HIKVISION

DS-K3G301(L)X Series Tripod Turnstile

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.
- Keep body parts away from fan blades. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.
- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.

  If the top caps should be open and the device should be powered on for maintenance, make sure:

  1. Power off the fan to prevent the operator from getting injured accidentally.
  2. Do not touch bare high-voltage components.
  3. Make sure the switch's wiring sequence is correct after maintenance.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- Operation of this equipment in a residential environment could cause radio interference.
- The device do not support the PoE network switch. Connecting with the PoE network switch may damage the control board.

⚠ Cautions:

- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- Ensure correct wiring of the terminals for connection to an AC mains supply.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- This equipment is suitable for mounting on concrete or other non-combustible surface only.
- Install the equipment according to the instructions in this manual.
- To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- The main element of the turnstile is stainless steel, which is rustless (antioxidant) and corrosion resistant (The anti corrosion ability in the medium of acid, alkali, and salt). In order to keep the stainless steel from being oxidized or corroded, you should clean and care the turnstile surface periodically.
  The instructions and tips for maintaining the turnstile are as follows:
  - Select different stainless steel types according to the variety of the environments. You can select 304 stainless steel for common circumstances and 316 stainless steel for the scenarios of seasides and chemical plants.
  - Keep the device surface clean and dry.
  - Use non-woven cloth and ethyl alcohol to clean the dirt on the device surface.
  - Use sourcing pad (do not use mesh cleaning ball) to clean the rust on the device surface by following the wire drawing on the stainless steel. And then use non-woven cloth and stainless steel cleaner to wipe the device surface.
  - Clean and maintain the device by using non-woven cloth and stainless steel cleaner periodically. It is suggest to clean the device every month in common circumstances and every week for severe environments (seaside and chemical plants for instance.

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

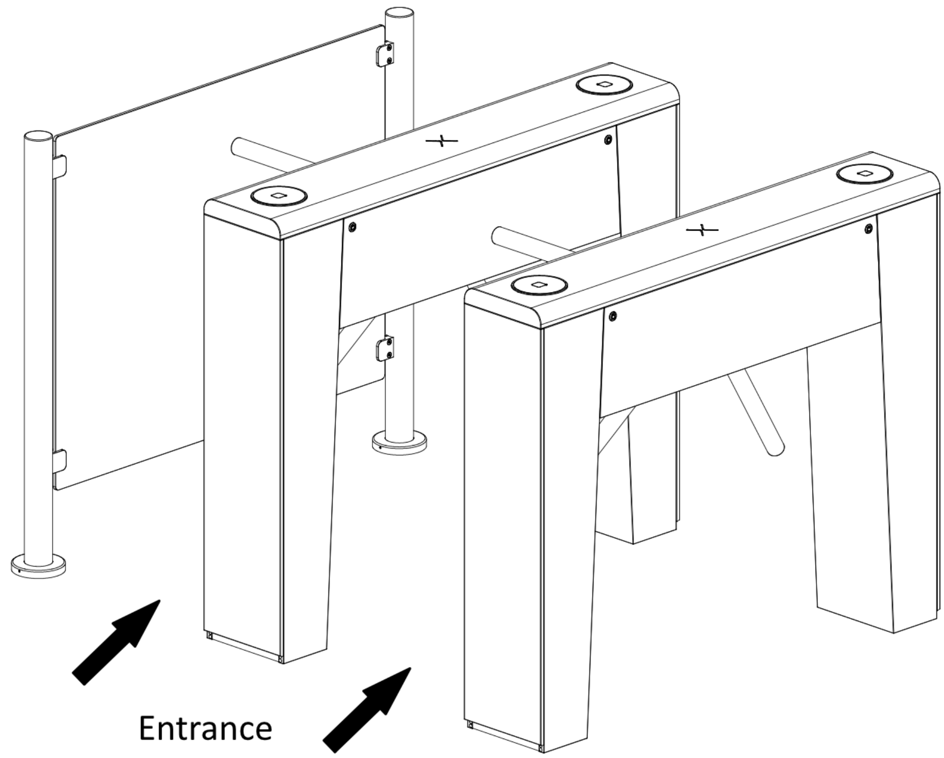
Contents

Chapter 1 Wiring

Scan the QR code to view the wiring guide video.

Chapter 2 Overview

2.1 Introduction



By adopting the turnstile integratedly with the access control system, person should authenticate to pass through the lane via presenting cards, face, or QR code, etc. It is widely used in attractions, office, construction sites, residences and other indoor scenes.

2.2 Main Features

- Bidirectional (Entering/Exiting) lane.
- Support remote control and management by HCP software.
- High-brightness LED indicates the entrance/exit and passing status except "Pg" type.
- Fire alarm passing: When triggered, the arms will be dropped automatically for emergency evacuation.
- Support PC web browser, easy to do the configuration.
- Support ISAPI protocol for 3rd party integration development.

Chapter 3 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 783 mm.
- If the installation area is close to the wall, make sure the distance between the pedestal and the wall should be more than 40 mm.

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

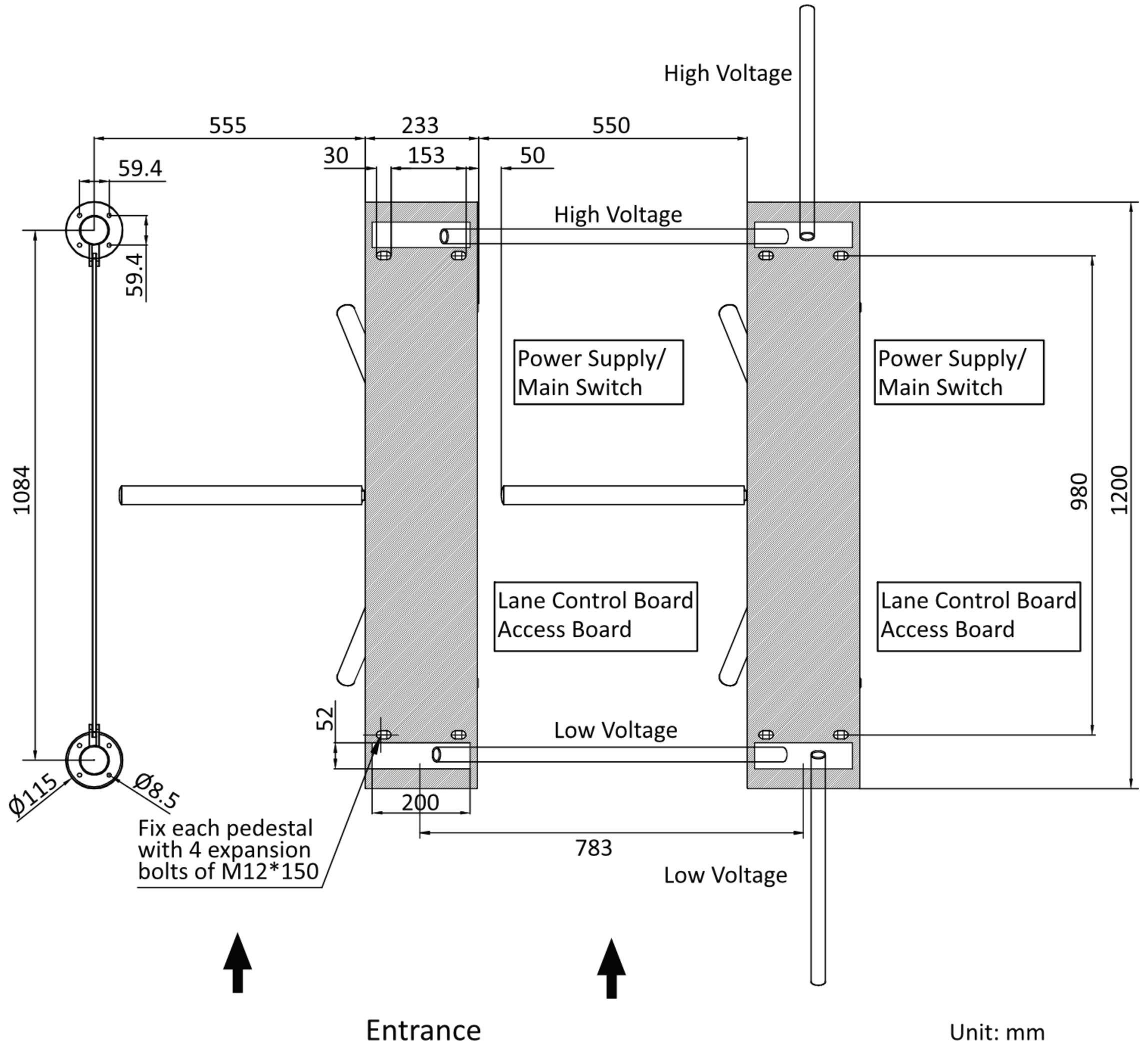


Figure 3-1 Hole Position Diagram

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

Note

- High voltage: 100 to 240 VAC, 50 to 60 Hz AC power input
  Low voltage: network communication cable
- The inner diameter of the low voltage conduit and of the high voltage (AC power cord) conduit should be larger than 30 mm. If any high-power authentication device is required to install on the left pedestal, the diameter of its conduits should be larger.
- If you want to bury both of the AC power cord and the low voltage cable, the two cables should be in separated conduits to avoid interference.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.

- The external AC power cord should be double-insulated.
- The network cable must be CAT5e or other cables with better performance.
- Before digging holes, evaluate the thickness of the installation surface to avoid puncturing.
- You can not thread cables in the diagonal area.

Chapter 4 Install Pedestals

Before You Start

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

Steps

Note

- Make sure the device is installed on flat surface. The foundation should be hard and the thickness should exceeds the length of the expansion bolt.
- Make sure the device is powered off during installation and other operations.
- The installation tools are put inside the package of the pedestal.
- In order to prevent stainless steel from rusting due to dirt during the installation, it is recommended to tear off the protective film after the device is installed.
- There may be residual glue at the film cutting position, and it is recommended to wipe the glue with WD-40 protective liquid after tearing the film.
- Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 713 mm.

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Align the pedestals with the pre-buried expansion bolts.
3. Remove the top cover with the key.

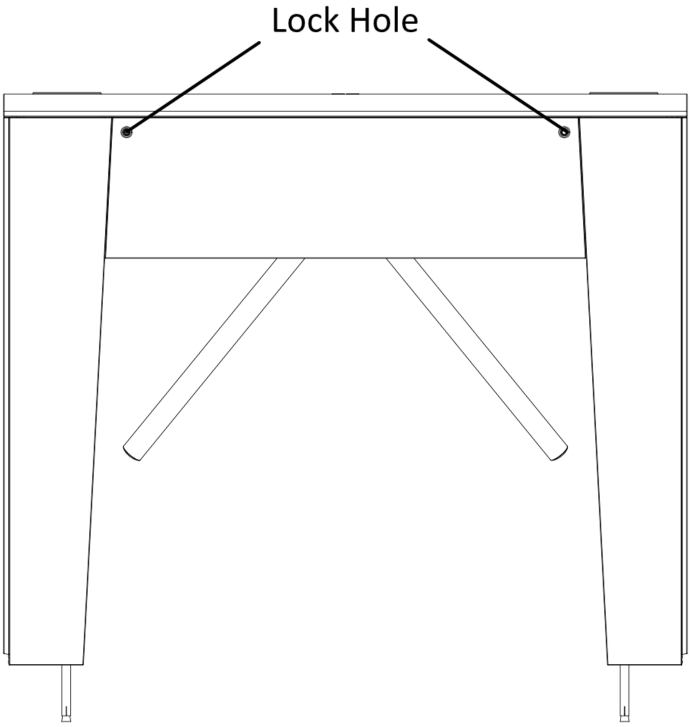


Figure 4-1 Lock Hole

4. Loosen four screws on the top with the screwdriver and remove the maintenance door on both sides.

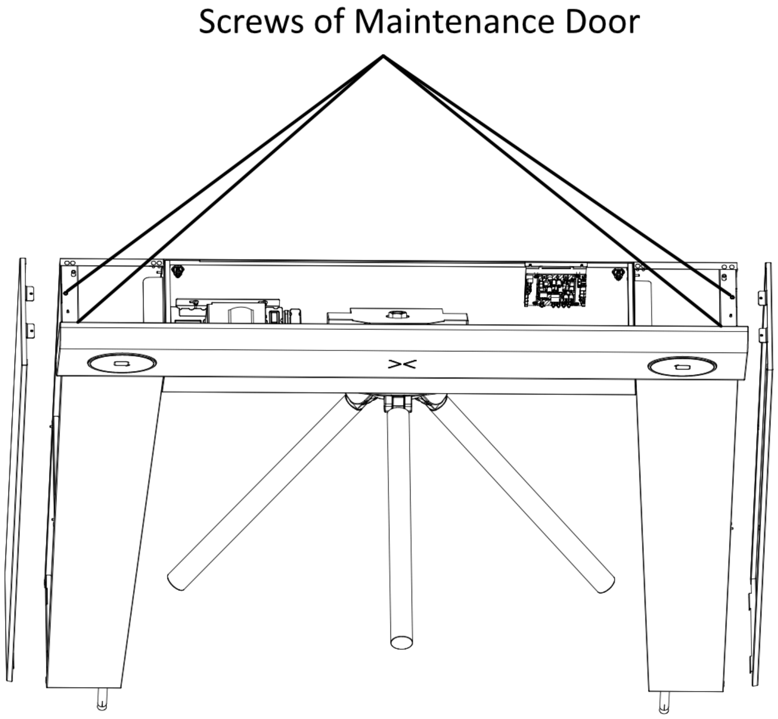


Figure 4-2 Screws of Maintenance Door

5. Secure each pedestal with expansion bolts, and fix the top cover and maintenance door to its original position.

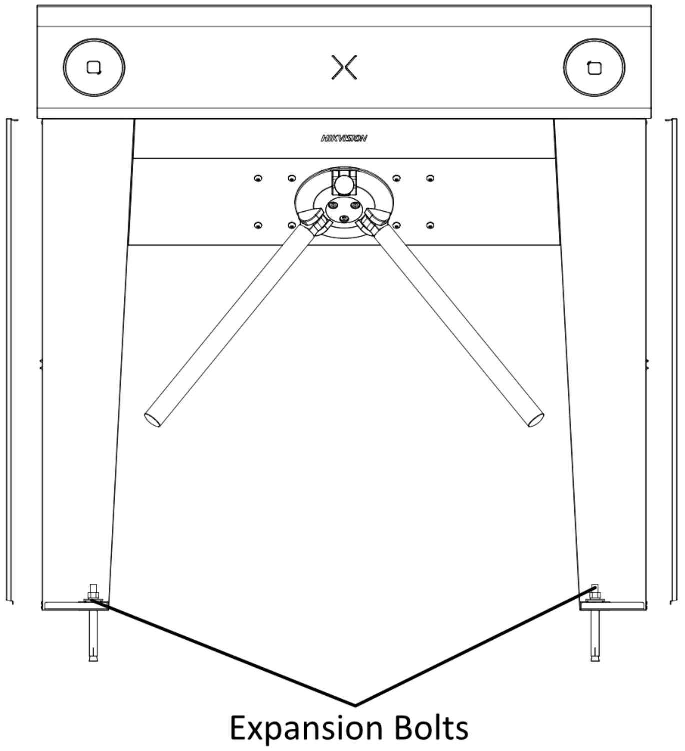


Figure 4-3 Expansion Bolts

Chapter 5 General Wiring

5.1 Components Introduction

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

Note

The voltage fluctuation of the electric supply is between 100 VAC and 240 VAC, 50 to 60 Hz.

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

Note

The diagram is for reference only.

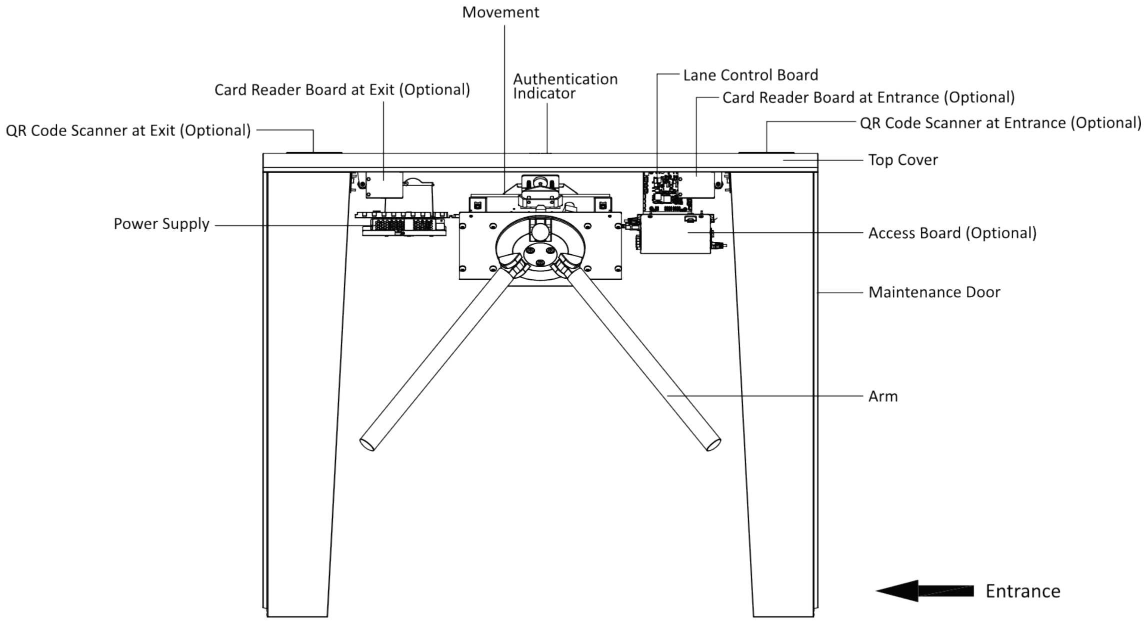

Movement
Card Reader Board at Exit (Optional)
Authentication Indicator
Lane Control Board
Card Reader Board at Entrance (Optional)
QR Code Scanner at Exit (Optional)
QR Code Scanner at Entrance (Optional)
Top Cover
Power Supply
Access Board (Optional)
Maintenance Door
Arm
Entrance

Figure 5-1 Components

5.2 Serial Port Introduction

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

View serial port position according to the diagram below.

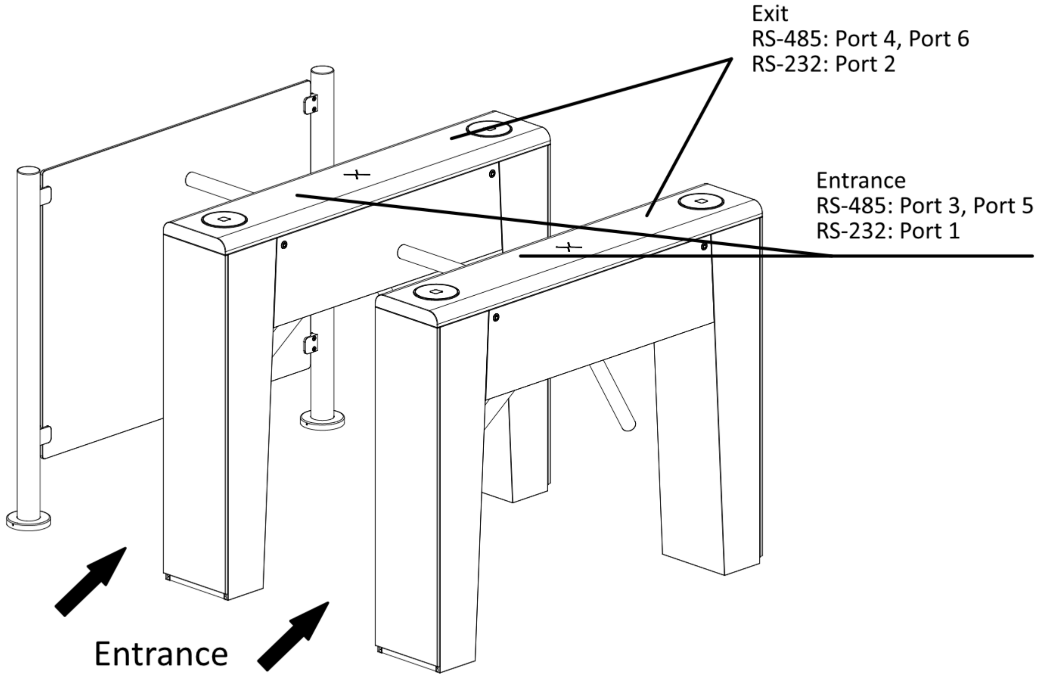


Figure 5-2 Serial Port

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

5.3 General Wiring

The general wiring of lane control board, access control board and card reader.

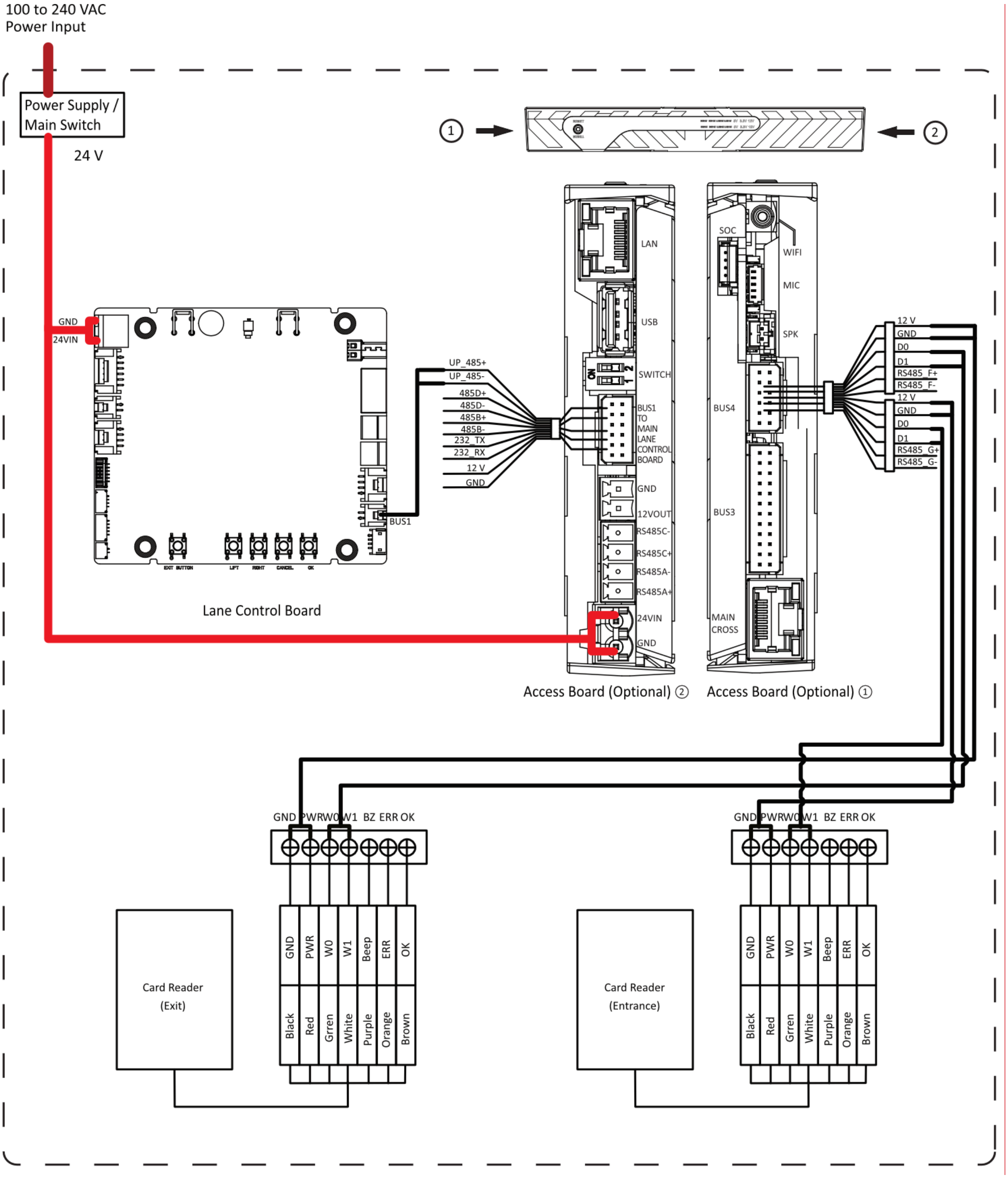


Figure 5-3 General Wiring

Note

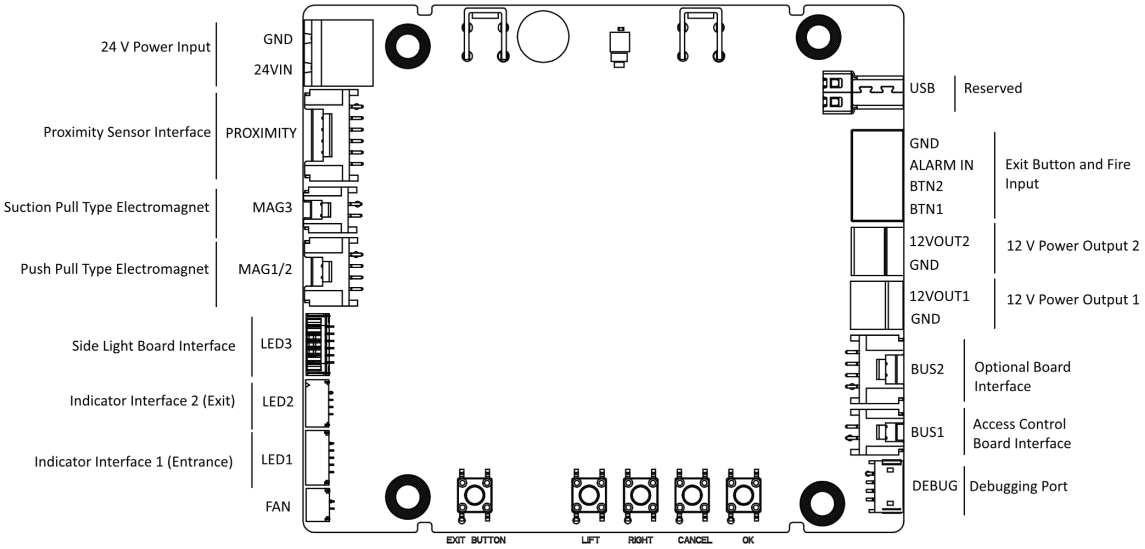
- The power cable from main switch to the lane control board has been connected. You will need to prepare the 14AWG power cable to connect the AC power input to power supply.
- Barrier opens at the entrance/exit: connect to BTN1/BTN2 and GND.

5.4 Terminal Description

5.4.1 Lane Control Board Terminal Description

The lane control board contains power input interface, exit button and fire input interface, access control board interface, debugging port, indicator interface, etc.

The picture displayed below is the lane control board diagram.


24 V Power Input
GND
24VIN
Proximity Sensor Interface
PROXIMITY
Suction Pull Type Electromagnet
MAG3
Push Pull Type Electromagnet
MAG1/2
Side Light Board Interface
LED3
Indicator Interface 2 (Exit)
LED2
Indicator Interface 1 (Entrance)
LED1
FAN
EXIT BUTTON
LIFT
RIGHT
CANCEL
OK
USB
Reserved
GND
ALARM IN
BTN2
BTN1
Exit Button and Fire Input
12VOUT2
GND
12 V Power Output 2
12VOUT1
GND
12 V Power Output 1
BUS2
Optional Board Interface
BUS1
Access Control Board Interface
DEBUG
Debugging Port

5.4.2 Access Board (Optional)

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

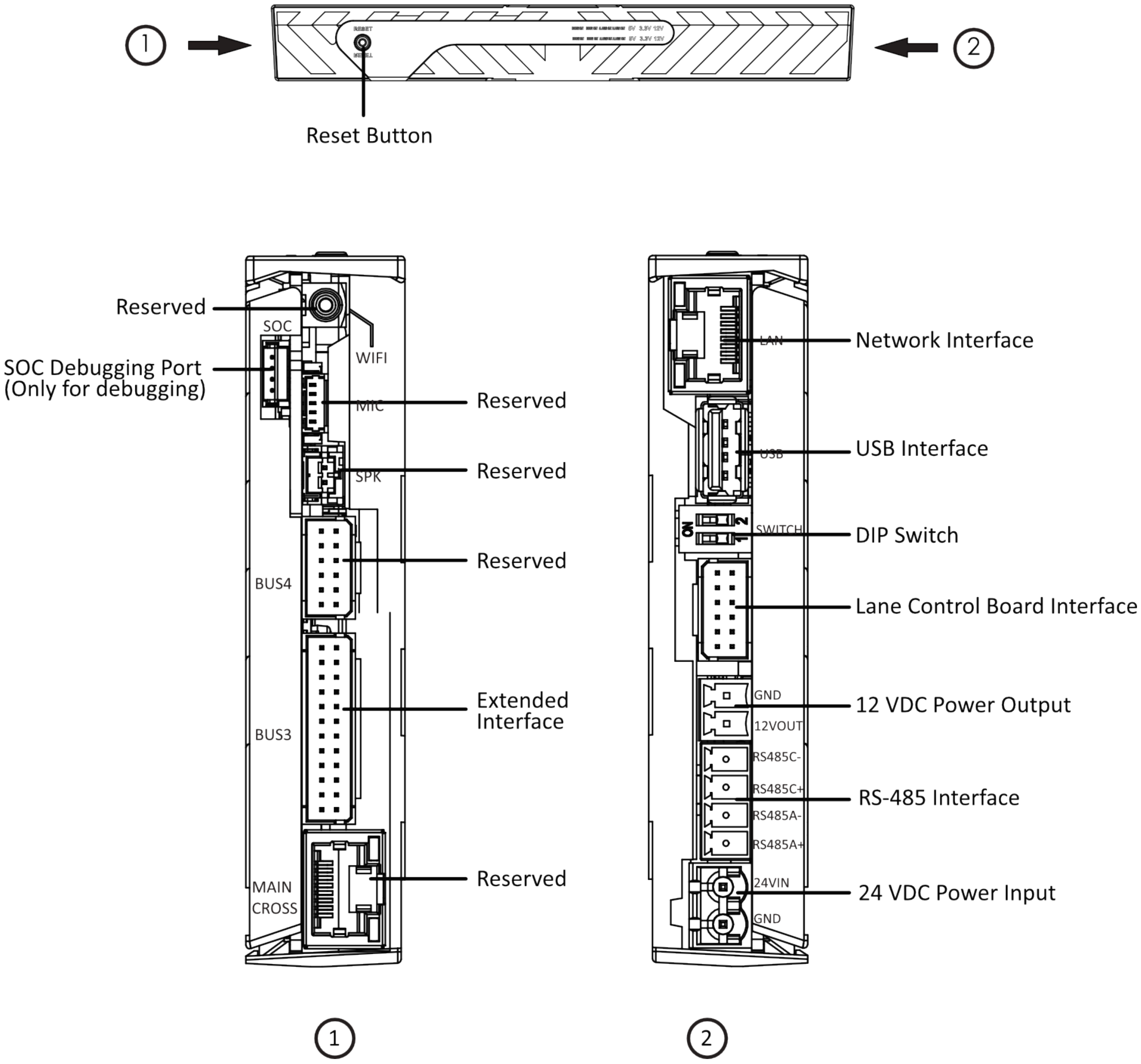


Figure 5-4 Access Board

Note

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

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

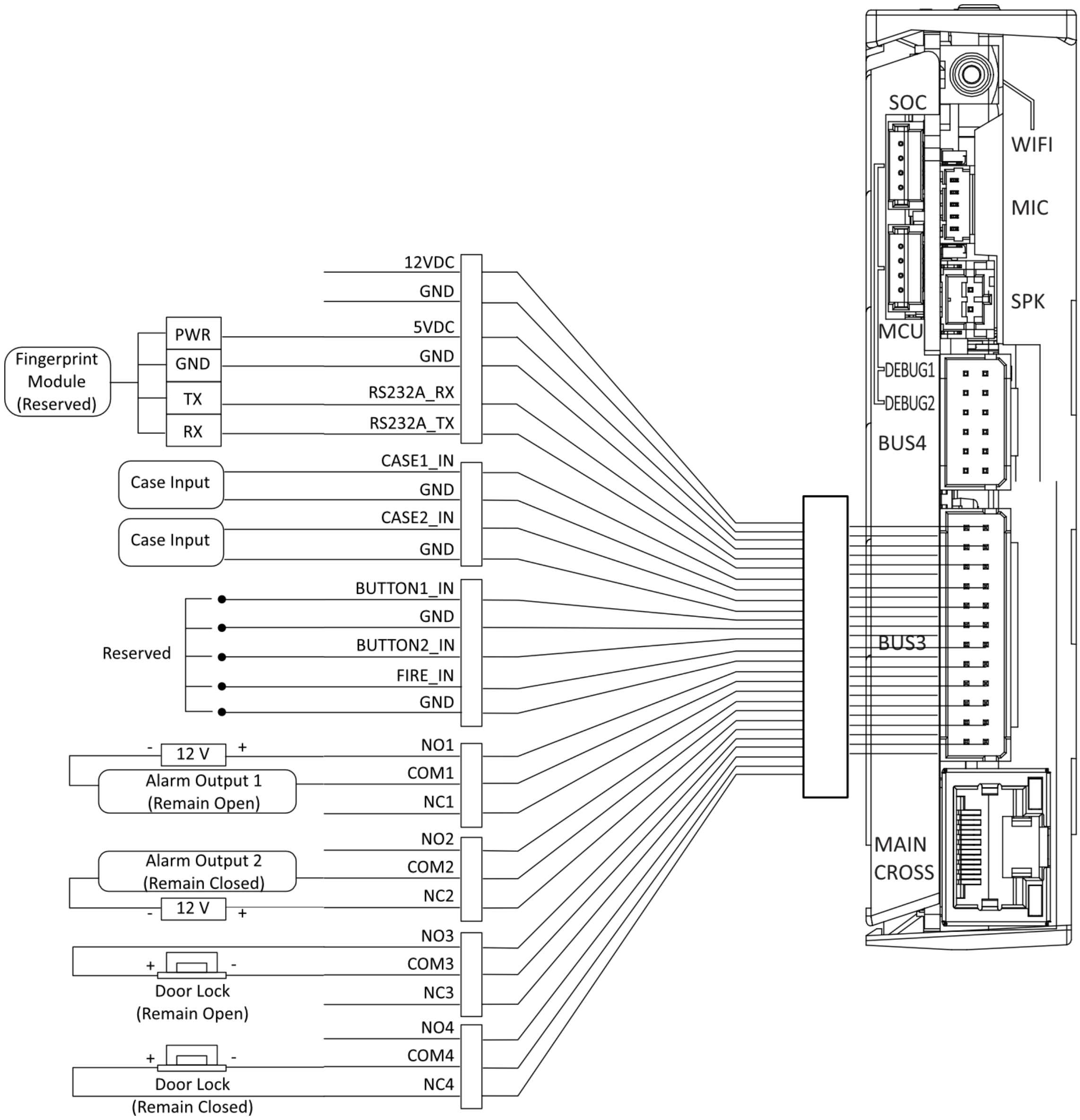


Figure 5-5 Wring Diagram of BUS3 Interface

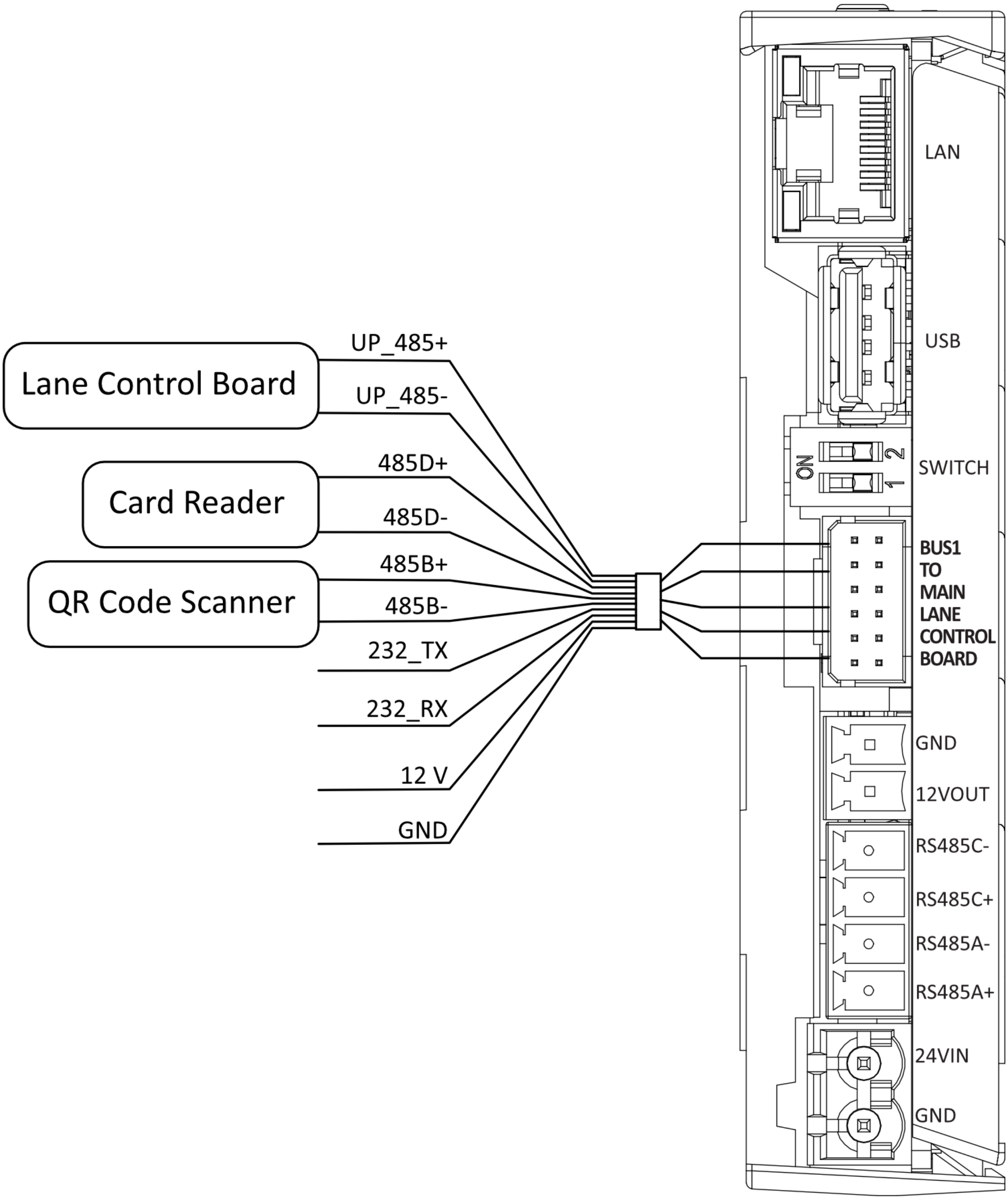


Figure 5-6 Wring Diagram of BUS1 Interface

Note

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

5.4.3 Card Reader

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

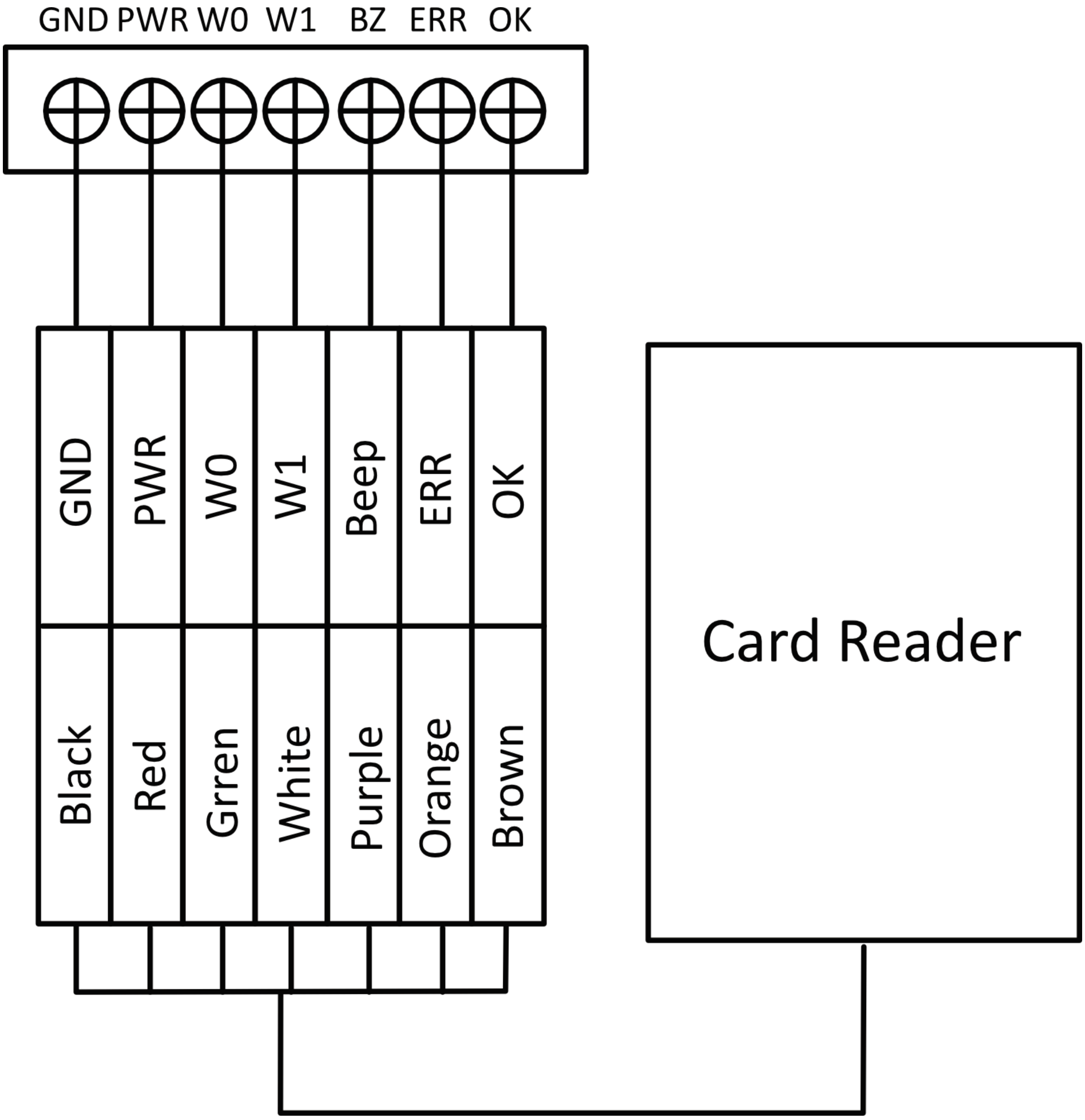


Figure 5-7 Card Reader

5.4.4 RS-485 Wiring

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

Note

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

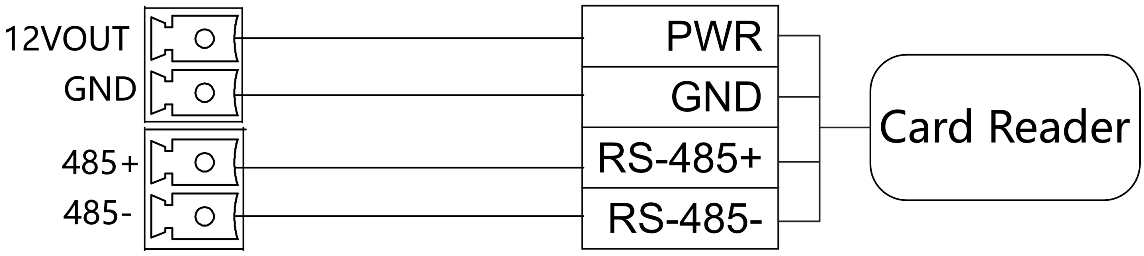


Figure 5-8 Wiring RS-485

5.4.5 RS-232 Wiring

Note

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

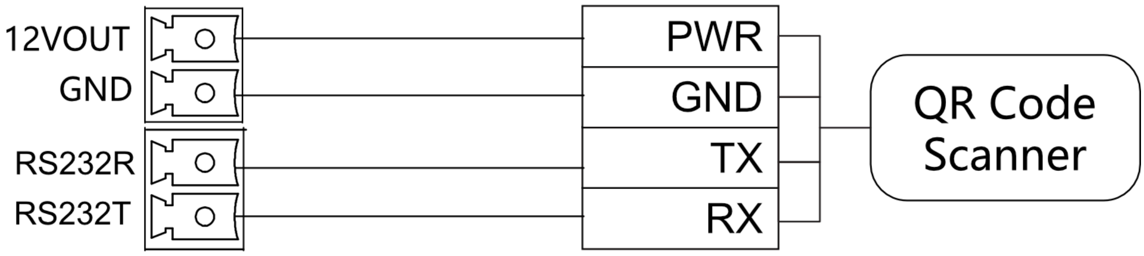


Figure 5-9 RS-232 Wiring

5.4.6 Alarm Input Wiring

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

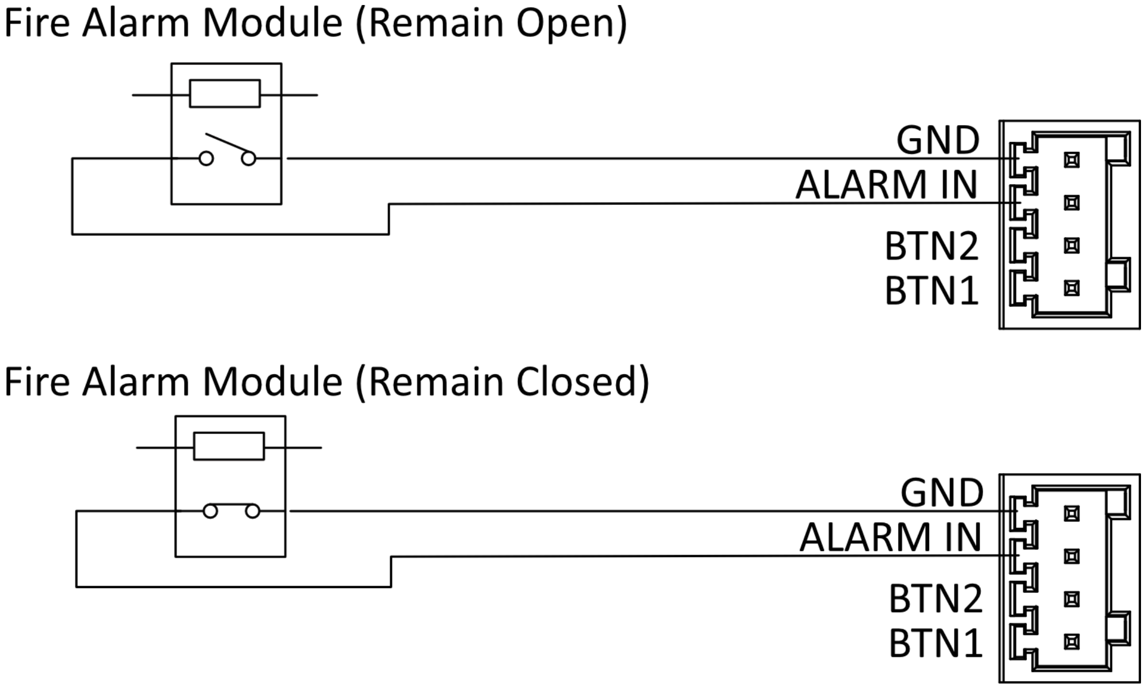

Fire Alarm Module (Remain Open)
GND
ALARM IN
BTN2
BTN1
Fire Alarm Module (Remain Closed)
GND
ALARM IN
BTN2
BTN1

Figure 5-10 Alarm Input

5.4.7 Exit Button Wiring

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

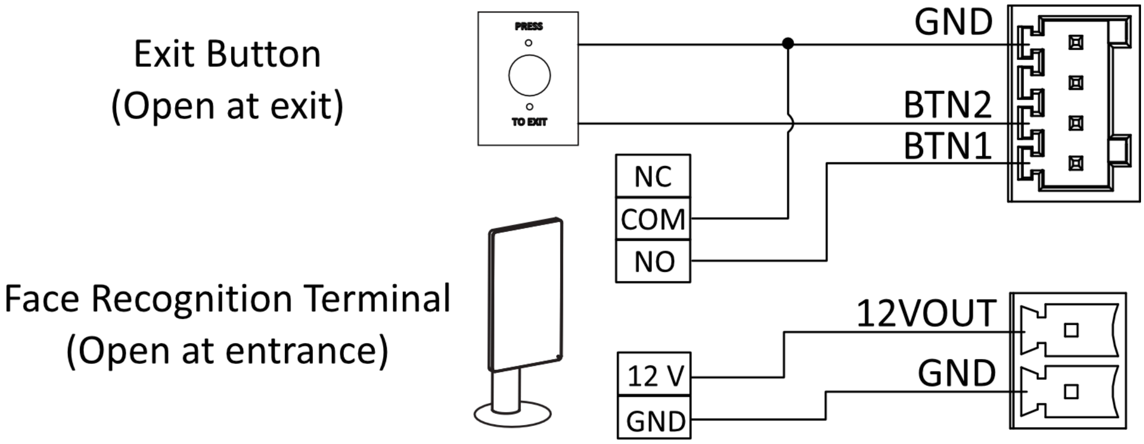


Figure 5-11 Exit Button Wiring

Note

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

5.5 Device Settings via Button

5.5.1 Configuration via Button

Button Description

The buttons are on the lane control board.

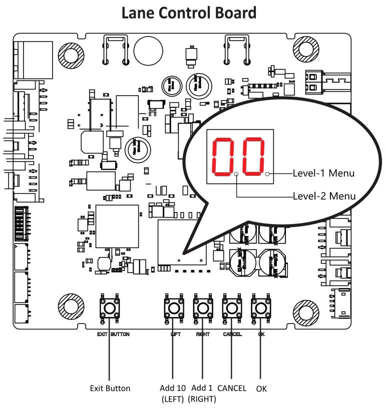


Figure 5-12 Button

Exit Button

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

Parameter Configuration Button

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

Note

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

Button Configuration Procedure

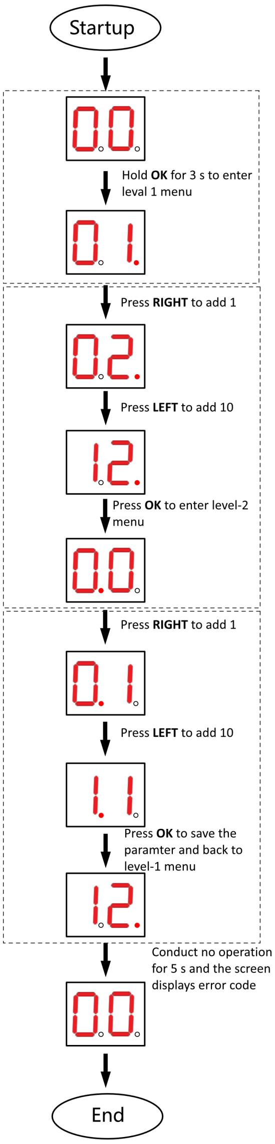

Startup
Hold **OK** for 3 s to enter leval 1 menu
Press **RIGHT** to add 1
Press **LEFT** to add 10
Press **OK** to enter level-2 menu
Press **RIGHT** to add 1
Press **LEFT** to add 10
Press **OK** to save the paramter and back to level-1 menu
Conduct no operation for 5 s and the screen displays error code
End

Figure 5-13 Procedure

Steps:

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

5.5.2 Keyfob Pairing

Pair keyfob via button or DIP switch.

Pair Keyfob via Button

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

Before You Start
Ask our technique supports or sales and purchase the keyfob.

Steps

Note

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

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

2. Hold the **Close** button for more than 10 seconds.

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

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

Pair Keyfob via DIP Switch (Optional)

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

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

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

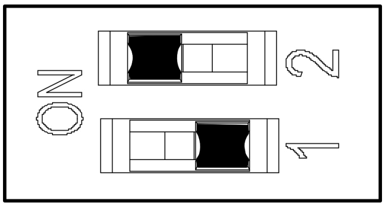


Figure 5-14 Enable Keyfob Paring Mode

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

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

Note

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

5.5.3 Initialize Device

Steps

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

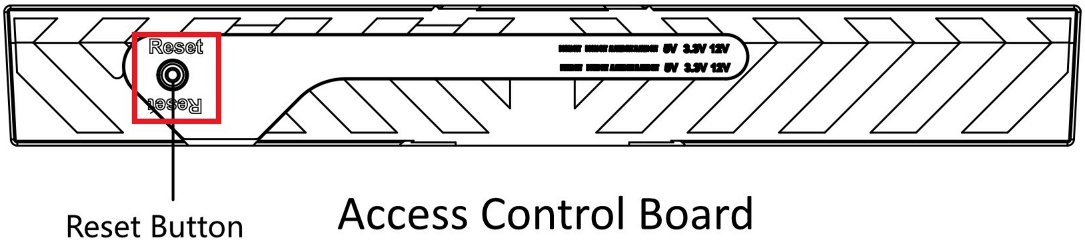


Figure 5-15 Initialization Button Position

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

⚠ **Caution**

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

Note

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

Chapter 6 Activation

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

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

The default values of the device are as follows:

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

6.1 Activate via Web Browser

You can activate the device via the web browser.

Steps

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

   Note

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

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

   Caution

   - The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.
   - Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
   - Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
   - Password cannot contain words such as hik, hkws, and hikvision (case insensitive).

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

6.2 Activate via 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

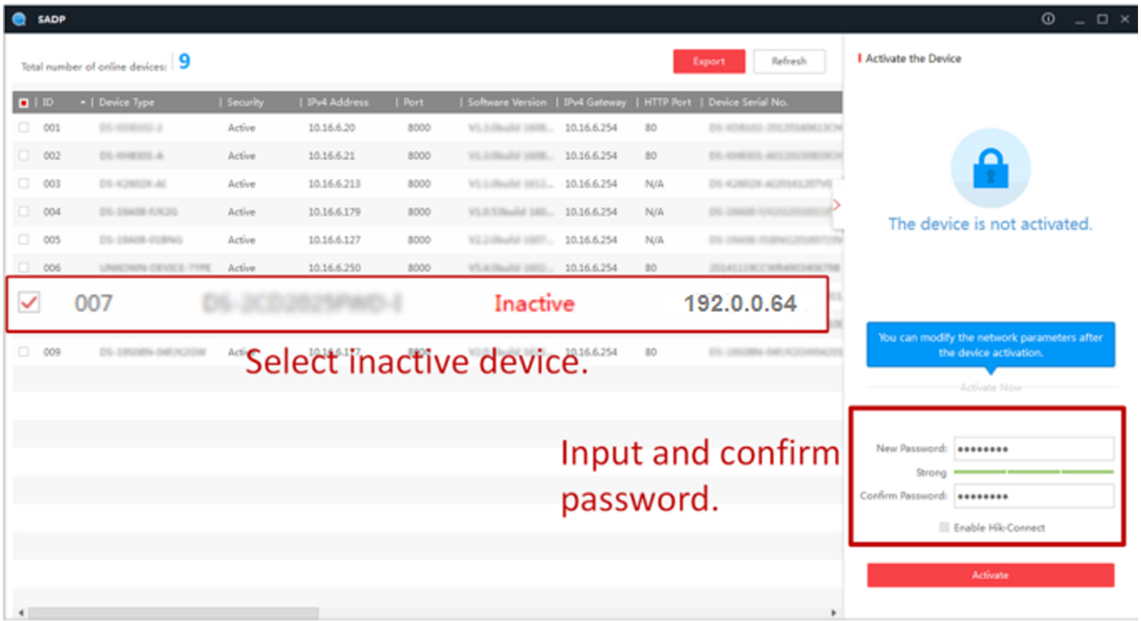
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

   ⚠**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.

   ℹ**Note**

   Characters containing admin and nimda are not supported to be set as activation password.
4. Click **Activate** to start activation.



Total number of online devices: 9

☐ ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐ 001	[redacted]	Active	10.16.6.20	8000	[redacted]	10.16.6.254	80	[redacted]
☐ 002	[redacted]	Active	10.16.6.21	8000	[redacted]	10.16.6.254	80	[redacted]
☐ 003	[redacted]	Active	10.16.6.213	8000	[redacted]	10.16.6.254	N/A	[redacted]
☐ 004	[redacted]	Active	10.16.6.179	8000	[redacted]	10.16.6.254	N/A	[redacted]
☐ 005	[redacted]	Active	10.16.6.127	8000	[redacted]	10.16.6.254	N/A	[redacted]
☐ 006	[redacted]	Active	10.16.6.250	8000	[redacted]	10.16.6.254	80	[redacted]
☑ 007	[redacted]	Inactive	192.0.0.64					
☐ 009	[redacted]	Acti	[illegible]	[illegible]	[redacted]	10.16.6.254	80	[redacted]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

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

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

6.3 Activate Device via iVMS-4200 Client Software

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

Steps

Note

This function should be supported by the device.

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

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

⚠ **Caution**

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

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

Note

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

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

Chapter 7 Quick Operation via Web Browser

7.1 Time Settings

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

Device Time

Display the device time in real time.

Time Zone

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

Time Synchronization Mode

NTP

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

Manual

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

DST

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

Click **Complete** to save the settings.

Chapter 8 Operation via Web Browser

8.1 Login

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

Note

Make sure the device is activated.

Login via Web Browser

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

Login via Remote Configuration of Client Software

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

8.2 Live View

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

Function Descriptions:

Device Component Status

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

Remote Control

🔓 / 🔒 / ▣ / ▢

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

Real-Time Event

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

Person Information

You can view the quantity information of person and card.

Network Status

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

Basic Information

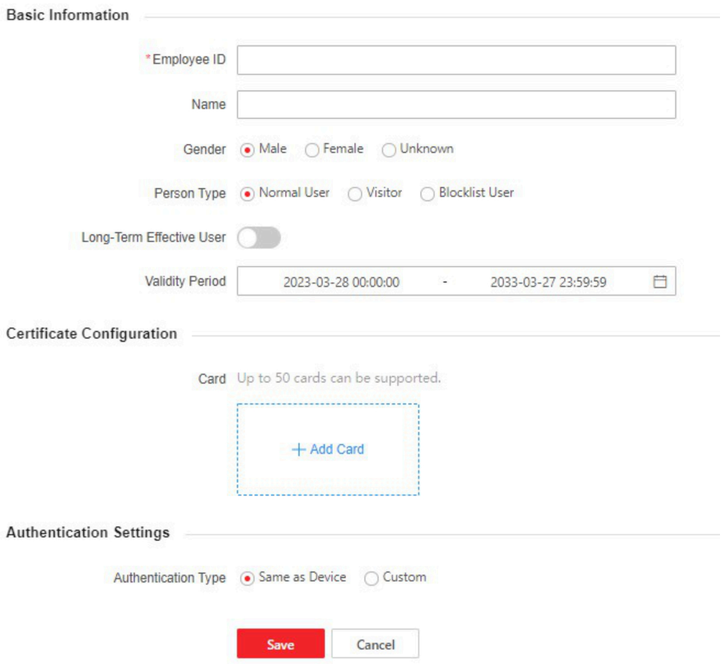
You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, card and event capacity.

8.3 Person Management

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



Basic Information

*Employee ID

Name

Gender ● Male ○ Female ○ Unknown

Person Type ● Normal User ○ Visitor ○ Blocklist User

Long-Term Effective User

Validity Period 2023-03-28 00:00:00 - 2033-03-27 23:59:59

Certificate Configuration

Card Up to 50 cards can be supported.

Authentication Settings

Authentication Type ● Same as Device ○ Custom

Figure 8-1 Add Person

Add Basic Information

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

Set Permission Time

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

Add Card

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

Note

Up to 50 cards can be added.

Click **Save** to save the settings.

Authentication Settings

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

Import/Export Person Data

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.

Note

- Please ensure the name of the imported file is "UserDataFile".

8.4 Search Event

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

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

The results will be displayed on the right panel.

8.5 Configuration

8.5.1 View Device Information

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

Click **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**.

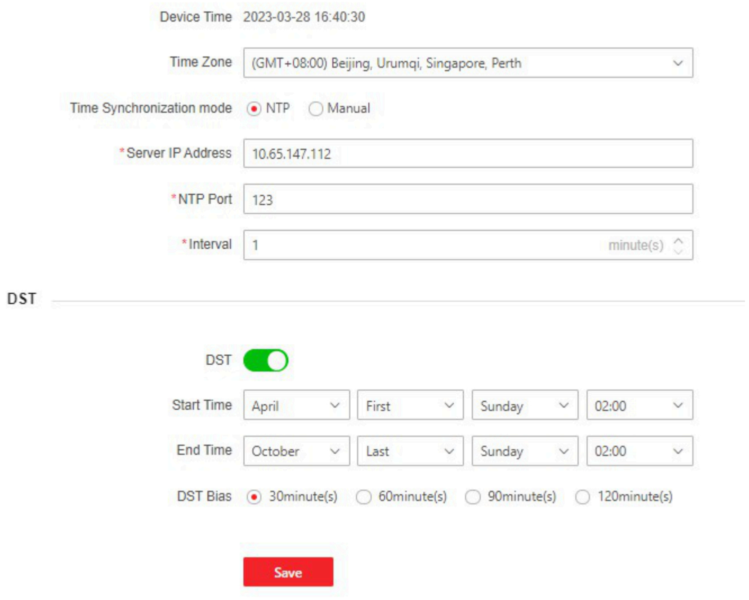
Click **Upgrade** to upgrade the firmware version.

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

8.5.2 Set Time

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

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



Device Time 2023-03-28 16:40:30

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Synchronization mode ● NTP ○ Manual

*Server IP Address 10.65.147.112

*NTP Port 123

*Interval 1 minute(s)

DST

DST ●

Start Time April First Sunday 02:00

End Time October Last Sunday 02:00

DST Bias ● 30minute(s) ○ 60minute(s) ○ 90minute(s) ○ 120minute(s)

Figure 8-2 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.

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.

Server IP Address/NTP Port/Interval

You can set the server IP address, NTP port, and interval.

8.5.3 Set DST

Steps

1. Click **Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

8.5.4 Change Administrator's Password

Steps

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

⚠ **Caution**

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

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

8.5.5 Online Users

The information of users logging into the device is shown.

Go to **Configuration → User Management → Online Users** to view the list of online users.

8.5.6 View Device Arming/Disarming Information

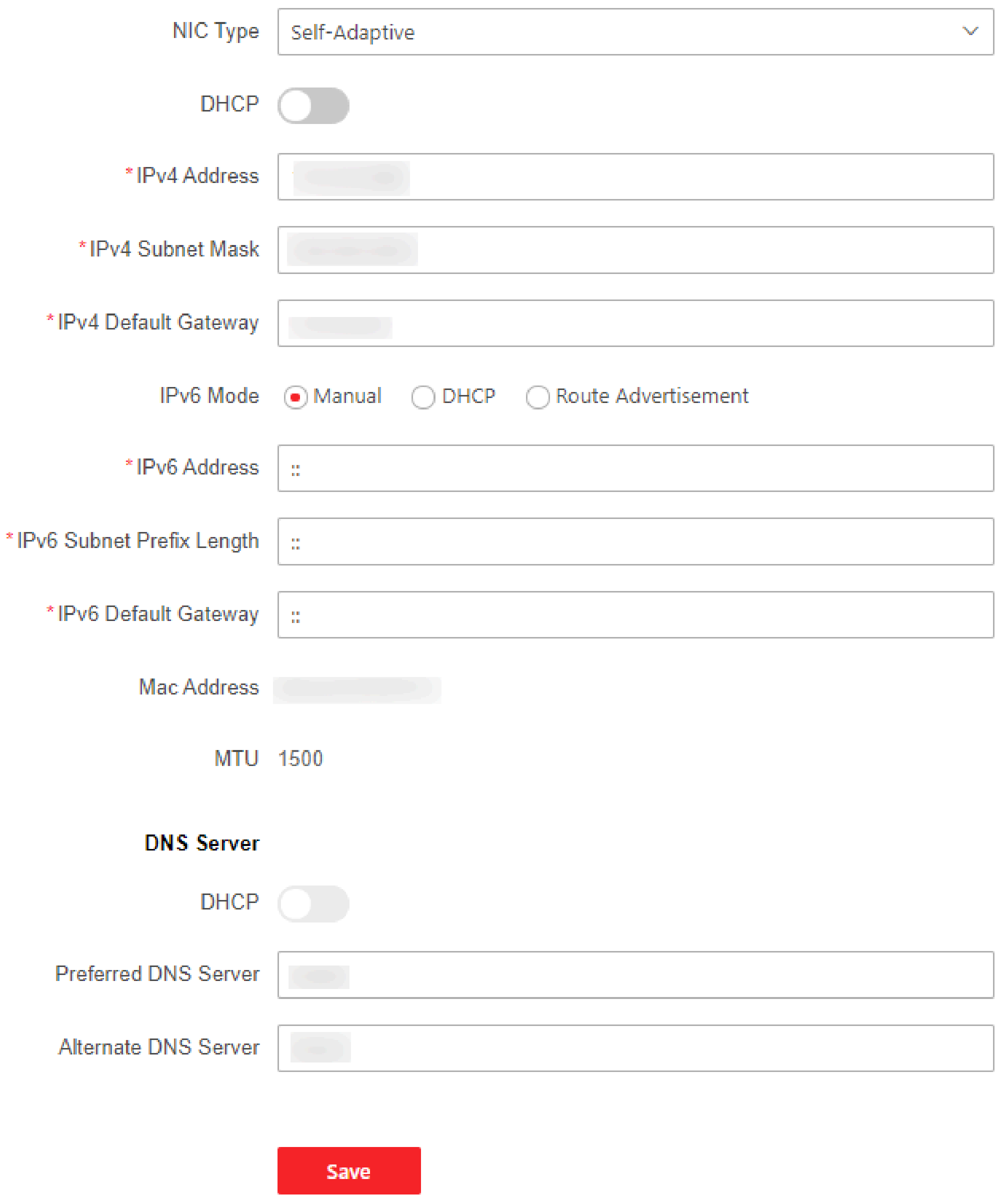
View device arming type and arming IP address.

Click **Configuration → System → User Management → Arming/Disarming Information** .
You can view the device arming/disarming information. Click **Refresh** to refresh the page.

8.5.7 Network Settings

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .
You can view the mac address and MTU.
Set the parameters and click **Save** to save the settings.



NIC Type: Self-Adaptive

DHCP: ○

* IPv4 Address

* IPv4 Subnet Mask

* IPv4 Default Gateway

IPv6 Mode: ● Manual ○ DHCP ○ Route Advertisement

* IPv6 Address: ::

* IPv6 Subnet Prefix Length: ::

* IPv6 Default Gateway: ::

Mac Address

MTU: 1500

DNS Server

DHCP: ○

Preferred DNS Server

Alternate DNS Server

Figure 8-3 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.

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.

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

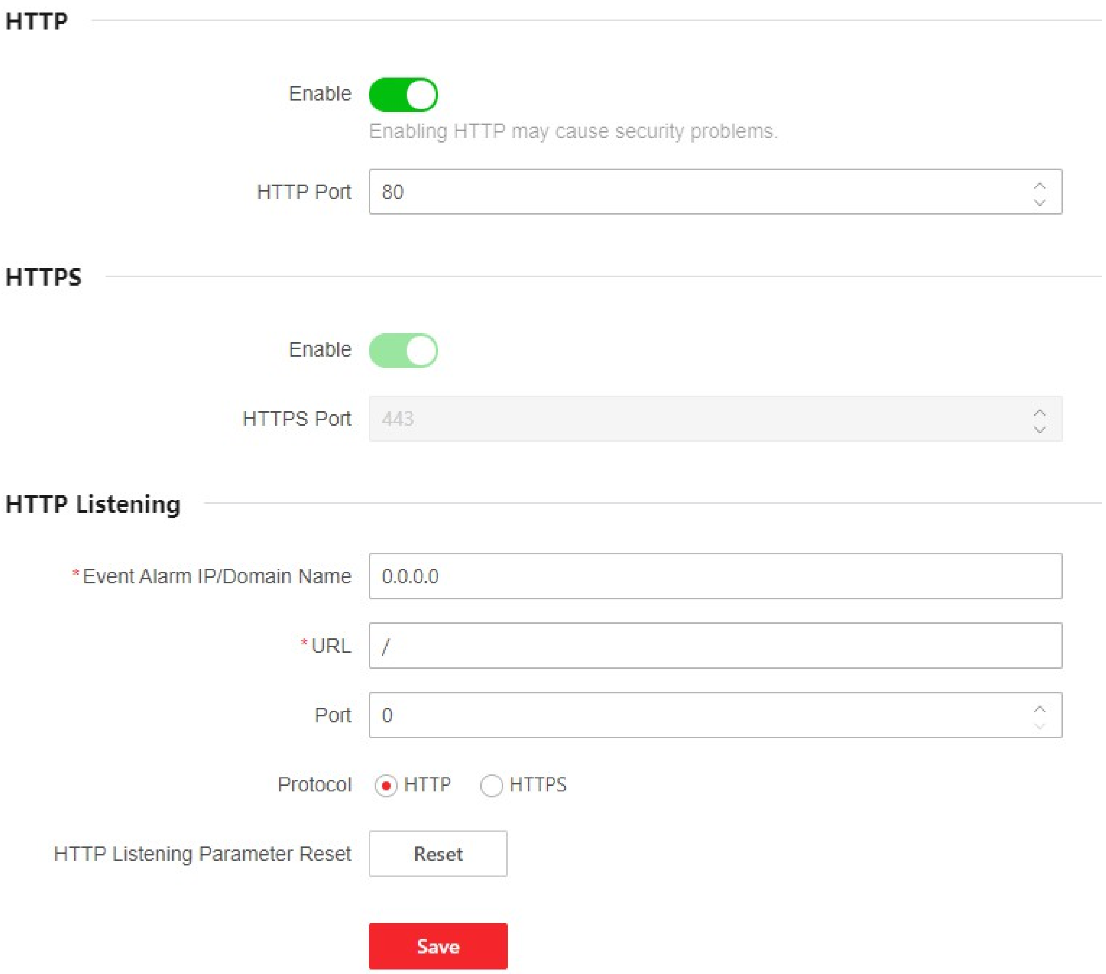
A mechanism for automatic address configuration in the IPv6 protocol stack. The device can complete IPv6 address configuration as long as there are routers in the environment that can provide routing notification messages.

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

Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening parameters.

Click **Configuration → Network → Network Service → HTTP(S)** .



HTTP

Enable: on

Enabling HTTP may cause security problems.

HTTP Port: 80

HTTPS

Enable: on

HTTPS Port: 443

HTTP Listening

*Event Alarm IP/Domain Name: 0.0.0.0

*URL: /

Port: 0

Protocol: ● HTTP ○ HTTPS

HTTP Listening Parameter Reset: Reset

Save

Figure 8-4 Set Port

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.

You can also click **Reset** to reset the HTTP listening parameters.

Set Network Penetration Service

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

Steps

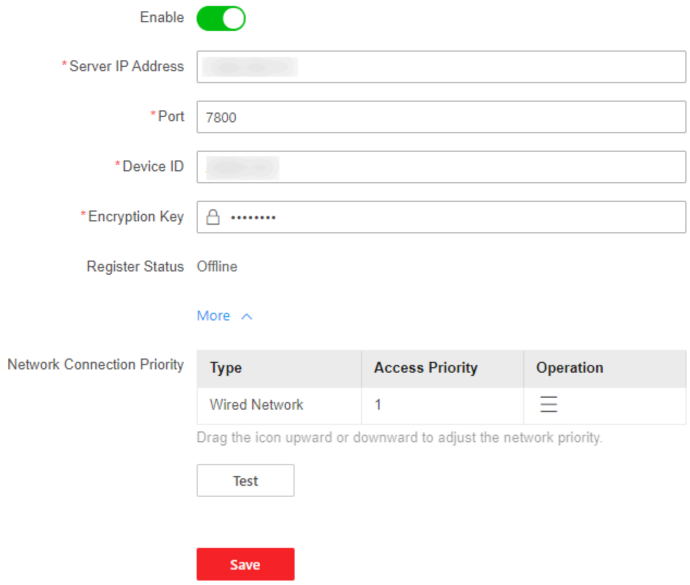
1. Click **Configuration → Network → Network Service → Network Penetration Service** .
2. Click to **Enable Penetration Service**.
3. Enter **Server IP Address** and **Server Port**.
4. Enter login **User Name** and **Password**.
5. Set **Heartbeat Timeout**. The range is1 to 6000.
6. Click **Save**.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

Set OTAP

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 **Configuration → Network → Device Access → OTAP** .



Enable

*Server IP Address [redacted]

*Port 7800

*Device ID [redacted]

*Encryption Key ••••••••

Register Status Offline

More

Network Connection Priority

Type	Access Priority	Operation
Wired Network	1	☰

Drag the icon upward or downward to adjust the network priority.

Test

Save

Figure 8-5 Set OTAP

2. Click to **Enable** OTAP.
3. Set **Server IP Address**, **Port**, **Device ID** and **Encryption Key**.
4. 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**.
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 **Save**.

Platform Access

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

Steps

1. Click **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. Click the slider to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. View the register status, and click **Refresh** to view the latest status.
5. Click **Save** to enable the settings.
6. View the account binding status, and click **Refresh** to view the latest status.
7. Bind the account.

- Binding via Code: Click **View** to view device QR code. Scan the QR code to bind the account.
- Manual Binding: View account verification code by the path: Phone APP-My-Account. Enter the **User Token**, and click **Bind** to bind the account.

8.5.8 Set Audio Parameters

Set the audio parameters.

Click **Configuration → Video/Audio → Audio** .

Set the output volume, and enable voice prompt according to your needs.

Click **Save** to save the settings.

8.5.9 Event Linkage

Set linked actions for events.

Steps

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

   Buzzer Linkage

   Enable **Buzzer Linkage** and select **Start Buzzing** or **Stop Buzzing** for the target event.

   Door Linkage

   Enable **Linked Door**, check **Entrance** or **Exit**, and set the door status 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.

   Linkage Audio Prompt

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

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

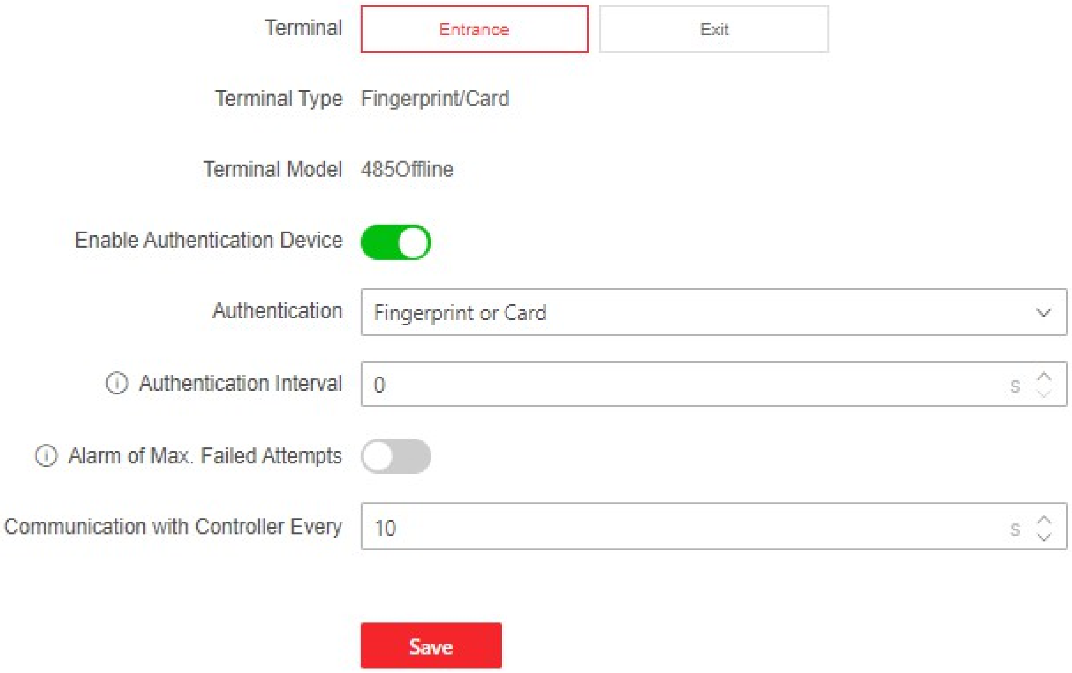
8.5.10 Access Control Settings

Set Authentication Parameters

Click **Configuration → Access Control → Authentication Settings** .

Note

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



Terminal: Entrance | Exit

Terminal Type: Fingerprint/Card

Terminal Model: 485Offline

Enable Authentication Device: ●

Authentication: Fingerprint or Card

Authentication Interval: 0 s

Alarm of Max. Failed Attempts: ○

Communication with Controller Every: 10 s

Figure 8-6 Set Authentication Parameters

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

Terminal

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

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

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.

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.

Communication with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Note

The authentication interval value ranges from 2 s to 255 s.

Set Door Parameters

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

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

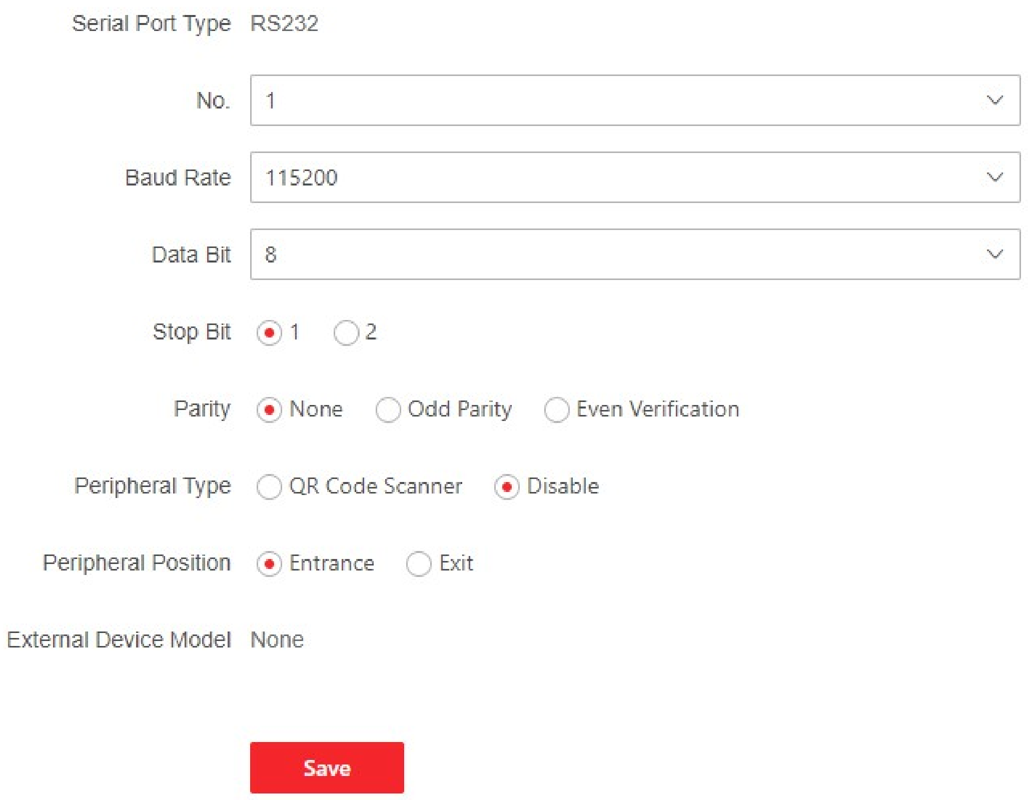
Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Serial Port Settings

Set serial port parameters.

Steps

1. Click **Configuration → Access Control → Serial Port Configuration** .



Serial Port Type RS232

No. 1

Baud Rate 115200

Data Bit 8

Stop Bit ● 1 ○ 2

Parity ● None ○ Odd Parity ○ Even Verification

Peripheral Type ○ QR Code Scanner ● Disable

Peripheral Position ● Entrance ○ Exit

External Device Model None

Figure 8-7 Serial Port Configuration

2. Select a serial port No., and the corresponding serial port type will display automatically.
3. 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.

4. Set the **Peripheral Type**.
5. Set the **Peripheral Position** as **Entrance** or **Exit**.
6. You can view the external device model.
7. Click **Save**.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

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

1. Click **Configuration → Access Control → Wiegand Settings** .
2. Select **Entrance** or **Exit**.
3. Enable **Wiegand** function.
4. The wiegand transmission direction is set **Input** by default.

   Note

   Input: the device can connect a Wiegand card reader.
5. Select **Wiegand Mode**.
6. Click **Save** to save the settings.

   Note

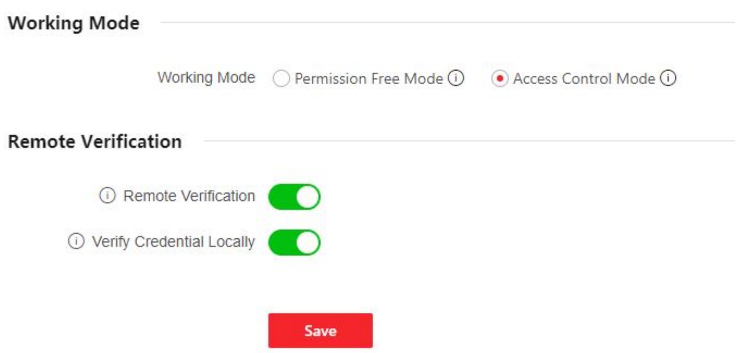
   If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Set Terminal Parameters

Set the working mode and remote verification.

Steps

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



Working Mode

Working Mode ○ Permission Free Mode ⓘ ● Access Control Mode ⓘ

Remote Verification

ⓘ Remote Verification: On

ⓘ Verify Credential Locally: On

Figure 8-8 Terminal Parameters

2. Set the device working mode.

   Permission Free Mode

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

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

   Access Control Mode

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

3. Set remote verification.

   1) Enable **Remote Verification**.

   Note

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

   2) **Optional:** Enable **Verify Credential Locally**.

   Note

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

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

8.5.11 Turnstile

Basic Parameters

Set turnstile basic parameters.

Steps

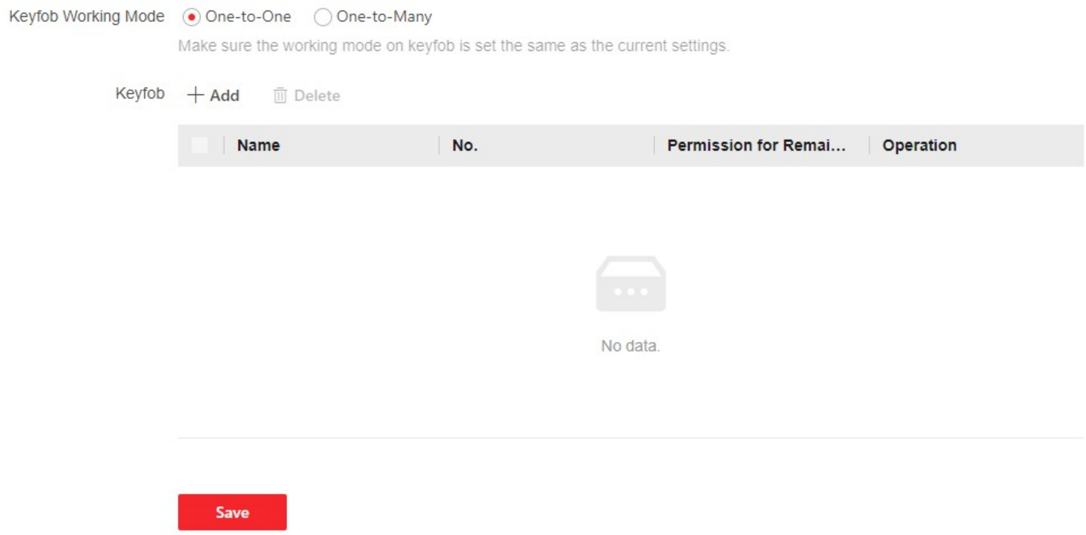
1. Click **Configuration → Turnstile Configuration → Basic Settings** to enter the page.
2. View the **Channel Type**, **Channel Model** and **Working Status**.
3. Set the passing mode.
   - If you choose **General Passing**, you can select the barrier status for the entrance and exit from the drop-down list.
   - If you choose **Weekly Schedule**, you can set a weekly schedule for entrance and exit barriers.
4. Click **Save**.

keyfob

Set keyfob parameters.

Steps

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



Keyfob Working Mode ● One-to-One ○ One-to-Many

Make sure the working mode on keyfob is set the same as the current settings.

Keyfob + Add Delete

□	Name	No.	Permission for Remai...	Operation

No data.

Save

Figure 8-9 keyfob

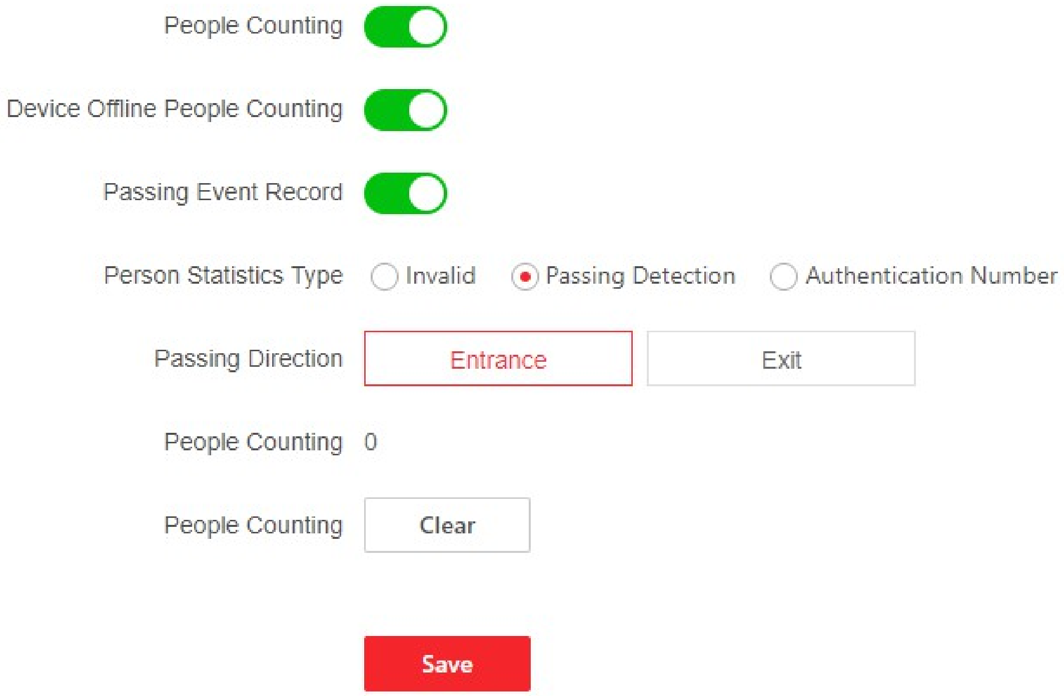
2. Set **Working Mode** as **One-to-One** or **One-to-Many**.
3. Add keyfob.
   1) Click **Add** and the keyfob adding window will pop up.
   2) Enter the **Name** and **Serial No.**.
   3) Check to enable **Permission for Remaining Open** at your actual needs.
   4) Click **Add** to add the keyfob.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

People Counting

Set people counting.

Steps

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



People Counting ☑

Device Offline People Counting ☑

Passing Event Record ☑

Person Statistics Type ○ Invalid ● Passing Detection ○ Authentication Number

Passing Direction [✓ Entrance] Exit

People Counting 0

People Counting Clear

Save

Figure 8-10 People Counting

2. Enable **People Counting**.
3. Enable **Device Offline People Counting**, the device will count people numbers even if it is offline.
4. Enable **Passing Event Record**, event records will be uploaded every time people pass through.

Note

The function only takes effect when the people statistics type is passing detection.

5. Select **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, face recognition, etc.

6. Select passing direction and view people counting results of entrance or exit.
7. **Optional:** Click **Clear** to clear all the people counting information.

Other Settings

Set other parameters.

Steps

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

   Alarm Output Duration

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

   Light Board Brightness

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

   Alarm Buzzing Duration

   Set the duration of alarm sound.

   Memory Mode

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

   Fire Input Type

   In the normally open state, closing triggers fire protection. In the normally closed state, disconnection triggers fire protection.
3. Click **Save**.

8.5.12 Card Settings

Set Card Security

Click **Configuration → Card Settings → Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

Reserved.

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 **Configuration → Card Settings → Card No. Auth. Settings** .

Select a card authentication mode and enable reversed card No. at your actual needs. Click **Save**.

8.5.13 Set Privacy Parameters

Set the event storage type.

Go to **Configuration → Security → Privacy Settings**

The event storage type is overwriting by default. The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

8.5.14 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration → Preference → Prompt Schedule** .
2. Enable the function.

3. Set the appellation.
4. Set the time period when authentication succeeded.
   1) Click **Add Time Duration**.
   2) Set the time duration.

   Note

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

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

   Note

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

   5) **Optional:** Repeat substep 1 to 3.
   6) **Optional:** Click 🗑 to delete the configured time duration.
5. Set the time duration when authentication failed.
   1) Click **Add Time Duration**.
   2) Set the time duration.

   Note

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

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

   Note

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

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

8.5.15 Upgrade and Maintenance

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

Reboot Device

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

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .

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

Note

Do not power off during the upgrading.

Restore Parameters

Click **Maintenance and Security → 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 device IP address and the user information.

Import and Export Parameters

Click **Maintenance and Security → 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.

8.5.16 Device Debugging

You can set device debugging parameters.

Steps

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

   Enable SSH

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

   Print Log

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

   Capture Network Packet

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

Debug Command Management

Select the command type, select quick command or enter custom command, and select the board type. Click **Send** to send the command.

View the received information in the execution result box.

Click **End Debugging**, the device returns to normal operating state.

8.5.17 Component Status

You can view the status of different components.

Main Lane Status

Device Component

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

Peripheral

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

Others

Passing Mode

You can view the entrance and exit mode.

Input and Output Status

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

Other Status

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

8.5.18 Log Query

You can search and view the device logs.

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

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

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

8.5.19 Certificate Management

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

Note

The function is only supported by certain device models.

Create and Import Self-signed Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Key** area, and select a certificate from the local, and click **Import**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

Note

The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Import**.

Chapter 9 Configure the Device via the Mobile Browser

9.1 Login

You can login via mobile browser.

Note

- Make sure the device is activated.
- Make sure the device and the phone are on the same network segment.

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

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

9.2 Overview

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

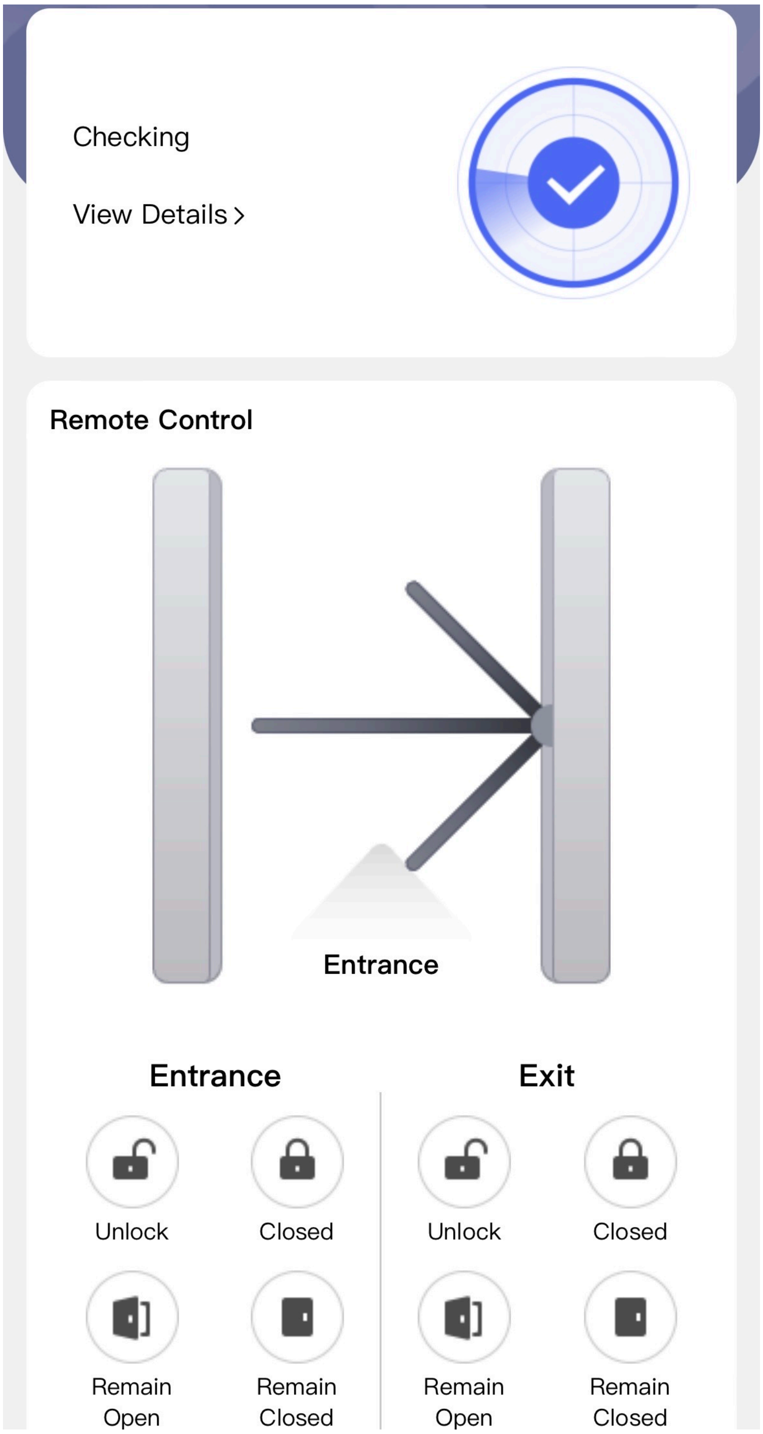


Figure 9-1 Status and Remote Control

You can view the device status. If there is exception, you can tap to view the component details. You can remotely control barrier by tap the icons.

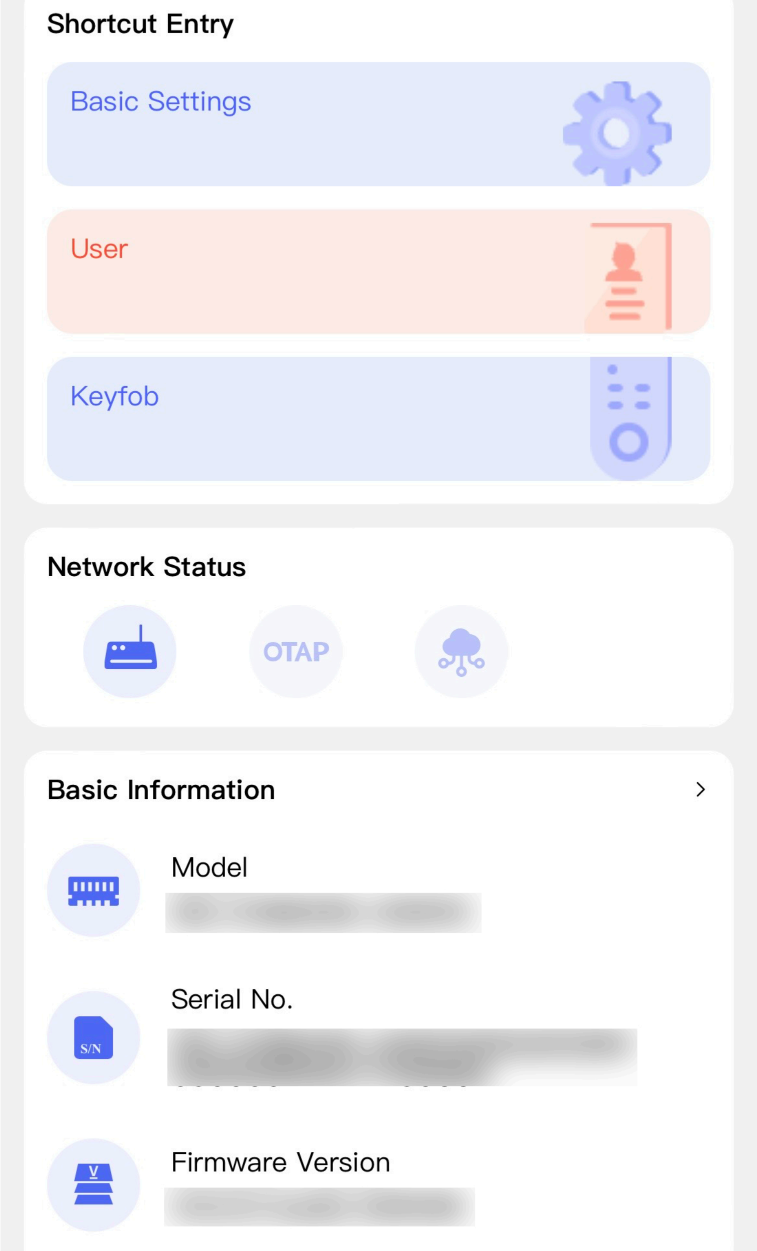


Figure 9-2 Shortcut Entry and Basic Information

You can tap to fast enter the basic settings page, user page, keyfob page and network page.

You can view 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 Parameters

You can set the basic parameters of the turnstile.

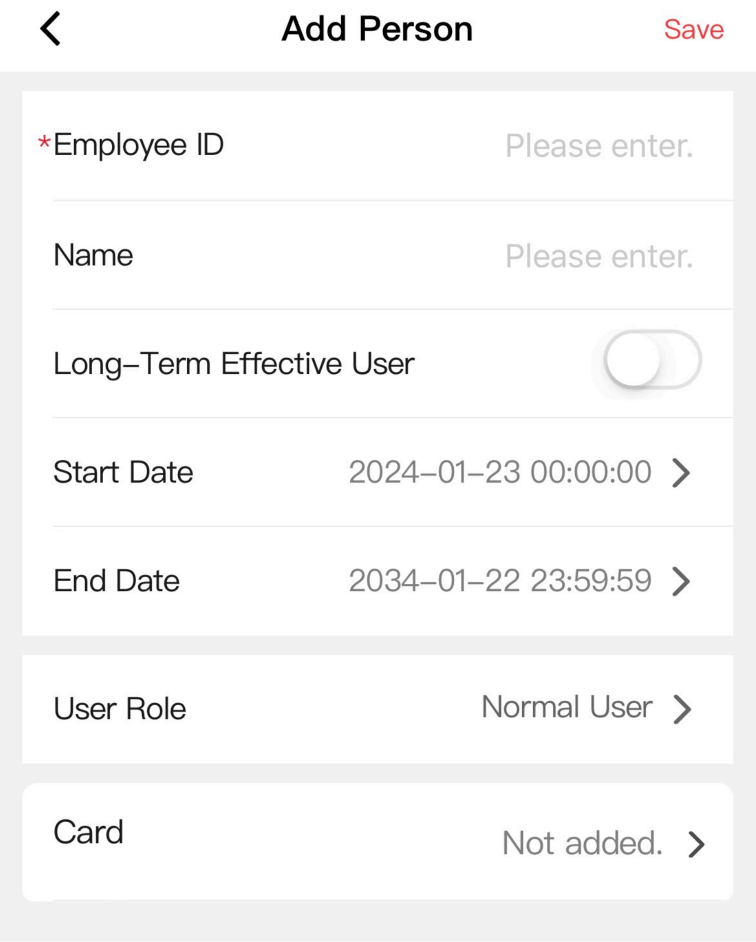
Tap **Basic Settings** of the shortcut entry on the overview page.
Set the regular passing mode for the entrance and exit.
Tap **Save**.

9.3.2 Person Management

You can add, edit, delete, and search person via mobile Web browser.

Steps

1. Tap **User** of the shortcut entry or tap ≡ → **Person Management** to enter the settings page.



*Employee ID Please enter.

Name Please enter.

Long–Term Effective User

Start Date 2024–01–23 00:00:00

End Date 2034–01–22 23:59:59

User Role Normal User

Card Not added.

Figure 9-3 Add Person

2. Add person.

1) Tap**+**.

2) Set the following parameters.

Employee ID

Enter the employee ID. The Employee ID cannot be 0 or exceed 32 characters. It can be a combination of uppercase, lowercase letters and numbers.

Name

Enter your name. The name supports numbers, uppercase and lowercase English, and characters. The name is recommended to be within 32 characters.

Long-Term Effective User

Set the user permission as long-term effective.

Start Date/End Date

Set **Start Date** and **End Date** of user permission.

User Role

Select your user role.

Card

Add card. Tap **+**. Enter the **Card No.**, and select the **Card Type**. Tap **Save** to add the card.

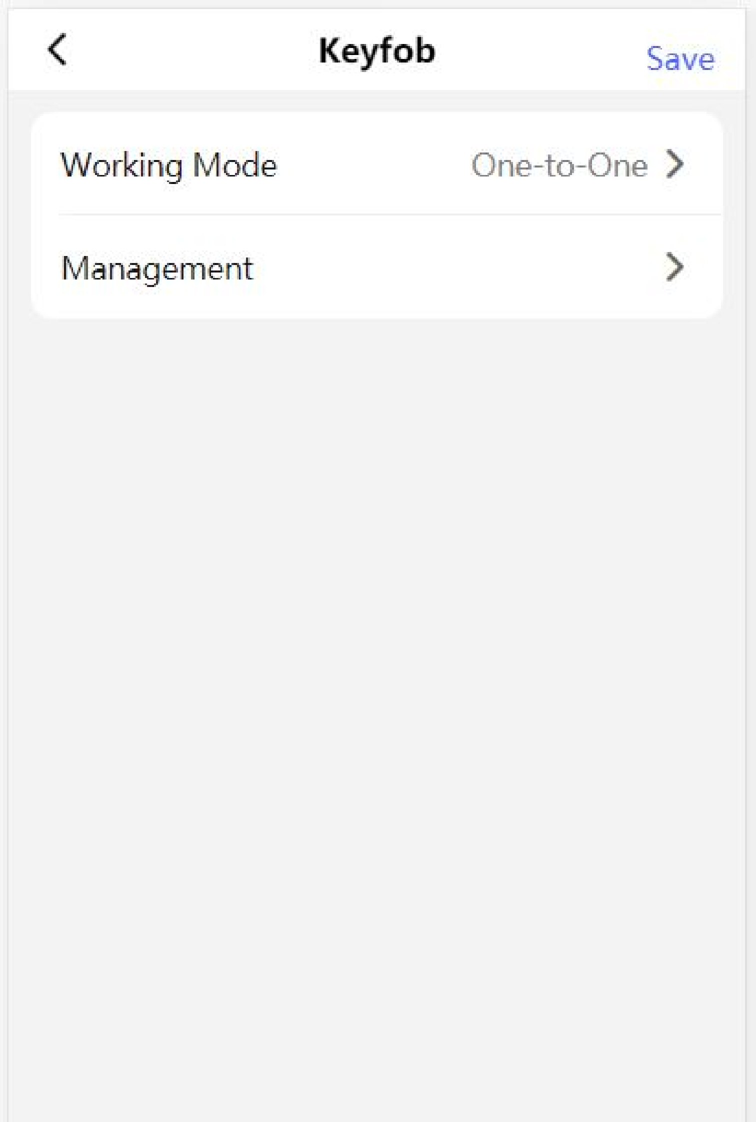
3) Tap **Save**.

3. Tap the user that needs to be edited in the user list to edit the information.

4. You can search the user by entering the employee ID in the search bar.

9.3.3 Keyfob Settings

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



Working Mode One-to-One

Figure 9-4 Keyfob Settings

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

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

9.3.4 View Device Basic Information

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

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

You can change the device name.

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

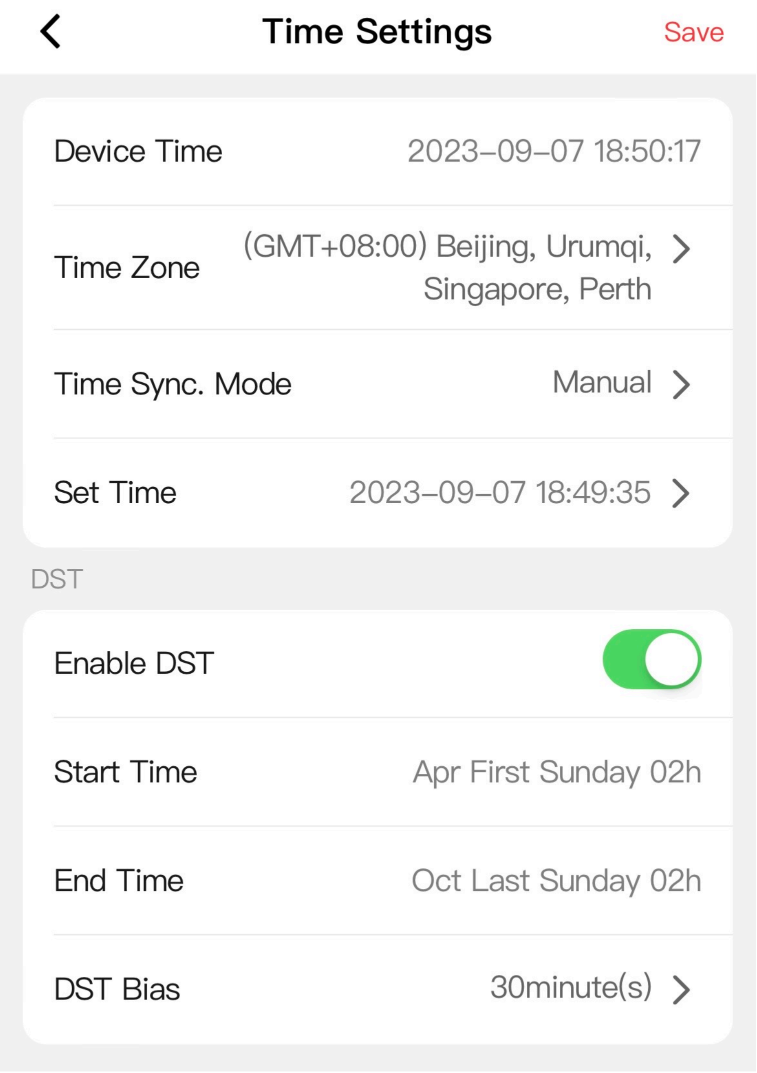
Tap **Device Capacity** to view the quantity and capacity of person, card and event.

Tap **Save**.

9.3.5 Time Settings

View current time and set the time zone.

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



Time Settings

Save

Device Time 2023–09–07 18:50:17

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Sync. Mode Manual

Set Time 2023–09–07 18:49:35

DST

Enable DST

Start Time Apr First Sunday 02h

End Time Oct Last Sunday 02h

DST Bias 30minute(s)

Figure 9-5 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**.

9.3.6 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**.

9.3.7 Network

Wired Network

Set wired network.

Tap ≡ → **Network Settings → Wired Network** to enter the configuration page.

NIC Type

Select a NIC type from the drop-down list.

DHCP

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

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

MAC Address and MTU

You can view the default MAC address and MTU.

IPv6 Mode

Route Advertisement

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

Note

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

Manual

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

DHCP

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

DNS Server

Note

Only when DHCP is enabled can DNS server be set.

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

Set Port Parameters

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

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

HTTP

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

HTTPS

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

Platform Access

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

Steps

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

   Note

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

2. Slide to enable the function.

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

Note

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

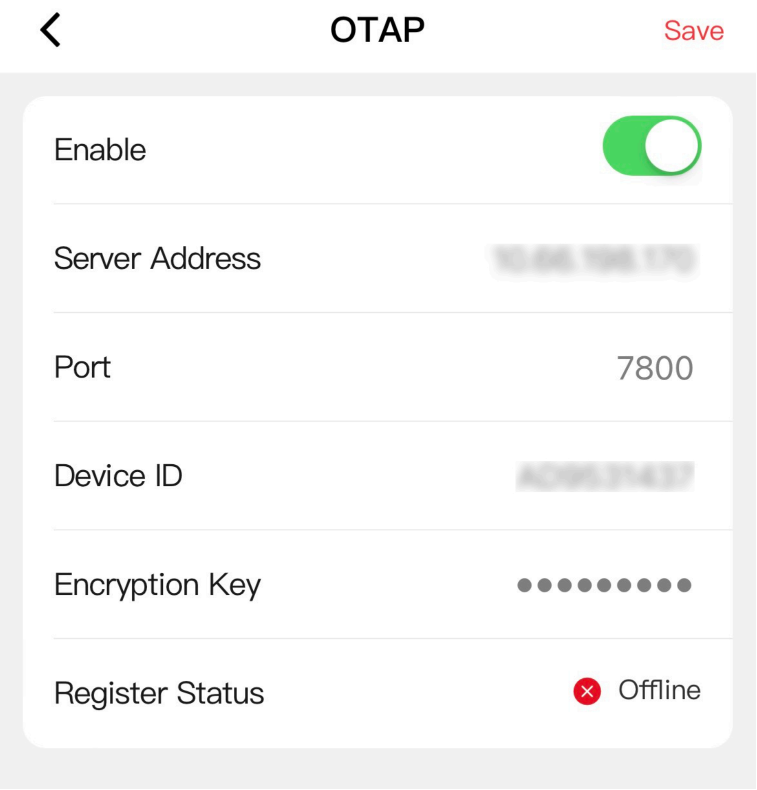
4. You can view **Register Status** and **Binding Status**.
5. Tap **Refresh** to view the latest register status.
6. You can tap **Bind An Account → View QR Code** , scan the QR code to bind an acount.
7. Tap **Save** to enable the settings.

Set OTAP Parameters

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. Tap ≡ **→ Device Access → OTAP** .



Enable

Server Address [redacted]

Port 7800

Device ID [redacted]

Encryption Key ●●●●●●●●●

Register Status ☒ Offline

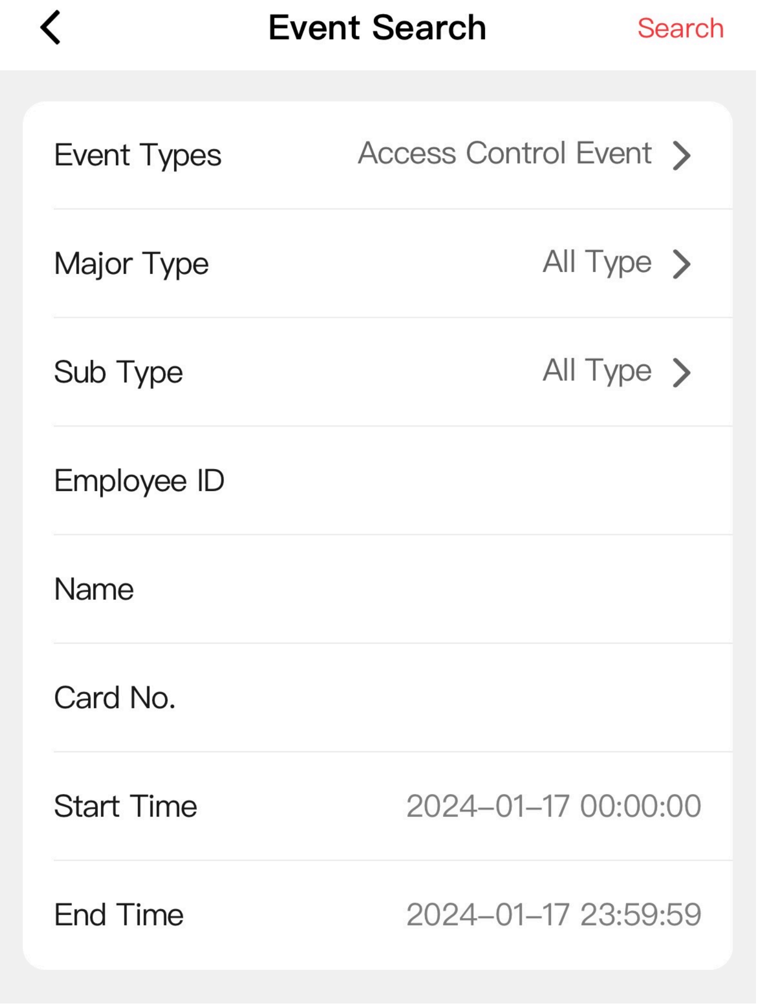
Figure 9-6 OTAP

2. Slide to **Enable**.
3. Set server address, port, device ID and encryption key.

4. Tap **Save**.
5. Refresh the page or reboot the device, and you can view the **Register Status**. Tap **Test** to test the register status.

9.3.8 Event Search

Tap ≡ → **Event Search** .



Event Search

Search

Event Types: Access Control Event

Major Type: All Type

Sub Type: All Type

Employee ID

Name

Card No.

Start Time: 2024–01–17 00:00:00

End Time: 2024–01–17 23:59:59

Figure 9-7 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.

9.3.9 Set Audio

Set the device volume.

Steps

1. Tap ≡ → **Audio** to enter the settings page.
2. You can adjust the device output volume according to your actual needs.
3. You can enable voice prompt according to your actual needs.

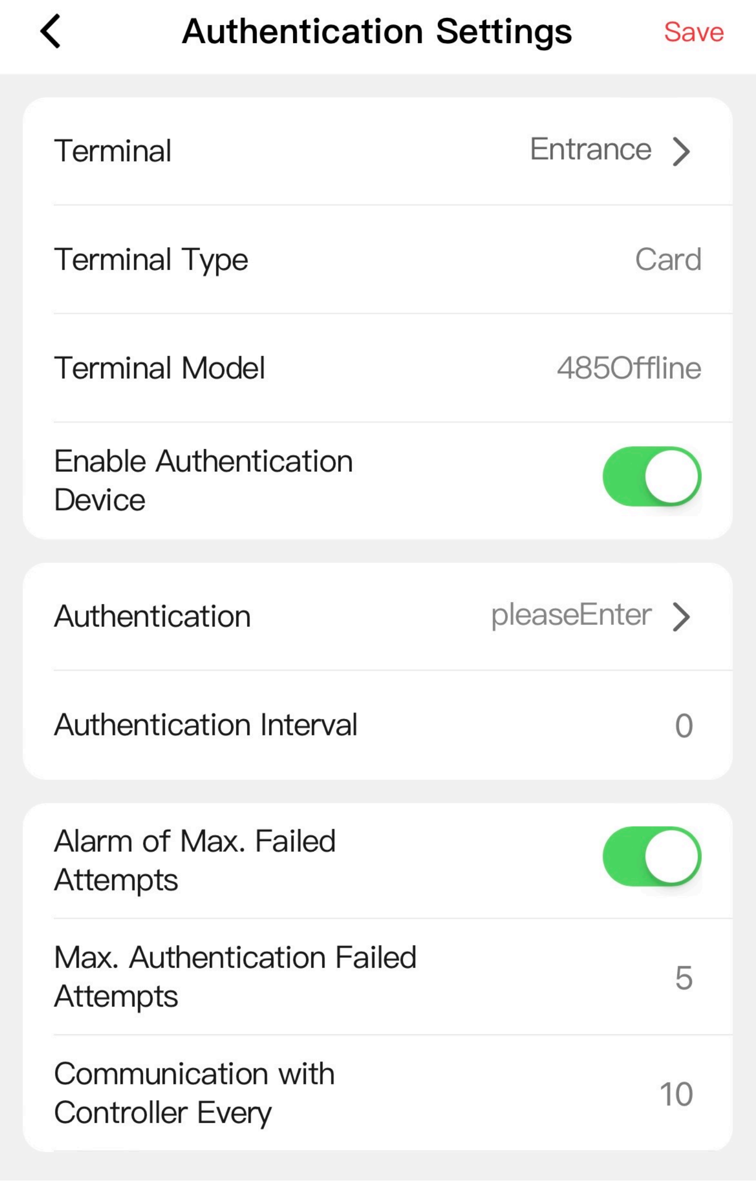
9.3.10 Access Control Settings

Set Authentication Parameters

Set authentication parameters.

Steps

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



Authentication Settings

Save

Terminal	Entrance >
Terminal Type	Card
Terminal Model	485Offline
Enable Authentication Device	●
Authentication	pleaseEnter >
Authentication Interval	0
Alarm of Max. Failed Attempts	●
Max. Authentication Failed Attempts	5
Communication with Controller Every	10

Figure 9-8 Authentication Settings

2. Tap **Save** after configuration.

Terminal

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

Terminal Type/Model

You can view the current terminal type and model.

Enable Authentication Device

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

Authentication

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

Authentication Interval

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

Note

The configuration range is 0 to 255 s.

Alarm of Max. Failed Attempts

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

Note

The configuration range is 1 to 10.

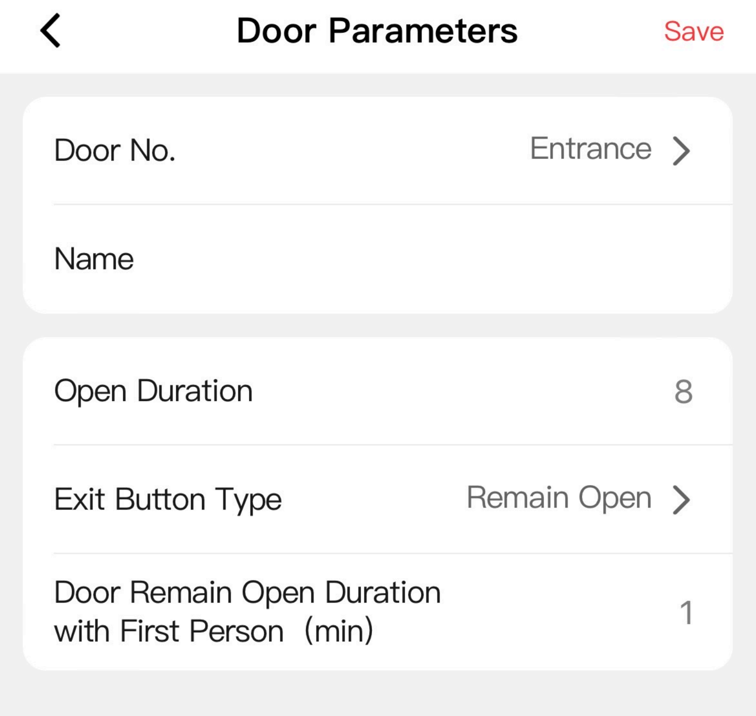
Communication with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Set Door Parameters

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

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



Door No. Entrance

Name

Open Duration 8

Exit Button Type Remain Open

Door Remain Open Duration with First Person (min) 1

Figure 9-9 Door Parameters

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

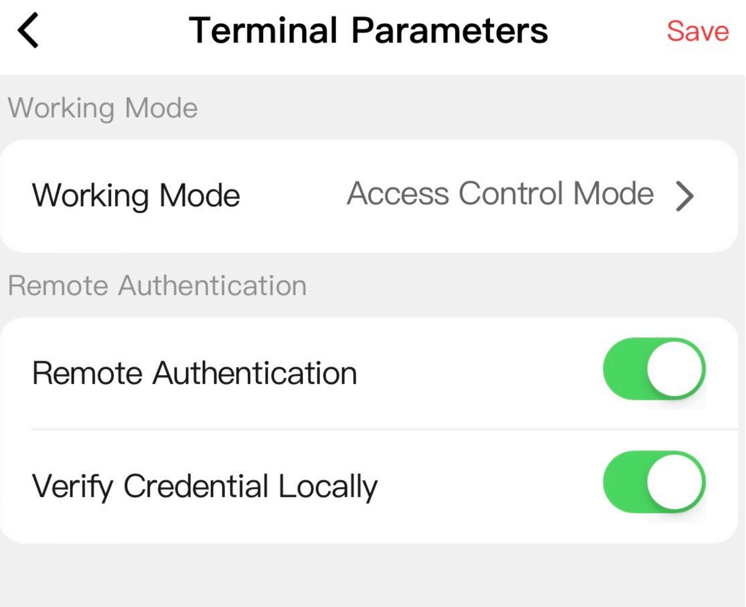
Configure **Door Remain Open Duration with First Person**. The mode is applicable for the passing of groups of persons, such as visitors entering the scenic spots. After the set person passes through, the door will open for a set time and other persons can pass through without authentication.

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

Terminal Settings

Set the working mode.

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



Terminal Parameters

Save

Working Mode

Working Mode: Access Control Mode

Remote Authentication

Remote Authentication: On

Verify Credential Locally: On

Figure 9-10 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.

Remote Authentication

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

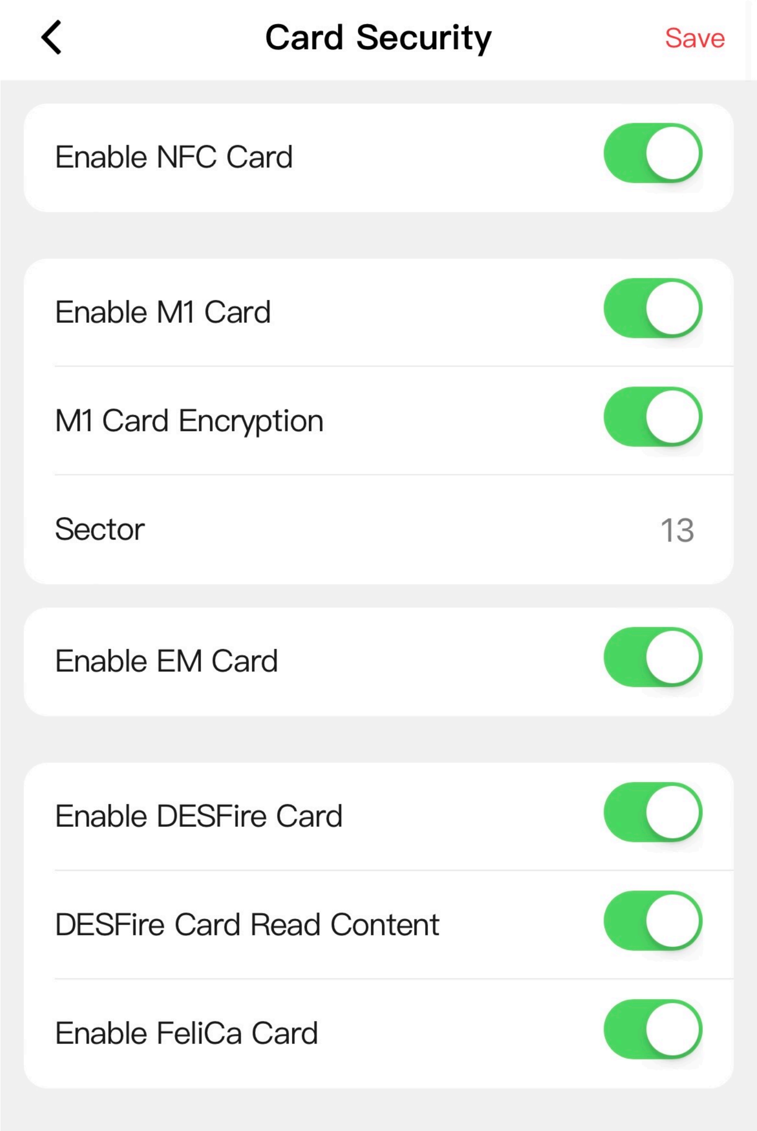
Verify Credential Locally

The device will only verify the person's permission without the schedule template, etc.

Set Card Security

Configure cards for the device.

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



Card Security

Enable NFC Card ●

Enable M1 Card ●

M1 Card Encryption ●

Sector 13

Enable EM Card ●

Enable DESFire Card ●

DESFire Card Read Content ●

Enable FeliCa Card ●

Figure 9-11 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.

9.3.11 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.

9.3.12 View Open Source Software License

Tap ≡ → **Open Source Software Licenses** to view the device license.

9.3.13 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 Other Platforms to Configure

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

iVMS-4200 Client Software

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

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

HikCentral Access Control (HCAC)

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

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

Appendix A. 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.

Appendix B. DIP Switch

B.1 DIP Switch Description

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

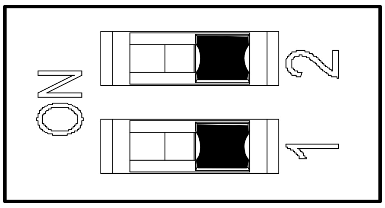
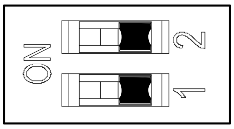
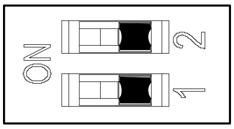
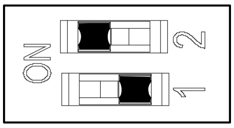


Figure B-1 DIP Switch

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

B.2 DIP Switch Corresponded Functions

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

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

Appendix C. Button Configuration Description

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

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions
2	keyfob Pairing Mode	1-Normal Mode 2-Pairing Mode **Note** By default, 1 will be displayed on the display screen.
3	Passing Mode	1-Both sides under control **Note** By default, 1 will be displayed on the display screen. 2-Entrance under control; exit prohibited 3-Entrance under control; exit free 4-Both sides free 5-Entrance free; exit under control 6-Entrance free; exit prohibited 7-Both sides prohibited 8-Entrance prohibited; exit under control 9-Entrance prohibited; exit free
4	Memory Mode	1-Disable 2-Enable **Note** By default, 2 will be displayed on the display screen.
9	Enter Duration	5-5s， 6-6s， 7-7s, ..., 60-60s

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions
		Note By default, 5 will be displayed on the display screen.
10	Exit Duration	5-5s， 6-6s， 7-7s, ..., 60-60s **Note** By default, 5 will be displayed on the display screen.
39	Brightness of Light	0-0， 1-1， 2-2, … , 10-10 **Note** By default, 6 will be displayed on the display screen.
42	Clearing People Counting	1-Default 2-Enable **Note** By default, 1 will be displayed on the display screen.
43	Fire Protection Type	1-Remain Closed 2-Remain Open **Note** By default, 2 will be displayed on the display screen.
99	Restore to Default	1-Default 2-Enable **Note** By default, 1 will be displayed on the display screen.

Appendix D. Event and Alarm Type

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

Appendix E. Table of Audio Index Related Content

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

Appendix F. Error Code Description

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

Error Reason	Code	Error Reason	Code
Main Optional Board Offline (If the board is not installed, the error code of "49" will appear but the device functions normally)	49	Sub Optional Board Offline	59

See Far, Go Further