



DS-K3G200(L)X Series Tripod Turnstile



See Far, Go Further

Legal Information

About this Document

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

Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL

OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

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

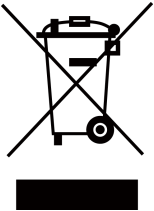
© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Regulatory Information

EU Conformity Statement



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



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



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

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:

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
If the top caps should be open and the device should be powered on for maintenance, make sure:
 - ⚡ Power off the fan to prevent the operator from getting injured accidentally.
 - ⚡ Do not touch bare high-voltage components.
 - ⚡ 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:

- 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
Tripod Turnstile	DS-K3G200(L)X

Contents

1 Overview	1
1.1 Introduction	1
1.2 Main Features	1
2 System Wiring	1
3 Installation	2
3.1 Disassemble Pedestals	2
3.2 Install Pedestals	2
4 General Wiring	3
4.1 Components Introduction	3
4.2 Wiring Electric Supply	4
4.3 Wiring	5
4.4 Terminal Description	5
4.4.1 Lane Control Board Terminal Description	5
4.4.2 Access Control Board Terminal Description (Optional)	5
4.4.3 Main Optional Board Terminal Description (Optional)	6
4.4.4 Sub Optional Board Terminal Description (Optional)	7
4.4.5 Card Reader Board Terminal Description	7
4.4.6 RS-485 Wiring	8
4.4.7 RS-232 Wiring	8
4.4.8 Alarm Input Wiring	8
4.4.9 Exit Button Wiring	9
4.5 Device Settings via Button	9
4.5.1 Configuration via Button	9
4.5.2 Initialize Device	11
5 Activation	11
5.1 Activate via SADP	11

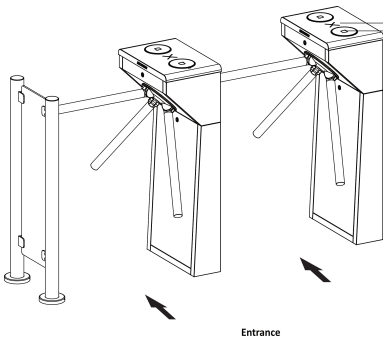
5.2 Activate Device via iVMS-4200 Client Software	12
5.3 Activate via Web Browser	13
6 Operation via Web Browser	13
6.1 Login	13
6.2 Forget Password	14
6.3 Overview	14
6.4 Person Management	15
6.5 Search Event	16
6.6 Configuration	17
6.6.1 View Device Information	17
6.6.2 Set Time	17
6.6.3 Set DST	17
6.6.4 Change Administrator's Password	18
6.6.5 Online Users	18
6.6.6 View Device Arming/Disarming Information	18
6.6.7 Network Settings	19
6.6.8 Event Linkage	20
6.6.9 Access Control Settings	22
6.6.10 Turnstile	25
6.6.11 Card Settings	27
6.6.12 Set Privacy Parameters	27
6.6.13 Upgrade and Maintenance	28
6.6.14 Device Debugging	28
6.6.15 Component Status	29
6.6.16 Log Query	29
6.6.17 Certificate Management	29
7 Client Software Configuration	30
7.1 Configuration Flow of Client Software	30

7.2 Device Management	31
7.2.1 Add Device	31
7.2.2 Reset Device Password	33
7.2.3 Manage Added Devices	34
7.3 Group Management	35
7.3.1 Add Group	35
7.3.2 Import Resources to Group	35
7.4 Person Management	36
7.4.1 Add Organization	36
7.4.2 Import and Export Person Identify Information	36
7.4.3 Get Person Information from Access Control Device	38
7.4.4 Issue Cards to Persons in Batch	39
7.4.5 Report Card Loss	40
7.4.6 Set Card Issuing Parameters	40
7.5 Configure Schedule and Template	41
7.5.1 Add Holiday	41
7.5.2 Add Template	42
7.6 Set Access Group to Assign Access Authorization to Persons	43
7.7 Configure Advanced Functions	45
7.7.1 Configure Device Parameters	45
7.7.2 Configure Device Parameters	49
7.8 Door Control	50
7.8.1 Control Door Status	50
7.8.2 Check Real-Time Access Records	51
A. DIP Switch	53
A.1 DIP Switch Description	54
B. Button Configuration Description	55
C. Event and Alarm Type	57

D. Error Code Description 58

1 Overview

1.1 Introduction



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

1.2 Main Features

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

2 System Wiring

The preparation before installation and general wiring.

Steps

1. Draw a line based on the outer edge of the left or right pedestal or column.
2. Draw other parallel lines for installing the other pedestals.



Note

The distance between the nearest two line is 836 mm.

3. Slot on the installation surface and dig installation holes according to the hole position. Put 4 expansion bolts for each pedestal.
4. Bury cables. Each lane buries 1 high voltage cable. For details, see the system wiring diagram below.

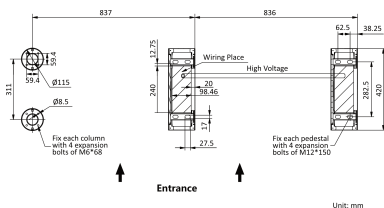


Figure 2-1 System Wiring Diagram



Note

- High voltage: AC power input
- The suggested inner diameter of the high voltage conduit is larger than 30 mm.
- The external AC power cord should be double-insulated.
- Before digging holes, evaluate the thickness of the installation surface to avoid puncturing.
- The network cable must be CAT5e or the network cable has better performance.
- If the usage scenarios of the equipment include kindergarten and primary school, it is recommended to design dedicated turnstiles for young children and lower grade students to reduce the safety risks.
If there is a scene where children pass through alone, it is recommended to use a children's bracket for face recognition terminal installation. When installing, it is recommended to choose a low angle installation or an external vertical children's bracket. The vertical children's bracket is recommended to be installed about 0.5 meters in front of the turnstile.

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.

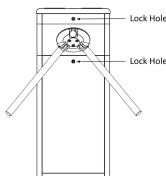


Figure 3-1 Lock Holes

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.
- To prevent stainless steel from rusting due to dirt during construction, it is recommended that the protective film be removed after the installation is completed. There may be residual adhesive at the film cutting position. It is recommended to use WD-40 protective liquid to wipe after tearing the film.
- The dimension is as follows.

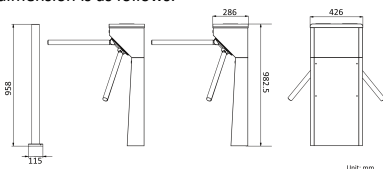


Figure 3-2 Dimension

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Seal the bottom of the turnstile to avoid water from entering.
3. 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.

4. 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.

5. Install the barrier arm.

4 General Wiring



Note

- After maintenance, you should close the water-proof cover over the high voltage module.
- When you should maintain or disassemble the high voltage modules, you should remove the entire high voltage modules and maintain it outside the turnstile. You should unplug the cables that connected to the peripherals before maintenance to avoid destroy of the device.

4.1 Components Introduction

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

 Note

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

The picture displayed below describes the serial port on the entrance and exit direction.

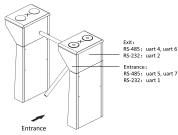


Figure 4-1 Serial Port

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

 Note

The diagram is for reference only.

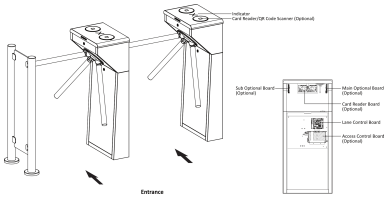
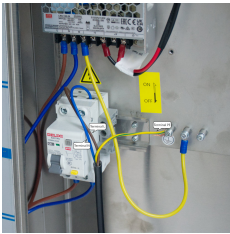


Figure 4-2 Components Diagram 1

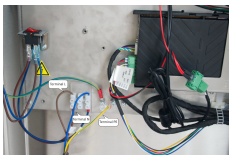
4.2 Wiring Electric Supply

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

For product with power switch, the wiring diagram is as follows:



For product with power adapter, the wiring diagram is as follows:



Warning

Terminal PE should connect to a ground wire to avoid hazard when people touching the device.



Note

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

4.3 Wiring

Scan the QR code to view the wiring guide video.

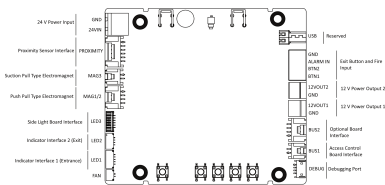


4.4 Terminal Description

4.4.1 Lane Control Board Terminal Description

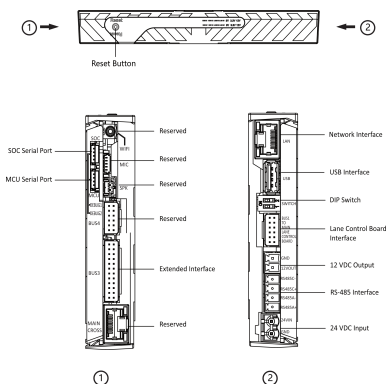
The lane control board contains power input interface, exit button and fire input interface, access control board interface, debugging port, indicator interface, etc.

The picture displayed below is the lane control board diagram.



4.4.2 Access Control Board Terminal Description (Optional)

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



Note

- RS-485A corresponds to UART 5 on web and is for QR code scanner connection at entrance by default; RS-485C corresponds to UART 7 on web and is for card reader connection at entrance by default.
- The SOC and MCU serial port are for maintenance and debugging use only.
- Press the Reset button for 5 s and the device will start to restore to factory settings.
- The DIP switch is for study mode setting. For detailed information about the DIP switch, see *DIP Switch Description*.

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

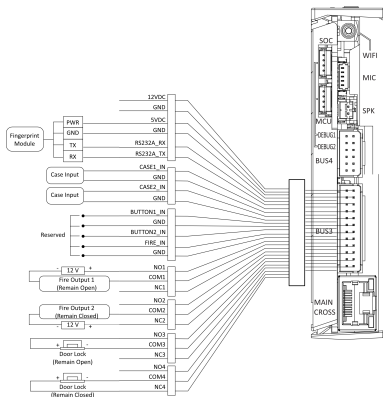


Figure 4-3 Wring Diagram of BUS3 Interface



Note

RS-232A corresponds to UART 1 on web.

4.4.3 Main Optional Board Terminal Description (Optional)

The main optional board contains the sub-1G antenna interface, loudspeaker interface, debugging port, Wiegand/exit button interface, 5 VDC output and communication interface.

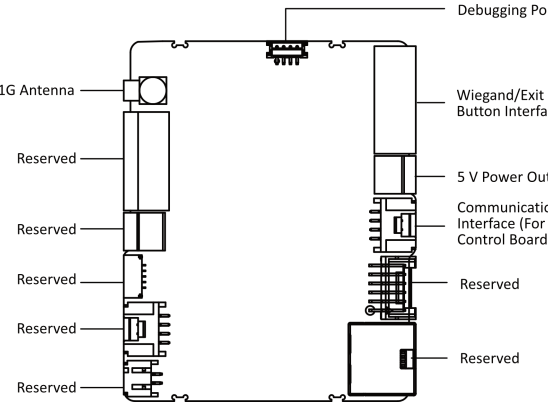


Figure 4-4 Main Optional Board Terminal

4.4.4 Sub Optional Board Terminal Description (Optional)

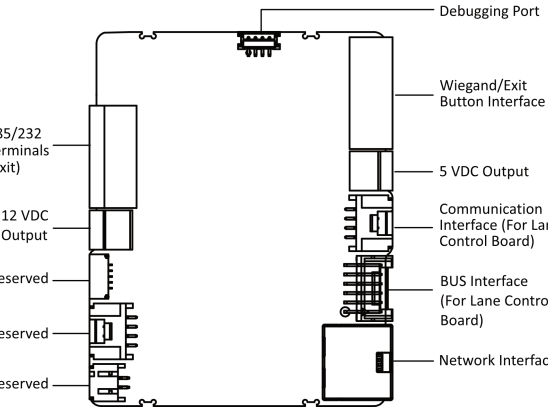


Figure 4-5 Sub Optional Board Terminal

Note

- RS-485B corresponds to port 6 on web and is for QR code scanner connection by default.
- RS-485D corresponds to port 4 on web and is for card reader connection by default.
- RS-232B corresponds to port 2 on web and is for fingerprint reader connection by default.

4.4.5 Card Reader Board Terminal Description

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

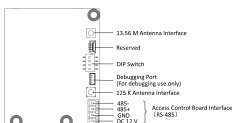


Figure 4-6 Card Reader Board

4.4.6 RS-485 Wiring

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

Note

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

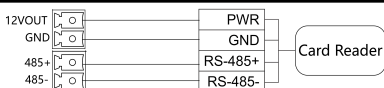


Figure 4-7 Wiring RS-485

4.4.7 RS-232 Wiring

Note

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

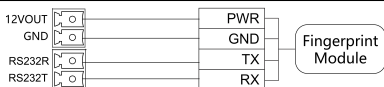


Figure 4-8 RS-232 Wiring

4.4.8 Alarm Input Wiring

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

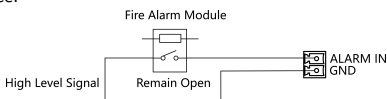


Figure 4-9 Remaining Open

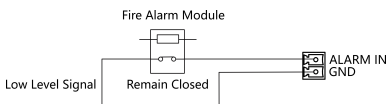


Figure 4-10 Remaining Closed

4.4.9 Exit Button Wiring

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

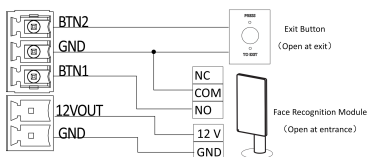


Figure 4-11 Exit Button Wiring



Note

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

4.5 Device Settings via Button

You can configure the device via button on the lane control board.

4.5.1 Configuration via Button

Button Description

The buttons are on the lane control board.

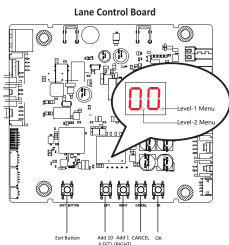


Figure 4-12 Button

Exit Button

Single press to open the gate from the entrance position.

Double press to open the gate from the exit position.

Parameter Configuration Button

LEFT: Press to add ten to configuration data

RIGHT: Press to add one configuration data

CANCEL: Return to the level-1 menu, or exit the configuration from the level-1 menu

OK: Confirm the data, or enter configuration mode, or enter the submenu



Note

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

Button Configuration Procedure

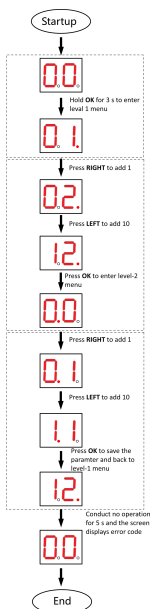


Figure 4-13 Procedure

Steps:

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

4.5.2 Initialize Device

Steps

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

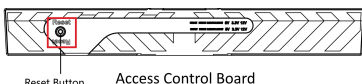


Figure 4-14 Initialization Button Position

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



Caution

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



Note

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

5 Activation

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

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

The default values of the device are as follows:

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

5.1 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

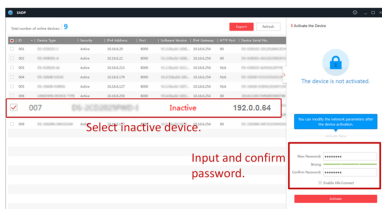
STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password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



Note

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

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



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

5. Modify IP address of the device.

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

5.2 Activate Device via iVMS-4200 Client Software

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

Steps



Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click  on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.
The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.



Caution

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

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



Note

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

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

5.3 Activate via Web Browser

You can activate the device via the web browser.

Steps

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



Note

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

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



Caution

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



Note

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

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

6 Operation via Web Browser

6.1 Login

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



Note

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

Login via Web Browser

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

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

Login via Remote Configuration of Client Software

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

6.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.

You will receive a verification code within 5 minutes in your reserved email.

Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

6.3 Overview

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

Function Descriptions:

Device Component Status

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

Remote Control



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

Real-Time Event

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

Person Information

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

Network Status

You can view the network connection status.

Basic Information

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

Device Capacity

You can view the person, card and event capacity.

6.4 Person Management

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

Basic Information

*Employee ID

Name

Gender

☒ Male

☐ Female

☐ Unknown

Long-Term Effective User

☐

Validity Period

2023-04-12 00:00:00

-

2023-04-11 23:59:59

Certificate Configuration

Card

Up to 50 cards can be supported.

+ Add Card

Authentication Settings

Authentication Type

☒ Same as Device

☐ Custom

Save

Cancel

Figure 6-1 Person Management

Add Basic Information

Click **Person Management** → **Add** to enter the Add Person page.

Add the person's basic information, including the employee ID, the person's name, etc.

Click **Save** to save the settings.

Set Permission Time

Click **Person Management** → **Add** to enter the Add Person page.

Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.

Click **Save** to save the settings.

Authentication Settings

Click **Person Management** → **Add** to enter the Add Person page.

Set the authentication type.

Click **Save** to save the settings.

Add Card

Click **Person Management** → **Add** to enter the Add Person page.

Click **Add Card**, enter the **Card No.** and select the **Property**, and click **Save** to add the card.
Click **Save** to save the settings.

Import/Export Person Data

Export Person Data

You can export added person data for back-up or importing to other devices.
Click **Export Person Data**, set an encryption password and confirm it. Click **OK**.

 Note

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

Importing Person Data

Click **Importing Person Data** and select the file. Click **Import**.
Enter the encryption password to import and synchronize the person data to devices.

 Note

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

6.5 Search Event

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

Event Types

Access Control Event

Employee ID

Name

Card No.

Start Time

2022-08-31 00:00:00

End Time

2022-08-31 23:59:59

Search

Figure 6-2 Search Event

Select the event type and enter the search conditions, including the employee ID, name, card No., start time, and end time, and click **Search**.
The results will be displayed on the right panel.

6.6 Configuration

6.6.1 View Device Information

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

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

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

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

6.6.2 Set Time

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

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

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

Time Zone:

Time Synchronization mode: ☒ NTP ☐ Manual

*Server IP Address:

*NTP Port:

*Interval: minutes

DST

DST: ☒

Start Time:

End Time:

DST Bias: ☒ 30minutestd ☐ 45minutestd ☐ 30minutestd ☐ 120minutestd

Figure 6-3 Time Settings

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

Time Zone

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

Time Sync.

Manual

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

Server IP Address/NTP Port/Interval

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

6.6.3 Set DST

Steps

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

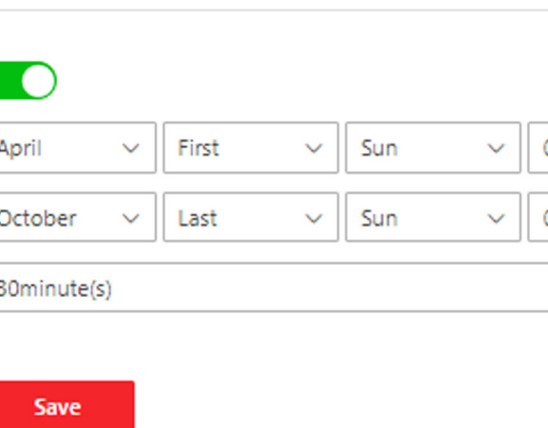


Figure 6-4 DST Page

2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

6.6.4 Change Administrator's Password

Steps

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



Caution

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

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

6.6.5 Online Users

The information of users logging into the device is shown.

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

6.6.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

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

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

6.6.7 Network Settings

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .

Network Type: Self-Adaptive

DHCP: ☐

IPv4 Address:

Subnet Mask:

Default Gateway:

Preferred DNS Address:

Alternate DNS Address:

MTU: 1500

Preferred DNS Server:

Alternate DNS Server:

Save

Figure 6-5 TCP/IP Settings Page

You can view the mac address and MTU.

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

NIC Type

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

DHCP

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

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

DNS Server

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

Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening parameters.

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

The screenshot shows the 'Network Service' configuration page. It has three main sections: 'HTTP', 'HTTPS', and 'HTTP Listening'. In the 'HTTP' section, 'Enable' is checked (green toggle) with a note 'Enabling HTTP may cause security problems', and 'HTTP Port' is set to '80'. In the 'HTTPS' section, 'Enable' is checked (green toggle) and 'HTTPS Port' is set to '443'. In the 'HTTP Listening' section, 'Event Alarm IP/Domain Name' is '8.8.8.8', 'URL' is '/', 'Port' is '80', and 'Protocol' is 'HTTP' (selected with a radio button). There is a 'Reset' button for 'HTTP Listening Parameter Port' and a red 'Save' button at the bottom.

Figure 6-6 Network Service

HTTP

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

HTTPS

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

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.



Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

6.6.8 Event Linkage

Set linked actions for events.

Steps

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

Event Source

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

* Card No.

Card Reader ☒ All ☐ Entrance ☐ Exit

Linkage Action

Buzzer Linkage ☐

Door Linkage ☒

☒ Entrance

☐ Exit

Linked Alarm Output ☒

☒ Alarm Output1

☒ Alarm Output2

Save

Figure 6-7 Event Linkage

2. Set event source.

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

3. Set linked action.

Buzzer Linkage

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

Door Linkage

Enable **Door Linkage**, check **Entrance** or **Exit**, and set the door status for the target event.

Linked Alarm Output

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

6.6.9 Access Control Settings

Set Authentication Parameters

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

 Note

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

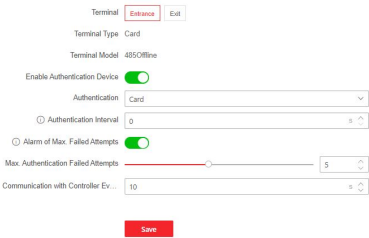


Figure 6-8 Set Authentication Parameters

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

Terminal

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

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

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

Authentication Interval

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

Alarm of Max. Failed Attempts

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

Max. Authentication Failed Attempts

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

Communication with Controller Every

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



Note

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

Set Door Parameters

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

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

Door No.

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

Door Name

You can create a name for the door.

Open Duration

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



Note

The open duration ranges from 5 s to 60 s.

Exit Button Type

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

Door Remain Open Duration with First Person

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

Serial Port Settings

Set serial port parameters.

Steps

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

Port Type RS232

No.

Baud Rate

Data Bit

Stop Bit ☒ 1 ☐ 2

Parity ☒ None ☐ Odd Parity ☐ Even Verification

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

Peripheral Position ☒ Entrance ☐ Exit

Device Model None

Software Version None

Save

Figure 6-9 Serial Port Settings

2. Set the **No.**, **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.
3. Set the **Peripheral Type** as **Card Reader**, **Card Receiver**, **QR Code Scanner** or **Disable**.
4. Set the **Peripheral Position** as **Entrance** or **Exit**.
5. You can view the serial port type, external device model and peripheral software version.
6. Click **Save**.

Set Terminal Parameters

You can set terminal parameters for accessing.

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

You can set **Working Mode** as **Permission Free Mode** or **Access Control Mode**.

Permission Free Mode

The device only judge your credential is in the valid duration, and will not authenticate the permission.

Enable **Verify Credential Locally**, the device will check permission but not estimate the plan template.

Access Control Mode

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

You can enable **Remote Verification** according to your actual needs. After enabling, you can verify remotely. And you can enable **Verify Credential Locally** according to your actual needs. Click **Save** to save the settings after the configuration.

6.6.10 Turnstile

Basic Parameters

Set turnstile basic parameters.

Steps

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

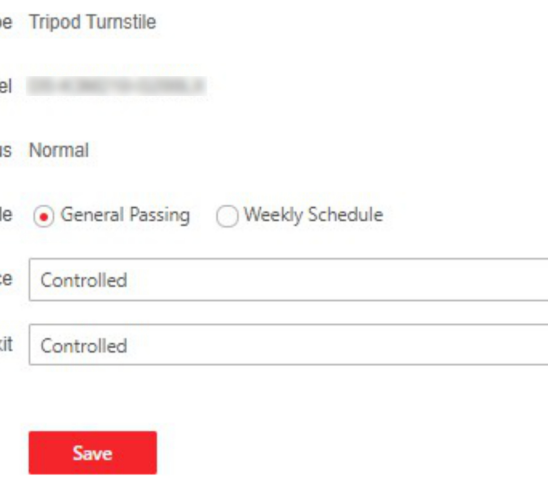


Figure 6-10 Basic Parameters

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

People Counting

Set people counting .

Steps

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

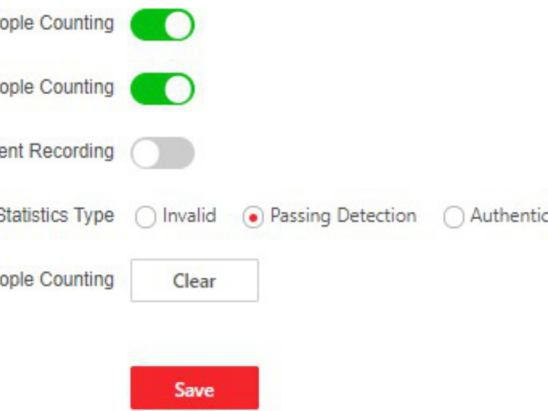


Figure 6-11 People Counting

2. Enable **People Counting**.
3. Enable **Device Offline People Counting** at your actual needs.



Note

Passing Event Recording is reserved.

4. Select **Person Statistics Type** as **Invalid**, **Passing Detection** or **Authentication Number**.
5. **Optional:** Click **Clear** to clear all the people counting information.

Other Settings

Set other parameters.

Steps

1. Click **Configuration** → **Turnstile Configuration** → **Other Settings** to enter the page.
2. Set **Alarm Output Duration**.



Note

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

3. Set **Temperature Unit**.
4. Drag the block or enter the value to adjust the light board brightness.
5. Set the alarm buzzer duration.
6. Enable **Memory Mode** at your actual needs.



Note

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

7. Set **Fire Input Type**.

8. Click **Save**.

6.6.11 Card Settings

Set Card Security

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

Set the parameters and click **Save**.

Enable NFC Card

Reserved.

Enable M1 Card

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

M1 Card Encryption Sector

M1 card encryption can improve the security level of authentication.

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

Enable EM Card

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



Note

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

Enable DESFire Card

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

DESFire Card Read Content

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

Enable FeliCa Card

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

Set Card No. Authentication Parameters

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

Go to **Configuration → Card Settings → Card No. Auth. Settings** .
Select a card authentication mode and enable reversed card No. at your actual needs. Click **Save**.

6.6.12 Set Privacy Parameters

Set the event storage type.

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

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

6.6.13 Upgrade and Maintenance

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

Reboot Device

Click **Maintenance and Security** → **Maintenance** → **Restart** .

Click **Restart** to reboot the device.

Upgrade

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

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



Note

Do not power off during the upgrading.

Restore Parameters

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

Restore All

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

Restore

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

Import and Export Parameters

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

Export

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



Note

You can import the exported device parameters to another device.

Import

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

6.6.14 Device Debugging

You can set device debugging parameters.

Steps

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

Enable SSH

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

Print Log

You can select a component from drop-down list and click **Export** to export log.

Capture Network Packet

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

6.6.15 Component Status

You can view the main lane and other status.

Main Lane Status

Device Component

You can view the status of the access control board, lane control board, user extended interface board.

Peripheral

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

Others

Passing Mode

You can view the entrance and exit mode.

Input and Output Status

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

Other Status

You can view the status of the barrier.

6.6.16 Log Query

You can search and view the device logs.

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

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

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

6.6.17 Certificate Management

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



Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

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

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

The certificate will be saved automatically.

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

Install Other Authorized Certificate

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

Steps

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

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

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



Note

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

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

7 Client Software Configuration

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

7.1 Configuration Flow of Client Software

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

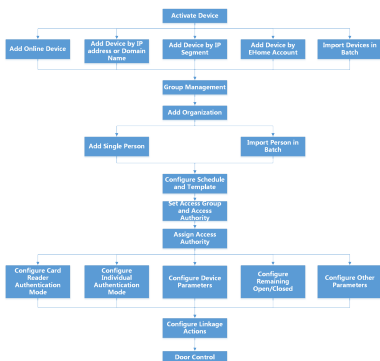


Figure 7-1 Flow Diagram of Configuration on Client Software

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 and IP segment. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

Add Device by IP Address or Domain Name

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

Steps

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

Name

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

Address

The IP address or domain name of the device.

Port

The devices to add share the same port number. The default value is **80**.

User Name

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

Password

Enter the device password.



Caution

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

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

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



Note

- This function should be supported by the device.
 - If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security.
 - You can log into the device to get the certificate file by web browser.
-

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

Example

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

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

Import Devices in a Batch

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

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.

- Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
- Open the exported template file and enter the required information of the devices to be added on the corresponding column.



Note

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

Adding Mode

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

Address

Edit the address of the device.

Port

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

User Name

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

Password

Enter the device password.



Caution

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

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

Import to Group

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

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

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

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

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

3. Select the device from the list and click  on the Operation column.
4. Reset the device password.
 - Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.



Note

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



Caution

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

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

7.2.3 Manage Added Devices

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

Table 7-1 Manage Added Devices

Edit Device	Click  to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click Delete to delete the selected devices.
Remote Configuration	Click  to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click  to view device status, including door No., door status, etc.  Note For different devices, you will view different information about device status.
View Online User	Click  to view the details of online user who access the device, including user

	name, user type, IP address and login time.
Refresh Device Information	Click  to refresh and get the latest device information.

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.

7.4 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 subordinated 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 Import and Export Person Identify Information

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

Import Person Information

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

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.

4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.



Note

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

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



Note

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

Import Person Pictures

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

Before You Start

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

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click  to select a face picture file.



Note

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

6. Click **Import** to start importing.
The importing progress and result will be displayed.

Export Person Information

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

Before You Start

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

Steps

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



Note

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

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

Export Person Pictures

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

Before You Start

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

Steps

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



Note

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

3. Click **Export** on the top menu bar.
4. Enter the super user name and password for verification.
The Export panel is displayed.
5. Check **Face** as the content to export.
6. Click **Export** and set an encryption key to encrypt the exported file.



Note

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

7.4.3 Get Person Information from Access Control Device

If the access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the added device and import them to the client for further operations.

Steps



Note

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

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



Note

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

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



Note

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

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



Note

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

The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

7.4.4 Issue Cards to Persons in Batch

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

Steps

1. Enter **Person** module.
2. **Optional:** Select a person group, and select the persons with no card issued.
 - The selected persons with no card issued in the person group will be displayed in the right panel.
 - If you do not select the persons with no card issued in a person group, all the added persons with no card issued will be displayed in the right panel.

3. Click **Batch Issue Cards**.

4. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.

5. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to .

6. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.

7. Click the **Card No.** column and enter the card number.

- Place the card on the card enrollment station.
- Swipe the card on the card reader.
- Manually enter the card number and press the **Enter** key.

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

7.4.5 Report Card Loss

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

Steps

1. Enter **Person** module.

2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.

3. In the **Credential → Card** panel, click  on the added card to set this card as lost card.

After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.

4. **Optional:** If the lost card is found, you can click  to cancel the loss.

After cancelling card loss, the access authorization of the person will be valid and active.

5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

7.4.6 Set Card Issuing Parameters

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

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

Local Mode: Issue Card by Card Enrollment Station

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

Card Enrollment Station

Select the model of the connected card enrollment station



Note

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

Card Type

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

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

Serial Port

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

Select the COM the card enrollment station connects to.

Buzzing

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

Card No. Type

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

M1 Card Encryption

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

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

Remote Mode: Issue Card by Card Reader

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

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.

Steps

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

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



Note

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

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

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

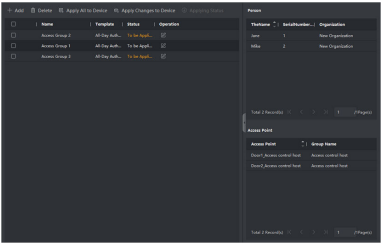


Figure 7-2 Display the Selected Person(s) and Access Point(s)

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

Apply All to Devices

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

Apply Changes to Devices

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

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



Note

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

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

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



Note

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

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

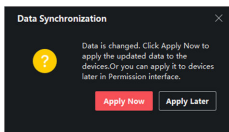


Figure 7-4 Data Synchronization

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 control points.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.

Before You Start

Add access control device to the client.

Steps

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



Note

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

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



Note

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

Enable NFC

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

Enable M1 Card

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

Enable EM Card

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

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

Configure Parameters for Door/Elevator

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

Before You Start

Add access control device to the client.

Steps

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



Note

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

Name

Edit the card reader name as desired.

Exit Button Type

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

Open Duration

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

5. Click **OK**.

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



Note

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

Configure Parameters for Card Reader

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

Before You Start

Add access control device to the client.

Steps

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



Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
 - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.
-

Name

Edit the card reader name as desired.

Card Authentication Interval

The time interval between two continuous card recognitions when authenticating.

Repeated Authentication Interval

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

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

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

Card Reader Type/Card Reader Description

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

4. Click **OK**.

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

Configure Parameters for Alarm Output

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

Before You Start

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

Steps

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

3. Set the alarm output parameters.

Name

Edit the card reader name as desired.

Alarm Output Active Time

How long the alarm output will last after triggered.

4. Click **OK**.

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

Configure Parameters for Lane Controller

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

Before You Start

Add access control device to the client.

Steps

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

3. Edit the parameters.

Passing Mode

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

Alarm Voice Prompt Time Duration

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



Note

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

Temperature Unit

Select the temperature unit that displayed in the device status.

Lightboard Brightness

Adjust the brightness of the device light.

Memory Mode

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

4. Click **OK**.

7.7.2 Configure Device Parameters

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

Set RS-485 Parameters

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

Before You Start

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

Steps

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

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** to enter the M1 Card Encryption page.
 4. Set the switch to on to enable the M1 card encryption function.
 5. Set the sector ID.

The sector ID ranges from 1 to 100.

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

7.8 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**.

7.8.1 Control Door Status

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

Before You Start

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

Steps

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



Note

For managing the access point group, refer to **Group Management**.

The doors in the selected access control group will display.

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



Note

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

4. Click the following buttons to control the door.

Unlock Door

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

Lock Door

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

Remain Unlocked

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

Remain Locked

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

Remain All Unlocked

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

Remain All Locked

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

Capture

Capture a picture manually.



Note

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

Remotely Unlocking Door Station

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



Note

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

Refresh Status

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

Result

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

7.8.2 Check Real-Time Access Records

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

Before You Start

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

Steps

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

Real-time access records are displayed on the bottom of the page. You can view record details, including card No., person name, event time, door location, temperature, authentication type etc.

Card No.	Person Name	Event Time	Door Location	Temperature	Abnormal Temperature	Authentication Type	Person	Linked Capture Picture	
00000001	Tom	2024-05-13 17:0144	Door1	36.4°C	No	CardFace			27
00000002	Tom	2024-05-13 17:0145	Door1	36.4°C	No	CardFace			
00000003	Tom	2024-05-13 17:0146	Door1	36.4°C	No	CardFace			
00000004	Tom	2024-05-13 17:0147	Door1	36.4°C	No	CardFace			

Figure 7-5 Real-time Access Records



Note

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

- Optional:** Select an access point group from the drop-down list in the upper-right corner to show the real time access records of the selected group.
- Optional:** Check the event type and event status.
The detected events of checked type and status will be displayed in the list below.
- Optional:** Check **Show Latest Event** to view the latest access record.
The record list will be listed reverse chronologically.
- Optional:** Check **Enable Abnormal Temperature Prompt** to enable abnormal skin-surface temperature prompt.



Note

When enabled, if there is abnormal temperature information, an Abnormal Temperature window pops up when you enter Monitoring module, displaying person's picture, skin-surface temperature, card No., person name, etc.

- Optional:** Click an event to view person pictures (including captured picture and profile).



Note

In **Linked Capture Picture** field, you can double click the captured picture to view an enlarged picture.

- Optional:** Click  to view details (including person's detailed information and the captured picture).



Note

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

A. DIP Switch

A.1 DIP Switch Description

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

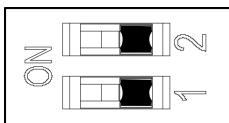


Figure A-1 DIP Switch

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

B. Button Configuration Description

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

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions
3	Passing Mode	1-Both sides under control  Note By default, 1 will be displayed on the display screen. 2-Entrance under control; exit prohibited 3-Entrance under control; exit free 4-Both sides free 5-Entrance free; exit under control 6-Entrance free; exit prohibited 7-Both sides prohibited 8-Entrance prohibited; exit under control 9-Entrance prohibited; exit free
4	Memory Mode	1-Disable 2-Enable  Note By default, 2 will be displayed on the display screen.
9	Enter Duration	5-5s, 6-6s, 7-7s, ..., 60-60s  Note By default, 5 will be displayed on the display screen.
10	Exit Duration	5-5s, 6-6s, 7-7s, ..., 60-60s  Note By default, 5 will be displayed on the display screen.
39	Brightness of Light	0-0, 1-1, 2-2, ... , 10-10

Level-1 Configuration No.	Description	Level-1 Configuration No. and Functions
		 Note By default, 6 will be displayed on the display screen.
42	Clearing People Counting	1-Default 2-Enable  Note By default, 1 will be displayed on the display screen.
43	Fire Protection Type	1-Remain Closed 2-Remain Open  Note By default, 2 will be displayed on the display screen.
99	Restore to Default	1-Default 2-Enable  Note By default, 1 will be displayed on the display screen.

C. Event and Alarm Type

Event	Alarm Type
Passing Timeout	None

D. Error Code Description

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

Error Reason	Code	Error Reason	Code
Optional Board Offline (If the board is not installed, the error code of "49" or "59" will appear but the device functions normally)	49/59	Obstruction	55
Encoder Exception	57	Motor Exception	58