DS-K3H4210(L)X Series Full Height 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.
- Do not touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- This equipment is not suitable for use in locations where children are likely to be present.
- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
  If the top caps should be open and the device should be powered on for maintenance, make sure:
  1. Power off the fan to prevent the operator from getting injured accidentally.
  2. Do not touch bare high-voltage components.
  3. Make sure the switch's wiring sequence is correct after maintenance.
- 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.
- Risk of explosion if the battery is replaced by an incorrect type.
  Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
  Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.

Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
Dispose of used batteries according to the instructions.

- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- Ensure correct wiring of the terminals for connection to an AC mains supply.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The serial port of the equipment is used for debugging only.
- Stainless steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

Available Models

Product Name	Model
Full Height Turnstile	DS-K3H4210LX Series
	DS-K3H4210X Series

Contents

Chapter 1 System Wiring 1

Chapter 2 Installation 2

Chapter 3 General Wiring 4

3.1 Components Introduction 4

3.2 Terminal Description 5

3.2.1 General Wiring 5

3.2.2 Connect Protective Ground Wire 6

3.2.3 Lane Control Board Terminal Description 9

3.2.4 Access Board Terminal Description (Optional) 10

3.2.5 Optional Board Terminal Description 12

3.2.6 Card Reader 13

3.2.7 RS-485 Wiring 14

3.2.8 Face Recognition Module Wiring 15

3.2.9 Loudspeaker Wiring 16

3.2.10 Alarm Input Wiring 18

3.2.11 Exit Button Wiring 18

3.2.12 Change From Normally Open (NO) to Normally Closed (NC) When Powering Off ... 19

3.3 Device Settings via Button 20

3.3.1 Configuration via Button 20

3.3.2 Initialize Device 23

3.3.3 Pair Keyfob via Button 23

Chapter 4 Activation 25

4.1 Activate via Web Browser 25

4.2 Activate via Mobile Web 25

4.3 Activate via SADP 27

4.4 Activate Device via iVMS-4200 Client Software 28

Chapter 5 Operation via Web Browser 30
5.1 Login 30
5.2 Forget Password 30
5.3 Quick Operation via Web Browser 30
5.3.1 Time Settings 30
5.4 Overview 31
5.5 Person Management 32
5.6 Turnstile 32
5.6.1 Search Event 32
5.6.2 Access Control Settings 33
5.6.3 Turnstile Configuration 38
5.7 System and Maintenance 43
5.7.1 View Device Information 44
5.7.2 Set Time 44
5.7.3 Change Administrator's Password 45
5.7.4 Online Users 45
5.7.5 View Device Arming/Disarming Information via PC Web 45
5.7.6 Set Working Mode via PC Web 46
5.7.7 Network Settings 46
5.7.8 Set Wiegand Parameters via PC Web 50
5.7.9 Serial Port Settings 51
5.7.10 Set Audio Parameters on PC Web 52
5.7.11 Event Linkage 53
5.7.12 Customize Audio Content 54
5.7.13 Upgrade and Maintenance 55
5.7.14 Device Debugging 56
5.7.15 Test Protocol via PC Web 56
5.7.16 Set Network Penetration Service via PC Web 57

5.7.17 Component Status 57
5.7.18 View Log via PC Web 58
5.7.19 Certificate Management 58
Chapter 6 Configure the Device via the Mobile Web 60
6.1 Login 60
6.2 Overview 60
6.3 Configuration 62
6.3.1 Turnstile Basic Settings 62
6.3.2 Person Management 63
6.3.3 Keyfob Settings 65
6.3.4 View Device Basic Information 65
6.3.5 Set Device Time 65
6.3.6 User Management 67
6.3.7 Network 67
6.3.8 Event Search 70
6.3.9 Audio Settings 70
6.3.10 Access Control Settings 70
6.3.11 People Counting Settings 77
6.3.12 Other Settings 78
6.3.13 Upgrade and Maintenance 79
6.3.14 System Upgrade & Maintenance 79
6.3.15 Device Debugging 80
6.3.16 View User Document 80
6.3.17 Open Source Software Licenses 80
6.3.18 Log Out 81
Chapter 7 Other Platforms to Configure 82
Appendix A. Stainless Steel Maintenance 83
Appendix B. Button Configuration Description 84

Appendix C. Event and Alarm Type 88

Appendix D. Table of Audio Index Related Content 89

Appendix E. Error Code Description 90

Chapter 1 System Wiring

The preparation before installation and general wiring.

Steps

1. Slot on the installation surface and dig installation holes according to the hole position.
2. Put 15 expansion bolts of M12*150 for each pedestal (4 on post, 3 on rotating pipe in the middle, 4 on each side below the card reader).
3. Bury cables. Each lane buries 1 high voltage cable. For details, see the system wiring diagram.

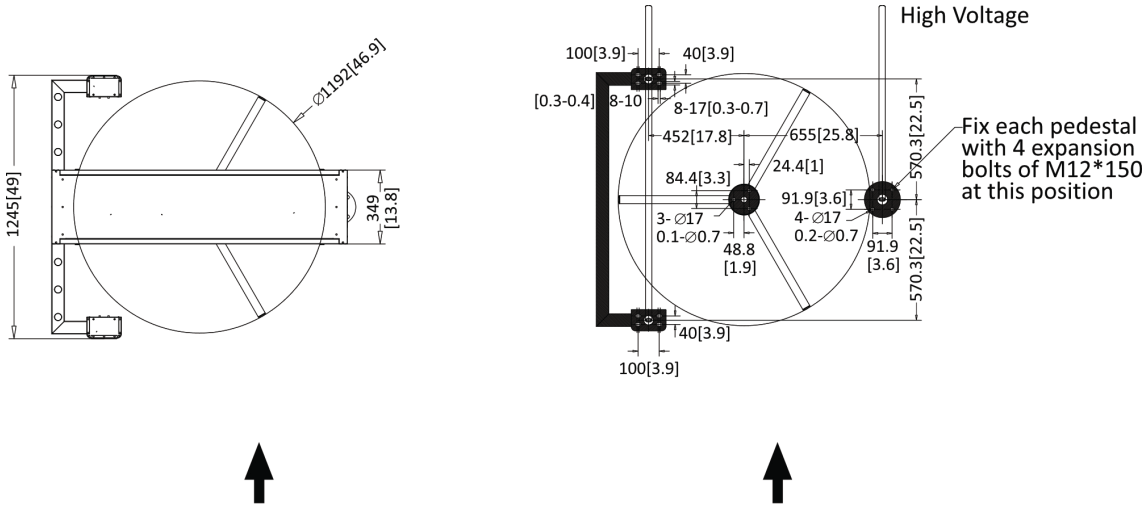


Figure 1-1 System Wiring

Note

- High voltage: AC power input
- The suggested inner diameter of the high voltage conduit is larger than 30 mm.
- The external AC power cord should be double-insulated. The network cable must be CAT5e or the network cable has better performance.
- Before digging holes, evaluate the thickness of the installation surface to avoid puncturing.

Chapter 2 Installation

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.
- To prevent stainless steel from rusting due to dirt during construction, it is recommended that the protective film be removed after the installation is completed. There may be residual adhesive at the film cutting position. It is recommended to use WD-40 protective liquid to wipe after tearing the film.
- Avoid immersing the pedestal in water. Under special circumstances, the immersion height should not exceed 1 m.



Figure 2-1 Dimension

1. Assemble each component according to the video.
2. Prepare installation tools, check the components, and clean the installation base.
3. Seal the bottom of the turnstile to avoid water from entering.
4. Place the pedestals properly on the base, and secure the pedestals with expansion bolts.

Chapter 3 General Wiring

Note

- When you should maintain or disassemble the high voltage modules, you should remove the entire high voltage modules and maintain it outside the turnstile. You should unplug the cables that connected to the peripherals before maintenance to avoid destroy of the device.
- When disassembling the high voltage module, you should disconnect the power to avoid injury.
- If only wiring is needed without maintenance, do not remove the high voltage modules.
- The switch and the main lane control board are already connected. The 14 AWG cable to connect between the AC electric supply and the switch should be purchased separately.

Scan the QR code to view the wiring guide video.

3.1 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 100 VAC and 240 VAC, 50 to 60 Hz.

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

Note

The diagram is for reference only.

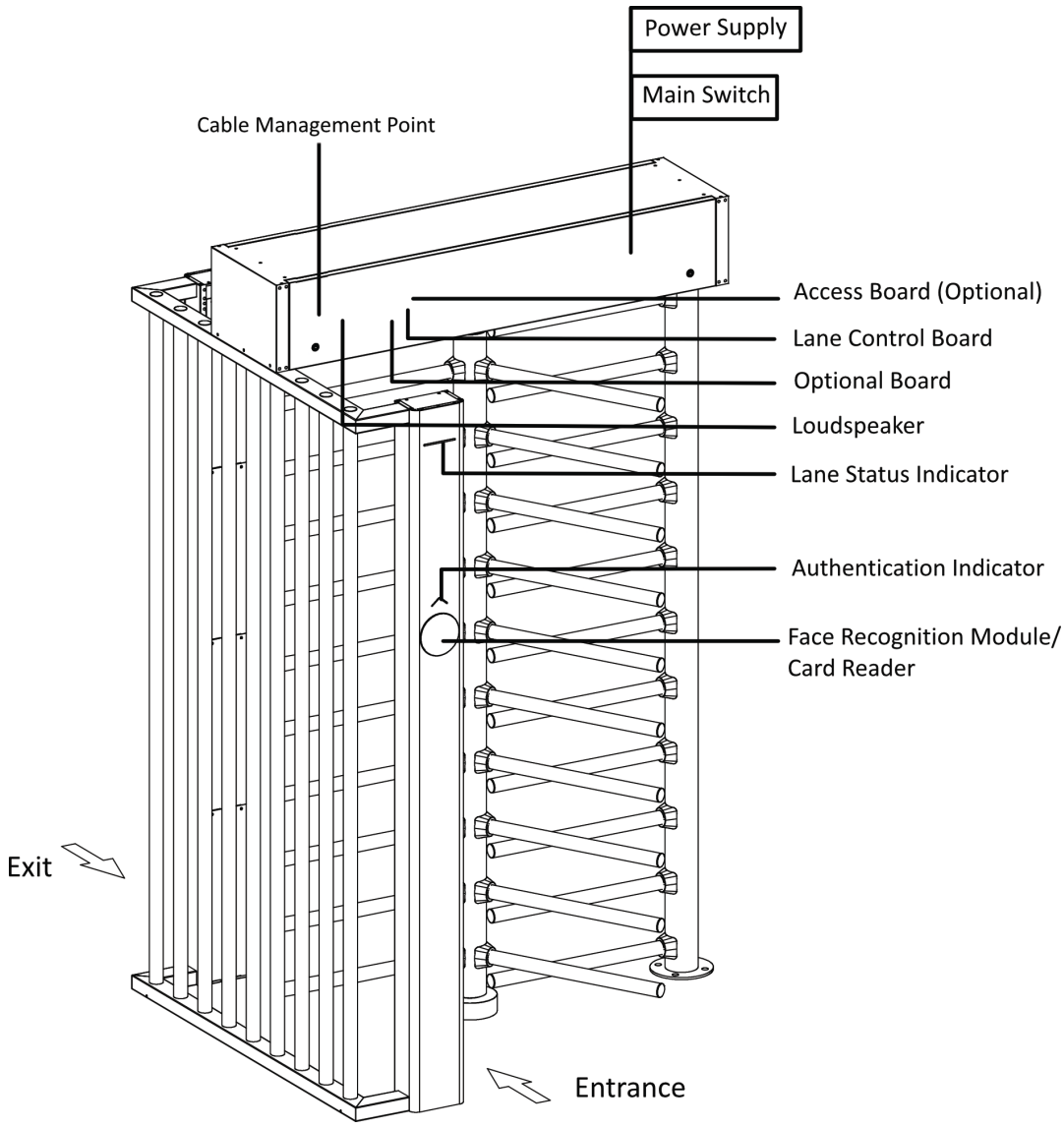


Figure 3-1 Components

3.2 Terminal Description

3.2.1 General Wiring

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

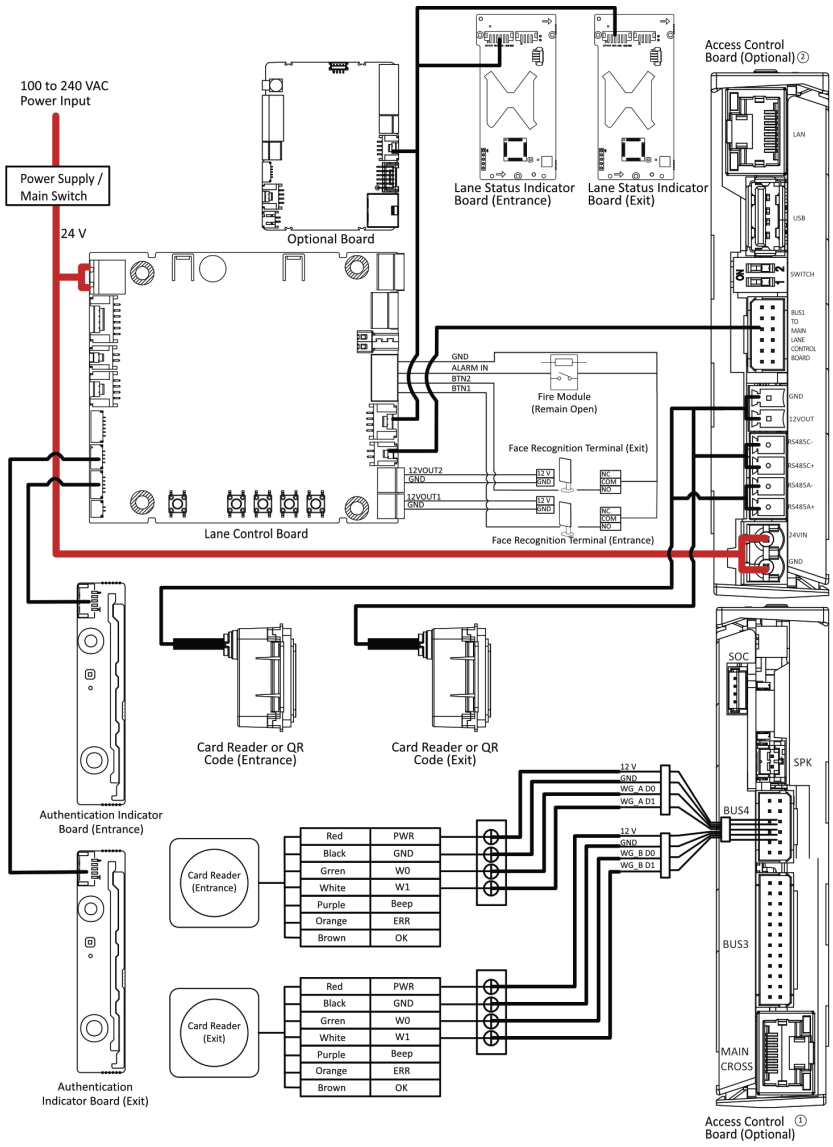


Figure 3-2 General Wiring

Note

- The power cable from power supply to the main lane control board has been connected. You will need to prepare the 14AWG power cable to connect the AC power input to power supply.
- Barrier opens at the entrance/exit: connect to BTN1/BTN2 and GND.
- The power-on process will last for 40 seconds. After waiting for 40 seconds, device can complete startup and you can continue to use.

3.2.2 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.

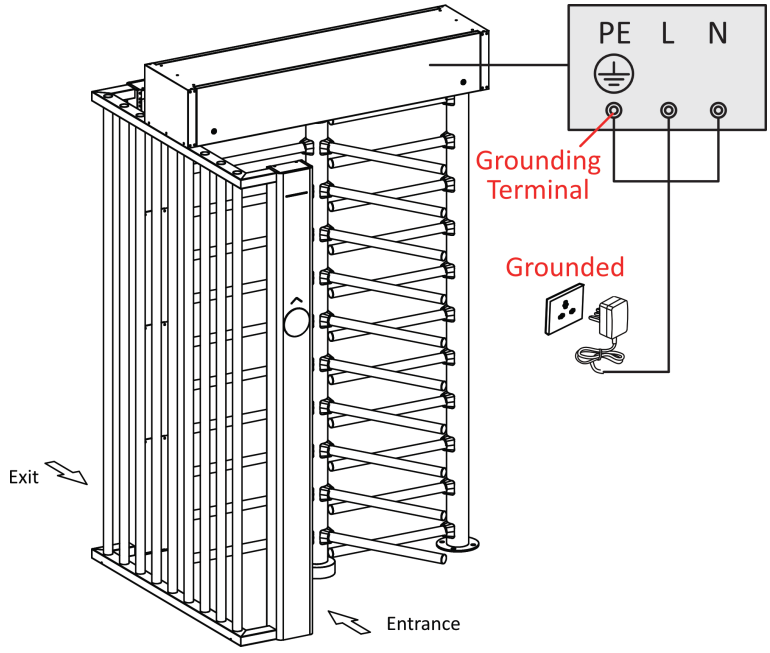


Figure 3-3 Power Cable Grounding Method

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.

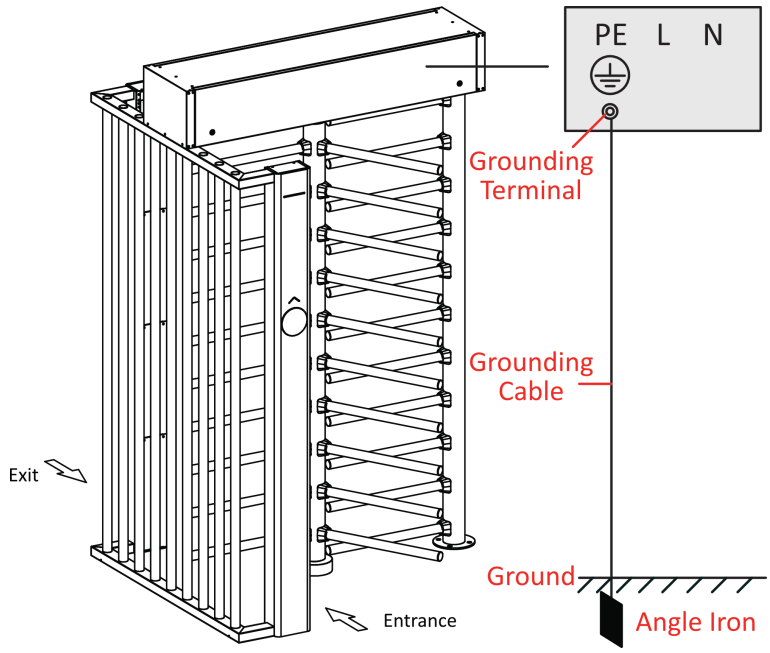


Figure 3-4 Simplified Diagram of Grounding Installation When Buried Grounding Electrode is Permitted Near the Equipment Room

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.

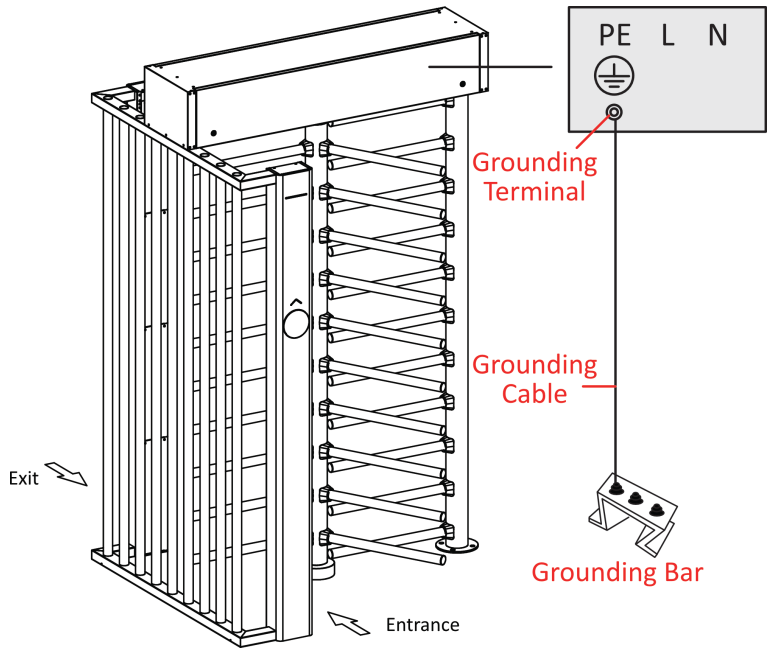


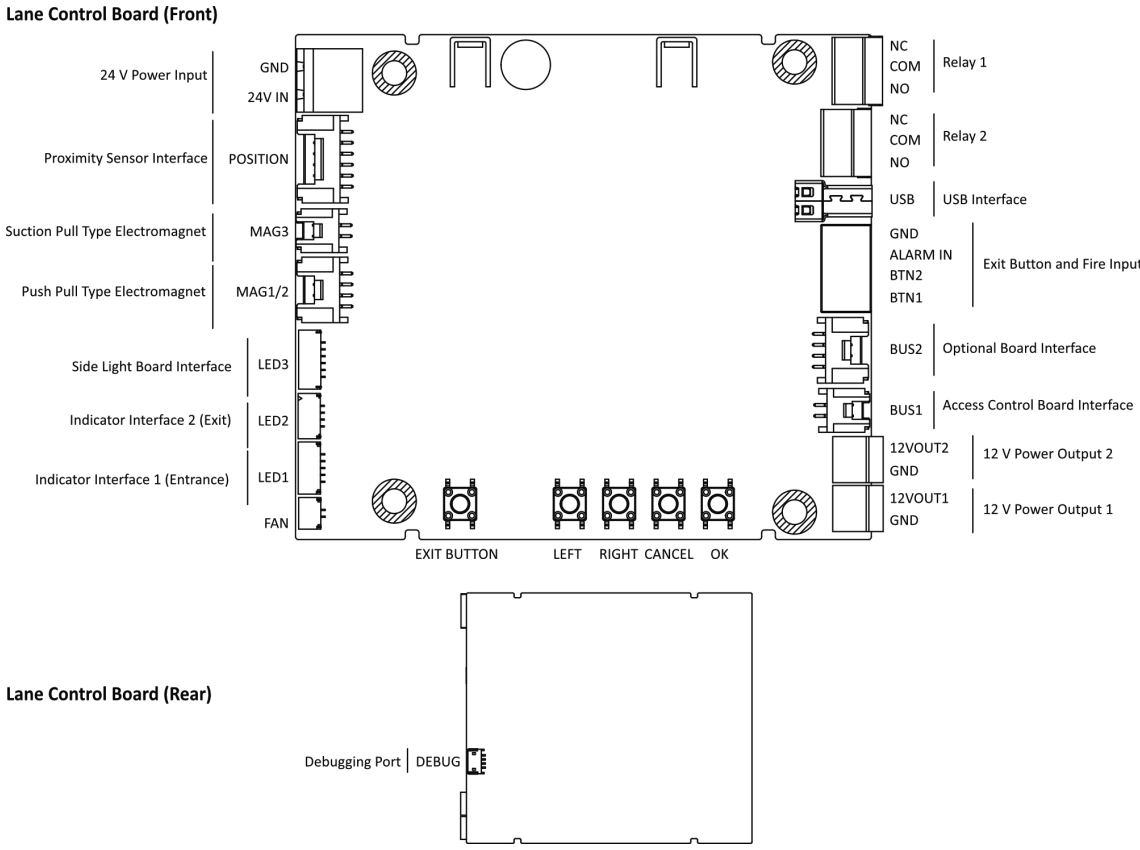
Figure 3-5 Simplified Diagram of Grounding Installation When Grounding Bar is Available in the Equipment Room

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.

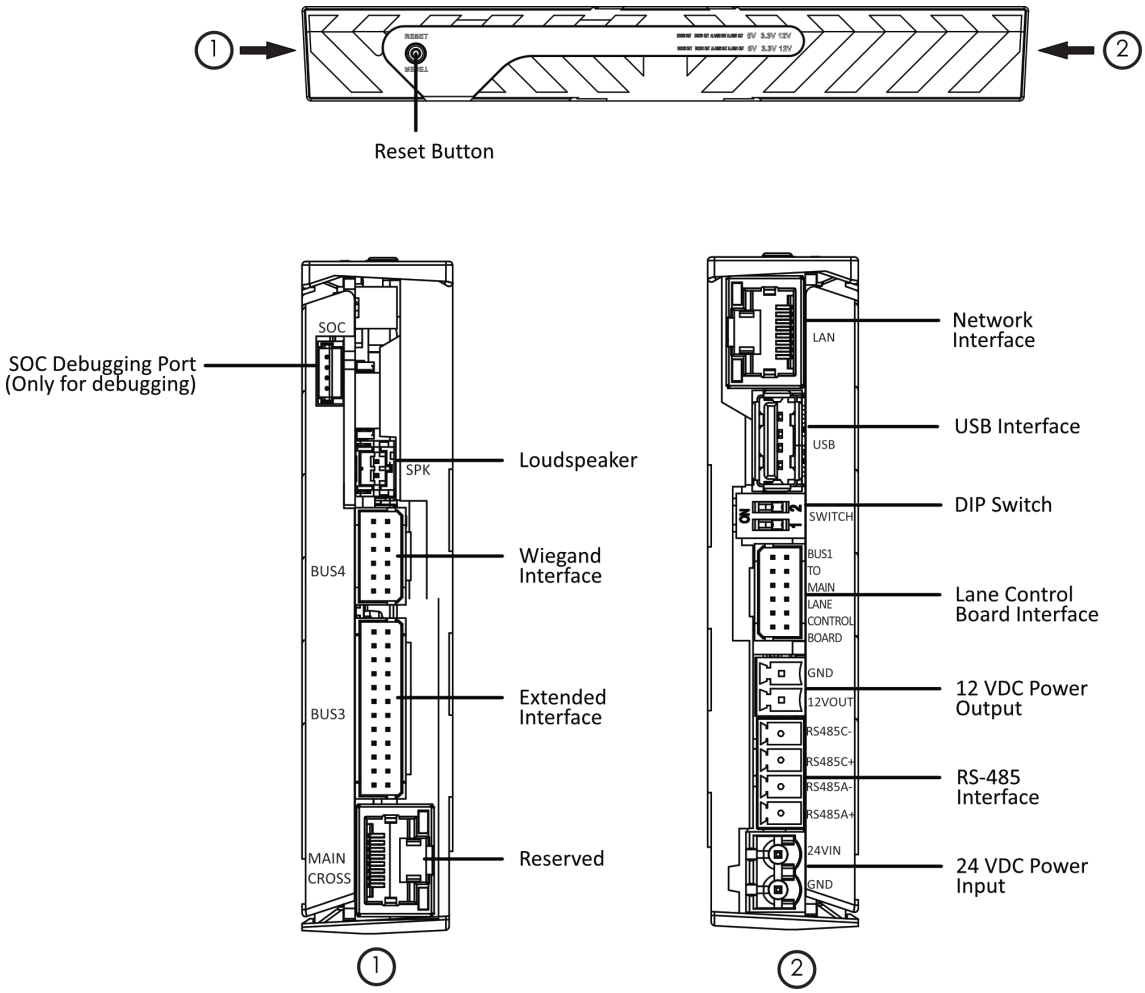
3.2.3 Lane Control Board Terminal Description

The picture displayed below is the main control board diagram.



3.2.4 Access Board Terminal Description (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.



Note

- Hold the reset button for 5 s, the device will beep for 3 s and start restoring to factory settings.
- RS-485A corresponds to port 3 on web and is for QR code scanner connection at entrance by default; RS-485C corresponds to port 5 on web and is for card reader connection at entrance by default.

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

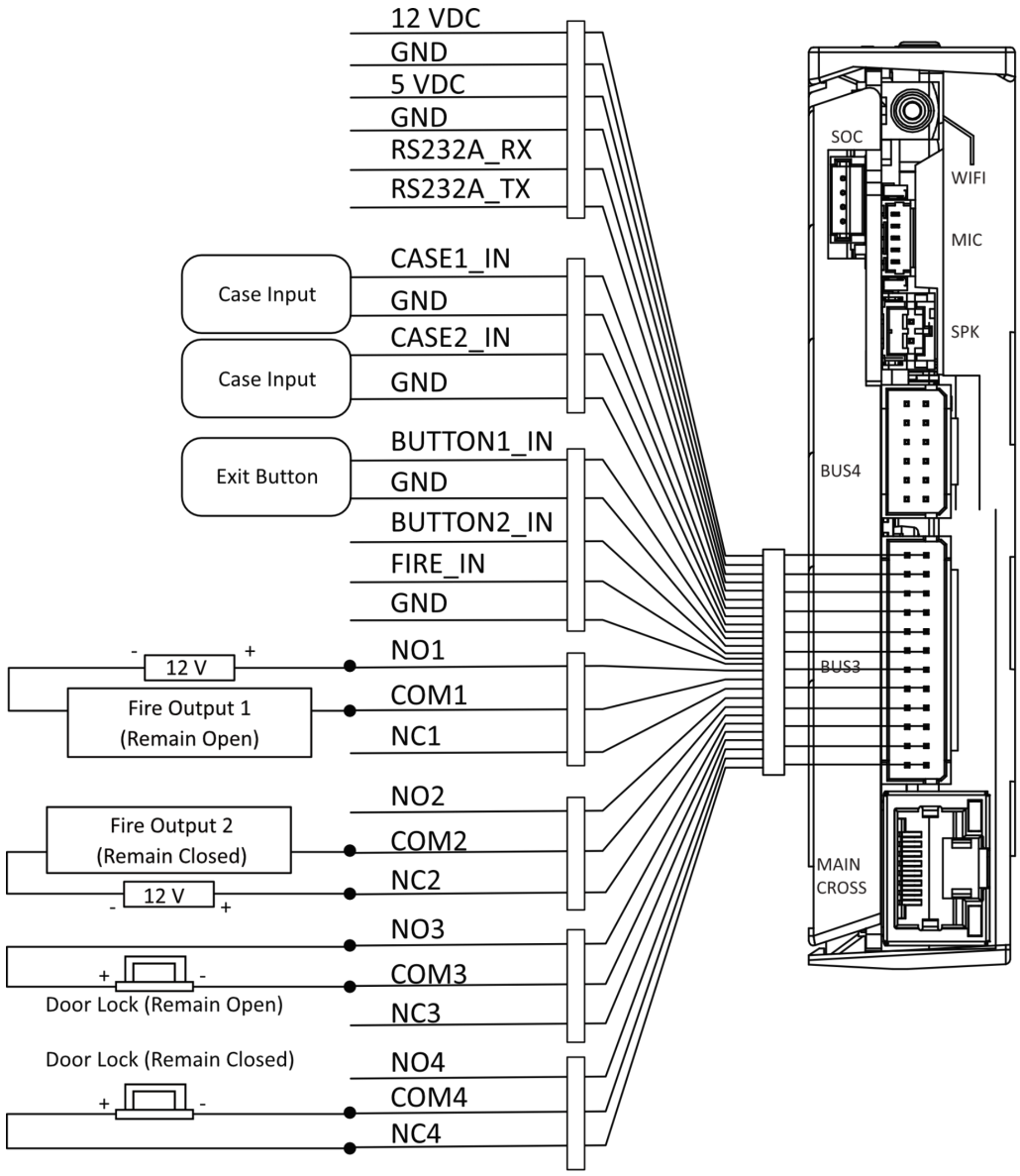


Figure 3-6 Wring Diagram of BUS3 Interface

3.2.5 Optional Board Terminal Description

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

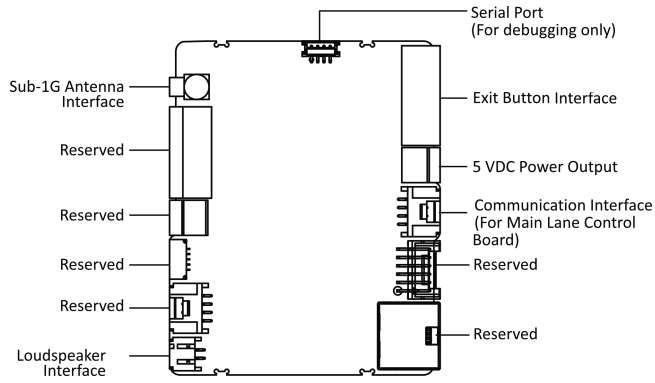


Figure 3-7 Optional Board Terminal

3.2.6 Card Reader

The card reader can be connected to the BUS4 of the access board.

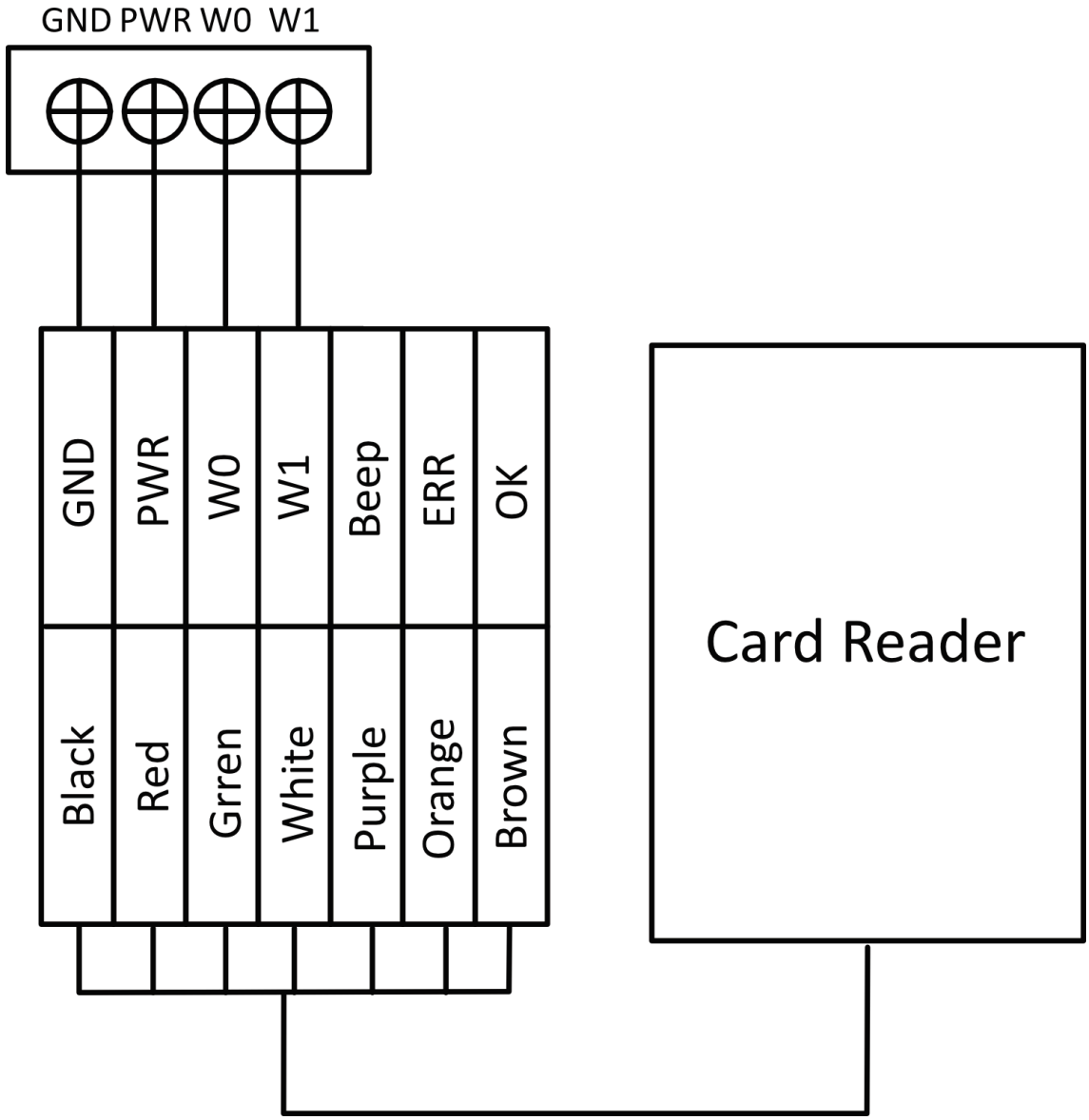


Figure 3-8 Card Reader

3.2.7 RS-485 Wiring

QR Code Wiring

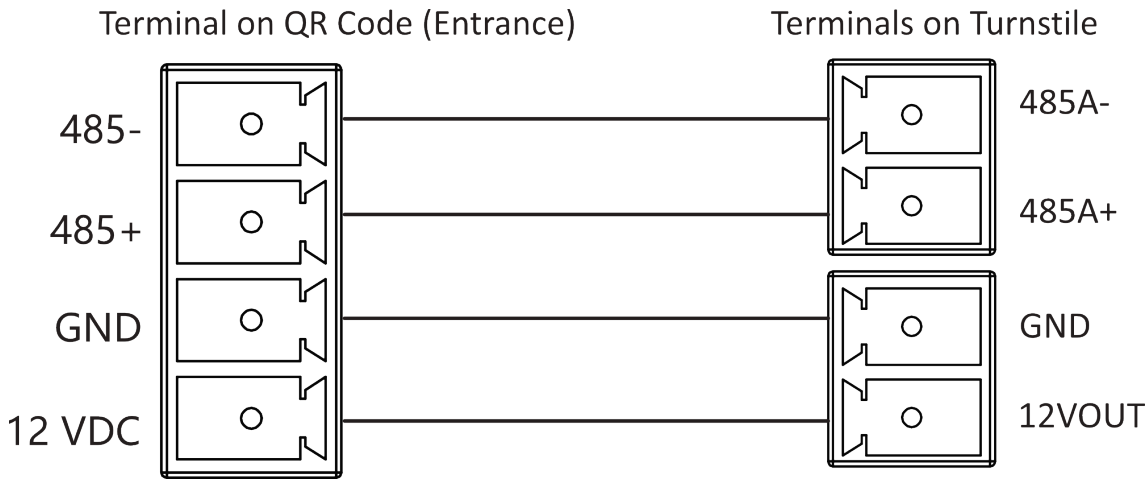


Figure 3-9 Wire with QR Code (Entrance)

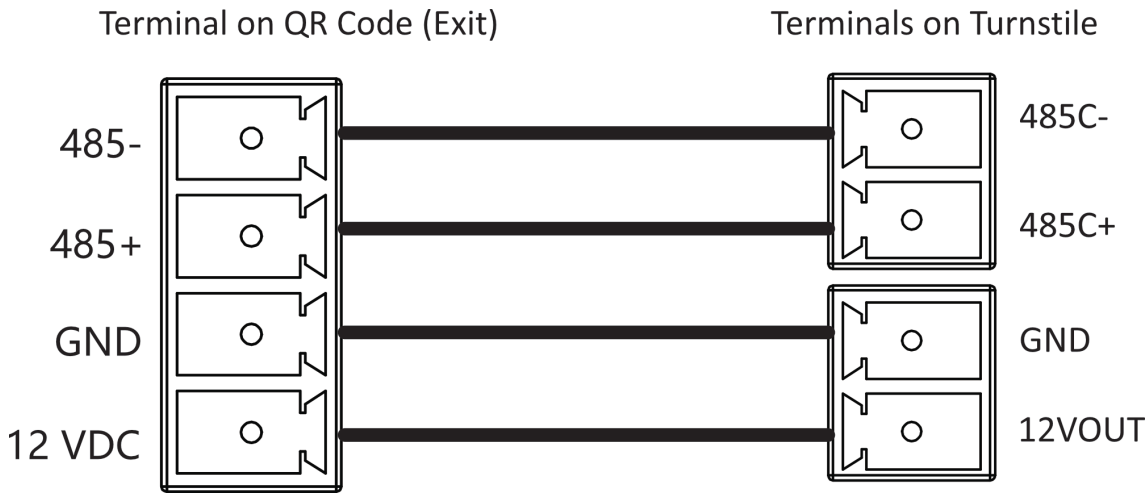


Figure 3-10 Wire with QR Code (Exit)

3.2.8 Face Recognition Module Wiring

Connect the face recognition module to the turnstile.

Face Recognition Module Wiring

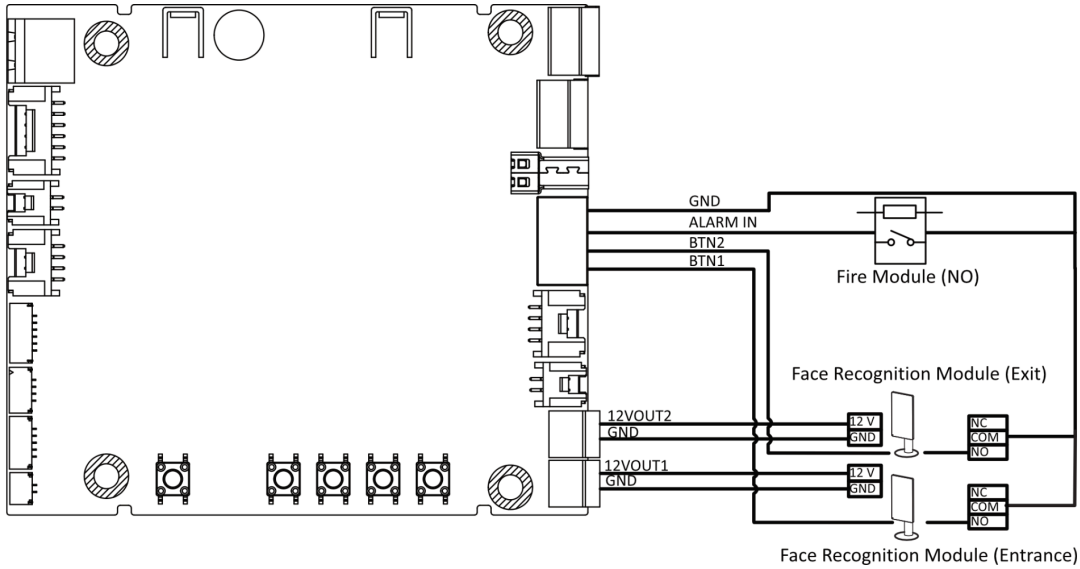


Figure 3-11 Wire with Face Recognition Module without Access Control Board

3.2.9 Loudspeaker Wiring

You should wire the loudspeaker to access board or optional board.

If he turnstile has NOT installed the access board, you can wire the loudspeaker with the optional board.

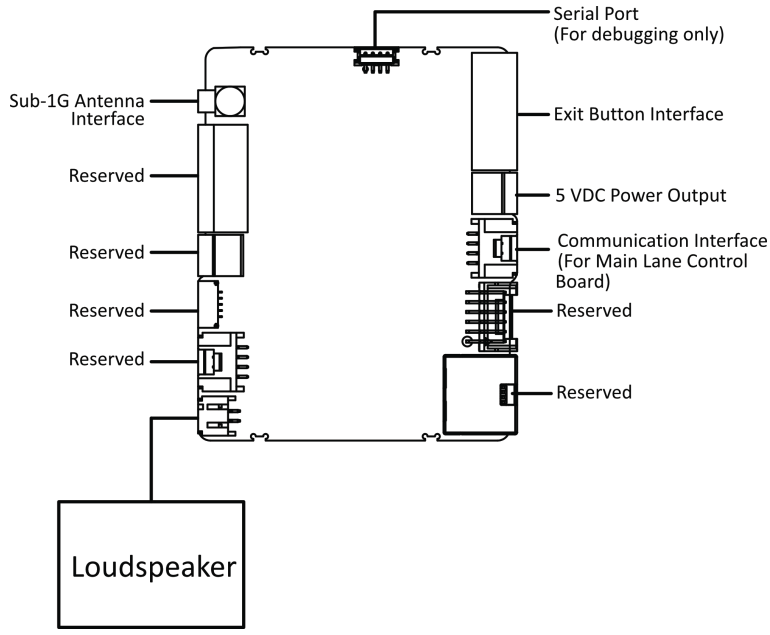


Figure 3-12 Wire Loudspeaker with Optional Board (Without Access Board)

If he turnstile has installed the access board, you can wire the loudspeaker with the access board.

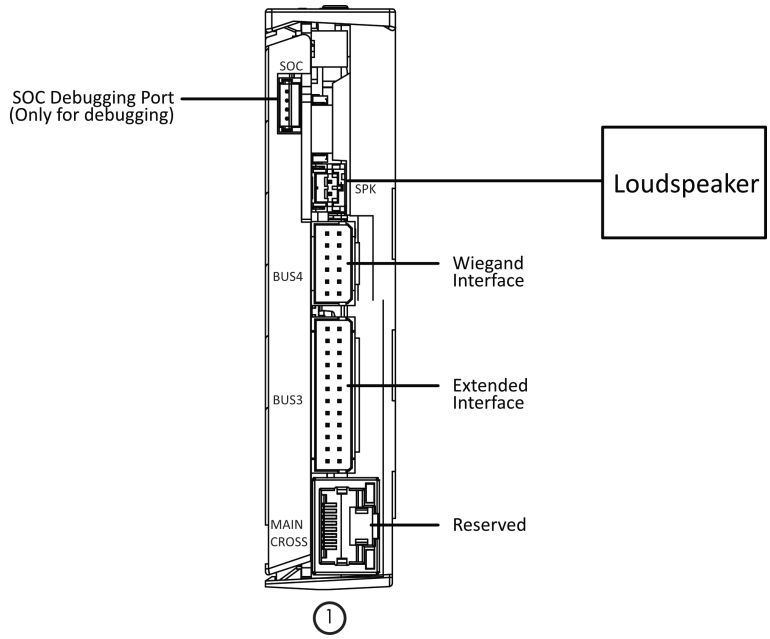


Figure 3-13 Wire Loudspeaker with Access Board

3.2.10 Alarm Input Wiring

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

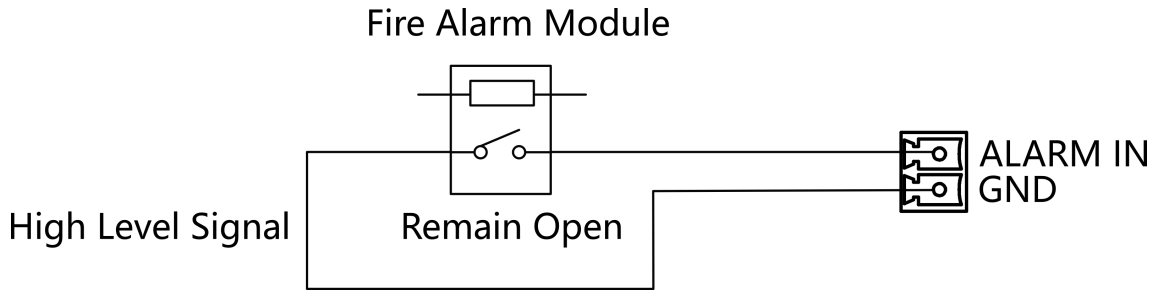


Figure 3-14 Remaining Open

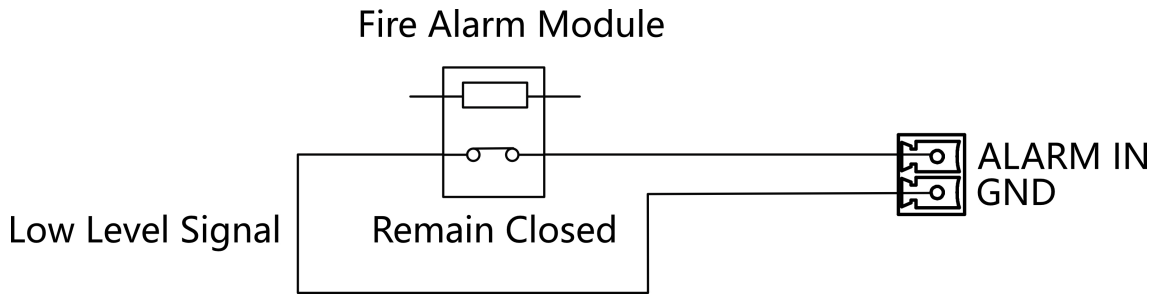


Figure 3-15 Remaining Closed

3.2.11 Exit Button Wiring

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

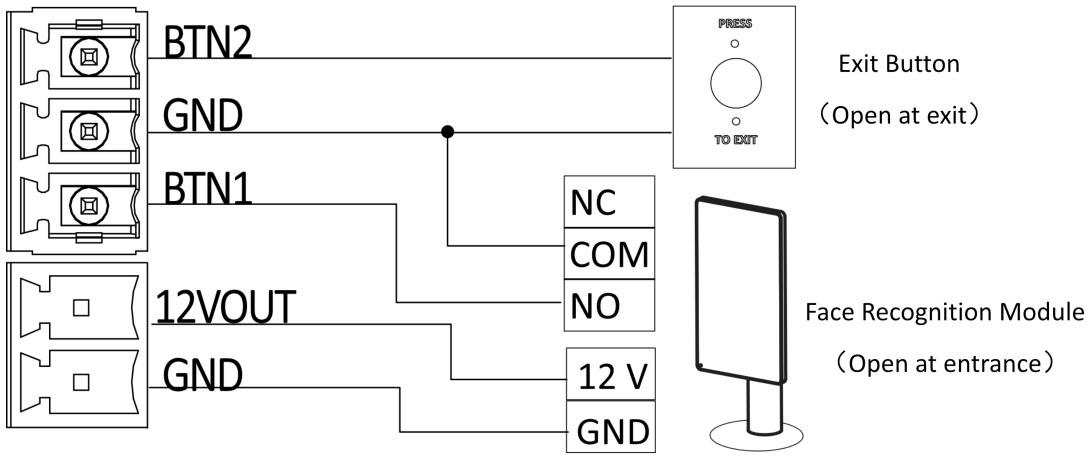


Figure 3-16 Exit Button Wiring

Note

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

3.2.12 Change From Normally Open (NO) to Normally Closed (NC) When Powering Off

Power-off locking is essential for safety-critical systems (e.g., machinery, emergency stops) to prevent unintended re-energization, ensure fail-safe states during power loss. It requires manual intervention to restore operation, mitigating hazards in industrial and process control applications.

Steps

Note

By default, the device is NO when power is off.

1. Open the upper cover and find the magnetic.
2. Remove the 4 screws for each magnet and change the 2 magnets' direction. Then secure the magnets with the screws.

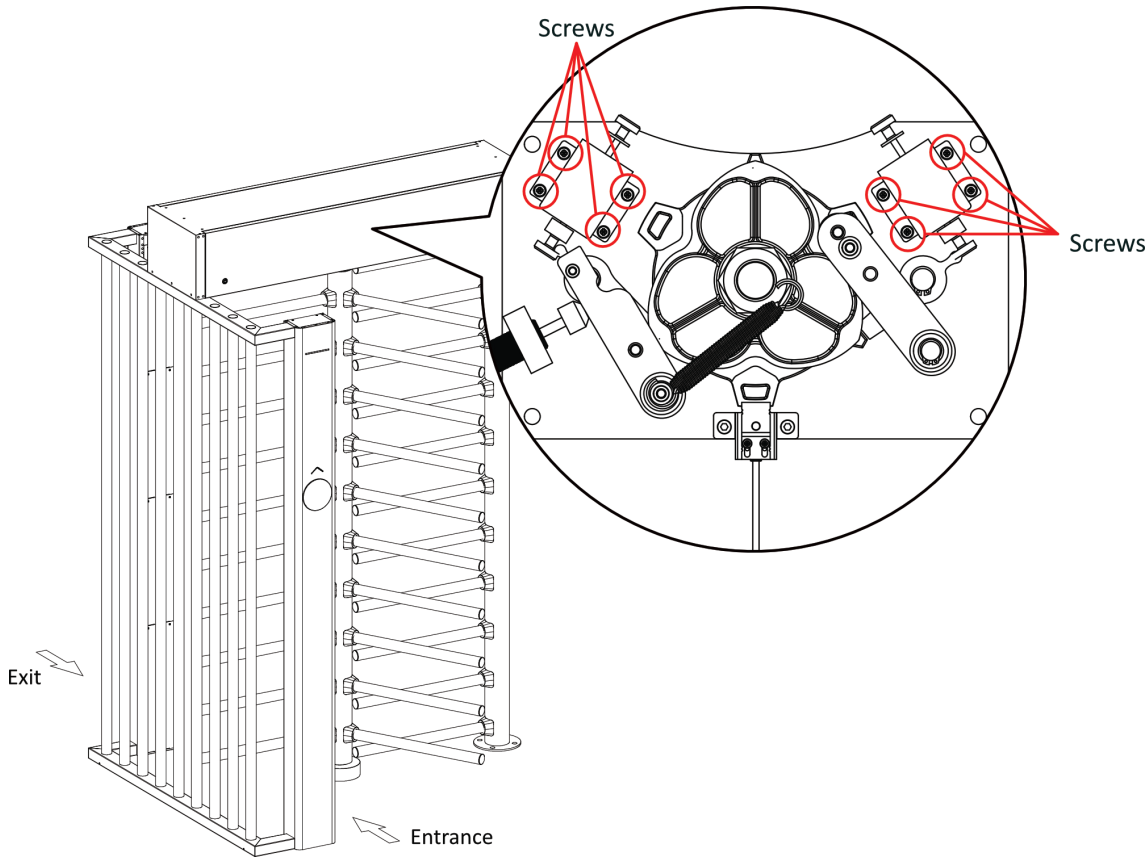


Figure 3-17 Magnet Position

3. Change to NC via web or button.
   - If the device has NOT installed an access board, you should set the NO/NC via button. Set the No. 50 as 2 - Close Barrier When Power Off.
   - If the device has stalled an access board, you can set the NO/NC via Web.

     On the Web configuration page, select **Close Barrier When Power Off** in the **Barrier Power on Mode**.

     Note

     For details, see ***Basic Parameters*** .

3.3 Device Settings via Button

3.3.1 Configuration via Button

Button Description

The buttons are on the lane control board.

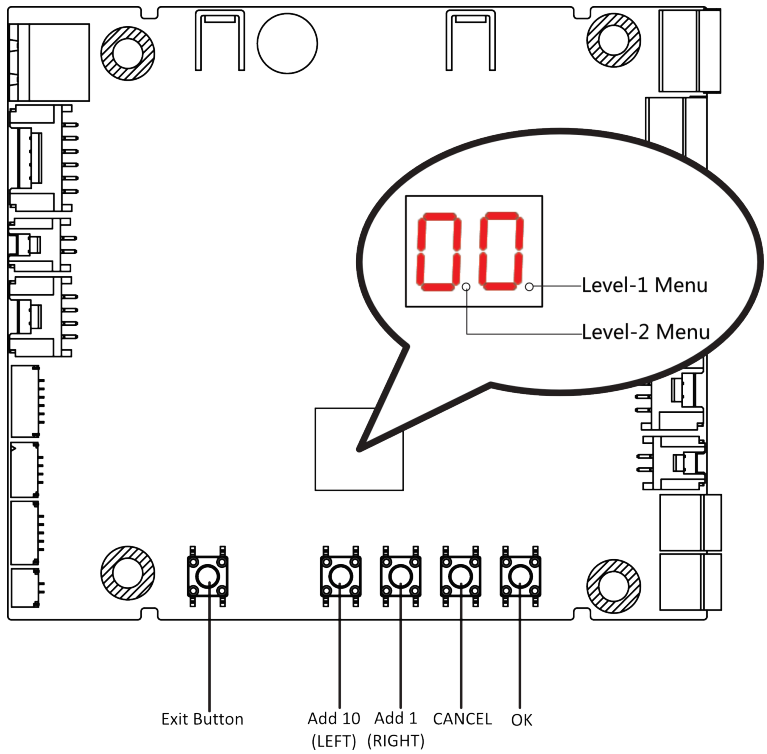


Figure 3-18 Button

Exit Button

- Single press to open the gate from the entrance position.
- Double press to open the gate from the exit position.

Parameter Configuration Button

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

Note

- Configuration data is displayed by two digital tubes.
- Level-1 Menu: If the decimal point on the right is on, it indicates the level-1 menu. The number represents the configuration item number.
- Level-2 Menu: if the decimal point in the middle is on, it indicates the level -2 menu. The number represents the parameters of a configuration item.

Button Configuration Procedure

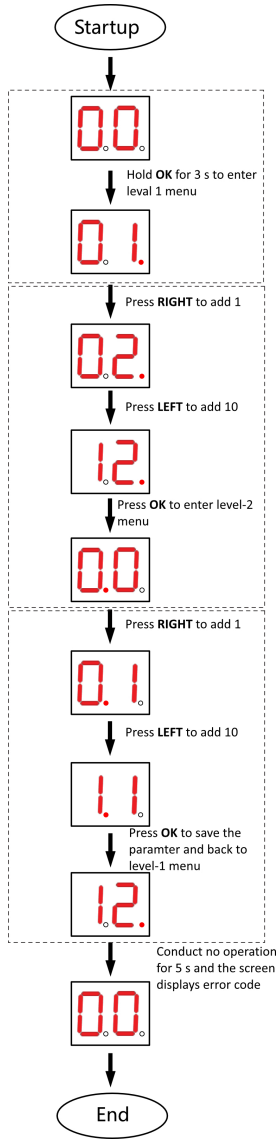


Figure 3-19 Procedure

Steps:

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

3.3.2 Initialize Device

Steps

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

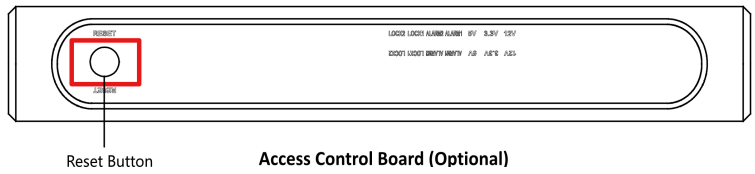


Figure 3-20 Initialization Button Position

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.

3.3.3 Pair Keyfob via Button

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

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

Note

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

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

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

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

Chapter 4 Activation

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

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

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 80
- The default user name: admin

4.1 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.

   Note

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

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

4.2 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: Enable the phone's Wi-Fi function, and connect to the current device's hotspot. After hotspot is connected, you will go to the login page.

Note

- Hotspot Name: AP_Serial No.
- Hotspot Password: Device's Serial No.

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. You can configure the turnsile basic parameters, keyfob settings, light settings, network settings, access control settings, etc.

4.3 Activate via SADP

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

Before You Start

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

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

Steps

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

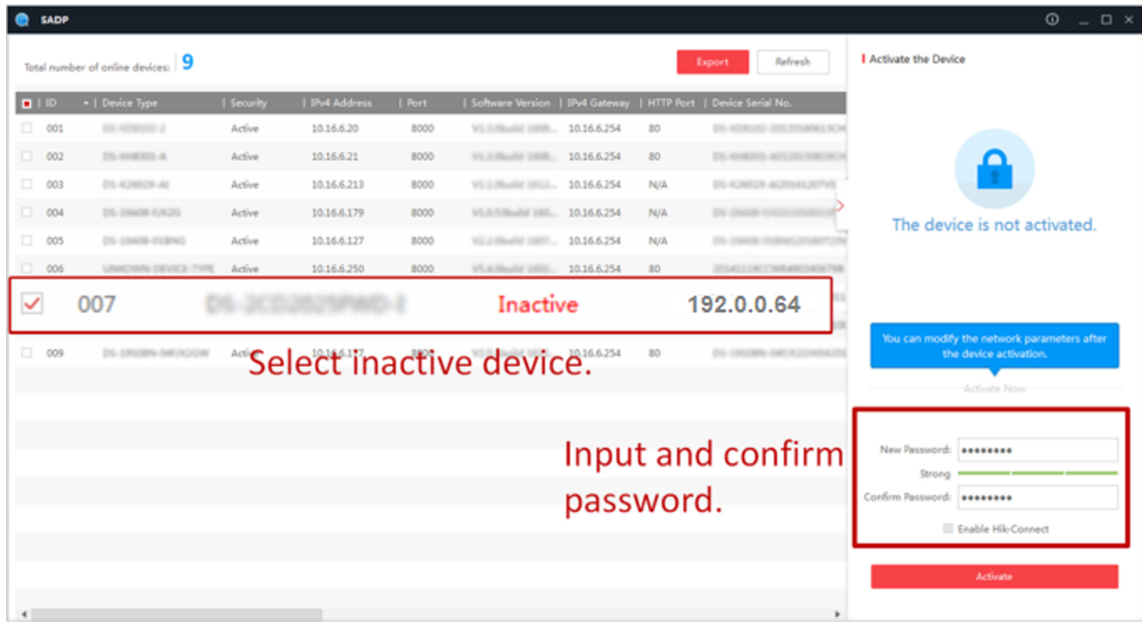
Caution

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

Note

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

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



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

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

4.4 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 5 Operation via Web Browser

5.1 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.

5.2 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.

5.3 Quick Operation via Web Browser

5.3.1 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.

5.4 Overview

You can view the device component status, 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 unlocked/closed/remaining open/remaining closed.

Event

You can view the event Employee ID, Name, Card No., and Event Type. You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Person Information

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

Network Status

You can view the network connection status.

Basic Information

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

Device Capacity

You can view the person, card and event capacity.

5.5 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.

5.6 Turnstile

5.6.1 Search Event

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

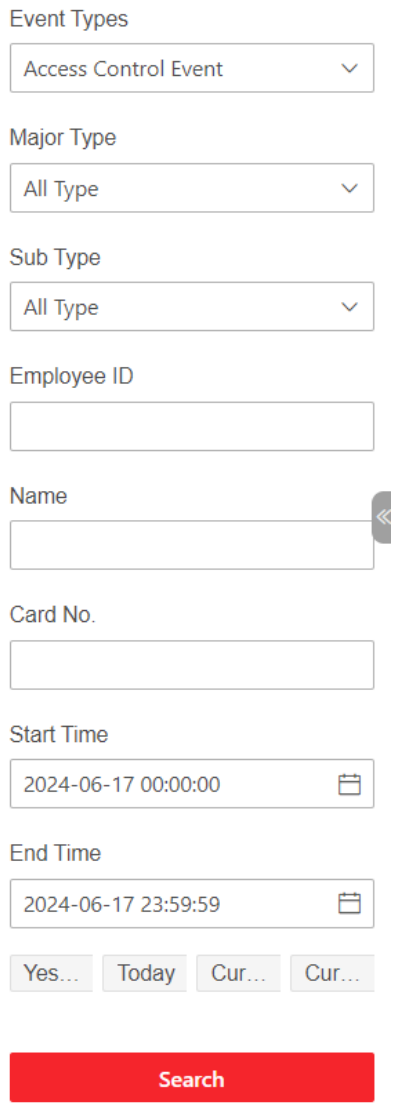


Figure 5-1 Search Event

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.

5.6.2 Access Control Settings

Set Door Parameters

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

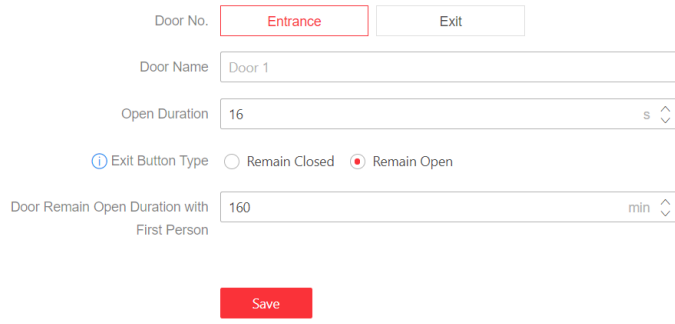


Figure 5-2 Door Parameters Settings

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.

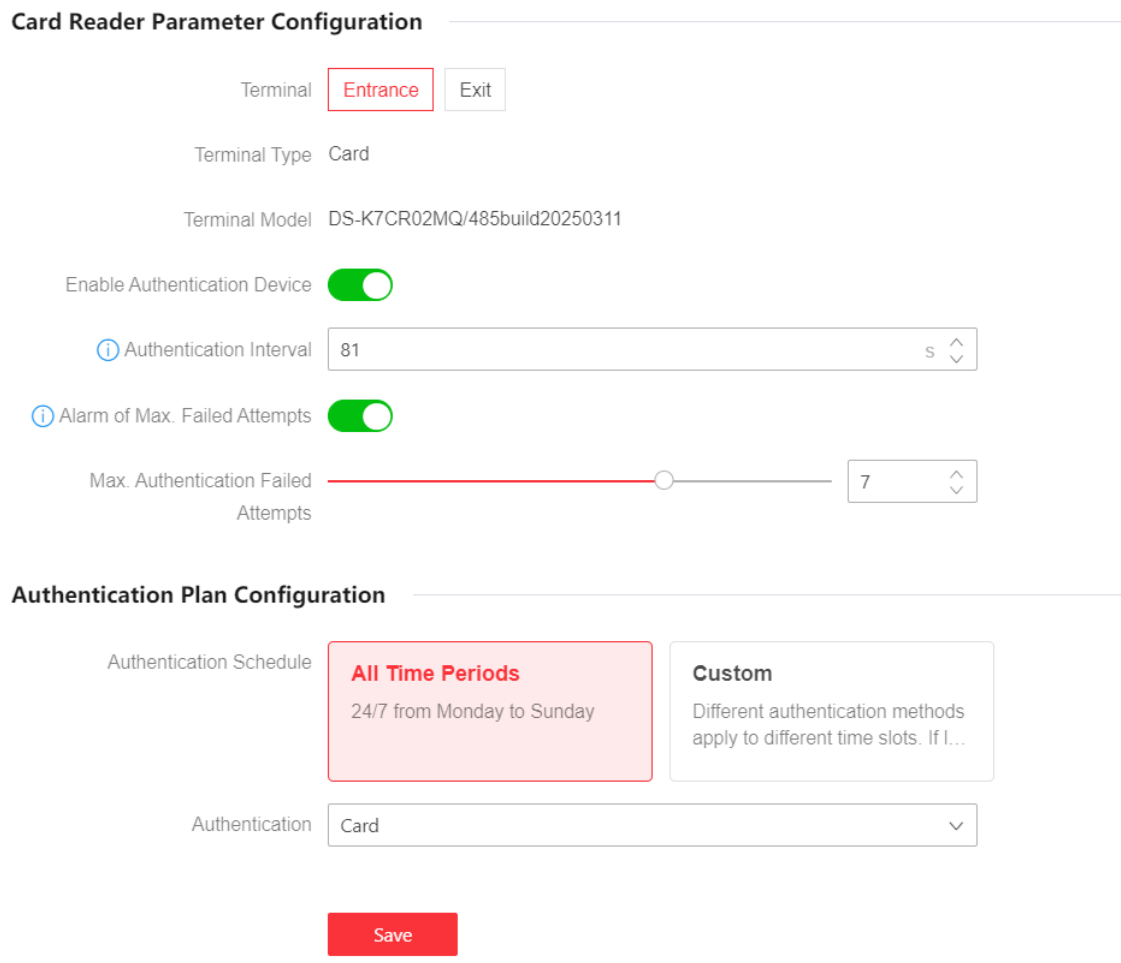


Figure 5-3 Authentication Settings

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.

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** .

Event Storage Settings

Select a method to delete the event. The device supports **Overwriting**.

Overwriting

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

5.6.3 Turnstile Configuration

Basic Parameters

Set turnstile basic parameters.

Steps

1. Click **Turnstile → Turnstile Configuration → Basic Parameters** to enter the page.
2. View the **Channel Type**, **Channel Model**, and **Working Status**.
3. Set parameters.

Channel Type/Channel Model/Channel Status

View the actual device type, model, and working status.

Passing Mode

General Passing

Select the passing method for **Entrance** and **Exit**. The device can operate according to the selected passing method throughout the day.

Note

When both the entrance and exit directions are **Controlled**, once one side is authenticated, the other side is not allowed to authenticate until the personnel passage is completed.

Weekly Schedule

Select the **Remain Open** or **Remian Closed** brush for **Entrance** or **Exit** as needed, and apply it to the required time periods on the timeline. The system controls the device to be always open or always closed based on the drawn timeline.

Barrier Power On Mode

Configure the barrier to open or close when power is off.

Open Barrier When Power Off

When power is off, the barrier opens, allowing free access.

Close Barrier When Power Off

When power is off, the barrier closes, preventing access.

4. Click **Save**.

Keyfob Settings

Set keyfob parameters.

Steps

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

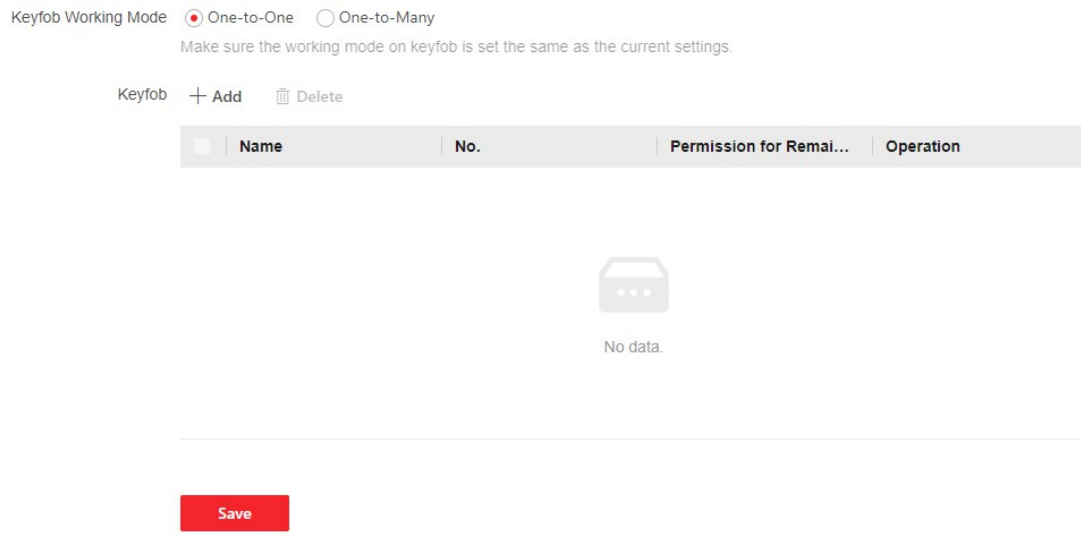


Figure 5-4 Keyfob Settings

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 Settings** to enter the page.

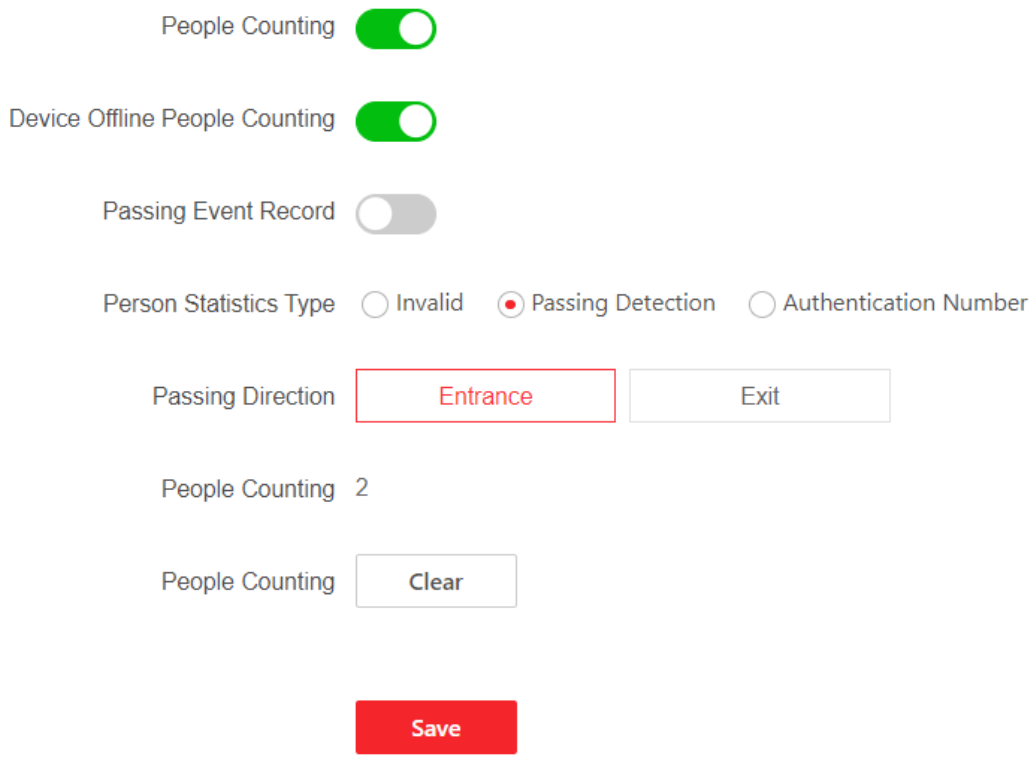


Figure 5-5 People Counting

2. Set people counting parameters and click **Save**.

People Counting

Enable the function and set the parameters.

Device Offline People Counting

The device will count people numbers even if it is offline.

Passing Event Record

The device will report passing event to the platform when people passing.

People Statistics Type

Invalid

Disable people counting.

Passing Detection

The number of all passing people, including authenticated one and IR triggered one.

Authentication Number

The number of passing people verified through credential authentication.

Passing Direction

Select the device passing direction according to actual needs.

People Counting

View the people counting number and you can also click **Clear** to clear all data.

Other Settings

Set other parameters.

Steps

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

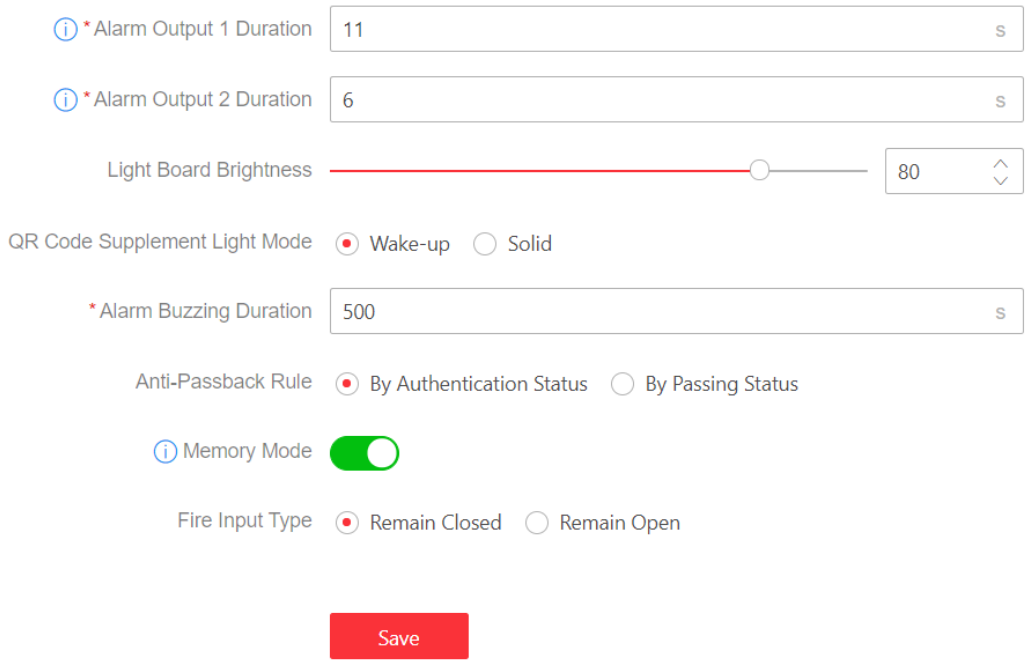


Figure 5-6 Other Settings Page

2. Set parameters.

Alarm Output Duration

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

Light Board Brightness

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

QR Code Supplement Light Mode

Set the mode as **Wake-up** or **Solid**.

Wake-up

When there is something closing to the device, the supplement light will be waked up.

Solid

The supplement light of the QR code will be on all the time.

Alarm Buzzing Duration

Set the duration of alarm sound.

Anti-Passback Rule

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

By Authentication Status

Anti-passback takes effect only after the person is authenticated.

By Passing Status

Anti-passback takes effect without the person being authenticated.

Note

Determine whether the product supports this function according to the specific model.

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.

Control Mode

Soft Mode: The barrier will be closed after the person has passed through the barrier when there are tailgating, forced accessing, etc.

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

Fire Input Type

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

Invert Entrance and Exit Direction

This function allows you to invert the entrance and exit direction of the reader if the installed entrance and exit direction reader is in the wrong position.

3. Click **More** to adjust **Barrier Open Angle**.
4. Click **Save**.

5.7 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.

5.7.1 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, face, card and event.

5.7.2 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** .

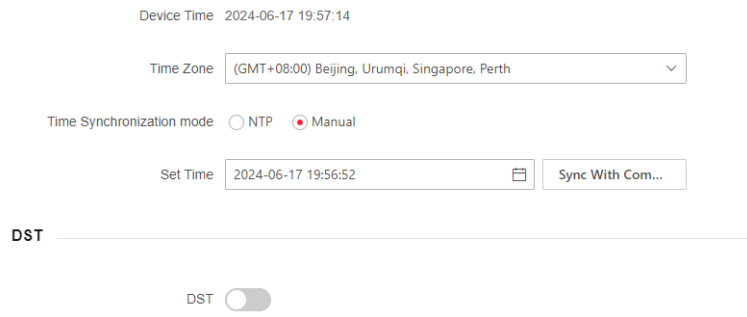


Figure 5-7 Time Settings

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.

5.7.3 Change Administrator's Password

Steps

1. Enter the password change page.
   - Click **System and Maintenance → System Configuration → System → User Management → User Management** and click ✎ .
   - Click **admin → Modify Password** at the upper right corner of the page.
2. Enter the old password and create a new password.
3. Confirm the new password.
4. 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.

5.7.4 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.

5.7.5 View Device Arming/Disarming Information via PC Web

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.

5.7.6 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.

5.7.7 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.

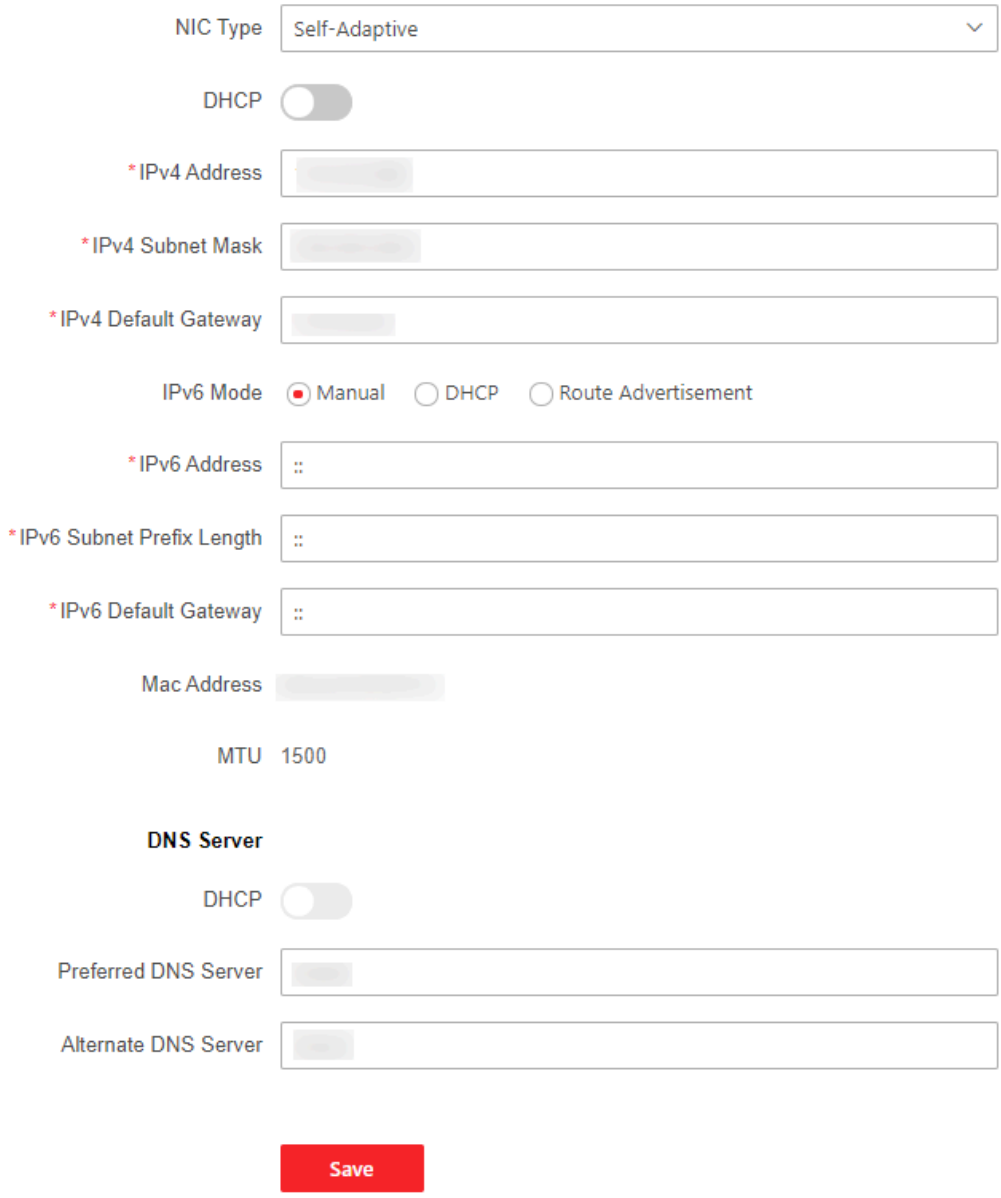


Figure 5-8 Set TCP/IP

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.

Device Hotspot

Set the device hotspot.

Click **System and Maintenance → System Configuration → Network → Network Settings → Device Hotspot** .

Click to **Enable Device Hotspot**. Set hotspot **Name** and **Password**.

Click **Save**. You can use your phone to connect the hotspot and set parameters on the mobile web.

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 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** .

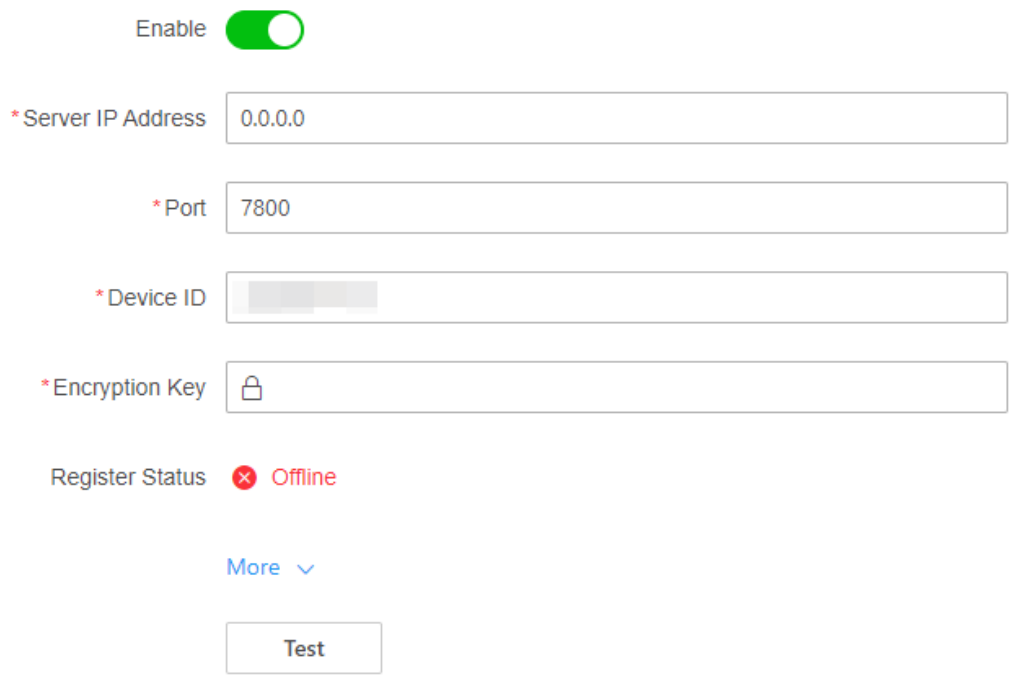


Figure 5-9 Set OTAP

2. Select central group.
3. Click to **Enable** OTAP.
4. Set **Server IP Address**, **Port**, **Device ID** and **Encryption Key**.
5. Click **More** to view the network type and access priority. Drag the operation icon upward or downward to adjust the network priority.
6. 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**.
7. 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.

5.7.8 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** .

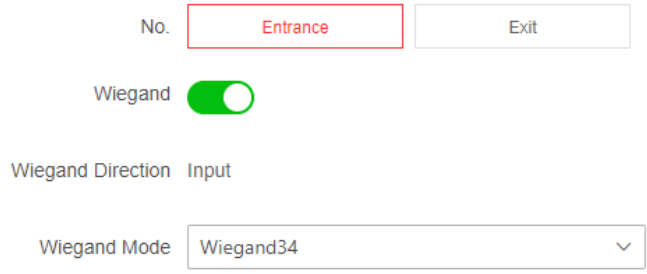


Figure 5-10 Wiegand Page

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.

5.7.9 Serial Port Settings

Set serial port parameters.

Steps

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

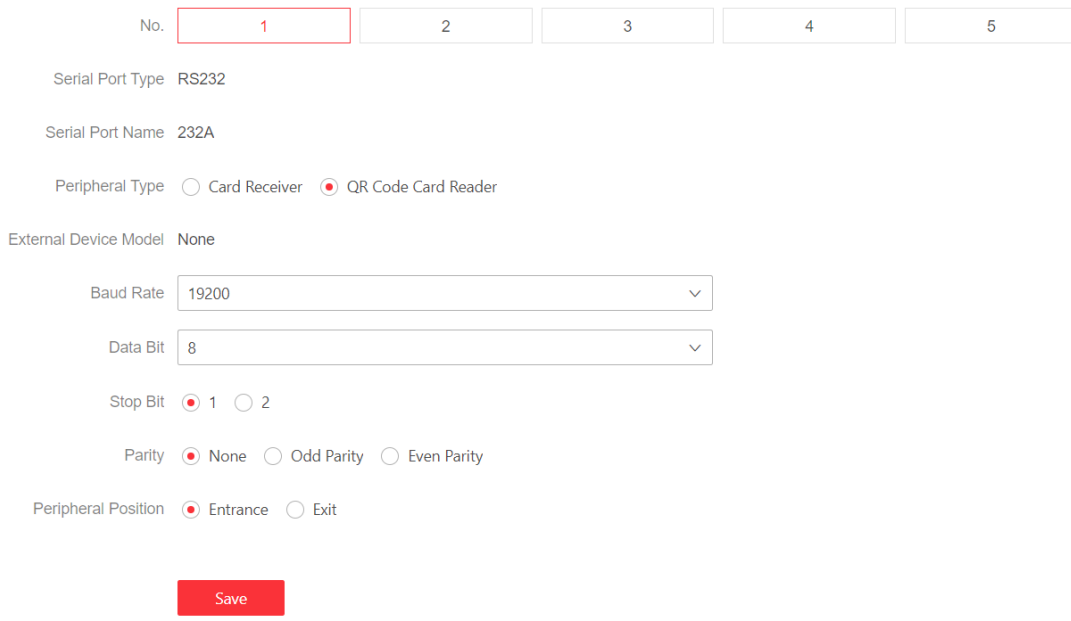


Figure 5-11 Serial Port Configuration

2. Select a serial port No., 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**.

5.7.10 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.

5.7.11 Event Linkage

Set linked actions for events.

Steps

1. Click **Turnstile → Parameters Settings → Linkage Configuration** to enter the settings page.
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.

   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, language, and prompt content.

   Voice Prompt Type

   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.

   Play Mode

   Select the audio playing mode as **Disable**, **Play Once**, or **Loop**.

   Language

   If select **TTS** as the **Voice Prompt Type**, you should select audio playing language.

   Prompt

   If select **TTS** as the **Voice Prompt Type**, you should set the prompt content. The audio prompt will play the entered text.

   Audio File

   If select **Audio File** as the **Voice Prompt Type**, you should select an audio file from the local PC. the voice prompt will play the select audio file.
4. Click **Save**.

5.7.12 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

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

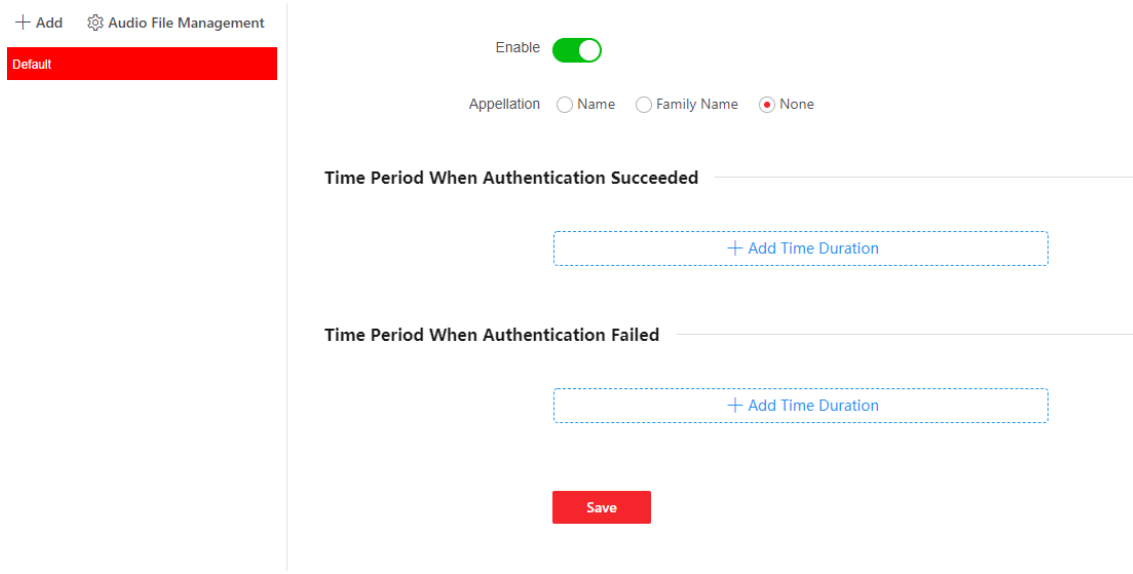


Figure 5-12 Customize Audio Content

2. Enable the function.
3. Set the appellation.
4. 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) Select the voice prompt type.
   4) Enter the audio prompt content or select audio file.

   Note

   You can click **+ Audio File** or **Audio File Management** to add audio files.
   5) **Optional:** Repeat substep 1 to 3.
   6) **Optional:** Click to delete the configured time duration.
5. Set the time duration when authentication failed.
   1) Click **Add Time Duration**.
   2) Set the time duration.

Note

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

3) Select the voice prompt type.
4) Enter the audio prompt content or select audio file.

Note

You can click **+ Audio File** or **Audio File Management** to add audio files.

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

6. Click **Save**.

5.7.13 Upgrade and Maintenance

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

Reboot Device

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

Upgrade

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

Note

Do not power off during the upgrading.

Restore Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the network parameters and the user information.

Import and Export Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note

You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

5.7.14 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.

5.7.15 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**.

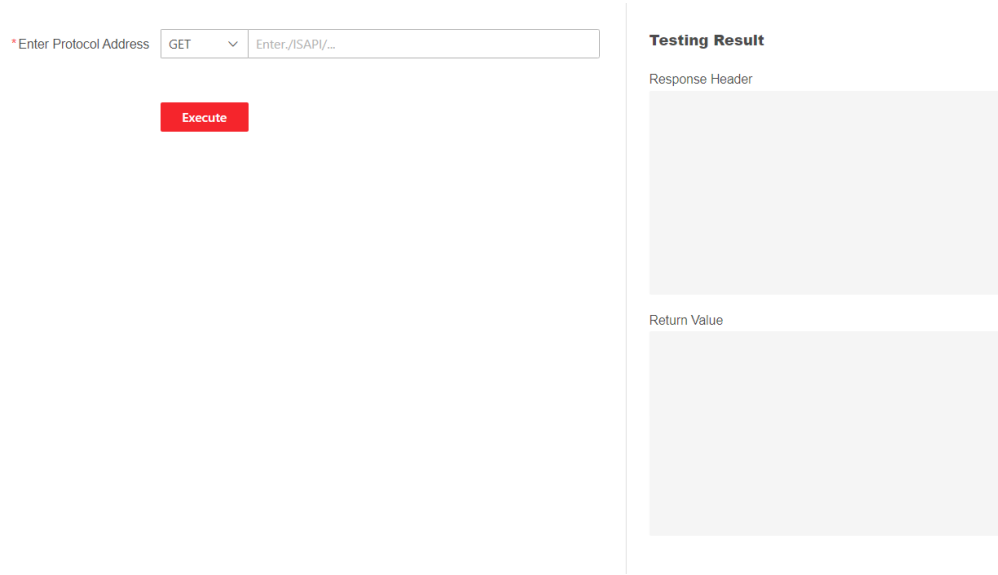


Figure 5-13 Protocol Testing

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

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

5.7.16 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.

5.7.17 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 Device

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

Others

Passing Mode

You can view the entrance and exit modes.

Input and Output Status

You can view the status of the event inputs, alarm outputs, and fire alarms.

Other Status

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

5.7.18 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.

5.7.19 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 6 Configure the Device via the Mobile Web

6.1 Login

You can login via mobile browser.

Note

Make sure the device is activated.

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.

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: Enable the phone's Wi-Fi function, and connect to the current device's hotspot. After hotspot is connected, you will go to the login page.

Hotspot Name: AP_Serial No.

Hotspot Password: Device's Serial No.

6.2 Overview

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

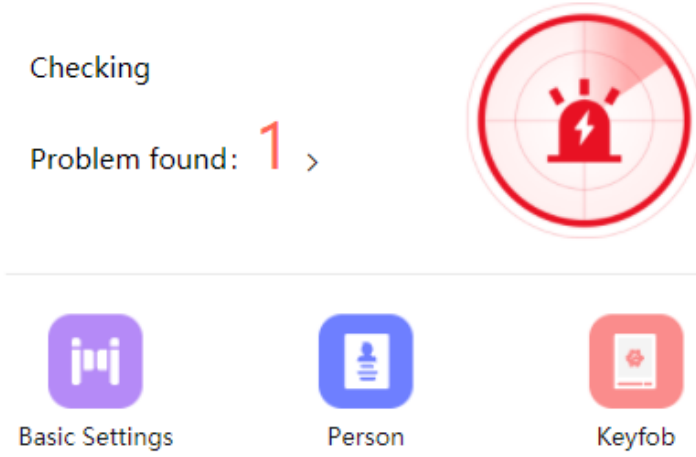


Figure 6-1 Status and Quick Settings

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, and keyfob settings page.

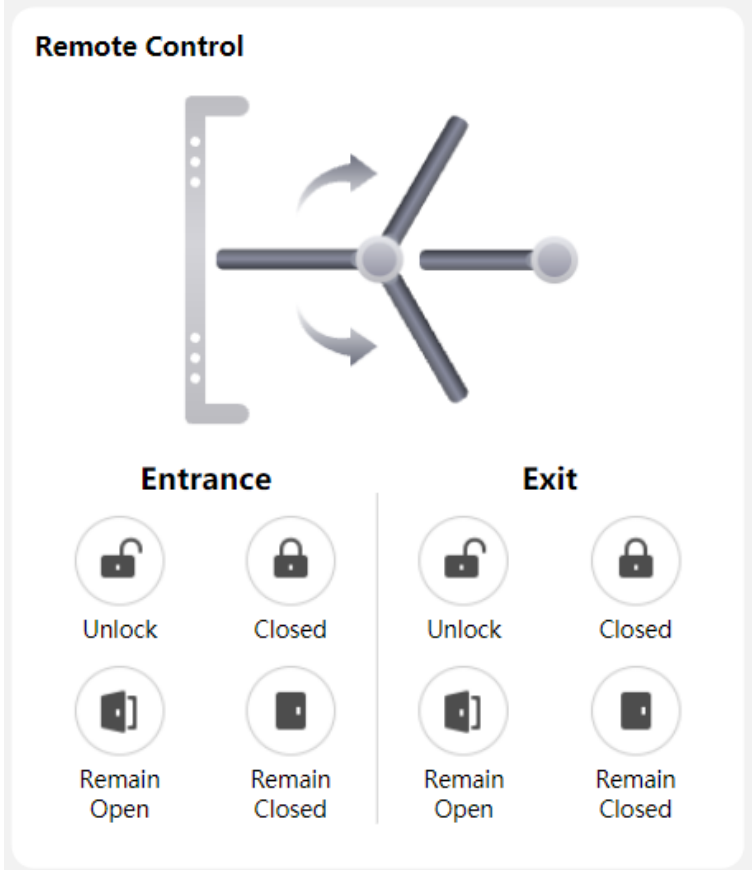


Figure 6-2 Remote Control

You can remotely control barrier by tap the icons.

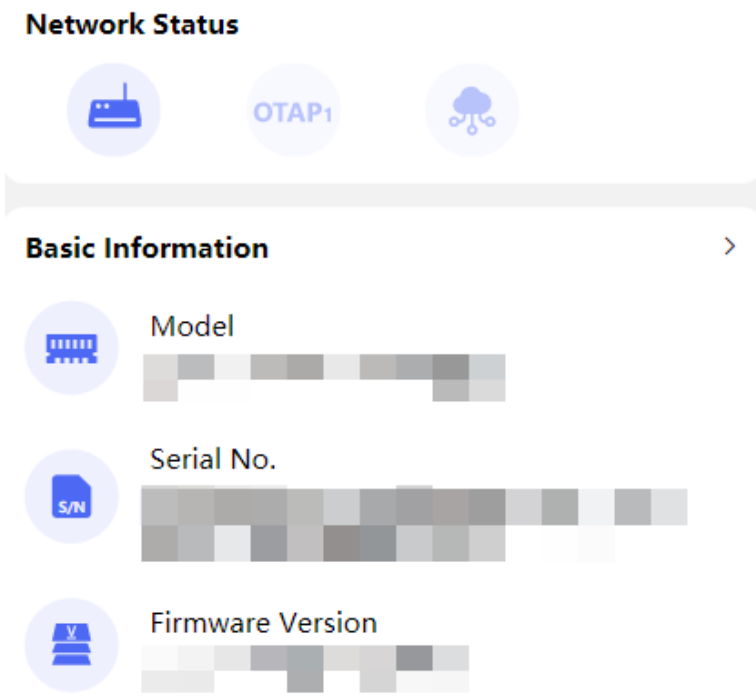


Figure 6-3 Network Status and Basic Information

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

6.3 Configuration

6.3.1 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** .

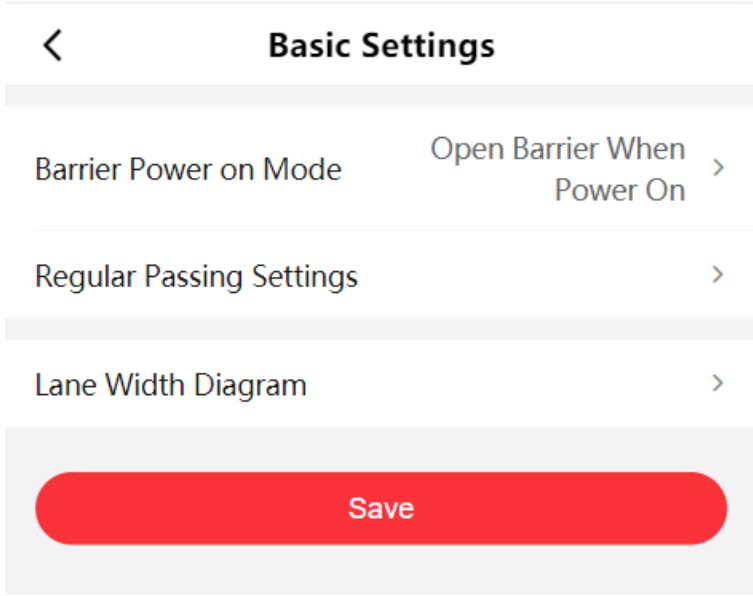


Figure 6-4 Turnstile Basic Parameters

Set basic parameters.

Barrier Power on Mode

Configure the barrier to open or close during a power outage.

Open Barrier When Power On

During a power outage, the barrier opens, allowing free access.

Close Barrier When Power Off

During a power outage, the barrier closes, prohibiting access.

Regular Passage Settings

Select the passage method for **Entrance** and **Exit**. The device operates according to the selected passage method throughout the day.

Note

When both the entrance and exit directions are **Controlled**, once one side is authenticated, the other side is not allowed to authenticate until the personnel passage is completed.

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

Tap **Save**.

6.3.2 Person Management

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

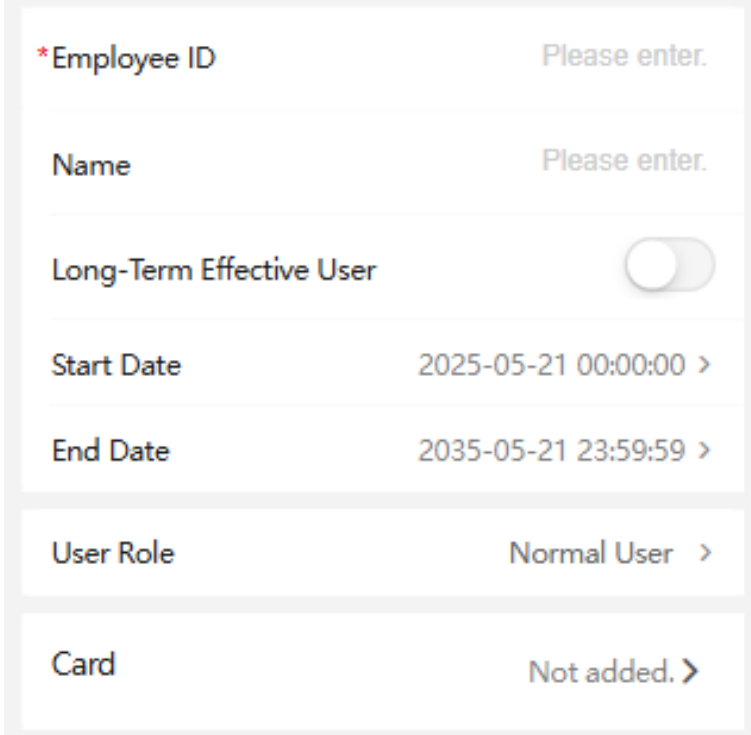


Figure 6-5 Person Management

Add Person Basic Information

On the person management page, tap **+**.
Create the person's employee ID, name, and select a user role.
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**.

6.3.3 Keyfob Settings

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

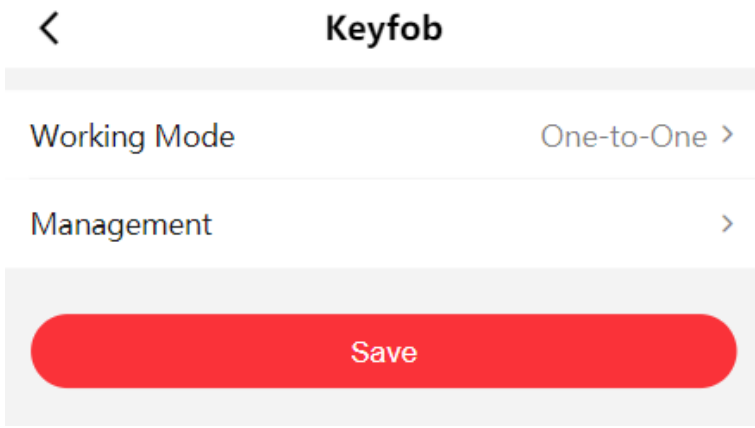


Figure 6-6 Keyfob Settings

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.

6.3.4 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**.

6.3.5 Set Device Time

Set the time zone of the device and the device current time.

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

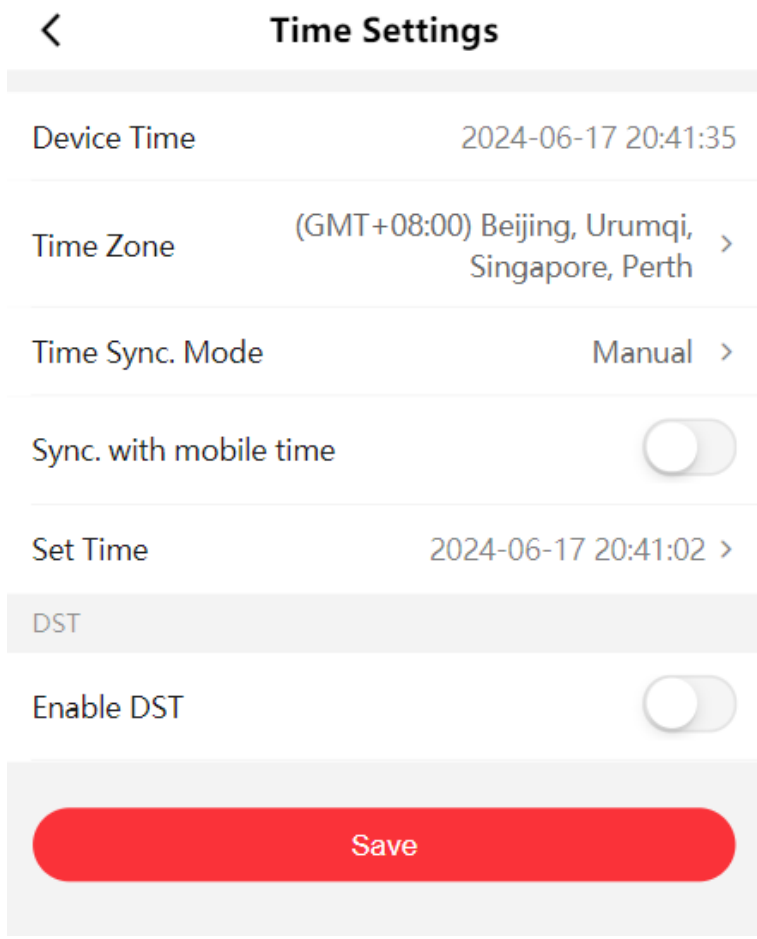


Figure 6-7 Time Settings

Time Zone

Tap to select a time zone for the device.

Time Sync. Mode

Manual

By default, manually synchronization is checked, you can set the device time manually.

NTP

You should Set the NTP server's IP address, NTP port, and interval.

Enable DST

You can enable DST and set the start time and end time of DST. And also you can set the bias.

Tap **Save**.

6.3.6 User Management

Changed the user's password.

On the home page, tap → **User Management**.

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

6.3.7 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 Device Hotspot

After enabling the device hotspot, you can use the mobile phone to connect the hotspot and set.

On the home page, tap → **Network Settings** → **Device Hotspot** .

Slide to **Enable Device Hotspot**, set hotspot's **Name**, enter password and confirm it. Tap **Save**.

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.

Cloud Service Accessing

The device can communicate via cloud service. You can add the device to mobile client and operate.

Steps

1. Tap → **Device Access** → **Hik-Connect** → **Guarding Vision** .
2. Check **Enable**.
3. **Optional:** You can enable **Custom** and edit the server IP address.
4. **Optional:** View the network connection status.
5. **Optional:** You can select to enable video encryption, and set the video encryption password.

   Note

   After the device adding to the mobile App, if you need to start live view, you should enter the video encryption password.
6. **Optional:** Tap **Link with Account** and view the device QR code. Use the App to scan the QR code to add the device.
7. Tap **Save**.

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** .

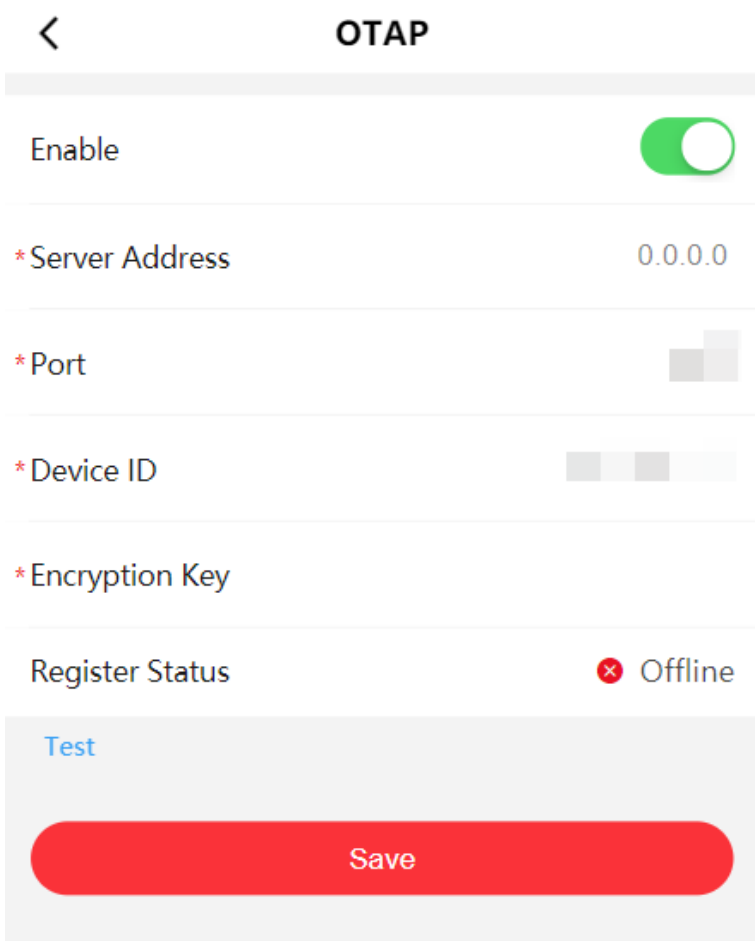


Figure 6-8 OTAP

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**.

6.3.8 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.

6.3.9 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 output volume.

Tap **Save**.

6.3.10 Access Control Settings

Set Authentication Parameters

Set authentication parameters.

Steps

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

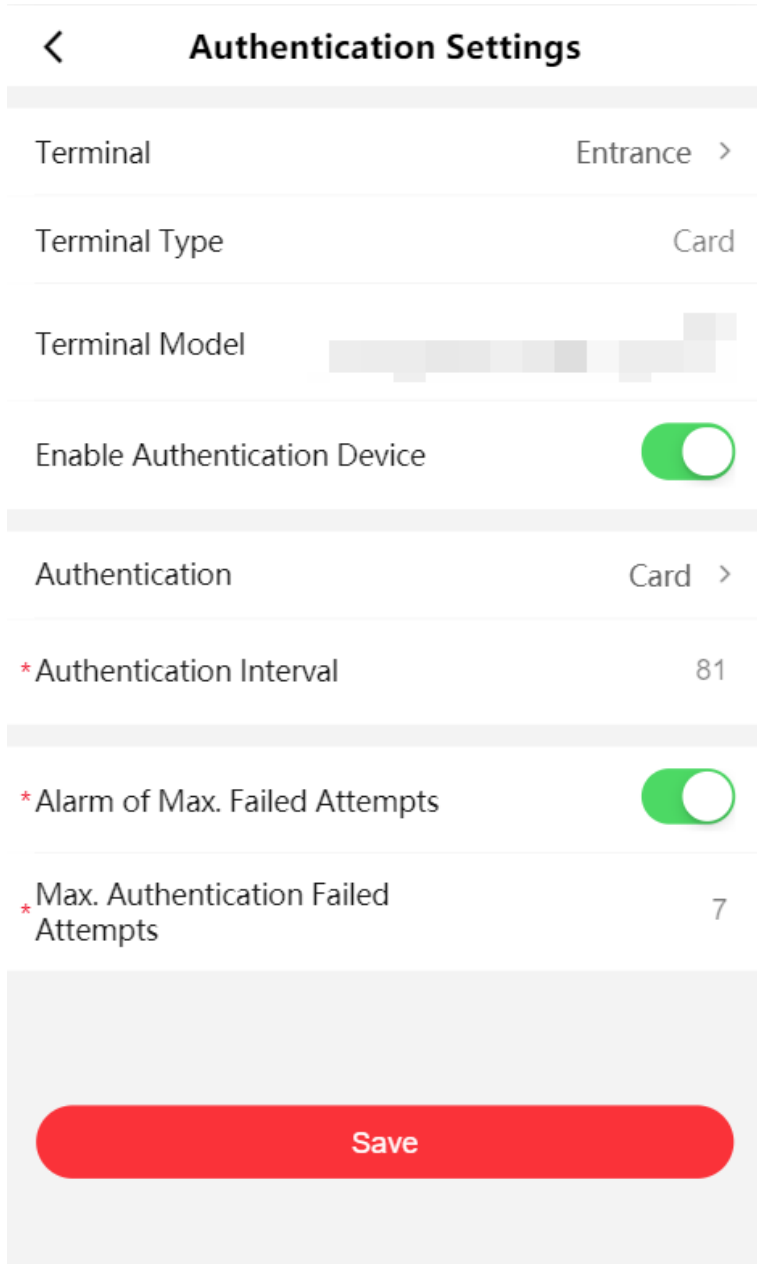


Figure 6-9 Authentication Settings

2. Tap **Save** after configuration.

Terminal

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

Terminal Type/Model

You can view the current terminal type and model.

Enable Authentication Device

The terminal can be used for card swiping normally when the function is enabled.

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 other people authenticate in the configured interval, this person can authenticate again.

Note

The configuration range is 0 to 255 s.

Alarm of Max. Failed Attempts

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

Note

The configuration range is 1 to 10.

Set Door Parameters

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

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

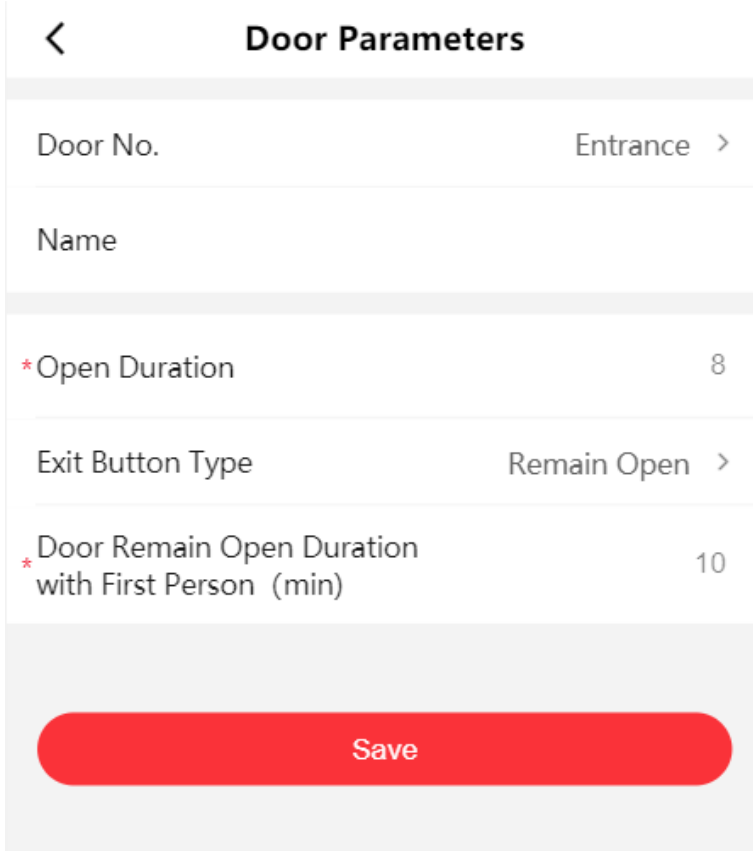


Figure 6-10 Door Parameters

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.

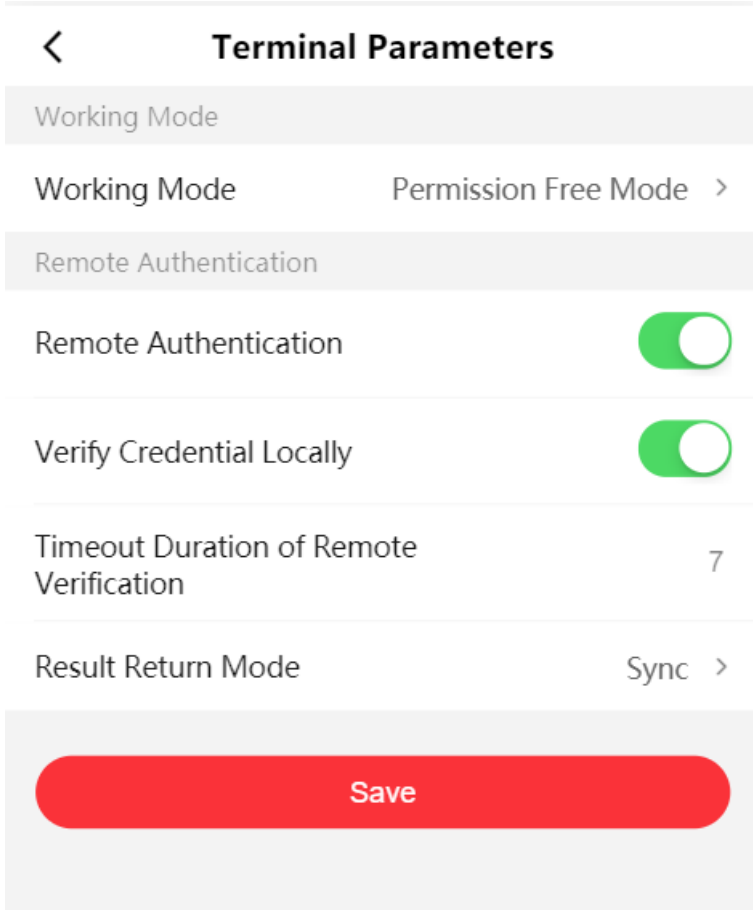


Figure 6-11 Terminal Parameters

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.

Result Return Mode

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

Set Serial Port Parameters

You can connect to access controller ,extension module, or card reader via serial port.

Tap → **Access Control** → **Serial Port Configuration** .

After settings, tap **Save**.

Baud Rate

The baud rate when the devices are communicating via the RS-485 protocol.

Data Bit

The data bit when the devices are communicating via the RS-485 protocol.

Parity/Flow Ctrl/Communication Mode

Enabled by default.

Peripheral Type

Select a peripheral from the drop-down list according the actual situation. You can select from **Card Receiver** or **QR Code Card Reader**

Note

After changing the device type, when you save the parameters, the device will reboot.

Set Card Security

Configure cards for the device.

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

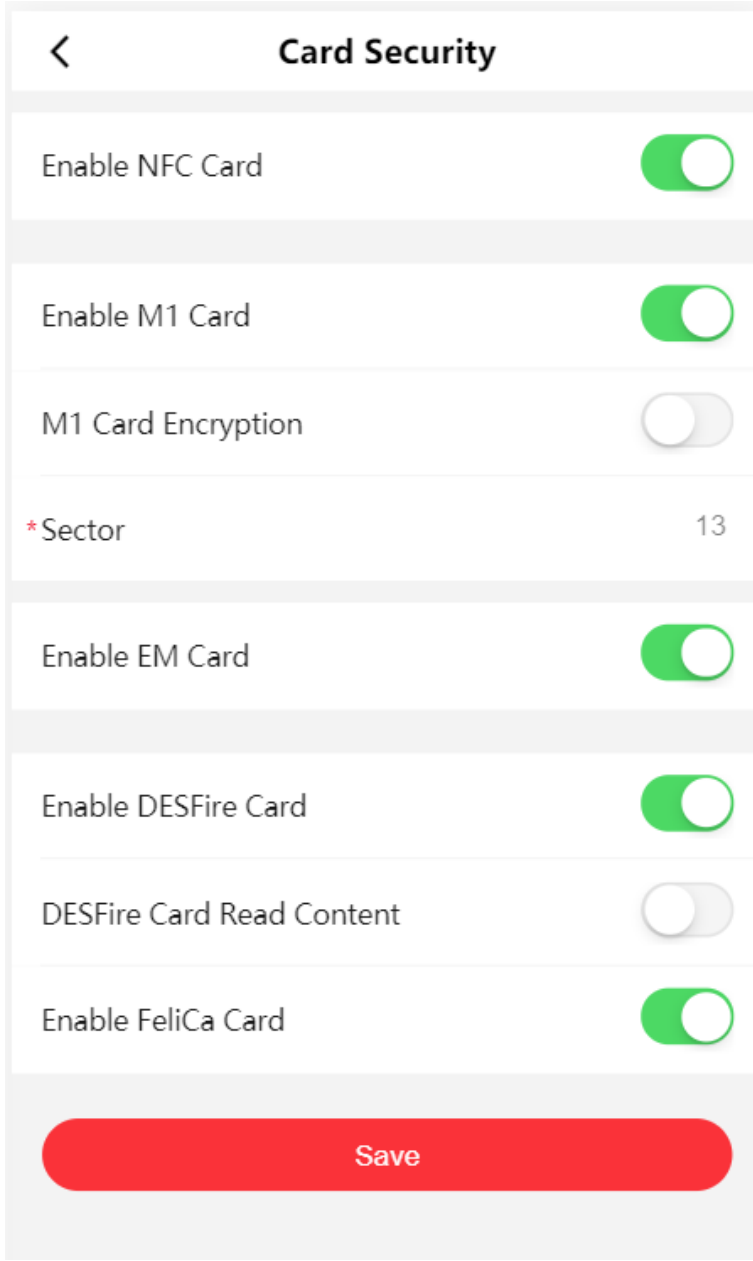


Figure 6-12 Card Security

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.

6.3.11 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 authenticated one and IR triggered one.

   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**.

6.3.12 Other Settings

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

Set the parameters and tap **Save**.

Alarm Output Duration

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

Light Board Brightness

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

QR Code Supplement Light Mode

Set the mode as **Wake-up** or **Solid**.

Wake-up

When there is something closing to the device, the supplement light will be waked up.

Solid

The supplement light of the QR code will be on all the time.

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.

By default, it is disabled.

Fire Input Type

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

6.3.13 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.

6.3.14 System Upgrade & Maintenance

Restart device, restore device and upgrade device.

Restart Device

Tap .
Tap **Restart** to restart the device.

Restore Parameters

Tap → **Default** to enter the settings page.

Restore to Default Settings

All data will be cleared except the network parameters and user account.

Restore to Factory Settings

All functions and parameters will be restored to factory settings. You should activate the device again to use.

Upgrade Device

On home page, tap → **Upgrade**.
Click **Upgrade** to upgrade the device.

Note

The upgrading process will take 1 to 10 minutes. Do not power off. The device will restart automatically after upgrading.

6.3.15 Device Debugging

Manage debugging commands.

Tap → **Device Debugging** .

Debug 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.

6.3.16 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.

6.3.17 Open Source Software Licenses

You can view the open source software licenses.

Tap to enter the page.

Tap **Open Source Software Licenses**.

6.3.18 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 7 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. Stainless Steel Maintenance

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).

Appendix B. Button Configuration Description

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

No.	Description	Default Value	Parameters	Notes
1	Normal/Study Mode	1	1-Normal Mode 2-Study Mode	
2	keyfob Pairing	1	1-Normal Mode 2-Pairing Mode	
3	Passing Mode	1	1-Both sides under control 2-Entrance under control; exit prohibited 3-Entrance under control; exit on inductive mode 4-Both sides on inductive mode 5-Entrance on inductive mode; exit under control 6-Entrance on inductive mode; exit prohibited 7-Both sides prohibited 8-Entrance prohibited; exit under control 9-Entrance prohibited; exit on inductive mode	
4	Memory Mode	2	1-Disable 2-Enable	
5	keyfob Remote Control	2	1-one to one	

No.	Description	Default Value	Parameters	Notes
			1-one to multiple	
6	Barrier Opening Speed	5	1-1, 2-2, …10-10	
7	Barrier Closing Speed	5	1-1, 2-2, …10-10	
8	Card Reading on the Alarm Area	2	1-Do not open 2-Open	
9	Enter Duration	5	2-2s,3-3s, 4-4s, 5-5s, 6-6s, 7-7s, ..., 60-60s	
10	Exit Duration	5	2-2s,3-3s, 4-4s, 5-5s, 6-6s, 7-7s, ..., 60-60s	
11	IR Sensing Duration	0	0-0s, 1-1s, 2-2s,..., 25-25s	
12	Intrusion Duration	0	0-0s, 1-1s, 2-2s,..., 20-20s	
13	Overstay Duration	0	0-0s, 1-1s, 2-2s,..., 20-20s	
14	Delay Time for Barrier Closing	0	0-0s, 1-1s, 2-2s, 3-3s, 4-4s, 5-5s	
15	Control Mode	1	1-Button Configuration 2-DIP Switch on Access Control Board	Unable to change
16	Authentication on Free Passing	1	1-Disable 2-Enable	
17	IR Configuration for Closing in Advance	1	1-1, 2-2, …, N-N	Unable to change
18	Swing Barrier Quantity	1	1-Dual Lanes 2-Single Lane	Unable to change

No.	Description	Default Value	Parameters	Notes
19	Motor Rotation	1	1-Clockwise 2-Anticlockwise	Unable to change
20	Motor Type	1	1-Dunker Motor 2-Control Motor	Unable to change
21	Volume	2	1-0, 2-1, 3-2, 4-3, 5-4	The device will be muted when set to "1".
22	Authenticated Passing	1	1-Disable 2-Enable	Unable to change
23	Invalid Card No.	1	1-Disable 2-Enable	Unable to change
25	Climbing over Barrier	1	1-Disable 2-Enable	
26	Reverse Passing	1	1-Disable 2-Enable	
27	Exceeding Passing Duration	1	1-Disable 2-Enable	
28	Intrusion Alarm	1	1-Disable 2-Enable	
29	Forced Passing	1	1-Disable 2-Enable	Unable to change
30	Tailgating Alarm	1	1-Disable 2-Enable	
31	Unauthorized Passing	1	1-Disable 2-Enable	Unable to change
32	Exceeding Authentication Duration	1	1-Disable 2-Enable	Unable to change
33	Failed Authentication	1	1-Disable 2-Enable	Unable to change
34	Expired Certificate	1	1-Disable	Unable to change

No.	Description	Default Value	Parameters	Notes
			2-Enable	
35	Overstaying Alarm	1	1-Disable 2-Enable	
36	Barrier Material	1	Acrylic	
37	Barrier Length	8	1-550 2-600 3-650 4-700 5-750 6-800 7-850 8-900	
38	Motor Inspection	1	1-Disable 2-Enable on Main Lane 3-Enable on Sub Lane	
39	Brightness of Light	3	0-0, 1-1, 2-2, … , 10-10	The higher the value is, the brighter the light will be.
40	Self-check Voice Prompt	2	1-Disable 2-Enable	Voice prompt of self-check at startup and motor inspection
41	Study Mode Voice Prompt	2	1-Disable 2-Enable	Voice prompt of study mode
44	Barrier Power on Mode	1	1 - Open Barrier When Power Off 2 - Close Barrier When Power Off	
99	Restore to Default	1	1- Default 2- Start	The device will reboot.

Appendix C. Event and Alarm Type

Event	Alarm Type
Passing Timeout	None

Appendix D. Table of Audio Index Related Content

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

Appendix E. Error Code Description

The turnstile 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
Optional Board Offline (If the board is not installed, the error code of "49" or "59" will appear but the device functions normally)	49/59


See Far, Go Further