DS-K6B961X Series Swing Barrier

User Manual

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.
- For the permanently connected device without a disconnect equipment, a readily accessible disconnect equipment (recommended rated voltage: 400 VAC, pole number: 2-pole, rated current: 6 A) shall be incorporated into the electrical installation of the connected building.
- Port 67: The integrated DHCP server listening port within the device is used to assign IP addresses to wireless terminals when they connect to the device's hotspot. This port is enabled when the device hotspot function is activated and disabled when the hotspot function is turned off.
- Port 53: The integrated DNS server listening port within the device is used to redirect domain names to the device's mobile web address when wireless terminals access the device. This port is enabled when the device hotspot function is activated and disabled when the hotspot function is turned off.
- Port 37020: The device's SADP service port is used for device network discovery and network information configuration. This port is enabled when the device hotspot function is activated and disabled when the hotspot function is turned off.
- Port 443: The device's HTTPS server port provides a more secure method for upper-layer platforms to access the device, enabling the retrieval and configuration of device parameters. This port is enabled when the device hotspot function is activated and disabled when the hotspot function is turned off.

Contents

Chapter 1 Overview 1

1.1 Introduction 1

1.2 Main Features 1

Chapter 2 System Wiring 3

Chapter 3 Install Pedestals 5

Chapter 4 General Wiring 8

4.1 Components Introduction 8

4.2 Wiring Electric Supply 10

4.3 UART Description 12

Chapter 5 Terminal Description 13

5.1 General Wiring 13

5.2 Main Control Board Terminal Description 13

5.3 Access Board 15

5.4 Interface Board Description 18

5.5 Indicator Board 19

5.6 Camera Board 20

5.7 Alarm Input Wiring 21

5.8 Exit Button Wiring 21

Chapter 6 Reset Device 23

Chapter 7 Light Description 24

Chapter 8 Activation 26

8.1 Activate via Web Browser 26

8.2 Activate via Mobile Web 27

8.3 Activate via SADP 28

8.4 Activate Device via iVMS-4200 Client Software 29

Chapter 9 Configure Device via Mobile Web 30

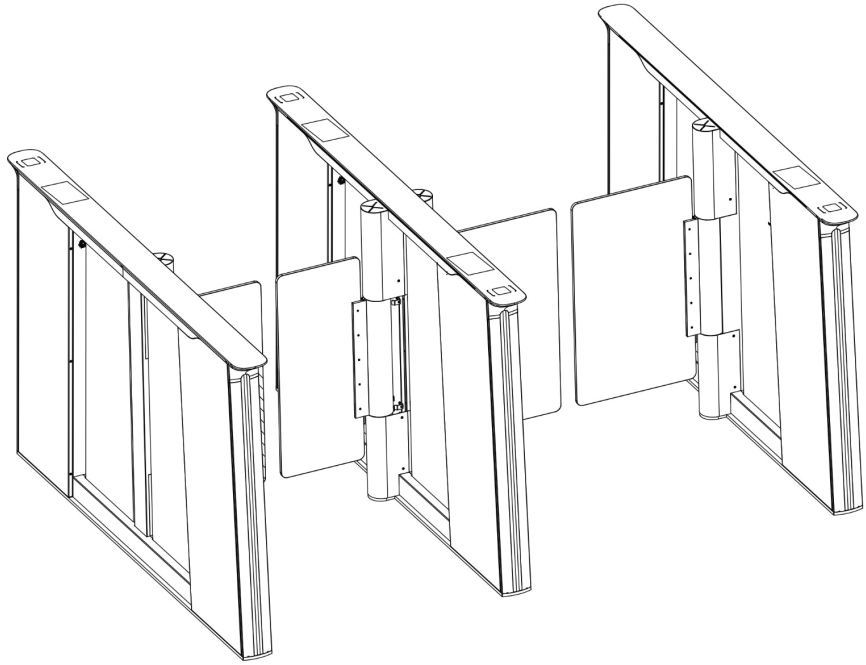
9.1 Login 30
9.2 Overview 30
9.3 Configuration 33
9.3.1 Turnstile Basic Settings 33
9.3.2 Person Management 35
9.3.3 Keyfob Settings 36
9.3.4 Device Management 36
9.3.5 View Device Basic Information 38
9.3.6 Time Settings 39
9.3.7 User Management 40
9.3.8 Network 40
9.3.9 Sub Access Control Board Settings 44
9.3.10 Event Search 44
9.3.11 Audio Settings 45
9.3.12 Access Control Settings 46
9.3.13 Turnstile Settings 54
9.3.14 Upgrade and Maintenance 60
9.3.15 Device Debugging 61
9.3.16 View User Document 62
9.3.17 Open Source Software Licenses 62
9.3.18 Log Out 62
Chapter 10 Operation via Web Browser 63
10.1 Overview 63
10.2 Login 63
10.3 Forget Password 64
10.4 Help 64
10.4.1 Open Source Software Licenses 64
10.4.2 View Online Help Document 64

10.4.3 Logout 65
10.5 Quick Operation via Web Browser 65
10.5.1 Time Settings 65
10.6 Person Management 65
10.7 Import Blocklist 66
10.8 Device Management 67
10.8.1 Sub Access Control Board Management 67
10.8.2 Batch Devices Management 68
10.9 Turnstile 70
10.9.1 Search Event 70
10.9.2 Paramenter Settings 71
10.9.3 Turnstile Configuration 77
10.10 System and Maintenance 87
10.10.1 View Device Information 87
10.10.2 Set Time 87
10.10.3 Change Administrator's Password 88
10.10.4 Online Users 88
10.10.5 View Device Arming/Disarming Information via PC Web 88
10.10.6 Set Working Mode via PC Web 89
10.10.7 Network Settings 89
10.10.8 Set Wiegand Parameters via PC Web 93
10.10.9 Serial Port Settings 94
10.10.10 Elevator Control via PC Web 95
10.10.11 Set Video and Audio Parameters via PC Web 97
10.10.12 Set Image Parameters 97
10.10.13 Event Linkage 98
10.10.14 Preference Settings 100
10.10.15 Upgrade and Maintenance 103

10.10.16 Device Debugging 104
10.10.17 Test Protocol via PC Web 105
10.10.18 Set Network Penetration Service via PC Web 106
10.10.19 Component Status 106
10.10.20 View Log via PC Web 107
10.10.21 Certificate Management 107
Chapter 11 Other Platforms to Configure 109
Appendix A. Event and Alarm Type 110
Appendix B. Legal Information 111

Chapter 1 Overview

1.1 Introduction



The swing barrier is designed to detect unauthorized passing from the entrance or exit. By adopting the swing barrier integratedly with the access control system, person should authenticate to pass through the lane via swiping IC or ID card, scanning QR code, etc. It is widely used in attractions, stadiums, construction sites, residences, etc.

1.2 Main Features

- Supports AP mode for mobile Web, for Android phones to access more easily by a simple touch via NFC function.
- Anti-passback: Supports cross-device anti-passback function, effectively preventing unauthorized personnel from following in.
- WEB management: Supports mobile Web and PC Web management, and can perform operations such as personnel management, parameter configuration, event query, and system maintenance.
- Fire linkage: The equipment has a fire linkage interface. When the fire signal is triggered, the barrier will be open automatically for emergency evacuation.
- Fire alarm passing

When the fire alarm is triggered, the barrier will be open automatically for emergency evacuation.

- Barrier is in free status when powering down, allowing people to pass freely. Super capacitor (optional) can realize automatic door opening in case of power failure.

Chapter 2 System Wiring

The preparation before installation and general wiring.

Steps

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

Note

The distance between the nearest two line is 581+200 mm. L represents the lane width.

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

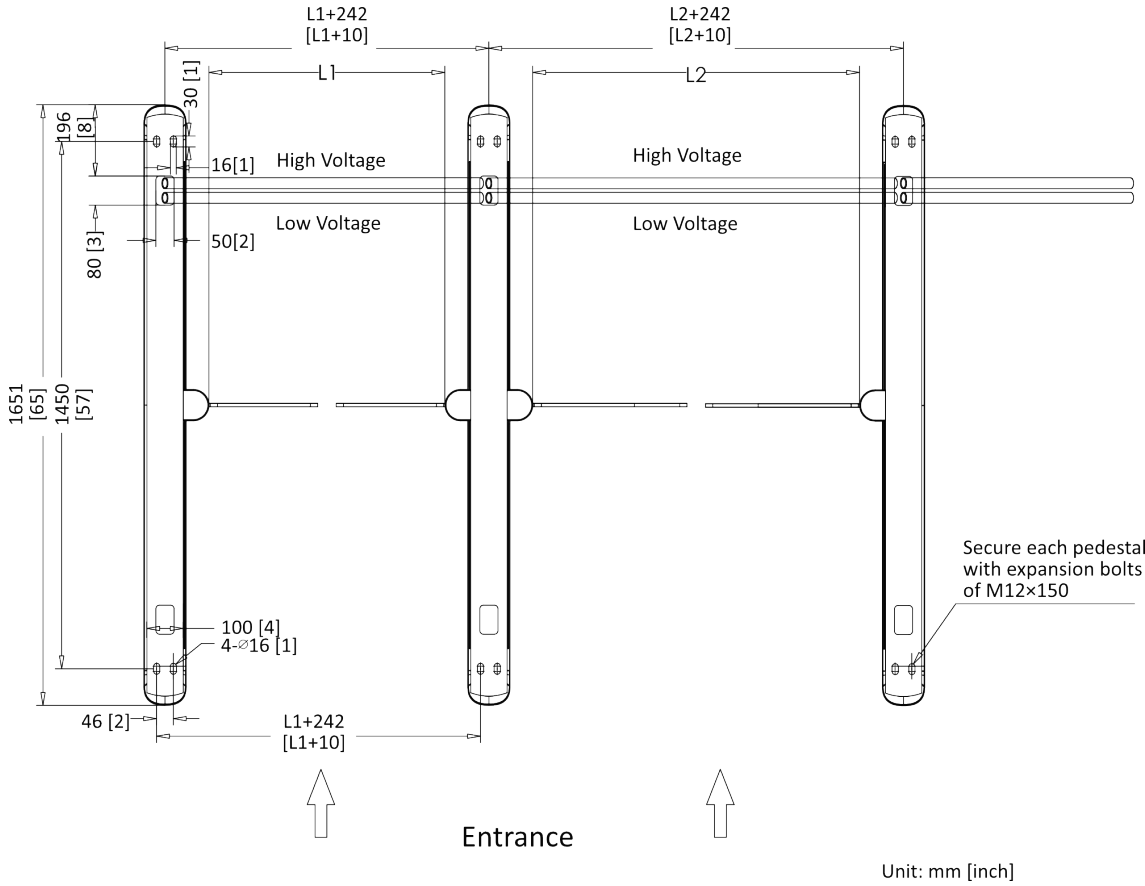


Figure 2-1 Hole Position Diagram

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

Note

- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- If the face recognition module are required to be connected on the left lane, you should increase the conduit diameter or bury another conduit for the external cables.
- You should bury one network cable and one high voltage conduit for the right and middle lane.
- The network cable must be CAT5e or the network cable has better performance. And the suggested network cable length should be less than 100 m.

Chapter 3 Install Pedestals

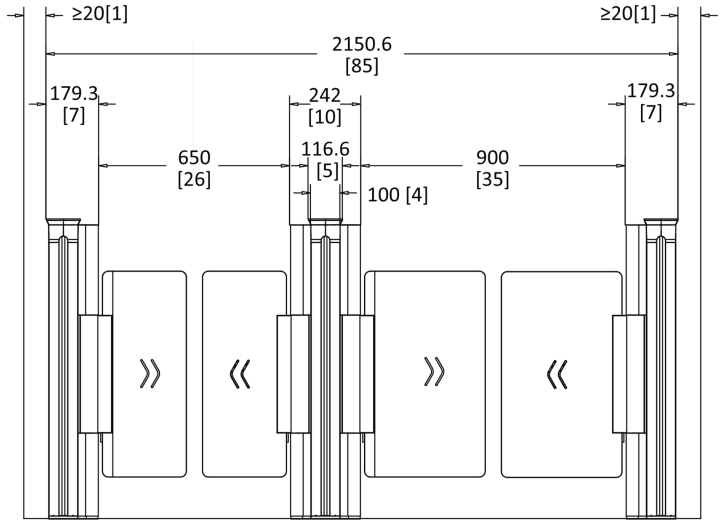
Before You Start

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

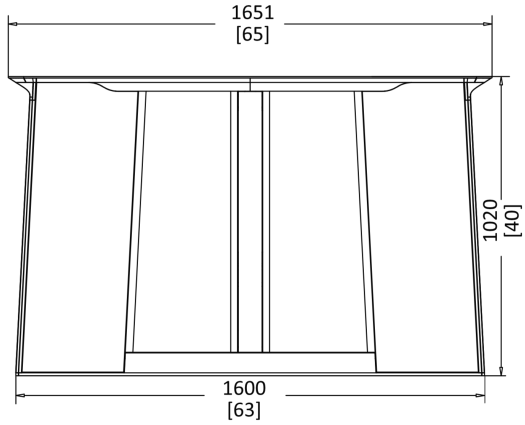
Steps

Note

- Make sure the device is installed on flat surface. The foundation should be hard and the thickness should exceeds the length of the expansion bolt.
- Make sure the device is powered off during installation and other operations.
- The installation tools are put inside the package of the pedestal.
- In order to prevent stainless steel from rusting due to dirt during the installation, it is recommended to tear off the protective film after the device is installed.
- There may be residual glue at the film cutting position, and it is recommended to wipe the glue with WD-40 protective liquid after tearing the film.
- Indoor use only. Do not immerse the pedestal in the water.
- If the installation area is close to the wall, make sure the distance between the pedestal and the wall should be more than 20 mm, or you might cause damage to the device or cannot open the pedestal's top panel.



Front View



Side View

Unit: mm [inch]

Figure 3-1 Dimension

1. Prepare installation tools, check the components, and clean the installation base.
2. Align the pedestals with the pre-buried expansion bolts, and remove the side maintenance door.
3. Secure each pedestal with expansion bolts, and fix the maintenance door to its original position.
   Scan the QR Code to view the installation and wiring guide video.

Chapter 4 General Wiring

Note

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

Scan the QR code to view the wiring guide video.

4.1 Components Introduction

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

Note

The voltage fluctuation of the electric supply is between 100 VAC and 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.

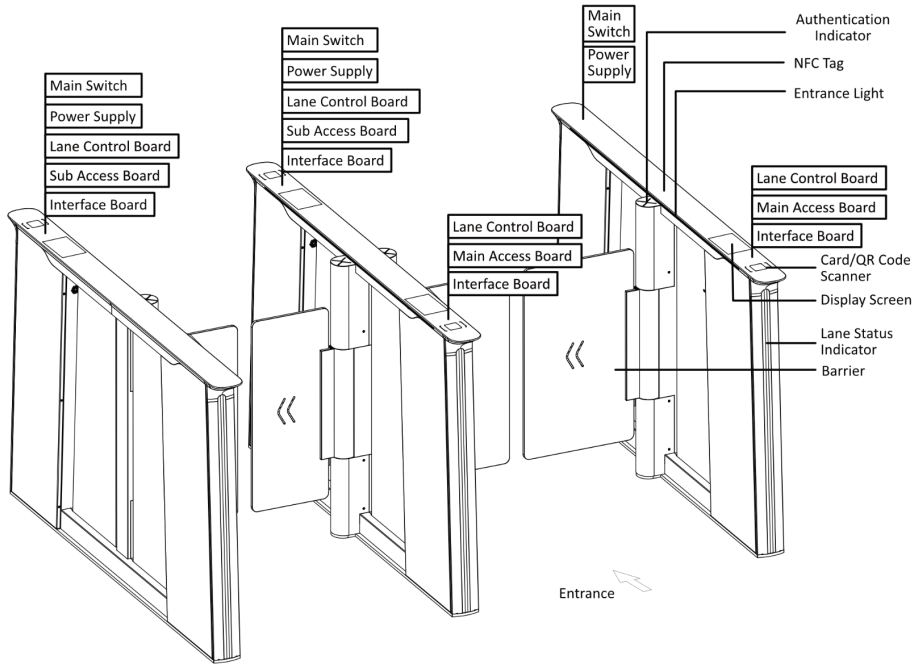


Figure 4-1 Components Diagram

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

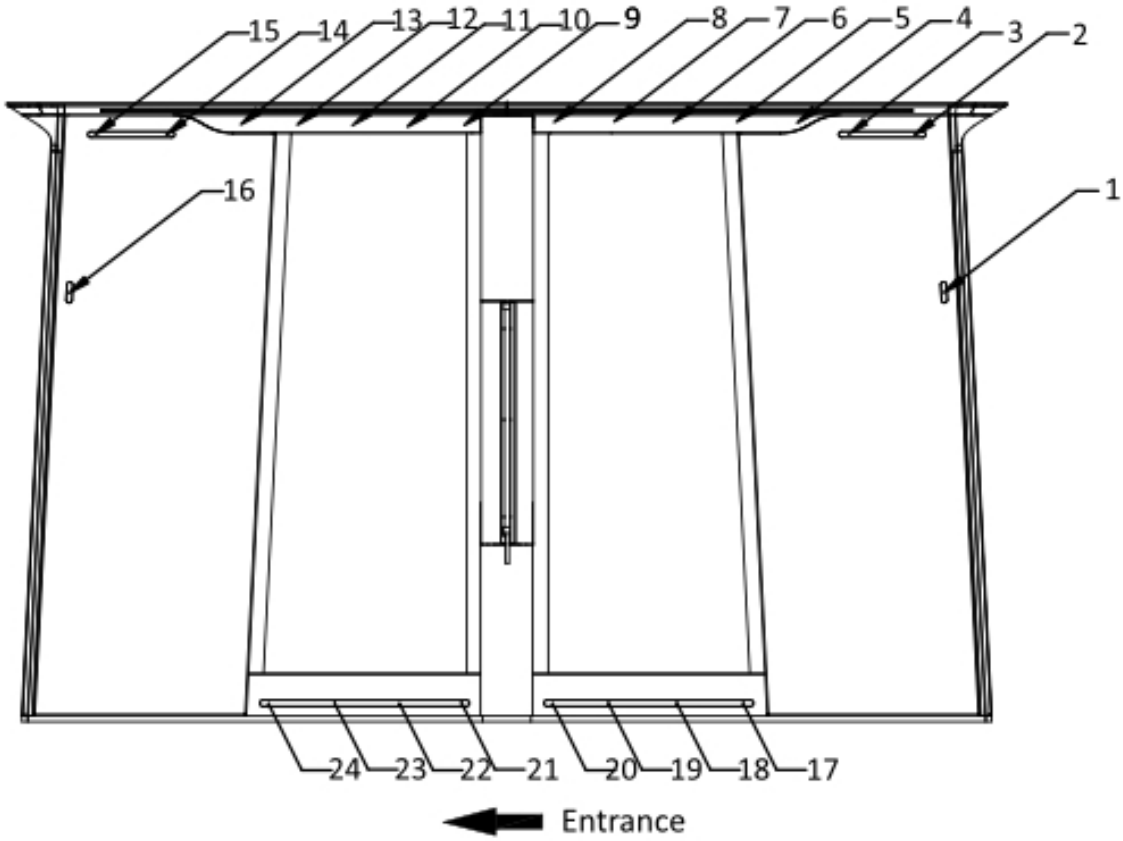


Figure 4-2 dToF Module

4.2 Wiring Electric Supply

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

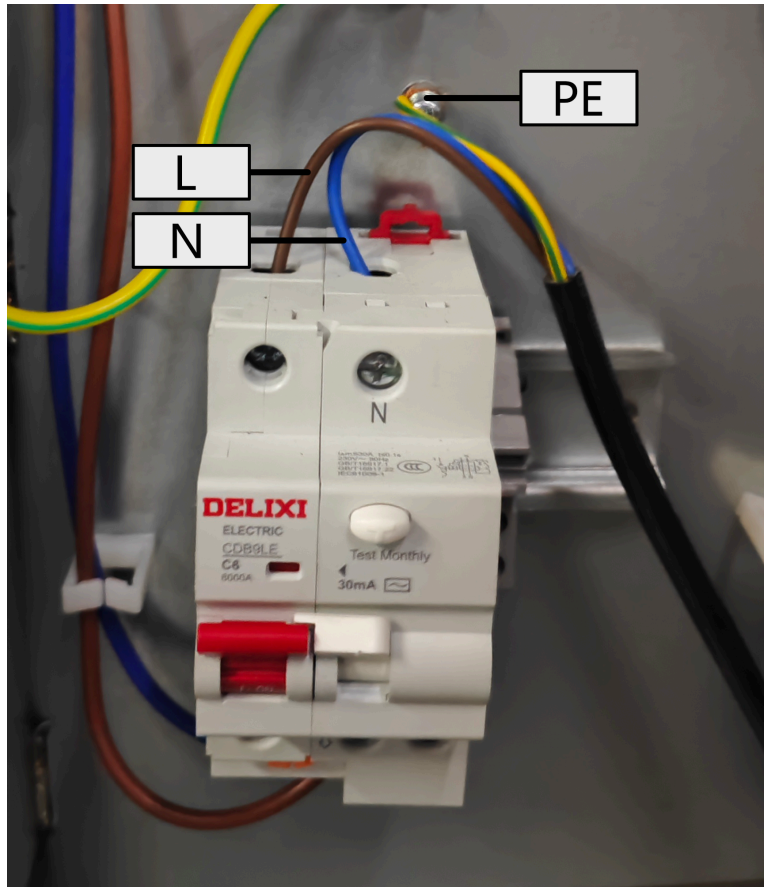


Figure 4-3 Wire Electric Supply

Caution

To avoid people injury and device damage, the PE terminal must connect to the ground.

Note

- The cable bare part should be no more than 8 mm. If possible, wear an insulation cap at the end of the bare cable. Make sure there's no bare copper or cable after the wiring.
- The Terminal L and the Terminal N cannot be wired reversely. Do not wire the input and output terminal reversely.
- To avoid people injury and device damage, when testing, the ground resistance of the equipotential points should not be larger than 2 Ω.
- Use the device in conjunction with an UPS.
- To avoid the injury when the grounding cable is ripped away, the cable for wiring the ground should be longer than the high voltage cable.

4.3 UART Description

If the device is not installed with the card reader, QR code scanner, etc., you can use the reserved UARTs to wire.

The following picture describes the UARTs' position.

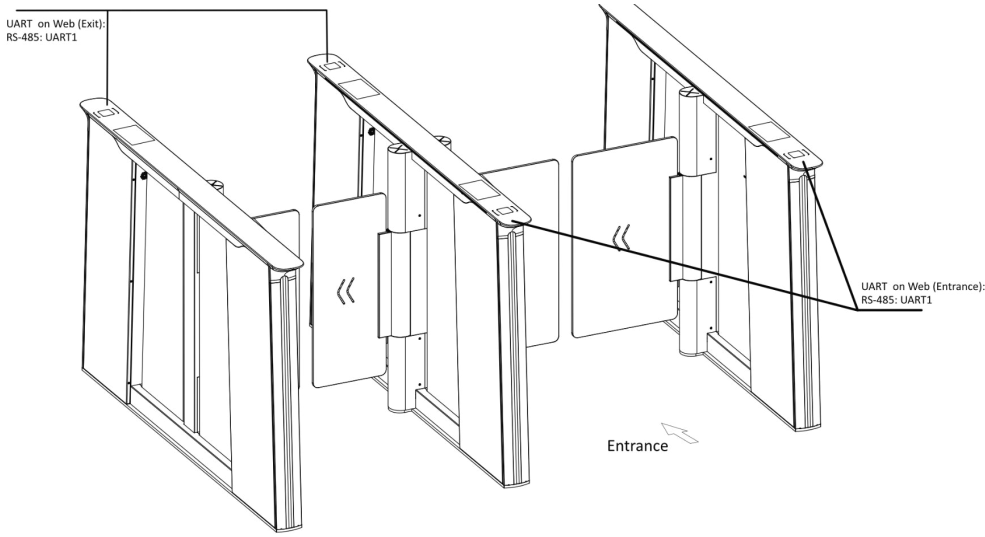


Figure 4-4 UART Description

Chapter 5 Terminal Description

5.1 General Wiring

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

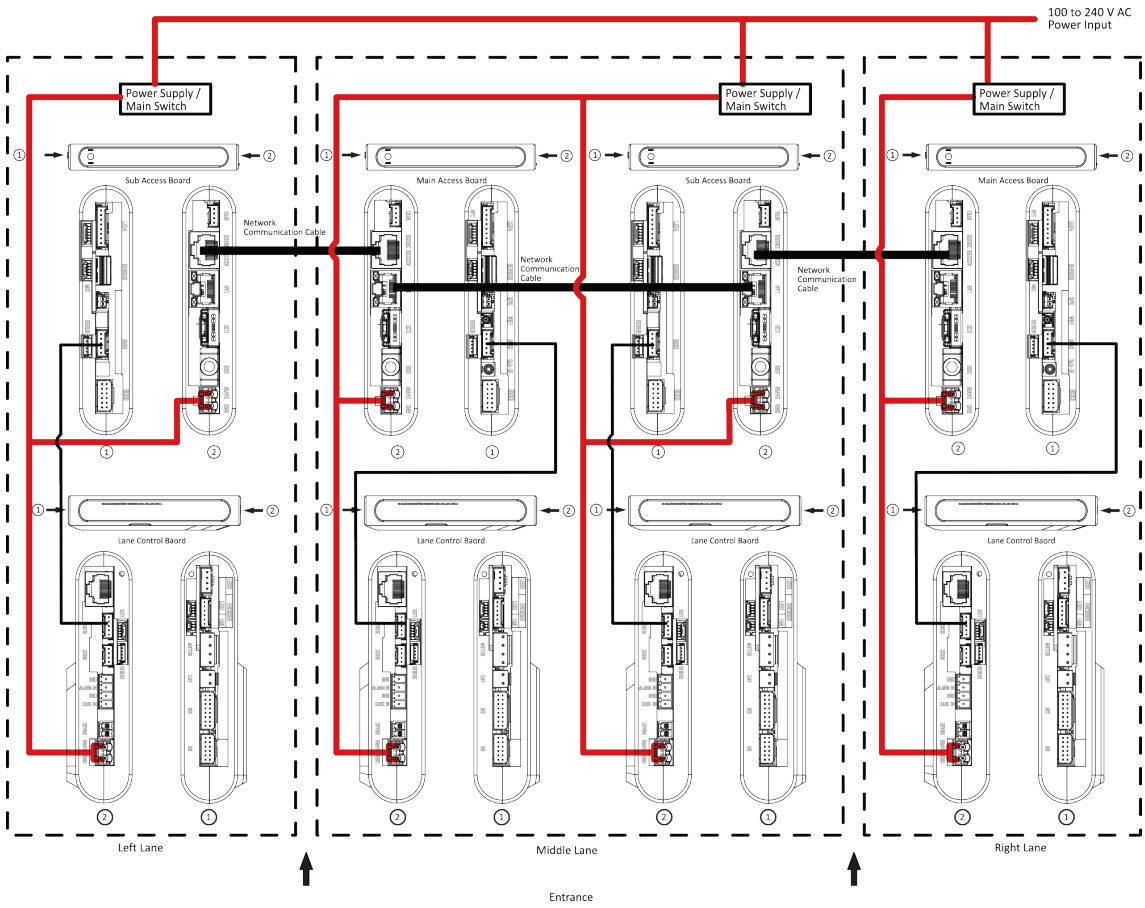


Figure 5-1 General Wiring

Note

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

5.2 Main Control Board Terminal Description

The picture displayed below is the main control board diagram.

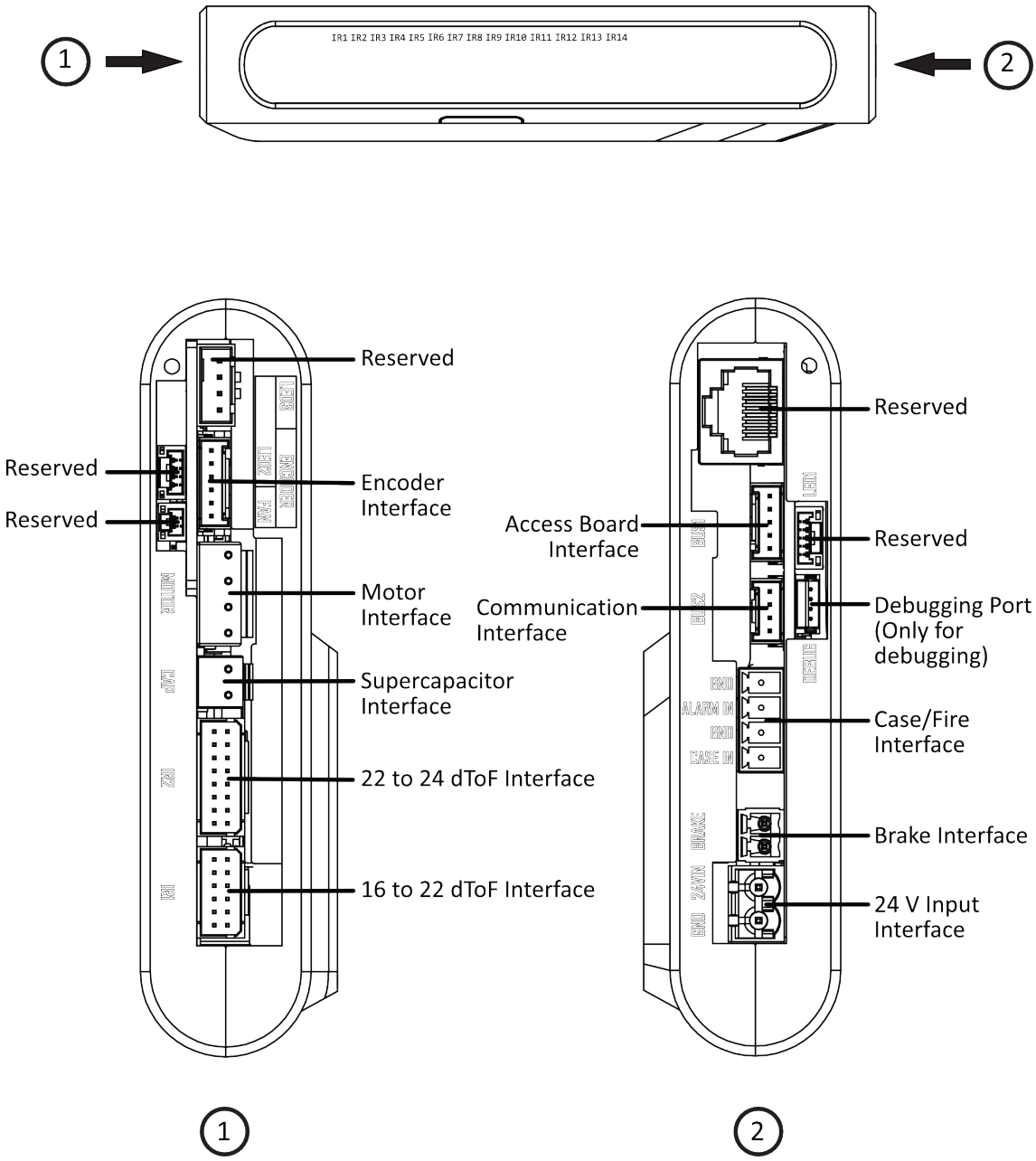


Figure 5-2 Main Control Board

Note

The communication interface can connect with the dToF sensor and arrow light board. You can connect the 1 to 16 dToF to the dToF sensor.

5.3 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

Only the main access board of the right pedestal contains SUB-1G antenna interface. Middle access board has no SUB-1G antenna interface.

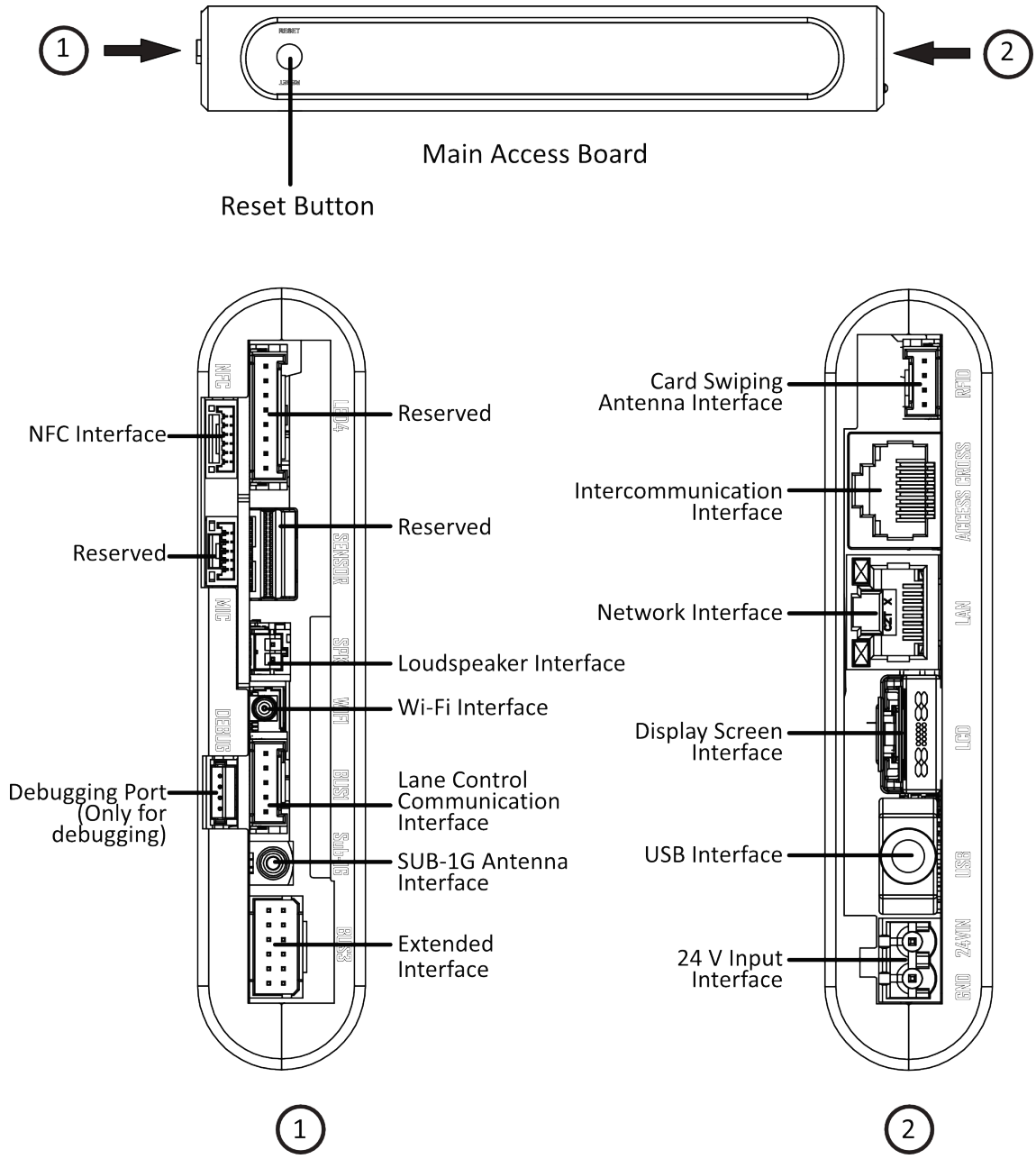


Figure 5-3 Main Access Board

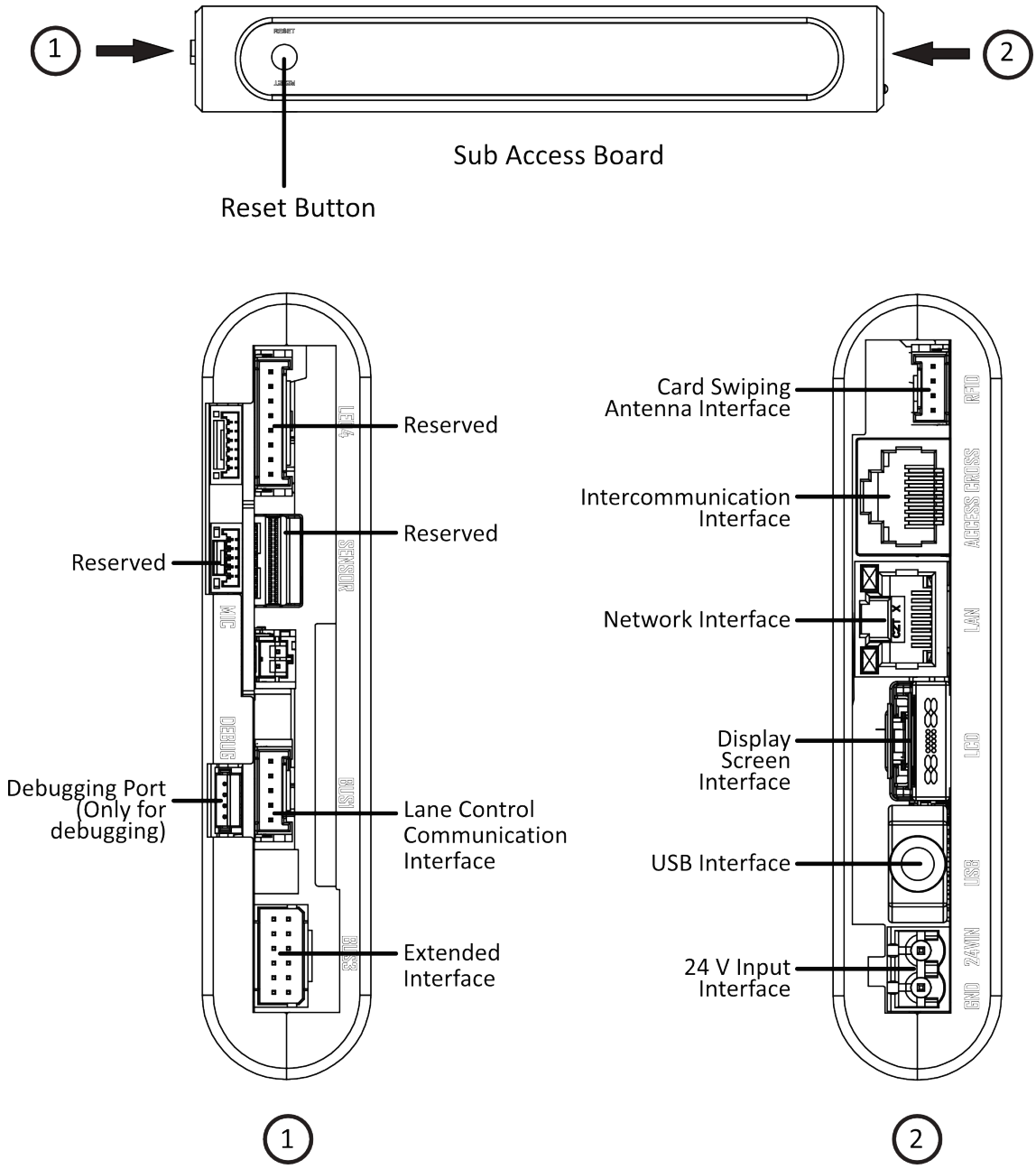


Figure 5-4 Sub Access Board

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

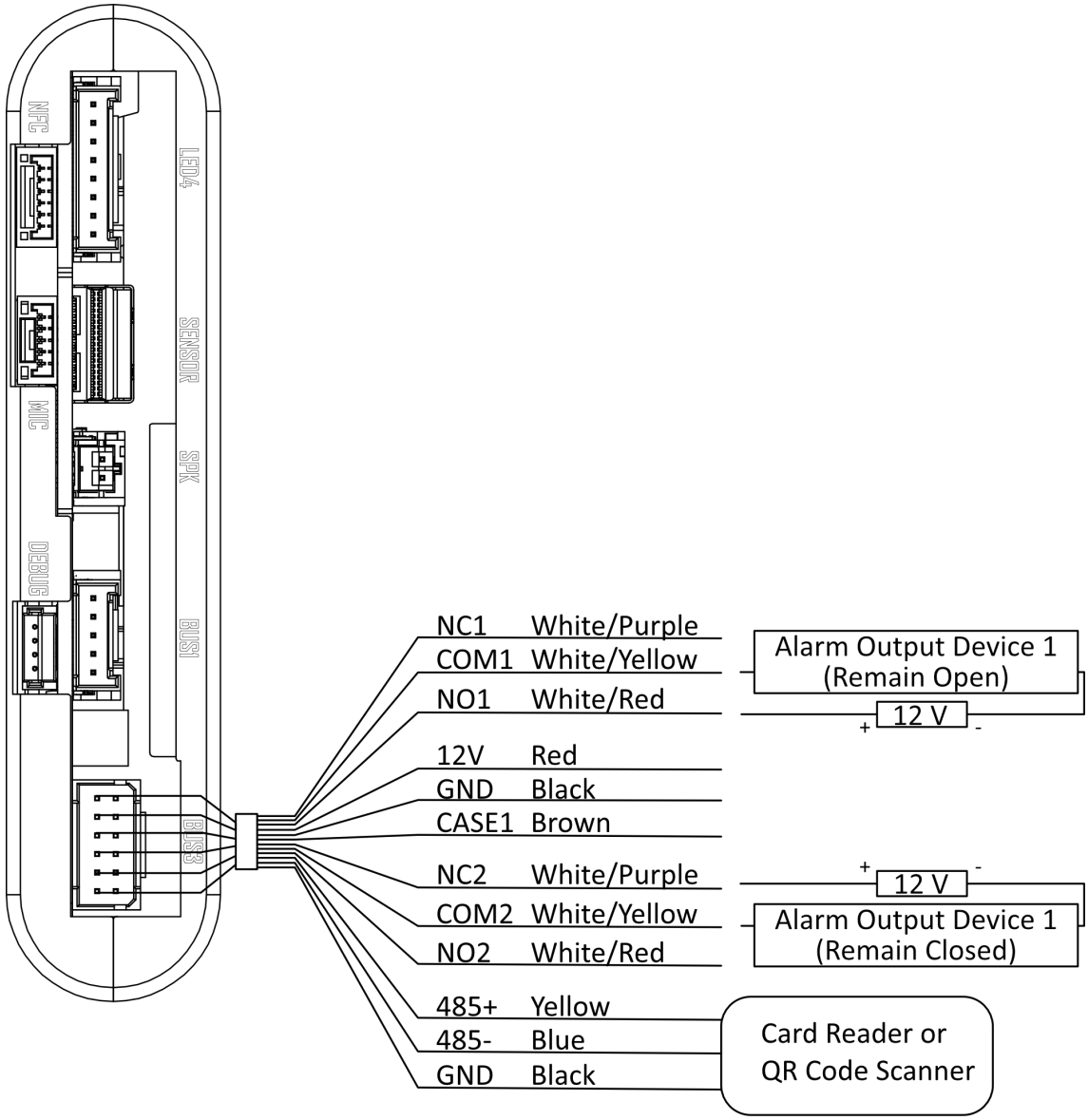


Figure 5-5 Wring Diagram of BUS3 Interface

5.4 Interface Board Description

The interface board can connect the card receiver, card reader, QR code scanner, people counting module, etc.

The interface board is shown as below:

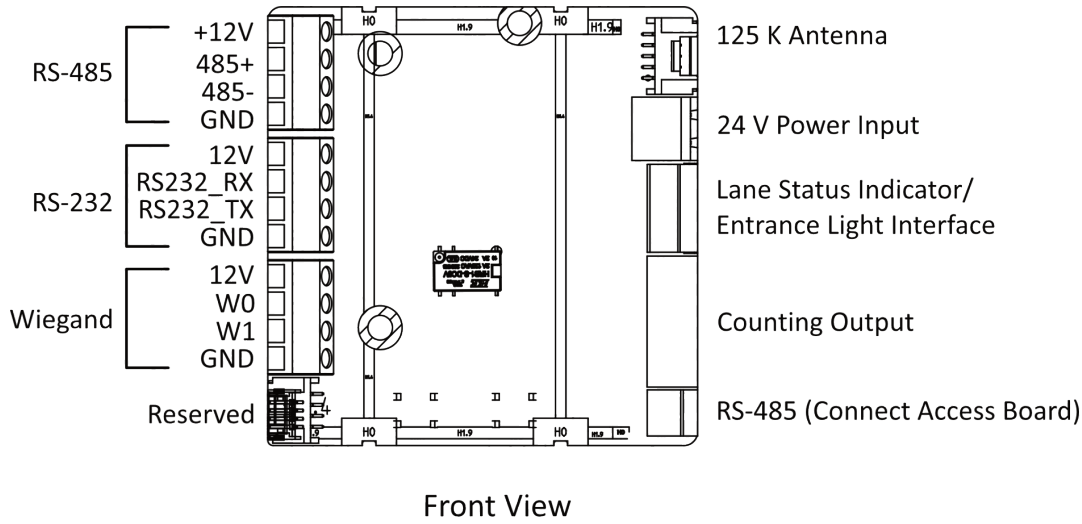


Figure 5-6 Interface Board (Front)

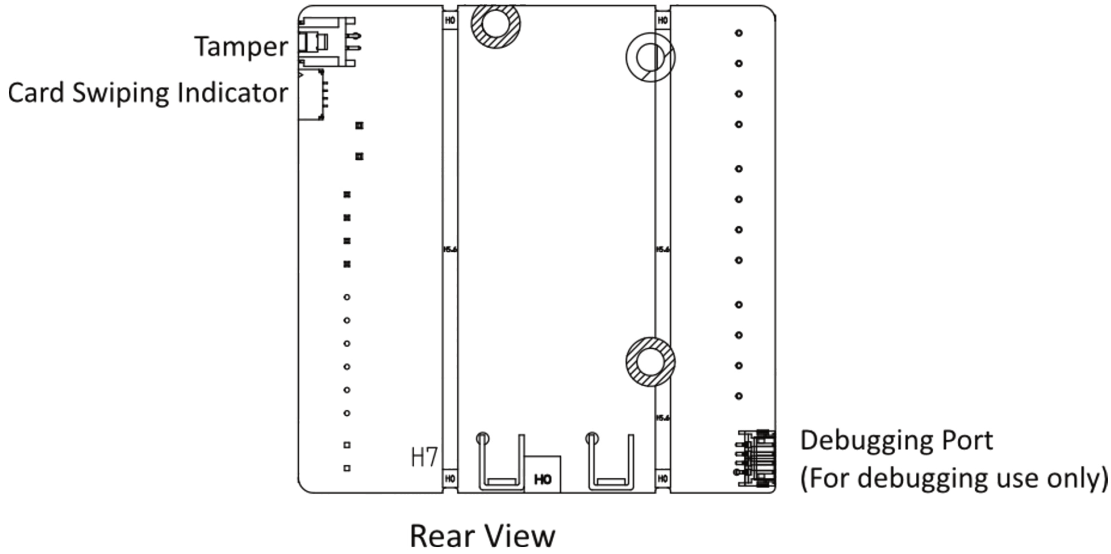


Figure 5-7 Interface Board (Rear)

5.5 Indicator Board

View the indicator board.

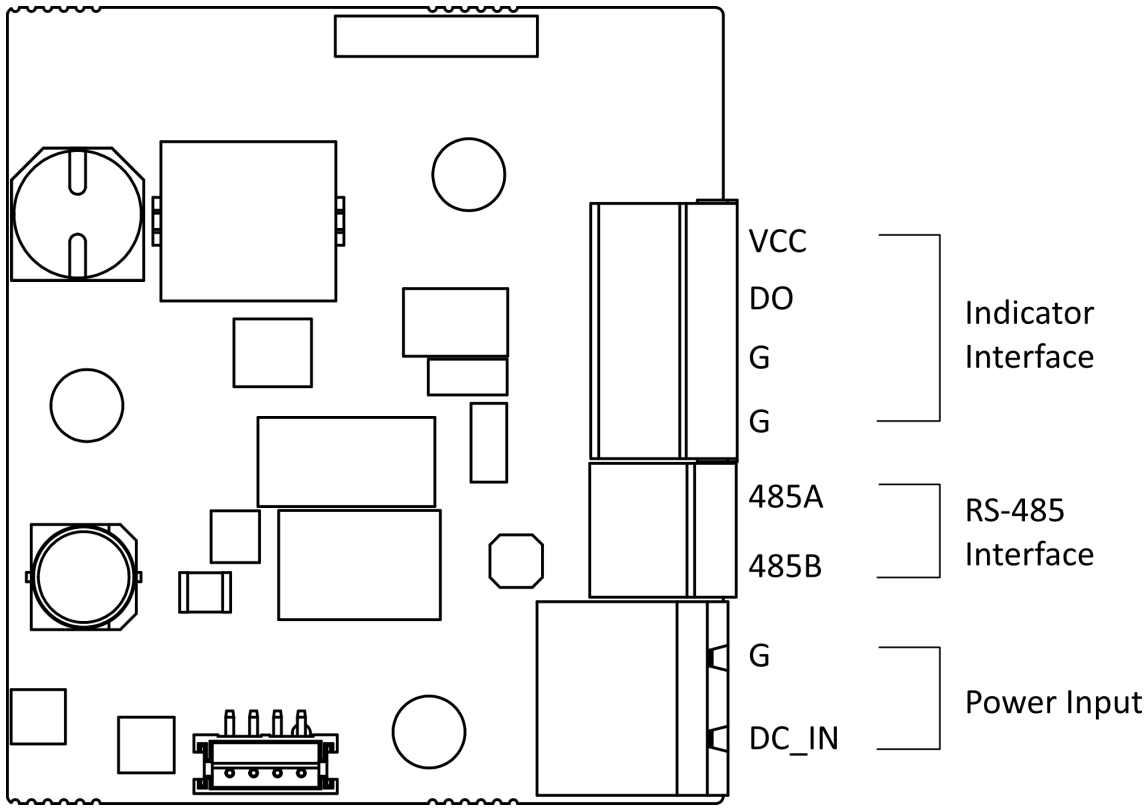


Figure 5-8 Indicator Board

5.6 Camera Board

View the camera board.

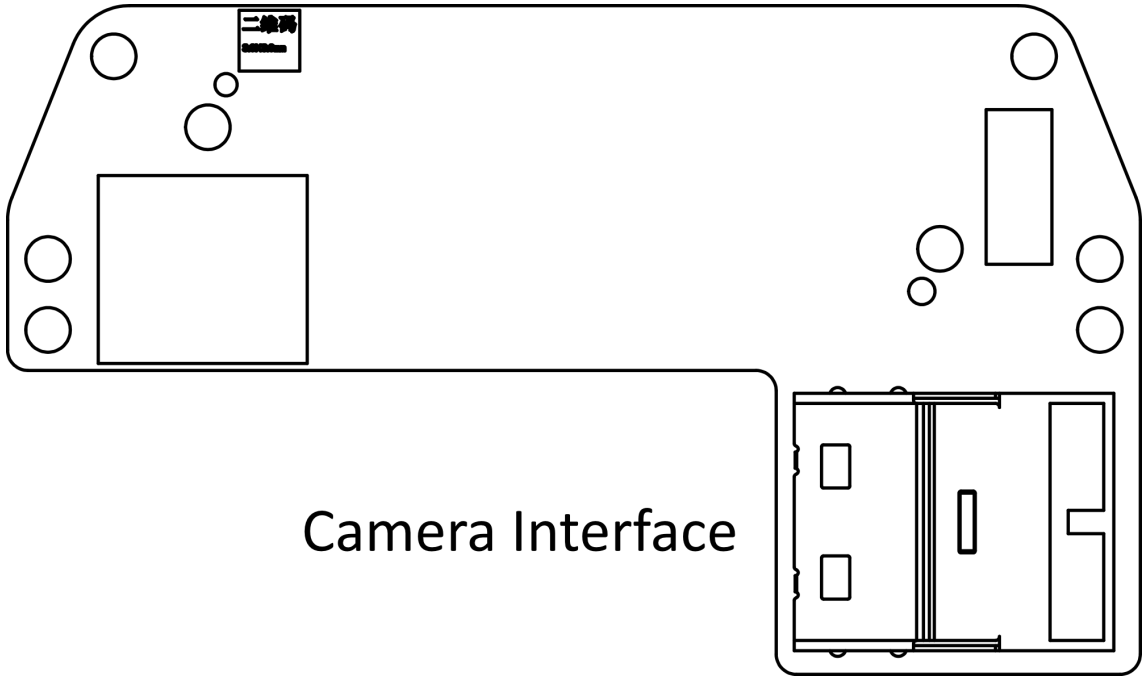


Figure 5-9 Camera Board

5.7 Alarm Input Wiring

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

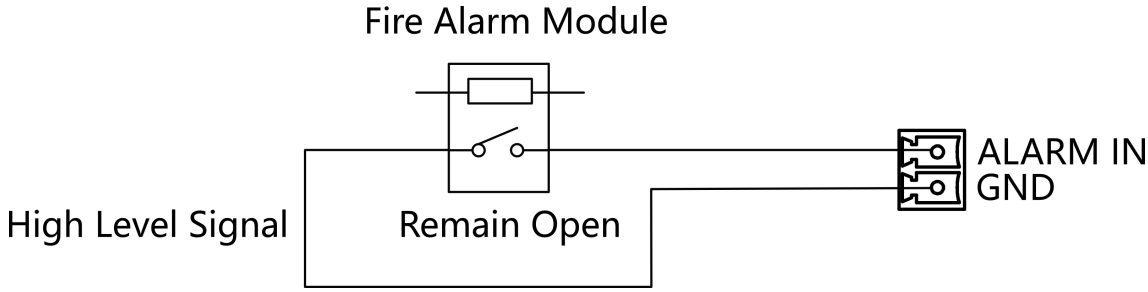


Figure 5-10 Remaining Open

5.8 Exit Button Wiring

You can view the exit button wiring diagram.

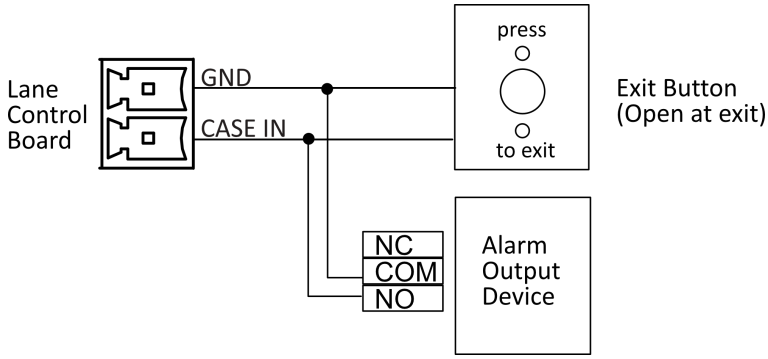


Figure 5-11 Exit Button Wiring

Chapter 6 Reset Device

Steps

1. Hold the reset button.

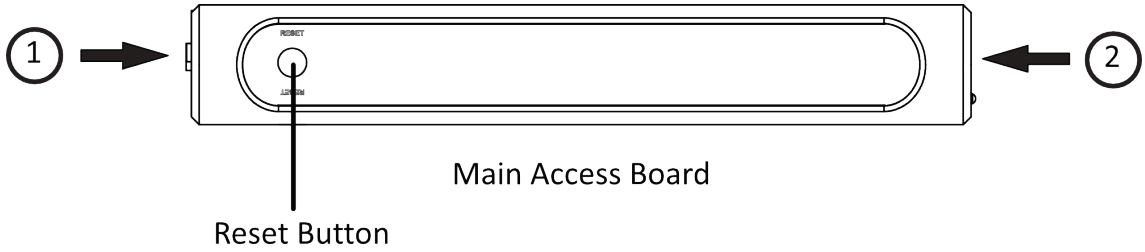


Figure 6-1 Initialization Reset Position

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 7 Light Description

Side Light

The side light indicates different status of the lane, including inductive, prohibited and authenticated passing.

Note

- When the device detects people within 1.5 m, the side light will be flashing.
- Only the right side light indicates the lane status.
- Light stays blue: free-passing
- Light stays green: authenticated passing
- Light stays red: passing prohibited

Entrance Light

Before Passing

- Light stays green: authenticated passing
- Light flashes green: free passing
- Light stays red: passing prohibited
- Light flashes red: authentication failed or exception alarm

During Passing

- The entrance light will be blinking in your heading direction when authentication succeeds, and will resume when you pass through.
- You can set colors for the entrance light to indicate different status, including standby, authentication completed, authentication failed and alarm.
- If a visitor enters the lane while another one from the opposite direction is authenticated, the barrier will stay open and the entrance light will switch direction until both visitors pass through.

Barrier Light

The barrier light stays white by default. You can set the barrier light color at your needs.
The barrier light will not change color according to the lane status or authentication results.

Card Light

The card light will stay white when the device detects people approaching until people pass through.

Arrow Light

- The arrow light stays off when the device is on standby mode.
- The light on the right side will flash green ready for authentication.

- The light on both left and right side will stay green for authenticated passing.
- The light on the right side will flash red when authentication fails.

Chapter 8 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

8.1 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.

8.2 Activate via Mobile Web

You can activate the device via mobile web.

Steps

1. If device hotspot is disabled: Make sure your mobile phone and the device are connected to the same network. Place your phone to the NFC area and the device IP address will pop up, tap the address to go to the login page.
2. If device hotspot is enabled:
   - Android System: Place your phone to the NFC area and the name and password of the device hotspot will be obtained automatically. Confirm to connect, you will go to the login page.
   - iOS Ssystem: Enable the phone's Wi-Fi function, and connect to the current device's hotspot. After hotspot is connected, you will go to the login page.

   Note

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

   Caution

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

   Note

   Characters containing admin and nimda are not supported to be set as activation password.
3. Create a new password (admin password) and confirm the password.

   Caution

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

   Note

   Characters containing admin and nimda are not supported to be set as activation password.
4. Click **Activate**.
5. You can configure the turnsile basic parameters, keyfob settings, light settings, network settings, access control settings, etc.

8.3 Activate via SADP

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

Before You Start

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

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

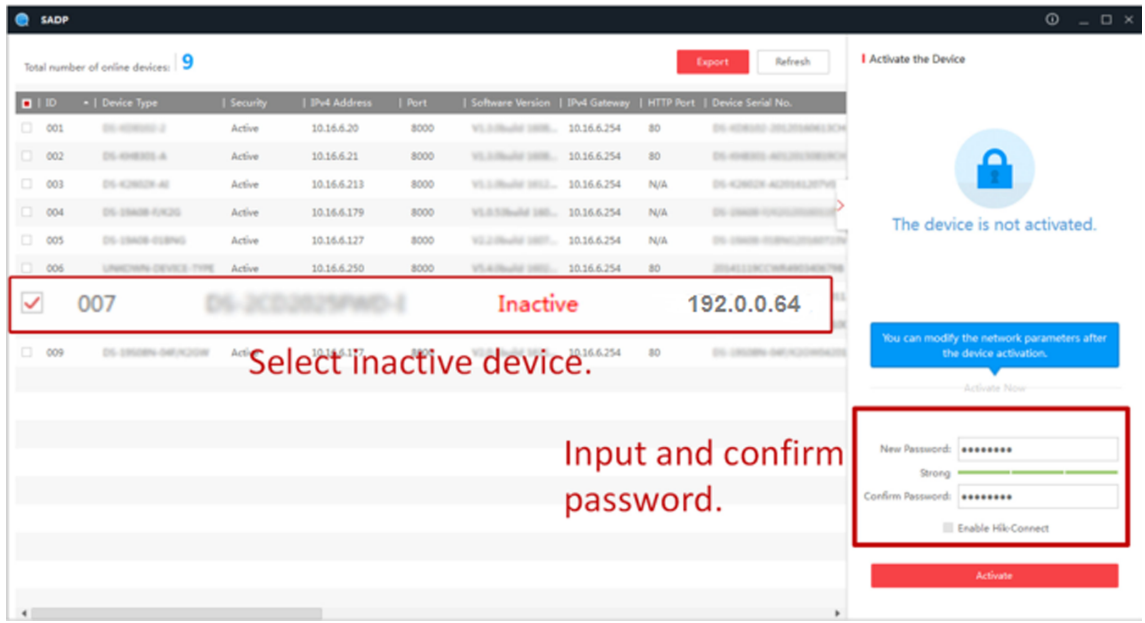
Steps

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

Caution

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

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



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

5. Modify IP address of the device.

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

8.4 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 9 Configure Device via Mobile Web

9.1 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.

9.2 Overview

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

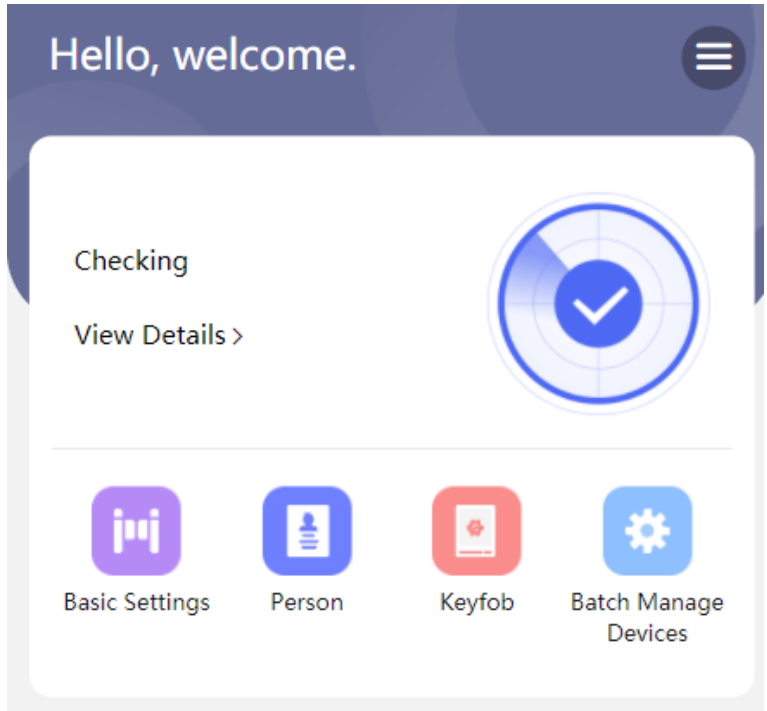


Figure 9-1 Status and Quick Settings

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, user page, keyfob page and network page batch device management page.

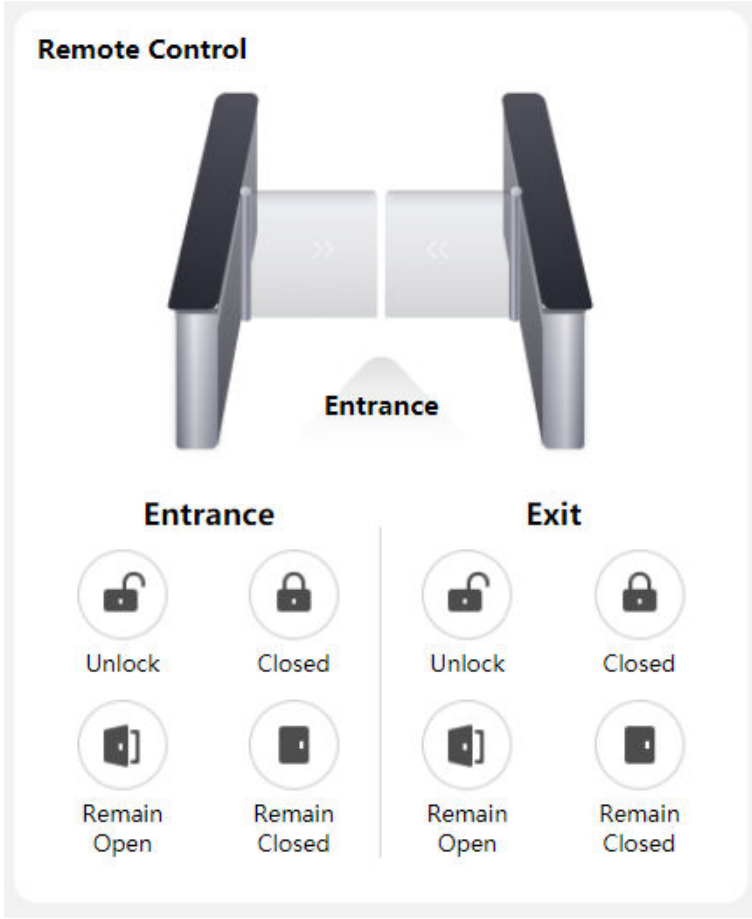


Figure 9-2 Remote Control

You can remotely control barrier by tap the icons.

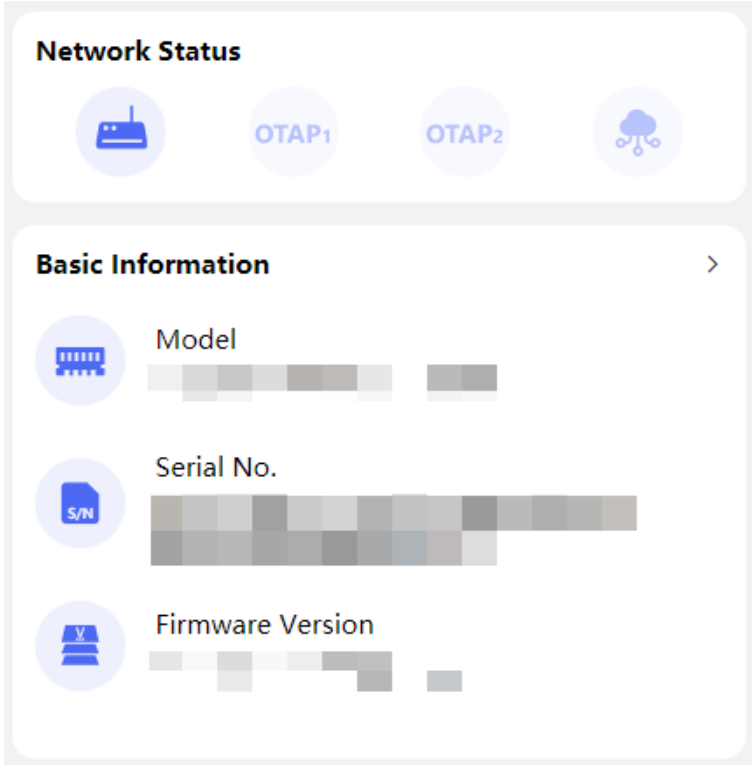


Figure 9-3 Network Status and Basic Information

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

9.3 Configuration

9.3.1 Turnstile Basic Settings

You can set the basic parameters of the turnstile.

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

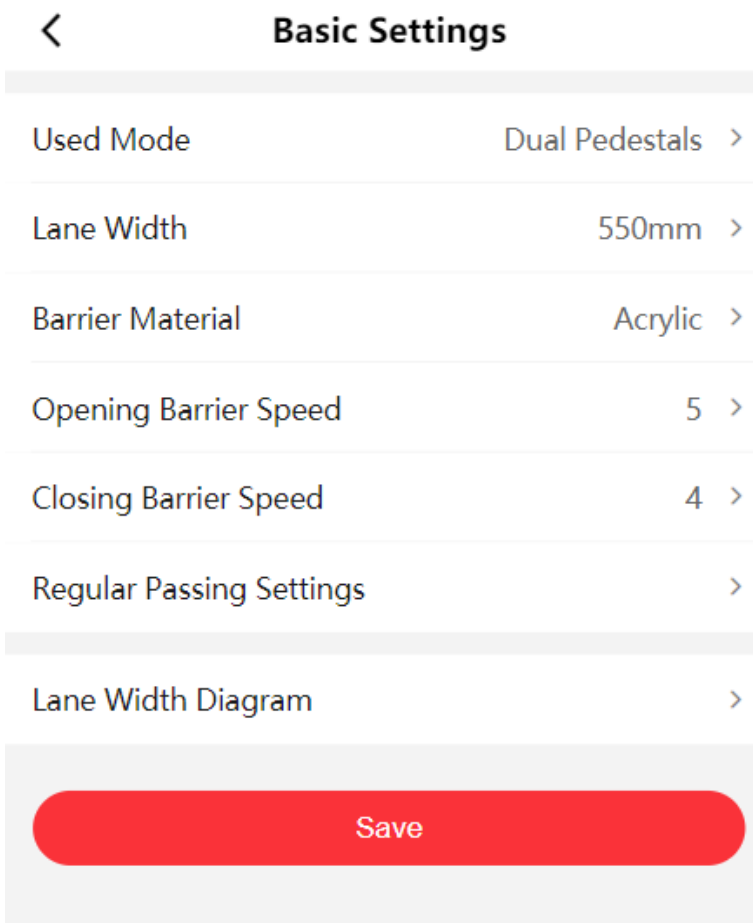


Figure 9-4 Turnstile Basic Parameters

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.

Barrier Material

Select a barrier material according to actual situation.

Lane Width

Select a lane width 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**.

9.3.2 Person Management

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

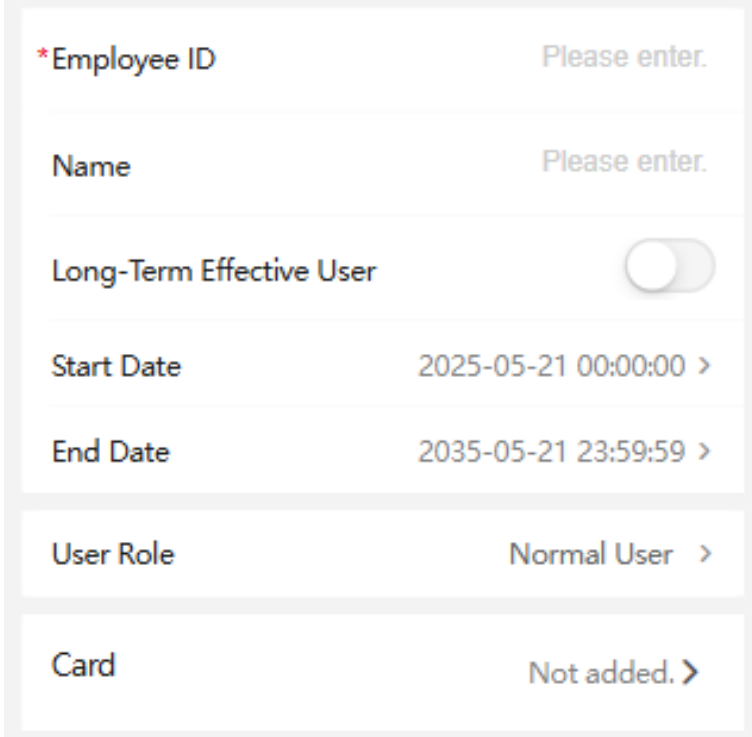


Figure 9-5 Person Management

Add Person Basic Information

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

Add Card

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

Set Person Permission

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

Tap **Save**.

Person Management

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

9.3.3 Keyfob Settings

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

Tap **Management** to enter the page. Tap **+** to add keyfob.

- Select **Manual Add** and the keyfob adding window will pop up. Enter the keyfob's **Name** and **Serial Number**. Tap **Save** to add the keyfob.

  Single Lane

  Tap **Single Lane** and check the device name. Tap **Confirm**. The selected device barrier can open/remain open.

  Multi-Lane

  Tap **Multi-Lane** and check the device name. Tap **Confirm**. Multiple devices barriers can open/remain open.
- Select **Device Pairing** . Stand close to the current device, then press and hold the button on the bottom left of the keyfob to add. Upon successful pairing, the keyfob's serial number is automatically added to the device. Tap **Complete** to add the keyfob.

9.3.4 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**.

9.3.5 View Device Basic Information

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

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

You can change the device name.

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

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

Tap **Save**.

9.3.6 Time Settings

View current time and set the time zone.

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

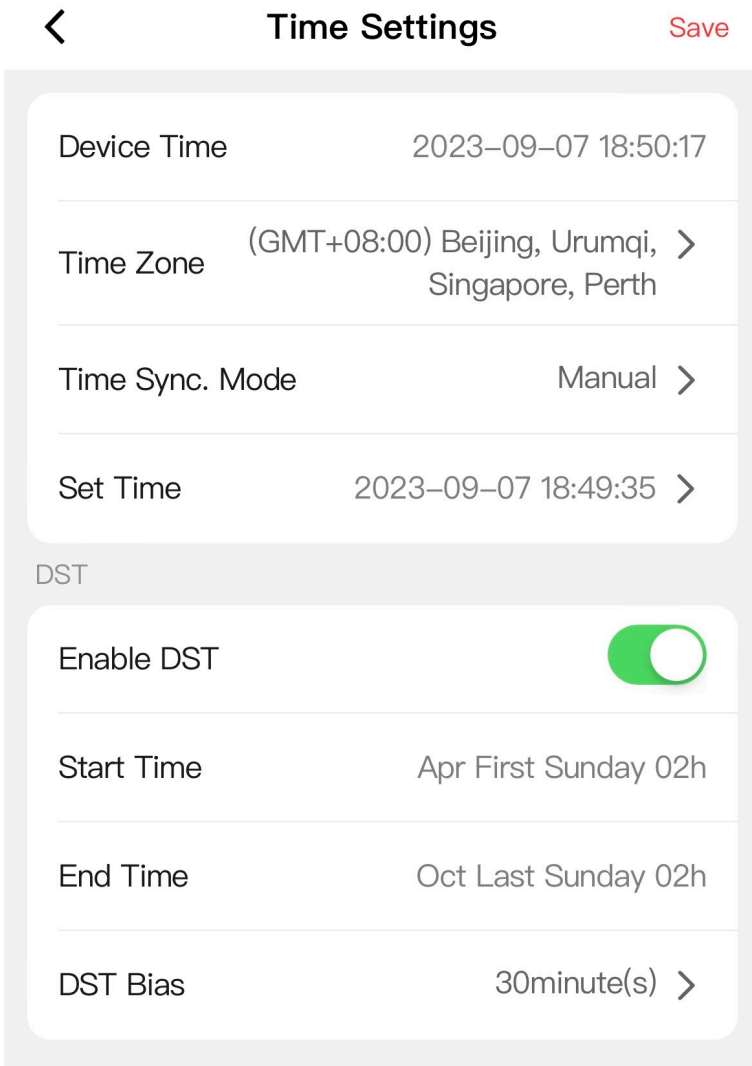


Figure 9-6 Time Settings

Device Time

You can view current time.

Time Zone

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

Time Sync. Mode

Manual

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

NTP

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

DST

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

Tap **Save**.

9.3.7 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**.

9.3.8 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 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** .

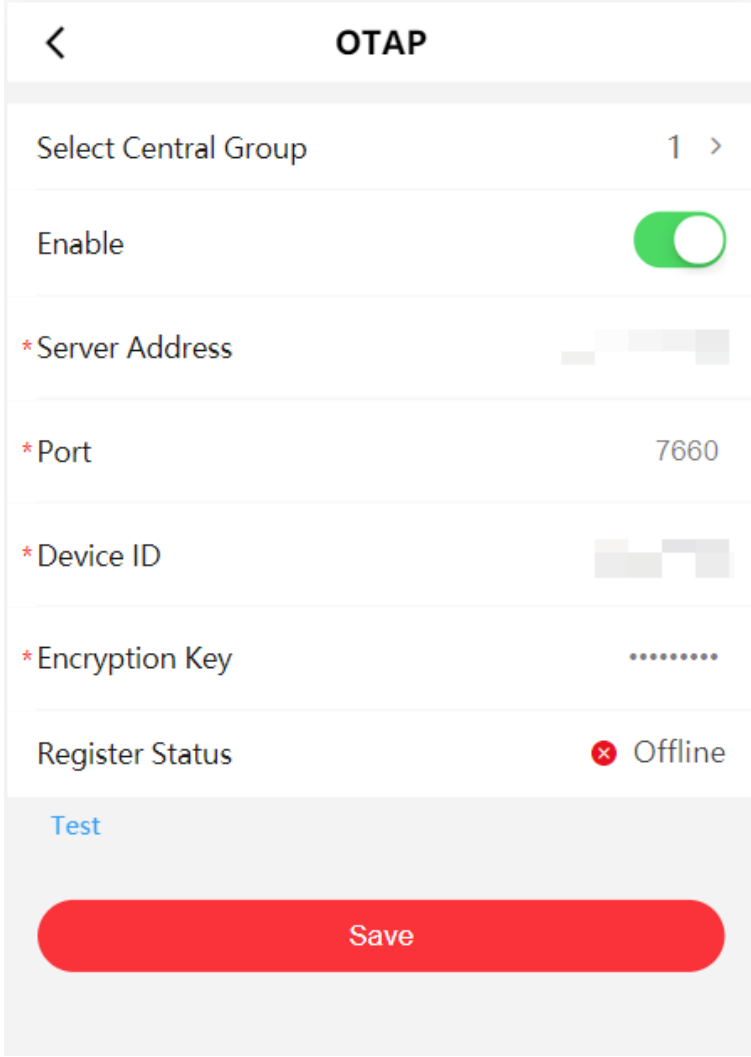


Figure 9-7 OTAP

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**.

9.3.9 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.

9.3.10 Event Search

Tap ≡ → **Event Search** .

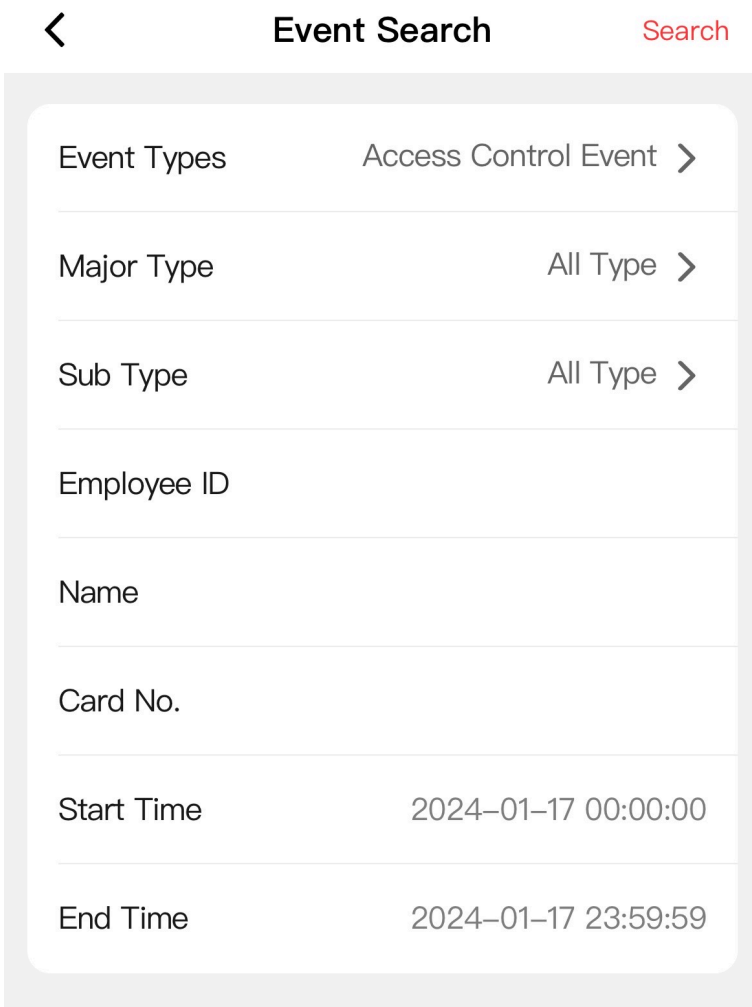


Figure 9-8 Event Search

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

Note

It supports searching for names within 128 digits.

The search results will be displayed in the list.

9.3.11 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.

You can enable **Audio Equalization**, the device will auto adjust frequency by audio algorithm to improve audio quality and equalize audio effect.

Tap **Save**.

9.3.12 Access Control Settings

Set Authentication Parameters

Set authentication parameters.

Steps

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

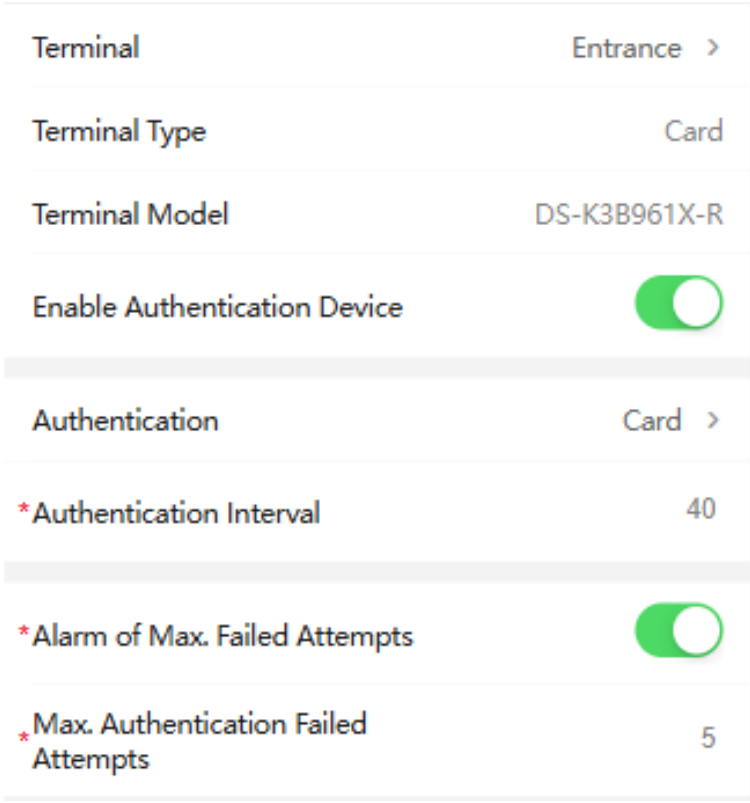


Figure 9-9 Authentication Settings

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

Terminal

Select terminal for settings.

Terminal Type

Display the terminal’s type. Read only.

Terminal Model

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

Enable Authentication Device

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

Authentication

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

Authentication Interval

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

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

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

Communication with Controller Every

If the card reader cannot communicate with the controller within the configured time duration, the card reader will be regarded as offline.

Set Door Parameters

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

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

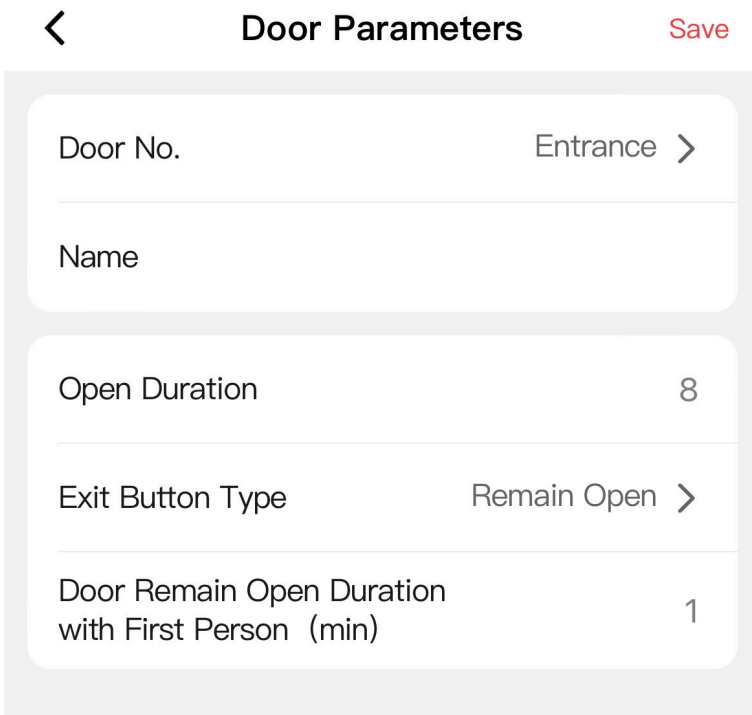


Figure 9-10 Door Parameters

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

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

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

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.

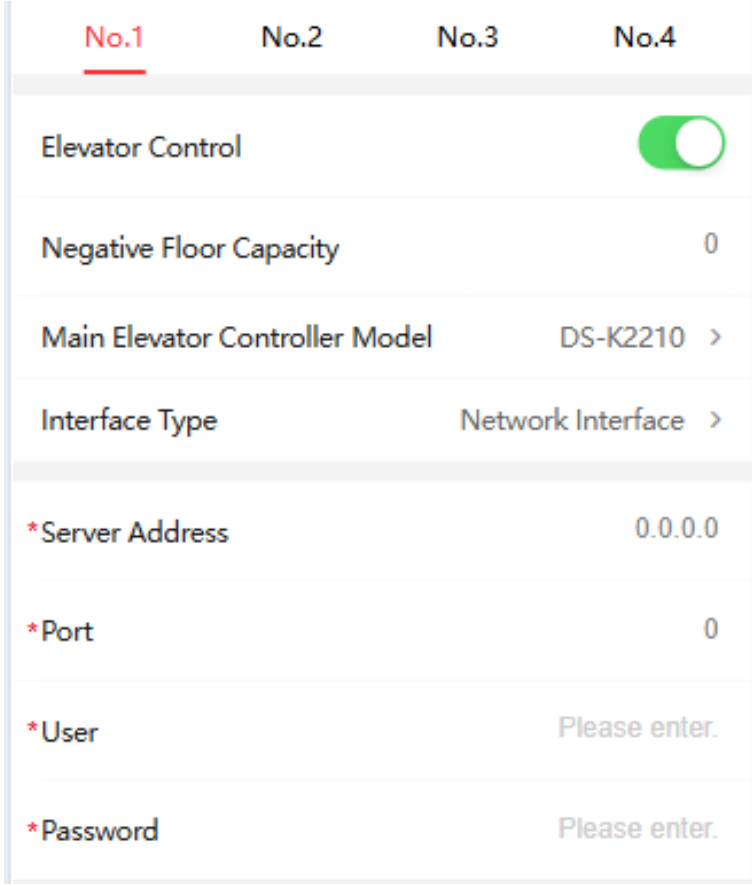


Figure 9-11 Elevator Control Parameters

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

p

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

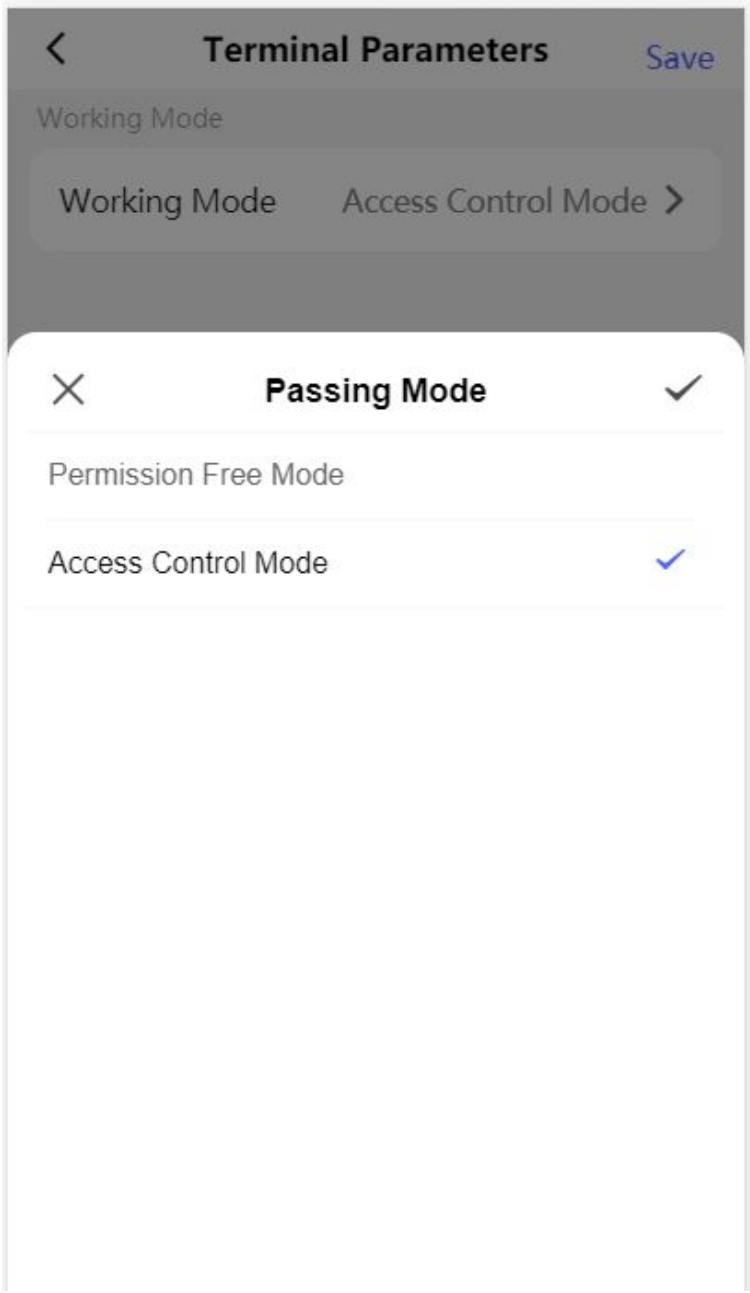


Figure 9-12 Terminal Parameters

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.

Serial Port Settings

Set serial port parameters.

Steps

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

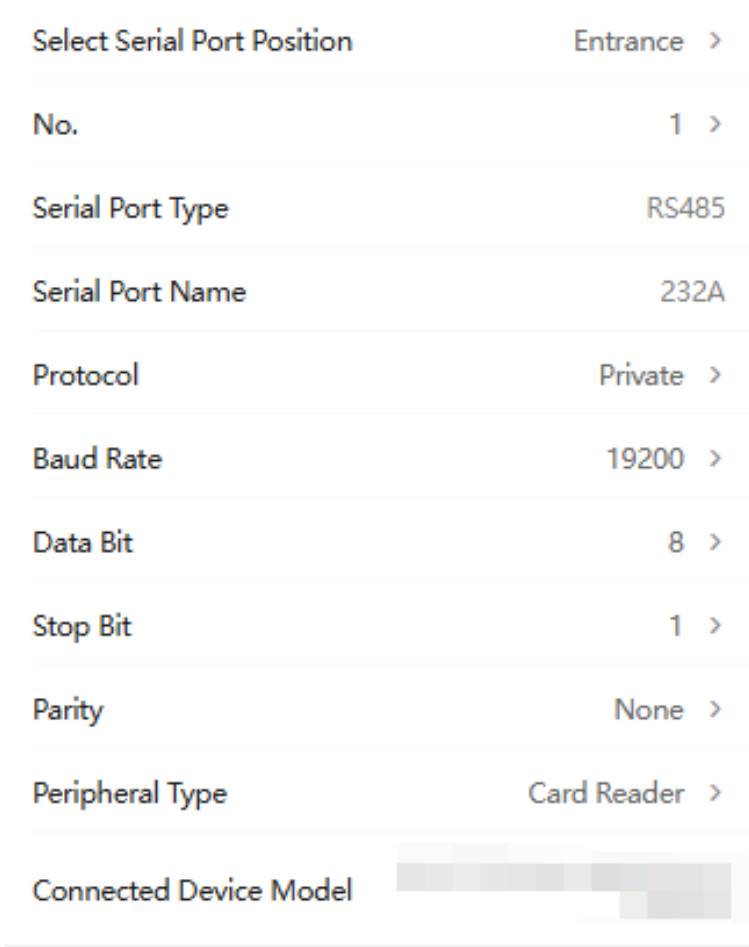


Figure 9-13 Serial Port Configuration

2. Set the serial port position as **Entrance** or **Exit**.
3. Select a serial port No., and the corresponding serial port type will display automatically.
4. Select a protocol.
   - Select the protocol as **Private**, set following 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.

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

- Set the protocol as **OSDP**, the serial port parameters will set automatically.

5. Click **Save**.

Set Card Security

Configure cards for the device.

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

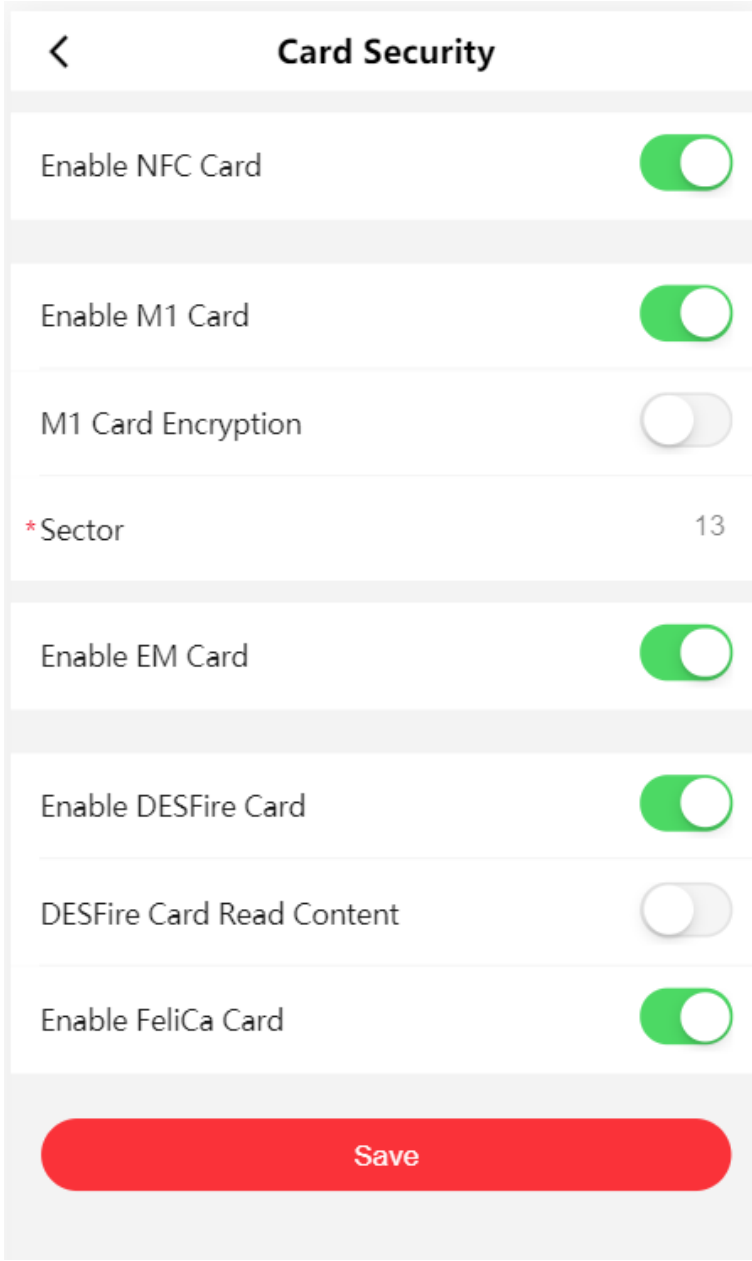


Figure 9-14 Card Security

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.

9.3.13 Turnstile Settings

dToF Sensor Settings

Set the dToF Sensor parameters.

Steps

1. Tap → **dToF Sensor Settings** to enter the configuration page.
2. Set **Inductive Mode (Entrance)** and **Inductive Mode (Exit)**.
3. You can customize dToF Sensor.

   Exceptional dToF Auto Shield

   If the dToF Sensor is damaged, the dToF Sensor can be shielded to temporarily restore the lane to use, but it may cause injury to passers-by when the barrier is open and closed.

Note

Exceptional dToF auto shield function is a short-term shield. If there is no exception for 1 hour, it will restore.

dToF Emergency Mode

If some dToF beams do not work properly, you can shield those dToF beams to restore the lane. But this action may hit person and cause injury.

Enable Custom Anti-pinch for Door Closing

Anti-pinch for door closing is used when the device detects that there are still people staying in the lane when the barrier closes, the barrier will not close. The barrier will close only when the person has completely exited the lane. When you enable the function, you can shield some dToF Sensors, so that the barrier can be closed in advance after people pass, but it may injure passers-by when the barrier is open and closed.

It is recommended to enable the function.

4. 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.

   Authentication Number

   The number of passing people verified through card swiping, etc.
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**.

Light Settings

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

Side Light

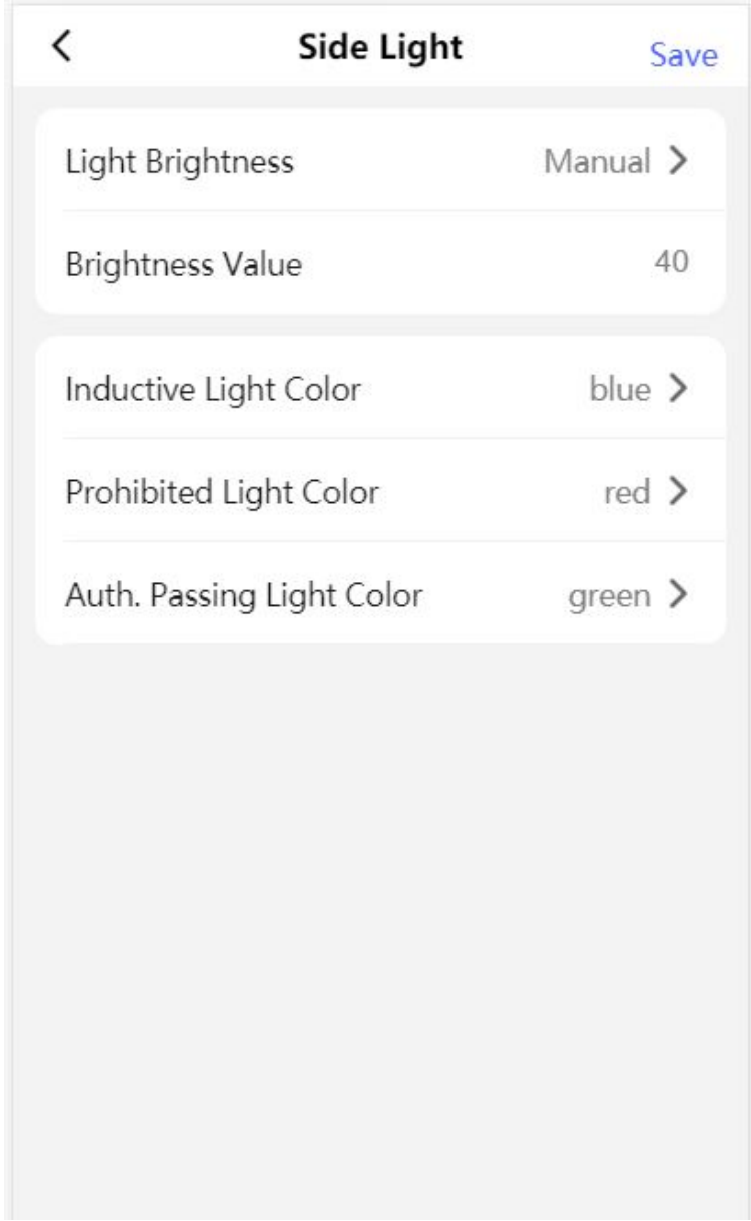


Figure 9-15 Side Light Settings

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

Barrier Light

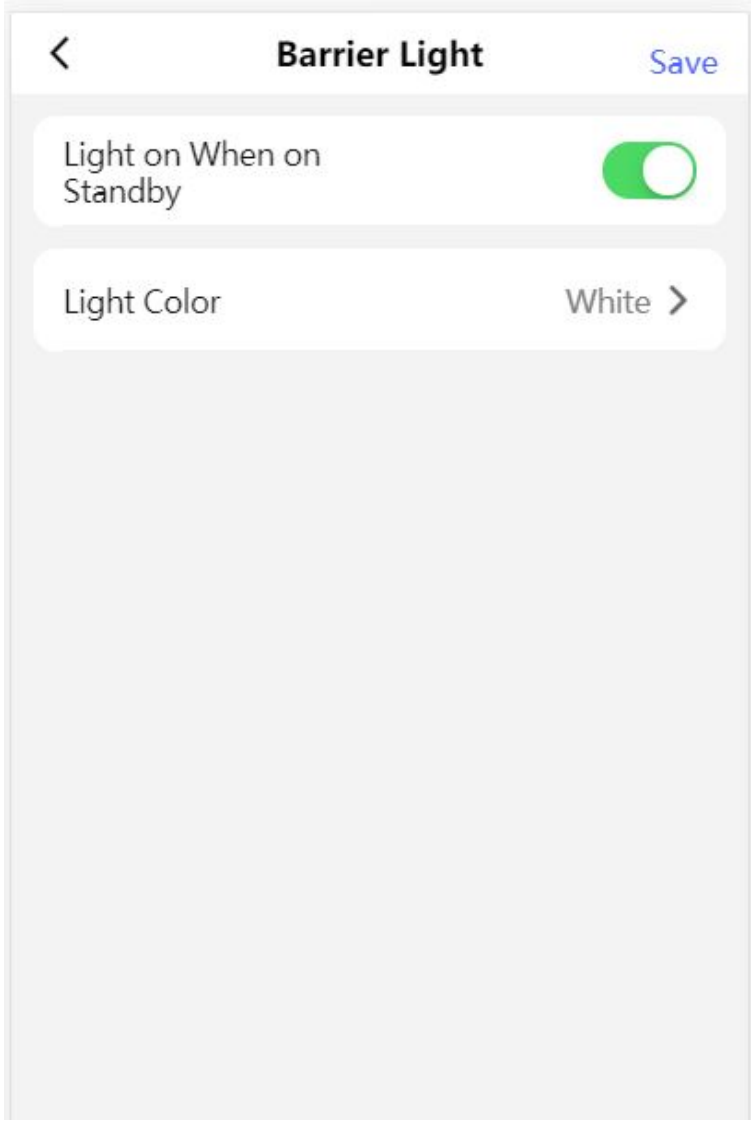


Figure 9-16 Barrier Light Settings

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

Welcome Light

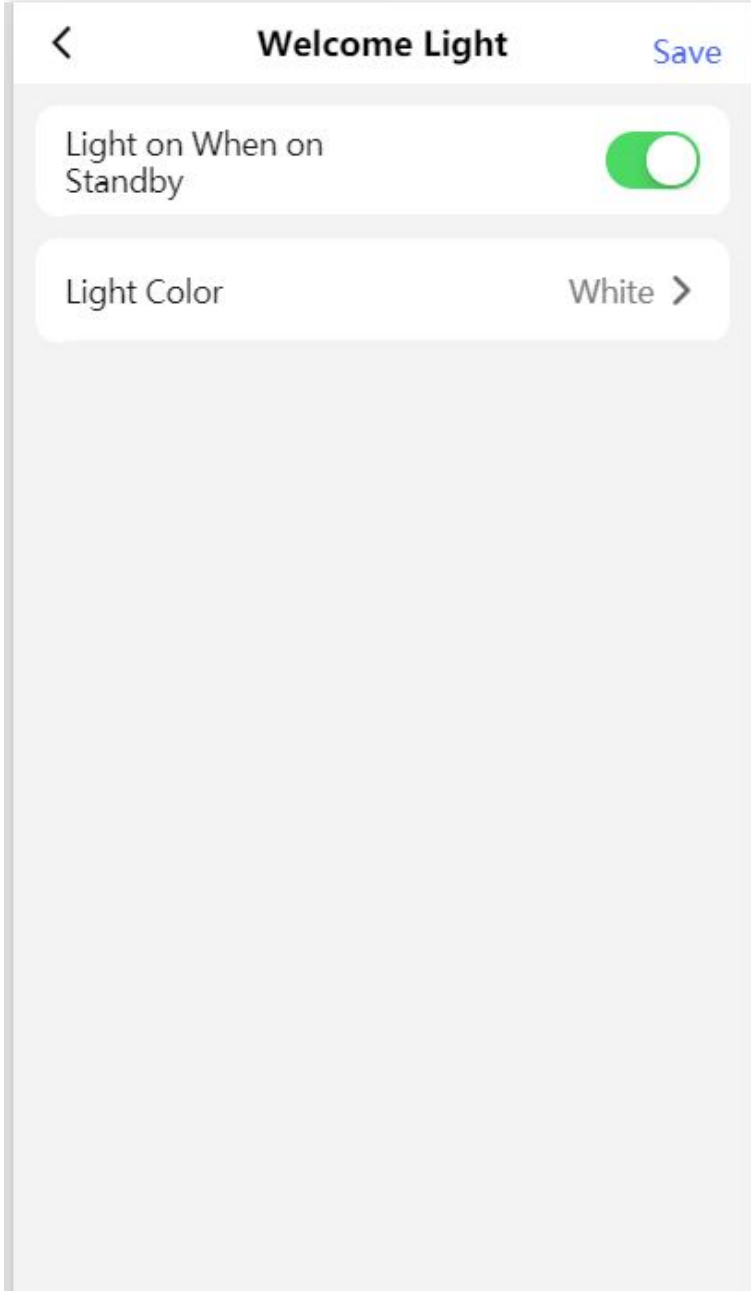


Figure 9-17 Welcome Light Settings

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

Other Configurations

Tap → **Other Settings** .

Set the basic parameters.

Alarm Output Duration

Set duration as 0 means remaining output.

Temperature Unit

Select 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.

Lightboard Brightness

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

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 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 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

You can Slide **Enable** 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

You can set the signal as **Remain Closed** or **Remain Open**. In the remain open state, closing triggers fire protection. In the remain closed state, disconnection triggers fire protection.

Invert Entrance and Exit Direction

If enable the function, the entrance and exit direction will be inverted.

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.

Tap **Save**to enable the settings.

9.3.14 Upgrade and Maintenance

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

Restart Device

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

Upgrade

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

Note

Do not power off during the upgrading.

Restore Parameters

Tap → **Default** .

Restore to Default Settings

The device will restore to the default settings, except for the device IP address and the user information.

Restore to Factory Settings

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.

9.3.15 Device Debugging

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

Tap → **Device Debugging** .

Lane Studying/Motor Self-Test

Lane Studying

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

Motor Self-Test

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

Encoder Self-Test

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

dToF Self-Test

Select a channel (lane) and tap **dToF Self-Test**, the device will test all dToF sensors. 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 dToF sensors reports.

9.3.16 View User Document

View the user document.

Note

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

Tap ≡ to enter the page.

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

9.3.17 Open Source Software Licenses

You can view the open source software licenses.

Tap ≡ to enter the page.

Tap **Open Source Software Licenses**.

9.3.18 Log Out

Log out the configuration page.

Tap ≡ → **Logout** , tap **OK**.

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

Chapter 10 Operation via Web Browser

10.1 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 and card.

Network Status

You can view the network connection status.

Basic Information

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

Device Capacity

You can view the person, card, event capacity.

10.2 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.

10.3 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.

10.4 Help

10.4.1 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.

10.4.2 View Online Help Document

You can view the help document for Web configuration.

Click → **Online Document** on the upper right of the Web page to view the document.

10.4.3 Logout

Log out the account.

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

10.5 Quick Operation via Web Browser

10.5.1 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.

10.6 Person Management

You can add the person's information, including the basic information, credentials, authentication and settings.

Add Basic Information

Click **Person → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, and person type.
If you select **Visitor** as the person type, you can set the visit times.
Click **Save** to save the settings.

Set Permission Time

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

Add Card

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

Import/Export Person Data

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

Export Person Data

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

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

Note

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

Importing Person Data

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

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

10.7 Import Blocklist

Import blocklist for user management.

Steps

1. Click **Person Management → Import Blocklist** .
2. Click **Download Template**. The blocklist template will be downloaded on your PC.
3. Fill in the blocklist user information following the template.
4. Click and choose the blocklist file.
5. Click **OK** to upload the file.
   - Click **Clear Blocklist** to delete all the blocklist user information.

10.8 Device Management

10.8.1 Sub Access Control Board Management

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

Steps

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

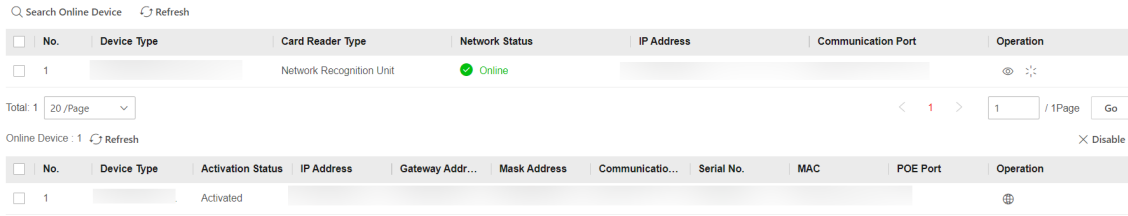


Figure 10-1 Device Management

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**.

10.8.2 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 → Batch Manage Devices** to enter page.

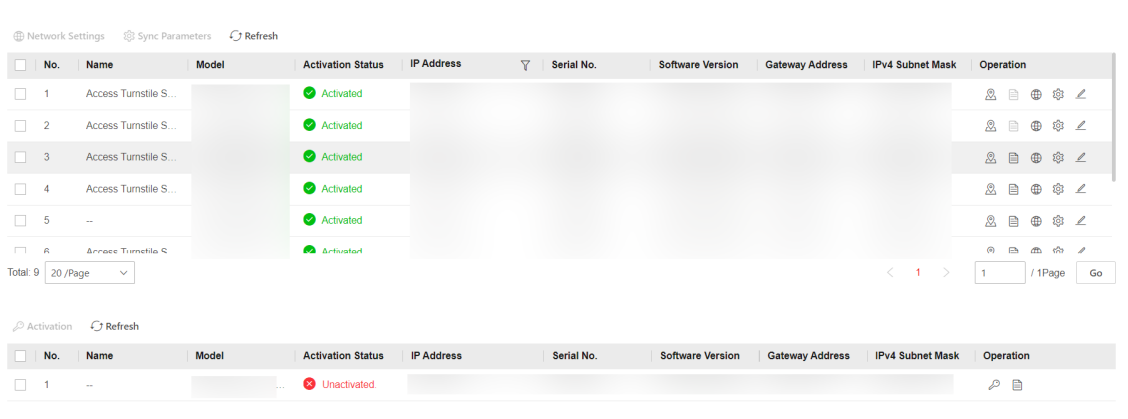


Figure 10-2 Batch Manage Devices Page

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**.

10.9 Turnstile

10.9.1 Search Event

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

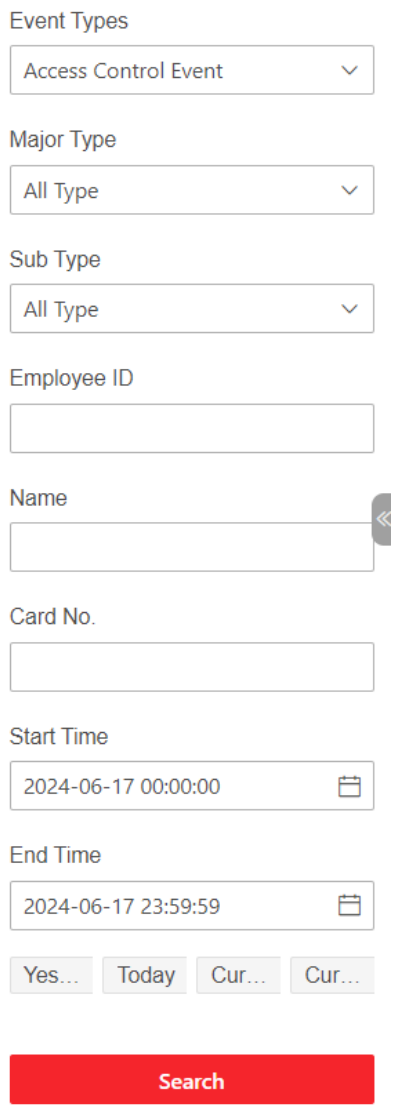


Figure 10-3 Search Event

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.

10.9.2 Paramenter Settings

Set Door Parameters

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

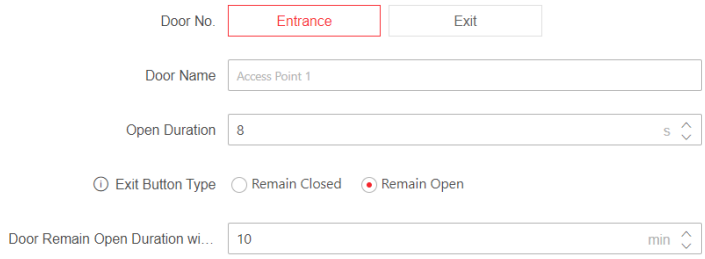


Figure 10-4 Door Parameters Settings

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 5 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.

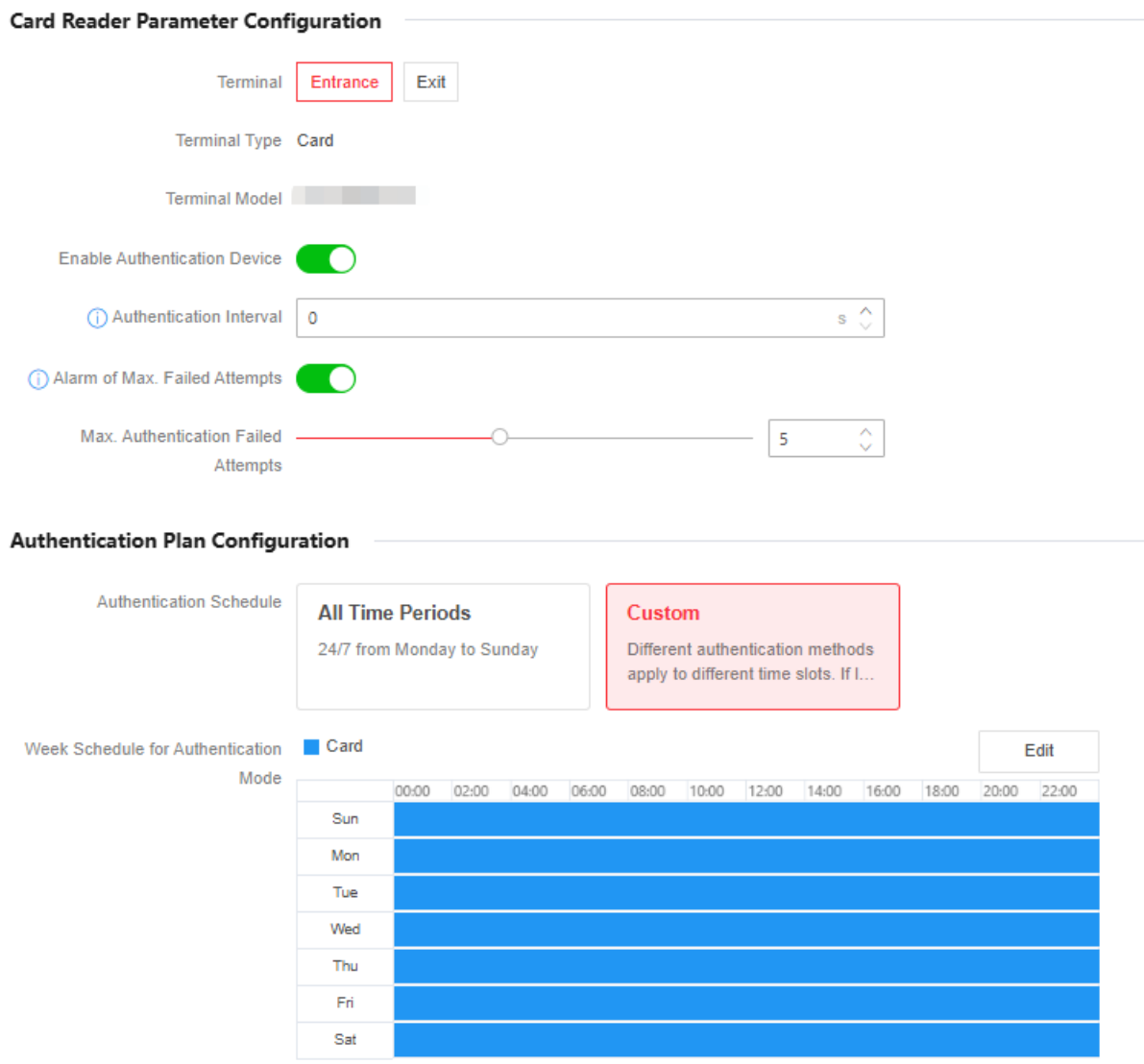


Figure 10-5 Authentication Settings

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

Terminal/Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication Interval

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

Alarm of Max. Failed Attempts

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

Max. Authentication Failed Attempts

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

Authentication Plan Configuration

You can choose one authentication mode, and select the area on the timetable to set the period, in which it only can be authenticated by the set mode.

Click **Clear** to clear the selected area on the timetable.

Click **Weekly Schedule** to fill the whole timetable. Click **Clear All** to clear all set periods.

Note

The selected authentication mode should be supported by card reader.

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

Set the working mode and remote verification.

Steps

1. Click **Turnstile → Access Control Parameters → Terminal Parameters** to enter the page.

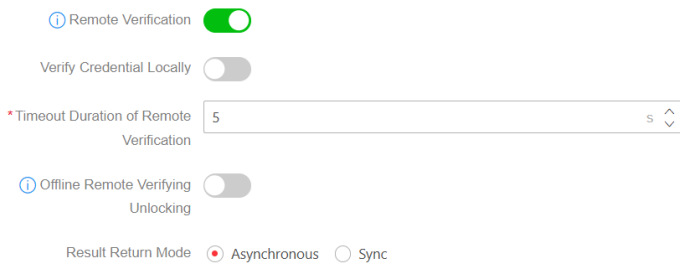


Figure 10-6 Terminal Parameters

2. Set remote verification.

Verify Credential Locally

The device will upload the person's authentication information to the platform. The platform will judge to open the barrier or not.

Verify Credential Locally

After enabling the function, the device will only verify the person's permission without the schedule template, etc.

Timeout Duration of Remote Verification

Enter the timeout for remote verification in seconds. The timeout is used to define the waiting duration for remote verification requests.

Offline Remote Verifying Unlocking

After enabling the function, you need to perform local authentication when the platform is offline or times out.

Result Return Mode

The default mode is **Asynchronous**.

Asynchronous

When this mode is selected, results will be returned asynchronously.

Sync

When this mode is selected, results will be returned synchronously.

3. Click **Save** to complete terminal parameter settings.

Set Privacy Parameters

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

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

Event Storage Settings

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

Overwriting

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

Authentication Settings

Display Authentication Result

You can check **Name**, and **Employee ID**, to display the authentication result.

Name De-identification

You can enable **Name De-identification**, and the whole name will not be displayed.

ID De-identification

You can enable **ID De-identification**, and the whole employee ID will not be displayed.

10.9.3 Turnstile Configuration

Basic Parameters

Set turnstile basic parameters.

Steps

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

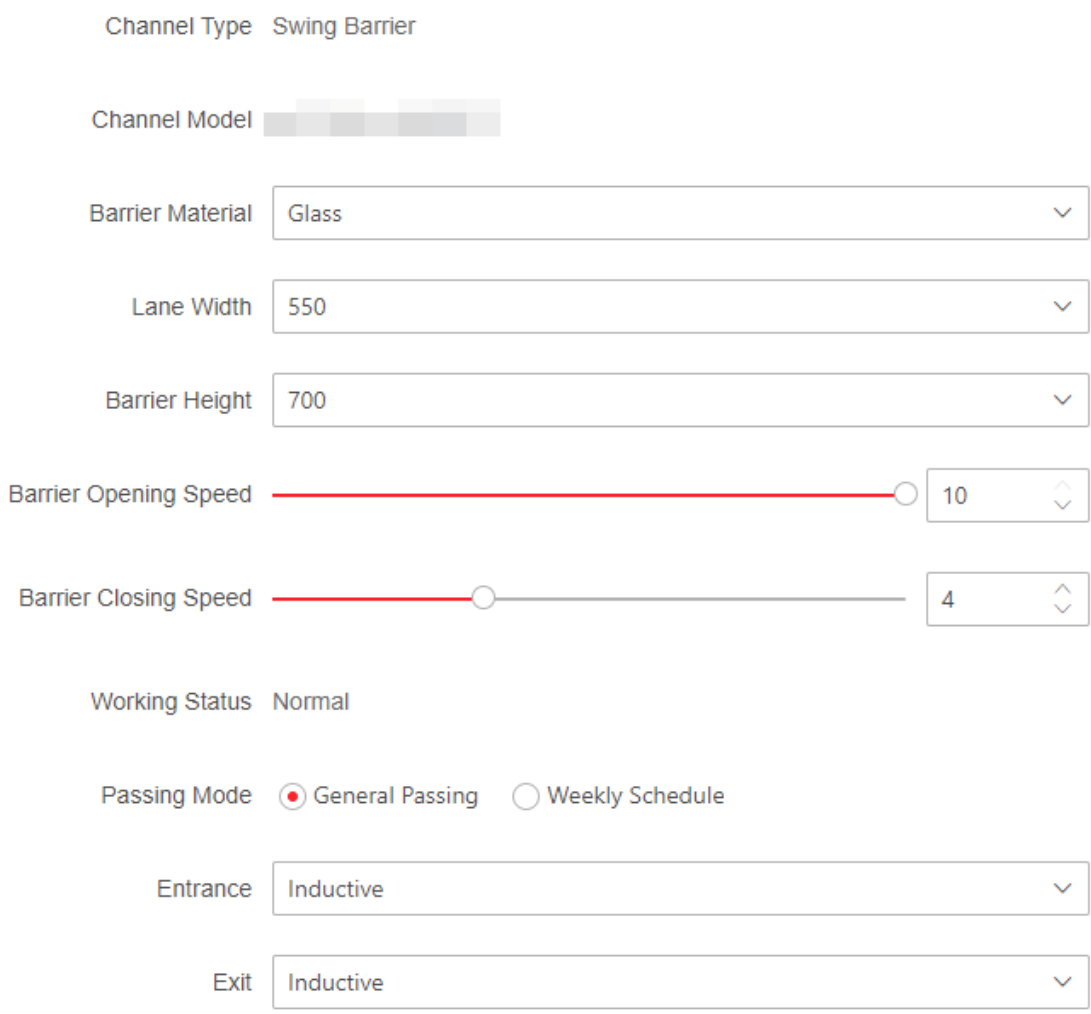


Figure 10-7 Basic Parameters

2. View the **Channel Type**, **Channel Model** and **Working Status**.
3. Set **Barrier Material**, **Lane Width**, **Barrier Height**, **Barrier Opening Speed** and **Barrier Closing Speed** according to your actual needs.
4. Set the passing mode.
   - If you choose **General Passing**, you can select the barrier status for the entrance and exit from the drop-down list.
   - If you choose **Weekly Schedule**, you can set a weekly schedule for entrance and exit barriers.
5. Set **Entrance** and **Exit** status.

   Controlled

   The barrier is controlled, the person should authenticate the credential to pass.

   Inductive

   When a person is walking through the lane, the barrier will be detected and open the barrier.

Remain Open/Closed

The barrier will remain open or closed whenever the person's authentication result is passed or denied.

Barrier-Free

The barrier will open all the time.

6. Click **Save**.

Keyfob Settings

Set keyfob parameters.

Steps

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

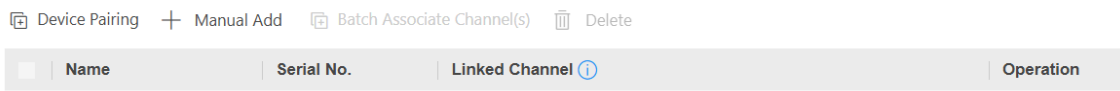


Figure 10-8 Keyfob Settings

- Click **Manual Add** and the keyfob adding window will pop up. Enter the keyfob's **Name** and **Serial No.**. Click **Save** to add the keyfob.
- Click **Device Pairing** ; stand close to the current device, then press and hold the button on the bottom left of the keyfob to add. Upon successful pairing, the keyfob's serial number is automatically added to the device.

Click **Batch Associate Channel(s)** to link multiple keyfobs to one or more channels simultaneously.

Select a keyfob and click or to edit or delete the keyfob.

2. Click **Save**.

dToF Sensor

Set dToF Sensor.

Steps

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

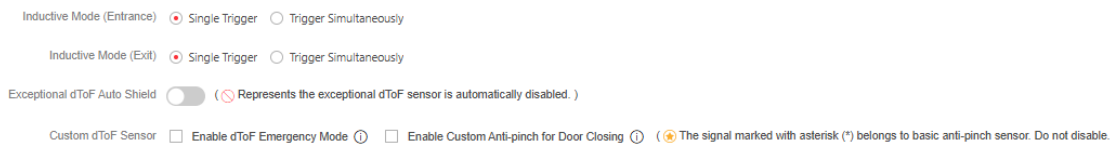


Figure 10-9 dToF Sensor

2. Set the entrance and exit inductive mode as **Single Triggered** or **Triggered Simultaneously**.
3. Enable **Exceptional dToF Auto Shield**. If the dToF Sensor is damaged, the dToF Sensor can be shielded to temporarily restore the lane to use, but it may cause injury to passers-by when the barrier is open and closed.

Note

Exceptional dToF auto shield function is a short-term shield. If there is no exception for 1 hour, it will restore.

4. Set custom dToF Sensor mode.

   Enable dToF Emergency Mode

   If some dToF beams do not work properly, you can shield those dToF beams to restore the lane. But this action may hit person and cause injury.

   Enable Custom Anti-pinch for Door Closing

   Anti-pinch for door closing refers that the barrier will not close if the device has detected person in the lane. Only after the person walks out of the lane, the barrier will close. If you enable the function, you can shield parts of the dToF beams for closing barrier in advance. But this action may hit person and cause injury.
5. Click **Save**.

People Counting

Set people counting.

Steps

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

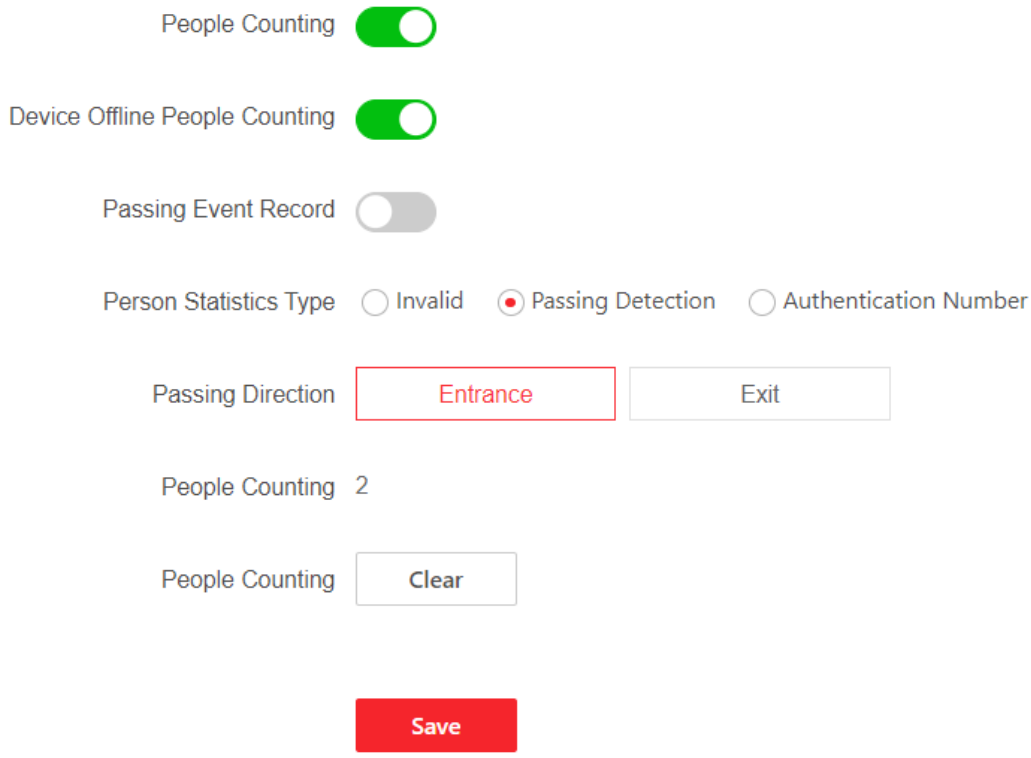


Figure 10-10 People Counting

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

People Counting

Enable the function and set the parameters.

Device Offline People Counting

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

Passing Event Record

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

People Statistics Type

Invalid

Disable people counting.

Passing Detection

The number of all passing people.

Authentication Number

The number of passing people verified through card swiping, etc.

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.

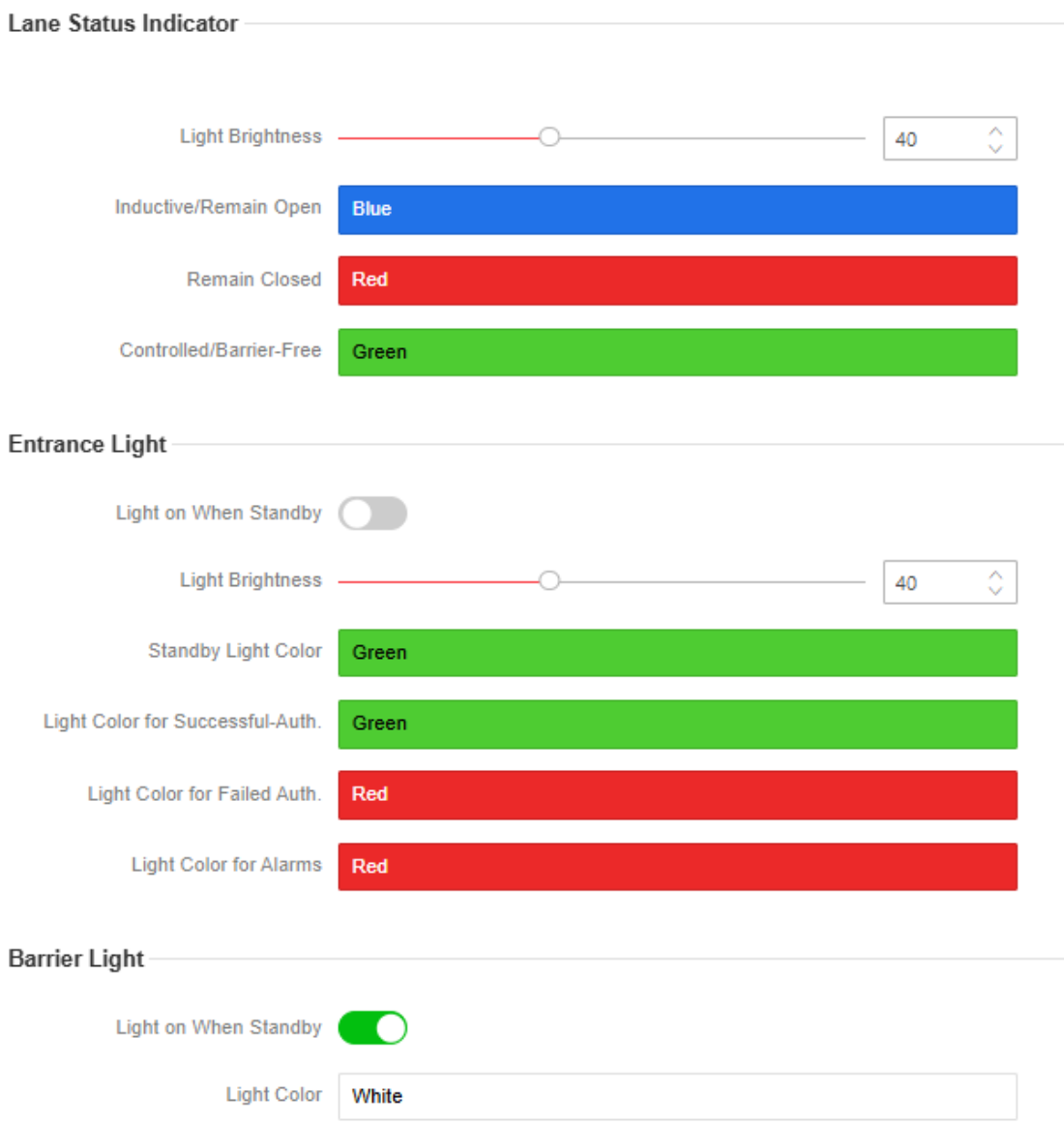


Figure 10-11 Light Settings

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

Lane Status Indicator

Set the lane status indicator's brightness and color.

Light Brightness

Drag the block or enter the value to adjust the light brightness manually.

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.

Entrance Light

Set the entrance light's brightness and color.

Light on When Standby

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

Light Brightness

Drag the block or enter the value to adjust the light brightness manually.

Standby Light Color

Set the light color when the device is in the standby status.

Light Color for Successful-Auth.

Set the light color when the person is authentication completed.

Light Color for Failed Auth.

Set the light color when the person is authentication failed.

Light Color for Alarms

Set the light color when the device is in alarm.

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.

3. Click **Save**.

Other Settings

Set other parameters.

Steps

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

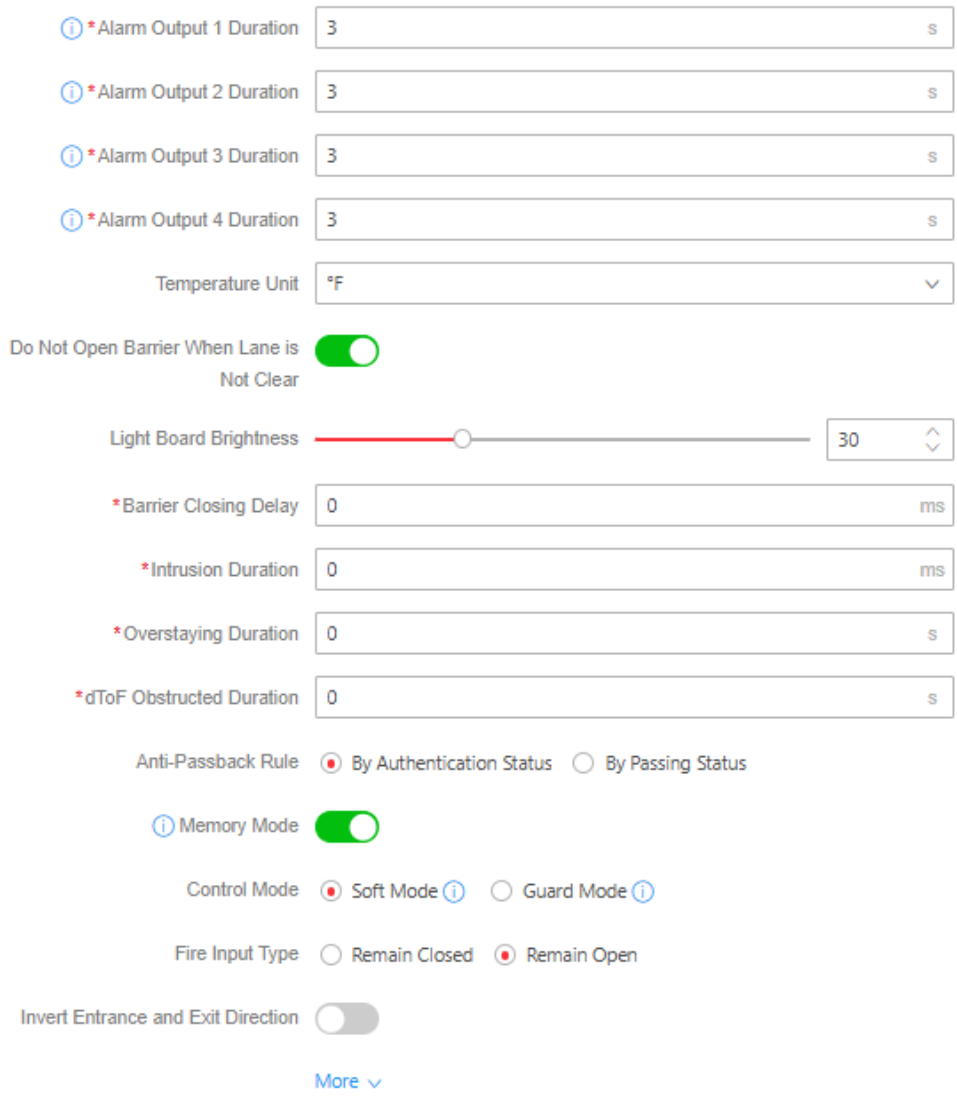


Figure 10-12 Other Settings Page

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.

Light Board Brightness

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

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 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 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

If enable the function, the entrance and exit direction will be inverted.

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

10.10 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.

10.10.1 View Device Information

View the device name, language, model, serial No., version, 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, local RS-485, alarm input and alarm output number.

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

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

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

10.10.2 Set Time

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

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

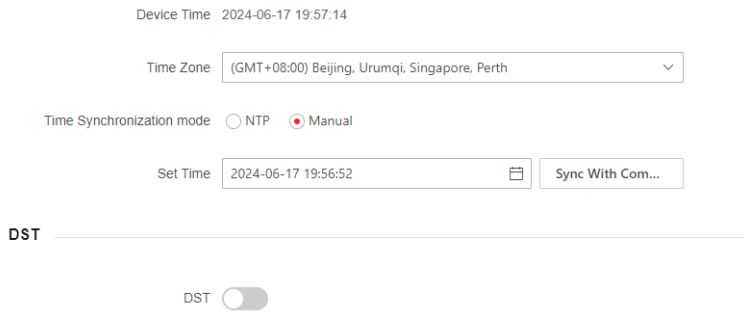


Figure 10-13 Time Settings

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.

10.10.3 Change Administrator's Password

Steps

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

Caution

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

10.10.4 Online Users

The information of users logging into the device is shown.

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

10.10.5 View Device Arming/Disarming Information via PC Web

View device arming type and arming IP address.

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

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

10.10.6 Set Working Mode via PC Web

You can set the terminal parameters of the device.

Note

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

Click **Access Control → Parameter Settings → Terminal Parameters** to enter the settings page.

Working Mode

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

Access Control Mode

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

10.10.7 Network Settings

Set Basic Network Parameters

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

You can view the mac address and MTU.

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

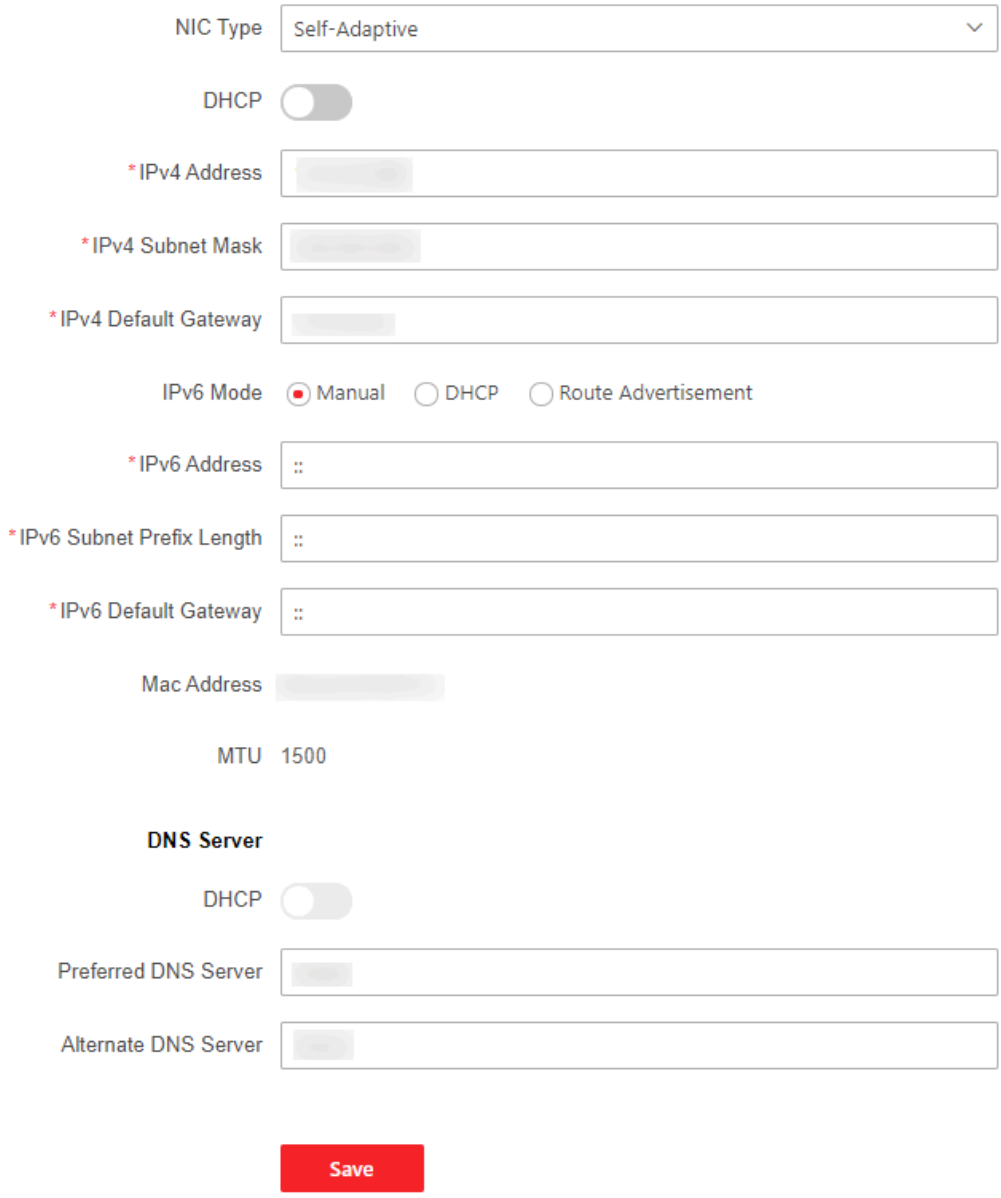


Figure 10-14 Set TCP/IP

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 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** .

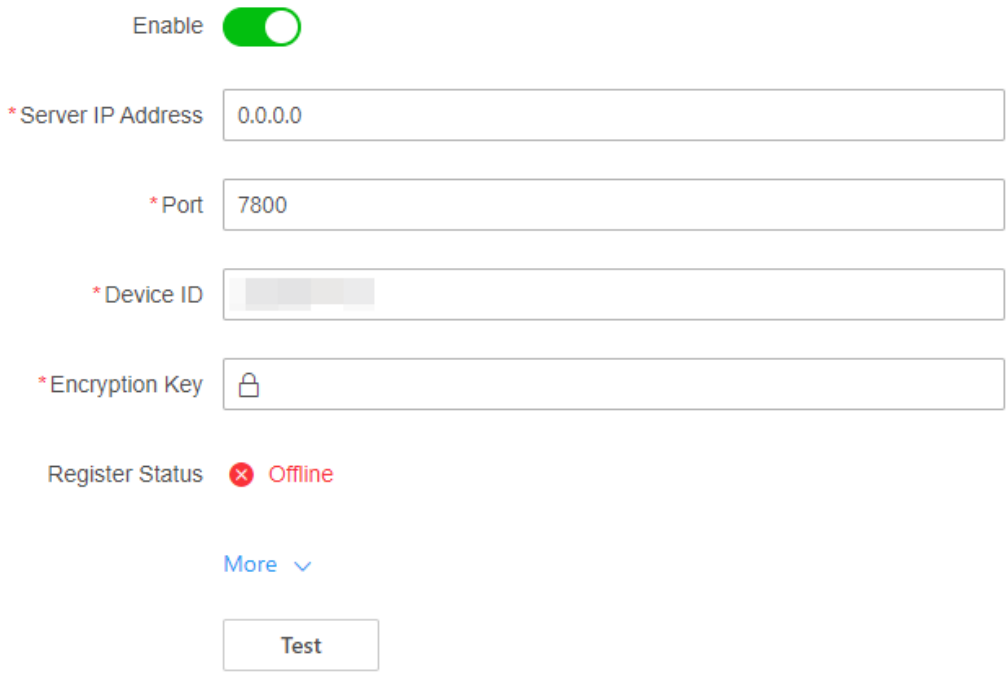


Figure 10-15 Set OTAP

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.

10.10.8 Set Wiegand Parameters via PC Web

You can set the Wiegand transmission direction.

Steps

Note

- Some device models do not support this function. Refer to the actual products when configuration.
- Only the device supporting interface board can set the Wiegand parameters.

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

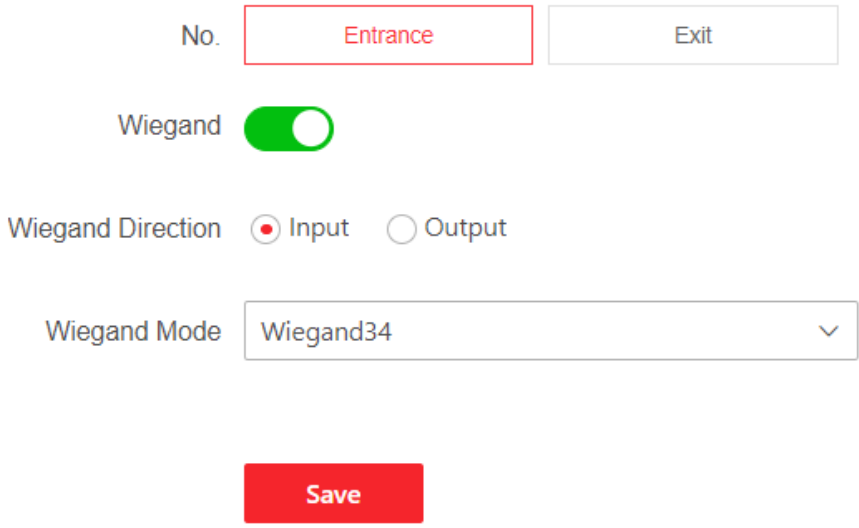


Figure 10-16 Wiegand Page

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.

10.10.9 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.
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**.

10.10.10 Elevator Control via PC Web

Steps

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

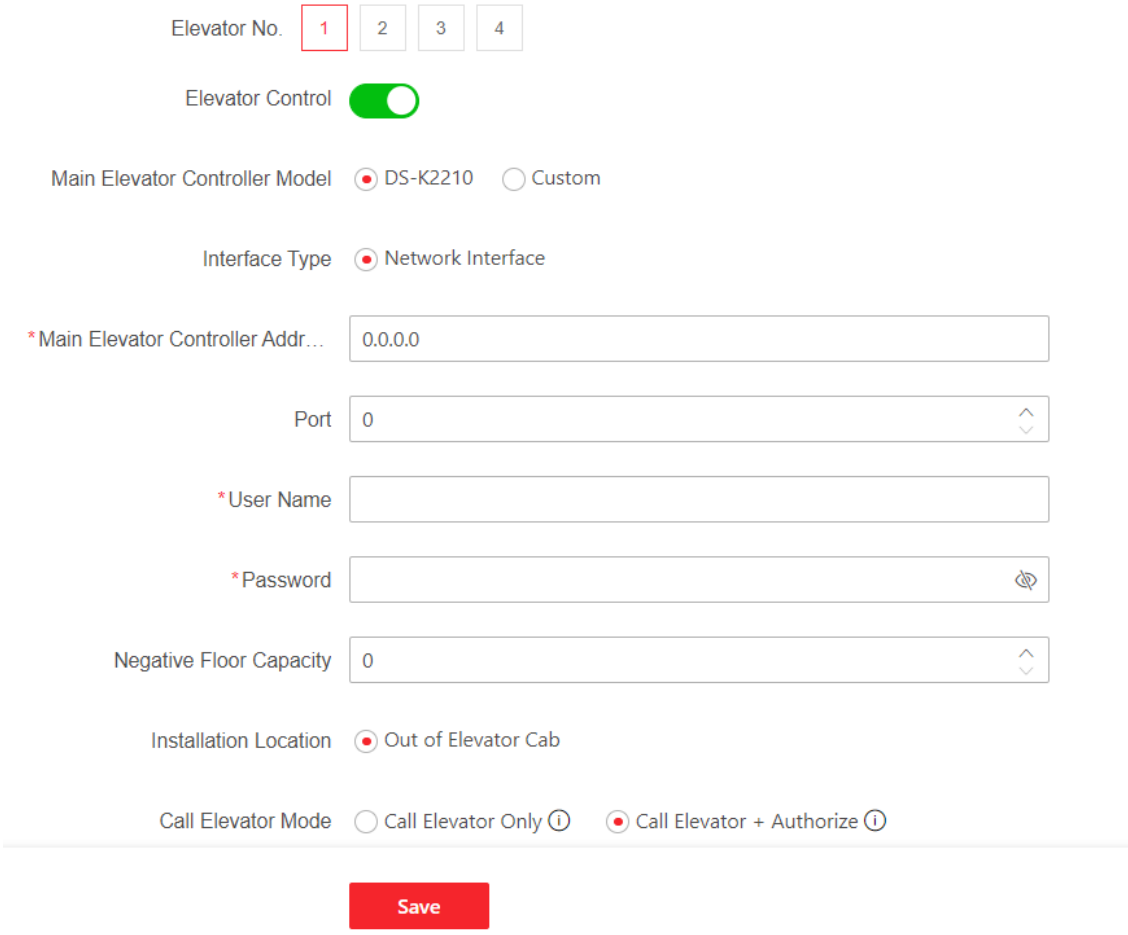


Figure 10-17 Elevator Control

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.

10.10.11 Set Video and Audio Parameters via PC Web

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.

Drag the block or enter the value to set **Output Volume**.

Click **Save**.

10.10.12 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.

10.10.13 Event Linkage

Set linked actions for events.

Steps

1. Click **System and Maintenance → System Configuration → Event → Event Configurations** to enter the settings page.

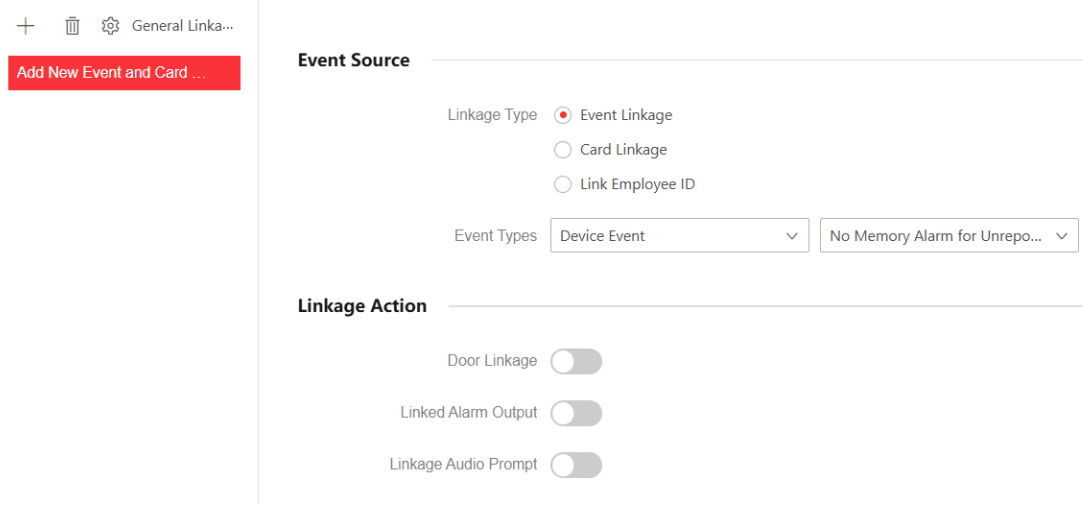


Figure 10-18 Event Linkage

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

   Door Linkage

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

   Linked Alarm Output

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

   Linked Audio Prompt

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

10.10.14 Preference Settings

Set Sleep Time via PC Web

The device will in sleep mode after the configured time duration. The function can reduce power consumption.

Go to **System and Maintenance → Preference → Screen Display** .

Select **Entrance** or **Exit**. The screen will execute the configured settings.

Slide **Enable Screen-off** . Drag the block or enter the value to set **Screen-off Time**.

Set Display Theme

You can set the display theme and the sleep time for the device.

Set Theme

Click **System and Maintenance → Preference → Screen Display** .
Set the theme mode.

Simple

After selecting this mode, the authentication page will not display the live view image. The person's name and employee ID will all be hidden after authentication.

Notice Publication

You can set the notice publication for the device.

Click **System and Maintenance → Preference → Notice Publication** .

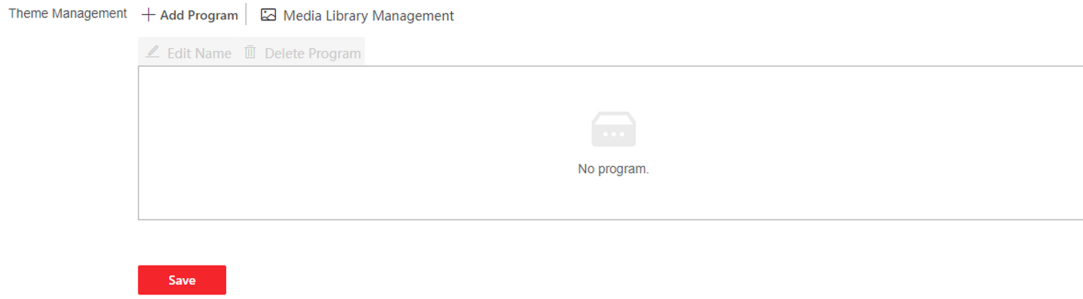


Figure 10-19 Notice

Theme Management

Click **Media Library Management → +** to upload the picture from the local PC.

Note

Only the format of JPG and JPEG is supported. Each picture should be smaller than 1 MB with resolution up to 1920*1280.

Add Program

Click **+ Add Program**. You can set the program name and select program type.

Picture

If you select picture, you can click **+** to add picture.

Welcome Message

If you select welcome message, you can set the template, content, font size and color of main and sub title. You can also custom the background picture.

Slide Show Interval

Drag the block or enter the number to set the slide show interval. The picture and video will be changed according to the interval.

Schedule Management

After you have created a theme, click **+ Add** on the schedule management panel. Select the drawn schedule, and you can edit the exact start and end time.

Select the drawn schedule and you can click **Clear** or **Clear All** to delete the schedule.

Click **Releasing Record** to view task name, releasing status, etc.

Click **View Terminal Schedule Info.** to view terminal name, schedule name, etc.

Prompt Schedule

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration → Preference → Prompt Schedule** .

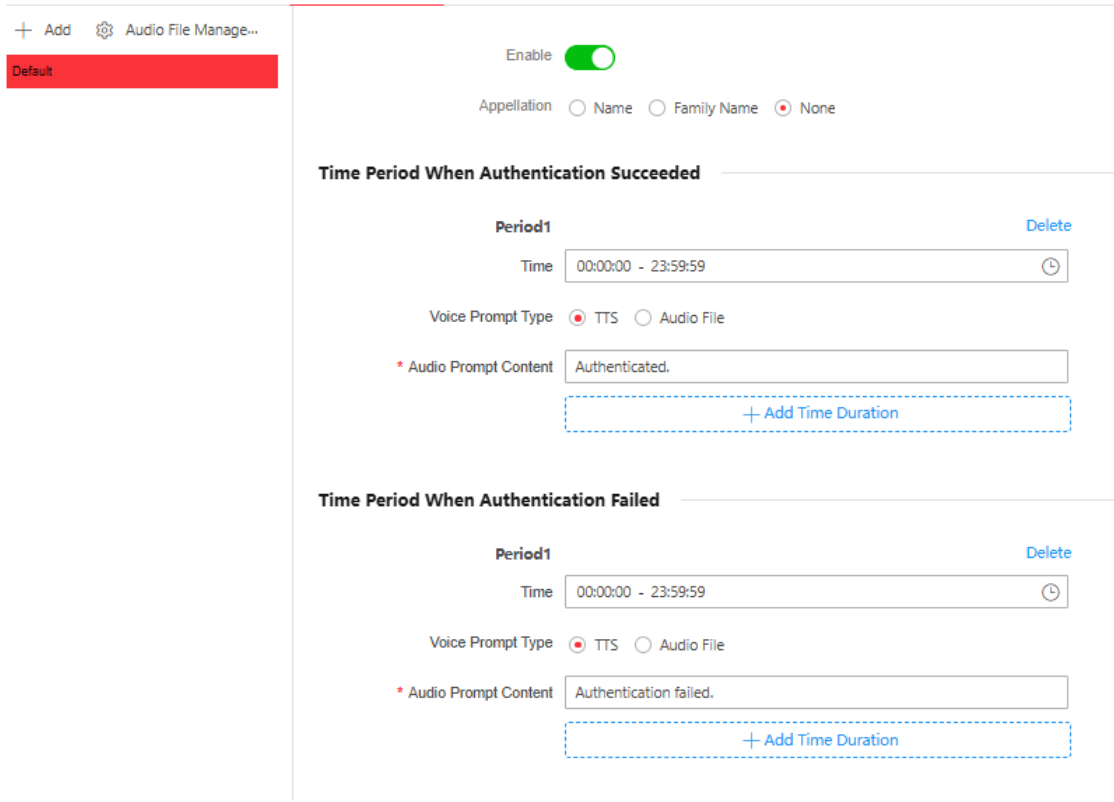


Figure 10-20 Customize Audio Content

2. Select time schedule.
3. Enable the function.
4. Set the appellation.
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.

10.10.15 Upgrade and Maintenance

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

Reboot Device

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

Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .

Local Upgrade

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

Online Upgrade

Check for upgrades.

Note

Do not power off during the upgrading.

Restore Parameters

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

Restore All

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

Restore

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

Import and Export Parameters

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

Export

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

Note

You can import the exported device parameters to another device.

Import

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

10.10.16 Device Debugging

You can set device debugging parameters.

Steps

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

Lane Studying/Motor Self-Test

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 Sensors reports.

10.10.17 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**.

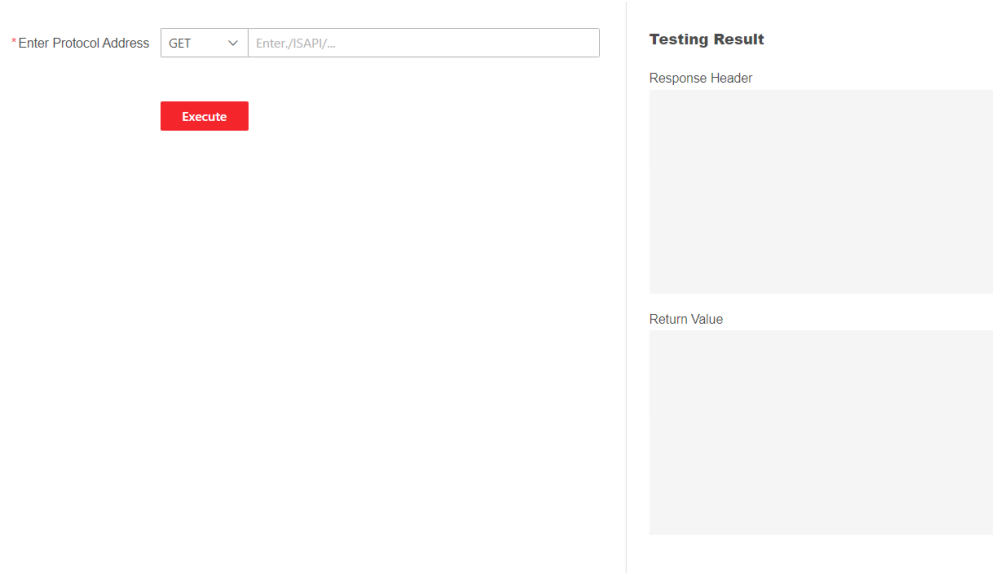


Figure 10-21 Protocol Testing

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

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

10.10.18 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.

10.10.19 Component Status

You can view the status of different components.

Main Lane Status

Device Component

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

Peripheral

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

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Sub 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.

10.10.20 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.

10.10.21 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 11 Other Platforms to Configure

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

iVMS-4200 Client Software

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

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

Appendix A. 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. Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

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

Data Protection

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

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

See Far, Go Further

UD42758B-A