DS-K3G530(L)X Series Tripod Turnstile

User Manual

Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

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

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

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.

Contents

Chapter 1 Overview 1
1.1 Introduction 1
1.2 Main Features 1
Chapter 2 System Wiring 3
Chapter 3 Install Pedestals 5
Chapter 4 General Wiring 8
4.1 Components Introduction 8
4.2 Connect Protective Ground Wire 10
4.3 Serial Port Introduction 12
4.4 General Wiring 13
4.5 Wiring 15
4.6 Terminal Description 15
4.6.1 Lane Control Board 15
4.6.2 Access Board (Optional) 16
4.6.3 Optional Board 20
4.6.4 Card Reader Board (Optional) 20
4.6.5 Lane Status Indicator Board 21
4.6.6 Authentication Indicator Board 22
4.6.7 RS-485 Wiring 22
4.6.8 RS-232 Wiring 23
4.6.9 Alarm Input Wiring 23
4.6.10 Exit Button Wiring 24
4.7 Device Settings 25
4.7.1 Configuration via Button 25
4.7.2 Study Mode Settings 28
4.7.3 Keyfob Pairing 30

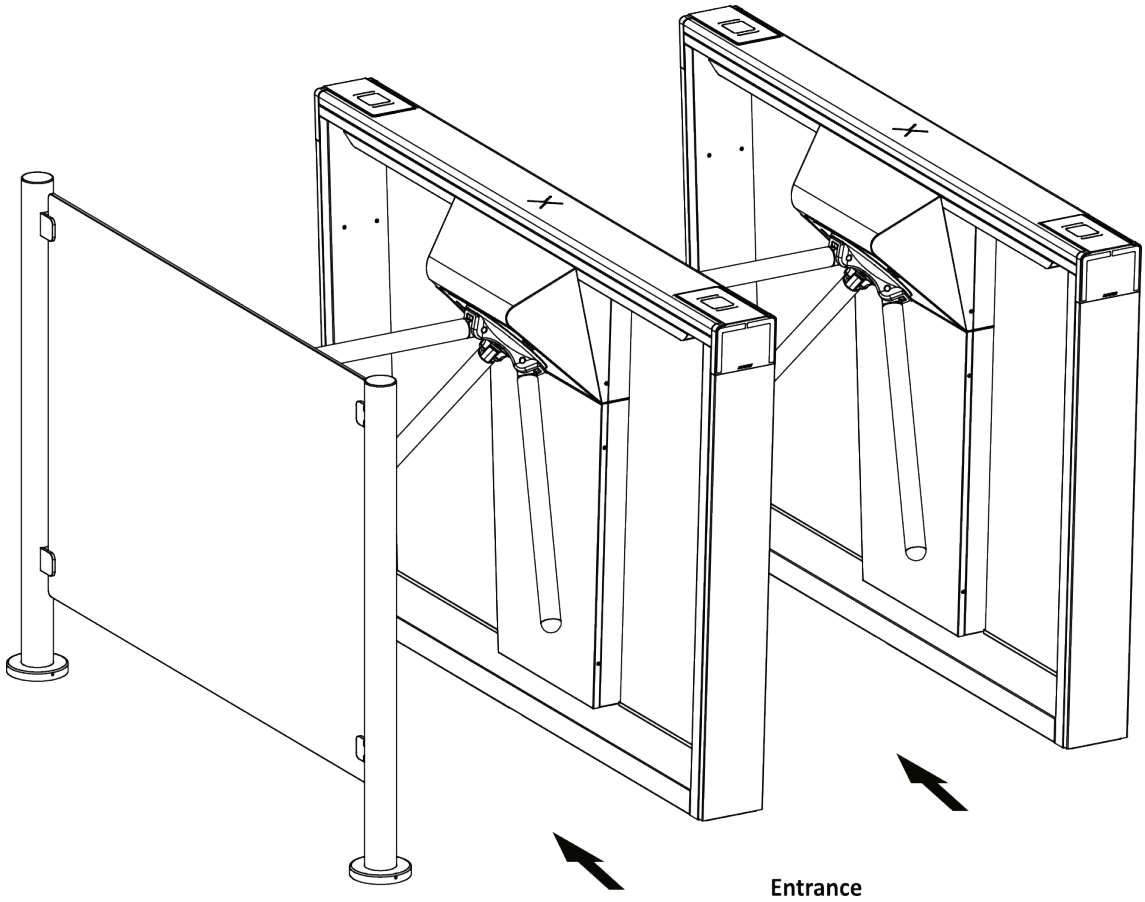
4.7.4 Initialize Device 32
Chapter 5 Activation 33
5.1 Activate via Web Browser 33
5.2 Activate via Mobile Web 33
5.3 Activate Device via HiTools Delivery 34
5.4 Activate Device via iVMS-4200 Client Software 36
Chapter 6 Operation via Web Browser 38
6.1 Login 38
6.2 Forget Password 38
6.3 Quick Operation via Web Browser 38
6.3.1 Time Settings 38
6.4 Live View 39
6.5 Person Management 40
6.6 Turnstile 41
6.6.1 Search Event 41
6.6.2 Access Control Settings 42
6.6.3 Turnstile Configuration 48
6.7 System and Maintenance 53
6.7.1 View Device Information 53
6.7.2 Set Time 53
6.7.3 Change Administrator's Password 54
6.7.4 Online Users 54
6.7.5 View Device Arming/Disarming Information 54
6.7.6 Set Working Mode via PC Web 55
6.7.7 Network Settings 55
6.7.8 Set Wiegand Parameters via PC Web 59
6.7.9 Serial Port Settings 60
6.7.10 Set Audio Parameters on PC Web 61

6.7.11 Event Linkage 62
6.7.12 Prompt Schedule 62
6.7.13 Maintenance 64
6.7.14 Device Debugging 66
6.7.15 Motor Learning 66
6.7.16 Test Protocol via PC Web 67
6.7.17 Set Network Penetration Service via PC Web 67
6.7.18 Component Status 68
6.7.19 View Log via PC Web 68
6.7.20 Certificate Management 69
Chapter 7 Configure the Device via the Mobile Web 71
7.1 Login 71
7.2 Overview 71
7.3 Configuration 73
7.3.1 Turnstile Basic Settings 73
7.3.2 Person Management 74
7.3.3 Keyfob Settings 76
7.3.4 Light Settings 76
7.3.5 View Device Basic Information 77
7.3.6 Time Settings 78
7.3.7 User Management 79
7.3.8 Network 79
7.3.9 Event Search 84
7.3.10 Audio Settings 84
7.3.11 Access Control Settings 84
7.3.12 People Counting Settings 90
7.3.13 Other Settings 91
7.3.14 Upgrade and Maintenance 91

7.3.15 Device Debugging 92
7.3.16 View User Document 93
7.3.17 Open Source Software Licenses 93
7.3.18 Log Out 93
Chapter 8 Other Platforms to Configure 94
Appendix A. DIP Switch 95
A.1 DIP Switch Description 95
A.2 DIP Switch Corresponded Functions 95
Appendix B. Button Configuration Description 96
Appendix C. Event and Alarm Type 99
Appendix D. Table of Audio Index Related Content 100
Appendix E. Error Code Description 101

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

- Bidirectional (Entering/Exiting) lane.
- Support remote control and management by HCP software.
- High-brightness LED indicates the entrance/exit and passing status.
- Fire alarm passing: When triggered, the arms will be dropped automatically for emergency evacuation.

- Support PC web configuration.
- Support ISAPI protocol for 3rd party integration development.

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 785.9 mm.

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

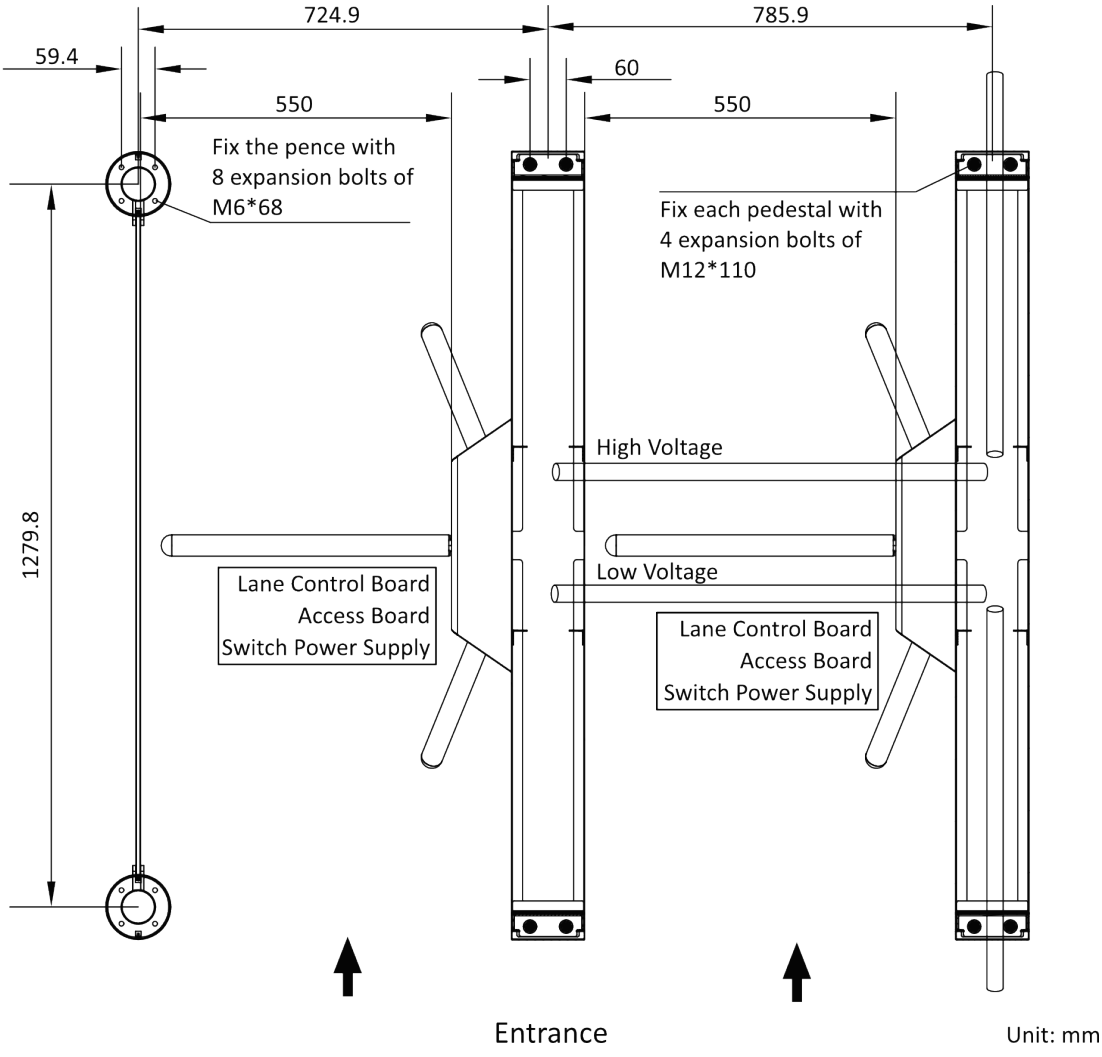


Figure 2-1 Hole Position Diagram

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

Note

- High voltage: AC power input
  Low voltage: network communication cable
- The inner diameter of the low voltage conduit and of the high voltage (AC power cord) conduit should be larger than 30 mm. If any high-power authentication device is required to install on the left pedestal, the diameter of its conduits should be larger.
- If you want to bury both of the AC power cord and the low voltage cable, the two cables should be in separated conduits to avoid interference.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.
- The external AC power cord should be double-insulated.
- The network cable must be CAT5e or other cables with better performance.
- Before digging holes, evaluate the thickness of the installation surface to avoid puncturing.

Chapter 3 Install Pedestals

Before You Start

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

Steps

Note

- Make sure the device is installed on flat surface. The foundation should be hard and the thickness should exceeds the length of the expansion bolt.
- Make sure the device is powered off during installation and other operations.
- The installation tools are put inside the package of the pedestal.
- In order to prevent stainless steel from rusting due to dirt during the installation, it is recommended to tear off the protective film after the device is installed.
- There may be residual glue at the film cutting position, and it is recommended to wipe the glue with WD-40 protective liquid after tearing the film.
- Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 150 mm.

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Align the pedestals with the pre-buried expansion bolts.
3. Remove 4 screws of each pedestal that fix the 2 side panels, and remove the side panels.
4. Secure the pedestals with expansion bolts and fix the side panels to its original position with screws.
5. Remove the maintenance door for cable wiring.

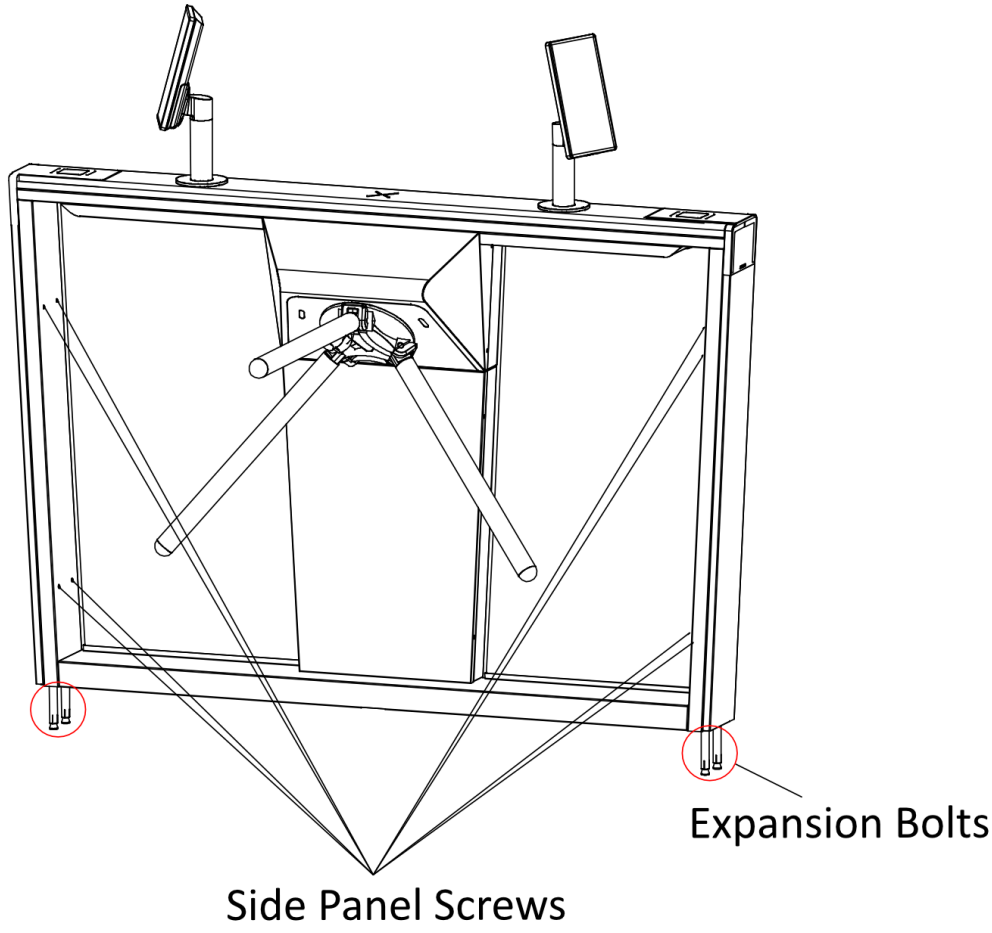


Figure 3-1 Remove Side Panel Screws

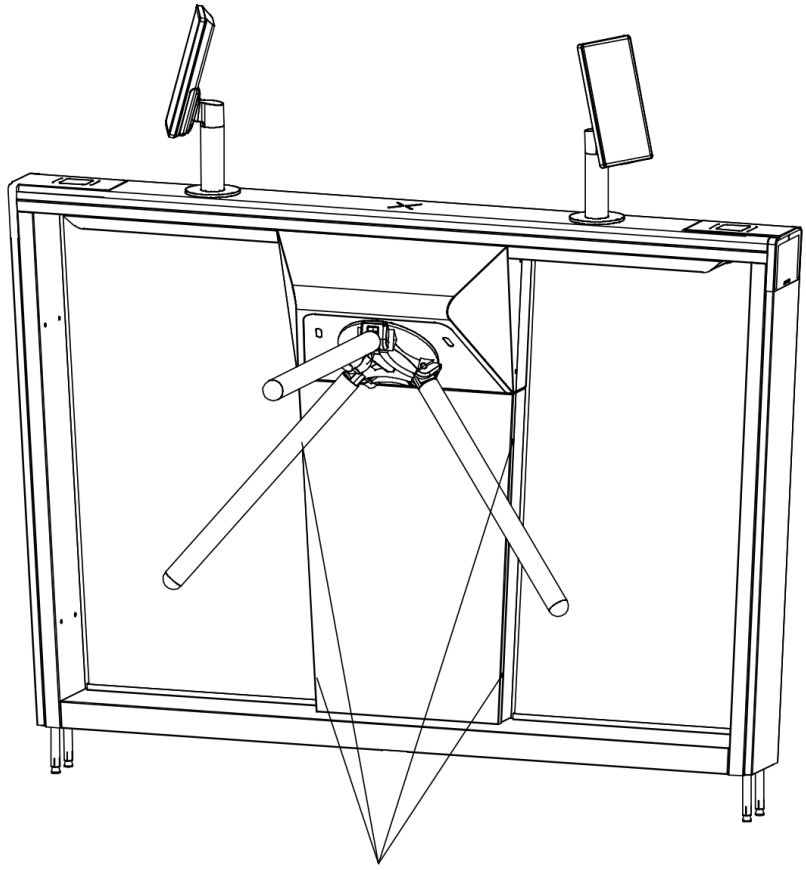


Figure 3-2 Remove Maintenance Door Screws

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 network cable and peripherals. 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 200 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.

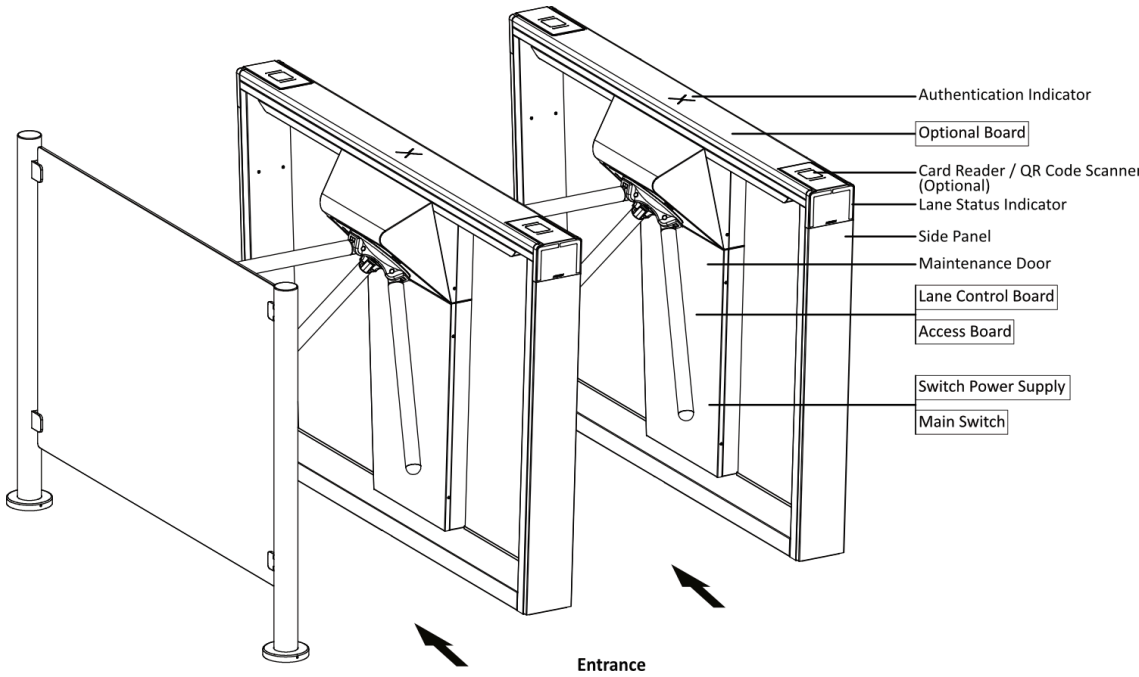


Figure 4-1 Components

Lane Status Indicator

The lane status indicator indicates different passing mode.

- Light stays blue: remain open
- Light stays red: remain closed
- Light stays white: controlled

Authentication Indicator

The authentication indicator indicates authentication and alarm status.

- The light stays off when the device is on standby mode.
- The light on both side will stay green for authenticated passing.
- The light on the authenticated side will flash red when authentication fails.
- When there is a reverse, tailgating, staying out of time, or accidental entry, the red light of both sides flashes until the alarm is reset.

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

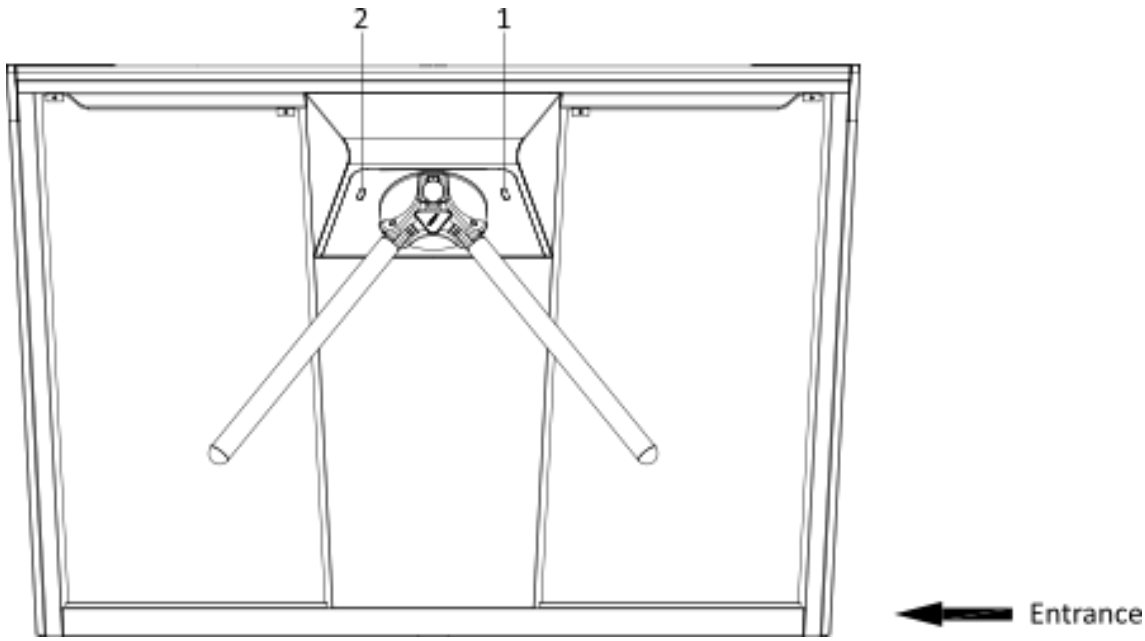


Figure 4-2 IR Module

4.2 Connect Protective Ground Wire

Grounding via Power Outlet

If there is a power outlet near the installation environment and the grounding pin inside the outlet is properly grounded, grounding can be achieved directly through the PE (Protective Earth) wire of the power cable. Note that the power cable used for the device must be a three-core cable with a protective grounding wire.

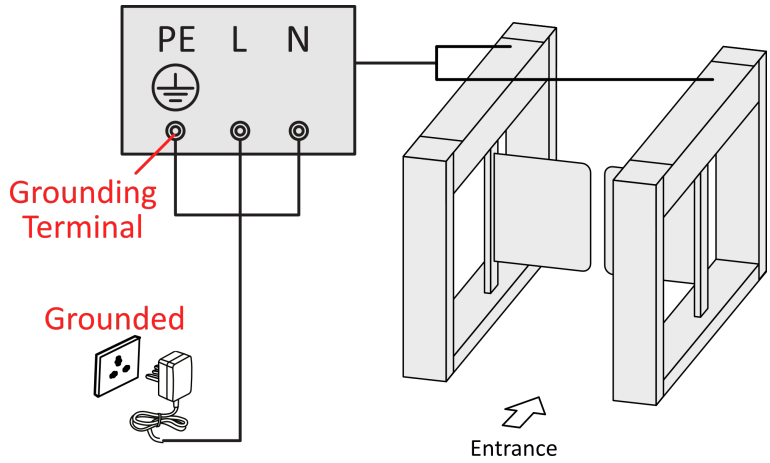
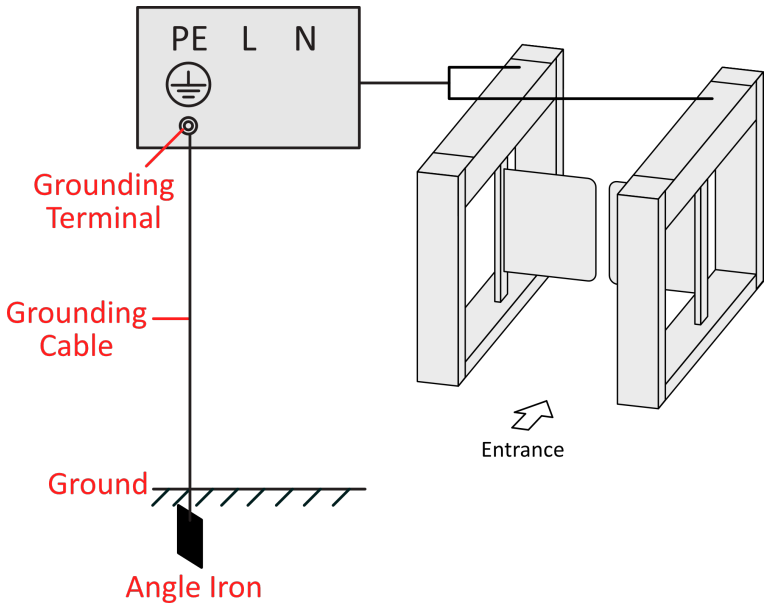


Figure 4-3 Power Cable Grounding Method (Taking Swing Barrier as An Example)

Grounding via Buried Grounding Electrode

If there is soil near the installation environment and it is permissible to bury a grounding electrode, follow these steps for grounding installation:
Drive an angle iron (or steel pipe) with a length of no less than 0.5 meters into the ground.
Weld one end of the grounding wire to the angle steel (or steel pipe) and apply anti-corrosion treatment (e.g., electroplating or coating) to the welded area.
Connect the other end of the grounding wire to the protective grounding terminal inside the gate chassis marked with a full-circle protective grounding symbol, and tighten the fixing screw.



Grounding via Grounding Bar

If there is a grounding bar near the installation environment, connect one end of the grounding wire to the terminal of the engineering grounding bar and the other end to the protective grounding terminal inside the gate chassis marked with a full-circle protective grounding symbol, then tighten the fixing screw.

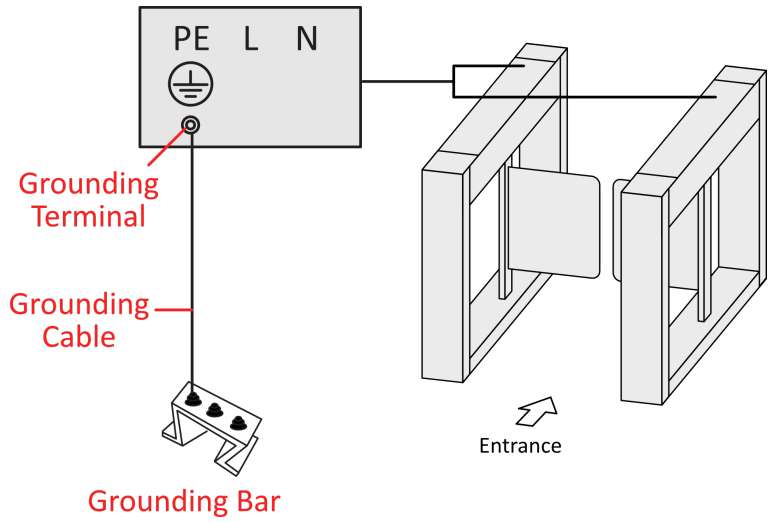


Figure 4-5 Simplified Diagram of Grounding Installation When Grounding Bar is Available in the Equipment Room (Taking Swing Barrier as An Example)

Note

- For all the above grounding methods, the grounding device connected to the product must comply with national standards, and the grounding resistance should not exceed 4Ω.
- The grounding wire and PE wire must use a yellow-green grounding wire of at least 18 AWG.

4.3 Serial Port Introduction

If card reader, QR code scanner, etc. are not installed on the device, you can wire according to the serial port.

View serial port position according to the diagram below.

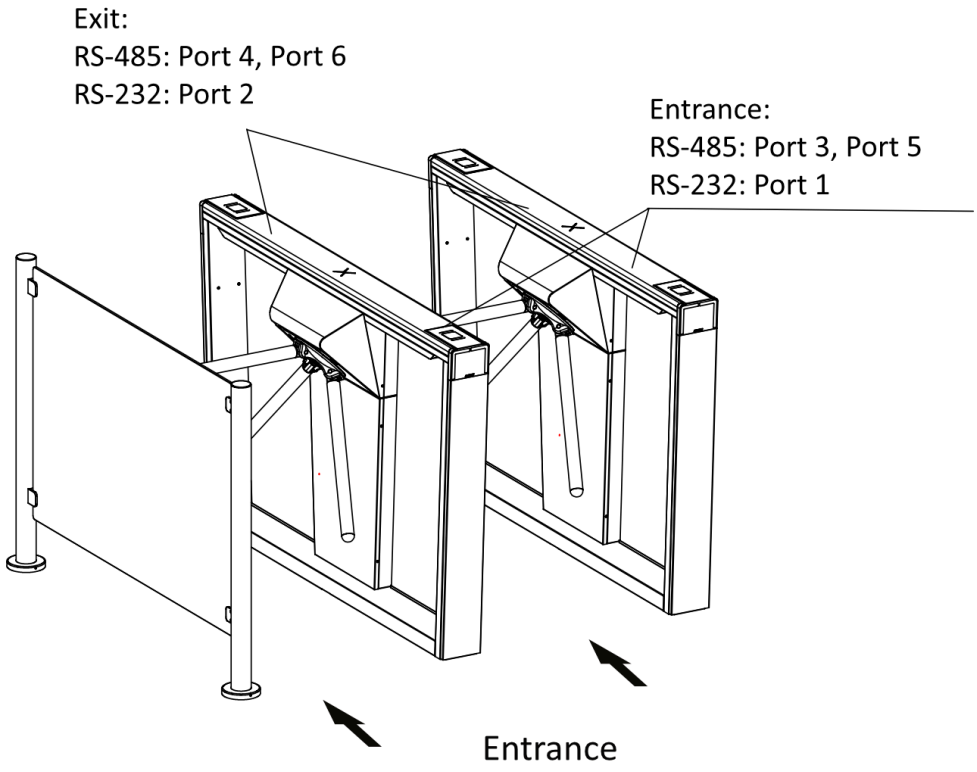


Figure 4-6 Serial Port

Serial Port No. on WEB	Communication Method	Peripheral Type
Port 1	RS-232A	QR Code Scanner (Entrance)
Port 2	RS-232B	QR Code Scanner (Exit)
Port 3	RS-485A	QR Code Scanner (Entrance)
Port 4	RS-485B	QR Code Scanner (Exit)
Port 5	RS-485C	Card Reader (Entrance)
Port 6	RS-485D	Card Reader (Exit)

4.4 General Wiring

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

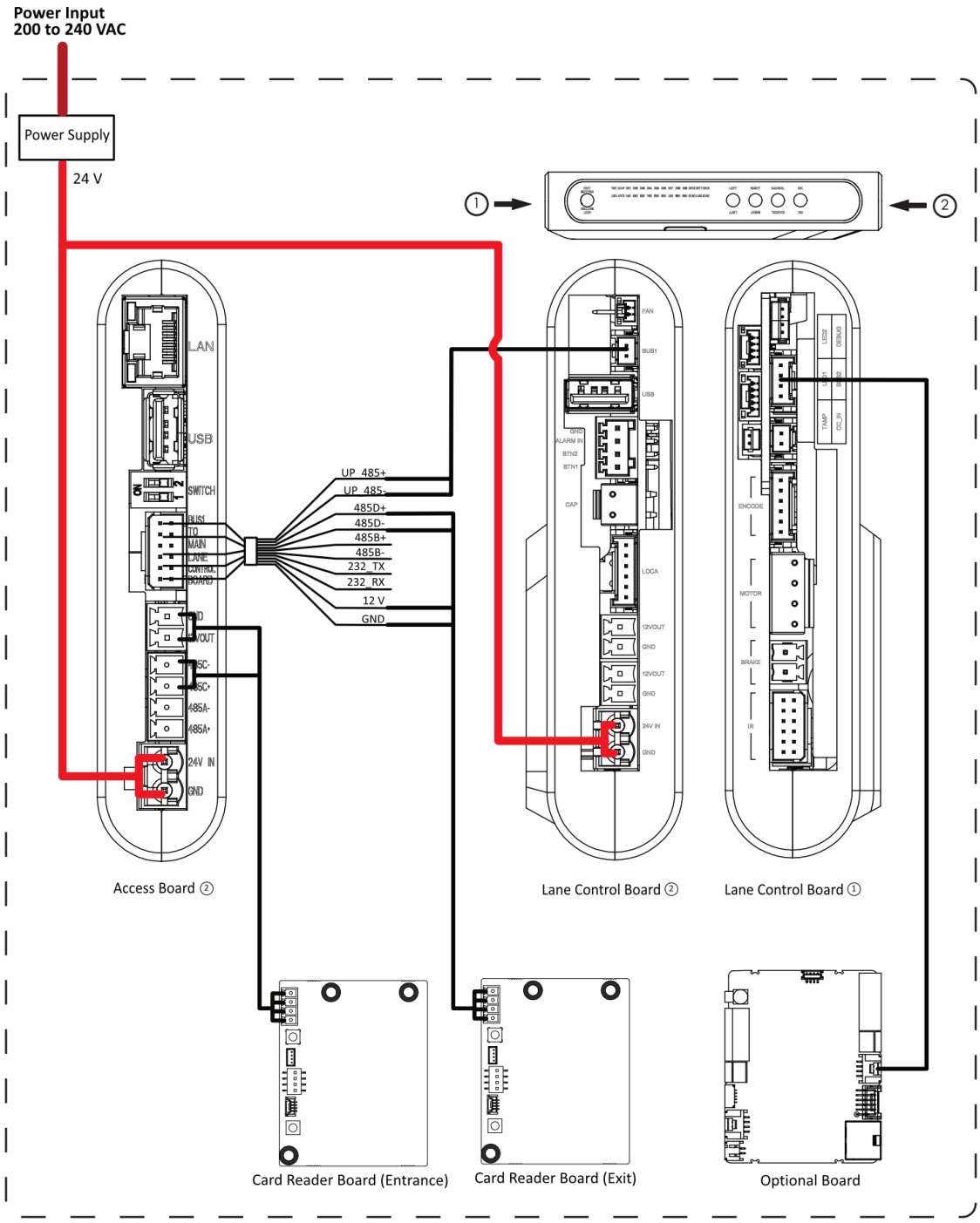


Figure 4-7 General Wiring

Note

- The power cable from main switch to the main lane control board has been connected. You will need to prepare the 14AWG power cable to connect the AC power input to power supply.
- Barrier opens at the entrance/exit: connect to BTN1/BTN2 and GND.

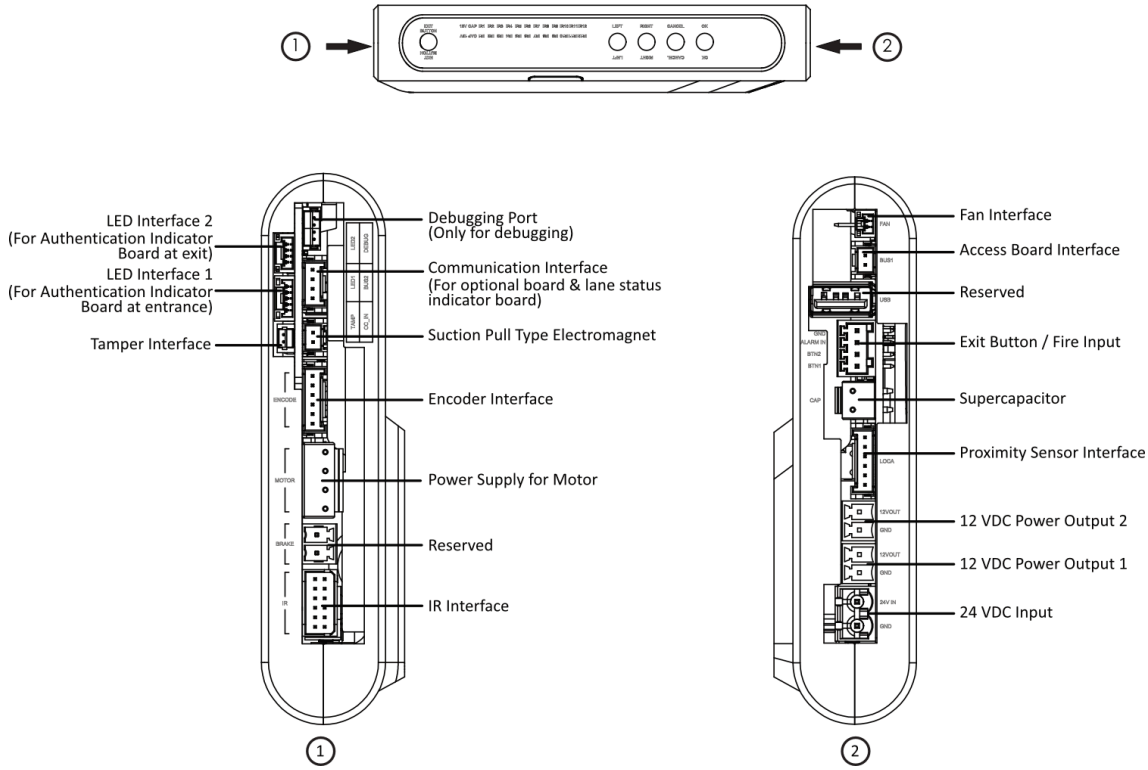
4.5 Wiring

Scan the QR code to view the wiring guide video.

4.6 Terminal Description

4.6.1 Lane Control Board

The picture displayed below is the lane control board diagram.



4.6.2 Access Board (Optional)

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

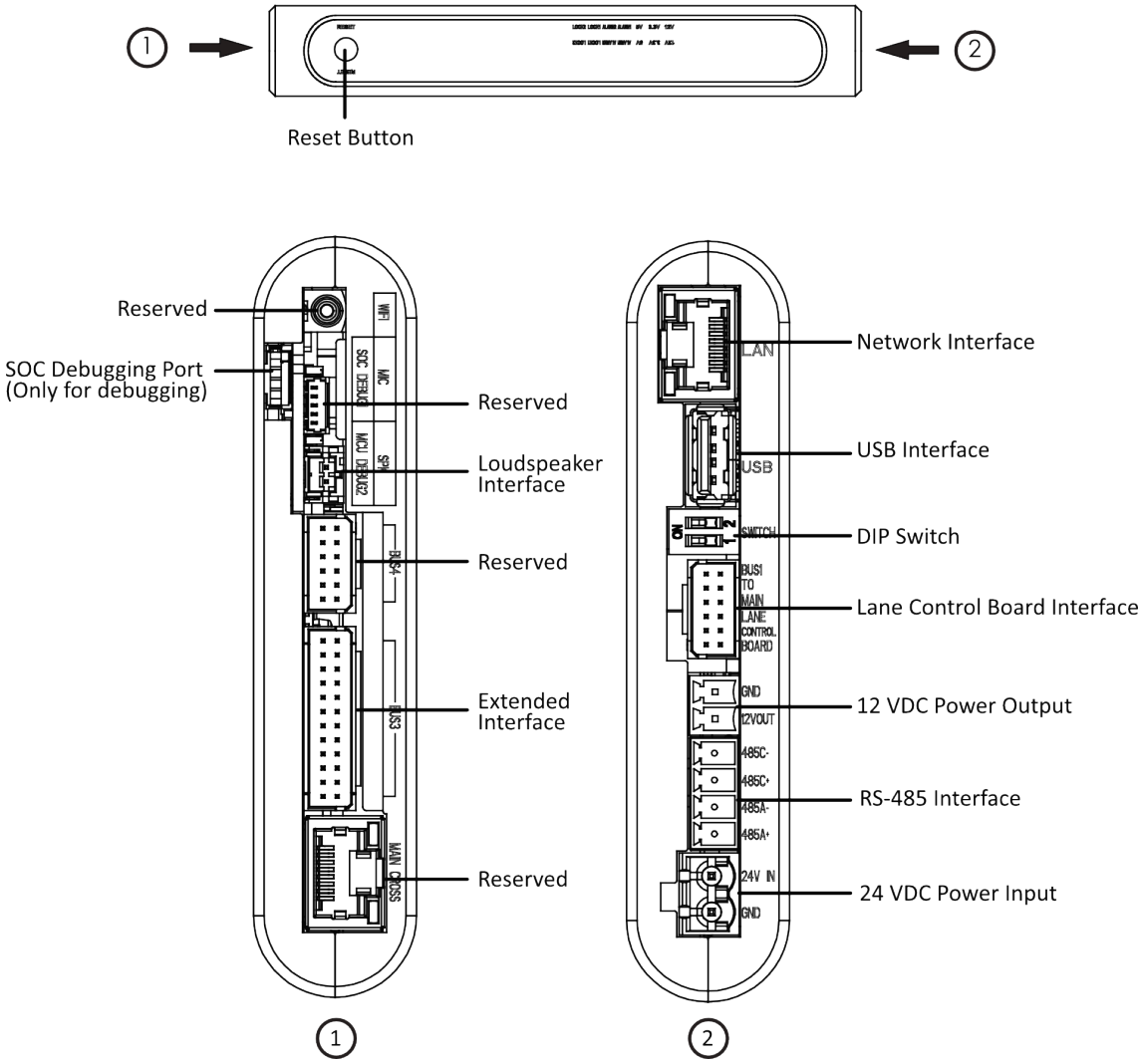


Figure 4-8 Access Board

Note

- RS-485A corresponds to port 3 on web and is for QR code scanner at entrance by default. RS-485C corresponds to port 5 on web and is for card reader at entrance by default.
- The SOC serial port are for maintenance and debugging use only.
- Press the Reset button for 5 s and the device will start to restore to factory settings.
- The DIP switch is for study mode setting and keyfob paring. For detailed information about the DIP switch, see *DIP Switch Description*.

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

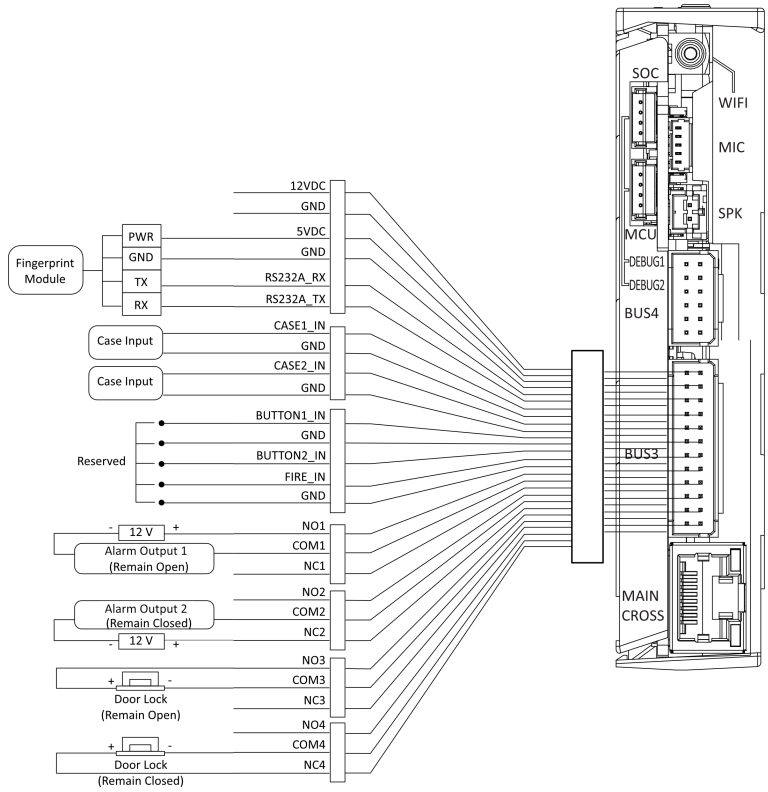


Figure 4-9 Wring Diagram of BUS3 Interface

Note

RS-232A corresponds to port 1 on web and is for QR code scanner at entrance by default.

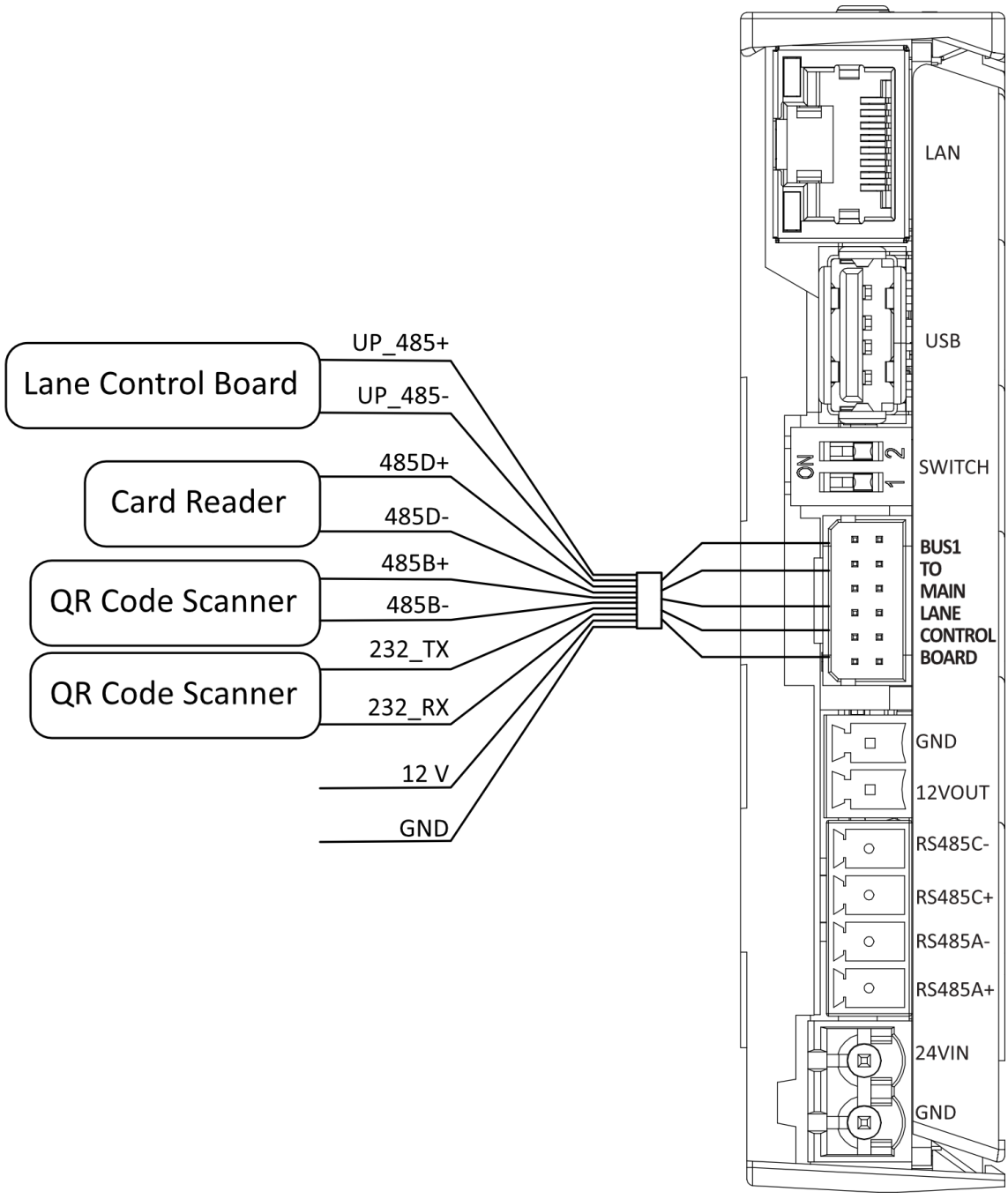


Figure 4-10 Wring Diagram of BUS1 Interface

Note

- RS-232 corresponds to port 2 on web and is for QR code scanner at exit by default.
- RS-485B corresponds to port 4 on web and is for QR code scanner at exit by default.
- RS-485D corresponds to port 6 on web and is for card reader at exit by default.

4.6.3 Optional Board

The picture displayed below is the optional board diagram.

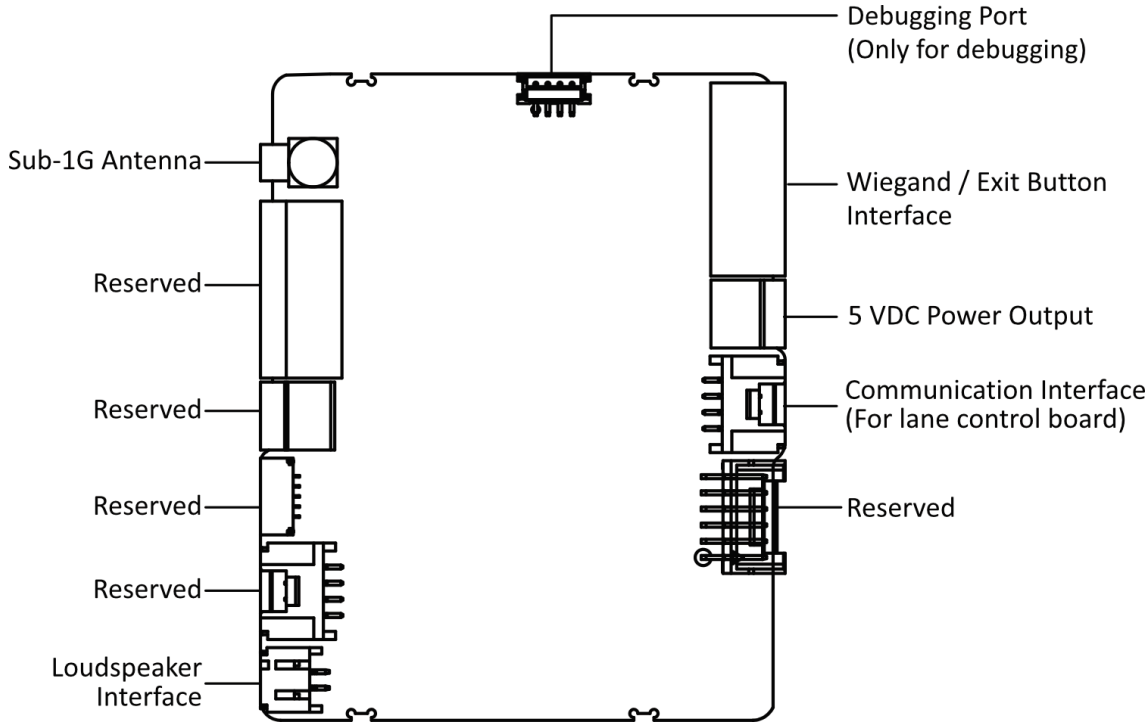


Figure 4-11 Optional Board

Note

If access board is installed, the loudspeaker can be connected to the access board; If access board is not installed, the loudspeaker can be connected to the optional board.

4.6.4 Card Reader Board (Optional)

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

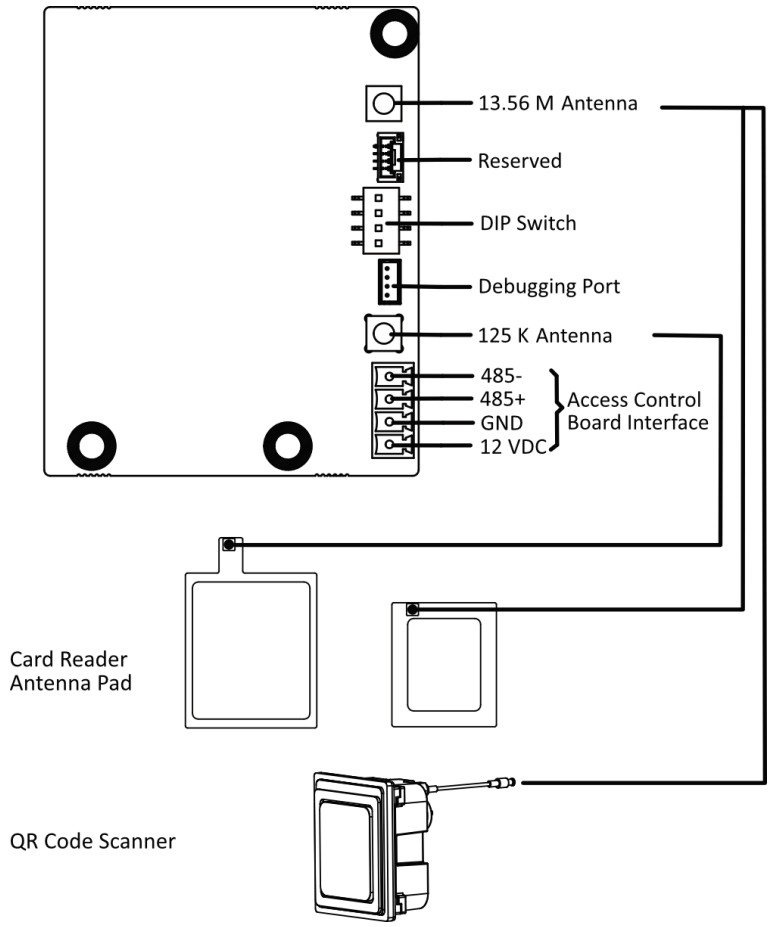
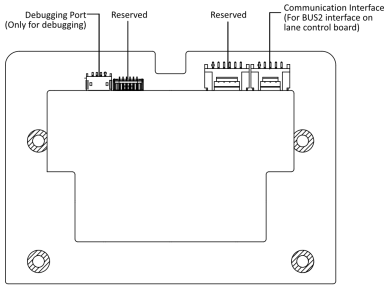
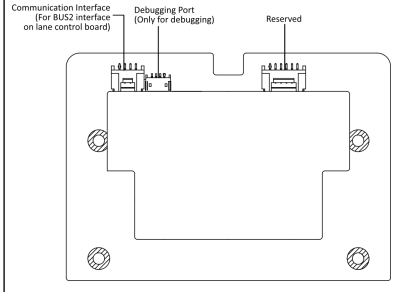


Figure 4-12 Card Reader Board

4.6.5 Lane Status Indicator Board

Lane status indicator board in different pedestals are shown as follows.

Table 4-1 Lane Status Indicator Board

Entrance	Exit
 Entrance (LED1)	 Exit (LED2)

4.6.6 Authentication Indicator Board

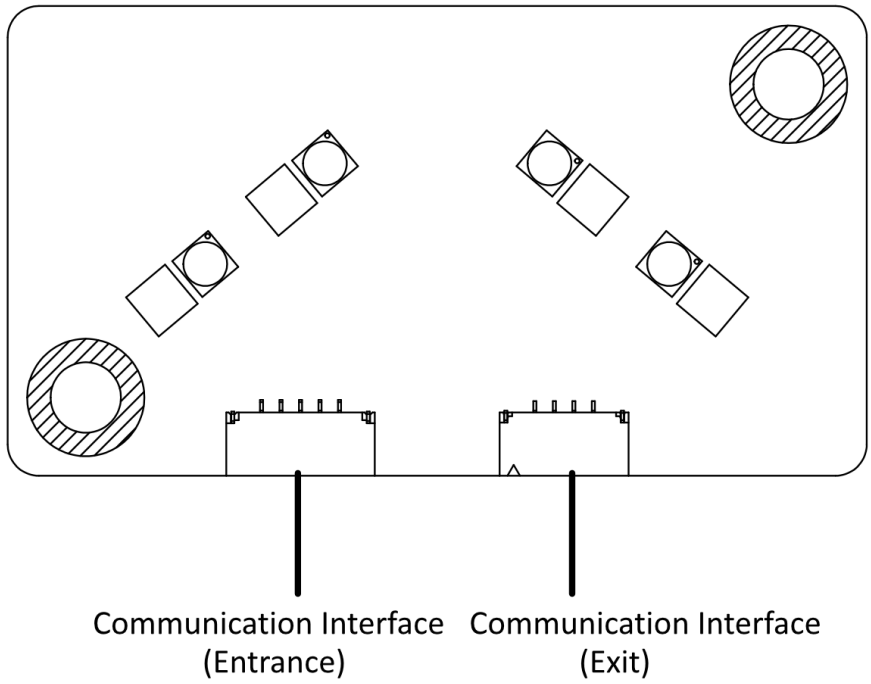


Figure 4-13 Authentication Indicator Board

The two interfaces of the authentication indicator board connect to the LED interface 1&2 on the lane control board.

4.6.7 RS-485 Wiring

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

Note

- If there are other RS-485 devices connecting, the ID of the RS-485 cannot be conflicted.
- The connected 12 V power interface for the face recognition terminal cannot be connected with other 12 V devices.

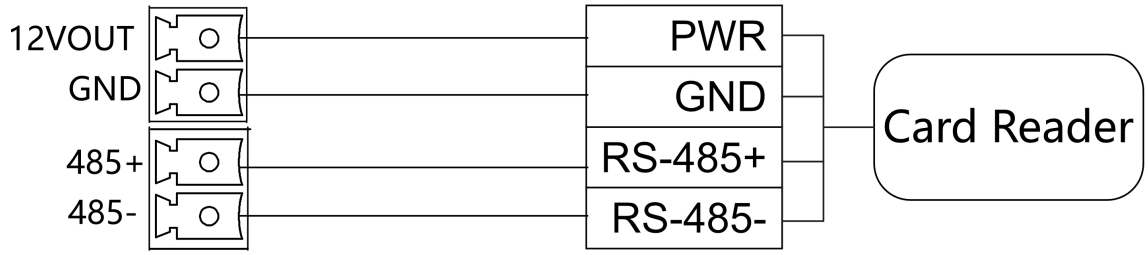


Figure 4-14 Wiring RS-485

4.6.8 RS-232 Wiring

Note

- There is 1 RS-232 interface on the extended interface of access board. The RS-232A corresponds to port 1 on web.
- There is 1 RS-232 interface on the BUS1 interface of access board. The RS-232B corresponds to port 2 on web.

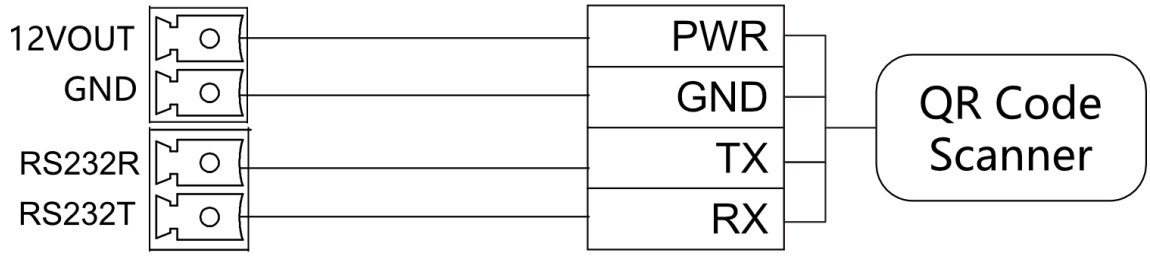


Figure 4-15 RS-232 Wiring

4.6.9 Alarm Input Wiring

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

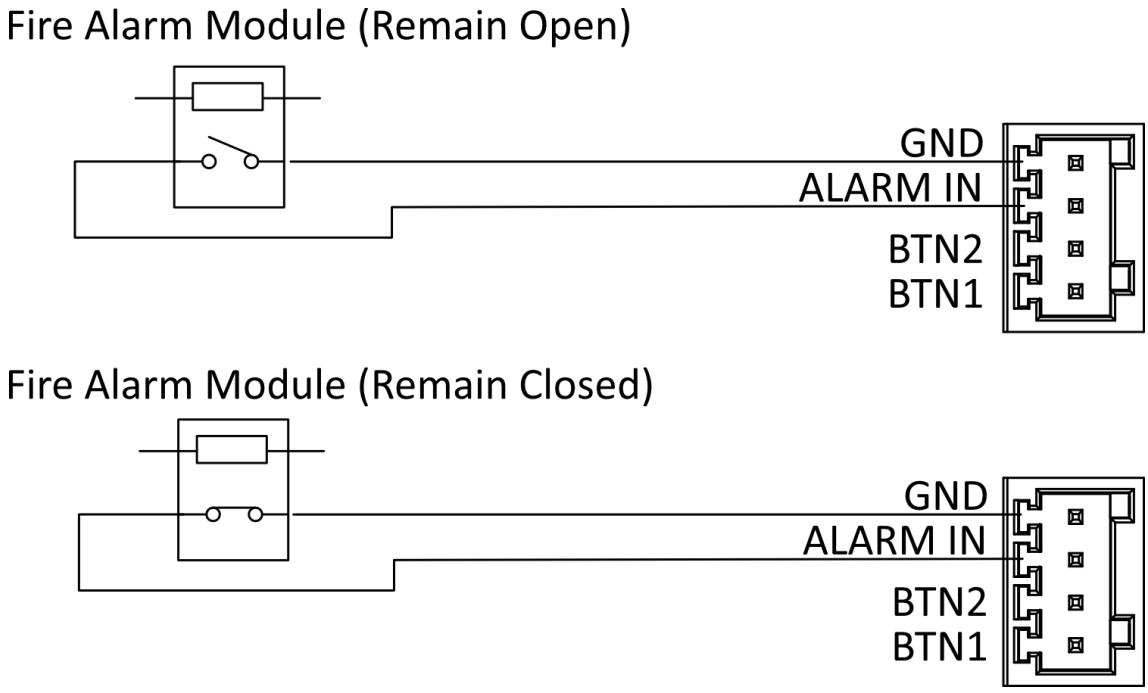


Figure 4-16 Alarm Input

4.6.10 Exit Button Wiring

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

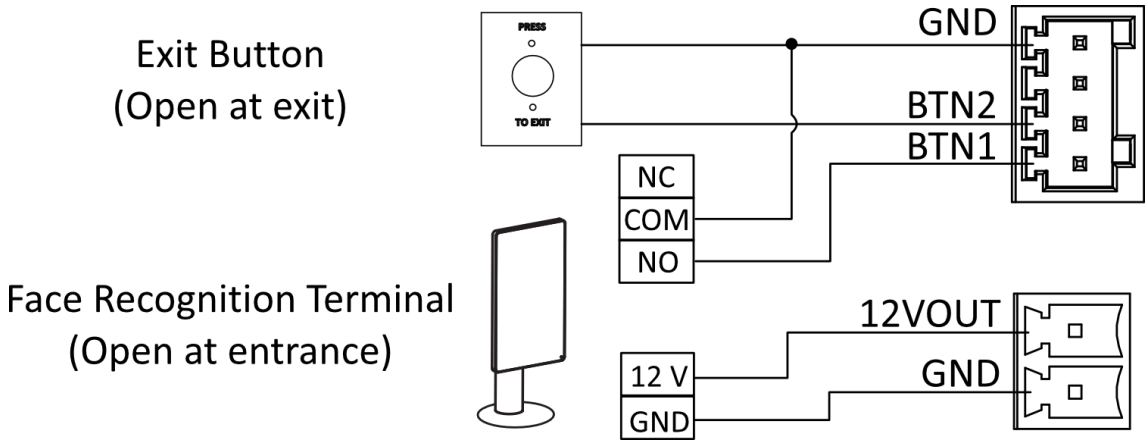


Figure 4-17 Exit Button Wiring

Note

- Barrier open at the entrance: connect to BTN1 and GND.
- Barrier open at the exit: connect to BTN2 and GND.
- The power supply for the face recognition terminal is 12 V, 2 A, 24 W.

4.7 Device Settings

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

Study Mode

The arm will study the closed position automatically.

Normal Mode

The device works normally.

Passing Mode

There are 9 kinds of passing mode.

Memory Mode

Memory mode is enabled by default. Multiple cards presenting for multiple person passing is allowable when enabling the memory mode. When the passing person's number exceeds the card presenting number, or after the latest person passing with no other person passing within the open duration, the arm can't be pushed open.

4.7.1 Configuration via Button

Button Description

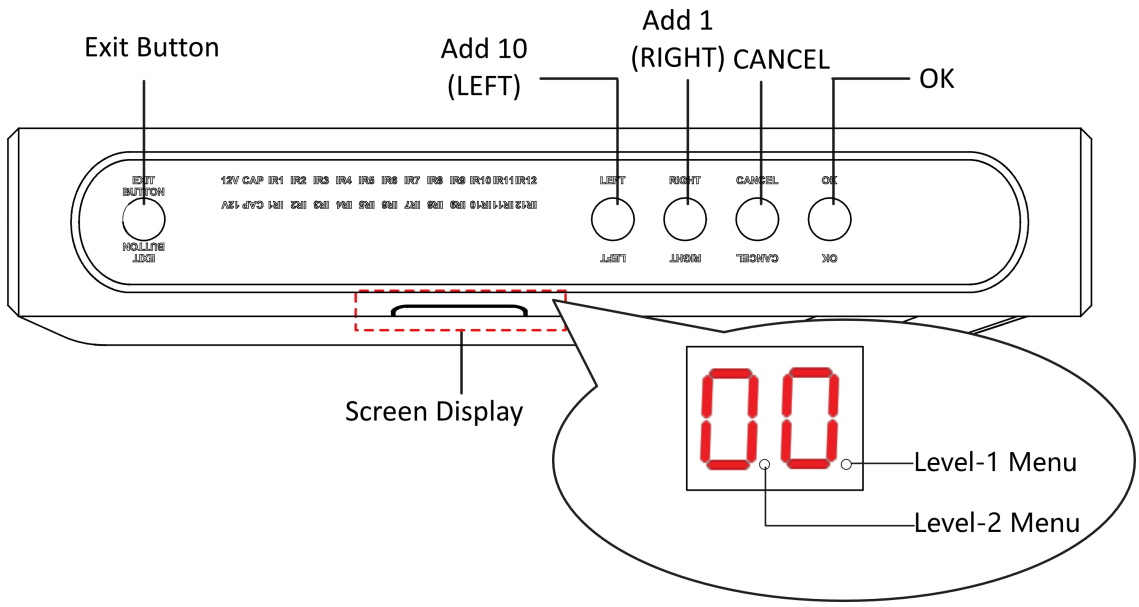


Figure 4-18 Button

Exit Button

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

Parameter Configuration Button

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

Note

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

Button Configuration Procedure

Here takes setting intrusion duration to 12 s as example:

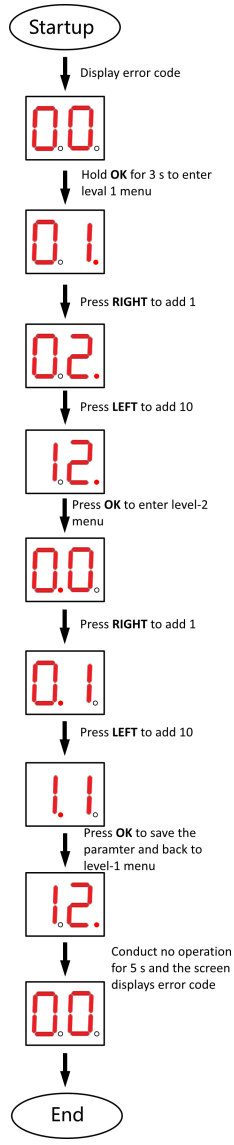


Figure 4-19 Procedure

Steps:

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

Note

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

4.7.2 Study Mode Settings

Set Study Mode via Button

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

Steps

Note

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

1. Enter the study mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **1**. The device will enter the study mode.
   3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the study mode.
2. Push the arm until it is vertical to the pedestal.
3. When you hear the continuous buzzing, stop push the arm and exit the lane.
4. When you hear **Studying completed, welcome**, the configuration is completed.

Set Study Mode

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

Steps

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

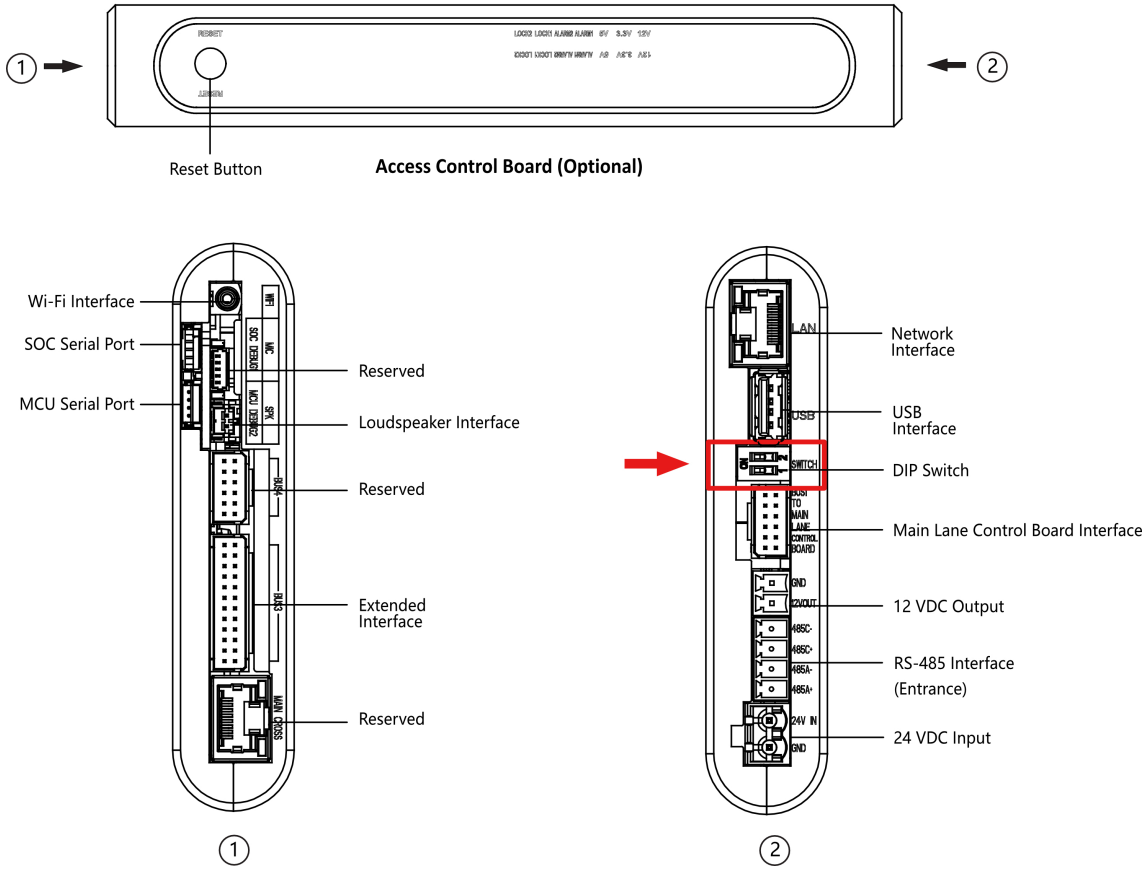


Figure 4-20 DIP Switch Location

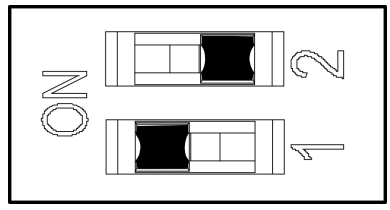


Figure 4-21 Study Mode

2. Push the arm until it is vertical to the pedestal.
3. When you hear the continuous buzzing, stop push the arm and exit the lane.
4. When you hear **Studying completed, welcome**, set the No.1 switches of the 2-digit DIP Switch on the access board by referring to the following figure.

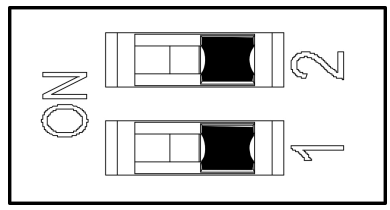


Figure 4-22 Normal Mode

5. Power on the device again.

Note

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

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

4.7.3 Keyfob Pairing

Pair keyfob via button or DIP switch.

Pair Keyfob via Button

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

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

Note

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

1. Enter the keyfob pairing mode.
   1) Enter the configuration mode.
   2) Set the configuration No. in Level-1 to **2**. The device will enter the keyfob pairing mode.
   3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the keyfob pairing mode.
2. Hold the **Close** button for more than 10 seconds.

   The keyfob's indicator will flash if the pairing is completed.
3. Exit the keyfob pairing mode.
   1) Enter the configuration mode.

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

Pair Keyfob via DIP Switch (Optional)

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

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

1. Power off the turnstile.

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

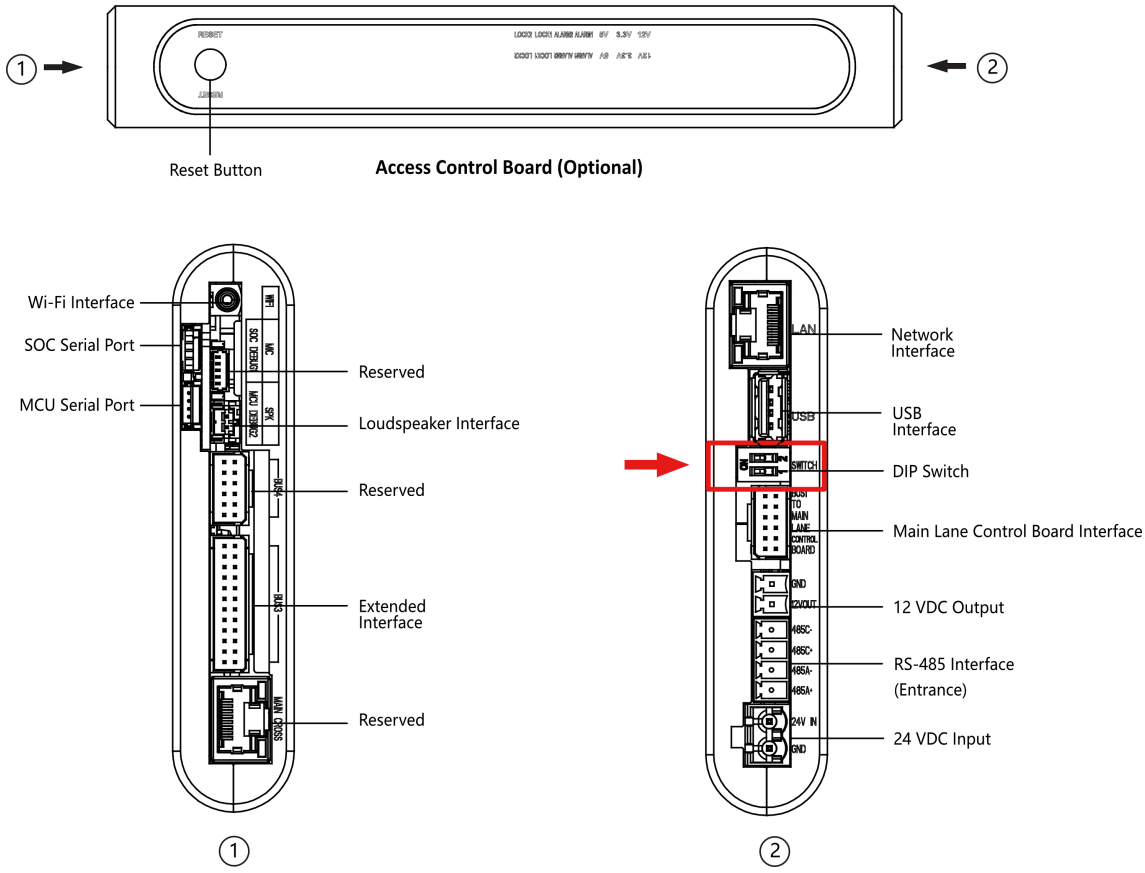


Figure 4-23 DIP Switch Location

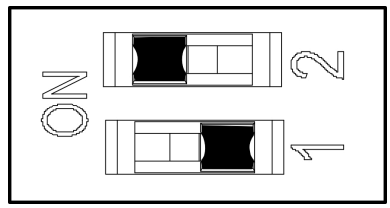


Figure 4-24 Enable Keyfob Paring Mode

3. Power on the turnstile and it will enter the keyfob pairing mode.
4. Hold the **Close** button for more than 10 seconds.

   The keyfob's indicator of the will flash twice if the pairing is completed.
5. Set the No.2 switch to the OFF side.

Note

- Only one turnstile can pair the keyfob. If multiple turnstiles are in the pairing mode, the keyfob will select only one of them to pair.
- For details about DIP switch value and meaning, see ***DIP Switch Description*** .

4.7.4 Initialize Device

Steps

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

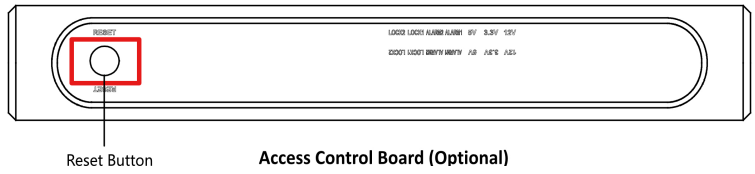


Figure 4-25 Initialization Button Position

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

Caution

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

Note

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

Chapter 5 Activation

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

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

The default values of the device are as follows:

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

5.1 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

   Note

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

2. Create a new password (admin password) and confirm the password.

   Caution

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

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

5.2 Activate via Mobile Web

You can activate the device via mobile web.

Steps

1. If device hotspot is disabled: Make sure your mobile phone and the device are connected to the same network. Place your phone to the NFC area and the device IP address will pop up, tap the address to go to the login page.

2. If device hotspot is enabled:
   - Android System: Place your phone to the NFC area and the name and password of the device hotspot will be obtained automatically. Confirm to connect, you will go to the login page.
   - iOS Ssystem: Use your phone to scan the QR code on the device label. The phone will connect to the current device's hotspot automatically. After hotspot is connected, you will go to the login page.

Caution

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

Note

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

3. Create a new password (admin password) and confirm the password.

Caution

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

Note

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

4. Click **Activate**.

5.3 Activate Device via HiTools Delivery

HiTools Delivery aims to streamline and enhance the activation, networking, and batch configuration for various devices. You can use the software to detect, activate, and modify the IP addresses of multiple devices over the LAN.

Before You Start

- Set the device and the computer that runs the software to the same network segment.
- Access the official website (***https://www.hikvision.com/en***) and enter **Support → Download → Software → HiTools → HiTools Delivery** to download HiTools Delivery and install it according to the prompts.

Steps

1. Run the software.
2. Click **Home Page → Search → Current Subnet** . Click **Refresh**, and the list will display all the online devices in the same network segment.
3. Select the inactive device(s) in the list. Set a new password according to the popup requirements and confirm the password.
4. Click **Activation**. The device activation status will change to **Activated** after successful activation.

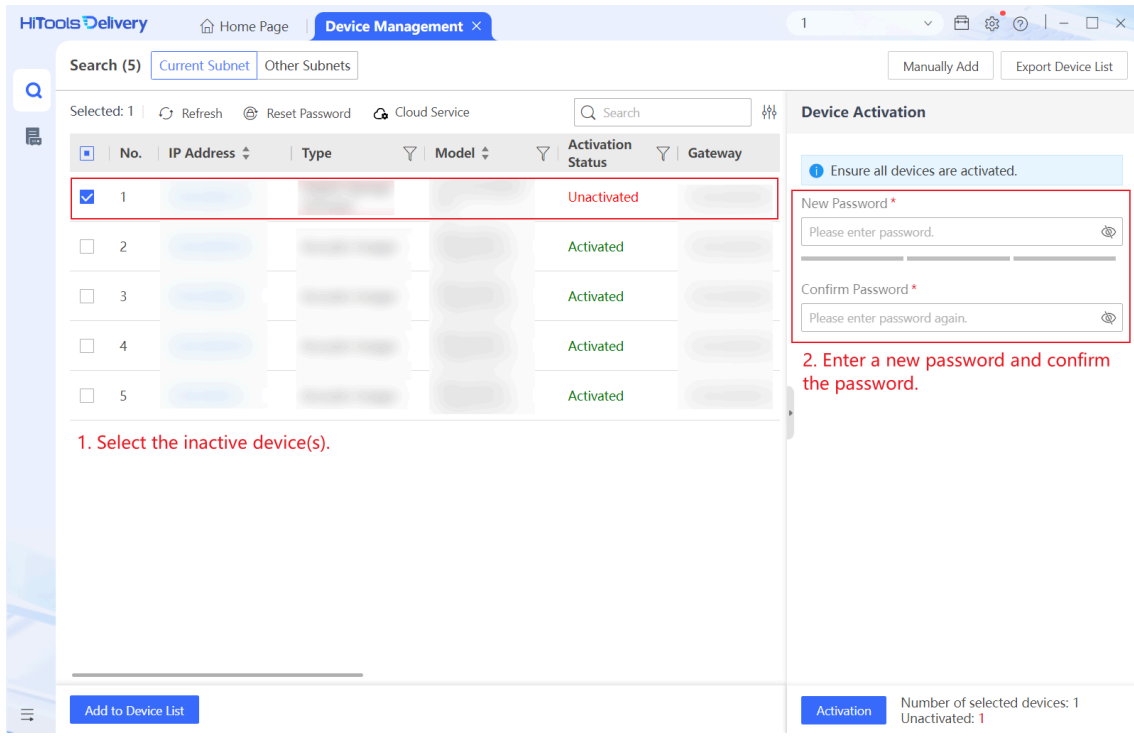


Figure 5-1 Activation

5. **Optional:** Change the IP address of the device.
   1) On **Current Subnet** interface, select multiple devices that need to change the IP addresses.
   2) On the right **Network Parameter** window, set the start IP address, port No., IPv4 subnet mask, IPv4 gateway, etc., and the selected devices will be automatically assigned to increasing IP addresses. Or check **Enable DHCP** to assign dynamic IP addresses.
   3) Enter the admin password and click **OK**.

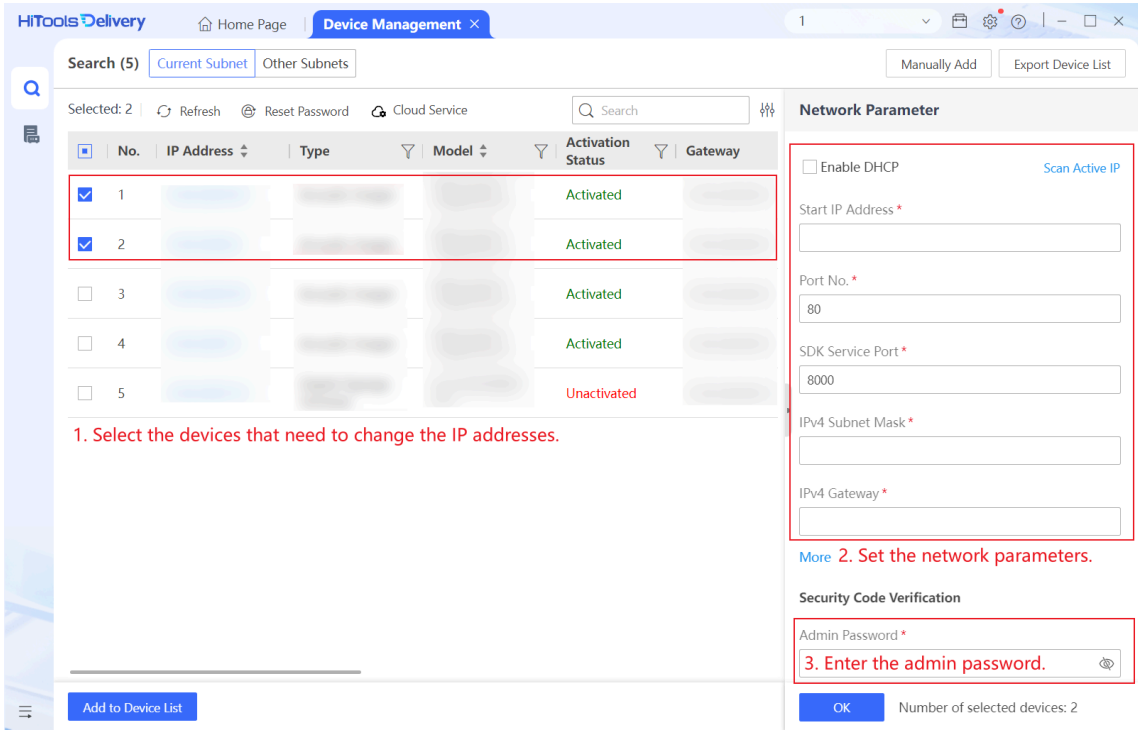


Figure 5-2 Modify Network Parameters

Note

- Set the device IP address to the same network segment with that of your computer.
- You can click **Scan Active IP** to detect and view the available IP addresses. Refer to the help of HiTools Delivery for details.
- You can also click **Home Page → Maintenance → Change IP** to change the IP addresses in batch by exporting and importing the template. Refer to the help of HiTools Delivery for details.

5.4 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 service provider and/or end-user.

Note

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

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

Chapter 6 Operation via Web Browser

6.1 Login

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

Note

Make sure the device is activated. For detailed information about activation, see ***Activation*** .

Login via Web Browser

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

Login via Remote Configuration of Client Software

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

6.2 Forget Password

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

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

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

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

6.3 Quick Operation via Web Browser

6.3.1 Time Settings

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

Device Time

Display the device time in real time.

Time Zone

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

Time Synchronization Mode

NTP

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

Manual

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

DST

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

Click **Complete** to save the settings.

6.4 Live View

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

Function Descriptions:

Device Component Status

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

Remote Control

/ / /

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

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the event search page.

Person Information

You can view the quantity information of person and card.

Network Status

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

Basic Information

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

Device Capacity

You can view the person, card and event capacity.

6.5 Person Management

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

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, and person type.
If you select **Visitor** as the person type, you can set the visit times.
If you select **Blocklist User** as the person type, an event will be uploaded when the person is authenticated.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **Save** to add the card.
Click **Save** to save the settings.

Authentication Settings

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

Blocklist Batch Operation

You can batch import or clear the blocklist person information.
Click **Blocklist Batch Operation → Import Blocklist** , and you can download the template and import the blocklist persons in batch.
Click **Blocklist Batch Operation → Clear Blocklist** , and you can delete all blocklist persons in the system.

Import/Export Person Data

Click **Person** to enter the Person page.

Export Person Data

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

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

Note

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

Import Person Data

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

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

6.6 Turnstile

6.6.1 Search Event

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

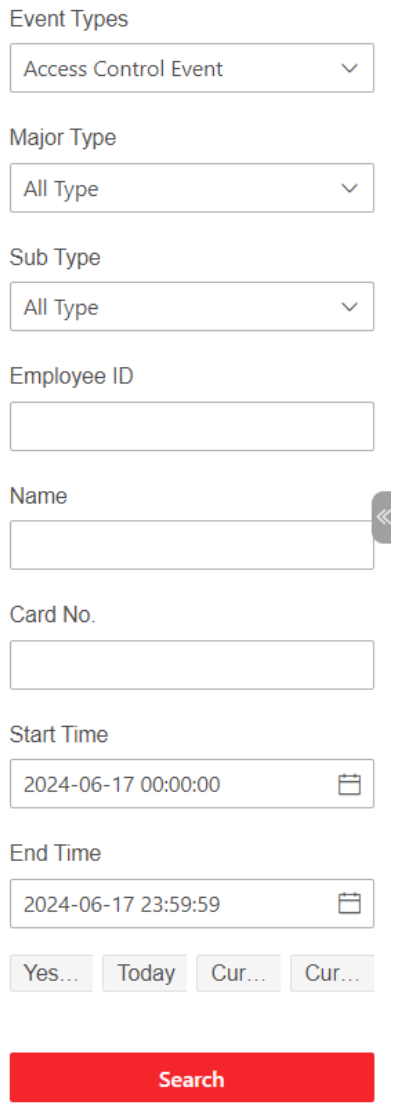


Figure 6-1 Search Event

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

The results will be displayed on the right panel.

6.6.2 Access Control Settings

Set Door Parameters

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

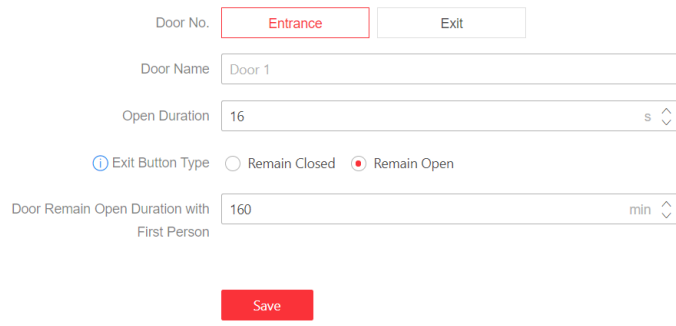


Figure 6-2 Door Parameters Settings

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

Door No.

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

Door Name

You can create a name for the door.

Open Duration

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

Note

The open duration ranges from 2 s to 60 s.

Exit Button Type

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

Door Remain Open Duration with First Person

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

Set Authentication Parameters

Click **Turnstile → Access Control Parameters → Authentication Settings** .

Note

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

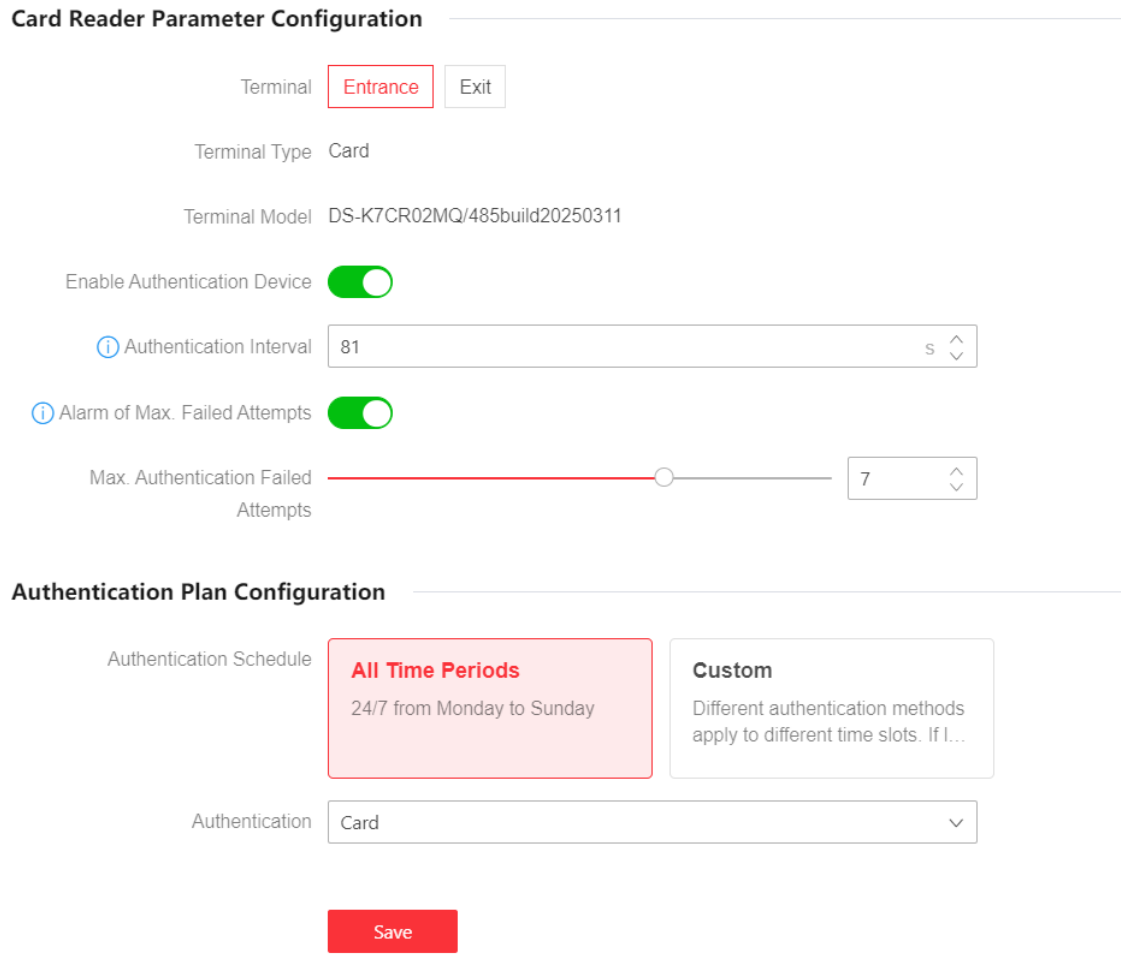


Figure 6-3 Authentication Settings

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

Card Reader Parameter Configuration

Terminal

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

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication Interval

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

Alarm of Max. Failed Attempts

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

Max. Authentication Failed Attempts

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

Authentication Plan Configuration

Authentication plan can be selected.

All Time Periods

When the selected authentication schedule is **All Time Periods**, select an authentication method from the drop-down list. The selected authentication method will be used 24/7 from Monday to Sunday to pass through the gate.

Custom

When the selected authentication plan is **Custom**, different authentication methods can be set for different time periods via the timeline.

Click **Edit** to enter the authentication method setup page, select an authentication method, and drag the mouse on the timeline to configure the planned time period. Authentication via this method is allowed within the configured time period.

Click **Erase**, then drag the mouse on the timeline to clear the planned time period.

Click **Save**.

After configuring the parameters, click **Save** to save the configuration.

Card Settings

Set Card Type

Click **Turnstile → Access Control Parameters → Card Settings** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption
Sector

M1 card encryption can improve the security level of authentication.

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

Enable EM Card

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

Note

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

Enable DESFire Card

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

DESFire Card Read Content

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

Enable FeliCa Card

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

Set Card No. Authentication Parameters

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

Go to **Turnstile → Access Control Parameters → Card Settings** .

Select a card authentication mode and click **Save**.

Card Authentication Mode

Full Card No.

All card No. will be read.

Wiegand 26 (3 bytes)

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

Wiegand 34 (4 bytes)

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

Corporate1000_35/Corporate1000_48/H10302_37/10304_37/H103130_332CSN/ Wiegand_56CSN/Wiegand_58

The device will read card via the other mode.

Enable Reversed Card No.

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

Set Terminal Parameters

You can set terminal parameters for accessing.

Click **Turnstile → Access Control Parameters → Terminal Parameters** .

Set the parameters and click **Save**.

Remote Verification

During personnel authentication, the device uploads authentication information to the platform, and the platform confirms whether to unlock the door.

Verifying Person Type Remotely

You can select the types of personnel requiring remote verification. Selected personnel will undergo remote verification by the platform or a third-party device; unselected personnel will only undergo local device verification.

Remote Verification Credential Type

Select the credential type. When authenticated person use the selected credential type, the remote verification function will be triggered preferentially, and verification will be performed by the platform or a third-party device. If personnel use other credential types, authentication will be performed locally on the device without triggering remote verification.

Remote Verification Channel Type

Choose the applicable protocol for remote verification. After selecting the corresponding protocol, remote verification can be performed via the platform, a third-party platform, or a device.

ISUP

If the third-party platform or device is not on the same local network as the local device, remote verification can be performed using the ISUP protocol. Communication requires configuring the ISUP protocol address (provided by the third-party platform or device) and ISUP listening (remote verification address, provided by the third party).

Note

For specific configuration methods, refer to ***Set ISUP Parameters via PC Web*** .

ISAPI

When the platform or a third-party platform is on the same local network as the local device, remote verification can be performed using the ISAPI protocol. The local device must be added to the platform or third-party platform before remote verification can be conducted.

Note

By default, devices use ISAPI for remote verification.

HTTP

When the platform or a third-party platform is on the same local network as the local device, and the third-party platform has its own server, remote verification can be performed using the HTTP protocol. Communication requires configuring HTTP (provided by the platform) and HTTP listening (provided by the platform).

Hik-Connect

If the third-party platform or device is not on the same local network as the local device, remote verification can be performed via Hik-Connect service.

Note

This method requires device support to be used.

Verify Credential Locally

After enabling **Remote Verification**, you can enable **Verify Credential Locally**. Once enabled, the device verifies personnel permissions locally but does not judge business rules like schedule templates.

Timeout Duration of Remote Verification

If the remote verification exceeds the configured duration, a timeout prompt will be returned.

Offline Remote Verifying Unlocking

When enabled, local authentication will be performed if the platform is offline or a timeout occurs.

Result Return Mode

Set the return mode for remote verification results to **Asynchronous** or **Sync**.

Set Privacy Parameters

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

Click **Turnstile → Access Control Parameters → Privacy Settings** .

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

Delete Old Events Periodically

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

Delete Old Events by Specified Time

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

Overwriting

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

6.6.3 Turnstile Configuration

Basic Settings

Set turnstile basic parameters.

Steps

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

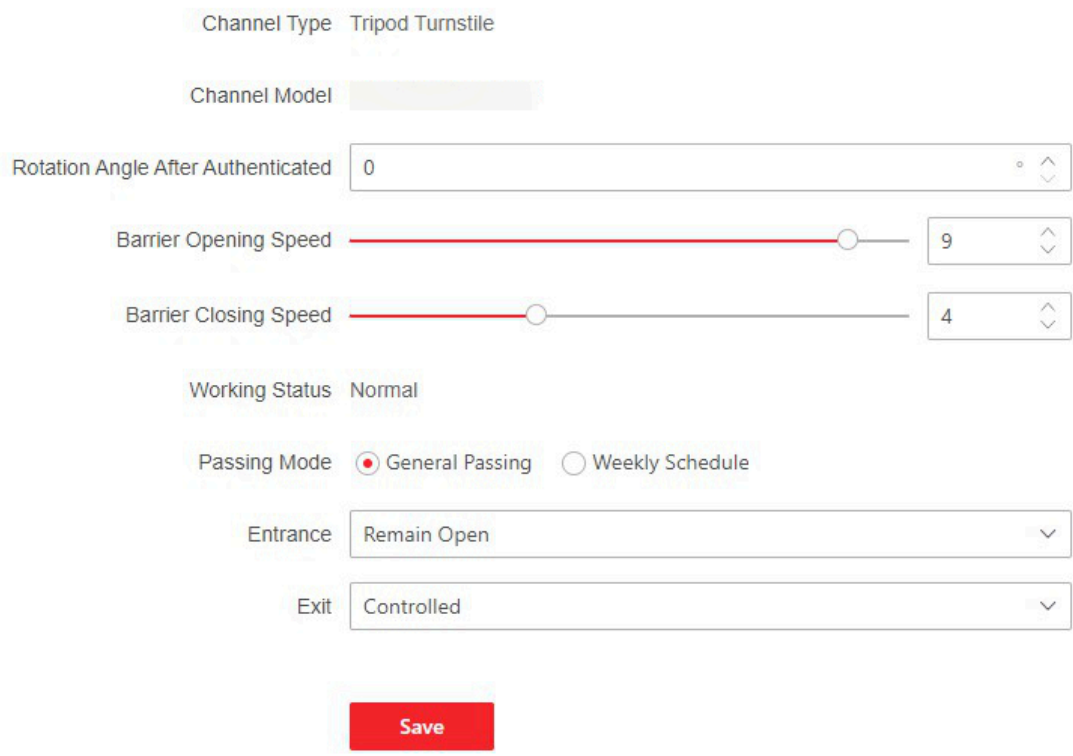


Figure 6-4 Basic Parameters

2. View the **Channel Type**, **Channel Model** and **Working Status**.
3. Set **Rotation Angle After Authenticated**. When authenticated, the arm will rotate the degree to inform users.
4. Set **Barrier Opening Speed** and **Barrier Closing Speed**.
5. Set the passing mode.
   - If you choose **General Passing**, you can select the barrier status for the entrance and exit from the drop-down list.
   - If you choose **Weekly Schedule**, you can set a weekly schedule for entrance and exit barriers.
6. Click **Save**.

Keyfob Settings

Set keyfob parameters.

Steps

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

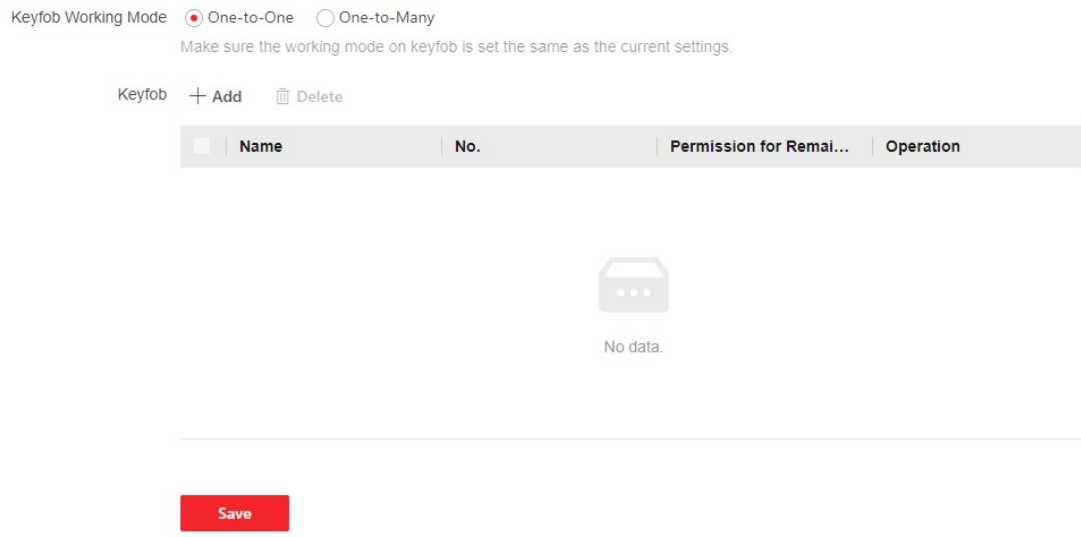


Figure 6-5 Keyfob Settings

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

People Counting

Set people counting.

Steps

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

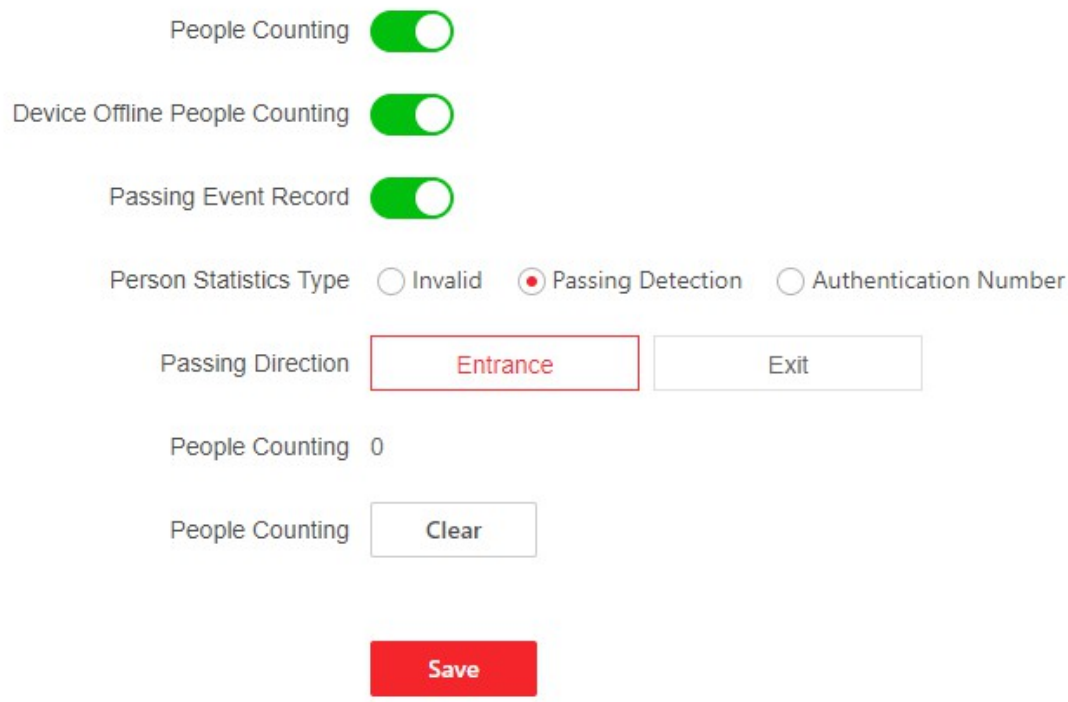


Figure 6-6 People Counting

2. Enable **People Counting**.
3. Enable **Device Offline People Counting**, the device will count people numbers even if it is offline.
4. Select **People Statistics Type**.

   Invalid

   Disable people counting.

   Passing Detection

   The number of all passing people, including remote barrier open, authentication verified open, free open, etc.

   Authentication Number

   The number of passing people verified through card swiping, face recognition, etc.
5. Select passing direction and view people counting results of entrance or exit.
6. **Optional:** Click **Clear** to clear all the people counting information.

Set Light

Set the lane status indicator and barrier light for the device.

Steps

1. Click **Turnstile → Turnstile Configuration → Light Settings** to enter the page.
2. Set light color for lane status indicator.

1) Drag the block or enter the value to adjust the light brightness manually.
2) Set color for remain open, remain closed and controlled.

3. Click **Save**.

Other Settings

Set other parameters.

Steps

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

Alarm Output Duration

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

Temperature Unit

Select unit.

Light Board Brightness

Drag the block or enter the value to adjust the brightness. The larger the value, the brighter the light becomes.

Alarm Buzzing Duration

Set the duration of alarm sound.

Inductive Passing Mode

When enabled, the arm will rotate automatically when the infrared detector on one side of the turnstile is triggered.

Memory Mode

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

Fire Input Type

In the normally open state, closing triggers fire protection. In the normally closed state, disconnection triggers fire protection.

Anti-Reversal

When enabled, the arm cannot be reversed. When disabled, people can reverse the arm up to 38° after entering the lane.

3. Click **Save**.

6.7 System and Maintenance

You can view the system information and the capacity. You can also upgrade the device, restore to factory settings, restore to default settings, and reboot the device.

6.7.1 View Device Information

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

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

You can view the language, model, serial No., version, IO input, IO output, alarm input and alarm output number.

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

Click **Upgrade** to upgrade the firmware version.

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

6.7.2 Set Time

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

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

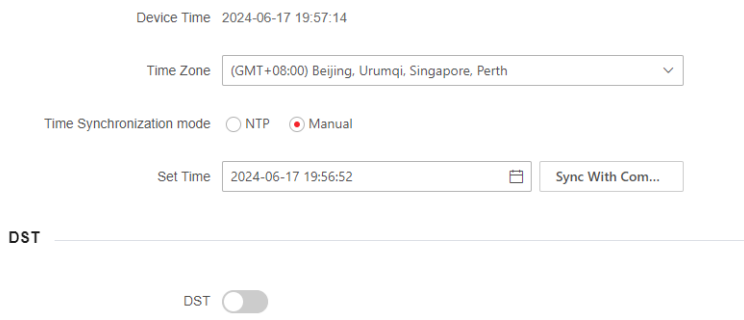


Figure 6-7 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

DST

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

6.7.3 Change Administrator's Password

Steps

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

Caution

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

6.7.4 Online Users

The information of users logging into the device is shown.

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

6.7.5 View Device Arming/Disarming Information

View device arming type and arming IP address.

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

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

6.7.6 Set Working Mode via PC Web

You can set the working mode for accessing.

Note

Only some models support this function, please refer to the specific device.

Go to **System and Maintenance → System Configuration → System → Working Mode** .

Click**Save** after the mode are configured.

Working Mode

You can set the working mode as permission free mode or access control mode.

Permission Free Mode

When accessing, the device only judge the card or ID card is in the valid duration, and will not authenticate the card or ID card's permission.

Access Control Mode

The access control mode is the device normal mode. You should authenticate your credential for accessing.

6.7.7 Network Settings

Set Basic Network Parameters

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

You can view the mac address and MTU.

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

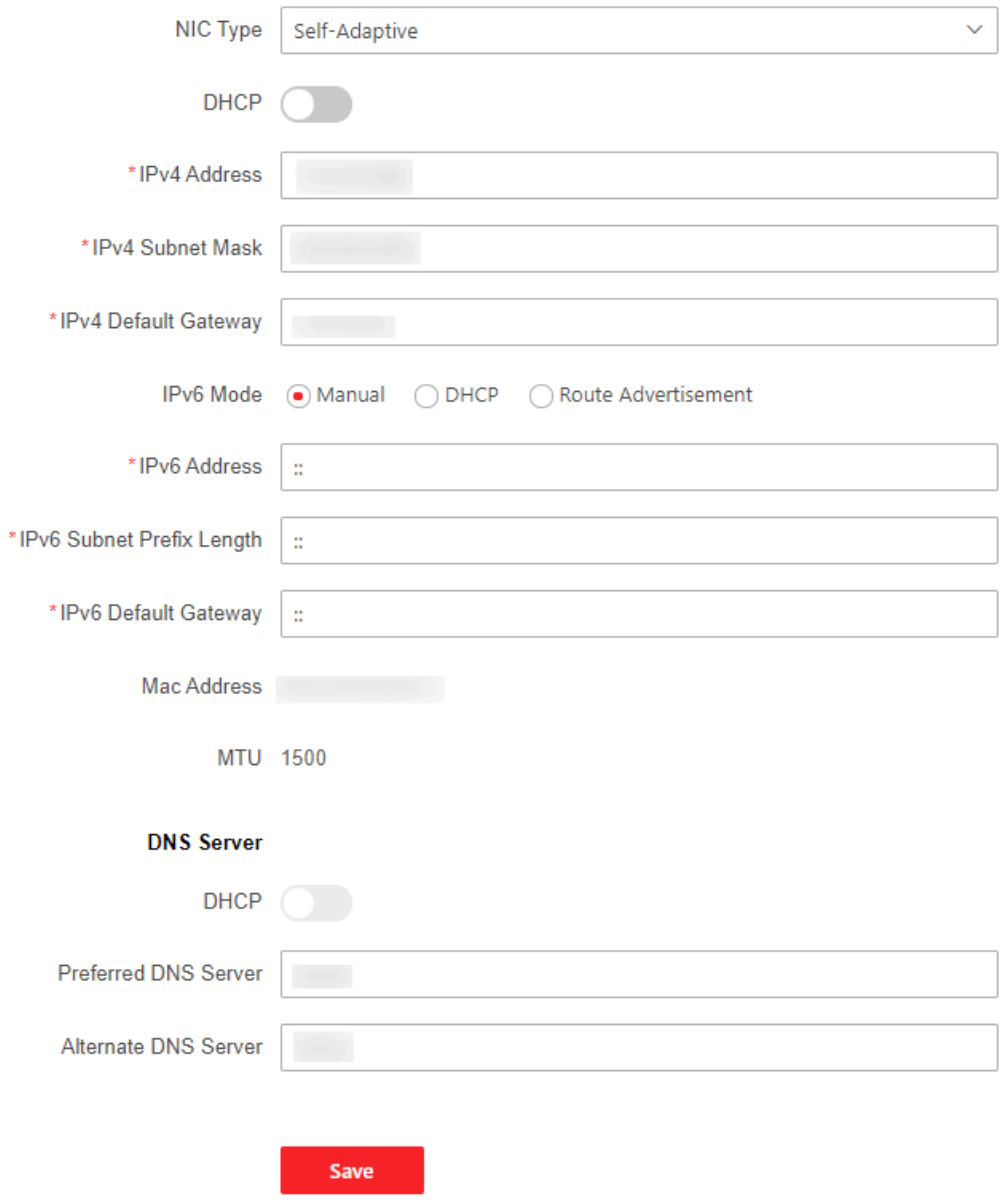


Figure 6-8 Set TCP/IP

NIC Type

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

DHCP

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

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

IPv6 Mode

Manual

Set the IPv6 address, IPv6 subnet prefix length and IPv6 default gateway manually.

DHCP

The system will allocate the IPv6 address, IPv6 subnet prefix length and IPv6 default gateway automatically.

Route Advertisement

A mechanism for automatic address configuration in the IPv6 protocol stack. The device can complete IPv6 address configuration as long as there are routers in the environment that can provide routing notification messages.

Click **View Route Advertisement** to view the IPv6 address list.

DNS Server

Note

Only when DHCP is enabled can DNS server be set.

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

Set Port via PC Web

Click **System and Maintenance → System Configuration → Network → Network Service** .

HTTP

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

HTTPS

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

HTTP Listening

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

Note

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

Set ISUP Parameters via PC Web

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Click **System and Maintenance → System Configuration → Network → Device Access → ISUP** .
2. Check **Enable**.
3. Set the ISUP version, server address, device ID, and the ISUP status.

   Note

   If you select 5.0 as the version, you should set the encryption key as well.
4. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
5. Click **Save**.

Set OTAP via PC Web

Connect the device to the platform through the OTAP protocol to obtain device information, upload operation status and alarm information, restart and upgrade the device.

Steps

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

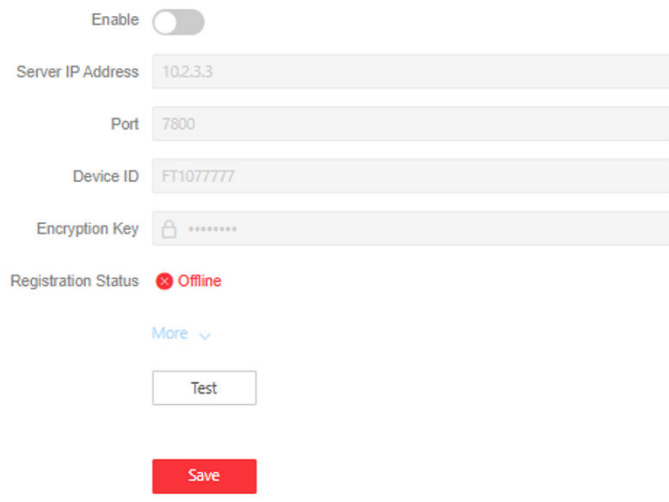


Figure 6-9 Set OTAP

2. Click to **Enable** OTAP.
3. Set **Server IP Address**, **Port**, **Device ID** and **Encryption Key**.
4. Click **More** to view the network type and access priority. Drag the operation icon upward or downward to adjust the network priority.

5. Click **Test** to ensure the device can connect to the server and register successfully. Refresh the page or restart the device to see the **Register Status**.
6. Click **Save**.

Platform Access via PC Web

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

Steps

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

   Note

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

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. **Optional:** Check **Enable** to enable video encryption, set an encryption password and confirm it.
6. Click **More** to view the network type and access priority. Drag the operation icon upward or downward to adjust the network priority.
7. Click **View** to view device QR code. Scan the QR code to bind the account.

   Note

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

8. Click **Save** to enable the settings.

6.7.8 Set Wiegand Parameters via PC Web

You can set the Wiegand transmission direction.

Steps

Note

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

1. Click **System and Maintenance → System Configuration → Access Configuration → Wiegand Settings** .

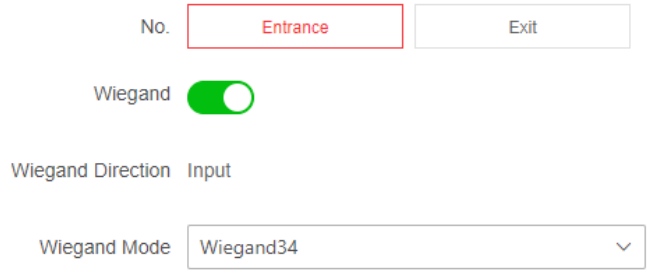


Figure 6-10 Wiegand Page

2. Select **Entrance** or **Exit** as the card reader's direction.
3. Enable **Wiegand** to enable the Wiegand function.
4. Set a transmission direction.

   Input

   The device can connect a Wiegand card reader.
5. Select **Wiegand Mode** from the drop-down list.
6. Click **Save**.

Note

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

6.7.9 Serial Port Settings

Set serial port parameters.

Steps

1. Click **System and Maintenance → System Configuration → Access Configuration → Serial Port Configuration** .

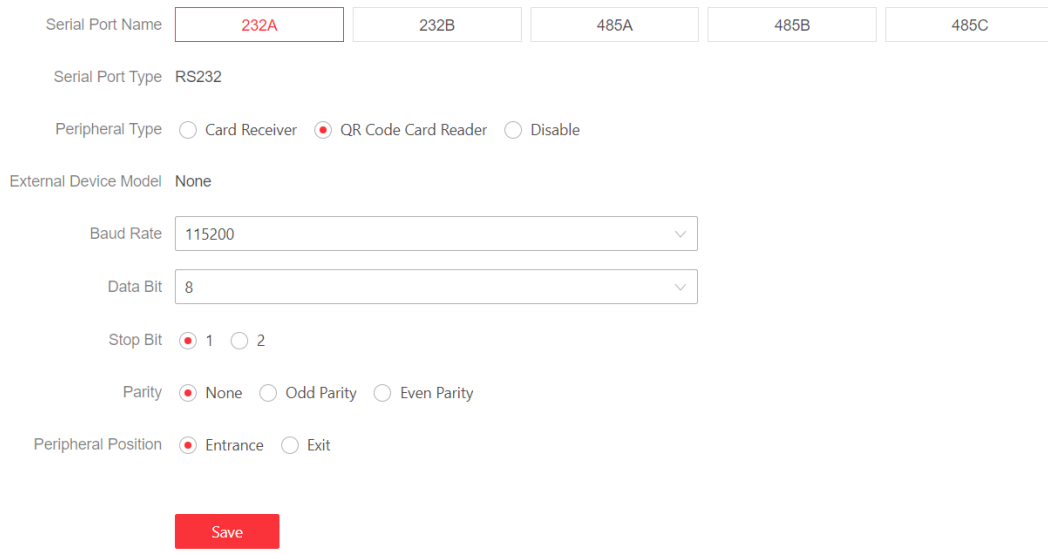


Figure 6-11 Serial Port Configuration

2. Select a serial port name, and the corresponding serial port type will display automatically.
3. Set the **Peripheral Type**.
4. Set the serial port parameters.

   Baud Rate

   Configure data transfer rate.

   Data Bit

   Configure the number of bits to send data.

   Stop Bit

   Select the end point for one frame of data.

   Parity

   Select the serial communication error detection principle. You can choose to detect that the number of 1 of the data bits and check digits is odd or even, or that there is no check digit.
5. Set the **Peripheral Position** as **Entrance** or **Exit**.
6. You can view the external device model.
7. Click **Save**.

6.7.10 Set Audio Parameters on PC Web

Steps

1. Click **System and Maintenance → System Configuration → Video/Audio → Audio** .
2. Slide to enable **Enable Voice Prompt** and the voice promt will be on on the device.
3. Set the output volume.

6.7.11 Event Linkage

Set linked actions for events.

Steps

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

   Buzzer Linkage

   Select **Start Buzzing** or **Stop Buzzing**. When an alarm is triggered, the buzzer will be started or stopped.

   Door Linkage

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

   Linked Alarm Output

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

   Linked Audio Prompt

   Enable **Linked Audio Prompt** and select the play mode.

   - If you choose **TTS**, you need to set language and enter the prompt content.
   - If you choose **Audio File**, you need to select an available audio file from the drop-down list or click **General Linkage Settings** to add a new audio file.

6.7.12 Prompt Schedule

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **System and Maintenance → Preference → Prompt Schedule** .

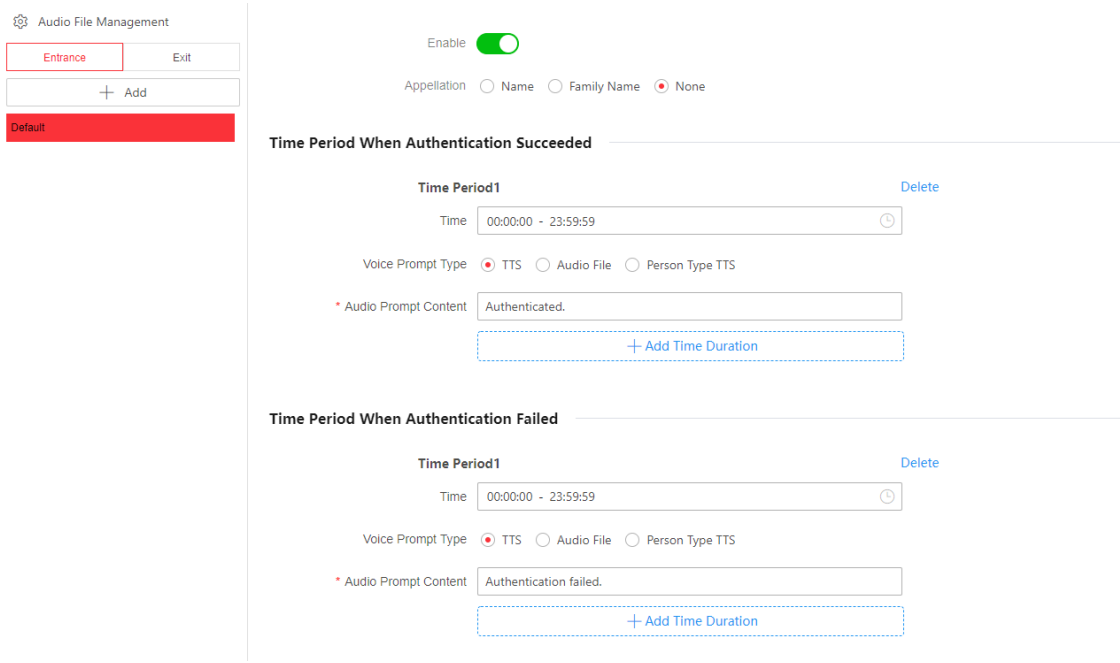


Figure 6-12 Customize Audio Content

2. Select **Entrance** or **Exit** for the settings.
3. Click **+Add** to add a schedule.
4. Enable the function.
5. Set the time period when authentication succeeded.
   1) Click **Add Time Duration**.
   2) Set the time duration.

   Note

   If authentication is succeeded in the configured time duration, the device will broadcast the configured content.

   3) Set the audio content.

   TTS

   If you choose TTS, you need to set the language and enter the prompt content of authentication success.

   Audio File

   If you choose audio file, you need to select an available audio file from the drop-down list or click **Audio File Management** to add a new file.

   Note

   The audio file's format should be wav, and the size should be within 200 KB.

   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click to delete the configured time duration.

6. Set the time duration when authentication failed.
   1) Click **Add**.
   2) Set the time duration.

      Note

      If authentication is failed in the configured time duration, the device will broadcast the configured content.

   3) Set the audio content.

      TTS

      If you choose TTS, you need to set the language and enter the prompt content of authentication failure.

      Audio File

      If you choose audio file, you need to select an available audio file from the drop-down list or click **Audio File Management** to add a new file.

      Note

      The audio file's format should be wav, and the size should be within 200 KB.

   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click to delete the configured time duration.
7. Click **Save** to save the settings.

6.7.13 Maintenance

Reboot

You can reboot the device.

Click **System and Maintenance → Maintenance → Restart** to enter the settings page.

Click **Restart** to reboot the device.

Upgrade

Upgrade Locally via PC Web

You can upgrade the device locally.

Click **System and Maintenance → Maintenance → Upgrade** to enter the settings page.

Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Online Upgrading via PC Web

You can upgrade the device online.

Click **System and Maintenance → Maintenance → Upgarde** to enter the settings page.

Click**Check for Updates**to check whether there is updated versions.

If the device is connected to the network and added to Hik-Connect App, you can tap **Device Upgrade → Online Upgrade** on device for upgrading when there is an updated version in Hik-Connect App.

Restoration

Restore to Factory Settings via Web Browser

You can restore device to factory settings.

Click **System and Maintenance → Maintenance → Backup and Reset** to enter the settings page.

Click **Restore All**, enter the admin password and click **OK**, all parameters will be restored to the factory settings. You should activate the device before usage.

Restore to Default Settings via PC Web

You can restore device to default settings.

Click **System and Maintenance → Maintenance → Backup and Reset** to enter the settings page.

Click **Restore**, enter the admin password and click **OK**, the device will restore to the default settings, except for the device IP address and the user information.

Export Device Parameters via PC Web

Export device parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

Backup

Click **Export** to export device parameters.

Note

Export device parameters and import those parameters to other devices.

Import Device Parameters via PC Web

Import the configuration parameters.

Go to **System and Maintenance → Maintenance → Backup and Reset** .

Import Config File

Click and select a file from local PC. Click **Import**.

6.7.14 Device Debugging

You can set device debugging parameters.

Steps

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

Enable SSH

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

Print Log

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

Capture Network Packet

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

Debug Command Management

Select the command type **Quick Command** or enter the content of **Custom Command**.

Select the board type from the drop-down list, click **Send** to send the debug command, you can view the received command information of the device in **Execution Result**.

Click **End Debugging**, the device restores to normal operation status.

Note

- To ensure the device performance, please click **End Debugging** to close the Debugging command
- If you do not tap **End Debugging**, the device will end the debugging mode within 7×24 hours automatically.

6.7.15 Motor Learning

You can set the lane studying and motor seft-test function.

Click **System and Maintenance → Maintenance → Device Debugging → Motor Learning** .

Lane Studying

Click **Start**, the device will enter the studying mode. It will study the closed position of the barrier.

Motor Self-Test

Click **Start**, the motor will test the operation status automatically.

Encoder Self-Test

Select a channel (lane), and click **Start**, the encoder of the selected lane will test the operation status automatically.

6.7.16 Test Protocol via PC Web

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **System and Maintenance → Maintenance → Device Debugging → Protocol Testing**.

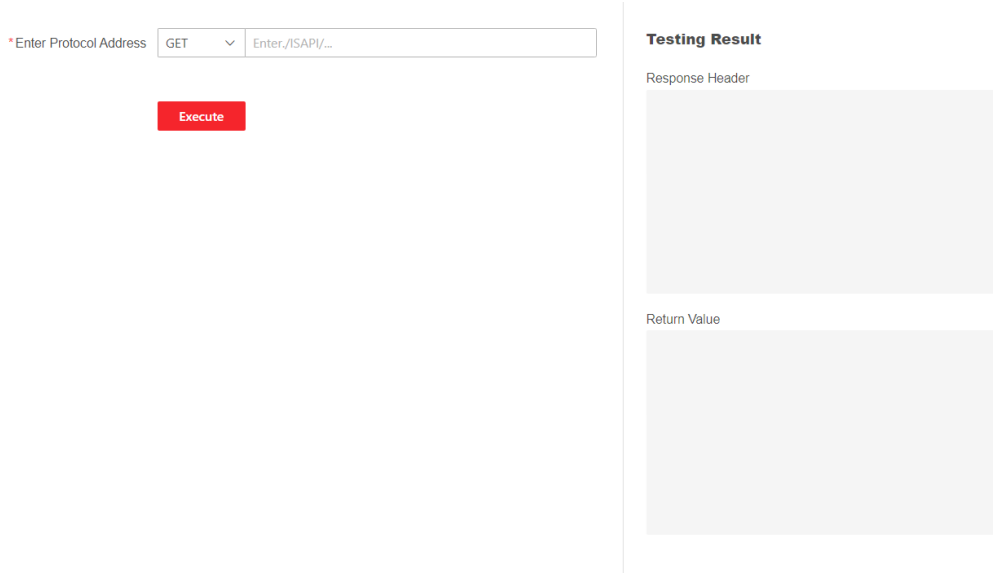


Figure 6-13 Protocol Testing

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

6.7.17 Set Network Penetration Service via PC Web

When the devcie is deployed in the LAN, you can enable the penetration service to realize device remote management.

Steps

1. Go to **System and Maintenance → Maintenance → Device Debugging → Network Penetration Service**.
2. Slide **Enable Penetration Service**.
3. Set **Server IP Address** and **Server Port**. Create **User Name** and **Password**.
4. **Optional:** You can set **Heartbeat Timeout**. The value range is 1 to 6000.
5. **Optional:** You can view the status of the penetration service. Click **Refresh** to refresh the status.
6. Click **Save**.

Note

The penetration service will auto disabled after 48 h.

6.7.18 Component Status

You can view the status of different components.

Main Lane Status

Device Component

You can view the status of the access control board, lane control board, etc.

Peripheral

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

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Others

Passing Mode

You can view the entrance and exit mode.

Input and Output Status

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

Other Status

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

6.7.19 View Log via PC Web

You can search and view the device logs.

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

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

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

6.7.20 Certificate Management

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

Note

The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

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

Create and Import SYSLOG Certificate

Steps

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

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

   Note

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

Chapter 7 Configure the Device via the Mobile Web

7.1 Login

You can login via mobile browser.

Note

Make sure the device is activated.

Enter the device IP address in the address bar of the mobile browser and press **Enter** to enter the login page.

Enter the device user name and the password. Click **Login**.

7.2 Overview

You can view the device status, conduct remote control, etc.

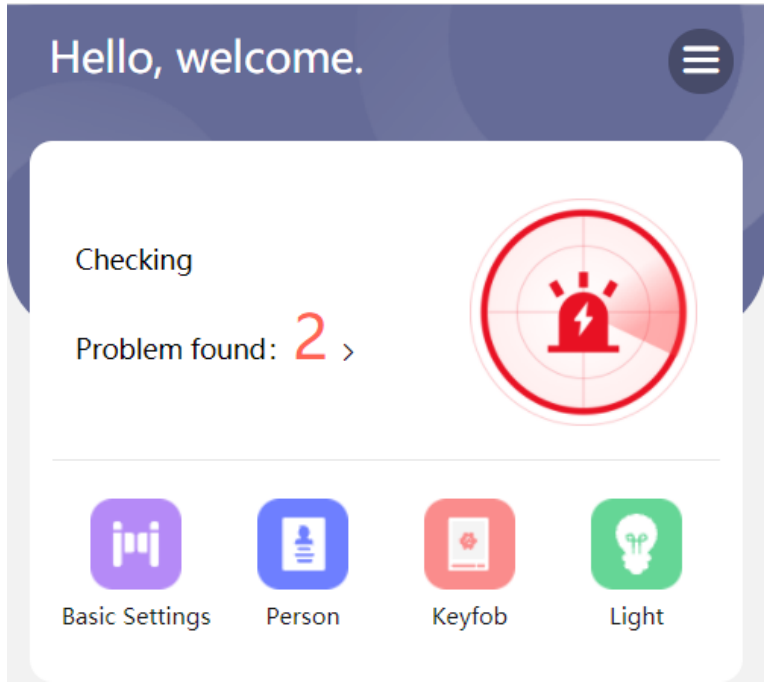


Figure 7-1 Status and Quick Settings

You can view the device status. If there is exception, you can tap to view the component details.

You can tap to fast enter the basic settings page, person page, device page and light page.

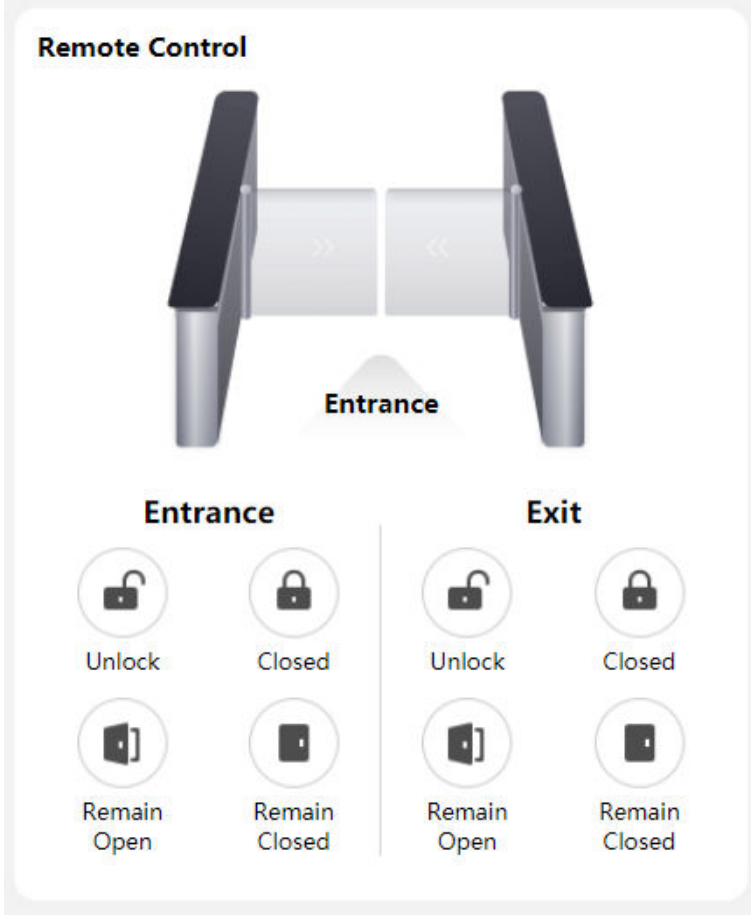


Figure 7-2 Remote Control

You can remotely control barrier by tap the icons.

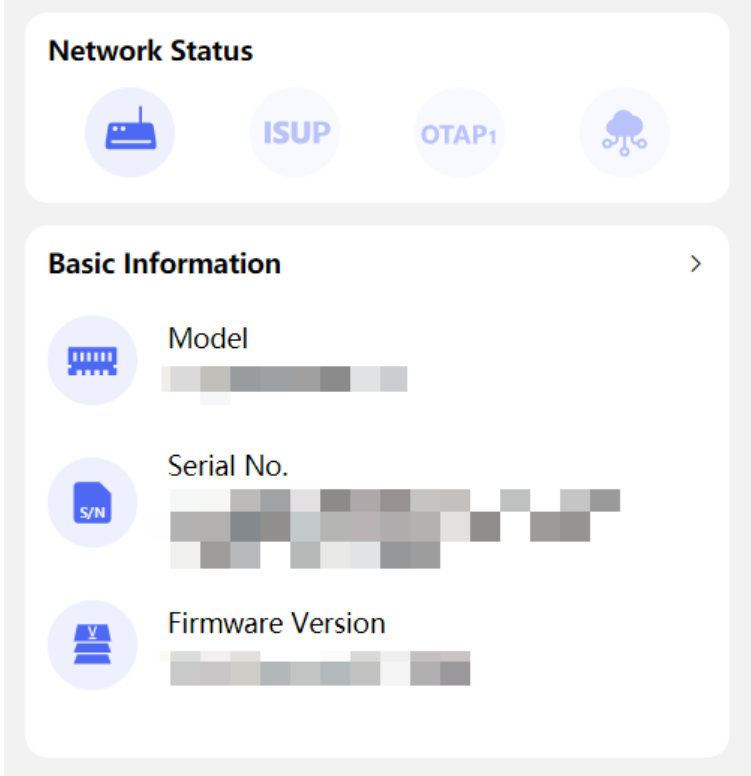


Figure 7-3 Network Status and Basic Information

You can view network status, model, serial No. and firmware version, and you can tap to fast enter the basic information page.

7.3 Configuration

7.3.1 Turnstile Basic Settings

You can set the basic parameters of the turnstile.

Tap **Basic Settings** of the shortcut entry on the overview page or tap → **Basic Settings** .

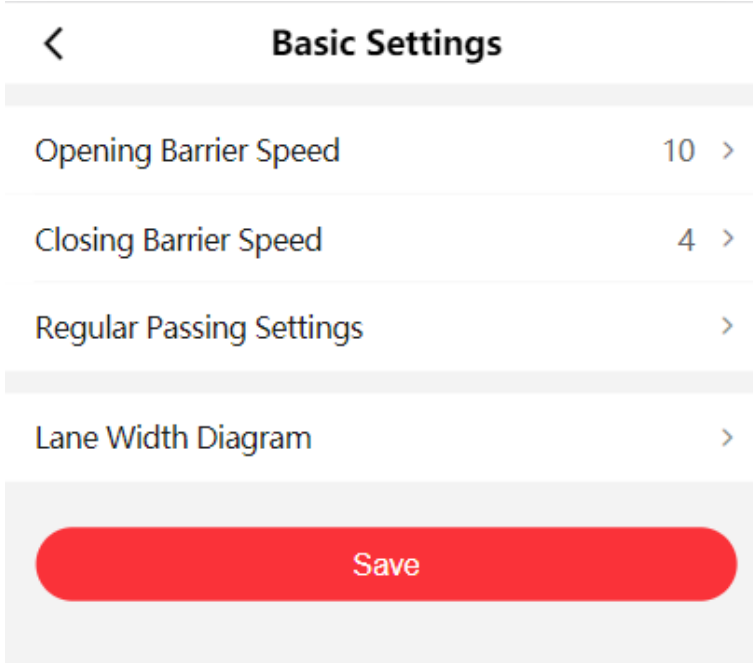


Figure 7-4 Turnstile Basic Parameters

Set **Lane Width**, **Opening Barrier Speed** and **Closing Barrier Speed**.

Tap **Regular Passing Settings** to set the entrance and exit's passing mode.

Tap **Lane Width Diagram** to view the device diagram.

Tap **Save**.

7.3.2 Person Management

Tap **Person** or tap → **Person Management** to enter the page.

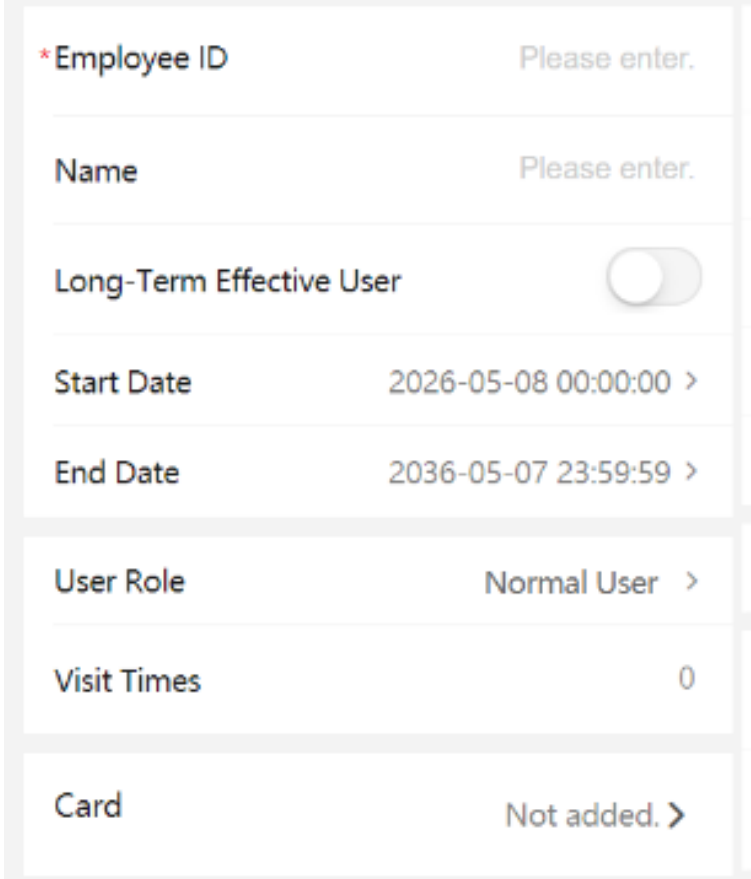


Figure 7-5 Person Management

Add Person Basic Information

On the person management page, tap **+**.
Create the person's employee ID, name, and select a user role.
If you select **Normal User** or **Visitor** as the user role, you can set **Visit Times** for the user. The user can only enter the device for the configured times.
Tap **Save**.

Add Card

On the person management page, tap **+ → Card**.
Tap **+**, enter the card No. and select a card property (type).
Tap **Save**.

Set Person Permission

On the person management page, tap **+**.
Enable **Long-Term Effective User** and set the start time and end time of the person.
Tap **Save**.

Person Management

Edit the person information on the management page.
Tap a person and edit the information.
Tap **Save**.

7.3.3 Keyfob Settings

Tap **Keyfob** of the shortcut entry on the overview page.

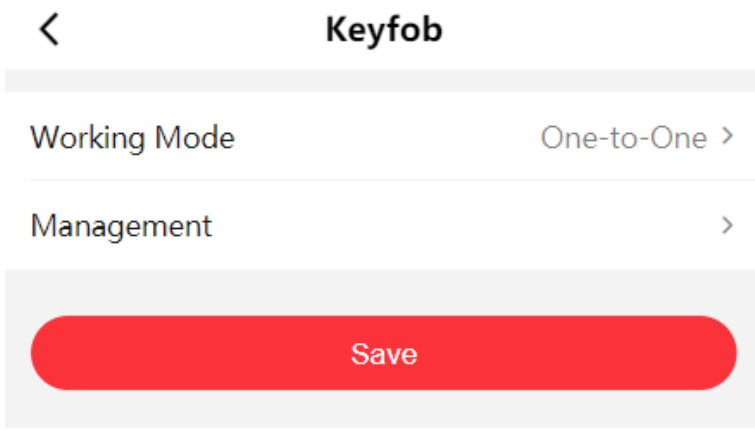


Figure 7-6 Keyfob Settings

Set **Working Mode** as **One-to-One** or **One-to-Many**.

Tap **Management** to enter the page. Tap **+** to add keyfob. Set keyfob name, serial No. and remain open permission.

7.3.4 Light Settings

Tap **Light** of the shortcut entry on the overview page.

Lane Status Indicator

Tap **Side Light** to enter the page.

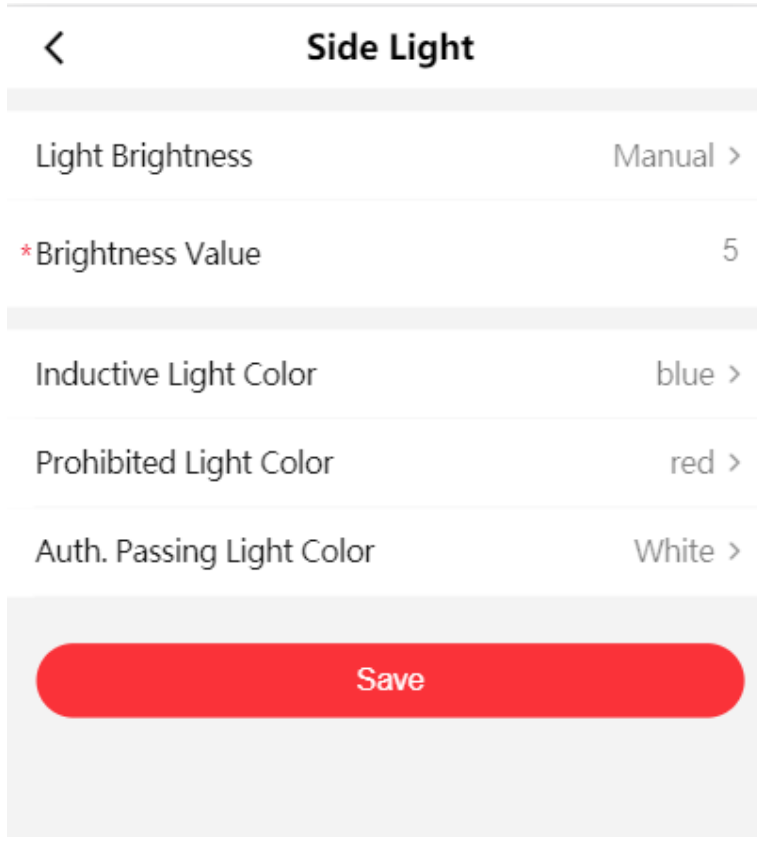


Figure 7-7 Side Light Settings

Set **Light Brightness** as **Auto** or **Fixed Brightness**. If you choose **Fixed Brightness**, you can enter the value to adjust the light brightness manually.
Set inductive, prohibited and Auth. passing light color.

7.3.5 View Device Basic Information

You can view the device name, language, model, serial No., version, and Mac address, etc.

Tap → **System Settings** → **Basic Information** .

You can change the device name.

You can view the device language, model, serial No., version, local RS-485 number, number of alarm input, number of alarm output, Mac address and factory information, etc.

Tap **Device Capacity** to view the quantity and capacity of person, card and event.

Tap **Save**.

7.3.6 Time Settings

View current time and set the time zone.

Tap → **System Settings** → **Time Settings** .

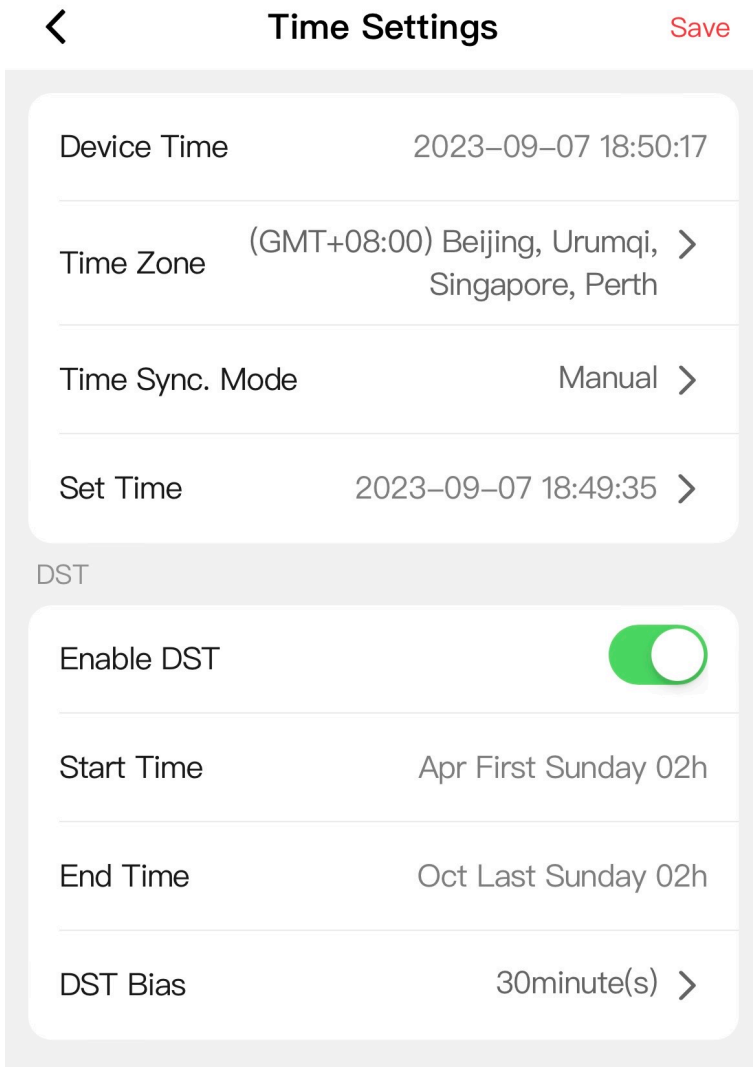


Figure 7-8 Time Settings

Device Time

You can view current time.

Time Zone

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

Time Sync. Mode

Manual

By default, the device time should be synchronized manually. You can set the device time manually.

NTP

Set the NTP server's IP address, port No., and interval.

DST

Slide to enable DST, and set the start time, end time and DST bias.

Tap **Save**.

7.3.7 User Management

You can change user password.

Tap → **User Management** on the home page.

Tap the user, enter the old password and create a new password, and confirm the password.

Tap **Save**.

7.3.8 Network

Wired Network

Set wired network.

Tap → **Network Settings** → **TCP/IP** to enter the configuration page.

NIC Type

Select a NIC type from the drop-down list.

DHCP

If you disable the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, IPv6 mode, IPv6 address, IPv6 subnet prefix length, IPv6 default gateway.

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

MAC Address and MTU

You can view the default MAC address and MTU.

IPv6 Mode

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

Manual

Enter **IPv6 Address**, **IPv6 Subnet Mask**, and **IPv6 Default Gateway**. Consult the network administrator for required information.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

DNS Server

Note

Only when DHCP is enabled can DNS server be set.

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

Set Port Parameters

You can set the HTTP, HTTPS according to actual needs when accessing the device via network.

Tap → **Network Service** → **HTTP(S)** to enter the setting page.

HTTP

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

HTTPS

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

Platform Access

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

Steps

1. Tap → **Device Access** → **Hik-Connect** to enter the settings page.

   Note

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

2. Slide to enable the function.
3. You can enable **Custom** to enter the server address.

Note

- 6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

4. You can view **Register Status** and **Binding Status**.
5. You can tap **Bind An Account → View QR Code** , scan the QR code to bind an acount.
6. Tap **Save** to enable the settings.

Set ISUP Parameters

Set the ISUP parameters for transmitting logs via ISUP protocol.

Tap → **Device Access → ISUP**.

Slide **Enable** to enable ISUP.

Set the server address and port.

Note

The protocol version is 5.0, you should set the encryption key.

Tap **Save**.

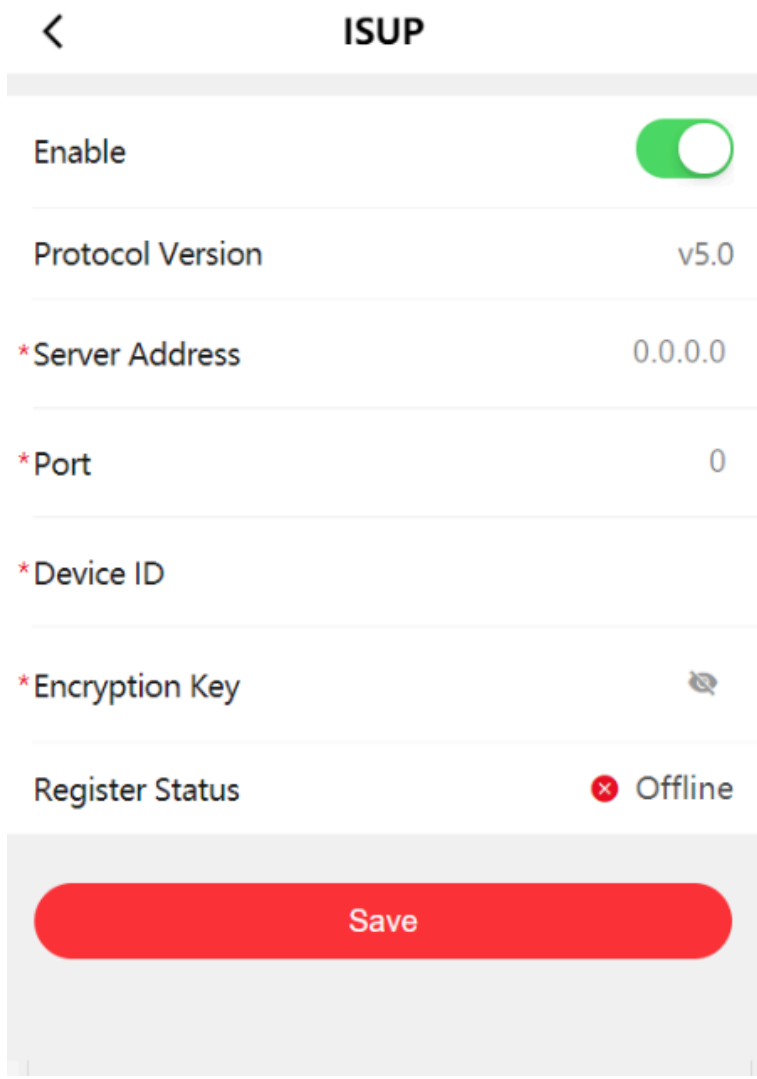


Figure 7-9 ISUP Settings Page

Set OTAP Protocol

You can access the device to the maintenance platform by OTAP protocol to realize searching and gaining device information, uploading device running status and exceptions, rebooting and upgrading.

Steps

1. Tap → **Device Access** → **OTAP** .

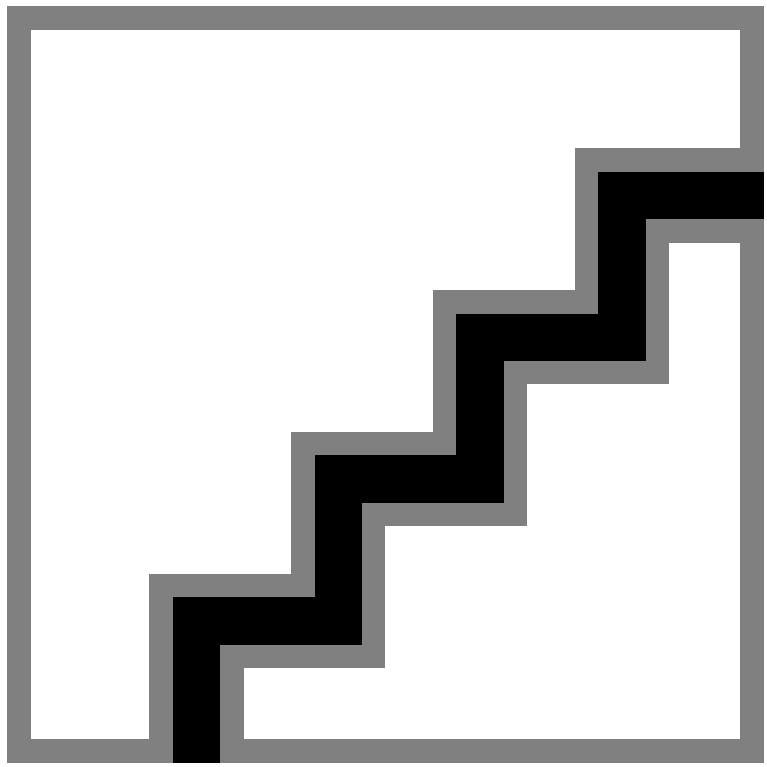


Figure 7-10 OTAP

2. Slide **Enable**.
3. Set server address, port, device ID and encryption key.
4. Tap **Test**, and make sure the device can connect to the server and registration completed.
5. Tap **Save**.

Result

Refresh the web page or reboot the device to make sure the OTAP's **Register Status** turns to online.

Set Network Penetration Service

When the device is deployed on the LAN, penetration service can be enabled to achieve remote device management.

Steps

1. Tap → **Device Access** → **Network Penetration Settings** to enter the configuration page.
2. Enable **Enable Penetration Service**.
3. Enter **Server IP Address** and **Server Port**.
4. Enter login **User** and **Password**.
5. Set **Heartbeat Timeout**. The range is1 to 6000.
6. You can view **Online Status**. Click **Refresh** to view the latest status.

7. Tap **Save**.

7.3.9 Event Search

Tap → **Event Search**.

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

Note

Support searching for names within 32 digits.

The result will display in the list.

7.3.10 Audio Settings

You can enable or adjust the audio.

Tap → **Audio**.

Enable **Enable Voice Prompt** according to actual needs. The device will prompt voice instructions. You can also adjust the audio volume.

7.3.11 Access Control Settings

Set Authentication Parameters

Set authentication parameters.

Steps

1. Tap → **Access Control** → **Authentication Settings**.

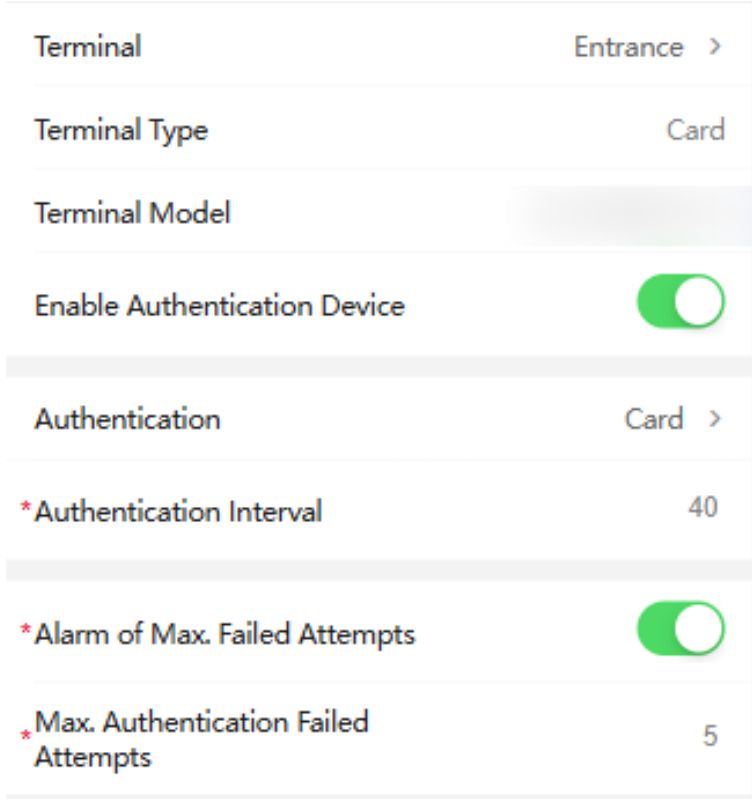


Figure 7-11 Authentication Settings

2. After settings, tap **Save**.

Terminal

Select terminal for settings.

Terminal Type

Display the terminal's type. Read only.

Terminal Model

When the terminal is online, it will display the terminal's model, or it will display offline. (Read-only)

Enable Authentication Device

If enable the function, you can authenticate credential on the terminal; or you cannot use credential to authenticate.

Authentication

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

Authentication Interval

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

failed. If there is another person authenticate in the configured interval, the person can authenticate again.

Alarm of Max. Failed Attempts/Max. Authentication Failed Attempts

Enable **Alarm of Max. Failed Attempts** and you can set the max. authentication failed attempts. When the authentication attempts reach the set value, the authentication will be failed and report to center.

Set Door Parameters

You can set door name, open duration and exit button parameters.

Tap → **Access Control** → **Door Parameters** .

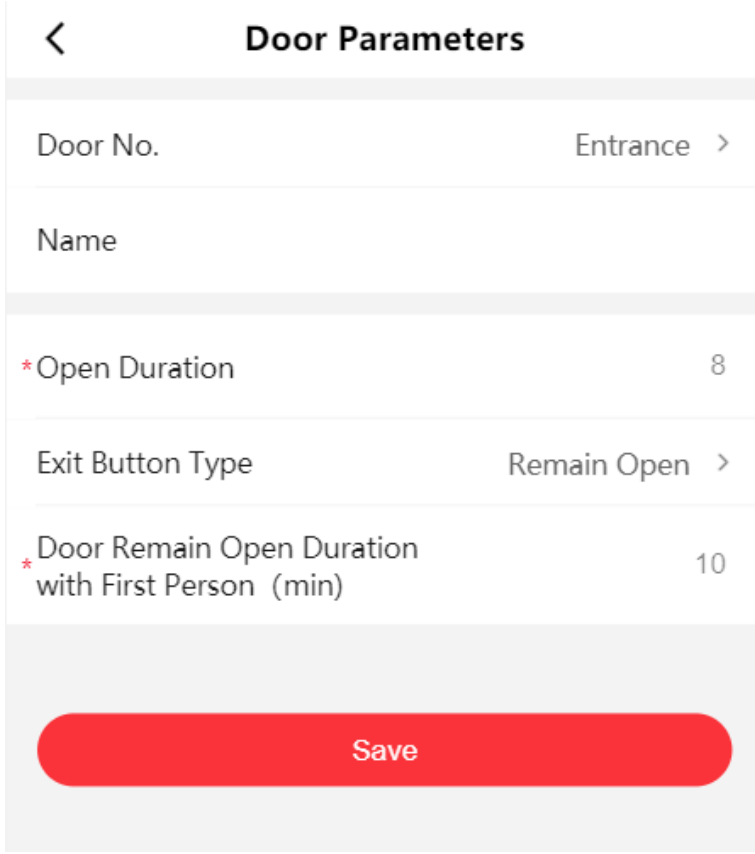


Figure 7-12 Door Parameters

Select entrance or exit for configuration, configure **Name** and **Open Duration**, and select **Exit Button Type**.

Configure **Door Remain Open Duration with First Person**. The mode is applicable for the passing of groups of persons, such as visitors entering the scenic spots. After the set person passes through, the door will open for a set time and other persons can pass through without authentication.

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

Terminal Settings

Set the working mode.

Tap → **Access Control** → **Terminal Parameters** to enter the settings page.

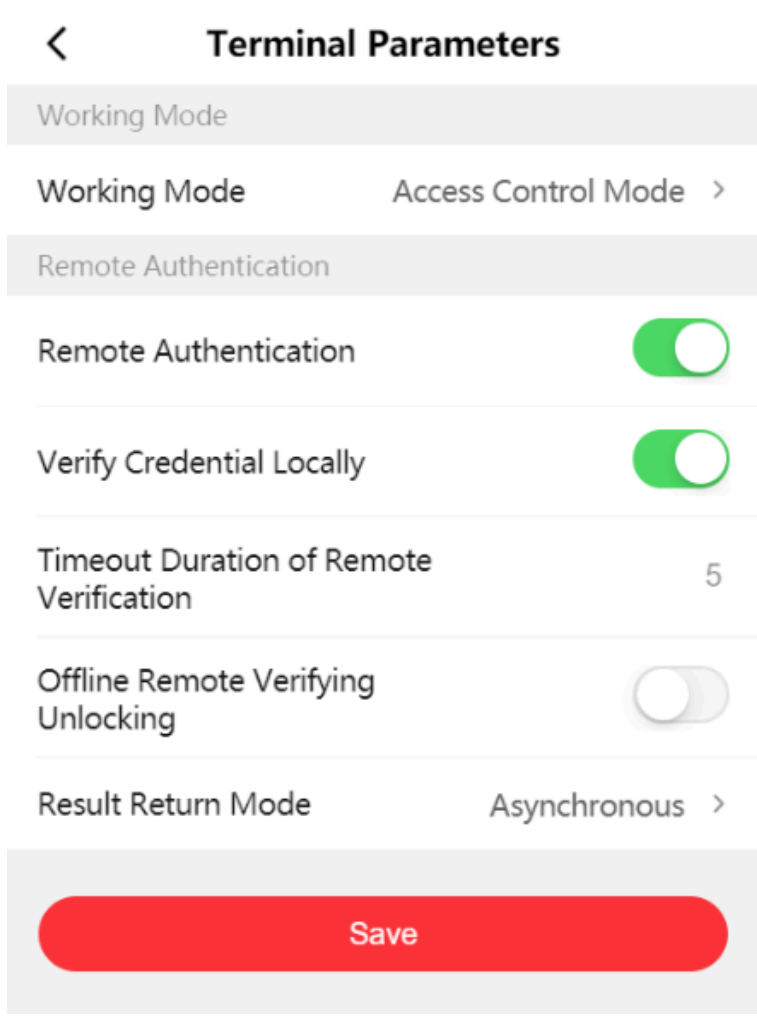


Figure 7-13 Terminal Parameters

Working Mode

Permission Free Mode

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

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

Access Control Mode

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

Remote Authentication

When personnel are authenticated, the device uploads authentication information to the platform, which confirms whether to open the door.

After enabling remote authentication, you can click to enable **Verify Credential Locally**.

Timeout Duration of Remote Verification

If remote verification exceeds the configured time, it will return a timeout.

Offline Remote Verifying Unlocking

When enabled, local authentication will be performed if the platform is offline or a timeout occurs.

Result Return Mode

Set the return mode of remote verification results to **Asynchronous** or **Sync**.

Serial Port Settings

Set serial port parameters.

Steps

1. Tap → **Access Configuration** → **Serial Port Configuration** to enter the setting page.
2. Set the serial port name and view the type.
3. Set the port's parameters

   Baud Rate

   Configure data transfer rate.

   Data Bit

   Configure the number of bits to send data.

   Stop Bit

   Select the end point for one frame of data.

   Parity

   Select the serial communication error detection principle. You can choose to detect that the number of 1 of the data bits and check digits is odd or even, or that there is no check digit.

   Peripheral Type

   Set the **Peripheral Type** the port connected. You can view the connected device model.

   Note

   If select Only effective for the DS-K7CR02 QR code scanner.
4. Click **Save**.

Set Card Security

Configure cards for the device.

Tap → **Access Control** → **Card Security** .

Configure card parameters, and click **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Sector

Enable the function and set the encryption sector.

Note

It is recommended to encrypt sector 13.

Enable EM Card

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

Note

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

Enable DESFire Card

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

DESFire Card Read Content

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

Enable FeliCa Card

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

Card Authentication Mode

You can select the card authentication mode from the drop-down list.

Enable Reversed Card No.

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

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

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

1. Tap → **Access Control** → **Wiegand Settings** .
2. Set Wiegand parameters.

   No.

   Select Wiegand No. for parameters settings.

   Wiegand

   Select to enable the card reader's Wiegand function.

   Wiegand Direction

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

   Wiegand Mode

   Select Wiegand Mode from the drop-down list.
3. Tap **Save** to save the settings.

7.3.12 People Counting Settings

Set people counting.

Steps

1. Tap → **People Counting Settings** to enter the configuration page.
2. Enable **People Counting**, and the devcie will count passing person's number.
3. Enable **Device Offline People Counting**, and the device will count people numbers even if it is offline.
4. Enable **Passing Event Record**, and the device will upload each person's passing event.
5. Set **Person Statistics Type**.

   Invalid

   Disable people counting.

   Passing Detection

   The number of all passing people, including remote barrier open, authentication verified open, free open, etc.

   Authentication Number

   The number of passing people verified through credential authentication.
6. Set **Passing Direction** and you can set the passing direction of the device.

7. Tap **Clear** to clear all people counting information.
8. Tap **Save**.

7.3.13 Other Settings

Tap → **Other Settings** to enter the configuration page.

Set the parameters and tap **Save**.

Alarm Output Duration

Set the alarm output device's output duration. The alarm output duration ranges from 0 s to 3599 s. 0 means continuous output.

Temperature Unit

Select the temperature unit.

Light Board Brightness

Drag the block or enter the value to adjust the brightness. The larger the value, the brighter the light becomes.

Anti-Passback Rule

Set the anti-passback rule as **By Authentication Status** or **By Passing Status**.

By Authentication Status

The person should pass the authentication or the anti-passback will be failed.

By Passing Status

The person cannot pass the authentication and the anti-passback will be completed.

Memory Mode

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

Fire Input Type

In the normally open state, closing triggers fire protection. In the normally closed state, disconnection triggers fire protection.

7.3.14 Upgrade and Maintenance

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

Restart Device

Tap → **Restart** .

Tap **Restart** to restart the device.

Upgrade

Tap → **Upgrade** .
Tap **Upgrade** to upgrade the device.

Note

Do not power off during the upgrading.

Restore Parameters

Tap → **Default** .

Restore to Default Settings

Tap **Restore to Default Settings**, enter the admin password and click **OK**. The device will restore to the default settings, except for the device IP address and the user information.

Restore to Factory Settings

Tap **Restore to Factory Settings**, enter the admin password and click **OK**. All parameters will be restored to the factory settings. You should activate the device before usage.

Log Export

Tap → **Log Export** .
Select the log type, and tap **Export** to download the maintenance log.

7.3.15 Device Debugging

You can finish studying and self-test, and mange the debugging.

Tap → **Device Debugging** .

Lane Studying/Motor Self-Test

Lane Studying

Tap **Lane Studying**, and the device will enter the studying mode. It will study the closed position of the barrier.

Motor Self-Test

Tap **Motor Self-Test**, and the device motor will start self-test.

Encoder Self-Test

1. Select a lane and start encode test.
2. Make sure the barrier is in the close position. Tap **OK**.
3. Rotate the barrier to the open position. Tap **Stop Testing**.
4. Wait for the result.

Debugging Command Management

Select a command type and select the command or tap the command manually. Tap **Send**. The command will send to the device.

When the command is complete, you can see the result in the page.

Tap **End Debugging** to finish the debugging.

Note

If you do not tap End Debugging, the device will end the debugging mode within 7×24 hours automatically.

7.3.16 View User Document

View the user document.

Note

Only when you enter the mobile web by IP address, can you view the user document. Login by hot spot does not support the function.

Tap ☰ to enter the page.

Tap **View Online Document** to view the user manual.

7.3.17 Open Source Software Licenses

You can view the open source software licenses.

Tap ☰ to enter the page.

Tap **Open Source Software Licenses**.

7.3.18 Log Out

Log out the configuration page.

Tap ☰ → **Logout** , tap **OK**.

If you need to enter the configuration page, you need to enter the user name and password again.

Chapter 8 Other Platforms to Configure

You can also configure the device via iVMS-4200 Client Software or HikCentral Access Control. For details, see the platforms' user manual.

iVMS-4200 Client Software

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

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

Appendix A. DIP Switch

A.1 DIP Switch Description

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

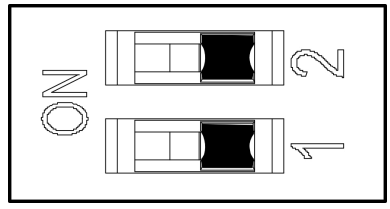
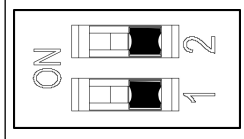
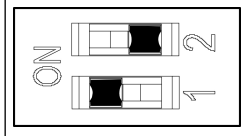
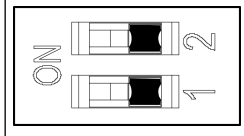
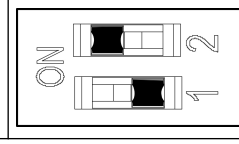


Figure A-1 DIP Switch

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

A.2 DIP Switch Corresponded Functions

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

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

Appendix B. Button Configuration Description

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

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions
1	Study Mode	1-Exit Study Mode/Normal Mode 2-Study Mode **Note** By default, 1 will be displayed on the display screen.
2	keyfob Pairing Mode	1-Normal Mode 2-Pairing Mode **Note** By default, 1 will be displayed on the display screen.
3	Passing Mode	1-Both sides under control **Note** By default, 1 will be displayed on the display screen. 2-Entrance under control; exit prohibited 3-Entrance under control; exit free 4-Both sides free 5-Entrance free; exit under control 6-Entrance free; exit prohibited 7-Both sides prohibited 8-Entrance prohibited; exit under control 9-Entrance prohibited; exit free

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions
4	Memory Mode	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.
5	keyfob Remote Control	1-one to one 2-one to multiple **Note** By default, 1 will be displayed on the display screen.
9	Enter Duration	5-5s，6-6s，7-7s, ..., 60-60s **Note** By default, 5 will be displayed on the display screen.
10	Exit Duration	5-5s，6-6s，7-7s, ..., 60-60s **Note** By default, 5 will be displayed on the display screen.
39	Brightness of Light	0-0，1-1，2-2, … , 10-10 **Note** By default, 6 will be displayed on the display screen.
42	Clearing People Counting	1-Default 2-Enable **Note** By default, 1 will be displayed on the display screen.
43	Fire Protection Type	1-Remain Closed

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions
		2-Remain Open **Note** By default, 2 will be displayed on the display screen.
99	Restore to Default	1-Default 2-Enable **Note** By default, 1 will be displayed on the display screen.

Appendix C. Event and Alarm Type

Event	Alarm Type
Force Accessing	None
Climb over Arm	Visual and Audible
Passing Timeout	None
Arm Obstructed	None

Appendix D. Table of Audio Index Related Content

Index	Content
1	Authenticated.
2	Card No. does not exist.
3	Climbing over the barrier.
4	Passing timeout.
5	Force accessing.
6	No permissions.
7	Authentication time out.
8	Authentication failed.
9	Expired card.

Appendix E. Error Code Description

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

Error Reason	Code	Error Reason	Code
First IR Beam Triggered	01	Second IR Beam Triggered	02
Optional Board Offline (If the board is not installed, the error code of "49" will appear but the device functions normally)	49		
Not Studying	54	Barrier Obstruction	55
Exceeding Studying Range	56	Encoder Offline	57
Motor Offline	58	Motor Drive Fault	64
Motor Fault	66	Motor Over-current	68
Motor Under-voltage	69	Motor Over-voltage	70
Motor Arm Opening Timeout	74	Motor Encoder Exception	76


See Far, Go Further