DS-K3B961TX Series Swing Barrier

User Manual

Legal Information

About this Document

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

About this Product

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

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

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.

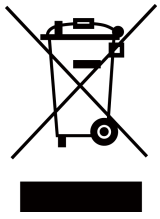
Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU



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



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

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

COMPLIANCE NOTICE

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

Safety Instruction

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

The precaution measure is divided into Dangers and Cautions:

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

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

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

⚠ Danger:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The equipment must be connected to an earthed mains socket-outlet.
- Shock hazard! Disconnect all power sources before maintenance.
- Do not touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- ϟ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- 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.)

⚠ 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.
- Stainless steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.

- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

Available Models

Product Name	Model	Description
Swing Barrier	DS-K3B961TX-L	Left Pedestal
	DS-K3B961TX-M	Middle Pedestal
	DS-K3B961TX-R	Right Pedestal

Contents

Chapter 1 Overview 1
1.1 Introduction 1
1.2 Main Features 1
1.3 Light Description 2
Chapter 2 System Wiring 4
Chapter 3 Installation 9
Chapter 4 General Wiring 10
4.1 Components Introduction 10
4.2 Wiring 12
4.3 Terminal Description 13
4.3.1 Main Lane Control Board Terminal Description 13
4.3.2 Sub Lane Control Board Terminal Description 14
4.3.3 Main Access Control Board Terminal Description 15
4.3.4 Sub Access Control Board Terminal Description 16
4.3.5 Main User Extended Interface Board 18
4.3.6 Sub User Extended Interface Board 21
4.3.7 User Core Board Terminal Description 23
4.3.8 RS-485 Wiring 23
4.3.9 RS-232 Wiring 24
4.3.10 Wiegand Wiring 24
4.3.11 Barrier Control Wiring 25
4.3.12 Alarm Output Wiring 25
4.3.13 Alarm Input Wiring 26
Chapter 5 Device Settings 28
5.1 Set Study Mode 28
5.2 Pair Keyfob (Optional) 29

5.3 Initialize Device 30
Chapter 6 Activation 33
6.1 Activate via Device 33
6.2 Activate via Web Browser 34
6.3 Activate via SADP 35
6.4 Activate Device via iVMS-4200 Client Software 36
Chapter 7 Quick Operation via Web Browser 37
7.1 Time Settings 37
7.2 Environment Settings 37
7.3 Privacy Settings 38
Chapter 8 Operation via Web Browser 39
8.1 Login 39
8.2 Overview 39
8.3 Person Management 40
8.4 Search Event 41
8.5 Device Management 41
8.6 Configuration 42
8.6.1 Set Local Parameters 42
8.6.2 View Device Information 42
8.6.3 Set Time 42
8.6.4 Set DST 43
8.6.5 Change Administrator's Password 43
8.6.6 Online Users 44
8.6.7 View Device Arming/Disarming Information 44
8.6.8 Network Settings 44
8.6.9 Set Video and Audio Parameters 45
8.6.10 Set Image Parameters 46
8.6.11 Event Linkage 46

8.6.12 Access Control Settings 47
8.6.13 Turnstile 51
8.6.14 Card Settings 56
8.6.15 Set Privacy Parameters 57
8.6.16 Set Biometric Parameters 58
8.6.17 Screen Display 60
8.6.18 Notice Publication 61
8.6.19 Customize Audio Content 62
8.6.20 Upgrade and Maintenance 64
8.6.21 Device Debugging 65
8.6.22 Component Status 65
8.6.23 Log Query 66
8.6.24 Certificate Management 66
Chapter 9 Client Software Configuration 68
9.1 Configuration Flow of Client Software 68
9.2 Device Management 69
9.2.1 Add Device 69
9.2.2 Reset Device Password 71
9.2.3 Manage Added Devices 72
9.3 Group Management 73
9.3.1 Add Group 73
9.3.2 Import Resources to Group 73
9.4 Person Management 74
9.4.1 Add Organization 74
9.4.2 Import and Export Person Identify Information 75
9.4.3 Get Person Information from Access Control Device 77
9.4.4 Issue Cards to Persons in Batch 78
9.4.5 Report Card Loss 78

9.4.6 Set Card Issuing Parameters 79
9.5 Configure Schedule and Template 80
9.5.1 Add Holiday 80
9.5.2 Add Template 81
9.6 Set Access Group to Assign Access Authorization to Persons 82
9.7 Configure Advanced Functions 84
9.7.1 Configure Device Parameters 85
9.7.2 Configure Other Parameters 92
9.8 Door/Elevator Control 94
9.8.1 Control Door Status 95
9.8.2 Check Real-Time Access Records 96
Appendix A. Tips When Collecting/Comparing Face Picture 98
Appendix B. DIP Switch 99
B.1 DIP Switch Description 99
B.2 DIP Switch Corresponded Functions 99
B.3 Light Board DIP Switch Description 100
Appendix C. Event and Alarm Type 106
Appendix D. Error Code Description 107
Appendix E. Communication Matrix and Device Command 109

Chapter 1 Overview

1.1 Introduction

The flap barrier with two barriers and 24 IR lights is designed to detect unauthorized entrance or exit. By adopting the flap barrier integratedly with the access control system, person should authenticate to pass through the lane via swiping IC or ID card, scanning QR code, etc. It is widely used in attractions, stadiums, construction sites, residences, etc.

1.2 Main Features

- 32-bit high-speed processor
- IP address conflict detection
- Remote control and management
- Online/offline operation
- 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, sensing 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; If the device is installed with lithium battery (optional), the barrier remains open 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
- Up to 10,0000 faces, up to 50,0000 cards and up to 100,000 events except can be added

- Custom broadcasting content
- LED indicates the entrance/exit and passing status
- White indicators for card and QR code authentication;
  Red and green arrow indicators;
  Adjustable brightness and color of entrance light and side light
- IR emergency mode and Custom Anti-pinch for Door Closing

1.3 Light Description

Side Light

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

Note

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

Entrance Light

Before Passing

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

During Passing

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

Barrier Light

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

Card Light

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

Arrow Light

- The arrow light stays off when the device is on standby mode.
- The light on the right side will flash green ready for authentication.
- The light on both left and right side will stay green for authenticated passing.
- The light on the right side will flash red when authentication fails.

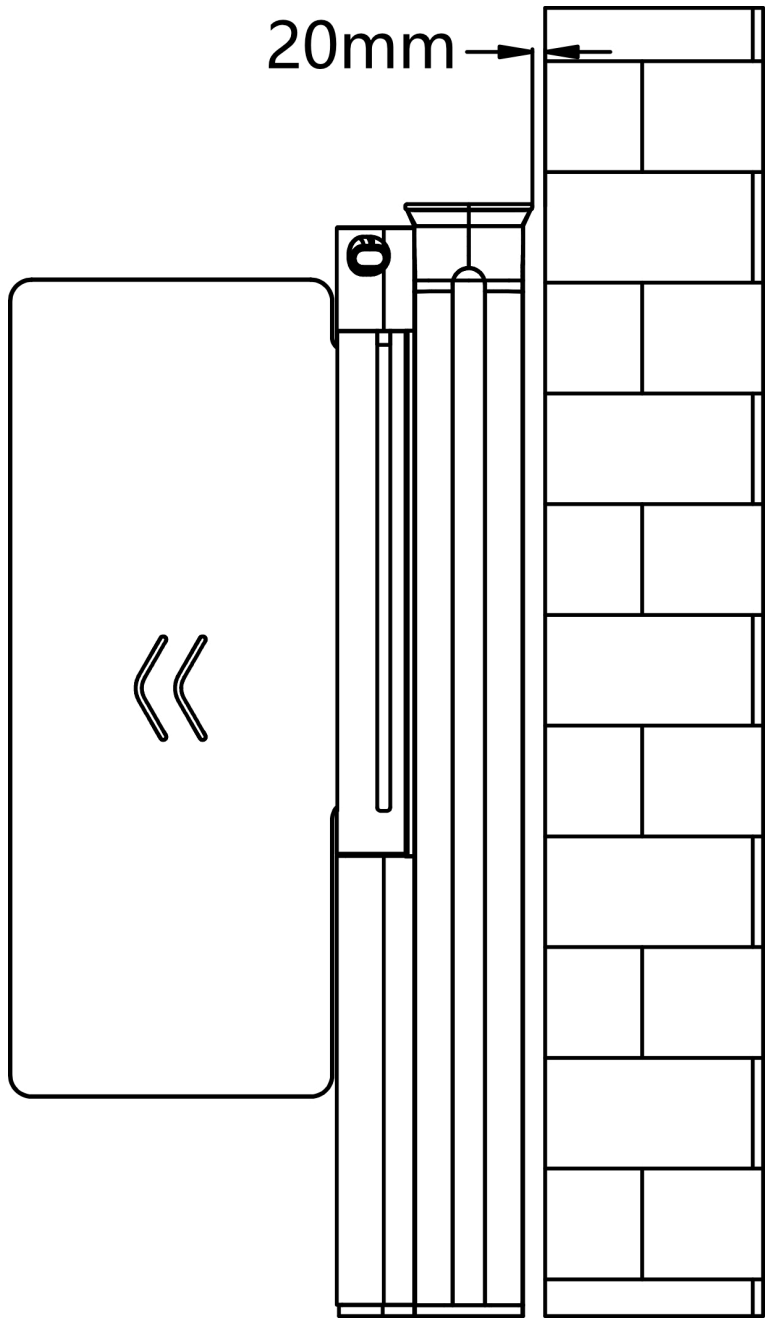
Chapter 2 System Wiring

The preparation before installation and general wiring.

Steps

Note

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



- The dimension is as follows.

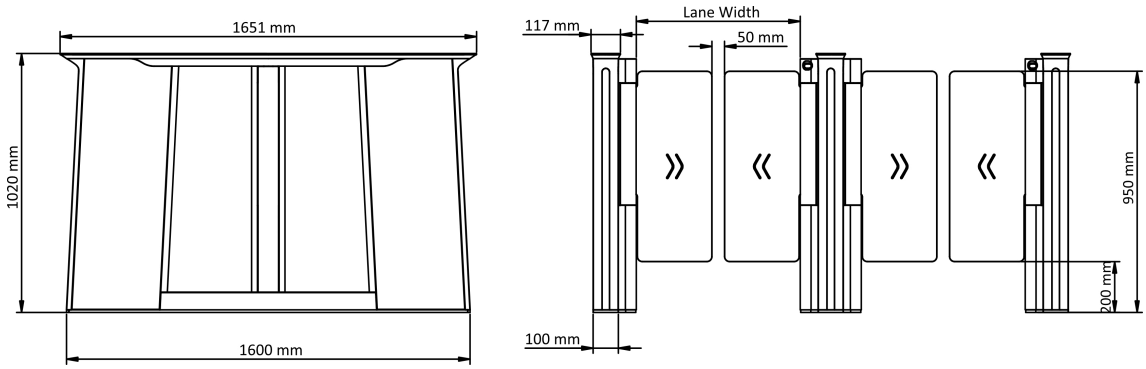


Figure 2-1 Dimension

1. Draw a central line on the installation surface of the left or right pedestal.

   Note

   If the installation area is near the wall, make sure the central line is at least 78.5 mm away from the wall, or you cannot open the pedestal's top panel.

2. Draw other parallel lines for installing the other pedestals.

   Note

   The distance between the nearest two line is L + 242 mm. L represents the lane width.

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

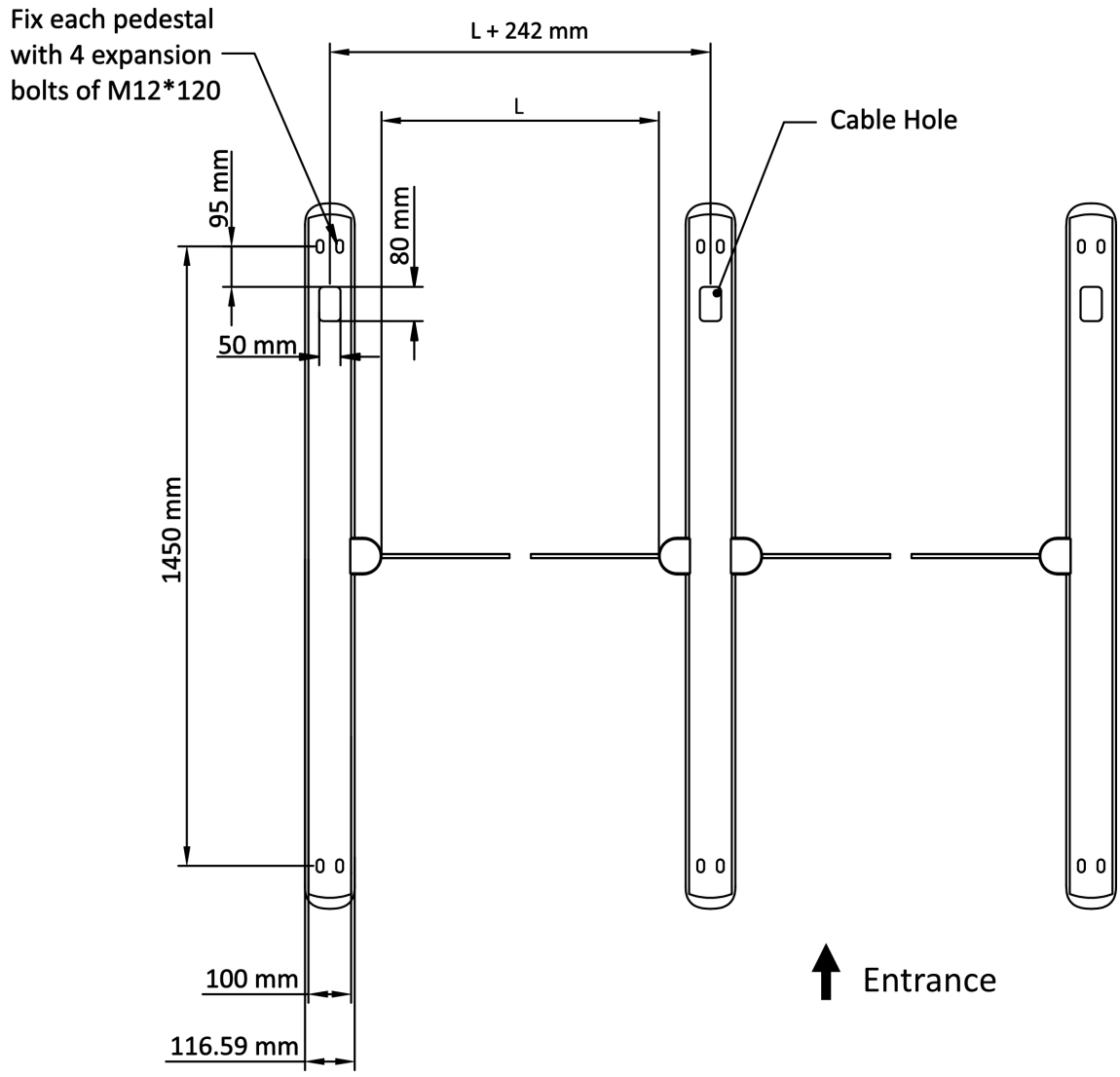


Figure 2-2 Hole Position Diagram

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

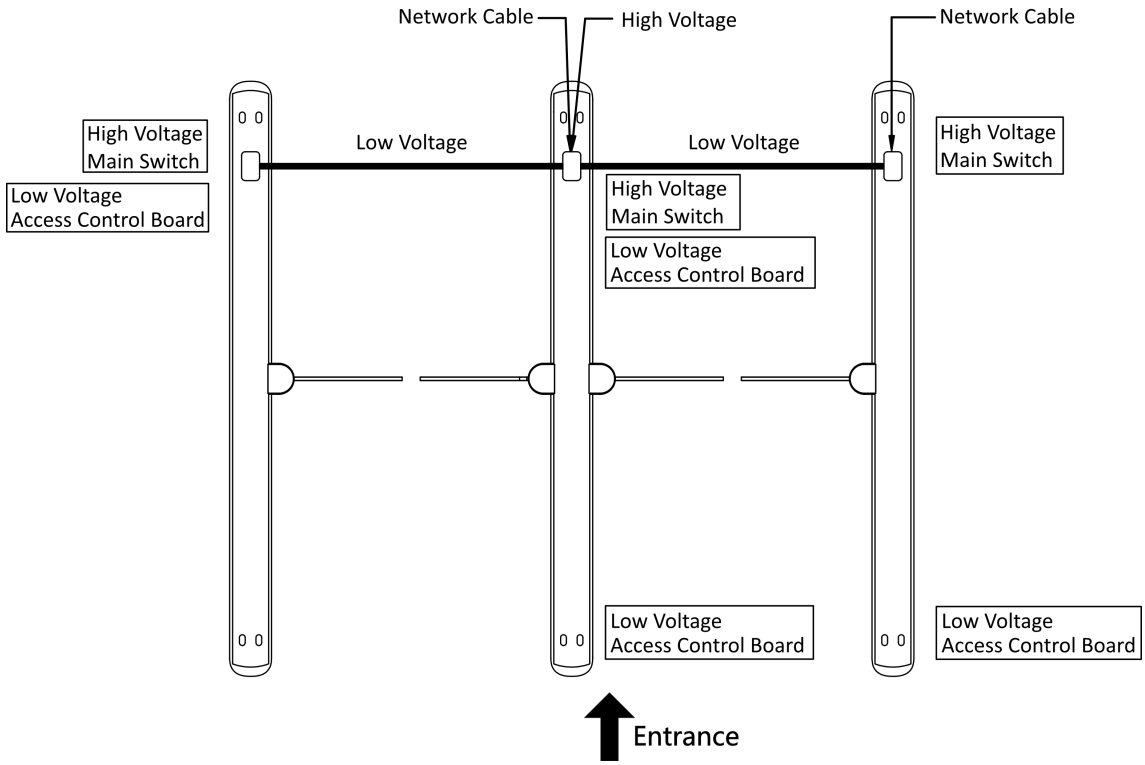


Figure 2-3 System Wiring Diagram (General Wiring)

Note

- The supplied interconnecting cable length is 5.5 m.
- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- If you want to bury both of the AC power cord and the low voltage cable, the two cables should be in separated conduits to avoid interference.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.
- The external AC power cord should be double-insulated.
- The network cable must be CAT5e or the network cable has better performance. And the suggested network cable length should be less than 100 m.

Chapter 3 Installation

1. Before installation, you should disassemble the pedestal with the key.
2. Keep the disassembled components and make sure the accessories are intact.
3. Prepare for system wiring and installation. For details, see ***System Wiring*** .
4. Fix the pedestal to the installation spot with screws.

Scan the QR Code to view the installation guide video.



Chapter 4 General Wiring

Note

- When you should maintain or disassemble the high voltage modules, you should remove the entire high voltage modules and maintain it outside the turnstile. You should unplug the cables that connected to the peripherals before maintenance to avoid destroy of the device.
- When disassembling the high voltage module, you should disconnect the power to avoid injury.
- If only wiring is needed without maintenance, do not remove the high voltage modules.
- The switch and the main lane control board are already connected. The 14 AWG cable to connect between the AC electric supply and the switch should be purchased separately.
- 2 interconnecting cables are supplied: 24 V Power Cable and Communication Cable.
  24 V Power Cable: 5 m long, which is in the middle and right pedestal.
  Communication Cable: 4 m long, CAT5e, which is in the package of middle and right pedestal.

4.1 Components Introduction

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

Note

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

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

Note

The diagram is for reference only.

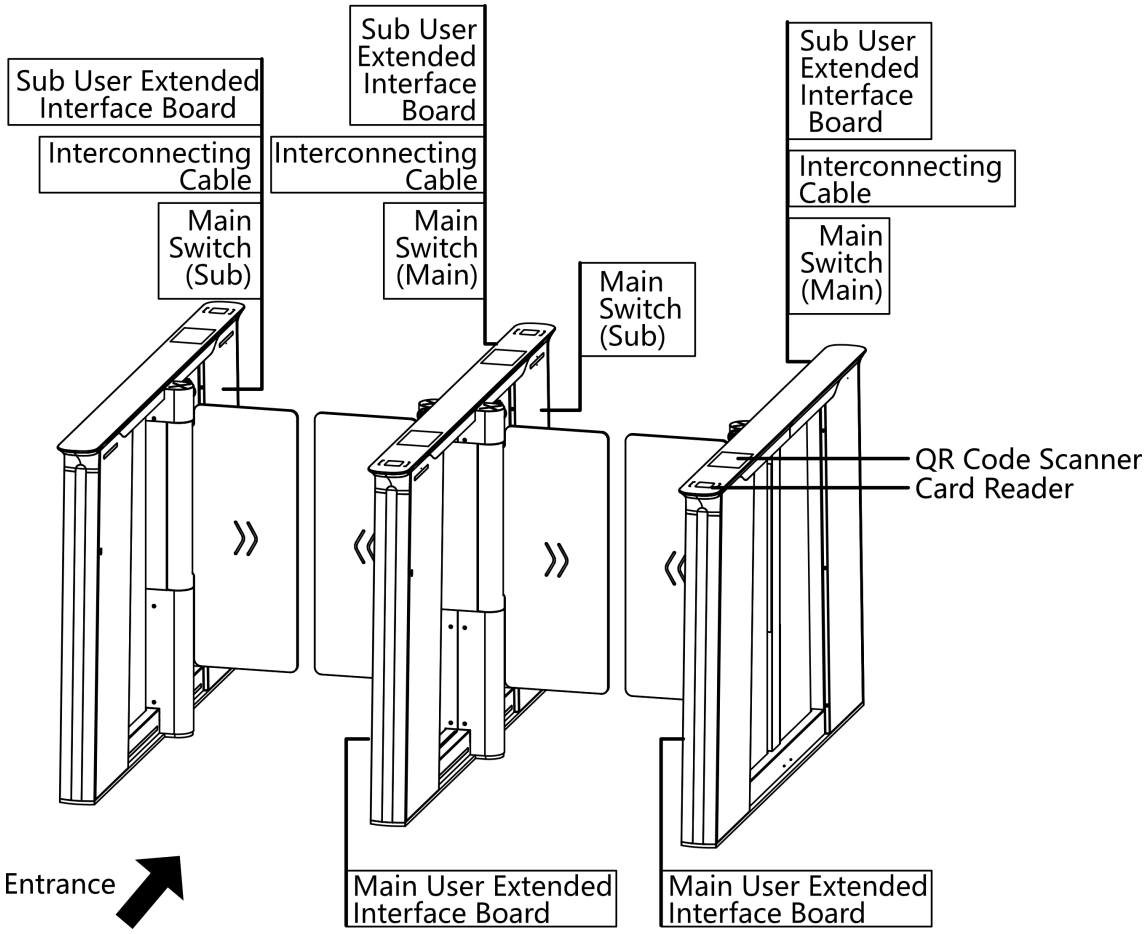


Figure 4-1 Components Diagram

Note

For details about wiring arrangement, refers to the actual device.

The picture displayed below describes the IR adapter and the IR sending/receiving module and their corresponding number on the pedestal.

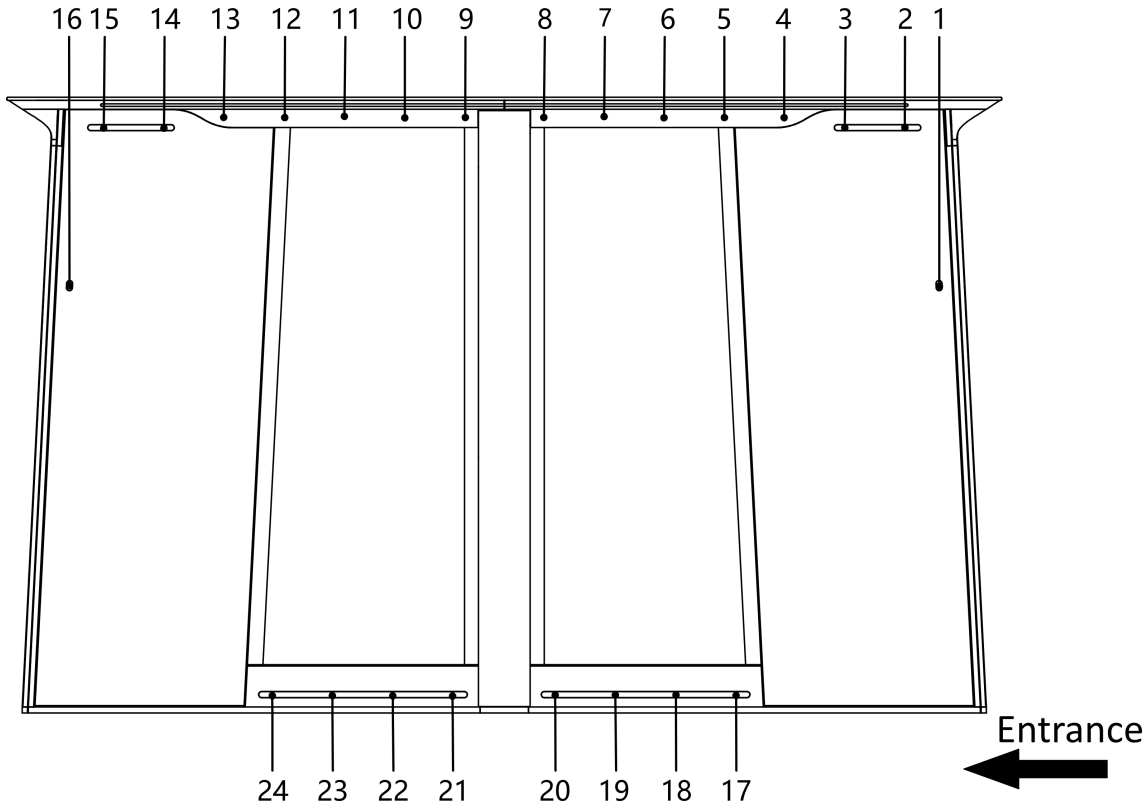


Figure 4-2 IR Modules

Note

- For details about wiring arrangement, refers to the actual device.
- If the turnstile contains two lanes, standing at the entrance position, the IR modules on the left pedestal are the IR sending modules. The IR modules on the right pedestal are the IR receiving modules. The IR modules on the left side of the middle pedestal are the IR receiving modules, while the IR modules on the right side of the middle pedestal are the IR sending modules.
- Safety Instructions can be viewed on the middle panel inside the pedestal.

4.2 Wiring

Scan the QR code to view the wiring guide video.



4.3 Terminal Description

The lane controller contains main lane controller and sub lane controller, which controls the IR beams, motor, and other components' work.

4.3.1 Main Lane Control Board Terminal Description

The main lane control board contains debugging port, access control board communication interface, power interface, supercapacitor, IR adapter and ArrowBoard interface, encoder interface, power supply for motor, brake interface, user extended interface board BUS, and interconnecting interface.

The picture displayed below is the main control board diagram.

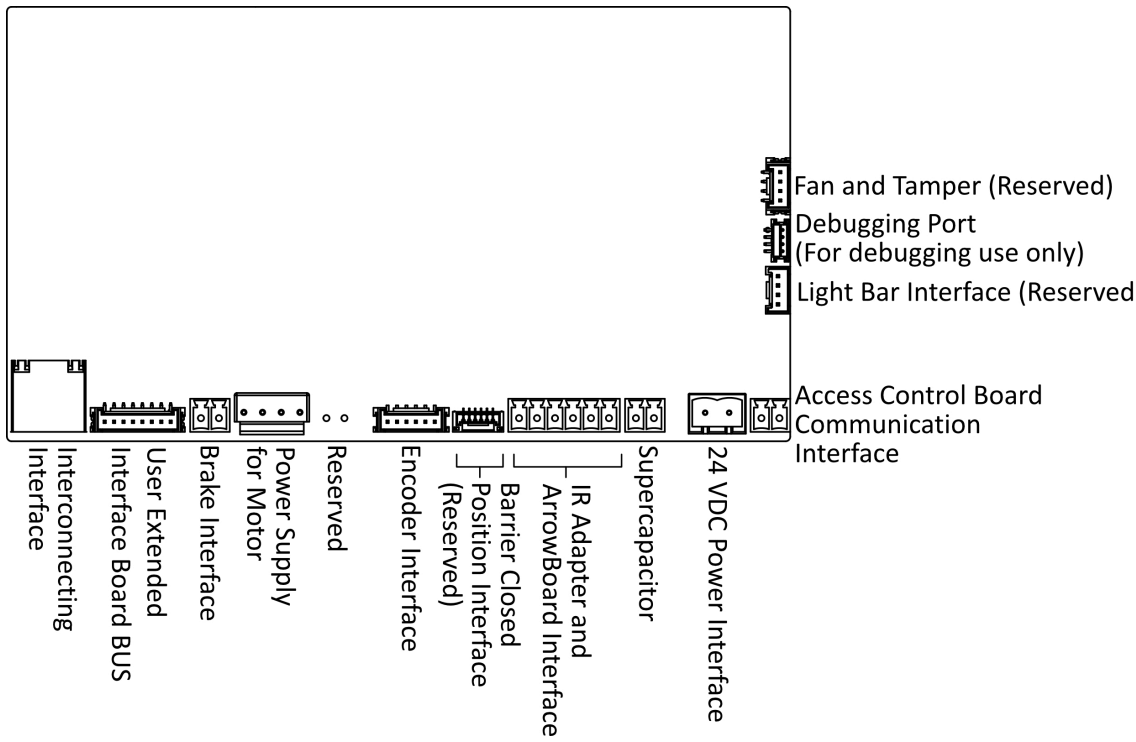


Figure 4-3 Main Lane Control Board Terminal

4.3.2 Sub Lane Control Board Terminal Description

The sub lane control board contains debugging port, access control board communication interface, power interface, supercapacitor, IR adapter and ArrowBoard interface, encoder interface, power supply for motor, brake interface, sub user extended interface board BUS and interconnecting interface.

The picture displayed below is the sub control board diagram.

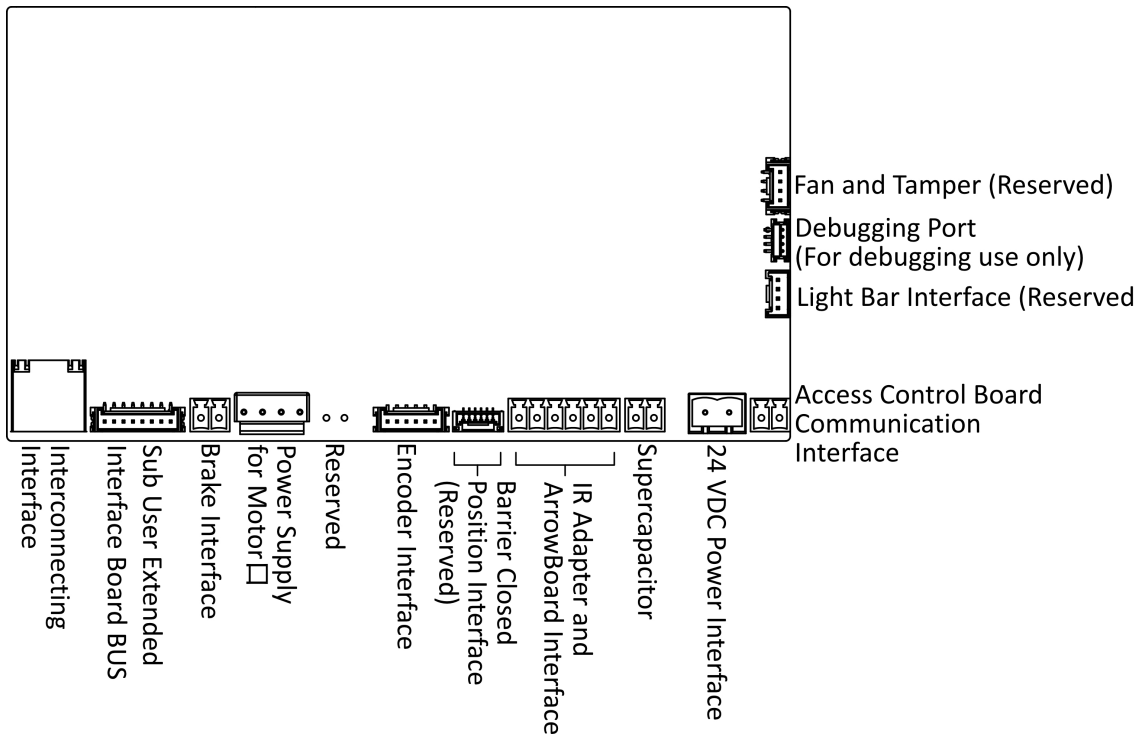


Figure 4-4 Sub Lane Control Board Terminal

4.3.3 Main Access Control Board Terminal Description

The main access control board contains screen adapter interface, sensor interface, loudspeaker interface, IR light interface, user extended interface board and lane control board communication interface, antenna interface, network switch interface, sub access control board interface, power interface, card reader board interface, TF card slot, initialization button, debugging port and USB flash drive interface.

The picture displayed below is the main access control board diagram.

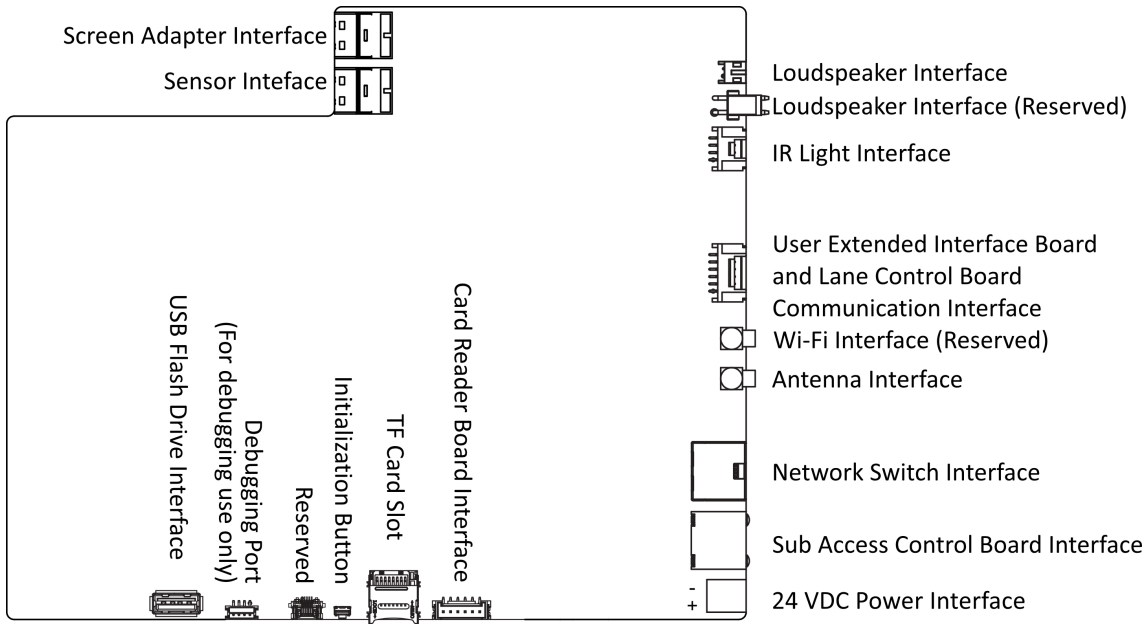


Figure 4-5 Main Access Control Board Terminal

4.3.4 Sub Access Control Board Terminal Description

The sub access control board contains screen adapter interface, sensor interface, loudspeaker interface, IR light interface, user extended interface board and lane control board communication interface, sub access control board interface, power interface, card reader board interface, TF card slot, initialization button, debugging port and USB flash drive interface.

The picture displayed below is the sub access control board diagram.

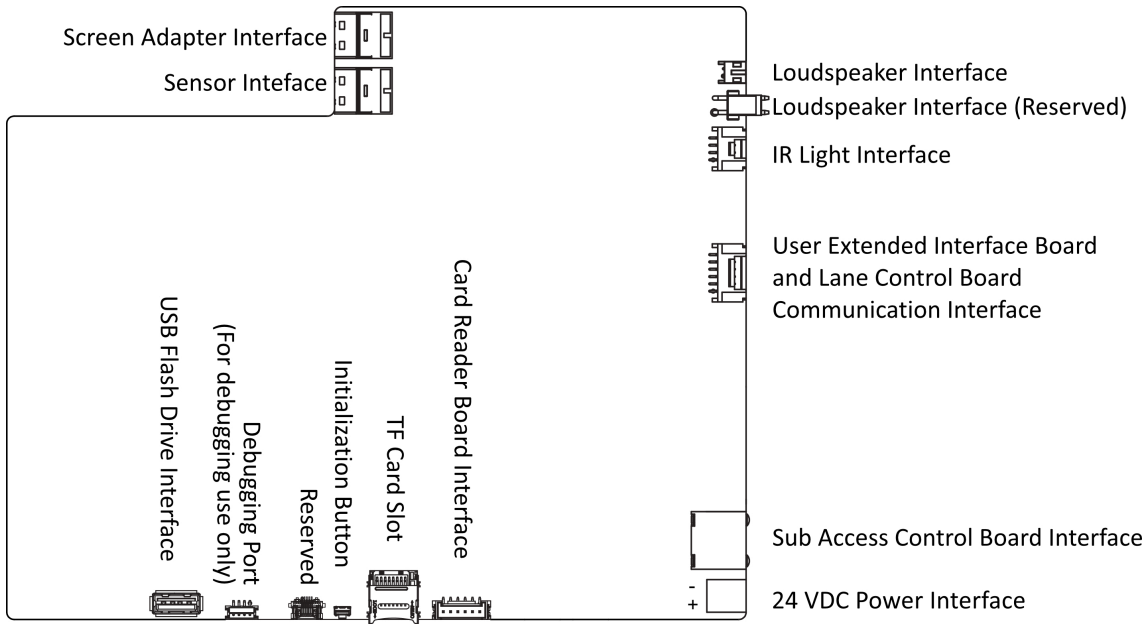


Figure 4-6 Sub Access Control Board Terminal

4.3.5 Main User Extended Interface Board

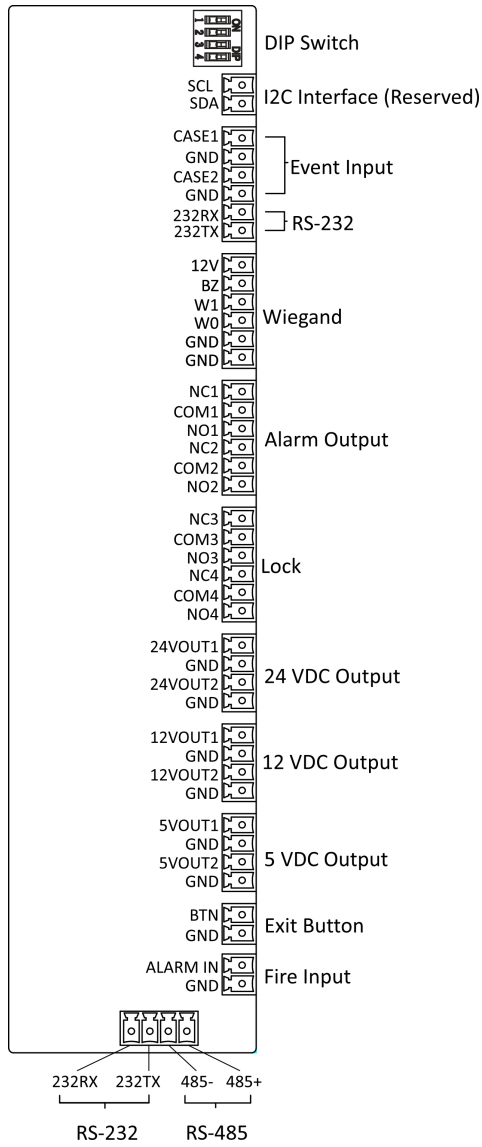


Figure 4-7 Main User Extended Interface

Main User Extended Interface Description		
I2C Interface	SCL	Reserved
	SDA	
Event Input	CASE1	Event Alarm Input 1
	CASE2	Event Alarm Input 2

Main User Extended Interface Description		
	GND	Grounding
RS-232 Interface	232RX	Connect to Card Reader RS-232RX
	232TX	Connect to Card Reader RS-232TX
RS-485	485-	Connect to Card Reader RS485-
	485+	Connect to Card Reader RS485+
Wiegand Card Reader	12 V	12 VDC Power Input
	BZ	Card Reader Buzzer Control Output
	W0	Wiegand Head Read Data Input Data0
	W1	Wiegand Head Read Data Input Data1
	GND	Grounding
Alarm Output	NO/NC1	Alarm Output Relay 1 (Dry Contact)
	COM1	
	NO/NC2	Alarm Output Relay 2 (Dry Contact)
	COM2	
Lock	NO/NC3	Door Relay Output (Dry Contact)
	COM3	
	NO/NC4	
	COM4	
Power Output 1	24VOUT1	24 VDC Power Output 1
	24VOUT2	24 VDC Power Output 2
	GND	Grounding
Power Output 2	12VOUT1	12 VDC Power Output 1
	12VOUT2	12 VDC Power Output 2
	GND	Grounding

Main User Extended Interface Description		
Power Output 3	5VOUT1	5 VDC Power Output 1
	5VOUT1	5 VDC Power Output 2
	GND	Grounding
Exit Button	BTN	Door Signal Input
	GND	Grounding
Fire Input	ALARM IN	Fire Alarm Input
	GND	Grounding

4.3.6 Sub User Extended Interface Board

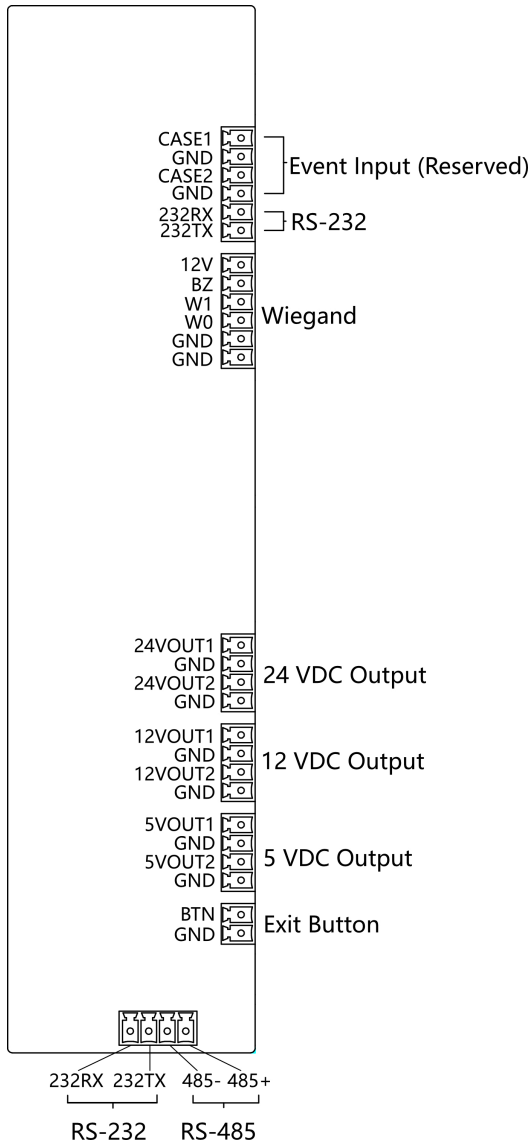


Figure 4-8 Sub User Extended Interface

Main User Extended Interface Description		
Event Input	CASE1	Reserved
	CASE2	
	GND	

Main User Extended Interface Description		
RS-232 Interface	232RX	Connect to Card Reader RS-232RX
	232TX	Connect to Card Reader RS-232TX
RS-485	485-	Connect to Card Reader RS485-
	485+	Connect to Card Reader RS485+
Wiegand Card Reader	12 V	12 VDC Power Input
	BZ	Card Reader Buzzer Control Output
	W0	Wiegand Head Read Data Input Data0
	W1	Wiegand Head Read Data Input Data1
	GND	Grounding
Power Output 1	24VOUT1	24 VDC Power Output 1
	24VOUT2	24 VDC Power Output 2
	GND	Grounding
Power Output 2	12VOUT1	12 VDC Power Output 1
	12VOUT2	12 VDC Power Output 2
	GND	Grounding
Power Output 3	5VOUT1	5 VDC Power Output 1
	5VOUT1	5 VDC Power Output 2
	GND	Grounding
Exit Button	BTN	Door Signal Input
	GND	Grounding

4.3.7 User Core Board Terminal Description

The user core board terminal contains network interface, BUS, USB card reader interface, access control board communication interface, card receiver and RS-485 card reader interface, power interface, programming interface and debugging port.

The picture displayed below is the user core board diagram.

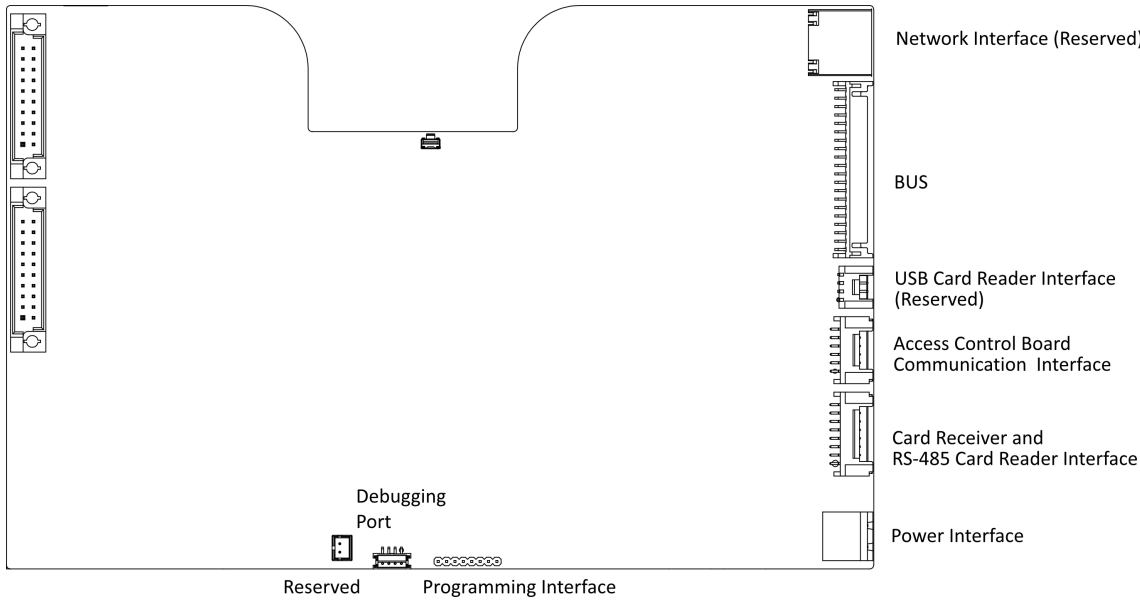


Figure 4-9 User Core Board Terminal

4.3.8 RS-485 Wiring

The main and sub user extended interface board each has one RS-485 interface.

Note

- If connecting the RS-485 with a card reader, by default, the DIP switch of the card reader is: 1 for entrance, and 4 for exit.
- 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.

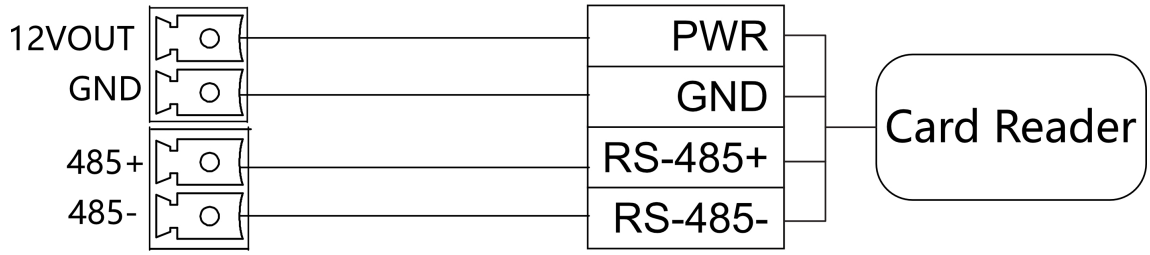


Figure 4-10 RS-485 Wiring

4.3.9 RS-232 Wiring

Note

The main and sub user extended interface board each has two RS-232 interface.

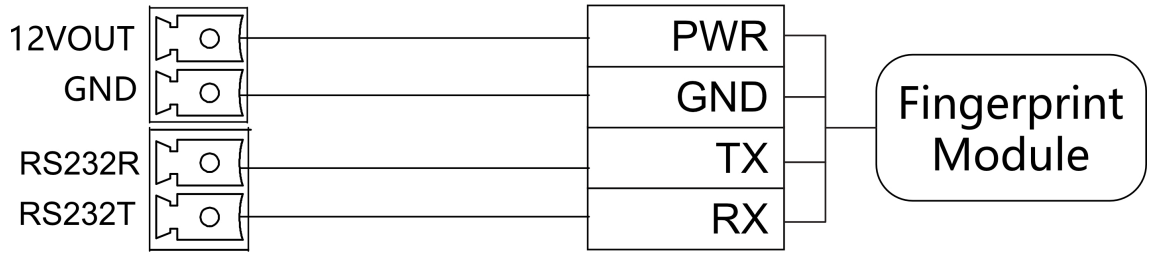
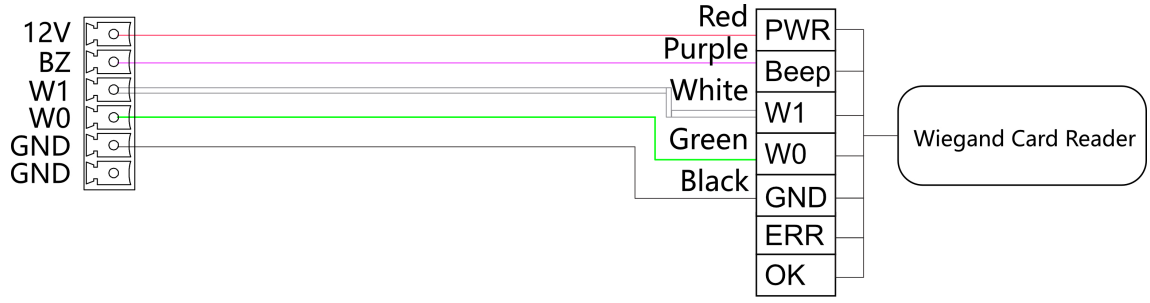


Figure 4-11 RS-232 Wiring

4.3.10 Wiegand Wiring



Note

Connect the OK/ERR/BZ if the access controller should control the LED and buzzer of the Wiegand card reader.

4.3.11 Barrier Control Wiring

According to the barrier control interfaces and the internal relays, the device provides 2 groups of the barrier control signals on the main user extended interface board, including 1 remaining open interface and 1 remaining closed interface.

NO: Remaining Open

NC: Remaining Closed

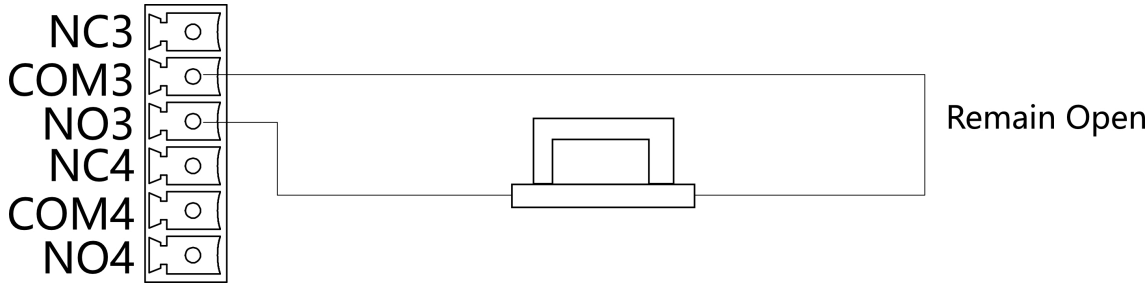


Figure 4-12 Barrier Control Wiring 1

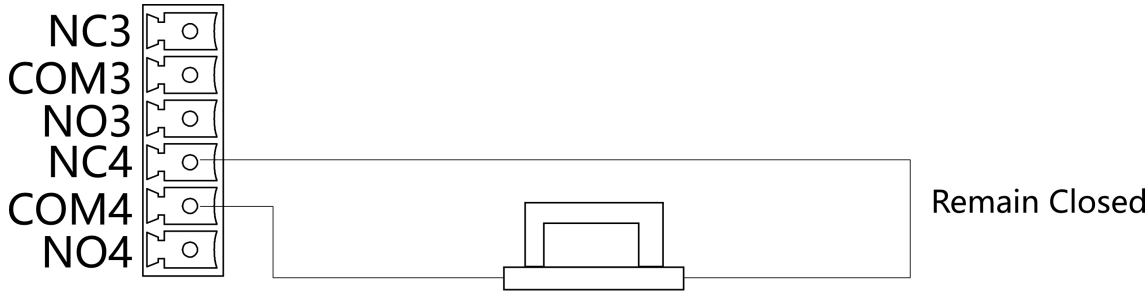


Figure 4-13 Barrier Control Wiring 2

4.3.12 Alarm Output Wiring

On the main user extended interface board, you can wire the alarm output interface.

According to the alarm output interfaces and the internal relays, the device provides 2 groups of the alarm output control signals, including 1 remaining open interface and 1 remaining closed interface.

NO: Remaining Open

NC: Remaining Closed

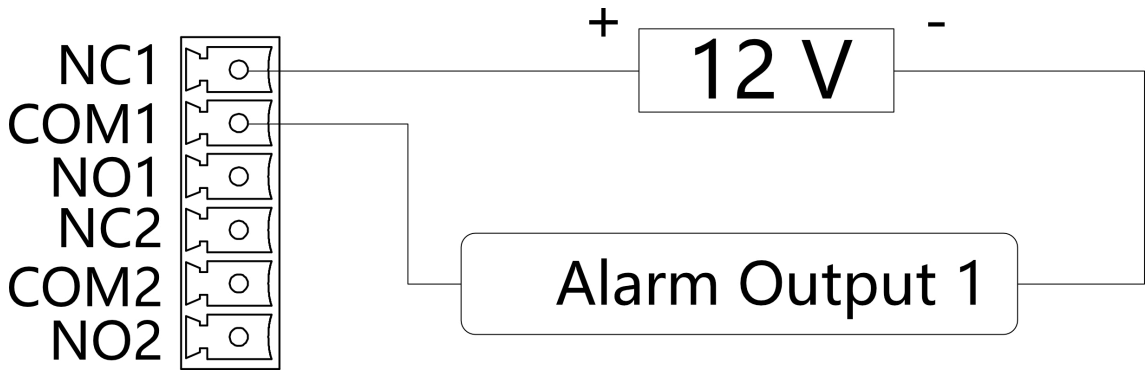


Figure 4-14 Alarm Output Wiring 1

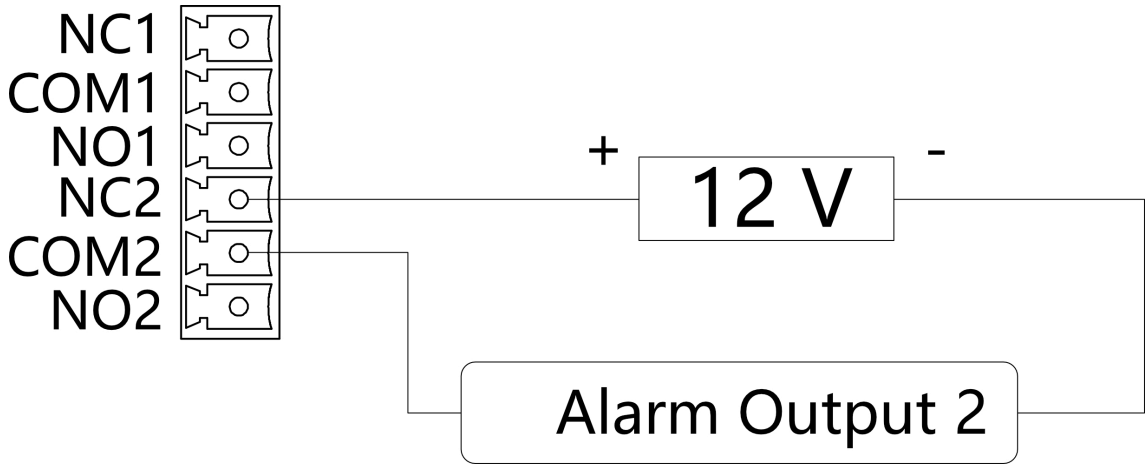


Figure 4-15 Alarm Output Wiring 2

4.3.13 Alarm Input Wiring

On the main user extended interface board, you can wire the fire alarm input interface.

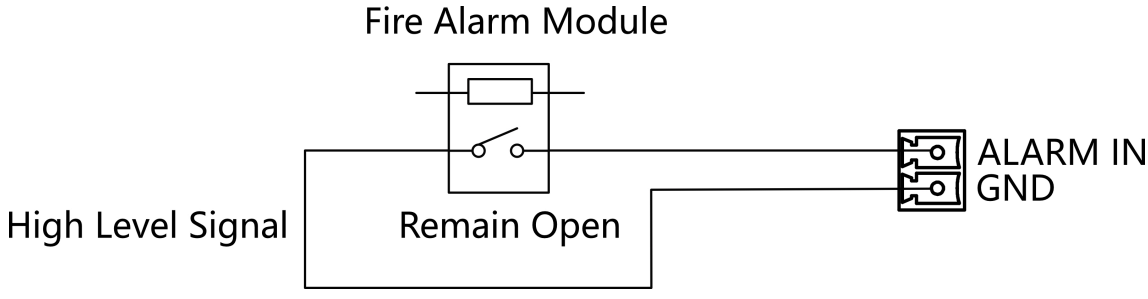


Figure 4-16 Remaining Open

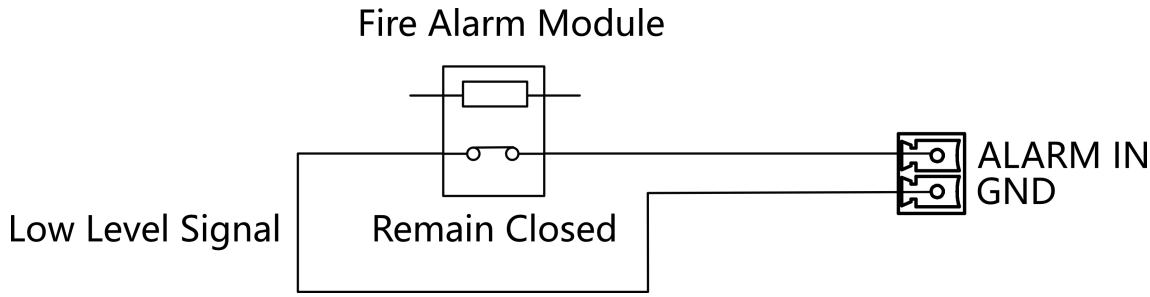


Figure 4-17 Remaining Closed

Chapter 5 Device Settings

After installation and wiring completed, the turnstile will study the open and closed position automatically.

After the learning, the turnstile is in the normal mode. You can also set the turnstile to study mode, normal mode, and pair the keyfob, initialize the hardware via the main user extended interface board (middle/right pedestal).

Study Mode

Study the closed position.

Normal Mode

The device will work properly.

Keyfob Pairing

Pair the keyfob and the turnstile.

5.1 Set Study Mode

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

Steps

1. Set The No.1 of the 4-digit DIP Switch on the main user extended interface board to ON by referring the following figure to enter the study mode.

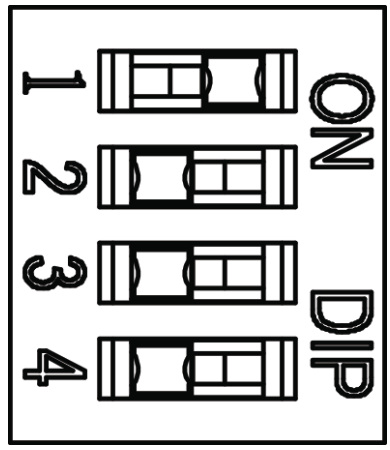


Figure 5-1 Study Mode

2. Adjust the closed position of the barrier.
3. Power on the device.

   The device will remember the current position (closed position) automatically.
4. Power off the device.

5. Set the No.1 switches of the 4-digit DIP Switch on the main user extended interface board by referring to the following figure.

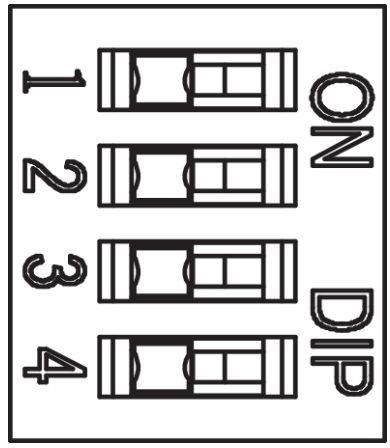


Figure 5-2 Normal Mode

6. 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.

5.2 Pair Keyfob (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 1 Switch on the access control board to the ON side.

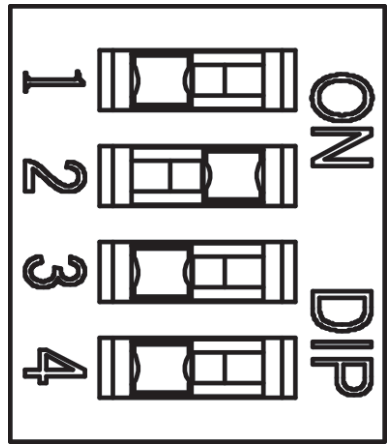


Figure 5-3 Enable Keyfob Paring Mode

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

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

5.3 Initialize Device

Steps

1. Hold the initialization button.



Figure 5-4 Initialization Button Position

2. Power off and reboot the device. The device buzzer buzzes a long beep.
3. When the beep stopped, release the initialization button.

Caution

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

Note

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

The initialization is completed.

Chapter 6 Activation

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

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

The default values of the device are as follows:

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

6.1 Activate via Device

If the device is not activated, you can activate the device after it is powered on.

On the Activate Device page, create a password and confirm the password. Tap **Activate** and the device will activated.

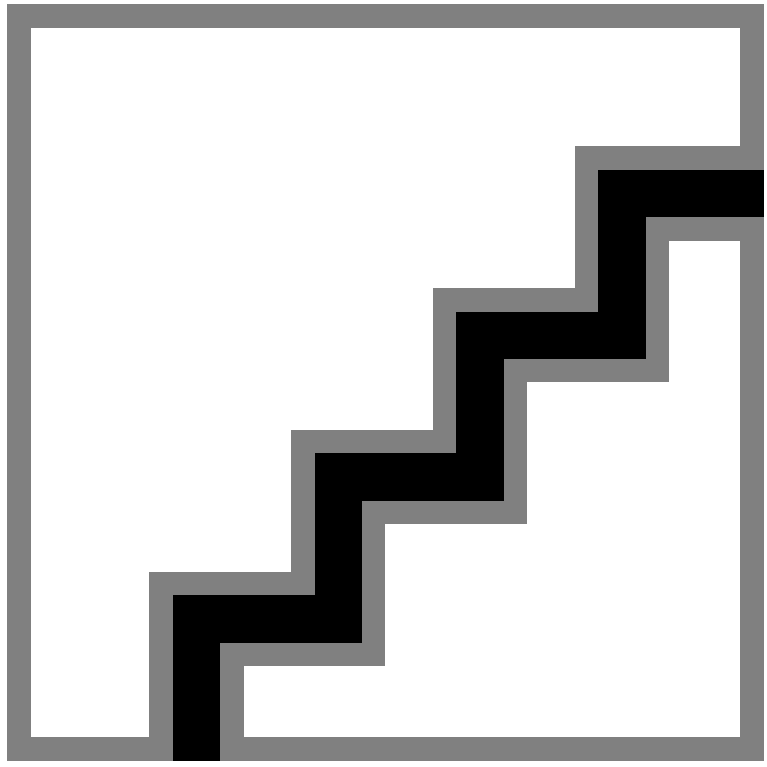


Figure 6-1 Activation Page

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 installer and/or end-user.

Note

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

After activation, you should select language, set password change type, set application mode, set network, set platform parameters, set privacy parameters, and set administrator.

6.2 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.

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

6.3 Activate via SADP

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

Before You Start

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

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

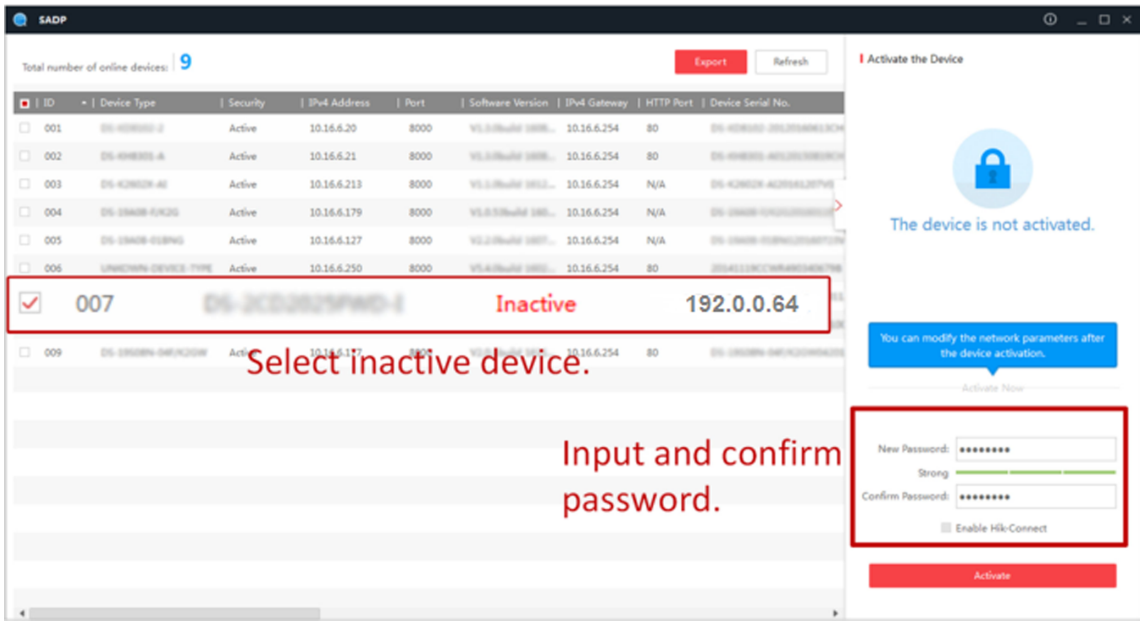
Steps

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

Caution

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

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



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

5. Modify IP address of the device.

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

6.4 Activate Device via iVMS-4200 Client Software

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

Steps

Note

This function should be supported by the device.

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

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

   Caution

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

   Note

   Characters containing admin and nimda are not supported to be set as activation password.
7. Click **OK** to activate the device.

Chapter 7 Quick Operation via Web Browser

7.1 Time Settings

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

Time Zone

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

Time Sync.

NTP

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

Manual

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

Server Address/NTP Port/Interval

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

DST

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

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

7.2 Environment Settings

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

Steps

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

Note

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

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

7.3 Privacy Settings

Set the picture uploading and storage parameters.

Click in the top right of the web page to enter the wizard page. After setting time and environment, you can click **Next** to enter the **Privacy Settings** page.

Picture Uploading and Storage

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Upload Picture After Linked Capture

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

Save Pictures After Linked Capture

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

Click **Complete** to finish settings.

Chapter 8 Operation via Web Browser

8.1 Login

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

Note

Make sure the device is activated. For detailed information about activation, see ***Activation*** .

Login via Web Browser

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

Login via Remote Configuration of Client Software

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

8.2 Overview

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

Function Descriptions:

Device Component Status

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

Remote Control

/ / /

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

Real-Time Event

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

Person Information

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

Network Status

You can view the network connection status.

Basic Information

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

Device Capacity

You can view the person, face, card and event capacity.

8.3 Person Management

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

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, and person type.
If you select **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 Face Picture

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

Note

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

Click **Save** to save the settings.

Add Card

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

8.4 Search Event

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

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

The results will be displayed on the right panel.

8.5 Device Management

You can manage the linked device on the page.

Steps

1. Click **Device Management** to enter the settings page.
2. You can view the **Device Type**, **Card Reader ID**, **Activation Status**, **Registration Status**, **IP Address**, **Gateway Address**, **Mask Address**, **Communication Port**, **Serial No.**, **MAC** and **PoE Port**.
3. Click to view the device network settings.
4. Click **Refresh** to get the device information.
5. **Optional:** Other operations.

View Device Information	Click to edit device information.
Reboot Device	Click to reboot the selected device.

8.6 Configuration

8.6.1 Set Local Parameters

Set the live view parameters, picture and clip settings.

Set Live View Parameters

Click **Configuration → Local** to enter the Local page. Configure the stream type, the play performance, auto start Live View and click **Save**.

Record File Settings

Click **Configuration → Local** to enter the Local page. Select a record file size and select a saving path from your local computer and click **Save**.
You can also click **Open** to open the file folder to view details.

Picture and Clip Settings

Click **Configuration → Local** to enter the Local page. Select image format, saving path and click **Save**.
You can also click **Open** to open the file folder to view details.

8.6.2 View Device Information

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

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view the language, model, serial No., version, IO input, IO output, local RS-485, alarm input and alarm output number.

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

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

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

8.6.3 Set Time

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

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

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

Time Zone

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

Time Sync.

Manual

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

Server IP Address/NTP Port/Interval

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

8.6.4 Set DST

Steps

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

8.6.5 Change Administrator's Password

Steps

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

Caution

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

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

8.6.6 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.

8.6.7 View Device Arming/Disarming Information

View device arming type and arming IP address.

Click **Configuration → System → User Management → Arming/Disarming Information** .

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

8.6.8 Network Settings

Set TCP/IP and port parameters.

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

Select a NIC type from the drop-down list. By default, it is **Self-Adaptive**.

DHCP

If you disable DHCP, you should manually set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, preferred DNS server, and alternate DNS server.

If you enable DHCP, the system will automatically allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway preferred DNS server and alternate DNS server.

DNS Server

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

Set Port Parameters

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

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

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 **Default** to reset the HTTP listening parameters.

Click **Configuration → Network → Network Service → RTSP** .

RTSP

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

8.6.9 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **Configuration → Video/Audio → Video** .
Choose a video channel and set the camera name, stream type, resolution and the video encoding.
Click **Save** to save the settings after the configuration.

Note

Video type, bitrate type, video quality, Max. bitrate, and I Frame Interval are read-only.

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .
Choose an audio channel and drag the block or enter value to adjust the device output volume.
Click to enable **Voice Prompt**.
Click **Save** to save the settings after the configuration.

Note

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

8.6.10 Set Image Parameters

You can adjust the image parameters.

Steps

1. Click **Configuration → Image** .
2. Select channel.
3. Configure the parameters to adjust the image.

   Image Adjustment

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

   LED Light

   Set the light type from the drop down list and select the mode to enable or disable it.

   If you select **Open**, you can set the light brightness.

   If you select **Disable**, the function will be disabled.

   Backlight

   Enable or disable WDR.

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

   Video Adjust(Video Standard)

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

   PAL

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

   NTSC

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

   Beauty

   Click to enable **Beauty** and set whiten and smooth value for the face appeared on the device live view page.
4. Click **Restore Default Settings** to restore the parameters to the default settings.

8.6.11 Event Linkage

Set linked actions for events.

Steps

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

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

Linked Buzzer

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

Linked Door

Enable **Linked Door**, check **Door 1** or **Door 2**, 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.

Linked Audio Prompt

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

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

Linked Capture

Enable **Linked Capture** and select entrance or exit to capture for the target event.

8.6.12 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.

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

Terminal

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

Enable Authentication Device

Enable the authentication function.

Authentication

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

Continuous Face Recognition Interval

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

Note

The recognition internal value ranges from 1 to 10.

Authentication Interval

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

Alarm of Max. Failed Attempts

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

Max. Authentication Failed Attempts

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

Communication with Controller Every

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

Note

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

Set Door Parameters

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

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

Door No.

Select **Entrance** or **Exit** for settings.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Note

The open duration ranges from 5 s to 60 s.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Remain Open Duration with First Person

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

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 the serial port position.
3. Select a serial port **No.**, and the corresponding serial port type will display automatically.
4. Set **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.
5. Set the **Peripheral Type** as **Card Reader**, **Card Receiver**, **QR Code Scanner**, or **Disable**.
6. You can view the connected device model and peripheral software version.
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.

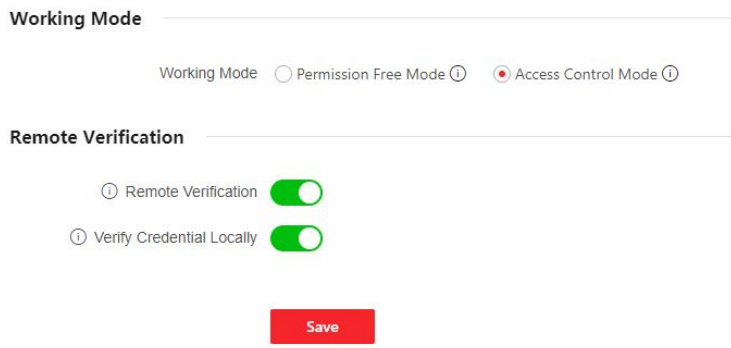


Figure 8-1 Terminal Parameters

2. Set the device working mode.

   Permission Free Mode

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

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

   Access Control Mode

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

3. Set remote verification.

   1) Enable **Remote Verification**.

   Note

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

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

Note

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

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

8.6.13 Turnstile

Basic Parameters

Set turnstile basic parameters.

Steps

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

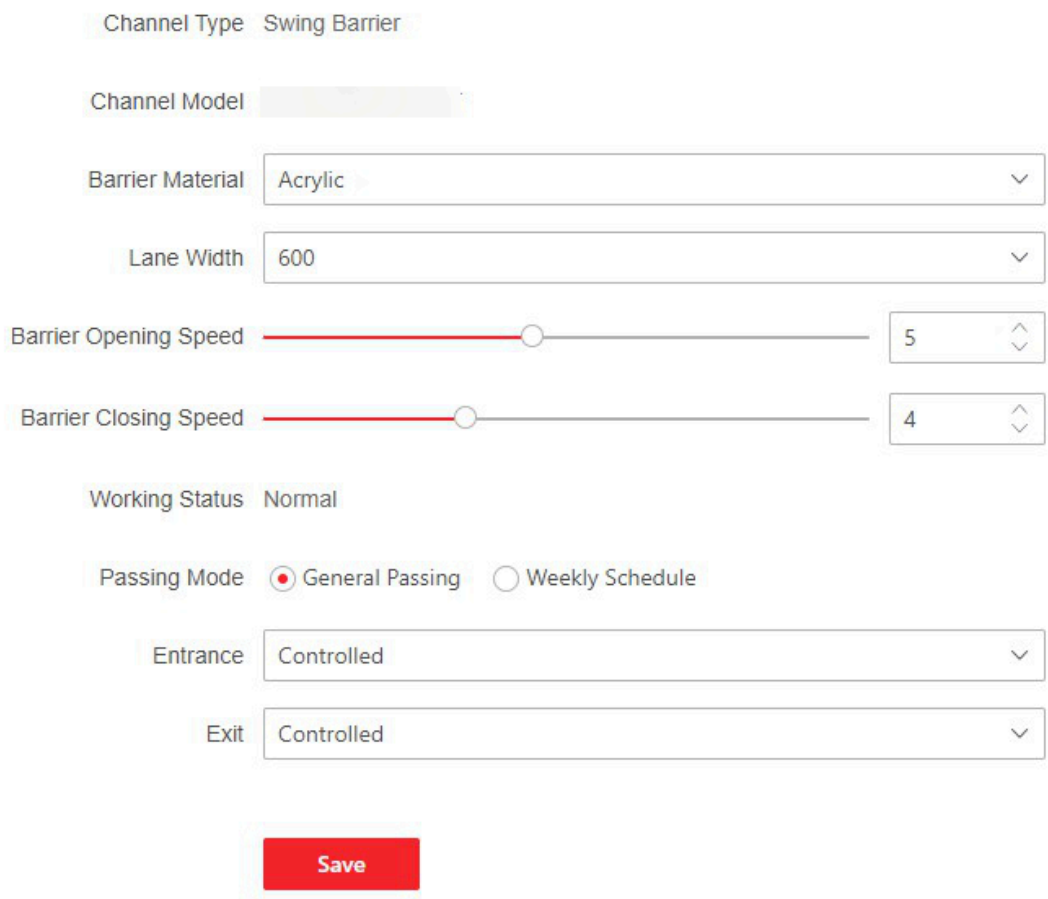


Figure 8-2 Basic Settings

2. View the **Channel Type** and **Channel Model** and **Working Status**.

3. Set **Barrier Material**, **Lane Width**, **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.

     Note

     If you set barrier-free mode, the barrier remains open and will close when authentication fails.
   - 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 Configuration → Keyfob Configuration** to enter the page.

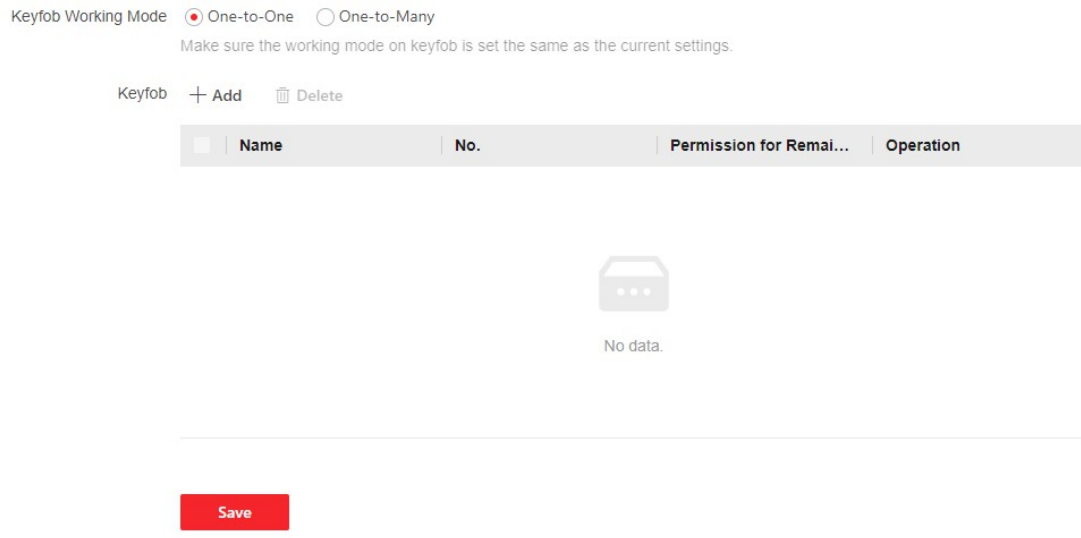


Figure 8-3 keyfob

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

IR Detector

Set IR detector.

Steps

1. Click **Configuration → Turnstile Configuration → IR Detector Settings** to enter the page.
2. Set the entrance and exit inductive mode as **Single Trigger** or **Trigger 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.

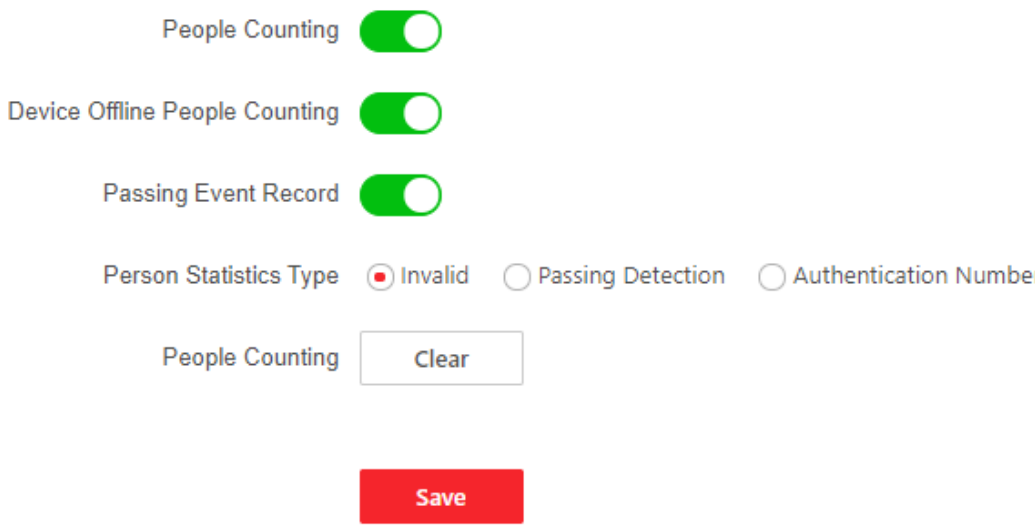


Figure 8-4 People Counting

2. Enable **People Counting**.
3. Enable **Device Offline People Counting**, the device will count people numbers even if it is offline.
4. Select **People Statistics Type**.

   Invalid

   Disable people counting.

   Passing Detection

   The number of all passing people.

   Authentication Number

   The number of passing people verified through card swiping, face recognition, etc.
5. **Optional:** Click **Clear** to clear all the people counting information.

Set Light Color

Set the color for the indicators.

Steps

1. Click **Configuration → Turnstile Configuration → Light Settings** to enter the page.
2. Set light color for lane status indicator.
   1) Set **Light Brightness** as **Auto** or **Fixed Brightness**. If you choose **Fixed Brightness**, you can 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 entrance light.
   1) Click to enable **Light on When on Standby** at your actual needs.

2) Set **Light Brightness** as **Auto** or **Manual**. If you choose **Manual**, you can drag the block or enter the value to adjust the light brightness manually.
3) Set the color for successful Auth., failed Auth. and alarms.

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

Other Settings

Set other parameters.

Steps

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

Alarm Output Duration

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

Temperature Unit

Select unit.

Do Not Open Barrier When Lane is Not Clear

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

Light Board Brightness

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

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.

Inductive Passing Mode

When enabled, the arm will rotate automatically when the infrared detector on one side of the turnstile is triggered.

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.

Memory Mode

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

Control Mode

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

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

Fire Input Type

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

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

8.6.14 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

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

Enable M1 Card

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

M1 Card Encryption
Sector

M1 card encryption can improve the security level of authentication.

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

Enable EM Card

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

Note

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

Enable DESFire Card

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

DESFire Card Read Content

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

Enable FeliCa Card

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

Set Card No. Authentication Parameters

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

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

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

8.6.15 Set Privacy Parameters

Click **Configuration → Security → Privacy Settings**

Event Storage 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.

Authentication Result Settings

Display Authentication Result

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

Name De-identification

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

ID De-identification

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

Picture Uploading and Storage

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

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

Save Pictures After Linked Capture

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

Upload Picture After Linked Capture

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

Clear All Pictures in Device

Note

All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

8.6.16 Set Biometric Parameters

Set Basic Parameters

Click **Configuration → Smart → Smart** .

Note

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

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

Terminal

Select a direction.

Face Recognition

After enabling, the device will support face recognition.

Face Anti-Spoofing

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

Note

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

Anti-Spoofing Detection Level

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

Recognition Distance

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

Application Mode

Select either other or indoor according to actual environment.

Pitch Angle

The maximum pitch angle when starting face authentication.

Yaw Angle

The maximum yaw angle when starting face authentication.

1:1 Matching Threshold

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

1:N Matching Threshold

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

Face Recognition Timeout Value

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

ECO Mode

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

ECO Mode Threshold

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

ECO Mode (1:1) Threshold

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

ECO Mode (1:N) Threshold

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

Face with Mask Detection

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

None

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

Reminder of Wearing Face Mask

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

Must Wear Face Mask

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

Face with Mask & Face (1:1)

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

Face with Mask 1:N Matching Threshold

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

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

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

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

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

Set Recognition Area

Click **Configuration → Smart → Area Configuration** .
Select terminal at entrance or exit, and enter values for the left, right, top, and bottom margin to adjust the recognition area. Only the face within the area can be recognized by the system.
Click **Save** to save the settings.

8.6.17 Screen Display

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

Click **Configuration → Preference → Screen Display** .

Click **Entrance** or **Exit** to set theme, Click **Save**.

Sleep

Enable **Sleep** and the device will enter the sleep mode when no operation within the configured sleep time.

Note

The sleep time ranges from 20 s to 999 s.

Display Mode

You can select display theme for device authentication. You can select **Display Mode** as **Simple**, **Authentication Mode**, or **Advertisement Mode**. When you select **Simple**, the information of name, ID, face picture will be not displayed. When you select **Advertisement**, the advertisement will be displayed in the screen.

8.6.18 Notice Publication

You can set the notice publication for the device.

Click **Configuration → Preference → Notice Publication** .

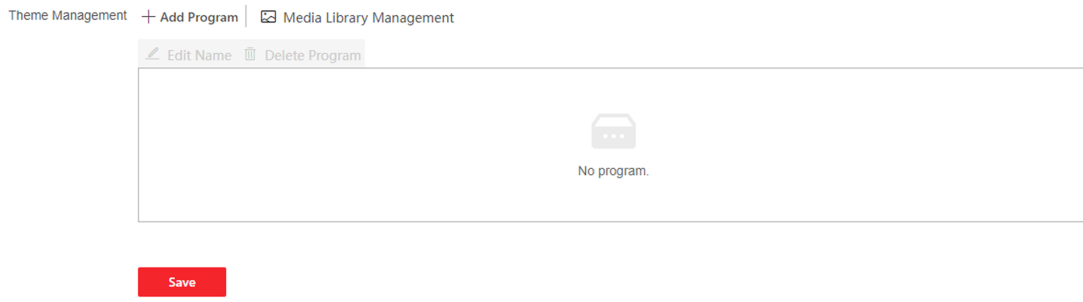


Figure 8-5 Notice

Theme Management

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

Note

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

Add Program

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

Picture

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

Welcome Message

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

Slide Show Interval

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

Schedule Management

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

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

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

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

8.6.19 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

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

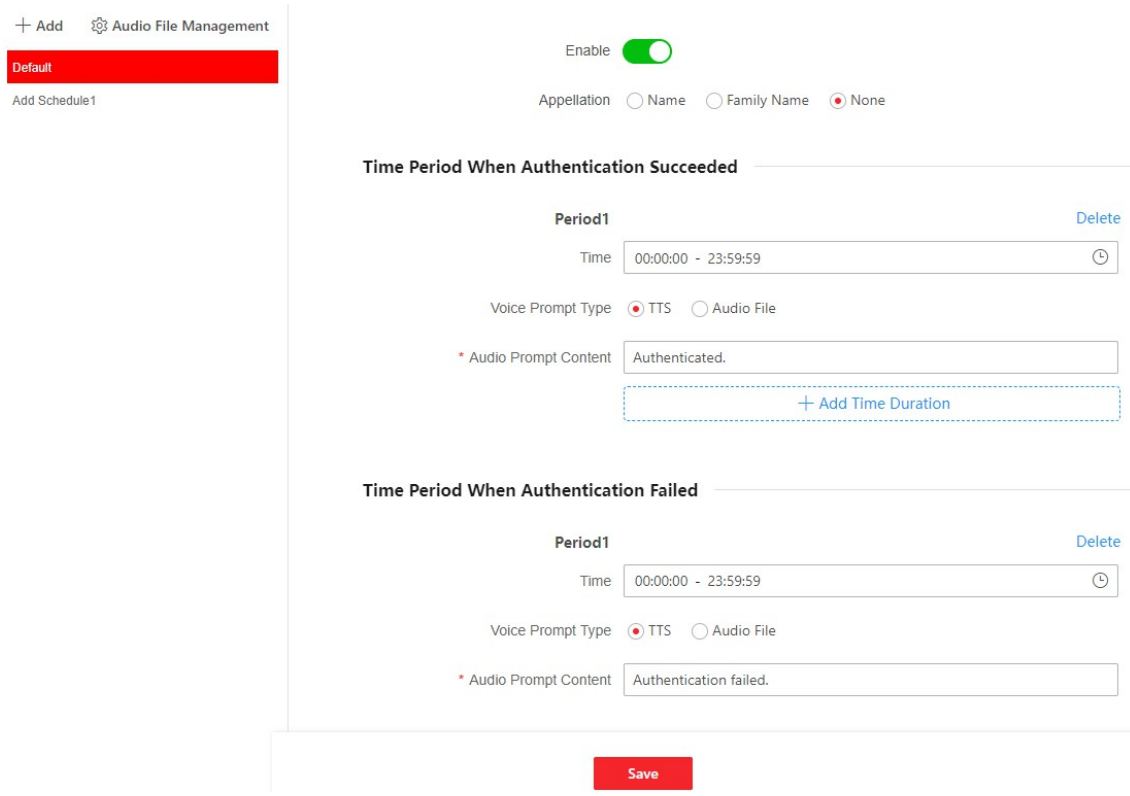


Figure 8-6 Customize Audio Content

2. Click **+ Add** to add a new schedule. Or select added time schedule.
3. Enable the function.

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

      Note

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

   3) Set the audio content.

      TTS

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

      Audio File

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

      Note

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

   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click **Delete** to delete the configured time duration.
6. 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) Set the audio content.

      TTS

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

      Audio File

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

      Note

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

   4) **Optional:** Repeat substep 1 to 3.
   5) **Optional:** Click **Delete** to delete the configured time duration.
7. Click **Save** to save the settings.

8.6.20 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.

8.6.21 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

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

Print Log

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

Capture Network Packet

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

8.6.22 Component Status

Main Lane Status

Device Component

You can view the status of boards, IR adaptors and camera.

Peripheral

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

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Sub Lane Status

Device Component

You can view the status of boards, IR adaptors and camera.

Peripheral

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

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Others

Passing Mode

You can view the entrance and exit mode.

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 protection alarm.

Other Status

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

8.6.23 Log Query

You can search and view the device logs.

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

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

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

8.6.24 Certificate Management

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

Note

The function is only supported by certain device models.

Create and Import Self-signed Certificate

Steps

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

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

The certificate will be saved automatically.

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

Import Other Authorized Certificate

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

Steps

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

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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

   Note

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

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

Chapter 9 Client Software Configuration

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

9.1 Configuration Flow of Client Software

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

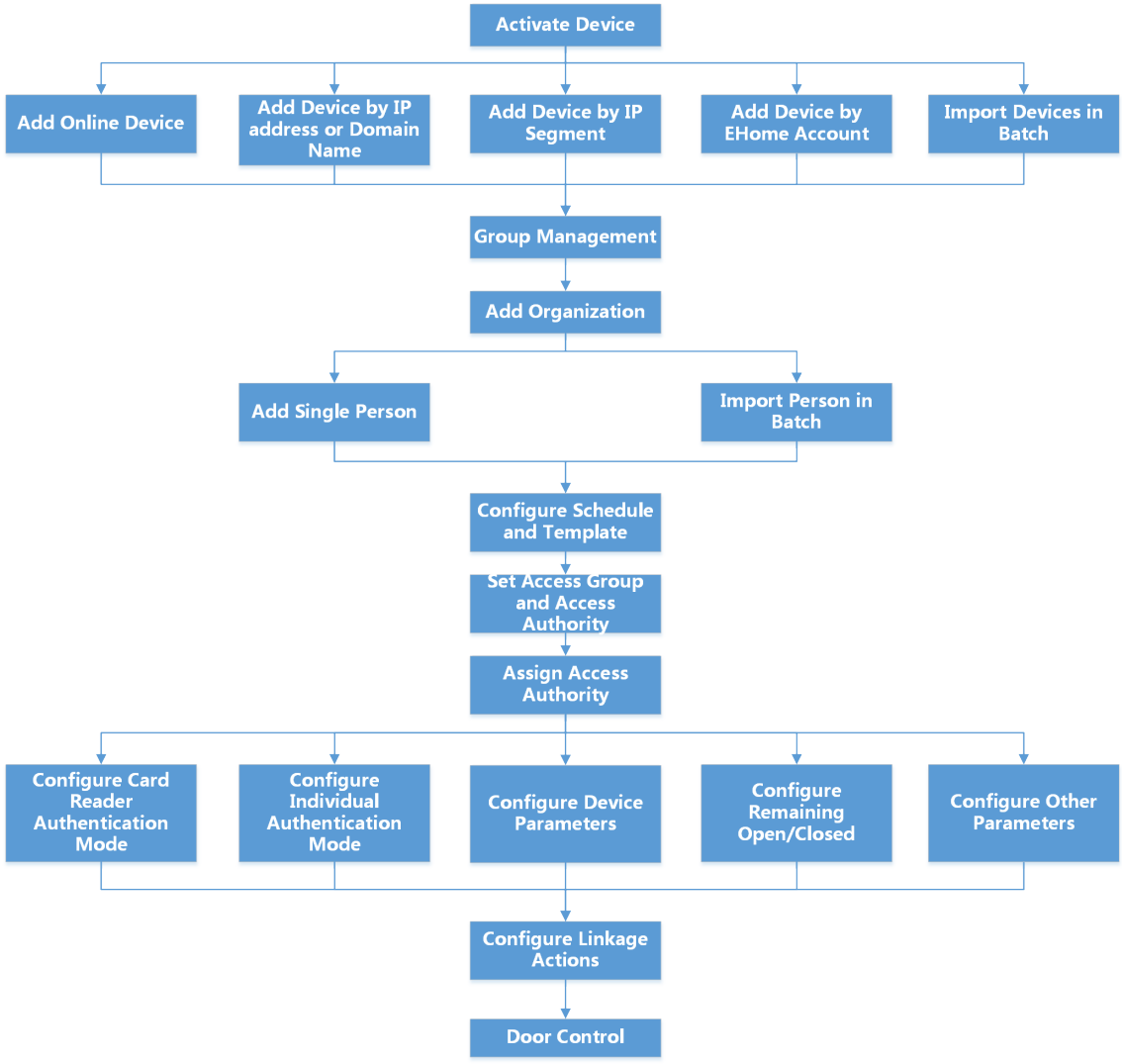


Figure 9-1 Flow Diagram of Configuration on Client Software

9.2 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.

9.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and EHome 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 installer 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 ***80***.

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 installer 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.

9.2.2 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 installer and/or end-user.

9.2.3 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 9-1 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 **Delete** 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. **Note** For different devices, you will view different information about device status.

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.

9.3 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.

9.3.1 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.

9.3.2 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.

9.4 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.

9.4.1 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 surbodinate 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).

Edit Organization	Hover the mouse on an added organization and click to edit its name.
Delete Organization	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.
Show Persons in Sub Organization	Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

9.4.2 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.

Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

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 and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click ... to select a face picture file.

Note

- The (folder of) face pictures should be in ZIP format.
- Each picture file should be in JPG format and should be no larger than 200 KB.
- Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

6. Click **Import** to start importing.

   The importing progress and result will be displayed.

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. See for details.

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.

Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start

- Make sure you have added persons and their face pictures to an organization.
- Make sure you have enabled the **Export Person Information** function to display the **Export** button. See for details.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

   Note

   All persons' face pictures will be exported if you do not select any organization.
3. Click **Export** on the top menu bar.
4. Enter the super user name and password for verification.

   The Export panel is displayed.
5. Check **Face** as the content to export.
6. Click **Export** and set an encryption key to encrypt the exported file.

   Note

   - The exported file is in ZIP format.
   - The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).

9.4.3 Get Person Information from Access Control Device

If the access control device has been configured with person information (including person details, fingerprint, and issued card 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, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

9.4.4 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. Click **Batch Issue Cards**.

   All the added persons with no card issued will be displayed in the right panel.
3. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to .
5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. 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).

9.4.5 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.

9.4.6 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.

9.5 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*** .

9.5.1 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**.

9.5.2 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.

9.6 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.

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to ***Group Management*** .
- Add template.

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, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, 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.

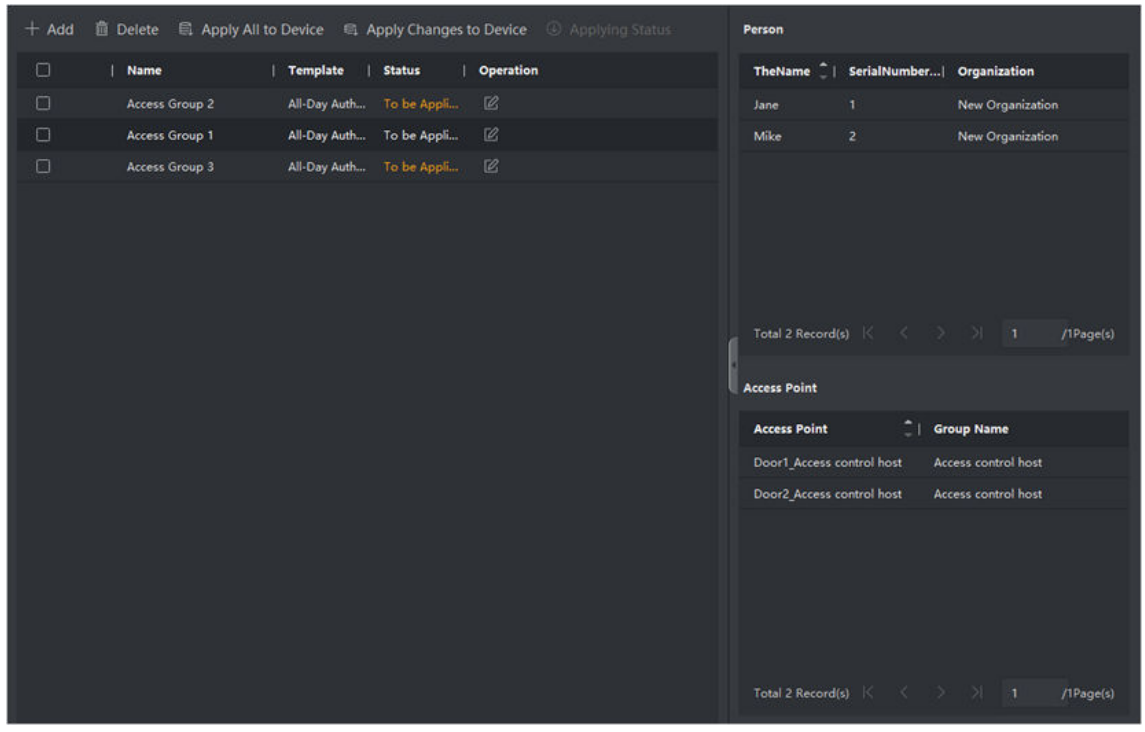


Figure 9-2 Display the Selected Person(s) and Access Point(s)

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) or fingerprints.

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**.

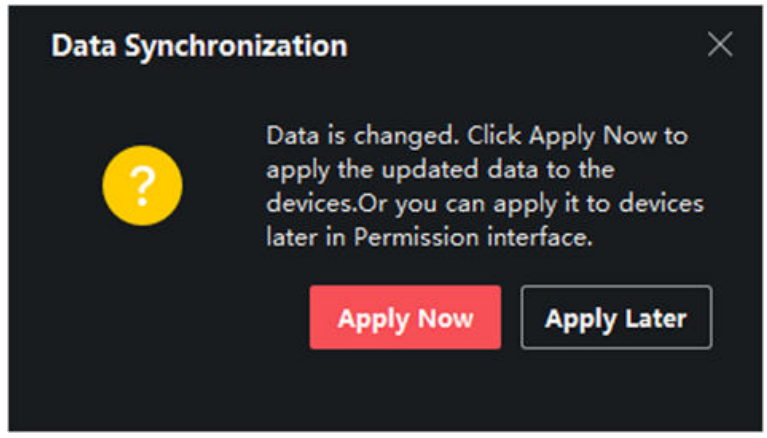


Figure 9-3 Data Synchronization

9.7 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.

9.7.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device (access controller), access control points (door or floor), alarm inputs, alarm outputs, card readers and lane controller.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, 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.
   - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

   RS-485 Comm. Redundancy

   You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

   Display Detected Face

   Display face picture when authenticating.

   Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

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.

Upload Pic. After Linked Capture

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

Save Pic. After Linked Capture

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

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

Wi-Fi Probe

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

3G/4G

If you enable this function, the device can communicate in 3G/4G network.

NFC Anti-Cloning

If you enable this function, you cannot use the cloned card for authentication and further enhance security.

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.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

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

Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

Extended Open Duration

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

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Lock Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password

The specific person can open the door by inputting the super password.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

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.
- 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.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Max. Interval When Entering PWD

When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

Alarm of Max. Failed Attempts

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

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate 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.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Card Reader Type/Card Reader Description

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

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

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

1:N Security Level

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

Live Face Detection

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

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

4. Click **OK**.
5. **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.

- If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.
- If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

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.

Audible Prompt 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.

4. Click **OK**.

9.7.2 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

Set Parameters for Face Recognition Terminal

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

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 **Face Recognition Terminal**.
4. Set the parameters.

Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blocklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blocklist.

If matched (the person is in the blocklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blocklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click **Save**.

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, communication mode, working mode, and connection mode in the drop-down list.

Note

When the connection mode is **Connect Access Control Device**, you can select **Card No.** or **Person ID** as the output type.

6. Click **Save**.
   - The configured parameters will be applied to the device automatically.
   - When you change the working mode or 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.

Before You Start

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

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 **Wiegand** to enter the Wiegand Settings page.
4. Set the switch to on to enable the Wiegand function for the device.
5. Select the Wiegand channel No. and the communication mode from the drop-down list.

Note

If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26** or **Wiegand 34**.

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

Note

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** to enter the M1 Card Encryption 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.
6. Click **Save** to save the settings.

9.8 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.

Note

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 .

9.8.1 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). For details, refer to .

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

   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

   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. For setting the saving path, refer to .

Result

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

9.8.2 Check Real-Time Access Records

The real-time access records can be displayed in the client, including card swiping records, face recognition records, skin-surface temperature information, etc. Also, you can view the person information and view the picture captured during access.

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, including card No., person name, event time, door location, temperature, authentication type etc.

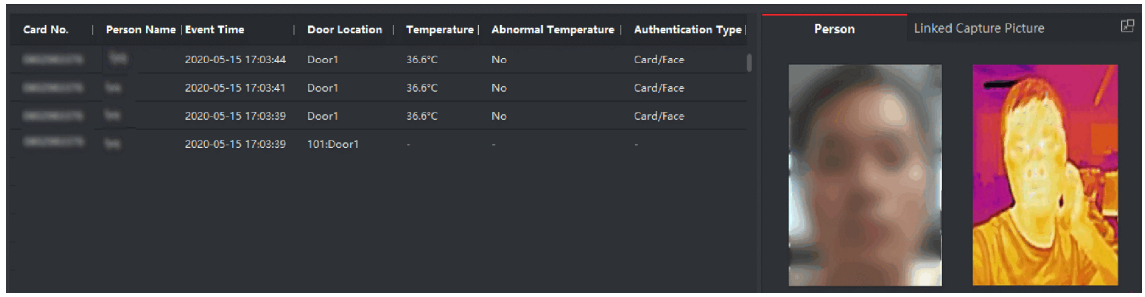


Figure 9-4 Real-time Access Records

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:** Check **Enable Abnormal Temperature Prompt** to enable abnormal skin-surface temperature prompt.

   Note

   When enabled, if there is abnormal temperature information, an Abnormal Temperature window pops up when you enter Monitoring module, displaying person's picture, skin-surface temperature, card No., person name, etc.
6. **Optional:** Click an event to view person pictures (including captured picture and profile).

   Note

   In **Linked Capture Picture** field, you can double click the captured picture to view an enlarged picture.
7. **Optional:** Click to view details (including person's detailed information and the captured picture).

   Note

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

Appendix A. Tips When Collecting/Comparing Face Picture

The position when collecting or comparing face picture is as below:

Expression

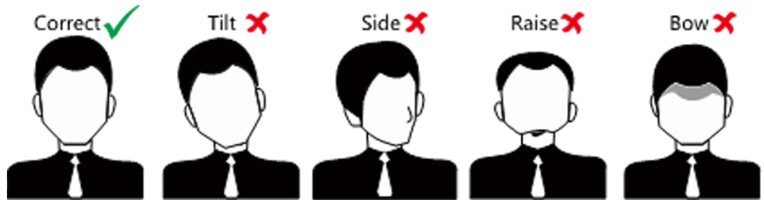
- Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.



- Do not wear hat, sunglasses, or other accessories that can affect the facial recognition function.
- Do not make your hair cover your eyes, ears, etc. and heavy makeup is not allowed.

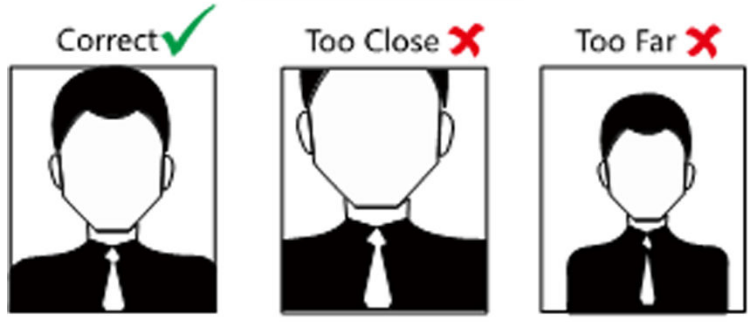
Posture

In order to get a good quality and accurate face picture, position your face looking at the camera when collecting or comparing face pictures.



Size

Make sure your face is in the middle of the collecting window.



Appendix B. DIP Switch

B.1 DIP Switch Description

The DIP switch is on the main user extended interface board. No.1 to No 4 is from the low bit to the high bit.

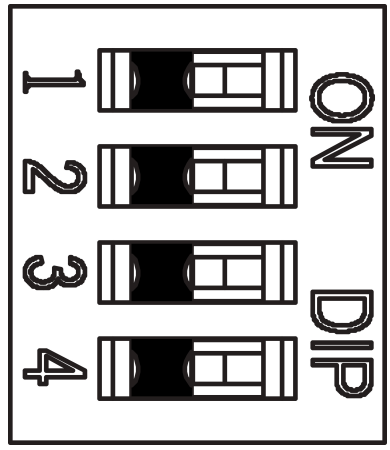


Figure B-1 DIP Switch

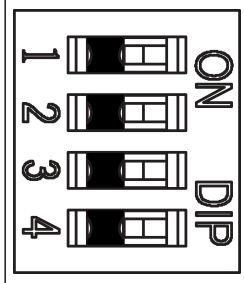
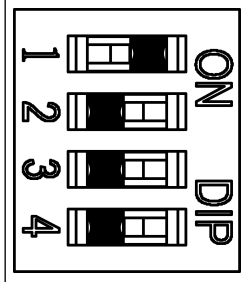
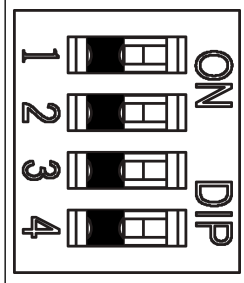
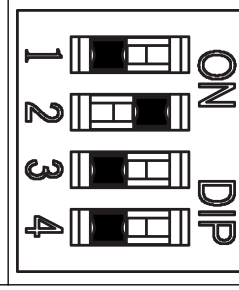
When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off.

B.2 DIP Switch Corresponded Functions

Note

After setting the DIP switch, you should reboot the device, or the function cannot take effect.

The 4-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	

B.3 Light Board DIP Switch Description

Configure the DIP switch address of side light and entrance light.

Side Light Board DIP Switch

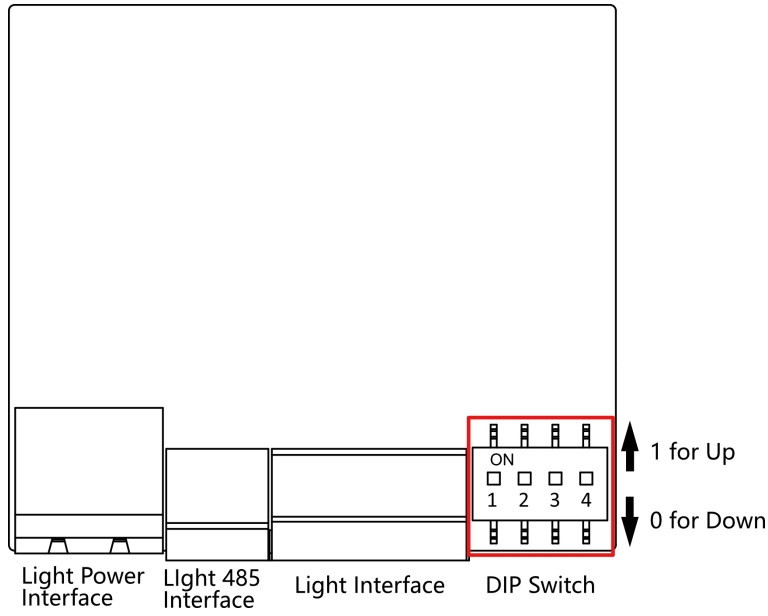


Figure B-2 Light Board DIP Switch

Table B-1 Light 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
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

Position	Address	Value (Start from Left)	
13	138	1101	1011
14	139	1110	0111
15	140	1111	1111

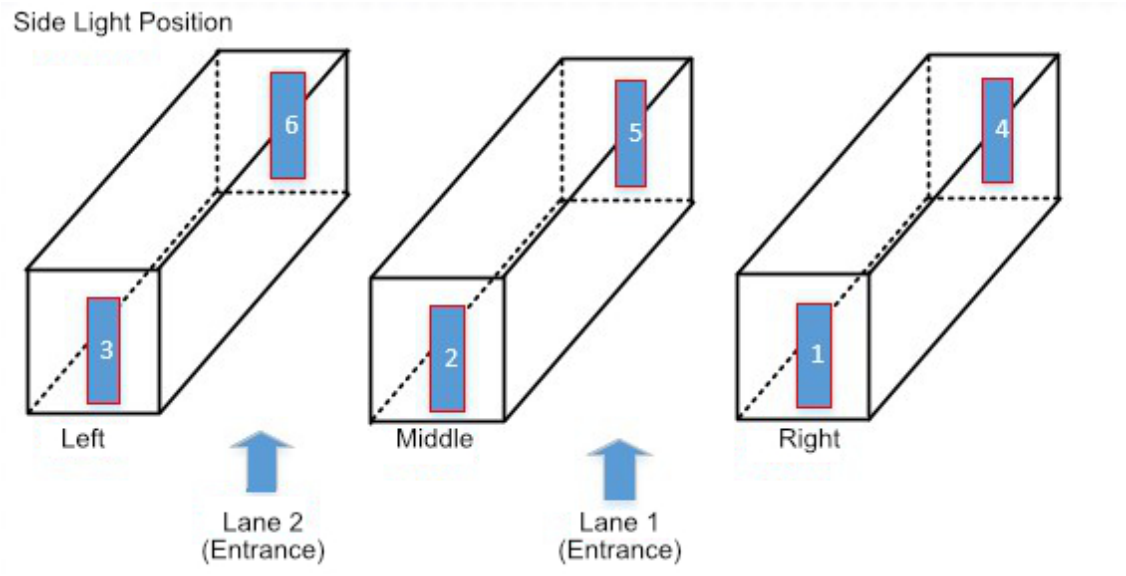


Figure B-3 Side Light Position

Single-Lane Scenario:
In single-lane scenario, the side lights are located at the position of NO. 1, 3, 4, 6. Side light No. 1 is near the main user extended interface board.

Table B-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 B-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

Entrance Light Board DIP Switch

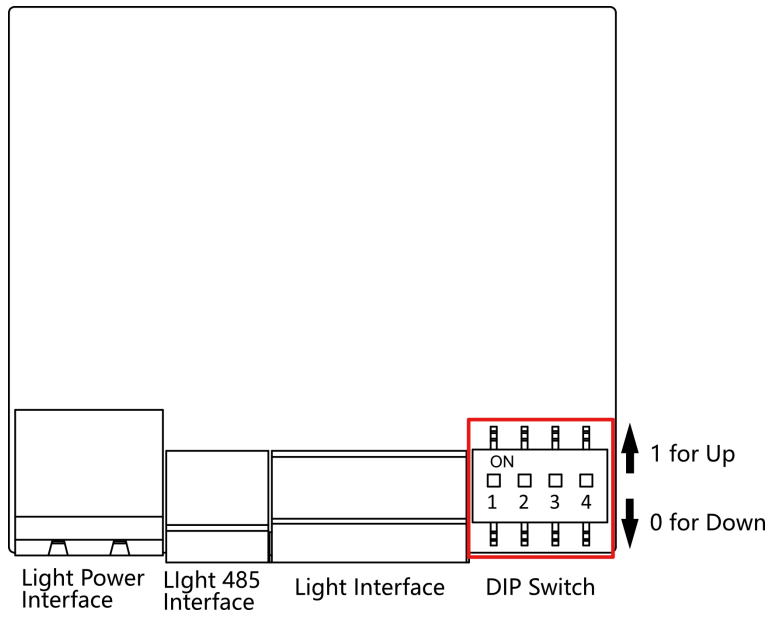


Figure B-4 Light Board DIP Switch

Table B-4 Light 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

Position	Address	Value (Start from Left)	
4	129	100	0010
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

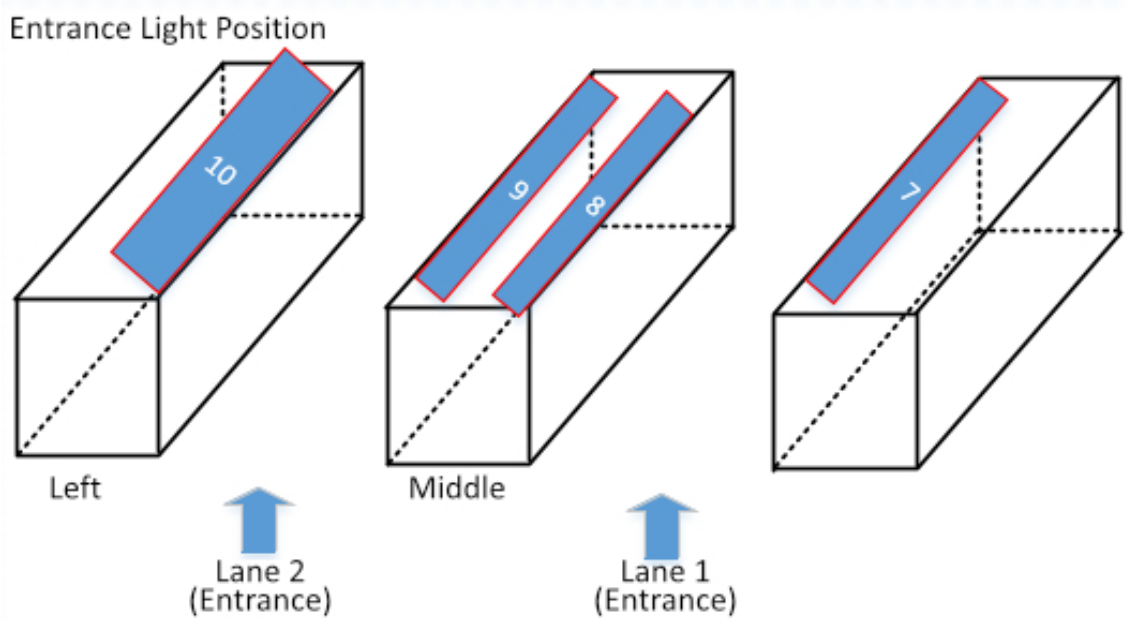


Figure B-5 Entrance Light Position

Single-Lane Scenario:
In single-lane scenario, the entrance lights are located at the position of NO. 7, 10. Entrance light No. 7 is near the main user extended interface board.

Table B-5 Single-Lane DIP Switch Description

Position	Address	Value
No. 7	129	0010
No. 10	130	1010

Dual-Lane Scenario:

Table B-6 Dual-Lane DIP Switch Description

Position	Address	Value
No. 7	129	0010
No. 8	130	1010
No. 9	129	0010
No. 10	130	1010

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 Authentication Failed	Visual
Barrier Obstructed	None

Appendix D. 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
Normal Working	00	Lower Fifth IR Beam Triggered	21
First IR Beam Triggered	01	Lower Sixth IR Beam Triggered	22
Second IR Beam Triggered	02	Lower Seventh IR Beam Triggered	23
Third IR Beam Triggered	03	Lower Eighth IR Beam Triggered	24
Fourth IR Beam Triggered	04	Lower Ninth IR Beam Triggered	25
Fifth IR Beam Triggered	05	Lower Tenth IR Beam Triggered	26
Sixth IR Beam Triggered	06	Lower Eleventh IR Beam Triggered	27
Seventh IR Beam Triggered	07	Lower Twelfth IR Beam Triggered	28
Eighth IR Beam Triggered	08	Lower Thirteenth IR Beam Triggered	29
Ninth IR Beam Triggered	09	Lower Fourteenth IR Beam Triggered	30
IR Beam Triggered	10	Lower Fifteenth IR Beam Triggered	31
Eleventh IR Beam Triggered	11	Lower Sixteenth IR Beam Triggered	32
Twelfth IR Beam Triggered	12	Light Board Offline (Entrance)	49
Thirteenth IR Beam Triggered	13	Light Board Offline (Exit)	50
Fourteenth IR Beam Triggered	14	IR Adapter Offline (Up)	51
Fifteenth IR Beam Triggered	15	IR Adapter Offline (Low)	52
Sixteenth IR Beam Triggered	16	CAN Bus Exception	53
Lower First IR Beam Triggered	17	Not Studying	54

Error Reason	Code	Error Reason	Code
Lower Second IR Beam Triggered	18	Obstruction	55
Lower Third IR Beam Triggered	19	Exceeding Studying Range	56
Lower Fourth IR Beam Triggered	20	Motor Exception	57

Appendix E. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.
Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.



Figure E-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.
Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.



Figure E-2 Device Command


See Far, Go Further