DS-K6BC402TX Series Swing Barrier

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.

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed

under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

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

COMPLIANCE NOTICE

The thermal series products might be subject to export controls in various countries or regions, including without limitation, the United States, European Union, United Kingdom and/or other member countries of the Wassenaar Arrangement. Please consult your professional legal or compliance expert or local government authorities for any necessary export license requirements if you intend to transfer, export, re-export the thermal series products between different countries.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The equipment must be connected to an earthed mains socket-outlet.
- Shock hazard! Disconnect all power sources before maintenance.
- Do not touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- ϟ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- This equipment is not suitable for use in locations where children are likely to be present.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.
- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
  If the top caps should be open and the device should be powered on for maintenance, make sure:
  1. Power off the fan to prevent the operator from getting injured accidentally.
  2. Do not touch bare high-voltage components.
  3. Make sure the switch's wiring sequence is correct after maintenance.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.

- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- Ensure correct wiring of the terminals for connection to an AC mains supply.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- 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 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

Contents

Chapter 1 System Wiring 1

Chapter 2 Installation 4

Chapter 3 General Wiring 5

3.1 Components Introduction 5

Chapter 4 Terminal Description 7

4.1 General Wiring 7

4.2 Control Board Terminal Description 9

4.3 Access Board 9

4.4 Interface Board 11

4.5 Card Reader 12

4.6 RS-485 Wiring 14

4.7 RS-232 Wiring 15

4.8 Alarm Input Wiring 15

4.9 Exit Button Wiring 15

Chapter 5 Reset Device 17

Chapter 6 Activation 18

6.1 Activate via Web Browser 18

6.2 Activate via Mobile Web 19

6.3 Activate Device via HiTools Delivery 19

6.4 Activate Device via iVMS-4200 Client Software 21

Chapter 7 Configure Device via Mobile Web 23

7.1 Login 23

7.2 Overview 23

7.3 Configuration 26

7.3.1 Turnstile Basic Settings 26

7.3.2 Person Management 28

7.3.3 Device Management 30
7.3.4 Light Settings 32
7.3.5 View Device Basic Information 34
7.3.6 Set Device Time 35
7.3.7 User Management 36
7.3.8 Network 36
7.3.9 Sub Access Control Board Settings 41
7.3.10 Event Search 41
7.3.11 Audio Settings 41
7.3.12 Access Control Settings 42
7.3.13 Set Smart Parameters 51
7.3.14 Turnstile Parameters Settings 54
7.3.15 Upgrade and Maintenance 57
7.3.16 Device Debugging 57
7.3.17 View User Document 58
7.3.18 Open Source Software Licenses 59
7.3.19 Log Out 59
Chapter 8 Operation via PC Web 60
8.1 Login 60
8.2 Forget Password 60
8.3 Quick Operation via Web Browser 60
8.3.1 Time Settings 60
8.3.2 Environment Settings 61
8.3.3 Privacy Settings 61
8.4 Help 62
8.4.1 Open Source Software Licenses 62
8.4.2 View Online Help Document 62
8.4.3 Logout 62

8.5 Overview 62
8.6 Person Management 63
8.7 Device Management 65
8.7.1 Sub Access Control Board Management 65
8.7.2 Batch Devices Management 66
8.8 Turnstile 68
8.8.1 Search Event 68
8.8.2 Paramenter Settings 69
8.8.3 Turnstile Configuration 79
8.9 System and Maintenance 88
8.9.1 Set Local Parameters 88
8.9.2 View Device Information 88
8.9.3 Set Time 88
8.9.4 Change Administrator's Password 89
8.9.5 Online Users 90
8.9.6 View Device Arming/Disarming Information via PC Web 90
8.9.7 Set Working Mode via PC Web 90
8.9.8 Network Settings 91
8.9.9 Set Wiegand Parameters via PC Web 96
8.9.10 Serial Port Settings 97
8.9.11 Elevator Control via PC Web 98
8.9.12 Set Video and Audio Parameters via PC Web 100
8.9.13 Set Image Parameters 100
8.9.14 Event Linkage 101
8.9.15 Prompt Schedule 103
8.9.16 Maintenance 104
8.9.17 Device Debugging 106
8.9.18 Motor Learning 107

8.9.19 Test Protocol via PC Web 108
8.9.20 Set Network Penetration Service via PC Web 108
8.9.21 Component Status 109
8.9.22 View Log via PC Web 109
8.9.23 Advanced Settings via PC Web 110
8.9.24 Certificate Management 110
Chapter 9 Other Platforms to Configure 112
Appendix A. Event and Alarm Type 113
Appendix B. Error Code Description 114

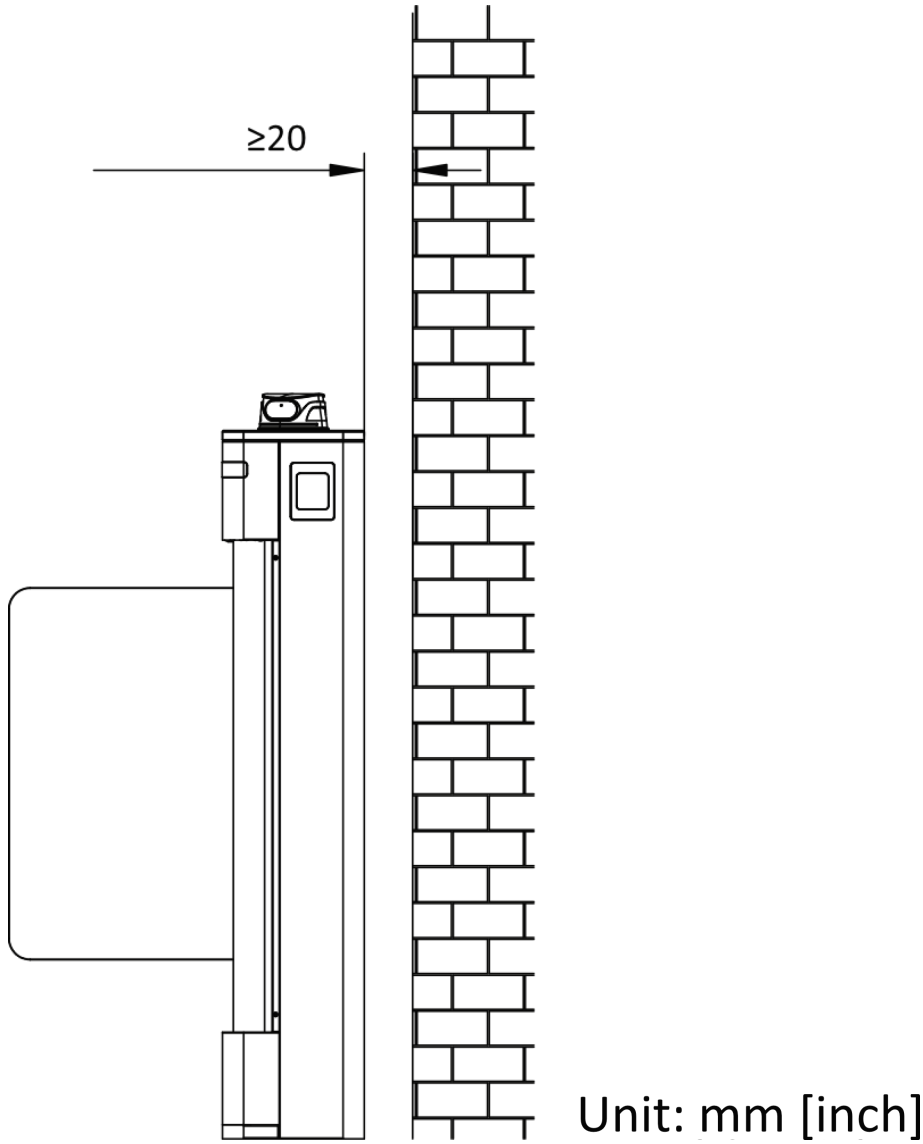
Chapter 1 System Wiring

The preparation before installation and general wiring.

Steps

Note

- The device should be installed on the concrete surface or other non-flammable surfaces.
- If the installation area is too close to the wall, make sure the distance between the pedestal and the wall should be no less than 20 mm, or you cannot open the pedestal's top panel.



- The dimension is as follows.

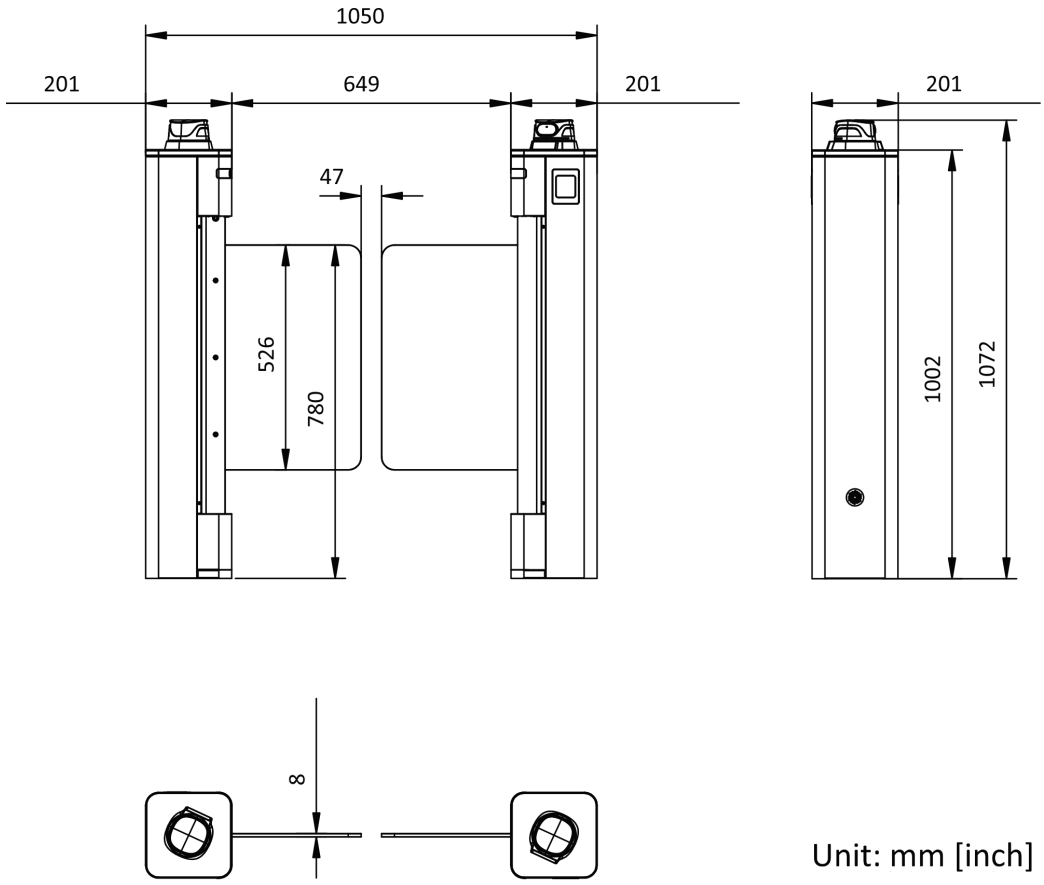


Figure 1-1 Dimension

1. Draw a central line on the installation surface of the left or right pedestal.
2. Draw other parallel lines for installing the other pedestals.

Note

The distance between the nearest two line is L mm. L represents the lane width.

3. Slot on the installation surface and dig installation holes. Put 4 expansion bolts of M12*150 for each pedestal.

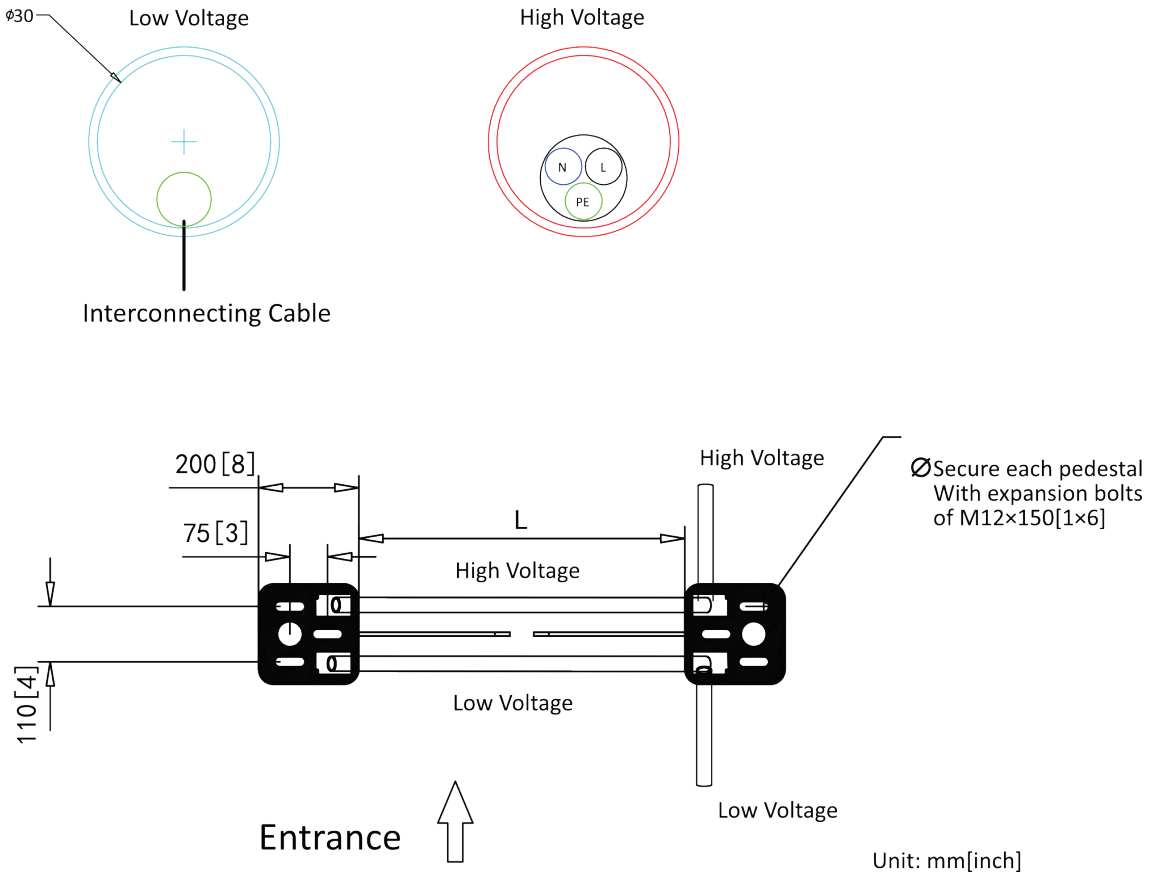


Figure 1-2 Hole Position and System Wiring

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

Note

- High voltage: 200 to 240 V AC, 50 to 60 Hz AC power input.
  Low voltage: 1 interconnecting cable (required for double gates or more), recommended cable length is L + 1.5 m. 1 network communication cable. Network Communication Cable has no length limitation. Pre-installation is suggested for future peripheral connection needs.
- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- If you want to bury both of the AC power cord and the low voltage cable, the two cables should be in separated conduits to avoid interference.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.
- The external AC power cord should be double-insulated.
- The network cable must be CAT5e or the network cable has better performance. And the suggested network cable length should be less than 100 m.
- Before digging holes, evaluate the thickness of the installation surface to avoid puncturing.

Chapter 2 Installation

1. Prepare for the installation tools, check the device and the accessories, and clear the installation base.
2. Position the gate over the pre-installed expansion bolts. Use a Phillips screwdriver to loosen the four screws beneath the top cover and remove it.
3. Release the four clips securing the card reader panels, then slide them backward to remove both side panels.
4. Remove the two screws (per side) with a Phillips screwdriver and detach the side maintenance doors.
5. PPlace the accessories (base clamping plates) over the expansion bolts and align them with the gate edges.
6. Tighten the expansion bolt nuts with an open-end wrench, then reinstall the side maintenance doors to their original positions.

Scan the QR Code to watch the installation guide video.



Chapter 3 General Wiring

3.1 Components Introduction

By default, basic components of the turnstile are connected well. The pedestals can communicate by wiring the interconnecting cables. And the turnstile supports wiring the AC electric supply for the whole system's power supply.

Note

The voltage fluctuation of the electric supply is between 100 VAC and 220 VAC, 50 to 60 Hz.

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

Note

The diagram is for reference only.

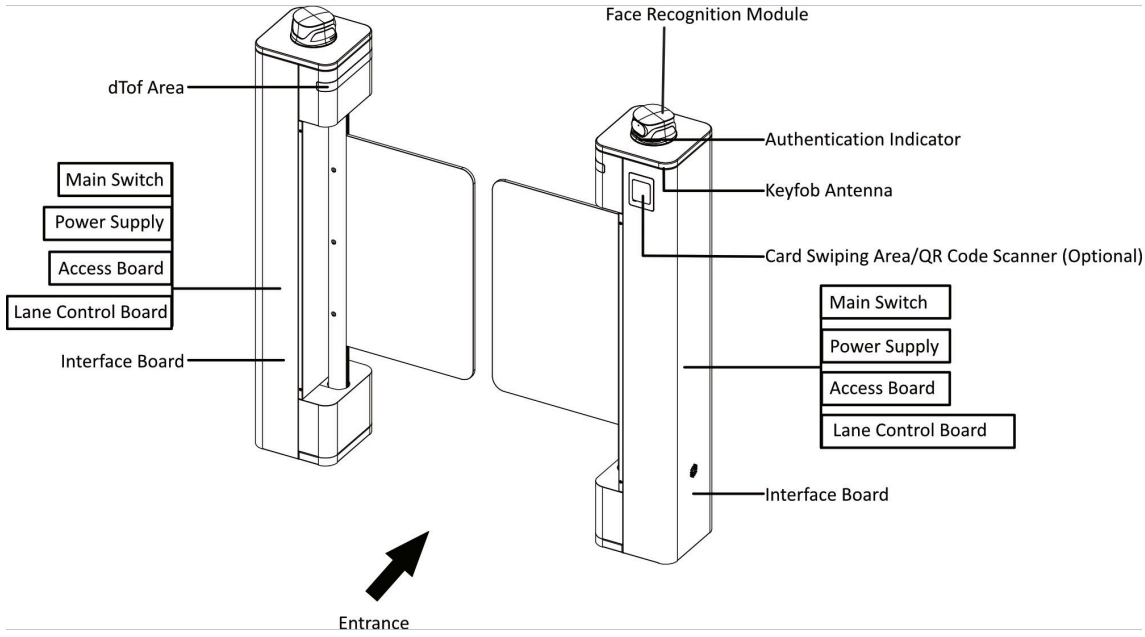


Figure 3-1 Component Diagram

The picture displayed below describes the dTof area and their corresponding number on the pedestal.

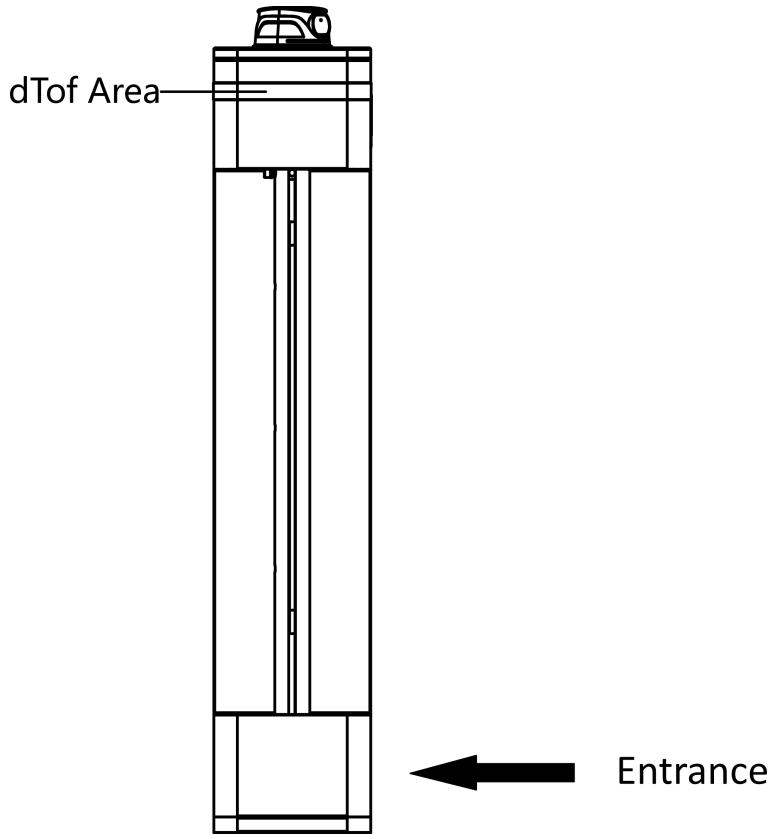


Figure 3-2 dTof Area

Chapter 4 Terminal Description

4.1 General Wiring

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

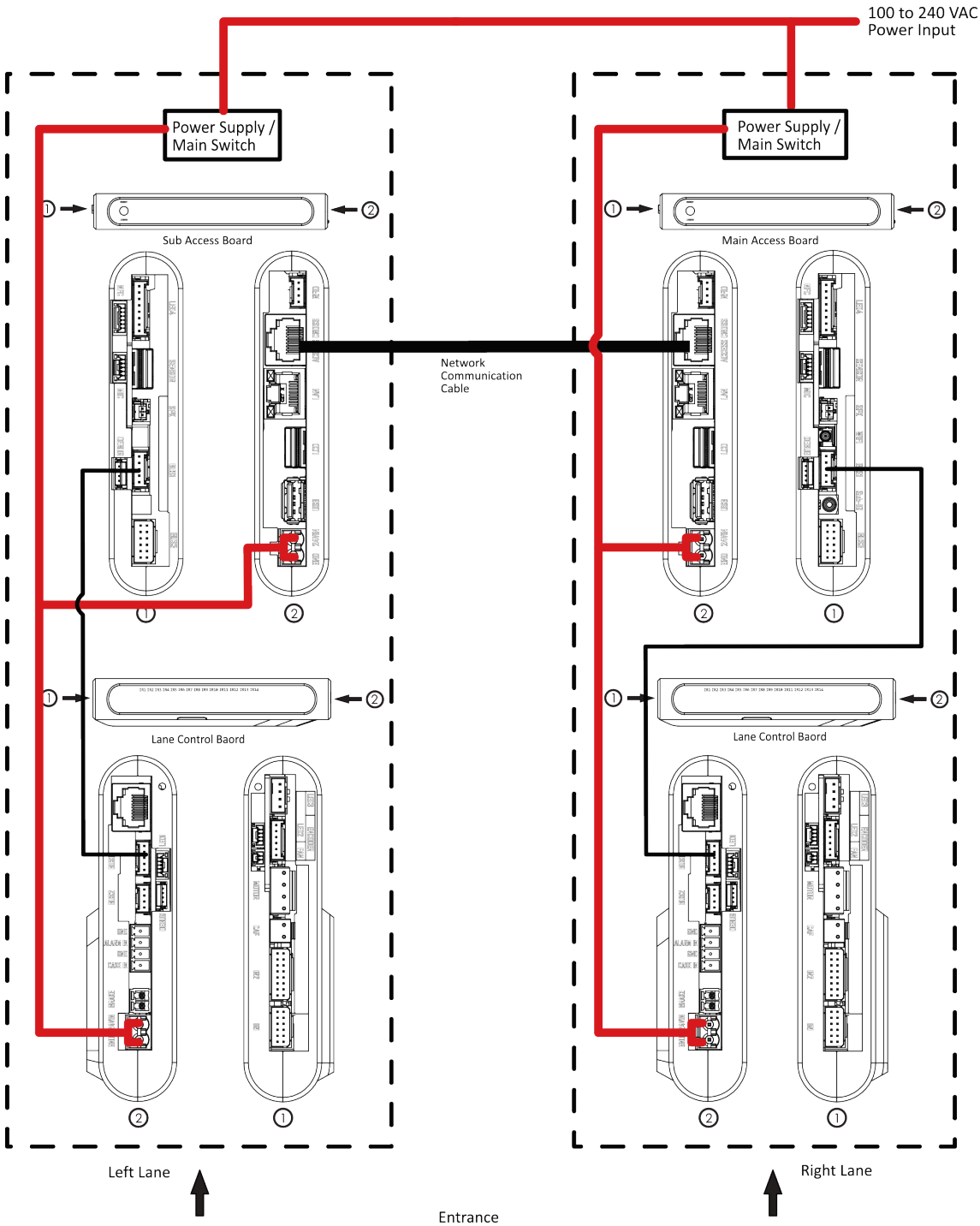


Figure 4-1 General Wiring

Note

- The power cable from power supply to the lane control board has been connected. You will need to prepare the 14AWG power cable to connect the AC power input to power supply.
- • The ① and ② refer to the two sides of a same board.

4.2 Control Board Terminal Description

The picture displayed below is the control board diagram.

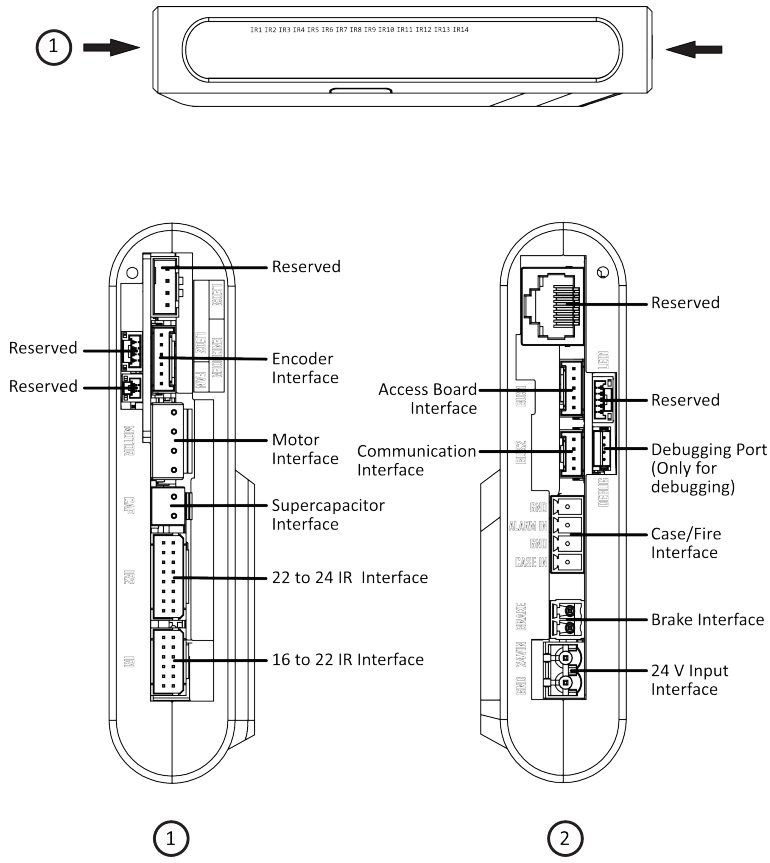


Figure 4-2 Lane Control Board

4.3 Access Board

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

- The diagram is for reference. Interfaces may differ in models.
- Only the main access board of the right pedestal contains SUB-1G antenna interface. Middle access board has no SUB-1G antenna interface.
- Hold the reset button for 5 s, the device will beep twice (main access board only) and start restoring to factory settings.

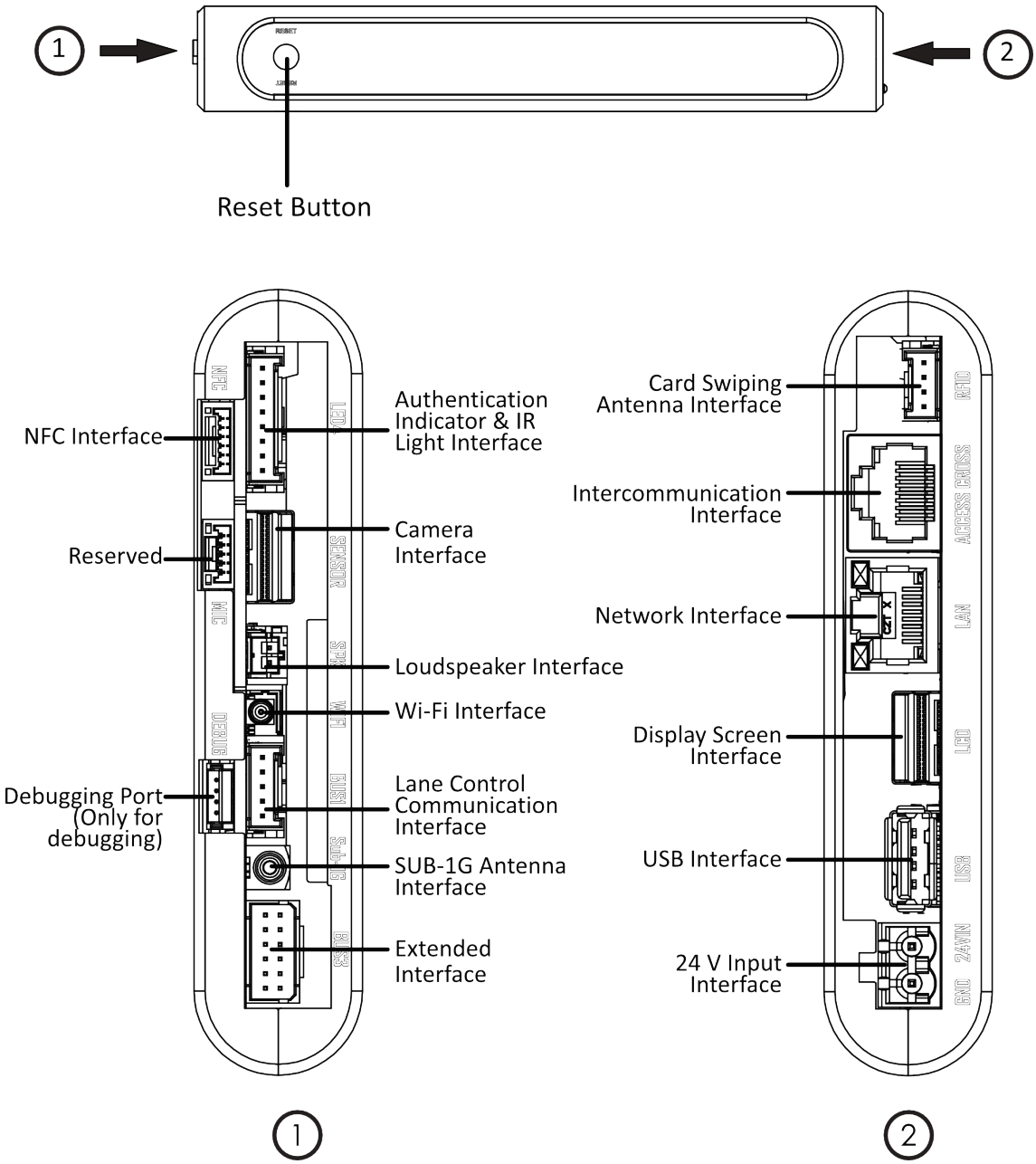


Figure 4-3 Main Access Board

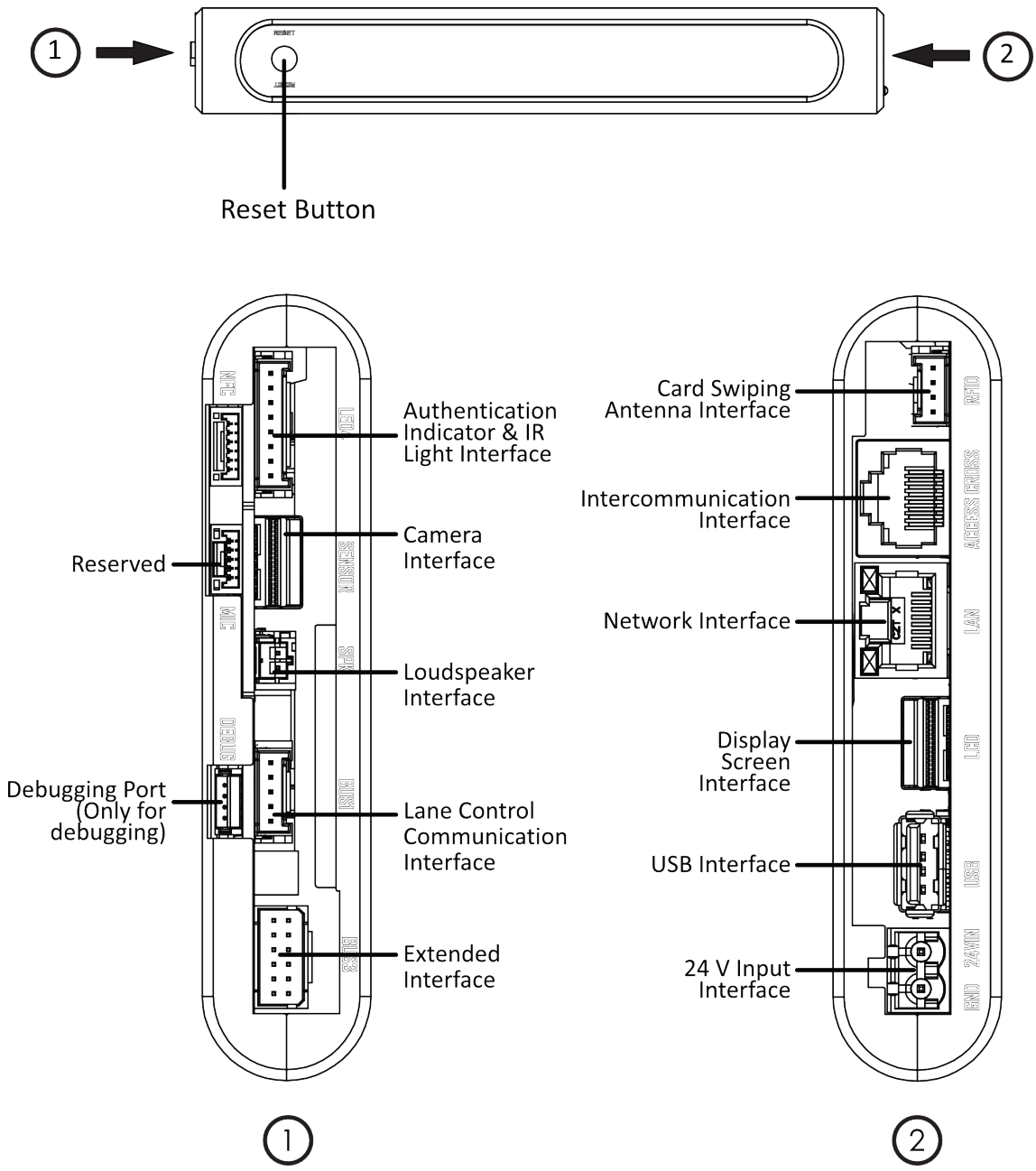
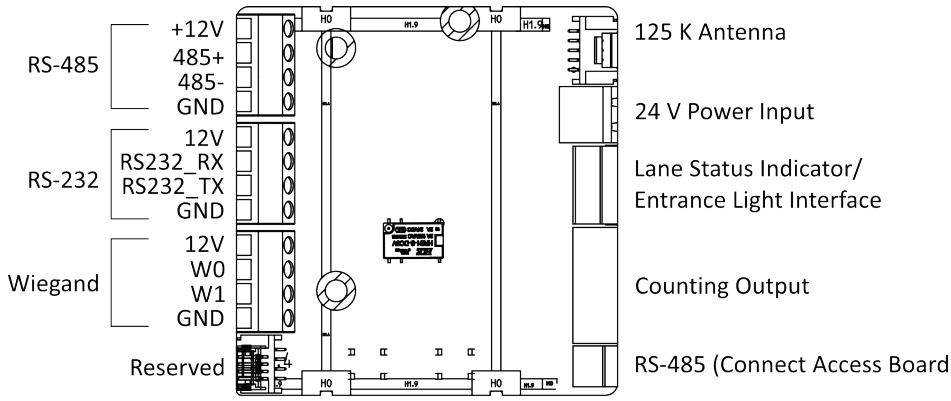


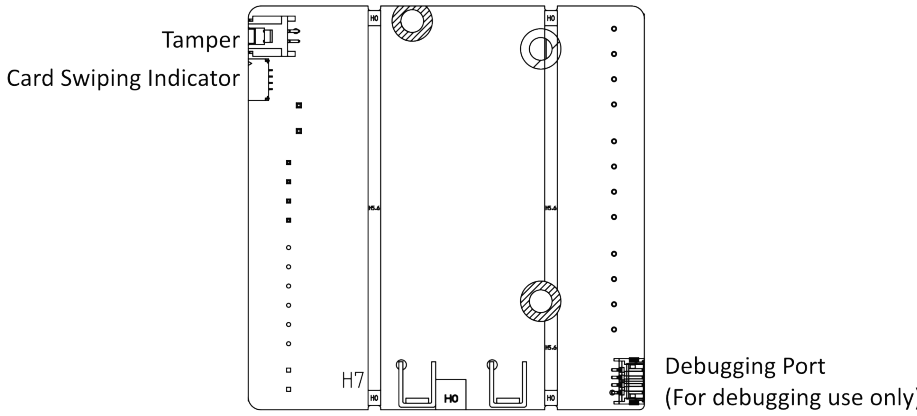
Figure 4-4 Sub Access Board

4.4 Interface Board

The picture displayed below is the interface board diagram.



Front View



Rear View

Figure 4-5 Interface Board

4.5 Card Reader

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

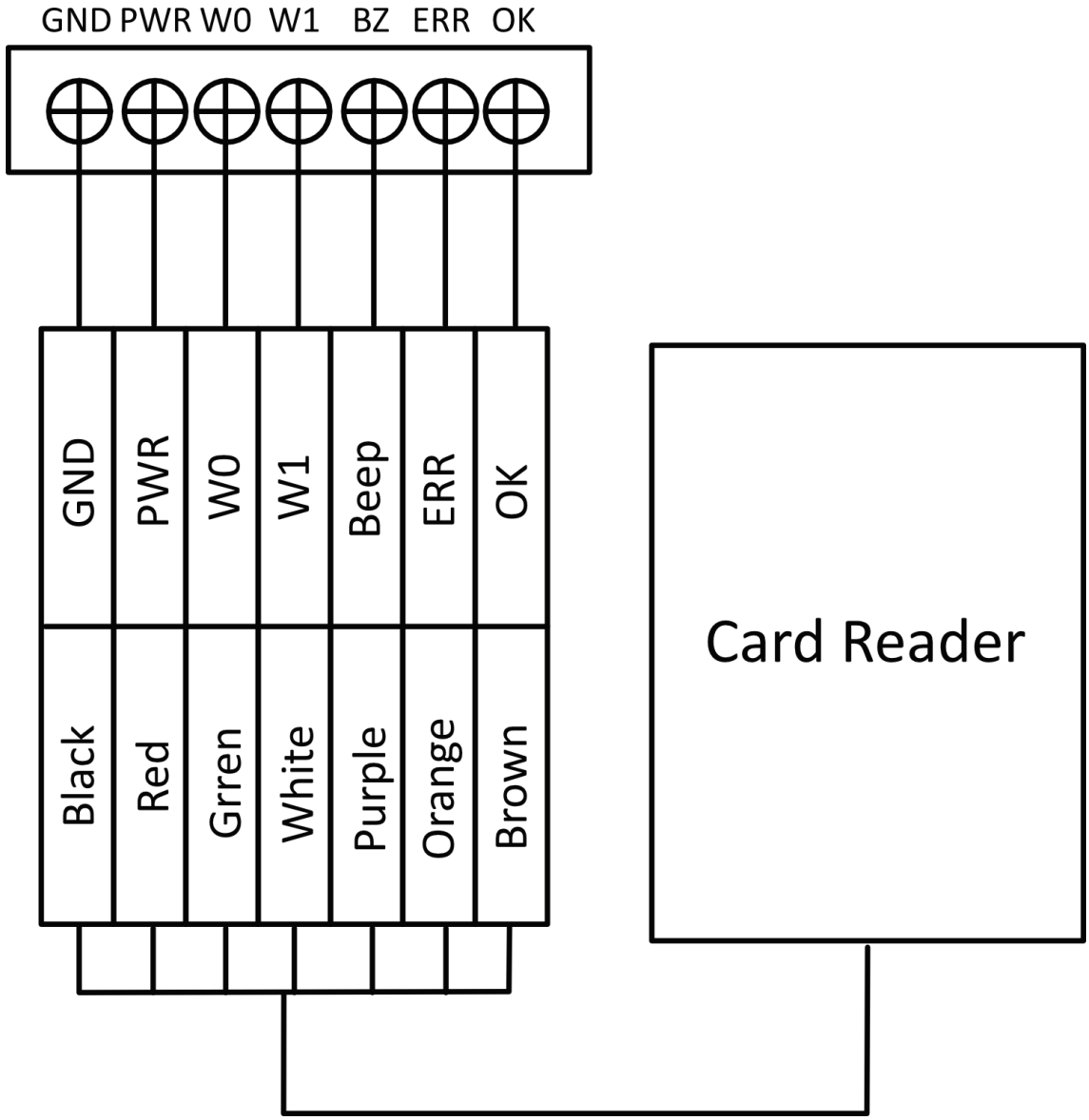
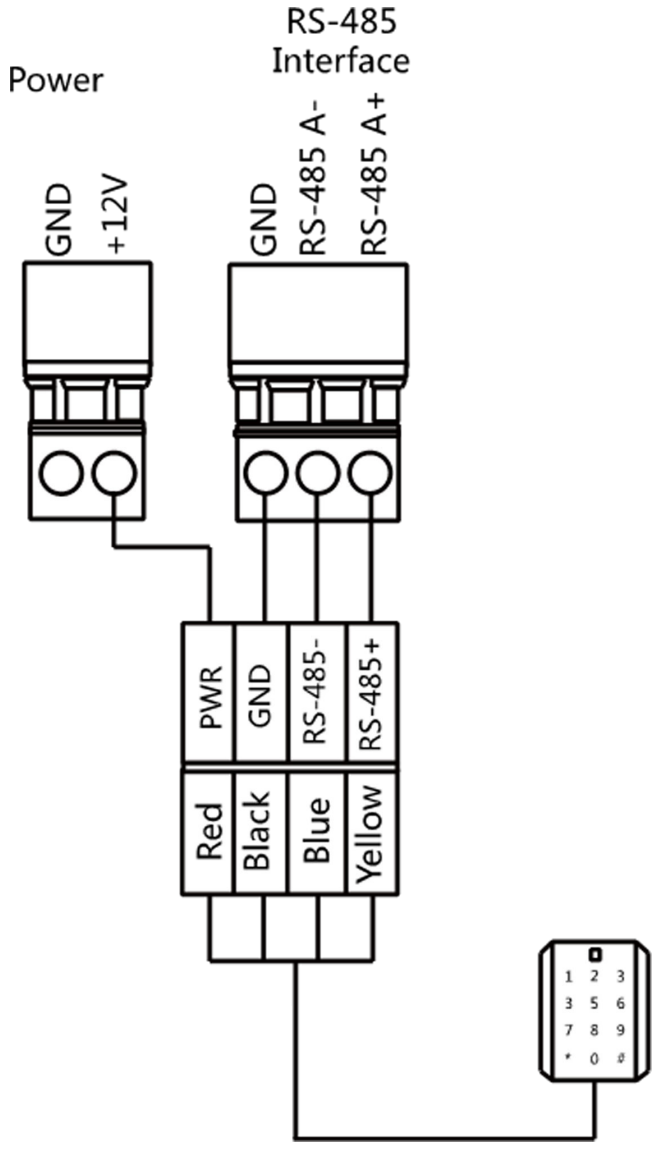


Figure 4-6 Card Reader

4.6 RS-485 Wiring



4.7 RS-232 Wiring

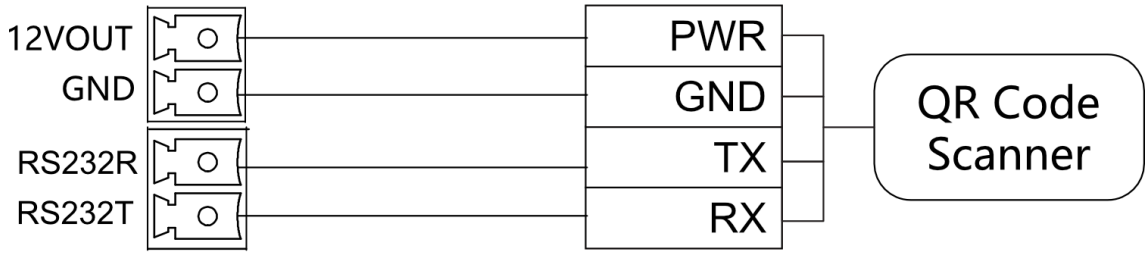


Figure 4-7 RS-232 Wiring

4.8 Alarm Input Wiring

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

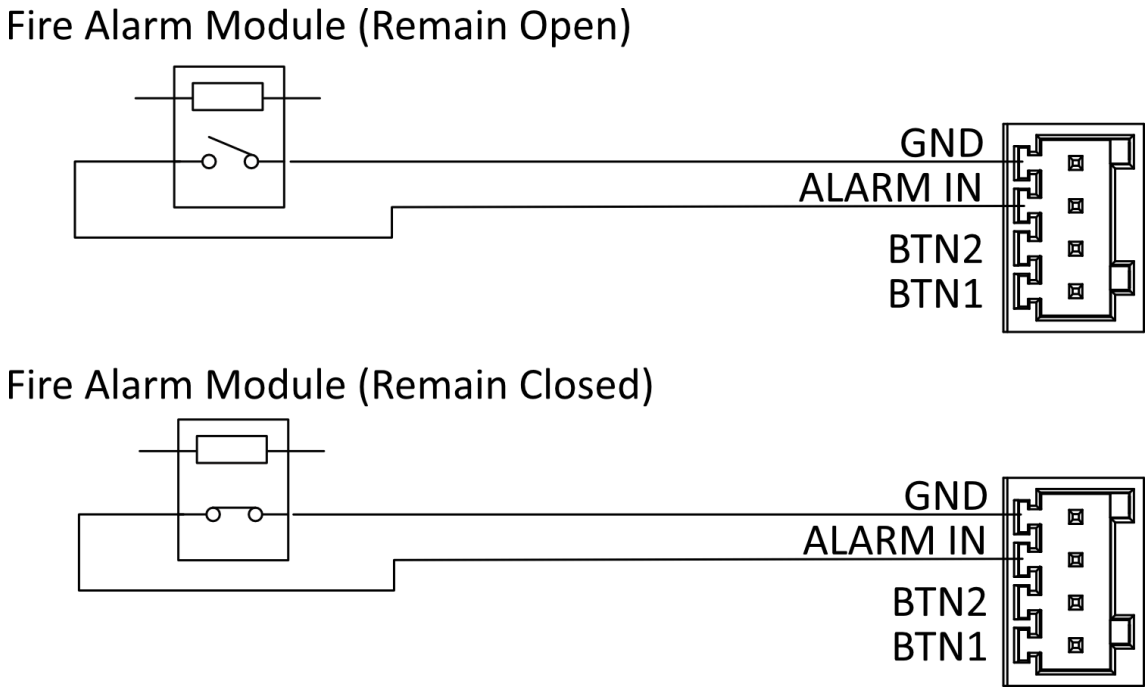


Figure 4-8 Alarm Input

4.9 Exit Button Wiring

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

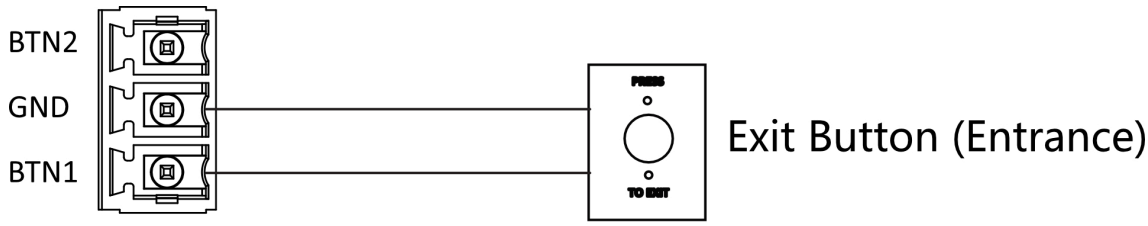


Figure 4-9 Exit Button Wiring (Entrance)

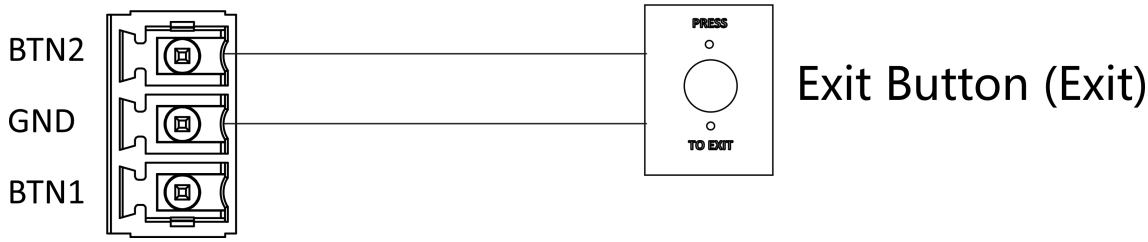


Figure 4-10 Exit Button Wiring (Exit)

Note

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

Chapter 5 Reset Device

Steps

1. Hold the reset button.

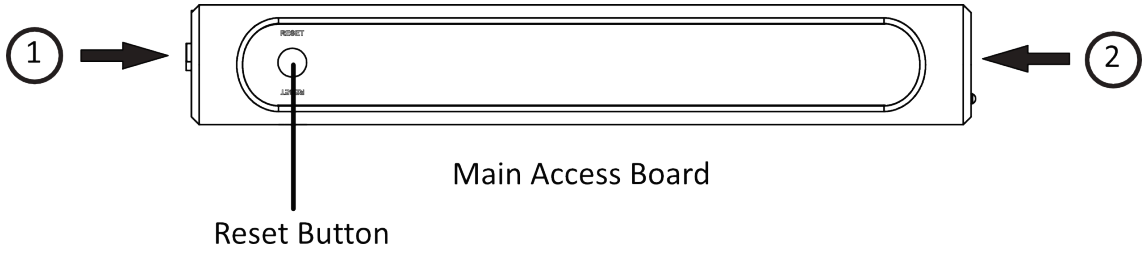


Figure 5-1 Initialization Reset Position

2. Hold the reset button for 5 s, the device will beep twice (main access board only) and start restoring to factory settings.

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.

The resetting is completed.

Chapter 6 Activation

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

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

The default values of the device are as follows:

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

6.1 Activate via 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

   - 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.
   - Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
   - Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

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.

6.2 Activate via Mobile Web

You can activate the device via mobile web.

Steps

1. Connect to the device hotspot with your mobile phone by entering the hotspot password.

   Note

   - For inactive devices, hotspot is enabled by default.
   - The default hotspot password is the device serial number.

   The login page will pop up.
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.

6.3 Activate Device via HiTools Delivery

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

Before You Start

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

Steps

1. Run the software.
2. Click **Home Page → Search → Current Subnet** . Click **Refresh**, and the list will display all the online devices in the same network segment.

3. Select the inactive device(s) in the list. Set a new password according to the popup requirements and confirm the password.
4. Click **Activation**. The device activation status will change to **Activated** after successful activation.

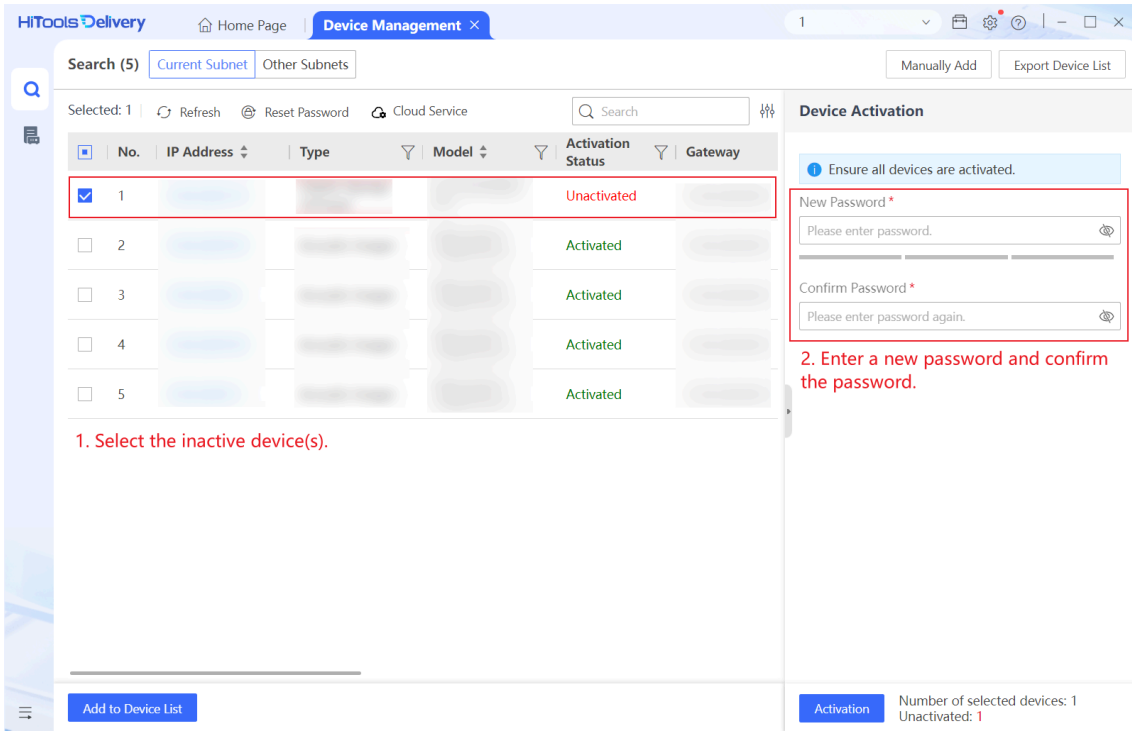


Figure 6-1 Activation

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

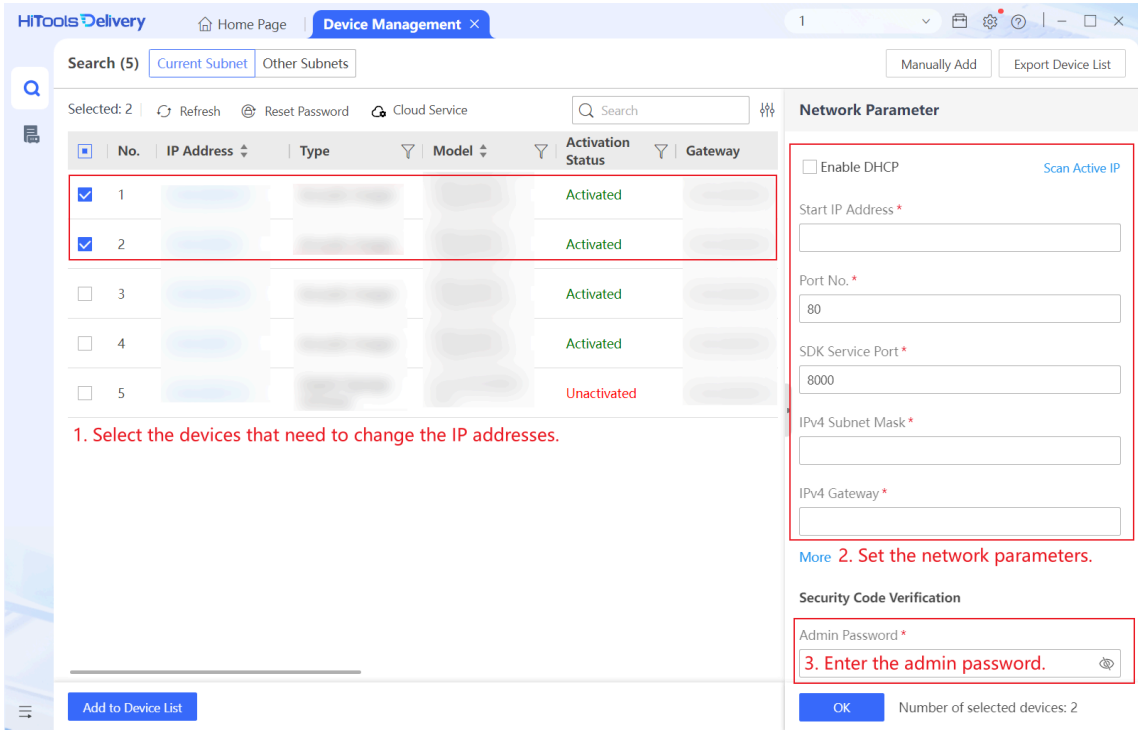


Figure 6-2 Modify Network Parameters

Note

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

6.4 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 7 Configure Device via Mobile Web

7.1 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.

7.2 Overview

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

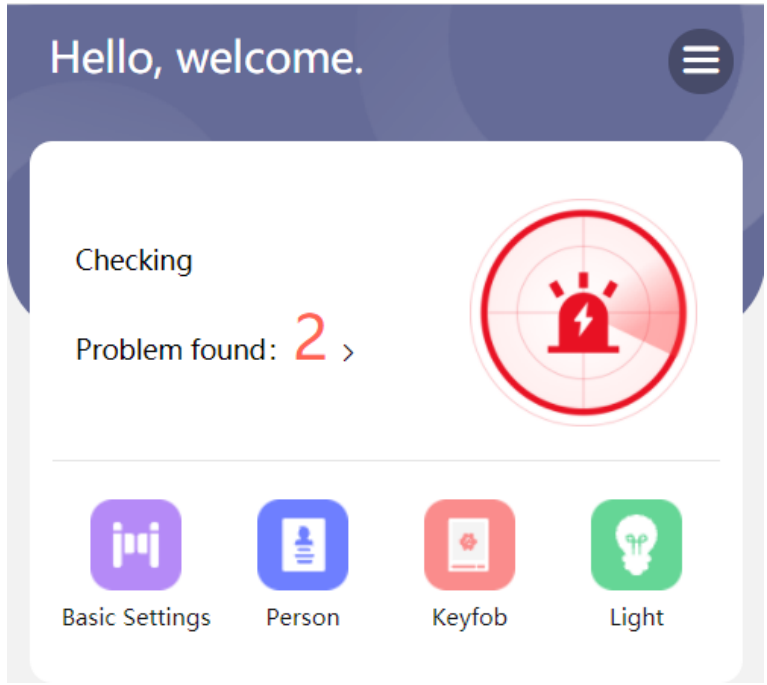


Figure 7-1 Status and Quick Settings

You can view the device status. If there is exception, you can tap to view the component details. You can tap to fast enter the basic settings page, person page, device page and light page.

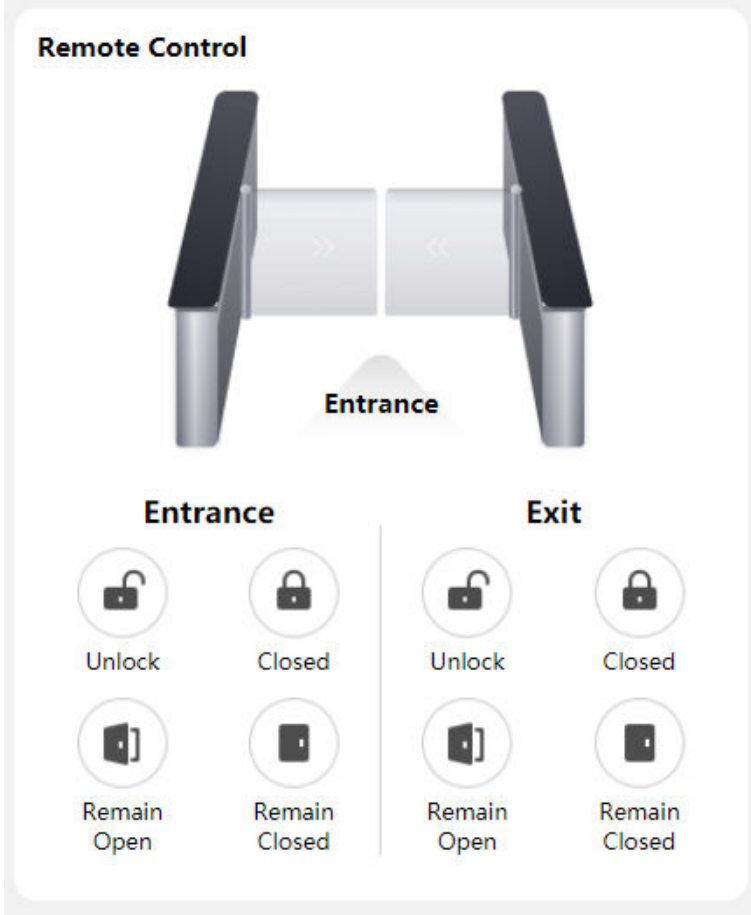


Figure 7-2 Remote Control

You can remotely control barrier by tap the icons.

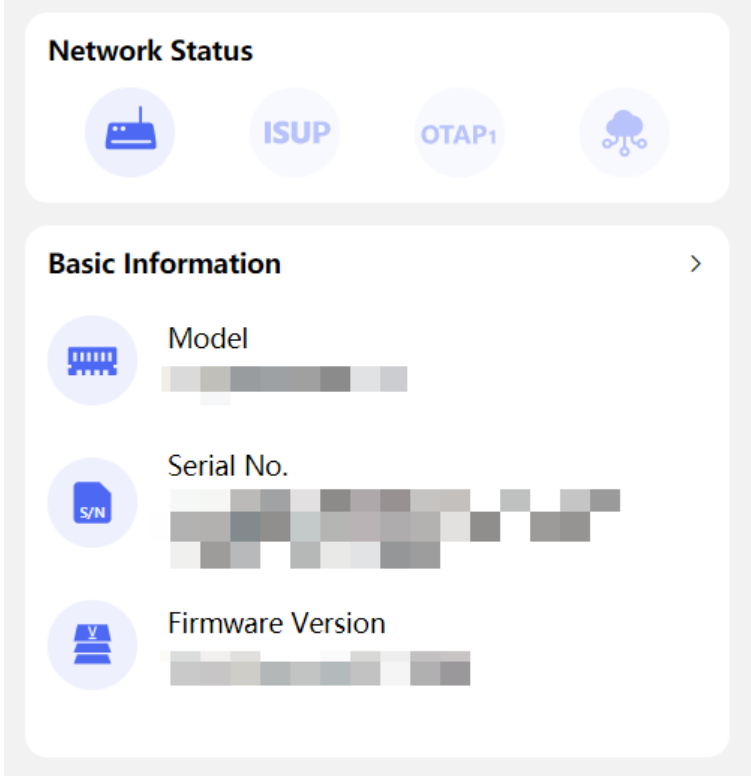


Figure 7-3 Network Status and Basic Information

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

7.3 Configuration

7.3.1 Turnstile Basic Settings

You can set the basic parameters of the turnstile.

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

Note

Lane width, barrier height, and barrier material must be filled in; otherwise, the barrier will not operate properly.

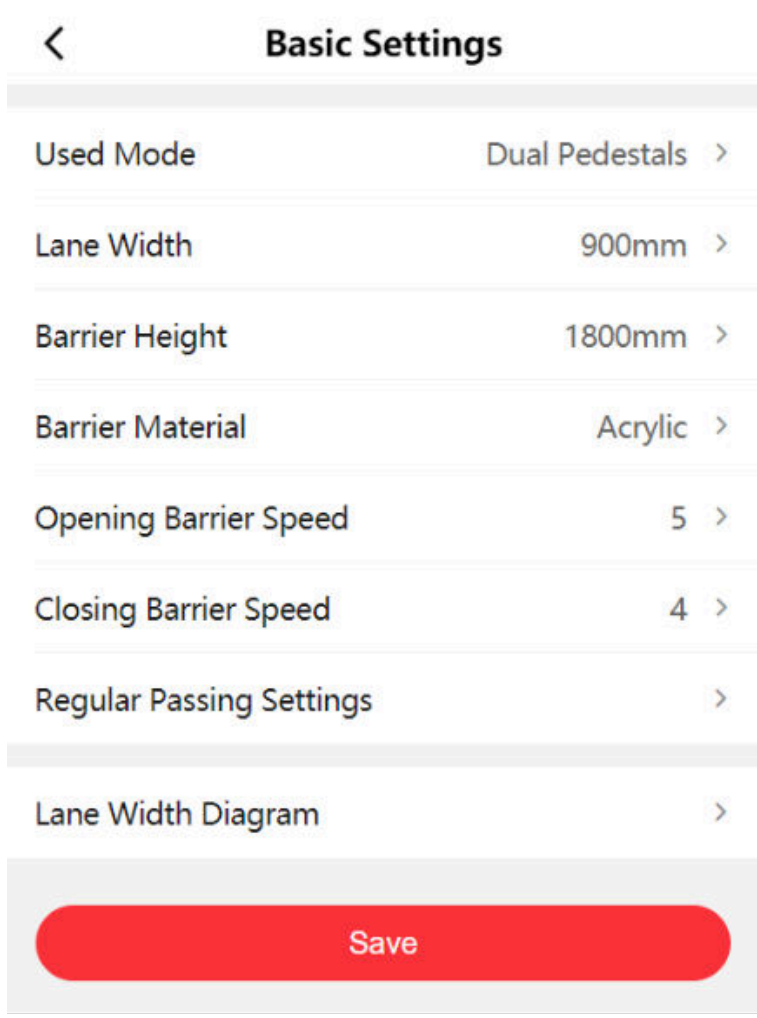


Figure 7-4 Turnstile Basic Parameters

Set **Used Mode**, **Lane Width**, **Barrier Material**, **Barrier Opening Speed** and **Barrier Closing Speed**.

Used Mode

Select **Single Pedestal** or **Dual Pedestals** according to actual needs.

Single Pedestal

When you only use one pedestal, you should select this option.

Dual Pedestals

When you only use dual pedestals, you should select this option.

Lane Width

Select a lane width according to actual situation.

Barrier Height

Select a barrier height according to actual situation.

Barrier Material

Select a barrier material according to actual situation.

Barrier Opening Speed/Barrier Closing Speed

Set the barrier opening or closing speed.

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

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

Tap **Save**.

7.3.2 Person Management

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

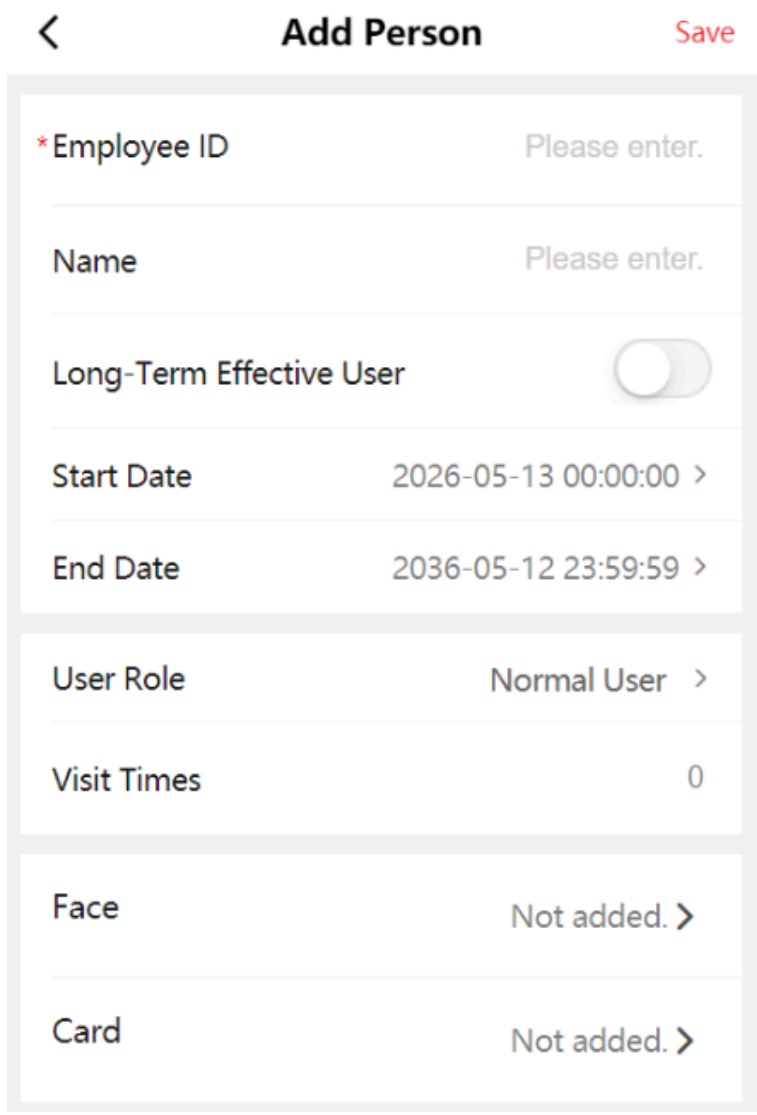


Figure 7-5 Person Management

Add Person Basic Information

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

Add Face Picture

On the person management page, tap **+ → Face**.
Tap **+**, take a picture or select a picture.

Tap **Save**.

Add Card

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

Set Person Permission

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

Person Management

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

7.3.3 Device Management

The mobile web can automatically detect online devices (main access controller) that are in the same network segment as the current mobile phone and automatically obtain the identified device information. You can view the model, activation status, IP, serial number, software version, gateway address, and IPv4 subnet mask of all devices in the same network segment. You can also view a single device's IP address of the main/sub access controller, synchronize the parameters with the sub access controller of the device, and edit the name of the main access controller of a the device. Batch network configuration, parameter synchronization, and device activation are also available for devices.

Tap**Batch Manage Devices** or tap → **Device Management → Batch Manage Devices** to enter the page.

Inactivated Device

You can do the following operations for the inactivated devices.
Tap and set the main access controller’s network of the device. Enter the administrator's password and tap **OK**.

DHCP

If disable the function, you should manually set IPv4 address, IPv4 subnet mask, and IPv4 default gateway.

If enabled the function, the system will allocate IPv4 address, IPv4 subnet mask, and IPv4 default gateway.

IPv6 Mode

Manual

Manually set IPv6 address, IPv6 subnet prefix length, and IPv6 default gateway.

DHCP

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

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.

Activated Devices

You can do the following operations for the activated devices.
Click a device in the list. Tap **Network Settings**. You can view the main access controller and sub access controller's basic information and set the network. Enter the administrator's password and tap **OK**.

DHCP

If disable the function, you should manually set IPv4 address, IPv4 subnet mask, and IPv4 default gateway.

If enabled the function, the system will allocate IPv4 address, IPv4 subnet mask, and IPv4 default gateway.

IPv6 Mode

Manual

Manually set IPv6 address, IPv6 subnet prefix length, and IPv6 default gateway.

DHCP

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

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.

Click a device in the list. Tap **Sync Parameters**. You can synchronize the selected device with this device. Enter the administrator's password and tap **Confirm**.
Tap and you can set the name of the main access controller of the device. Enter the administrator's password and tap **Save**.

Batch Settings

You can do the following batch operations for devices.
On the Activated page, tap **Set Network Parameters**. Select the devices that you need to set network, and tap **Set Network Parameters**. After network settings, tap **OK**.

DHCP

If disable the function, you should manually set IPv4 address, IPv4 subnet mask, and IPv4 default gateway.

If enabled the function, the system will allocate IPv4 address, IPv4 subnet mask, and IPv4 default gateway.

IPv6 Mode

Manual

Manually set IPv6 address, IPv6 subnet prefix length, and IPv6 default gateway.

DHCP

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

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.

On the Activated page, tap **Batch Parameters Sync**. Select the devices that you need to set network, and tap **Batch Parameters Sync**. You can synchronize the selected devices with this device. Enter administrator's password and tap **Confirm**.
On the Inactivated page, tap **Batch Activate**. Select the devices that you need to activate, and tap **Batch Activate**. Enter administrator's password and tap **Confirm**.

7.3.4 Light Settings

Tap **Light** of the shortcut entry on the overview page. Or tap → **Light** .

Lane Status Indicator

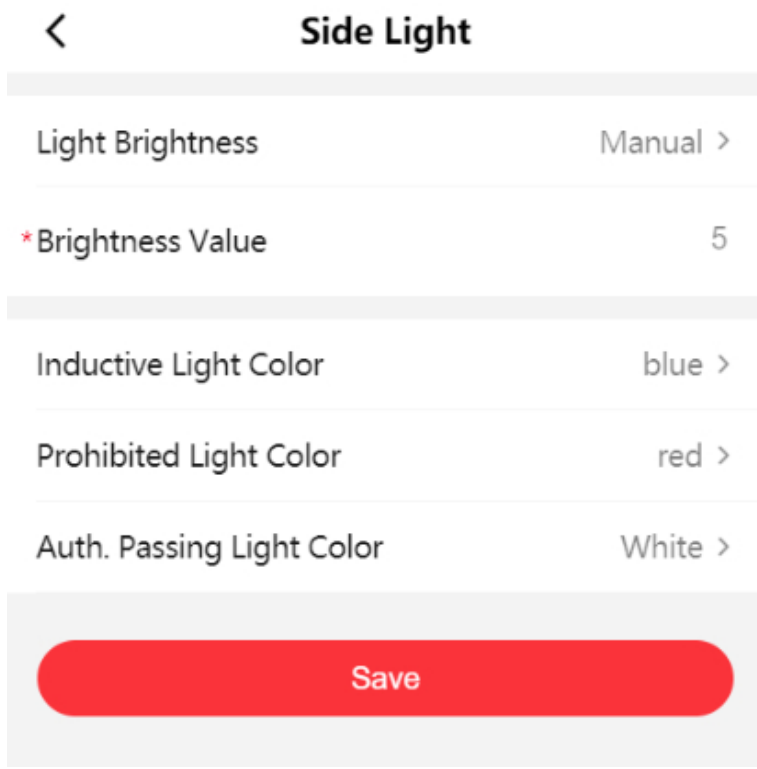


Figure 7-6 Lane Status Indicator Settings

Light Brightness is set **Manual** by default. Enter the value to adjust the light brightness manually. Set light color for inductive/remain open, remain closed and controlled/barrier-free mode respectively.

Barrier Light

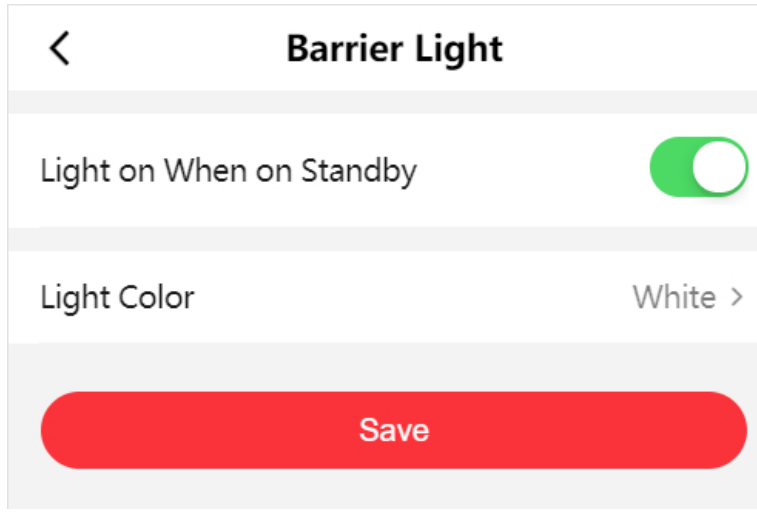


Figure 7-7 Barrier Light Settings

Tap to enable **Light on When on Standby** at your actual needs and set the barrier light color.

Camera Indicator Light

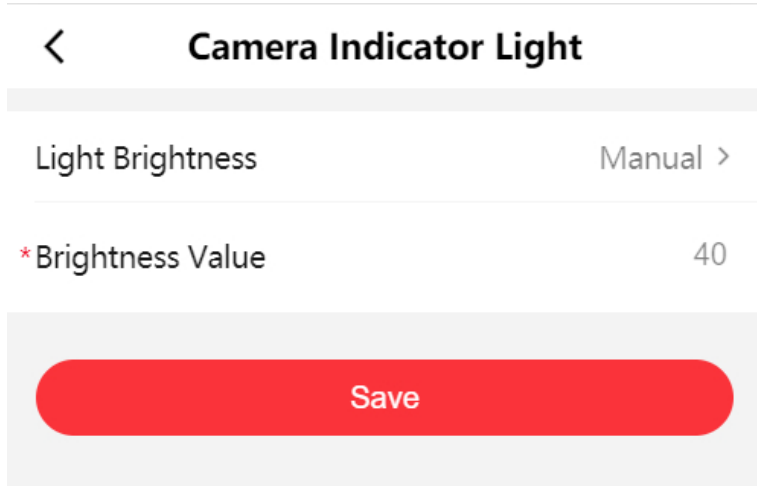


Figure 7-8 Camera Indicator Light Settings

Select **Auto** or **Fixed Brightness** for the camera light.

7.3.5 View Device Basic Information

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

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

You can change the device name.

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

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

Tap **Save**.

7.3.6 Set Device Time

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

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

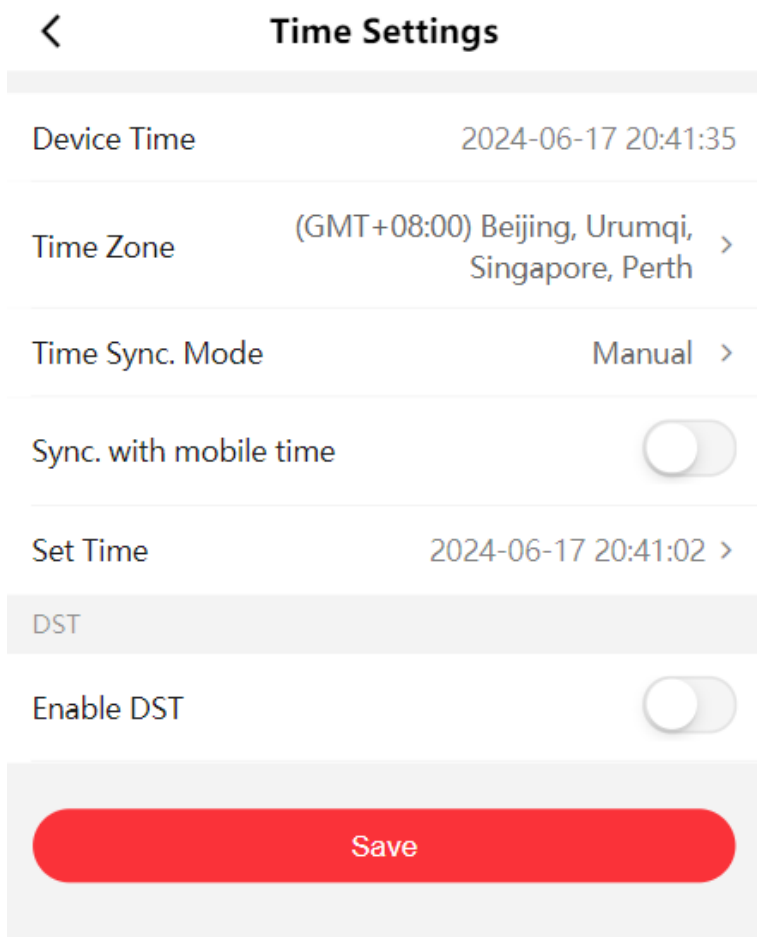


Figure 7-9 Time Settings

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**.

7.3.7 User Management

You can change user password.

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

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

Tap **Save**.

7.3.8 Network

Wired Network

Set wired network.

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

NIC Type

Select a NIC type from the drop-down list.

DHCP

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

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

MAC Address and MTU

You can view the default MAC address and MTU.

IPv6 Mode

Route Advertisement

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

Note

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

Manual

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

DHCP

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

DNS Server

Note

Only when DHCP is enabled can DNS server be set.

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

Set 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.

Platform Access

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

Steps

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

Note

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

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

Note

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

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

Set ISUP Parameters

Set the ISUP parameters for transmitting logs via ISUP protocol.

Tap → **Device Access → ISUP**.

Slide **Enable** to enable ISUP.

Set the server address and port.

Note

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

Tap **Save**.

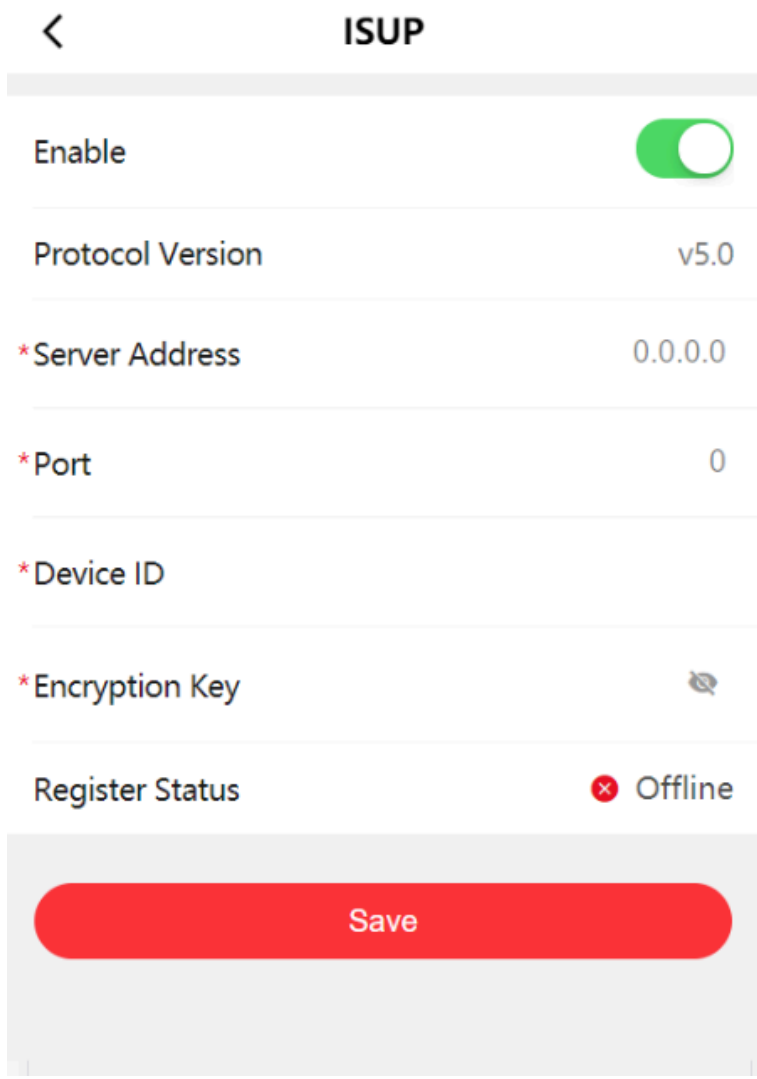


Figure 7-10 ISUP Settings Page

Set OTAP Protocol

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

Steps

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

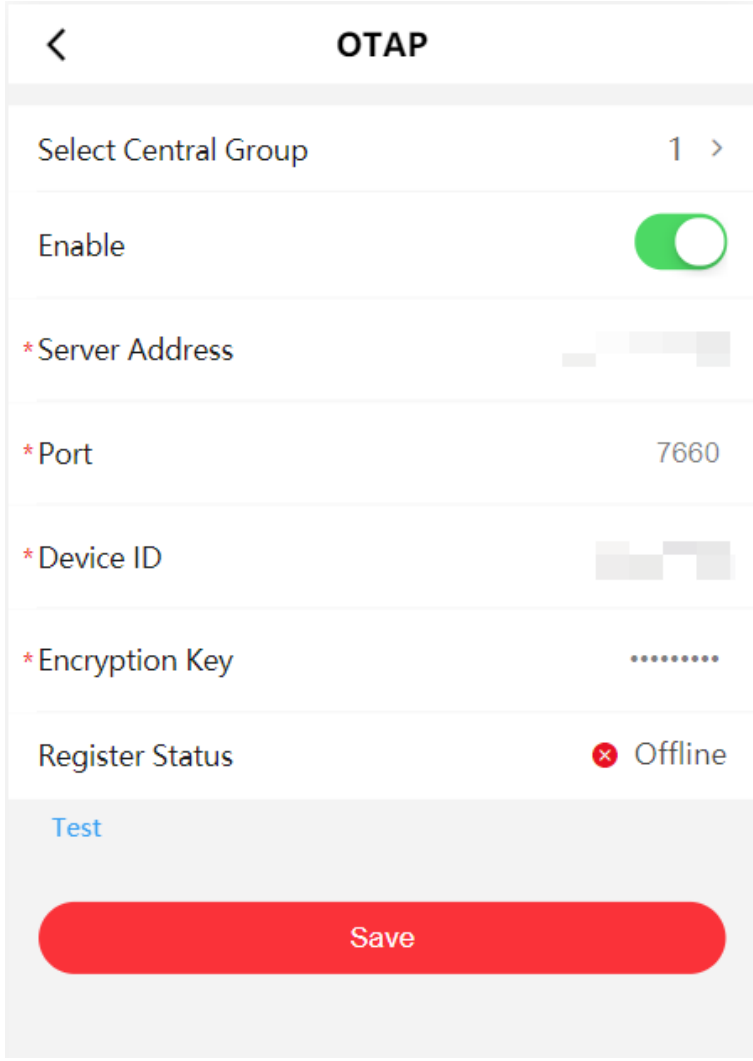


Figure 7-11 OTAP

2. Select 1 or 2 from **Select Central Group**.
3. Slide **Enable**.
4. Set server address, port, device ID and encryption key.
5. Tap **Test**, and make sure the device can connect to the server and registration completed.
6. Tap **Save**.

Result

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

Set Network Penetration Service

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

Steps

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

7.3.9 Sub Access Control Board Settings

The mobile web automatically detects the sub access controller paired with the IP address of the current computer. You can view the information of the sub access controller of the device and set network parameters.

Steps

1. Tap → **Device Management** → **Sub Access Control Board** .
2. Tap **Network Settings** and set the IP address, gateway address, subnet mask, and communication port. Enter the administrator's password and tap **Save**.
3. Tap **Device Details** and you can view the device name, language, model, serial No., version, and alarm input/output number.

7.3.10 Event Search

Tap → **Event Search**.

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

Note

Support searching for names within 32 digits.

The result will display in the list.

7.3.11 Audio Settings

You can enable or adjust the audio.

Tap → **Audio**.

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

7.3.12 Access Control Settings

Set Authentication Parameters

Set authentication parameters.

Steps

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

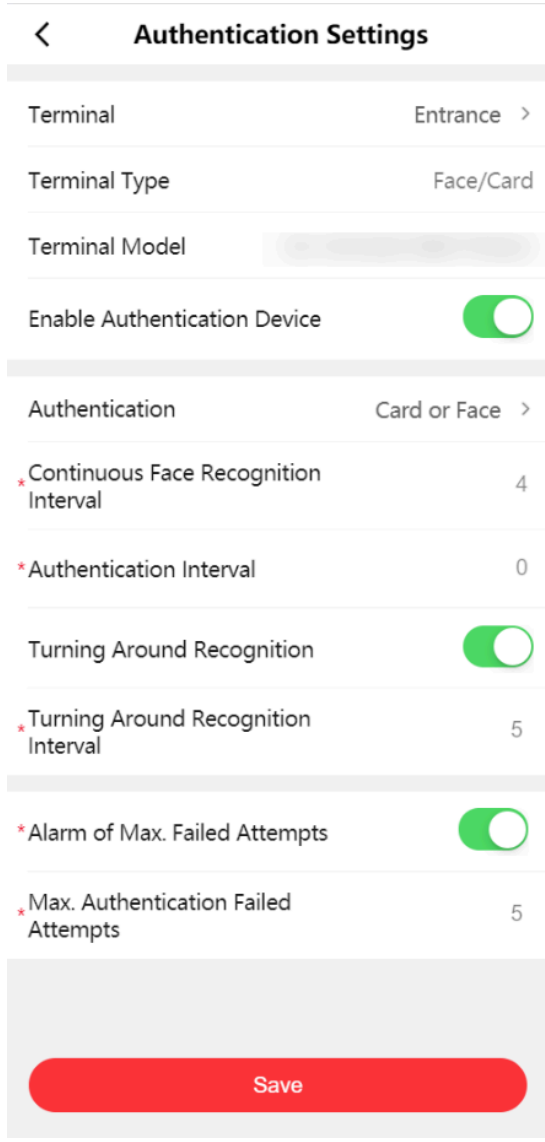


Figure 7-12 Authentication Settings

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

Terminal

Select terminal for settings.

Terminal Type

Display the terminal's type. Read only.

Terminal Model

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

Enable Authentication Device

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

Authentication

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

Continuous Face Recognition Interval

Set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, the same person can only recognized once.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed. If there is another person authenticate in the configured interval, the person can authenticate again.

Turning Around Recognition

When enable the function, after authentication from one side, the device will not authenticate the passing person from the other side within the configured interval.

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

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

Set Door Parameters

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

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

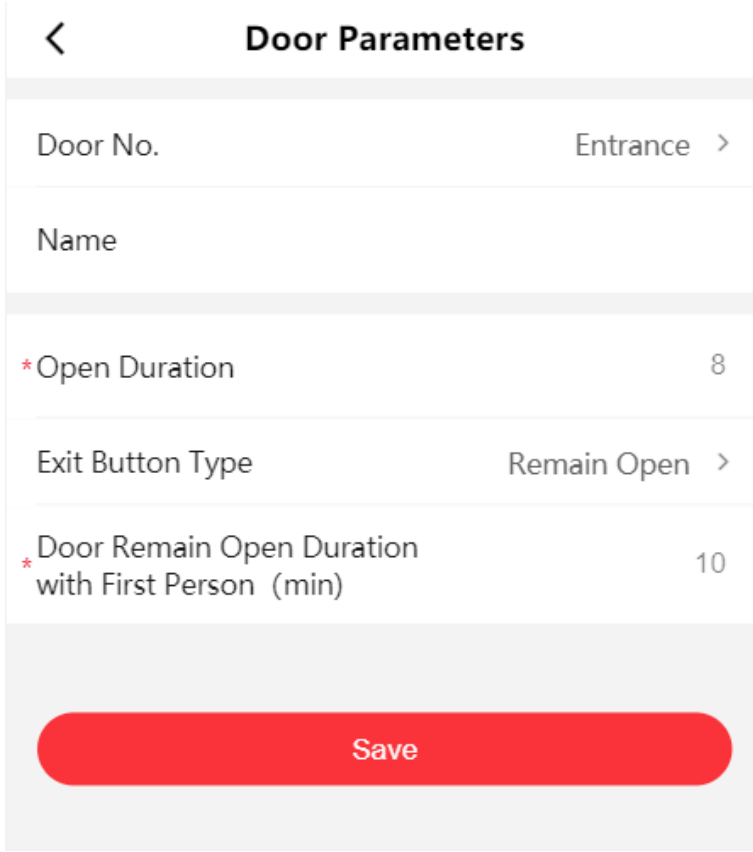


Figure 7-13 Door Parameters

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.

Elevator Control Parameters

Tap → **Access Control** → **Elevator Control Parameters** to enter the configuration page.

Note

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

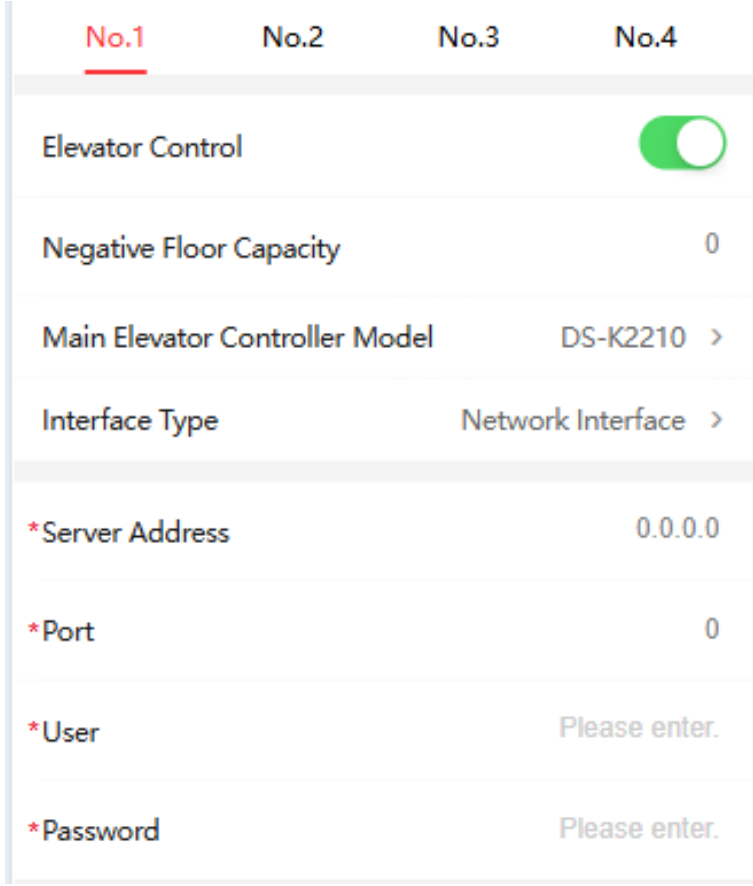


Figure 7-14 Elevator Control Parameters

Select **No.** as the elevator's No. Tap to enable **Elevator Control**.

Negative Floor Capacity

Enter the negative floor number that the elevator can control.

Main Elevator Controller

Model Select the main elevator controller's model.

Interface Type

Select the connection type between the elevator controller and the turnstile. If you select **Network Interface** as interface type, you should set server address, port, user, and password.

Tap **Save**.

Terminal Settings

Set the working mode.

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

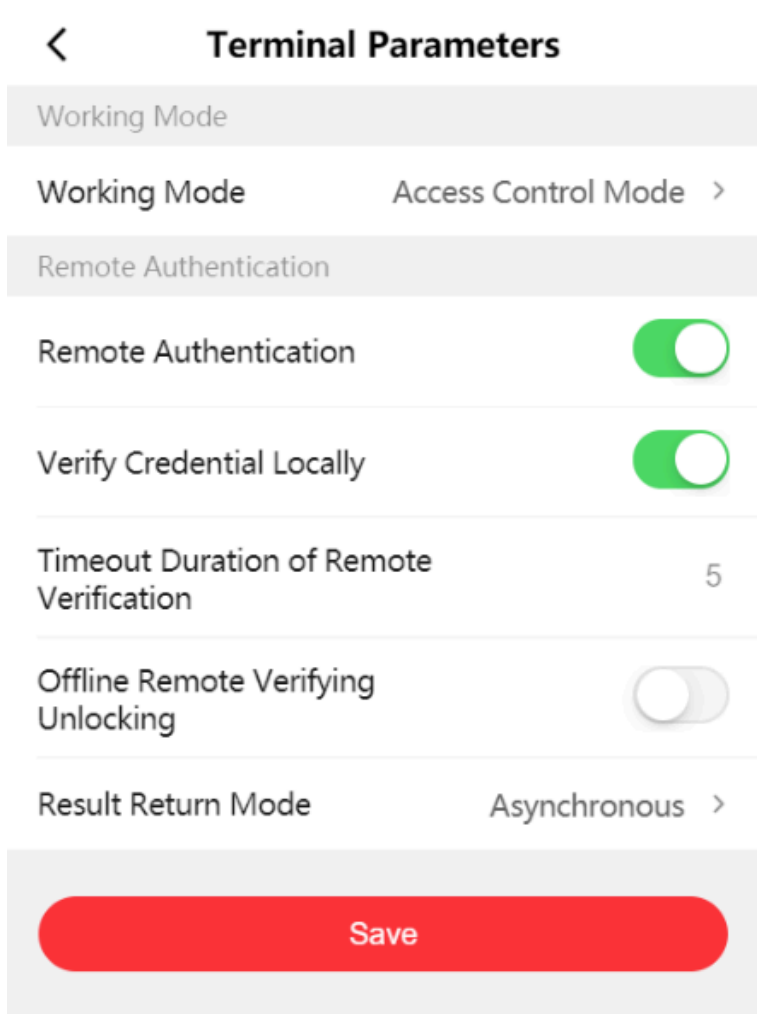


Figure 7-15 Terminal Parameters

Working Mode

Permission Free Mode

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

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

Access Control Mode

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

Remote Authentication

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

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

Timeout Duration of Remote Verification

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

Offline Remote Verifying Unlocking

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

Result Return Mode

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

Serial Port Settings

Set serial port parameters.

Steps

1. Tap ≡ → **Access Configuration** → **Serial Port Configuration** to enter the setting page.

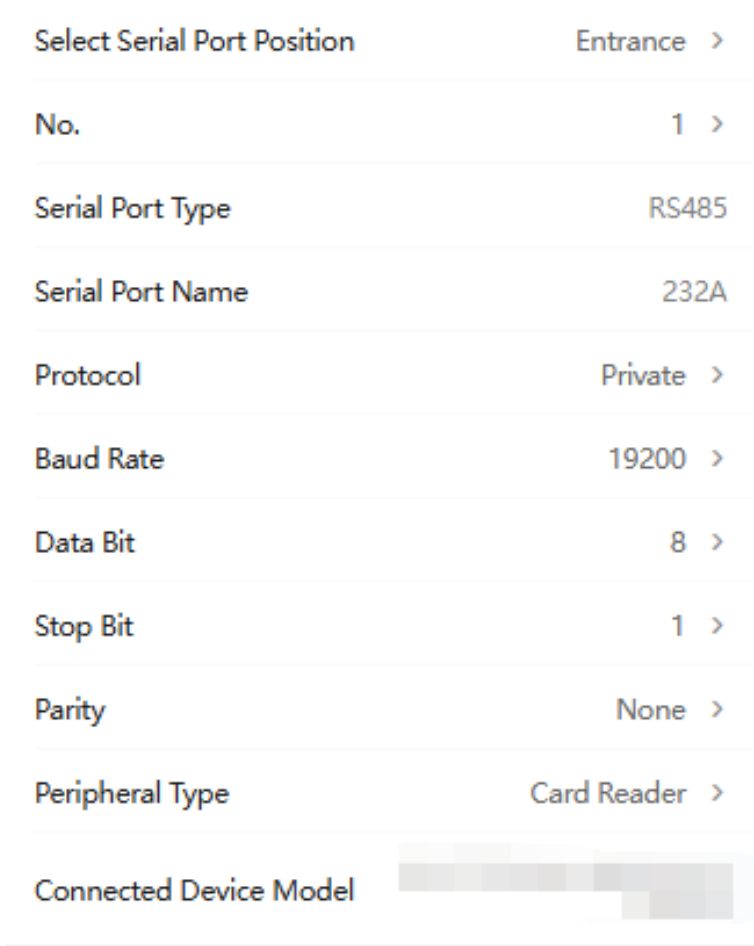


Figure 7-16 Serial Port Configuration

2. Set the serial port name and view the type.

3. Set the port's parameters

Baud Rate

Configure data transfer rate.

Data Bit

Configure the number of bits to send data.

Stop Bit

Select the end point for one frame of data.

Parity

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

Peripheral Type

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

Note

If select Only effective for the DS-K7CR02 QR code scanner.

4. Click **Save**.

Set Card Security

Configure cards for the device.

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

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

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Sector

Enable the function and set the encryption sector.

Note

It is recommended to encrypt sector 13.

Enable EM Card

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

Note

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

Enable DESFire Card

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

DESFire Card Read Content

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

Enable FeliCa Card

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

Card Authentication Mode

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

Enable Reversed Card No.

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

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

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

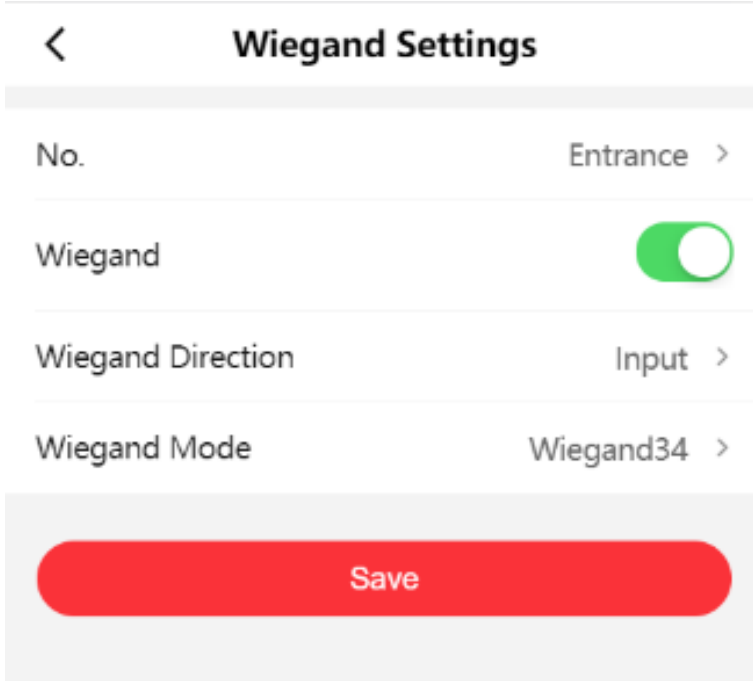


Figure 7-17 Wiegand Page

2. Select **Entrance** or **Exit**.
3. Enable **Wiegand** to enable the Wiegand function.
4. Set a transmission direction.

Note

The transmission direction can only be **Input**.

5. Select **Wiegand Mode**。
6. Click **Save** to save the settings.

7.3.13 Set Smart Parameters

Set face recognition related parameters.

Set Face Parameters

Tap → **Smart** → **Face Recognition Parameters** to enter the configuration page.

Note

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

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

Terminal

Select **Entrance** or **Exit** as the terminal direction.

Face Anti-spoofing

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

Note

Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Live Face Detection Security Level

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

Recognition Distance

Select the distance between the authenticating user and the device camera.

Application Mode

Select either others or indoor according to actual environment.

1:1 Matching Threshold

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

1:N Matching Threshold

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

Face Recognition Timeout Value

Set the timeout value when face recognizing. If the face recognition time is longer than the configured value, the system will pop up a prompt.

Face Recognition Area

You can set the face recognition area when authentication.

Select the terminal as **Entrance** or **Exit**.

Set **Margin (Left)**, **Margin (Right)**, **Margin (Top)**, and **Margin (Bottom)**. When authenticating, the person should in the configured area. Tap **Save**.

Set ECO Mode

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment.

Tap → **Smart** → **ECO Mode Settings** to enter the configuration page.

Note

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

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

Terminal

Select **Entrance** or **Exit** as the terminal direction.

ECO Mode

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. And you can set the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).

Enable Mode

You can set **Auto** or **Time to Sleep** to enable the ECO mode.

When you select **Time to Sleep**, you should tap **Time Schedule** to set the time duration that the device will enable ECO mode. Tap **Save**.

ECO Mode Threshold

The larger the value, the device enter the ECO Mode easier.

ECO Mode (1:1) Threshold

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

ECO Mode (1:N) Threshold

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

Set Face Mask Parameters

After enabling the face without mask detection, the system will recognize the face with mask or not.

Steps

1. Tap → **Smart** → **Face Mask Detection Parameters** to enter the configuration page.

   Note

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

2. After enabling the face with mask detection, the system will recognize the face with mask or not.

   Terminal

   Select **Entrance** or **Exit** as the terminal direction.

   Face with Mask Detection

Enable the function and the device will detect the person whether wearing a face mask or not.

Face with Mask & Face (1:1)

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

Face with Mask 1:N Matching Threshold

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

Face withouth Mask Strategy

Select a strategy when detect person not wearing a face mask.

None

The function is disabled. The device will not detect whether a person is wearing a face mask or not.

Reminder of Wearing Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will open.

Must Wear Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will keep closed.

3. Click **Save**.

7.3.14 Turnstile Parameters Settings

dToF Sensor Settings

Set the dToF Sensor parameters.

Steps

1. Tap → **dToF Sensor Settings** to enter the configuration page.
2. Set parameters and tap **Save**.

dToF Sensor Inductive Distance

Configurable inductive distance for door opening. Larger values increase the inductive coverage area.

dToF Sensor Anti-Pinch Distance

Configurable safety distance during passage. Larger values expand the protected area.

dToF Sensor Shield (Entrance/Exit)

If dToF sensors in the passage are damaged, temporarily disable them to restore functionality. Warning: Gate operation may pose collision risks to passersby when sensors are disabled.

dToF Sensor Diagram

View the diagram of the inductive distance and anti-pinch distance.

3. Tap **Save**.

People Counting Settings

Set people counting.

Steps

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

   Invalid

   Disable people counting.

   Passing Detection

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

   Authentication Number

   The number of passing people verified through credential authentication.
6. Set **Passing Direction** and you can set the passing direction of the device.
7. Tap **Clear** to clear all people counting information.
8. Tap **Save**.

Other Settings

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

Set the parameters and tap **Save**.

Alarm Output Duration

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

Temperature Unit

Select the temperature unit.

Do Not Open Barrier When Lane is Not Clear

When enabled, the barrier will not open when people is authenticated in the lane.

Barrier Closing Delay

After a person passes through the lane, the barrier will close after the set time period.

Intrusion Duration

If a person mistakenly enters the lane for more than the set time, or if the person passes longer than the set time, the device will start alarming.

Overstaying Duration

If someone or something is detected to be stuck in the lane for more than the set time, the device will start alarming.

dToF Obstructed Duration

If the dTof target is obstructed for more than the set time, the device will start alarming. 0 indicates that the function is not enabled.

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.

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.

Barrier Open Angle

Tap **Barrier Open Angle** and set the angle. The barrier can open the configured angle.

Note

- You can set the angle between 85° and 91°. 0.1° is the minimum adjust unit.

7.3.15 Upgrade and Maintenance

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

Restart Device

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

Upgrade

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

Note

Do not power off during the upgrading.

Restore Parameters

Tap → **Default** .

Restore to Default Settings

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

Restore to Factory Settings

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

Log Export

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

7.3.16 Device Debugging

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

Tap → **Device Debugging** .

Lane Studying/Motor Self-Test

Lane Studying

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

Motor Self-Test

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

Encoder Self-Test

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

dToF Self-Test

Select a channel (lane) and tap **dToF Self-Test**, the device will test all detectors. After enabling dToF self-test function, the device will sound to exit the channel (lane) before opening/closing. The barrier is forced to open in entrace/exit at the highest speed, at this time dToF anti-pinch is defunct. If dToF is triggered or blocked, the device will sound detection failure.

Note

Make sure there are no person in the lane.

Debugging Command Management

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

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

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

Note

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

dToF Exception Info.

Tap **Export** to export the exceptional detectors reports.

Demo Mode

After enabled, the device will automatically add and authenticate after face recognition.

You can set the validity period.

If disabled, all person information added in the demo mode will be cleared after disabled.

7.3.17 View User Document

View the user document.

Note

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

Tap ☰ to enter the page.

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

7.3.18 Open Source Software Licenses

You can view the open source software licenses.

Tap ☰ to enter the page.

Tap **Open Source Software Licenses**.

7.3.19 Log Out

Log out the configuration page.

Tap ☰ → **Logout** , tap **OK**.

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

Chapter 8 Operation via PC Web

8.1 Login

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

Note

Make sure the device is activated.

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.

8.2 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.

8.3 Quick Operation via Web Browser

8.3.1 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 **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

8.3.2 Environment Settings

After activating the device, you should select an application mode for better device application.

Steps

1. Click in the top right of the web page to enter the wizard page. After setting time, you can click **Next** to enter the **Environment Settings** page.
2. Select **Indoor** or **Other**.

Note

- If you install the device indoors near the window or the face recognition function is not working well, select **Others**.
- If you do not configure the application mode and tap **Next**, the system will select **Indoor** by default.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip environment settings.

8.3.3 Privacy Settings

Set the picture uploading and storage parameters.

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

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Upload Picture After Linked Capture

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

Save Pictures After Linked Capture

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

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip privacy settings.

8.4 Help

8.4.1 Open Source Software Licenses

You can view open source software licenses.

Click → **Open Source Software Statement** on the upper-right corner to view the licenses.

8.4.2 View Online Help Document

You can view the help document for Web configuration.

Click → **User Manual** or scan the QR code on the upper right of the Web page to view the document.

8.4.3 Logout

Log out the account.

Click **admin → Logout → OK** to logout.

8.5 Overview

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

Function Descriptions:

Device Component Status

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

Remote Control

/ / /

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

Real-Time Event

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

Person Information

You can view the added and not added information of person, face, 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, face, card, event capacity.

8.6 Person Management

You can add the person's information, including the basic information, credentials, No. settings, and authentication 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 **Normal User** or **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 Face Picture

Click **Person Management → Add** to enter the Add Person page.
Click **+** on the right to upload a face picture from the local PC.

Note

The picture format should be JPG or JPEG or PNG, and the size should be less than 200 K.

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.

Device No. Settings

Click **Person Management → Add** to enter the Add Person page.
You can link a room No. for the person to realize elevator calling function after the person passing through the turnstile.
Click **Add**, enter the **Room No.** and **Floor No.**
You can also click to delete the room No.
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.

Import/Export/Clear Person Data

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

Export Person Data

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

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

Note

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

Importing Person Data

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

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

Clear All

Click **Clear All** and enter the admin password. Then you can delete all users.

8.7 Device Management

8.7.1 Sub Access Control Board Management

You can manage the sub access control board on the page.

Steps

1. Click **Device Management → Device Management → Sub Access Control Board** to enter page.

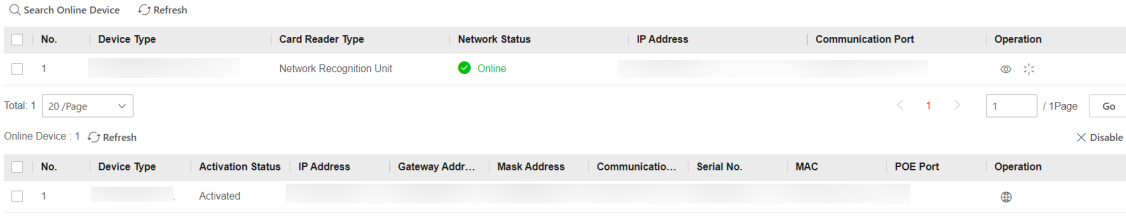


Figure 8-1 Device Management

2. Set device parameters.

Function	Description
	Set **Device Name** and view the **Device Model**, **Serial No.**, **Version**, **Version**, **Alarm Inputs** and **Alarm Outputs**.
	Reboot the device.
Refresh	Refresh the device list.
	Edit network parameters of the sub access control board, such as **IP address** and view the **Gateway Address**, **IPv4 Subnet Mask**, and **Communication Port**, enter the admin password.

Note

Make sure the IP address of the sub access board and the main access board's should be in the same IP segment, or the sub access board can be offline.

3. Click **Save**.

8.7.2 Batch Devices Management

You can view the information of all the main access control boards, which are under the same network segment with the current device. You can locate the barrier, set the network parameters, synchronize parameter with sub access control board and edit the device name of single main access control board. You can also select batch devices to set network parameters, sync parameters and activate.

Steps

1. Click **Device Management → Device Management → Batch Manage Devices** to enter page.

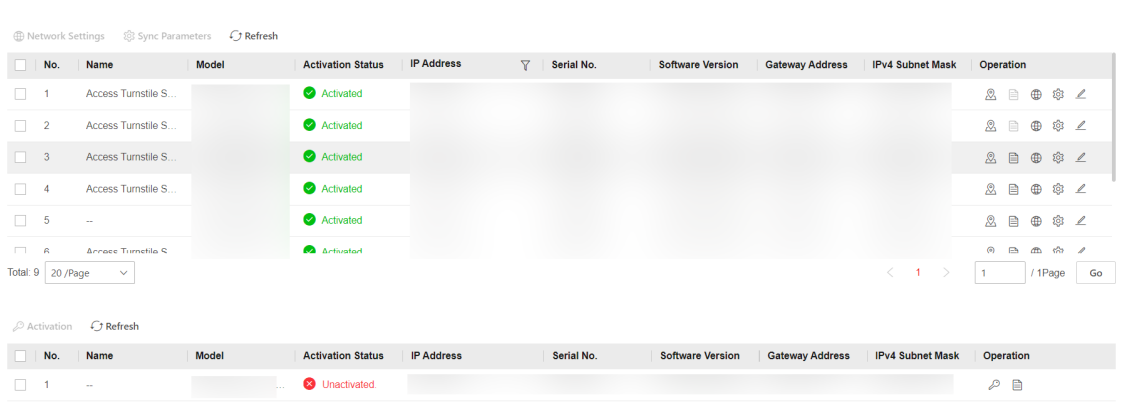


Figure 8-2 Batch Manage Devices Page

All the devices (main access control board), which are under the same network with the sub access control board, will be displayed in the page.

Note

The upper area of the page is the activated devices; and the bottom area is non-activated devices.

2. You can operate the following actions to the activated devices.

Click the icon to locate the barrier via the barrier's status.

Click the icon to view the information of sub access control board and set the network parameters, enter the admin password and click **Save**.

Note

- If uncheck the DHCP function, you should set the IPv4 address, IPv4 subnet mask, and gateway address.
- If you check the DHCP function, the system will allocate the IPv4 address, IPv4 subnet mask, and gateway address automatically.

Click the icon to set the network parameters of main and sub access control boards, enter the admin password and click **Save**.

DHCP

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

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

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.

Click the icon to sync the corresponding parameters with the current device's, enter the admin password and click **Save**.

Click the icon to edit the name of the device, enter the admin password and click **Save**.

3. You can operate the following actions to the non-activated devices.

Click the icon to set the network parameters of main and sub access control boards, enter the admin password and click **Save**.

4. You can manage the batch devices as follows:

Select the devices and click the icon to set the network parameters of main access control boards, and enter the admin password and click **Save**.

Note

The system will allocate IP addresses to the selected devices in turns. The sub access board's IP will be main access board's IP+1.

Select the devices and click the icon to sync the corresponding parameters of with the current device, and enter the admin password and click **Save**.

Select the devices and click the icon to activate, and enter the admin password and click **Save**.

8.8 Turnstile

8.8.1 Search Event

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

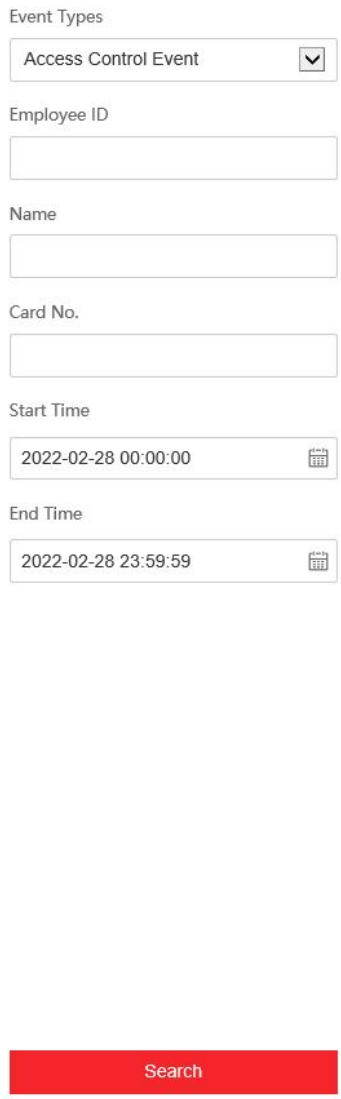


Figure 8-3 Search Event

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.

8.8.2 Paramenter Settings

Set Door Parameters

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

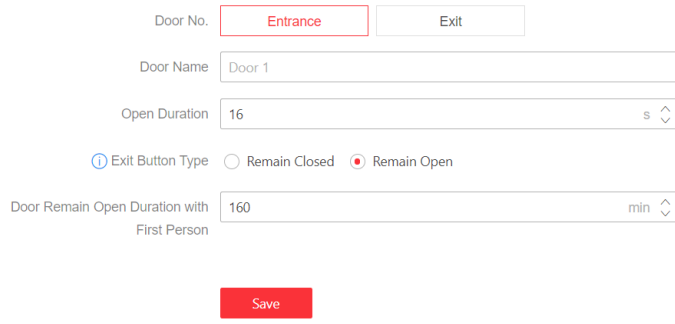


Figure 8-4 Door Parameters Settings

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.

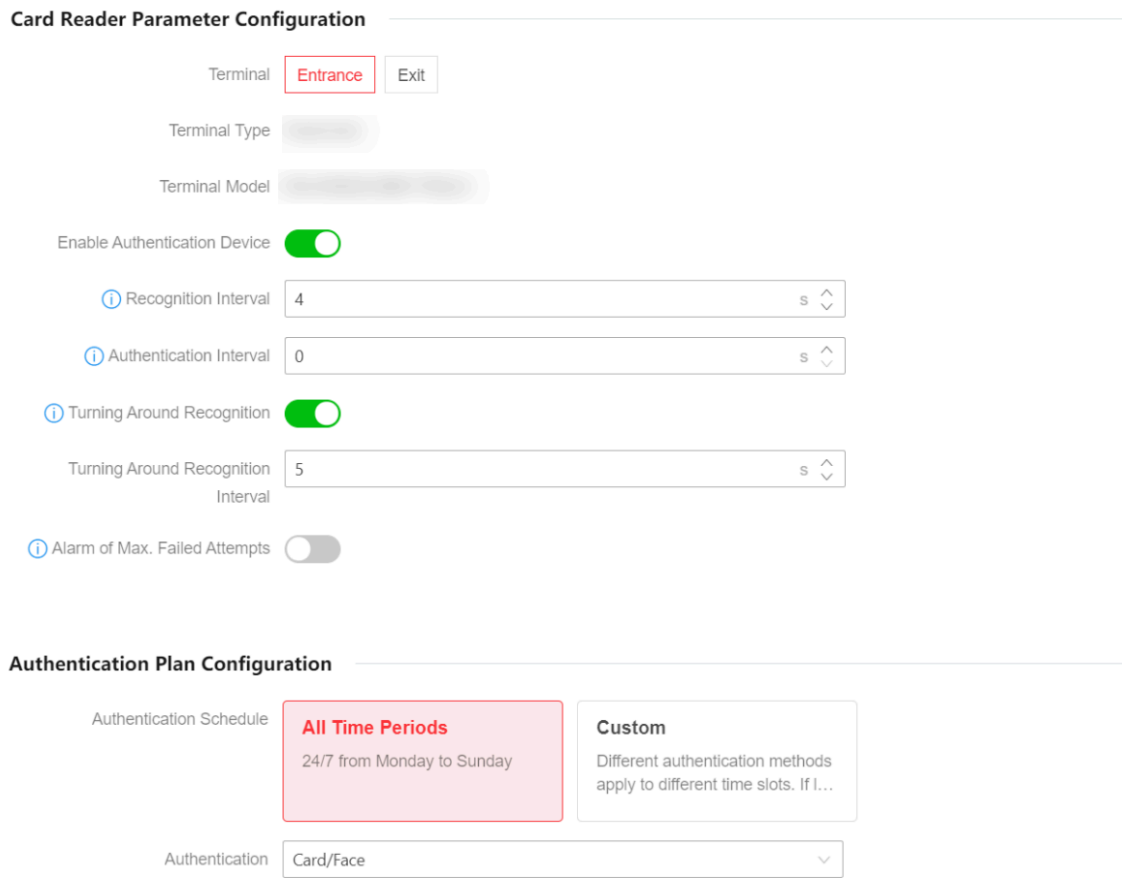


Figure 8-5 Set Authentication Parameters

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.

Recognition Interval

You can set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, Person A can only recognized once. If another person (Person B) has recognized during the interval, Person A can recognized again.

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.

Turning Around Recognition

When enable the function, after authentication from one side, the device will not authenticate the passing person from the other side within the configured interval.

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.

Set Smart Parameters

Set Face Recognition Parameters

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

Note

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

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

Terminal

Select a direction for the settings.

Face Recognition

After enabling, the device will support face recognition.

Face Anti-Spoofing

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

Note

Biometric recognition products are not absolutely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Anti-Spoofing Detection Level

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

Recognition Distance

Select the distance between the authenticating user and the device camera.

Application Mode

Select either other or indoor according to actual environment.

Pitch Angle

The maximum pitch angle when starting face authentication.

Yaw Angle

The maximum yaw angle when starting face authentication.

1:1 Matching Threshold

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

1:N Matching Threshold

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

Face Recognition Timeout Value

Set the timeout value when face recognizing. If the face recognition time is longer than the configured value, the system will pop up a prompt.

Face Recognition Area

Click **Area Configuration** to enter the page.

Select **Entrance** or **Exit** as the terminal direction.

Drag the block or enter the parameters to set the face recognition area.

Click **Save**.

Set ECO Mode Parameters

ECO Mode

After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. And you can set the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).

Enable Mode

You can set **Auto** or **Timing** to enable the ECO mode.

When you select **Timing**, you should click **Set** to set the time duration that the device will enable ECO mode. Click **Save**.

ECO Mode Threshold

The larger the value, the device enter the ECO Mode easier.

ECO Mode (1:1) Threshold

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

ECO Mode (1:N) Threshold

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

Face with Mask Detection

After enabling the face without mask detection, the system will recognize the captured face with mask picture or not. You can set face with mask1:N matching threshold, it's ECO mode, and the strategy.

None

The function is disabled. The device will not detect whether a person is wearing a face mask or not.

Reminder of Wearing Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will open.

Must Wear Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will keep closed.

Face with Mask & Face (1:1)

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

Face with Mask 1:N Matching Threshold

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

Face with Mask & Face 1:1 Matching Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Face with Mask & Face 1:N Matching Threshold (ECO)

Set the matching threshold when authenticating with face mask via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Card Settings

Set Card Type

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

Set the parameters and click **Save**.

Enable NFC Card

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

Enable M1 Card

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

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

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

Enable EM Card

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

Note

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

Enable DESFire Card

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

DESFire Card Read Content

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

Enable FeliCa Card

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

Set Card No. Authentication Parameters

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

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

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

Card Authentication Mode

Full Card No.

All card No. will be read.

Wiegand 26 (3 bytes)

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

Wiegand 34 (4 bytes)

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

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

The device will read card via the other mode.

Enable Reversed Card No.

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

Set Terminal Parameters

You can set terminal parameters for accessing.

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

Set the parameters and click **Save**.

Remote Verification

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

Verifying Person Type Remotely

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

Remote Verification Credential Type

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

Remote Verification Channel Type

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

ISUP

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

Note

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

ISAPI

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

Note

By default, devices use ISAPI for remote verification.

HTTP

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

Hik-Connect

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

Note

This method requires device support to be used.

Verify Credential Locally

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

Timeout Duration of Remote Verification

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

Offline Remote Verifying Unlocking

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

Result Return Mode

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

Set Privacy Parameters

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

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

Event Storage Settings

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

Delete Old Events Periodically

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

Delete Old Events by Specified Time

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

Overwriting

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

Picture Uploading and Storage

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Save Pictures After Linked Capture

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

Upload Picture After Linked Capture

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

Clear All Pictures in Device

Note

All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

8.8.3 Turnstile Configuration

Basic Parameters

Set turnstile basic parameters.

Steps

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

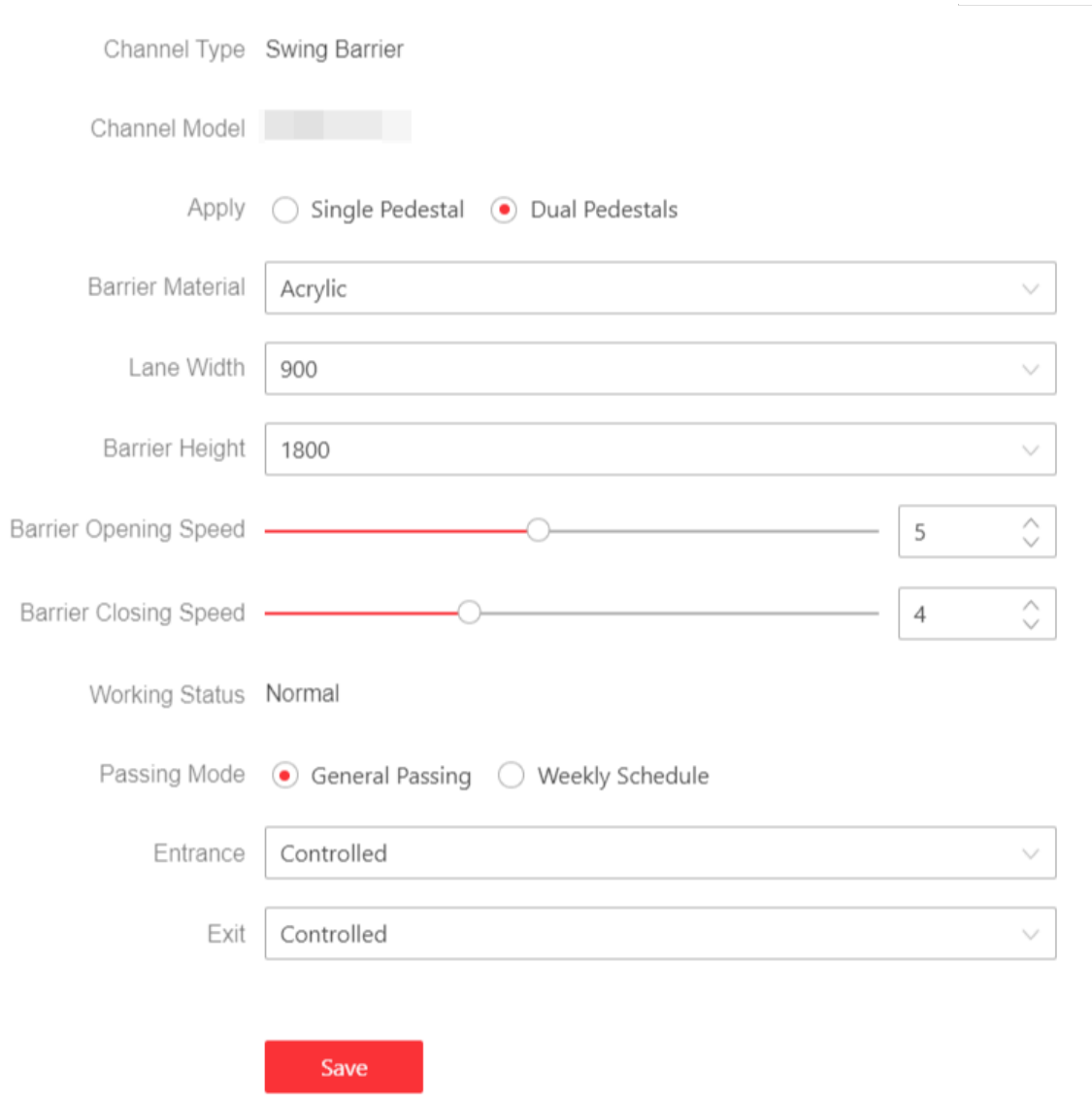


Figure 8-6 Basic Parameters

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

Note

Lane width, barrier height, and barrier material must be filled in; otherwise, the barrier will not operate properly.

Channel Type/Channel Model/Working Status

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

Apply

Select **Single Pedestal** or **Dual Pedestals** according to actual needs.

Single Pedestal

When you only use one pedestal, you should select this option.

Dual Pedestals

When you only use dual pedestals, you should select this option.

Note

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

Barrier Material

Select a barrier material according to actual situation.

Lane Width

Select a lane width according to actual situation.

Barrier Height

Select a barrier height according to actual situation.

Barrier Opening Speed/Barrier Closing Speed

Set the barrier opening or closing speed.

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.

3. Click **Save**.

IR Detector

Set IR detector.

Steps

1. Click **Configuration → Turnstile Configuration → dToF Sensor Configuration** to enter the page.

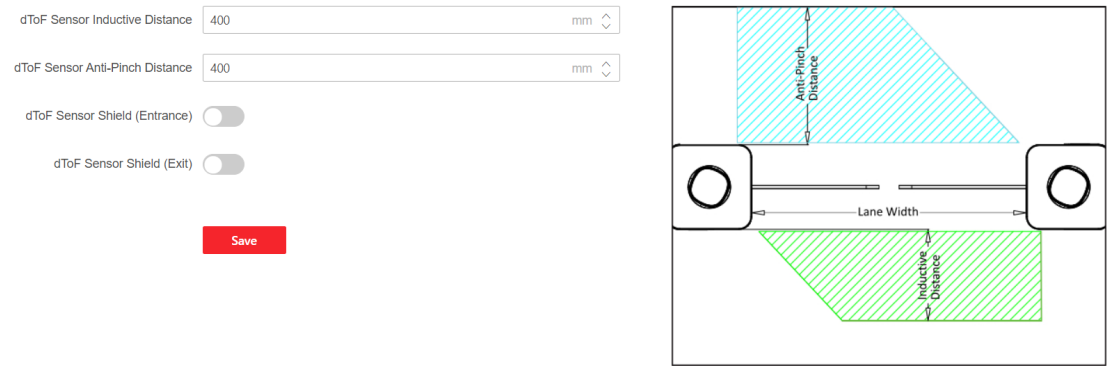


Figure 8-7 dToF Sensor Settings

2. Set the parameters.

   dToF Sensor Inductive Distance

   Configurable inductive distance for door opening. Larger values increase the inductive coverage area.

   dToF Sensor Anti-Pinch Distance

   Configurable safety distance during passage. Larger values expand the protected area.

   dToF Sensor Shield (Entrance/Exit)

   If dToF sensors in the passage are damaged, temporarily disable them to restore functionality. Warning: Gate operation may pose collision risks to passersby when sensors are disabled.

3. Click **Save**.

People Counting

Set people counting.

Steps

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

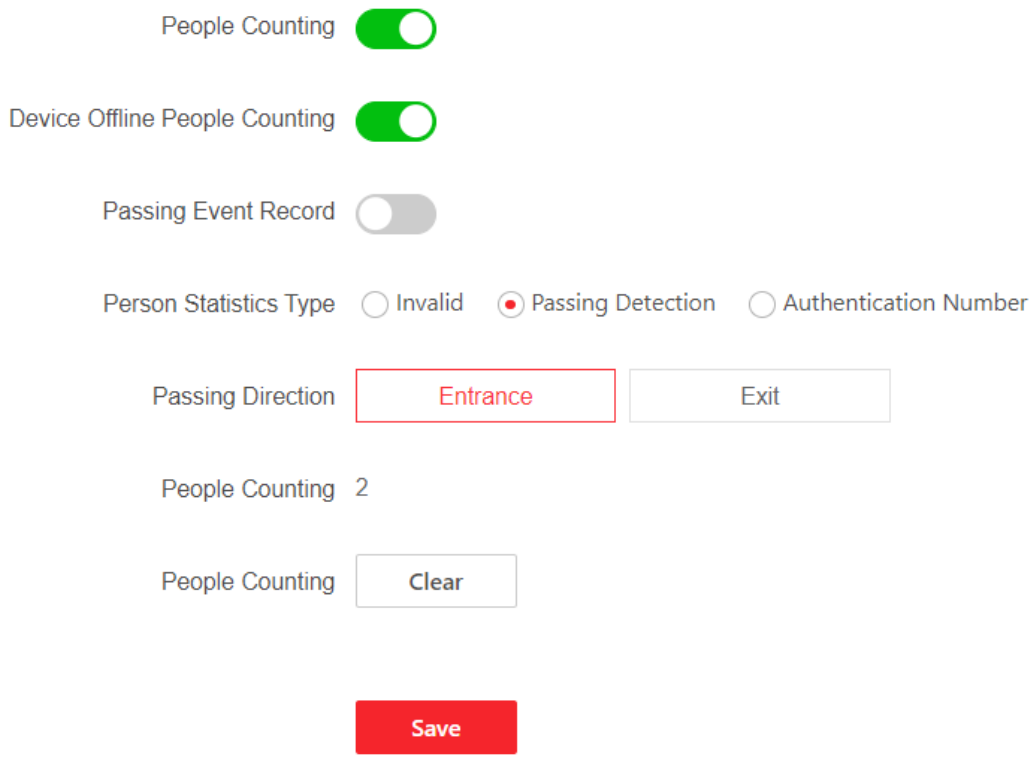


Figure 8-8 People Counting

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 number of all passing people.

People Statistics Type

Invalid

Disable people counting.

Passing Detection

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

Authentication Number

The number of passing people verified through 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.

Set Light

Set the light brightness when authentication of the device.

Steps

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

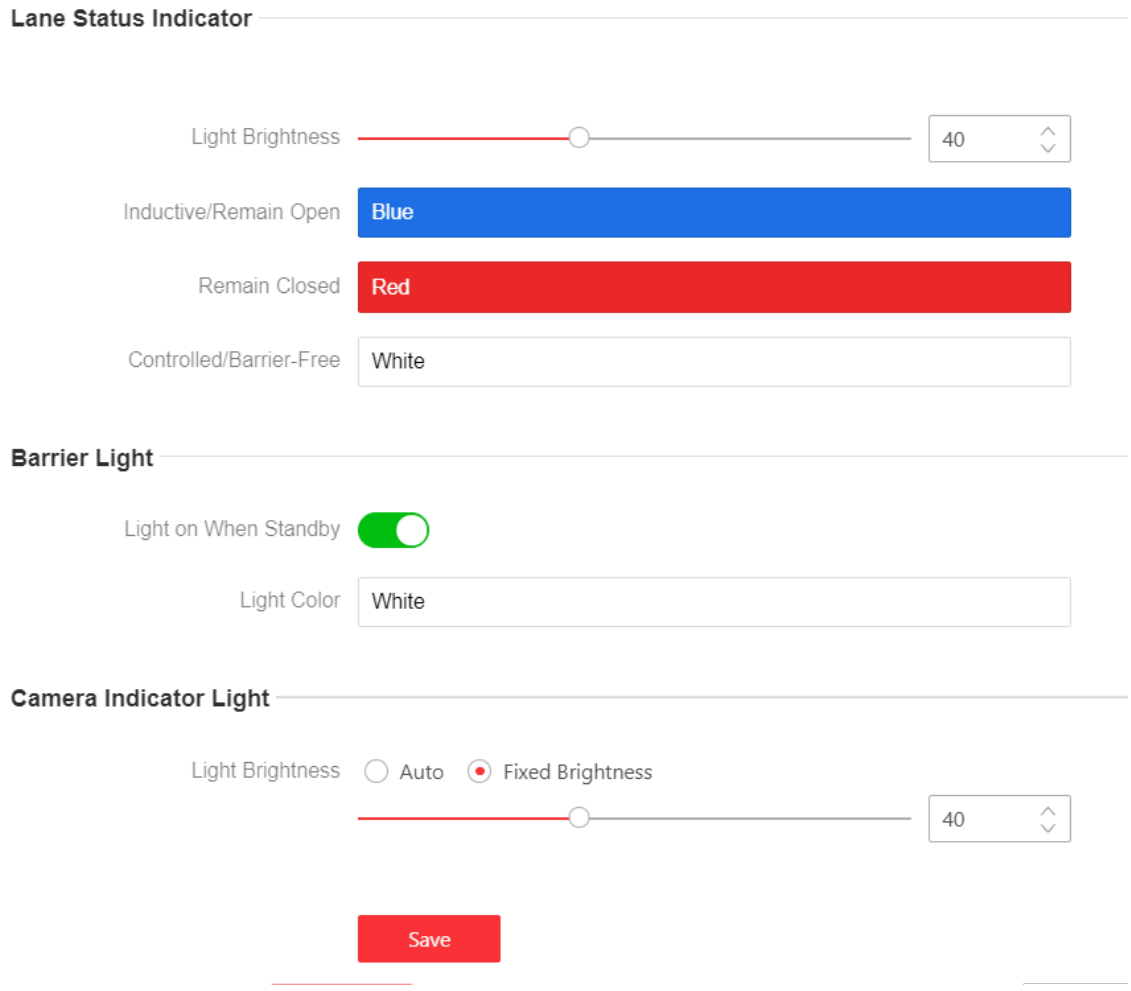


Figure 8-9 Light Settings

2. Set indicator or light's brightness and color.

Lane Status Indicator

Set the lane status indicator's brightness and color.

Light Brightness

Select **Auto** and the device will adjust the indicator's brightness automatically. Or select**Fixed Brightness** and set the brightness value.

Inductive/Remain Open

Set the indicator's color when the barrier is in inductive or remain open status.

Remain Closed

Set the indicator's color when the barrier is in remain closed status.

Controlled/Barrier-Free

Set the indicator's color when the barrier is in Controlled or barrier-free status.

Barrier Light

Set he light color and brightness.

Light on When Standby

When enable the function, and if the device is in standby status, the light will be on.

Light Color

Select a color from the drop-down list. And the device's barrier will display the select color.

Camera Indicator Light

Set the camera light brightness.

Light Brightness

Select **Auto** or **Fixed Brightness** for the camera light.

3. Click **Save**.

Other Settings

Set other parameters.

Steps

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

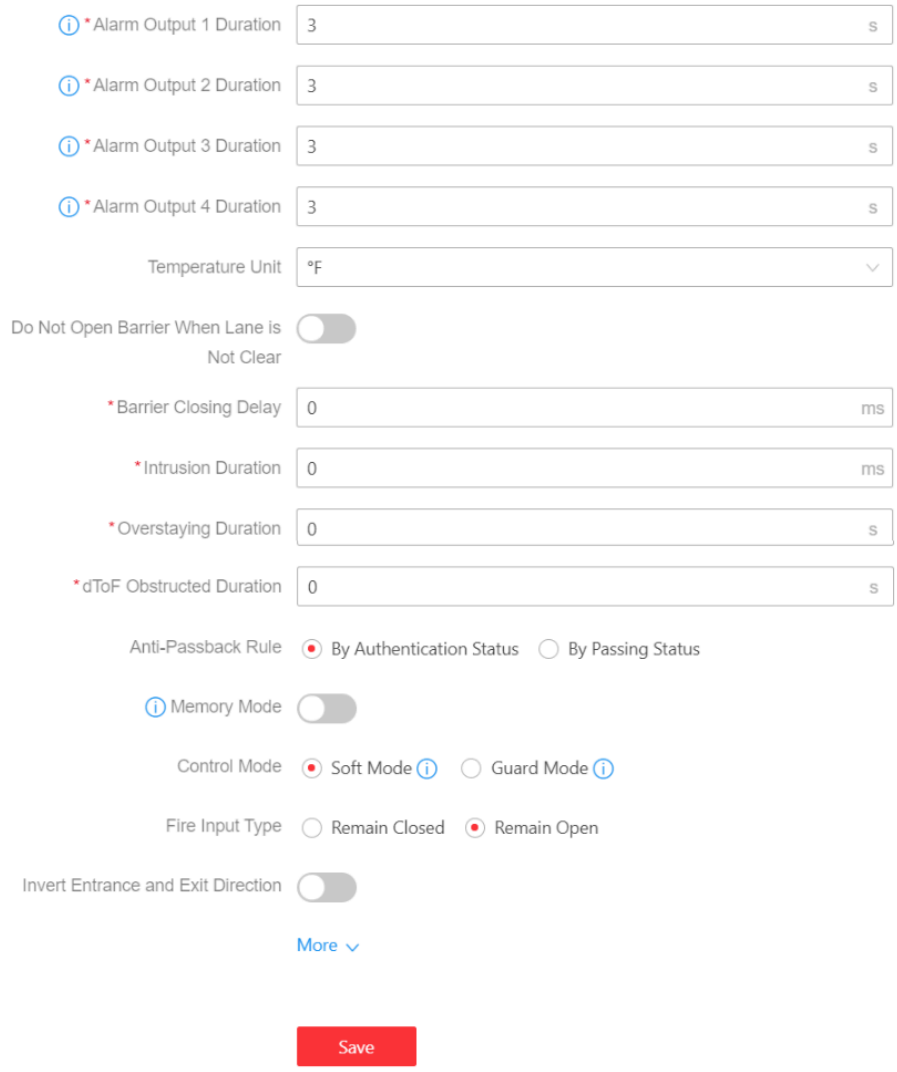


Figure 8-10 Other Settings Page

2. Set parameters.

Alarm Output Duration

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

Temperature Unit

Select unit.

Do Not Open Barrier When Lane is Not Clear

When enabled, the barrier will not open when people is authenticated in the lane.

Barrier Closing Delay

After a person passes through the lane, the barrier will close after the set time period.

Intrusion Duration

If a person mistakenly enters the lane for more than the set time, or if the person passes longer than the set time, the device will start alarming.

Overstaying Duration

If someone or something is detected to be stuck in the lane for more than the set time, the device will start alarming.

IR Obstructed Duration

If the infrared target is obstructed for more than the set time, the device will start alarming. 0 indicates that the function is not enabled.

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**.

8.9 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.

8.9.1 Set Local Parameters

Set the live view parameters, picture and clip settings.

Click **System and Maintenance → System Configuration → Local** to enter the Local page.

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

Set Live View Parameters

Configure the stream type, the play performance.

Record File Settings

Select a record file size and select a saving path from your local computer .
You can also click **Open** to open the file folder to view details.

Picture and Clip Settings

Select image format, saving path.
You can also click **Open** to open the file folder to view details.

8.9.2 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.

8.9.3 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** .

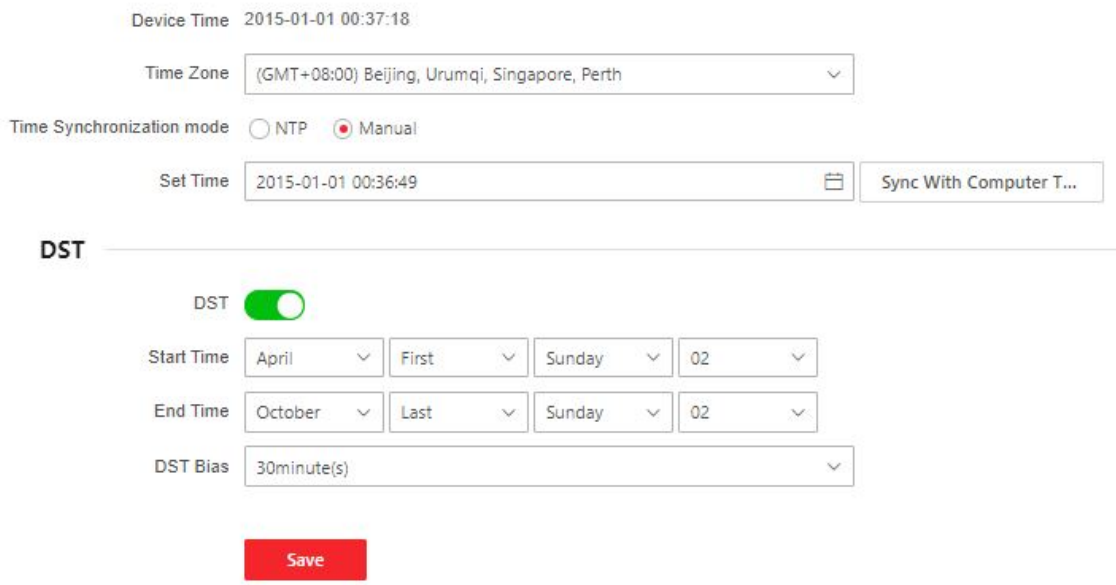


Figure 8-11 Time Settings

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.

8.9.4 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.

8.9.5 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.

8.9.6 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.

8.9.7 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.

8.9.8 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.

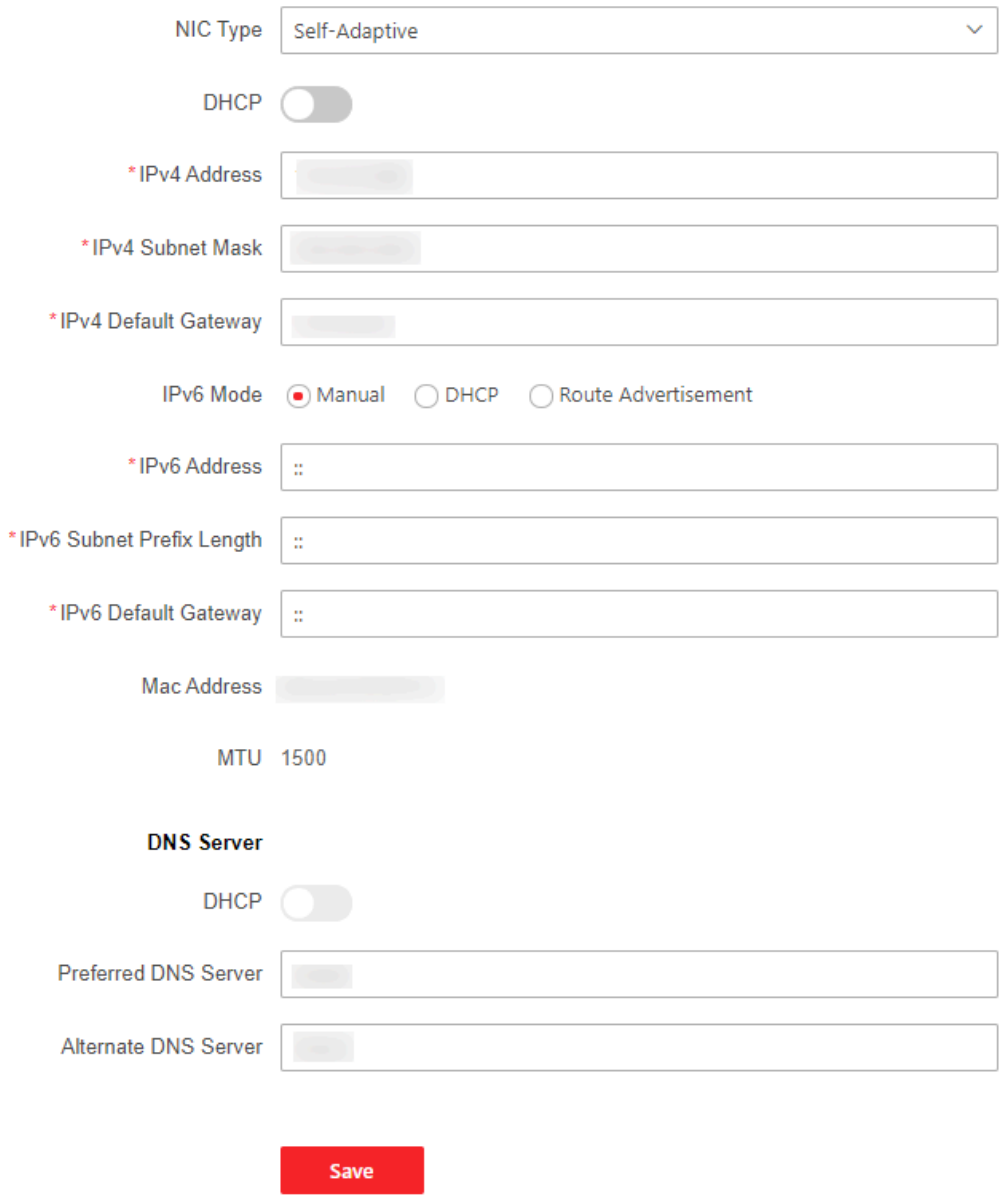


Figure 8-12 Set TCP/IP

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.

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

RTSP

It refers to the port of real-time streaming protocol.

Set ISUP Parameters via PC Web

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

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

   Note

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

Set OTAP via PC Web

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

Steps

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

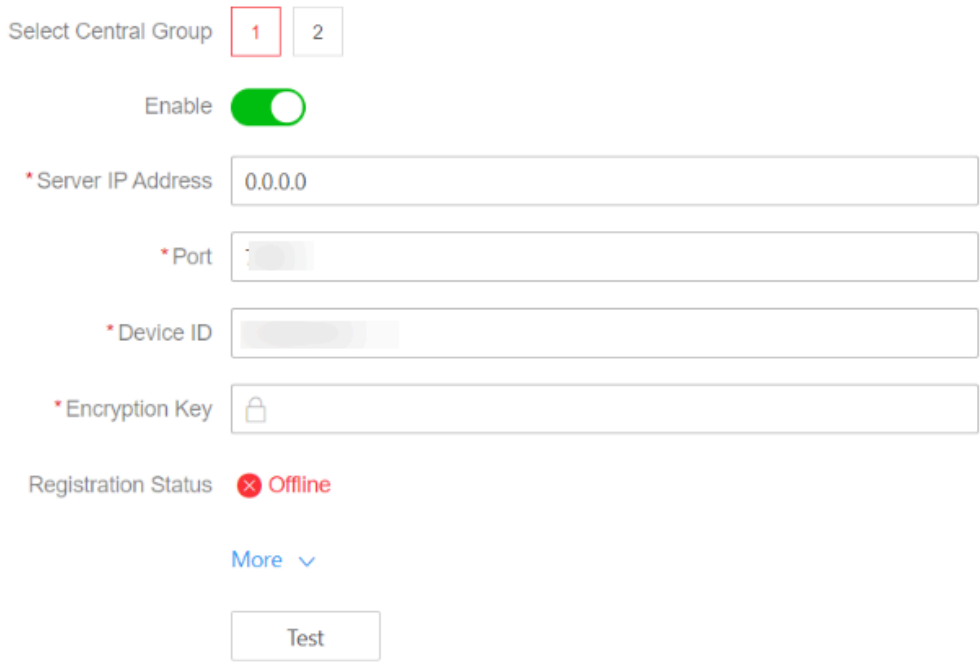


Figure 8-13 Set OTAP

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.

8.9.9 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.
- Only the device supporting interface board can set the Wiegand parameters.

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

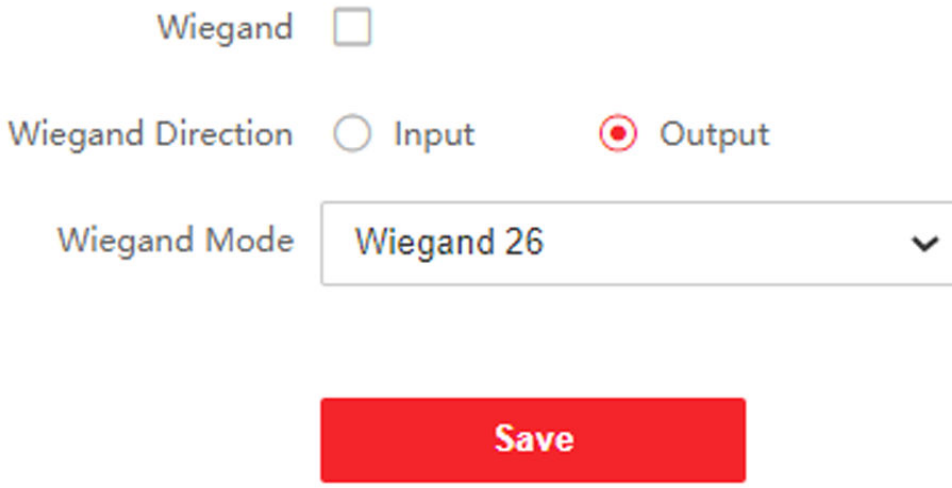


Figure 8-14 Wiegand Page

2. Check **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

   Input

   The device can connect a Wiegand card reader.

   Output

   The can connect an external access controller. And you should set the output type.
4. Click **Save** to save the settings.

Note

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

8.9.10 Serial Port Settings

Set serial port parameters.

Steps

1. Click **System and Maintenance → System Configuration → Access Configuration → Serial Port Configuration** .
2. Set the serial port position as **Entrance** or **Exit**.
3. Select a serial port No.; the corresponding serial port type and serial port name will display automatically.
4. Set the **Protocol** .

5. Set the **Peripheral Type** the port connected.

Note

If select Only effective for the DS-K7CR02 QR code scanner.

6. You can view the external device model.
7. 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.

8. Click **Save**.

8.9.11 Elevator Control via PC Web

Steps

1. Click **System and Maintenance → System Configuration → Access Configurations → Elevator Control Parameters** .

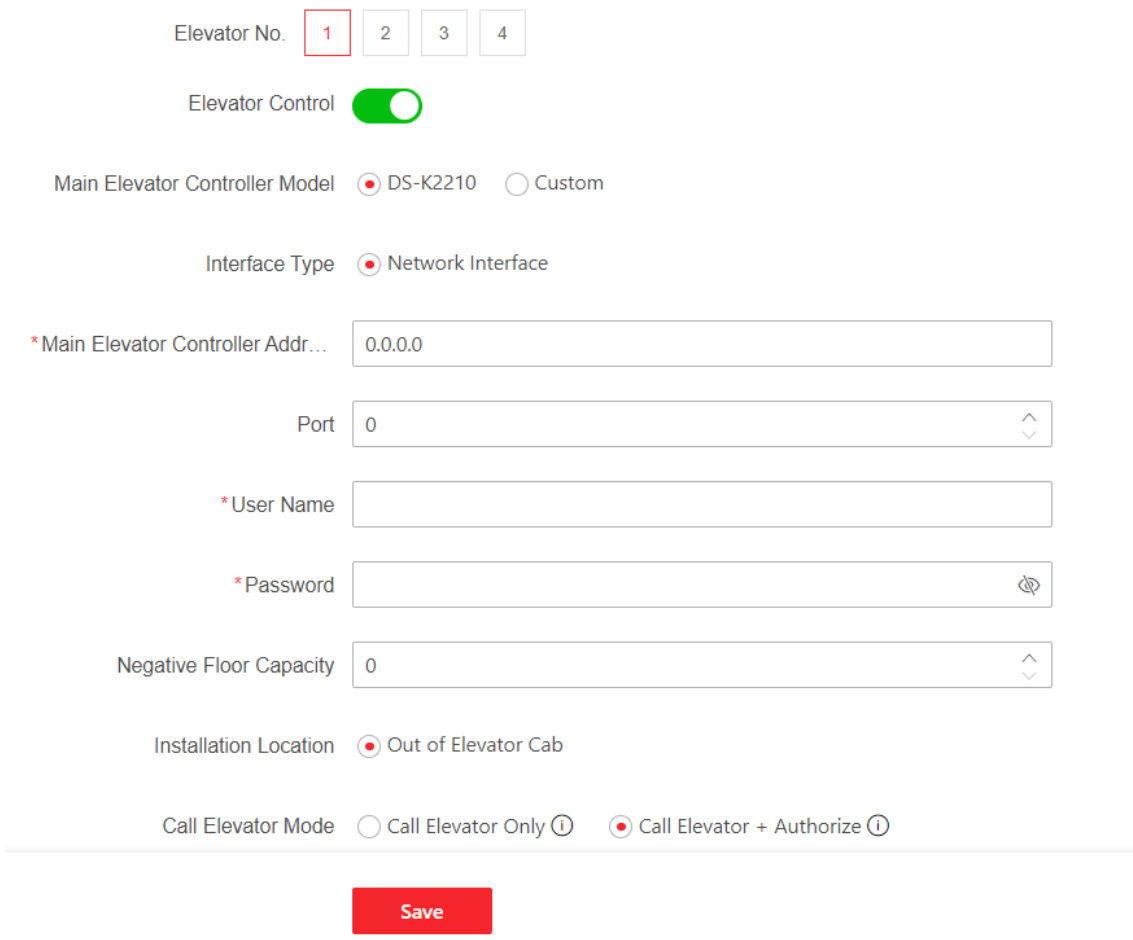


Figure 8-15 Elevator Control

2. Select an elevator No., the parameters settings below will affect the selected elevator.
3. Enable **Elevator Control**.
4. Set the elevator parameters.

Main Elevator Controller Model

View the elevator model.

Interface Type

Select a communication type from the drop-down list for elevator communication.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

Negative Floor Capacity

Set the negative floor number.

Installation Location

Select the device installation position. By default, it is out of elevator cab.

Call Elevator Mode

Call Elevator Only

After person passes authentication on device, the device will call elevator to its floor.

Call Elevator+Authorize

After person passes authentication on device, the device will call elevator to its floor and authorize the permission of the floor linked to person room. The person can get to the target floor by pressing corresponding floor No.

Note

- Up to 4 elevator controllers can be connected to 1 device.
- Up to 10 negative floors can be added.
- Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.

8.9.12 Set Video and Audio Parameters via PC Web

Configure Video Parameters via Web Browser

You can set quality, resolution and other parameters of device camera.

Click **System and Maintenance → System Configuration → Video/Audio → Video** to enter the settings page.

Set camera name, stream type, video type, resolution, bit rate type, video quality, frame rate, Max. bitrate, video encoding and I frame interval.

Click **Save**.

Configure Audio Parameters via Web Browser

You can set device volume.

Click **System and Maintenance → System Configuration → Video/Audio → Audio** to enter the settings page.

Slide to enable voice prompt function.

Slide to set **Output Volume**.

Click **Save**.

8.9.13 Set Image Parameters

You can adjust the image parameters.

Steps

1. Click **System and Maintenance → System Configuration → Image** .
2. Set the lane as **Entrance** or **Exit**.
3. Configure the parameters to adjust the image.

   Image Adjustment

   Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

   LED Light

   Set the supplement light type and mode. You can also set the brightness.

   Backlight

   Enable or disable **WDR**.

   When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.

   You can select **Auto** or **Timing**.

   If you select **Timing**, you can set the duration of enable the WDR function.

   Video Adjustment (Video Standard)

   Set the video frame rate when performing live view remotely. After changing the standard, you should reboot the device to take effect.

   PAL

   25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

   NTSC

   30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

   Beauty

   Enable **Beauty**, drag the block or enter numbers to set the whiten and smooth level.

   Start All Recording

   You can click to record when starting live view.

   Capture

   You can click to capture image when starting live view.

   Full Screen

   You can click for full screen view.
4. Click **Restore Default Settings** to restore the parameters to the default settings.

8.9.14 Event Linkage

Set linked actions for events.

Steps

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

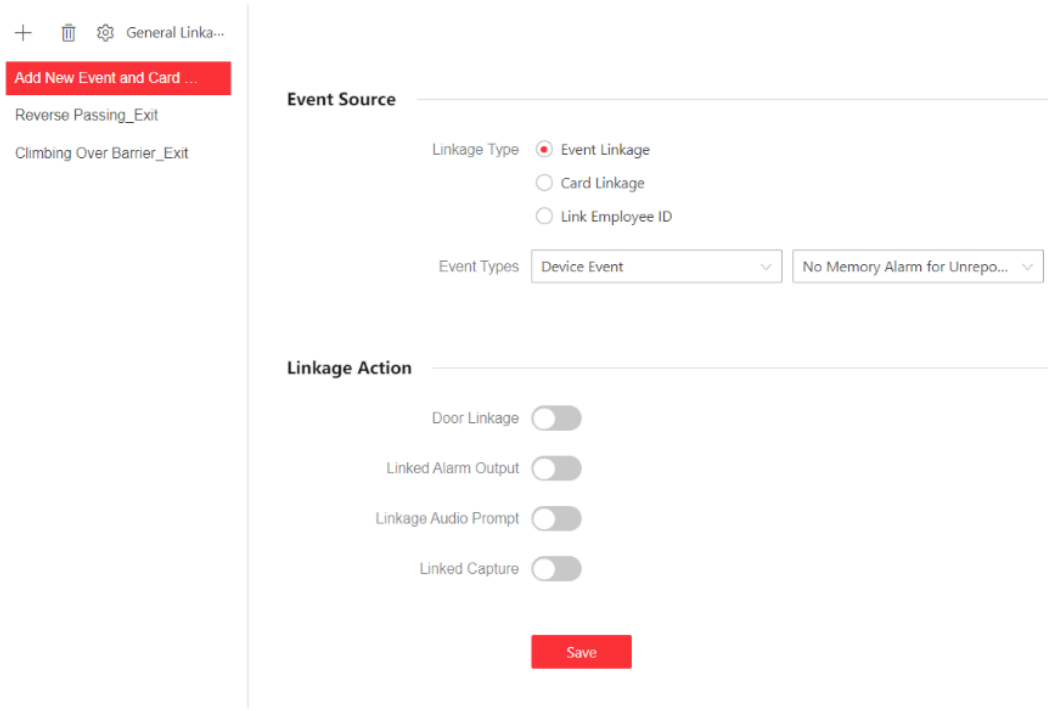


Figure 8-16 Event Linkage

2. Set event source.
   - If you choose **Linkage Type** as **Event Linkage**, you need to select event types from the drop-down list.
   - If you choose **Linkage Type** as **Card Linkage**, you need to enter the card No. and select the card reader.
   - If you choose **Linkage Type** as **Employee ID Linkage**, you need to enter the employee ID and select the card reader.
3. Set linked action.

   Door Linkage

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

   Linked Alarm Output

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

   Linkage Audio Prompt

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

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

Capture Linkage

Enable **Capture Linkage** and select the card reader (entrance or exit) to capture for the target event.

8.9.15 Prompt Schedule

Customize the output audio content when authentication succeeded and failed.

Steps

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

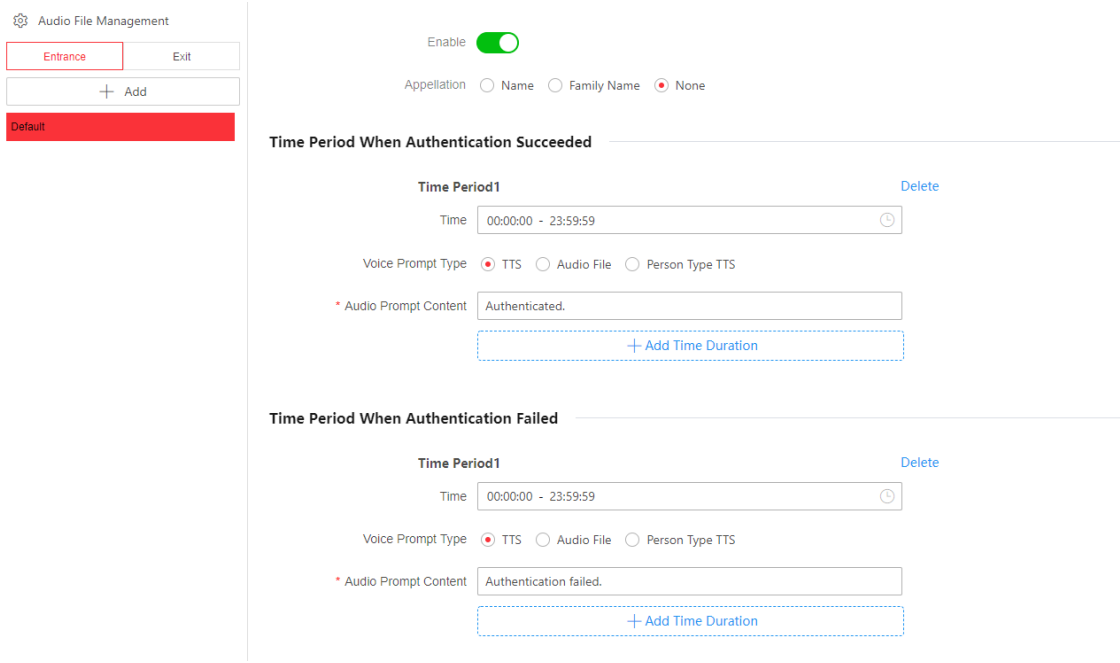


Figure 8-17 Customize Audio Content

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

   Note

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

   3) Set the audio content.

   TTS

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

Audio File

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

Note

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

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

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

Note

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

3) Set the audio content.

TTS

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

Audio File

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

Note

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

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

7. Click **Save** to save the settings.

8.9.16 Maintenance

Reboot

You can reboot the device.

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

Click **Restart** to reboot the device.

Upgrade

Upgrade Locally via PC Web

You can upgrade the device locally.

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

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

Online Upgrading via PC Web

You can upgrade the device online.

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

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

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

Restoration

Restore to Factory Settings via Web Browser

You can restore device to factory settings.

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

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

Restore to Default Settings via PC Web

You can restore device to default settings.

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

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

Export Device Parameters via PC Web

Export device parameters.

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

Backup

Click **Export** to export device parameters.

Note

Export device parameters and import those parameters to other devices.

Import Device Parameters via PC Web

Import the configuration parameters.

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

Import Config File

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

8.9.17 Device Debugging

You can set device debugging parameters.

Steps

1. Click **System and Maintenance → Maintenance → Device Debugging → Log for 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 Capture** 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.

dTof Exception Info.

Click **Export** to export the exceptional dTof reports.

Demo Mode

After enabled, the device will automatically add and authenticate after face recognition. You can set the validity period.

If disabled, all person information added in the demo mode will be cleared after disabled.

8.9.18 Motor Learning

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

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

Lane Studying/Motor Self-Test

Lane Studying

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

Motor Self-Test

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

Encoder Self-Test

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

dToF Self-Check

After enabling the function, the device will sound to exit the lane before opening/closing. The barrier is forced to open in entrace/exit at the highest speed, at this time dToF anti-pinch is defunct. If dToF is triggered or blocked, the device will sound detection failure.

Click **dToF Self-Check**, the device will test all dToFs.

Note

Make sure there are no person in the lane.

8.9.19 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**.

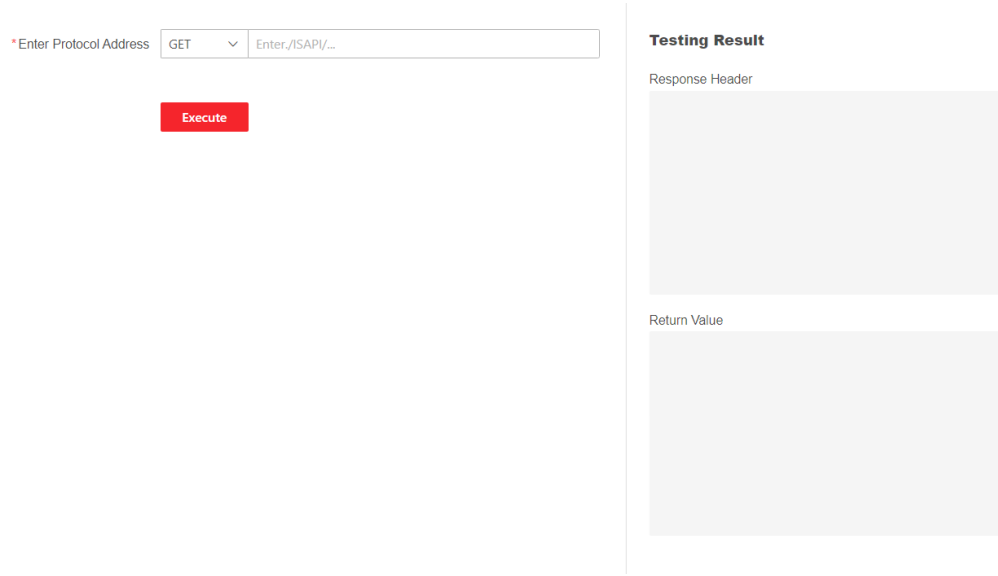


Figure 8-18 Protocol Testing

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

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

8.9.20 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.

8.9.21 Component Status

You can view the status of different components.

Lane Status

Device Component

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

Peripheral

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

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Others

Passing Mode

You can view the entrance and exit mode.

dToF Sensor Status

You can view the dToF sensor status.

Input and Output Status

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

Other Status

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

8.9.22 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.

8.9.23 Advanced Settings via PC Web

You can configure face parameters and view version information.

Go to **System and Maintenance → Maintenance → Advanced Settings** .

Enter the device activation password and click **Enter**.

Face Parameter

Enable **Custom Anti-Spoofing Detection** and you can set the **Anti-Spoofing Detection Threshold 1:1**, **Anti-Spoofing Detection Threshold 1:N**.
Enable **Lock Face for Authentication**, and set **Lock Duration**. The face will be locked for the set lock duration after the failed attempt limit of anti-spoofing detection has been reached.
Click **Save**.

Version Information

You can view the different version information here.

8.9.24 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 9 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

HikCentral Access Control (HCAC)

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

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

Appendix A. Event and Alarm Type

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

Appendix B. Error Code Description

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

Error Reason	Code	Error Reason	Code
First IR Beam Triggered	01	Second IR Beam Triggered	02
Third IR Beam Triggered	03	Fourth IR Beam Triggered	04
Fifth IR Beam Triggered	05	Sixth IR Beam Triggered	06
Seventh IR Beam Triggered	07	Eighth IR Beam Triggered	08
Ninth IR Beam Triggered	09	Tenth IR Beam Triggered	10
Eleventh IR Beam Triggered	11	Twelfth IR Beam Triggered	12
Thirteenth IR Beam Triggered	13	Fourteenth IR Beam Triggered	14
Fifteenth IR Beam Triggered	15	Sixteenth IR Beam Triggered	16
Seventh IR Beam Triggered	17	Eighteenth IR Beam Triggered	18
Nineteenth IR Beam Triggered	19	Twentieth IR Beam Triggered	20
Optional Board Offline (If the board is not installed, the error code of "59" will appear but the device functions normally)	59	Interconnecting Exception	53
Not Studying	54	Barrier Obstruction	55
Exceeding Studying Range	56	Main Encoder Offline	57
Main Motor Offline	58	Sub Motor Obstruction	60
Sub Motor Exceeding Studying Range	61	Sub Encoder Offline	62
Sub Motor Offline	63	Main Motor Drive Fault	64
Sub Motor Drive Fault	65	Main Motor Fault	66
Sub Motor Fault	67	Main Motor Over-current	68
Main Motor Under-voltage	69	Main Motor Over-voltage	70
Sub Motor Over-current	71	Sub Motor Under-voltage	72
Sub Motor Over-voltage	73	Main Motor Barrier Opening Timeout	74

Error Reason	Code	Error Reason	Code
Sub Motor Barrier Opening Timeout	75	Main Motor Encoder Exception	76
Sub Motor Encoder Exception	77		


See Far, Go Further