



## **DS-K3B631X Series Swing Barrier**

## Legal Information

### About this Document

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

### About this Product

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



### Acknowledgment of Intellectual Property Rights

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

### LEGAL DISCLAIMER

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

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

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

### **Data Protection**

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

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

## Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

|                                                                                   |                                                                                           |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
|  |          |
| <b>Dangers:</b> Follow these safeguards to prevent serious injury or death.       | <b>Cautions:</b> 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.
- ⚡ 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 seashores 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.

## Available Models

| Product Name  | Model        | Description     |
|---------------|--------------|-----------------|
| Swing Barrier | DS-K3B631X-L | Left Pedestal   |
|               | DS-K3B631X-M | Middle Pedestal |
|               | DS-K3B631X-R | Right Pedestal  |

# Contents

|                                                               |           |
|---------------------------------------------------------------|-----------|
| <b>Chapter 1 Application Scenarios .....</b>                  | <b>1</b>  |
| <b>Chapter 2 Overview .....</b>                               | <b>2</b>  |
| 2.1 Introduction .....                                        | 2         |
| 2.2 Main Features .....                                       | 2         |
| <b>Chapter 3 Light Introduction .....</b>                     | <b>4</b>  |
| 3.1 Light Description .....                                   | 4         |
| 3.2 Lane Status Indicator Board DIP Switch Description .....  | 5         |
| <b>Chapter 4 System Wiring .....</b>                          | <b>8</b>  |
| <b>Chapter 5 Install Pedestals .....</b>                      | <b>10</b> |
| <b>Chapter 6 General Wiring .....</b>                         | <b>12</b> |
| 6.1 Components Introduction .....                             | 12        |
| 6.2 Serial Port Introduction .....                            | 14        |
| 6.3 Wiring .....                                              | 16        |
| 6.4 Terminal Description .....                                | 16        |
| 6.4.1 General Wiring .....                                    | 16        |
| 6.4.2 Main Control Board Terminal Description .....           | 17        |
| 6.4.3 Sub Control Board Terminal Description .....            | 18        |
| 6.4.4 Access Board Terminal Description .....                 | 19        |
| 6.4.5 Main Optional Board Terminal Description .....          | 20        |
| 6.4.6 Sub Optional Board Terminal Description .....           | 21        |
| 6.4.7 Card Reader Board Terminal Description (Optional) ..... | 21        |
| 6.4.8 Upper IR Adaptor Board Terminal Description .....       | 23        |
| 6.4.9 Lower IR Adaptor Board Terminal Description .....       | 24        |
| 6.4.10 RS-485 Wiring .....                                    | 24        |
| 6.4.11 RS-232 Wiring .....                                    | 25        |
| 6.4.12 Alarm Input Wiring .....                               | 25        |

|                                                         |           |
|---------------------------------------------------------|-----------|
| 6.4.13 Exit Button Wiring .....                         | 26        |
| <b>Chapter 7 Device Settings .....</b>                  | <b>28</b> |
| 7.1 Configuration via Button .....                      | 28        |
| 7.2 Study Mode Settings .....                           | 31        |
| 7.2.1 Set Study Mode via Button .....                   | 31        |
| 7.2.2 Set Study Mode via DIP Switch (Optional) .....    | 31        |
| 7.3 Keyfob Pairing .....                                | 33        |
| 7.3.1 Pair Keyfob via Button .....                      | 33        |
| 7.3.2 Pair Keyfob via DIP Switch (Optional) .....       | 34        |
| 7.4 Initialize Device .....                             | 35        |
| <b>Chapter 8 Activation .....</b>                       | <b>36</b> |
| 8.1 Activate via Web Browser .....                      | 36        |
| 8.2 Activate via Mobile Web .....                       | 36        |
| 8.3 Activate via SADP .....                             | 37        |
| 8.4 Activate Device via iVMS-4200 Client Software ..... | 38        |
| <b>Chapter 9 Quick Operation via Web Browser .....</b>  | <b>40</b> |
| 9.1 Time Settings .....                                 | 40        |
| <b>Chapter 10 Operation via Web Browser .....</b>       | <b>41</b> |
| 10.1 Login .....                                        | 41        |
| 10.2 Live View .....                                    | 41        |
| 10.3 Person Management .....                            | 42        |
| 10.4 Search Event .....                                 | 43        |
| 10.5 Configuration .....                                | 45        |
| 10.5.1 View Device Information .....                    | 45        |
| 10.5.2 Set Time .....                                   | 45        |
| 10.5.3 Set DST .....                                    | 46        |
| 10.5.4 Change Administrator's Password .....            | 46        |
| 10.5.5 Online Users .....                               | 46        |

|                                                                     |           |
|---------------------------------------------------------------------|-----------|
| 10.5.6 View Device Arming/Disarming Information .....               | 47        |
| 10.5.7 Network Settings .....                                       | 47        |
| 10.5.8 Set Audio Parameters .....                                   | 51        |
| 10.5.9 Event Linkage .....                                          | 51        |
| 10.5.10 Access Control Settings .....                               | 53        |
| 10.5.11 Turnstile .....                                             | 57        |
| 10.5.12 Card Settings .....                                         | 61        |
| 10.5.13 Set Privacy Parameters .....                                | 62        |
| 10.5.14 Customize Audio Content .....                               | 62        |
| 10.5.15 Upgrade and Maintenance .....                               | 64        |
| 10.5.16 Device Debugging .....                                      | 65        |
| 10.5.17 Component Status .....                                      | 66        |
| 10.5.18 Log Query .....                                             | 67        |
| 10.5.19 Certificate Management .....                                | 67        |
| <b>Chapter 11 Configure the Device via the Mobile Browser .....</b> | <b>69</b> |
| 11.1 Login .....                                                    | 69        |
| 11.2 Overview .....                                                 | 69        |
| 11.3 Configuration .....                                            | 72        |
| 11.3.1 Turnstile Basic Parameters .....                             | 72        |
| 11.3.2 Person Management .....                                      | 73        |
| 11.3.3 Keyfob Settings .....                                        | 75        |
| 11.3.4 Light Settings .....                                         | 76        |
| 11.3.5 View Device Basic Information .....                          | 78        |
| 11.3.6 Time Settings .....                                          | 79        |
| 11.3.7 User Management .....                                        | 80        |
| 11.3.8 Network .....                                                | 80        |
| 11.3.9 Event Search .....                                           | 84        |
| 11.3.10 Set Audio .....                                             | 85        |

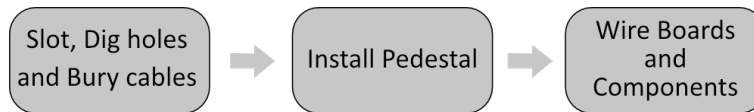
|                                                                       |           |
|-----------------------------------------------------------------------|-----------|
| 11.3.11 Access Control Settings .....                                 | 86        |
| 11.3.12 Upgrade and Maintenance .....                                 | 91        |
| 11.3.13 Device Debugging .....                                        | 92        |
| 11.3.14 View Open Source Software License on Mobile Web .....         | 92        |
| 11.3.15 Log Out .....                                                 | 92        |
| <b>Chapter 12 Client Software Configuration .....</b>                 | <b>93</b> |
| 12.1 Configuration Flow of Client Software .....                      | 93        |
| 12.2 Device Management .....                                          | 94        |
| 12.2.1 Add Device .....                                               | 94        |
| 12.2.2 Reset Device Password .....                                    | 96        |
| 12.2.3 Manage Added Devices .....                                     | 97        |
| 12.3 Group Management .....                                           | 98        |
| 12.3.1 Add Group .....                                                | 98        |
| 12.3.2 Import Resources to Group .....                                | 98        |
| 12.4 Person Management .....                                          | 99        |
| 12.4.1 Add Organization .....                                         | 99        |
| 12.4.2 Import and Export Person Identify Information .....            | 100       |
| 12.4.3 Get Person Information from Access Control Device .....        | 101       |
| 12.4.4 Issue Cards to Persons in Batch .....                          | 102       |
| 12.4.5 Report Card Loss .....                                         | 102       |
| 12.4.6 Set Card Issuing Parameters .....                              | 103       |
| 12.5 Configure Schedule and Template .....                            | 104       |
| 12.5.1 Add Holiday .....                                              | 104       |
| 12.5.2 Add Template .....                                             | 105       |
| 12.6 Set Access Group to Assign Access Authorization to Persons ..... | 106       |
| 12.7 Configure Advanced Functions .....                               | 108       |
| 12.7.1 Configure Device Parameters .....                              | 109       |
| 12.7.2 Configure Device Parameters .....                              | 113       |

|                                                               |            |
|---------------------------------------------------------------|------------|
| 12.8 Door/Elevator Control .....                              | 115        |
| 12.8.1 Control Door Status .....                              | 115        |
| 12.8.2 Check Real-Time Access Records .....                   | 117        |
| <b>Appendix A. DIP Switch .....</b>                           | <b>118</b> |
| A.1 DIP Switch Description .....                              | 118        |
| A.2 DIP Switch Corresponded Functions .....                   | 118        |
| <b>Appendix B. Button Configuration Description .....</b>     | <b>119</b> |
| <b>Appendix C. Event and Alarm Type .....</b>                 | <b>131</b> |
| <b>Appendix D. Table of Audio Index Related Content .....</b> | <b>132</b> |
| <b>Appendix E. Error Code Description .....</b>               | <b>133</b> |

# Chapter 1 Application Scenarios

## Application Scenarios1

Application Scenarios: Install pedestals, and wire boards and optional accessories to control the systematic operation of components.

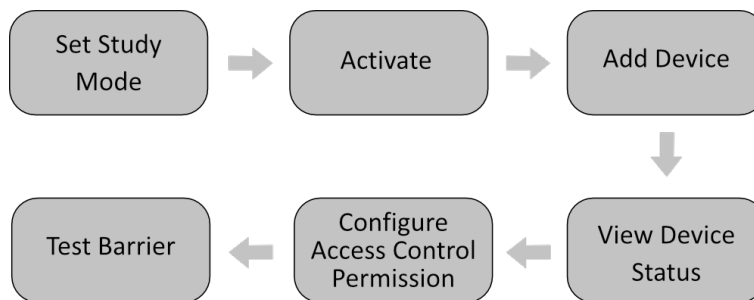


**Figure 1-1 Application Scenarios1**

For detailed operation methods, please refer to: **System Wiring** -- **Install Pedestals** -- **General Wiring**

## Application Scenarios2

Application Scenarios: After installing pedestals, power on and debug the device to ensure the normal operation of the device.

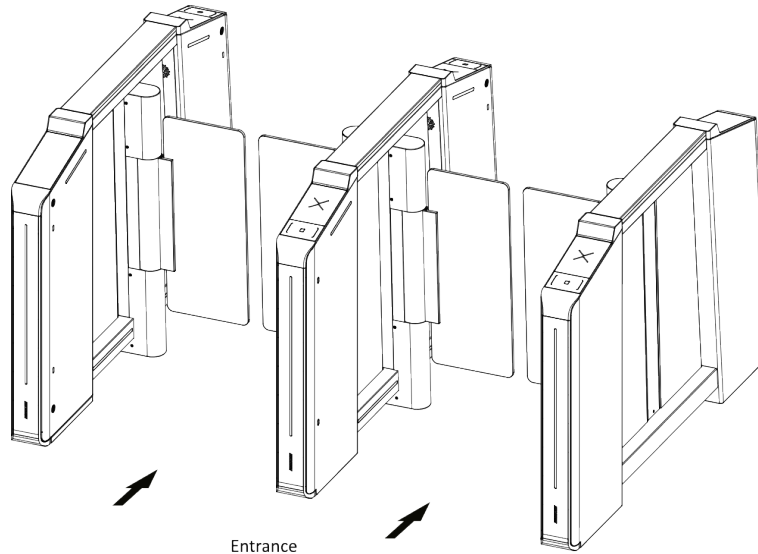


**Figure 1-2 Application Scenarios2**

For detailed operation methods, please refer to: **Study Mode Settings** -- **Activation** -- **Add Device** -- **Manage Added Devices** --

## Chapter 2 Overview

### 2.1 Introduction



The swing barrier with two barriers and 20 IR lights 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.

### 2.2 Main Features

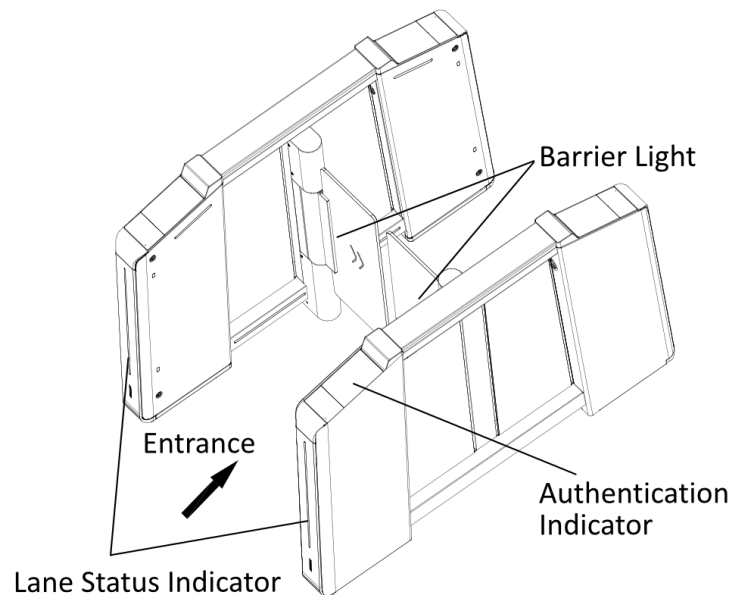
- 32-bit high-speed processor
- IP address conflict detection
- Remote control and management
- Online/offline operation
- Configuration via local operation, PC web and mobile web
- TCP/IP network communication
  - The communication data is specially encrypted to relieve the concern of privacy leak
- Person authentication
- Permissions validation and anti-tailgating
- Control mode, inductive mode, remaining open/closed mode and free passing mode selectable
- Bidirectional (Entering/Exiting) lane
  - The barrier opening and closing speed can be configured according to the visitor flow
- Single or multiple IR detector triggering
- Opens/Closes barrier according to the schedule template
- Cross controller anti-passback

- The barrier will be locked or stop working when people are nipped
- Anti-forced-accessing  
The barrier will be locked automatically without open-barrier signal. It can bear the force of up to 120 Nm
- Self-detection, Self-diagnostics, and automatic alarm
- Audible and visual alarm will be triggered when detecting intrusion, tailgating, reverse passing, and climbing over barrier
- Barrier is in free status when powered down
- Fire alarm passing  
When the fire alarm is triggered, the barrier will be open automatically for emergency evacuation
- Valid passing duration settings  
System will cancel the passing permission if a person does not pass through the lane within the valid passing duration
- Custom broadcasting content
- LED indicates the entrance/exit and passing status
- White indicators for card and QR code authentication;  
Red and green authentication indicators;  
Adjustable brightness and color of lane status indicator
- IR emergency mode and Custom Anti-pinch for Door Closing

## Chapter 3 Light Introduction

Description of light and how to set light via DIP switch.

### 3.1 Light Description



**Figure 3-1 Light Position**

#### Lane Status Indicator

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



#### Note

- When the device detects people within 2 m, the lane status indicator will be flashing.
  - Light stays blue: free-passing
  - Light stays green: authenticated passing
  - Light stays red: passing prohibited
- 

#### 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.

## Authentication Indicator

- The authentication indicator 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.

## 3.2 Lane Status Indicator Board DIP Switch Description

Configure the DIP switch address of lane status indicator.

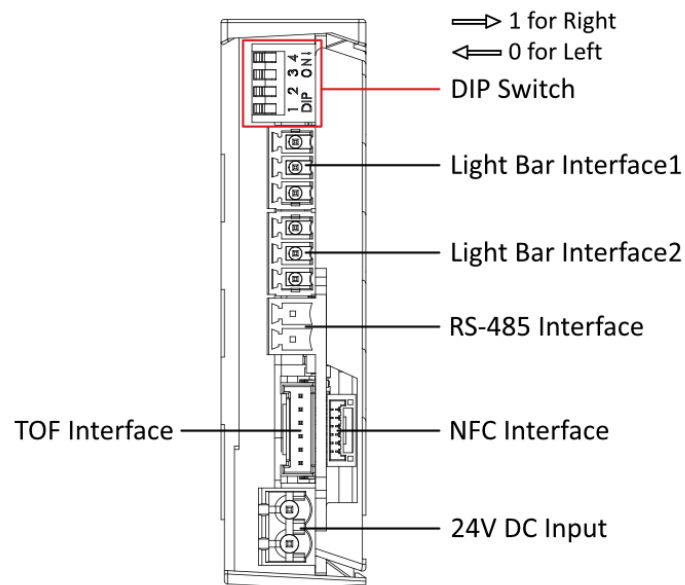


Figure 3-2 Lane Status Indicator Board DIP Switch

Table 3-1 Lane Status Indicator Board DIP Switch Description

| Position | Address | Value (Start from Left) |      |
|----------|---------|-------------------------|------|
| 0        | 65      | 0                       | 0000 |
| 1        | 81      | 1                       | 1000 |
| 2        | 97      | 10                      | 0100 |
| 3        | 113     | 11                      | 1100 |
| 4        | 129     | 100                     | 0010 |

| Position | Address | Value (Start from Left) |      |
|----------|---------|-------------------------|------|
| 5        | 130     | 101                     | 1010 |
| 6        | 131     | 110                     | 0110 |
| 7        | 132     | 111                     | 1110 |
| 8        | 133     | 1000                    | 0001 |
| 9        | 134     | 1001                    | 1001 |
| 10       | 135     | 1010                    | 0101 |
| 11       | 136     | 1011                    | 1101 |
| 12       | 137     | 1100                    | 0011 |
| 13       | 138     | 1101                    | 1011 |
| 14       | 139     | 1110                    | 0111 |
| 15       | 140     | 1111                    | 1111 |

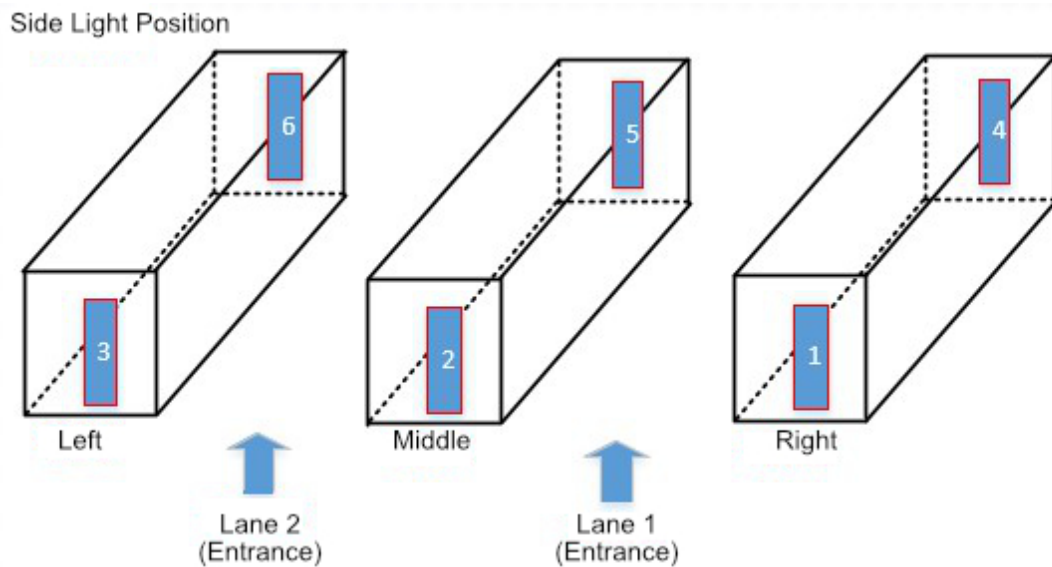


Figure 3-3 Lane Status Indicator Position

### Single-Lane Scenario

In single-lane scenario, the lane status indicators are located at the position of NO. 1, 3, 4, 6. Lane status indicator No. 1 is near the main lane control board.

**Table 3-2 Single-Lane DIP Switch Description**

| Position | Address | Value |
|----------|---------|-------|
| No. 1    | 65      | 0000  |
| No. 3    | 113     | 1100  |
| No. 4    | 81      | 1000  |
| No. 6    | 97      | 0100  |

**Dual-Lane Scenario**

**Table 3-3 Dual-Lane DIP Switch Description**

| Position | Address | Value |
|----------|---------|-------|
| No. 1    | 65      | 0000  |
| No. 2    | 65      | 0000  |
| No. 3    | 113     | 1100  |
| No. 4    | 81      | 1000  |
| No. 5    | 97      | 0100  |
| No. 6    | 97      | 0100  |

## Chapter 4 System Wiring

The preparation before installation and general wiring.

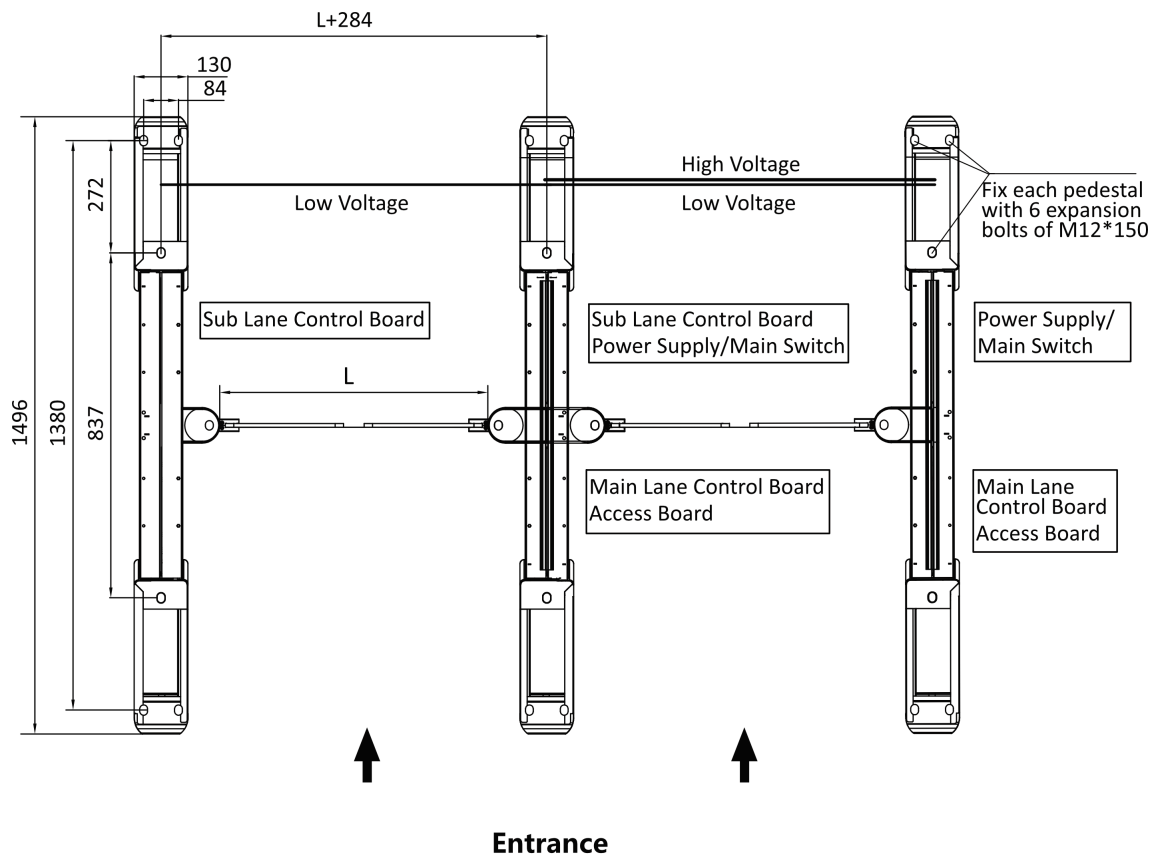
### Steps

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  $L+284$  mm.  $L$  represents the lane width.

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



**Figure 4-1 Hole Position Diagram**

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



### **Note**

- High voltage: AC power input  
Low voltage: network cable (CAT5E or CAT6), interconnecting cable (communication cable and 24 V power cable)
  - The suggested inner diameter of the low voltage conduit is larger than 30 mm. If high-power authentication devices need to be installed in the left lane, this conduit needs to be widened.
  - If there are no pre-buried high voltage cables, it is necessary to bury high voltage cable conduit. If you want to bury both of the high voltage cable and the interconnecting 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.
-

## Chapter 5 Install Pedestals

### Before You Start

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

### Steps

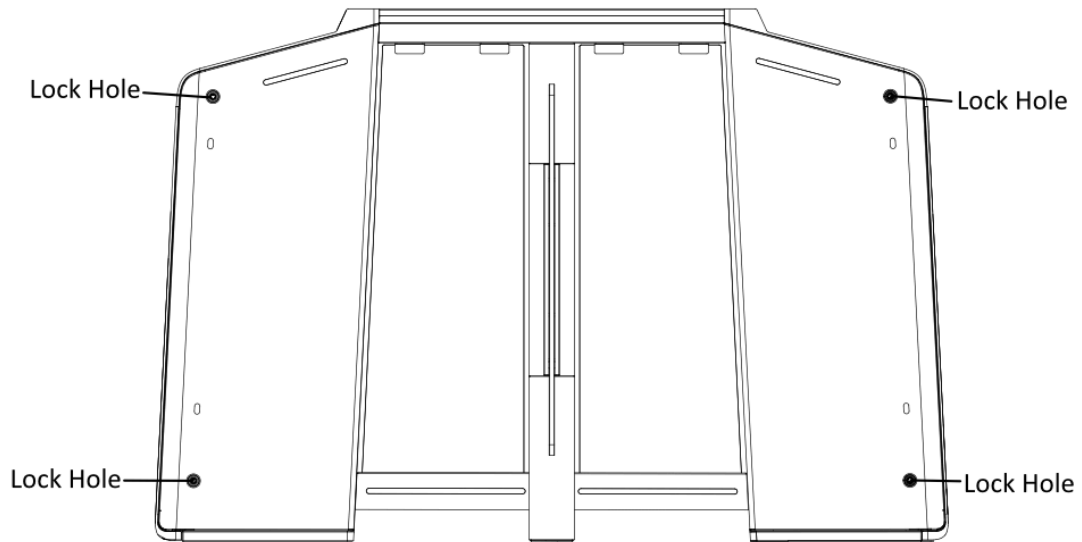
---



#### Note

- The device should be installed on the concrete surface or other flat non-flammable surfaces.
  - 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 60 mm.
- 

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Place the pedestals properly on the base, and open the maintenance door with the key.



**Figure 5-1 Lock Holes**

- 3.** Secure the pedestals with expansion bolts.
- 4.** Install the maintenance door back.

## Chapter 6 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.
- 

### 6.1 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 240 VAC, 50 to 60 Hz.

---

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

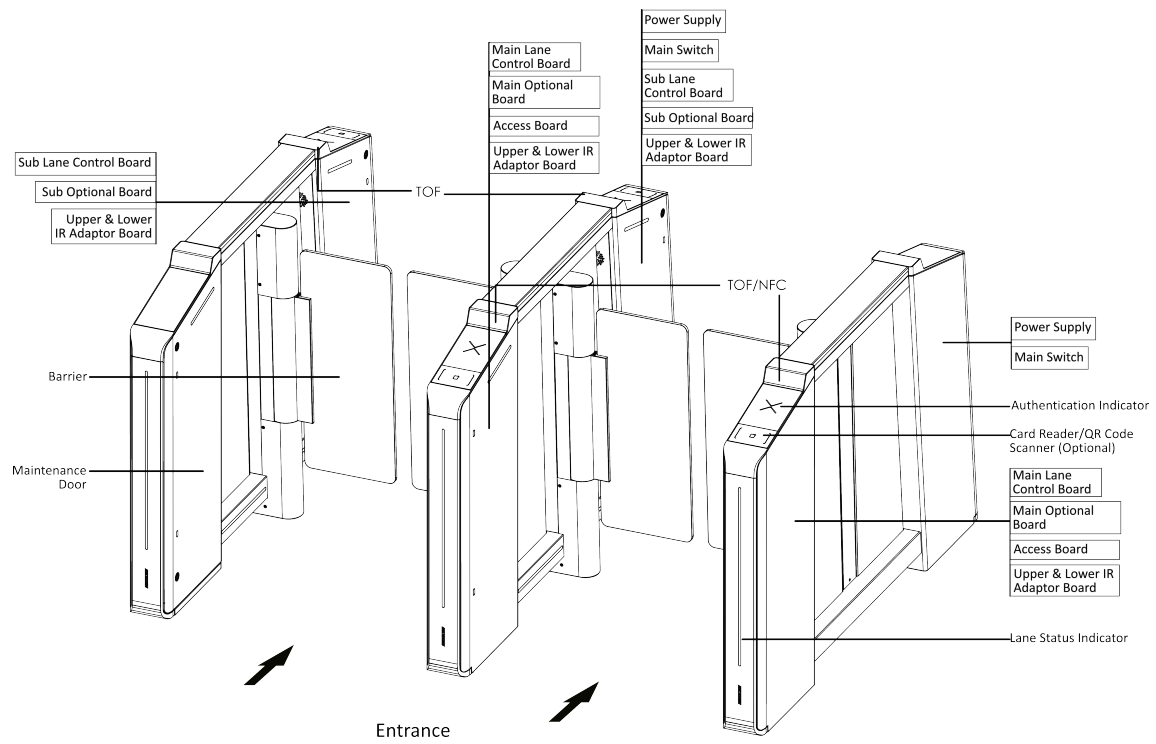
---

### Note

The diagram is for reference only.

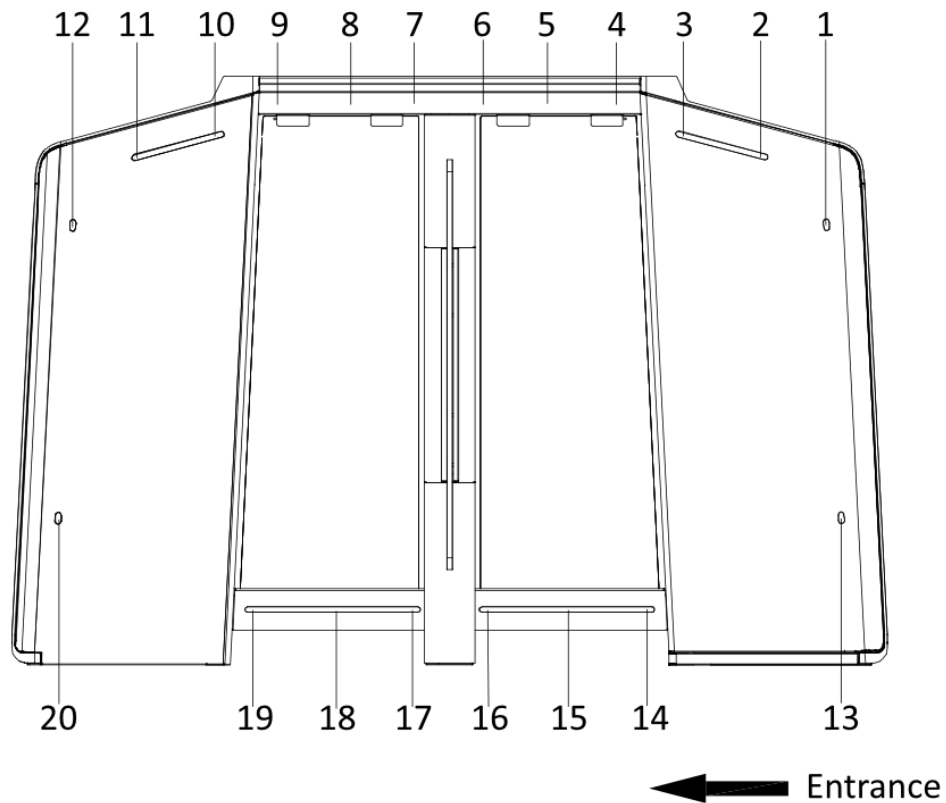
---

## DS-K3B631X Series Swing Barrier



**Figure 6-1 Components**

The picture displayed below describes the IR module position on the pedestal.



**Figure 6-2 IR Module Position**

## **6.2 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.

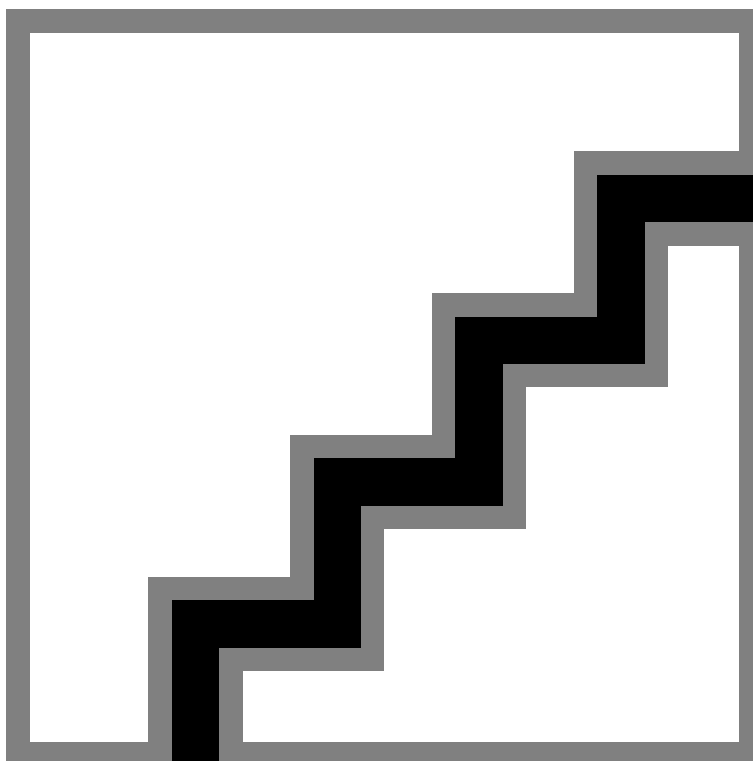


Figure 6-3 Serial Port

| Serial Port No. | Communication Method and Board Location                          | Peripheral Type            |
|-----------------|------------------------------------------------------------------|----------------------------|
| Port1           | RS-232A<br><b><u>Access Board Terminal Description</u></b>       | QR Code Scanner (Entrance) |
| Port 2          | RS-232B<br><b><u>Sub Optional Board Terminal Description</u></b> | QR Code Scanner (Exit)     |
| Port 3          | RS-232C<br><b><u>Sub Optional Board Terminal Description</u></b> | Card Receiver              |
| Port 4          | RS-485D<br><b><u>Sub Optional Board Terminal Description</u></b> | Card Reader (Exit)         |
| Port 5          | RS-485C                                                          | Card Reader (Entrance)     |

| Serial Port No. | Communication Method and Board Location         | Peripheral Type |
|-----------------|-------------------------------------------------|-----------------|
|                 | <u><i>Access Board Terminal Description</i></u> |                 |

## 6.3 Wiring

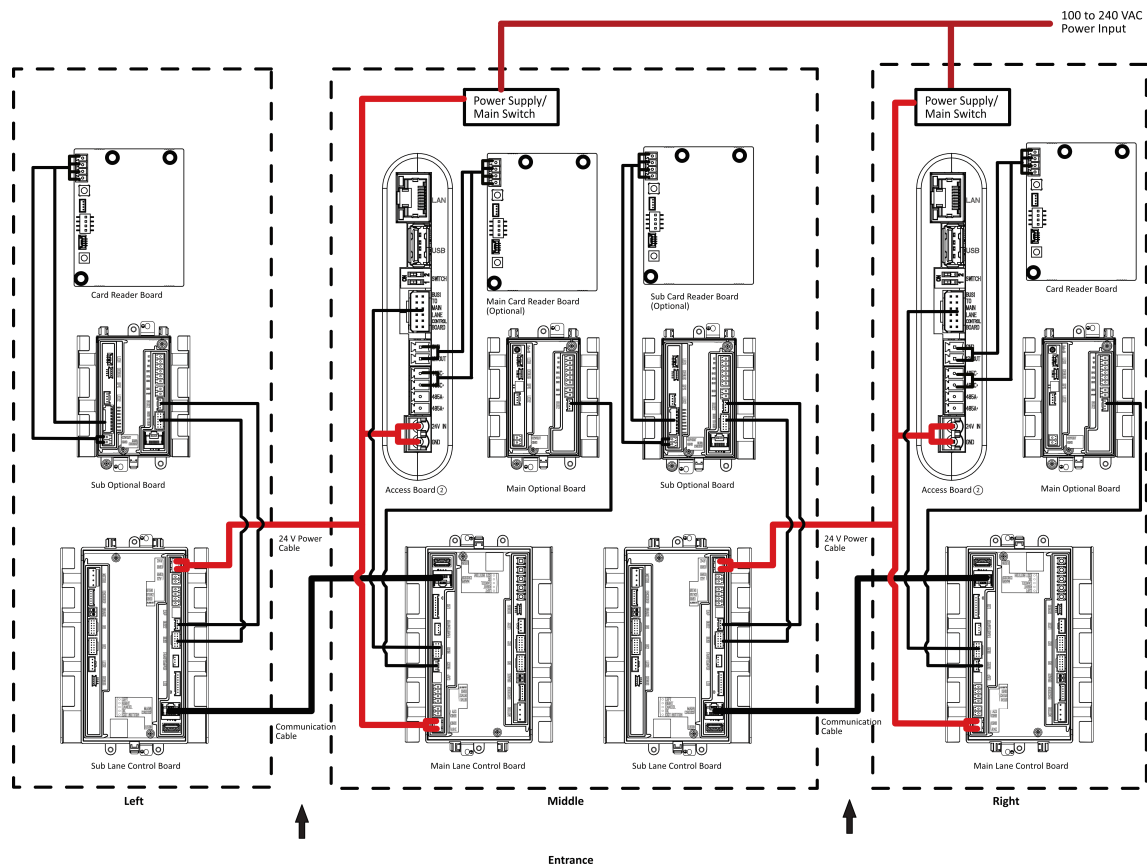
Scan the QR code to view the wiring guide video.



## 6.4 Terminal Description

### 6.4.1 General Wiring

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



**Figure 6-4 General Wiring**

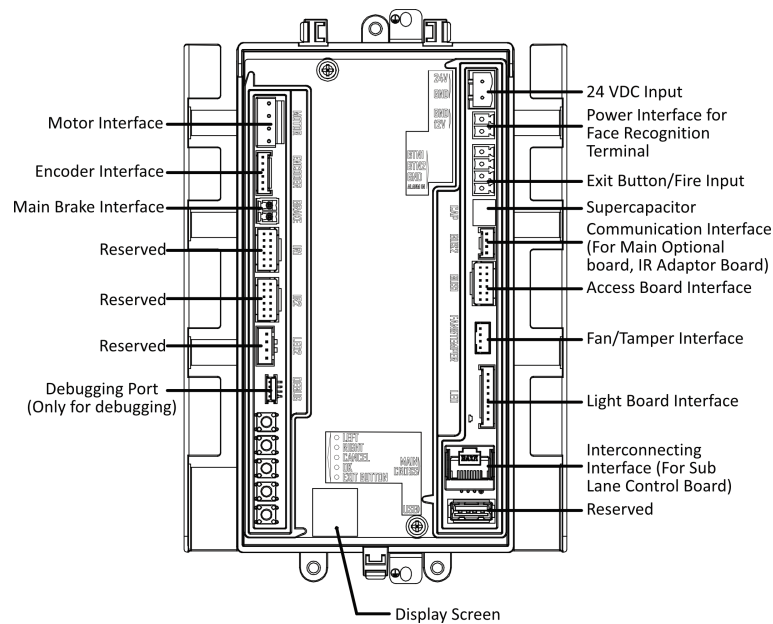
## Note

- 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.

## 6.4.2 Main Control Board Terminal Description

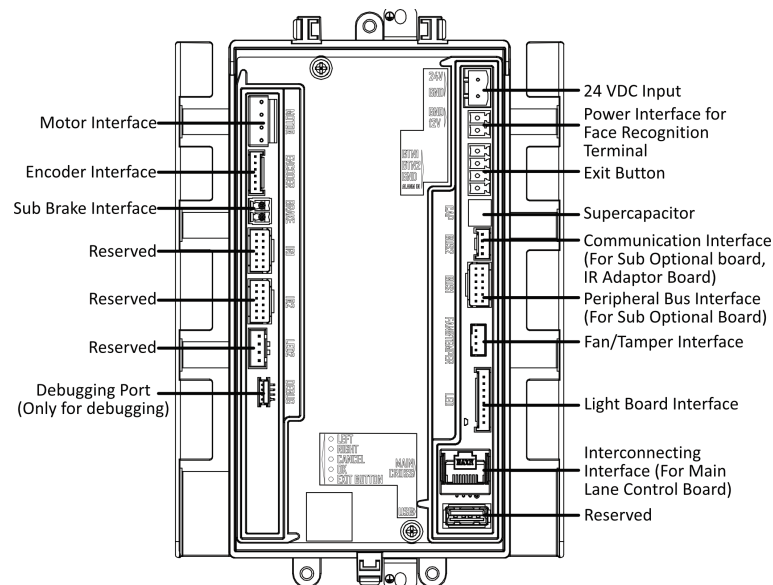
The picture displayed below is the main control board diagram.

## DS-K3B631X Series Swing Barrier



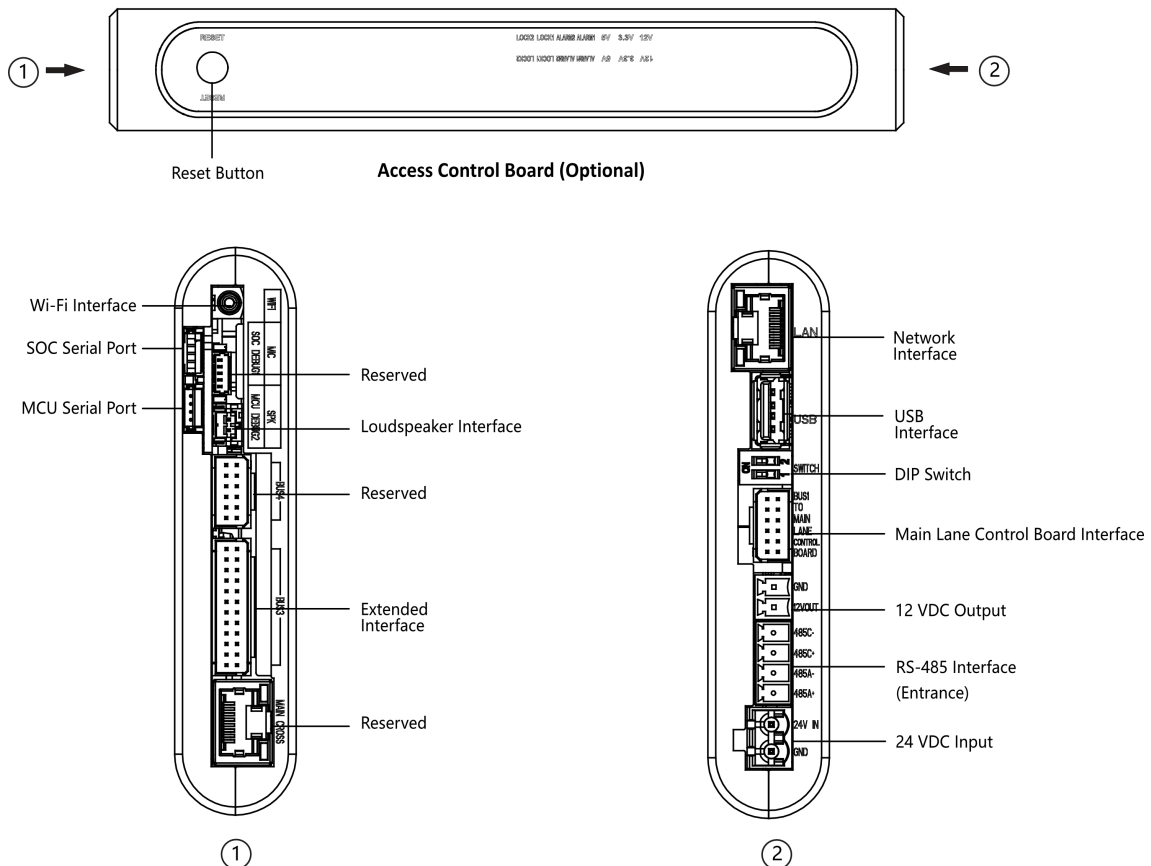
### 6.4.3 Sub Control Board Terminal Description

The picture displayed below is the sub control board diagram.



## 6.4.4 Access Board Terminal Description

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.

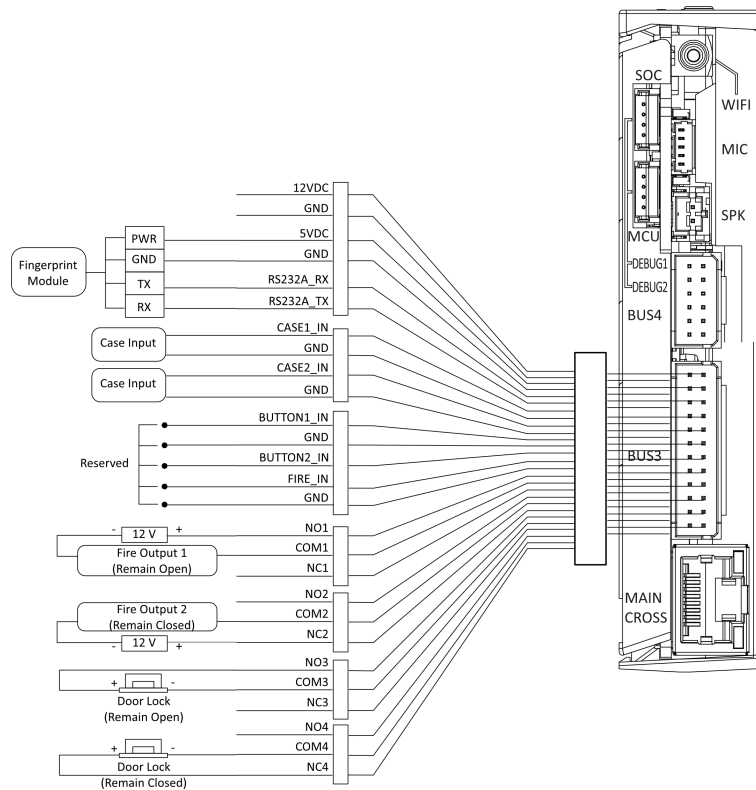


**Figure 6-5 Access Board**

### Note

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

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



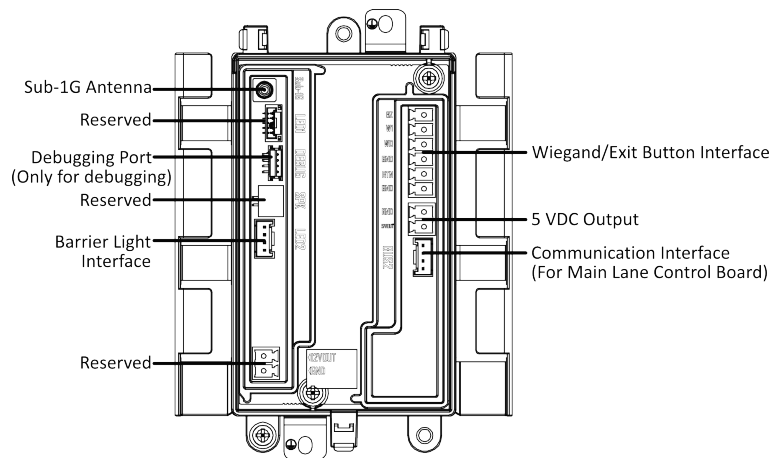
**Figure 6-6 Wiring Diagram of BUS3 Interface**

## Note

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

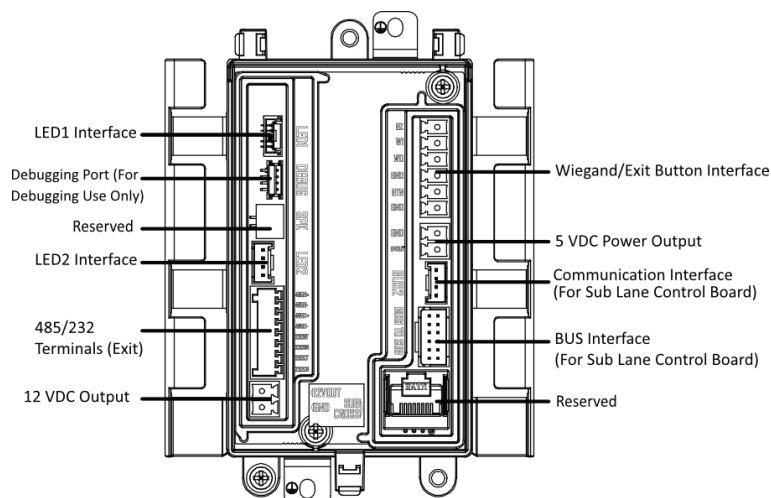
## 6.4.5 Main Optional Board Terminal Description

The main optional board contains the sub-1G antenna interface, lane control board interface, loudspeaker interface, LED interface, wiegand interface, 5 V power output and debugging port.



**Figure 6-7 Main Optional Board**

### 6.4.6 Sub Optional Board Terminal Description



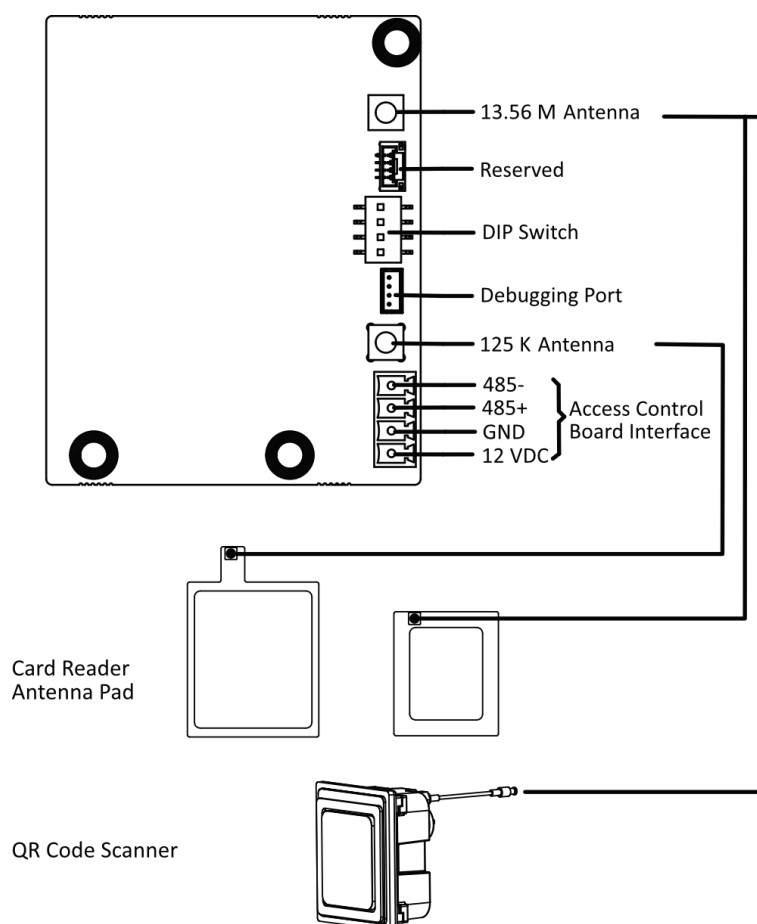
**Figure 6-8 Sub Optional Board Terminal**

#### Note

- RS-485D corresponds to serial port 4 on web and is for card reader connection by default.
- RS-232B corresponds to serial port 2 on web and is for QR code scanner connection by default.
- RS-232C corresponds to serial port 3 and is for card receiver by default.

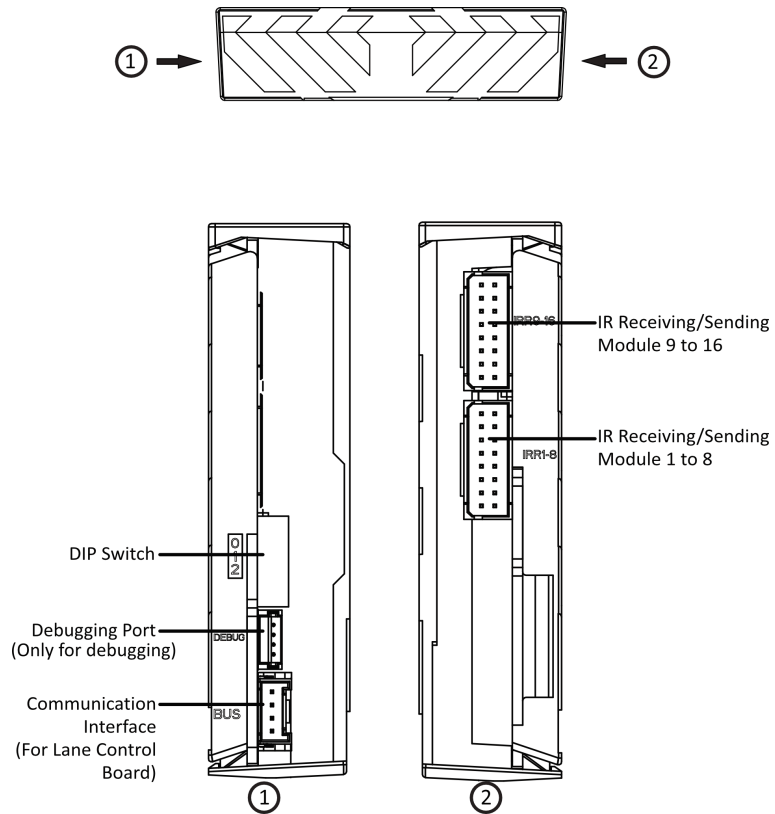
### 6.4.7 Card Reader Board Terminal Description (Optional)

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



**Figure 6-9 Card Reader Board**

#### 6.4.8 Upper IR Adaptor Board Terminal Description



**Figure 6-10 Upper IR Adaptor Board**

---

**Note**

Set DIP switch to the 1 position.

The communication interface of the IR adaptor board connects to the lane control board. IR receiving/sending interface connects to the IR module.

---

### 6.4.9 Lower IR Adaptor Board Terminal Description

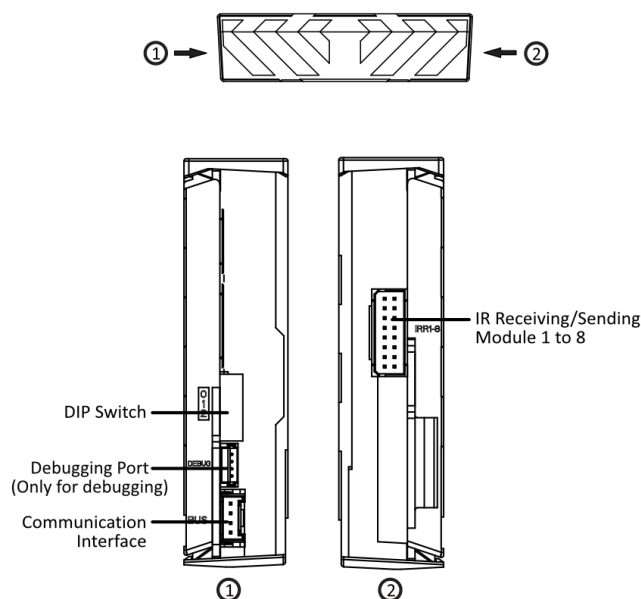


Figure 6-11 Lower IR Adaptor Board

#### Note

Set DIP switch to the 2 position.

The communication interface of the IR adaptor board connects to the lane control board. IR receiving/sending interface connects to the IR module.

### 6.4.10 RS-485 Wiring

The RS-485 interfaces on the access control board and sub extended interface 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

- There are 2 RS-485 interfaces on the access control board for entrance. Refer to **Access Board Terminal Description** for details.  
There are 2 RS-485 interfaces on the sub extended interface board for exit. Refer to **Sub Optional Board Terminal Description** for details.
- If connecting the RS-485 with a card reader, by default, the DIP switch of the card reader should be set as follows:

- For entrance, set the No.1 of the 4-digit DIP switch to ON side.
- For exit, set the No.3 of the 4-digit DIP switch to ON side.
- 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.

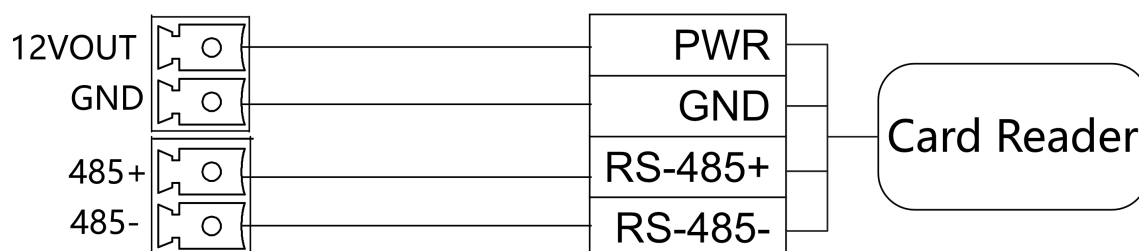


Figure 6-12 Wiring RS-485

### 6.4.11 RS-232 Wiring

#### Note

- There is 1 RS-232 interface on the extended interface of access control board, see [\*\*Access Board Terminal Description\*\*](#) . The RS-232A corresponds to UART 1 on web.
- There is 1 RS-232 interface on the sub extended interface board, see [\*\*Sub Optional Board Terminal Description\*\*](#) . The RS-232B corresponds to UART 2 on web. The RS-232C interface is reserved.

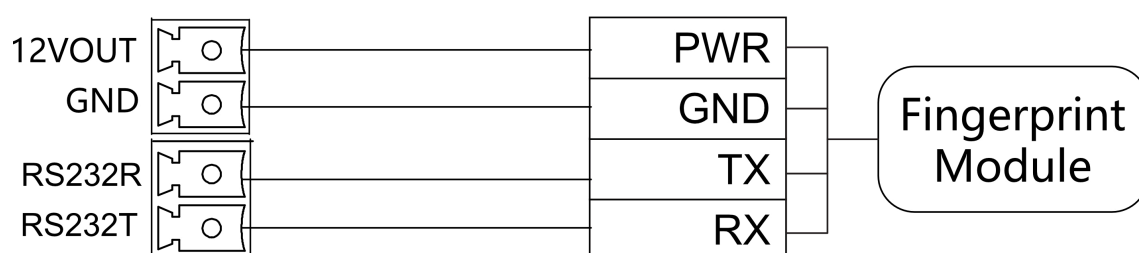


Figure 6-13 RS-232 Wiring

### 6.4.12 Alarm Input Wiring

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

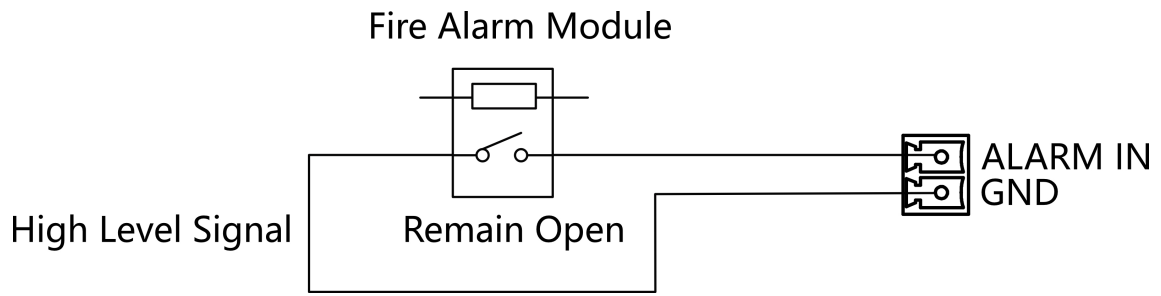


Figure 6-14 Remaining Open

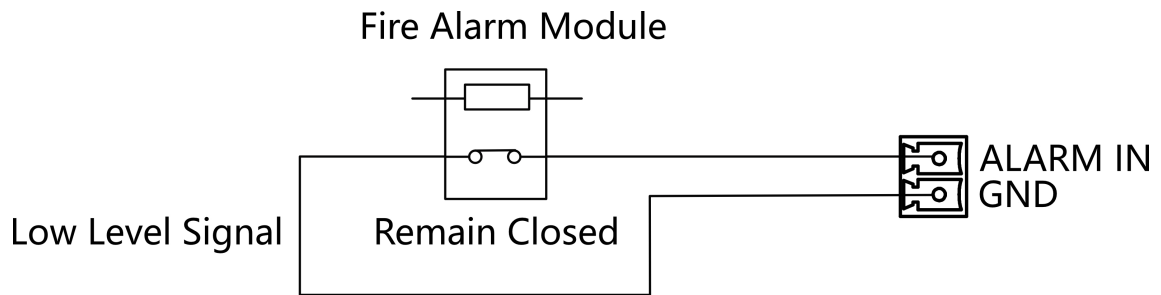


Figure 6-15 Remaining Closed

### 6.4.13 Exit Button Wiring

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

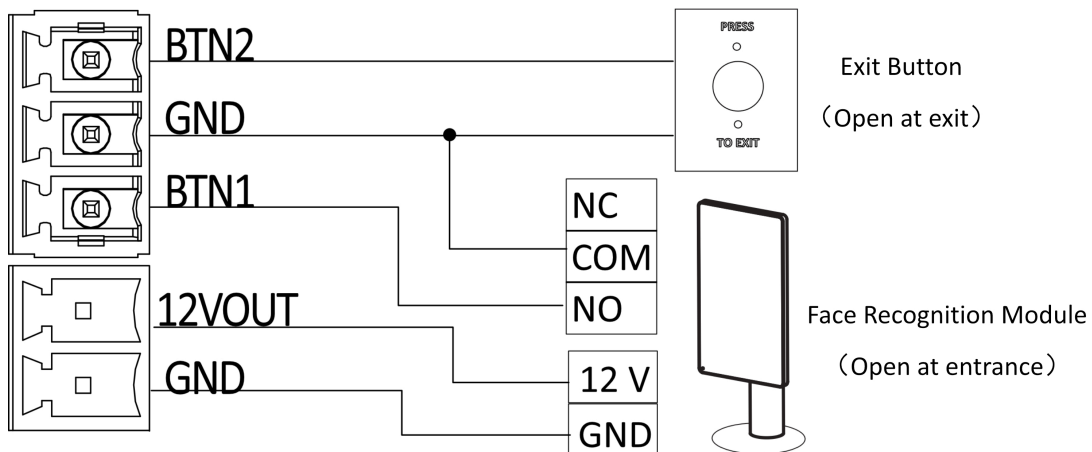


Figure 6-16 Exit Button Wiring

---

### **Note**

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

## Chapter 7 Device Settings

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

| Function          | Main Lane Control Board & Access Control Board & Loudspeaker (Connected to Access Control Board)                                                                                                                                                                                                                              |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Normal/Study Mode | <ol style="list-style-type: none"> <li>1. Configure via button (refer to <b><u>Set Study Mode via DIP Switch (Optional)</u></b> )</li> <li>2. Configure via DIP switch (refer to <b><u>Set Study Mode via DIP Switch (Optional)</u></b> )</li> <li>3. Configure via web (refer to <b><u>Device Debugging</u></b> )</li> </ol> |
| keyfob Pairing    | <ol style="list-style-type: none"> <li>1. Configure via button (refer to <b><u>Pair Keyfob via DIP Switch (Optional)</u></b> )</li> <li>2. Configure via DIP switch (refer to <b><u>Pair Keyfob via DIP Switch (Optional)</u></b> )</li> <li>3. Configure via web (refer to <b><u>keyfob</u></b> )</li> </ol>                 |
| Passing Mode      | Configure via button/web                                                                                                                                                                                                                                                                                                      |
| Memory Mode       | Configure via button/web                                                                                                                                                                                                                                                                                                      |
| Control Mode      | Configure via button/web                                                                                                                                                                                                                                                                                                      |
| Application Mode  | Configure via button                                                                                                                                                                                                                                                                                                          |

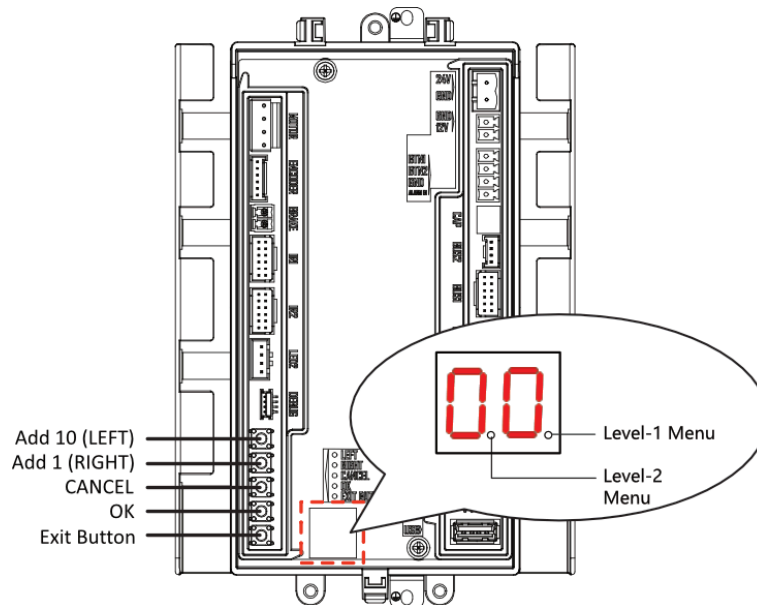


### Note

- Refer to **Button Configuration Description** for detailed information.
- You can set custom broadcasting context via web. For details, see **Customize Audio Content** .

### 7.1 Configuration via Button

### Button Description



**Figure 7-1 Button**

#### Exit Button

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

#### Parameter Configuration Button

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

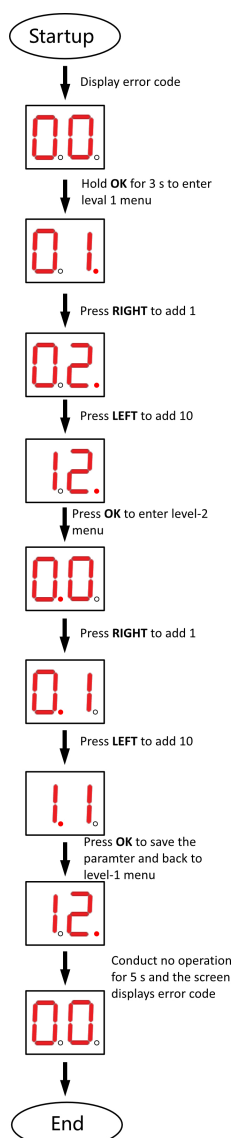


#### Note

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

### Button Configuration Procedure

Here takes setting intrusion duration to 12 s as example:



**Figure 7-2 Procedure**

**Steps:**

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

---

### Note

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

## 7.2 Study Mode Settings

Set the closed position of the device barrier.

### 7.2.1 Set Study Mode via Button

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

#### Steps

---

### Note

- If the device is equipped with access control board, you can set study mode via DIP switch on the access control board only.
  - For details about button's operation, see **Configuration via Button** .
  - For details about the configuration No. and its related function, see **Button Configuration Description** .
- 

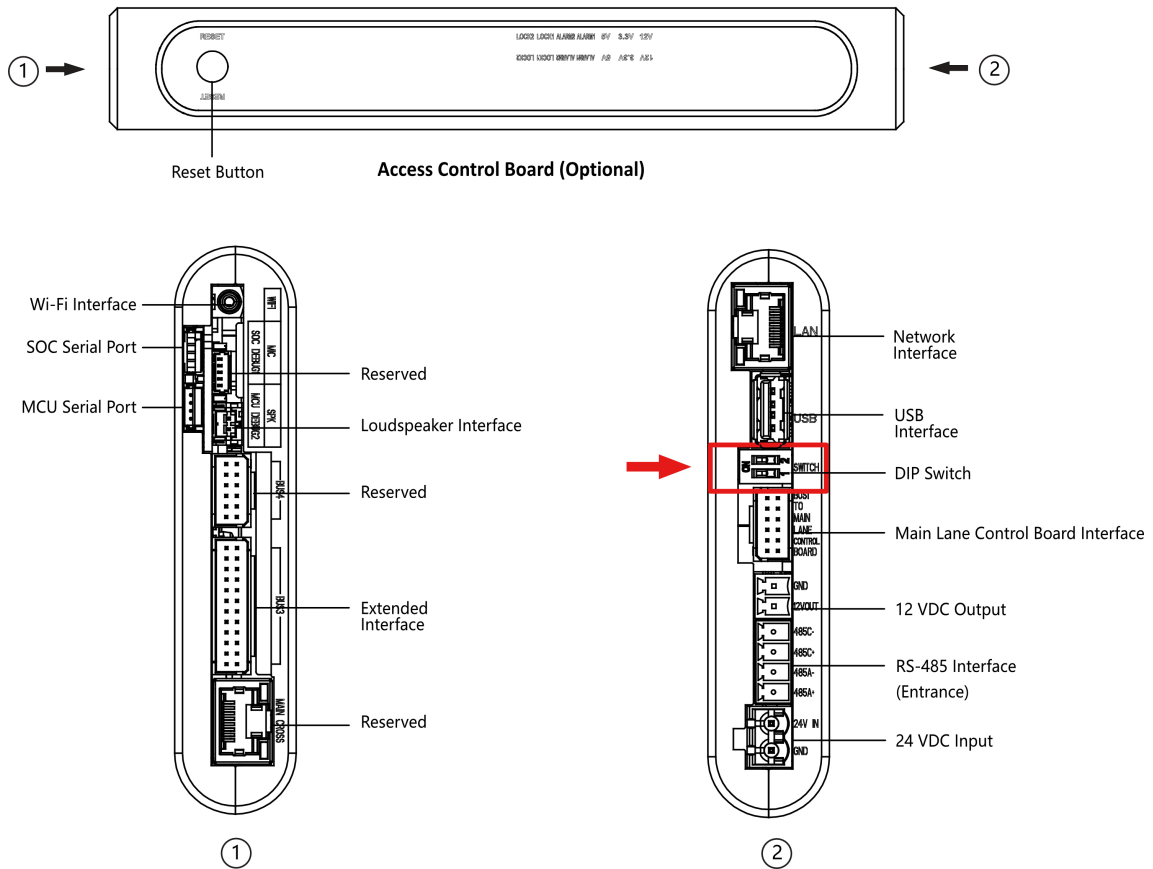
1. Enter the study mode.
  - 1) Enter the configuration mode.
  - 2) Set the configuration No. in Level-1 to **1**. The device will enter the study mode.
  - 3) Set the configuration No. in the Level-2 menu to **2**. The device will enter the study mode.
2. Swing the barrier until it is vertical to the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

### 7.2.2 Set Study Mode via DIP Switch (Optional)

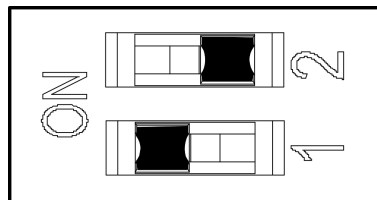
Enter the study mode through DIP switching to set the closed position of the device barrier.

#### Steps

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



**Figure 7-3 DIP Switch Location**



**Figure 7-4 Study Mode**

2. Swing the barrier until it is vertical to the pedestal.
3. When you hear the continuous buzzing, stop swing the barrier and exit the lane.
4. When you hear **Studying completed, welcome**, set the No.1 switches of the 2-digit DIP Switch on the main user extended interface board by referring to the following figure.

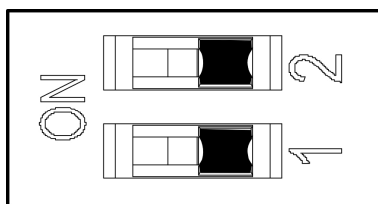


Figure 7-5 Normal Mode

5. Power on the device again.



#### Note

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

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

## 7.3 Keyfob Pairing

Pair keyfob via button or DIP switch.

### 7.3.1 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

- If the device is equipped with access control board, you can pair keyfob via DIP switch on the access control board only.
- 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.
4. Reboot the device to take effect.

## 7.3.2 Pair Keyfob via DIP Switch (Optional)

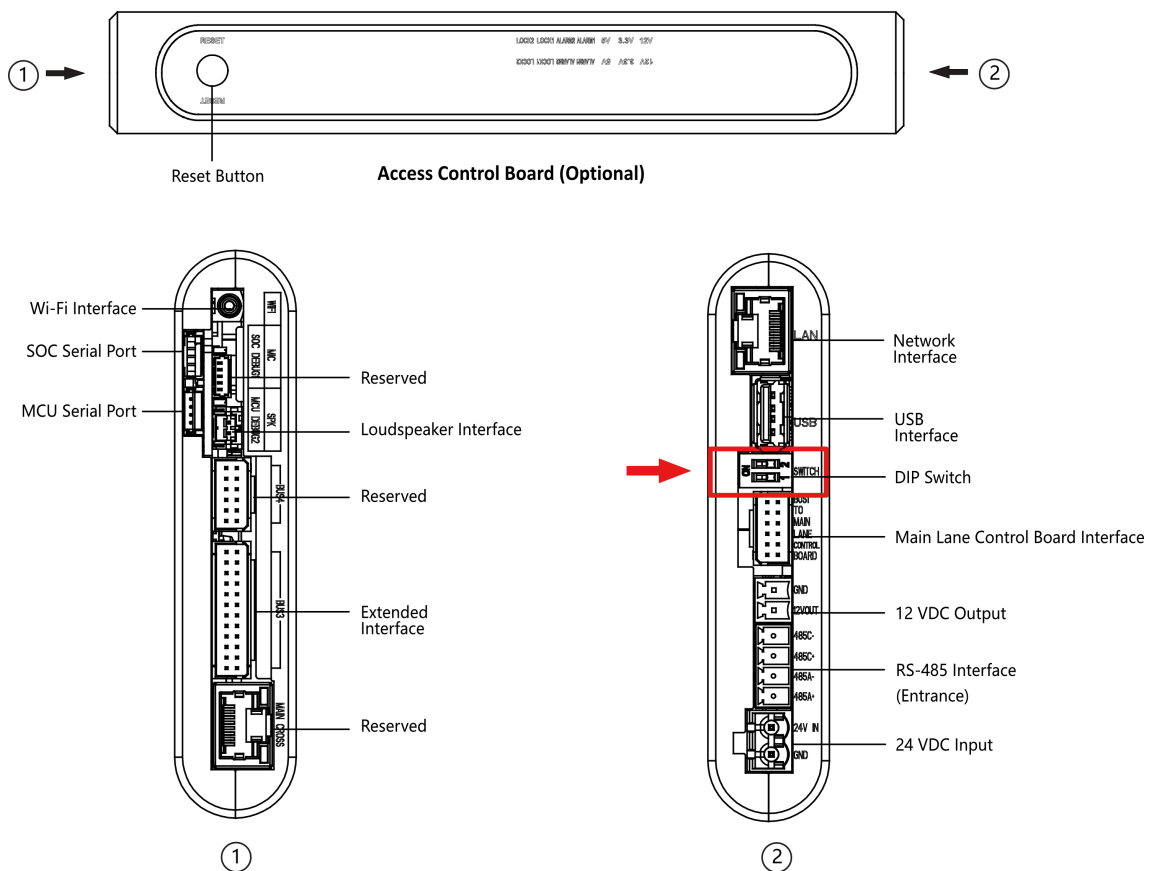
Pair the remote control to the device through DIP switch to open/close the barrier remotely.

### Before You Start

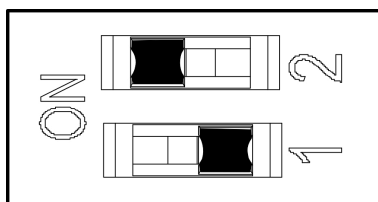
Ask our technique supports or sales and purchase the keyfob.

### 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 7-6 DIP Switch Location**



**Figure 7-7 Enable Keyfob Pairing 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 will flash twice if the pairing is completed.
5. Set the No.2 switch to the OFF side, and reboot the turnstile to take effect.

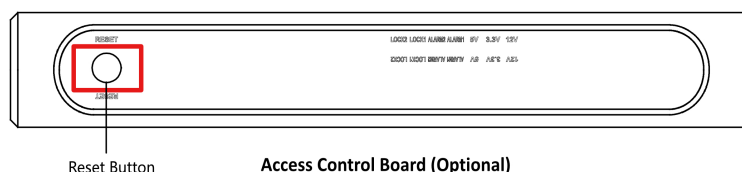
## Note

- 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](#).
6. **Optional:** Go to **System → User → Keyfob User** on the remote control page of the client software to delete the keyfob.

## 7.4 Initialize Device

### Steps

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



**Figure 7-8 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 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.: 80
- 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

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



#### Note

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

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

### 8.2 Activate via Mobile Web

You can activate the device via mobile web.

### Steps

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



#### Note

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

---

The login page will pop up.

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



#### Caution

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



#### Note

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

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

## 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

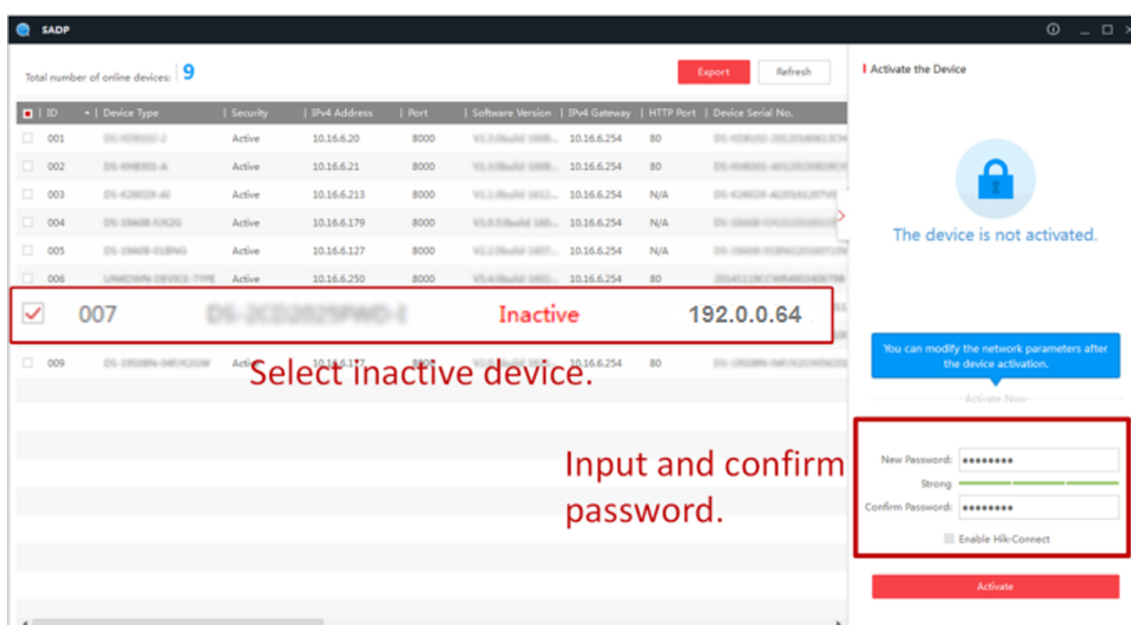
**STRONG PASSWORD RECOMMENDED**-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your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



## Note

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

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



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

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

## 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 Quick Operation via Web Browser

### 9.1 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 10 Operation via Web Browser

### 10.1 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.

### 10.2 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.

## 10.3 Person Management

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

The screenshot displays a web-based form for adding a new person. It is divided into three main sections: Basic Information, Certificate Configuration, and Authentication Settings. The Basic Information section includes fields for Employee ID, Name, Gender (Male, Female, Unknown), Person Type (Normal User, Visitor, Blocklist User), a Long-Term Effective User toggle, and a Validity Period date range. The Certificate Configuration section shows a dashed box for adding a card, with a note that up to 50 cards can be supported. The Authentication Settings section includes an Authentication Type dropdown (Same as Device, Custom) and Save/Cancel buttons at the bottom.

Basic Information

\*Employee ID

Name

Gender ☒ Male ☐ Female ☐ Unknown

Person Type ☒ Normal User ☐ Visitor ☐ Blocklist User

Long-Term Effective User ☐

Validity Period  -

Certificate Configuration

Card Up to 50 cards can be supported.

Authentication Settings

Authentication Type ☒ Same as Device ☐ Custom

Figure 10-1 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.

---

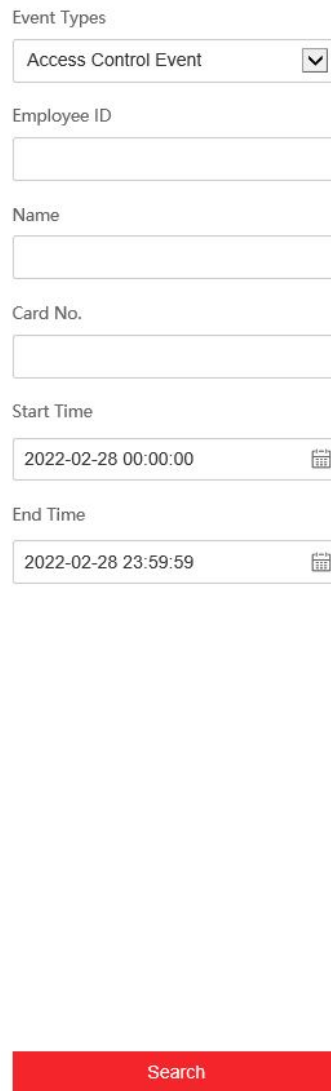


### Note

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

## 10.4 Search Event

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



The form is titled "Search Event" and contains several input fields for filtering event data. It includes a dropdown menu for "Event Types", and text input fields for "Employee ID", "Name", and "Card No.". There are also date and time pickers for "Start Time" and "End Time". A red "Search" button is located at the bottom of the form.

|                      |
|----------------------|
| Event Types          |
| Access Control Event |
| Employee ID          |
| Name                 |
| Card No.             |
| Start Time           |
| 2022-02-28 00:00:00  |
| End Time             |
| 2022-02-28 23:59:59  |
| Search               |

**Figure 10-2 Search Event**

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

The results will be displayed on the right panel.

## 10.5 Configuration

### 10.5.1 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**.

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

### 10.5.2 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)

Save

**Figure 10-3 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.

### 10.5.3 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.

### 10.5.4 Change Administrator's Password

#### Steps

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



#### Caution

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

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

---

### 10.5.5 Online Users

The information of users logging into the device is shown.

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

10.5.6 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.

10.5.7 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

Save

Figure 10-4 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.

### Device Hotspot

Set the device hotspot.

Click **Configuration → Network → Network Settings → Device Hotspot** .

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

Click **Save**.

### Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening, RTSP and Server port parameters.

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

Serial Port Type RS232

No.

Baud Rate

Data Bit

Stop Bit ☒ 1 ☐ 2

Parity ☒ None ☐ Odd Parity ☐ Even Verification

Peripheral Type ☐ Card Reader ☒ Card Receiver ☐ QR Code Scanner ☐ Disable

Peripheral Position ☒ Entrance ☐ Exit

External Device Model None

**Figure 10-5 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 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 is 1 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

\* Port

\* Device ID

\* Encryption Key

Register Status Offline

[More](#) ^

| Type          | Access Priority | Operation |
|---------------|-----------------|-----------|
| Wired Network | 1               | ⋮         |

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

**Figure 10-6 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. Check **Enable** 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 **More** to view the network type and access priority. Check **Allow Access** to allow or deny the network access. Drag the operation icon up or down to adjust the access priority of the network type.
6. Click **Save** to enable the settings.
7. View the account binding status, and click **Refresh** to view the latest status.
8. 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.

### 10.5.8 Set Audio Parameters

Set the audio parameters.

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

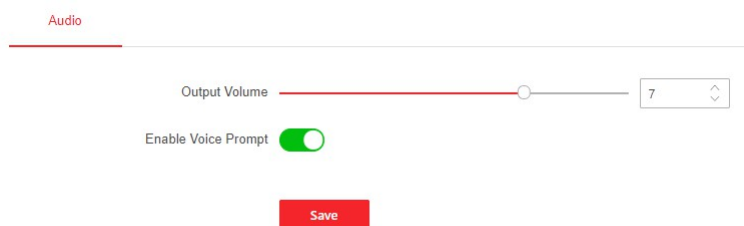


Figure 10-7 Audio Settings Page

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

Click **Save** to save the settings.

### 10.5.9 Event Linkage

Set linked actions for events.

#### Steps

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

Linkage Settings

+ Add General Linkage...

Add New Event and Card Linkage

Event Source

Linkage Type ☒ Event Linkage  
☐ Card Linkage  
☐ Link Employee ID

Event Types Device Event No Memory Alarm for Unrepo...

Linkage Action

Buzzer Linkage ☒  
☒ Start Buzzing ☐ Stop Buzzing

Door Linkage ☒  
☒ Entrance ☐ Exit Unlock

Linked Alarm Output ☒  
☒ Alarm Output1 Open ☐ Alarm Output2

Linkage Audio Prompt ☒  
Voice Prompt Type ☐ TTS ☒ Audio File  
Play Mode ☒ Disable ☐ Play Once ☐ Loop  
Audio File Authenticated\_16K.wav

Save

Figure 10-8 Event Linkage

2. Set event source.

- If you choose **Linkage Type** as **Event Linkage**, you need to select event types from the drop-down list.
- If you choose **Linkage Type** as **Card Linkage**, you need to enter the card No. and select the card reader.
- If you choose **Linkage Type** as **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.

### 10.5.10 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.

---

The screenshot shows a web-based configuration interface for the DS-K3B631X Series Swing Barrier. At the top, there are two buttons: 'Entrance' (highlighted with a red border) and 'Exit'. Below these are three read-only fields: 'Terminal Type' set to 'Card', and 'Terminal Model' set to '4850Offline'. The 'Enable Authentication Device' option is a green toggle switch that is turned on. Below this is a dropdown menu for 'Authentication' currently set to 'Card'. The 'Authentication Interval' is a numeric input field set to '0' with a unit selector 's' and up/down arrows. The 'Alarm of Max. Failed Attempts' is a grey toggle switch that is turned off. The 'Communication with Controller Ev...' is another numeric input field set to '0' with a unit selector 's' and up/down arrows. At the bottom center is a red 'Save' button.

**Figure 10-9 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.



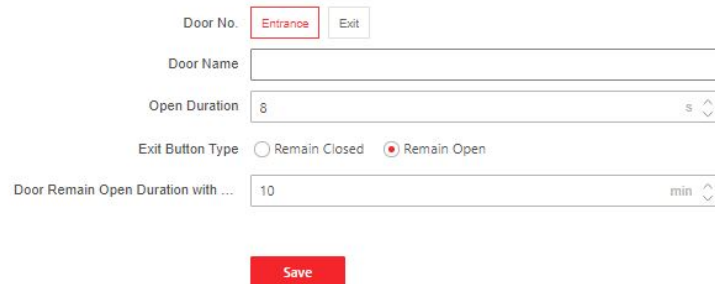
#### Note

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

---

## Set Door Parameters

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



The screenshot shows the 'Door Parameters' settings page. It includes fields for 'Door No.' with 'Entrance' and 'Exit' buttons, 'Door Name' (text input), 'Open Duration' (spinner set to 8 s), 'Exit Button Type' (radio buttons for 'Remain Closed' and 'Remain Open'), and 'Door Remain Open Duration with ...' (spinner set to 10 min). A red 'Save' button is at the bottom.

**Figure 10-10 Door Parameters Settings Page**

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.



#### Note

The duration ranges from 1 s to 1440 s.

---

### Serial Port Settings

Set serial port parameters.

#### Steps

1. Click **Configuration** → **Access Control** → **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** as **Card Reader**, **Card Receiver**, **QR Code Scanner** or **Disable**.
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 ① ☐ Access Control Mode ①

Remote Verification

① Remote Verification ☒

① Verify Credential Locally ☒

Save

**Figure 10-11 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.

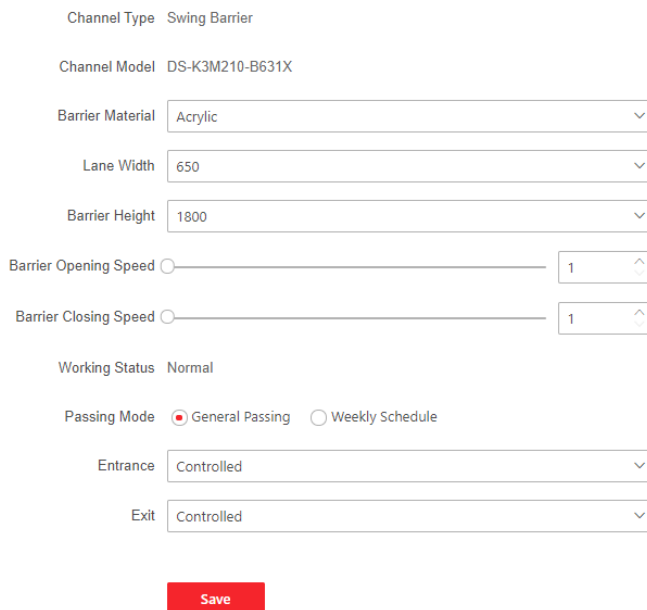
## 10.5.11 Turnstile

### Basic Parameters

Set turnstile basic parameters.

#### Steps

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



The screenshot shows the 'Basic Parameters' configuration page for a turnstile. The page has a light gray background and a white content area. At the top, there are two labels: 'Channel Type' with the value 'Swing Barrier' and 'Channel Model' with the value 'DS-K3M210-B631X'. Below these are three dropdown menus: 'Barrier Material' set to 'Acrylic', 'Lane Width' set to '650', and 'Barrier Height' set to '1800'. There are two sliders for 'Barrier Opening Speed' and 'Barrier Closing Speed', both set to '1'. Below the sliders, there is a 'Working Status' label with the value 'Normal'. Then, there are two radio buttons for 'Passing Mode': 'General Passing' (selected) and 'Weekly Schedule'. At the bottom, there are two more dropdown menus: 'Entrance' set to 'Controlled' and 'Exit' set to 'Controlled'. A red 'Save' button is located at the bottom center of the form.

**Figure 10-12 Basic Parameters**

2. View the **Channel Type**, **Channel Model** and **Working Status**.
3. Set **Barrier Material**, **Lane Width**, **Lane Height**, **Barrier Opening Speed** and **Barrier Closing Speed**.
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. Click **Save**.

### keyfob

Set keyfob parameters.

#### Steps

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

Keyfob Working Mode ☒ One-to-One ☐ One-to-Many

Keyfob + Add Delete

| Name | No. | Permission for Remai... | Operation |
|------|-----|-------------------------|-----------|
|------|-----|-------------------------|-----------|

No data.

Save

**Figure 10-13 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 **Remain Open Permission** at your actual needs.
- 4) Click **OK** to add the keyfob.

4. **Optional:** Select a keyfob and click **Delete** to delete the keyfob.

5. Click **Save**.

### IR Detector

Set IR detector.

#### Steps

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

2. Set the entrance and exit inductive mode as **Single Triggered** or **Triggered Simultaneously**.

3. Set custom IR detector mode.

#### Enable IR Emergency Mode

If some IR beams do not work properly, you can shield those IR 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 IR beams for closing barrier in advance. But this action may hit person and cause injury.

It is recommended to enable custom anti-pinch for door closing function for the recommended detector.

4. Click **Save**.

### People Counting

Set people counting .

#### Steps

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

People Counting ☒

Device Offline People Counting ☒

Passing Event Record ☒

Person Statistics Type ☒ Invalid ☐ Passing Detection ☐ Authentication Number

People Counting

**Figure 10-14 People Counting**

2. Enable **People Counting**.

3. Enable **Device Offline People Counting** and **Passing Event Record** at your actual needs.

4. Select **Person Statistics Type** as **Invalid**, **Passing Detection** or **Authentication Number**.

5. **Optional:** Click **Clear** to clear all the people counting information.

6. Click **Save**.

### Set Light

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

#### Steps

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

2. Set light color for lane status indicator.

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

2) Set color for inductive/remain open, remain closed and controlled/barrier-free.

3. Set barrier light color.
  - 1) Click to enable **Light on When on Standby** at your actual needs.
  - 2) Set the barrier light color.
4. Click **Save**.

### Other Settings

Set other parameters.

#### Steps

1. Click **Configuration → Turnstile → Other Settings** to enter the page.
2. Enable **People Detection**. When the device detects that people is approaching, it will link the lighting effect.
3. Set **Alarm Output Duration**.



#### Note

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

---

4. Set **Temperature Unit**.
5. Enable **Do Not Open Barrier When Lane is Not Clear**.
6. Drag the block or enter the value to adjust the lightboard brightness.
7. Set the duration parameters.

#### Alarm Buzzing Duration

Set the duration of alarm sound.

#### Barrier Closing Delay

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

#### Intrusion Duration

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

#### Overstaying Duration

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

#### IR Obstructed Duration

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

8. Enable **Memory Mode** at your actual needs.



#### Note

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.

---

**9. Choose the 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.

**10. Set Fire Input Type.** In the normally open state, closing triggers fire protection. In the normally closed state, disconnection triggers fire protection.

**11. Click More** to adjust barrier open angle.

**12. Click Save.**

### 10.5.12 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**.

### **10.5.13 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.

### **10.5.14 Customize Audio Content**

Customize the output audio content when authentication succeeded and failed.

#### **Steps**

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

Enable ☒

Appellation ☐ Name ☐ Family Name ☒ None

**Time Period When Authentication Succeeded**

Period1

Time

Voice Prompt Type ☒ TTS ☐ Audio File

\* Audio Prompt Content

[+ Add Time Duration](#)

**Time Period When Authentication Failed**

Period1

Time

Voice Prompt Type ☒ TTS ☐ Audio File

\* Audio Prompt Content

[+ Add Time Duration](#)

**Figure 10-15 Customize Audio Content**

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

---

 **Note**

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

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

---

 **Note**

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

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

---

### **Note**

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

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

---

### **Note**

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

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

## 10.5.15 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.

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

---

### **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 network parameters 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.

## 10.5.16 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.

#### Motor Study & Self-Test

Click **Start**, the device will enter the study mode. Swing the barrier until it is vertical to the pedestal. When you hear the continuous buzzing, stop swing the barrier and exit the lane. When you hear "Studying completed, welcome", the configuration is completed.

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

Select the lane and click **Start**, the encoder will test the operation status automatically.

#### Print Log

Select object, and click **Export** to export log of the object.

#### TOF Capture

Select the lane direction, and click **Start Capture** to capture TOF data.

#### Capture Network Packet

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

#### 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.

### 10.5.17 Component Status

You can view the main lane and sub lane status.

#### Main Lane Status

##### Device Component

You can view the status of the access control board, lane control board, user extended interface board, indicator and IR adaptor.

##### Peripheral

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

##### Temperature

You can view the pedestal temperature.

##### Movement

You can view the status of motor encoder and brake.

#### Sub Lane Status

##### Device Component

You can view the status of the lane control board, indicator and IR adaptor.

##### Peripheral

You can view the status of the RS-485 card reader, RS-232 card receiver and tamper input.

##### Movement

You can view the status of motor encoder and brake.

#### Others

##### Passing Mode

You can view the entrance and exit mode.

##### IR Detector Status

You can view the status of each pair of the IR beam sensors.

##### 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.

### 10.5.18 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.

### 10.5.19 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 Install 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 Passwords** area, and select a certificate from the local, and click **Install**.
  - 2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Install**.

## Install 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 Passwords** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Install**.

### Install 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 **Install**.

## Chapter 11 Configure the Device via the Mobile Browser

### 11.1 Login

You can login via mobile browser.



#### Note

Make sure the device is activated.

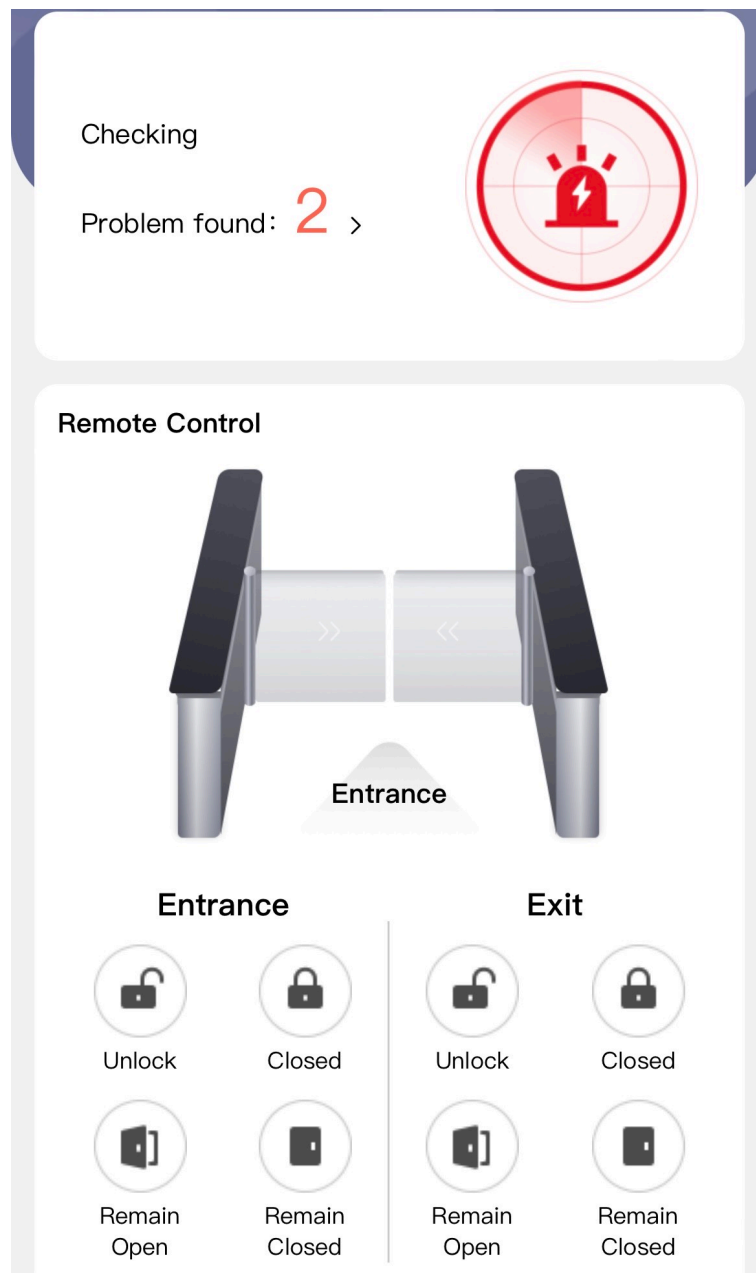
---

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

When the device hotspot is enabled, you can also scan the QR code and the login page will pop up. Enter the user name and the password. Tap **Login**.

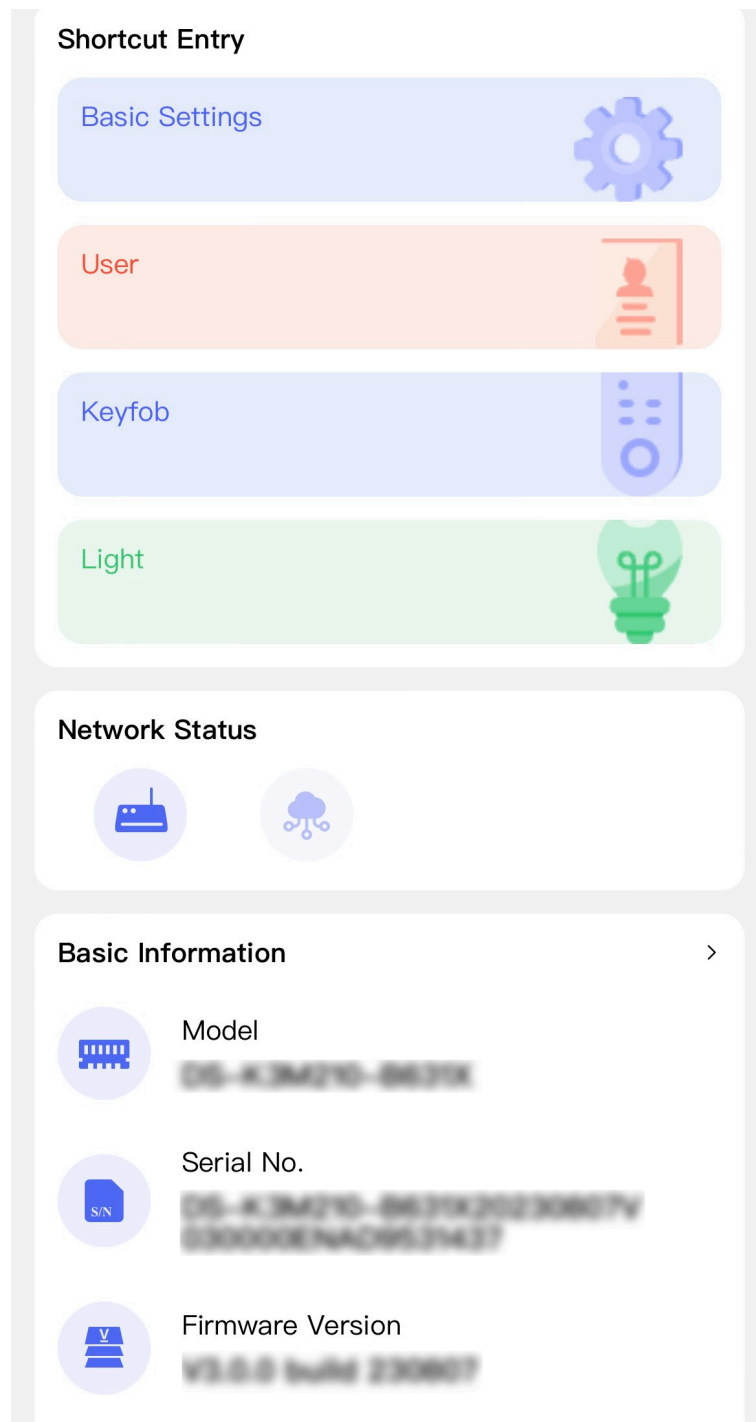
### 11.2 Overview

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



**Figure 11-1 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 11-2 Shortcut Entry and Basic Information**

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

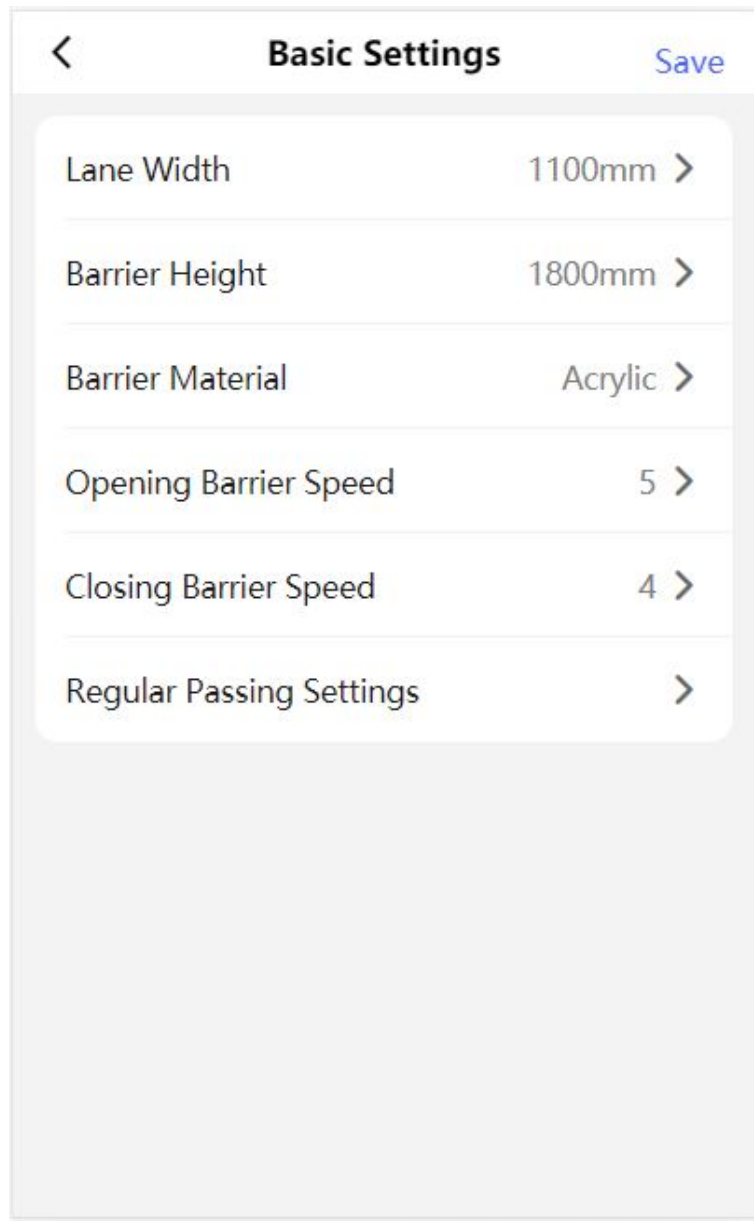
You can view model, serial No. and firmware version, and you can tap to fast enter the basic information page.

### 11.3 Configuration

#### 11.3.1 Turnstile Basic Parameters

You can set the basic parameters of the turnstile.

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



**Figure 11-3 Turnstile Basic Parameters**

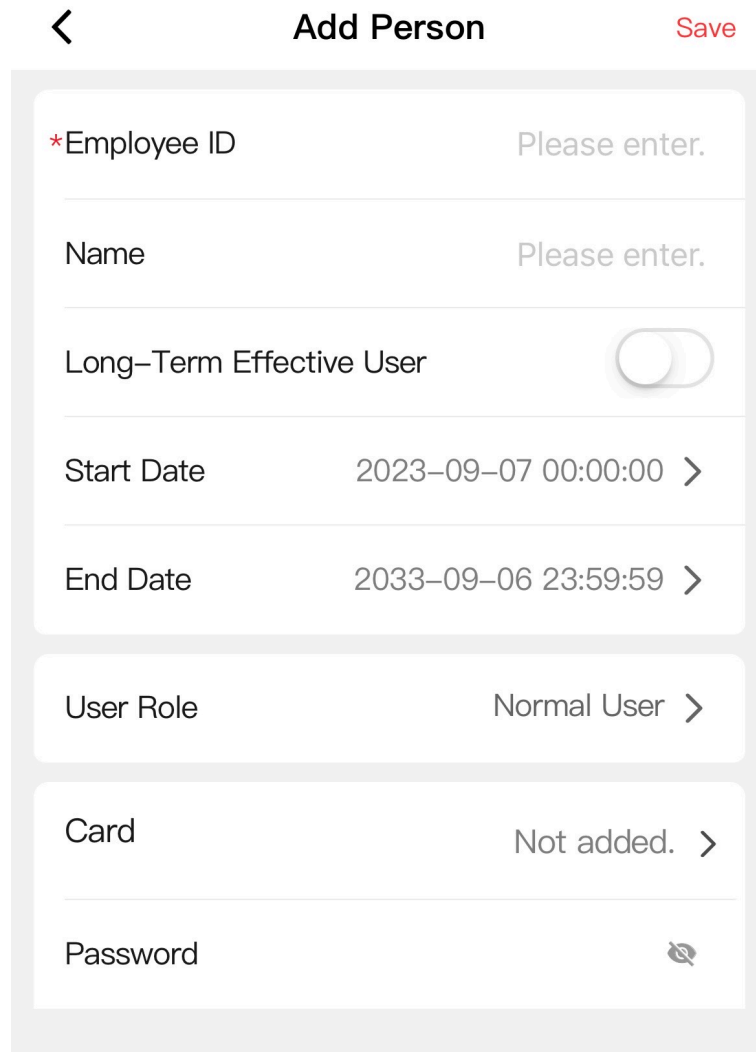
Set **Lane Width**, **Barrier Height**, **Barrier Height**, **Barrier Opening Speed** and **Barrier Closing Speed**. Set the regular passing mode for the entrance and exit. Tap **Save**.

### **11.3.2 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.



← Add Person Save

\*Employee ID Please enter.

Name Please enter.

Long-Term Effective User ☐

Start Date 2023-09-07 00:00:00 >

End Date 2033-09-06 23:59:59 >

User Role Normal User >

Card Not added. >

Password 

**Figure 11-4 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.

### **Password**

Enter the password. The password only supports numbers of 0 to 8 characters.

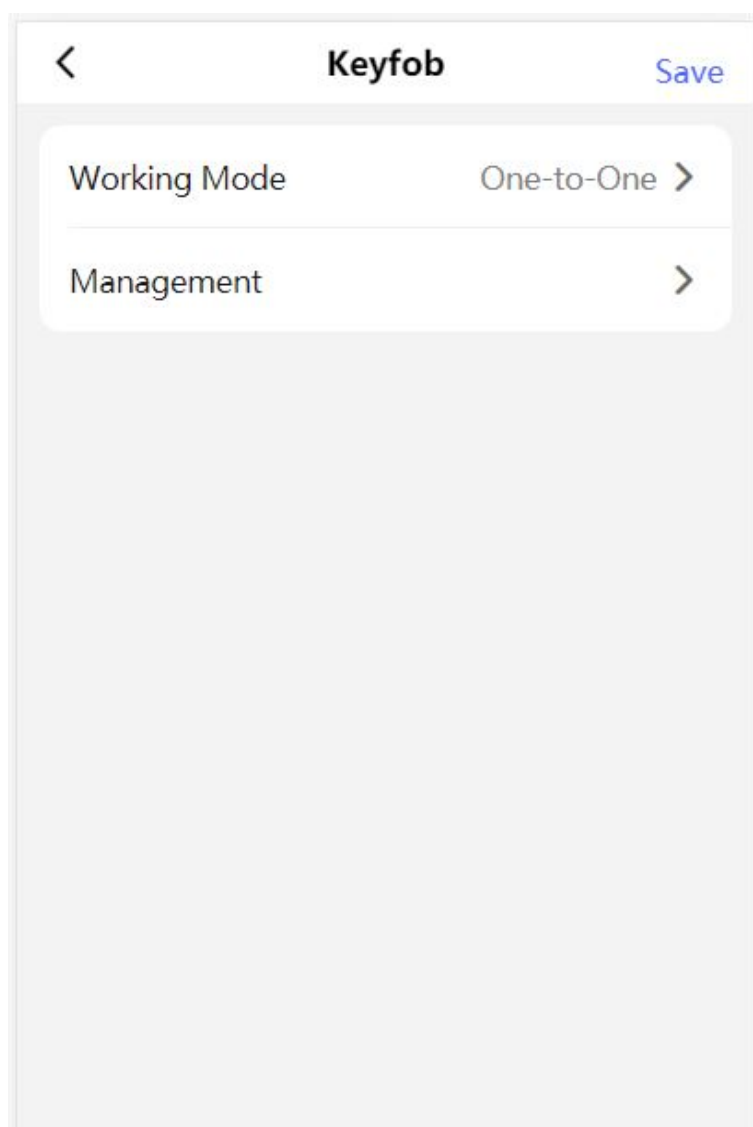
3) Tap **Save**.

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.

### **11.3.3 Keyfob Settings**

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



**Figure 11-5 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.

### **11.3.4 Light Settings**

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

## Lane Status Indicator

< Lane Status Indicator Save

|                  |          |
|------------------|----------|
| Light Brightness | Manual > |
| Brightness Value | 40       |

|                         |         |
|-------------------------|---------|
| Inductive/Remain Open   | Blue >  |
| Remain Closed           | Red >   |
| Controlled/Barrier-Free | Green > |

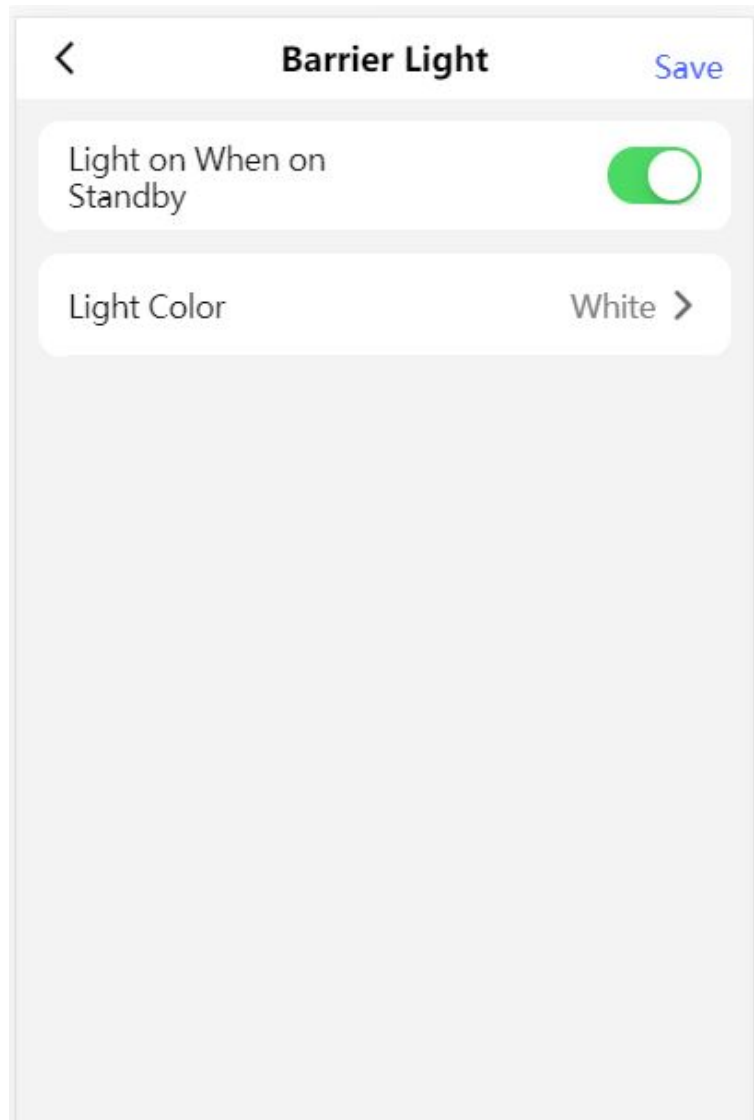
**Figure 11-6 Lane Status Indicator Settings**

Enter the value to adjust the light brightness manually.

Set inductive/remain open, remain closed and controlled/barrier-free light color.

Tap **Save**.

## Barrier Light



**Figure 11-7 Barrier Light Settings**

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

### 11.3.5 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.

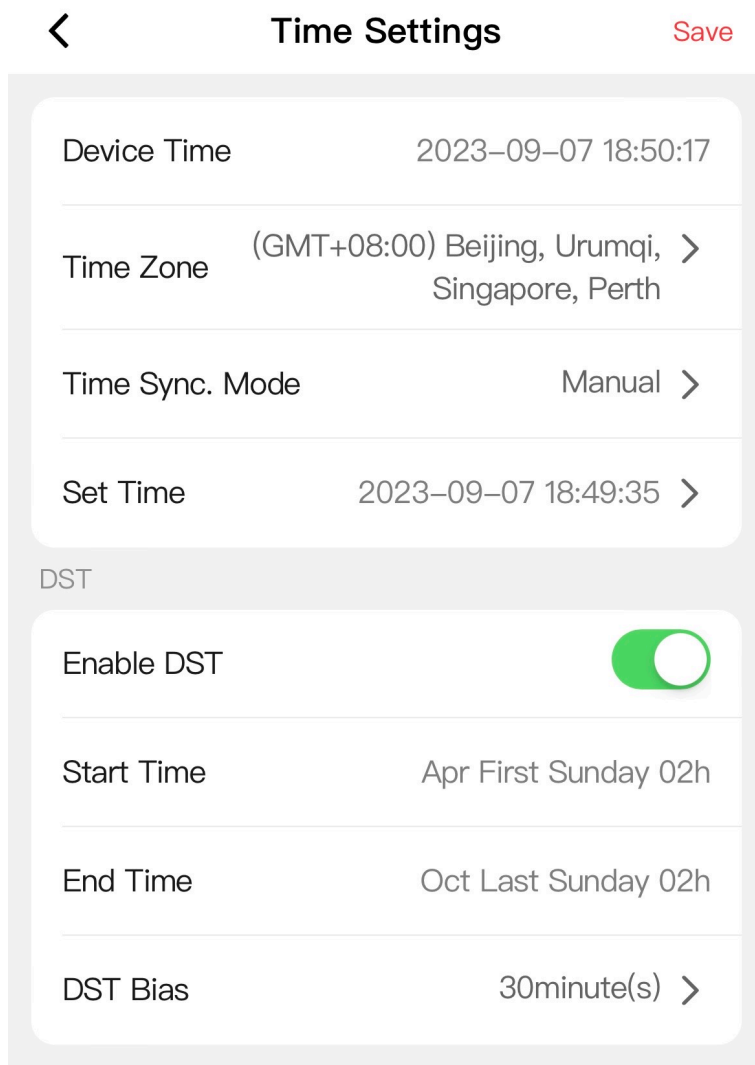
Tap **Device Capacity** to view the quantity and capacity of person, card and event.

Tap **Save**.

### 11.3.6 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 11-8 Time Settings**

#### Device Time

You can view current time.

### Time Zone

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

### Time Sync. Mode

#### Manual

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

#### NTP

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

#### DST

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

Tap **Save**.

## 11.3.7 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**.

## 11.3.8 Network

### Wired Network

Set wired network.

Tap  → **Communication 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.

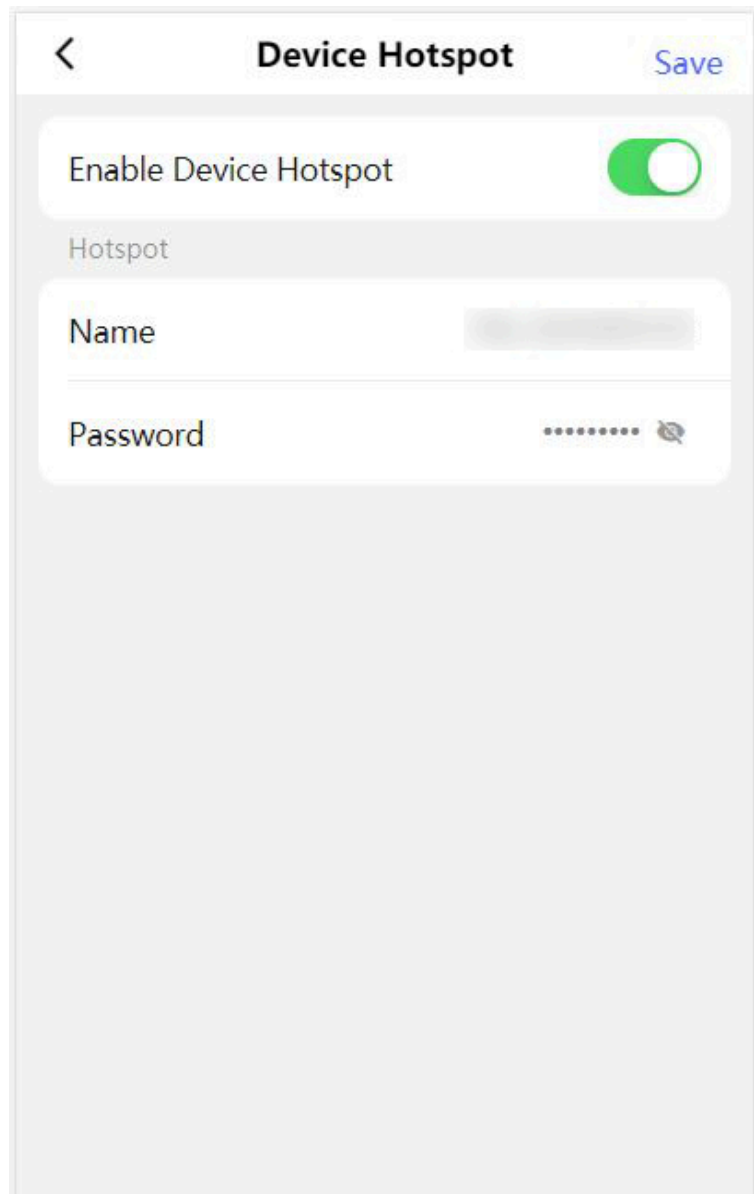
---

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

### Device Hotspot

Set device hotspot.

Tap  → **Communication Settings** → **Device Hotspot** to enter the configuration page.



**Figure 11-9 Device Hotspot**

Tap to **Enable Device Hotspot**. Set hotspot name and password.  
Click **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.

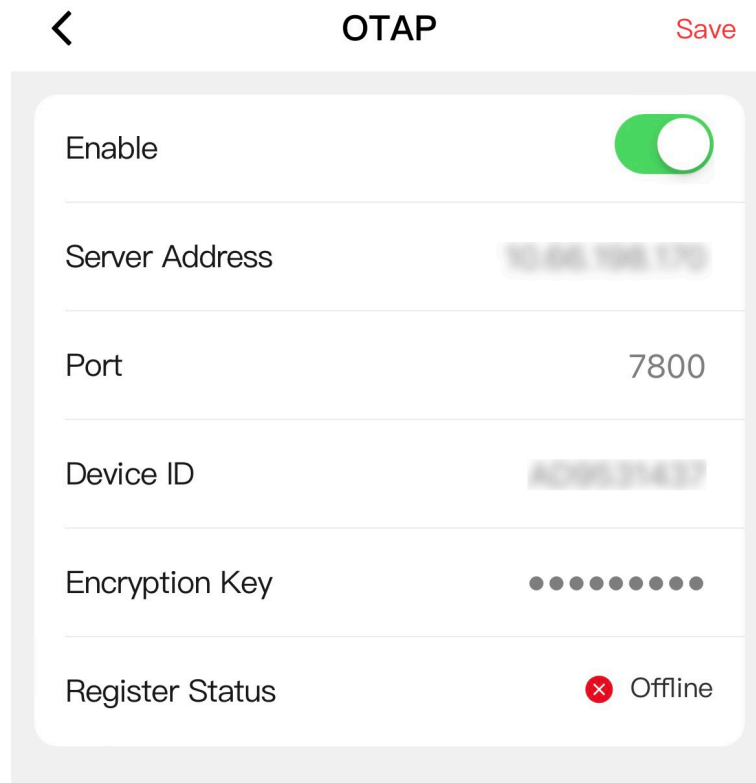
4. You can view **Register Status** and **Binding Status**.
5. You can tap **Bind An Account** → **View QR Code** , scan the QR code to bind an account.
6. Tap **Save** to enable the settings.

## 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** .



The screenshot shows the OTAP configuration interface. At the top, there is a navigation bar with a back arrow on the left, the title 'OTAP' in the center, and a 'Save' button on the right. Below the navigation bar is a light gray container holding a white form. The form contains the following fields: 'Enable' with a green toggle switch, 'Server Address' with a blurred IP address, 'Port' with the value '7800', 'Device ID' with a blurred hex string, 'Encryption Key' with ten dots, and 'Register Status' with a red 'X' icon and the text 'Offline'.

**Figure 11-10 OTAP**

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

**Result**

Refresh the page or reboot the device, and you can view the **Register Status**.

### 11.3.9 Event Search

Tap  → **Event Search** .

< **Event Search** Search

Event Types Access Control Event >

---

Employee ID

---

Name

---

Card No.

---

Start Time 2023-09-07 00:00:00

---

End Time 2023-09-07 23:59:59

**Figure 11-11 Event Search**

Select event types, and 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.

### 11.3.10 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.

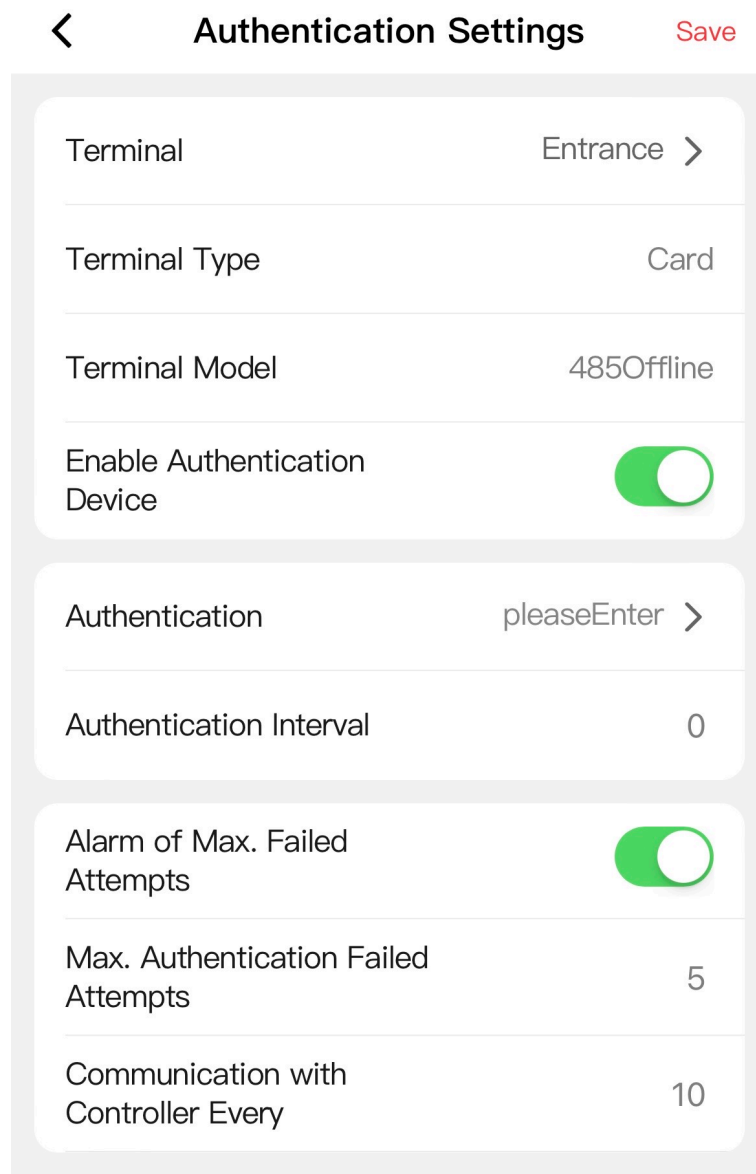
### 11.3.11 Access Control Settings

#### Set Authentication Parameters

Set authentication parameters.

##### Steps

1. Tap  → Access Control → Authentication Settings .



| Authentication Settings             |                                     |
|-------------------------------------|-------------------------------------|
| Terminal                            | Entrance >                          |
| Terminal Type                       | Card                                |
| Terminal Model                      | 485Offline                          |
| Enable Authentication Device        | <input checked="" type="checkbox"/> |
| Authentication                      | pleaseEnter >                       |
| Authentication Interval             | 0                                   |
| Alarm of Max. Failed Attempts       | <input checked="" type="checkbox"/> |
| Max. Authentication Failed Attempts | 5                                   |
| Communication with Controller Every | 10                                  |

**Figure 11-12 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 Parameters Save

Door No. Entrance >

Name

Open Duration 8

Exit Button Type Remain Open >

Door Remain Open Duration with First Person (min) 1

**Figure 11-13 Door Parameters**

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

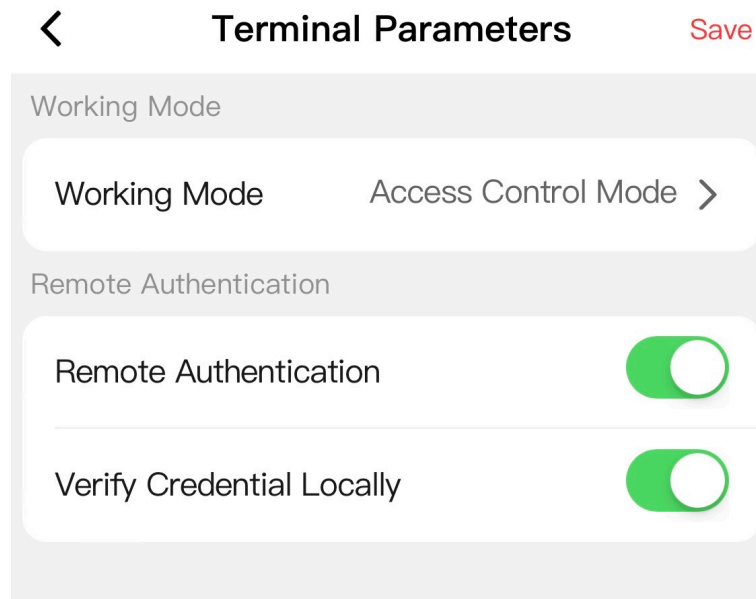
Configure **Door Remain Open Duration with First Person**. The mode is applicable for the passing of groups of persons, such as visitors entering the scenic spots. After the set person passes through, the door will open for a set time and other persons can pass through without authentication.

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

## Terminal Settings

Set the working mode.

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



**Figure 11-14 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.

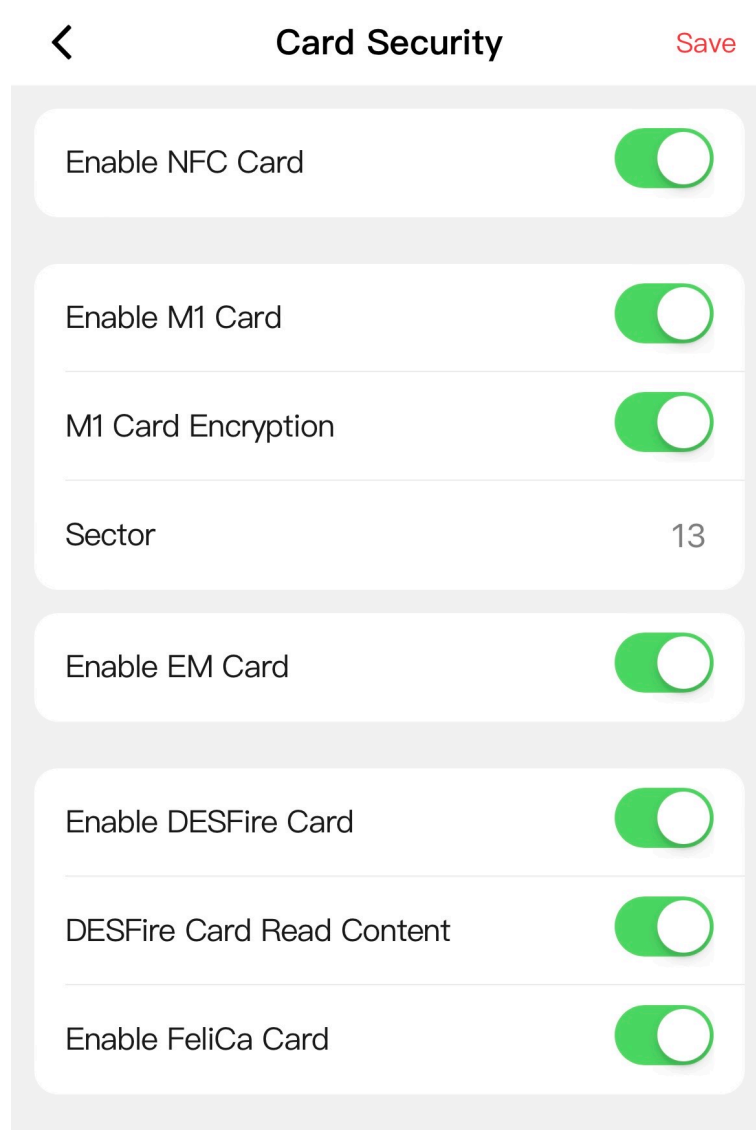
#### **Verify Credential Locally**

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** .



**Figure 11-15 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.

## 11.3.12 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.

### 11.3.13 Device Debugging

You can set device debugging parameters.

Tap  → **Device Debugging** .

Select the lane direction, and tap **Start Capture** to capture TOF data.

### 11.3.14 View Open Source Software License on Mobile Web

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

### 11.3.15 Log Out

Log out the configuration page.

Tap  → **Log Out** on the home page, tap **OK**.

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

## Chapter 12 Client Software Configuration

You can call the hotline to get the iVMS-4200 client software installation package.

### 12.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

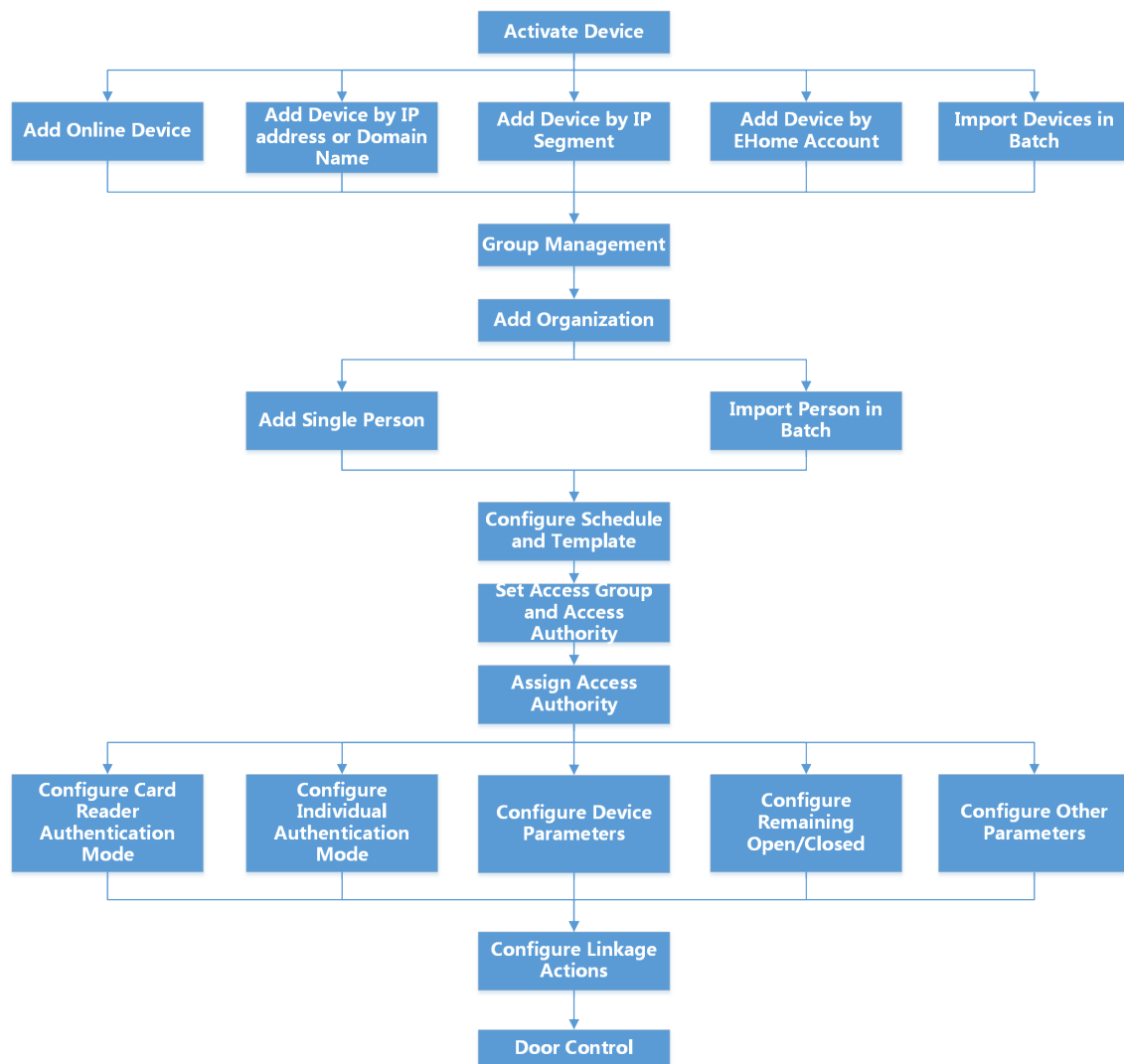


Figure 12-1 Flow Diagram of Configuration on Client Software

## 12.2 Device Management

The client supports managing access control devices and video intercom devices.

### Example

You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

### 12.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and ISUP protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

#### Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

#### Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.  
The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

#### Name

Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

#### Address

The IP address or domain name of the device.

#### Port

The devices to add share the same port number. The default value is **8000**.



#### Note

For some device types, you can enter **80** as the port No. This function should be supported by the device.

---

#### User Name

Enter the device user name. By default, the user name is **admin**.

#### Password

Enter the device 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.

- 
5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.
- 



### Note

- This function should be supported by the device.
  - If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See for details about enabling certificate verification.
  - You can log into the device to get the certificate file by web browser.
- 
6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

### Example

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

8. Finish adding the device.
- Click **Add** to add the device and back to the device list page.
  - Click **Add and New** to save the settings and continue to add other device.

## Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

### Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.

5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.



### Note

For detailed description of the required fields, refer to the introductions in the template.

---

### Adding Mode

Enter **0** or **1** or **2**.

### Address

Edit the address of the device.

### Port

Enter the device port number. The default port number is **8000**.

### User Name

Enter the device user name. By default, the user name is **admin**.

### Password

Enter the device 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.

---

### Import to Group

Enter **1** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter **0** to disable this function.

6. Click  and select the template file.
7. Click **Add** to import the devices.

## 12.2.2 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

### Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.

All the online devices sharing the same subnet will be displayed in the list.

3. Select the device from the list and click  on the Operation column.

4. Reset the device password.

- Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.



### Note

For the following operations for resetting the password, contact our technical support.

---



### 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.

---

### 12.2.3 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device parameters, remote configuration, viewing device status, etc.

**Table 12-1 Manage Added Devices**

|                      |                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Edit Device          | Click  to edit device information including device name, address, user name, password, etc.                                                                                                                                                                                  |
| Delete Device        | Check one or more devices, and click <b>Delete</b> to delete the selected devices.                                                                                                                                                                                                                                                                              |
| Remote Configuration | Click  to set remote configuration of the corresponding device. For details, refer to the user manual of device.                                                                                                                                                             |
| View Device Status   | Click  to view device status, including door No., door status, etc.<br><br><div>  <b>Note</b><br/> For different devices, you will view different information about device status. </div> |

|                            |                                                                                                                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View Online User           | Click  to view the details of online user who access the device, including user name, user type, IP address and login time. |
| Refresh Device Information | Click  to refresh and get the latest device information.                                                                    |

## 12.3 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

### Example

For example, on the 1st floor, there mounted 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can control door status, and do some other operations of the devices after managing the resources by groups.

### 12.3.1 Add Group

You can add group to organize the added device for convenient management.

#### Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Create a group.
  - Click **Add Group** and enter a group name as you want.
  - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.



#### Note

The resources (such as alarm inputs/outputs, access points, etc.) of this device will be imported to the group by default.

---

### 12.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, access points, etc.) to the added group in a batch.

#### Before You Start

Add a group for managing devices. Refer to [\*\*Add Group\*\*](#) .

#### Steps

1. Enter the Device Management module.

2. Click **Device Management** → **Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.



**Note**

You can click  or  to switch the resource display mode to thumbnail view or to list view.

---

6. Click **Import** to import the selected resources to the group.

## 12.4 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

### 12.4.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a subordinate organization for the added one.

#### Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.



**Note**

Up to 10 levels of organizations can be added.

---

4. **Optional:** Perform the following operation(s).

|                          |                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit Organization</b> | Hover the mouse on an added organization and click  to edit its name. |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                            |                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Delete Organization</b> | Hover the mouse on an added organization and click  to delete it. |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|

---



**Note**

- The lower-level organizations will be deleted as well if you delete an organization.
  - Make sure there is no person added under the organization, or the organization cannot be deleted.
- 

|                                         |                                                                                                                    |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Show Persons in Sub Organization</b> | Check <b>Show Persons in Sub Organization</b> and select an organization to show persons in its sub organizations. |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------|

### 12.4.2 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

#### Import Person Information

You can enter the information of multiple persons in a predefined template (CSV/Excel file) to import the information to the client in a batch.

##### Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.



##### Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

- 
7. Click  to select the CSV/Excel file with person information from local PC.
  8. Click **Import** to start importing.
- 



##### Note

- If a person No. already exists in the client's database, delete the existing information before importing.
  - You can import information of no more than 2,000 persons.
- 

#### Export Person Information

You can export the added persons' information to local PC as a CSV/Excel file.

##### Before You Start

- Make sure you have added persons to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button.

##### Steps

1. Enter the Person module.

2. **Optional:** Select an organization in the list.



### Note

All persons' information will be exported if you do not select any organization.

---

3. Click **Export**.
4. Enter the super user name and password for verification.  
The Export panel is displayed.
5. Check **Person Information** as the content to export.
6. Check desired items to export.
7. Click **Export** to save the exported file in CSV/Excel file on your PC.

### 12.4.3 Get Person Information from Access Control Device

If the access control device has been configured with person information, you can get the person information from the added device and import them to the client for further operations.

#### Steps

---



### Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
  - If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.
- 

1. Enter **Person** module.
  2. Select an organization to import the persons.
  3. Click **Get from Device**.
  4. Select an added access control device or the enrollment station from the drop-down list.
- 



### Note

If you select the enrollment station, you should click **Login**, and enter IP address, port No., user name and password of the device.

---

5. Select the **Getting Mode**.
- 



### Note

The getting mode varies according to different devices. The access control device supports getting the person information by employee ID. Up to 5 employee IDs can be specified each time.

---

6. Click **Import** to start importing the person information to the client.
- 



### Note

Up to 2,000 persons and 5,000 cards can be imported.

---

The person information, and the linked cards (if configured), will be imported to the selected organization.

### 12.4.4 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

#### Steps

1. Enter **Person** module.
2. **Optional:** Select a person group, and select the persons with no card issued.
  - The selected persons with no card issued in the person group will be displayed in the right panel.
  - If you do not select the persons with no card issued in a person group, all the added persons with no card issued will be displayed in the right panel.
3. Click **Batch Issue Cards**.
4. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
5. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to *Issue a Card by Local Mode*.
6. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
7. Click the **Card No.** column and enter the card number.
  - Place the card on the card enrollment station.
  - Swipe the card on the card reader.
  - Manually enter the card number and press the **Enter** key.

The person(s) in the list will be issued with card(s).

### 12.4.5 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

#### Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click  on the added card to set this card as lost card.

After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click  to cancel the loss.

After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to

apply the changes to the device. After applying to device, these changes can take effect on the device.

### 12.4.6 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

#### Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

##### Card Enrollment Station

Select the model of the connected card enrollment station



##### Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

---

##### Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

##### Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

##### Buzzing

Enable or disable the buzzing when the card number is read successfully.

##### Card No. Type

Select the type of the card number according to actual needs.

##### M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

## Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

## 12.5 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.



### Note

For access group settings, refer to [\*\*\*Set Access Group to Assign Access Authorization to Persons\*\*\*](#) .

---

### 12.5.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

#### Steps



### Note

You can add up to 64 holidays in the software system.

---

1. Click **Access Control** → **Schedule** → **Holiday** to enter the Holiday page.
  2. Click **Add** on the left panel.
  3. Create a name for the holiday.
  4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
  5. Add a holiday period to the holiday list and configure the holiday duration.
- 



### Note

Up to 16 holiday periods can be added to one holiday.

---

- 1) Click **Add** in the Holiday List field.
  - 2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.
- 



### Note

Up to 8 time durations can be set to one holiday period.

---

- 3) **Optional:** Perform the following operations to edit the time durations.

- Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
  - Click the time duration and directly edit the start/end time in the appeared dialog.
  - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
- 4) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
  - 5) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
  - 6) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.
6. Click **Save**.

## 12.5.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

### Steps

---



#### Note

You can add up to 255 templates in the software system.

---

1. Click **Access Control → Schedule → Template** to enter the Template page.
- 



#### Note

There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

#### All-Day Authorized

The access authorization is valid in each day of the week and it has no holiday.

#### All-Day Denied

The access authorization is invalid in each day of the week and it has no holiday.

---

2. Click **Add** on the left panel to create a new template.
  3. Create a name for the template.
  4. Enter the descriptions or some notification of this template in the Remark box.
  5. Edit the week schedule to apply it to the template.
    - 1) Click **Week Schedule** tab on the lower panel.
    - 2) Select a day of the week and draw time duration(s) on the timeline bar.
- 



#### Note

Up to 8 time duration(s) can be set for each day in the week schedule.

---

- 3) **Optional:** Perform the following operations to edit the time durations.

- Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
  - Click the time duration and directly edit the start/end time in the appeared dialog.
  - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
- 4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.



### Note

Up to 4 holidays can be added to one template.

---

- 1) Click **Holiday** tab.
  - 2) Select a holiday in the left list and it will be added to the selected list on the right panel.
  - 3) **Optional:** Click **Add** to add a new holiday.
- 



### Note

For details about adding a holiday, refer to **Add Holiday**.

---

- 4) **Optional:** Select a selected holiday in the right list and click  to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.
7. Click **Save** to save the settings and finish adding the template.

## 12.6 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

### Steps

When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, face picture, linkage between card number and linkage between card number and card password, card effective period, etc).

1. Click **Access Control** → **Authorization** → **Access Group** to enter the Access Group interface.
  2. Click **Add** to open the Add window.
  3. In the **Name** text field, create a name for the access group as you want.
  4. Select a template for the access group.
- 



### Note

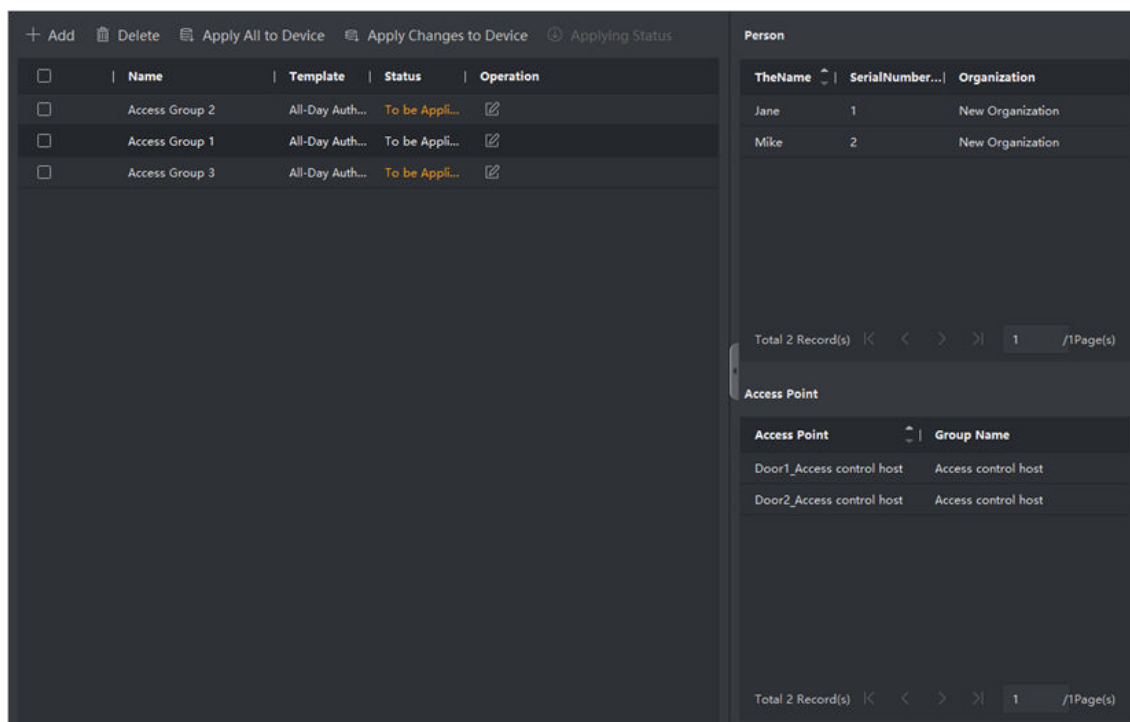
You should configure the template before access group settings. Refer to **Configure Schedule and Template** for details.

---

5. In the left list of the Select Person field, select person(s) to assign access authority.

6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

You can view the selected person(s) and the selected access point(s) on the right side of the interface.



**Figure 12-2 Display the Selected Person(s) and Access Point(s)**

8. After adding the access groups, you need to apply them to the access control device to take effect.
  - 1) Select the access group(s) to apply to the access control device.
  - 2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
  - 3) Click **Apply All to Devices** or **Apply Changes to Devices**.

### **Apply All to Devices**

This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

### **Apply Changes to Devices**

This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).

- 4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

---

### Note

You can check **Display Failure Only** to filter the applying results.

The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s).

**9. Optional:** Click  to edit the access group if necessary.

---

### Note

If you change the persons' access information or other related information, you will view the prompt **Access Group to Be Applied** on the right corner of the client.

You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.

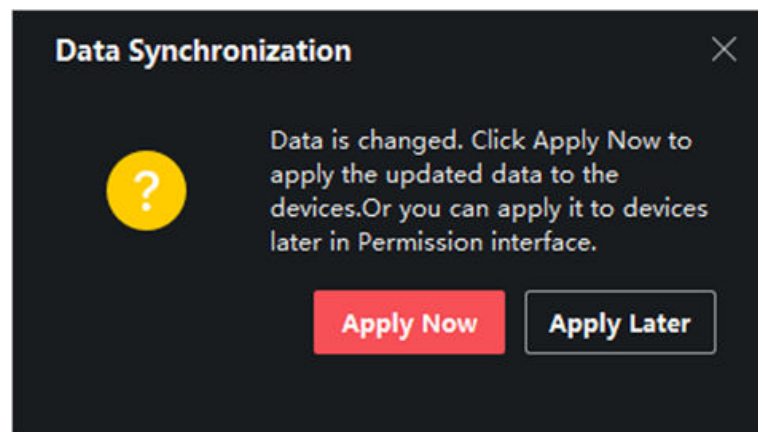


Figure 12-4 Data Synchronization

---

## 12.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene, such as multi-factor authentication, anti-passback, etc.

---

### Note

- For the card related functions(the type of access control card/multi-factor authentication), only the card(s) with access group applied will be listed when adding cards.
  - The advanced functions should be supported by the device.
  - Hover the cursor on the Advanced Function, and then Click  to customize the advanced function(s) to be displayed.
-

### 12.7.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device, access control points.

#### Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including voice prompt, card etc.

##### Before You Start

Add access control device to the client.

##### Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .



##### Note

If you can not find Device Parameter in the Advanced Function list, hover the cursor on the Advanced Function, and then Click  to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.



##### Note

- The displayed parameters may vary for different access control devices.

---

##### Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

##### Enable NFC

If enable the function, the device can recognize the NFC card. You can present NFC card on the device.

##### Enable M1 Card

If enable the function, the device can recognize the M1 card. You can present M1 card on the device.

##### Enable EM Card

If enable the function, the device can recognize the EM card. You can present EM card on the device.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

### Configure Parameters for Door/Elevator

After adding the access control device, you can configure its access point (door or floor) parameters.

#### Before You Start

Add access control device to the client.

#### Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. Select an access control device on the left panel, and then click  to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.



#### Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

---

#### Name

Edit the card reader name as desired.

#### Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

#### Open Duration

The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

5. Click **OK**.
6. **Optional:** Click **Copy to** , and then select the door/floor(s) to copy the parameters in the page to the selected doors/floor(s).



#### Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

---

### Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

#### Before You Start

Add access control device to the client.

### Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. In the device list on the left, click  to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.



### Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.

---

### Name

Edit the card reader name as desired.

### Card Authentication Interval

The time interval between two continuous card recognitions when authenticating.

### Repeated Authentication Interval

Within the specified interval, repeated authentication of the same card number (uploaded by different devices) is invalid, and only one authentication is performed.

### Enable Failed Attempts Limit of Authentication/Max. Failed Attempts for Authentication

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

### Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

4. Click **Advanced** to configure more parameters.

### Basic Information

#### Enable Card Reader

Enable the function and the device can be used as a card reader.

#### 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.

5. Click **OK**.
6. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

## Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

### Before You Start

Add access control device to the client, and make sure the device supports alarm output.

### Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

#### **Name**

Edit the card reader name as desired.

#### **Alarm Output Active Time**

How long the alarm output will last after triggered.

4. Click **OK**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

## Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

### **Before You Start**

Add access control device to the client.

### Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

#### **Passing Mode**

Select the controller which will control the barrier status of the device.

#### **Permission Controller Passing Mode**

Select the passing mode as **Normal Mode** or **Schedule Template Mode**.

#### **Alarm Voice Prompt Time Duration**

Set how long the audio will last, which is played when an alarm is triggered .



#### **Note**

0 refers to the alarm audio will be played until the alarm is ended.

---

#### **Temperature Unit**

Select the temperature unit that displayed in the device status.

#### **Lightboard Brightness**

Adjust the brightness of the device light.

### Barrier Material

Select the material of the barrier gate. You can select the barrier material from the drop-down list.



#### Note

The barrier material will affect the device working. Select a correct barrier material or the barrier may not open.

---

### Lane Length

The width of the lane. You can set the lane width.



#### Note

The lane width will affect the device working. Set a correct lane width or the barrier may not open.

---

### Do Not Open Gate When Lane is Not Clear

If there is someone or something in the lane, the gate will not open even if the credential is authenticated.

This function is designed to avoid more than one person passing through the gate with only one authentication.

### Opening/Closing Barrier Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.



#### Note

The recommended value is 6.

---

### Memory Mode

Multiple cards presenting for multiple persons 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 closed automatically.

4. Click **OK**.

## 12.7.2 Configure Device Parameters

After adding the access control device, you can set its parameters such as network parameters.

### Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

### Before You Start

Add access control device to the client, and make sure the device supports RS-485 interface.

### Steps

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters**.
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, and connection mode in the drop-down list.
6. Click **Save**.
  - The configured parameters will be applied to the device automatically.
  - When you change the connection mode, the device will reboot automatically.

### Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

### Steps



#### Note

This function should be supported by the device.

---

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters**.
3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
4. Select the Wiegand channel No. and the communication mode from the drop-down list.



#### Note

**Communication Direction** is **Accepted** by default, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.

---

5. Check **Enable Wiegand** to enable the Wiegand function.
6. Click **Save**.
  - The configured parameters will be applied to the device automatically.
  - After changing the communication direction, the device will reboot automatically.

### Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

### Steps

---



The function should be supported by the access control device and the card reader.

---

1. Enter the Access Control module.
  2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
  3. Select an access control device in the device list and click **M1 Card Encryption Verification** to enter the M1 Card Encryption Verification page.
  4. Set the switch to on to enable the M1 card encryption function.
  5. Set the sector ID.
- 



- The sector ID ranges from 1 to 100.
  - By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.
- 

6. Click **Save** to save the settings.
- 

## 12.8 Door/Elevator Control

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

---



For the user with door/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or the icons used for control will not show. For setting the user permission, refer to .

---

### 12.8.1 Control Door Status

You can control the status for the door(s), including unlock door, locking door, remaining the door unlock, remaining the door locked, remain all unlocked, etc.

#### Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (doors). For details, refer to **Person Management** and **Set Access Group to Assign Access Authorization to Persons** .
- Make sure the operation user has the permission of the access points (doors).

### Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.



### Note

For managing the access point group, refer to [\*\*\*Group Management\*\*\*](#).

---

The doors in the selected access control group will display.

3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.
- 



### Note

For **Remain All Unlocked** and **Remain All Locked**, ignore this step.

---

4. Click the following buttons to control the door.
- 

#### Unlock Door

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

#### Lock Door

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

#### Remain Unlocked

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

#### Remain Locked

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

#### Remain All Unlocked

All doors in the group will be unlocked (no matter closed or open). All the persons can access the doors with no credentials required.

#### Remain All Locked

All doors in the group will be closed and locked. No person can access the doors even if he/she has the authorized credentials, except the super users.

#### Capture

Capture a picture manually.

---



### Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client.

---

#### Remotely Unlocking Door Station

When the group includes door stations, you can check **Lock1** or **Lock2**, then click **Unlock Door** to unlock the door station.



### Note

By default, **Lock1** is checked for door stations.

---

### Refresh Status

Click **Refresh Status** to get the door's newest status.

### Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

## 12.8.2 Check Real-Time Access Records

The real-time access records can be displayed in the client. Also, you can view the person information.

### Before You Start

You have added person(s) and access control device(s) to the client. For details, refer to [\*\*Person Management\*\*](#) and [\*\*Add Device\*\*](#).

### Steps

1. Click **Monitoring** to enter monitoring module.

Real-time access records are displayed on the bottom of the page. You can view record details



### Note

You can right click the column name of access event table to show or hide the column according to actual needs.

---

2. **Optional:** Select an access point group from the drop-down list in the upper-right corner to show the real time access records of the selected group.
3. **Optional:** Check the event type and event status.

The detected events of checked type and status will be displayed in the list below.

4. **Optional:** Check **Show Latest Event** to view the latest access record.

The record list will be listed reverse chronologically.

5. **Optional:** Click  to view details.
- 



### Note

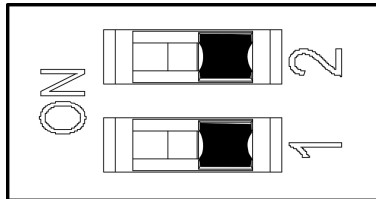
In the pop-up window, you can click  to view details in full screen.

---

## Appendix A. DIP Switch

### A.1 DIP Switch Description

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



**Figure A-1 DIP Switch**

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

### A.2 DIP Switch Corresponded Functions

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

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

## Appendix B. Button Configuration Description

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

| Level-1 Configuration No. | Description         | Level-1 Configuration No. and Functions                                                                                                                                                                                                                                                                                        | Notes                                                                                 |
|---------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 1                         | Study Mode          | 1-Exit Study Mode/<br>Normal Mode<br>2-Study Mode<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.                                                                                                                   | If the device is equipped with access control board, you can only set via DIP switch. |
| 2                         | keyfob Pairing Mode | 1-Normal Mode<br>2-Pairing Mode<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.                                                                                                                                   | If the device is equipped with access control board, you can only set via DIP switch. |
| 3                         | Passing Mode        | 1-Both sides under control<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.<br><br>2-Entrance under control; exit prohibited<br>3-Entrance under control; exit on inductive mode<br>4-Both sides on inductive mode |                                                                                       |

| Level-1 Configuration No. | Description | Level-1 Configuration No. and Functions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Notes |
|---------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                           |             | 5-Entrance on inductive mode; exit under control<br>6-Entrance on inductive mode; exit prohibited<br>7-Both sides prohibited<br>8-Entrance prohibited; exit under control<br>9-Entrance prohibited; exit on inductive mode<br>10-Entrance under control; exit remaining open<br>11-Entrance under control; exit on free mode<br>12-Entrance on inductive mode; exit remaining open<br>13-Entrance on inductive mode; exit on free mode<br>14-Entrance prohibited; exit remaining open<br>15-Entrance prohibited; exit on free mode<br>16-Entrance remaining open; exit under control<br>17-Entrance remaining open; exit on inductive mode |       |

| Level-1 Configuration No. | Description           | Level-1 Configuration No. and Functions                                                                                                                                                                                                                                                                                                                                                          | Notes |
|---------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                           |                       | 18-Entrance remaining open; exit remaining open<br>19-Entrance remaining open; exit on free mode<br>20-Entrance remaining open; exit prohibited<br>21-Entrance on free mode; exit under control<br>22-Entrance on free mode; exit on inductive mode<br>23-Entrance on free mode; exit remaining open<br>24-Entrance on free mode; exit on free mode<br>25-Entrance on free mode; exit prohibited |       |
| 4                         | Memory Mode           | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 2 will be displayed on the display screen.                                                                                                                                                                                                               |       |
| 5                         | keyfob Remote Control | 1-one to one<br>2-one to multiple<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.                                                                                                                                                                                                   |       |

| Level-1 Configuration No. | Description                    | Level-1 Configuration No. and Functions                                                                                                                                                    | Notes |
|---------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| 6                         | Barrier Opening Speed          | 1-1, 2-2, ...10-10<br> <b>Note</b><br>By default, 5 will be displayed on the display screen.              |       |
| 7                         | Barrier Closing Speed          | 1-1, 2-2, ...10-10<br> <b>Note</b><br>By default, 5 will be displayed on the display screen.              |       |
| 8                         | Card Reading on the Alarm Area | 1-Do not open<br>2-Open<br> <b>Note</b><br>By default, 2 will be displayed on the display screen.       |       |
| 9                         | Enter Duration                 | 5-5s, 6-6s, 7-7s, ..., 60-60s<br> <b>Note</b><br>By default, 5 will be displayed on the display screen. |       |
| 10                        | Exit Duration                  | 5-5s, 6-6s, 7-7s, ..., 60-60s<br> <b>Note</b><br>By default, 5 will be displayed on the display screen. |       |
| 11                        | IR Sensing Duration            | 0-0s, 1-1s, 2-2s,..., 25-25s                                                                                                                                                               |       |

| Level-1 Configuration No. | Description                    | Level-1 Configuration No. and Functions                                                                                                                                                                                         | Notes            |
|---------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
|                           |                                |  <b>Note</b><br>By default, 0 will be displayed on the display screen.                                                                         |                  |
| 12                        | Intrusion Duration             | 0-0s, 1-1s, 2-2s,..., 20-20s<br><br> <b>Note</b><br>By default, 0 will be displayed on the display screen.                                     |                  |
| 13                        | Overstay Duration              | 0-0s, 1-1s, 2-2s,..., 20-20s<br><br> <b>Note</b><br>By default, 0 will be displayed on the display screen.                                    |                  |
| 14                        | Delay Time for Barrier Closing | 0-0s, 1-1s, 2-2s, 3-3s, 4-4s, 5-5s<br><br> <b>Note</b><br>By default, 0 will be displayed on the display screen.                             |                  |
| 15                        | Control Mode                   | 1-Button Configuration<br>2-DIP Switch on Access Control Board<br><br> <b>Note</b><br>By default, 1 will be displayed on the display screen. |                  |
| 18                        | Lane Number                    | 1-Dual Lanes                                                                                                                                                                                                                    | Unable to change |

| Level-1 Configuration No. | Description           | Level-1 Configuration No. and Functions                                                                                                                                                   | Notes                                     |
|---------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
|                           |                       | 2-Single Lane<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.                  |                                           |
| 19                        | Motor Rotation        | 1-Clockwise<br>2-Anticlockwise<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. | Unable to change                          |
| 21                        | Volume                | 1-0, 2-1, 3-2, 4-3, 5-4<br> <b>Note</b><br>By default, 2 will be displayed on the display screen.      | The device will be muted when set to "1". |
| 22                        | Authenticated Passing | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.        | Unable to change via button               |
| 23                        | Invalid Card No.      | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.        | Unable to change via button               |

| Level-1 Configuration No. | Description                | Level-1 Configuration No. and Functions                                                                                                                                            | Notes                       |
|---------------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 24                        | Fingerprint Unmatched      | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.   | Unable to change via button |
| 25                        | Climbing over Barrier      | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.   |                             |
| 26                        | Reverse Passing            | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. |                             |
| 27                        | Exceeding Passing Duration | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. |                             |
| 28                        | Intrusion Alarm            | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. |                             |

| Level-1 Configuration No. | Description                       | Level-1 Configuration No. and Functions                                                                                                                                            | Notes                       |
|---------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 29                        | Forced Passing                    | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.   | Unable to change via button |
| 30                        | Tailgating Alarm                  | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen.   |                             |
| 31                        | Unauthorized Passing              | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. | Unable to change via button |
| 32                        | Exceeding Authentication Duration | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. | Unable to change via button |
| 33                        | Failed Authentication             | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. | Unable to change via button |

## DS-K3B631X Series Swing Barrier

---

| Level-1 Configuration No. | Description        | Level-1 Configuration No. and Functions                                                                                                                                          | Notes                       |
|---------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 34                        | Expired Credential | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. | Unable to change via button |
| 35                        | Overstaying Alarm  | 1-Disable<br>2-Enable<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. |                             |
| 36                        | Barrier Material   | 1-Acrylic<br>2-Stainless Steel<br>3-Glass                                                                                                                                        |                             |
| 37                        | Barrier Length     | 1-550<br>2-600<br>3-650<br>4-700<br>5-750<br>6-800<br>7-850<br>8-900<br>9-950<br>10-1000<br>11-1100<br>12-1200<br>13-1300<br>14-1400                                             |                             |

| Level-1 Configuration No. | Description             | Level-1 Configuration No. and Functions                                                                                                                                                                                   | Notes                                                    |
|---------------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
|                           |                         |  <b>Note</b><br>By default, 8 will be displayed on the display screen.                                                                   |                                                          |
| 38                        | Motor Inspection        | 1-Disable<br>2-Enable on Main Lane<br>3-Enable on Sub Lane<br><br> <b>Note</b><br>By default, 1 will be displayed on the display screen. |                                                          |
| 39                        | Brightness of Light     | 0-0, 1-1, 2-2, ... , 10-10<br><br> <b>Note</b><br>By default, 3 will be displayed on the display screen.                               | The higher the value is, the brighter the light will be. |
| 40                        | Self-check Voice Prompt | 1-Disable<br>2-Enable<br><br> <b>Note</b><br>By default, 2 will be displayed on the display screen.                                    |                                                          |
| 41                        | Study Mode Voice Prompt | 1-Disable<br>2-Enable<br><br> <b>Note</b><br>By default, 2 will be displayed on the display screen.                                    |                                                          |

## DS-K3B631X Series Swing Barrier

| Level-1 Configuration No. | Description              | Level-1 Configuration No. and Functions                                                                                                                                   | Notes                       |
|---------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 42                        | c                        | 4-4, 6-6, 8-8,<br> <b>Note</b><br>By default, 4 will be displayed on the display screen. | Unable to change via button |
| 43                        | Application Mode         | 1-Wind-proof<br>2-Indoor<br>By default, 1 will be displayed on the display screen.                                                                                        |                             |
| 44                        | Barrier Recover Duration | 1-Normal Speed<br>2-Fast Recover<br>By default, 1 will be displayed on the display screen.                                                                                |                             |
| 45                        | Brake                    | 1-Disable<br>2-Barrier Position Exception<br>3-Intrusion<br>By default, 2 will be displayed on the display screen.                                                        |                             |
| 46                        | Brake Angle              | 1-5°<br>2-10°<br>3-15°<br>By default, 1 will be displayed on the display screen.                                                                                          |                             |
| 47                        | IR Sensing               | 1-Single Triggered<br>2-Triggered Simultaneously                                                                                                                          |                             |

## DS-K3B631X Series Swing Barrier

---

| Level-1 Configuration No. | Description        | Level-1 Configuration No. and Functions                                                                                                                                             | Notes |
|---------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                           |                    | By default, 1 will be displayed on the display screen.                                                                                                                              |       |
| 48                        | Fan                | 1-Disabled<br>2-Enabled<br>By default, 2 will be displayed on the display screen.                                                                                                   |       |
| 49                        | Barrier Height     | 1-700<br>2-1200<br>3-1400<br>4-1600<br>5-1800<br>By default, 5 will be displayed on the display screen.                                                                             |       |
| 99                        | Restore to Default | 1- Default<br>2- Start<br> <b>Note</b><br>By default, 1 will be displayed on the display screen. |       |

## Appendix C. 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<br>Authentication Failed | Visual and Audible |
| Barrier Obstructed                    | None               |

## Appendix D. Table of Audio Index Related Content

---

 **Note**

- If the device is not equipped with access control board, the loudspeaker shall be connected to the main optional board.
  - If the device is equipped with access control board, the loudspeaker shall be connected to the access control board. You can set custom broadcasting context via web.
- 

| Content                    |
|----------------------------|
| Climbing over the barrier. |
| Reverse passing.           |
| Passing timeout.           |
| Intrusion.                 |
| Tailgating.                |
| Overstay.                  |

## Appendix E. Error Code Description

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

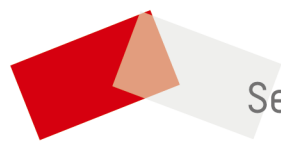
| Error Reason                                                                                                                 | Code | Error Reason                       | Code |
|------------------------------------------------------------------------------------------------------------------------------|------|------------------------------------|------|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

---

## DS-K3B631X Series Swing Barrier

---

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



See Far, Go Further