



DS-K3B411X Series Swing Barrier

User Manual

Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

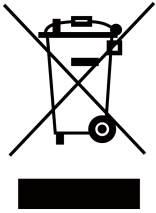
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

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, LVD Directive 2014/35/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

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

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.
- ⚡ 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 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

Available Models

Product Name	Model Type	Example	Description
Swing Barrier	DS-K3B411X-L	DS-K3B411X-L/M	Left Pedestal
	DS-K3B411X-M	DS-K3B411X-M/M DS-K3B411X-M/M 868	Middle Pedestal
	DS-K3B411X-R	DS-K3B411X-R/M DS-K3B411X-R/M 868	Right Pedestal
	DS-K3B411X-LS	DS-K3B411X-LS/M	Left Pedestal (No Barrier)
	DS-K3B411X-MS	DS-K3B411X-MS/M	Middle Pedestal (Single Barrier)

Contents

Chapter 1 Overview	1
1.1 Introduction	1
1.2 Main Features	1
Chapter 2 System Wiring	3
Chapter 3 Installation	6
3.1 Disassemble Pedestals	6
3.2 Install Pedestals	6
Chapter 4 General Wiring	10
4.1 Components Introduction	10
4.2 Wiring Electric Supply	11
4.3 Wire Interconnecting Cable	12
4.3.1 Pull Interconnecting Cable	13
4.4 Wire Network Switch (Optional)	17
4.5 Terminal Description	19
4.5.1 Main Control Board Terminal Description	19
4.5.2 Sub Control Board Terminal Description	20
4.5.3 BUS Terminal Description	20
4.5.4 Access Control Board Terminal Description	22
4.5.5 Access Control Board Serial Port ID Description	27
4.5.6 RS-485 Wiring	32
4.5.7 RS-232 Wiring	33
4.5.8 Barrier Control Wiring	33
4.5.9 Alarm Output Wiring	34
Chapter 5 Device Settings	36
5.1 Pair Keyfob (Optional)	36
5.2 Initialize Device	37

5.3 Switch Relay Output Mode (NO/NC)	38
5.3.1 Barrier Control Relay Output Mode	38
5.3.2 Alarm Relay Output Mode (NO/NC)	39
Chapter 6 Activation	41
6.1 Activate via SADP	41
6.2 Activate Device via Client Software	42
Chapter 7 Client Software Configuration	44
7.1 Configuration Flow of Client Software	44
7.2 Device Management	44
7.2.1 Add Device	45
7.2.2 Reset Device Password	52
7.3 Group Management	53
7.3.1 Add Group	53
7.3.2 Import Resources to Group	53
7.3.3 Edit Resource Parameters	54
7.3.4 Remove Resources from Group	54
7.4 Person Management	54
7.4.1 Add Organization	55
7.4.2 Configure Basic Information	55
7.4.3 Issue a Card by Local Mode	56
7.4.4 Upload a Face Photo from Local PC	58
7.4.5 Take a Photo via Client	58
7.4.6 Collect Face via Access Control Device	60
7.4.7 Collect Fingerprint via Client	60
7.4.8 Configure Access Control Information	61
7.4.9 Customize Person Information	63
7.4.10 Configure Resident Information	63
7.4.11 Configure Additional Information	64

7.4.12 Import and Export Person Identify Information	64
7.4.13 Import Person Information	65
7.4.14 Import Person Pictures	65
7.4.15 Export Person Information	66
7.4.16 Export Person Pictures	66
7.4.17 Get Person Information from Access Control Device	67
7.4.18 Move Persons to Another Organization	67
7.4.19 Issue Cards to Persons in Batch	68
7.4.20 Report Card Loss	68
7.4.21 Set Card Issuing Parameters	69
7.5 Configure Schedule and Template	70
7.5.1 Add Holiday	70
7.5.2 Add Template	71
7.6 Set Access Group to Assign Access Authorization to Persons	72
7.7 Configure Advanced Functions	74
7.7.1 Configure Device Parameters	74
7.7.2 Configure Remaining Open/Closed	80
7.7.3 Configure Multi-Factor Authentication	81
7.7.4 Configure Custom Wiegand Rule	83
7.7.5 Configure Card Reader Authentication Mode and Schedule	84
7.7.6 Configure First Person In	86
7.7.7 Configure Anti-Passback	87
7.7.8 Configure Device Parameters	88
7.8 Configure Linkage Actions for Access Control	89
7.8.1 Configure Client Actions for Access Event	89
7.8.2 Configure Device Actions for Access Event	90
7.8.3 Configure Device Actions for Card Swiping	92
7.9 Door Control	93

7.9.1 Control Door Status	93
7.9.2 Check Real-Time Access Records	94
7.10 Event Center	95
7.10.1 Enable Receiving Events from Devices	95
7.10.2 View Real-Time Events	96
7.10.3 Search Historical Events	97
7.11 Time and Attendance	100
7.11.1 Configure Attendance Parameters	100
7.11.2 Add General Timetable	106
7.11.3 Add Shift	109
7.11.4 Manage Shift Schedule	111
7.11.5 Manually Correct Check-in/out Record	114
7.11.6 Add Leave and Business Trip	115
7.11.7 Calculate Attendance Data	116
7.11.8 Attendance Statistics	118
7.12 Remote Configuration via Client Software	121
7.12.1 Check Device Information	121
7.12.2 Edit Device Name	121
7.12.3 Edit Time	121
7.12.4 Set System Maintenance	121
7.12.5 Manage Network User	122
7.12.6 Manage Keyfob User	122
7.12.7 Set Security	123
7.12.8 Configure Screen Parameters	123
7.12.9 Configure Screen Parameters	124
7.12.10 Configure Advanced Network	125
7.12.11 Configure Audio File	125
7.12.12 View Relay Status	126

Appendix A. DIP Switch Description 127

Appendix B. Event and Alarm Type 128

Appendix C. Table of Audio Index Related Content 129

Appendix D. Error Code Description 130

Appendix E. Communication Matrix and Device Command 132

Chapter 1 Overview

1.1 Introduction

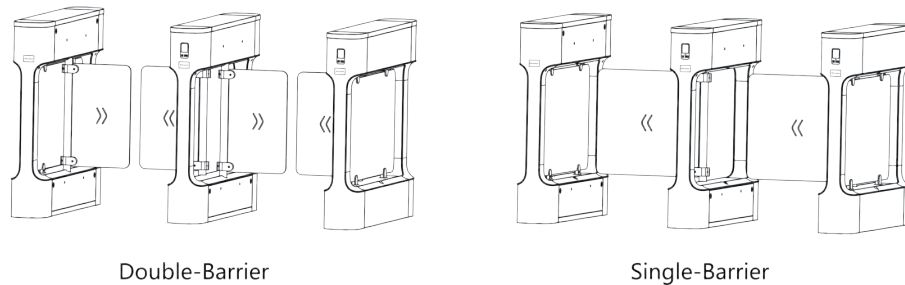


Figure 1-1 Appearance

The swing barrier is designed to detect unauthorized entrance or exit. By adopting the swing barrier integratedly with the access control system, personnel 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

- Excellent performance and fast speed with 32-bit high-speed processor
- TCP/IP network communication and network speed adaptive
The communication data is specially encrypted to relieve the concern of privacy leak
- Permissions validation and anti-tailgating
- Remaining open/closed mode selectable
- Bidirectional (Entering/Exiting) lane
The barrier opening and closing speed can be configured according to the visitor flow
- 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 50 N·m
- Self-detection, Self-diagnostics, and automatic alarm
- Audible and visual alarm will be triggered when detecting intrusion, tailgating, reverse passing, and climbing over barrier
- IP conflict detection
- Remote control and management
- Online/offline operation
- LED indicates the entrance/exit and passing status
- Barrier is in open status when powered down; If the device is installed with supercapacitor, 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

- Opens/Closes barrier according to the schedule template
- Up to 60,000 cards can be added
- Up to 180,000 card swiping records can be saved

Chapter 2 System Wiring

The preparation before installation and general wiring.

Steps

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



Note

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

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

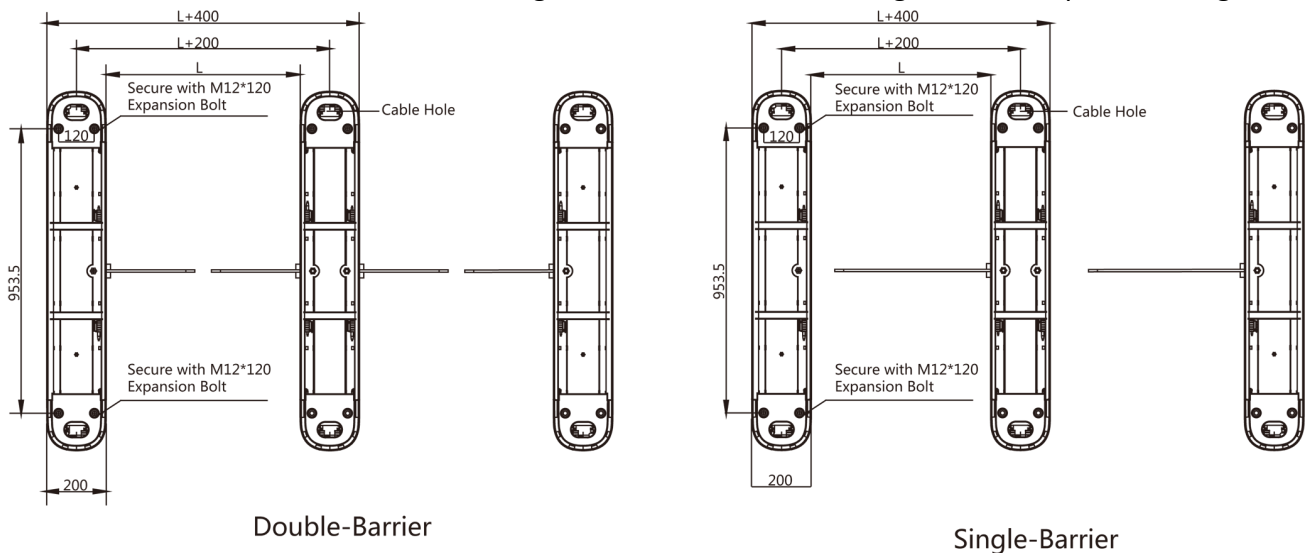


Figure 2-1 Hole Position Diagram

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

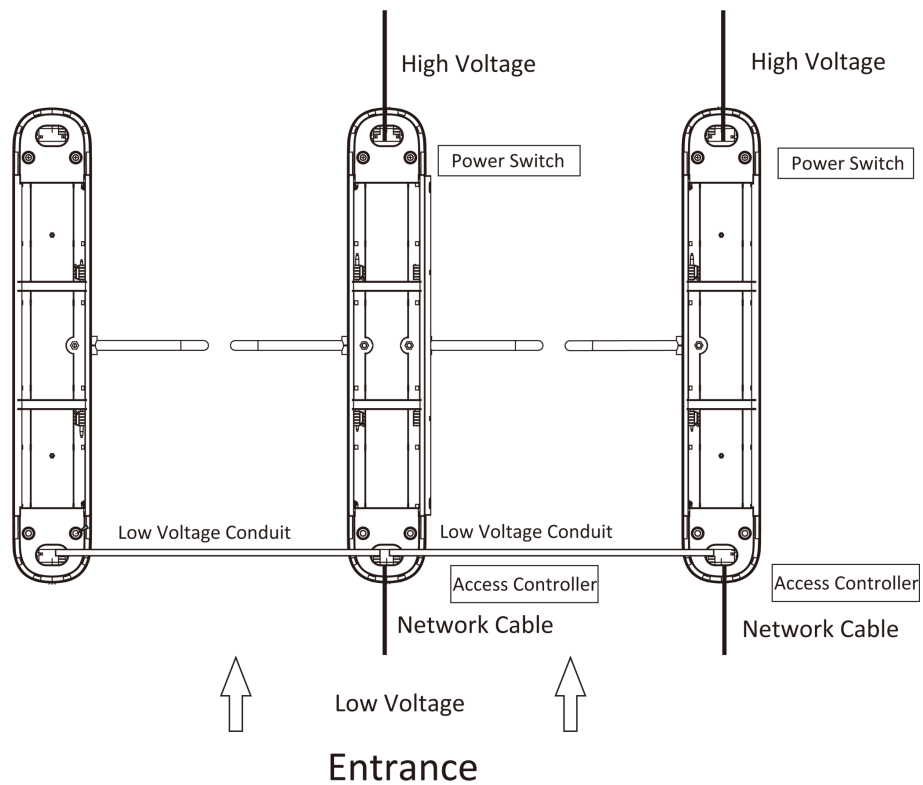


Figure 2-2 System Wiring Diagram (General Wiring)

 Note

- The supplied interconnecting cable length is 3.75 m. If you need a longer one, you can buy a new accessory.
 - 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 at the entrance, 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.
-

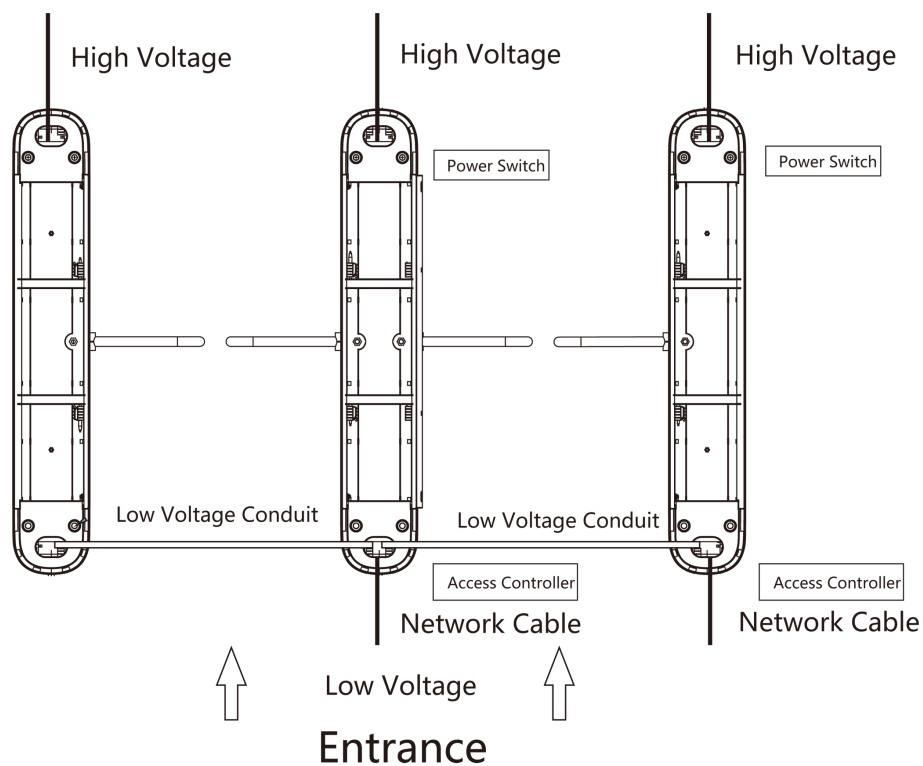


Figure 2-3 Wire Face Recognition Terminal

Note

- The face recognition terminal installed on the left pedestal will gain power from the sub switch, which should connect to high voltage.
 - The suggested inner diameter of the low voltage conduit is larger than 30 mm.
 - The supplied interconnecting cable length is 3.75 m. If you need a longer one, you can extend the cable by yourself.
 - If you want to bury both of the AC power cord and the low voltage cable at the entrance, 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

3.1 Disassemble Pedestals

Before installation, you should use the key to open the pedestals.

View the pictures below to find the lock holes.

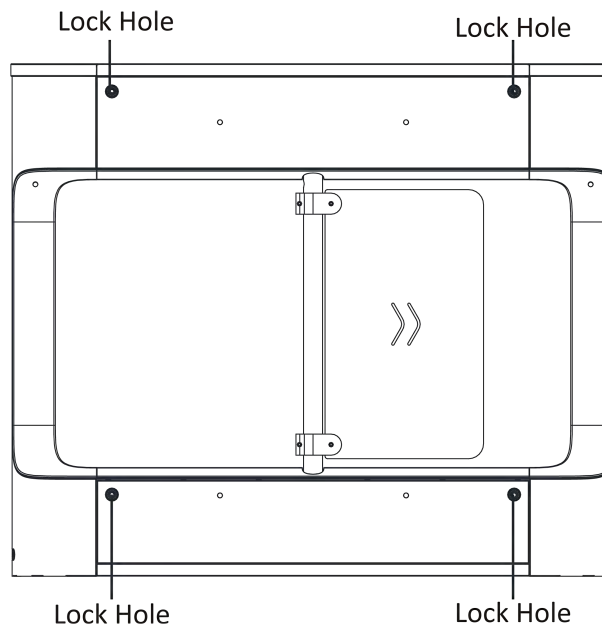


Figure 3-1 Lock Holes

3.2 Install Pedestals

Before You Start

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

Steps



Note

- The device should be installed on the concrete surface or other non-flammable surfaces.
- In order to prevent stainless steel from rusting due to dirt during the construction process, it is recommended to tear off the protective film after the device is installed. There may be residual glue at the film cutting position, and it is recommended to wipe the film with WD-40 protective liquid after tearing the film.

- No face recognition terminal installed: If the installation area is too close to the wall, make sure the distance between the pedestal and the wall should be more than 20 mm, or the surface may be scratched.

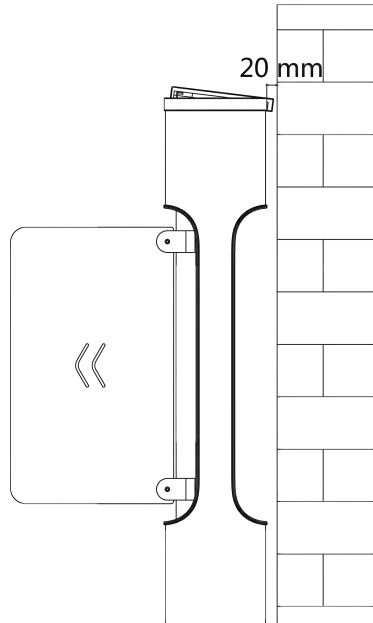


Figure 3-2 Installation Distance (Without Face Recognition Terminal)

- Face recognition terminal installed: If the installation area is too close to the wall, make sure the distance between the pedestal and the wall should be more than 20 mm, or the surface may be scratched.

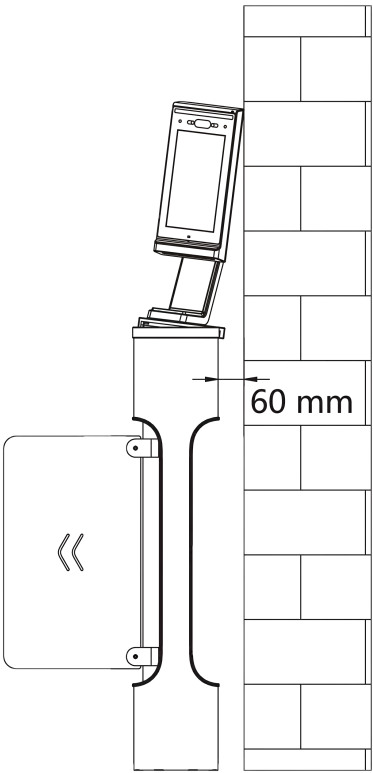


Figure 3-3 Installation Distance (With Face Recognition Terminal)

The dimension is as follows.

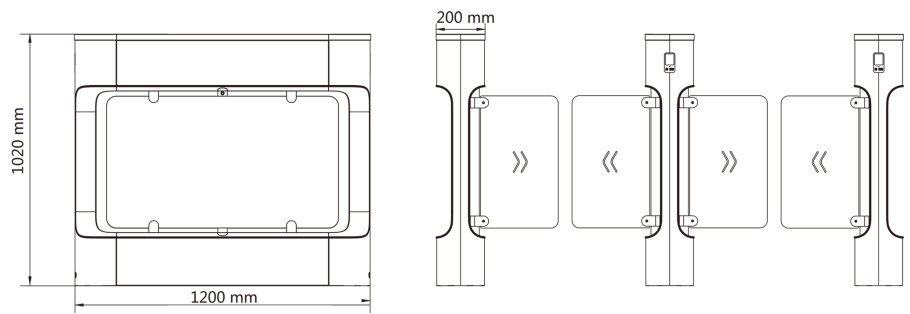


Figure 3-4 Double-Barrier Dimension

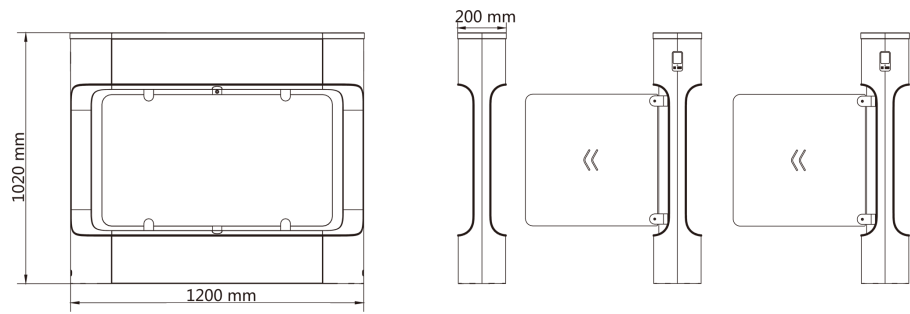


Figure 3-5 Single-Barrier Dimension

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Drill holes on the ground according to the installation holes on the pedestals and insert the expansion sleeves.
3. Seal the bottom of the turnstile to avoid water from entering.
4. According to the entrance and exit marks on the pedestals, move the pedestals to the corresponded positions.



Note

Make sure the installation holes on the pedestals and the base are aligned with each other.

5. Secure the pedestals with expansion bolts.



Note

- Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 150 mm.
- The installation footprint is as follows:

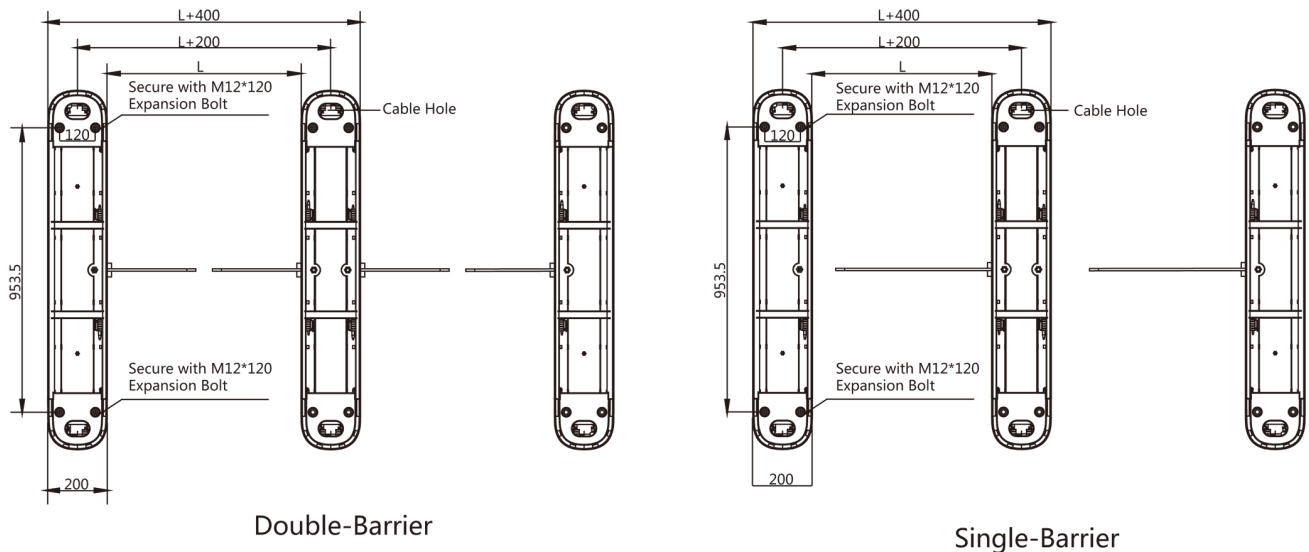


Figure 3-6 Installation Footprint

Chapter 4 General Wiring

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 85 VAC and 264 VAC, 50 to 60 Hz.

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

 Note

The diagram is for reference only.

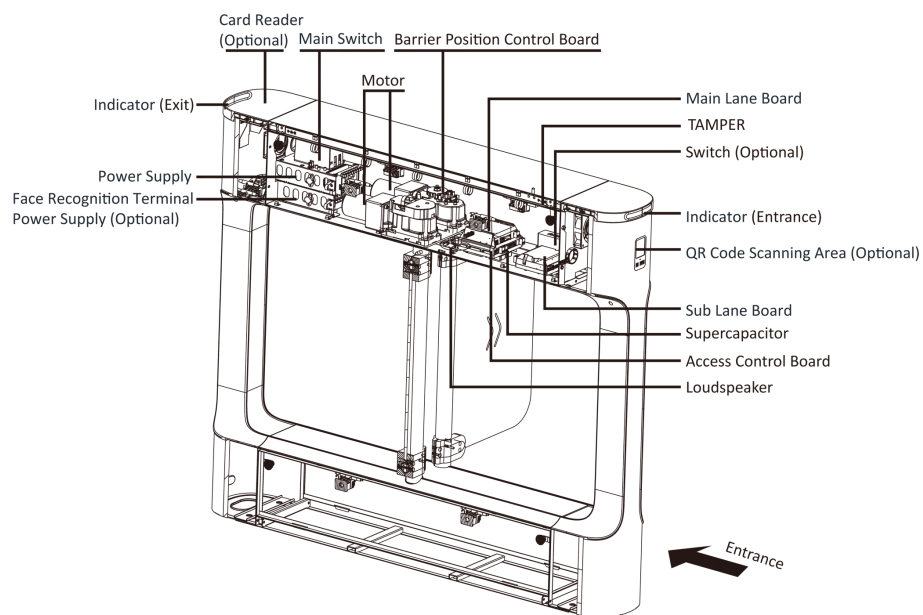


Figure 4-1 Components Diagram 1

 Note

The reinstalled supercapacitor needs to be powered on for at least 3 minutes before it can work normally.

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

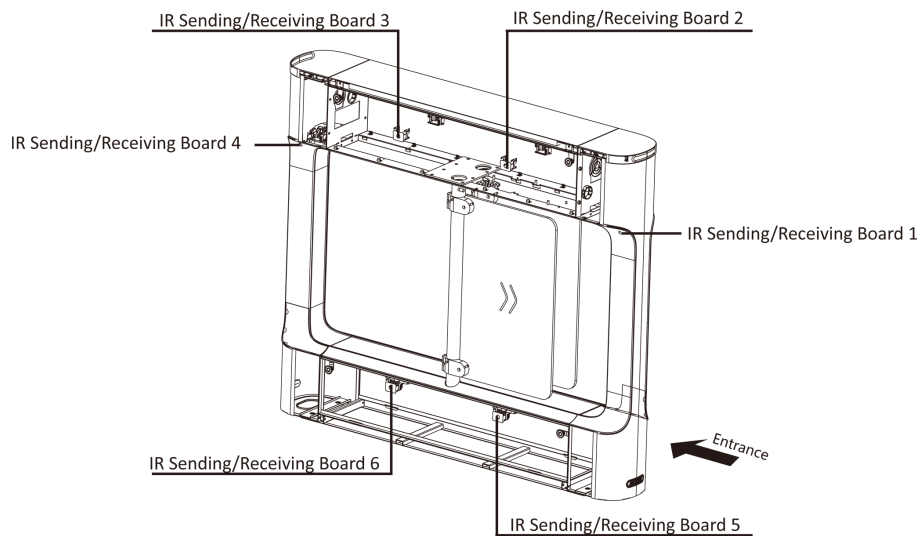


Figure 4-2 Components 2

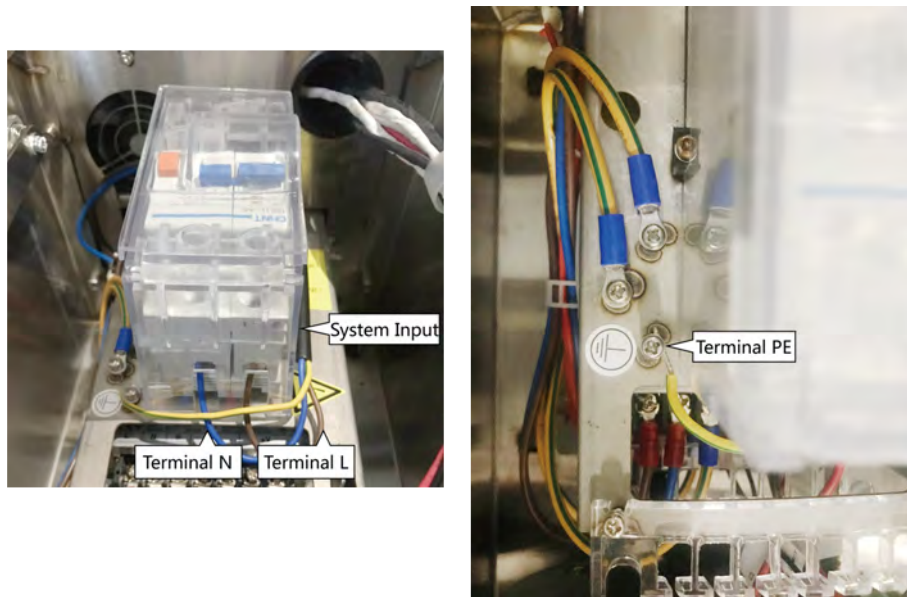
 Note

- If the turnstile contains two lanes, standing at the entrance position, the IR boards on the left pedestal are the IR sending boards. The IR boards on the right pedestal are the IR receiving boards. The IR boards on the left side of the middle pedestal are the IR receiving boards, while the IR boards on the right side of the middle pedestal are the IR sending boards.
 - Warning tags can be viewed on the side panel of each pedestal.
 - Safety Instructions can be viewed on the middle panel inside the pedestal.
-

4.2 Wiring Electric Supply

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

Before wiring, open the protective cover outside the switch.



Note

- The cable bare part should be no more than 8 mm. It is suggested that you can immerse the bare part into the liquid tin. If possible, wear an insulation cap at the end of the bare cable. Make sure there's no bare copper or cable after the wiring.
 - The Terminal L and the Terminal N cannot be wired reversely. Do not wire the input and output terminal reversely.
 - To avoid people injury and device damage, when testing, the ground resistance of the equipotential points should not be larger than 2 Ω .
-

4.3 Wire Interconnecting Cable

You should use interconnecting cables to connect the main lane board and the sub lane board for components communication.

The picture displayed below describes the cable hole's position on the pedestals.

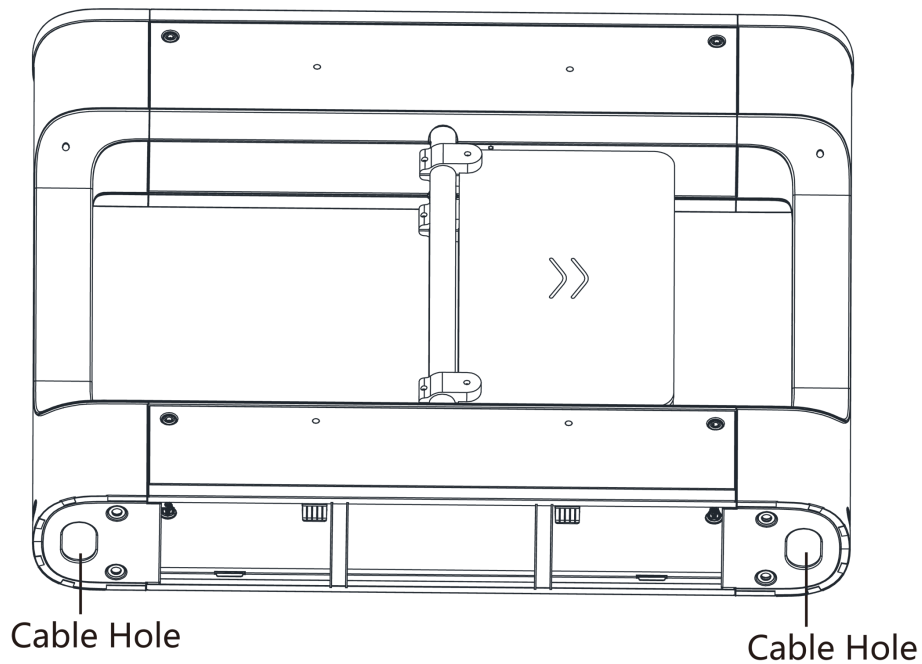


Figure 4-3 Cable Hole of Interconnecting Cable

Follow the instructions below to connect the interconnecting cable.

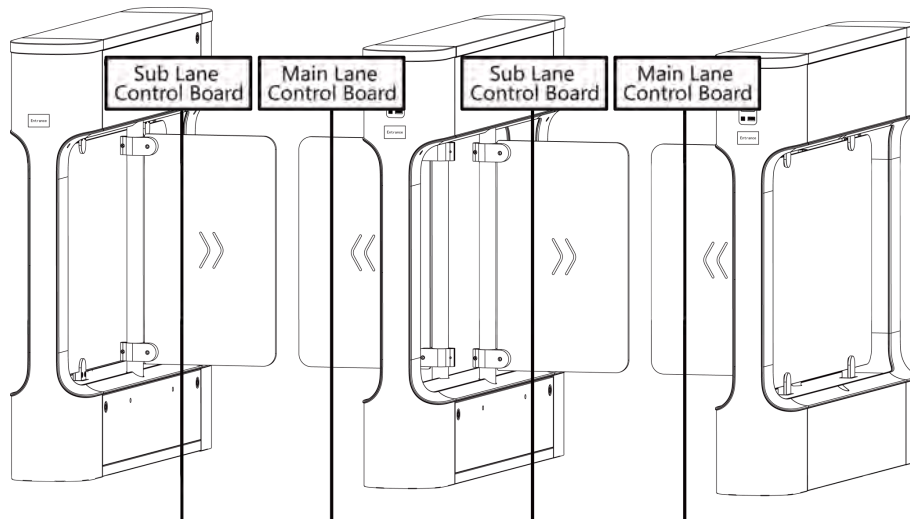


Figure 4-4 Connect Interconnecting Cable

4.3.1 Pull Interconnecting Cable

Steps

1. Use the key to unlock the upper lock of the pedestals and remove the top cover.

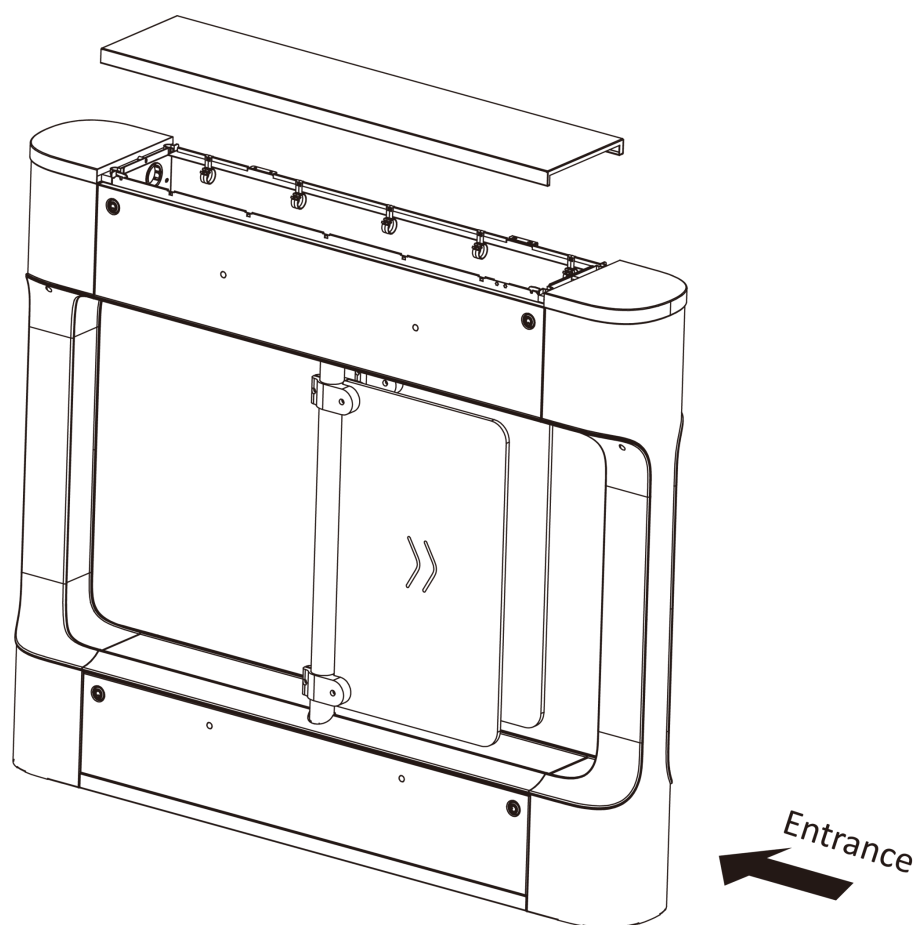


Figure 4-5 Dissemble Top Cover

2. Dissemble the card presenting board.

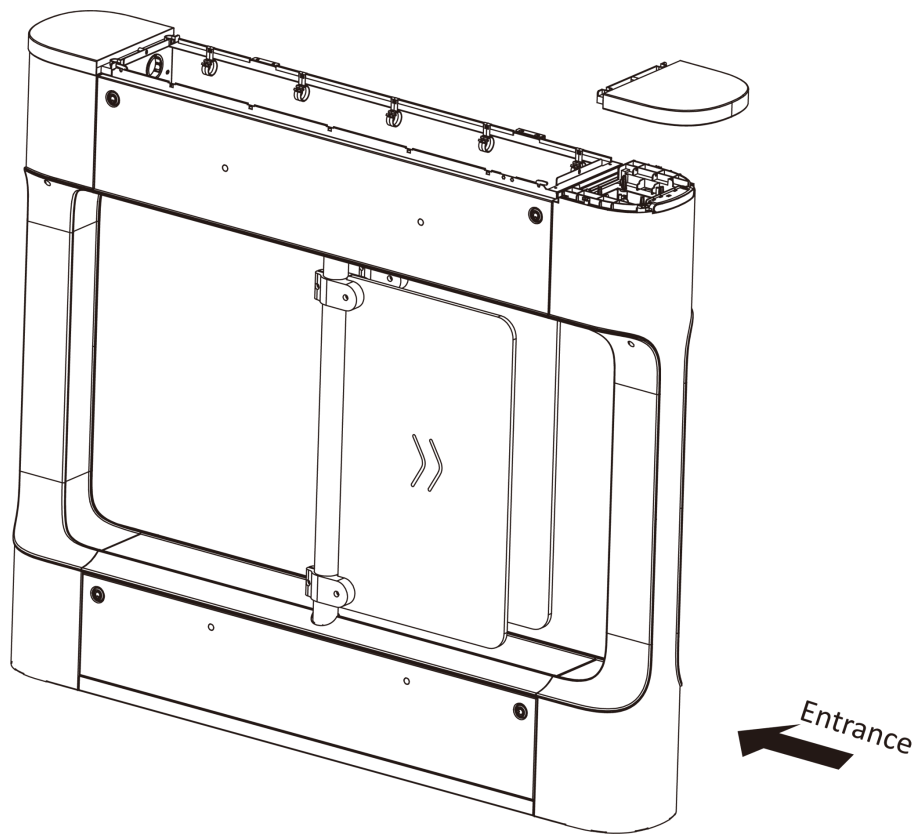


Figure 4-6 Disassemble Card Presenting Board

3. Disassemble the card reader module.

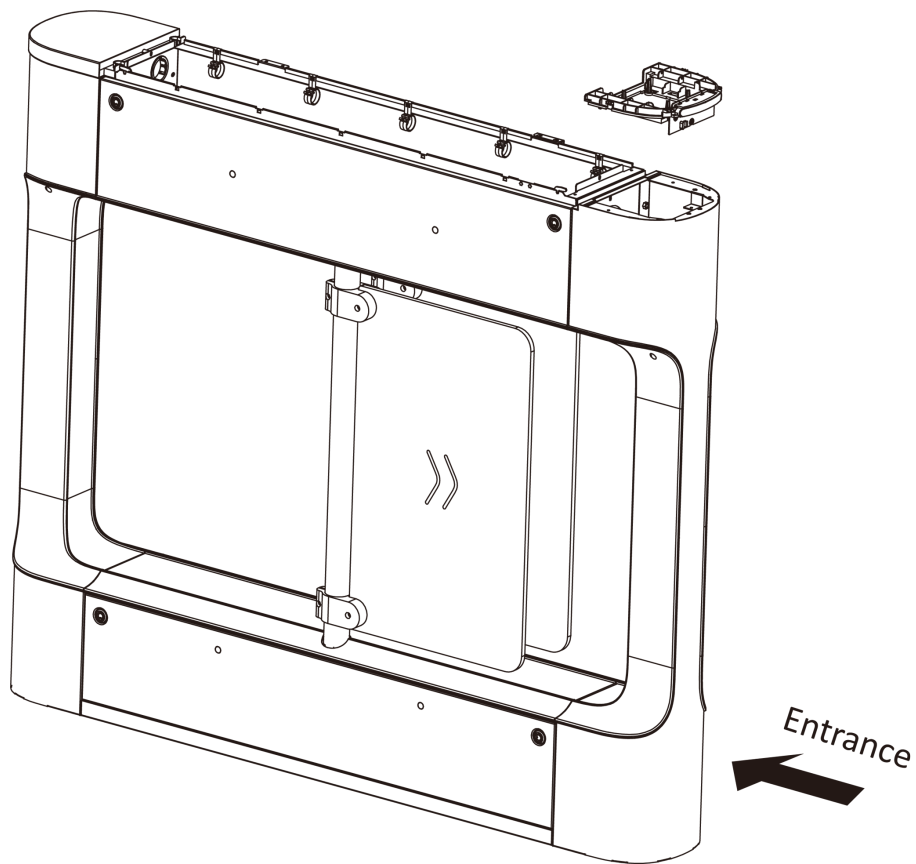


Figure 4-7 Dissemble Card Reader Module

4. Pull the interconnecting cable out from the bottom up with pull-out tool, and other wiring operations can be performed.

 Note

Interconnecting cable includes a network cable and a power supply cable of 24 V.

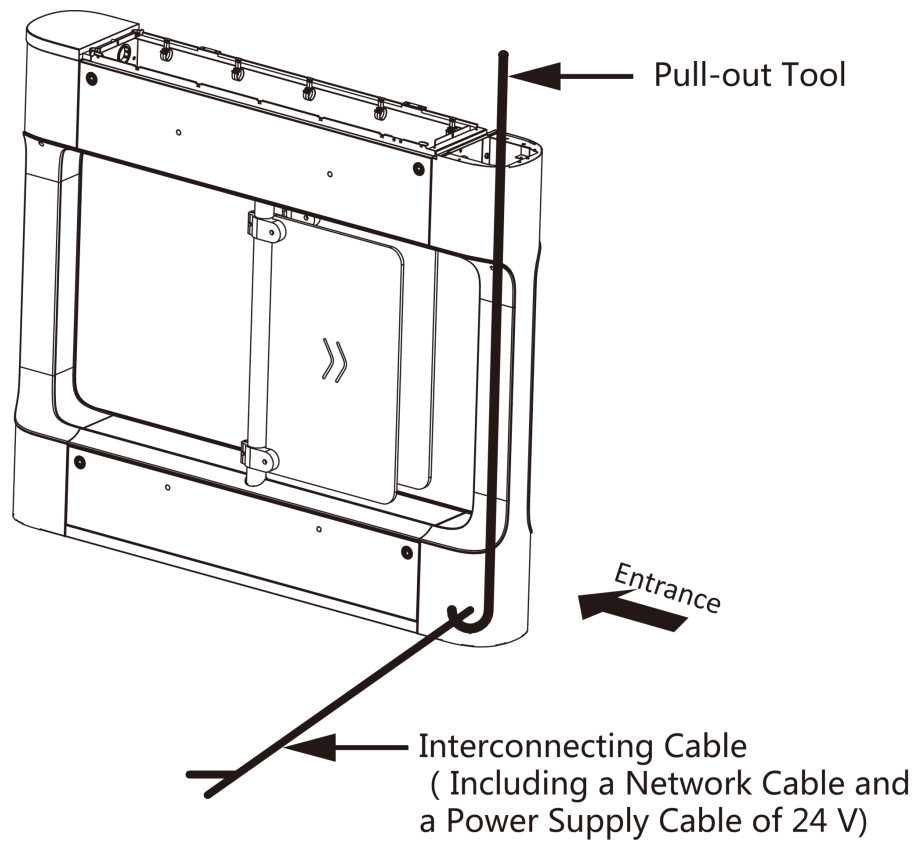


Figure 4-8 Pull out Interconnecting Cable

4.4 Wire Network Switch (Optional)

Connect the network cable and the network switch.

Steps

- 1.** Use the key to open the top cover of the pedestal.

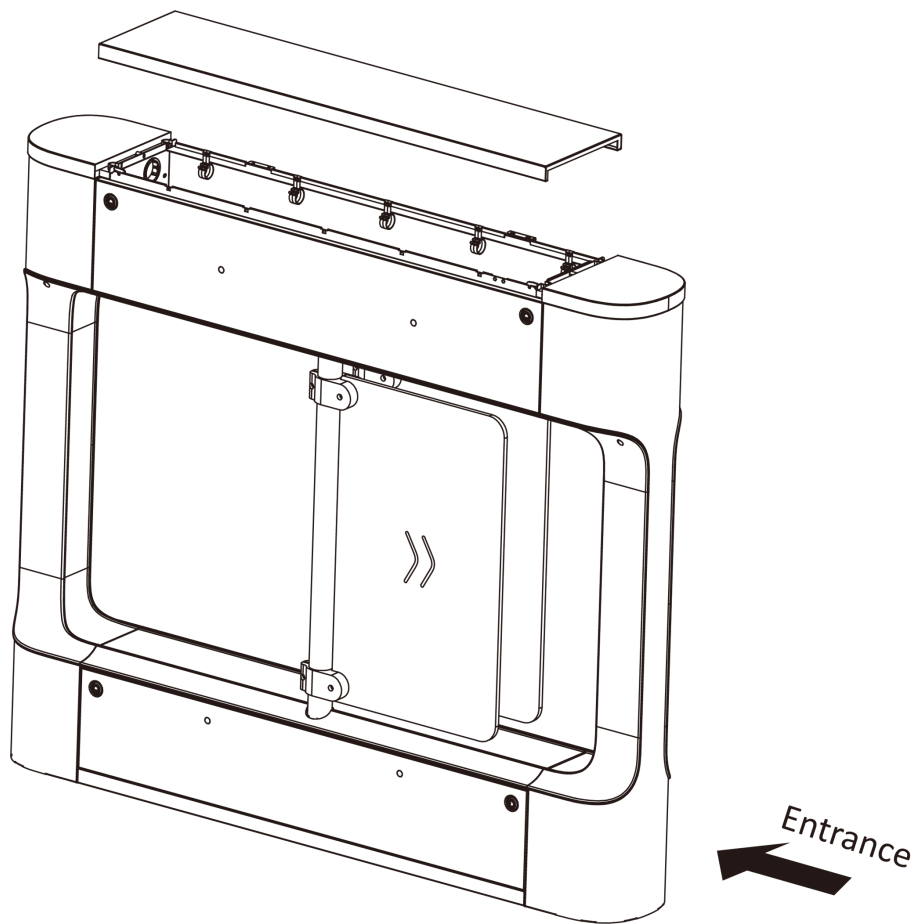


Figure 4-9 Open Top Cover

2. Attach the network switch to the position shown in the figure with adhesive.

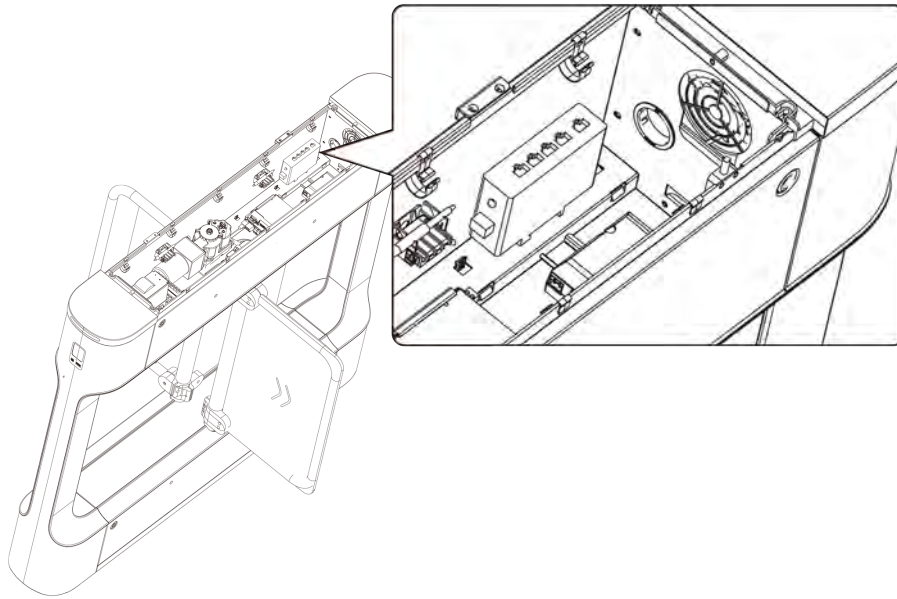


Figure 4-10 Network Switch Position

3. Lead out the 12 V power supply from the power switch and connect it to the switch power interface.
4. Connect the network cable according to your actual needs.

4.5 Terminal Description

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

4.5.1 Main Control Board Terminal Description

The main lane control board contains power input, BUS interface, interconnecting interface, supercapacitor interface, IR interface, barrier position control board interface and motor drive interface.

The picture displayed below is the main control board diagram.

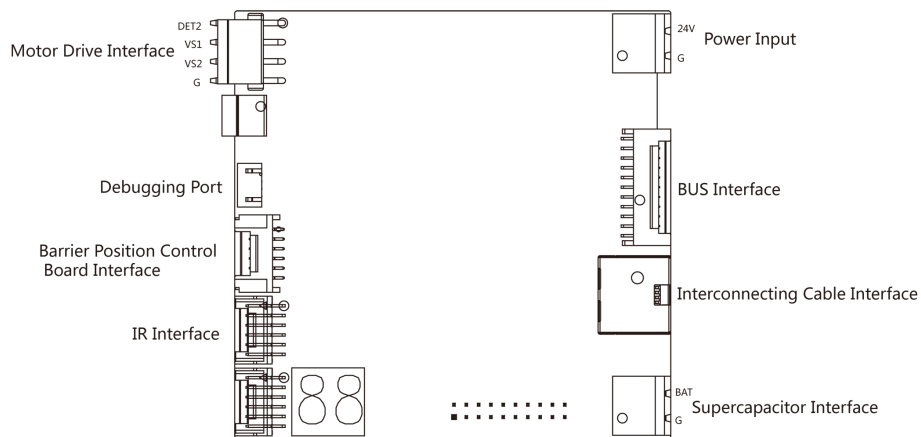


Figure 4-11 Main Control Board Terminal

4.5.2 Sub Control Board Terminal Description

The sub lane control board contains power input, BUS interface, interconnecting interface, supercapacitor interface, IR interface, barrier position control board interface and motor drive interface.

The picture displayed below is the sub control board diagram.

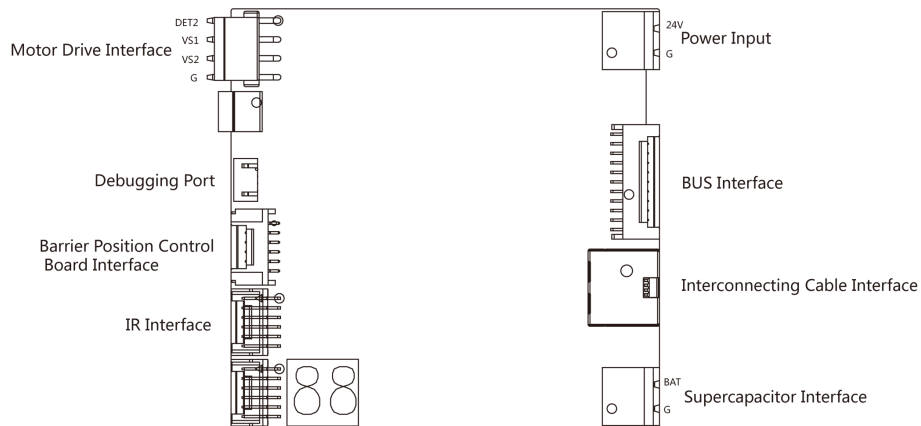


Figure 4-12 Sub Control Board Terminal

4.5.3 BUS Terminal Description

You can connect the lane controller light board, fan, TAMPER, lane control board, card reader, face recognition terminal, QR code scanner, etc. via the BUS terminal.

Note

Part of the wiring has been completed at the factory, please connect according to actual needs.

Table 4-1 BUS Terminal in Main Lane Controller

Terminal Name	Description
Lane Controller Light Board 1	Connects lane controller light board 1
Lane Controller Light Board 2	Connects lane controller light board 2
Fan 1	Connects fan 1
Fan 2	Connects fan 2
TAMPER	Connects TAMPER
Lane Controller Board	Connect sub lane controller board
5 V	Reserved
Port 1  Note External card reader is recommended to access.	Red 12 V: connects 12 VDC power supply terminal
	Yellow 485A/232A+: card reader RS-485A+/RS-232A+ access terminal
	Blue 485A/232A-: card reader RS-485A-/RS-232A- access terminal
	Black GND: grounding

Table 4-2 BUS Terminal in Sub Lane Controller (Left Pedestal)

Terminal Name	Description
Lane Controller Light Board 1	Connects lane controller light board 1
Lane Controller Light Board 2	Connects lane controller light board 2
Fan 1	Connects fan 1
Fan 2	Connects fan 2
TAMPER	Connects TAMPER
Lane Controller Board	Connect main lane controller board
Port 5  Note External card reader is recommended to access.	Red 12 V: connects 12 VDC power supply terminal
	Yellow 485E/232E+: card reader RS-485E+/RS-232E+ access terminal
	Blue 485E/232E-: card reader RS-485E-/RS-232E- access terminal
	Black GND: grounding
Port 6	Red 12 V: connects 12 VDC power supply terminal
	Yellow 485F/232F+: card reader RS-485F+/RS-232F+ access terminal

Terminal Name	Description
 Note External face recognition terminal is recommended to access.	Blue 485F/232F-: card reader RS-485F-/RS-232F- access terminal
	Black GND: grounding

Table 4-3 BUS Terminal in Sub Lane Controller (Middle Pedestal)

Terminal Name	Description
Lane Controller Light Board 1	Connects lane controller light board 1
Lane Controller Light Board 2	Connects lane controller light board 2
Lane Controller Board	Connect main lane controller board
Port 5	Red 12 V: connects 12 VDC power supply terminal
 Note External card reader is recommended to access.	Yellow 485E/232E+: card reader RS-485E+/RS-232E+ access terminal
	Blue 485E/232E-: card reader RS-485E-/RS-232E- access terminal
	Black GND: grounding
Port 6	Red 12 V: connects 12 VDC power supply terminal
 Note External face recognition terminal is recommended to access.	Yellow 485F/232F+: card reader RS-485F+/RS-232F+ access terminal
	Blue 485F/232F-: card reader RS-485F-/RS-232F- access terminal
	Black GND: grounding

4.5.4 Access Control Board Terminal Description

Access control board is mainly used for authority identification, external device accessing, and communication with the upper platform and lane controller.

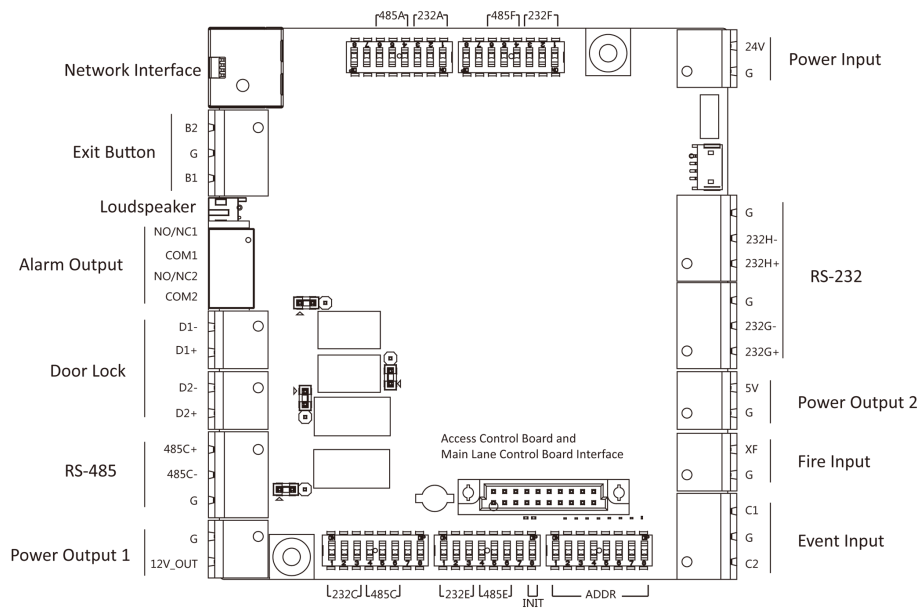


Figure 4-13 Access Control Board Terminal

Table 4-4 Access Control Board Terminal Description

Access Control Board Terminal Description			
Power Output 1	+12 V	12 VDC Power Output	/
	G	Grounding	
RS-485 Interface	RS-485 C+	Connect to Card Reader RS485+	RS-485 card reader ID factory DIP is 1 and 3. 1 represents the passage entrance, and 3 represents the passage exit. UART 1 in the main control board corresponds to the entrance card reader, and UART 5 in the main
	RS-485 C-	Connect to Card Reader RS485-	
	GND	Grounding	

Access Control Board Terminal Description			
			control board corresponds to the exit card reader. - If the user has configured a guest card, the exit needs to be connected to two card readers, one with the DIP 4 and the other with the DIP 3. The card reader 3 and the card receiver are used together, the ordinary user swipes the card on the card reader 4, and the guest user swipes the card on the card reader 3. - This is the RS-485 interface, which cannot be switched by dialing.
Power Output 2	5 V	5 VDC Power Output	/
	G	Grounding	

Access Control Board Terminal Description			
RS-232 Interface	G	Grounding	- This is the RS-232 interface, which cannot be switched by dialing. - By default, there is no QR code scanner on the left pedestal of the device entrance. If you need to connect an additional QR code scanner, you need to connect it through the RS-232 interface here. After the cable is connected to the RS-232 interface, it passes through the embedded pipe and connects with the QR code on the left.
	RS-232 G-	Connect to RS-232G-	
	RS-232 G+	Connect to Card Reader RS-232G+	
	G	Grounding	
	RS-232 H-	Connect to RS-232H-	
	RS-232 H+	Connect to Card Reader RS-232H+	
Power Input	+24 V	24 VDC Power Input	/
	GND	Grounding	

Access Control Board Terminal Description			
Event Input	C1	Event Alarm Input 1	The event alarm input hardware interface is remaining open, and only supports access to remaining open signals, which can be linked to the host buzzer output, card reader buzzer output, alarm relay output, door open relay output, etc.
	G	Grounding	
	C2	Event Alarm Input 2	
Exit Button	B2	Door 2 Signal Input	/
	G	Grounding	
	B1	Door 1 Signal Input	
Door Lock (Relay)	D1-	Door 1 Relay Output (Dry Contact)	If necessary, the door lock relay can be used to control the third-party barrier switch. D1 controls the door opening for ordinary entrance, and D2 controls the door opening for ordinary exit.
	D1+		
	D2-	Door 2 Relay Output (Dry Contact)	If necessary, the door lock relay can be used to control
	D2+		

Access Control Board Terminal Description			
			the third-party barrier switch. D1 controls the door opening for ordinary entrance, and D2 controls the door opening for ordinary exit.
Alarm Output	NO/NC1	Alarm Output Relay 1 (Dry Contact)	The alarm output supports switch output.
	COM1		
	NO/NC2	Alarm Output Relay 2 (Dry Contact)	The alarm output supports switch output.
	COM2		
Loudspeaker	/	Connect to loudspeaker	/
Network Interface	LAN	Network Accessing	/
Fire Input	XF	Fire input	/
	G	Grounding	

**Note**

- You can switch between RS-485 and RS-232 via the DIP switch on the access control board. For details about DIP switch and switching method, see **Access Control Board Serial Port ID Description**.
- For details about DIP switch operation, see **DIP Switch Description**.

4.5.5 Access Control Board Serial Port ID Description

You can set the device mode, switch the communication mode of the corresponding UART, and initialize the device through the DIP on the access control board.

The DIP switch of the access control board is shown in the figure below:

**Note**

The diagram is for reference only.

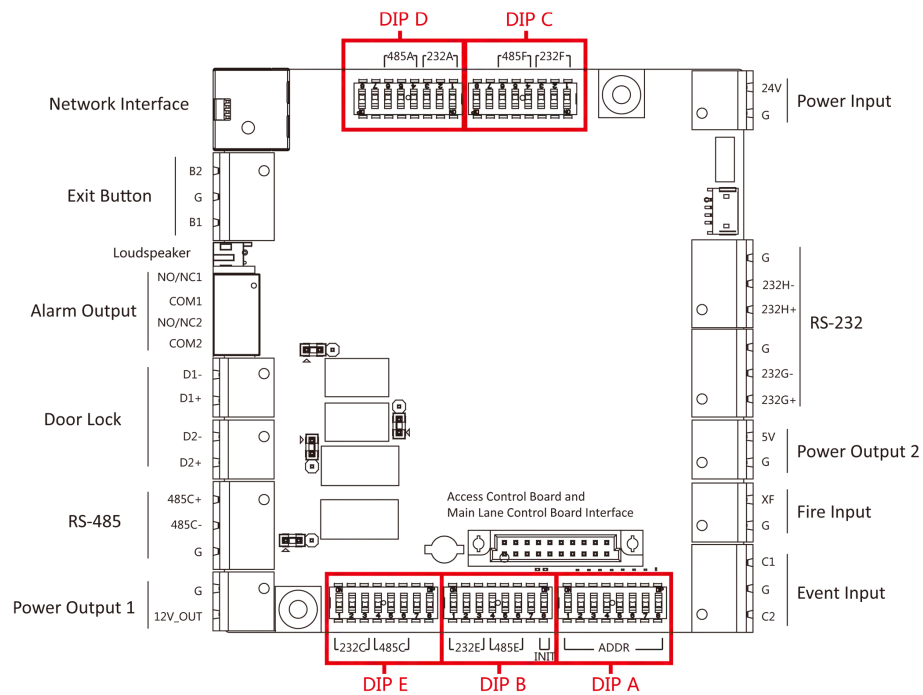


Figure 4-14 DIP Switch on Access Control Board

DIP A can set the device mode, DIP 2 to 5 can set the RS-485/RS-232 interface, and DIP B can also be used to initialize the device.

The UART corresponding to the DIP Switch is shown in the figure below:

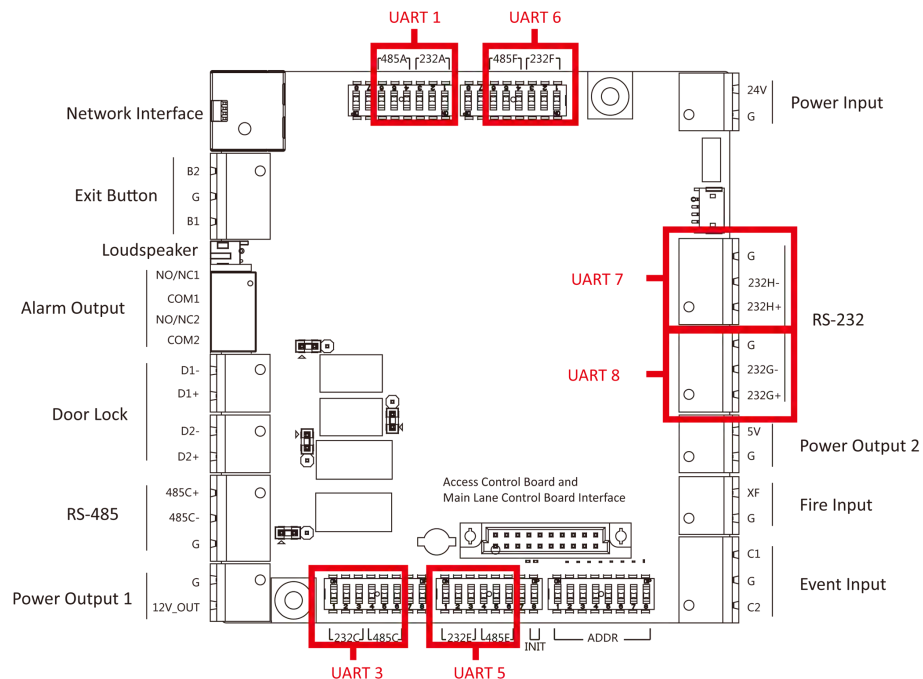


Figure 4-15 UART No. Description

The corresponding functions of different DIP Switch are described as follows:

No.	Device Mode	UART No.	Function	Binary Value
DIP A	1 to 2: Work Mode	/	Normal Mode	ON 1 2 3 4 5 6 7 8
			Test Mode	ON 1 2 3 4 5 6 7 8
	3: Memory Mode		Enable Memory Mode	ON 1 2 3 4 5 6 7 8
			Disable Memory Mode	ON 1 2 3 4 5 6 7 8
	4: Keyfob Paring Mode		Enable Keyfob Paring Mode	ON 1 2 3 4 5 6 7 8
			Disable Keyfob Paring Mode	ON 1 2 3 4 5 6 7 8
	5 to 8: Passing Mode		Controlled Bi-direction	ON 1 2 3 4 5 6 7 8
			Controlled Entrance and Prohibit Exit	ON 1 2 3 4 5 6 7 8
			Controlled Entrance and Free Exit	ON 1 2 3 4 5 6 7 8
			Free Bi-direction	ON 1 2 3 4 5 6 7 8
			Free Entrance and Controlled Exit	ON 1 2 3 4 5 6 7 8

No.	Device Mode	UART No.	Function	Binary Value
			Free Entrance and Prohibit Exit	
			Prohibited Bi-direction	
			Prohibit Entrance and Controlled Exit	
			Prohibit Entrance and Free Exit	
DIP B	1 to 3	UART 5	ON: UART 5 is RS-232E Interface	/
	4 to 6		ON: UART 5 is RS-485E Interface	/
	7	/	Reserved	/
	8	/	Default is OFF. You can dial to ON for initial operation	/
DIP C	1 to 3	UART 6	ON: UART 6 is RS-232F Interface	/
	4 to 6		ON: UART 6 is RS-485F Interface	/
	7	/	Reserved	/
	8	/	Reserved	/
DIP D	1 to 3	UART 1	ON: UART 1 is RS-232A Interface	/
	4 to 6		ON: UART 1 is RS-485A Interface	/
	7	/	Reserved	/
	8	/	Reserved	/
DIP E	1 to 3	UART 3	ON: UART 3 is RS-232C Interface	/

No.	Device Mode	UART No.	Function	Binary Value
	4 to 6		ON: UART 3 is RS-485C Interface	/
	7	/	Reserved	/
	8	/	Reserved	/

Note

Switch 1 to 3, 4 to 6, 7, and 8 of DIP B, DIP C, DIP D, and DIP E cannot be turned ON at the same time.

The reserved UART terminal positions in the turnstile and their corresponded UART No. are as follows:

Note

The diagram is for reference only.

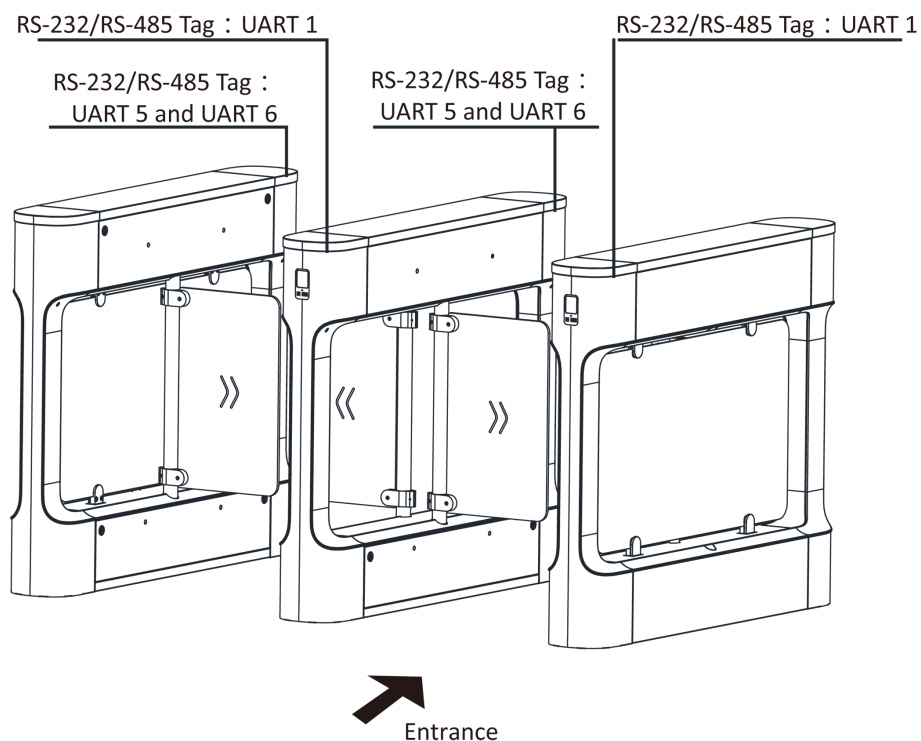
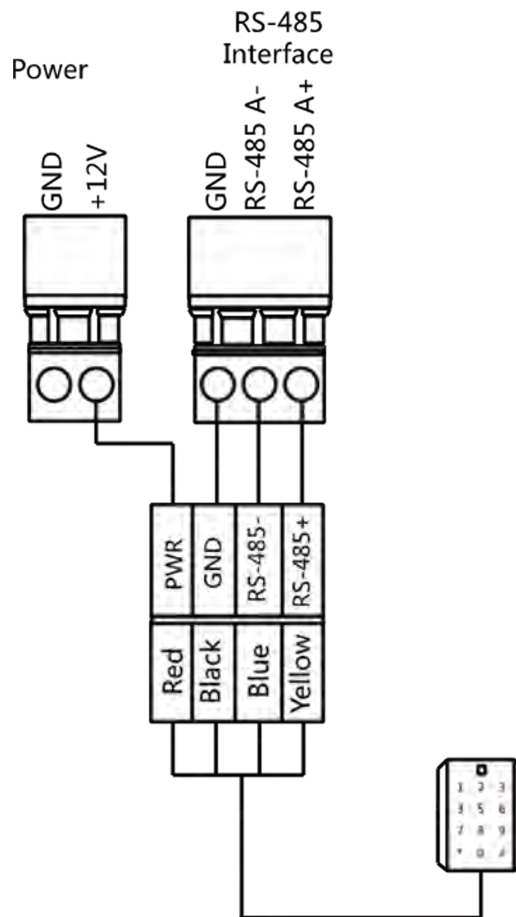


Figure 4-16 Interface and Corresponded UART No.

4.5.6 RS-485 Wiring



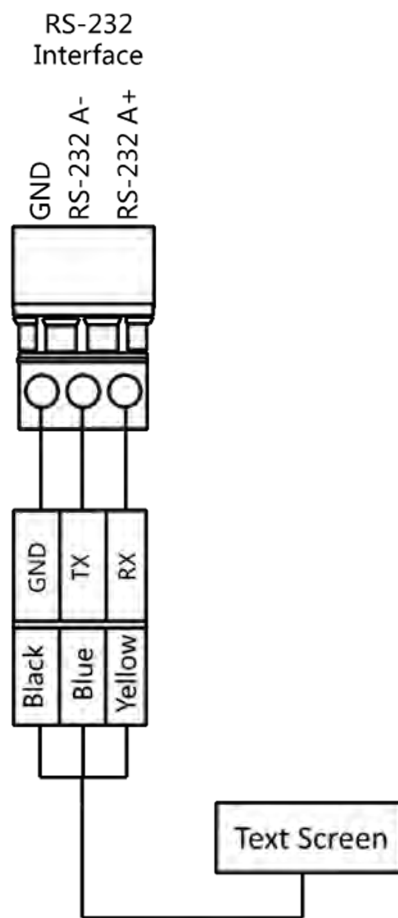
Note

- The RS-485 interfaces are for connecting ID card reader, IC card reader, QR code scanner, card reader, card recycler, text screen, and face recognition terminal. Take the wiring of RS-485 card reader as an example.
 - For details about text screen, see *Configuring Screen Parameters* in *User Manual of iVMS-4200 AC Client Software*.
-

4.5.7 RS-232 Wiring

Note

- Access control board of pedestal can connect QR code scanner, card recycler, text screen and face recognition terminal via RS-232 interface.
- For details about text screen, see *Configuring Screen Parameters* in *User Manual of iVMS-4200 AC Client Software*.
- Take the wiring of text screen as an example.



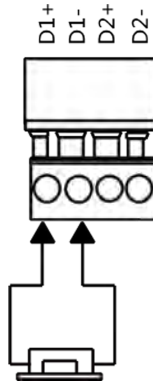
4.5.8 Barrier Control Wiring

By default, the barrier has connected with the access control board. The lane control board can control the barrier status. If possible, the device can connect with a third party lane control board to control the third party barriers. Interface D1 controls barrier opening for entrance, while interface D2 controls barrier opening for exit.

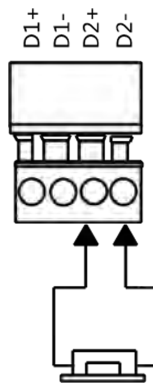
Note

Use the jumper cap to switch the relay status. For details, see **Barrier Control Relay Output Mode** .

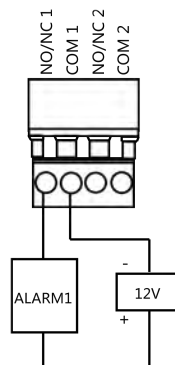
Entering Wiring



Exiting Wiring



4.5.9 Alarm Output Wiring





Note

For details about changing the relay output status via the jumper cap, see ***Alarm Relay Output Mode (NO/NC)*** .

Chapter 5 Device Settings

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

After the learning, the turnstile is in the normal mode. You can also set the turnstile to test mode, passing mode and memory mode, pair the keyfob, initialize the hardware, switching between RS-485 communication mode and RS-232 communication mode, and view relay output NO/NC diagram by setting the DIP switch on the access control board.

- Normal Mode: The device will work properly.
- Test Mode: Test mode is the same as the normal mode except that the device cannot report the alarm, the event, or the people counting information to the center.
- Passing Mode: There are 9 passing modes, including controlled bi-direction, controlled entrance and prohibited exit, controlled entrance and free exit, free bi-direction, free entrance and controlled exit, free entrance and prohibited exit, prohibited bi-direction, prohibited entrance and free exit.
- Memory Mode: By default, the memory mode is enabled. When multiple cards are presented and authenticated, it allows multiple persons passing through the lane. When it counts the passing people number is equal to the card presented times, or no person passing through the lane after the last person passing, the barriers will be closed.



Note

You can also set the DIP switch on the access control board to control the entrance and exit controlling type, keyfob pairing, etc. For details about the DIP switch value, see **Access Control Board Serial Port ID Description** .

5.1 Pair Keyfob (Optional)

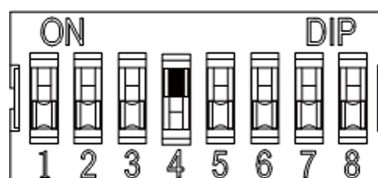
Pair the remote control to the device through DIP switch to open/close the barrier remotely.

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

1. Power off the turnstile.
2. Set the No.4 switch of the DIP 1 Switch on the access control board to the ON side.



3. Power on the turnstile and it will enter the keyfob pairing mode.

4. Hold the **Close** button for more than 10 seconds. Or pair turnstile and keyfob in the client software, see **Manage Keyfob User** for more details.

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

5. Set the No.4 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.

5.2 Initialize Device

Steps

1. Set the No.8 switch of the DIP 2 Switch on the access control board to the ON side.

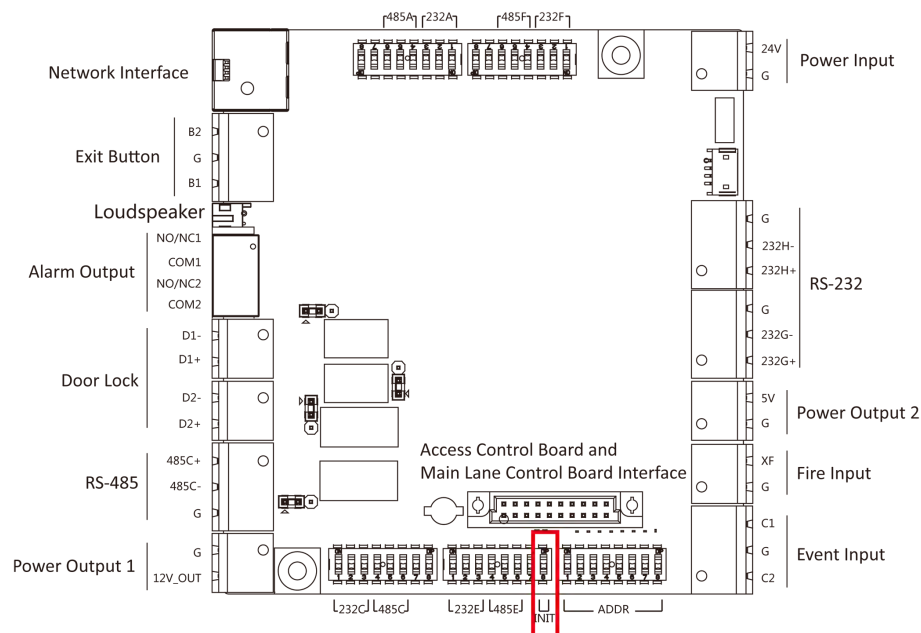


Figure 5-1 Initialization Jumper Cap

2. Disconnect the power and reboot the device. The device buzzer buzzes a long beep.
3. When the beep stopped, set the No.8 switch to the OFF side, and reboot the turnstile to take effect.
4. Disconnect the power and power on the device again.



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.

5.3 Switch Relay Output Mode (NO/NC)

5.3.1 Barrier Control Relay Output Mode

The jumper cap of the barrier control relay on the access control board is as below:

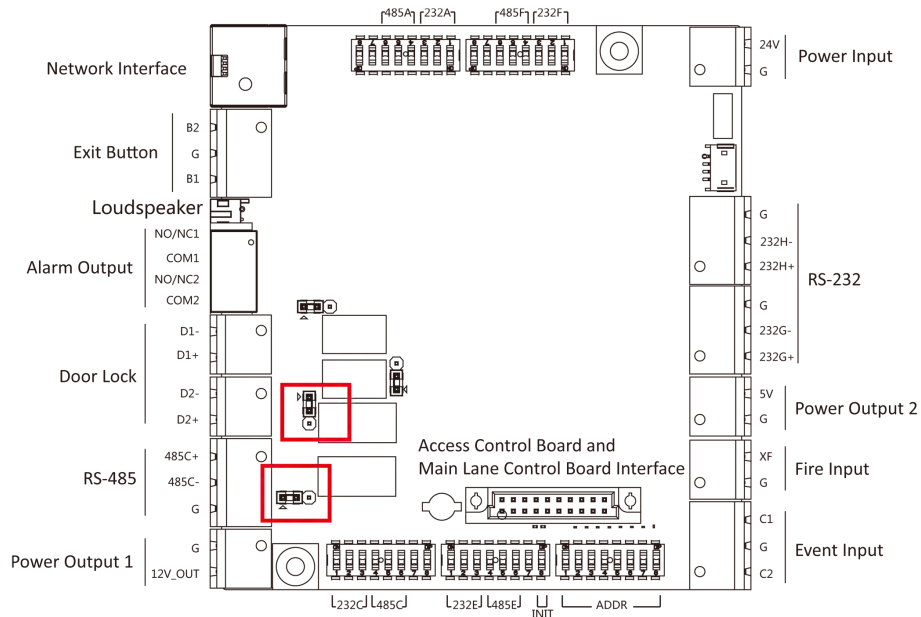


Figure 5-2 Jumper Cap Location (Barrier Control Relay Output Mode)

The jumper cap position of barrier opening (NO) is as below:



Figure 5-3 Barrier Opening (NO)

The jumper cap position of barrier closing (NC) is as below:

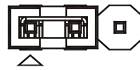


Figure 5-4 Barrier Closing (NC)



Note

The default status is NC.

5.3.2 Alarm Relay Output Mode (NO/NC)

The jumper cap of the alarm relay on the access control board is as below:

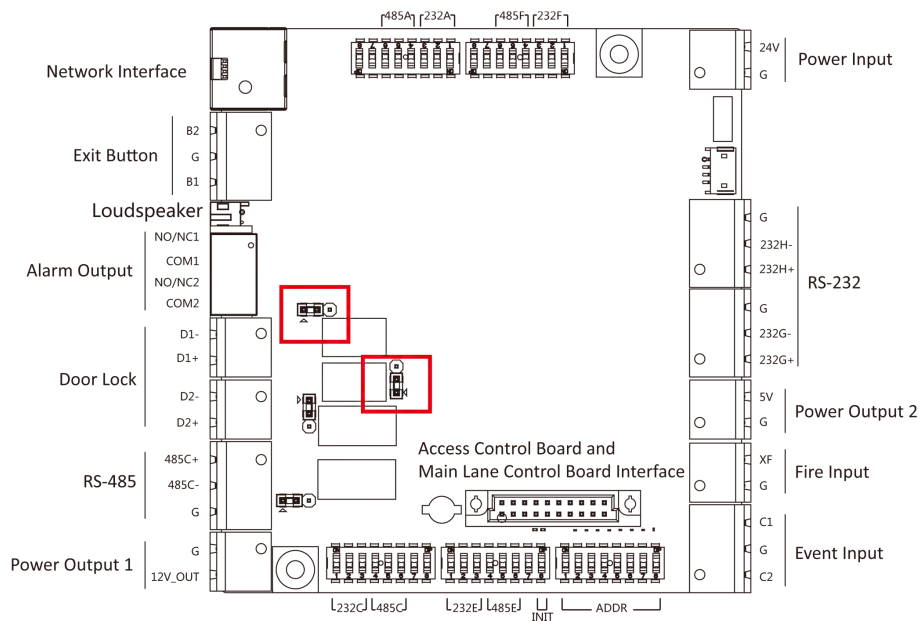


Figure 5-5 Jumper Cap Location (Alarm Relay Output Mode)

The jumper cap position of alarm opening (NO) is as below:

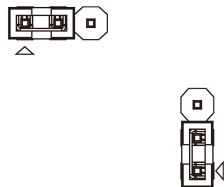


Figure 5-6 Alarm Opening (NO)

The jumper cap position of alarm closing (NC) is as below:

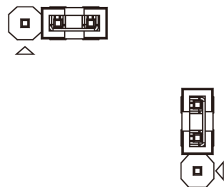


Figure 5-7 Alarm Closing (NC)

Note

The default status is NO.

Chapter 6 Activation

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

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

The default values of the device are as follows:

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

6.1 Activate via 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

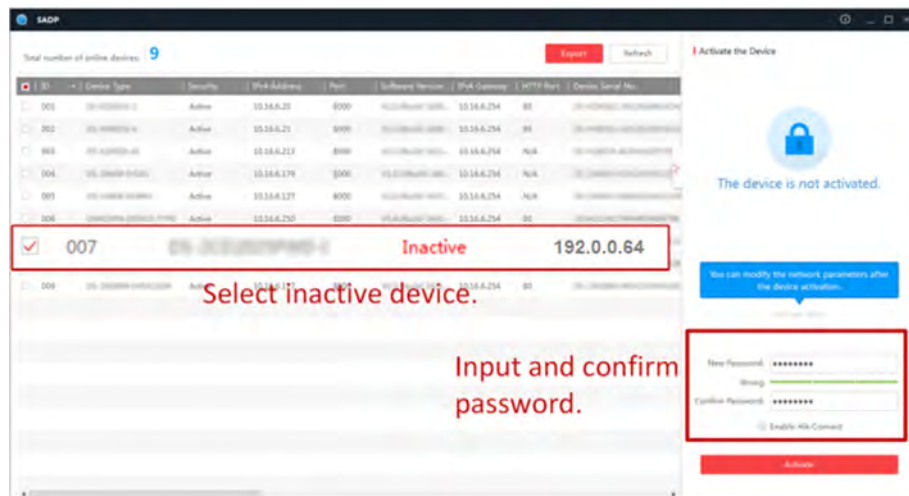
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.



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.

6.2 Activate Device via Client Software

For some devices, you are required to create the password to activate them before they can be added to the 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.

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

Chapter 7 Client Software Configuration

7.1 Configuration Flow of Client Software

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

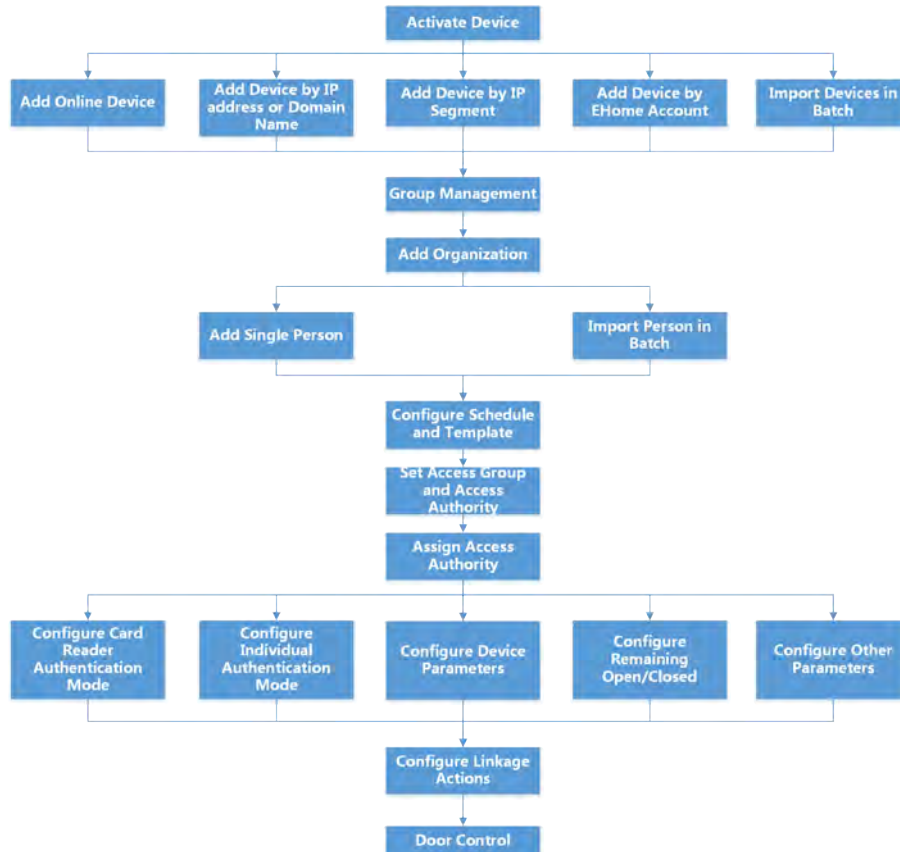


Figure 7-1 Flow Diagram of Configuration on Client Software

7.2 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.

7.2.1 Add Device

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

Add Online Device

The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area. You can click **Refresh Every 60s** to refresh the information of the online devices.

Add Single Online Device

You can add single online device to the client software.

Steps

1. Enter the Device Management module.
2. **Optional:** 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. Select an online device from the **Online Device** area.



Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to **Activation** .

5. Click **Add** to open the device adding window.
6. Enter the required information.

Name

Enter a descriptive name for the device.

Address

The IP address of the device is obtained automatically in this adding mode.

Port

The port number is obtained automatically.

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.

7. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
 8. **Optional:** Check **Import to Group** to create a group by the device name.
-



Note

You can import all the channels of the device to the corresponding group by default.

9. Click **OK** to add the device.

Add Multiple Online Devices

You can add multiple online devices to the client software.

Steps

1. Enter the Device Management module.
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. Select multiple devices.
-



Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to **Activation**.

5. Click **Add** to open the device adding window.
6. Enter the required information.

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.

7. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the devices to the client.
 8. **Optional:** Check **Import to Group** to create a group by the device name.
-



Note

You can import all the channels of the device to the corresponding group by default.

9. Click **OK** to add the devices.

Add Device by IP Address or Domain Name

When 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**.

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: Add the offline devices.

- 1) Check **Add Offline Device**.
- 2) Enter the required information, including the device channel number and alarm input number.



Note

When the offline device comes online, the software will connect it automatically.

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.
8. Finish adding the device.
 - Click **Add** to add the device and back to the device list page.
 - Click **Add and Continue** to save the settings and continue to add other device.
9. Optional: Perform the following operation(s).

Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.



Note

For detail operation steps for the remote configuration, see the user manual of the device.

Device Status

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.

Edit Device Information

Click  on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User

Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh

Click  on Operation column to get the latest device information.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

Add Devices by IP Segment

If the devices share the same port No., user name and password, and their IP addresses are sharing an IP segment. You can specify the start IP address and the end IP address, port No., user name, password, etc of the devices to add them to the client.

Steps

1. Enter the 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.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

Start IP

Enter a start IP address.

End IP

Enter an end IP address in the same network segment with the start IP.

Port

Enter the device port No. The default value is **8000**.

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.

6. **Optional:** Add the offline devices.

- 1) Check **Add Offline Device**.

- 2) Enter the required information, including the device channel number and alarm input number.



Note

When the offline device comes online, the software will connect it automatically.

7. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. **Optional:** Check **Import to Group** to create a group by the device name.
9. Finish adding the device.
- Click **Add** to add the device and back to the device list page.
 - Click **Add and Continue** to save the settings and continue to add other device.
10. **Optional:** Perform the following operation(s).

Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.



Note

For detail operation steps for the remote configuration, see the user manual of the device.

Device Status

Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.

Edit Device Information

Click  on Operation column to edit the device information, such as IP address, user name, and password.

Check Online User

Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

Refresh

Click  on Operation column to get the latest device information.

Delete Device

Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

Import Devices in a Batch

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

Steps

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

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



Note

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

Adding Mode

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

Address

Edit the address of the device.

Port

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

User Name

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

Password

Enter the device password.



Caution

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

Proper configuration of all passwords and other security settings is the responsibility of the 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.
8. **Optional:** Perform the following operation(s).

Remote Configuration

Click  on Operation column to set remote configuration of the corresponding device.



Note

For detail operation steps for the remote configuration, see the user manual of the device.

Device Status	Click  on Operation column to view device status, including cameras, recording status, signal status, hardware status, etc.
Edit Device Information	Click  on Operation column to edit the device information, such as IP address, user name, and password.
Check Online User	Click  on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.
Refresh	Click  on Operation column to get the latest device information.
Delete Device	Select one or multiple devices and click Delete to delete the selected device(s) from the client.

7.2.2 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.

7.3 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.

7.3.1 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.

7.3.2 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.

7.3.3 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For access point, you can edit the access point name. For alarm input, you can edit the alarm input name. Here we take access point as an example.

Before You Start

Import the resources to group.

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
All the added groups are displayed on the left.
3. Select a group on the group list and click **Access Point**.
The access points imported to the group will display.
4. Click  in the Operation column to open the Edit Resource window.
5. Edit the resource name.
6. Click **OK** to save the new settings.

7.3.4 Remove Resources from Group

You can remove the added resources from the group.

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
All the added groups are displayed on the left.
3. Click a group to show the resources added to this group.
4. Select the resource(s) and click **Delete** to remove the resource(s) from the group.

7.4 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.

7.4.1 Add Organization

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

Steps

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



Note

Up to 10 levels of organizations can be added.

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

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.

7.4.2 Configure Basic Information

You can add person to the client one by one and configure the person's basic information such as name, gender, email, phone number, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.
The Person ID will be generated automatically.
4. Enter the basic information including person name, gender, telephone number, email address, validity period, etc.

Basic Information

* Person ID HZ000002

* Name

Gender ☒ Male ☐ Female

Email

Tel.

Validity Period (Access Control) 2020-07-16 00:00:00-2030-07-15 23:59:59 **Extend**

Remark

Add Face

Figure 7-2 Configure Basic Information



Note

Once validity period expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors. You can click **Extend** to extend the person's validity period for 1 month, 3 months, 6 months, or 1 year.

5. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

7.4.3 Issue a Card by Local Mode

If a card enrollment station is available, you can issue a card by local mode. To read the card number, you should connect the card enrollment station to the PC running the client by USB interface or COM, and place the card on the card enrollment station.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

3. In the **Credential → Card** area, click +.
4. Click **Settings** to enter the Settings page.
5. Select **Local** as the card issuing mode.

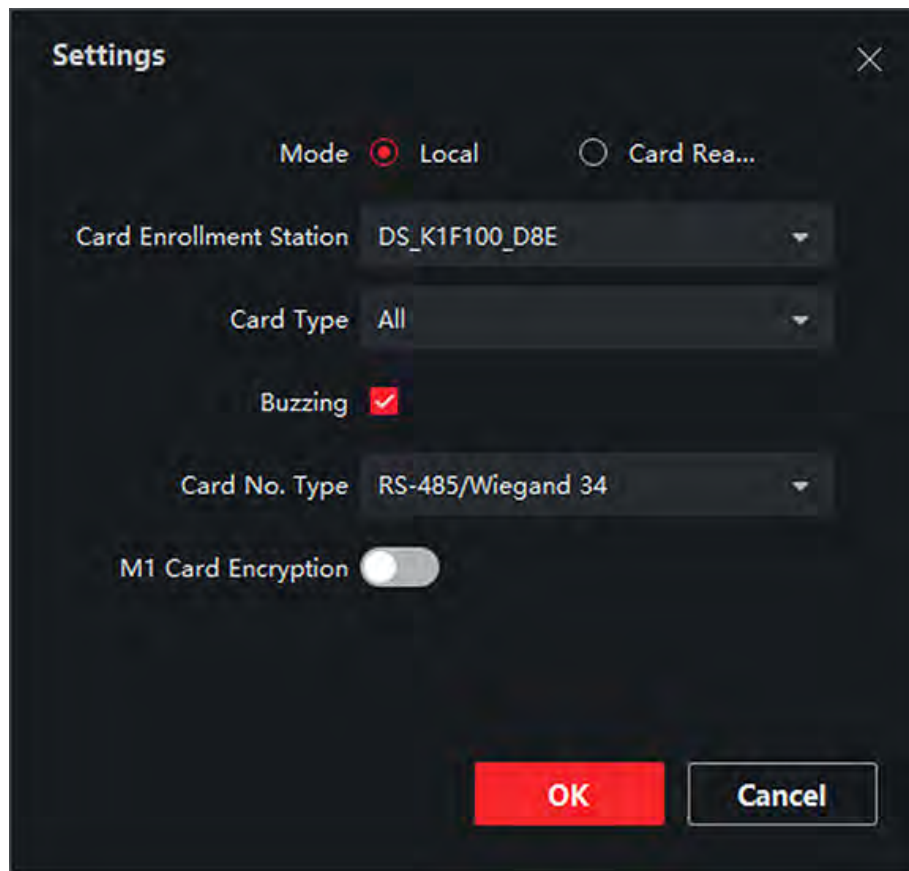


Figure 7-3 Issue a Card by Local Mode

6. Set other related parameters.

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 Mifare card according to the actual card type.

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, then you can enable the M1 Card Encryption function and select the sector of the card to encrypt.

7. Click **OK** to confirm the operation.
8. Place the card on the card enrollment station, and click **Read** to get the card number.
The card number will display in the Card No. field automatically.
9. Click **Add**.
The card will be issued to the person.

7.4.4 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

3. Click **Add Face** in the Basic Information panel.
4. Select **Upload**.
5. Select a picture from the PC running the client.



Note

The picture should be in JPG or JPEG format and smaller than 200 KB.

6. **Optional:** Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

7.4.5 Take a Photo via Client

When adding a person, you can take a photo of the her/him via the client and set this photo as the person's profile.

Before You Start

Make sure PC running the client has a camera or you have connected other USB camera to the PC.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person window.



Note

Enter the person's basic information first. For details, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information area.
4. Select **Take Photo** to enter Take Photo window.
5. **Optional:** Enable **Verify by Device** to check whether the captured face photo can meet the uploading requirements.
6. Take a photo.
 - 1) Face to the camera and make sure your face is in the middle of the collecting window.
 - 2) Click  to capture a face photo.
 - 3) **Optional:** Click  to capture again.
 - 4) Click **OK** to save the captured photo.

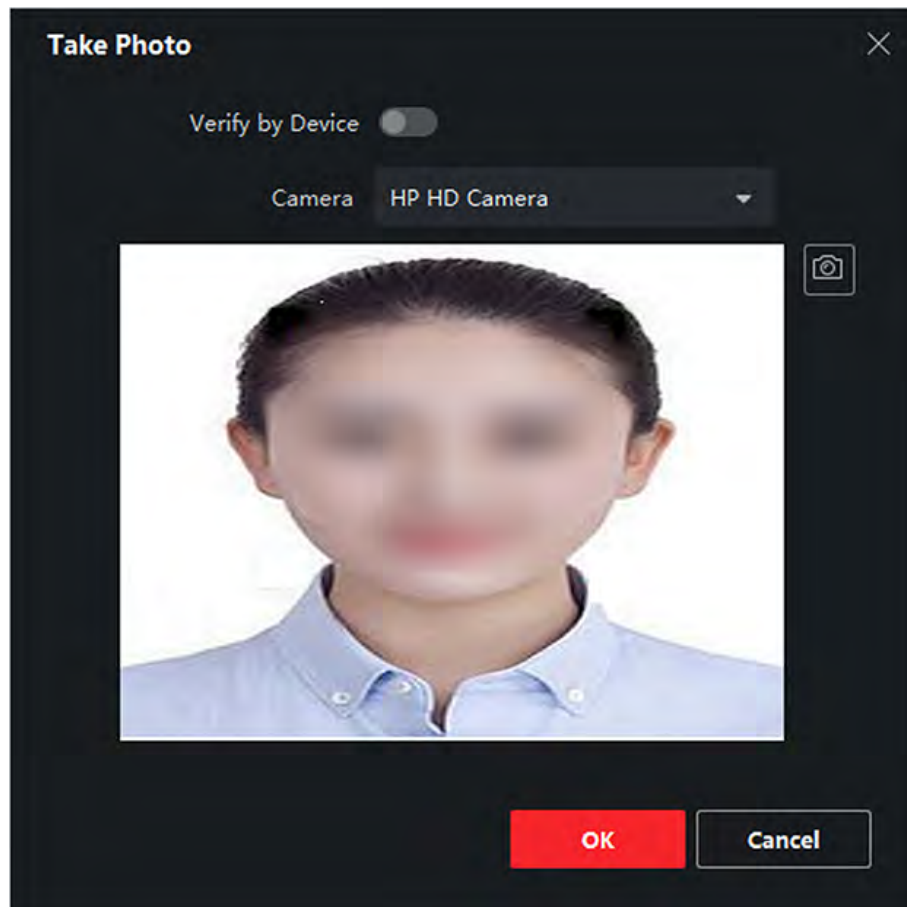


Figure 7-4 Take a Photo via Client

7. Confirm to add the person.

- Click **Add** to add the person and close the Add Person window.
- Click **Add and New** to add the person and continue to add other persons.

7.4.6 Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information panel.
4. Select **Remote Collection**.
5. Select an access control device which supports face recognition function from the drop-down list.
6. Collect face.
 - 1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
 - 2) Click  to capture a photo.
 - 3) Click **OK** to save the captured photo.
7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

7.4.7 Collect Fingerprint via Client

Collecting fingerprints locally means you can collect the fingerprint via the fingerprint recorder connected directly to the PC running the client. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Connect the fingerprint recorder to the PC running the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information***.

3. In the **Credential → Fingerprint** panel, click **+**.
 4. In the pop-up window, select the collection mode as **Local**.
 5. Select the model of the connected fingerprint recorder.
-



Note

If the fingerprint recorder is DS-K1F800-F, you can click **Settings** to select the COM the fingerprint recorder connects to.

6. Collect the fingerprint.
 - 1) Click **Start**.
 - 2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.
 - 3) Click **Add** to save the recorded fingerprint.
 7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.
-



Note

Once the fingerprint is added, the fingerprint type cannot be changed.

7.4.8 Configure Access Control Information

When adding a person, you can set her/his access control information, such as binding an access control group with the person, configuring PIN code, setting the person as a visitor, a blocklist person, or a super user, etc.

Steps

1. Enter **Person** module.
 2. Select an organization in the organization list to add the person and click **Add**.
 3. In the **Access Control** area, click  to select access group(s) for the person.
-



Note

For details, refer to ***Set Access Group to Assign Access Authorization to Persons***.

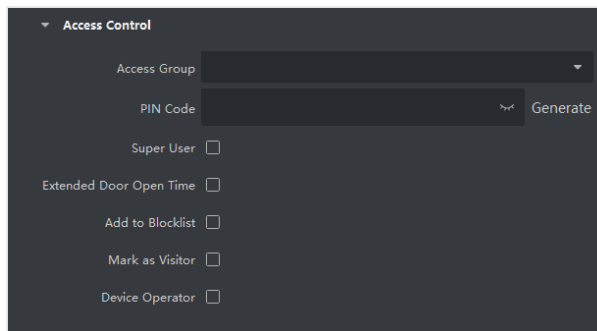


Figure 7-5 Configure Access Control Information

4. Set a unique PIN code for the person which can be used for access authentication.
 - Manually enter a PIN code containing 4 to 8 digits.



Note

Persons' PIN codes cannot be repeated.

- Click **Generate** to randomly generate an unrepeated PIN code of 6 digits.



Note

If there are repeated PIN codes, a prompt will pop up on the client. The admin can generate a new PIN code to replace the repeated PIN code and notify related persons.

5. Check the person's operation permissions.

Super User

If the person is set as a super user, he/she will have authorization to access all the doors/floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

Extended Door Open Time

Use this function for persons with reduced mobility. When accessing the door, the person will have more time than others to pass through doors.

For details about setting the door's open duration, refer to ***Configure Parameters for Door***.

Add to Blocklist

Add the person to the blocklist and when the person tries to access doors/floors, an event will be triggered and sent to the client to notify the security personnel.

Mark as Visitor

If the person is a visitor, you should set the her/his valid times for visit.



Note

The valid times for visit is between 1 and 100. You can also check **No Limit**, then there are no limited times for the visitor to access doors/floors.

Device Operator

For person with device operator role, he/she is authorized to operate on the access control devices.



Note

The Super User, Extended Door Open Time, Add to Blocklist, and Mark as Visitor functions cannot be enabled concurrently. For example, if one person is set as super user, you cannot enable extended door open time for her/him, add her/him to the blocklist, or set her/him as visitor.

6. Confirm to add the person.

- Click **Add** to add the person and close the Add Person window.
- Click **Add and New** to add the person and continue to add other persons.

7.4.9 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
 - 1) Click **Custom Property**.
 - 2) Click **Add** to add a new property.
 - 3) Enter the property name.
 - 4) Click **OK**.
3. Set the custom information when adding a person.
 - 1) Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to **Configure Basic Information**.

- 2) In the **Custom Information** panel, enter the person information.
- 3) Click **Add** to add the person and close the Add Person window, or click **Add and New** to add the person and continue to add other persons.

7.4.10 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

Steps

1. Enter **Person** module.

2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Resident Information** panel, select the indoor station to bind it to the person.



Note

If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

7.4.11 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Additional Information** panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
4. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

7.4.12 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.

7.4.13 Import Person Information

You can enter the information of multiple persons in a predefined template (a CSV 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 file with person information.
 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 10,000 persons.
-

7.4.14 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.

7.4.15 Export Person Information

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

Before You Start

Make sure you have added persons to an organization.

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** to open the Export panel and check **Person Information** as the content to export.
4. Check desired items to export.
5. Click **Export** to save the exported CSV file in your PC.

7.4.16 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.

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** to open the Export panel and check **Face** as the content to export.
4. Click **Export** to start exporting.



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).
-

7.4.17 Get Person Information from Access Control Device

If the added 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 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.
 - The gender of the persons will be **Male** by default.
 - 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 the access control device from the drop-down list.
5. Click **Get** to start importing the person information to the client.

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.

7.4.18 Move Persons to Another Organization

You can move the added persons to another organization if you need.

Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

Steps

1. Enter **Person** module.
2. Select an organization in the left panel.

The persons under the organization will be displayed in the right panel.

3. Select the person to move.
4. Click **Change Organization**.
5. Select the organization to move persons to.

6. Click **OK**.

7.4.19 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).

7.4.20 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.

7.4.21 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.

7.5 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*.

7.5.1 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**.

7.5.2 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.

7.6 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.

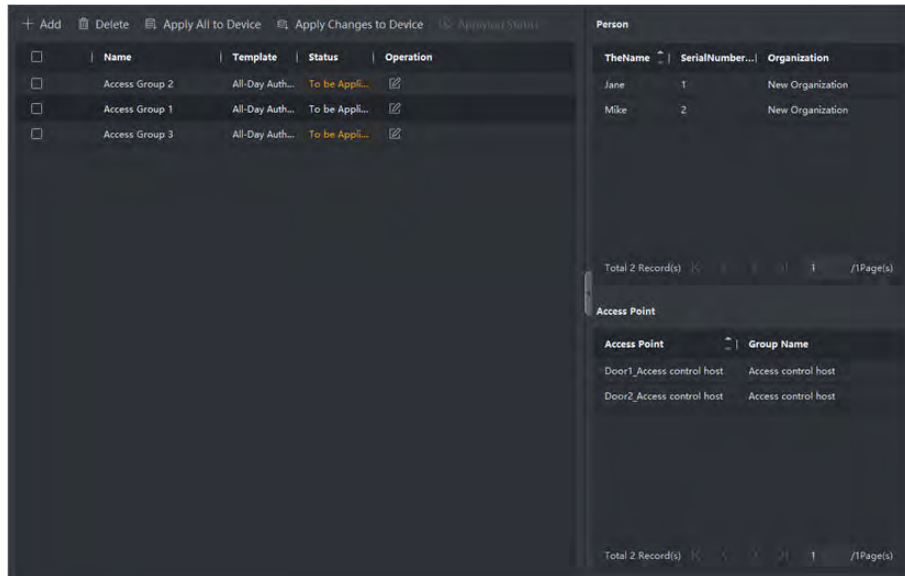


Figure 7-6 Display the Selected Person(s) and Access Point(s)

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**.

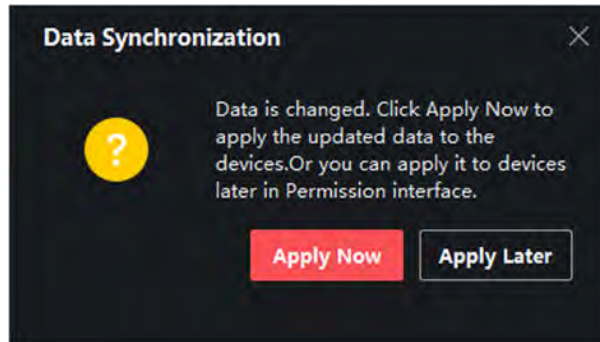


Figure 7-8 Data Synchronization

7.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene.

Note

- For the card related functions(the type of access control card), 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.
-

7.7.1 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.

Steps

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



Note

If you can 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.

RS-485 Communication Redundancy

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

Enable NFC

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

Enable M1 Card

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

Enable EM Card

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

Enable CPU Card

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

Enable ID Card

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

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

Configure Parameters for Door

After adding the access control device, you can configure its access point door parameters.

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

s

The displayed parameters may vary for different access control devices.

Name

Edit the card reader name as desired.

Exit Button Type

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

Open Duration

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

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.

Super Password

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

5. Some of the following parameters are not listed in the Basic Information page, click **Advanced** to edit the parameters.

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.

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.
-

6. Click **OK**.

7. **Optional:** Click **Copy to** , and then select the door(s) to copy the parameters in the page to the selected doors(s).



Note

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

Configure Parameters for Card Reader

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

Steps

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



Note

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

Name

Edit the card reader name as desired.

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.

Alarm of Max. Failed Attempts

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

Card Reader Type/Card Reader Description

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

4. **Optional:** Some of the following parameters are not listed in the Basic Information page, click **Advanced** to edit the parameters.

Enable Card Reader

If enabling the function, user can present card on the card reader. If disabling the function, the card reader for entrance cannot be used.

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.

Buzzing Time

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

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.

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.

Fingerprint Recognition Level

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

5. Click **OK**.

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

Configure Parameters for Alarm Output

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

Before You Start

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

Steps

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

Name

Edit the card reader name as desired.

Alarm Output Active Time

How long the alarm output will last after triggered.

4. Click **OK**.

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

Configure Parameters for Lane Controller

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

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 DIP Settings**, the device will follow the controller's DIP settings to control the barrier. The settings on the software will be invalid.
- If you select **According to Door's Schedule Settings**, the device will follow the schedule configured in the client software to control the barrier. The DIP settings of the controller will be invalid.

Enable Free Passing Authentication

After enabling free passing authentication, the alarm will be triggered when the passing personnel has no legal authentication in free passing mode.

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.

Alarm Voice Prompt Time Duration

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



Note

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

Temperature Unit

Select the temperature unit that displayed in the device status.

Lightboard Brightness

Set the strip light brightness.

Barrier Material

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



Note

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

Lane Length

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



Note

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

Do Not Open Gate When Lane is Not Clear

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

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

4. Click **OK**.

7.7.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed. For example, you can set the door remaining closed in the holiday, and set the door remaining open in the specified period of the work day.

Before You Start

Add the access control devices to the system.

Steps

1. Click **Access Control** → **Advanced Function** → **Remain Open/Closed** to enter the Remain Open/Closed page.
2. Select the door that need to be configured on the left panel.
3. To set the door status during the work day, click the **Week Schedule** and perform the following operations.
 - 1) Click **Remain Open** or **Remain Closed**.
 - 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 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) Click **Save**.

Related Operations

Copy to Whole Week	Select one duration on the time bar, click Copy to Whole Week to copy all the duration settings on this time bar to other week days.
Delete Selected	Select one duration on the time bar, click Delete Selected to delete this duration.
Clear	Click Clear to clear all the duration settings in the week schedule.

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.
- 1) Click **Remain Open** or **Remain Closed**.
 - 2) Click **Add**.
 - 3) Enter the start date and end date.
 - 4) 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.

- 5) 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 .
 - 6) **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).
 - 7) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
 - 8) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.
 - 9) Click **Save**.
5. **Optional:** Click **Copy** to copy the door status settings of this door to other door(s).

7.7.3 Configure Multi-Factor Authentication

You can manage the persons by group and set the authentication for multiple persons of one access control point (door).

Before You Start

Set access group and apply the access group to the access control device. For details, refer to **Set Access Group to Assign Access Authorization to Persons**.

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control** → **Advanced Function** → **Multi-Factor Auth**.
2. Select an access control device in device list on the left panel.
3. Add a person/card group for the access control device.
 - 1) Click **Add** on the right panel.
 - 2) Create a name for the group as desired.
 - 3) Specify the start time and end time of the effective period for the person/card group.
 - 4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

Note

Make sure you have issue card to the person.

Make sure you have set access group and apply the access group to the access control device successfully.

-
- 5) Click **Save**.
 - 6) **Optional**: Select the person/card group(s), and then click **Delete** to delete it(them).
 - 7) **Optional**: Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.
 4. Select an access control point (door) of selected device on the left panel.
 5. Enter the maximum interval when entering password.
 6. Add an authentication group for the selected access control point.
 - 1) Click **Add** on the Authentication Groups panel.
 - 2) Select a configured template as the authentication template from the drop-down list.
-

Note

For setting the template, refer to ***Configure Schedule and Template*** .

-
- 3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.
-

Local Authentication

Authentication by the access control device.

Local Authentication and Remotely Open Door

Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.

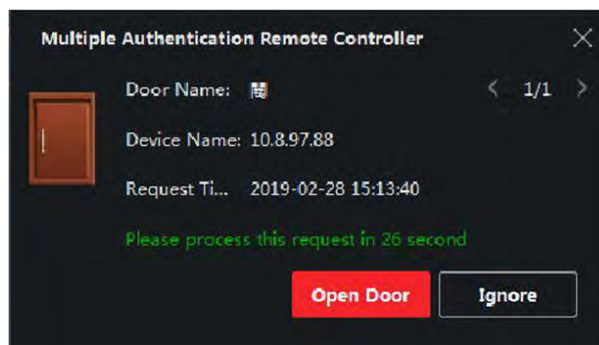


Figure 7-9 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

- 4) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.
- 5) Click the added authentication group in the right list to set authentication times in the Auth Times column.



Note

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
- The maximum value of authentication times is 16.

-
- 6) Click **Save**.



Note

- For each access control point (door), up to four authentication groups can be added.
- For the authentication group of which authentication type is **Local Authentication**, up to 8 person/card groups can be added to the authentication group.
- For the authentication group of which authentication type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 person/card groups can be added to the authentication group.

-
7. Click **Save**.

7.7.4 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start

Wire the third party card readers to the device.

Steps



Note

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom Wiegands can be set.
- For details about the custom Wiegand, see .

-
1. Click **Access Control → Advanced Function → Custom Wiegand** to enter the Custom Wiegand page.
 2. Select a custom Wiegand on the left.
 3. Create a Wiegand name.



Note

Up to 32 characters are allowed in the custom Wiegand name.

4. Click **Select Device** to select the access control device for setting the custom wiegand.
 5. Set the parity mode according to the property of the third party card reader.
-



Note

- Up to 80 bits are allowed in the total length.
 - The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
 - The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
-

6. Set output transformation rule.
 - 1) Click **Set Rule** to open the Set Output Transformation Rules window.

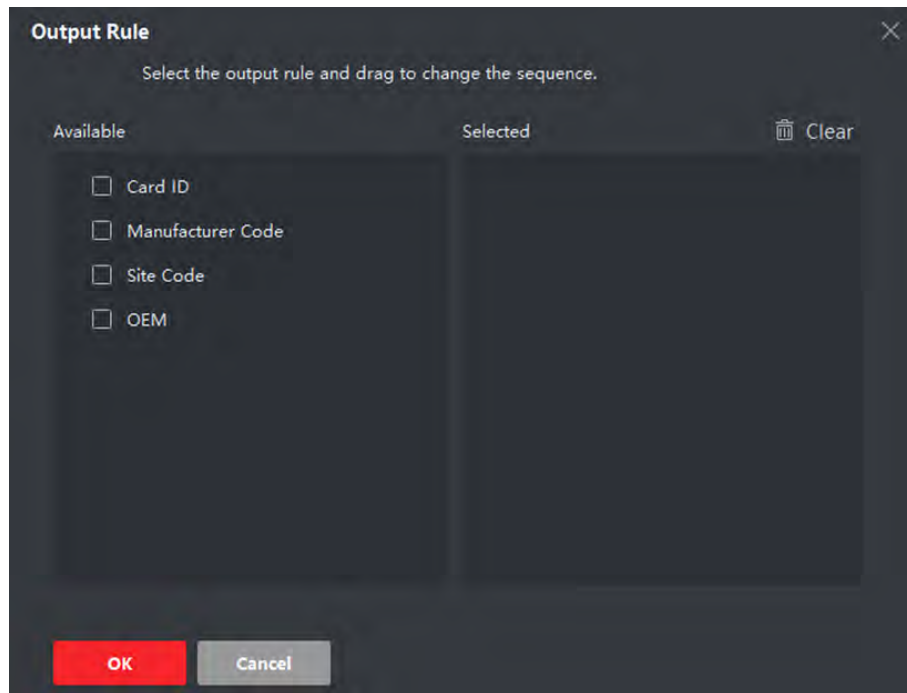


Figure 7-10 Set Output Transformation Rule

- 2) Select rules on the left list.

The selected rules will be added to the right list.
 - 3) **Optional:** Drag the rules to change the rule order.
 - 4) Click **OK**.
 - 5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.
7. Click **Save**.

7.7.5 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Steps

1. Click **Access Control** → **Advanced Function** → **Authentication** to enter the authentication mode configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
 - 1) Click **Configuration**.

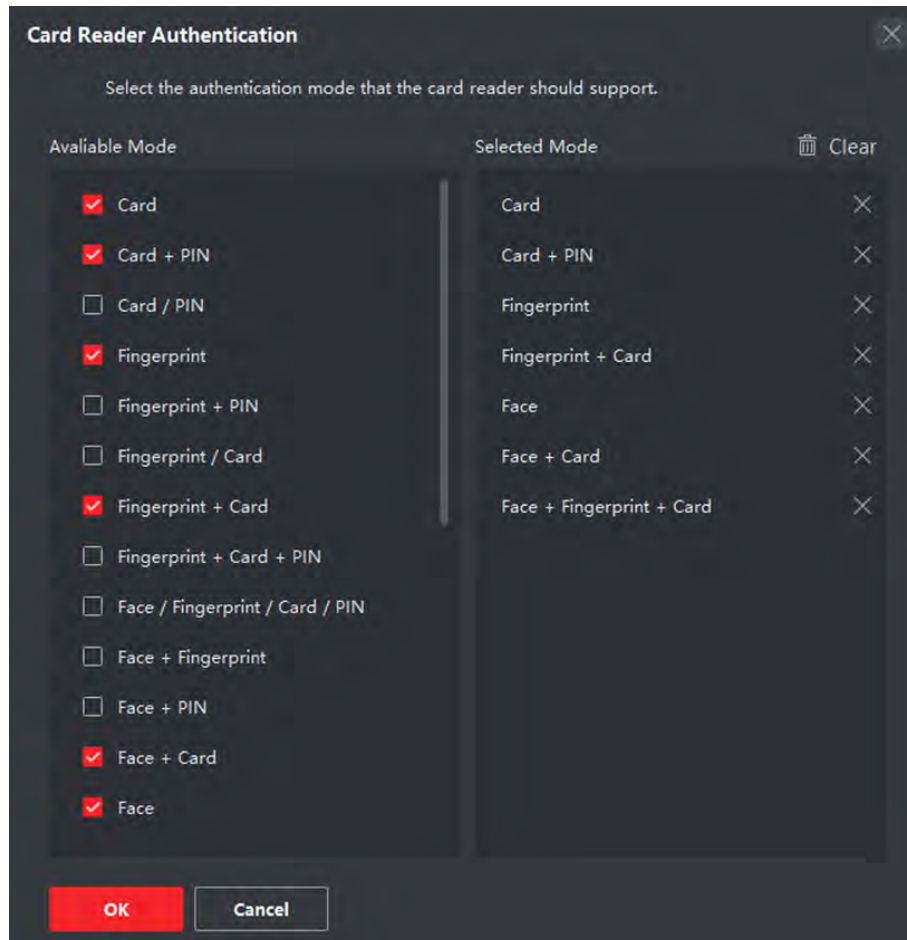


Figure 7-11 Select Card Reader Authentication Mode



Note

PIN refers to the PIN code set to open the door. Refer to ***Configure Access Control Information***.

- 2) Check the modes in the Available Mode list and they will be added to the selected modes list.
- 3) Click **OK**.

After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.
5. Repeat the above step to set other time periods.

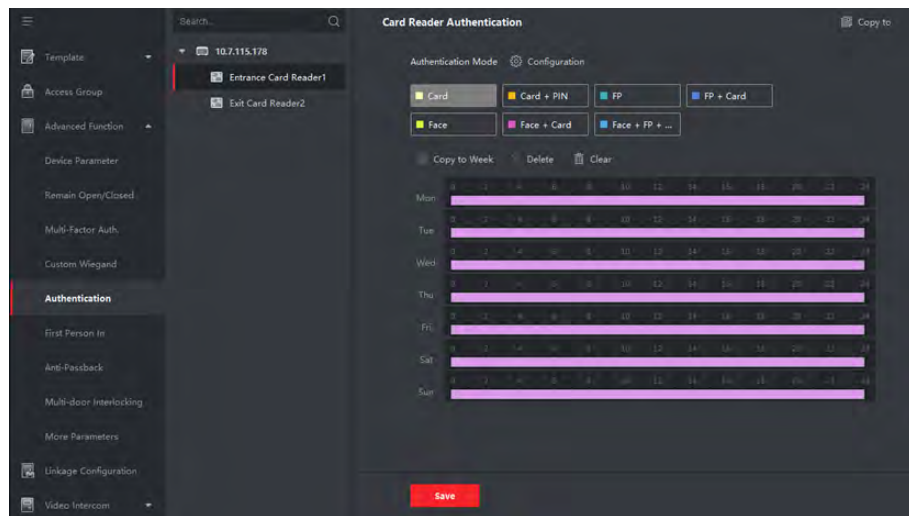


Figure 7-12 Set Authentication Modes for Card Readers

6. **Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. **Optional:** Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

7.7.6 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

- Add access control device to the client, and make sure the device supports the first person in function.
- Add person and assign access authorization to designed person. For details, refer to **Person Management** and **Set Access Group to Assign Access Authorization to Persons**.

Steps

1. Click **Access Control** → **Advanced Function** → **First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.
3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

Enable Remaining Open after First Person

The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the remain open duration.



Note

The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

Disable Remaining Open after First Person

Disable the function of first person in, namely normal authentication.

Authorization by First Person

All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.



Note

You can authenticate by the first person again to disable the first person mode.

4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.
The added first person(s) will list in the First Person List
6. **Optional:** Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

7.7.7 Configure Anti-Passback

You can set to only pass the access control point according to the specified path and only one person could pass the access control point after swiping the card.

Before You Start

Enable the anti-passing back function of the access control device.

Perform this task when you want to configure the anti-passing back for the access control device.

Steps



Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to .

1. Click **Access Control** → **Advanced Function** → **Anti-Passback** to enter the Anti-Passpack Settings page.
2. Select an access control device on the left panel.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.
4. Click  of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
5. Select the afterward card readers for the first card reader.



Note

Up to four afterward card readers can be added as afterward card readers for one card reader.

6. Click **OK** in the dialog to save the selections.
7. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

Example

Set Card Swiping Path

If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

7.7.8 Configure Device Parameters

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

Set RS-485 Parameters

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

Steps



Note

The RS-485 Settings 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 **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 serial number, external device, authentication center, baud rate, data bit, stop bit, parity type, flow control type, communication mode, and working mode in the drop-down list.
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.

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps



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

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



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

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

7.8 Configure Linkage Actions for Access Control

You can configure different linkage actions for the event detected by the access control device. After that, linkage actions will be triggered once the event happens. This mechanism is used for notifying the security personnel the event, or triggering automatic access control in real time.

Two types of linkage actions are supported:

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client making an audible warning..
- **Device Actions:** When the event is detected, it will trigger the actions of a specific device, such as buzzing of a card reader and, opening/closing of a door, ..

7.8.1 Configure Client Actions for Access Event

Even if you are far away from an access point, you can still know what happens and how urgent the event is by configuring linked actions of access event on the client. You will be notified on the client once an event is triggered, so that you can response to the event instantly. You can also configure client actions of access points in a batch at a time.

Steps



The linkage actions here refer to the linkage of the client software's own actions such as audible warning, email linkage, etc.

1. Click **Event Management → Access Control Event**.

The added access control devices will display in the device list.

2. Select a resource (including device, alarm input, door/elevator, and card reader) from the device list.

The event types which the selected resource supports will display.

3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.
4. Set the linkage actions of the event.
 - 1) Select the event(s) and click **Edit Linkage** to set the client actions when the events triggered.

Audible Warning

The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.



Note

For setting the alarm sound, please refer to *Set Alarm Sound* in the user manual of client software..

Send Email

Send an email notification of the alarm information to one or more receivers.

For details about setting email parameters, refer to *Set Email Parameters* in the user manual of client software..

- 2) Click **OK**.
5. Enable the event so that when the event is detected, an event will be sent to the client and the linkage actions will be triggered.
6. **Optional:** Click **Copy to...** to copy the event settings to other access control device, alarm input, door, or card reader.

7.8.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. After that, when an event is triggered, it can trigger the alarm output, buzzer on access controller, and other actions.

Steps



Note

The linkage actions should be supported by the device.

1. Click **Access Control → Linkage Configuration**.
2. Select the access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select **Event Linkage** as the event source.
5. select the event type and detailed event to set the linkage.
6. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Capture

An event-related picture will be captured when the selected event happens.

Recording

An event-related picture will be captured when the selected event happens.



Note

The device should support recording.

Buzzer on Reader

The audible warning of card reader will be triggered.

Alarm Output

The alarm output will be triggered for notification when the selected event happens

Alarm Input

Arm or disarm the alarm input.



Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain close will be triggered.



Note

The target door and the source door cannot be the same one.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click **Save**.

8. **Optional:** After adding the device linkage, you can do one or more of the followings:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click Delete to delete it.

7.8.3 Configure Device Actions for Card Swiping

You enable access control device's linkage actions (such as disarming a zone and triggering audio prompt) for the swiping of a specific card. In this way, you can monitor the card holder's behaviors and whereabouts.

Steps



Note

It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration**.
2. Select the access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select **Card Linkage** as the event source.
5. Enter the card number or select the card from the drop-down list.
6. Select the card reader where the card swipes.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

An event-related picture will be captured when the selected event happens.

Recording

An event-related picture will be captured when the selected event happens.



Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.



Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save.**

When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. Optional: After adding the device linkage, you can do one or more of the followings:

Delete Linkage Settings	Select the configured linkage settings in the device list and click Delete to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

7.9 Door Control

In Monitoring module, you can view the real-time status of the doors managed by the added access control device. You can also control the doors 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 control permission, the user can enter the Monitoring module and control the door. Or the icons used for control will not show. For setting the user permission, refer to ***Person Management*** .

7.9.1 Control Door Status

You can control the status for a single door, including opening door, closing door, remaining the door open, and remaining the door closed.

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* in the user manual of the client software.

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

Open Door

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

Close Door

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

Remain Open

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

Remain Closed

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.

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 *Set File Saving Path* in the user manual of the client software.

Result

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

7.9.2 Check Real-Time Access Records

The access records will display in real time, including card swiping records, face recognitions records, fingerprint comparison records, etc. You can view the person information and view the picture captured during access.

Steps

1. Click **Monitoring** and select a group from the drop-down list on the upper-right corner.

The access records triggered at the doors in the selected group will display in real time. You can view the details of the records, including card No., person name, organization, event time, etc.

2. **Optional:** Check the event type and event status so that these events will show in the list if the events are detected. The events of unchecked type or status will not be displayed in the list.
3. **Optional:** Check **Show Latest Event** and the latest access record will be selected and displayed at the top of the record list.
4. **Optional:** Click the event to view the accessed person details, including person pictures (captured picture and profile), person No., person name, organization, phone, contact address, etc.



Note

You can double click the captured picture to enlarge it to view the details.

- Optional:** Right click on the column name of the access event table to show or hide the column according to actual needs.

7.10 Event Center

The event information (for example, device offline) received by the client displays. In the Event Center, you can check the detailed information of the real-time and historical events, view the event linked video, handle the events, and so on.

Before the client can receive the event information from the device, you need to enable the events of the resource and arm the device first. For details, refer to and ***Enable Receiving Events from Devices***.

7.10.1 Enable Receiving Events from Devices

Before the client can receive the event information from the device, you need to arm the device first.

Steps

- Click → **Tool** → **Device Arming Control** open Device Arming Control page.
All the added devices display on this page.
- In the Operation column, turn on the switch to enable auto-arming, or click **Arm All** to arm all the devices.

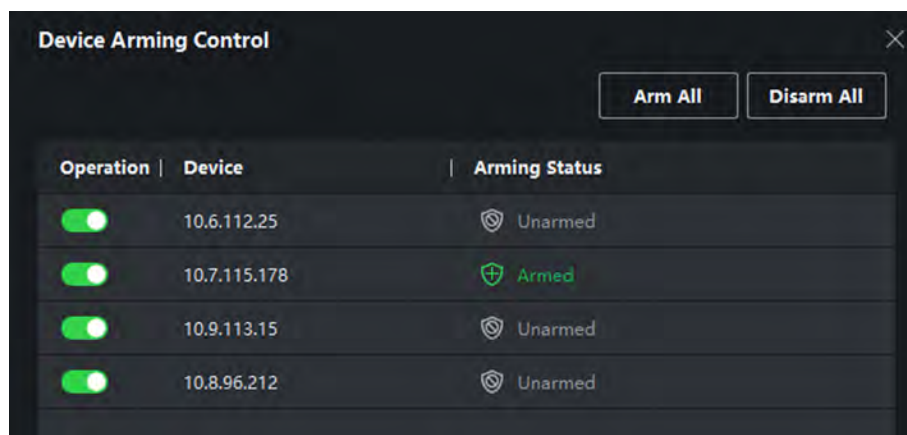


Figure 7-13 Device Arming Control

- View the arming status of each device in the Arming Status column.

Result

The events of armed device(s) are automatically uploaded to the client when the event is triggered.

7.10.2 View Real-Time Events

The real-time event information received by the client of the connected resources are displayed. You can check the real-time event information, including event source, event time, priority, etc.

Before You Start

Enable receiving events from devices before the client can receive event from the device, see *Enable Receiving Events from Devices* for details.

Steps

1. Click **Event Center** → **Real-time Event** to enter the real-time event page and you can view the real-time events received by the client.

Event Time

For encoding device, event time is the client time when it receives the event. For other device types, event time is the time when the event is triggered.

Priority

Priority represents the emergency degree of the event.

2. Filter the events.

Filter by Device Type and (or) Priority

Select device type(s) and (or) priorities to filter events.

Filter by Keywords

Enter the keywords to filter the events.

3. **Optional:** Right-click the table header of the event list to customize the event related items to be displayed in the event list.
4. View the event details.
 - 1) Select an event in the event list.
 - 2) Click **Expand** in the right-lower corner of the page.
 - 3) View the detail description and handing records of the event.
5. **Optional:** Perform the following operations if necessary.

Handle Single Event

Click **Handle** to enter the processing suggestion, and then click **Commit**.



After an event is handled, the **Handle** button will become **Add Remark**. Click **Add Remark** to add more remarks for this handled event.

Handle Events in a Batch

Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **Commit**.

Enable/Disable Alarm Audio

Click **Enable Audio/Disable Audio** to enable/disable the audio of the event.

Select the Latest Event Automatically

Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.

Clear Events

Click **Clear** to clear the all the events in the event list.

Send Email

Select an event and then click **Send Email**, and the information details of this event will be sent by email.



Note

You should configure the email parameters first, see for details.

7.10.3 Search Historical Events

In the Event Search module of the event center page, you can search the historical events via time, device type, and other conditions according to the specified device type, and then process the events.

Before You Start

Enable receiving events from devices before the client can receive event information from the device, see *Enable Receiving Events from Devices* for details.

Steps

1. Click **Event Center** → **Event Search** to enter the event search page.

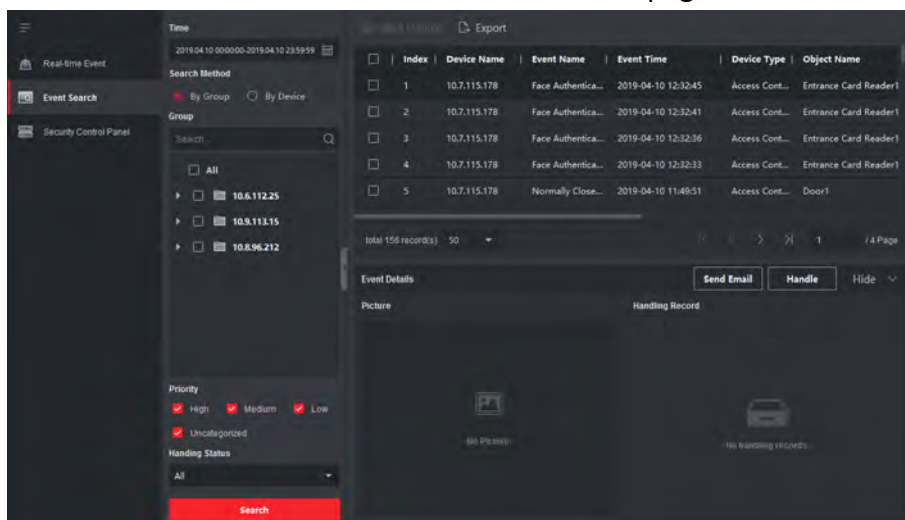


Figure 7-14 Search History Event

2. Set the filter conditions to display the required events only.

Time

The client time when the event starts.

Search by

Group: Search the events occurred on the resources in the selected group.

Device: Search the events occurred on the selected device.

Device Type

The type of device that occurred the event.

All

All the device types, and you can set the following filter conditions: group, priority, and status.

Video Intercom

For the events of video intercom, you need to select searching scope: All Record and Only Unlocking.

- **All Records:** You can filter the events from all the video intercom events, and you need to set the following filter conditions: device, priority, status.
- **Only Unlocking:** You can filter the events from all the video intercom unlocking events, and you need to set the following filter conditions: device, unlocking type.

Access Control

For the events of access control, you can set the following filter conditions: device, priority, status, event type, card reader type, person name, card no., organization.



Note

Click **Show More** to set the event type, card reader type, person name, card no., organization.

Group

The group of the device that occurred the event. You should set the group as condition only when you select the Device Type as **All**.

Device

The device that occurred the event.

Priority

The priority including low, medium, high and uncategorized which indicates the urgent degree of the event.

Status

The handling status of the event.

3. Click **Search** to search the events according the conditions you set.
4. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.

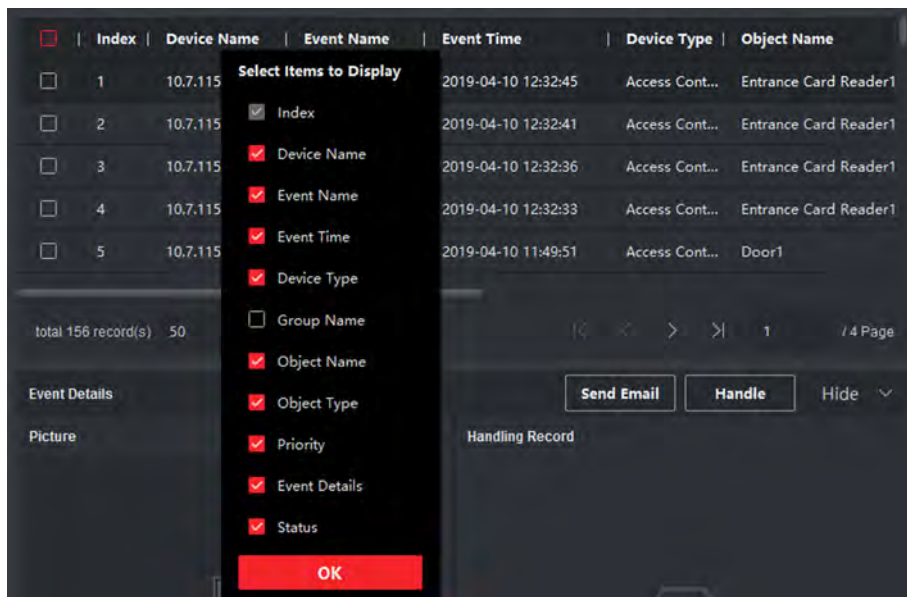


Figure 7-15 Customize Event Related Items to be Displayed

5. Optional: Handle the event(s).

- Handle single event: Select one event that need to be processed, and then click **Handle** in the event information details page, and enter the processing suggestion.
- Handle events in a batch: Select the events which need to be processed, and then click **Handle in Batch**, and enter the processing suggestion.



Note

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

6. Optional: Select an event and then click **Send Email**, and the information details of this event will be sent by email.



Note

You should configure the email parameters first, see *Set Email Parameters* in the user manual of client software for details.

- 7. Optional:** Click **Export** to export the event log or event pictures to the local PC in CSV format. You can set the saving path manually.
- 8.** Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.

7.11 Time and Attendance

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.



In this section, we introduce the configurations before you can getting the attendance reports. The access records recorded after these configurations will be calculated in the statistics.

7.11.1 Configure Attendance Parameters

You can configure the attendance parameters, including the general rule, overtime parameters, attendance check point, holiday, leave type, etc.

Set Weekend

The days of weekends may vary in different countries and regions. The client provides weekends definition function. You can select one or more days as the weekends according to actual requirements, and set different attendance rules for weekends from workdays.

Steps



The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

1. Enter Time & Attendance module.
2. Click **Attendance Settings → General Rule** .
3. Select the day(s) as weekend, such as Saturday and Sunday.
4. Click **Save**.

Configure Overtime Parameters

You can configure the overtime parameters for workday and weekend, including overtime level, work hour rate, attendance status for overtime, etc.

Steps

1. Click **Time & Attendance → Attendance Settings → Overtime** .
2. Set required information.

Overtime Level for Workday

When you work for a certain period after end-work time on workday, you will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3. You can set different work hour rate for three overtime levels, respectively.

Work Hour Rate

Work Hour Rate is used to calculate work hours by multiplying it by overtime. When you work for a certain period after end-work time on workday, you will reach different overtime level. You can set different work hour rates (1-10, can be a decimal) for three overtime levels. For example, your valid overtime is one hour (in overtime level 1), and the work hour rate of overtime level 1 is set as 2, then the work hours in the period will be calculated as 2 hours.

Overtime Rule for Weekend

You can enable overtime rule for weekend and set calculation mode.

3. Click **Save**.

Configure Attendance Check Point

You can set the card reader(s) of the access control device as the attendance check point(s), so that the authentication on the card readers will be recorded for attendance.

Before You Start

- You have added access control device(s). For details, refer to **Add Device**.
- You have enabled T&A Status. For details, refer to **Add General Timetable**.

By default, all card readers of the added access control devices are set as start/end-work check points. If you need to edit check point function of card reader(s), you can perform the following operations.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **Attendance Check Point** to enter the attendance check point settings page.
3. Set **Set All Card Readers as Check Points** switch to off.
4. Check the desired card reader(s) as attendance check point(s) in the list below.
5. Set check point function as **Start/End-Work**, **Start-Work** or **End-Work**.



Note

When selecting **Start-Work** or **End-Work**, the attendance status uploaded from the device will be decided by the check point function you set here.

Start-Work

Attendance status uploaded from the device will all be calculated as Check-in.

End-Work

Attendance status uploaded from the device will all be calculated as Check-out.

Start/End-Work

Attendance status will be calculated as Check in/out according to the actual attendance status on the device.

6. Click Set as Check Point.

The configured attendance check point(s) are displayed on the right list.

7. Optional: After setting attendance check points, and perform the following operations.

Edit Check Point	Check one attendance check point, click Edit to edit its information including name, check point function, etc. Check two or more attendance check points, click Edit to batch edit check point function, enter remark, etc.
Delete Check Point	Check one or more check points, and click Delete to delete it/them.

Configure Holiday

You can add the holiday during which the check-in or check-out will not be recorded.

Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Check **Regular Holiday** as holiday type.
4. Custom a name for the holiday.
5. Set the first day of the holiday.
6. Enter the number of the holiday days.
7. Set the attendance status if the employee works on holiday.
8. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year.
9. Click **OK**.

The added holiday will display in the holiday list and calendar.

If the date is selected as different holidays, it will be recorded as the first-added holiday.

10. Optional: After adding the holiday, perform one of the following operations.

Edit Holiday	Click  to edit the holiday information.
Delete Holiday	Select one or more added holidays, and click Delete to delete the holiday(s) from the holiday list.

Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Click **Add** to open the Add Holiday page.
4. Check **Irregular Holiday** as holiday type.
5. Custom a name for the holiday.
6. Set the start date of the holiday.

Example

If you want to set the forth Thursday in November, 2019 as the Thanksgiving Day holiday, you should select 2019, November, 4th, and Thursday from the four drop-down lists.

7. Enter the number of the holiday days.
8. Set the attendance status if the employee works on holiday.
9. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year
10. Click **OK**.

The added holiday will display in the holiday list and calendar.

If the date is selected as different holidays, it will be recorded as the first-added holiday.

11. **Optional:** After adding the holiday, perform one of the following operations.

- | | |
|-----------------------|--|
| Edit Holiday | Click  to edit the holiday information. |
| Delete Holiday | Select one or more added holidays, and click Delete to delete the holiday(s) from the holiday list. |

Configure Leave Type

You can customize the leave type (major leave type and minor leave type) according to actual needs. You can also edit or delete the leave type.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Leave Type** to enter the Leave Type Settings page.
3. Click **Add** on the left to add a major leave type.
4. **Optional:** Perform one of the following operations for major leave type.

- | | |
|---------------|---|
| Edit | Move the cursor over the major leave type and click  to edit the major leave type. |
| Delete | Select one major leave type and click Delete on the left to delete the major leave type. |

5. Click **Add** on the right to add a minor leave type.

6. **Optional:** Perform one of the following operations for minor leave type.

Edit Move the cursor over the minor leave type and click  to edit the minor leave type.

Delete Select one or multiple major leave types and click **Delete** on the right to delete the selected minor leave type(s).

Synchronize Authentication Record to Third-Party Database

The attendance data recorded on the client can be used by other system for calculation or some other operations. You can enable synchronization function to apply the authentication record from the client to the third-party database automatically.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings → Third-Party Database**.
3. Set **Apply to Database** switch to on to enable synchronization function.
4. Select database Type as **SQLServer** or **MySQL**.



Note

If you select **MySQL**, you should import the configuration file (libmysql.dll) from local PC.

5. Set the other required parameters of the third-party database, including server IP address, port No., database name, user name and password.



Note

The default port No. of the selected database type is displayed automatically. You can enter a number ranging from 1 to 65535 to customize the port No if needed.

6. Set table parameters of database according to the actual configuration.
 - 1) Enter the table name of the third-party database.
 - 2) Set the mapped table fields between the client and the third-party database.
7. Click **Save** to test whether database can be connected and save the settings for the successful connection.
 - The attendance data will be written to the third-party database.
 - During synchronization, if the client disconnects with the third-party database, the client will start reconnection every 30 mins. After being reconnected, the client will synchronize the data recorded during the disconnected time period to the third-party database.

Configure Break Time

You can add break time and set start time, end time, duration, calculation mode and other parameters for the break. The added break time can also be edited or deleted.

Steps

1. Click **Time & Attendance → Timetable → Break Time**.

The added break time is displayed in the list.

2. Click **Break Time Settings** to enter Break Time Settings window.
3. Click **Add**.
4. Enter a name for the break time.
5. Set related parameters for the break time.

Start Time / End Time

Set the time when the break starts and ends.

No Earlier Than / No Later Than

Set the earliest swiping time for starting break and the latest swiping time for ending break.

Break Duration

The duration from start time to end time of the break.

Calculation

Auto Deduct

The break duration will be automatically calculated as 60 minutes.

Must Check

The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.

Return from Break Early for

The actual check-in and check-out time does not exceed the break time, and can be marked as normal work or work overtime.

Return from Break Late for

The actual check-in and check-out time exceeds the break time, and can be marked as late, absent or early leave.

Calculated by

Each Check in/out: Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the break time duration.

First In & Last Out: The first check-in time is recorded as start break time and the last check-out time is recorded as the end break time.

Enable T&A Status

Set **Enable T&A Status** switch to on to calculate the actual break time according to attendance status on the device.



Note

This function should be supported by the device.

Valid Authentication Interval

During the valid authentication interval, person swiping card for several times will only be calculated as once when calculating attendance data.

6. Click **Save** to save the settings.
7. **Optional:** Click **Add** to continue adding break time.

Configure Report Display

You can configure display contents displayed in the attendance report, such as the company name, logo, date format, time format, and mark.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Statistics → Report Display**.
3. Set the display settings for attendance report.

Company Name

Enter a company name to display the name in the report.

Attendance Status Mark

Enter the mark and select the color. The related fields of attendance status in the report will display with the mark and color.

Weekend Mark

Enter the mark and select the color. The weekend fields in the report will display with the mark and color.

4. Click **Save**.

7.11.2 Add General Timetable

On the timetable page, you can add general timetable for employees, which requires the fixed start-work time and end-work time. Also, you can set valid check-in/out time, allowable timetable for being late and leaving early.

Steps

1. Click **Time and Attendance → Timetable** to enter the timetable settings page.
2. Click **Add** to enter add timetable page.

Basic Settings

Name: New Period1 

Timetable Type: General

Calculated by: First In & Last Out

① Enable T&A Status: ☐

① Calculate Break Time into Attended Duration: ☒

Attendance Time

Start-Work Time: 9:00

End-Work Time: 18:00

Valid Check-in Time: 8:30 to 9:30

Valid Check-out Time: 17:30 to 18:30

Calculated as: 540 min

Late Allowable: 10 min

Early Leave Allowable: 10 min

Configuration Result

Save Cancel

Figure 7-16 Add Timetable

3. Create a name for the timetable.

 Note

You can click the color icon beside the name to customize the color for the valid timetable on the time bar in the Configuration Result area.

4. Select the timetable type as general.
5. Select calculation method.

First In & Last Out

The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

Each Check-In/Out

Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid working duration.

You need to set **Valid Authentication Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

6. **Optional:** Set **Enable T&A Status** switch to on to calculate according to attendance status of the device.



Note

This function should be supported by the device.

7. Optional: Enable **Calculate Break Time into Attended Duration**.



Note

When enabled, break time will be calculated into the overall attendance duration. That is, the actual attendance duration equals to the overall attendance duration (includes break time).

8. Set the related attendance time parameters as the following:

Start/End-Work Time

Set the start-work time and end-work-time.

Valid Check-in/out Time

On the time bar, adjust the yellow bar to set the timetable during which the check-in or check-out is valid.

Calculated as

Set the duration calculated as the actual work duration.

Late/Early Leave Allowable

Set the timetable for late or early leave.

9. Set absence related parameters.

Check-In, Late for

You can set the late time duration for the employee who has checked in but is late for work. If the employee exceeds the required time period, his/her attendance data will be marked as absent.

Check-Out, Early Leave for

You can set the early leave time duration for the employee who checks out earlier than the normal leave time, and his/her attendance data will be marked as absent.

No Check-in

If the employee does not check in, his/her attendance data may be marked as absent or late.

No Check-Out

If the employee does not check out, his/her attendance data may be marked as absent or early leave.

10. Click **Save** to add the timetable.

11. Optional: Perform one or more following operations after adding timetable.

Edit Timetable Select a timetable from the list to edit related information.

Delete Timetable Select a timetable from the list and click **Delete** to delete it.

7.11.3 Add Shift

You can add shift for employees including setting shift period (day, week, month) and the effective attendance time. According to the actual requirements, you can adding multiple timetables in one shift for employees, which requires them to check in and check out for each timetable.

Before You Start

Add a timetable first. See **Add General Timetable** for details.

Steps

1. Click **Time & Attendance** → **Shift** to enter shift settings page.
2. Click **Add** to enter Add Shift page.
3. Enter the name for shift.
4. Select the shift period from the drop-down list.
5. Select the added timetable and click on the time bar to apply the timetable.

The screenshot shows the 'Shift' configuration page. The 'Name' field is 'Default Shift'. The 'Period' is '1' and 'Week(s)' is '1'. The 'Timetable 1' section is active, showing a grid for days of the week (Mon. to Sun.) and time slots (00:00 to 24:00). Blue bars indicate the shift period from 09:00 to 18:00 for all days. At the bottom, there are 'Save' and 'Assign' buttons.

Figure 7-17 Add Shift

Note

You can select more than one timetables. The start and end work time and the valid check-in and out time in different time tables can not be overlapped.

The screenshot shows a 'Shift' configuration window. At the top, there's a 'Name' field with 'New Shift 1'. Below it are 'Period' (set to 1) and 'Week(s)' dropdowns. There are two tabs: 'Timetable 1' (active) and 'Timetable 2'. Below the tabs are 'Delete' and 'Clear' buttons. A status bar indicates 'Timetable 1 : 09:00 - 18:00'. The main area is a grid with days of the week (Mon. to Sun.) on the y-axis and time slots (00:00 to 24:00 in 2-hour increments) on the x-axis. Blue bars represent the shift schedule, starting at 09:00 and ending at 18:00 for Monday through Saturday, and from 09:00 to 18:00 on Sunday. At the bottom are 'Save' and 'Assign' buttons.

Figure 7-18 Add Multiple Timetables

6. Click **Save.**

The added shift lists on the left panel of the page. At most 64 shifts can be added.

7. Optional: Assign the shift to organization or person for a quick shift schedule.

1) Click **Assign**.

2) Select **Organization** or **Person** tab and check the desired organization(s) or person(s) box.

The selected organizations or persons will list on the right page.

3) Set the Expire Date for the shift schedule.

4) Set other parameters for the schedule.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

5) Click **Save** to save the quick shift schedule.

7.11.4 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.

You can set department schedule, person schedule, and temporary schedule.

Set Department Schedule

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Before You Start

In Time & Attendance module, the department list is the same with the organization. You should add organization and persons in Person module first. See **Person Management** for details.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Department Schedule** to enter Department Schedule page.
3. Select the department from the organization list on the left.



Note

If **Include Sub Organization** is checked, when selecting the organization, its sub organizations are selected at the same time.

4. Select the shift from the drop-down list.
5. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.



Note

This is only available for shift with only one timetable.

Multiple Shift Schedules

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

Flexible Shift Schedule on Weekend

The person's attendance on the weekend will be recorded as overtime.

8. Click **Save**.

Set Person Schedule

You can assign the shift schedule to one or more persons. You can also view and edit the person schedule details.

Before You Start

Add department and person in Person module. See ***Person Management*** for details.

Steps



Note

The person schedule has the higher priority than department schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule page.
 2. Click **Person Schedule** to enter Person Schedule page.
 3. Select the organization and select the person(s).
 4. Select the shift from the drop-down list.
 5. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.
-



Note

This is only available for shift with only one timetable.

Multiple Shift Schedules

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

Check-in Not Required

Persons in this schedule do not need to check-in when they come to work.

Check-out Not Required

Persons in this schedule do not need to check-out when they end work.

Scheduled on Holidays

On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

Flexible Shift Schedule on Weekend

The person's attendance on the weekend will be recorded as overtime.

8. Click **Save**.

Set Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and edit the temporary schedule details.

Before You Start

Add department and person in Person module. See ***Person Management*** for details.

Steps



Note

The temporary schedule has higher priority than department schedule and person schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Temporary Schedule** to enter Temporary Schedule page.
3. Select the organization and select the person(s).
4. Click one date or click and drag to select multiple dates for the temporary schedule.
5. Select **Workday** or **Non-Workday** from drop-down list.

If **Non-Workday** is selected, you need to set the following parameters.

Calculated as

Select normal or overtime level to mark the attendance status for temporary schedule.

Timetable

Select a timetable from drop-down list.

Multiple Shift Schedule

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

Rule

Set other rule for the schedule, such as **Check-in Not Required**, and **Check-out Not Required**.

6. Click **Save**.

Check Shift Schedule

You can check the shift schedule in calendar or list mode. You can also edit or delete the shift schedule.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Select the organization and corresponding person(s).
3. Click  or  to view the shift schedule in calendar or list mode.

Calendar

In calendar mode, you can view the shift schedule for each day in one month. You can click the temporary schedule for one day to edit or delete it.

List

In list mode, you can view the shift schedule details about one person or organization, such as shift name, type, effective period and so on. Check the shift schedule(s), and click **Delete** to delete the selected shift schedule(s).

7.11.5 Manually Correct Check-in/out Record

If the attendance status is not correct, you can manually correct the check-in or check out record. You can also edit, delete, and export the check-in or check-out record.

Before You Start

- You should add organizations and persons in Person module. For details, refer to **Person Management**.
- The person's attendance status is incorrect.

Steps

1. Click **Time & Attendance → Attendance Handling** to enter attendance handling page.
2. Click **Correct Check-in/out** to enter adding check-in/out correction page.
3. Select one or more persons from left list for correction.
4. Select the correction date.

5. Select the correction type as **Check-in**, **Check-out**, **Break-in**, **Break-out**, etc., and set the correct time.



Note

You can click  to add multiple correction items. At most 8 check-in/out items can be added.

6. **Optional:** Enter the remark information as desired.

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

8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

View Click  or  to view the added attendance handling information in calendar or list mode.

Edit

- In calendar mode, click  → **Edit** to edit the details.
- In list mode, double-click the related field in Date, Handling Type, Time, or Remark column to edit the details.



Note

The edited check-in/out correction will take affect.

Delete

- In calendar mode, select one check-in/out correction, and click **Delete** to delete the selected item.
- In list mode, check one or more check-in/out corrections, and click **Delete** to delete the selected items.



Note

The deleted check-in/out correction will no longer take affect.

Export In list mode, check one or more check-in/out corrections to export the attendance handling details (CSV file) to local PC.

7.11.6 Add Leave and Business Trip

You can add leave and business trip when the employee want to ask for leave or go on a business trip.

Before You Start

You should add organizations and persons in the Person module. For details, refer to **Person Management** .

Steps

1. Click **Time & Attendance** → **Attendance Handling** to enter attendance handling page.
2. Click **Apply for Leave/Business Trip** to enter adding the leave/business trip page.
3. Select person from left list.
4. Set the date(s) for your leave or business trip.

5. Select the major leave type and minor leave type from the drop-down list.



Note

You can set the leave type in Attendance Settings. For details, refer to **Configure Leave Type** .

6. Set the time for leave.
7. **Optional:** Enter the remark information as desired.
8. Click **Save**.
9. **Optional:** After adding the leave and business trip, perform one of the following operations.

View Click  or  to view the added attendance handling information in calendar or list mode.



Note

In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.

Edit

- In calendar mode, click the related label on date to edit the details.
- In list mode, double-click the filed in Date, Handling Type, Time, or Remark column to edit the related information.

Delete Delete the selected items.

Export Export the attendance handling details to local PC.



Note

The exported details are saved in CSV format.

7.11.7 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

Automatically Calculate Attendance Data

You can set a schedule so that the client can automatically calculate attendance data of the previous day at the time you configured every day.

Steps



Note

1. Enter the Time & Attendance module.
2. Click **Attendance Settings** → **General Rule** .

3. In the Auto-Calculate Attendance area, set the time that you want the client to calculate the data.
4. Click **Save**.
The client will calculate the attendance data of the previous day from the time you have configured.

Manually Calculate Attendance Data

You can manually calculate attendance data by setting conditions including attendance time, department, attendance status, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Calculation**.
3. Set the start time and end time to define the attendance data range.
4. Select the department from the drop-down list.
5. **Optional:** Set other conditions, including name and person ID.
6. Check attendance status (supports multi-selection).
7. Click **Calculate**.

Note

Only the attendance data within three months can be calculated.

8. **Optional:** Perform one of the following operations.

Correct Check-in/out

Select one person, click **Correct Check-in/out** to add check-in/out correction.

Select Items to Display

Click  on the upper right corner, or right click the table header of the attendance data list to customize the items to be displayed in the list.

Adjust Items Sequence

Click one item (except Person ID) and move the mouse to customize the sequence of different items.

Generate Report

Click **Report** to generate the attendance report.

Note

The report items will be displayed in the sequence you have set.

Export Report

Click **Export** to export attendance data (CSV file) to local PC.

Note

The report items will be displayed in the sequence you have set.

7.11.8 Attendance Statistics

You can check the original attendance record, generate and export the attendance report based on the calculated attendance data.

Get an Overview of Employees' Attendance Data

You can search and view the employee's attendance data on the client, including attendance time, attendance status, check point, etc.

Before You Start

- You should add organizations and persons in Person module and the persons have swiped cards. For details, refer to **Person Management**.
- Calculate the attendance data.



Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
 - Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to **Manually Calculate Attendance Data**.
-

Steps

1. Enter the Time & Attendance module.
 2. Click **Attendance Statistics → Attendance Record**.
 3. Set the attendance start time and end time that you want to search.
 4. Set other search conditions, including department, name, and person ID.
 5. Select data source as **All, Original Records on Device** or **Manually Handled Records**.
 6. **Optional:** Click **Get Events from Device** to get the attendance data from the device.
-



Note

There are two methods for getting attendance events from the device, including **Online** and **Import File**. For more details about operations, refer to .

7. **Optional:** Click **Reset** to reset all the search conditions and edit the search conditions again.
8. Click **Search**.
9. **Optional:** For the displayed search results, perform one of the following operations.

Edit Attendance Status

Select one incorrect record, double click the field of **Attendance Status** column and select from the drop-down list to edit single piece of attendance status.

Check two or more incorrect records, click **Edit Attendance Status** on the upper left corner and select from the drop-down list to batch edit multiple pieces of attendance status.

- | | |
|------------------------|---|
| Generate Report | Click Report to generate the attendance report. |
| Export Report | Click Export and select saving path to export the attendance report (CVS file) to the local PC. |
| Custom Export | Click Custom Report and set conditions to export attendance records according to actual needs. For details, refer to . |

Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start

Calculate the attendance data.



Note

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to **Calculate Attendance Data** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Report** .
3. Select a report type.
4. Select the department or person to view the attendance report.
5. Set the start time and end time during which the attendance data will be displayed in the report.
6. Click **Report** to generate the statistics report and open it.

Send Report Regularly

The client supports multiple report types and you can pre-define the report content and it can send the report automatically to the email address you configured.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Regularly Send Report** .
3. Click **Add** to enter the add custom report page.
4. Set the report content.

Report Name

Enter a name for the report.

Report Type

Select one report type and this report will be generated.

Report Time

The time to be selected may vary for different report type.

Person

Select the added person(s) whose attendance records will be generated for the report.



Note

You can view the selected person(s) in the right side of the Person area.

5. Set the schedule to send the report to the email address(es) automatically.
-



Note

The **Auto-Send Email** function is enabled by default.

- 1) Set the Effective Period during which the client will send the report on the selected sending date(s).
- 2) Select the Sending Date(s) on which the client will send the report.
- 3) Set the Sending Time at which the client will send the report.

Example

If you set the effective period as **2018/3/10 to 2018/4/10**, select **Friday** as the sending date, and set the sending time as **20:00:00**, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.



Note

Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to **Calculate Attendance Data**.

- 4) Enter the receiver email address(es).
-



Note

Up to 5 email addresses can be added. You can click **+** to add a new email address.

- 5) **Optional:** Click **Preview** to view the email details.

6. Click **OK**.

7. **Optional:** After adding the custom report, you can do one or more of the followings:

- | | |
|------------------------|---|
| Edit Report | Select one added report and click Edit to edit its settings. |
| Delete Report | Select one added report and click Delete to delete it. |
| Generate Report | Select one added report and click Report to generate the report instantly and you can view the report details. |

7.12 Remote Configuration via Client Software

Configure device parameters remotely.

7.12.1 Check Device Information

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click  to enter the remote configuration page.
3. Click **System → Device Information** and view the device basic information and the device version information.

7.12.2 Edit Device Name

Click **Maintenance and Management → Device Management → Device** to enter the device list.

Click  to enter the remote configuration page.

Click **System → General** to configure the device name and overwrite record files parameter.

Click **Save**.

7.12.3 Edit Time

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click  to enter the remote configuration page.
3. Click **System → Time** to configure the time zone.
4. **Optional:** Check **Enable NTP** and set the NTP server address, the NTP port, and the synchronization interval.
5. **Optional:** Check **Enable DST** and set the DST start time, end time and the bias.
6. Click **Save**.

7.12.4 Set System Maintenance

You can reboot the device remotely, restore the device to default settings, etc.

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click  to enter the remote configuration page.
3. Click **System → System Maintenance**.
4. Maintain the device.

Reboot

The device starts rebooting.

Restore Default Settings

Restore the device settings to the default ones, excluding the IP address.

Restore All

Restore the device parameters to the default ones. The device should be activated after restoring.

5. Remotely upgrade the device.

- 1) In the Remote Upgrade part, select an upgrade type.



Note

- You need to set the device ID before upgrading if you select Controller Upgrade File as the remote upgrade type.
- Only the card reader that connected via RS-485 protocol supports upgrading.

- 2) Click ... to select an upgrade file.
- 3) Click **Upgrade** to start upgrading.



Note

Do not power off during the upgrading.

7.12.5 Manage Network User

Steps

1. Click **Maintenance and Management** → **Device Management** → **Device** to enter the device list.
2. Click  to enter the remote configuration page.
3. Click **System** → **User** → **Network User** .
4. Click **Add** to add the user.
5. **Optional:** Select a user in the user list and click **Edit** to edit the user.
You are able to edit the user password, the IP address, the MAC address and the user permission.
6. Click **OK**.

7.12.6 Manage Keyfob User

Steps

1. Click **Maintenance and Management** → **Device Management** → **Device** to enter the device list.
2. Click  to enter the remote configuration page.
3. Click **System** → **User** → **Keyfob User** .
4. Click **Add** to add the user.
5. Check **Enable** in the pop-up window and set the keyfob's serial No.
6. **Optional:** Enable the Remain Open Status of the turnstile.



Note

If enabling this function, after the keyfob is matching completed, you can set the barrier as remaining open by using the keyfob.

7. Set the door open direction
 8. Click **OK**.
-



Note

Up to 32 keyfob users can be added.

7.12.7 Set Security

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click  to enter the remote configuration page.
3. Click **System → Security**.
4. Select the security level in the drop-down list.
5. You can select **Compatible Mode** or **Security Mode**.

Compatible Mode

The user information verification is compatible with the old client software version when logging in.

Security Mode

High security level during the user information verification when logging in.

6. Click **Save**.

7.12.8 Configure Screen Parameters

The device can connect to a text screen. You can set the display parameters on this page.

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
 2. Click  to enter the remote configuration page.
 3. Click **System → Screen Configuration**.
 4. Set the screen parameters.
-



Note

For better performance, it is suggested to use the default parameters.

Screen Position

Select the screen's position on the device. If select **Exit** from the drop-down list, the screen will be installed at the exit position of the device.

Screen Model

Select the screen model from the drop-down list.

Font Size

Select the text font size in the screen.

Screen Orientation

Select the text orientation on the screen.

Line Space

Set the space between two lines.

Column Spacing

Set the space between two columns.

Initial Position

Set the first character's position displayed on the screen.

5. Click **Save**.

7.12.9 Configure Screen Parameters

You can set the people counting's parameters and after the configuration.

Steps

1. Click **Maintenance and Management** → **Device Management** → **Device** to enter the device list.
2. Click  to enter the remote configuration page.
3. Click **System** → **People Counting**.
4. Set the people counting parameters.

Clear Counted Number

Click **Clear** and the counted people number will be restored to zero.

Device People Counting

Click **Enable** or **Disable** to enable or disable the people counting function.

Offline People Counting

Click **Enable** or **Disable** to enable or disable function of the offline people counting on the client.

If enabling the function and if the device is offline, the device will continue counting the people and the number will be stored in the device. When the device is online, the client will read the updated number from the device automatically.

People Counting Type

You can select from **Invalid**, **By Detection**, and **By Authentication Number**.

Invalid

The device will not count people. If the device people counting function is enabled, the people counting function is still disabled.

By Detection

The device will count the people who passing through the device depending on the detection result.

By Authentication Number

The device will count the people who authenticating on the device.

The failed authentication will also count as once.

5. Click **Save**.

7.12.10 Configure Advanced Network

Click **Maintenance and Management → Device Management → Device** to enter the device list.

Click  to enter the remote configuration page.

Click **Network → Advanced Settings** and you can configure the DNS IP address 1 and the DNS IP address.

Click **Save** to save the settings.

7.12.11 Configure Audio File

You can relate the audio file to the corresponding playing scene. You can also export the audio file from the system and import the audio file from the local.

Steps

1. Click **Maintenance and Management → Device Management → Device** to enter the device list.
2. Click  to enter the remote configuration page.
3. Click **Other → Audio File**.



Note

By default, the system contains the audio content. For details about the index related audio content, see ***Table of Audio Index Related Content***.

4. Select the index (the playing content) corresponded play scene.
5. **Optional:** Input the descriptions of the play scene.
6. Click **Save Parameters** to save the relationship between the index (the playing content) and the play scene.
7. **Optional:** Click **Export** to export the default audio file to the local computer.
8. **Optional:** Click **...** and select audio file from the local computer. Click **Import** to import the file to the device.



Note

- The imported audio file should be in MEM format.
 - For details about converting other format of the audio file to MEM format, see the audio conversion manual.
 - If you use the third part software to create or edit an audio file, the volume of the audio file should be no less than 0×68 . If the volume is less than the value, it will exceed the loudspeaker's power consumption, so that damage the loudspeaker.
-

7.12.12 View Relay Status

Click **Maintenance and Management** → **Device Management** → **Device** to enter the device list.

Click  to enter the remote configuration page.

Click **Status** → **Relay** and you can view the relay status.

Appendix A. DIP Switch Description

The DIP switch is on the main lane control board. The left side to the right side is from the low bit to the high bit.



When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off. If you set the DIP switch like the figure displayed below, its binary value is 00001100, and its decimal value is 12.



Appendix B. 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 C. Table of Audio Index Related Content

Index	Content
1	Authenticated.
2	Card No. does not exist.
3	Card No. and fingerprint mismatch.
4	Climbing over the barrier.
5	Reverse passing.
6	Passing timeout.
7	Intrusion.
8	Force accessing.
9	Tailgating.
10	No permissions.
11	Authentication time out.
12	Authentication failed.
13	Expired card.
14	Stay out of time.

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	Upper IR Board 5 Offline	29
The First IR Beam on Upper IR Board Triggered	01	Upper IR Board 6 Offline	30
The Second IR Beam on Upper IR Board Triggered	02	Upper IR Board 7 Offline	31
The Third IR Beam on Upper IR Board Triggered	03	Upper IR Board 8 Offline	32
The Fourth IR Beam on Upper IR Board Triggered	04	Upper IR Board 9 Offline	33
The Fifth IR Beam on Upper IR Board Triggered	05	Upper IR Board 10 Offline	34
The Sixth IR Beam on Upper IR Board Triggered	06	Upper IR Board 11 Offline	35
The Seventh IR Beam on Upper IR Board Triggered	07	Upper IR Board 12 Offline	36
The Eighth IR Beam on Upper IR Board Triggered	08	Lower IR Board 1 Offline	37
The Ninth IR Beam on Upper IR Board Triggered	09	Lower IR Board 2 Offline	38
The Tenth IR Beam on Upper IR Board Triggered	10	Lower IR Board 3 Offline	39
The Eleventh IR Beam on Upper IR Board Triggered	11	Lower IR Board 4 Offline	40
The Twelfth IR Beam on Upper IR Board Triggered	12	Lower IR Board 5 Offline	41
The First IR Beam on Lower IR Board Triggered	13	Lower IR Board 6 Offline	42
The Second IR Beam on Lower IR Board Triggered	14	Lower IR Board 7 Offline	43

Error Reason	Code	Error Reason	Code
The Third IR Beam on Lower IR Board Triggered	15	Lower IR Board 8 Offline	44
The Fourth IR Beam on Lower IR Board Triggered	16	Lower IR Board 9 Offline	45
The Fifth IR Beam on Lower IR Board Triggered	17	Lower IR Board 10 Offline	46
The Sixth IR Beam on Lower IR Board Triggered	18	Lower IR Board 11 Offline	47
The Seventh IR Beam on Lower IR Board Triggered	19	Lower IR Board 12 Offline	48
The Eighth IR Beam on Lower IR Board Triggered	20	Light Board Offline (Entrance)	49
The Ninth IR Beam on Lower IR Board Triggered	21	Light Board Offline (Exit)	50
The Tenth IR Beam on Lower IR Board Triggered	22	IR Adapter Offline (Up)	51
The Eleventh IR Beam on Lower IR Board Triggered	23	IR Adapter Offline (Low)	52
The Twelfth IR Beam on Lower IR Board Triggered	24	CAN Bus Exception	53
Upper IR Board 1 Offline	25	Not Studying	54
Upper IR Board 2 Offline	26	Obstruction	55
Upper IR Board 3 Offline	27	Exceeding Studying Range	56
Upper IR Board 4 Offline	28	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

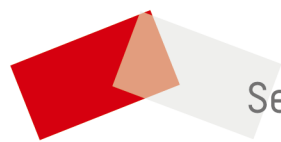
Device Command

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