DS-K3G501S Series Tripod Turnstile

Quick Start Guide

Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

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

Trademarks

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

Disclaimer

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

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

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
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

CE

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

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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.)
- Operation of this equipment in a residential environment could cause radio interference.
- The device do not support the PoE network switch. Connecting with the PoE network switch may damage the control board.

⚠ 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.
- The main element of the turnstile is stainless steel, which is rustless (antioxidant) and corrosion resistant (The anti corrosion ability in the medium of acid, alkali, and salt). In order to keep the stainless steel from being oxidized or corroded, you should clean and care the turnstile surface periodically.
  The instructions and tips for maintaining the turnstile are as follows:
  - Select different stainless steel types according to the variety of the environments. You can select 304 stainless steel for common circumstances and 316 stainless steel for the scenarios of seasides and chemical plants.
  - Keep the device surface clean and dry.
  - Use non-woven cloth and ethyl alcohol to clean the dirt on the device surface.
  - Use sourcing pad (do not use mesh cleaning ball) to clean the rust on the device surface by following the wire drawing on the stainless steel. And then use non-woven cloth and stainless steel cleaner to wipe the device surface.
  - Clean and maintain the device by using non-woven cloth and stainless steel cleaner periodically. It is suggest to clean the device every month in common circumstances and every week for severe environments (seaside and chemical plants for instance.

- 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
Tripod Turnstile	DS-K3G501SX

Scan the QR code to get User Manual of Tripod Turnstile. Note that mobile data charges may apply if Wi-Fi is unavailable.



Figure 1-1 QR Code

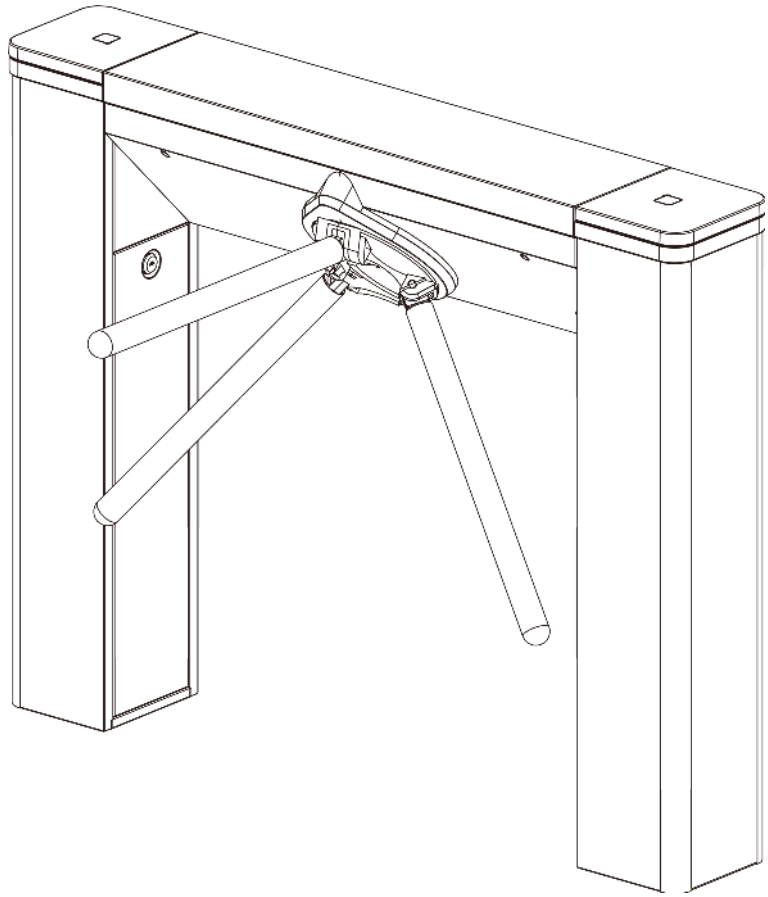
Contents

Chapter 1 Overview 1
1.1 Introduction 1
1.2 Main Features 1
Chapter 2 System Wiring 3
Chapter 3 Installation 5
3.1 Disassemble Pedestals 5
3.2 Install Pedestals 5
Chapter 4 General Wiring 9
4.1 Components Introduction 9
4.2 Wiring Electric Supply 9
4.3 Terminal Description 10
4.3.1 Access Control Board Terminal and BUS Description 10
4.3.2 Access Control Board Serial Port ID Description 15
4.3.3 RS-485 Wiring 17
4.3.4 RS-232 Wiring 18
4.3.5 Wiegand Wiring 19
4.3.6 Barrier Control Wiring 19
4.3.7 Alarm Output Wiring 21
4.3.8 Exit Button Wiring 22
Chapter 5 Device Settings 23
5.1 Pair Keyfob (Optional) 23
5.2 Initialize Device 24
5.3 Switch to RS-485/RS-232 Mode 25
5.4 Alarm Relay Output Mode (NO/NC) 26
Chapter 6 Activation 27
6.1 Activate via SADP 27

6.2 Activate Device via iVMS-4200 Client Software 28
Appendix A. Tips for Scanning Fingerprint 30
Appendix B. DIP Switch 32
B.1 DIP Switch Description 32
B.2 DIP Switch Corresponded Functions 32
Appendix C. Event and Alarm Type 34
Appendix D. Table of Audio Index Related Content 35
Appendix E. Communication Matrix and Device Command 36

Chapter 1 Overview

1.1 Introduction



The tripod turnstile is designed to detect unauthorized entrance or exit. By adopting the turnstile 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
  The communication data is specially encrypted to relieve the concern of privacy leak
- Remaining open/closed mode selectable
- Bidirectional (Entering/Exiting) lane
  The barrier opening and closing speed can be configured according to the visitor flow

- Self-detection, Self-diagnostics, and automatic alarm
- Remote control and management
- Online/offline operation
- LED indicates the entrance/exit and passing status
- Barrier is in free status when powered down. People can pass through the lane along single/both singe and double directions
- Fire alarm passing
  When the fire alarm is triggered, the barrier will be dropped down 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
- Up to 3000 visitor cards and up to 60,000 cards except for visitor cards can be added
- Up to 180,000 presenting card events can be recorded
- Adjustable strip light brightness

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 782 mm. L represents the lane width.

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

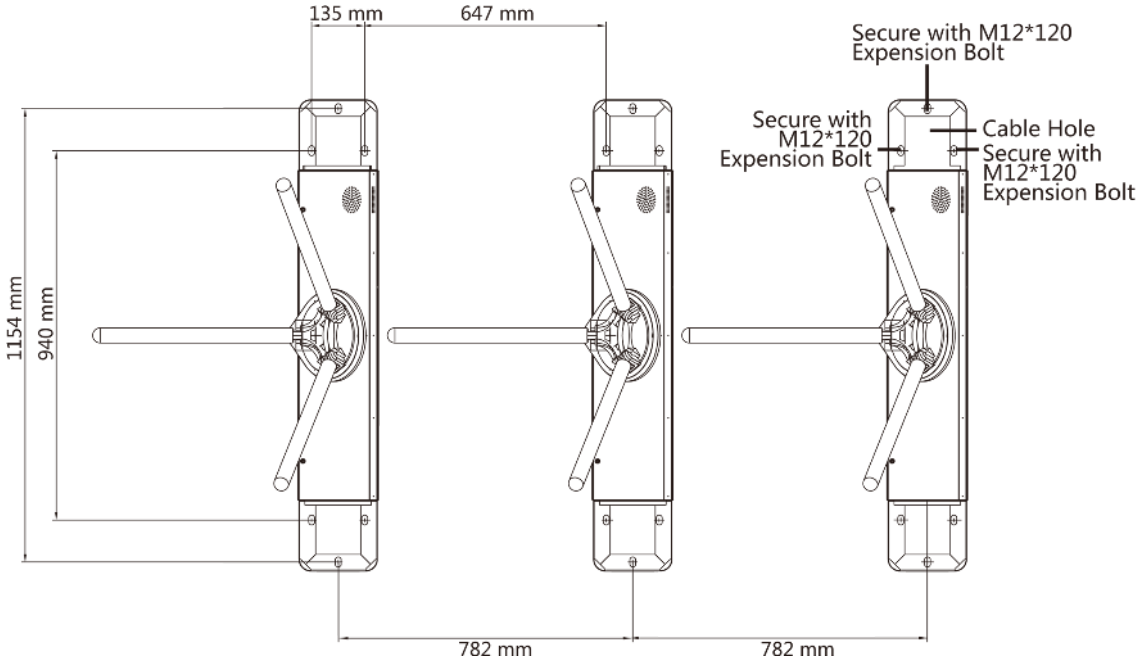


Figure 2-1 Hole Position Diagram

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

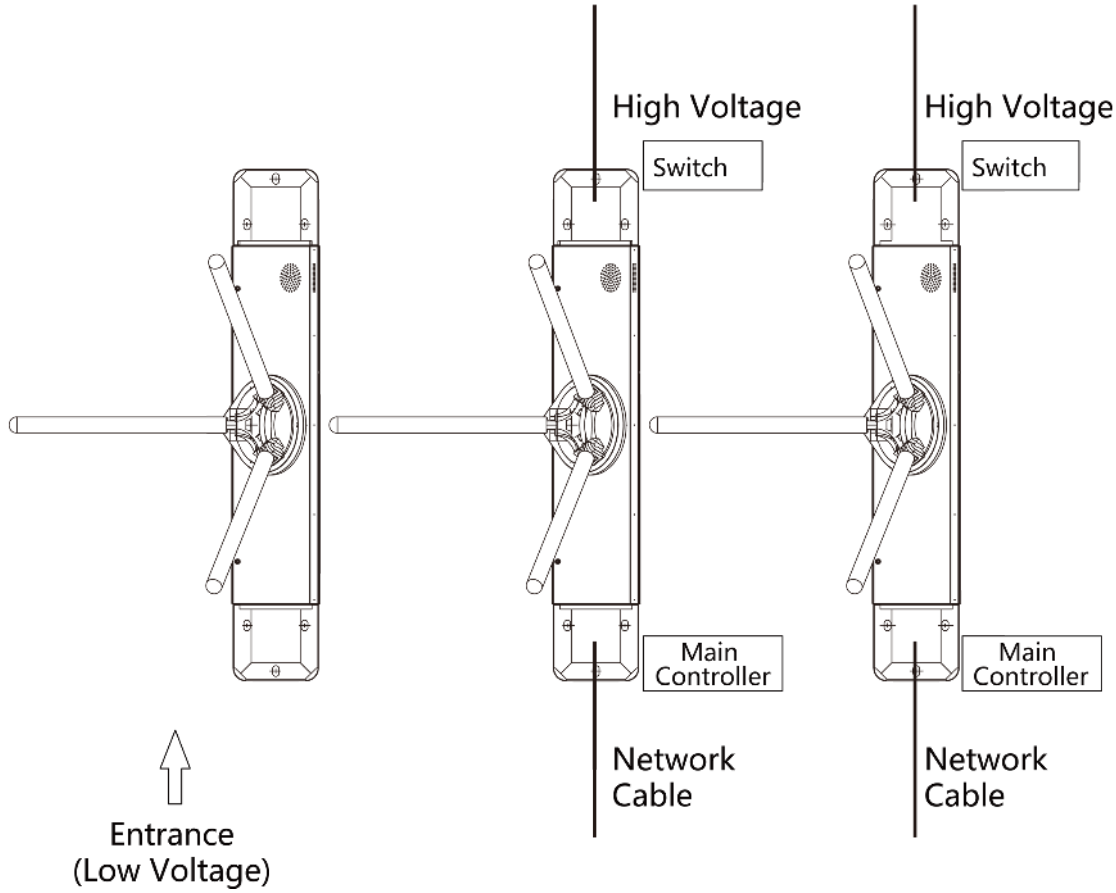


Figure 2-2 System Wiring Diagram

Note

- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- If the face recognition module are required to be connected on the left lane, you should increase the conduit diameter or bury another conduit for the external cables.
- You should bury one network cable and one high voltage conduit for the right and middle lane.
- 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.

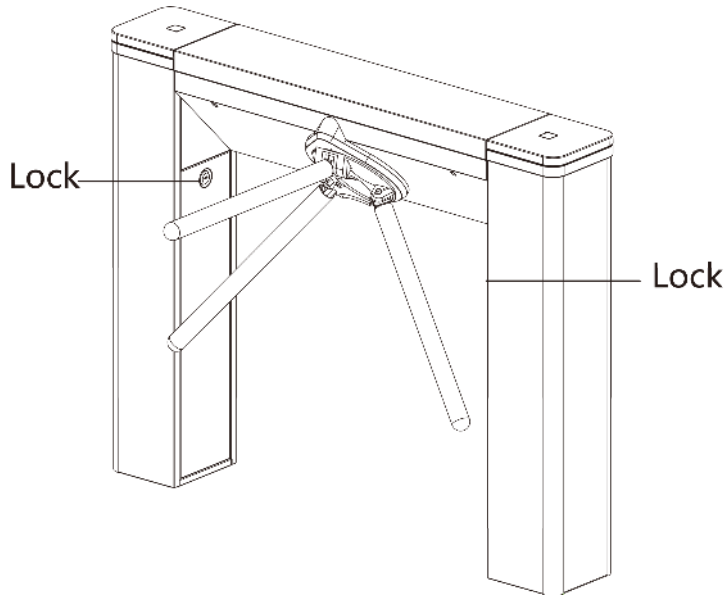


Figure 3-1 Lock Holes

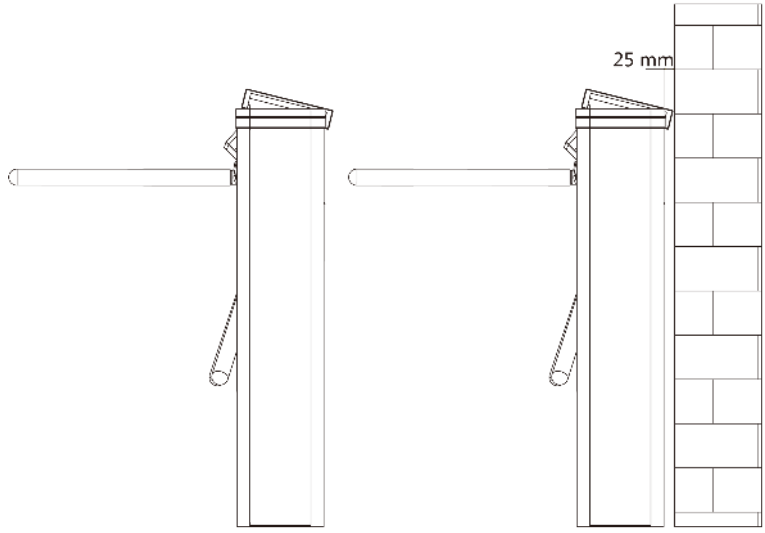
3.2 Install Pedestals

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

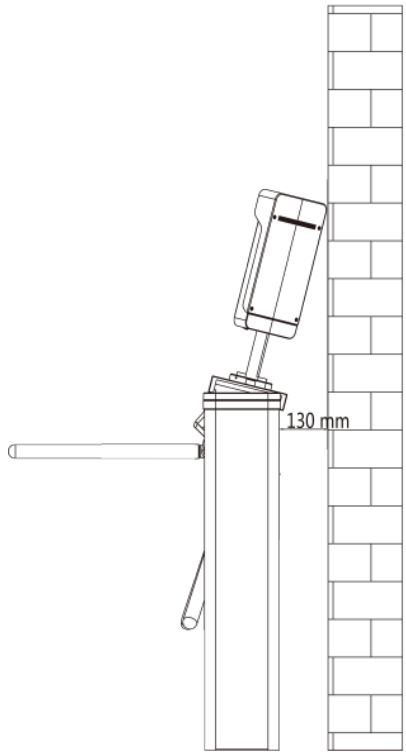
Steps

Note

- The device should be installed on the concrete surface or other non-flammable surfaces.
- No face recognition terminal installed: If the installation area is too close to the wall, make sure the distance between the pedestal and the wall should be more than 25 mm, or the surface may be scratched.



Face recognition terminal installed: If the installation area is too close to the wall, make sure the distance between the pedestal and the wall should be more than 130 mm, or the surface may be scratched.



- The dimension is as follows.

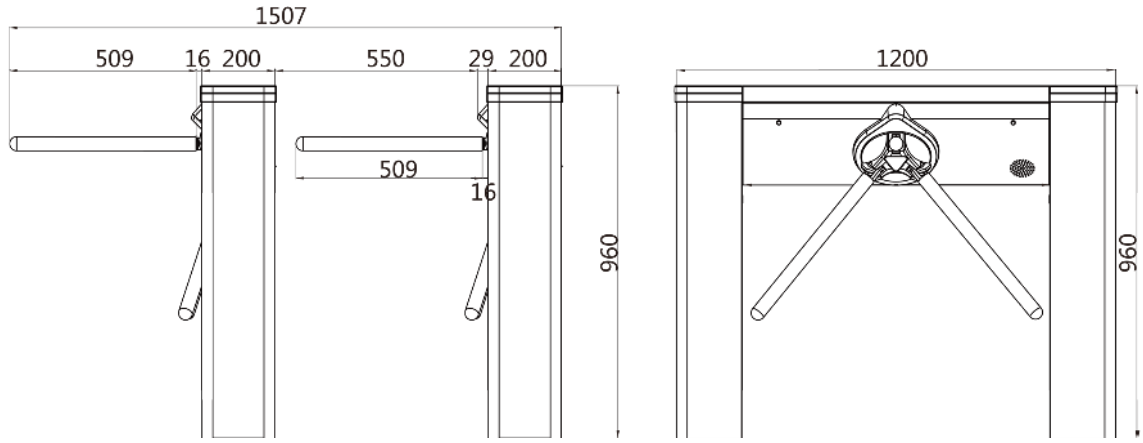


Figure 3-2 Dimension

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. Seal the bottom of the turnstile to avoid water from entering.

Note

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

5. Secure the pedestals with expansion bolts.

Note

- Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 690 mm.
- The installation footprint is as follows:

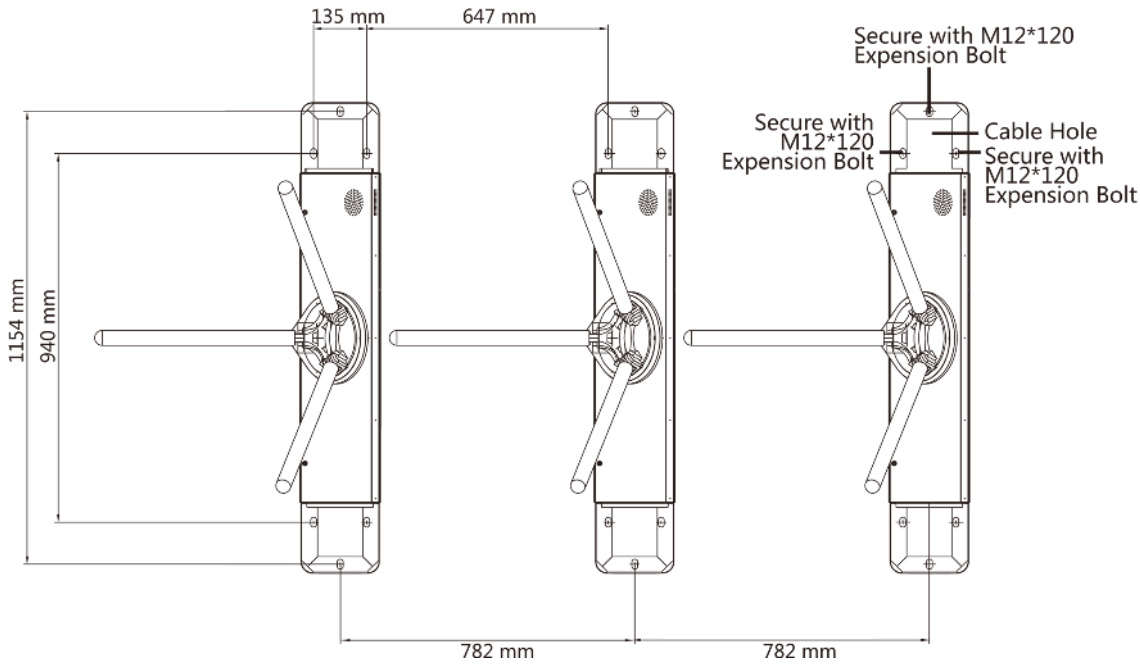


Figure 3-3 Installation Footprint

Chapter 4 General Wiring

4.1 Components Introduction

By default, basic components of the turnstile are connected well. 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 220 VAC, 50 to 60 Hz.

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

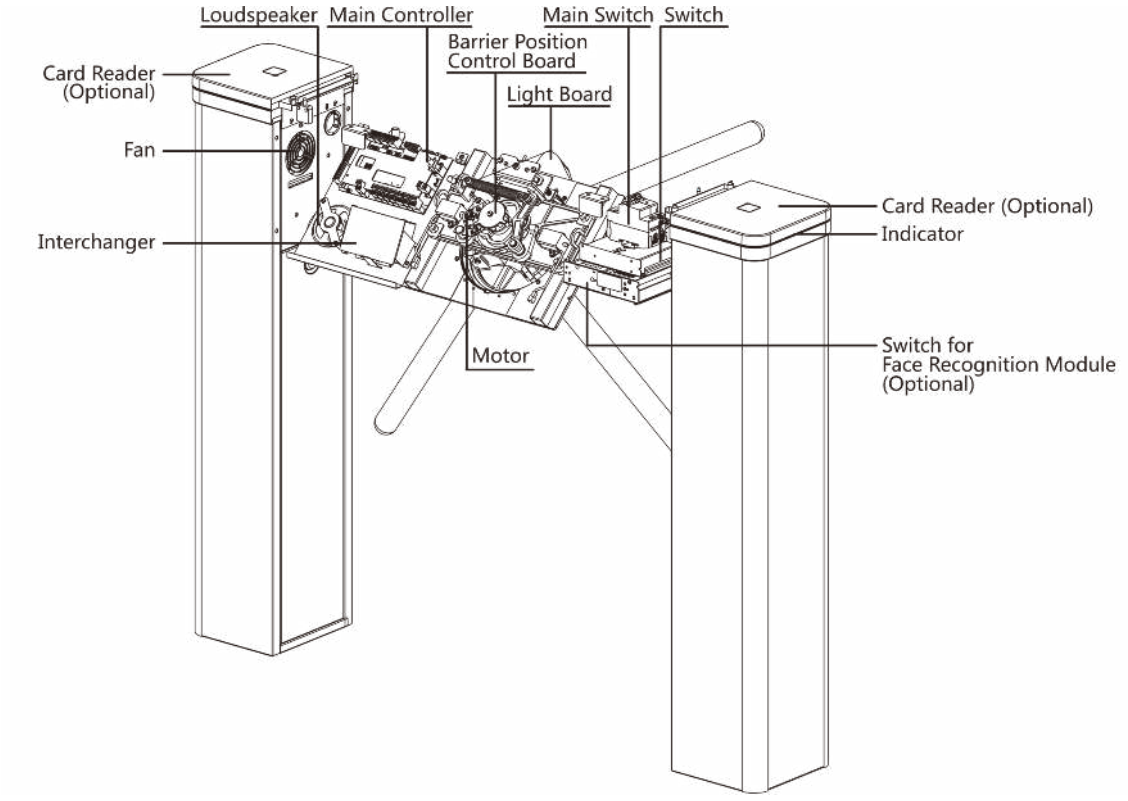
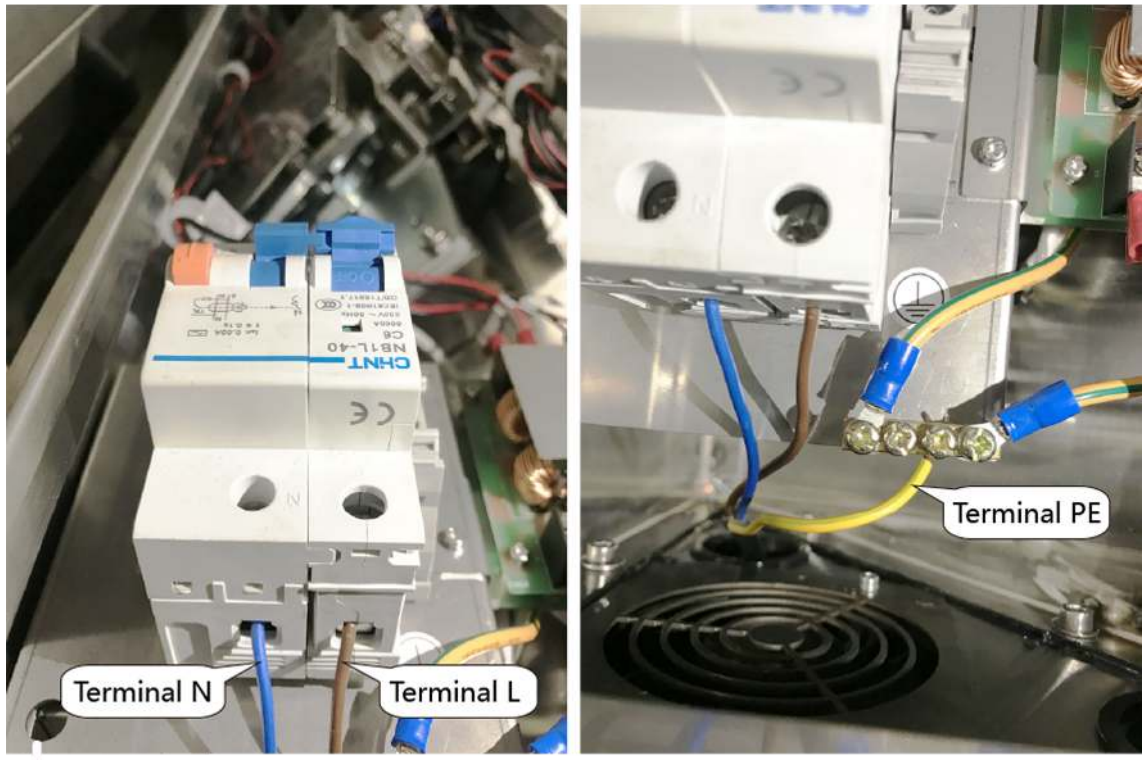


Figure 4-1 Components Diagram 1

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).



Warning

Terminal PE should connect to a ground wire to avoid hazard when people touching the device.

Note

- The cable bare part should be no more than 8 mm. 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。

4.3 Terminal Description

4.3.1 Access Control Board Terminal and BUS Description

Access Control Board Terminal Description

You can view the access control board's terminals.

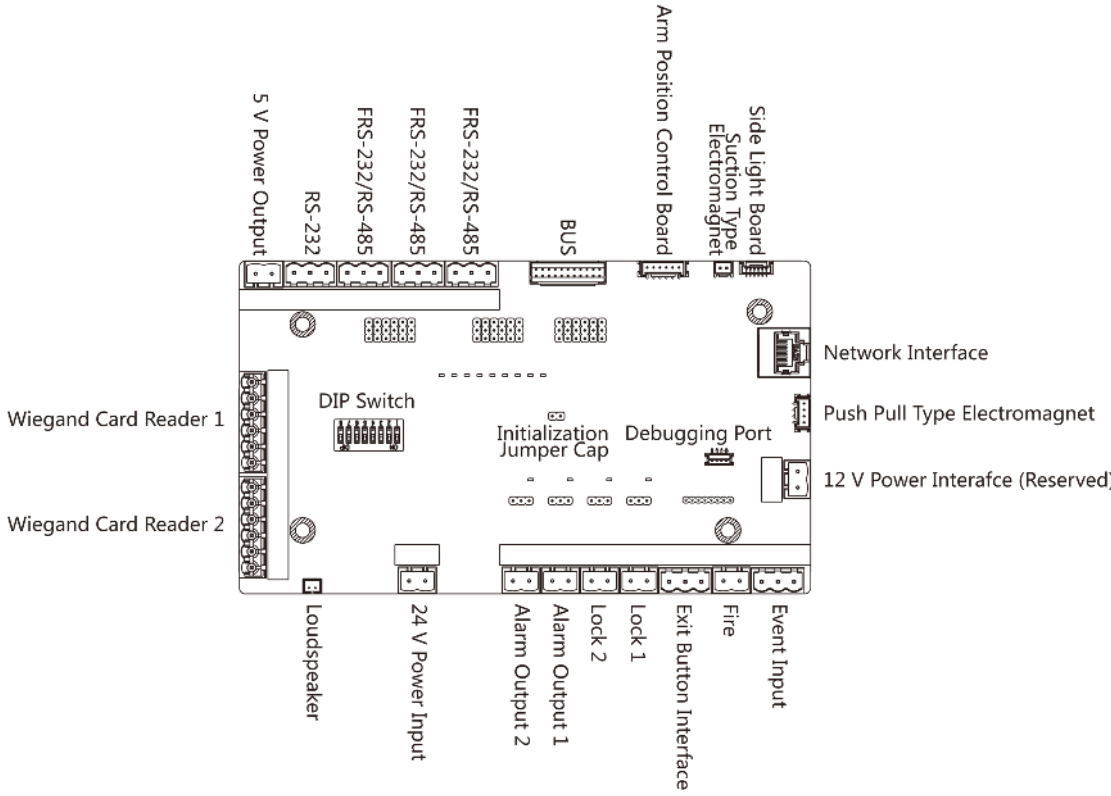


Figure 4-2 Access Control Board Diagram

Table 4-1 Table of Access Control Board Terminal Description

Access Control Board Terminal Description		
24 V Power Input	+24 V	Power Input
	GND	Grounding
Wiegand Card Reader 1	OK	Indicator of Card Reader Control Output (Invalid Card Output)
	ERR	Indicator of Card Reader Control Output (Valid Card Output)
	BZ	Card Reader Buzzer Control Output
	W1	Wiegand Head Read Data Input Data1
	W0	Wiegand Head Read Data Input Data0
	GND	Grounding

Access Control Board Terminal Description		
Wiegand Card Reader 2	OK	Indicator of Card Reader Control Output (Invalid Card Output)
	ERR	Indicator of Card Reader Control Output (Valid Card Output)
	BZ	Card Reader Buzzer Control Output
	W1	Wiegand Head Read Data Input Data1
	W0	Wiegand Head Read Data Input Data0
	GND	Grounding
RS-485 Interface (In the BUS)	GND	Grounding
	RS-485 B-	Connect to Card Reader RS485-
	RS-485 B+	Connect to Card Reader RS485+
	GND	Grounding
	RS-485 A-	Connect to Card Reader RS485-
	RS-485 A+	Connect to Card Reader RS485+
5 V Power Output	5 V	5 VDC Power Output
	GND	5 VDC Grounding
RS-232 Interface (QR Code Scanner Interface, Parts of Interfaces are in the BUS)	GND	Grounding
	RS-232 G-	Connect to Card Reader RS232-
	RS-232 G+	Connect to Card Reader RS232+
	GND	Grounding
	RS-232 H-	Connect to Card Reader RS232-
	RS-232 H+	Connect to Card Reader RS232+
Fire	XF	Connect to Fire Module
	GND	Grounding
Event Input	C1	Event Alarm Input 1
	GND	Grounding
	C2	Event Alarm Input 2
Exit Button	K2	Door 2 Signal Input
	GND	Grounding

Access Control Board Terminal Description		
	K1	Door 1 Signal Input
Door Lock	D1-	Door 1 Relay Output (Dry Contact)
	D1+	
	D2-	Door 2 Relay Output (Dry Contact)
	D2+	
Alarm Output1/ Alarm Output 2	NO/NC1	Alarm Output Relay 1 (Dry Contact)
	COM1	
	NO/NC2	Alarm Output Relay 2 (Dry Contact)
	COM2	
Network Interface	LAN	Network Accessing

Note

- The alarm input hardware interface is normally open by default. So only the normally open signal is allowed. It can be linked to the buzzer of the card reader and access controller, and the alarm relay output and open door relay output.
- The DIP of RS485 card ID is set as 1 and 4 by default. 1 is for entering, and 4 is for exiting. Set the DIP as 3 for connecting visitor card reader.
- The Wiegand card reader 1 and 2 respectively refer to the entering and exiting card reader.
- The alarm output supports relay output.
- For detailed information about the DIP switch, see *DIP Switch Description*.

BUS Description

You can use the BUS to connect card reader, fingerprint module, etc.

Table 4-2 Table of BUS Terminal Description

Terminal Group	Terminal Name	Color	Description
Fingerprint Module Terminal Group	5V	Red	5 V Power Terminal
	485/232+	Purple	Connect to Fingerprint Module RS-485+
	485/232-	Yellow	Connect to Fingerprint Module RS-485-
	GND	Black	Grounding

Terminal Group	Terminal Name	Color	Description
QR Code Scanner Terminal Group	5V	Red	5 V Power Terminal
	232+	Blue	Connect to QR Code Scanner RS-232+
	232-	Green	Connect to QR Code Scanner RS-232-
	GND	Black	Grounding
Tamper Terminal (Connected)	TAMPER	Brown	Tamper Terminal
Fan Power Terminal Group (Connected)	12_FS	Red	Connect to Fan
	GND	Black	Grounding
Card Reader Terminal Group (Entrance)	12V	Red	12 V Power Terminal
	485/232+	Yellow	Connect to Card Reader RS-485+
	485/232-	Blue	Connect to Card Reader RS-485-
	GND	Black	Grounding
Card Reader Terminal Group (Exit)	12V	Red	12 V Power Terminal
	485/232+	Yellow	Connect to Card Reader RS-485+
	485/232-	Blue	Connect to Card Reader RS-485-
	GND	Black	Grounding
Light Board Terminal Group (Connected)	12V	Red	12 V Power Terminal
	485+	Yellow	Connect to Light Board RS-485+
	485-	Blue	Connect to Light Board RS-485-
	GND	Black	Grounding

4.3.2 Access Control Board Serial Port ID Description

You can use the jumper cap on the access control board to switch the interface communication mode. For details about switching between RS-232 and RS-485 communication type, see *Switching RS-485/RS-232 Mode*.

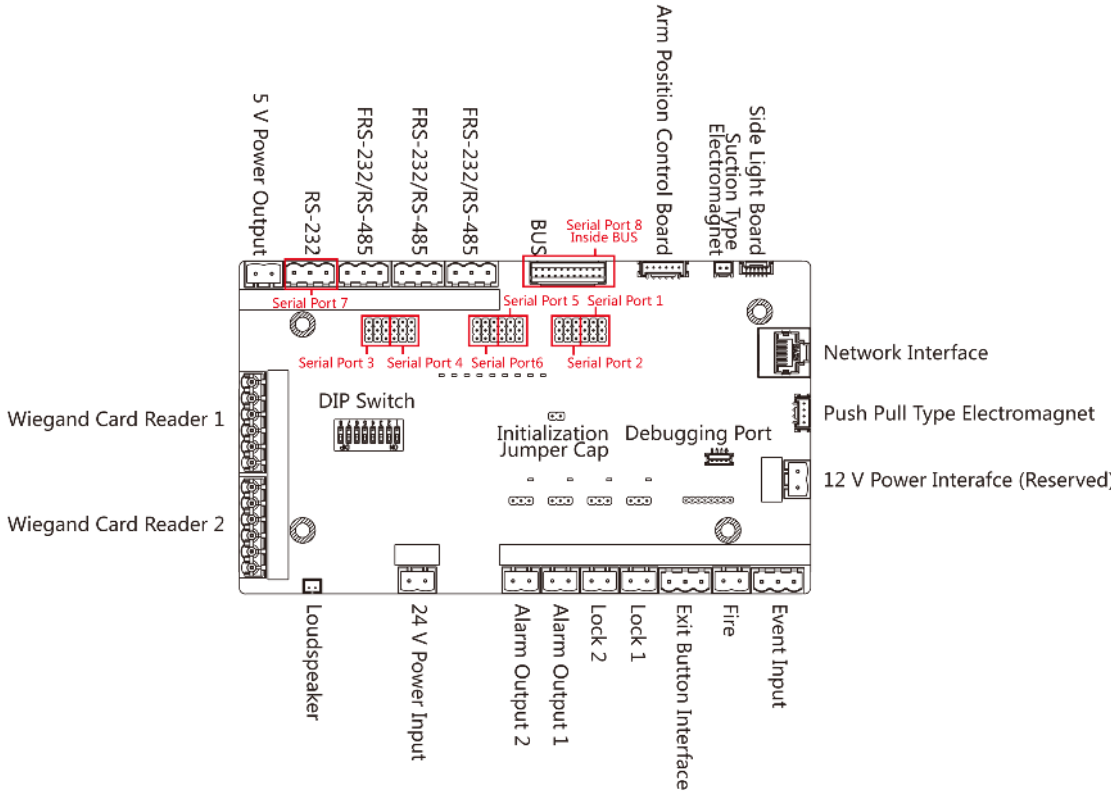


Figure 4-3 Access Control Board

According to the picture above, the serial port 1 to 6 refers to the RS-485/RS-232 interface. You can use the jumper cap to change the communication type.

The access control board descriptions are as follows:

Serial Port 1

RS-485 communication interface. You can connect RS-485 card reader and so on.

Serial Port 5 Jumper Cap

Use the jumper cap to switch the serial port communication mode. You can switch between the RS-485 communication mode and the RS-232 communication mode. By default, it is in RS-485 communication mode.

Serial Port 2

RS-232 communication interface. You can connect the fingerprint and so on.

Serial Port 3 Jumper Cap

Use the jumper cap to switch the serial port communication mode. You can switch between the RS-232 communication mode and the RS-485 communication mode. By default, it is in RS-232 communication mode. Use the serial port to connect with fingerprint module.

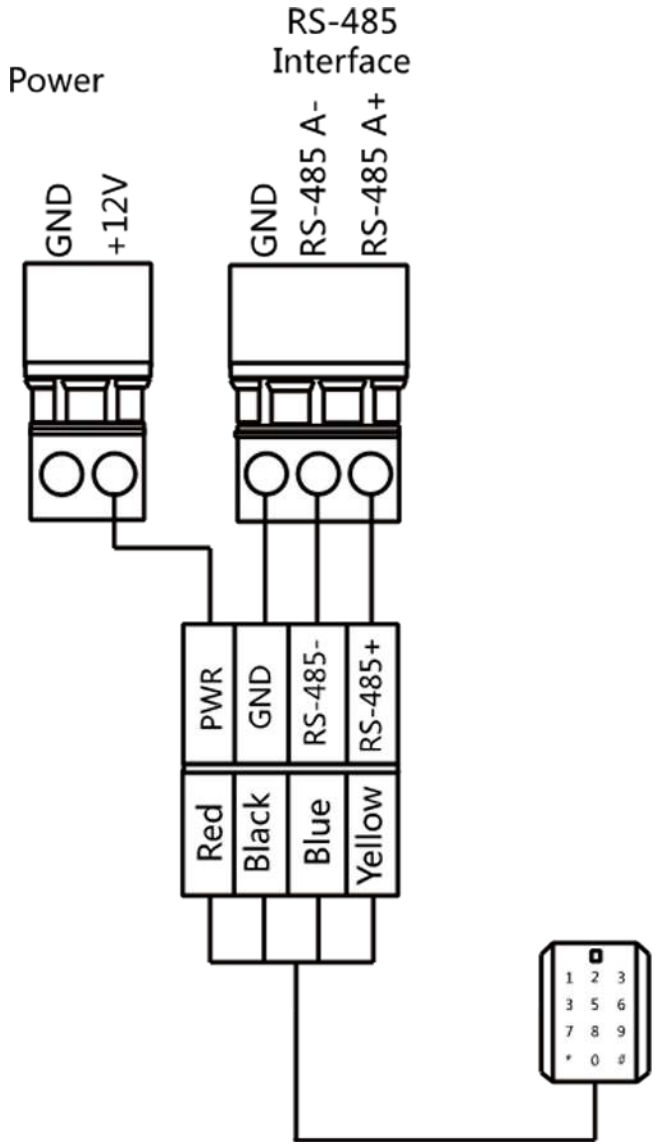
Serial Port 4/Serial Port 6 Jumper Cap

Use the jumper cap to switch the serial port communication mode. You can switch between the RS-485 communication mode and the RS-232 communication mode. By default, it is in RS-485 communication mode. Use the serial port to connect with face recognition module.

Serial Port 7/Serial Port 8

The serial port has a fixed RS-232 communication mode. It has no jumper cap and cannot change the communication mode. The RS-232 interface's QR code transmission database should no more than 64 bit.

4.3.3 RS-485 Wiring



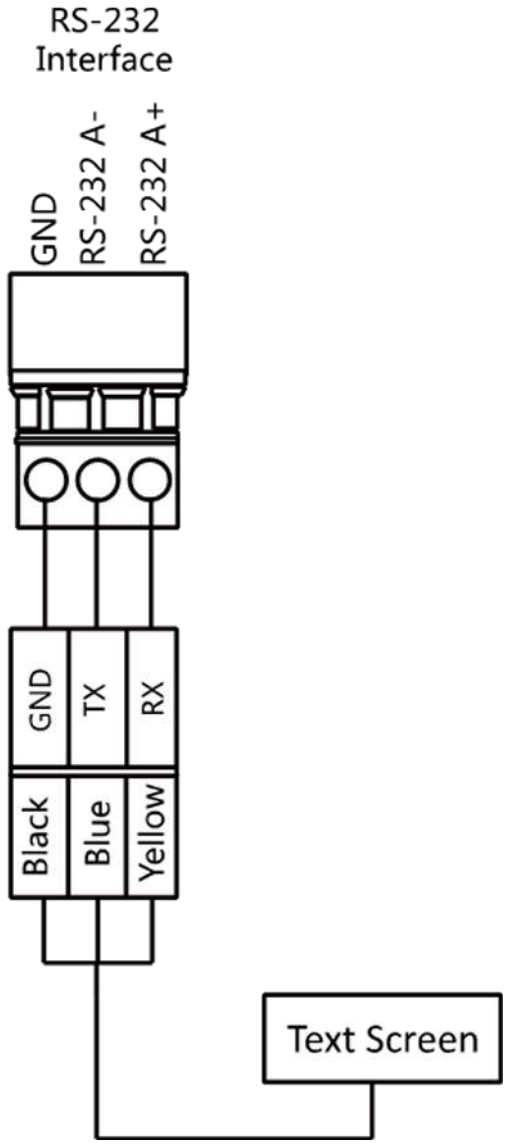
Note

- There are four RS-485 interfaces, which are for connecting ID card reader, IC card reader, QR code scanner, fingerprint and card reader, card recycler, text screen, fingerprint reader, 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*.

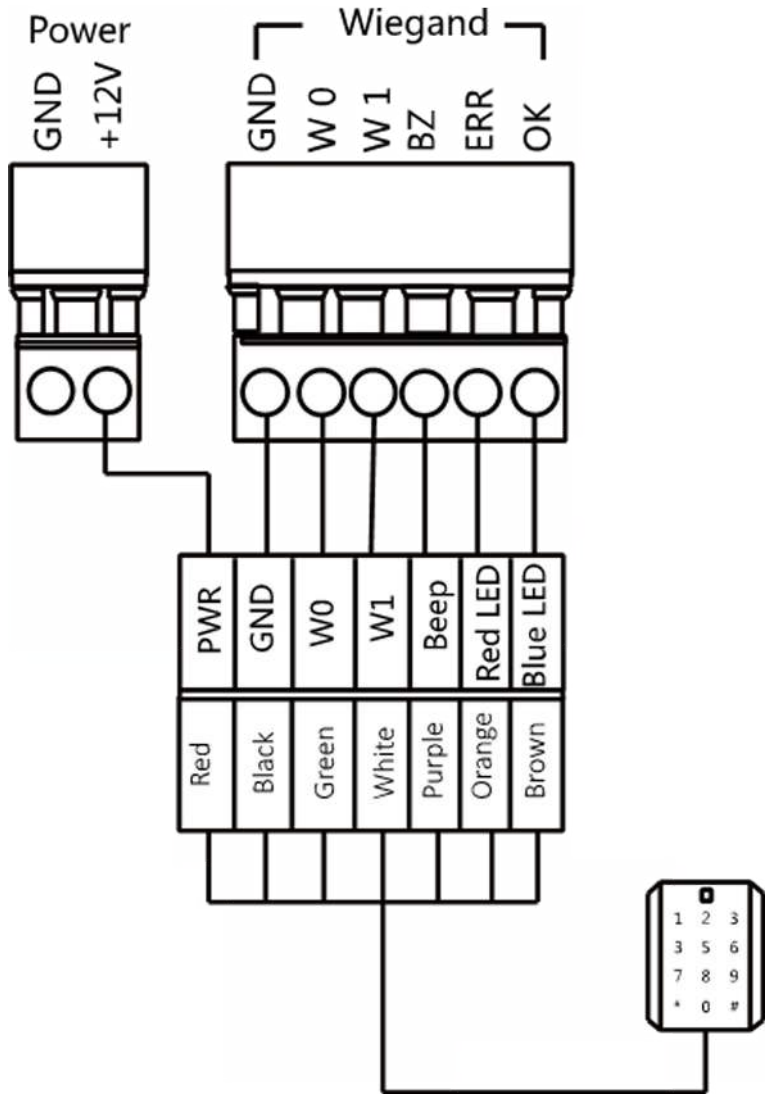
4.3.4 RS-232 Wiring

Note

- The RS-232 interfaces can connect QR code scanner, and card recycler.
- 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.



4.3.5 Wiegand Wiring



Note

Connect the OK/ERR/BZ if the access controller should control the LED and buzzer of the Wiegand card reader.

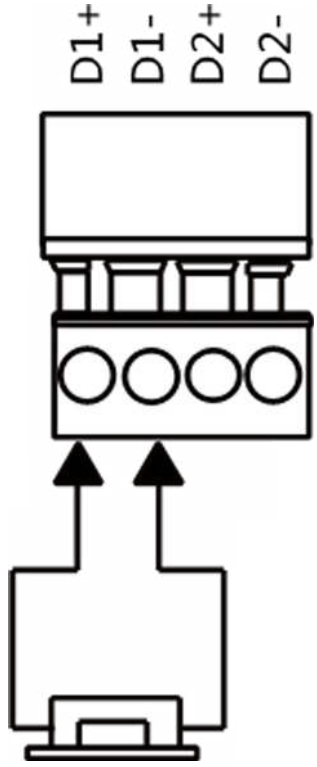
4.3.6 Barrier Control Wiring

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

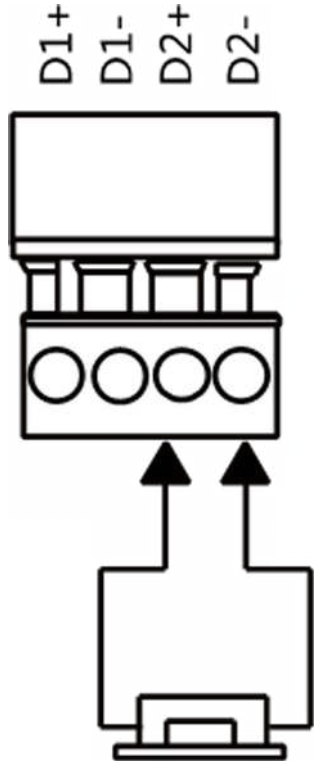
Note

The output signal is relay. The terminals cannot connect with the devices carrying voltage.

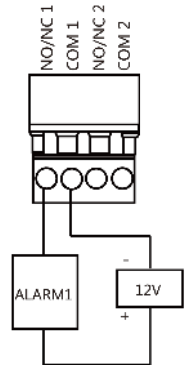
Entering Wiring



Exiting Wiring



4.3.7 Alarm Output Wiring



Note

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

4.3.8 Exit Button Wiring

You can view the exit button wiring diagram.

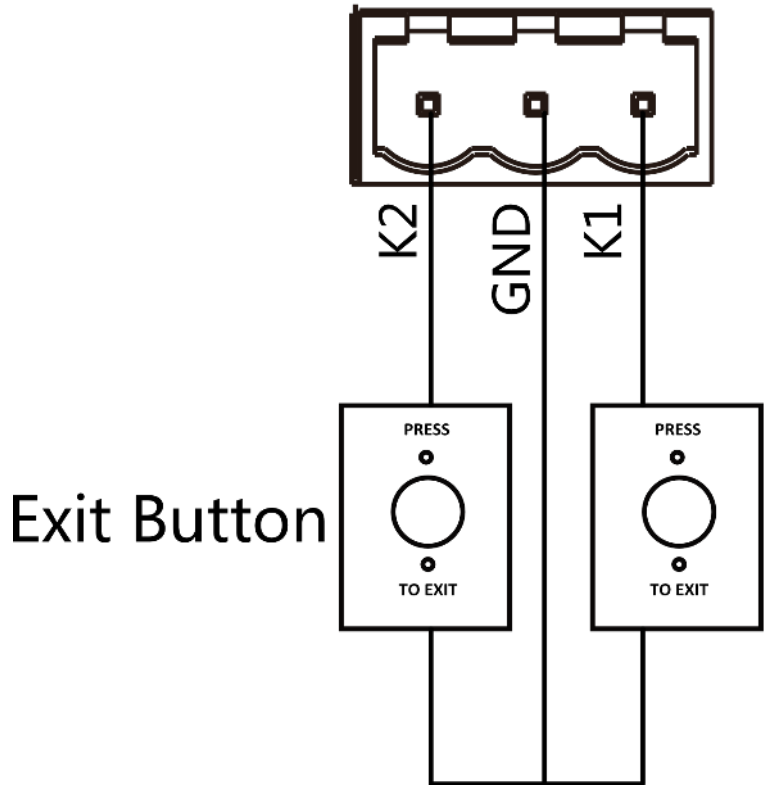


Figure 4-4 Exit Button Wiring

Chapter 5 Device Settings

You can also set the turnstile to 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.
- 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 ***DIP Switch*** .

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.

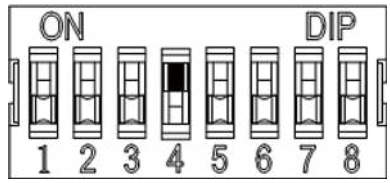
  One-to-One Mode

  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* of the user manual 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 Serial Port ID 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. Remove the jumper cap of initialization pin on the access control board.

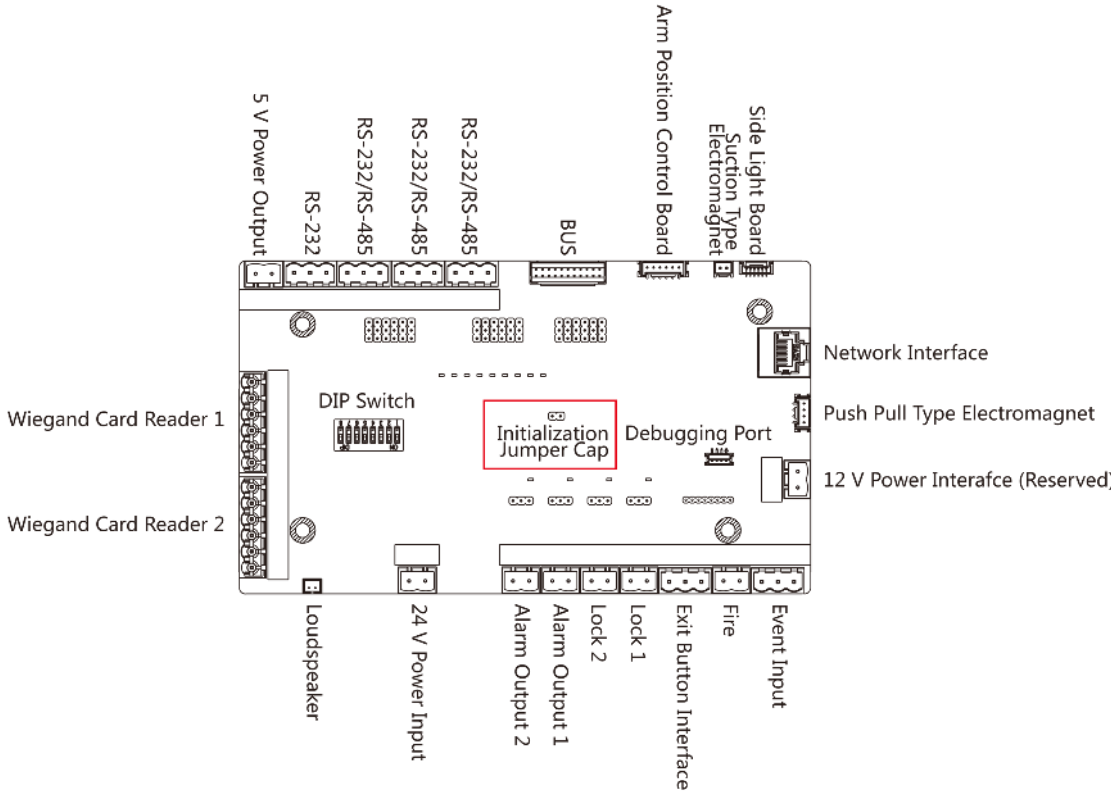


Figure 5-1 Initialization Jumper Cap

2. Disconnect the power and reboot the device. The device buzzer buzzes a long beep.
3. When the beep stopped, plug the jumper cap back.
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 to RS-485/RS-232 Mode

Take the Serial Port 4 and on the access control board as an example. If the Jumper cap's position is like the picture displayed below. (The black part is the jumper cap.) The serial port is in RS-485 communication mode.

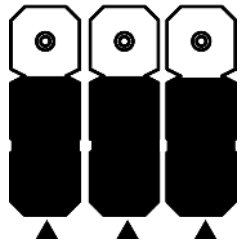


Figure 5-2 Jumper Cap Status of RS-485 Interface

If the Jumper cap's position is like the picture displayed below. (The black part is the jumper cap.) The serial port is in RS-232 communication mode.

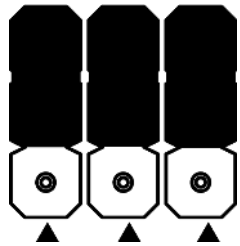


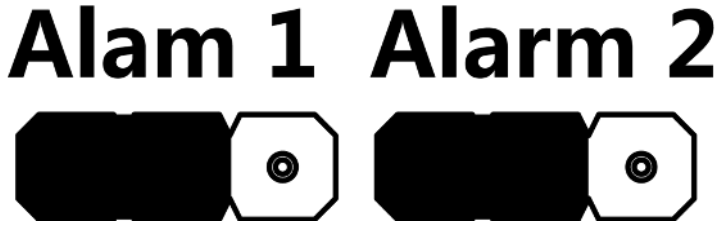
Figure 5-3 Jumper Cap Status of RS-232 Interface

5.4 Alarm Relay Output Mode (NO/NC)

Alarm Relay Output Mode (NO):



Alarm Relay Output Mode (NC):



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 (super administrator): 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.

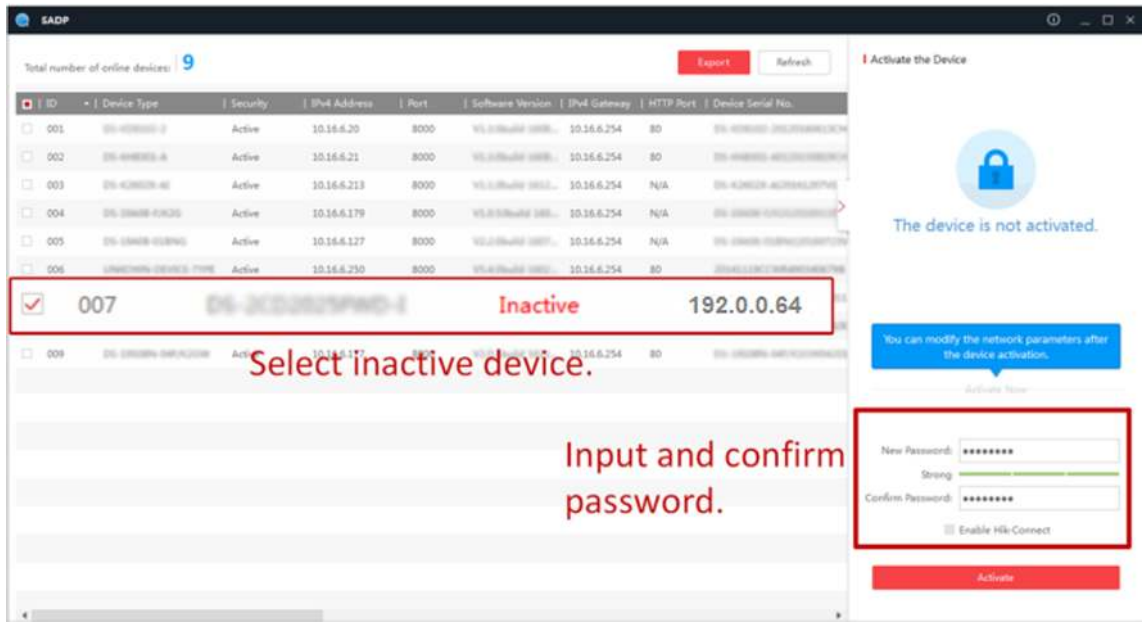
Caution

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.

Note

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

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



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

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

6.2 Activate Device via iVMS-4200 Client Software

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

Steps

Note

This function should be supported by the device.

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

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

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

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

Note

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

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

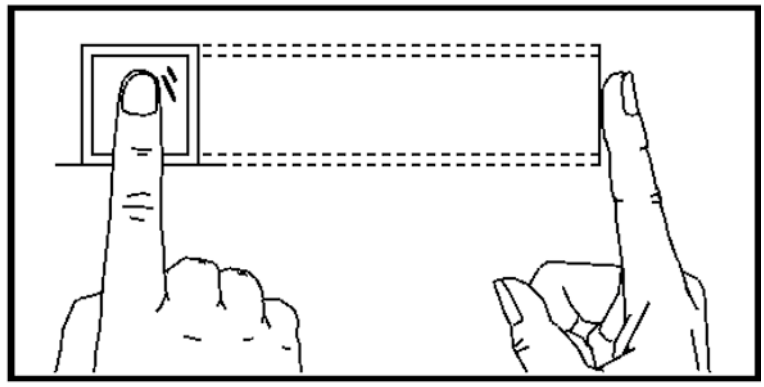
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

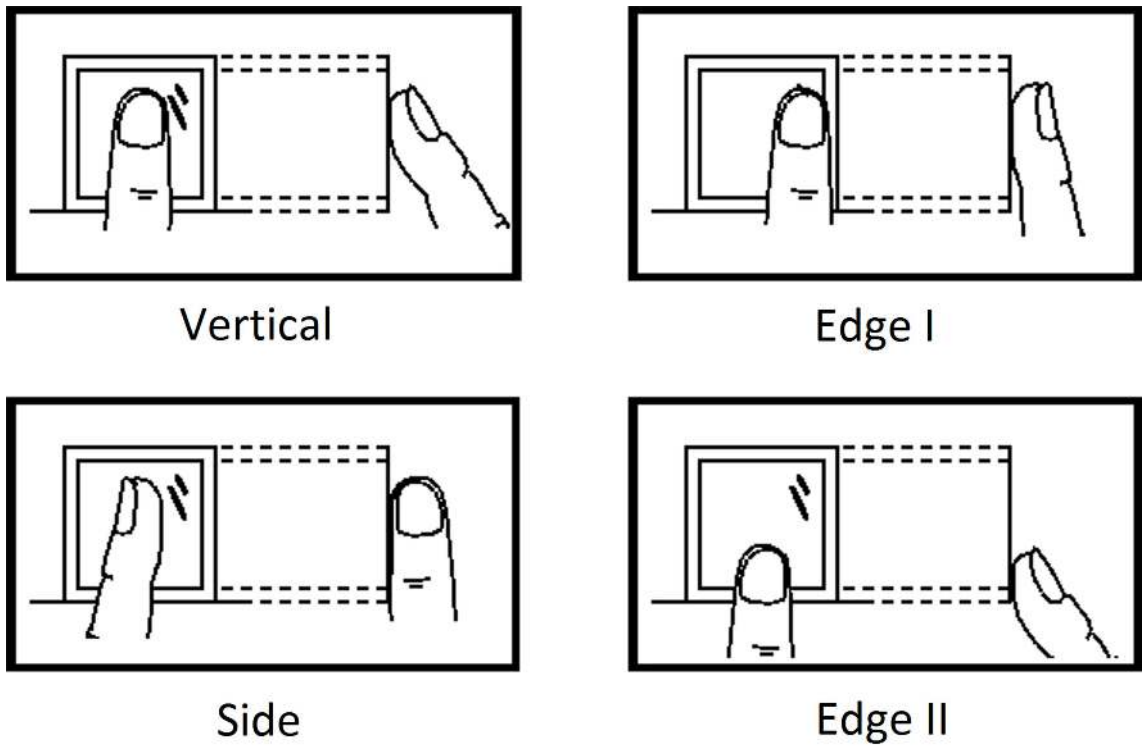
The figure displayed below is the correct way to scan your finger:



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

Incorrect Scanning

The figures of scanning fingerprint displayed below are incorrect:



Environment

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

Others

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

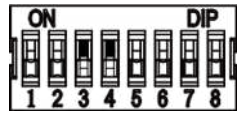
Appendix B. DIP Switch

B.1 DIP Switch Description

The DIP switch is on the access control board. No.1 to No 8 is from the low bit to the high bit.

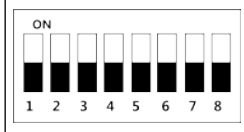
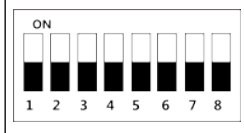
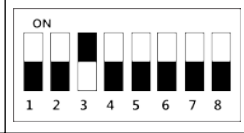
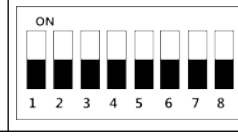


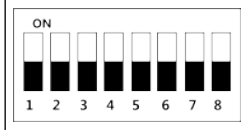
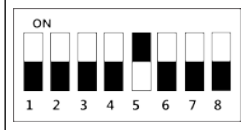
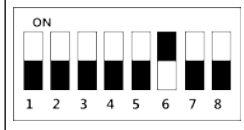
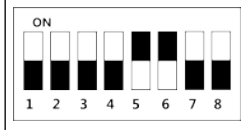
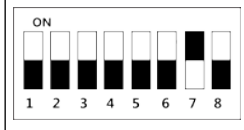
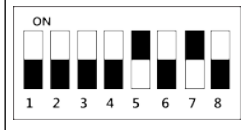
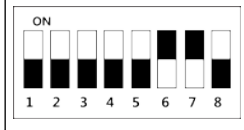
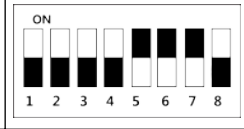
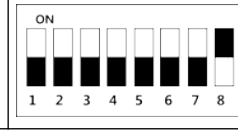
When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off. If you set the DIP switch like the figure displayed below, its binary value is 00001100, and its decimal value is 12.



B.2 DIP Switch Corresponded Functions

The 8-bit DIP switch corresponded functions on the access control board are as follows:

Bit	Device Mode	Function	Decimal Value	Binary Value
1 to 2	Work Mode	Normal Mode	0	
3	Memory Mode	Enable Memory Mode	0	
		Disable Memory Mode	1	
4	Keyfob Paring Mode	Enable Keyfob Paring Mode	1	
		Disable Keyfob Paring Mode	0	

Bit	Device Mode	Function	Decimal Value	Binary Value
5 to 8	Passing Mode	Controlled Bi-direction	0	
		Controlled Entrance and Prohibit Exit	1	
		Controlled Entrance and Free Exit	2	
		Free Bi-direction	3	
		Free Entrance and Controlled Exit	4	
		Free Entrance and Prohibit Exit	5	
		Prohibited Bi-direction	6	
		Prohibit Entrance and Controlled Exit	7	
		Prohibit Entrance and Free Exit	8	

Appendix C. Event and Alarm Type

Event	Alarm Type
Passing Timeout	None

Appendix D. Table of Audio Index Related Content

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

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