60 DS-K3Y411X-M2/M-Dp60-S12
	DS-K3Y411X-R	Right Pedestal	DS-K3Y411X-R/M-Dp60 DS-K3Y411X-R/M-Dp60-S12

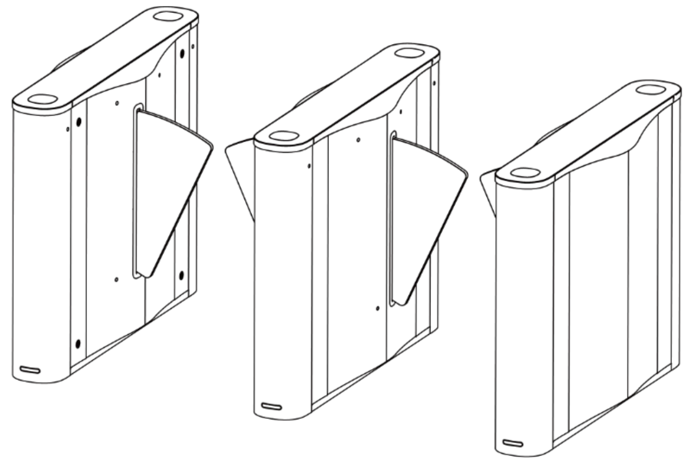
You can follow the picture below to select pedestals:



Contents

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

- 32-bit high-speed processor
- TCP/IP network communication and network speed adaptive
  The communication data is specially encrypted to relieve the concern of privacy leak
- Permissions validation and anti-tailgating
- Remaining open/closed mode selectable
- Bidirectional (Entering/Exiting) lane
  The barrier opening and closing speed can be configured according to the visitor flow
- 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
- IP conflict detection
- Remote control and management
- Online/offline operation
- LED indicates the entrance/exit and passing status

- Barrier is in open status when powered down; If the device is installed with supercapacitor, 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
- Opens/Closes barrier according to the schedule template

Chapter 2 System Wiring

The preparation before installation and general wiring.

Steps

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+200 mm. L represents the lane width.

3. Slot on the installation surface and dig installation holes according to the hole position diagram.

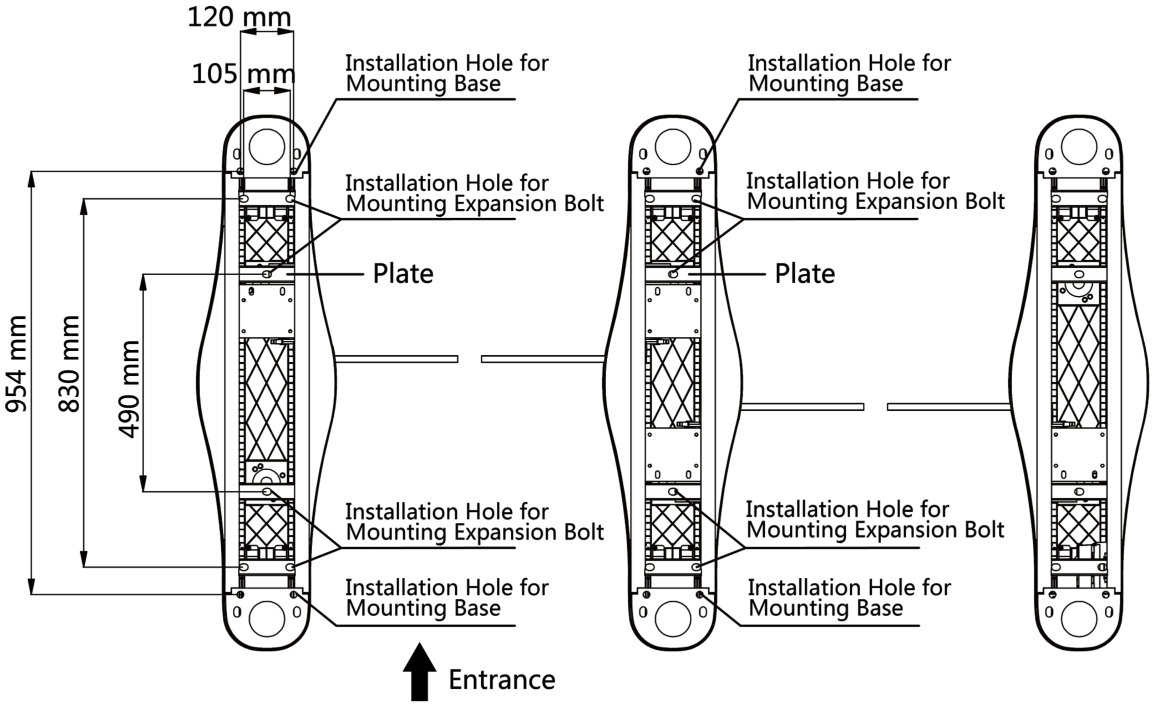

120 mm
105 mm
Installation Hole for Mounting Base
Installation Hole for Mounting Base
Installation Hole for Mounting Expansion Bolt
Installation Hole for Mounting Expansion Bolt
Plate
Plate
954 mm
830 mm
490 mm
Installation Hole for Mounting Expansion Bolt
Installation Hole for Mounting Expansion Bolt
Installation Hole for Mounting Base
Installation Hole for Mounting Base
Entrance

Figure 2-1 Hole Position Diagram

4. Bury cables. Each lane buries 1 network cable and 1 high voltage cable. For details, see the system wiring diagram below.

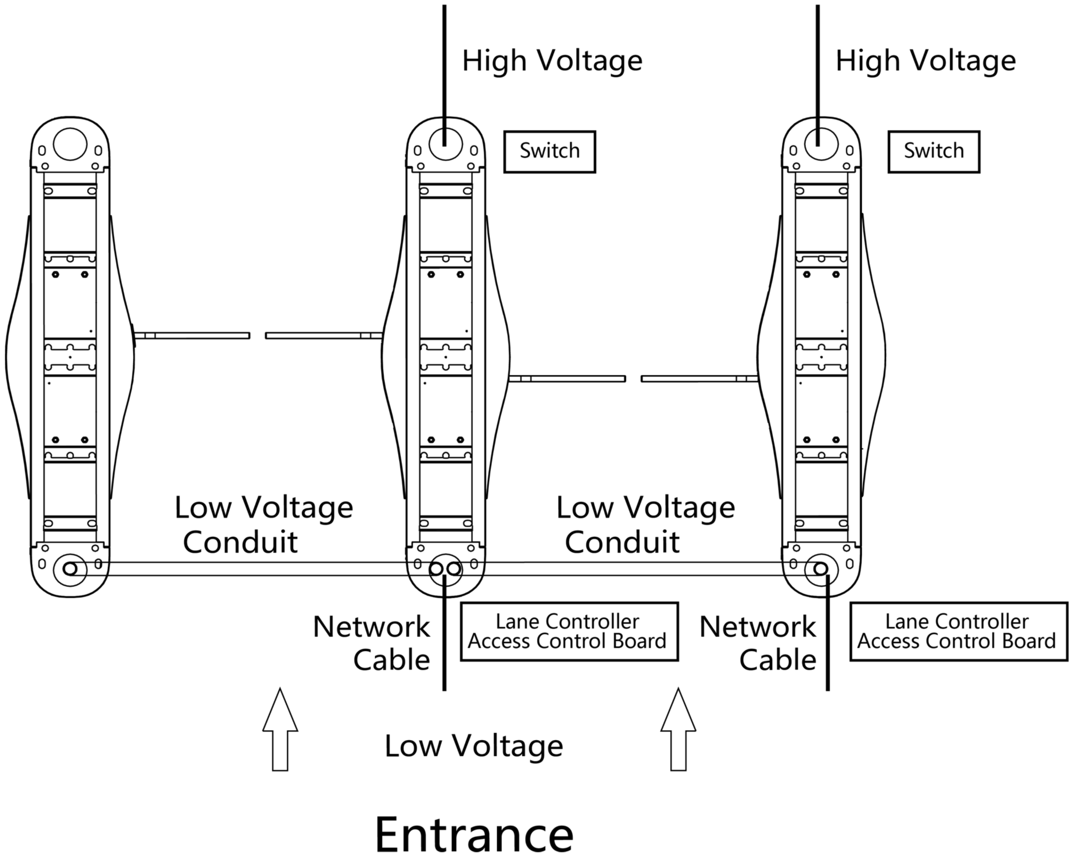


Figure 2-2 System Wiring Diagram (General Wiring)

Note

- The supplied interconnecting cable length is 3.75 m. If you need a longer one, you can buy a new accessory.
- 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 at the entrance, 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. And the suggested network cable length should be less than 100 m.

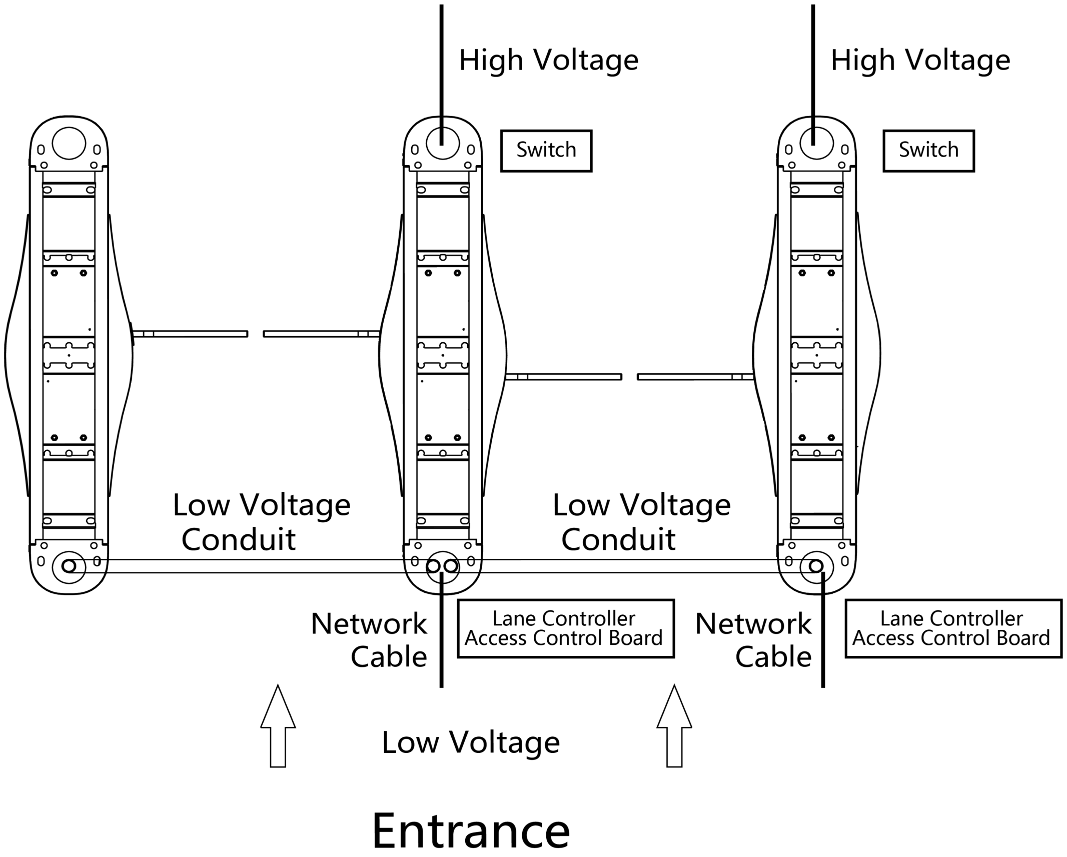


Figure 2-3 Wire Face Recognition Terminal

Note

- The face recognition terminal installed on the left pedestal will gain power from the sub switch, which should connect to high voltage.
- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- The supplied interconnecting cable length is 3.75 m. If you need a longer one, you can extend the cable by yourself.
- If you want to bury both of the AC power cord and the low voltage cable at the entrance, 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. And the suggested network cable length should be less than 100 m.

Chapter 3 Installation

3.1 Disassemble Pedestals

Before installation, you should use the key to open the pedestals.

View the pictures below to find the lock holes.

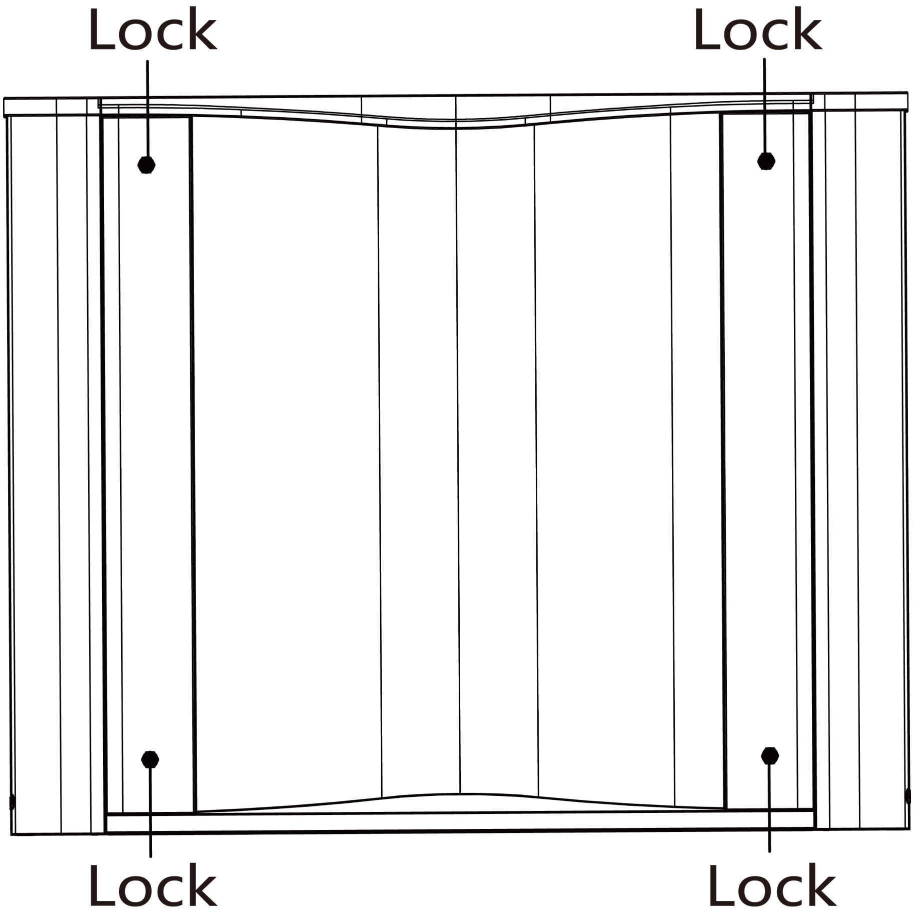


Figure 3-1 Lock Holes

Note

Please check and avoid metal pieces dropped into the high and low voltage modules, which will cause short circuit.

3.2 Install Pedestals

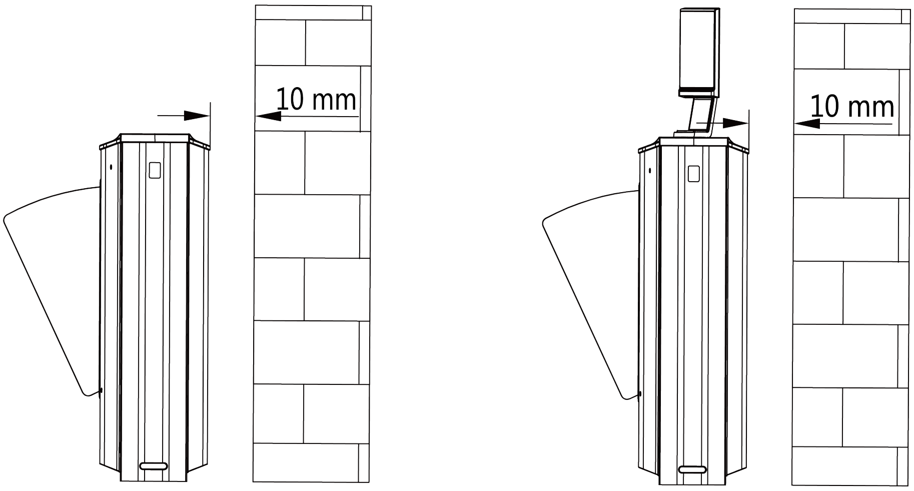
Before You Start

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

Steps

Note

- The device should be installed on the concrete surface or other non-flammable surfaces.
- For opening the pedestal conveniently, make sure the distance between the pedestal and the wall should be more than 10 mm.



- The dimension is as follows.

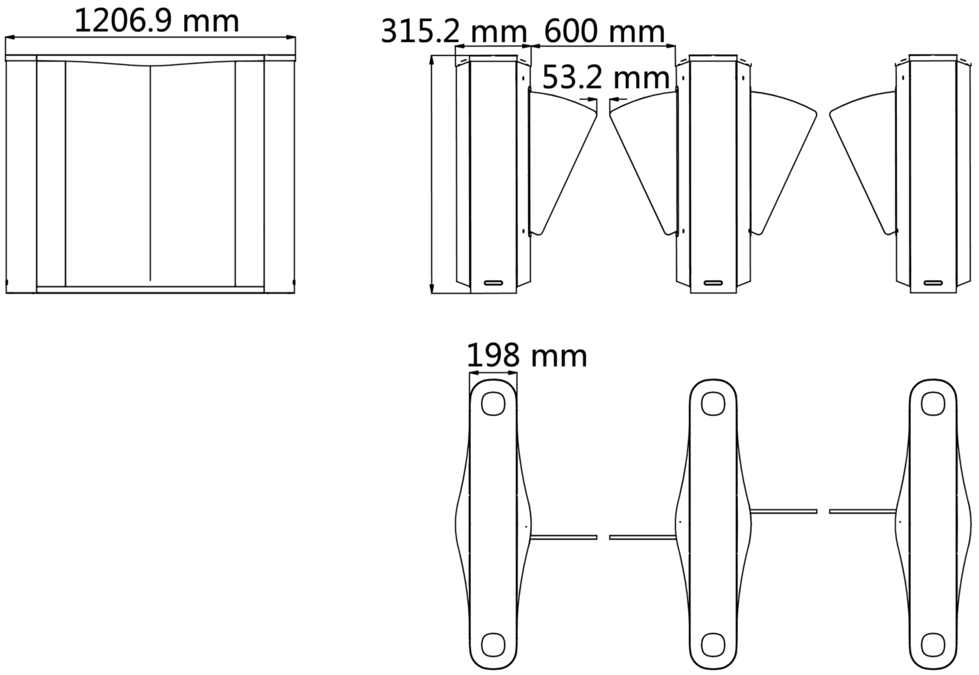


Figure 3-2 Dimension

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Drill holes on the ground according to the installation holes on the pedestals and insert the expansion sleeves.
3. According to the entrance and exit marks on the pedestals, move the pedestals to the corresponded positions.

Note

Make sure the installation holes on the pedestals and the base are aligned with each other.

4. Secure the pedestals with expansion bolts.

Note

- The suggested expansion bolt's size is M12*150. You can change or transform the expansion bolt according to your actual needs. But make sure that do not drill through the floor. If the floor is too soft to install, it is suggested to apply the construction adhesive to strengthen.
- Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 150 mm.
- The installation footprint is as follows:

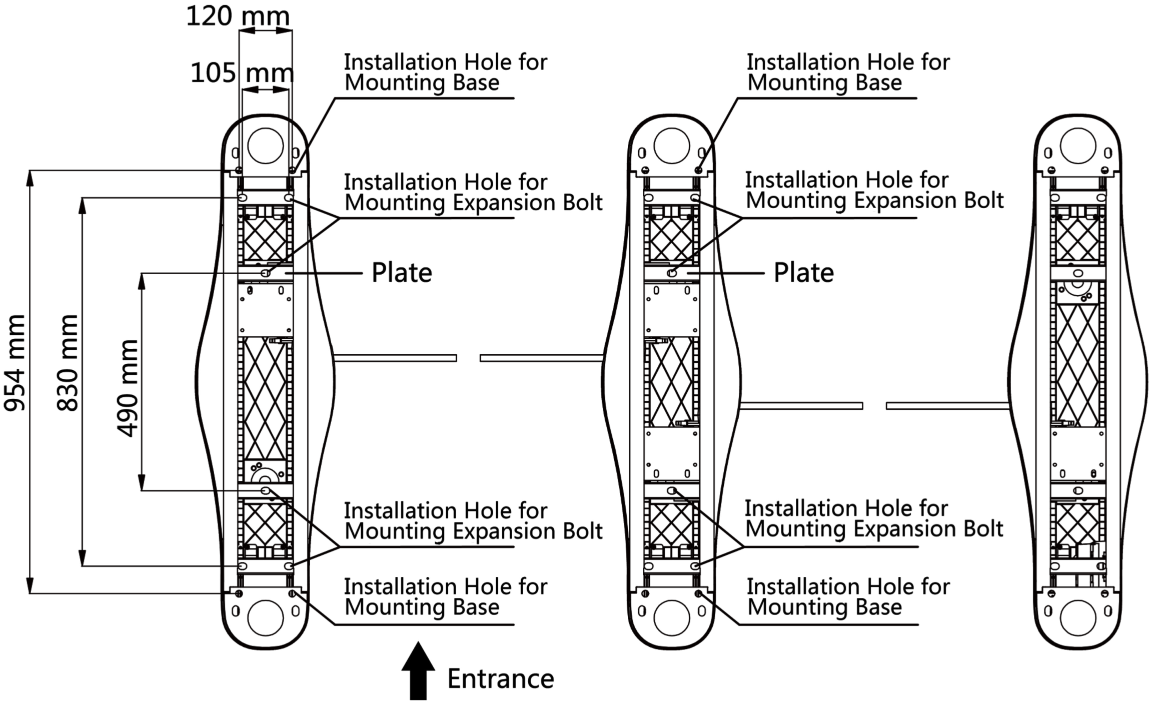

120 mm
105 mm
954 mm
830 mm
490 mm
Installation Hole for Mounting Base
Installation Hole for Mounting Expansion Bolt
Plate
Installation Hole for Mounting Expansion Bolt
Installation Hole for Mounting Base
Entrance
Installation Hole for Mounting Base
Installation Hole for Mounting Expansion Bolt
Plate
Installation Hole for Mounting Expansion Bolt
Installation Hole for Mounting Base

Figure 3-3 Installation Footprint

5. After installation, assemble the components and screws back to the pedestal in reverse order (except for protective sheets).

Chapter 4 General Wiring

Note

- After maintenance, you should close the water-proof cover over the high/low voltage module.
- 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.

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 240 VAC, 50 to 60 Hz.

The picture displayed below describes each component's position on the turnstile.

Note

The diagram is for reference only.

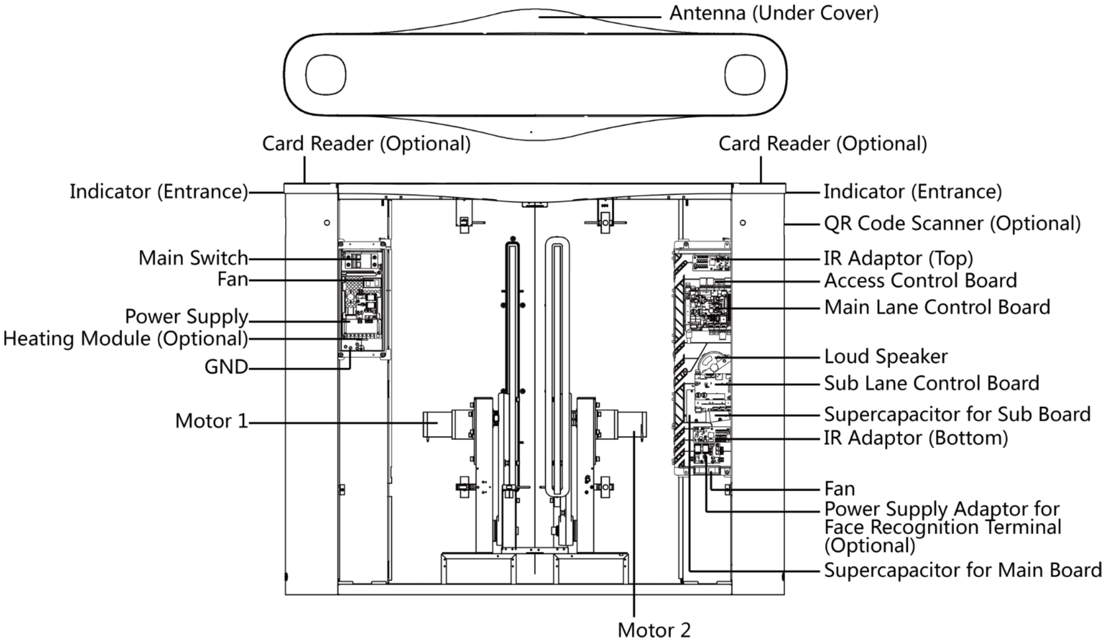
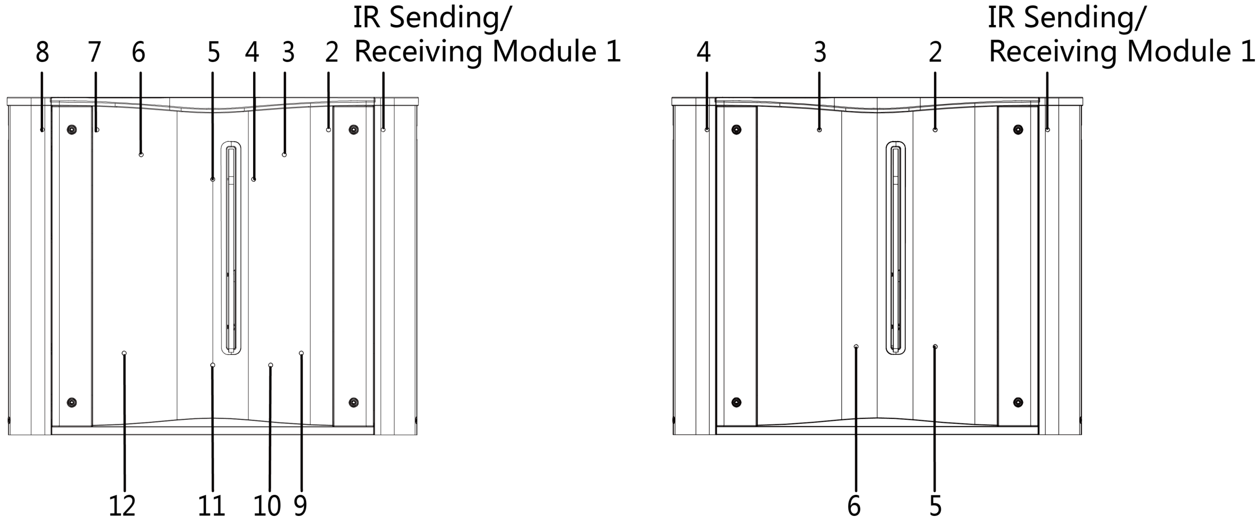


Figure 4-1 Components Diagram 1

Note

The reinstalled supercapacitor needs to be powered on for at least 3 minutes before it can work normally.

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


8
7
6
5
4
3
2
IR Sending/ Receiving Module 1
12
11
10
9
4
3
2
IR Sending/ Receiving Module 1
6
5

12 IR Sending/Receiving Modules

6 IR Sending/Receiving Module

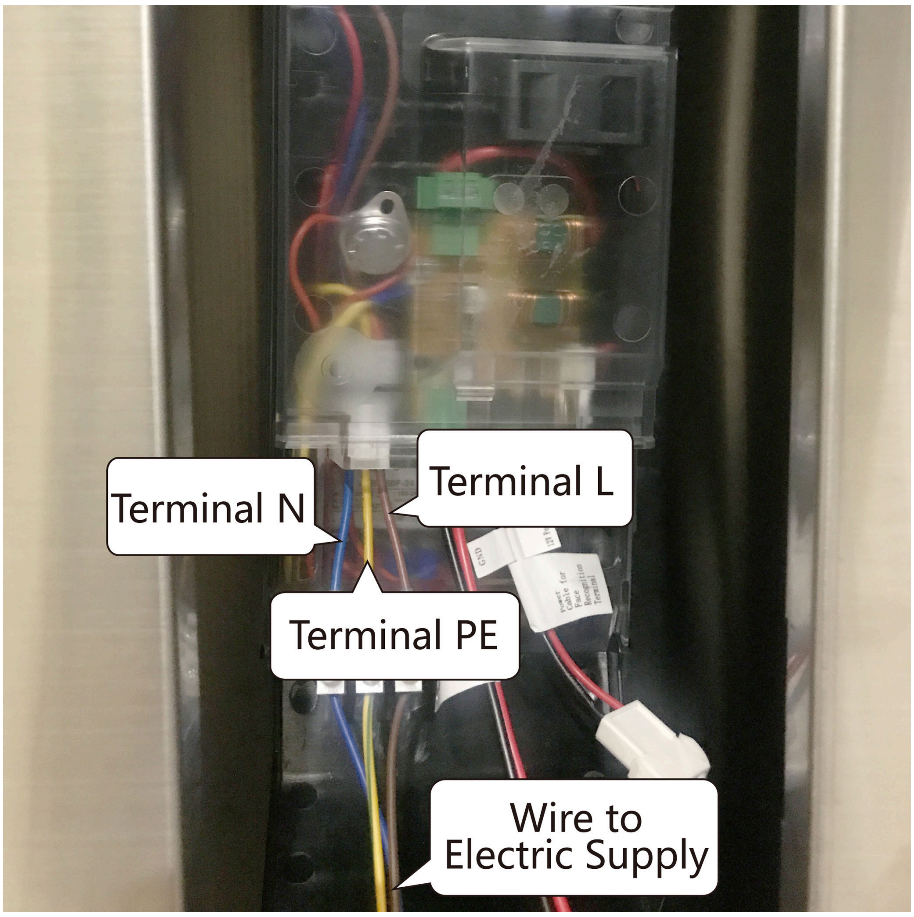
Figure 4-2 Components 2

Note

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

4.2 Wiring Electric Supply

Wire electric supply with the switch in the pedestal. Terminal L and terminal N are on the switch, while terminal PE should connect to a ground wire (yellow and green wire).



Note

- The cable bare part should be no more than 8 mm. It is suggested that you can immerse the bare part into the liquid tin. If possible, wear an insulation cap at the end of the bare cable. Make sure there's no bare copper or cable after the wiring.
- The Terminal L and the Terminal N cannot be wired reversely. Do not wire the input and output terminal reversely.
- To avoid people injury and device damage, when testing, the ground resistance of the equipotential points should not be larger than 2 Ω。
- Use the device in conjunction with an UPS.

4.3 Wire Interconnecting Cable

You should use interconnecting cables to connect the main lane board and the sub lane board for components communication.

Note

The right/middle pedestal contains an interconnecting cable, including one network cable (3.75 m) and one 2-core cable.

The picture displayed below describes the cable hole's position on the pedestals.

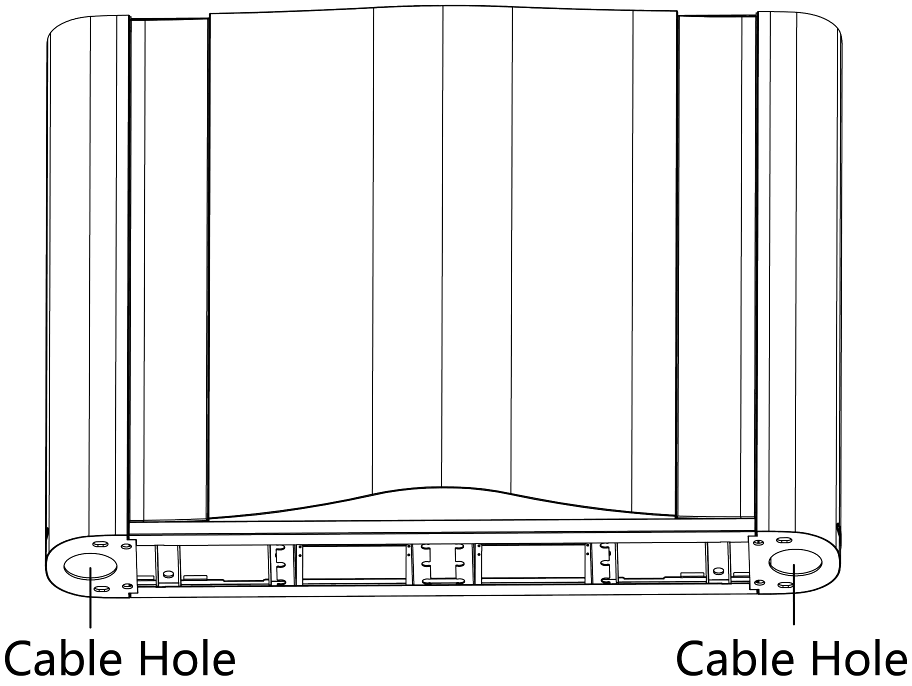


Figure 4-3 Cable Hole of Interconnecting Cable

Follow the instructions below to connect the interconnecting cable.

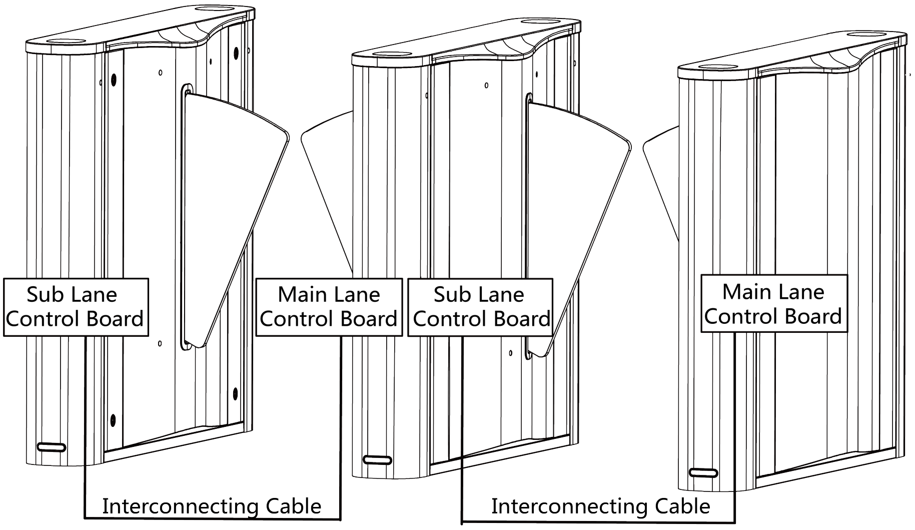


Figure 4-4 Connect Interconnecting Cable

4.4 Face Recognition Terminal Power Supply Wiring (Optional)

If connect to face recognition terminals, the face recognition terminals of right pedestal and middle pedestal (entrance) will power supplied by 12 V terminal on left side of the pedestal.

The face recognition terminal of left pedestal and middle pedestal (exit) will power supplied by 12 V terminal of the power adaptor of the right pedestal. The sub lane control board will power supplied by the power adaptor.

For details about the wiring, see the picture below:

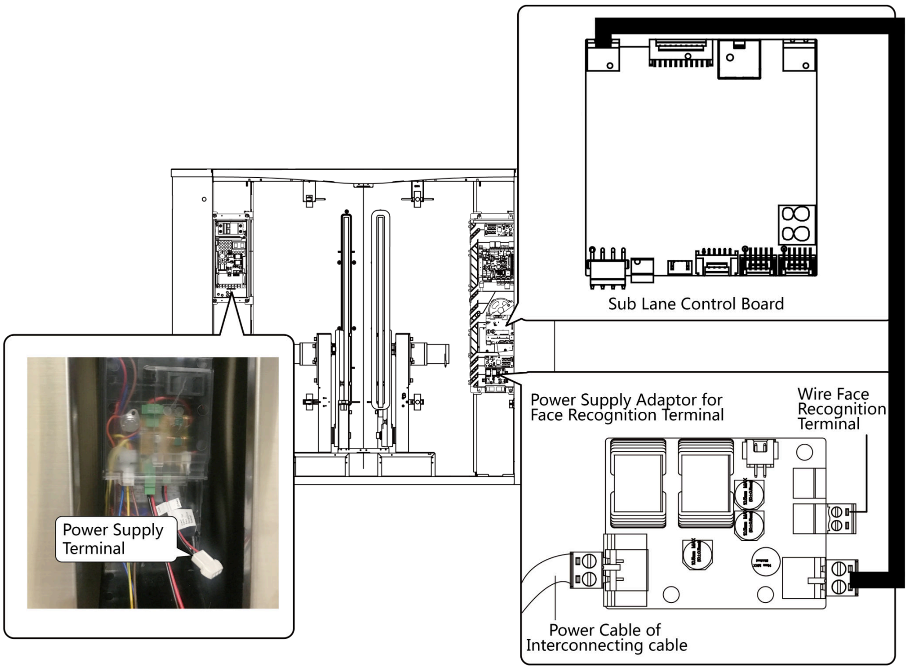

Sub Lane Control Board
Power Supply Adaptor for Face Recognition Terminal
Wire Face Recognition Terminal
Power Supply Terminal
Power Cable of Interconnecting cable

Figure 4-5 Face Recognition Terminal Power Supply Wiring

4.5 Terminal Description

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

4.5.1 UART Related Terminal and Position

View the UART position on the lane control board and the access control board. You can also view the UART related terminals and DIP switch information.

The reserved UART terminal positions in the turnstile and their corresponded UART No. are as follows:

Note

The diagram is for reference only.

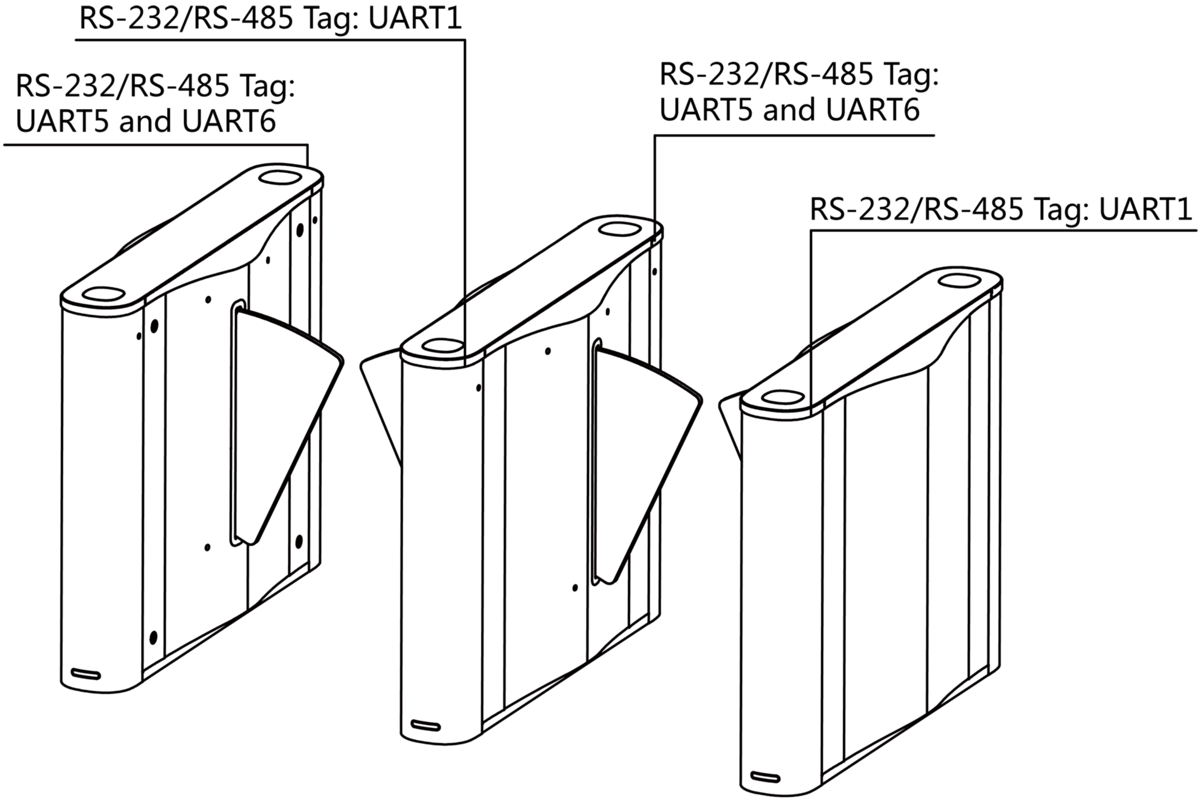

RS-232/RS-485 Tag: UART1
RS-232/RS-485 Tag: UART5 and UART6
RS-232/RS-485 Tag: UART5 and UART6
RS-232/RS-485 Tag: UART1

Figure 4-6 Interface and Corresponded UART No.

The UART related terminals are on the access control board and BUS of the lane control board. You can switch between the RS-232 and the RS-485 communication modes via DIP switch.

The UART and the related DIP switch information is as follows:

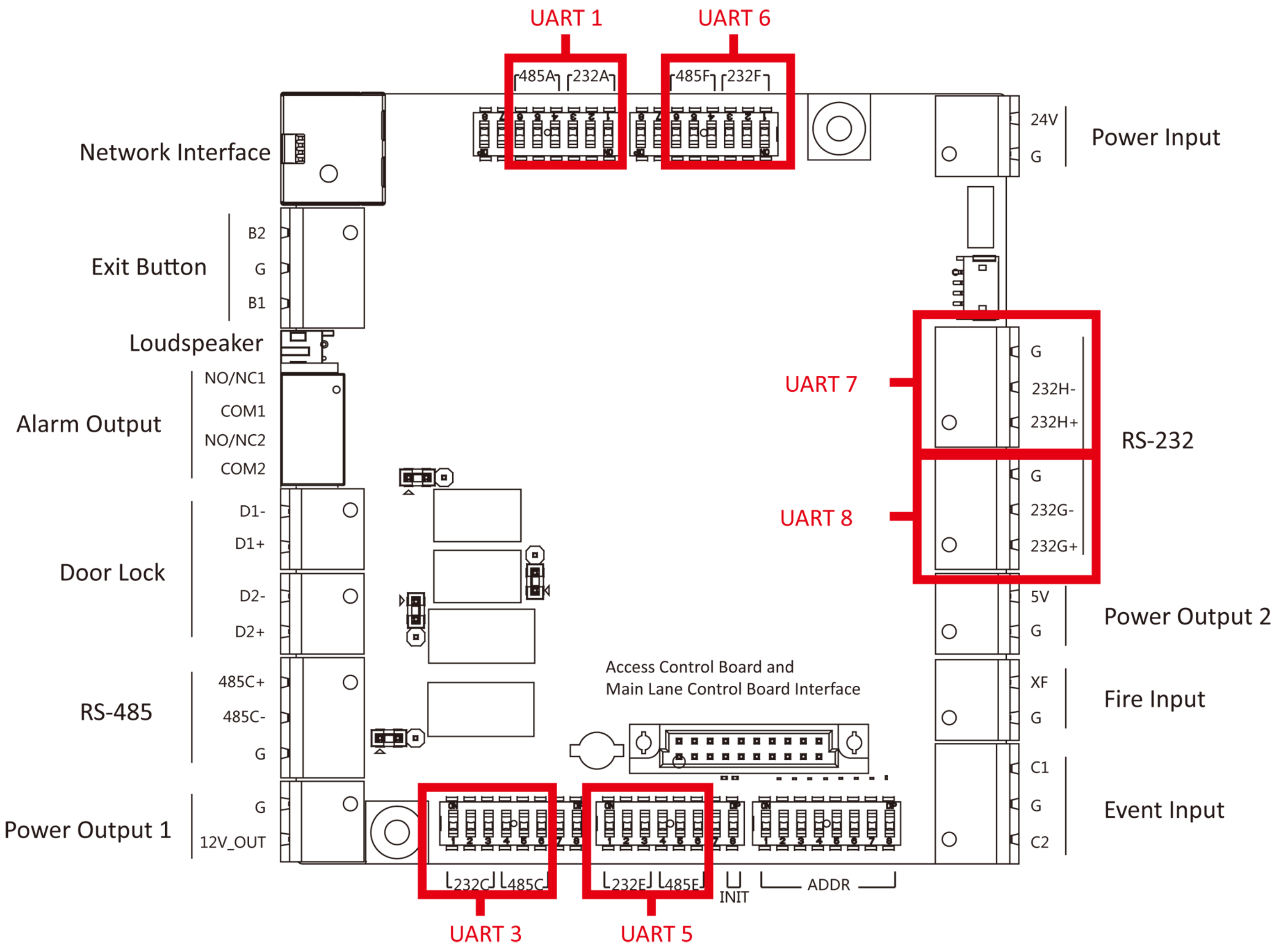


Figure 4-7 UART No. Description

Table 4-1 UART Related Position/Terminals/DIP Switch Introduction

UART No.	Related Terminals	Terminal Position	DIP Switch No.	Function
UART1 **Note** External card reader is recommended to access.	485A/232A	BUS of Main Lane Control Board	1 to 3	ON: UART1 is RS-232A Interface
			4 to 6	ON: UART1 is RS-485A Interface
			7	Reserved
			8	Reserved
UART3	485C+/232C+	Access Control Board	1 to 3	ON: UART3 is RS-232C Interface

UART No.	Related Terminals	Terminal Position	DIP Switch No.	Function
Note External card reader is recommended to access.			4 to 6	ON: UART3 is RS-485C Interface
	485C-/232C-		7	Reserved
			8	Reserved
UART5 **Note** External card reader is recommended to access.	485E+/232E+	BUS of Sub Lane Control Board	1 to 3	ON: UART3 is RS-232E Interface
			4 to 6	ON: UART3 is RS-485E Interface
	485E-/232E-		7	Reserved
			8	Reserved
UART6 **Note** Face recognition terminal is recommended to access.	485F+/232F+	BUS of Sub Lane Control Board	1 to 3	ON: UART3 is RS-232F Interface
			4 to 6	ON: UART3 is RS-485F Interface
	485F-/232F-		7	Reserved
			8	Reserved
UART7	232G+/232G-	Access Control Board	/	/
UART8	232H+/232H-	Access Control Board	/	/

4.5.2 Main Control Board Terminal Description

The main lane control board contains power input, BUS interface, interconnecting interface, supercapacitor interface, barrier position control board interface and motor drive interface.

The picture displayed below is the main control board diagram.

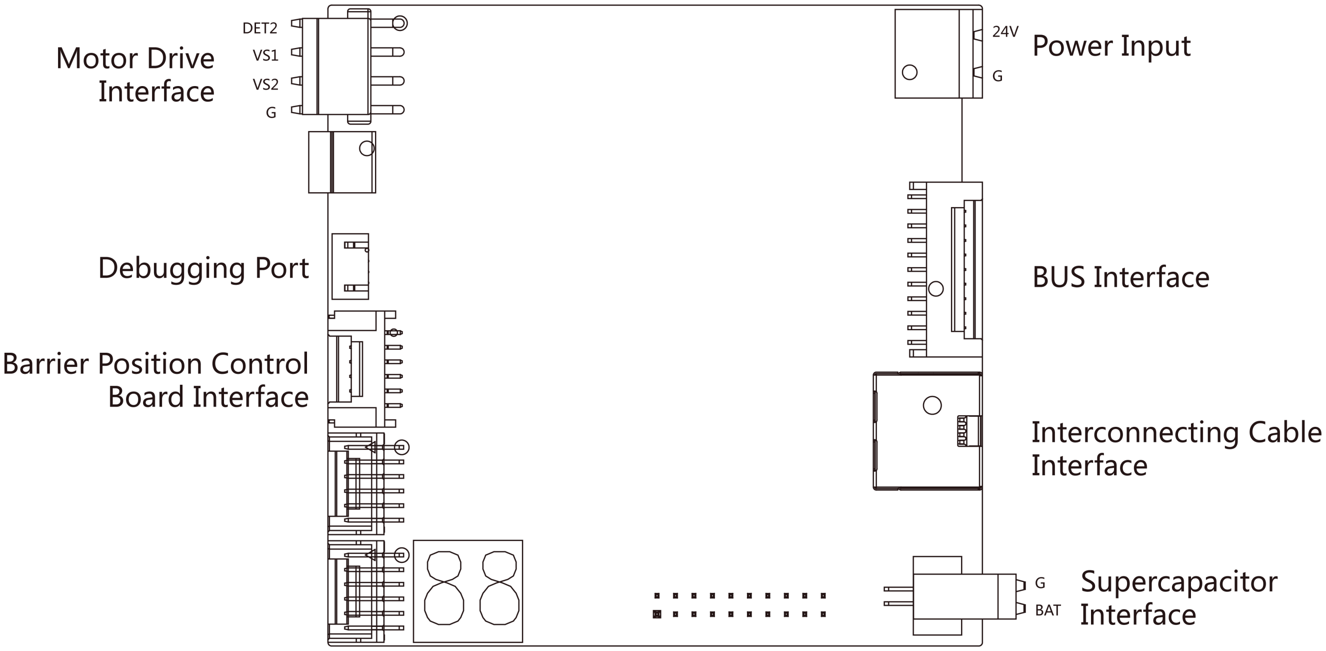


Figure 4-8 Main Control Board Terminal

4.5.3 Sub Control Board Terminal Description

The sub lane control board contains power input, BUS interface, interconnecting interface, supercapacitor interface, barrier position control board interface and motor drive interface.

The picture displayed below is the sub control board diagram.

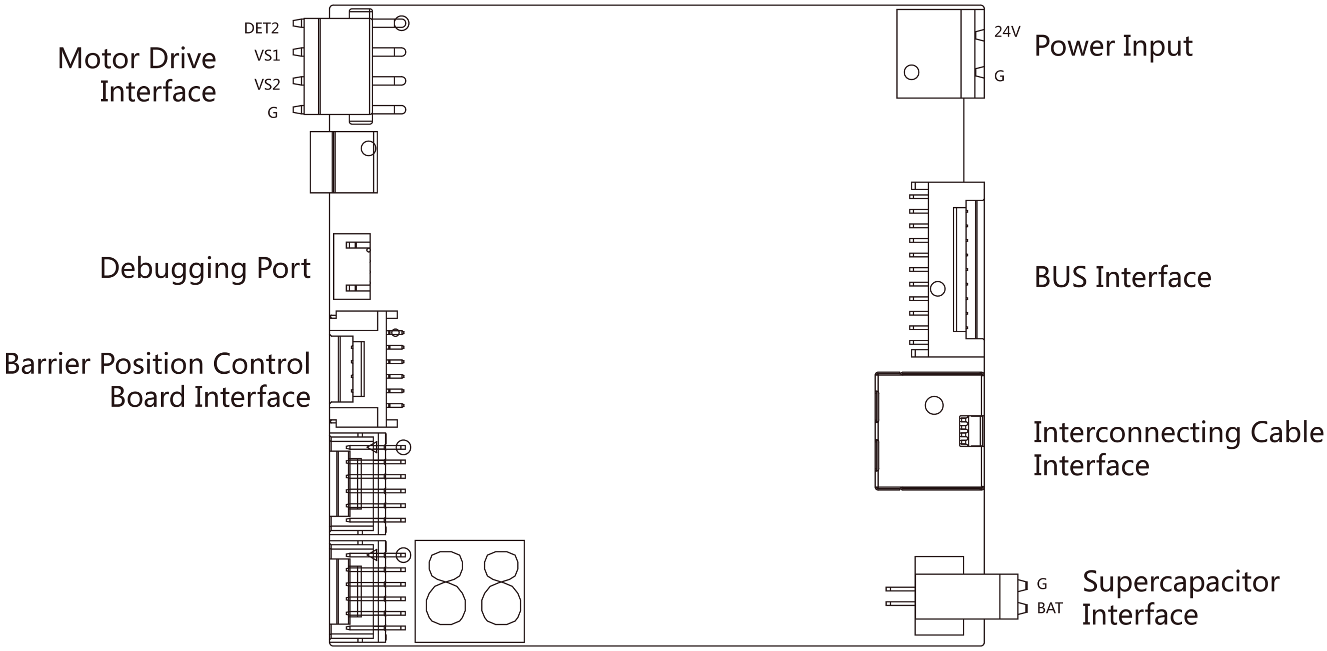


Figure 4-9 Sub Control Board Terminal

4.5.4 BUS Terminal Description

You can connect the lane controller light board, fan, TAMPER, lane control board, card reader, face recognition terminal, QR code scanner, etc. via the BUS terminal.

Note

Part of the wiring has been completed at the factory, please connect according to actual needs.

Table 4-2 BUS Terminal in Main Lane Controller

Terminal Name	Description
Lane Controller Light Board 1	Connects lane controller light board 1
Lane Controller Light Board 2	Connects lane controller light board 2
Fan	Connects fan
TAMPER1	Connects TAMPER1
TAMPER2	Connects TAMPER2
Lane Controller Board	Connects main lane controller board
5 V	Reserved
IR Adaptor	Connects IR adaptor

Terminal Name	Description
UART 1 **Note** External card reader is recommended to access.	Red 12 V: connects 12 VDC power supply terminal
	Yellow 485A/232A+: card reader RS-485A+/RS-232A+ access terminal
	Blue 485A/232A-: card reader RS-485A-/RS-232A- access terminal
	Black GND: grounding

Table 4-3 BUS Terminal in Sub Lane Controller (Left Pedestal)

Terminal Name	Description
Lane Controller Light Board 1	Connects lane controller light board 1
Lane Controller Light Board 2	Connects lane controller light board 2
Fan	Connects fan
TAMPER1	Connects TAMPER1
TAMPER2	Connects TAMPER2
Lane Controller Board	Connect sub lane controller board
5 V	Reserved
IR Adaptor	Connects IR adaptor
UART 5 **Note** External card reader is recommended to access.	Red 12 V: connects 12 VDC power supply terminal
	Yellow 485E/232E+: card reader RS-485E+/RS-232E+ access terminal
	Blue 485E/232E-: card reader RS-485E-/RS-232E- access terminal
	Black GND: grounding
UART 6 **Note** External face recognition terminal is recommended to access.	Red 12 V: connects 12 VDC power supply terminal
	Yellow 485F/232F+: card reader RS-485F+/RS-232F+ access terminal
	Blue 485F/232F-: card reader RS-485F-/RS-232F- access terminal
	Black GND: grounding

Table 4-4 BUS Terminal in Sub Lane Controller (Middle Pedestal)

Terminal Name	Description
Lane Controller Light Board 1	Connects lane controller light board 1
Lane Controller Light Board 2	Connects lane controller light board 2

Terminal Name	Description
Lane Controller Board	Connect sub lane controller board
5 V	Reserved
IR Adaptor	Connects IR adaptor
UART 5 **Note** External card reader is recommended to access.	Red 12 V: connects 12 VDC power supply terminal
	Yellow 485E/232E+: card reader RS-485E+/RS-232E+ access terminal
	Blue 485E/232E-: card reader RS-485E-/RS-232E- access terminal
	Black GND: grounding
UART 6 **Note** External face recognition terminal is recommended to access.	Red 12 V: connects 12 VDC power supply terminal
	Yellow 485F/232F+: card reader RS-485F+/RS-232F+ access terminal
	Blue 485F/232F-: card reader RS-485F-/RS-232F- access terminal
	Black GND: grounding

4.5.5 Access Control Board Terminal Description

Access control board is mainly used for authority identification, external device accessing, and communication with the upper platform and lane controller.

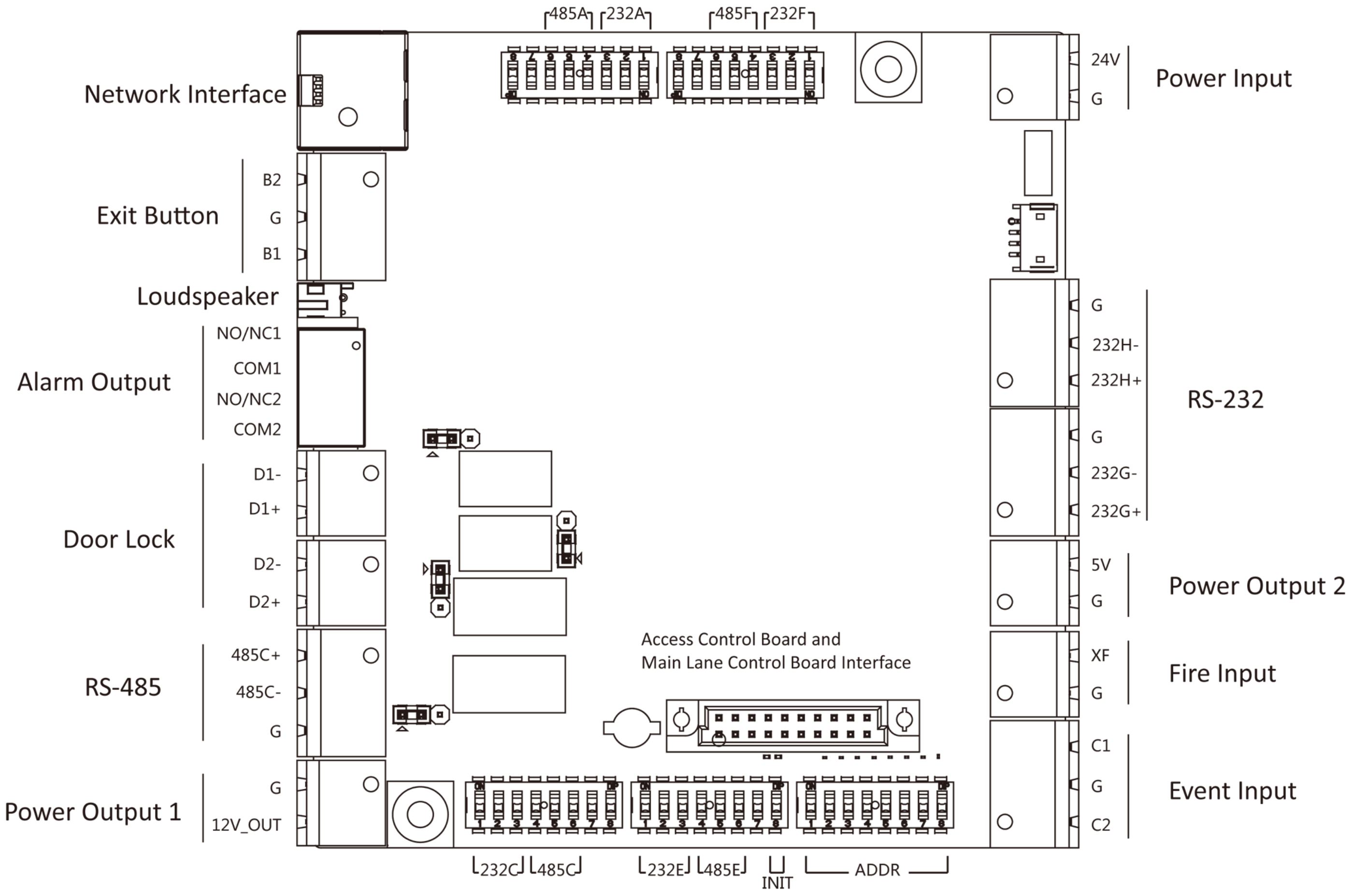


Figure 4-10 Access Control Board Terminal

Table 4-5 Access Control Board Terminal Description

Access Control Board Terminal Description			
Power Output 1	+12 V	12 VDC Power Output	/
	G	Grounding	
RS-485 Interface	RS-485 C+	Connect to Card Reader RS485+	• RS-485 card reader ID factory DIP is 1 and 3. 1 represents the passage entrance, and 3 represents the passage exit. UART 1
	RS-485 C-	Connect to Card Reader RS485-	
	GND	Grounding	

Access Control Board Terminal Description			
			in the main control board corresponds to the entrance card reader, and UART 5 in the main control board corresponds to the exit card reader. • If the user has configured a guest card, the exit needs to be connected to two card readers, one with the DIP 4 and the other with the DIP 3. The card reader 3 and the card receiver are used together, the ordinary user swipes the card on the card reader 4, and the guest user swipes the card on the

Access Control Board Terminal Description			
			card reader 3. - This is the RS-485 interface, which cannot be switched by dialing.
Power Output 2	5 V	5 VDC Power Output	/
	G	Grounding	
RS-232 Interface	G	Grounding	- This is the RS-232 interface, which cannot be switched by dialing. - By default, there is no QR code scanner on the left pedestal of the device entrance. If you need to connect an additional QR code scanner, you need to connect it through the RS-232 interface here. After the cable is connected to the RS-232 interface, it passes
	RS-232 G-	Connect to RS-232G-	
	RS-232 G+	Connect to Card Reader RS-232G+	
	G	Grounding	
	RS-232 H-	Connect to RS-232H-	
	RS-232 H+	Connect to Card Reader RS-232H+	

Access Control Board Terminal Description			
			through the embedded pipe and connects with the QR code on the left.
Power Input	+24 V	24 VDC Power Input	/
	GND	Grounding	
Event Input	C1	Event Alarm Input 1	The event alarm input hardware interface is remaining open, and only supports access to remaining open signals, which can be linked to the host buzzer output, card reader buzzer output, alarm relay output, door open relay output, etc.
	G	Grounding	
	C2	Event Alarm Input 2	
Exit Button	B2	Door 2 Signal Input	/
	G	Grounding	
	B1	Door 1 Signal Input	
Door Lock (Relay)	D1-	Door 1 Relay Output (Dry Contact)	If necessary, the door lock relay can be used to control the third-party barrier switch. D1 controls the door opening
	D1+		

Access Control Board Terminal Description			
			for ordinary entrance, and D2 controls the door opening for ordinary exit.
	D2-	Door 2 Relay Output (Dry Contact)	If necessary, the door lock relay can be used to control the third-party barrier switch. D1 controls the door opening for ordinary entrance, and D2 controls the door opening for ordinary exit.
	D2+		
Alarm Output	NO/NC1	Alarm Output Relay 1 (Dry Contact)	The alarm output supports switch output.
	COM1		
	NO/NC2	Alarm Output Relay 2 (Dry Contact)	The alarm output supports switch output.
	COM2		
Loudspeaker	/	Connect to loudspeaker	/
Network Interface	LAN	Network Accessing	/
Fire Input	XF	Fire input	/
	G	Grounding	

Note

- You can swtich between RS-485 and RS-232 via the DIP switch on the access control board. For details about DIP switch and swiching method, see ***Access Control Board UART Description*** .
- For details about DIP switch operation, see ***DIP Switch Description*** .

4.5.6 Access Control Board UART Description

You can set the device mode, switch the communication mode of the corresponding UART, and initialize the device through the DIP on the access control board.

The DIP switch of the access control board is shown in the figure below:

Note

The diagram is for reference only.

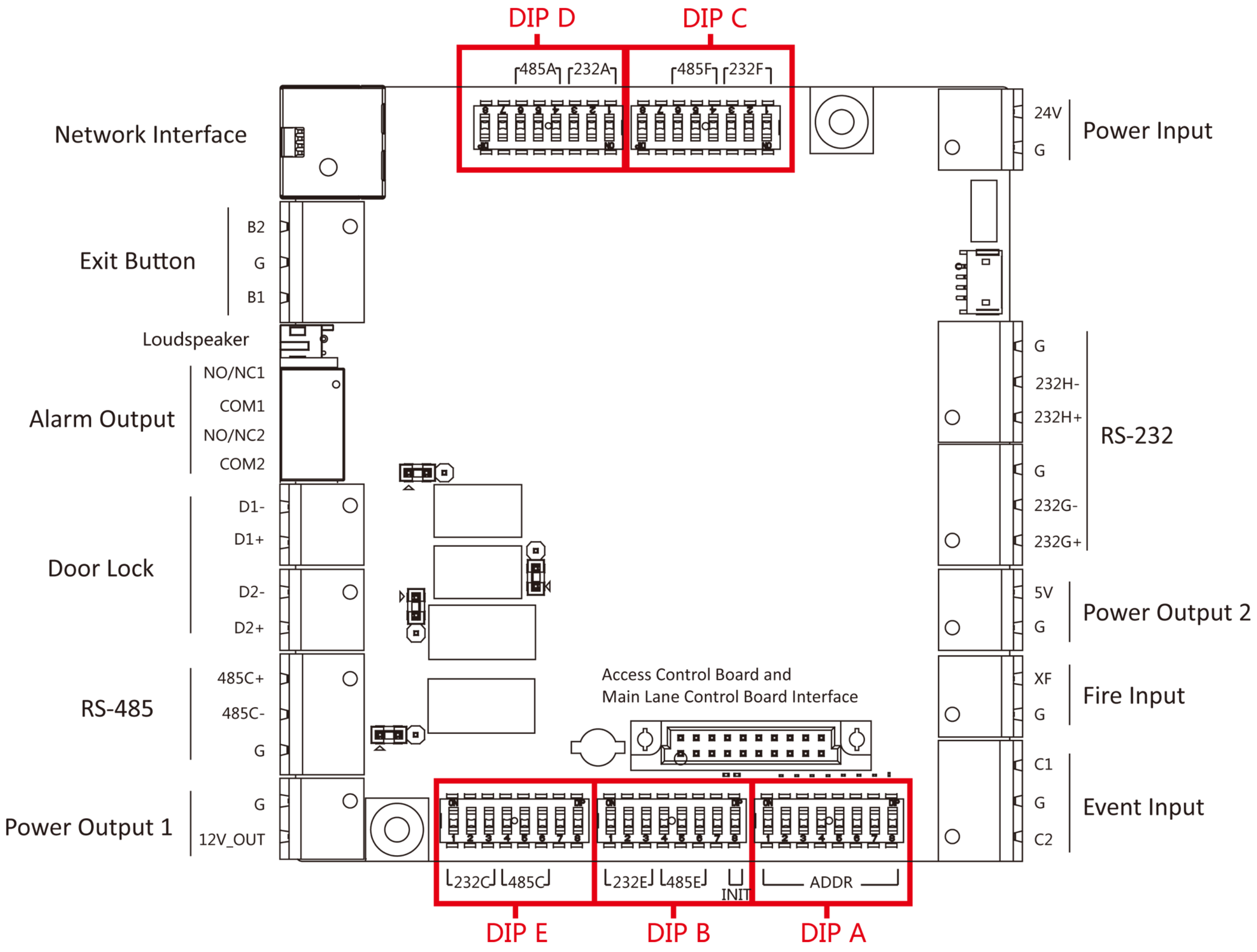


Figure 4-11 DIP Switch on Access Control Board

DIP A can set the device mode, DIP 2 to 5 can set the RS-485/RS-232 interface, and DIP B can also be used to initialize the device.

The UART corresponding to the DIP Switch is shown in the figure below:

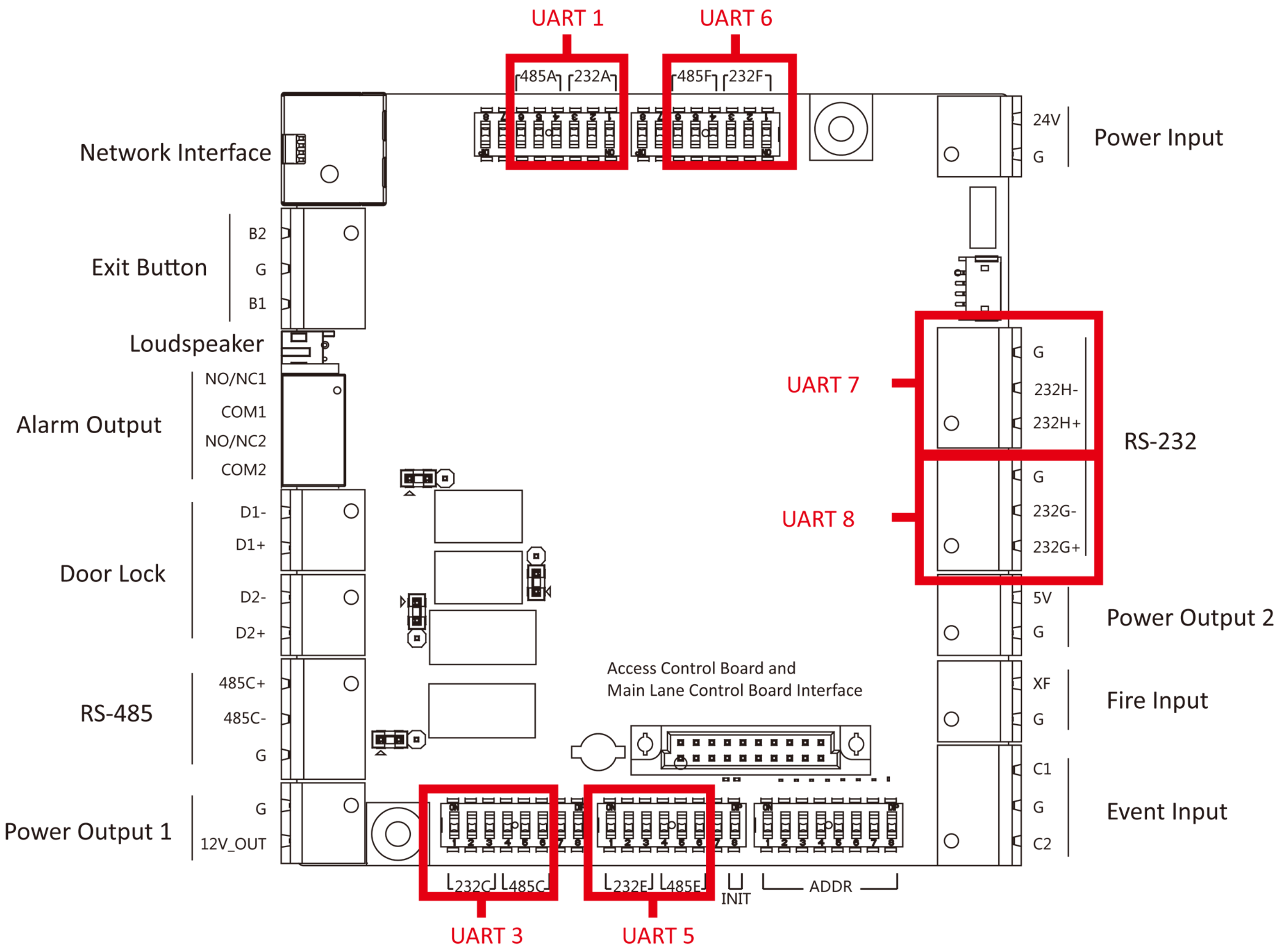
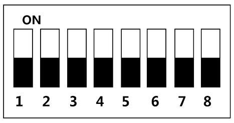
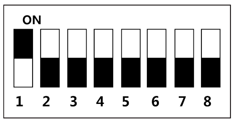
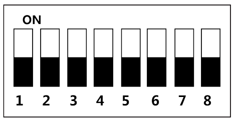
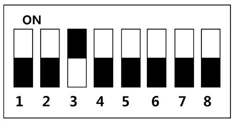
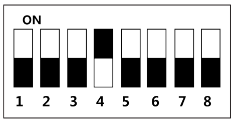
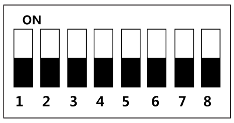
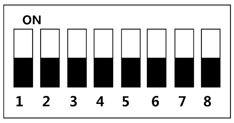
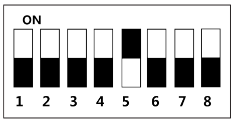
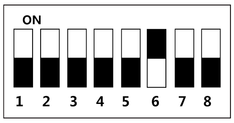
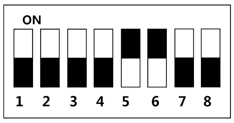
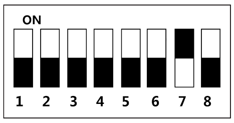
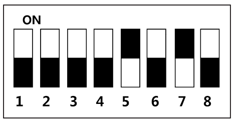
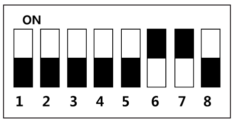
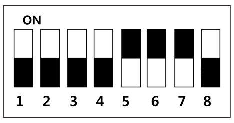
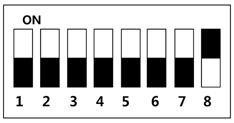


Figure 4-12 UART No. Description

The corresponding functions of different DIP Switch are described as follows:

No.	Device Mode	UART No.	Function	Binary Value
DIP A	1 to 2: Work Mode	/	Normal Mode	
			Test Mode	
	3: Memory Mode		Enable Memory Mode	

No.	Device Mode	UART No.	Function	Binary Value
			Disable Memory Mode	
	4: Keyfob Paring Mode		Enable Keyfob Paring Mode	
			Disable Keyfob Paring Mode	
	5 to 8: Passing Mode		Controlled Bi-direction	
			Controlled Entrance and Prohibit Exit	
			Controlled Entrance and Free Exit	
			Free Bi-direction	
			Free Entrance and Controlled Exit	
			Free Entrance and Prohibit Exit	
			Prohibited Bi-direction	
			Prohibit Entrance and Controlled Exit	

No.	Device Mode	UART No.	Function	Binary Value
			Prohibit Entrance and Free Exit	
DIP B	1 to 3	UART 5	ON: UART 5 is RS-232E Interface	/
	4 to 6		ON: UART 5 is RS-485E Interface	/
	7	/	Reserved	/
	8	/	Default is OFF. You can dial to ON for initial operation	/
DIP C	1 to 3	UART 6	ON: UART 6 is RS-232F Interface	/
	4 to 6		ON: UART 6 is RS-485F Interface	/
	7	/	Reserved	/
	8	/	Reserved	/
DIP D	1 to 3	UART 1	ON: UART 1 is RS-232A Interface	/
	4 to 6		ON: UART 1 is RS-485A Interface	/
	7	/	Reserved	/
	8	/	Reserved	/
DIP E	1 to 3	UART 3	ON: UART 3 is RS-232C Interface	/
	4 to 6		ON: UART 3 is RS-485C Interface	/
	7	/	Reserved	/
	8	/	Reserved	/

Note

For proper communication between turnstile and peripherals, DIP Switch No. 1 to 3, 4 to 6, 7, and 8 of DIP B, DIP C, DIP D, and DIP E cannot be turned ON at the same time.

The reserved UART terminal positions in the turnstile and their corresponded UART No. are as follows:

Note

The diagram is for reference only.

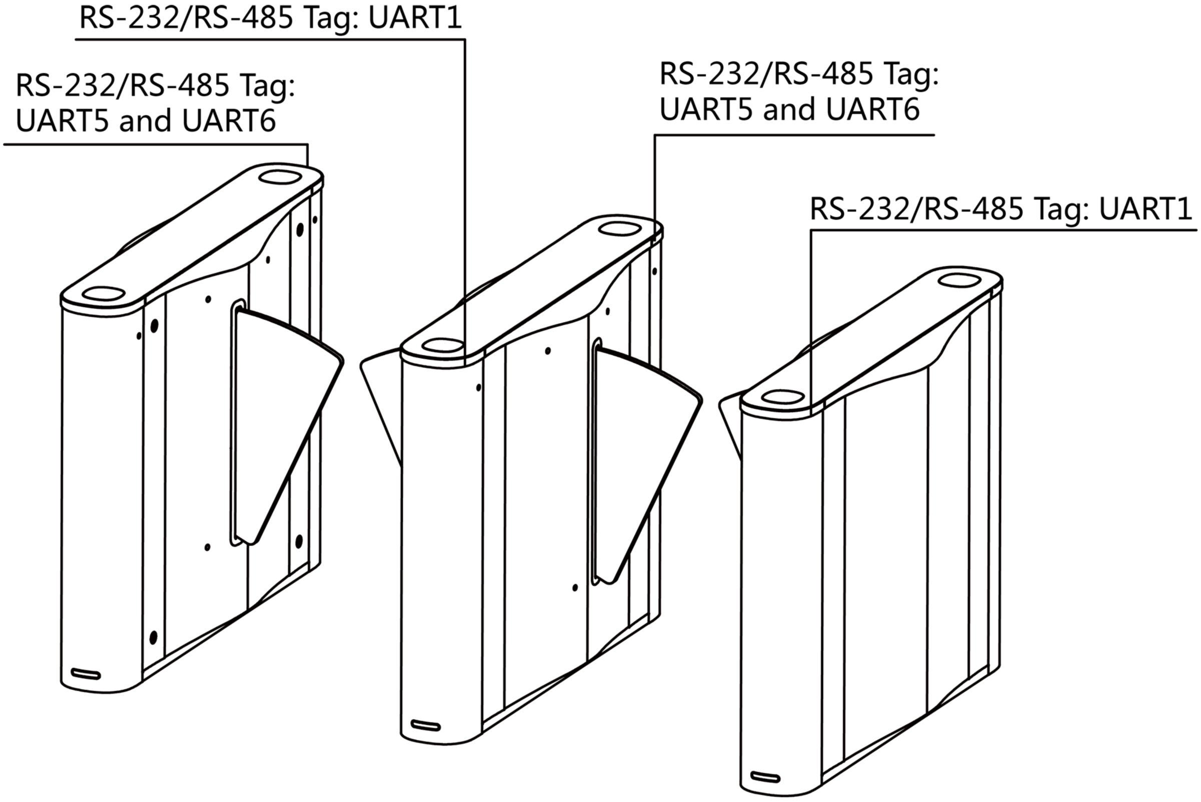
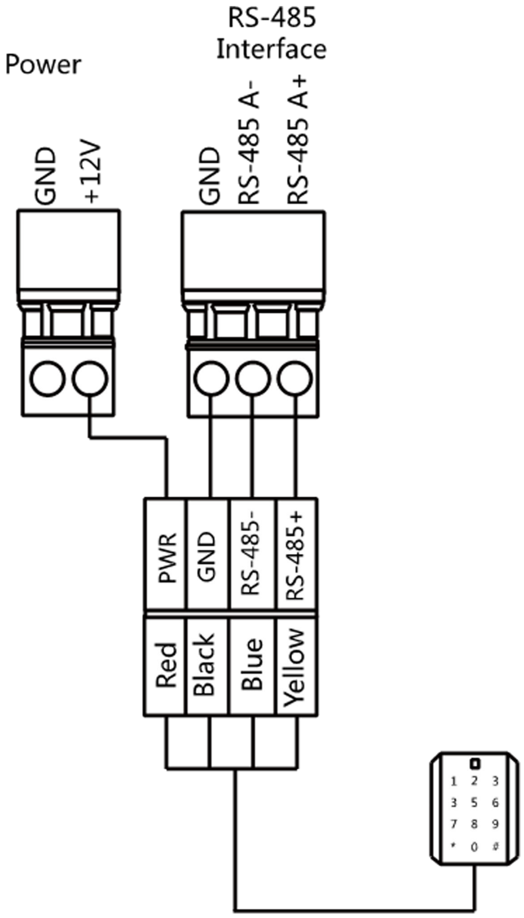

RS-232/RS-485 Tag: UART1
RS-232/RS-485 Tag: UART5 and UART6
RS-232/RS-485 Tag: UART5 and UART6
RS-232/RS-485 Tag: UART1

Figure 4-13 Interface and Corresponded UART No.

4.5.7 RS-485 Wiring



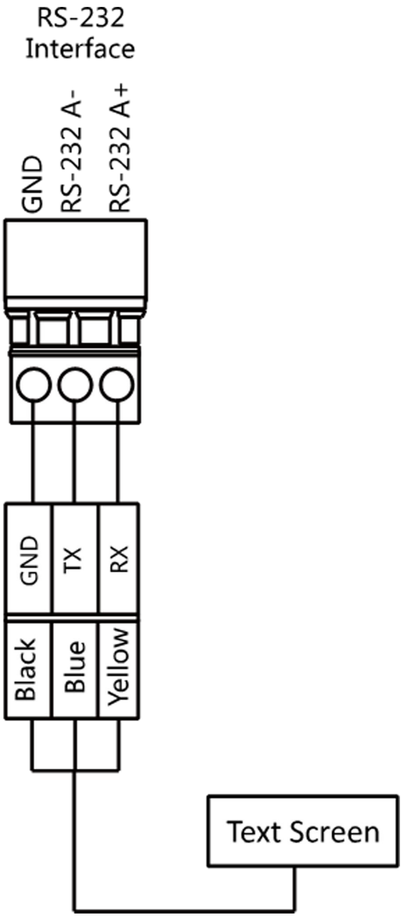
Note

- The RS-485 interfaces are for connecting ID card reader, IC card reader, card reader, card recycler, text screen, and face recognition terminal. Take the wiring of RS-485 card reader as an example.
- For details about text screen, see *Configuring Screen Parameters* in *User Manual of iVMS-4200 AC Client Software*.

4.5.8 RS-232 Wiring

Note

- Access control board of pedestal can connect QR code scanner, card recycler, text screen and face recognition terminal via RS-232 interface.
- For details about text screen, see *Configuring Screen Parameters* in *User Manual of iVMS-4200 AC Client Software*.
- Take the wiring of text screen as an example.



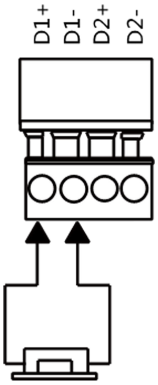
4.5.9 Barrier Control Wiring

By default, the barrier has connected with the access control board. The lane control board can control the barrier status. If possible, the device can connect with a third party lane control board to control the third party barriers. Interface D1 controls barrier opening for entrance, while interface D2 controls barrier opening for exit.

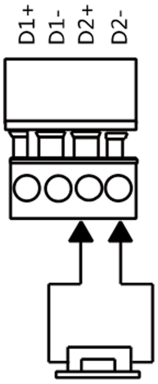
Note

Use the jumper cap to switch the relay status. For details, see ***Barrier Control Relay Output Mode*** .

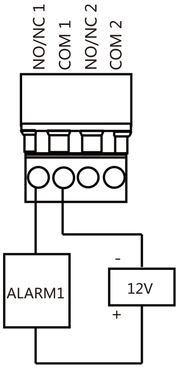
Entering Wiring



Exiting Wiring



4.5.10 Alarm Output Wiring



Note

For details about changing the relay output status via the jumper cap, see ***Alarm Relay Output Mode (NO/NC)*** .

Chapter 5 Device Settings

After installation and wiring completed, the turnstile will learn the open and closed position automatically.

After the learning, the turnstile is in the normal mode. You can also set the turnstile to test mode, passing mode and memory mode, pair the keyfob, initialize the hardware, switching between RS-485 communication mode and RS-232 communication mode, and view relay output NO/NC diagram by setting the DIP switch on the access control board.

- Normal Mode: The device will work properly.
- Test Mode: Test mode is the same as the normal mode except that the device cannot report the alarm, the event, or the people counting information to the center.
- Passing Mode: There are 9 passing modes, including controlled bi-direction, controlled entrance and prohibited exit, controlled entrance and free exit, free bi-direction, free entrance and controlled exit, free entrance and prohibited exit, prohibited bi-direction, prohibited entrance and free exit.
- Memory Mode: By default, the memory mode is enabled. When multiple cards are presented and authenticated, it allows multiple persons passing through the lane. When it counts the passing people number is equal to the card presented times, or no person passing through the lane after the last person passing, the barriers will be closed.

Note

You can also set the DIP switch on the access control board to control the entrance and exit controlling type, keyfob pairing, etc. For details about the DIP switch value, see ***Access Control Board UART Description*** .

5.1 Pair Keyfob (Optional)

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

Note

- Up to 32 keyfobs can be added to the turnstile.
- You can set the keyfob to one-to-one mode or one-to-many mode via the DIP switch on the keyfob. Here takes one-to-one mode as an example to explain. For one-to-many mode, see the keyfob user manual.

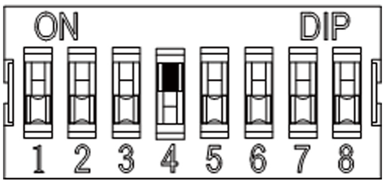
  One-to-One Mode

By default, the keyfob is in one-to-one mode. The keyfob's DIP switch is towards 1 (OFF). The keyfob can control only one turnstile.

One-to-Many Mode

The keyfob's DIP switch is ON. In this mode, the keyfob can control multiple turnstiles.

1. Power off the turnstile.
2. Set the No.4 switch of the DIP Switch on the access control board to the ON side.



3. Power on the turnstile and it will enter the keyfob pairing mode.
4. Hold the **Close** button for more than 10 seconds. Or pair turnstile and keyfob in the client software, see ***Manage Keyfob User*** for more details.

   The keyfob's indicator of the will flash twice if the pairing is completed.
5. Set the No.4 switch to OFF, 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 ***Access Control Board UART Description*** .

6. **Optional:** Go to **System → User → Keyfob User** on the remote control page of the client software to delete the keyfob.

5.2 Initialize Device

Steps

1. Set the No.8 switch of the DIP 2 Switch on the access control board to the ON side.

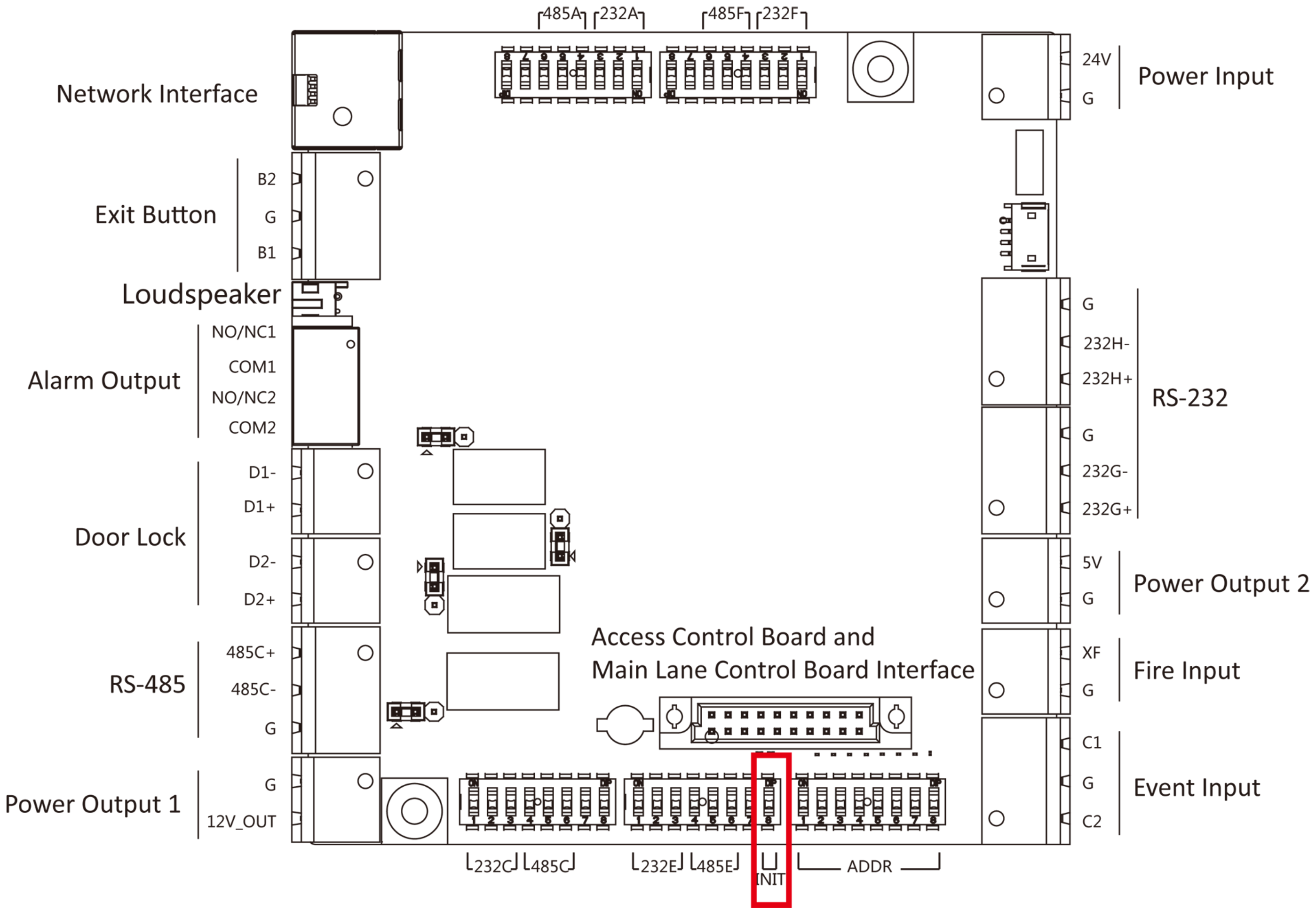


Figure 5-1 Initialization Jumper Cap

2. Disconnect the power and reboot the device.
3. When the beep stopped, set the No.8 switch to the OFF side, and reboot the turnstile to take effect.
4. Disconnect the power and power on the device again.

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.

5.3 Switch Relay Output Mode (NO/NC)

5.3.1 Barrier Control Relay Output Mode

The jumper cap of the barrier control relay on the access control board is as below:

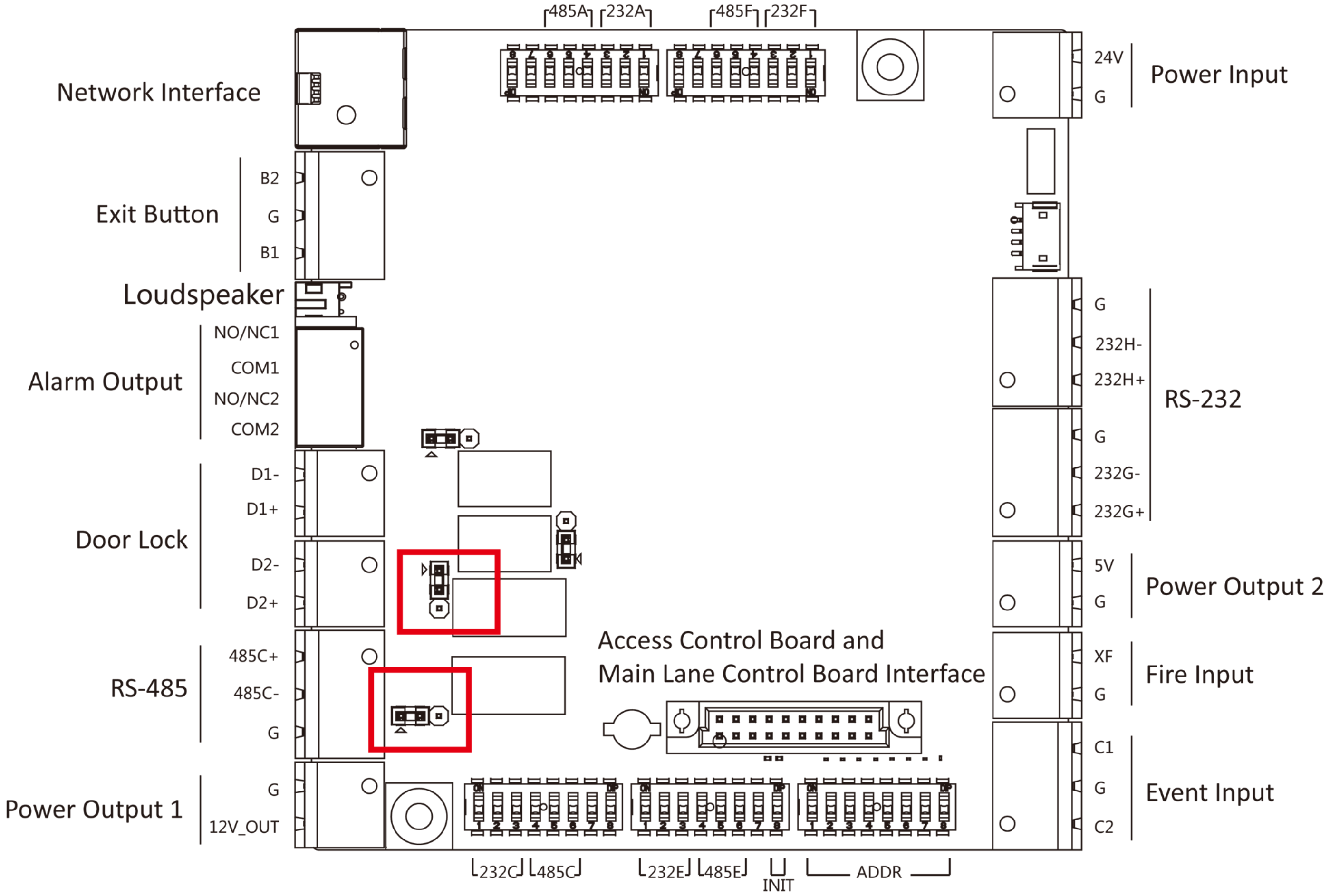


Figure 5-2 Jumper Cap Location (Barrier Control Relay Output Mode)

The jumper cap position of barrier opening (NO) is as below:

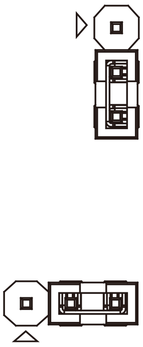


Figure 5-3 Barrier Opening (NO)

The jumper cap position of barrier closing (NC) is as below:

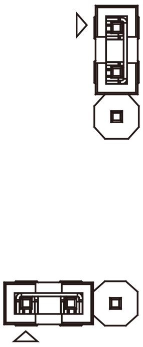


Figure 5-4 Barrier Closing (NC)

Note

The default status is NC.

5.3.2 Alarm Relay Output Mode (NO/NC)

The jumper cap of the alarm relay on the access control board is as below:

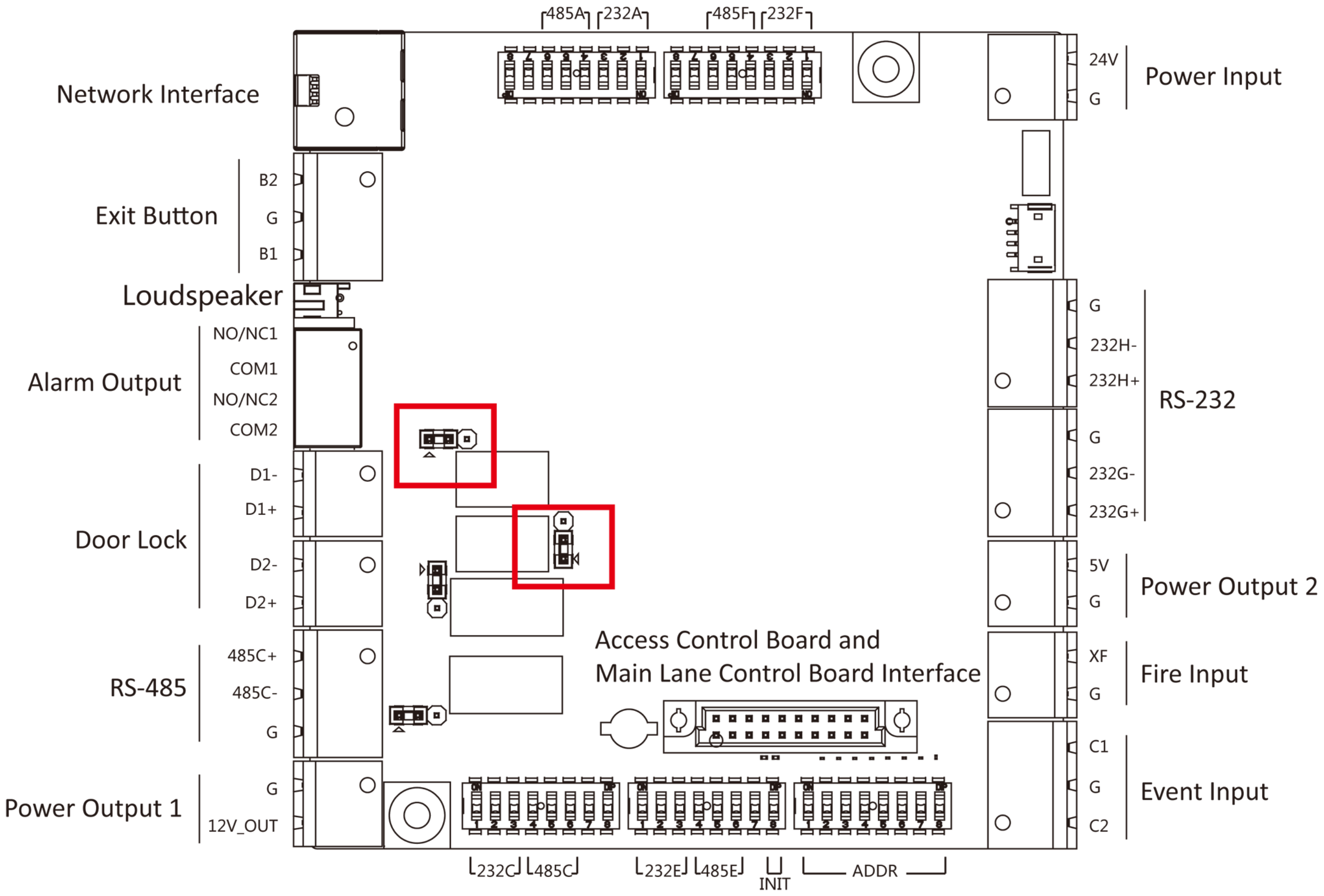


Figure 5-5 Jumper Cap Location (Alarm Relay Output Mode)

The jumper cap position of alarm opening (NO) is as below:

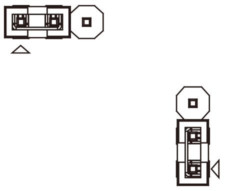


Figure 5-6 Alarm Opening (NO)

The jumper cap position of alarm closing (NC) is as below:

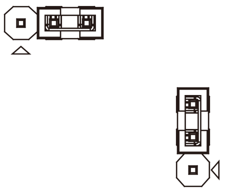


Figure 5-7 Alarm Closing (NC)

Note

The default status is NO.

Chapter 6 Activation

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

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

The default values of the device are as follows:

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

6.1 Activate via 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.

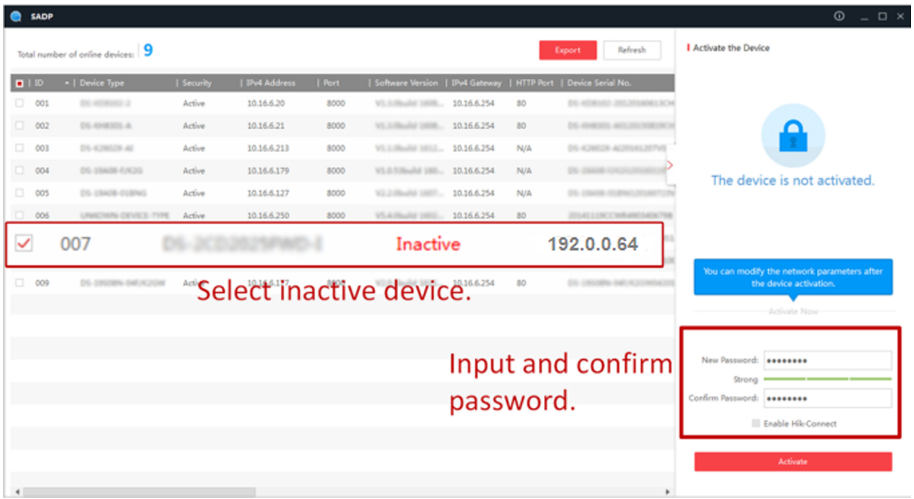
   ⚠ **Caution**

   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.

   ℹ **Note**

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

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



Total number of online devices: 9

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

Select inactive device.

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ••••••••
Strong
Confirm Password: ••••••••
☐ Enable Hik-Connect

Input and confirm password.

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

5. Modify IP address of the device.

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

6.2 Activate Device via Client Software

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

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.

2. Click ▴ on the right of **Device Management** and select **Device**.

3. Click **Online Device** to show the online device area.

The searched online devices are displayed in the list.

4. Check the device status (shown on **Security Level** column) and select an inactive device.

5. Click **Activate** to open the Activation dialog.

6. Create a password in the password field, and confirm the password.

Caution

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

three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you 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 7 Client Software Configuration

7.1 Configuration Flow of Client Software

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

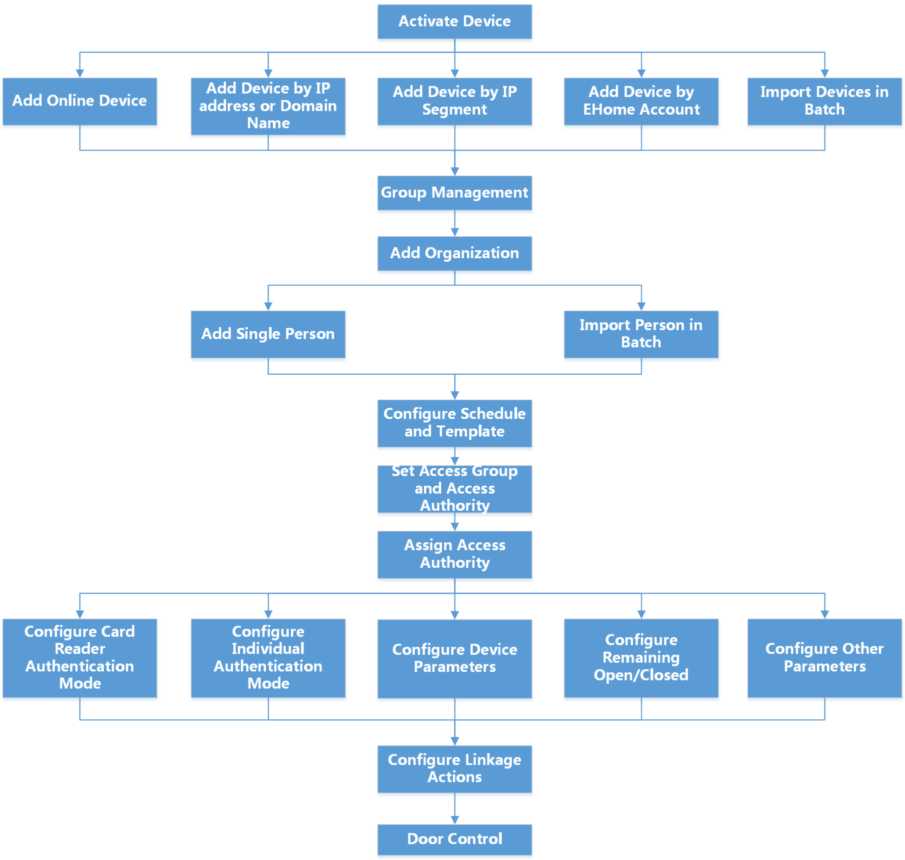

Activate Device
Add Online Device
Add Device by IP address or Domain Name
Add Device by IP Segment
Add Device by EHome Account
Import Devices in Batch
Group Management
Add Organization
Add Single Person
Import Person in Batch
Configure Schedule and Template
Set Access Group and Access Authority
Assign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

Figure 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***.

   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	Click ⚙ to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click ▤ to view device status, including door No., door status, etc. ℹ **Note** For different devices, you will view different information about device status.
View Online User	Click 👤 to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click ⟳ to refresh and get the latest device information.

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 surbodinate organization for the added one.

Steps

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

Note

Up to 10 levels of organizations can be added.

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

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

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

Note

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

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

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.

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** to open the Export panel.
4. Check **Person Information** as the content to export.
5. Check desired items to export.
6. 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.

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** to open the Export panel and check **Face** as the content to export.

4. Click **Export** to start exporting.

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

Steps

Note

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

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

Note

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

5. 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, 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.

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, face picture, linkage between card number and linkage between card number and card password, card effective period, etc).

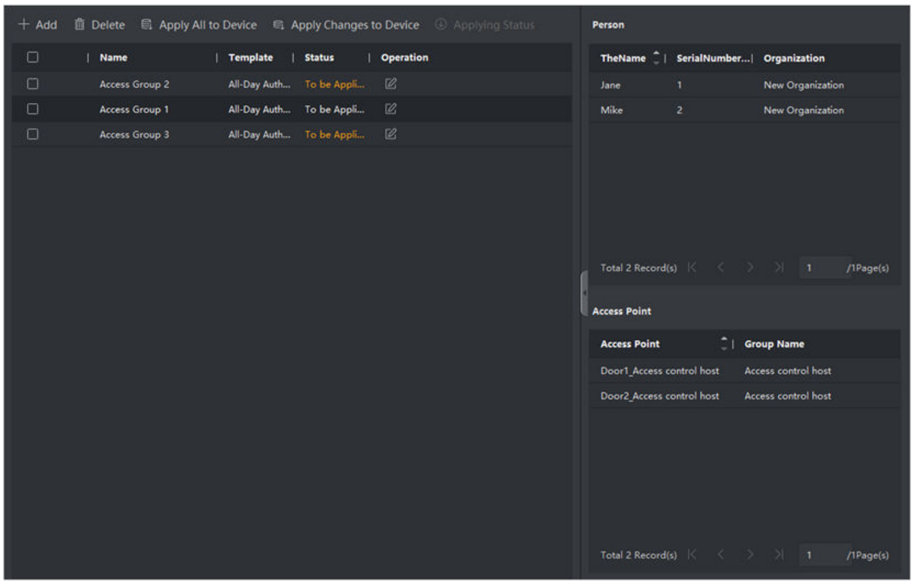
1. Click **Access Control → Authorization → Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

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.



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

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

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

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

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

Figure 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.

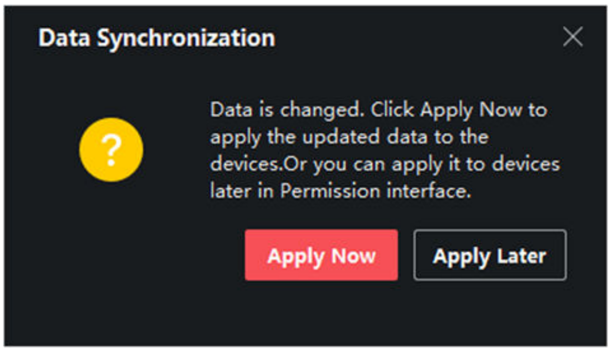
The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s).

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 promptAccess Group to Be Applied on the right corner of the client.

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



Data Synchronization

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

Figure 7-4 Data Synchronization

7.7 Configure Advanced Functions

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

Note

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

7.7.1 Configure Device Parameters

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

Configure Parameters for Access Control Device

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

Steps

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

Note

If you can 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.

RS-485 Communication Redundancy

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

Enable NFC

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

Enable M1 Card

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

Enable EM Card

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

Enable CPU Card

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

Enable ID Card

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

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

Configure Parameters for Door

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

Steps

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

Note

s
The displayed parameters may vary for different access control devices.

Name

Edit the card reader name as desired.

Exit Button Type

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

Open Duration

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

Door Left Open Timeout Alarm

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

Super Password

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

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

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.

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.

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

Note

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

Configure Parameters for Card Reader

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

Steps

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

   Note

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

   Name

   Edit the card reader name as desired.

   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.

   Alarm of Max. Failed Attempts

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

   Card Reader Type/Card Reader Description

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

4. **Optional:** Some of the following parameters are not listed in the Basic Information page, click **Advanced** to edit the parameters.

   Enable Card Reader

   If enabling the function, user can present card on the card reader. If disabling the function, the card reader for entrance cannot be used.

   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.

   Buzzing Time

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

   Max. Interval When Entering PWD

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

   Tampering Detection

   Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

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

Fingerprint Recognition Level

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

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

Configure Parameters for Alarm Output

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

Before You Start

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

Steps

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

   Name

   Edit the card reader name as desired.

   Alarm Output Active Time

   How long the alarm output will last after triggered.

4. Click **OK**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Parameters for Lane Controller

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

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 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 Door's Schedule Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

Enable 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.

Alarm Voice Prompt Time Duration

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

Note

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

Temperature Unit

Select the temperature unit that displayed in the device status.

Motor Rotation Direction

Set the motor rotation as **Clockwise** or **Anticlockwise**. The motor rotation direction is the barrier's open direction.

Note

- For single pedestal scenario, the motor rotation direction should set as **Clockwise**.
- For multiple pedestals scenario, standing at the entrance, the motor rotation direction from right to left should set as: **Clockwise**, **Anticlockwise**, **Clockwise**, etc. respectively.

Lightboard Brightness

Set the lightboard brightness.

Barrier Material

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

Note

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

Lane Length

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

Note

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

Do Not Open Barrier in Authenticates in Lane

If there is someone or something in the lane, the gate will not open even if the credential is authenticated.

This function is designed to avoid more than one person passing through the gate with only one authentication.

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.

4. Click **OK**.

7.7.2 Configure Device Parameters

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

Set RS-485 Parameters

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

Steps

Note

The RS-485 Settings 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 **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 serial number, external device, authentication center, baud rate, data bit, stop bit, parity type, flow control type, communication mode, and working mode in the drop-down list.
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.

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 Verification** to enter the M1 Card Encryption Verification page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

   Note

   - The sector ID ranges from 1 to 100.
   - By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.
6. Click **Save** to save the settings.

7.8 Door Control

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

Note

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

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 *Set File Saving Path* in the user manual of the client software.

Result

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

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.

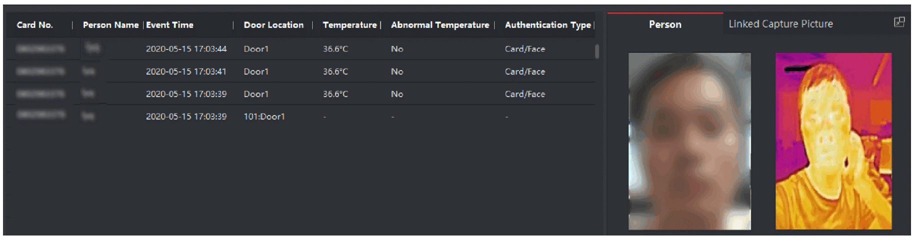
Before You Start

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
[redacted]	[redacted]	2020-05-15 17:03:44	Door1	36.6°C	No	Card/Face
[redacted]	[redacted]	2020-05-15 17:03:41	Door1	36.6°C	No	Card/Face
[redacted]	[redacted]	2020-05-15 17:03:39	Door1	36.6°C	No	Card/Face
[redacted]	[redacted]	2020-05-15 17:03:39	101:Door1	-	-	-

Figure 7-5 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 details (including person's detailed information and the captured picture).

   Note

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

7.9 Remote Configuration via Client Software

Configure device parameters remotely.

7.9.1 Check Device Information

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → Device Information** and view the device basic information and the device version information.

7.9.2 Edit Device Name

Click **Maintenance and Management → Device** to enter the device list.

Click ⚙ to enter the remote configuration page.

Click **System → General** to configure the device name.

Click **Save**.

7.9.3 Edit Time

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → Time** to configure the time zone.
4. **Optional:** Check **Enable NTP** and set the NTP server address, the NTP port, and the synchronization interval.
5. **Optional:** Check **Enable DST** and set the DST start time, end time and the bias.
6. Click **Save**.

7.9.4 Set System Maintenance

You can reboot the device remotely, restore the device to default settings, etc.

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → System Maintenance** .
4. Maintain the device.

   Reboot

   The device starts rebooting.

   Restore Default Settings

   Restore the device settings to the default ones, excluding the IP address.

   Restore All

   Restore the device parameters to the default ones. The device should be activated after restoring.
5. Remotely upgrade the device.
   1) In the Remote Upgrade part, select an upgrade type.

      Note

      - You need to set the device ID before upgrading if you select Controller Upgrade File as the remote upgrade type.
      - Only the card reader that connected via RS-485 protocol supports upgrading.
   2) Click **...** to select an upgrade file.
   3) Click **Upgrade** to start upgrading.

      Note

      Do not power off during the upgrading.

7.9.5 Manage Network User

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → User → Network User** .
4. Click **Add** to add the user.
5. **Optional:** Select a user in the user list and click **Edit** to edit the user.

   You are able to edit the user password, the IP address, the MAC address and the user permission.
6. Click **OK**.

7.9.6 Manage Keyfob User

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → User → Keyfob User** .
4. Click **Add** to add the user.
5. Check **Enable** in the pop-up window and set the keyfob's serial No.
6. **Optional:** Enable the Remain Open Status of the turnstile.

   Note

   If enabling this function, after the keyfob is matching completed, you can set the barrier as remaining open by using the keyfob.
7. Set the door open direction
8. Click **OK**.

   Note

   Up to 32 keyfob users can be added.

7.9.7 Set Security

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → Security** .
4. Select the density level in the drop-down list.
5. You can select **Compatible Mode** or **Security Mode**.

   Compatible Mode

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

Security Mode

High security level during the user information verification when logging in.

6. Click **Save**.

7.9.8 Configure Lane Parameters

You can set the passing parameters for a person to pass through the turnstile.

Steps

1. Click **Maintenance and Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → Lane Settings** .
4. Set the lane parameters.

Door Closing Delay Time

Set the delayed time duration when barrier is closing. The barrier will be closed after the configured delayed time.

Max. Intrusion Duration

If a person has entered the lane or passed through the lane for more than the configured time duration, an alarm will be triggered. 0 represents the function is disabled.

Note

The suggested minimum detection time duration is 2 s.

Overstaying Duration

If the device detects persons or things staying in the lane for more than the configured time duration, an alarm will be triggered.

Max IR Obstructed Duration

Set the maximum time duration for the obstruction of the IR light. If the IR light is obstructed for more than the configured time duration, the alarm will be triggered. 0 represents the function is disabled.

5. Click **Save**.

7.9.9 Configure Screen Parameters (Reserved)

You can set the display parameters.

Steps

Note

The function should be supported by the device.

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → Screen Configuration** .
4. Set the screen parameters.

   Note

   For better performance, it is suggested to use the default parameters.

   Screen Position

   Select the screen's position on the device. If select **Exit** from the drop-down list, the screen will be installed at the exit position of the device.

   Screen Model

   Select the screen model from the drop-down list.

   Font Size

   Select the text font size in the screen.

   Screen Orientation

   Select the text orientation on the screen.

   Line Space

   Set the space between two lines.

   Column Spacing

   Set the space between two columns.

   Initial Position

   Set the first character's position displayed on the screen.
5. Click **Save**.

7.9.10 Configure Screen Parameters

You can set the people counting's parameters and after the configuration.

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → People Counting** .
4. Set the people counting parameters.

   Clear Device People Counting

Click **Reset** and the counted people number will be restored to zero.

Device People Counting

Click **Enable** or **Disable** to enable or disable the people counting function.

Client Offline People Counting

Click **Enable** or **Disable** to enable or disable function of the offline people counting on the client.

If enabling the function and if the device is offline, the device will continue counting the people and the number will be stored in the device. When the device is online, the client will read the updated number from the device automatically.

People Counting Type

You can select from **Invalid**, **By Detection**, and **By Authentication Number**.

Invalid

The device will not count people. If the device people counting function is enabled, the people counting function is still disabled.

By Detection

The device will count the people who passing through the device depending on the detection result.

By Authentication Number

The device will count the people who authenticating on the device.

The failed authentication will also count as once.

5. Click **Save**.

7.9.11 Configure Advanced Network

Click **Maintenance and Management → Device Management → Device** to enter the device list.

Click ⚙ to enter the remote configuration page.

Click **Network → Advanced Settings** and you can configure the DNS1 IP address and the DNS2 IP address.

Click **Save** to save the settings.

7.9.12 Configure Audio File

You can relate the audio file to the corresponding playing scene. You can also export the audio file from the system and import the audio file from the local.

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **Other → Audio File** .

Note

By default, the system contains the audio content. For details about the index related audio content, see ***Table of Audio Index Related Content*** .

4. Select the index (the playing content) corresponded play scene.
5. **Optional:** Input the descriptions of the play scene.
6. Click **Save Parameters** to save the relationship between the index (the playing content) and the play scene.
7. **Optional:** Click **Export** to export the default audio file to the local computer.
8. **Optional:** Click **...** and select audio file from the local computer. Click **Import** to import the file to the device.

Note

- The imported audio file should be in MEM format.
- For details about converting other format of the audio file to MEM format, see the audio conversion manual.
- If you use the third part software to create or edit an audio file, the volume of the audio file should be no less than 0 × 68. If the volume is less than the value, it will exceed the loudspeaker's power consumption, so that damage the loudspeaker.

7.9.13 View Relay Status

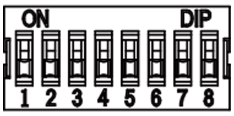
Click **Maintenance and Management → Device Management → Device** to enter the device list.

Click ⚙ to enter the remote configuration page.

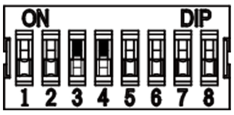
Click **Status → Relay** and you can view the relay status.

Appendix A. DIP Switch Description

The DIP switch is on the main lane control board. The left side to the right side is from the low bit to the high bit.



When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off. If you set the DIP switch like the figure displayed below, its binary value is 00001100, and its decimal value is 12.



Appendix B. 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
Barrier Obstructed	None

Appendix C. Table of Audio Index Related Content

Index	Content
1	Authenticated.
2	Card No. does not exist.
3	Card No. and fingerprint mismatch.
4	Climbing over the barrier.
5	Reverse passing.
6	Passing timeout.
7	Intrusion.
8	Force accessing.
9	Tailgating.
10	No permissions.
11	Authentication time out.
12	Authentication failed.
13	Expired card.
14	Stay out of time.

Appendix D. 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
Normal Working	00	Lower Fifth IR Beam Triggered	17
Upper First IR Beam Triggered	01	Lower Sixth IR Beam Triggered	18
Upper Second IR Beam Triggered	02	Lower Seventh IR Beam Triggered	19
Upper Third IR Beam Triggered	03	Lower Eighth IR Beam Triggered	20
Upper Fourth IR Beam Triggered	04	Lower Ninth IR Beam Triggered	21
Upper Fifth IR Beam Triggered	05	Lower Tenth IR Beam Triggered	22
Upper Sixth IR Beam Triggered	06	Lower Eleventh IR Beam Triggered	23
Upper Seventh IR Beam Triggered	07	Lower Twelfth IR Beam Triggered	24
Upper Eighth IR Beam Triggered	08	Light Board Offline (Entrance)	49
Upper Ninth IR Beam Triggered	09	Light Board Offline (Exit)	50
Upper Tenth IR Beam Triggered	10	IR Adapter Offline (Up)	51
Upper Eleventh IR Beam Triggered	11	IR Adapter Offline (Low)	52
Upper Twelfth IR Beam Triggered	12	CAN Bus Exception	53
Lower First IR Beam Triggered	13	Not Studying	54
Lower Second IR Beam Triggered	14	Obstruction	55
Lower Third IR Beam Triggered	15	Exceeding Studying Range	56
Lower Fourth IR Beam Triggered	16	Motor Exception	57

Appendix E. 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 E-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 E-2 Device Command

See Far, Go Further