

Access Control Terminal

User Manual

User Manual

©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

This manual is applied for access control terminal.

Product Serials	Model	Product Name
DS-K1T802	DS-K1T802E	Access Control Terminal (EM Card)
	DS-K1T802M	Access Control Terminal (M1 Card)

It includes instructions on how to use the Product. The software embodied in the Product is governed by the user license agreement covering that Product.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, SECURITY BREACHES, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF OR RELIANCE ON THIS MANUAL, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY OR CERTAIN DAMAGES, SO SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU.

Support

Should you have any questions, please do not hesitate to contact your local dealer.

Regulatory Information

FCC Information

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

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC Conditions

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

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

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/30/EU, the RoHS Directive 2011/65/EU.

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

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

collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

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

Safety Instruction

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

The precaution measure is divided into **Warnings** and **Cautions**:

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

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

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

 **Warnings**

- 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.
- 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.
- 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**

- 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 appropriate operation temperature is 0℃ to +45℃, and the storage temperature should be -10℃ to +55℃.
- 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.

Table of Contents

Chapter 1 Overview 1
1.1 Introduction 1
1.2 Main Features 1
Chapter 2 Appearance 3
2.1 Appearance of the Terminal 3
2.2 Description of Keypad Items 4
Chapter 3 Terminal Connection 5
3.1 Terminal Description 5
3.2 External Device Wiring 5
Chapter 4 Installation 7
4.1 Mounting with Gang Box 7
4.2 Mounting without Gang Box 8
Chapter 5 Activating the Access Control Terminal 10
5.1 Activating via SADP Software 10
5.2 Activating via Client Software 11
Chapter 6 Basic Operation 14
6.1 User Management 15
6.1.1 Adding User 15
6.1.2 Editing User 16
6.1.3 Searching User 17
6.1.4 Deleting User 18
6.2 Communication Settings 18
6.3 System Settings 19
6.3.1 Restoring Settings 19
6.3.2 Setting login Password 20
6.3.3 Door Settings 20
6.3.4 Settings Authentication Mode 21
6.3.5 Rebooting Device 22
6.4 Time Settings 22
6.5 Permission Settings 22
6.6 System Information 24

Chapter 7 Client Operation 26
7.1 Function Module 26
7.2 User Registration and Login 29
7.3 System Configuration 30
7.4 Access Control Management 31
7.4.1 Adding Access Control Device 32
7.4.2 Viewing Device Status 46
7.4.3 Editing Basic Information 47
7.4.4 Network Settings 48
7.4.5 Capture Settings 50
7.4.6 RS-485 Settings 51
7.4.7 Wiegand Settings 52
7.4.8 M1 Card Encryption 52
7.4.9 Remote Configuration 53
7.5 Person and Card Management 60
7.5.1 Organization Management 61
7.5.2 Person Management 62
7.6 Schedule and Template 71
7.6.1 Week Schedule 72
7.6.2 Holiday Group 73
7.6.3 Template 74
7.7 Permission Configuration 76
7.7.1 Adding Permission 77
7.7.2 Applying Permission 78
7.8 Advanced Functions 78
7.8.1 Access Control Parameters 79
7.8.2 Card Reader Authentication 81
7.8.3 Multiple Authentication 83
7.8.4 Open Door with First Card 86
7.8.5 Anti-Passing Back 87
7.8.6 Cross-Controller Anti-passing Back 88
7.8.7 Multi-door Interlocking 91
7.8.8 Authentication Password 92
7.8.9 Custom Wiegand 93
7.9 Searching Access Control Event 95
7.10 Access Control Event Configuration 96
7.10.1 Access Control Event Linkage 96
7.10.2 Access Control Alarm Input Linkage 98
7.10.3 Event Card Linkage 98
7.10.4 Cross-Device Linkage 100
7.11 Door Status Management 102

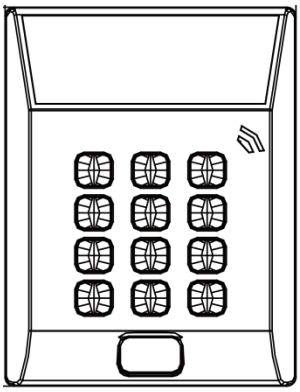
7.11.1 Access Control Group Management 102
7.11.2 Anti-control the Access Control Point (Door) 103
7.11.3 Status Duration Configuration 105
7.11.4 Real-time Card Swiping Record 106
7.11.5 Real-time Access Control Alarm 107
7.12 Arming Control 108

Appendix A Sound Prompt and Indicator 110

Appendix B Custom Wiegand Rule Descriptions 111

Chapter 1Overview

1.1 Introduction



DS-K1T802 is a series of standalone access control terminal designed with a LCD display screen. It supports TCP/IP network communication, offline records storage functions and so on.

1.2 Main Features

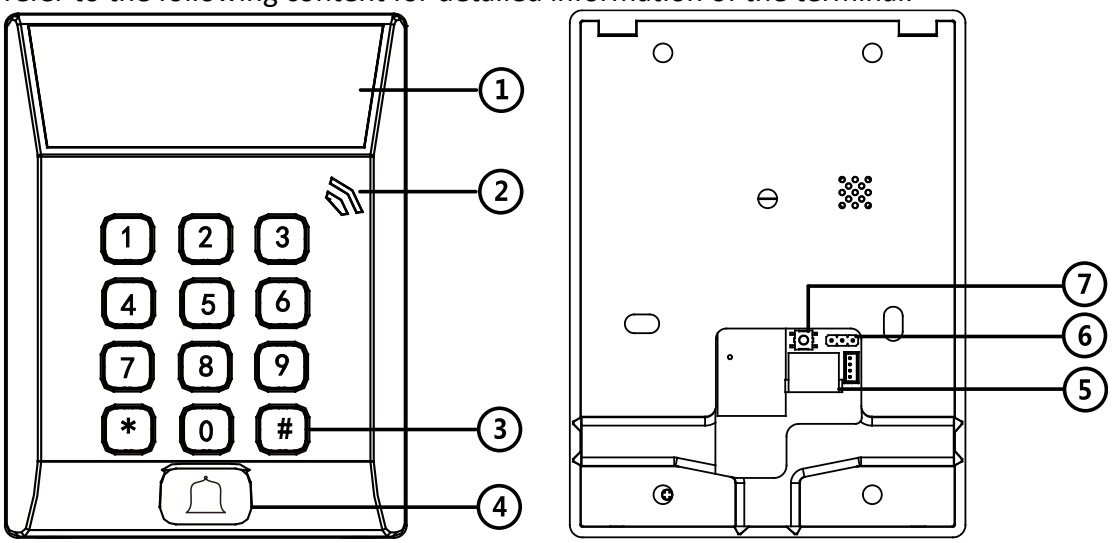
- Equipped with 32-bit high-speed processor
- Supports TCP/IP network communication, with self-adaptive network interface. The communication data is specially encrypted to relieve the concern of privacy leak
- Supports EM card and M1 card reading
- Supports authentication methods of card, card and password, card or password
- Doorbell ring design
- Supports time synchronization via NTP, manual or automatic method
- Supports online upgrade, remote control of the doors, first card open function, first card authentication function, super card, super password function and device rebooting control
- The access controller can store 3 thousand legal cards and 10 thousand card swiping records
- Supports event card linkage
- Supports M1 card encryption function
- Supports IP address conflict detection
- Supports up to 500 groups of authentication password
- Unlocking overtime alarm, invalid card swiping over times alarm, blocklist alarm, and duress card/code alarm
- Supports various card types as normal/ blocklist/ patrol/ guest/ duress/ super card, card for door extended opening, etc.
- Supports multiple events uploading methods: channel, and listening; The device can upload one integrated event and four real-time events via channel uploading method
- Supports getting device events via SDK

- Data can be permanently saved after power-off
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal
- Remotely device rebooting control
- Supports alarm of offline event exceeding 90%

Chapter 2 Appearance

2.1 Appearance of the Terminal

Please refer to the following content for detailed information of the terminal.



No.	Name	Description	
1	LCD Display Screen	First Line: display date Second Line: display time Third Line: display authentication information or swiping status	
2	Power Indicator	Slow Flashing Green	Card reader is working properly.
		Solid Green for a time period	The operation of pressing keys or swiping card is valid.
		Solid Red for a time period	The operation of pressing keys or swiping card is invalid.
3	Keypad	Numeric key 0 to 9, Clearing key *, and Confirming key #	
4	Door Bell	Door Bell Ring	
5	Wiring Terminals	Wire the device with power supply, doorbell, and door lock.	
6	Jumper	Control the status of the lock relay.	
7	Initialization Button	When rebooting the device, hold the button for about 8s to enter the initialization mode. When initializing, the device buzzer will beep for 8s.	

2.2 Description of Keypad Items

No.	Description
0 to 9	Numeric Keys: Enter number in the textbox.
2 and 8	Direction Keys: Select icons in the menu.
*	Exiting Key: Click the key to exit the menu.
#	Confirming Key: Click the key to confirm operations.

Chapter 3Terminal Connection

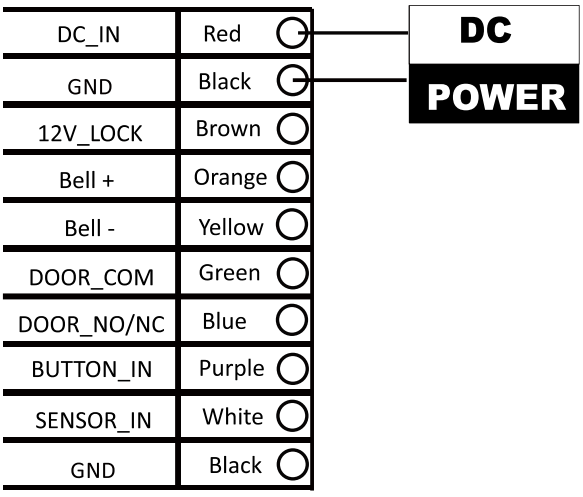
3.1 Terminal Description

The following table shows the terminals description:

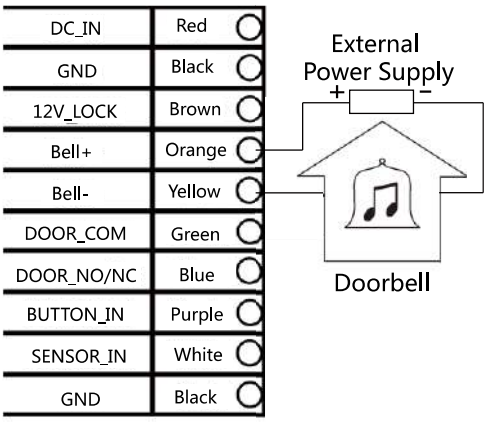
Description		Color
Power Input	12V DC	Red
	GND	Black
Bell	Bell+	Orange
	Bell-	Yellow
Door Lock	BUTTON_IN	Purple
	DOOR_COM	Green
	DOOR_NO/NC	Blue
	SENSOR_IN	White
	GND	Black
	12V_LOCK	Brown

3.2 External Device Wiring

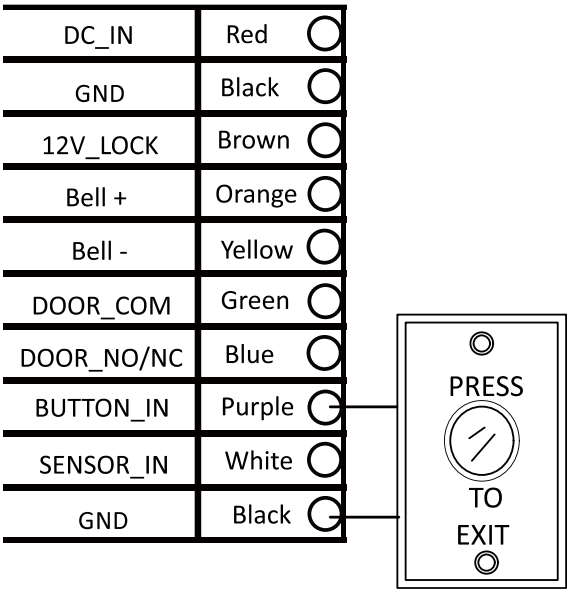
Power Supply Wiring



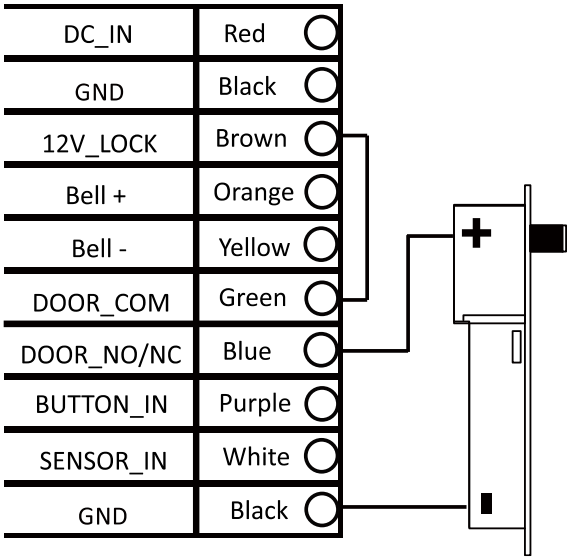
Doorbell Wiring



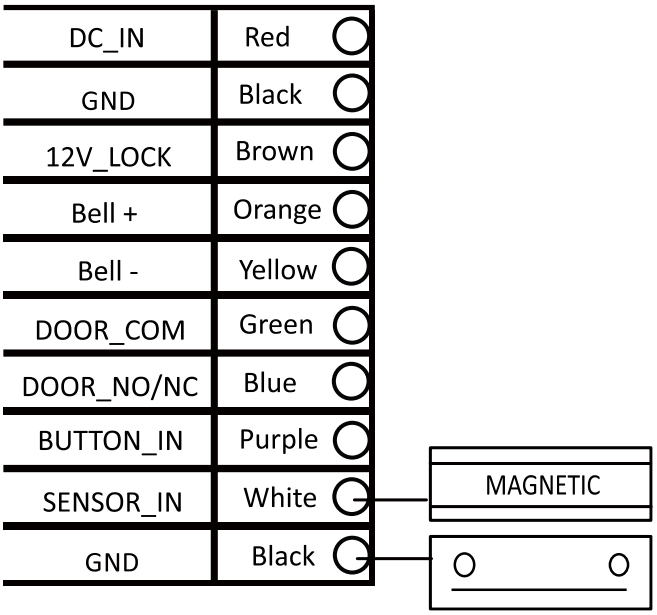
Door Button Wiring



Door Lock Wiring



Door Magnetic Wiring



Chapter 4Installation

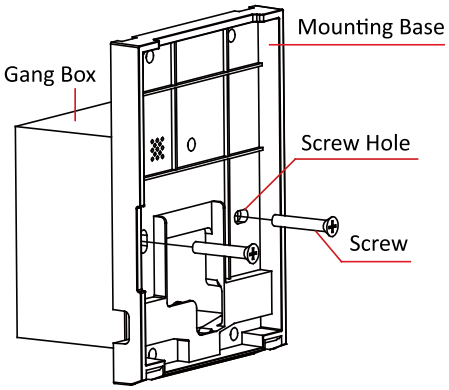
Before you start

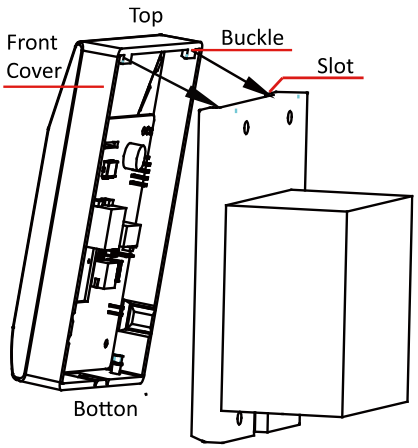
- Please make sure that the device in the package is in good condition and all the assembly parts are included.
- Make sure that all the related equipment is power-off during the installation.
- Check the specification of the products for the installation environment.
- Check whether the power supply is matched with your AC outlet to avoid damage.
- If the product does not function properly, please contact your dealer or the nearest service center. Do not disassemble the camera for repair or maintenance by yourself.
- Please make sure the wall is strong enough to withstand three times the weight of the camera and the mounting.

4.1 Mounting with Gang Box

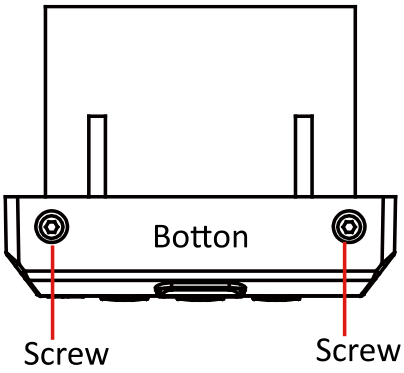
Steps:

1. Route the cables through the cable hole of the mounting base.
2. Align the screw holes on mounting base with the screw holes on gang box.
3. Fix the mounting base on the gang box with inserting two KA4*22-SUS screws (supplied) into the two screw holes.





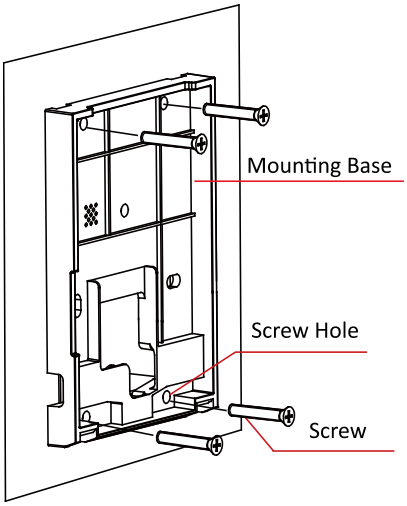
4. Connect the corresponded cables.
5. Align the buckle of the front cover with the slot of the mounting base, and hang the front cover onto the mounting base. Make sure the buckle is embedded into the slot.
6. Secure the front cover with inserting and tightening two screws on the bottom of device.

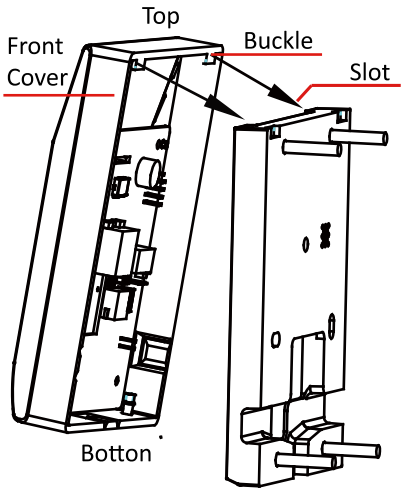


4.2 Mounting without Gang Box

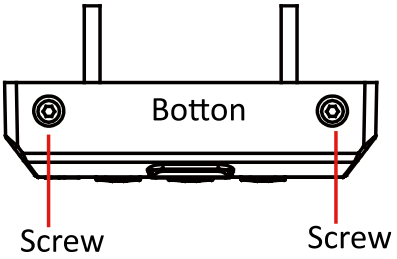
Steps:

1. Drill 4 screw holes in the wall according to the holes of the mounting base, and then insert expansion screws sockets (not supplied) into the holes.
2. Route the cables through the cable hole of the mounting base.
3. Align the screw holes on the base with the screw sockets on the wall.
4. Attach the mounting base on the wall with Inserting 4 KA4*22-SUS screws (supplied) into the 4 screw sockets.





5. Connect the corresponded cables.
6. Align the buckle of the front cover with the slot of the mounting base, and hang the front cover onto the mounting base. Make sure the buckle is embedded into the slot.
7. Secure the front cover with inserting and tightening two screws on the bottom of device.



Chapter 5 Activating the Access Control Terminal

Purpose:

You are required to activate the terminal first before using it.

Activation via SADP, and Activation via client software are supported.

The default values of the control terminal are as follows.

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

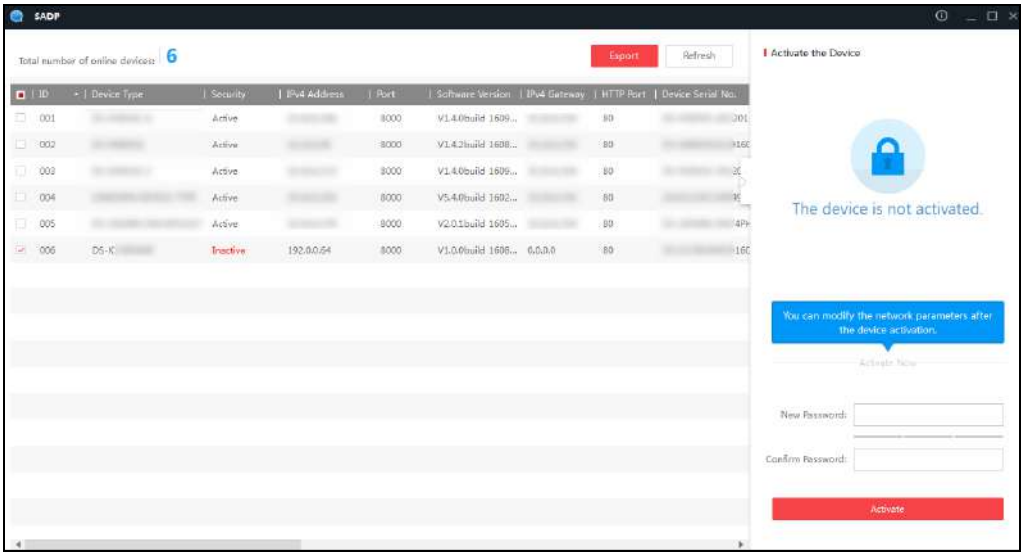
5.1 Activating via SADP Software

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the control panel.

Steps:

1. Run the SADP software to search the online devices.
2. Check the device status from the device list, and select an inactive device.



3. Create a password and input the password in the password field, and confirm the password.



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

4. Click **Activate** to activate the device.
5. Check the activated device. You can change the device IP address to the same network

segment with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.



6. Input the password and click the **Modify** button to activate your IP address modification.

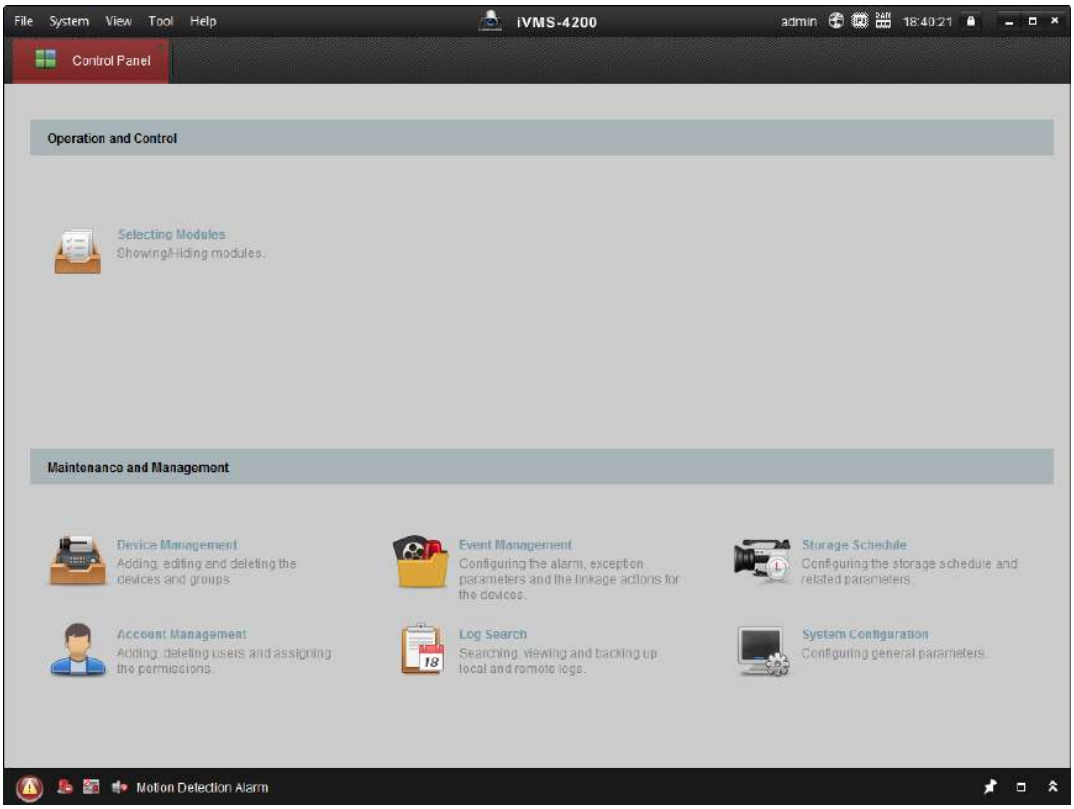
5.2 Activating via Client Software

The client software is versatile video management software for multiple kinds of devices.

Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.



2. Click the **Device Management** to enter the Device Management interface.
3. Check the device status from the device list, and select an inactive device.



4. Click the **Activate** button to pop up the Activation interface.
5. In the pop-up window, create a password in the password field, and confirm the password.

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.*



6. Click **OK** button to start activation.
7. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.
8. Change the device IP address to the same network segment with your computer by either modifying the IP address manually.
9. Input the password and click the **OK** button to save the settings.

Chapter 6 Basic Operation

Before You Start:

- You should activate the device before the first login. Otherwise, after powered on, the system will switch into activation notifying interface. For detailed information about activation, see Chapter 5.
- You should enter the default password for the first login.

  Enter **Sys Opt-Login Pwd** to reset the login password.
  The default password is 12345.

Steps:

1. The device enters the initial interface automatically after powered on.



2. Enter [*] + [0] + [#] to enter the login interface

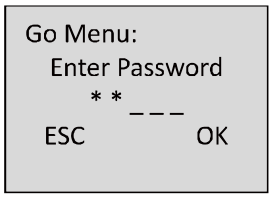


Figure 1-1 Login Interface

3. Enter the login password.
4. Click the # key to confirm the settings. If the configuration password authentication failed, the system will return to the initial interface, and if the configuration password is successfully authenticated, the system will enter the menu operation interface。

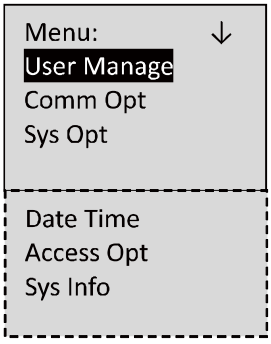


Figure 1-2 Menu Operation Interface

On the menu operation interface, you can manage users, set communication parameters, set system parameters, and so on.

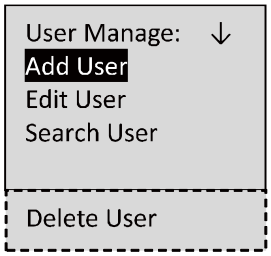
6.1 User Management

Purpose:

On the user management interface, you can add and manage users.

Steps:

1. Move the cursor to **User Manage** (user management) with the direction keys.
2. Click the **#** key to enter the adding user interface.



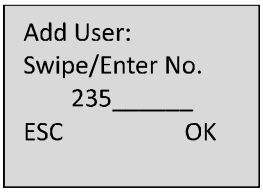
6.1.1 Adding User

Purpose:

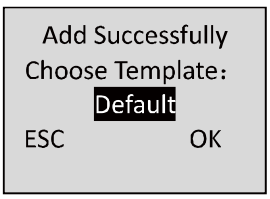
In the **Add User** menu, you can add users, and register card for the corresponding person.

Steps:

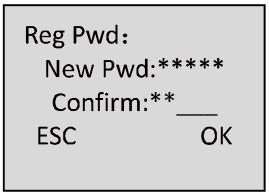
1. Move the cursor to **Add User** (add user) by using the direction keys.
2. Click the **#** key to enter the card registration interface.



3. Register the card.
   - Register the card by swiping the card.
     1) Place the card on the induction area.
     2) The system displays the card No. in the textbox automatically with a beep sound if the card No. has been recognized. .
   - Register the card by entering the card number into the **or enter the Card No.** textbox.
4. After registering the card, select the permission template.



5. Click the **#** key to enter the password registration interface. If the password is registered, the card holder will be able to open the door with swiping card and entering password.



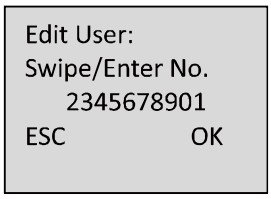
6. Register password.
    1) Enter a new password.
    2) Confirm the new password.
    3) Click the **#** key to confirm the settings.

    Note: The valid length of the password is 1 to 8 characters.
7. If the password registration is not required, click the # key to return to the Add User interface.

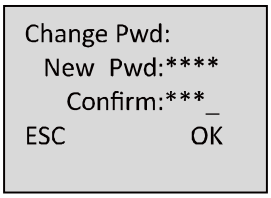
6.1.2 Editing User

Steps:

1. Move the cursor to **Edit User** by using direction keys on the user management interface.
2. Click the **#** key to enter the managing user interface.

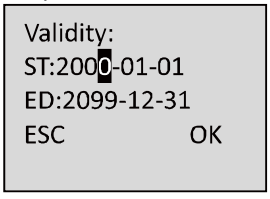


3. Swipe the card or enter the card No. .
4. Click the **#** key to enter the password settings interface.
    1) Move the cursor to **Change PWD** to enter the password changing interface.
    2) Enter a new password.
    3) Confirm the new password.
    4) Click the **#** key to confirm the settings.



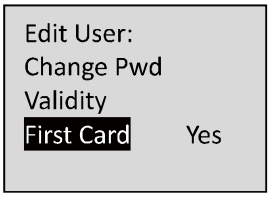
5. If the password is not required, click the # key to clear the configured password.
6. Change the valid date

    You can set the valid date (start/end date) of the card.



Click the **#** key to confirm the settings.

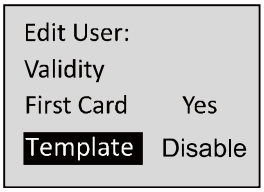
7. Enable the first card permission of the user.
   1) Click the **#** key to enter the editing mode.
   2) Press the direction key to select whether to enable the first card for the user.
   3) Click the **#** key to confirm the editing.



Note: After enabling first card, the door remains open during the pre-defined valid duration.

8. Select the template for the user.
   1) Click the **#** key to enter the editing mode.
   2) Press the direction key to select the template No.

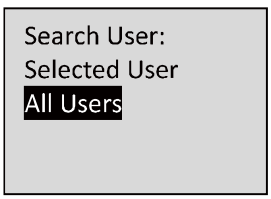
   Note: Max.65 templates are selectable (including 64 schedule templates and 1 template disabling option)， the schedule template value is from **01** to **64**, and **Default** indicates the template 01. The template disabling option value is **00**.
   3) Click the **#** key to confirm the editing.



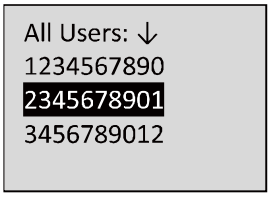
6.1.3 Searching User

Steps:

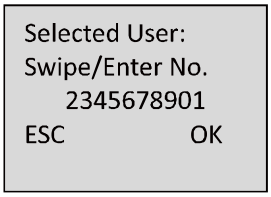
1. Move the cursor to **Search User**.
2. Click the **#** key to enter the searching interface.



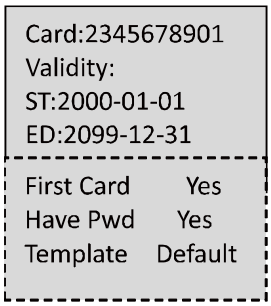
3. Select **All User** and the list of all user will be displayed.



4. Select the **Selected User** to enter the query specified user interface.
5. Swipe card or enter the card No.



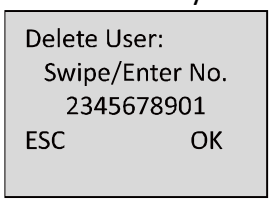
6. Click the **#** key to view the basic information about the card holder.



6.1.4 Deleting User

Steps:

1. Move the cursor to **Delete User**, and click the **#** key to enter the deleting interface.



2. Swipe card or enter the card No.
3. Click the **#** key to enter the confirmation page.
4. Select whether to confirm the settings

Note: You can click * key to return to the main menu.

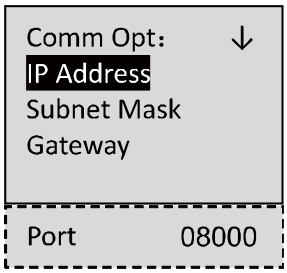
6.2 Communication Settings

Purpose:

On the communication settings interface, you can set network parameters,

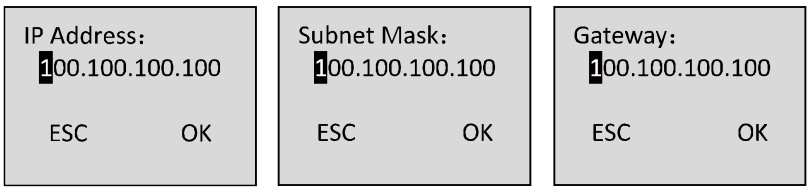
Steps:

1. Move the cursor to **Comm Opt** (communication settings) by using the direction keys.
2. Click the **#** key to enter the communication settings interface.



Note: The valid port No. range is from 2000 to 65535.

3. Modify network parameters of the device, including IP address, subnet mask, and gateway address.

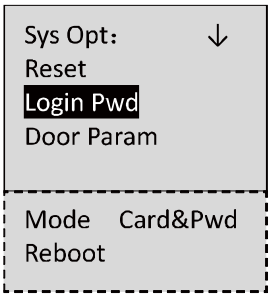


4. Edit the port No. of the terminal.
5. Click the **#** key to complete the settings.

6.3 System Settings

Steps:

1. Move the cursor to **Sys Opt** (system parameters) by using direction keys.
2. Click the **#** key to enter the system parameters interface.



Reset: The device can be restored into factory defaults or default settings.
Login Pwd (Login Password): Change the login password.
Door Param (Door Parameters): Set parameters of the access control terminal, including Open Time (Door Action Time), Open Time-out(Delayed Door Alarm), Door Magnetic (Door Magnetic Status Settings), Button Type (Exit Button Status Settings), and First Card settings.
Mode (Authentication Mode): You can select the card authentication mode.
Reboot (Reboot Device): You can reboot the device

6.3.1 Restoring Settings

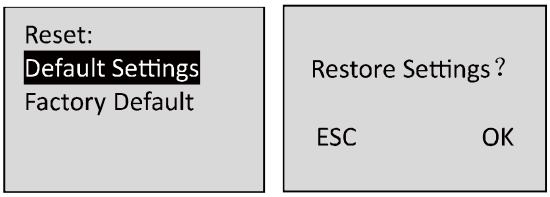
Purpose:

On the restore settings interface, you can restore Factory Defaults or Default Settings.

Steps:

1. Move the cursor to **Reset** (restore settings) by using direction keys on the system settings interface.

2. Click the **#** key to enter the restore settings interface.

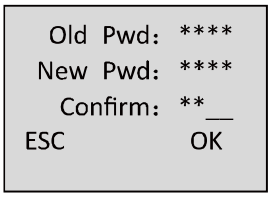


3. Select to Factory Defaults or Default Settings.
   Factory Defaults: After restoring factory defaults, all parameters of the device are returned to the factory defaults.
   Default Settings: After restoring defaults settings, parameters, excluding network parameters and event parameters, are returned to the factory defaults.
4. Click the **#** key to implement the settings.

6.3.2 Setting login Password

Steps:

1. Click the **#** key to enter the password settings interface.



   1) Enter the old password.
   2) Enter a new password.
   3) Confirm the new password.

Note: The valid password length should be 5 characters.

2. Click the **#** key to confirm the settings.

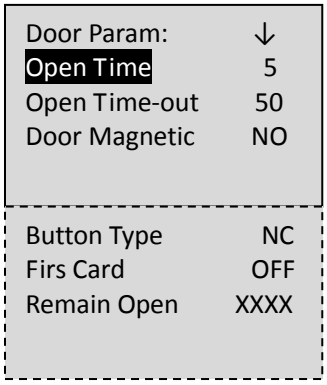
6.3.3 Door Settings

Purpose:

On the door settings interface, you can set door parameters, including Open Time (Door Action Time), Open Time-out (Delayed Door Alarm), Door Magnetic (Door Magnetic Status Settings), Button Type (Exit Button Status Settings), First Card (First Card Mode Settings), and Remain Open (Remain Open Duration Settings).

Steps:

1. Move the cursor to **Door Param** (door settings) by using direction keys in the system settings interface.
2. Click the **#** key to enter the door settings interface.



3. Edit door parameters.
   Open Time: Door action time, set the door action time: 1 ~ 255 s.
   Open Time-out : Delayed door alarm, set the delayed door alarm threshold: 0 ~ 255s.
   Door Magnetic: Door magnetic status settings, Remain open and remain closed are selectable.
   Button Type: Exit button status settings, Remain open and remain closed are selectable.
   First Card: Set the first card mode, you can select from ON (enable remain open with first card), OFF (disable remain open with first card), and Auth. (first card authorization).
   Remain Open: You can set remain open duration for if you select the ON mode.
4. Click the **#** key to confirm the settings.

Notes:

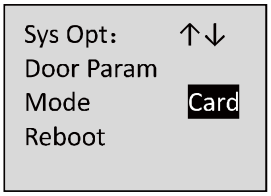
- **Remain Open with First Card:** The door remains open for the configured time duration after the first card swiping until the remain open duration ends.
- **First Card Authorization:** All authentications, except for the authentications of super card, duress card, and duress code, are allowed only after the first card authorization.

6.3.4 Settings Authentication Mode

In this section, you can set the controller authentication mode for opening the door, that is, **Card** (Swipe Card Only), **Card & Pwd** (Card and Password), and **Card/Pwd** (Card or Password).

Steps:

1. Move the cursor to **Mode** (Authentication Settings) by using direction keys in the system settings interface.



Notes:

- The password of Card & Pwd is the password configured via the device.
- The password of Card/Pwd is the authentication code applied by the client software.

2. Click the **#** key to select the authentication mode.

6.3.5 Rebooting Device

Steps:

1. Move the cursor to **Reboot** by using direction keys
2. Click the **#** key to start the rebooting operation of the device.

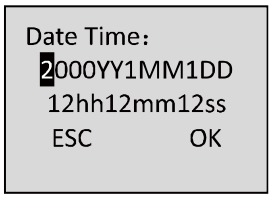
6.4 Time Settings

Steps:

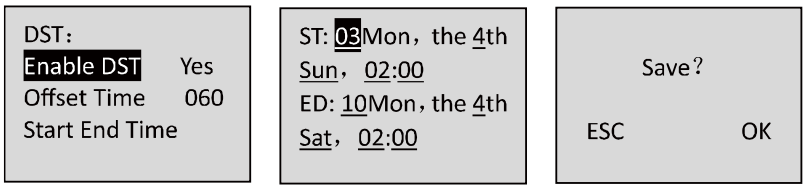
1. Move the cursor to **Date Time** (time settings) by using direction keys.
2. Click the **#** key to enter the time settings interface.



3. Select to edit the Edit **Date Time** or **DST (Daylight Saving Time)** parameters of the device.
   - Edit **Date Time:**



   - Edit **DST (Daylight Saving Time)**



   When enabling DST, you should set the offset time, the start time, and the end time of DST.

Notes:

- Press * key to cancel the date/time settings, and return to the **Date Time** interface.
- Press # key to confirm the date/time settings, and return to the **Date Time** interface.

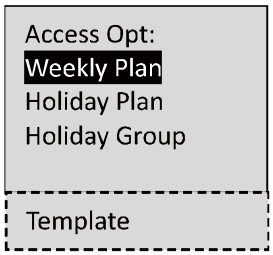
6.5 Permission Settings

Purpose:

On the permission settings section, you can set the weekly schedule, holiday schedule, Holiday group and template.

Steps:

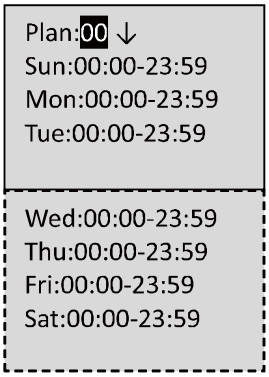
1. Move the cursor to **Access Opt** (Access Operation) by using direction keys.
2. Click the **#** key to enter the interface.



Weekly Schedule Settings

Steps:

1. Move the cursor to **Weekly Plan** by using direction keys.
2. Click the **#** key to enter the weekly schedule configuration interface.

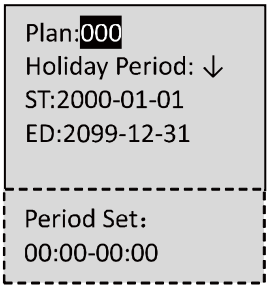


3. Set the plan No., with entering the plan No. by the numeric keys.
   Max. 32 plans can be configured, and the plan No. range is from 1 to 32.
4. Set the detailed time periods from Sunday to Saturday with entering the start time and end time by the numeric keys.
5. Click the ***** key to return to the **Access Opt** interface.

Holiday Schedule Settings

Steps:

1. Move the cursor to **Holiday Plan** by using direction keys.
2. Click the **#** key to enter the holiday schedule configuration interface.

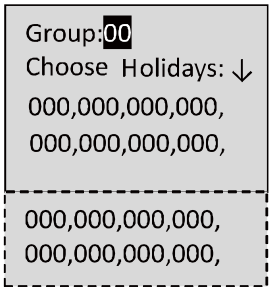


3. Set the plan No., with entering the plan No. by the numeric keys.
   Max. 128 plans can be configured, and the plan No. range is from 1 to 128.
4. Set the detailed holiday information.
   Date: Enter the start date and end date by the numeric keys.
   Period: Enter the start time and end time by the numeric keys.
5. Click the ***** key to return to the **Access Opt** interface.

Holiday Group Settings

Steps:

1. Move the cursor to **Holiday Group** by using direction keys.
2. Click the **#** key to enter the holiday group configuration interface.

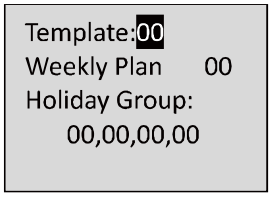


3. Set the group No., with entering the group No. by the numeric keys.
   Max. 64 groups can be configured, and the group No. range is from 1 to 64.
4. Set the holiday group. Move the cursor to holiday No.(the default is 000), and
   Enter the holiday No. configured in **Holiday Schedule Settings** by the numeric keys.
   The holiday schedule No. is separated by a comma.
5. Click the ***** key to return to the **Access Opt** interface.

Template Settings

Steps:

1. Move the cursor to **Template** by using direction keys.
2. Click the **#** key to enter the template configuration interface.

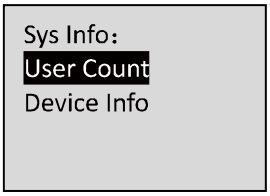


3. Set the template No., with entering the template No. by the numeric keys.
   Max. 64 templates can be configured, and the template No. range is from 1 to 64.
4. Enter the Weekly Plan No. by the numeric keys.
5. Set the Holiday groups. Move the cursor to holiday group No.(the default is 000), and Enter the holiday group No. configured in **Holiday Group Settings** by the numeric keys.
   The holiday group No. is separated by a comma.
6. Click the ***** key to return to the **Access Opt** interface.

6.6 System Information

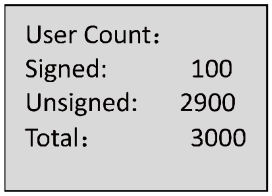
Steps:

1. Move the cursor to **Sys Info** (system information) by using direction keys.
2. Click the **#** key to enter the system information interface.



3. Select **User Count** or Device **Information**.

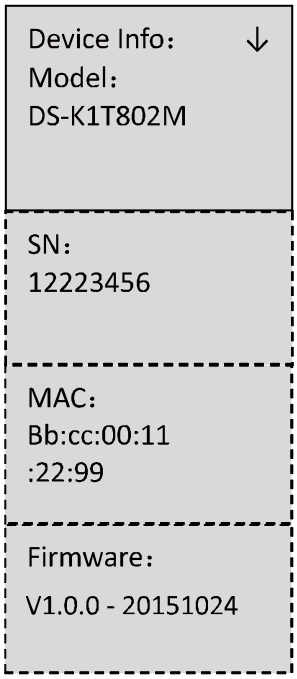
- **User Capacity**



Registered Amount: the count of user that is registered
Remainder Amount: the count of remainder registration amount
Total Amount: It refers to the maximum amount of cards
Note: The default maximum card amount is 2000.

- **Device Information**

In the device information interface, you can view the device name, the serial No., Mac address, and so on.

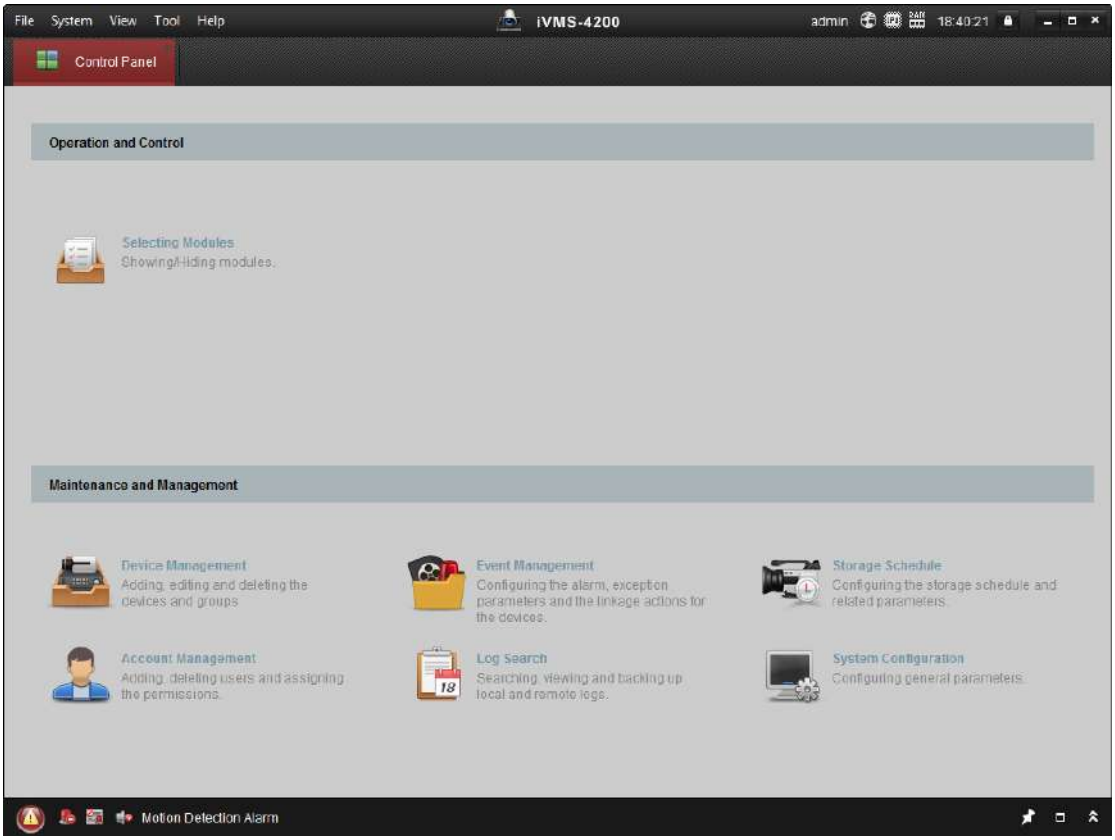


Chapter 7Client Operation

You can set and operate the access control devices via the client software. This chapter will introduce the access control device related operations in the client software. For integrated operations, refer to *User Manual of iVMS-4200 Client Software*.

7.1 Function Module

Control Panel of iVMS-4200:



Menu Bar:

File	**Open Image File**	Search and view the captured pictures stored on local PC.
	Open Video File	Search and view the video files recorded on local PC.
	Open Log File	View the backup log files.
	Exit	Exit the iVMS-4200 client software.
System	**Lock**	Lock screen operations. Log in the client again to unlock.
	Switch User	Switch the login user.
	Import System Config File	Import client configuration file from your computer.
	Export System Config File	Export client configuration file to your computer.
	Auto Backup	Set the schedule for backing up the database

		including person, attendance data, and permission data automatically.
View	**1024*768**	Display the window at size of 1024*768 pixels.
	1280*1024	Display the window at size of 1280*1024 pixels.
	1440*900	Display the window at size of 1440*900 pixels.
	1680*1050	Display the window at size of 1680*1050 pixels.
	Maximize	Display the window in maximum mode.
	Control Panel	Enter Control Panel interface.
	Main View	Open Main View page.
	Remote Playback	Open Remote Playback page.
	Access Control	Enter the Access Control Module.
	Status Monitor	Enter the Status Monitor Module.
	Time and Attendance	Enter the Time and Attendance Module.
	Security Control Panel	Enter the Security Control Panel Module.
	Real-time Alarm	Enter the Real-time Alarm Module.
	Video Wall	Open Video Wall page.
	E-map	Open E-map page.
	Auxiliary Screen Preview	Open Auxiliary Screen Preview window.
Tool	**Device Management**	Open the Device Management page.
	Event Management	Open the Event Management page.
	Storage Schedule	Open the Storage Schedule page.
	Account Management	Open the Account Management page.
	Log Search	Open the Log Search page.
	System Configuration	Open the System Configuration page.
	Broadcast	Select camera to start broadcasting.
	Device Arming Control	Set the arming status of devices.
	Alarm Output Control	Turn on/off the alarm output.
	Batch Wiper Control	Batch starting or stopping the wipers of the devices.
	Batch Time Sync	Batch time synchronization of the devices.
	Player	Open the player to play the video files.
	Message Queue	Display the information of Email message to be sent.
Help	**Open Video Wizard**	Open the video guide for the video security configuration.
	Open Video Wall Wizard	Open the guide for the video wall configuration.
	Open Security Control Panel Wizard	Open the guide for the security control panel configuration.
	Open Access Control and Video Intercom Wizard	Open the guide for the access control and video intercom configuration.
	Open Attendance Wizard	Open the guide for the time and attendance configuration.
	User Manual (F1)	Click to open the User Manual; you can also open the User Manual by pressing **F1** on your keyboard.
	About	View the basic information of the client software.

	Language	Select the language for the client software and reboot the software to activate the settings.

For the first time running the software, you can click 

on the control panel to select the modules to display on the Operation and Control area of the control pane.

Steps:

1. Click  to pop up the following dialog.



2. Check the module checkboxes to display them on the control panel according to the actual needs.
3. Click **OK** to save the settings.

Notes:

- After adding the access control device in Device Management module, the Access Control, Status, and Time and Attendance module will be displayed on the control panel automatically.
- After adding the security control panel in Device Management module, the Security Control Panel and Real-time Alarm modules will be displayed on the control panel automatically.

The iVMS-4200 client software is composed of the following function modules:

	The Main View module provides live view of network cameras and video encoders, and supports some basic operations, such as picture capturing, recording, PTZ control, etc.
	The Remote Playback module provides the search, playback, export of video files.
	The Access Control module provides managing the organizations, persons, permissions, and advanced access control functions. Provides video intercom function.

	The Status Monitor module provides monitoring and controlling the door status, viewing the real-time card swiping records and access control events.
	The Time and Attendance module provides setting the attendance rule for the employees and generating the reports.
	The Security Control Panel module provides operations such as arming, disarming, bypass, group bypass, and so on for both the partitions and zones.
	The Real-time Alarm module provides displaying the real-time alarm of security control panel, acknowledging alarms, and searching the history alarms.
	The Alarm Event module displays the alarm and event received by the client software.
	The Video Wall module provides the management of decoding device and video wall and the function of displaying the decoded video on video wall.
	The E-map module provides the displaying and management of E-maps, alarm inputs, hot regions and hot spots.
	The Device Management module provides the adding, modifying and deleting of different devices and the devices can be imported into groups for management.
	The Event Management module provides the settings of arming schedule, alarm linkage actions and other parameters for different events.
	The Storage Schedule module provides the schedule settings for recording and pictures.
	The Account Management module provides the adding, modifying and deleting of user accounts and different permissions can be assigned for different users.
	The Log Search module provides the query of system log files and the log files can be filtered by different types.
	The System Configuration module provides the configuration of general parameters, file saving paths, alarm sounds and other system settings.

The function modules are easily accessed by clicking the navigation buttons on the control panel or by selecting the function module from the **View** or **Tool** menu.

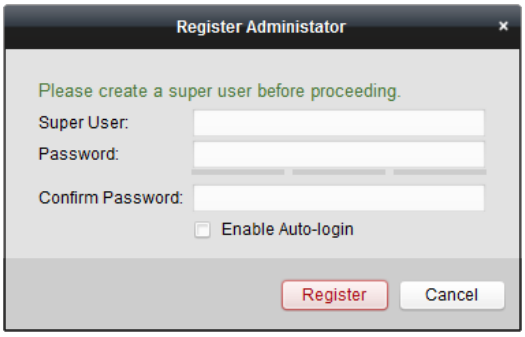
You can check the information, including current user, network usage, CPU usage, memory usage and time, in the upper-right corner of the main page.

7.2 User Registration and Login

For the first time to use iVMS-4200 client software, you need to register a super user for login.

Steps:

1. Input the super user name and password. The software will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.
2. Confirm the password.
3. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
4. Click **Register**. Then, you can log into the software as the super user.

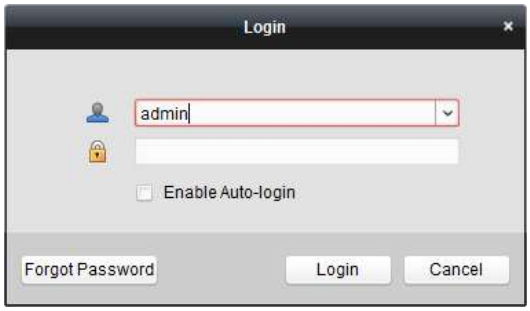


- *A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.*
- *For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

When opening iVMS-4200 after registration, you can log into the client software with the registered user name and password.

Steps:

1. Input the user name and password you registered.
   Note: If you forget your password, please click **Forgot Password** and remember the encrypted string in the pop-up window. Contact your dealer and send the encrypted string to him to reset your password.
2. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
3. Click **Login**.



After running the client software, you can open the wizards (including video wizard, video wall wizard, security control panel wizard, access control and video intercom wizard, and attendance wizard), to guide you to add the device and do other settings and operations. For detailed configuration about the wizards, please refer to the *Quick Start Guide of iVMS-4200*.

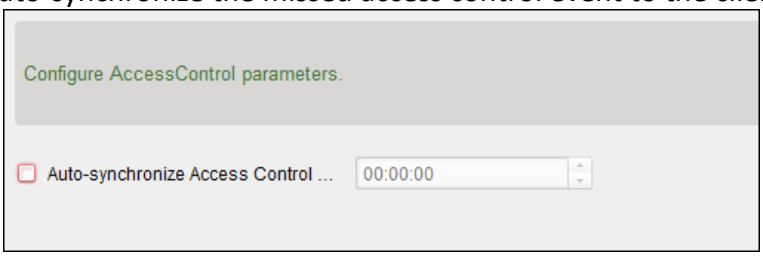
7.3 System Configuration

Purpose:

You can synchronize the missed access control events to the client.

Steps:

1. Click **Tool** – **System Configuration**.
2. In the System Configuration window, check the **Auto-synchronize Access Control Event** checkbox.
3. Set the synchronization time.
   The client will auto-synchronize the missed access control event to the client at the set time.



7.4 Access Control Management

Purpose:

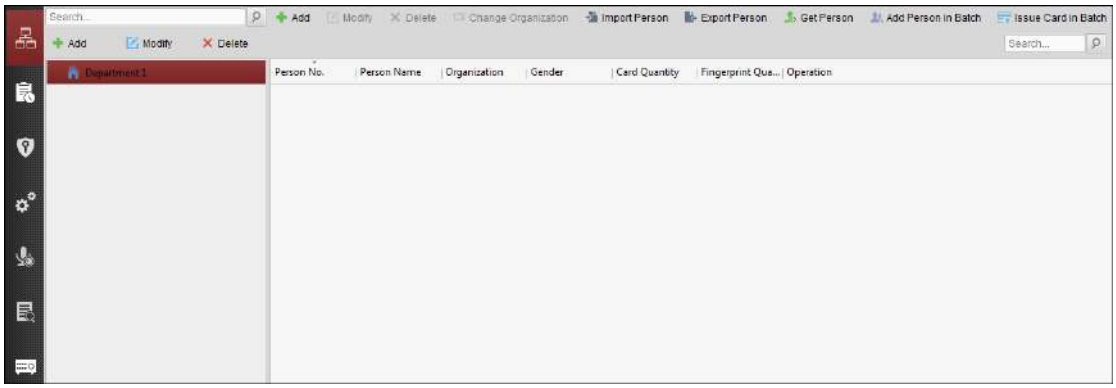
The Access Control module is applicable to access control devices and video intercom. It provides multiple functionalities, including person and card management, permission configuration, access control status management, video intercom, and other advanced functions.

You can also set the event configuration for access control and display access control points and zones on E-map.

Note: For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings.

Click  in the control panel, and check **Access Control** to add the Access Control module to the control panel.

Click  to enter the Access Control module.



Before you start:

For the first time opening the Access Control module, the following dialog will pop up and you are required to select the scene according to the actual needs.

You can select the scene as **Non-residence** and **Residence**.



Notes:

- Once the scene is configured, you cannot change it later.
- When you select **Non-Residence** mode, you cannot configure the Attendance Rule when adding person.

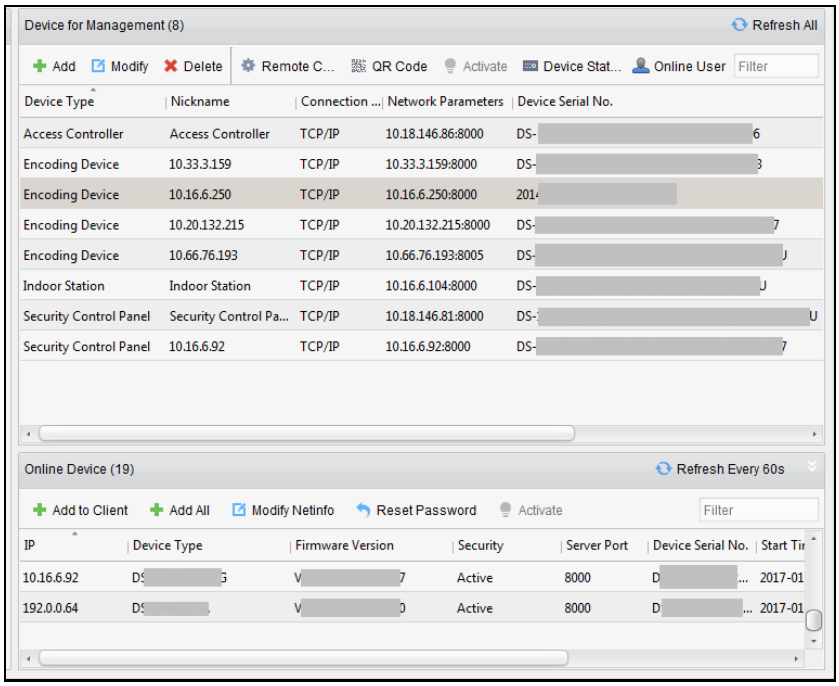
The Access Control module is composed of the following sub modules.

	Person and Card	Managing the organizations, persons, and assigning cards to persons.
	Schedule and Template	Configuring the week schedule, holiday group, and setting the template.
	Permission	Assigning access control permissions to persons and applying to the devices.
	Advanced Function	Providing advanced functions including access control parameters settings, card reader authentication, opening door with first card, anti-passing back, multi-door interlocking, and authentication password.
	Video Intercom	Video intercom between client and resident, searching the dial log, and releasing notice.
	Search	Searching history events of access control; Searching call logs, unlocking logs, and released notices.
	Device Management	Managing the access control devices and video intercom devices.

Note: In this chapter, we only introduce the operations about access control.

7.4.1 Adding Access Control Device

Click  in the Access Control module to enter the following interface.



Note: After adding the device, you should check the device arming status in **Tool** – **Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, refer *7.12 Arming Control*.

Creating Password

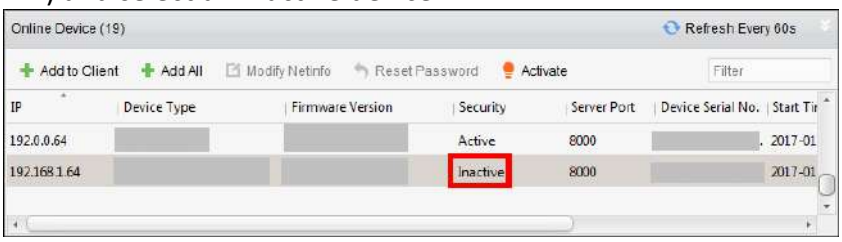
Purpose:

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

Note: This function should be supported by the device.

Steps:

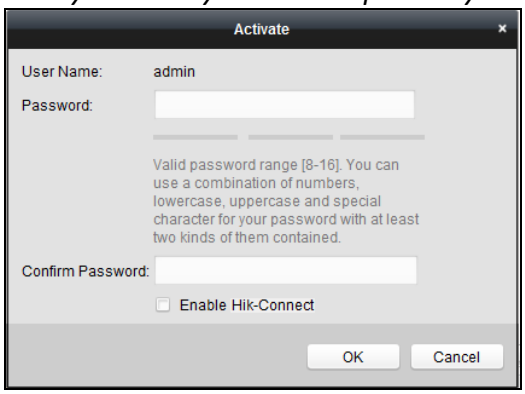
1. Enter the Device Management page.
2. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.



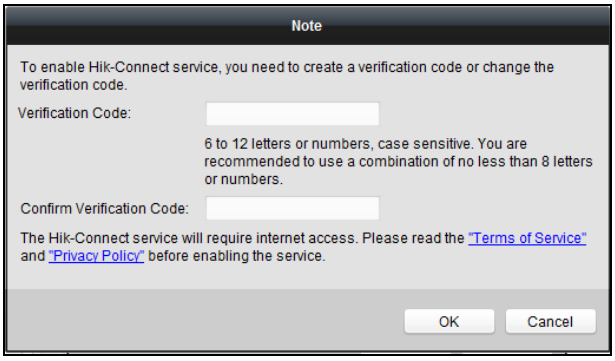
3. Click the **Activate** button to pop up the Activation interface.
4. Create a password in the password field, and confirm the password.

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,*

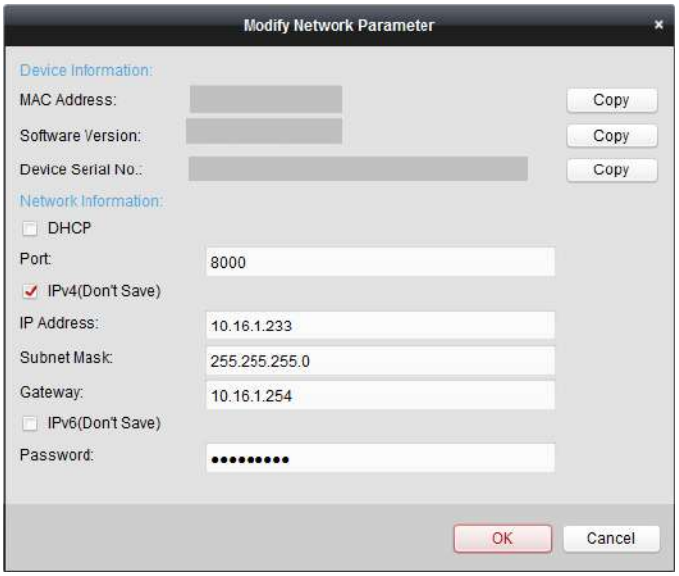
resetting the password monthly or weekly can better protect your product.



5. (Optional) Enable Hik-Connect service when activating the device if the device supports.
   1) Check **Enable Hik-Connect** checkbox to pop up the Note dialog.



   2) Create a verification code.
   3) Confirm the verification code.
   4) Click **Terms of Service** and **Privacy Policy** to read the requirements.
   5) Click **OK** to enable the Hik-Connect service.
6. Click **OK** to activate the device.
   A “The device is activated.” window pops up when the password is set successfully.
7. Click **Modify Netinfo** to pop up the Modify Network Parameter interface.
   Note: This function is only available on the **Online Device** area. You can change the device IP address to the same subnet with your computer if you need to add the device to the software.
8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of DHCP.
9. Input the password set in step 4 and click **OK** to complete the network settings.



Adding Online Device

Purpose:

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

Note: You can click to hide the **Online Device** area.



Steps:

1. Select the devices to be added from the list.

   Note: For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, please refer to *Chapter 5 Activating the Access Control Terminal.*

2. Click **Add to Client** to open the device adding dialog box.
3. Input the required information.

   Nickname: Edit a name for the device as you want.

   Address: Input the device's IP address. The IP address of the device is obtained automatically in this adding mode.

   Port: Input the device port No. The default value is *8000*.

   User Name: Input the device user name. By default, the user name is *admin*.

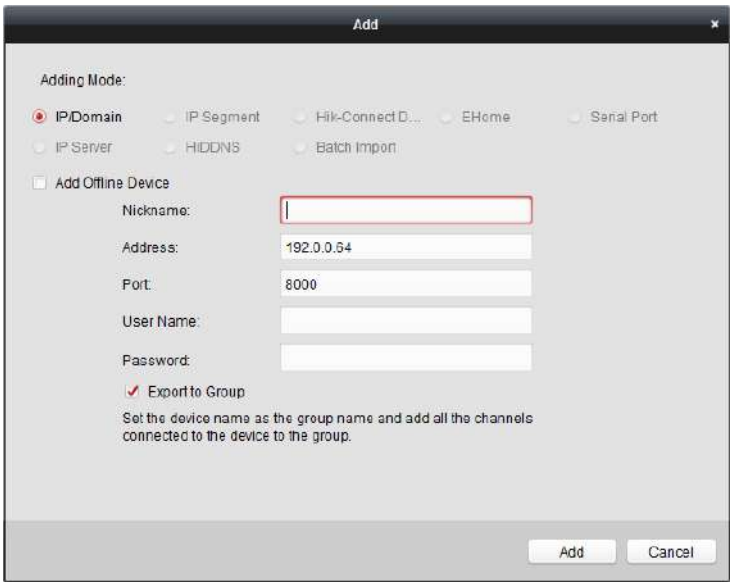
   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a

minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.

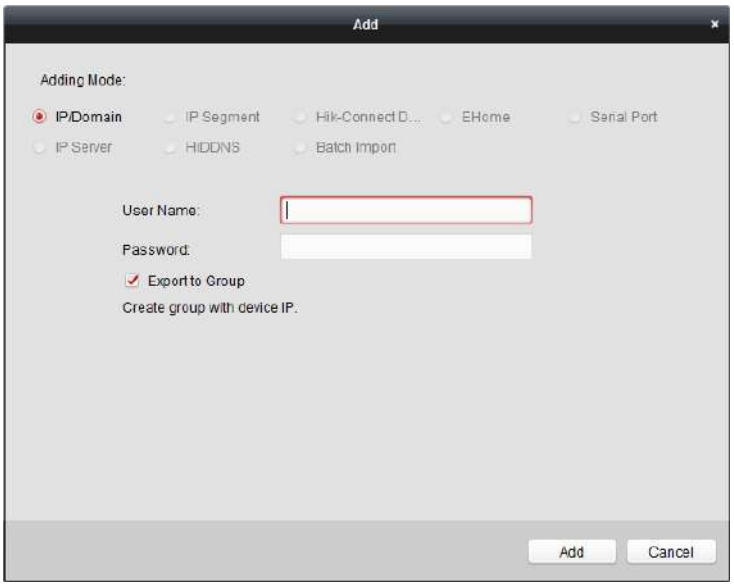


➢ Adding Multiple Online Device

If you want to add multiple online devices to the client software, click and hold *Ctrl* key to select multiple devices, and click **Add to Client** to open the device adding dialog box. In the pop-up message box, enter the user name and password for the devices to be added.

➢ Adding All Online Devices

If you want to add all the online devices to the client software, click **Add All** and click **OK** in the pop-up message box. Then enter the user name and password for the devices to be added.



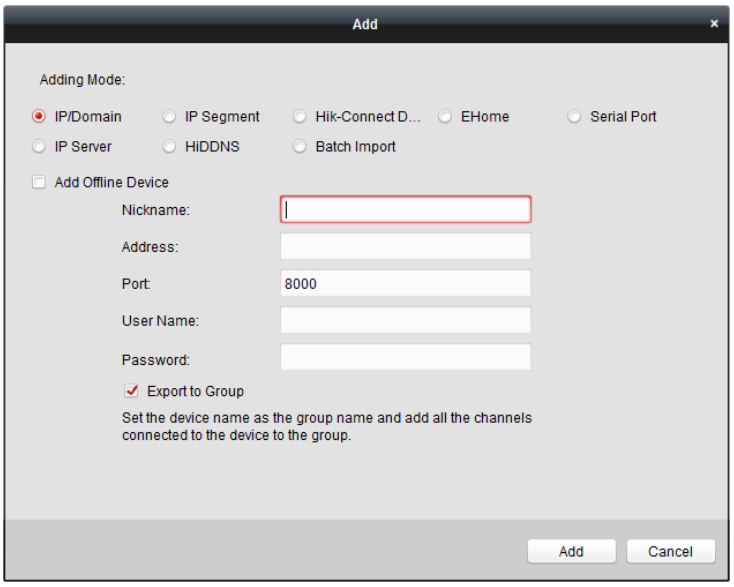
Adding Devices by IP or Domain Name

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP/Domain** as the adding mode.
3. Input the required information.
   Nickname: Edit a name for the device as you want.
   Address: Input the device's IP address or domain name.
   Port: Input the device port No.. The default value is *8000*.
   User Name: Input the device user name. By default, the user name is *admin*.
   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.



Adding Devices by IP Segment

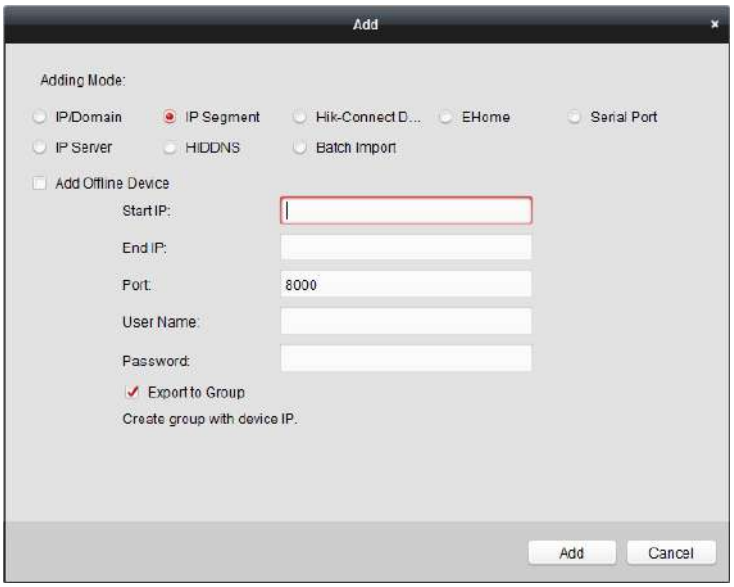
Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP Segment** as the adding mode.
3. Input the required information.
   Start IP: Input a start IP address.
   End IP: Input an end IP address in the same network segment with the start IP.
   Port: Input the device port No.. The default value is *8000*.
   User Name: Input the device user name. By default, the user name is *admin*.
   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
5. Click **Add**.
   You can add the device which the IP address is between the start IP and end IP to the device

list.



Adding Devices by Hik-Connect Domain

Purpose:

You can add the devices connected via Hik-Connect by inputting the Hik-Connect account and password.

Before you start: Add the devices to Hik-Connect account via iVMS-4200, iVMS-4500 Mobile Client, or Hik-Connect first. For details about adding the devices to Hik-Connect account via iVMS-4200, refer to *the User Manual of iVMS-4200 Client Software.*

➢ Add Single Device

Steps:

1. Click **Add** to open the device adding dialog.
2. Select **Hik-Connect Domain** as the adding mode.
3. Select **Single Adding**.
4. Input the required information.

   Nickname: Edit a name for the device as you want.

   Device Serial No.: Input the device serial No.

   User Name: Input the device user name. By default, the user name is *admin*.

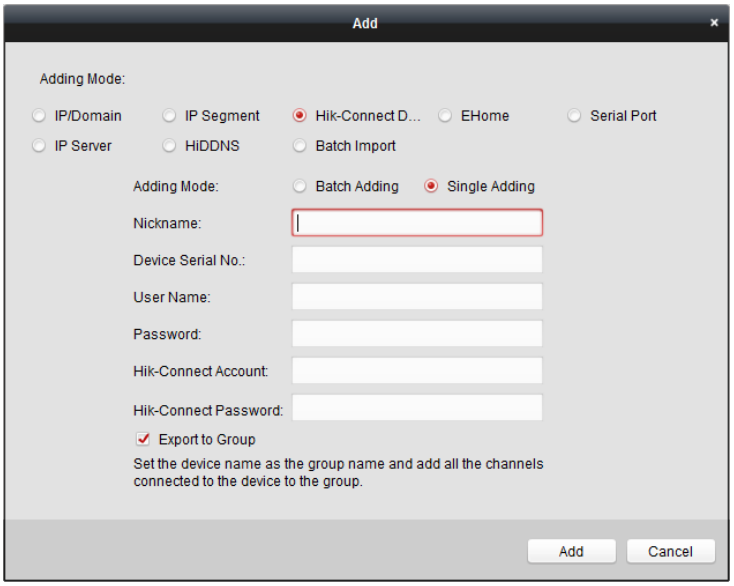
   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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.

   Hik-Connect Account: Input the Hik-Connect account.

   Hik-Connect Password: Input the Hik-Connect password.

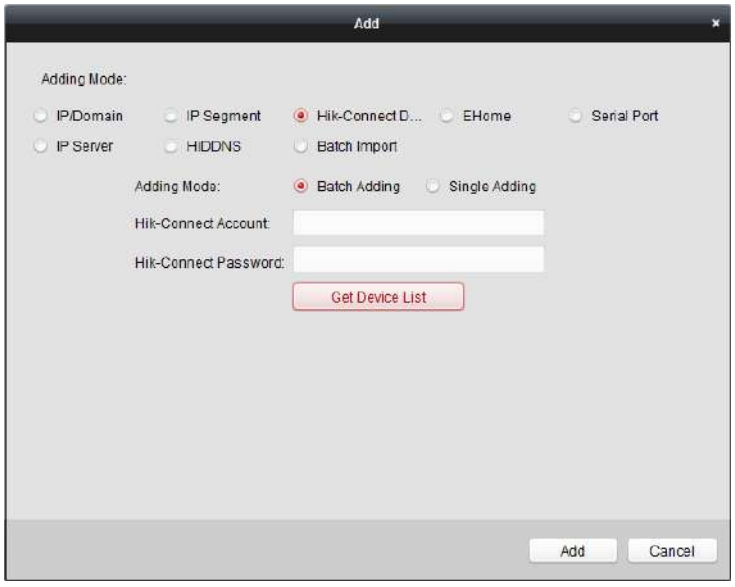
5. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
6. Click **Add** to add the device.



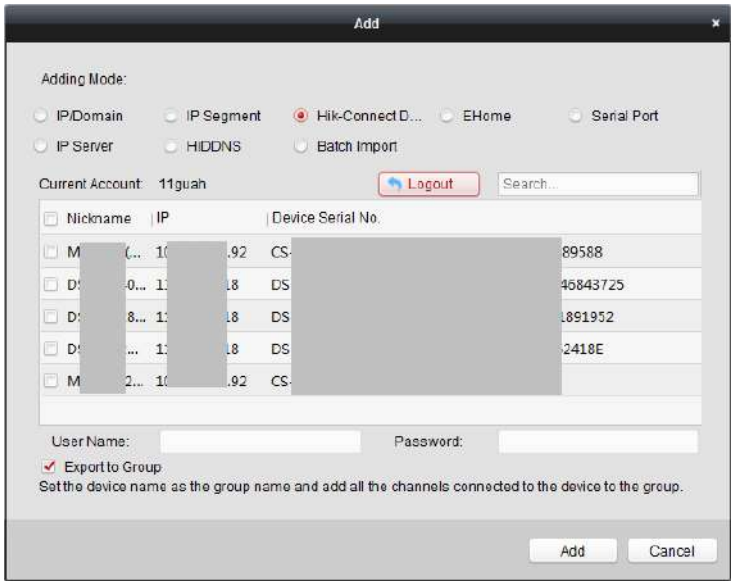
Add Devices in Batch

Steps:

1. Click **Add** to open the device adding dialog.



2. Select **Hik-Connect Domain** as the adding mode.
3. Select **Batch Adding**.
4. Input the required information.
   Hik-Connect Account: Input the Hik-Connect account.
   Hik-Connect Password: Input the Hik-Connect password.
5. Click **Get Device List** to show the devices added to Hik-Connect account.



6. Check the checkbox(es) to select the device as desired.
7. Input the user name and password for the devices to be added.
8. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
9. Click **Add** to add the devices.

Adding Devices by EHome Account

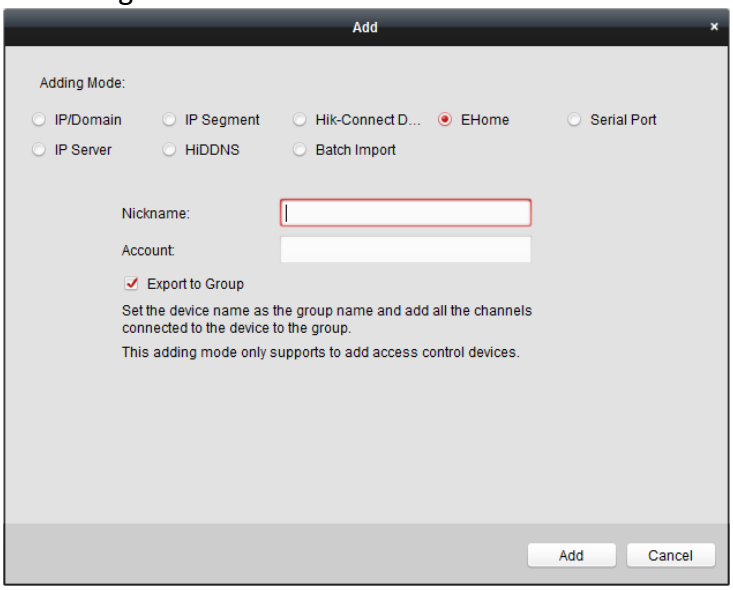
Purpose:

You can add access control device connected via EHome protocol by inputting the EHome account.

Before you start: Set the network center parameter first. For details, refer to *Chapter 7.4.4 Network Settings.*

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **EHome** as the adding mode.



3. Input the required information.

Nickname: Edit a name for the device as you want.
Account: Input the account name registered on EHome protocol.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.

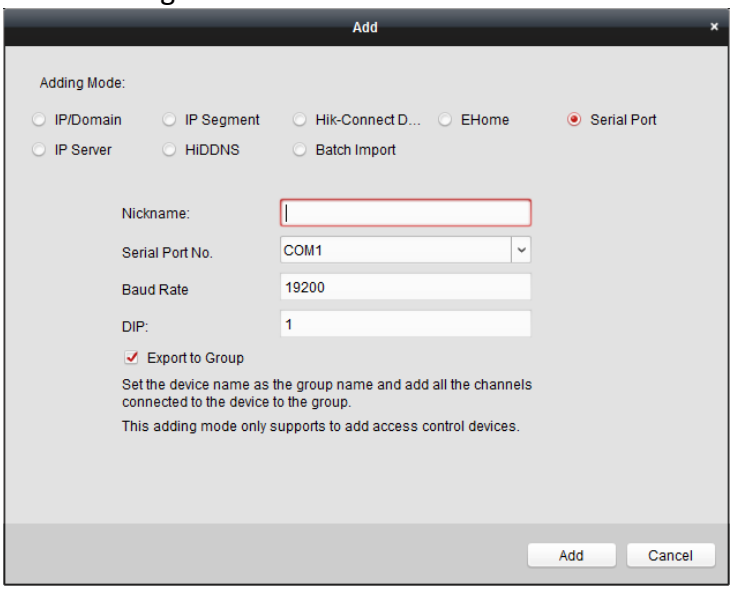
Adding Devices by Serial Port

Purpose:

You can add access control device connected via serial port.

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **Serial Port** as the adding mode.



3. Input the required information.
   Nickname: Edit a name for the device as you want.
   Serial Port No.: Select the device's connected serial port No.
   Baud Rate: Input the baud rate of the access control device.
   DIP: Input the DIP address of the device.
4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.

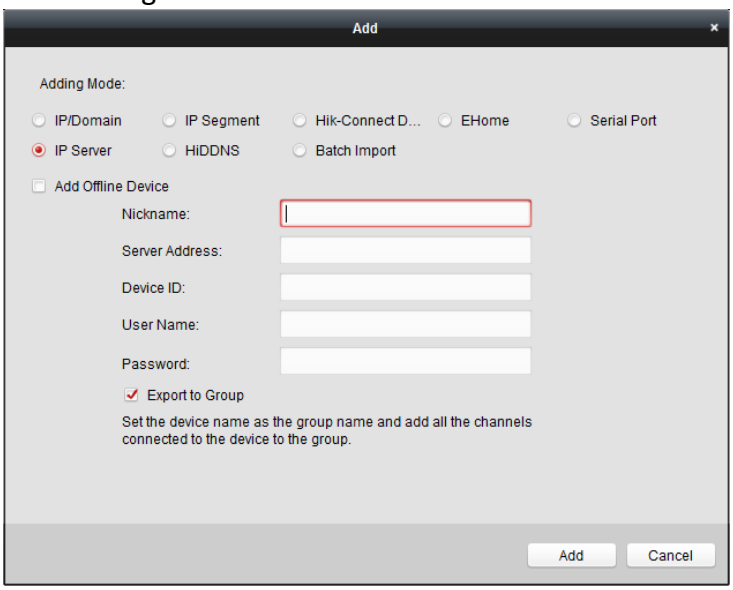
3) Click **Add**.
When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

Adding Devices by IP Server

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **IP Server** as the adding mode.



3. Input the required information.
Nickname: Edit a name for the device as you want.
Server Address: Input the IP address of the PC that installs the IP Server.
Device ID: Input the device ID registered on the IP Server.
User Name: Input the device user name. By default, the user name is *admin*.
Password: Input the device password.



The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name.
You can import all the channels of the device to the corresponding group by default.
Note: iVMS-4200 also provides a method to add the offline devices.
1) Check the **Add Offline Device** checkbox.
2) **I**nput the required information, including the device channel number and alarm input number.
3) Click **Add**.

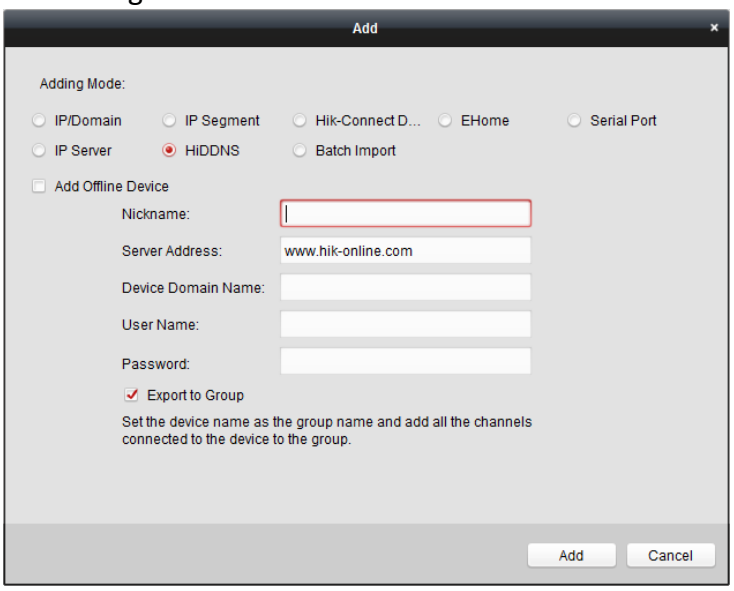
When the offline device comes online, the software will connect it automatically.

5. Click **Add** to add the device.

Adding Devices by HiDDNS

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **HiDDNS** as the adding mode.



3. Input the required information.
   Nickname: Edit a name for the device as you want.
   Server Address: *www.hik-online.com*.
   Device Domain Name: Input the device domain name registered on HiDDNS server.
   User Name: Input the device user name. By default, the user name is *admin*.
   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices.
   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

5. Click **Add** to add the device.

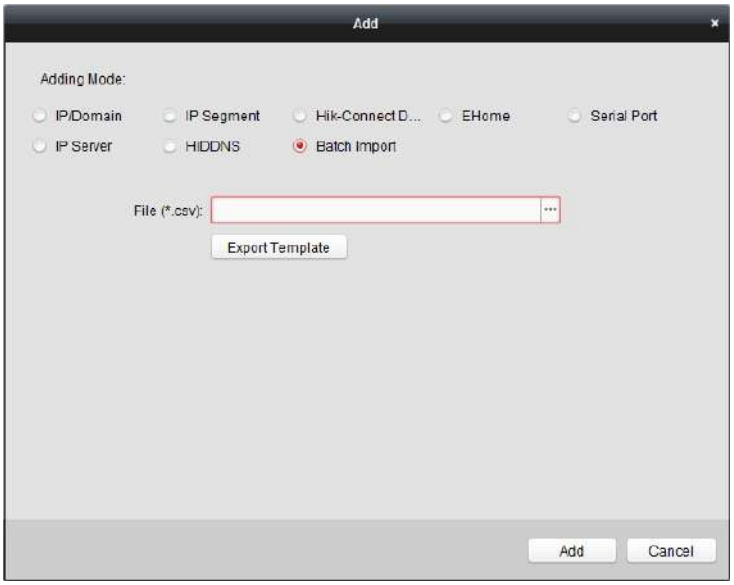
Importing Devices in Batch

Purpose:

The devices can be added to the software in batch by inputting the device information in the pre-defined CSV file.

Steps:

1. Click **Add** to open the device adding dialog box.
2. Select **Batch Import** as the adding mode.



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

   Nickname: Edit a name for the device as you want.

   Adding Mode: You can input 0, 2, 3, 4, 5, or 6 which indicated different adding modes. 0 indicates that the device is added by IP address or domain name; 2 indicates that the device is added via IP server; 3 indicates that the device is added via HiDDNS; 4 indicates that the device is added via EHome protocol; 5 indicates that the device is added by serial port; 6 indicates that the device is added via Hik-Connect Domain.

   Address: Edit the address of the device. If you set 0 as the adding mode, you should input the IP address or domain name of the device; if you set 2 as the adding mode, you should input the IP address of the PC that installs the IP Server; if you set 3 as the adding mode, you should input *www.hik-online.com*.

   Port: Input the device port No.. The default value is *8000*.

   Device Information: If you set 0 as the adding mode, this field is not required; if you set 2 as the adding mode, input the device ID registered on the IP Server; if you set 3 as the adding mode, input the device domain name registered on HiDDNS server; if you set 4 as the adding mode, input the EHome account; if you set 6 as the adding mode, input the device serial No.

   User Name: Input the device user name. By default, the user name is *admin*.

   Password: Input the device password.



The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something 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.

Add Offline Device: You can input 1 to enable adding the offline device, and then the software will automatically connect it when the offline device comes online. 0 indicates disabling this function.

Export to Group: You can input 1 to create a group by the device name (nickname). All the channels of the device will be imported to the corresponding group by default. 0 indicates disabling this function.

Channel Number: If you set 1 for Add Offline Device, input the channel number of the device. If you set 0 for Add Offline Device, this field is not required.

Alarm Input Number: If you set 1 for Add Offline Device, input the alarm input number of the device. If you set 0 for Add Offline Device, this field is not required.

Serial Port No.: If you set 5 as the adding mode, input the serial port No. for the access control device.

Baud Rate: If you set 5 as the adding mode, input the baud rate of the access control device.

DIP: If you set 5 as the adding mode, input the DIP address of the access control device.

Hik-Connect Account: If you set 6 as the adding mode, input the Hik-Connect account.

Hik-Connect Password: If you set 6 as the adding mode, input the Hik-Connect password.

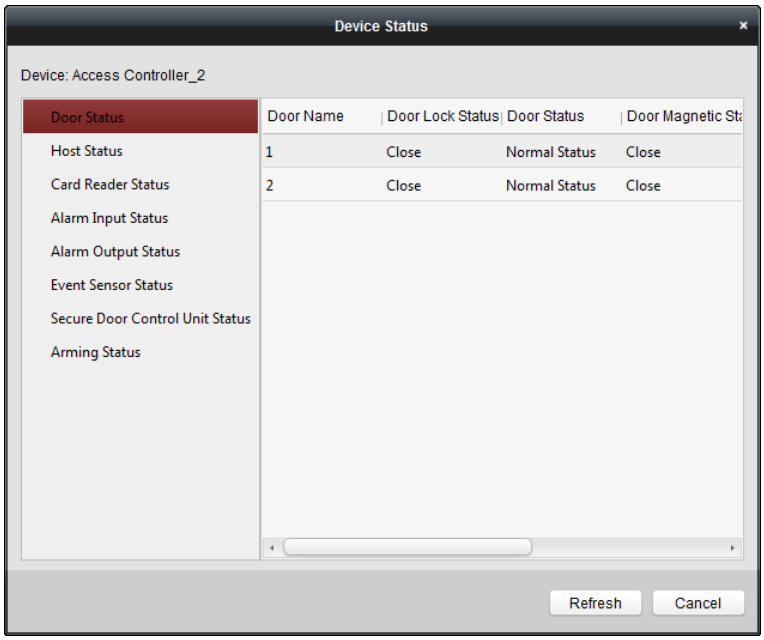
5. Click ··· and select the template file.
6. Click **Add** to import the devices.

The devices will be displayed on the device list for management after added successfully. You can check the resource usage, HDD status, recording status, and other information of the added devices on the list.

Click **Refresh All** to refresh the information of all added devices. You can also input the device name in the filter field for search.

7.4.2 Viewing Device Status

In the device list, you can select the device and then click **Device Status** button to view its status.



Note: The interface may different from the picture displayed above. Refer to the actual interface when adopting this function.

Door Status: The status of the connected door.

Host Status: The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, and Host Anti-Tamper Status.

Card Reader Status: The status of card reader.

Note: If you use the card reader with RS-485 connection, you can view the status of online or offline. If you use the card reader with Wiegand connection, you can view the status of offline.

Alarm Input Status: The alarm input status of each port.

Alarm Output Status: The alarm output status of each port.

Event Sensor Status: The event sensor status of each port.

Secure Door Control Unit Status: The online status and tamper status of the Secure Door Control Unit.

Arming Status: The status of the device.

7.4.3 Editing Basic Information

Purpose:

After adding the access control device, you can edit the device basic information.

Steps:

1. Select the device in the device list.
2. Click **Modify** to pop up the modifying device information window.
3. Click **Basic Information** tab to enter the Basic Information interface.



4. Edit the device information, including the adding mode, the device name, the device IP address, port No., user name, and the password.

7.4.4 Network Settings

Purpose:

After adding the access control device, you can set the uploading mode, and set the network center and wireless communication center.

Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **Network Settings** tab to enter the network settings interface.

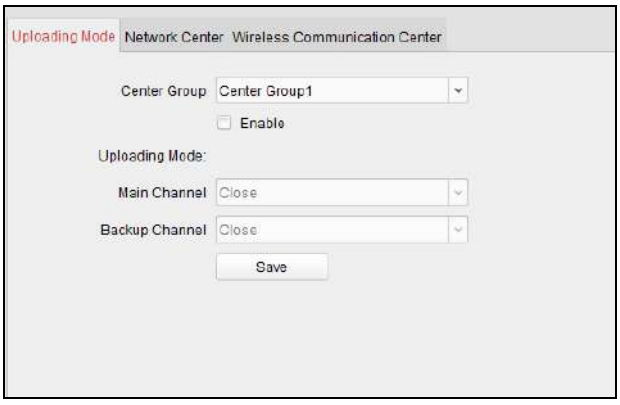
Uploading Mode Settings

Purpose：

You can set the center group for uploading the log via the EHome protocol.

Steps:

1. Click the **Uploading Mode** tab.



2. Select the center group in the dropdown list.
3. Check the **Enable** checkbox to enable the selected center group.
4. Select the uploading mode in the dropdown list. You can enable **N1/G1** for the main channel and the backup channel, or select **Close** to disable the main channel or the backup channel.
   Note: The main channel and the backup channel cannot enable N1 or G1 at the same time.

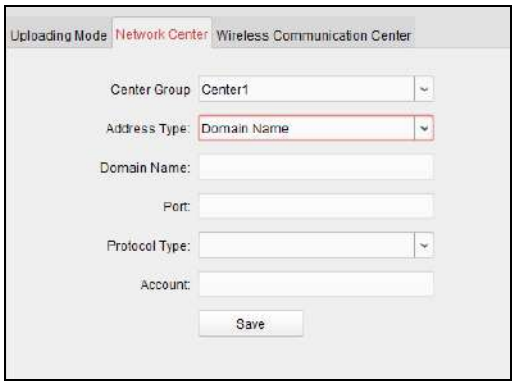
5. Click **Save** button to save parameters.

Network Center Settings

You can set the account for EHome protocol in Network Settings page. Then you can add devices via EHome protocol.

Steps:

1. Click the **Network Center** tab.



2. Select the center group in the dropdown list.
3. Select the address type.
4. Set the IP address/domain name.
5. Set the port No. for EHome protocol. By default, the port No. is 7660.
6. Select the protocol type as EHome.
7. Set an account name for the network center.
8. Click **Save** button to save parameters.

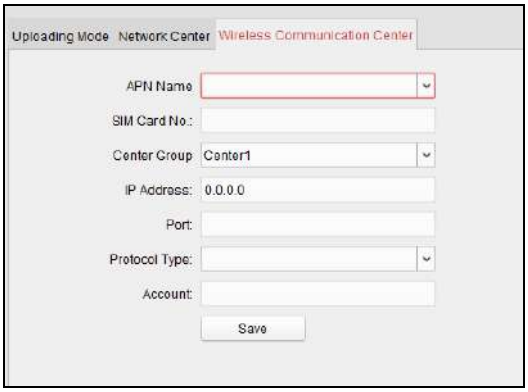
Notes:

- The account should contain 1 to 32 characters and only letters and numbers are allowed.
- The port No. of the wireless network and wired network should be consistent with the port No. of EHome.
- You can set the domain name in Enable NTP area *Time* section in Remote Configuration. For details, refer to *Time* in *7.4.9 Remote Configuration*.

Wireless Communication Center Settings

Steps:

1. Click the **Wireless Communication Center** tab.



2. Select the APN name as CMNET or UNINET.
3. Input the SIM Card No.
4. Select the center group in the dropdown list.
5. Input the IP address and port No.
6. Select the protocol type as EHome. By default, the port No. for EHome is 7660.
7. Set an account name for the network center. A consistent account should be used in one platform.
8. Click **Save** button to save parameters.

Note: The port No. of the wireless network and wired network should be consistent with the port No. of EHome.

7.4.5 Capture Settings

You can set the parameters of capture linkage and manual capture.
Select the device in the device list, and click **Modify** to pop up the modifying device information window.
Click **Capture Settings** tab to enter the capture settings interface.

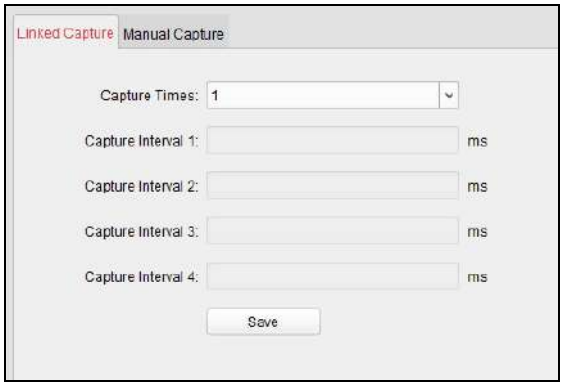
Notes:

- The **Capture Settings** should be supported by the device.
- Before setting the capture setting, you should configure the storage server for picture storage.

Linked Capture

Steps:

1. Select the **Linked Capture** tab.



2. Set the linked capture times once triggered.
   Set the capture interval according to the capture times.
3. Click **Save** to save the settings.

Manual Capture

Steps:

1. Select the **Manual Capture** tab.



2. Select the resolution of the captured pictures from the dropdown list.
   Note: The supported resolution types are CIF, QCIF, 4CIF/D1, SVGA, HD720P, VGA, WD1, and AUTO.
3. Select the picture quality as High, Medium, or Low.
4. Click **Save** to save the settings.
5. You can click **Restore Default Value** to restore the parameters to default settings.

7.4.6 RS-485 Settings

Purpose:

You can set the RS-485 parameters including the serial port, the baud rate, the data bit, the stop bit, the parity type, the communication mode, and the working mode.

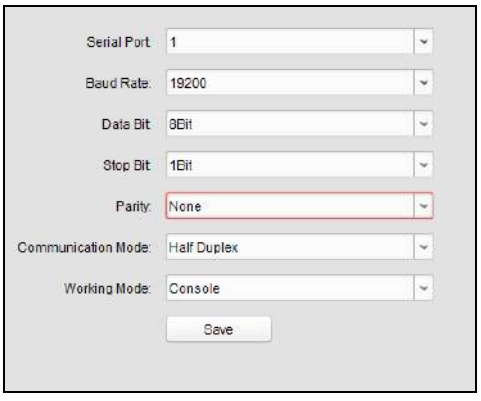
Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **RS-485 Settings** tab to enter the RS-485 settings interface.

Note: The RS-485 Settings should be supported by the device.

Steps:

1. Click **RS-485 Settings** tab to enter the RS-485 settings interface.



2. Select the serial No. of the port from the dropdown list to set the RS-485 parameters.
3. Set the baud rate, data bit, the stop bit, parity type, communication mode, and work mode in the dropdown list.
4. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

Note: After changing the working mode, the device will be rebooted. A prompt will be popped up after changing the working mode.

7.4.7 Wiegand Settings

Purpose:

You can set the Wiegand channel and the communication mode.

Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **Wiegand-485 Settings** tab to enter the Wiegand settings interface.

Note: The Wiegand Settings should be supported by the device.

Steps:

1. Click the **Wiegand Settings** tab to enter the Wiegand Settings interface.



2. Select the Wiegand channel No. and the communication mode in the dropdown list.
   If you set the **Communication Direction** as **Send**, you are required to set the Wiegand Mode as Wiegand 26 or Wiegand 34.
3. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

Note: After changing the communication direction, the device will be rebooted. A prompt will be popped up after changing the communication direction.

7.4.8 M1 Card Encryption

The M1 Card Encryption function increases the authentication security level, which should be applied together with the card enrollment station of our company via the client software or the web client. After issuing the card, you can set the M1 card encryption function on the controller.

Notes:

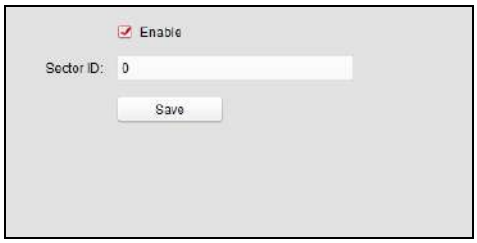
- The function should be supported by the device.
- For details about issuing card, refer to *Adding Person (Card)* in *7.5.2 Person Management.*

Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **M1 Card Encryption** tab to enter the M1 Card Encryption interface.

Steps:

1. In the M1 Card Encryption interface, check **Enable** checkbox to enable the M1 card encryption function.



2. Set the sector ID.
3. Click **Save** to save the settings.

   Note: The sector ID ranges from 1 to 100.

7.4.9 Remote Configuration

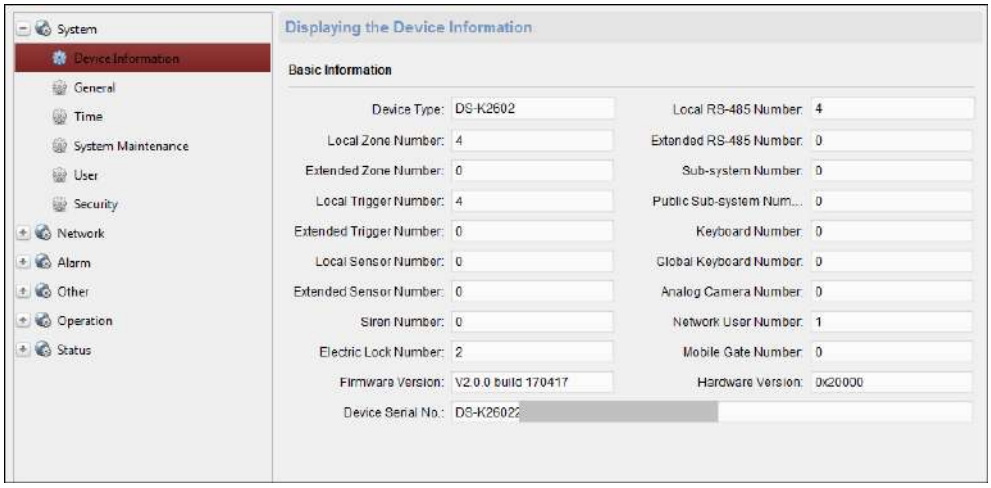
Purpose:

In the device list, select the device and click **Remote Configuration** button to enter the remote configuration interface. You can set the detailed parameters of the selected device.

Checking Device Information

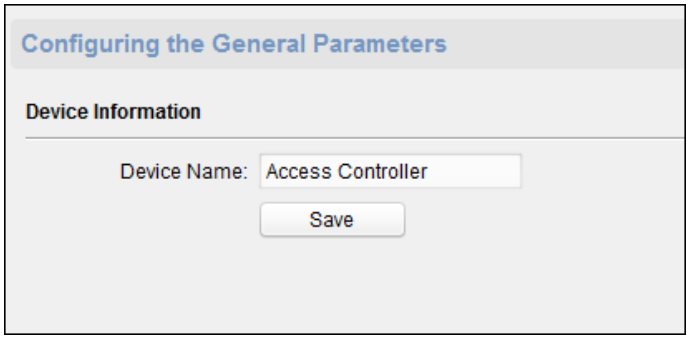
Steps:

1. In the device list, you can click **Remote Configuration** to enter the remote configuration interface.
2. Click **System** -> **Device Information** to check the device basic information and the device version information.



Editing Device Name

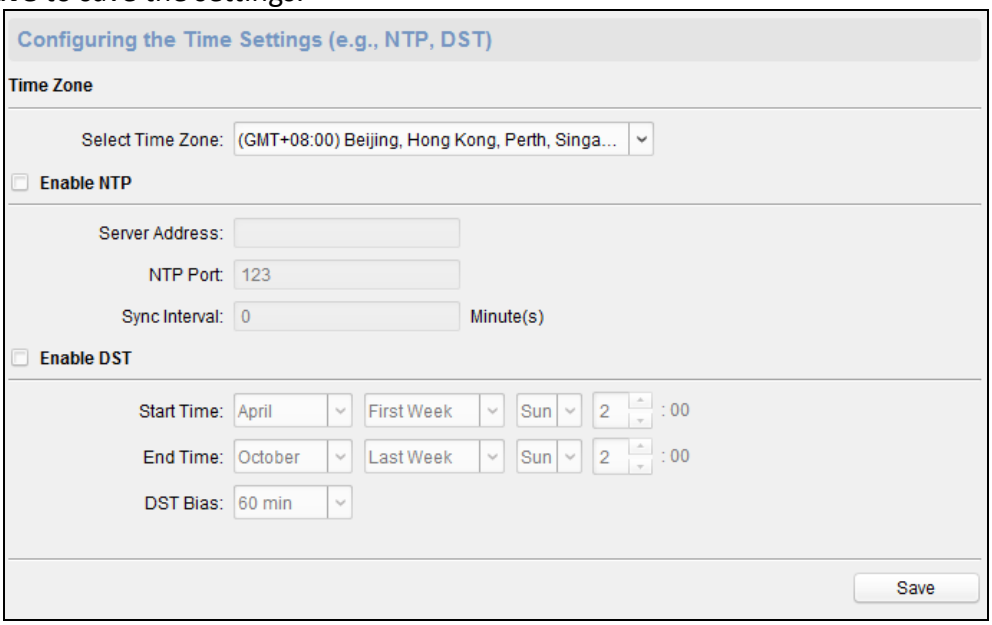
In the Remote Configuration interface, click **System** -> **General** to configure the device name and overwrite record files parameter. Click **Save** to save the settings.



Editing Time

Steps:

1. In the Remote Configuration interface, click **System** -> **Time** to configure the time zone.
2. (Optional) Check **Enable NTP** and configure the NTP server address, the NTP port, and the synchronization interval.
3. (Optional) Check **Enable DST** and configure the DST star time, end time and the bias.
4. Click **Save** to save the settings.

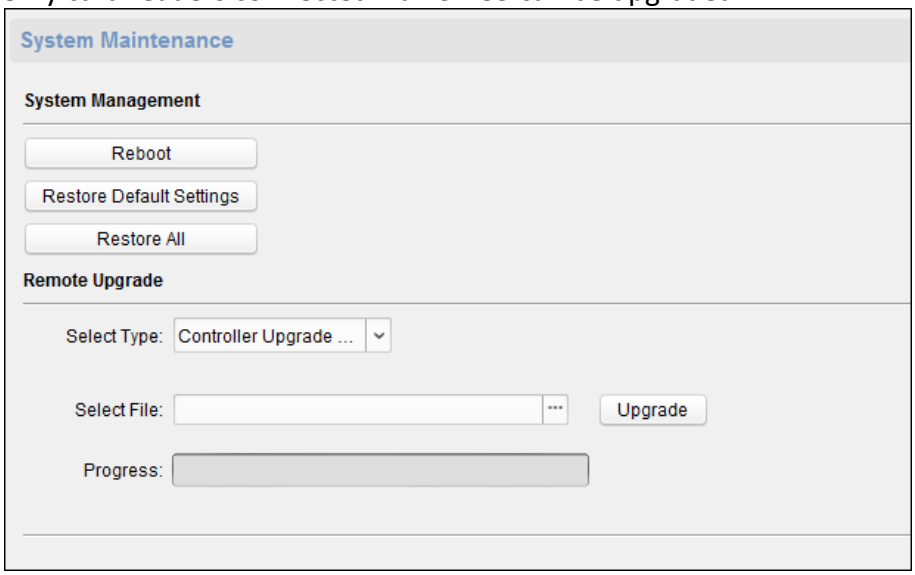


Setting System Maintenance

Steps:

1. In the Remote Configuration interface, click **System** -> **System Maintenance**.
2. Click **Reboot** to reboot the device.
   Or click **Restore Default Settings** to restore the device settings to the default ones, excluding the IP address.
   Or click **Restore All** to restore the device parameters to the default ones. The device should be activated after restoring.
   Note: The configuration file contains the device parameters.
3. You can also remote upgrade the device.
   1) In the Remote Upgrade part, select an upgrade file type in the dropdown list.
      You can select Controller Upgrade File or Card Reader Upgrade in the drop-down list.

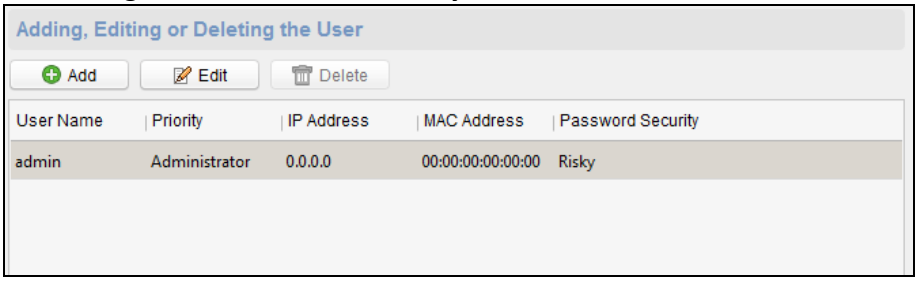
2) Click ··· to select the upgrade file.
3) Click **Upgrade** to start upgrading.
   Note: Only card readers connected via RS-485 can be upgraded.



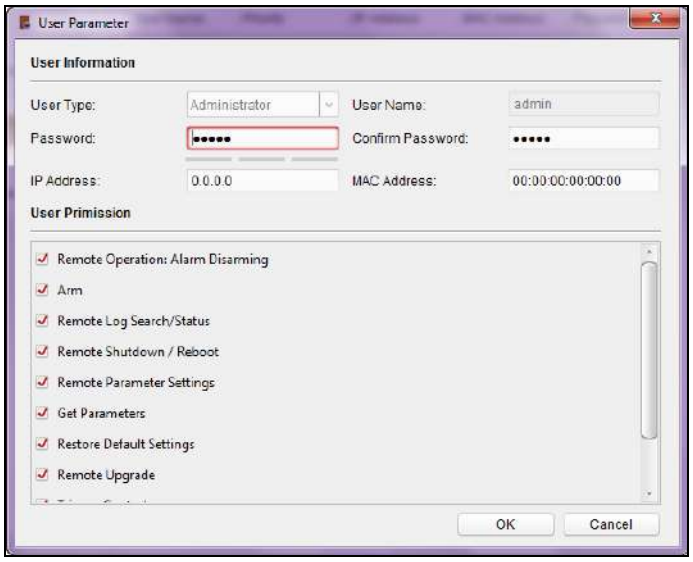
Managing User

Steps:

1. In the Remote Configuration interface, click **System** -> **User**.



2. Click **Add** to add the user (Do not support by the elevator controller.).
   Or select a user in the user list and click **Edit** to edit the user. You are able to edit the user password, the IP address, the MAC address and the user permission. Cilck **OK** to confirm editing.



Setting Security

Steps:

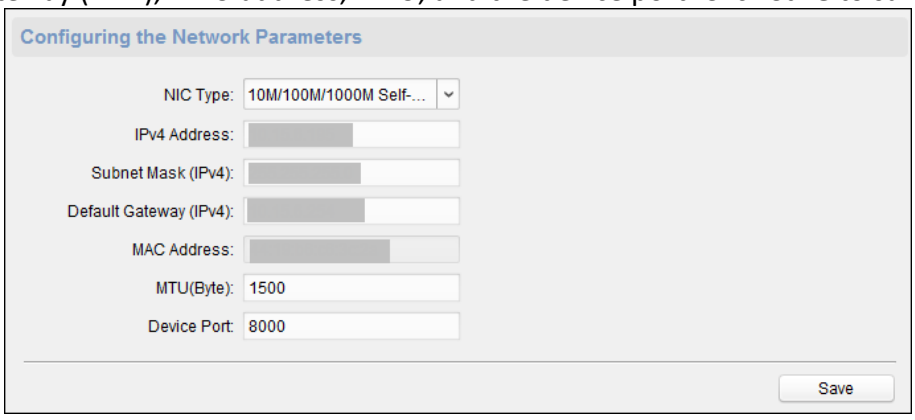
1. Click **System** -> **Security**.



2. Select the encryption mode in the dropdown list.
   You can select Compatible Mode or Encryption Mode.
3. Click **Save** to save the settings.

Configuring Network Parameters

Click **Network** -> **General**. You can configure the NIC type, the IPv4 address, the subnet mask (IPv4), the default gateway (IPv4), MTU address, MTU, and the device port. Click **Save** to save the settings.



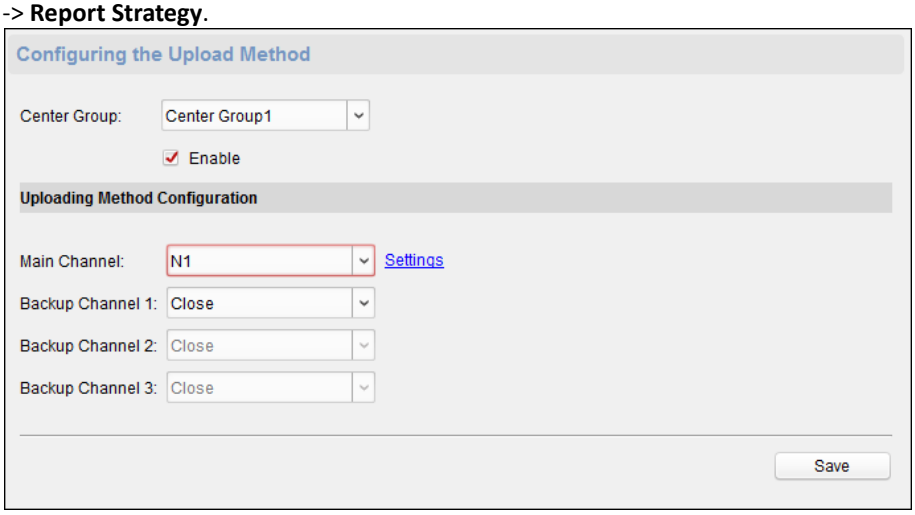
Configuring Upload Method

Purpose：

You can set the center group for uploading the log via the EHome protocol.

Steps:

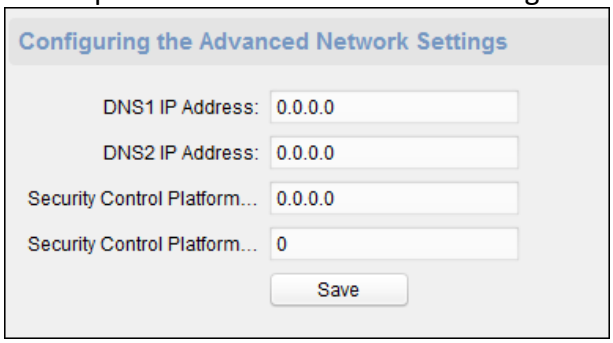
1. Click **Network** -> **Report Strategy**.



2. Select a Center Group from the drop-down list.
3. Check the **Enable** check box.
4. Set the uploading method.
   You can set the main channel and the backup channel.
5. Click **Settings** on the right of the channel field to set the detailed information.
6. Click **Save** to save the settings.

Configuring Advanced Network

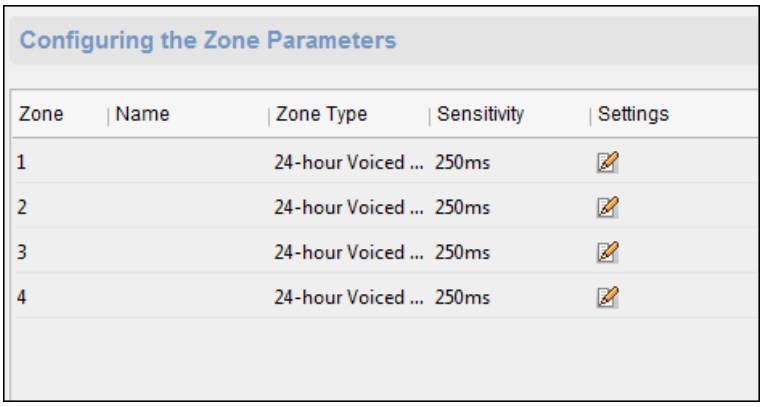
Click **Network** -> **Advanced Settings**. You can configure the DNS address 1, the DNS address 2, the alarm host IP and the alarm host port. Click **Save** to save the settings.



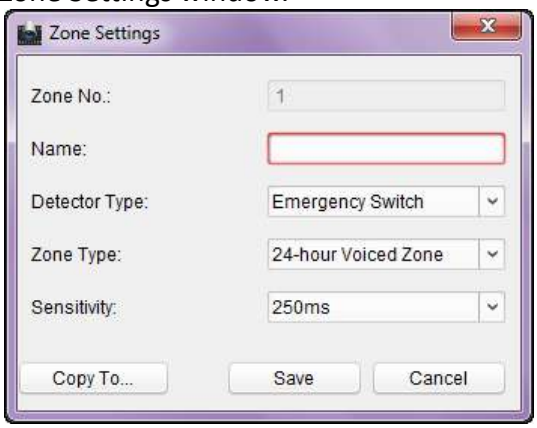
Configuring Zone Parameters

Step:

1. Click **Alarm** -> **Zone** to enter the Zone interface.



2. Click  to pop up the Zone Settings window.

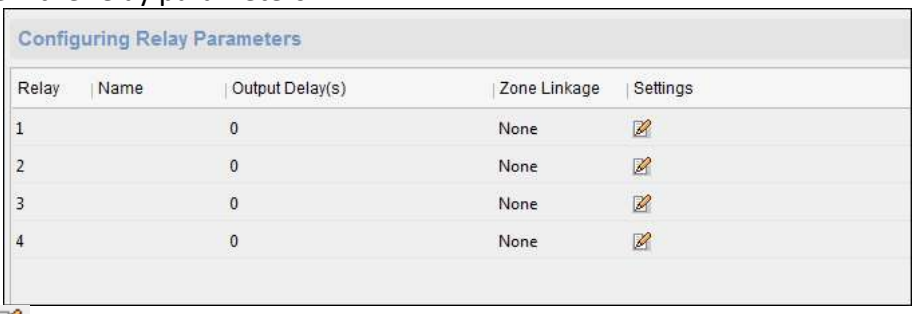


3. Set the zone name, the detector type, the zone type and the sensitivity.
4. Click **Save** to save the settings.
   Or click **Copy to...** to copy the parameters to other zones.

Configuring Relay Parameters

Steps:

1. Click **Alarm** -> **Relay**.
   You can view the relay parameters.

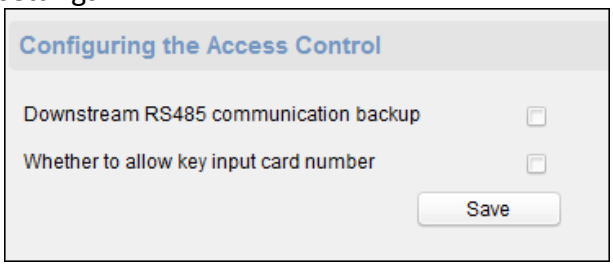


2. Click the  to pop up the Relay Parameters Settings window.
3. Set the relay name and the output delay.
4. Click **Save** to save the paramters.
   Or click **Copy to...** to copy the relay information to other relays.

Configuring Access Control Parameters

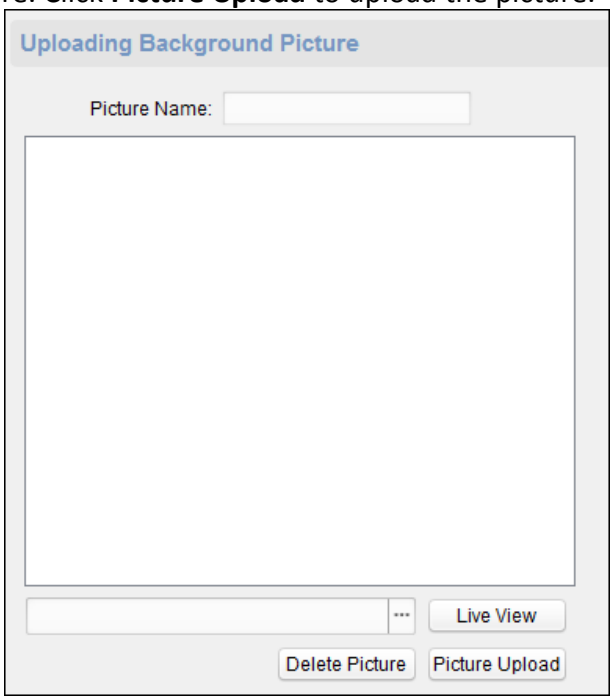
Steps:

1. In the Remote Configuration interface, click **Other** -> **Access Control Parameters**.
2. Select and check the **Downstream RS-485 Communication Backup** checkbox or the **Press Key to Input Card No.** checkbox.
3. Click **Save** to save the settings.



Uploading Background Picture

Click **Other** -> **Picture Upload**. Click ··· to select the picture from the local. You can also click **Live View** to preview the picture. Click **Picture Upload** to upload the picture.



Configuring Face Detection Parameters

Click **Other** -> **Face Detection**. You can check the **Enable** checkbox to enable the device face detection function.

Note: Only devices with video function support this function.

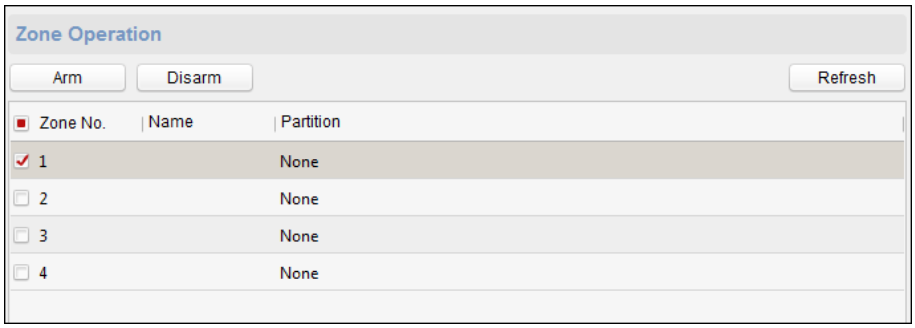


Operating Zone

Steps:

1. Click **Operation** -> **Zone**.

You can view the zone information.

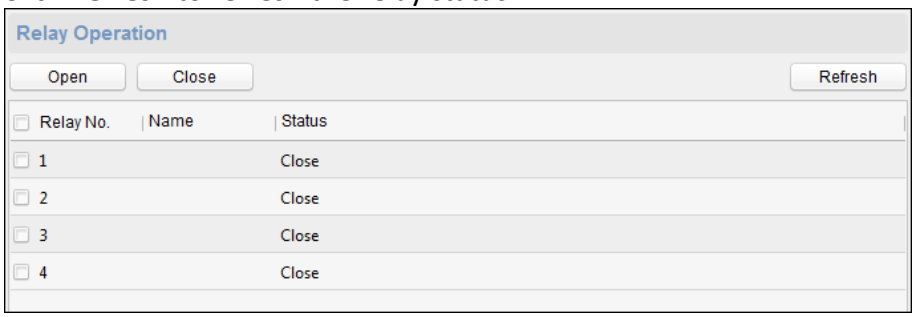


2. Check the zone checkbox.
3. Click **Arm** or **Disarm** to arm or disarm the zone.
4. (Optional) click **Refresh** to refresh the zone status.

Operating Relay

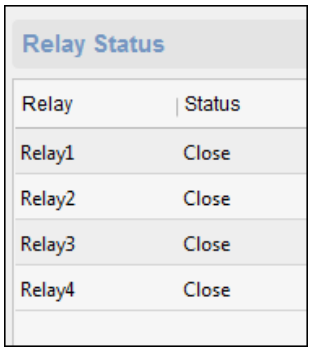
Steps:

1. Click **Operation** -> **Relay**.
   You can view the relay status.
2. Check the relay checkbox
3. Click **Open** or **Close** to open/close the relay.
4. (Optional) Click **Refresh** to refresh the relay status.



Viewing Relay Status

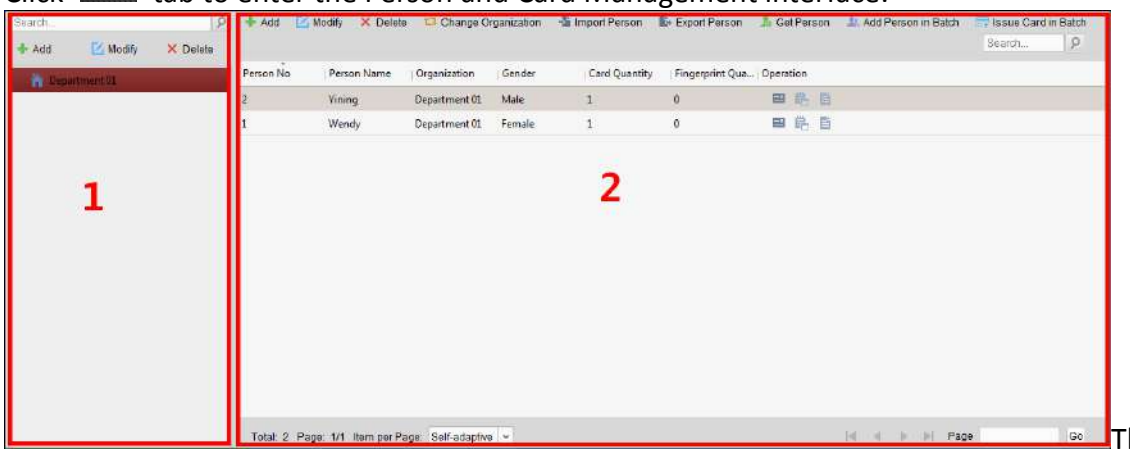
Click **Status** -> **Relay** to view the relay status.



7.5 Person and Card Management

You can add, edit, and delete the organization and person in Person and Card Management module.

Click  tab to enter the Person and Card Management interface.



The interface is divided into two parts: Organization Management and Person Management.

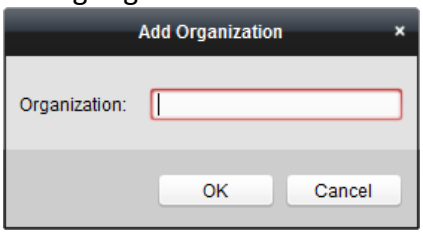
1	**Organization Management**	You can add, edit, or delete the organization as desired.
2	**Person Management**	After adding the organization, you can add the person to the organization and issue card to persons for further management.

7.5.1 Organization Management

Adding Organization

Steps:

1. In the organization list on the left, you should add a top organization as the parent organization of all organizations.
   Click **Add** button to pop up the adding organization interface.



2. Input the Organization Name as desired.
3. Click **OK** to save the adding.
4. You can add multiple levels of organizations according to the actual needs.
   To add sub organizations, select the parent organization and click **Add**.
   Repeat *Step 2* and *3* to add the sub organization.
   Then the added organization will be the sub-organization of the upper-level organization.

Note: Up to 10 levels of organizations can be created.

Modifying and Deleting Organization

You can select the added organization and click **Modify** to modify its name.
You can select an organization, and click **Delete** button to delete it.

Notes:

- 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.

7.5.2 Person Management

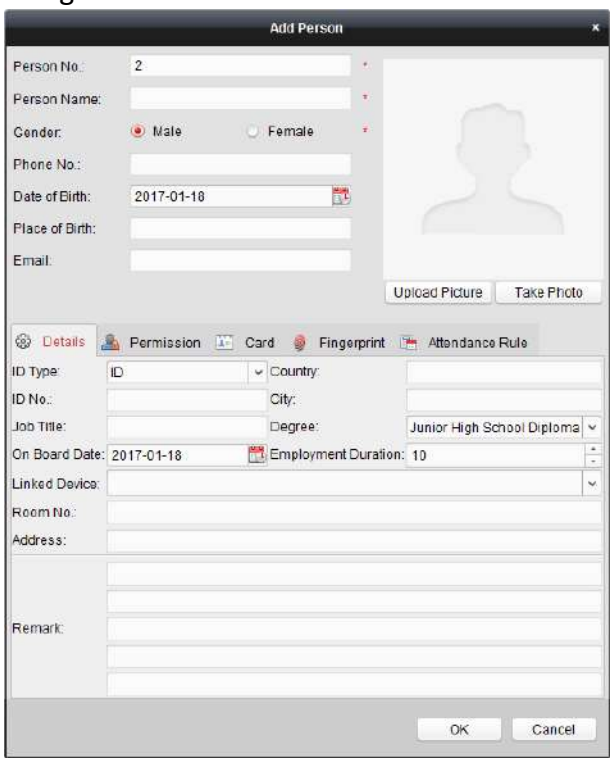
After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting persons information in batch, etc.
Note: Up to 10,000 persons or cards can be added.

Adding Person

Adding Person (Basic Information)

Steps:

1. Select an organization in the organization list and click **Add** button on the Person panel to pop up the adding person dialog.

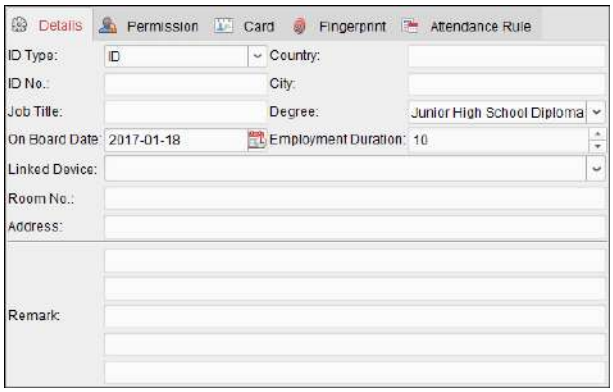


2. The Person No. will be generated automatically and is not editable.
3. Input the basic information including person name, gender, phone No., birthday details, and email address.
4. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
   Note: The picture should be in *.jpg format.
5. (Optional) You can also click **Take Phone** to take the person's photo with the PC camera.
6. Click **OK** to finish adding.

Adding Person (Detailed Information)

Steps:

1. In the Add Person interface, click **Details** tab.



2. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.
   - **Linked Device:** You can bind the indoor station to the person.
     Note: If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.
   - **Room No.:** You can input the room No. of the person.
3. Click **OK** to save the settings.

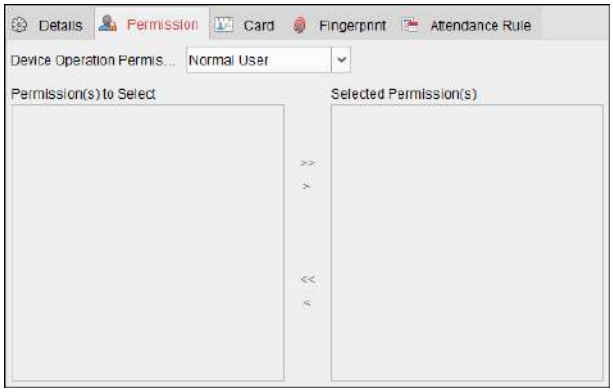
Adding Person (Permission)

You can assign the permissions (including operation permissions of access control device and access control permissions) to the person when adding person.

Note: For setting the access control permission, refer to *Chapter 7.7 Permission Configuration.*

Steps:

1. In the Add Person interface, click **Permission** tab.



2. In the Device Operation Role field, select the role of operating the access control device.
   Normal User: The person has the permission to check-in/out on the device, pass the access control point, etc.
   Administrator: The person has the normal user permission, as well as permission to configure the device, including adding normal user, etc.
3. In the Permission(s) to Select list, all the configured permissions display.
   Check the permission(s) checkbox(es) and click **>** to add to the Selected Permission(s) list.

(Optional) You can click **>>** to add all the displayed permissions to the Selected Permission(s) list.

(Optional) In the Selected Permission(s) list, select the selected permission and click **<** to remove it. You can also click **<<** to remove all the selected permissions.

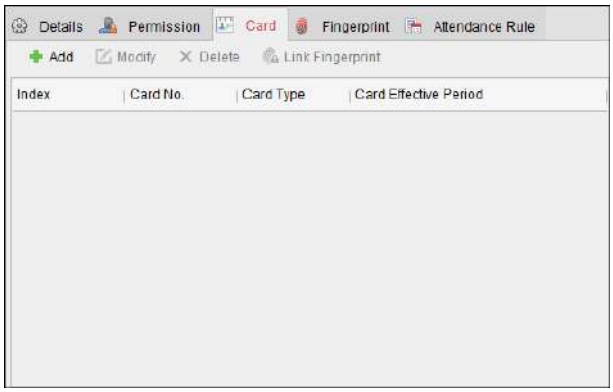
4. Click **OK** to save the settings.

Adding Person (Card)

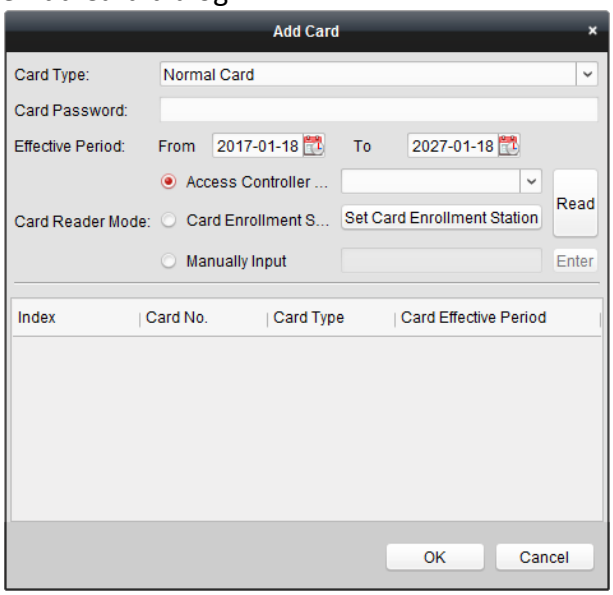
You can add card and issue the card to the person.

Steps:

1. In the Add Person interface, click **Card** tab.



2. Click **Add** to pop up the Add Card dialog.



3. Select the card type according to actual needs.
   - **Normal Card**
   - **Card for Door Extended Opening**: The door will remain open for the configured time period for the card holder.
   - **Card in Blocklist**: The card swiping action will be uploaded and the door cannot be opened.
   - **Patrol Card**: The card swiping action can used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
   - **Duress Card**: The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.

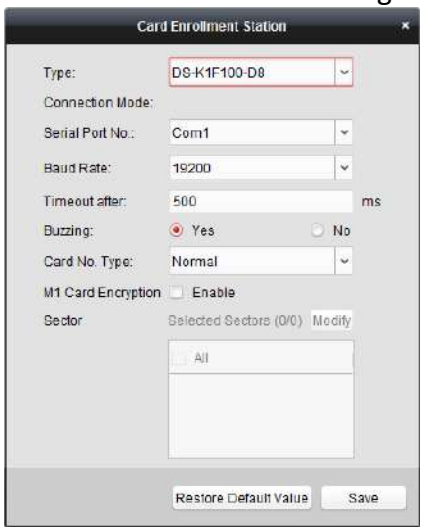
- **Super Card**: The card is valid for all the doors of the controller during the configured schedule.
- **Visitor Card**: The card is assigned for visitors. For the Visitor Card, you can set the **Max. Swipe Times**.

  Notes:
  - The Max. Swipe Times should be between 0 and 255. When your swiping card times is more than the configured times, card swiping will be invalid.
  - When set the times as 0, it means the card swiping is unlimited.

4. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

   Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, *Chapter 7.8.2 Card Reader Authentication.*
5. Click  to set the effective time and expiry time of the card.
6. Select the Card Reader Mode for reading the card No.
   - **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
   - **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.

     Note: The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



   2) Select the Card Enrollment Station type.

      Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

   3) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.

      If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.

4) Click **Save** button to save the settings.
You can click **Restore Default Value** button to restore the defaults.

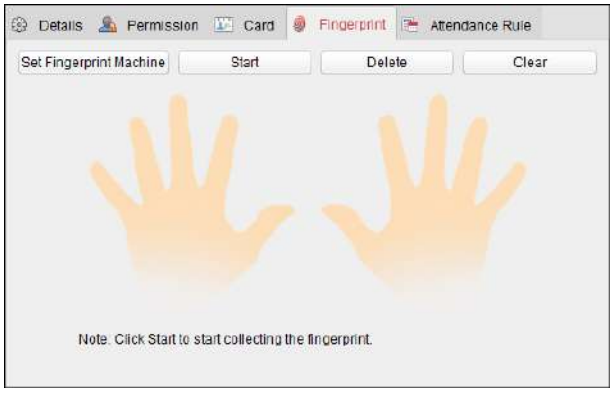
- **Manually Input:** Input the card No. and click **Enter** to input the card No.

7. Click **OK** and the card(s) will be issued to the person.
8. (Optional) You can select the added card and click **Edit** or **Delete** to edit or delete the card.
9. (Optional) You can click **Link Fingerprint** to link the card with the person's fingerprint, so that the person can place the finger on the scanner instead of swiping card when passing the door.
10. Click **OK** to save the settings.

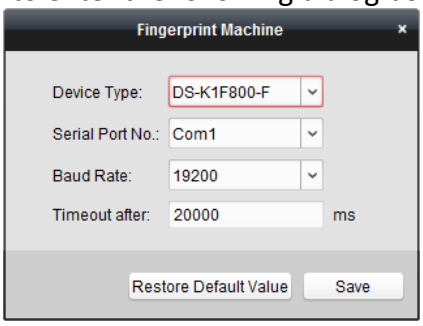
Adding Person (Fingerprint)

Steps:

1. In the Add Person interface, click **Fingerprint** tab.



2. Before inputting the fingerprint, you should connect the fingerprint machine to the PC and set its parameters first.
Click **Set Fingerprint Machine** to enter the following dialog box.



1) Select the device type.
Currently, the supported fingerprint machine types include DS-K1F800-F, DS-K1F300-F, and DS-K1F810-F.
2) For fingerprint machine type DS-K1F800-F, you can set the serial port number, baud rate, and overtime parameters of the fingerprint machine.
3) Click **Save** button to save the settings.
You can click **Restore Default Value** button to restore the default settings.

Notes:

- The serial port number should correspond to the serial port number of PC. You can check the serial port number in Device Manager in your PC.
- The baud rate should be set according to the external fingerprint card reader. The default

value is 19200.

- **Timeout after** field refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.

3. Click **Start** button, click to select the fingerprint to start collecting.
4. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.
5. Click **Stop** button can stop collecting.
   You can also click **Collect from Device** button and select the device to collect fingerprint. (The function should be supported by the device.
6. After collecting the fingerprint, click Card in the Add Person window to enter the Card tab.
7. Click **Link Fingerprint** to link the fingerprint to the card.
   You can select the registered fingerprint and click **Delete** to delete it.
   You can click **Clear** to clear all fingerprints.
8. Click **OK** to save the fingerprints.

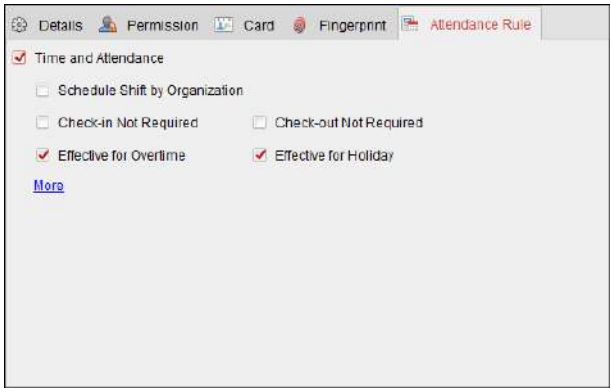
Adding Person (Attendance Rule)

You can set the attendance rule for the person.

Note: This tab page will display when you select **Non-Residence** mode in the application scene when running the software for the first time.

Steps:

1. In the Add Person interface, click **Attendance Rule** tab.



2. If the person joins in the time and attendance, check the **Time and Attendance** checkbox to enable this function for the person. Then the person's card swiping records will be recorded and analyzed for time and attendance.
   For details about Time and Attendance, click **More** to go to the Time and Attendance module.
3. Click **OK** to save the settings.

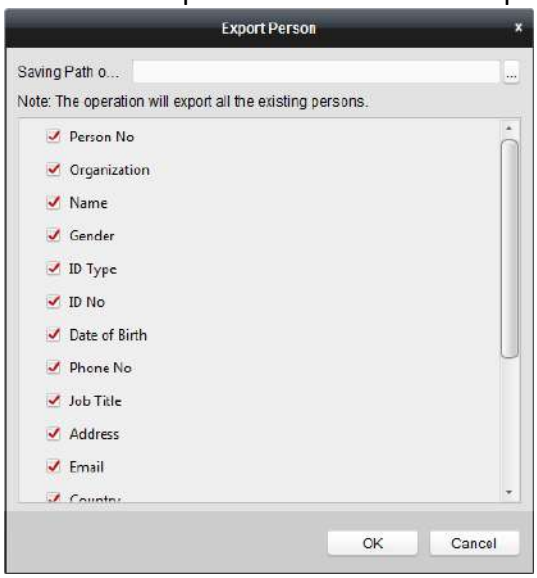
Importing and Exporting Person Information

The person information can be imported and exported in batch.

Steps:

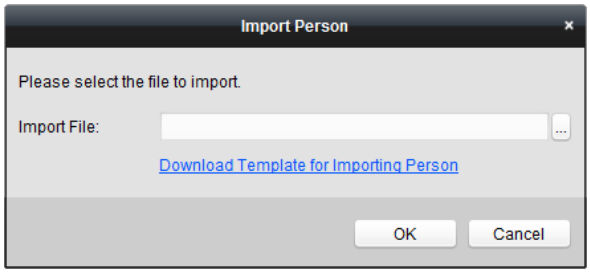
1. **Exporting Person:** You can export the added persons' information in Excel format to the local PC.
   1) After adding the person, you can click **Export Person** button in the Person and Card tab to pop up the following dialog.

2) Click ... to select the path of saving the exported Excel file.
3) Check the checkboxes to select the person information to export.



4) Click **OK** to start exporting.

2. **Importing Person:** You can import the Excel file with persons information in batch from the local PC
   1) click **Import Person** button in the Person and Card tab.



   2) You can click **Download Template for Importing Person** to download the template first.
   3) Input the person information to the downloaded template.
   4) Click ... to select the Excel file with person information.
   5) Click **OK** to start importing.

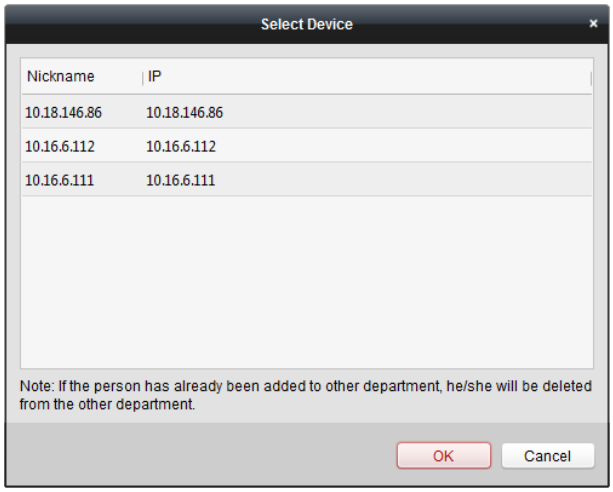
Getting Person Information from Access Control Device

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

Note: This function is only supported by the device the connection mothod of which is TCP/IP when adding the device.

Steps:

1. In the organization list on the left, click to select an organization to import the persons.
2. Click **Get Person** button to pop up the following dialog box.



3. The added access control device will be displayed.
4. Click to select the device and then click **OK** to start getting the person information from the device.
   You can also double click the device name to start getting the person information.

Notes:

- The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- Up to 10000 persons with up to 5 cards each can be imported.

Managing Person

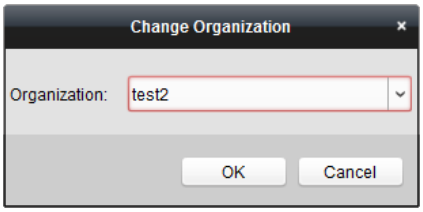
Modifying and Deleting Person

To modify the person information and attendance rule, click or in the Operation column, or select the person and click **Modify** to open the editing person dialog.
You can click to view the person's card swiping records.
To delete the person, select a person and click **Delete** to delete it.
Note: If a card is issued to the current person, the linkage will be invalid after the person is deleted.

Changing Person to Other Organization

You can move the person to another organization if needed.
Steps:

1. Select the person in the list and click **Change Organization** button.



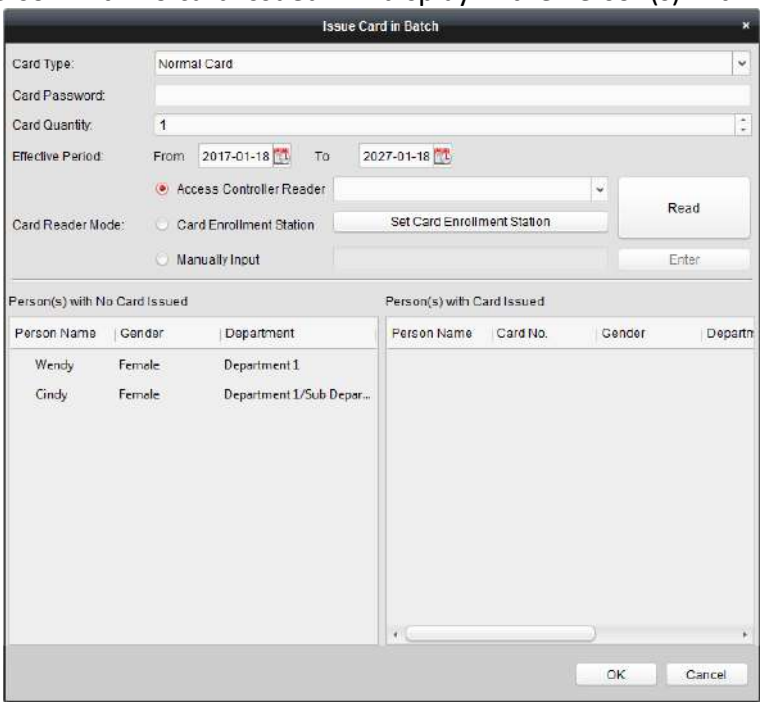
2. Select the organization to move the person to.
3. Click **OK** to save the settings.

Issuing Card in Batch

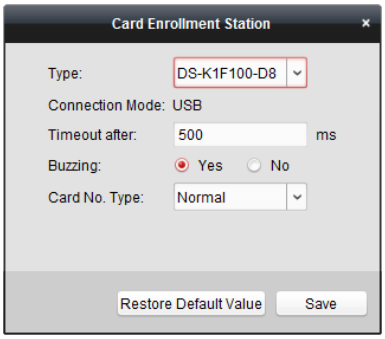
You can issue multiple cards for the person with no card issued in batch.

Steps:

1. Click **Issue Card in Batch** button to enter the following dialog.
   All the added person with no card issued will display in the Person(s) with No Card Issued list.



2. Select the card type according to actual needs.
   Note: For details about the card type, refer to *Adding Person.*
3. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.
   Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to *Chapter 7.8.2 Card Reader Authentication.*
4. Input the card quantity issued for each person.
   For example, if the Card Quantity is 3, you can read or enter three card No. for each person.
5. Click to set the effective time and expiry time of the card.
6. Select the Card Reader Mode for reading the card No.
   - **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
   - **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.
     Note: The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



1) Select the Card Enrollment Station type.
   Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.
2) Set the parameters about the connected card enrollment station.
   If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.
3) Click **Save** button to save the settings.
   You can click **Restore Default Value** button to restore the defaults.

- **Manually Input:** Input the card No. and click **Enter** to input the card No.

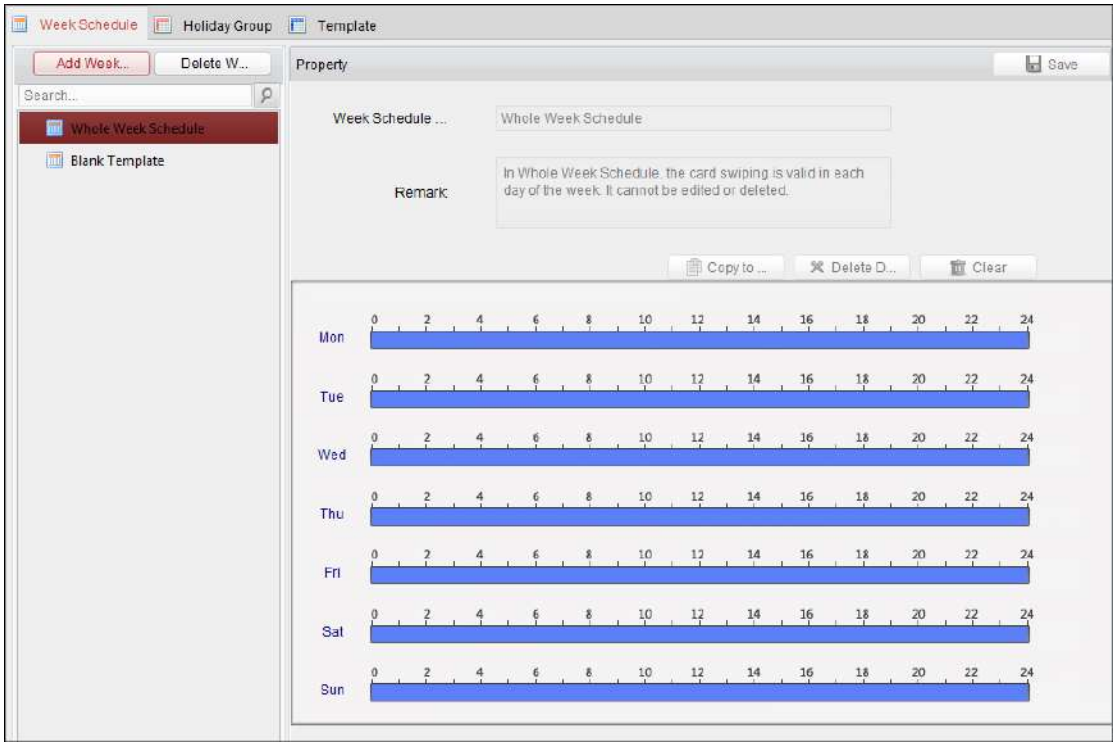
7. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.
8. Click **OK** to save the settings.

7.6 Schedule and Template

Purpose:

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

Click  to enter the schedule and template interface.



You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, please refer to *Chapter 7.7 Permission Configuration.*

7.6.1 Week Schedule

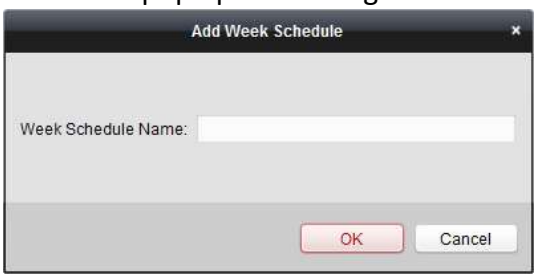
Click **Week Schedule** tab to enter the Week Schedule Management interface.
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

- **Whole Week Schedule:** Card swiping is valid on each day of the week.
- **Blank Schedule:** Card swiping is invalid on each day of the week.

You can perform the following steps to define custom schedules on your demand.

Steps:

1. Click **Add Week Schedule** button to pop up the adding schedule interface.



2. Input the name of week schedule and click **OK** button to add the week schedule.
3. Select the added week schedule in the schedule list and you can view its property on the right. You can edit the week schedule name and input the remark information.
4. On the week schedule, click and drag on a day to draw on the schedule, which means in that

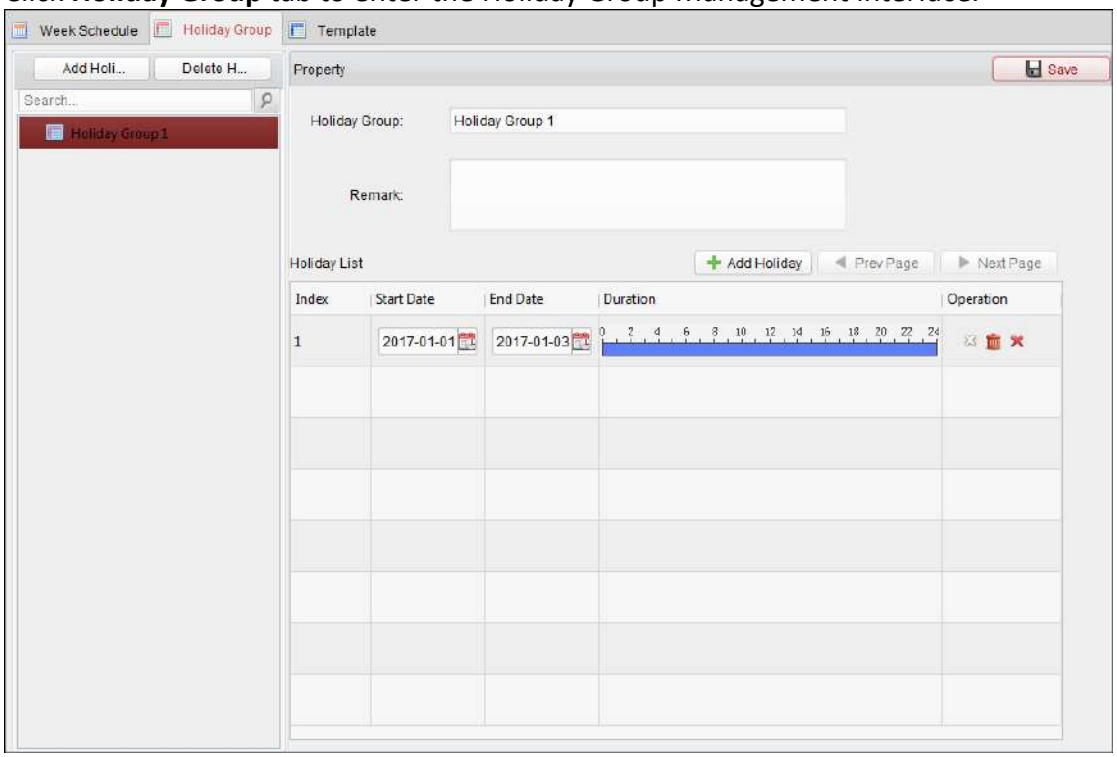
period of time, the configured permission is activated.

Note: Up to 8 time periods can be set for each day in the schedule.

5. When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
   When the cursor turns to , you can lengthen or shorten the selected time bar.
6. Optionally, you can select the schedule time bar,
   and then click **Delete Duration** to delete the selected time bar,
   or click **Clear** to delete all the time bars,
   or click **Copy to Week** to copy the time bar settings to the whole week.
7. Click **Save** to save the settings.

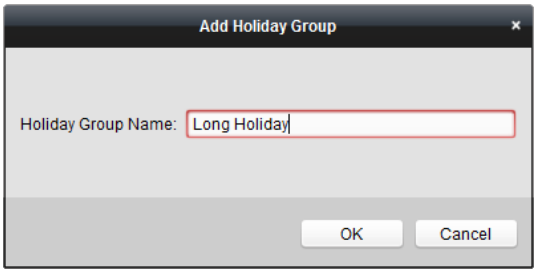
7.6.2 Holiday Group

Click **Holiday Group** tab to enter the Holiday Group Management interface.



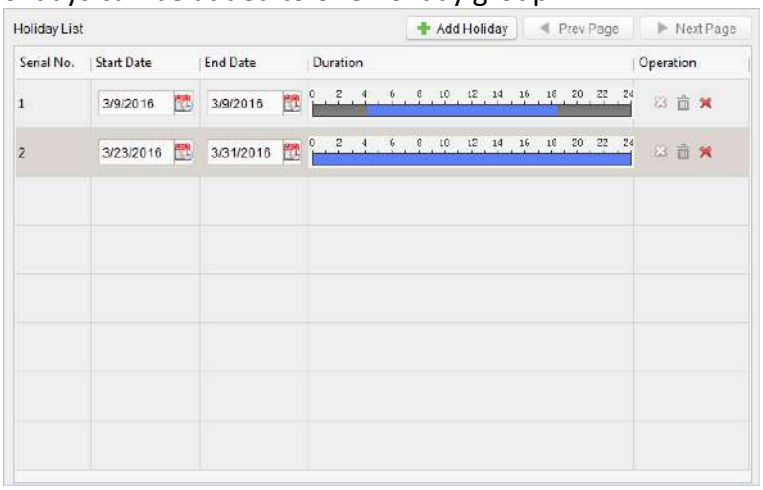
Steps:

1. Click **Add Holiday Group** button on the left to pop up the adding holiday group interface.



2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.

3. Select the added holiday group and you can edit the holiday group name and input the remark information.
4. Click **Add Holiday** icon on the right to add a holiday period to the holiday list and configure the duration of the holiday.
   Note: Up to 16 holidays can be added to one holiday group.



   1) On the period schedule, click and drag to draw the period, which means in that period of time, the configured permission is activated.
      Note: Up to 8 time durations can be set for each period in the schedule.
   2) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
   3) When the cursor turns to , you can lengthen or shorten the selected time bar.
   4) Optionally, you can select the schedule time bar,
      and then click to delete the selected time bar,
      or click to delete all the time bars of the holiday,
      or click to delete the holiday directly.
5. Click **Save** to save the settings.

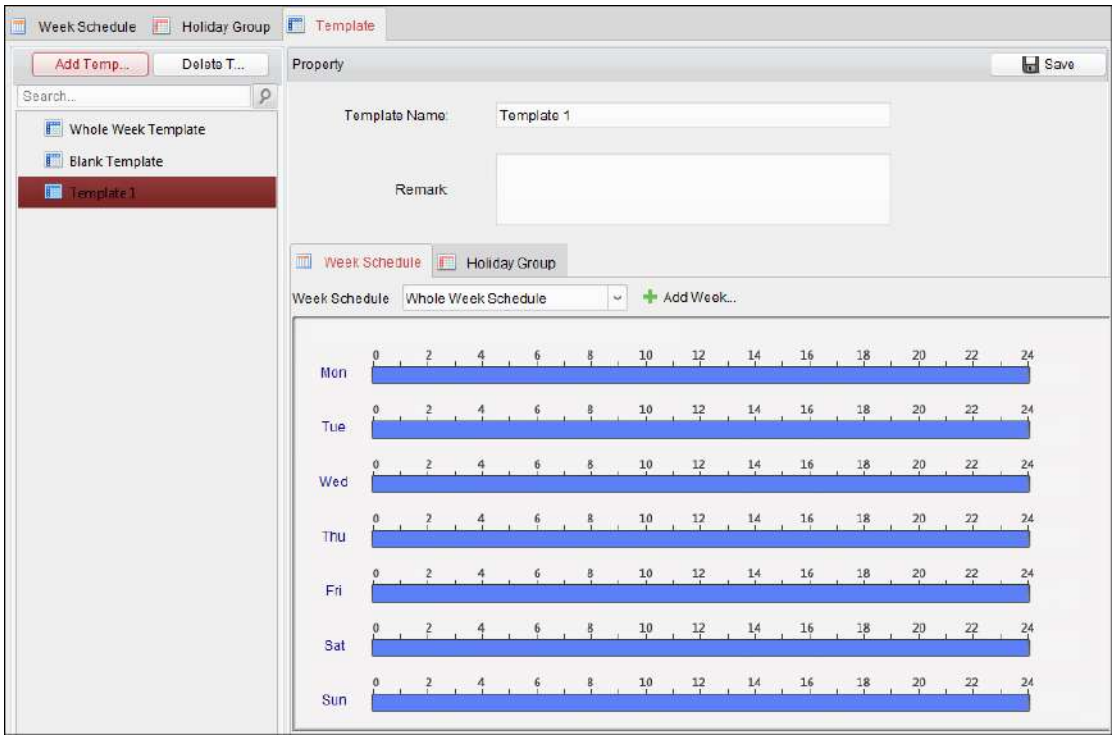
Note: The holidays cannot be overlapped with each other.

7.6.3 Template

After setting the week schedule and holiday group, you can configure the template which contains week schedule and holiday group schedule.

Note: The priority of holiday group schedule is higher than the week schedule.

Click **Template** tab to enter the Template Management interface.



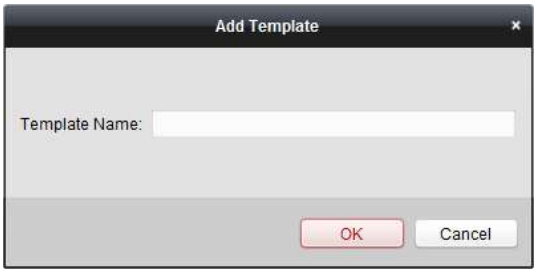
There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

- **Whole Week Template:** The card swiping is valid on each day of the week and it has no holiday group schedule.
- **Blank Template:** The card swiping is invalid on each day of the week and it has no holiday group schedule.

You can define custom templates on your demand.

Steps:

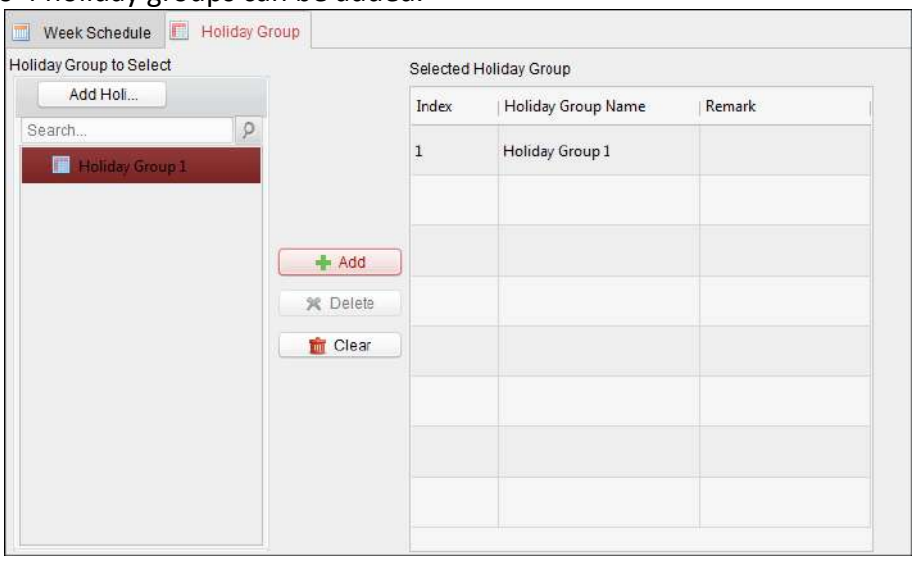
1. Click **Add Template** to pop up the adding template interface.



2. Input the template name in the text filed and click **OK** button to add the template.
3. Select the added template and you can edit its property on the right. You can edit the template name and input the remark information.
4. Select a week schedule to apply to the schedule.
   Click **Week Schedule** tab and select a schedule in the dropdown list.
   You can also click **Add Week Schedule** to add a new week schedule. For details, refer to *Chapter 7.6.1 Week Schedule.*



5. Select holiday groups to apply to the schedule.
   Note: Up to 4 holiday groups can be added.

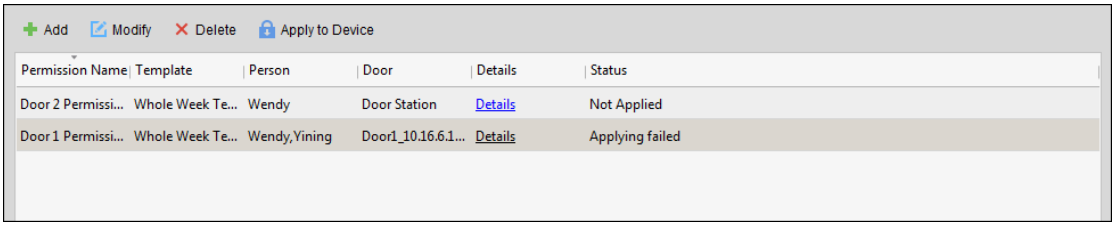


   Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one. For details, refer to *Chapter 7.6.2 Holiday Group.*
   You can click to select an added holiday group in the right-side list and click **Delete** to delete it.
   You can click **Clear** to delete all the added holiday groups.
6. Click **Save** button to save the settings.

7.7 Permission Configuration

In Permission Configuration module, you can add, edit, and delete the access control permission, and then apply the permission settings to the device to take effect.

Click  icon to enter the Access Control Permission interface.



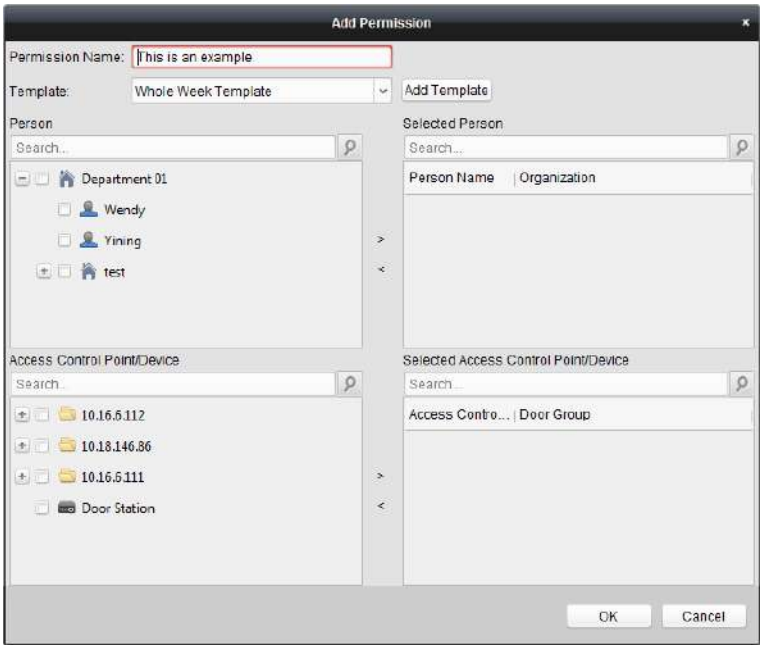
7.7.1 Adding Permission

Purpose:

You can assign permission for persons to enter/exist the access control points (doors) in this section.

Steps:

1. Click **Add** icon to enter following interface.



2. In the Permission Name field, input the name for the permission as desired.
3. Click on the dropdown menu to select a template for the permission.

   Note: You should configure the template before permission settings. You can click **Add Template** button to add the template. Refer to *Chapter 7.6 Schedule and Template* for details.
4. In the Person list, all the added persons display.

   Check the checkbox(es) to select person(s) and click **>** to add to the Selected Person list.

   (Optional) You can select the person in Selected Person list and click **<** to cancel the selection.
5. In the Access Control Point/Device list, all the added access control points (doors) and door stations will display.

   Check the checkbox(es) to select door(s) or door station(s) and click **>** to add to the selected list.

   (Optional) You can select the door or door station in the selected list and click **<** to cancel the selection.
6. Click **OK** button to complete the permission adding. The selected person will have the

permission to enter/exit the selected door/door station with their linked card(s) or fingerprints.

7. (Optional) after adding the permission, you can click **Details** to modify it. Or you can select the permission and click **Modify** to modify.
   You can select the added permission in the list and click **Delete** to delete it.

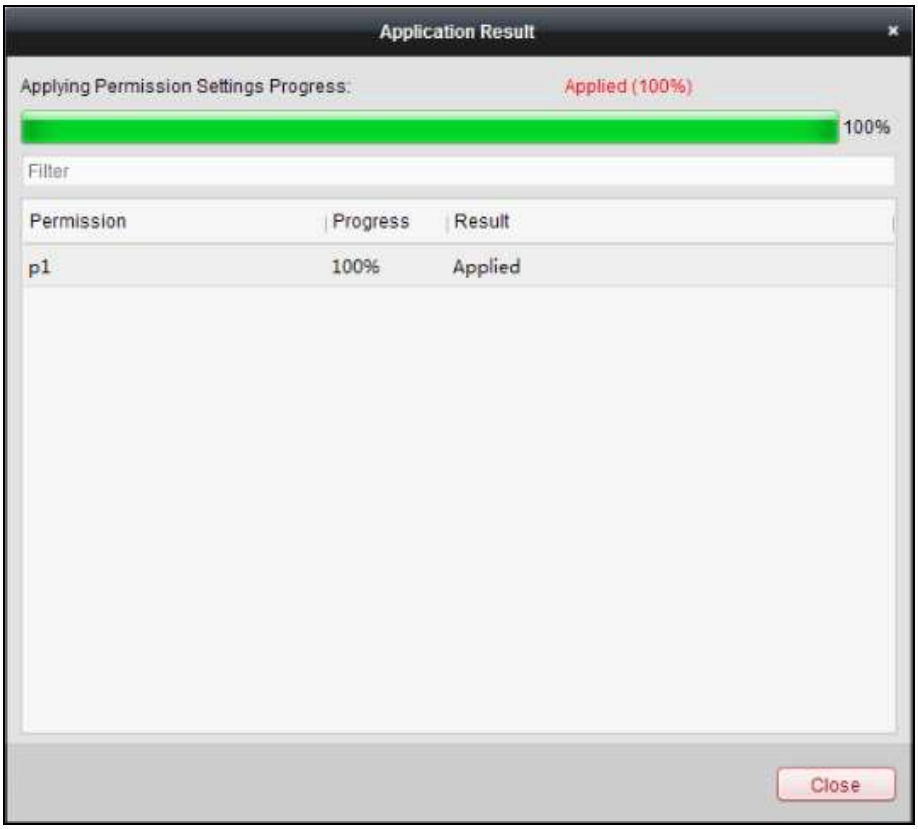
7.7.2 Applying Permission

Purpose:

After configuring the permissions, you should apply the added permission to the access control device to take effect.

Steps:

1. Select the permission(s) to apply to the access control device. To select multiple permissions, you can hold the *Ctrl* or *Shift* key and select permissions.
2. Click **Apply to Device** to start applying the selected permission(s) to the access control device or door station.
3. The following window will pop up, indicating the applying permission result.



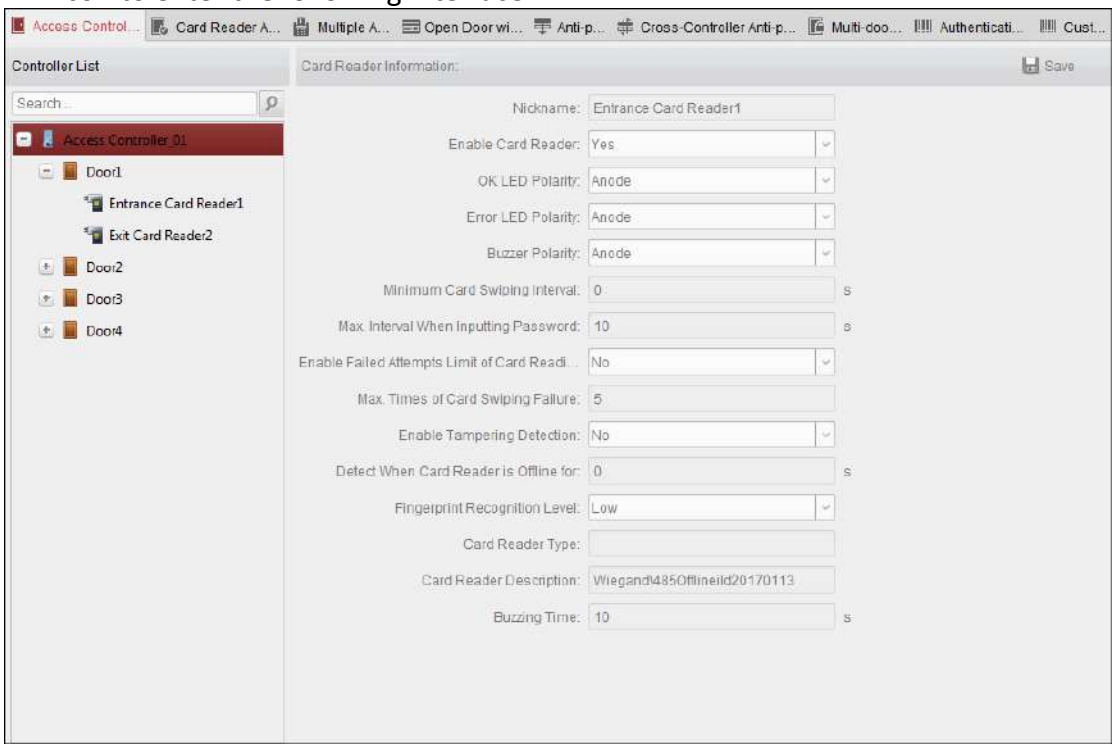
7.8 Advanced Functions

Purpose:

After configuring the person, template, and access control permission, you can configure the advanced functions of access control application, such as access control parameters, authentication password, and opening door with first card, anti-passing back, etc.

Note: The advanced functions should be supported by the device.

Click  icon to enter the following interface.



7.8.1 Access Control Parameters

Purpose:

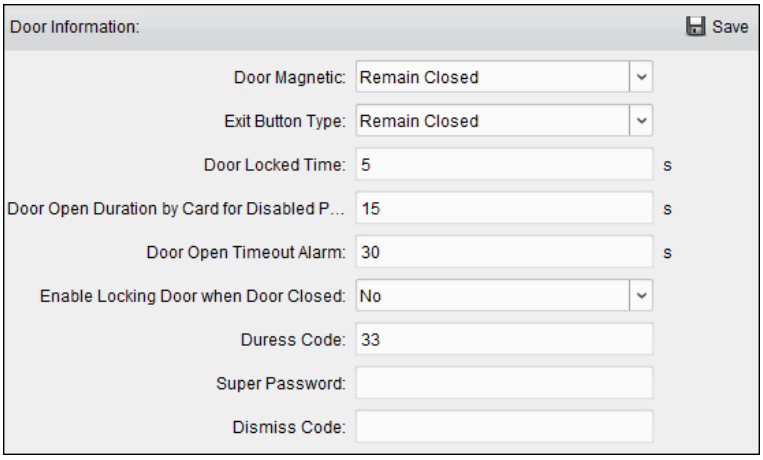
After adding the access control device, you can configure its access control point (door)'s parameters, and its card readers' parameters.

Click **Access Control Parameters** tab to enter the parameters settings interface.

Door Parameters

Steps:

1. In the controller list on the left, click  to expand the access control device, select the door (access control point) and you can edit the information of the selected door on the right.

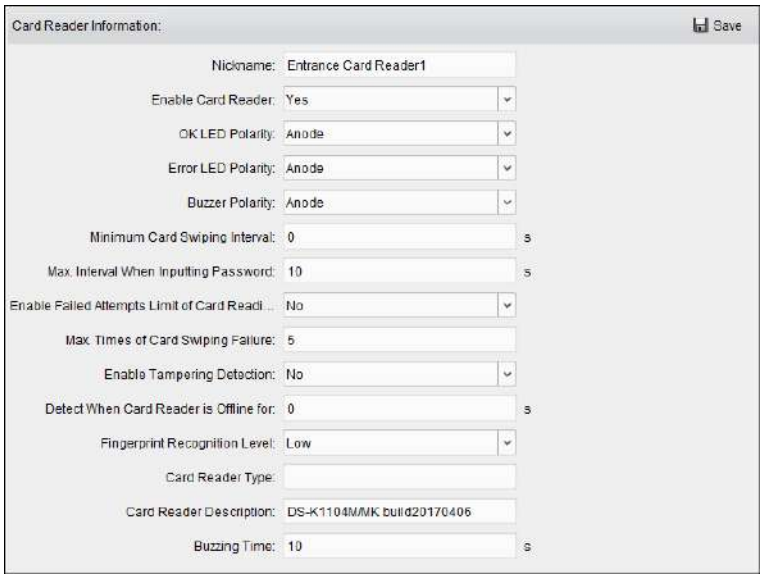


2. You can editing the following parameters:
   Door Magnetic: The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
   Exit Button Type: The Exit Button Type is in the status of **Remain Open** (excluding special conditions).
   Door Locked Time: After swiping the normal card and relay action, the timer for locking the door starts working.
   Door Open Duration by Card for Door Extended Opening: The door magnetic can be enabled with appropriate delay after card holder swipes the card.
   Door Open Timeout Alarm: The alarm can be triggered if the door has not been close
   Enable Locking Door when Door Closed: The door can be locked once it is closed even if the Door Locked Time is not reached.
   Duress Code: The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.
   Super Password: The specific person can open the door by inputting the super password.
   Dismiss Code: Input the dismiss code to stop the buzzer of the card reader.
   Notes:
   - The duress code, Super password, and dismiss code should be different.
   - The duress code, super password, and the dismiss code should be different from the authentication password.
   - The duress code, super password, and the dismiss code should contain 4 to 8 numerics.
3. Click **Save** button to save parameters.

Card Reader Parameters

Steps:

1. In the device list on the left, click ⊞ to expand the door, select the card reader name and you can edit the card reader parameters on the right.



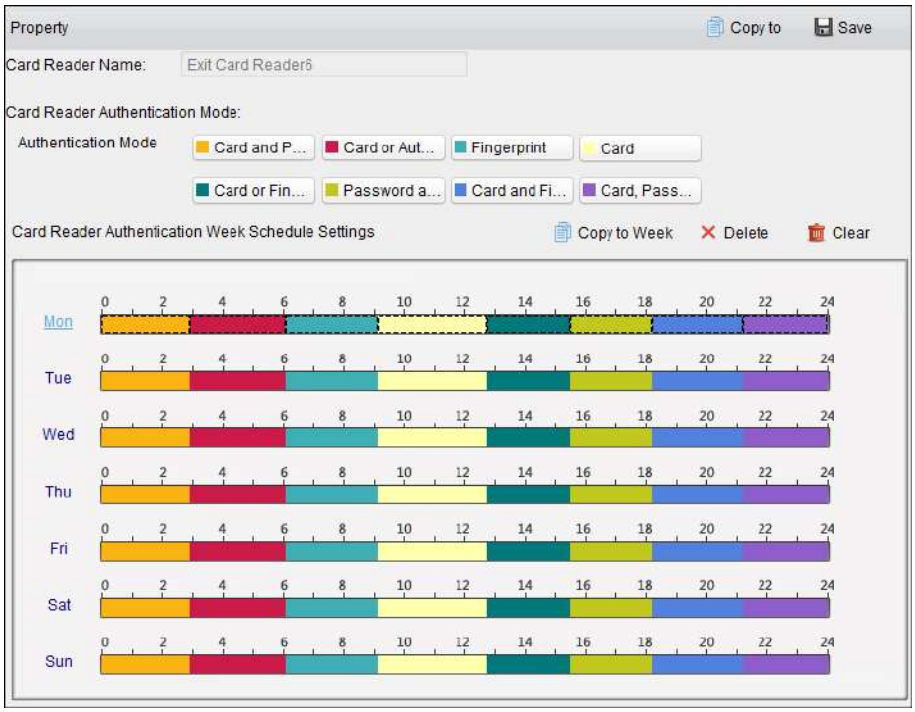
2. You can editing the following parameters:
   Nickname: Edit the card reader name as desired.
   Enable Card Reader: Select **Yes** to enable the card reader.
   OK LED Polarity: Select the OK LED Polarity of the card reader mainboard.
   Error LED Polarity: Select the Error LED Polarity of the card reader mainboard.
   Buzzer Polarity: Select the Buzzer LED Polarity of the card reader mainboard.
   Minimum Card Swiping Interval: If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.
   Max. Interval When Inputting Password: When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.
   Enable Failed Attempts Limit of Card Reading: Enable to report alarm when the card reading attempts reach the set value.
   Max. Times of Card Swiping Failure: Set the max. failure attempts of reading card.
   Enable Tampering Detection: Enable the anti-tamper detection for the card reader.
   Detect When Card Reader is Offline for: When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.
   Fingerprint Recognition Level: Select the fingerprint recognition level in the dropdown list. By default, the level is Low.
   Card Reader Type: Read the card reader's type.
   Card Reader Description: Read the card reader description.
   Buzzing Time: Set the card reader buzzing time. The available time ranges from 0 to 5999s. 0 represents continuous buzzing.
3. Click the **Save** button to save parameters.

7.8.2 Card Reader Authentication

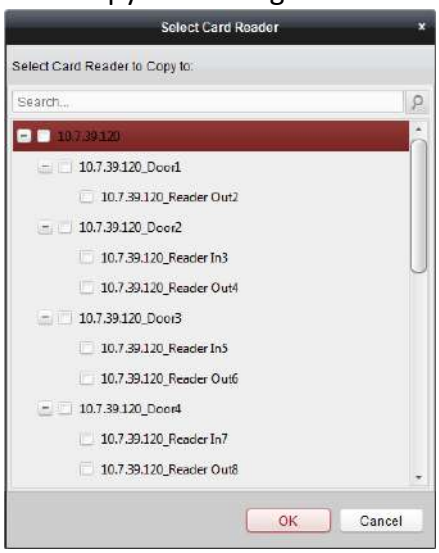
Purpose:
You can set the passing rules for the card reader of the access control device.

Steps:

1. Click **Card Reader Authentication** tab and select a card reader on the left.
2. Select a card reader authentication mode. The available authentication modes depend on the card reader type:
   - **Card and Password**: The door can open by both inputting the card password and swiping the card.
     Note: Here the password refers to the password set when issuing the card to the person. *Chapter 7.5.2 Person Management.*
   - **Card or Authentication Password**: The door can open by inputting the authentication password or swiping the card.
     Note: Here the authentication password refers to the password set to open the door. Refer to *Chapter 7.8.8 Authentication Password.*
   - **Fingerprint**: The door can open by only inputting the fingerprint.
   - **Card**: The door can open by only swiping the card.
   - **Card or Fingerprint:** The door can open by inputting the fingerprint or swiping the card.
   - **Password and Fingerprint**: The door can open by both inputting the card password and inputting the fingerprint.
     Note: Here the password refers to the card password set when issuing the card to the person. Refer to *Chapter 7.5.2 Person Management.*
   - **Card and Fingerprint**: The door can open by both inputting the fingerprint and swiping the card.
   - **Card, Password and Fingerprint**: The door can open by both inputting the fingerprint, inputting the card password, and swiping the card.
     Note: Here the password refers to the card password set when issuing the card to the person. Refer to *Chapter 7.5.2 Person Management.*
3. Click and drag your mouse on a day to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.



4. Repeat the above step to set other time periods.
   Or you can select a configured day and click **Copy to Week** button to copy the same settings to the whole week.
   (Optional) You can click **Delete** button to delete the selected time period or click **Clear** button to delete all the configured time periods.
5. (Optional) Click **Copy to** button to copy the settings to other card readers.



6. Click **Save** button to save parameters.

7.8.3 Multiple Authentication

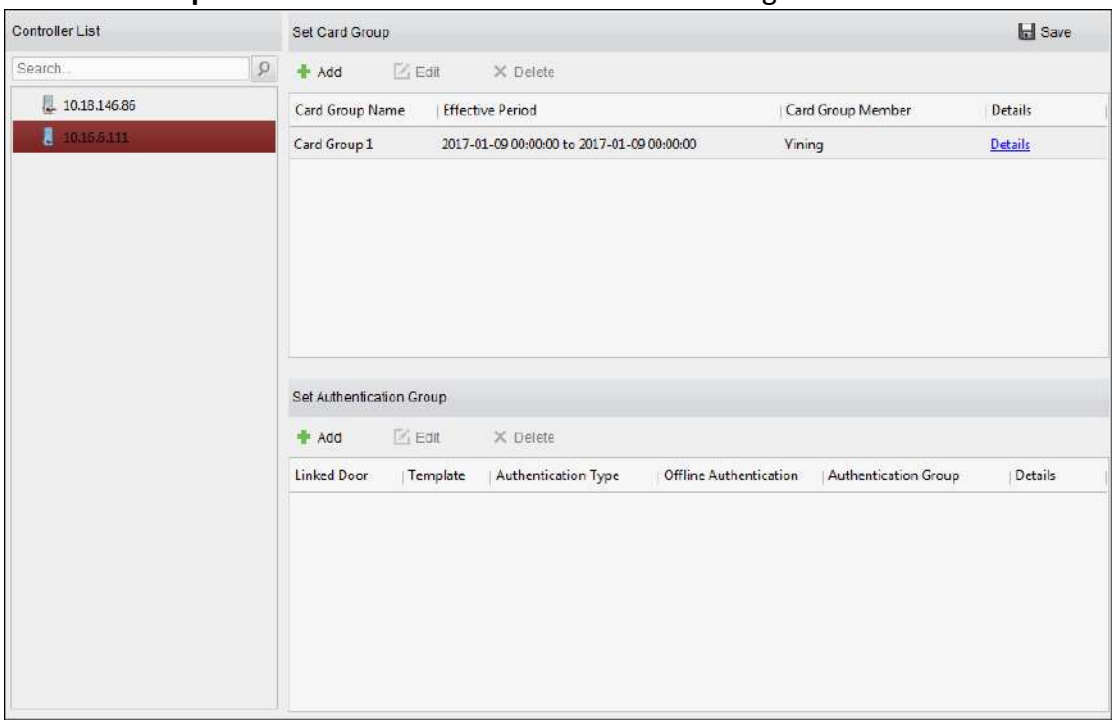
Purpose:

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

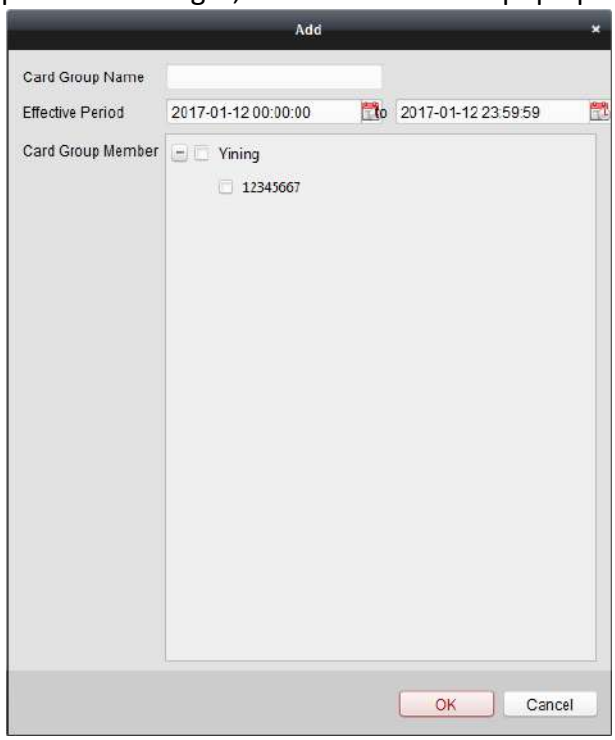
Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration.*

Steps:

1. Click **Multiple Authentication** tab to enter the following interface.

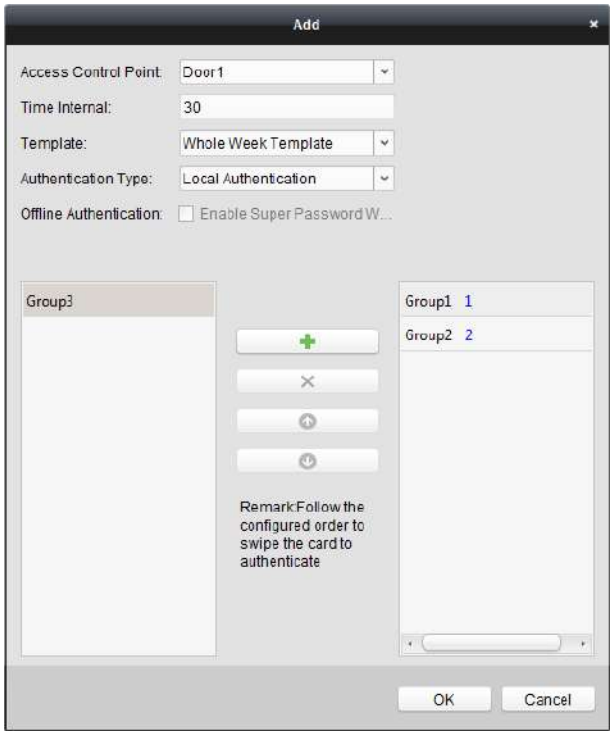


2. Select access control device from the list on the left.
3. In the Set Card Group panel on the right, click **Add** button to pop up the following dialog:



1) In the Card Group Name field, input the name for the group as desired.
2) Click to set the effective time and expiry time of the card group.
3) Check the checkbox(es) to select the card(s) to add the card group.
4) Click **OK** to save the card group.

4. In the Set Authentication Group panel on the left, click **Add** to pop up the following dialog.



1) Select the access control point (door) of the device for multiple authentication.
2) Input the time interval for card swiping.
3) Select the template of the authentication group from the dropdown list. For details about setting the template, refer to *Chapter 7.6 Schedule and Template*.
4) Select the authentication type of the authentication group from the dropdown list.
   - **Local Authentication:** Authentication by the access control device.
   - **Local Authentication and Remotely Open Door:** Authentication by the access control device and by the client.
     For Local Authentication and Remotely Open Door type, you can check the checkbox to enable the super password authentication when the access control device is disconnected with the client.
   - **Local Authentication and Super Password:** Authentication by the access control device and by the super password.
5) In the list on the left, the added card group will display. You can click the card group and click to add the group to the authentication group.
   You can click the added card group and click to remove it from the authentication group.
   You can also click or to set the card swiping order.
5) Input the **Card Swiping Times** for the selected card group.
   Notes:

- The Card Swiping Times should be larger than 0 and smaller than the added card quantity in the card group.
- The upper limit of Card Swiping Times is 16.

6) Click **OK** to save the settings.

5. Click **Save** to save and take effect of the new settings.

Notes:

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

7.8.4 Open Door with First Card

Purpose:

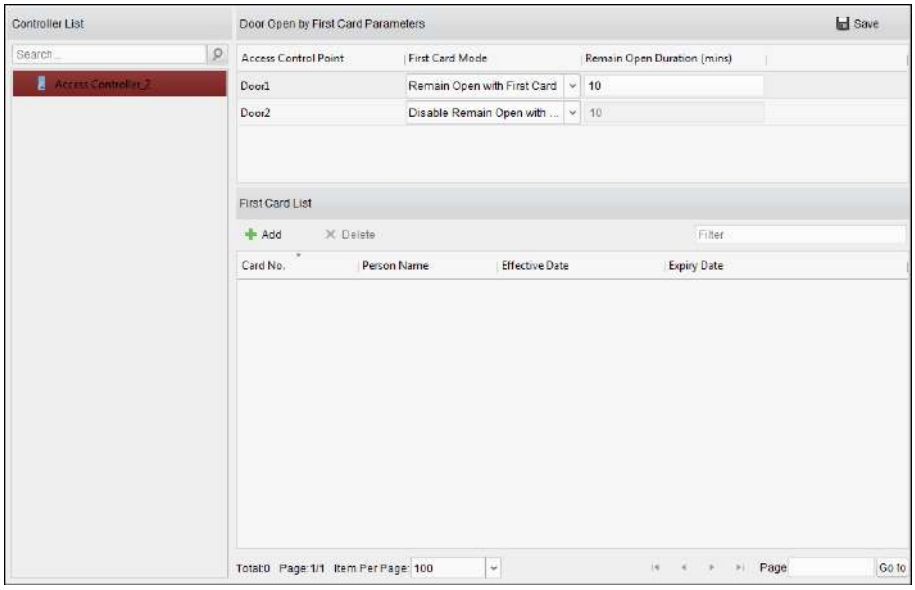
You can set multiple first cards for one access control point. After the first card swiping, it allows multiple persons access the door or other authentication actions. The first card mode contains Remain Open with First Card, Disable Remain Open with First Card, and First Card Authorization.

Remain Open with First Card: The door remains open for the configured time duration after the first card swiping until the remain open duration ends.

First Card Authorization: All authentications, except for the authentications of super card, duress card, and duress code, are allowed only after the first card authorization.

Steps:

1. Click **Open Door with First Card** tab to enter the following interface.



2. Select an access control device from the list on the left.
3. Select the first card mode in the drop-down list for the access control point.
4. (Optional) If you select Remain Open with First Card, you should set remain open duration.

Notes:

- The Remain Open Duration should be between 0 and 1440 minutes. By default, it is 10 minutes.
- In the First Card Authorization mode, you can access the door when swiping the super card, the duress card or input the duress code without swiping the first card.
- You can swipe the first card again to disable the first card mode.
- The first card authorization is effective only on the current day. The authorization will be expired after 24:00 on the current day.

5. In the First Card list, Click **Add** button to pop up the following dialog box.



1) Select the cards to add as first card for the door

   Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration.*

2) Click **OK** button to save adding the card.

6. You can click **Delete** button to remove the card from the first card list.
7. Click **Save** to save and take effect of the new settings.

7.8.5 Anti-Passing Back

Purpose:

You can set anti-passing back for card readers in the same access controller. You should swipe the card according to the configured swiping card route. And only one person could pass the access control point after swiping the card.

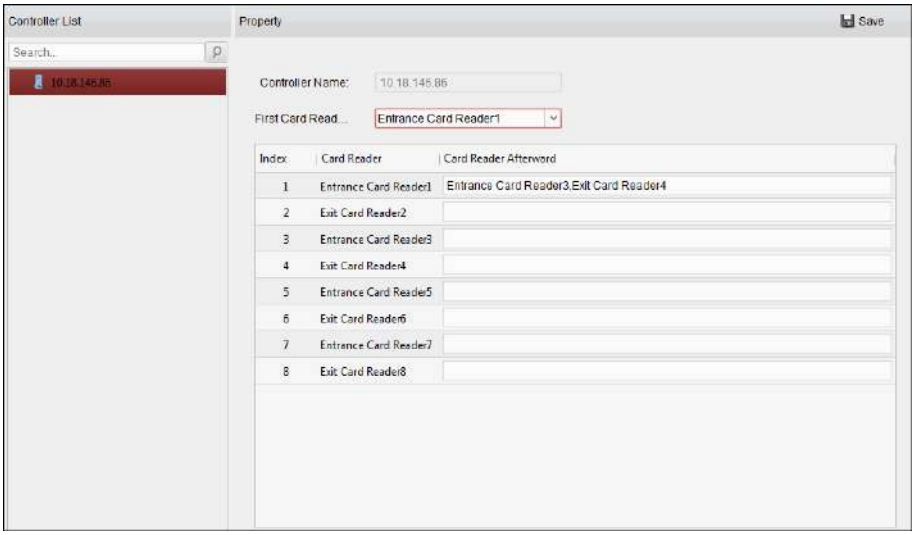
Notes:

- Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time.
- You should enable the anti-passing back function on the access control device first.

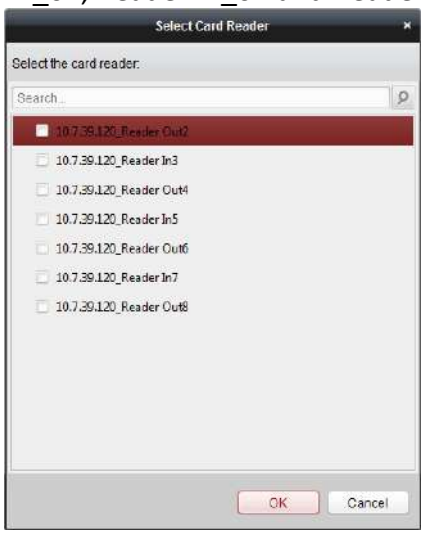
Setting the Path of Swiping Card (Card Reader Order)

Steps:

1. Click **Anti-passing Back** tab to enter the following interface.



2. Select an access control device from the device list on the left.
3. In the First Card Reader field, select the card reader as the beginning of the path.
4. In the list, click the text filed of **Card Reader Afterward** and select the linked card readers.
   Example: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.



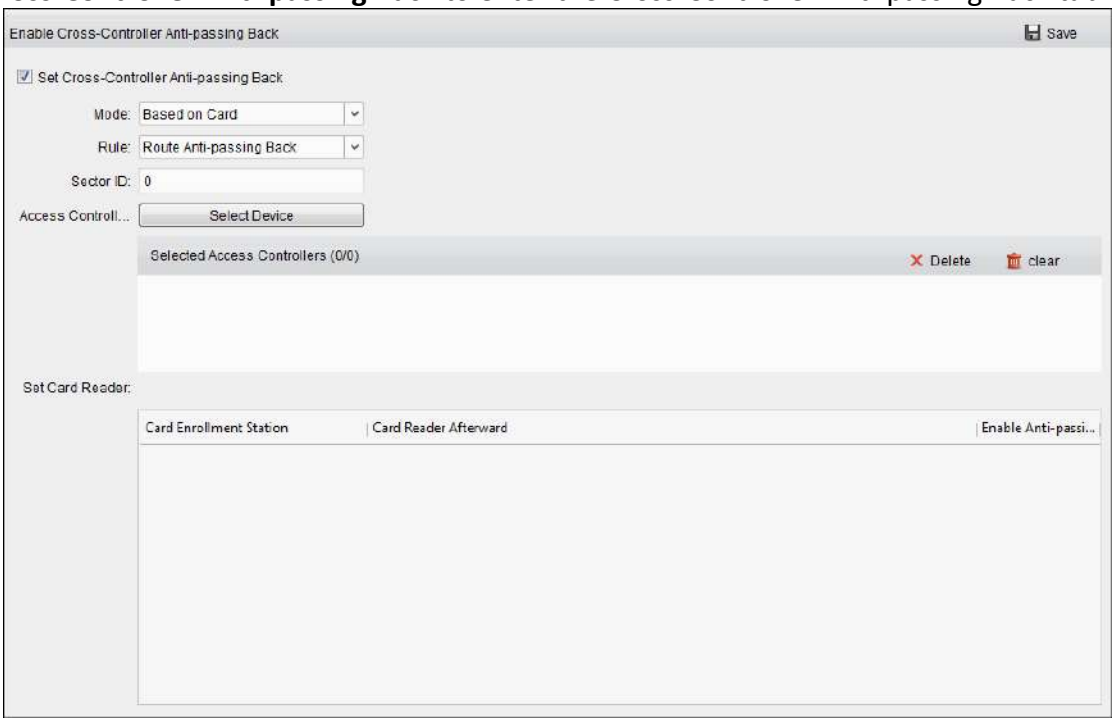
   Note: Up to four afterward card readers can be added for one card reader.
5. (Optional) You can enter the Select Card Reader dialog box again to edit its afterward card readers.
6. Click **Save** to save and take effect of the new settings.

7.8.6 Cross-Controller Anti-passing Back

Purpose:

You can set anti-passing back for card readers in multiple access controllers. You should swipe the card according to the configured swiping card route. And only one person could pass the access control point after swiping the card.

Click **Cross-Controller Anti-passing Back** to enter the Cross-Controller Anti-passing Back tab.



Setting Route Anti-passing Back

Purpose:

The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards.

Steps:

1. Check the **Enable Cross-Controller Anti-passing Back** checkbox to enable the function.
2. Set the anti-passing back parameters.
   - **Based on Card**

     Note: The system will judge the anti-passing back according to the entrance and exit records on the card.

     1) Select **Based on Card** as the anti-passing back mode in the drop-down list.
     2) Select Route Anti-passing Back as the rule.
     3) Set the sector ID.
     4) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
     5) In the Set Card Reader area, click the icon on the left of the card enrollment station column to select the first card reader. The icon will turn to .
     6) Click the card reader afterward input field to select the card readers afterward in the pop-up window.
     7) Check the checkbox in the Enable Anti-passing Back column to enable the anti-passing

back function.

Notes:

- The displayed card readers in the card reader afterward input field should be in authentication order.
- Up to 64 controllers with anti-passing back function can be added.
- Up to 16 card readers afterward can be added for each card reader.
- It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to *7.4.8 M1 Card Encryption*.

➢ **Based on Network**

Note: Authenticate the anti-passing back according to the entrance and exit information on the card reader.

1) Select **Based on Network** as the anti-passing back mode in the drop-down list.
2) Select Route Anti-passing Back as the rule.
3) Select a server in the drop-down list for judging the anti-passing back.
4) (Optional) You can click **Delete Anti-passing Back Record** and select the card in the pop-up window to delete the card swiping information in all devices.
   The user should be start swiping card again from the first card reader.
5) In the Set Card Reader area, click the icon on the left of the card enrollment station column to select the first card reader. The icon will turn to .
6) Click the card reader afterward input field to select the card readers afterward in the pop-up window.
7) Check the checkbox in the Enable Anti-passing Back column to enable the anti-passing back function.

   Notes:

   - The displayed card readers in the card reader afterward input field should be in authentication order.
   - Up to 64 controllers with anti-passing back function can be added.
   - Up to 16 card readers afterward can be added for each card reader.
   - Up to 5000 cards' swiping records can be stored in the selected server.

Setting Entrance/Exit Anti-passing Back

Purpose:

You can set the entrance card reader and the exit card reader only for entering and exiting, without setting the first card reader and the card readers afterwards.

Steps:

1. In the Cross-Controller Anti-passing Back tab, check the **Enable Cross-Controller Anti-passing Back** checkbox to enable the function.
2. Set the anti-passing back parameters.

   ➢ **Based on Card**

   Note: The system will judge the anti-passing back according to the entrance and exit records on the card.

   1) Select **Based on Card** as the anti-passing back mode in the drop-down list.

2) Select Entrance/Exit Anti-passing Back as the rule.
3) Set the sector ID.
4) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
5) In the Set Card Reader area, check the checkboxes in the Enable Anti-passing Back column to select the entrance card reader and the exit card reader.
6) Click **Save** to save the settings.

Notes:

- Up to one entrance carder and one exit card reader should be checked.
- Up to 64 controllers with anti-passing back function can be added.
- It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to *7.4.8 M1 Card Encryption*.

➢ **Based on Network**

Note: Authenticate the anti-passing back according to the entrance and exit information on the card reader.

1) Select **Based on Network** as the anti-passing back mode in the drop-down list.
2) Select Entrance/Exit Anti-passing Back as the rule.
3) Select the server in the dropdown list for judging the anti-passing back.
4) (Optional) You can click **Delete Record** and select the card in the pop-up window to delete the card swiping information in all devices.
5) Click **Select Device** to select a device in the pop-up window for anti-passing back authentication.
6) In the Set Card Reader area, check the checkboxes in the Enable Anti-passing Back column to select the entrance card reader and the exit card reader.
7) Click **Save** to save the settings.

Notes:

- Up to one entrance carder and one exit card reader should be checked.
- Up to 64 controllers with anti-passing back function can be added.
- Up to 5000 cards' swiping records can be stored in the selected server.

7.8.7 Multi-door Interlocking

Purpose:

You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Notes:

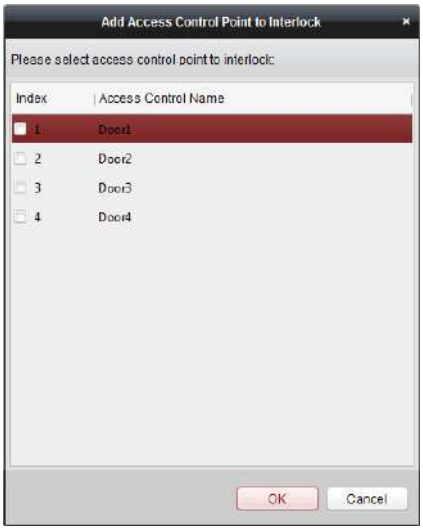
- The Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time.

Steps:

1. Click **Multi-door Interlocking** tab to enter the multi-door interlock settings page.



2. Select an access controller from the Controller List.
3. Click **Add** to pop up the Add Access Control Point to Interlock interface.



4. Select the access control point (door) from the list.
   Note: Up to four doors can be added in one multi-door interlocking combination.
5. Click **OK** to save the adding.
6. (Optional) After adding the multi-door interlocking combination, you can select it from the list and click **Delete** to delete the combination.
7. Click **Save** button to save and take effect.

7.8.8 Authentication Password

Purpose:

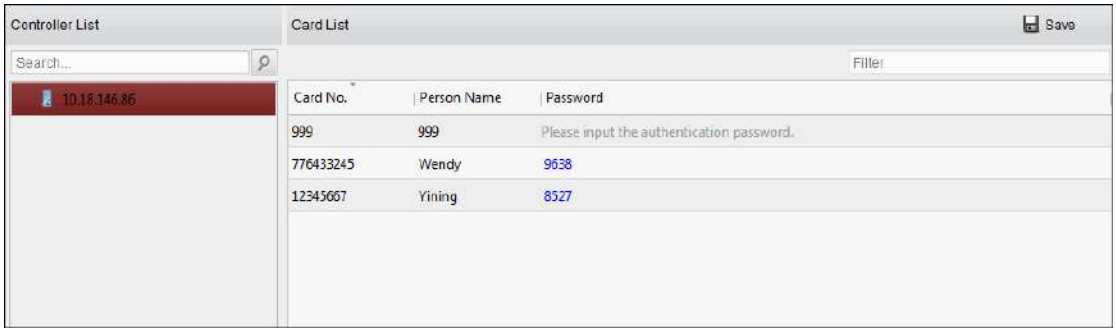
You can open the door by inputting the authentication password on the card reader keypad after finishing the operation of setting authentication password.

Notes:

- This authentication password function is only valid during the schedules when the card reader authentication mode for the access control device is set as **Card or Authentication Password**. For details, please refer to *Chapter 7.8.2 Card Reader Authentication.*
- This function should be supported by the access control device.

Steps:

1. Click **Authentication Password** tab and select an access control device from the list.



All the cards and persons which have been applied to the device will be displayed.

Note: For setting and applying the permissions to the device, refer to *Chapter 7.7 Permission Configuration.*

2. Click the **Password** field of the card and input the authentication password for the card.

   Note: The authentication password should contain 4 to 8 digits.
3. After setting the authentication password, the authentication password function of the card will be enabled by default.
4. (Optional) You can input the keywords of card No., person name, or authentication password to search.

Notes:

- Up to 500 cards with authentication password can be added to one access control device.
- The password should be unique and cannot be the same with super password, duress code, and dismiss code in the access control parameters.

7.8.9 Custom Wiegand

Purpose:

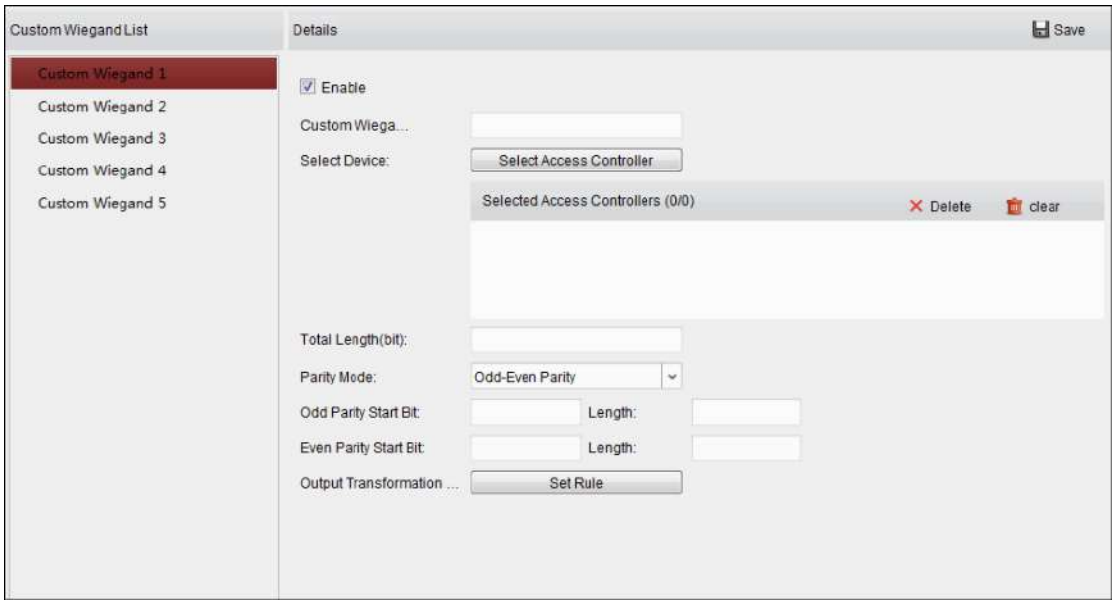
Based on the knowledge of uploading rule for the third party wiegand, you can set multiple customized wiegand protocols to communicate between the controller and the third party card readers.

Before you start:

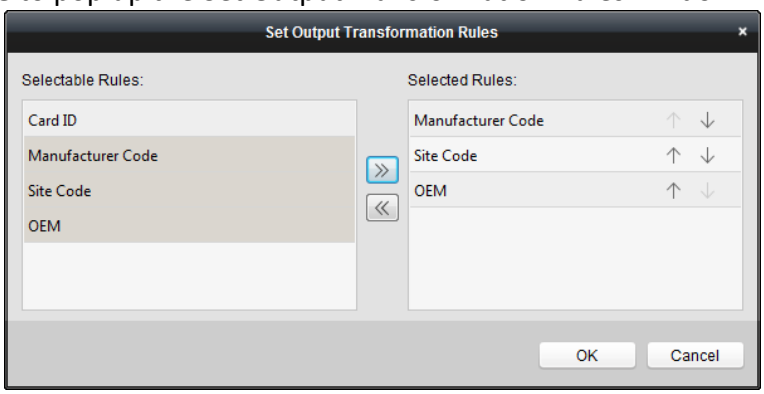
Wire the third party card readers to the controller.

Steps:

1. Click **Custom Wiegand** to enter the Custom Wiegand tab.



2. Select a custom wiegand on the left of the interface.
3. Check **Enable** checkbox to enable the custom wiegand.
4. Set the wiegand name.
5. Select device.
   1) Click **Select Device**.
   2) Select the device need to use custom wiegand.
   3) Click **OK** to save the settings.
6. Input the Total Length and select the parity mode in the drop-down list.
   If you select Odd-Even Parity, you should set the odd parity start bit, the odd parity length, the even parity start bit and the even parity length.
   If you select XOR Parity, you should set the XOR parity start bit, length per group and total length.
   If you select None, you are no need to set the parity mode.
7. Set output transformation rule.
   1) Click **Set Rule** to pop up the Set Output Transformation Rules window**.**



   2) Select rules on the left list.
      Note: Press the *Shift* key to select multiple rules.
   3) Click  to move the selected rules to the right list.

4) (Optional) Click  or  to change the rule order.
5) (Optional) Select the rules in the Selected Rule list and click  to remove the rule from the list on the right.
6) Click **OK** to save the settings.
7) In the Custom Wiegand tab, set the rule start bit, length, and the decimal digit.

8. Click **Save** at the upper right corner of the interface to save the settings.

Notes:

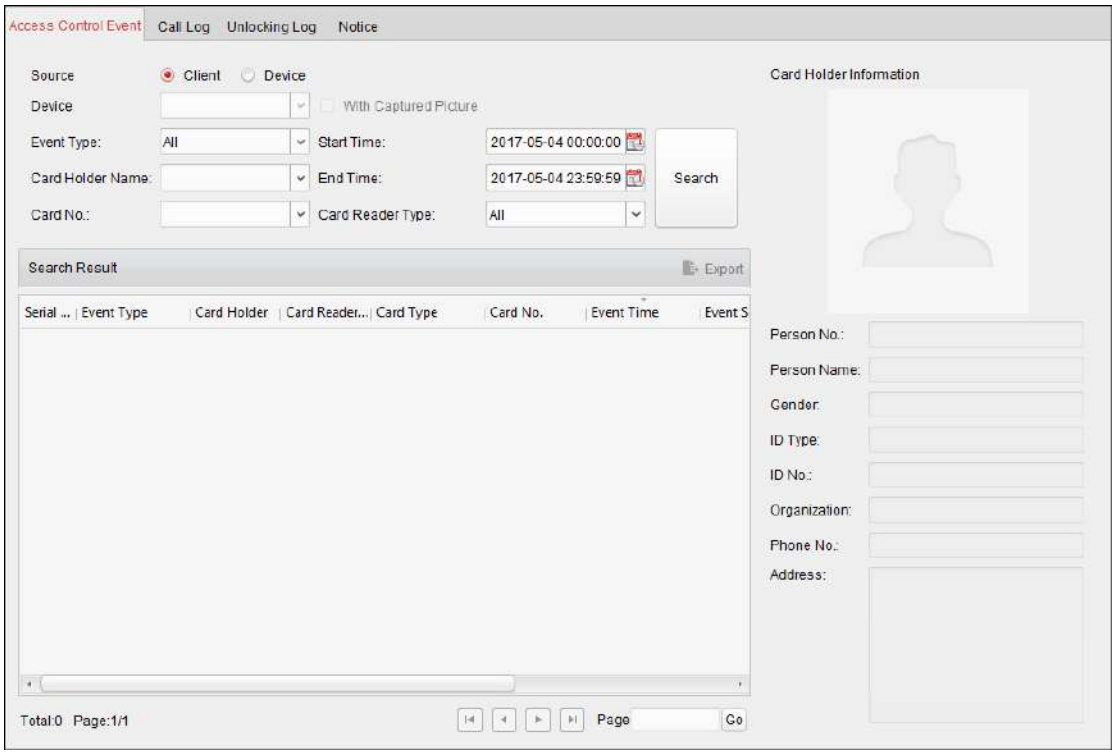
- By default, the device disables the custom wiegand function.
- If the device enables the custom wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom wiegands can be set.
- Up to 32 characters are allowed in the custom wiegand name.
- Up to 80 bits are available in the total length.
- The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
- The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
- For details about the custom wiegand, see Appendix.

7.9 Searching Access Control Event

Purpose:

You can search the access control history events including device exception event, door event, alarm input, and card reader event.

Click  icon and click Access Control Event tab to enter the following interface.



Steps:

1. Select the source.
   You can select Client or Device.
2. Enter the search condition (source, event type/card holder name/card No./capture/start & end time).
3. Click **Search** to get the search results.
4. View the event information in the event list.
5. Click an event to view the information of the card holder on the **Card Holder Information** panel on the left side of the page.
6. You can click **Export** button to export the search results to the local PC.

7.10 Access Control Event Configuration

Purpose:

For the added access control device, you can configure its access control linkage including access control event linkage, access control alarm input linkage, event card linkage, and cross-device linkage.

Click the  icon on the control panel,
or click **Tool**->**Event Management** to open the Event Management page.

7.10.1 Access Control Event Linkage

Purpose:

You can assign linkage actions to the access control event by setting up a rule. For example, when the access control event is detected, an audible warning appears or other linkage actions happen.

Note: The linkage here refers to the linkage of the client software's own actions.

Steps:

1. Click the **Access Control Event** tab.
2. The added access control devices will display in the Access Control Device panel on the left. Select the access control device, or alarm input, or access control point (door), or card reader to configure the event linkage.
3. Select the event type to set the linkage.
4. Select the triggered camera. The image or video from the triggered camera will pop up when the selected event occurs.
   To capture the picture of the triggered camera when the selected event occurs, you can also set the capture schedule and the storage in Storage Schedule.
5. Check the checkboxes to activate the linkage actions. For details, refer to *Table 14.1 Linkage Actions for Access Control Event*.
6. Click **Save** to save the settings.
7. You can click Copy to button to copy the access control event to other access control device, alarm input, access control point, or card reader.
   Select the parameters for copy, select the target to copy to, and click **OK** to confirm.

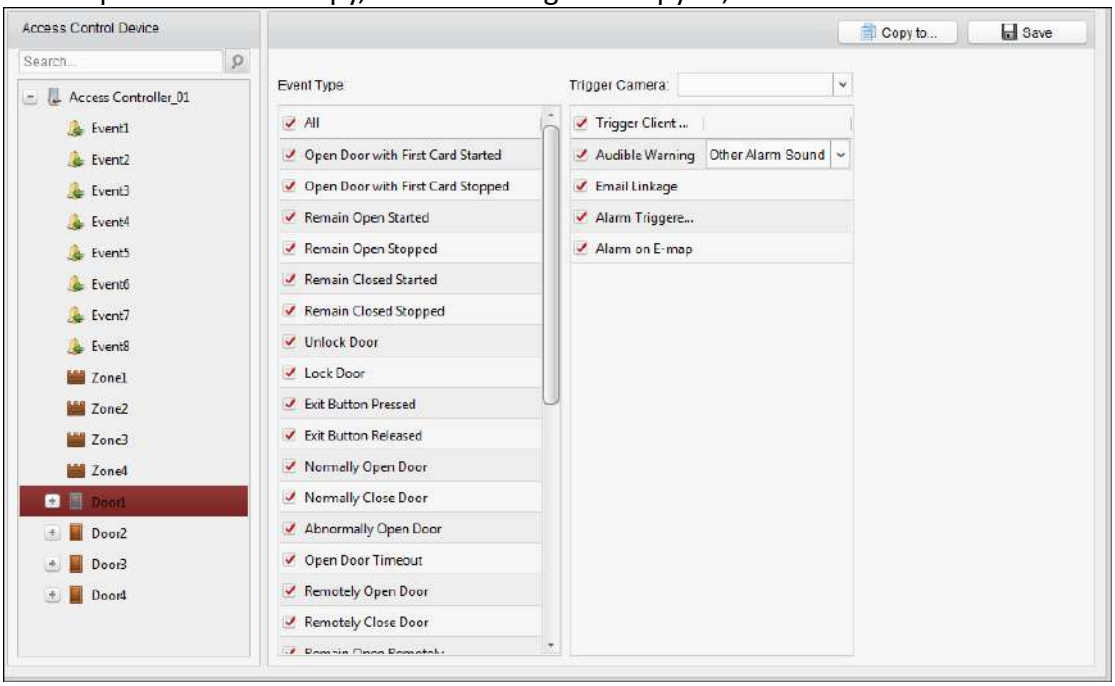


Table 1. 1 Linkage Actions for Access Control Event

Linkage Actions	Descriptions
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning.
Email Linkage	Send an email notification of the alarm information to one or more receivers.
Alarm on E-map	Display the alarm information on the E-map. ***Note:*** This linkage is only available to access control point and alarm input.

Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered.

7.10.2 Access Control Alarm Input Linkage

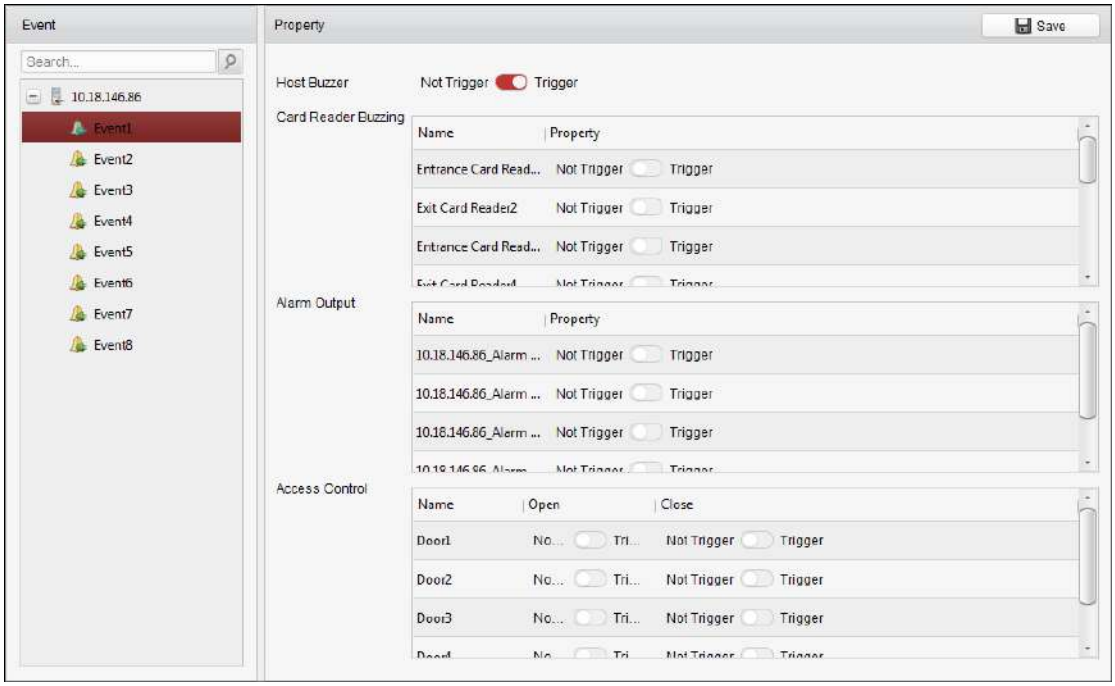
Purpose:

The access control alarm inputs can be linked to some actions (e.g., alarm output, host buzzer) when it is triggered.

Note: The linkage here refers to the linkage of the client software's own actions.

Steps:

1. Click **Access Control Alarm Input** tab to enter the following interface.



2. In the event list on the left, select an alarm input.
3. Switch the property from to to enable this action.
   Host Buzzer: The audible warning of controller will be triggered.
   Card Reader Buzzer: The audible warning of card reader will be triggered.
   Alarm Output: The alarm output will be triggered for notification.
   Access Control Point (Open/Close): The door will be open or closed when the case is triggered.
   Note: The Door cannot be configured as open or closed at the same time.
4. Click **Save** button to save the settings.

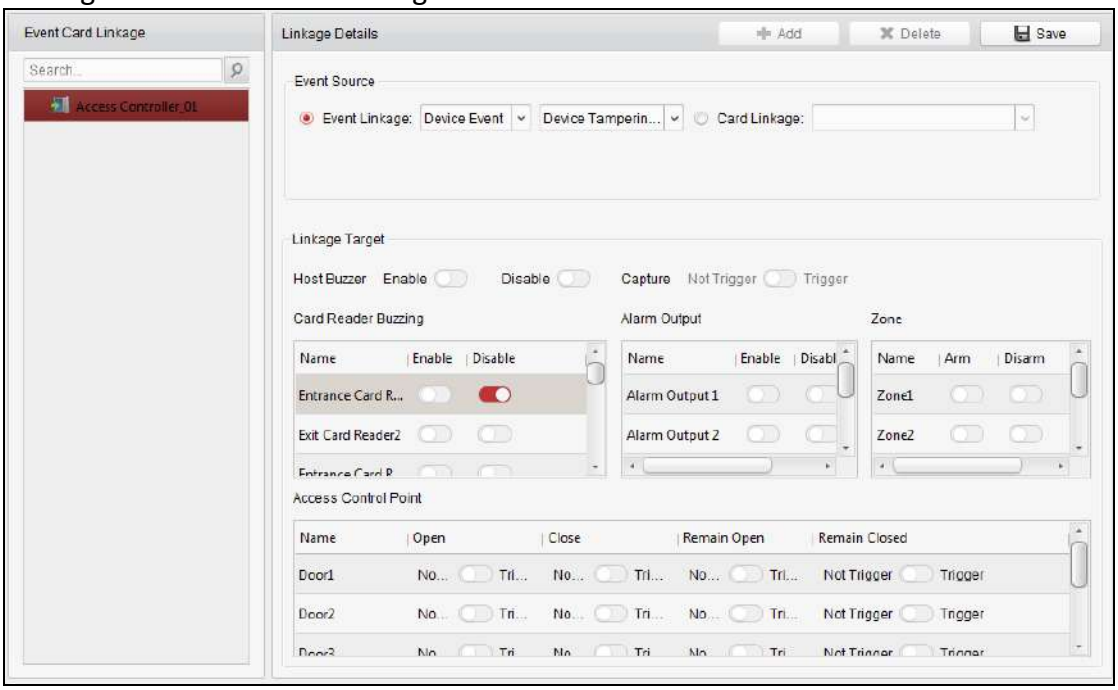
7.10.3 Event Card Linkage

Click **Event Card Linkage** tab to enter the following interface.

Notes:

- The Event Card Linkage should be supported by the device.

- The linkage here refers to the linkage of the client software's own actions.



Select the access control device from the list on the left.

Click **Add** button to add a new linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, and card reader event.

Steps:

1. Click to select the linkage type as **Event Linkage**, and select the event type from the dropdown list.
   - For Device Event, select the detailed event type from the dropdown list.
   - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
   - For Door Event, select the detailed event type and select the source door from the table.
   - For Card Reader Event, select the detailed event type and select the card reader from the table.
2. Set the linkage target, and switch the property from to to enable this function.
   - **Host Buzzer:** The audible warning of controller will be enabled/.
   - **Capture:** The real-time capture will be enabled.
   - **Card Reader Buzzer:** The audible warning of card reader will be enabled/disabled.
   - **Alarm Output:** The alarm output will be enabled/disabled for notification.
   - **Zone:** Arm or disarm the zone.
   - **Access Control Point:** The door status of open, close, remain open, and remain closed will be enabled.

     Notes:

- The door status of open, close, remain open, and remain close cannot be triggered at the same time.
- The target door and the source door cannot be the same one.

3. Click **Save** button to save and take effect of the parameters.

Card Linkage

Steps:

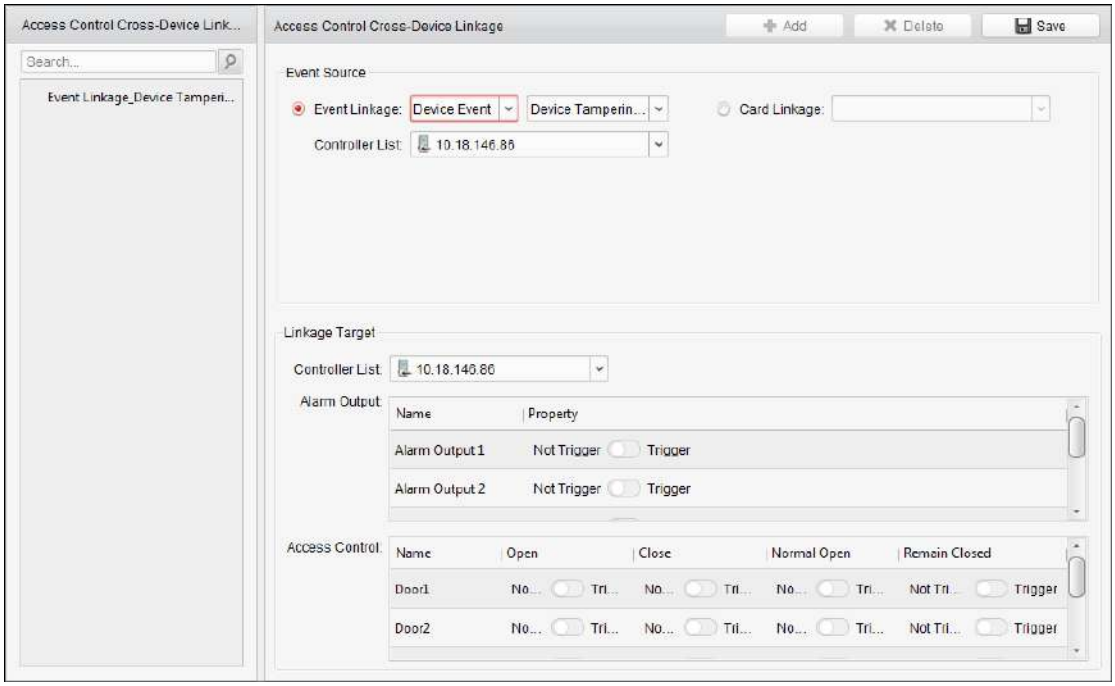
1. Click to select the linkage type as **Card Linkage**.
2. Input the card No. or select the card from the dropdown list.
3. Select the card reader from the table for triggering.
4. Set the linkage target, and switch the property from to  to enable this function.
   - **Host Buzzer:** The audible warning of controller will be enabled/disabled.
   - **Capture:** The real-time capture will be enabled.
   - **Card Reader Buzzer:** The audible warning of card reader will be enabled/disabled.
   - **Alarm Output:** The alarm output will be enabled/disabled for notification.
   - **Zone:** Arm or disarm the zone.
   - **Access Control Point:** The door status of open, close, remain open, and remain closed will be enabled.
5. Click **Save** button to save and take effect of the parameters.

7.10.4 Cross-Device Linkage

Purpose:

You can assign to trigger other access control device's action by setting up a rule when the access control event is triggered.

Click **Cross-Device Linkage** tab to enter the following interface.



Click **Add** button to add a new client linkage. You can select the event source as **Event Linkage** or **Card Linkage**.

Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, and card reader event.

Steps:

1. Click to select the linkage type as **Event Linkage**, select the access control device as event source, and select the event type from the dropdown list.
   - For Device Event, select the detailed event type from the dropdown list.
   - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
   - For Door Event, select the detailed event type and select the door from the table.
   - For Card Reader Event, select the detailed event type and select the card reader from the table.
2. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from to to enable this function.
   - **Alarm Output**: The alarm output will be triggered for notification.
   - **Access Control Point**: The door status of open, close, remain open, and remain close will be triggered. ***Note:*** The door status of open, close, remain open, and remain close cannot be triggered at the same time.
3. Click **Save** button to save parameters.

Card Linkage

Steps:

1. Click to select the linkage type as **Card Linkage**.

2. Select the card from the dropdown list and select the access control device as event source.
3. Select the card reader from the table for triggering.
4. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from to to enable this function.
   Alarm Output: The alarm output will be triggered for notification.
5. Click **Save** button to save parameters.

7.11 Door Status Management

Purpose:

The door status of the added access control device will be displayed in real time. You can check the door status and the linked event(s) of the selected door. You can control the status of the door and set the status duration of the doors as well.

7.11.1 Access Control Group Management

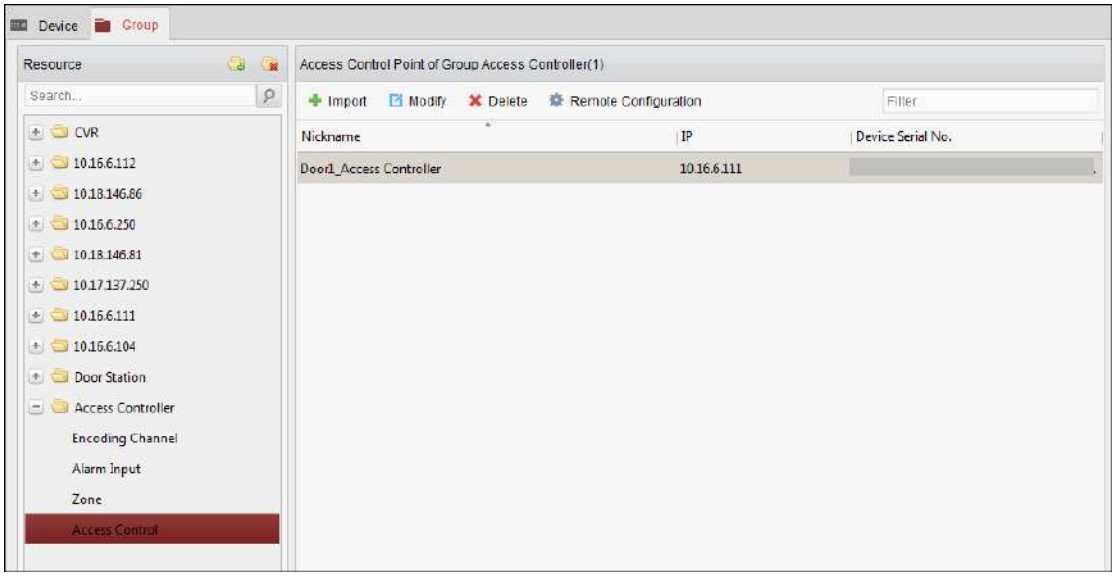
Purpose:

Before controlling the door status and setting the status duration, you are required to organize it into group for convenient management.

Perform the following steps to create the group for the access control device:

Steps:

1. Click on the control panel to open the Device Management page.
2. Click **Group** tab to enter the Group Management interface.



3. Perform the following steps to add the group.
   1) Click to open the Add Group dialog box.
   2) Input a group name as you want.
   3) Click **OK** to add the new group to the group list.
      You can also check the checkbox **Create Group by Device Name** to create the new group by

the name of the selected device.

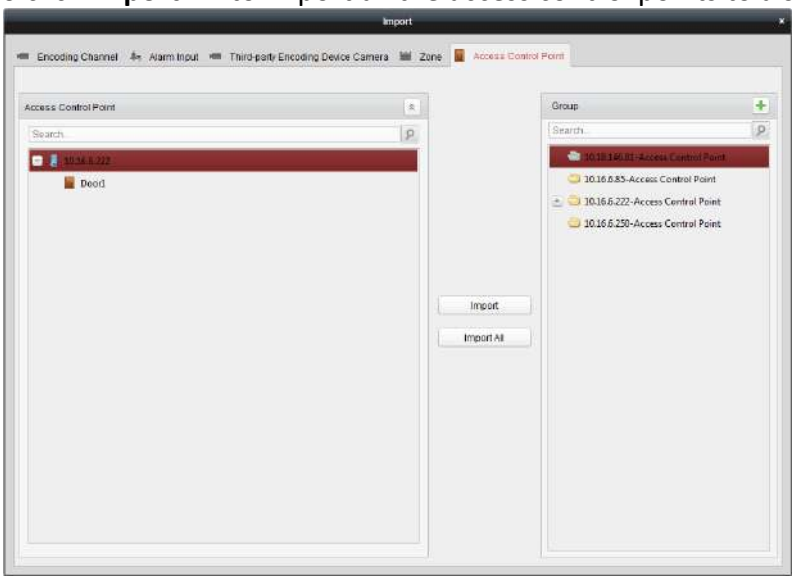


4. Perform the following steps to import the access control points to the group:
   1) Click **Import** on Group Management interface, and then click the **Access Control** tab to open the Import Access Control page.

      Notes:

      - You can also select **Alarm Input** tab and import the alarm inputs to group.
      - For the Video Access Control Terminal, you can add the cameras as encoding channel to the group.

   2) Select the names of the access control points in the list.
   3) Select a group from the group list.
   4) Click **Import** to import the selected access control points to the group.
      You can also click **Import All** to import all the access control points to a selected group.



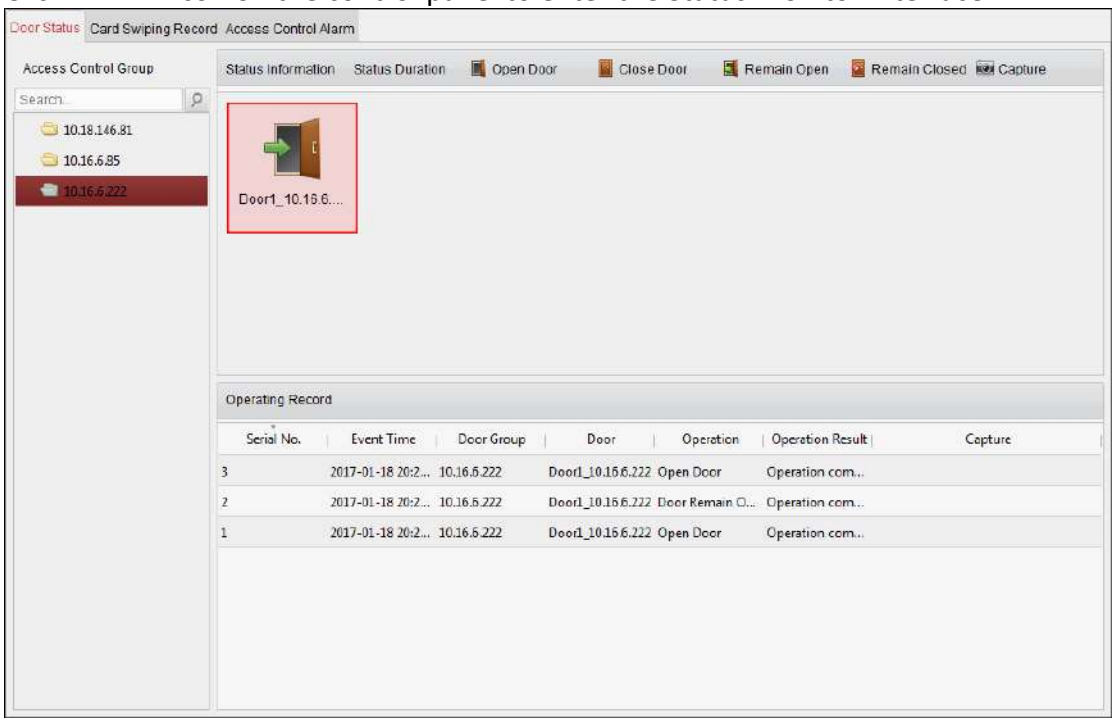
5. After importing the access control points to the group, you can click , or double-click the group/access control point name to modify it.

7.11.2 Anti-control the Access Control Point (Door)

Purpose:

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

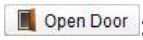
Click  icon on the control panel to enter the Status Monitor interface.



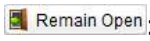
Steps:

1. Select an access control group on the left. For managing the access control group, refer to *Chapter 7.11.1 Access Control Group Management.*
2. The access control points of the selected access control group will be displayed on the right.

   Click icon  on the Status Information panel to select a door.
3. Click the following button listed on the **Status Information** panel to control the door.

    : Click to open the door once.

    : Click to close the door once.

    : Click to keep the door open.

    : Click to keep the door closed.

    : Click to capture the picture manually.
4. You can view the anti-control operation result in the Operation Log panel.

Notes:

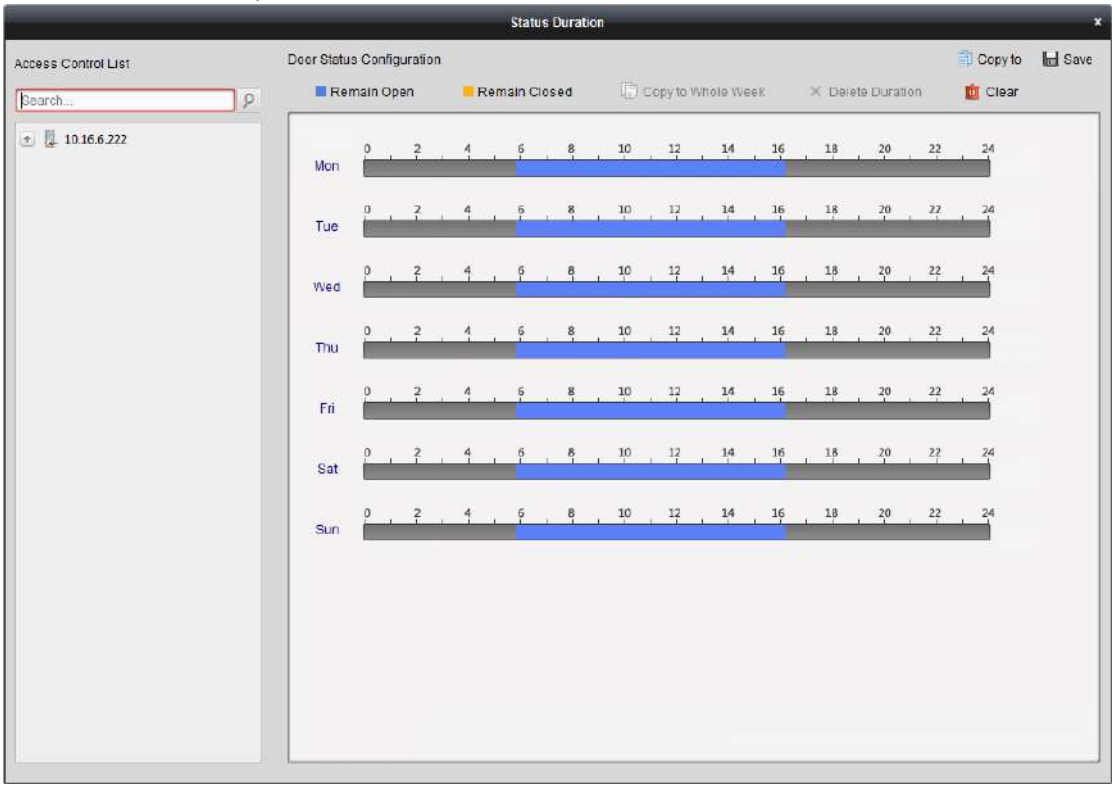
- If you select the status as **Remain Open/Remain Closed**, the door will keep open/closed until a new anti-control command being made.
- The **Capture** button is available when the device supports capture function. And it cannot be realized until the storage server is configured.
- If the door is in remain closed status, only super card can open the door or open door via the client software.

7.11.3 Status Duration Configuration

Purpose:

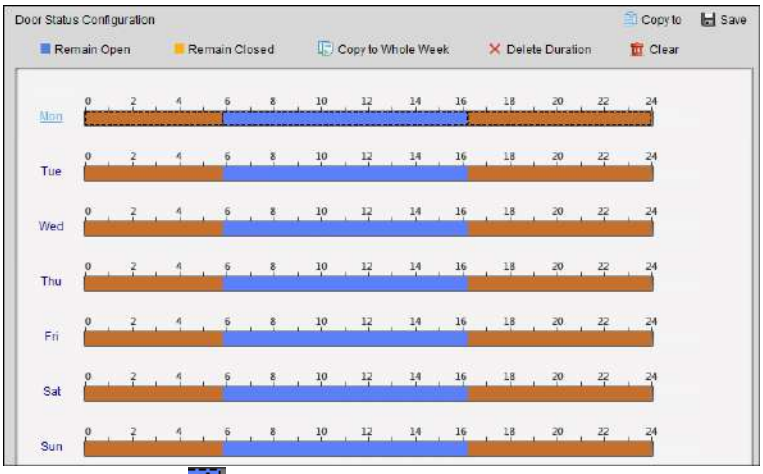
You can schedule weekly time periods for an access control point (door) to remain open or remain closed.

In the Door Status module, click **Status Duration** button to enter the Status Duration interface.



Steps:

1. Click to select a door from the access control device list on the left.
2. On the Door Status Configuration panel on the right, draw a schedule for the selected door.
   1) Select a door status brush as Remain Open or Remain Closed.
      Remain Open: The door will keep open during the configured time period. The brush is marked as .
      Remain Closed: The door will keep closed during the configured duration. The brush is marked as .
   2) Click and drag on the timeline to draw a color bar on the schedule to set the duration.

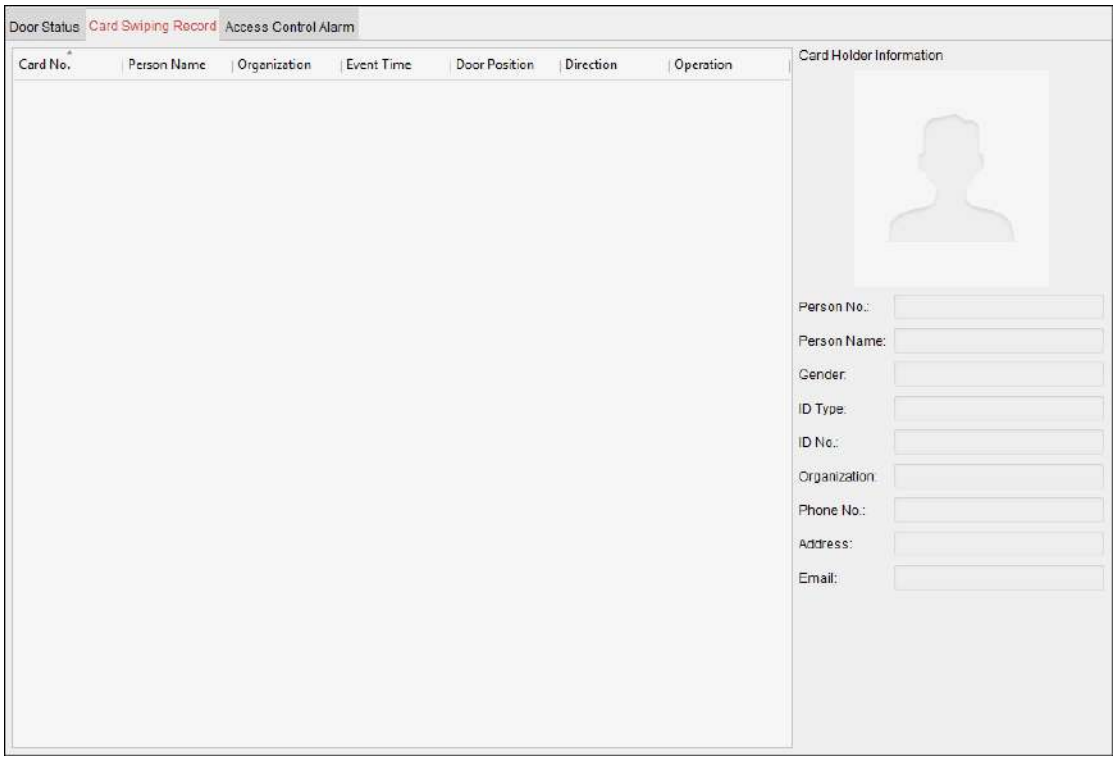


3) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
   When the cursor turns to , you can lengthen or shorten the selected time bar.

3. Optionally, you can select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
4. You can select the time bar and click **Delete Duration** to delete the time period.
   Or you can click **Clear** to clear all configured durations on the schedule.
5. Click **Save** to save the settings.
6. You can click **Copy to** button to copy the schedule to other doors.

7.11.4 Real-time Card Swiping Record

Click **Card Swiping Record** tab to enter the following interface.



The logs of card swiping records of all access control devices will display in real time. You can view the details of the card swiping event, including card No., person name, organization, event time, etc.

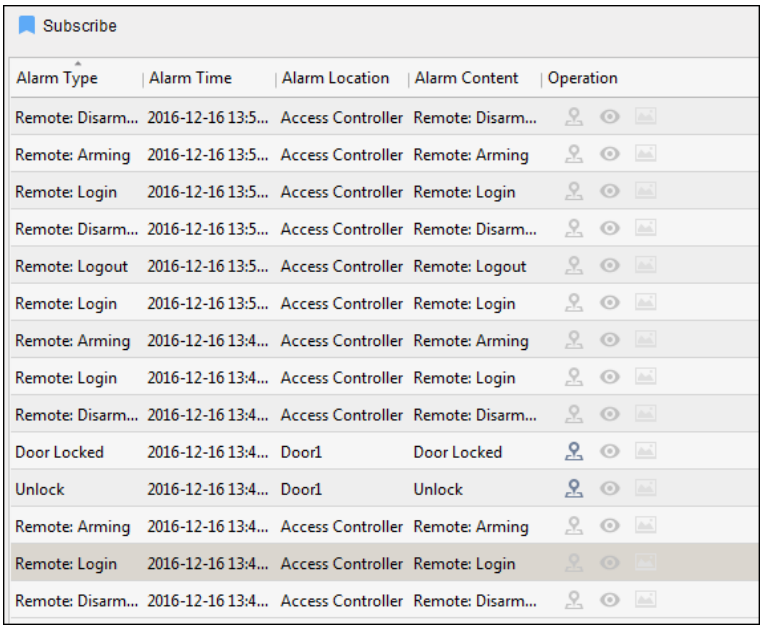
You can also click the event to view the card holder details, including person No., person name, organization, phone, contact address, etc.

7.11.5 Real-time Access Control Alarm

Purpose:

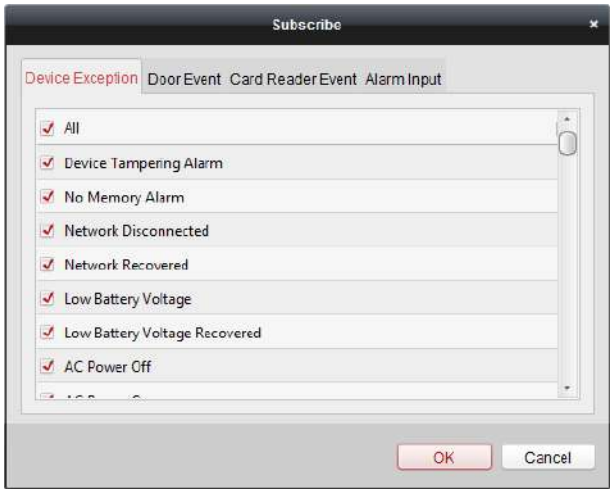
The logs of access control events will be displayed in real time, including device exception, door event, card reader event, and alarm input.

Click **Access Control Alarm** tab to enter the following interface.



Steps:

1. All access control alarms will display in the list in real time.
   You can view the alarm type, alarm time, location, etc.
2. Click to view the alarm on E-map.
3. You can click or to view the live view or the captured picture of the triggered camera when the alarm is trigged.
   Note: For setting the triggered camera, refer to *Chapter 7.10.1 Access Control Event Linkage.*
4. Click **Subscribe** to select the alarm that the client can receive when the alarm is triggered.



   1) Check the checkbox(es) to select the alarm(s), including device exception alarm, door event alarm, card reader alarm, and alarm input.
   2) Click **OK** to save the settings.

7.12 Arming Control

Purpose:

You can arm or disarm the device. After arming the device , the client can receive the alarm information from the device.

Steps:

1. Click **Tool->Device Arming Control** to pop up the Device Arming Control window.
2. Arm the device by checking the corresponding checkbox.
   Then the alarm information will be auto uploaded to the client software when alarm occurs.



Appendix A Sound Prompt and Indicator

After the card reader is powered on, LED status indicator will turn blue and blink for 1 time. Then it will turn red and blink for 3 times. At last the buzzer will send out a beep sound indicating the starting up process is completed.

During using the card reader, it will send out different sounds prompt and the LED indicator on it have different statuses. You can refer to tables below for detailed information.

Table 7-1 Description of Prompt Sound

Sound Prompt	Description
One beep	RS-485 protocol: Pressing keys prompt; Swiping card prompt; Time out prompt for pressing keys or swiping card. Wiegand protocol: Pressing keys prompt; Swiping card prompt.
Two rapid beeps	The operation of pressing keys or swiping card is valid.
Three slow beeps	The operation of pressing keys or swiping card is invalid.
Rapidly continuous beeps	Alarm of tamper-proof.
Slowly continuous beeps	The card reader is unencrypted.

Table 7-2 Description of LED Indicator

LED Indicator Status	Description
Green and blinking	Card reader is working normally.
Solid green	The operation of pressing keys or swiping card is valid.
Solid red	The operation of pressing keys or swiping card is invalid.
Red and blinking	For RS-485 protocol: Registering failed or card reader is offline. Failed to get key files of PSAM card; Failed to detect the PSAM card.
Red and Keeping rapidly blinking	Available for reading file mode of CPU card: PSAM is not inserted or undetected.

Appendix B Custom Wiegand Rule Descriptions

Take Wiegand 44 as an example, the setting values in the Custom Wiegand tab are as follows:

Custom Wiegand Name:	Wiegand 44					
Total Length	44					
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]					
Parity Mode	XOR Parity					
Odd Parity Start Bit		Length				
Even Parity Start Bit		Length				
XOR Parity Start Bit	0	Length per Group	4	Total Length	40	
Card ID Start Bit	0	Length	32	Decimal Digit		10
Site Code Start Bit		Length		Decimal Digit		
OEM Start Bit		Length		Decimal Digit		
Manufacturer Code Start Bit	32	Length	8	Decimal Digit		3

Wiegand Data = Valid Data + Parity Data

Total Length: Wiegand data length.

Transportation Rule: 4 bytes. Display the combination types of valid data. The example displays the combination of Card ID and Manufacturer Code. The valid data can be single rule, or combination of multiple rules.

Parity Mode: Valid parity for wiegand data. You can select either odd parity or even parity.

Odd Parity Start Bit, and Length: If you select Odd Parity, these items are available. If the odd parity start bit is 1, and the length is 12, then the system will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0. (Bit 0 is the first bit.)

Even Parity Start Bit, and Length: If you select Even Parity, these items are available. If the even parity start bit is 12, and the length is 12, then the system will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

XOR Parity Start Bit, Length per Group, and Total Length: If you select XOR Parity, these items are available. Depending on the table displayed above, the start bit is 0, the length per group is 4, and the total length is 40. It means that the system will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits. (The result length is the same as the length per group.)

Card ID Start Bit, Length, and Decimal Digit: If you use the transformation rule, these items are available. Depending on the table displayed above, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The

length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit: If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit: If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit: If you use the transformation rule, these items are available. Depending on the table displayed above, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

0200001080228


See Far, Go Further