Main Elevator Controller

User Manual

User Manual

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

This manual is applied for main elevator controller.

Name	Model
Main Elevator Controller	DS-K2210

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.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

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 RE Directive 2014/53/EU, the EMC Directive 2014/30/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

Use only power supplies listed in the user instructions:

Model	Manufacturer	Standard
C2000IC12.0-24P-DE	MOSO Power Supply Technology Co., Ltd.	CEE
C2000IC12.0-24P-GB	MOSO Power Supply Technology Co., Ltd.	BS

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 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 8
1.1 Introduction 8
1.2 Main Features 8
Chapter 2 Appearance 9
2.1 Device Appearance Introduction 9
2.2 Indicator Information 10
Chapter 3 Installation 11
Chapter 4 Device Wiring 12
Chapter 5 Activation 14
5.1 Activating via Web Client 14
5.2 Activating via SADP Software 14
5.3 Activating via Client Software 16
Chapter 6 Web Client Operation 19
6.1 Overview 19
6.1.1 Introduction 19
6.1.2 Running Environment 19
6.2 Login/Logout Web Client 19
6.2.1 Login 19
6.2.2 Logout 20
6.3 Setting Device via Web Client 20
6.3.1 System Settings 20
6.3.2 Network Settings 22
6.3.3 System Maintenance 23
6.3.4 Elevator Control Settings 24
Chapter 7 Client Operation 28
7.1 User Registration and Login 28
7.2 System Configuration 29
7.3 Access Control Management 29
7.3.1 Adding Access Control Device 30
7.3.2 Viewing Device Status 45
7.3.3 Editing Basic Information 46
7.3.4 Network Settings 47
7.3.5 RS-485 Settings 49
7.3.6 Remote Configuration 50

7.4 Organization Management 55
7.4.1 Adding Organization 55
7.4.2 Modifying and Deleting Organization 55
7.5 Person Management 55
7.5.1 Adding Person 56
7.5.2 Managing Person 66
7.5.3 Issuing Card in Batch 66
7.6 Schedule and Template 68
7.6.1 Week Schedule 69
7.6.2 Holiday Group 70
7.6.3 Template 71
7.7 Permission Configuration 73
7.7.1 Adding Permission 74
7.7.2 Applying Permission 75
7.8 Advanced Functions 76
7.8.1 Access Control Parameters 76
7.8.2 Card Reader Authentication 78
7.8.3 Open Door with First Card 80
7.8.4 Relay Settings 81
7.9 Searching Access Control Event 84
7.9.1 Searching Local Access Control Event 85
7.9.2 Searching Remote Access Control Event 85
7.10 Access Control Event Configuration 86
7.10.1 Access Control Event Linkage 86
7.10.2 Event Card Linkage 87
7.10.3 Cross-Device Linkage 89
7.11 Door Status Management 91
7.11.1 Access Control Group Management 91
7.11.2 Controlling Floor Status 93
7.11.3 Status Duration Configuration 94
7.11.4 Real-time Card Swiping Record 95
7.11.5 Real-time Access Control Alarm 96
7.12 Arming Control 98

Updated

- Optimize the NTP and DST function.
- Support connecting to fingerprint and card reader.
- Get the armed device IP address via the client software.
- If swiping card when the door is in sleep mode, the authentication will be failed and the client software will receive the event.
- If swiping card when the card reader is in sleep mode, the authentication will be failed and the client software will receive the event.
- Optimize card effective date format
- Optimize relay time
- Add IP addresses conflicted alarm

Chapter 1 Overview

1.1 Introduction

The elevator controller contains main elevator controller and distributed elevator controller. It can be applied to buildings, public areas and so on. The main elevator controller can communicate with the distributed elevator controller, the card reader, the video intercom devices, etc. via RS-485. You can also control the main elevator controller by the web client, guarding expert access control client software and other systems.

1.2 Main Features

- TCP/IP communication, Wiegand communication and RS-485 communication
- Manages the distributed elevator controller via the RS-485 connection
- Manages the video intercom device via the RS-485 connection
- Connection of the fire alarm button, the panic button and the maintenance button
- Connectable with up to 24 distributed elevator controllers
- Multiple authentication modes: Card, Fingerprint, Card and Fingerprint, Card and Password, Employee ID and Password, Super Password and Duress Code
- Calling elevator by visitor or by resident
- Remote control of the main elevator controlling via the web client, the guarding expert access control client software, or other systems
- Connectable to the Third party system
- Supports managing the floor status through the main elevator controller. The floor status includes “Disable”, “Controlled”, and ”Free”
- Linkage of the distributed elevator controller and reporting the alarm event to the system
- IP addresses conflicted alarm
- NTP and DST

Chapter 2 Appearance

2.1 Device Appearance Introduction

The device appearance introduction is shown as follows:

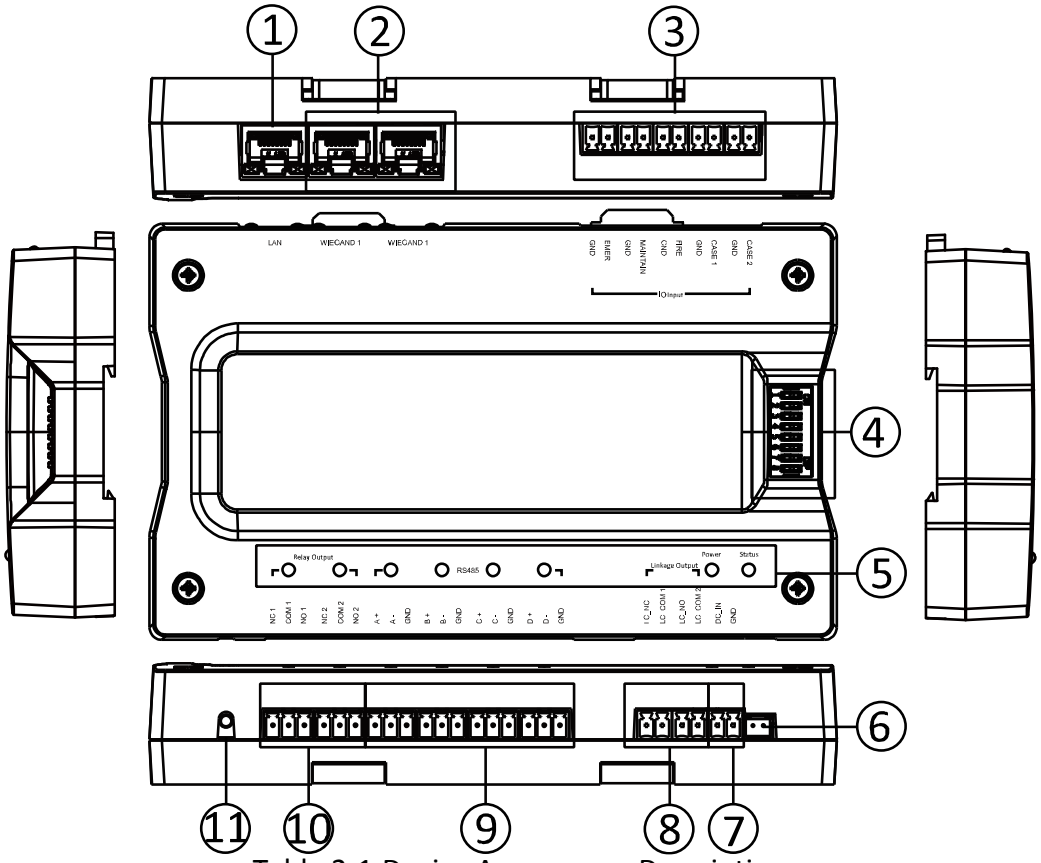


Table 2-1 Device Appearance Description

No.	Description
1	Tamper-Proof
2	Wiegand Terminal
3	IO Input Terminal
4	DIP Switch (Reserved)
5	Indicator
6	Tamper-Proof Interface
7	Power Input
8	Linkage Output Terminal
9	RS-485 Terminal
10	Relay Output Terminal
11	GND Tread Interface

2.2 Indicator Information

The indicator information is as follows:

Table 2-2 Indicator Description

Description	Indicator
Relay NC Closed	Off
Relay NO Closed	Solid Green
Serial Port Not Communicating	Off
Serial Port Communicating	Solid Green
Network Disconnected	Off
Network Cable Connected	Solid Yellow, Flashing Green
Network Armed	Solid Yellow, Flashing Green
Power On	Solid Green
Running Properly	Flashing Green
Running Exception	Solid Red

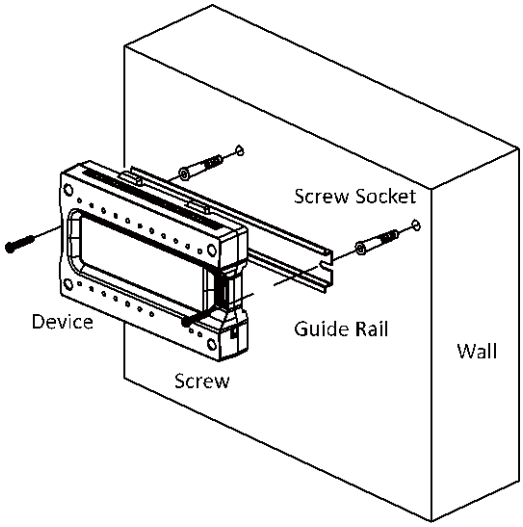
Chapter 3 Installation

Before your start:

- The minimum bearing weight of the wall or other places should be three times heavier than the device weight.
- Dial-up before you install.

Steps:

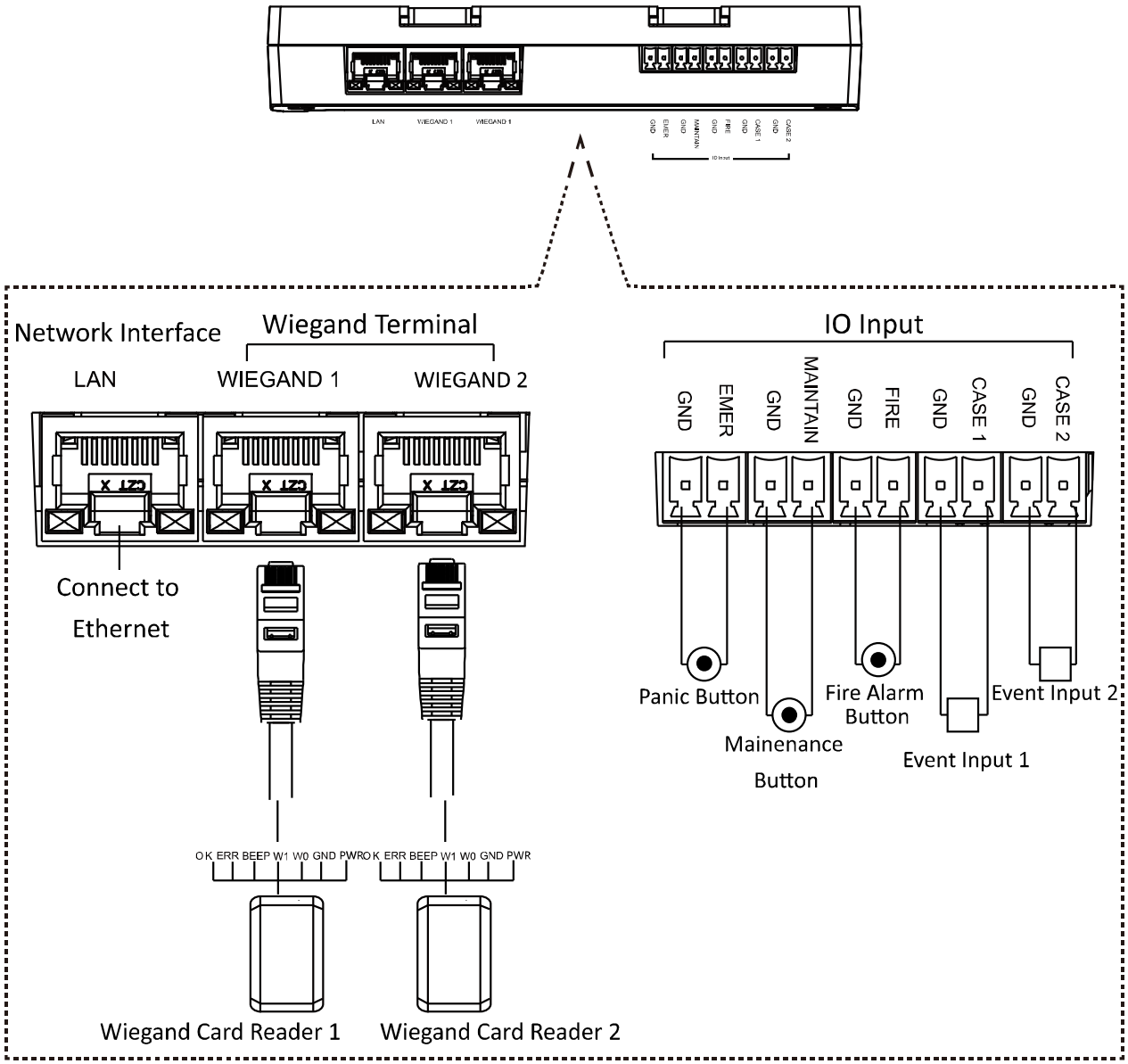
1. Drill holes on the wall or other places according to the holes on the guide rail.
2. Insert the screw sockets of the set screws (supplied) in the drilled holes.
3. Secure the guide rail on the wall or other places with the screws (supplied).
4. Push the device to the guide rail and fix it.



Chapter 4 Device Wiring

When the panic button, the maintenance button, fire alarm button, and the event alarm are triggered, the main elevator controller will control the distributed controller to perform the linked actions via the linkage output.

The wiring of the device upper side is as follows:



Notes:

- When the panic button is triggered, all relays keep connected. It is valid for all floors.
- When the fire alarm button is triggered, all relays keep disconnected. It is invalid for all floors.
- When the maintenance button is triggered, all relays keep disconnected. It is invalid for all floors.

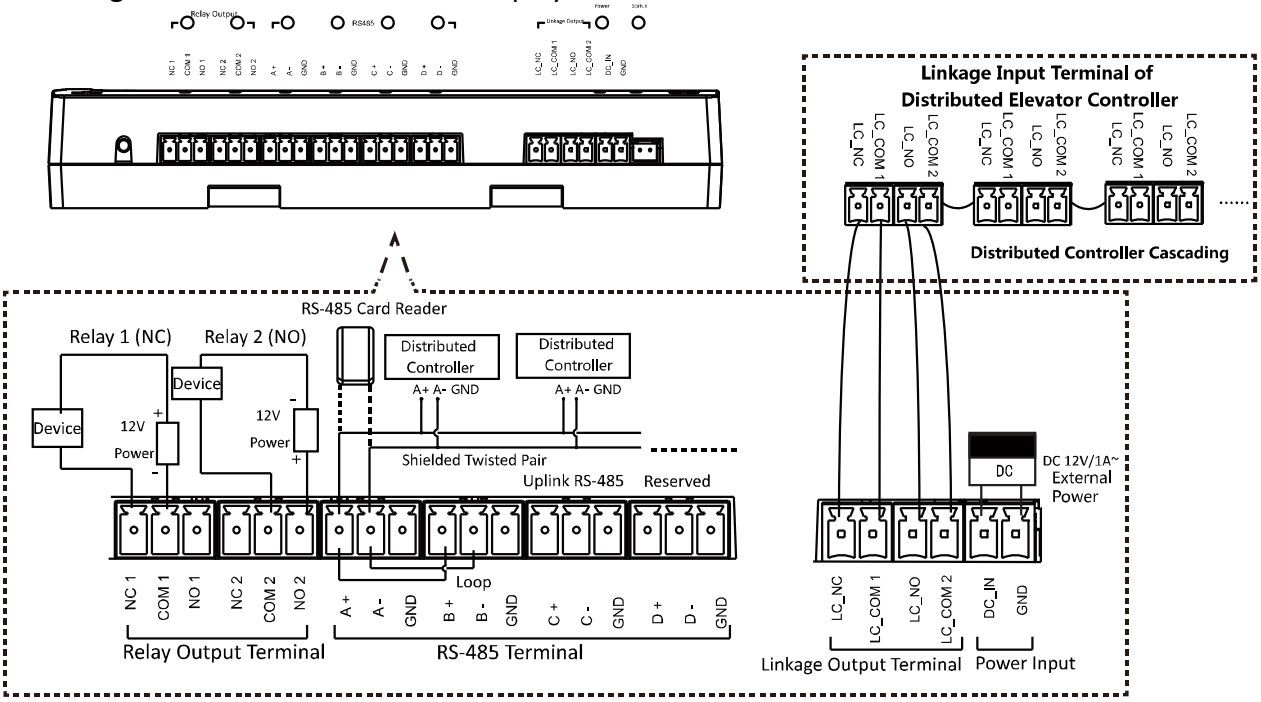
Cautions

- The maximum power supply for the relay is DC 30 V, 2 A or AC 125 V, 0.5A.
- Confirm with elevator manufacturers on wiring methods to avoid faults caused by wrong wiring.

The Wiegand sequence is displayed as follows:

Wiegand Sequence		
	Orange&White	OK
	Orange	ERR
	Green&White	BEEP
	Blue	W1
	Blue&White	W0
	Green / Brown&White	GND
	Brown	12V

The wiring of the device lower side is displayed as follows:



Notes:

- Each main elevator controller supports up to 24 distributed elevator controllers, including 8 call elevator distributed controllers, 8 auto button distributed controllers, and 8 button distributed controllers.

Cautions

- The maximum power supply for the relay is DC 30 V, 2 A or AC 125 V, 0.5A.
- Confirm with elevator manufacturers on wiring methods to avoid faults caused by wrong wiring.

Chapter 5 Activation

Purpose:

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

Activation via the web client, activation via SADP, and activation via client software are supported.

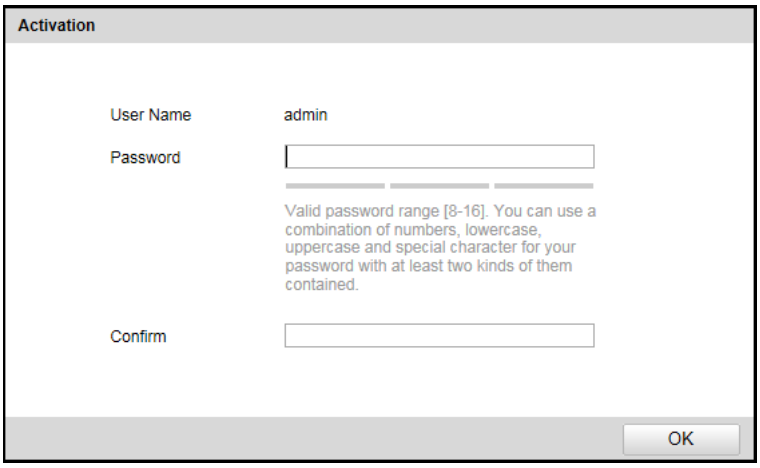
The default values of the control terminal are as follows.

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

5.1 Activating via Web Client

Steps:

1. Open the web browser.
2. For your first login, input the IP address of the main elevator controller to enter device activation interface.



3. Input the password and confirm the password.

<u>STRONG PASSWORD RECOMMENDED</u>– *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 **OK** to activate the device. You will login the web client automatically.
   Note: The device IP segment should be the same with the PC's.

5.2 Activating via SADP Software

Purpose:

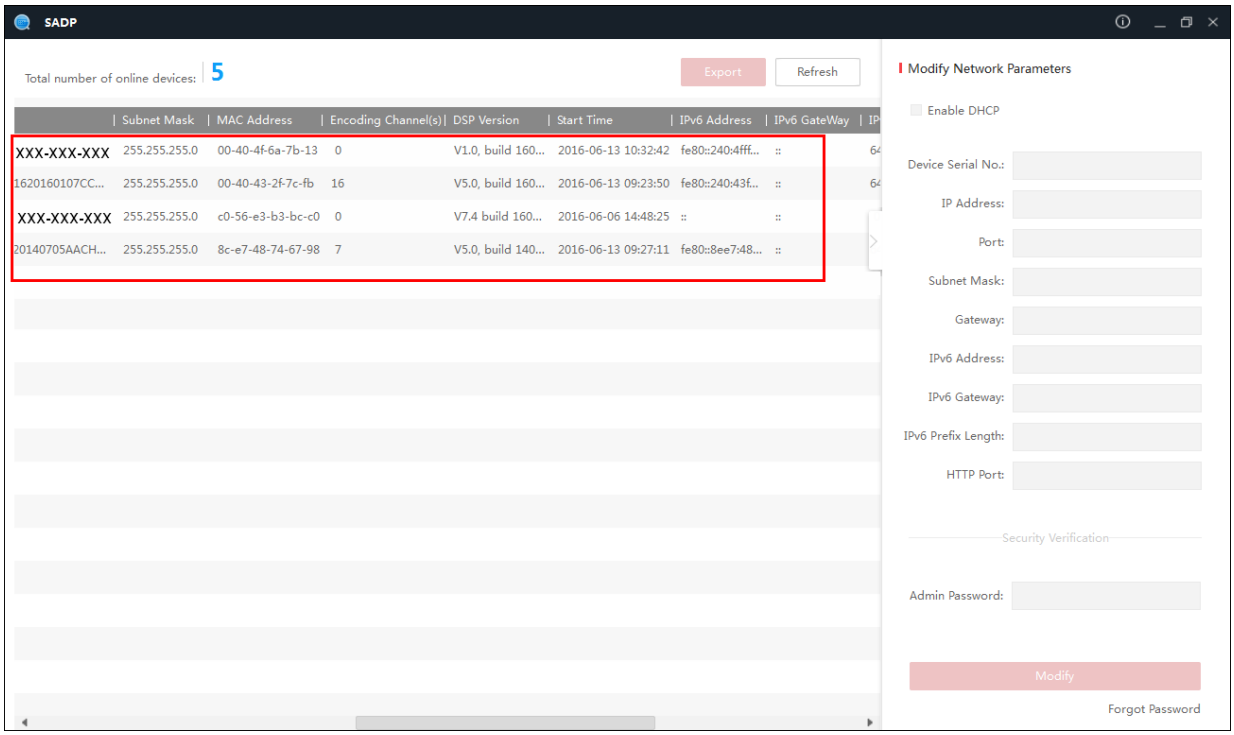
SADP software is used for detecting the online device, activating the device, and resetting the

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 device.

Steps:

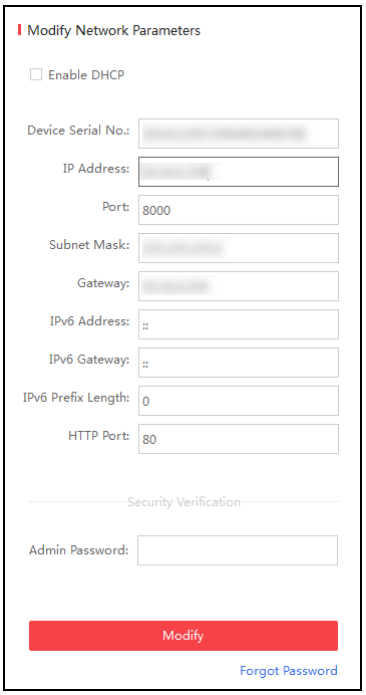
1. Run the SADP software to search the online devices.
2. Check the device status from the device list, and select an inactive device.



3. Create a password 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 editing the IP address manually or checking the Enable DHCP checkbox.



6. Input the password and click **Modify** to save the IP address.

5.3 Activating via Client Software

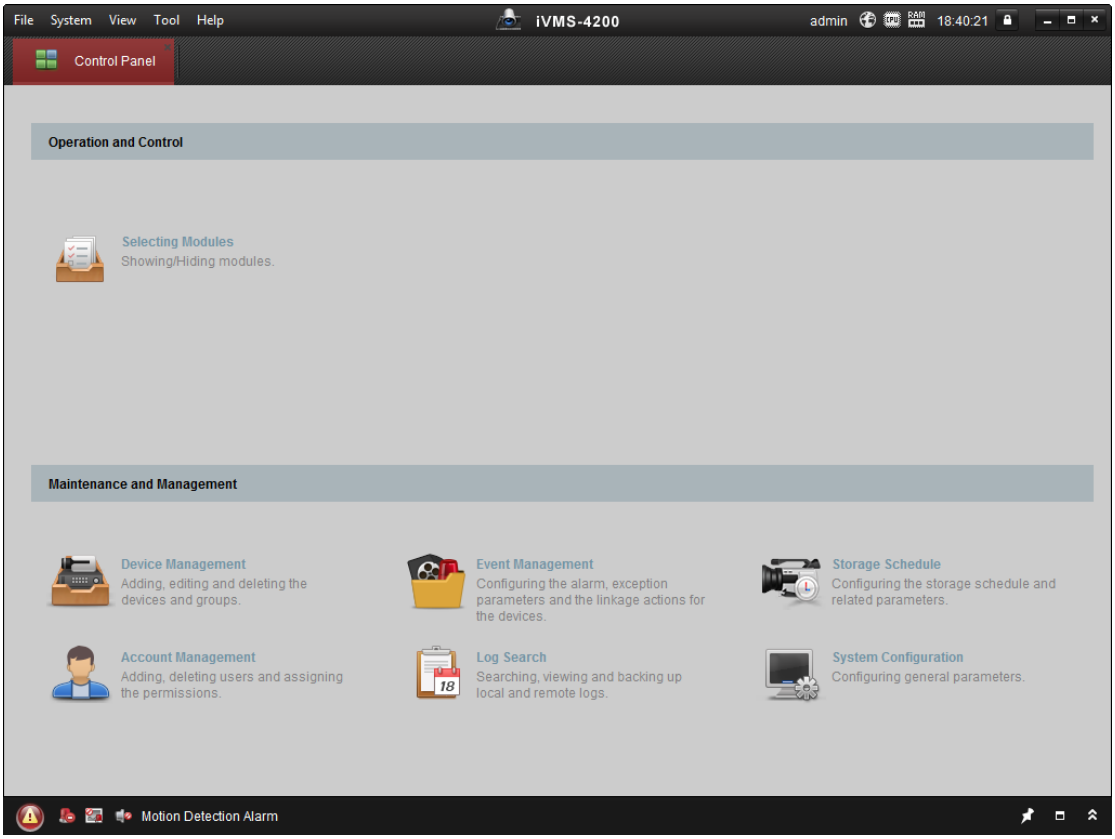
Purpose:

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

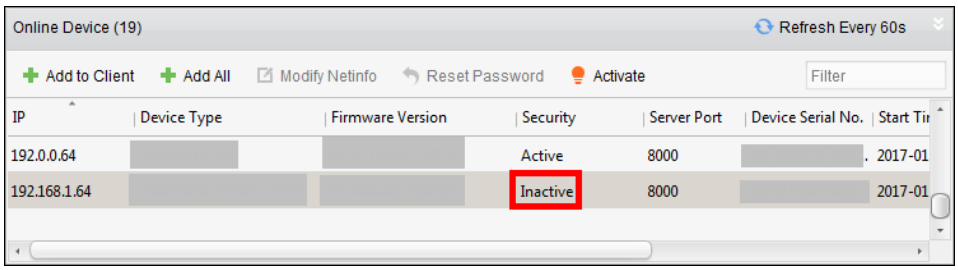
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

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



2. Click **Device Management** to enter the Device Management interface.
3. Select an inactive device.



4. Check the device status from the device list, and select an inactive device.
5. Click **Activate** to pop up the Activation interface.
6. 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.*

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

Chapter 6 Web Client Operation

6.1 Overview

6.1.1 Introduction

You can access to the elevator controller via the web browser for remote elevator controller management. You can control the elevator, check the elevator running status, and configure the elevator parameters via the web client.

6.1.2 Running Environment

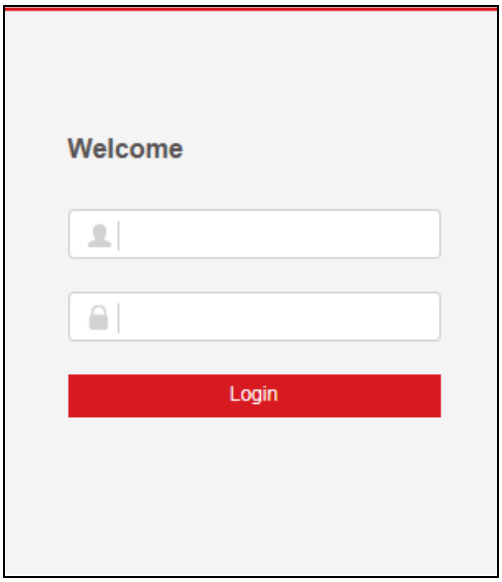
Operating System: Microsoft Windows XP SP1 or later
CPU: Intel Pentium 2.0GHz or later
RAM (Memory): 1G or more
Display: Resolution of 1024 X 768 or higher
Web Browser: Internet Explorer 8.0 or later; Mozilla Firefox 5.0 or later; Google Chrome 18 or later

6.2 Login/Logout Web Client

Before you start:
Make sure the device is activated. For details, refer to 5.1 Activating via Web Client.

6.2.1 Login

Steps:
1. Open the web browser and input the device IP in the address field.
2. Click **Enter** key on your keyboard to enter the login page.



3. Input the user name and the password.
4. Click **Login** to enter the device web client.

Notes:

- The device IP address will be locked if logging in with the wrong password for 5 times. The locking duration is 30min.
- Up to 16 web clients can be online at the same time.

6.2.2 Logout

Steps:

1. In the web client interface, click the **Logout** button on the upper right side of the page.
2. Click **Yes** in the pop-up dialog box to log out.

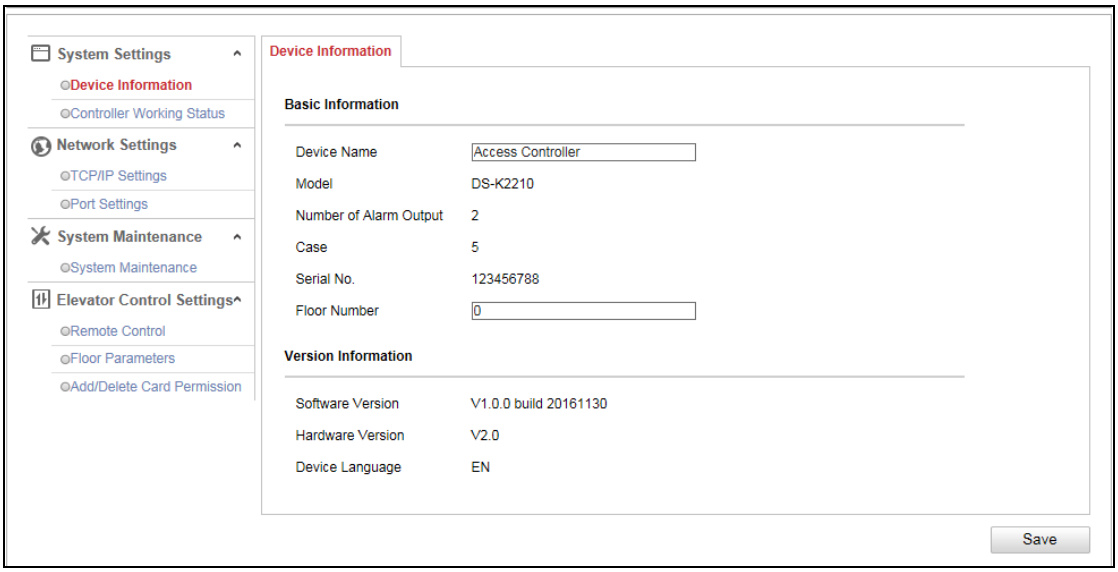
6.3 Setting Device via Web Client

6.3.1 System Settings

Managing Device Information

Steps:

1. Click **System Settings** –> **Device Information** to enter the Device Information page.

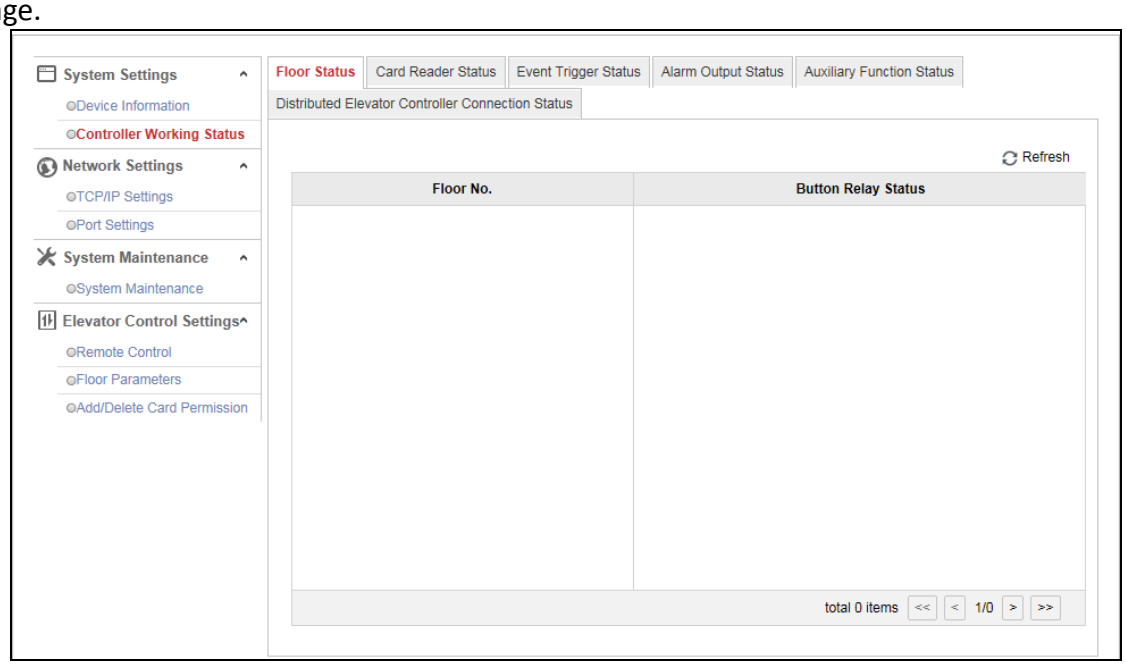


2. Check the device basic information (including the device name, the device type, the alarm output No., the case, the device serial No. and the floor number) and the version information (including the software version, the device language, and the hardware version).
3. (Optional) Edit the device name and the floor No.
4. Click **Save** to save the settings.

Checking Controller Working Status

Steps:

1. Click **System Settings** -> **Controller Working Status** to enter the Controller Working Status page.



2. Check the floor status, the card reader status, the event trigger status, the alarm output status, the auxiliary function status, the distributed elevator controller connection status. For more information, refer to Table 6-1.

Table 6-1 Status Information Table

Floor Status	Floor Status No.

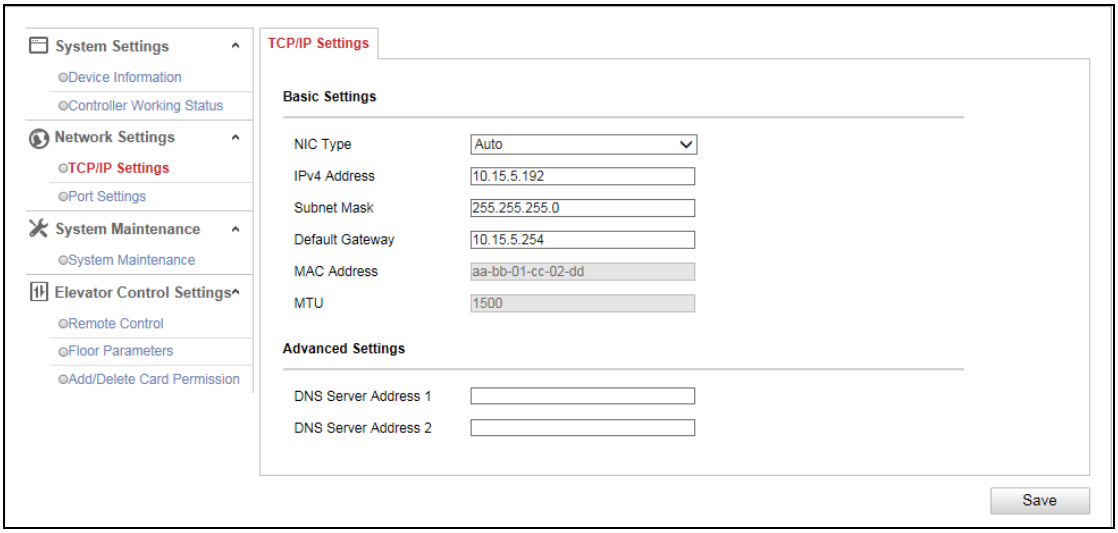
	Button Relay Status: Open, Close
Card Reader Status	Card Reader No.
	Online Status: Online, Offline
	Tamper-Proof Status: Open, Close
	Verification Type: Card, Card and Password, Card or Password, Fingerprint, Fingerprint and Password, Card or Fingerprint, Card and Fingerprint, Card and Fingerprint and Password, Employee ID and Password, etc.
Event Trigger Status	Event Trigger No.
	Status: Triggered, Not Triggered
Alarm Output Status	Alarm Output No.
	Status: Triggered, Not Triggered
Auxiliary Function Status	Power Supply Status
	Card Added
	Main Controller Tamper-Proof
Distributed Elevator Controller Connection Status	Distributed Elevator Controller No.
	Status: Online, Offline

6.3.2 Network Settings

Setting TCP/IP

Steps:

1. Click **Network Settings** -> **TCP/IP Settings** to enter the TCP/IP Settings page.



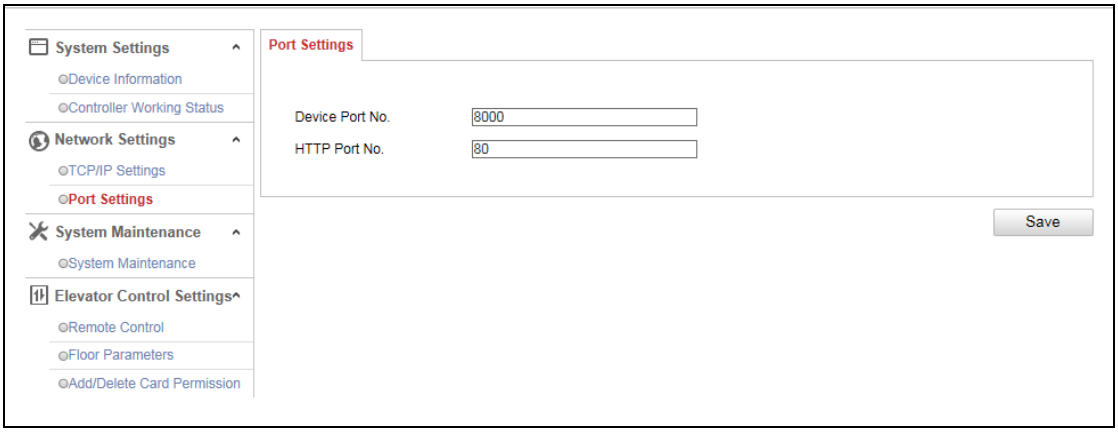
2. Check or edit the device network parameters. You are able to set the NIC type, the device IPv4 address, the subnet mask, the default gateway, the DNS1 server address and the DNS2 server address.
   You can also check the MAC address and the MTU.

3. Click **Save** to the settings.

Setting Port

Steps:

1. Click **Network Settings** -> **Port Settings** to enter the Port Settings page.



2. Check and edit the device port No. and the HTTP port.
3. Click **Save** to save the settings.

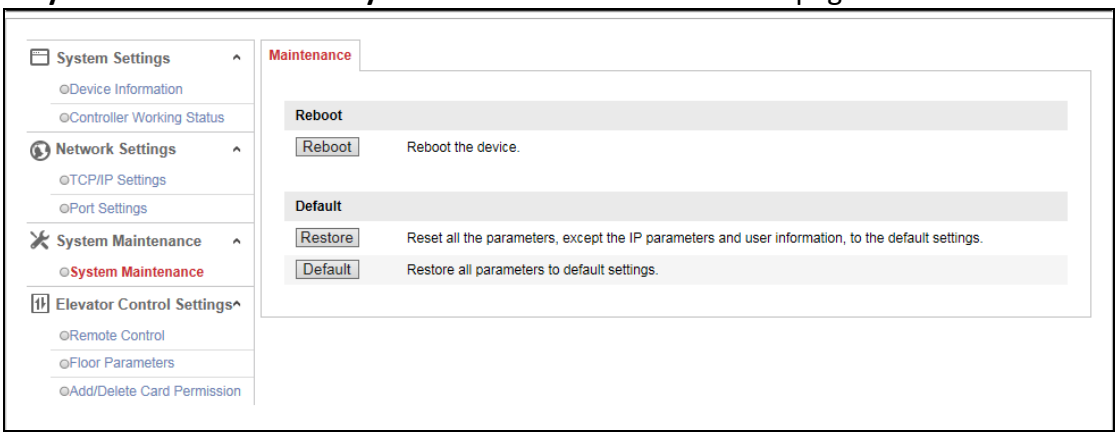
Notes:

- The default device port No. is 8000.
- The default device HTTP port is 80.

6.3.3 System Maintenance

Steps:

1. Click **System Maintenance** -> **System Maintenance** to enter the page.



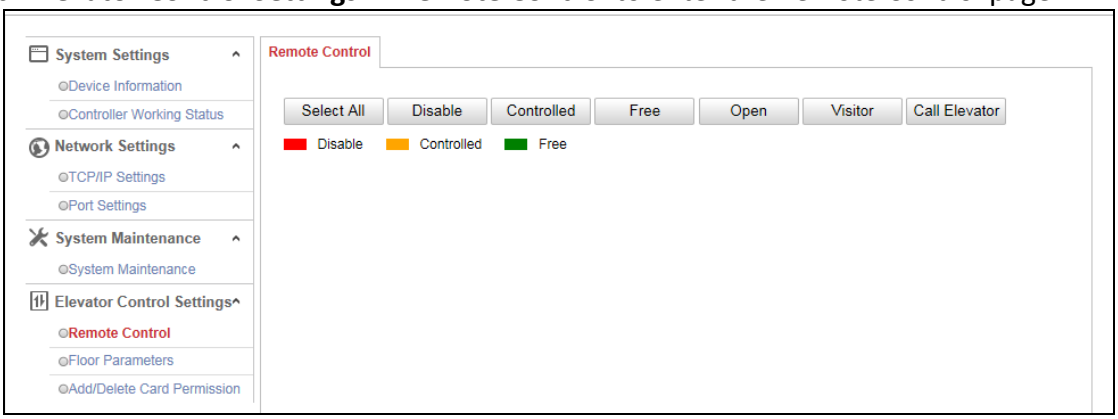
2. Click **Reboot** to remotely reboot the device.
   Or click **Restore** to reset all parameters, except the IP parameters and user parameters and user information to the default settings.
   Or click **Default** to reset all parameters to the default settings.

6.3.4 Elevator Control Settings

Setting Remote Control

Steps:

1. Click **Elevator Control Settings** -> **Remote Control** to enter the Remote Control page.



2. Check the floor button that need to control (multiple choice is allowed).
   Or click **Select All** to check all floor buttons.
3. Click the control button in the interface to control the floor button. You can select **Disable**, **Controlled**, **Free**, **Open**, **Visitor (Call Elevator by Visitor)**, or **Call Elevator (Call Elevator by Resident)**.
   Disable: You cannot go to the selected floor.
   Controlled: You should swipe the card to press the selected floor button. And the elevator can got to the selected floor.
   Free: The selected floor button will be valid all the time.
   Open: The floor button will be valid for a period of time.
   Visitor: The elevator will go down to the first floor. The visitor can only press the selected floor button.
   Call Elevator: Call the elevator to the selected floor.

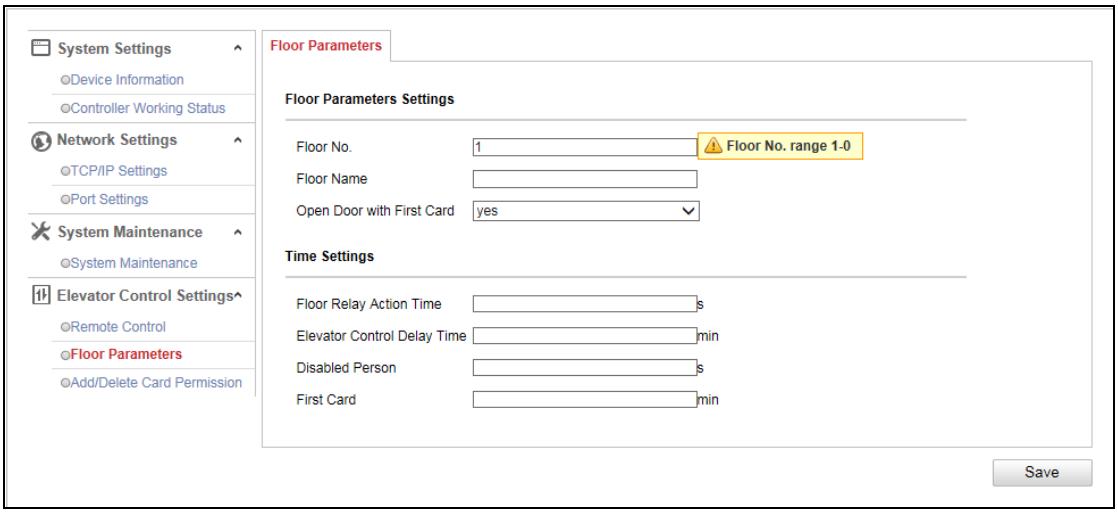
Notes:

- The elevator cannot be controlled by other client software if the elevator status changes.
- Only one client software can control elevator each time.
- The client software which has controlled the elevator can receive the alarm information and the elevator status. Other client software cannot.
- ■ represents the floor button is disabled; ■ represents the floor button is controlled; ■ represents the floor button is free.

Setting Floor Parameters

Steps:

1. Click **Elevator Control Settings** -> **Floor Parameters** to enter the Floor Parameters interface.



2. Set the floor parameters.

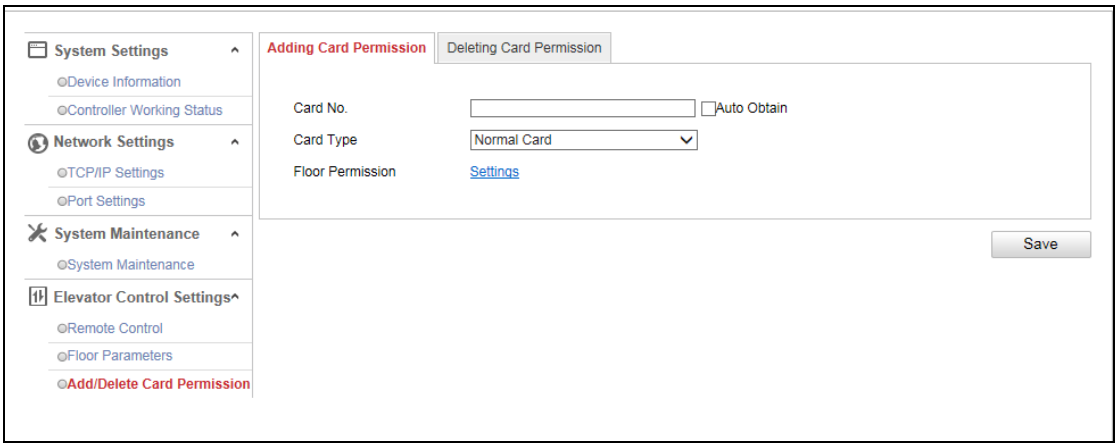
Floor No.:	Set the floor No.
Floor Name:	Set the floor Name.
Open Door with First Card:	Select to enable/disable the first card function The door remains open for the configured time duration after the first card swiping until the remain open duration ends.
Floor Relay Action Time:	The relay closed time duration after swiping the normal card. It refers to the available using duration of the elevator button after assigning the permission to the card. The default action time is 5s.
Elevator Control Delay Time:	The time duration of the visitor using the elevator. The default delay time is 5s.
Door Extended Opening:	The door can be open with appropriate delay after swiping the card. The default time duration is 15s.
First Card:	Set the door open duration for the function of Open Door with First Card. The default time duration is 10min.

3. Click **Save** to save the settings.
4. Edit the floor No. and repeat Step 2 and Step 3 to set other floor parameters.

Adding and Deleting Card Permission

Adding Card Permission

1. Click **Elevator Settings** -> **Add/Delete Card Permission** -> **Adding Card Permission** to enter the Adding Card Permission page.

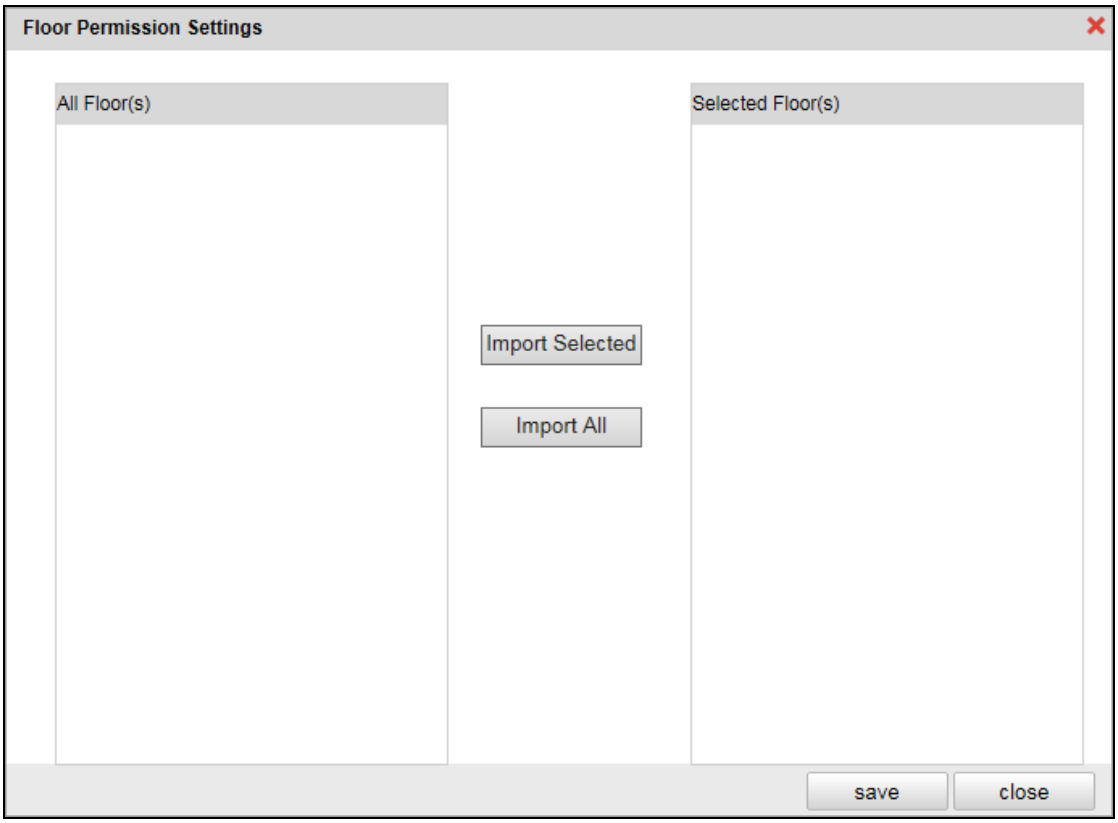


2. Input the card No.
   Or check the **Auto Obtain** checkbox, and swipe the card on the external card reader to get the card No.
3. Select a card type in the drop-down list.
   You can select from normal card, card for door extended opening, card in blocklist, patrol card, duress card, super card, visitor card and dismiss card. For detailed information about the card information, refer to Table 6-2.

Table 6-2 Card Type Description

Card Type	Description
Normal Card	By default, the card is 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 floor button cannot be controlled.
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 can be swiped for limited times. Configure the parameter in the client software.
Dismiss Card	Swipe the card to cancel the alarm.

4. Click **Settings** to enter the Floor Permission Settings window.

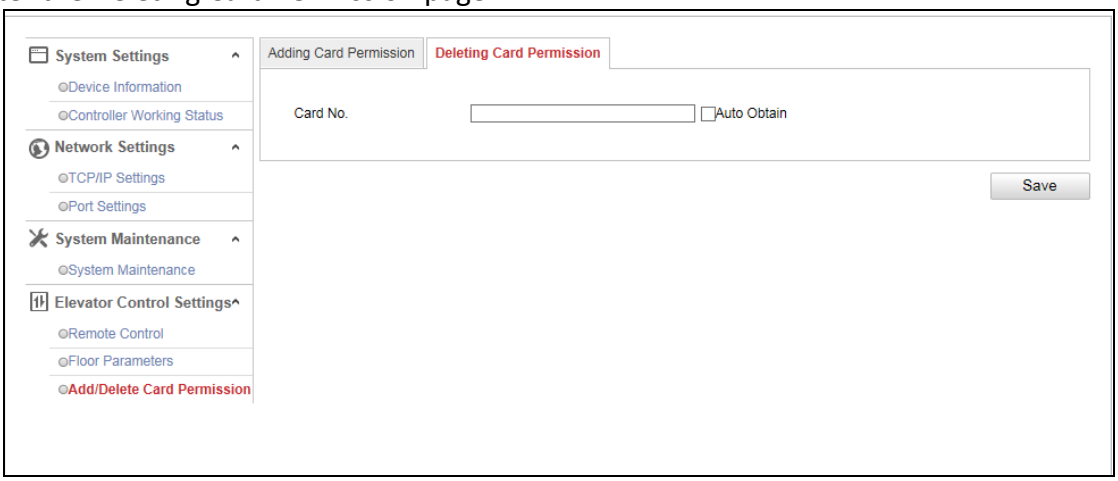


5. Check the floor checkbox(es) in the All Floor(s) list. And click **Import Selected Item** to import the selected floors to the Selected Floor(s) list.
6. Click **Save** to save the settings and the window will be automatically exited. The configured card will contain the selected floors permissions.
7. In the **Adding Card Permission** interface, click **Save** to save the settings.

Deleting Card Permission

Steps:

1. Click **Elevator Control Settings** -> **Add/Delete Card Permission** -> **Deleting Card Permission** to enter the Deleting Card Permission page.



2. Input the card No.
   Or check the Auto Obtain, and swipe the card on the external card reader to get the card No.
3. Click **Save**. The card permission will be deleted.

Chapter 7 Client Operation

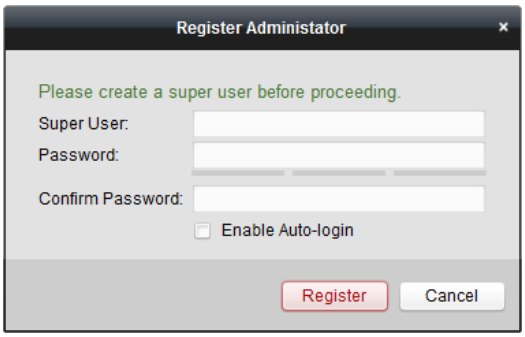
You can set and operate the access control devices via the client software. This chapter will introduce the access control device related operations in the client software. For integrated operations, refer to *User Manual of iVMS-4200 Client Software*.

7.1 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.

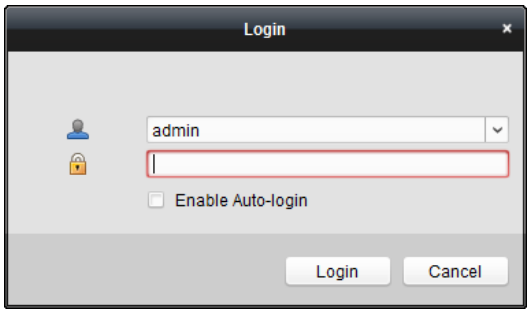


- *A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.*
- *For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case 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.
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*.

7.2 System Configuration

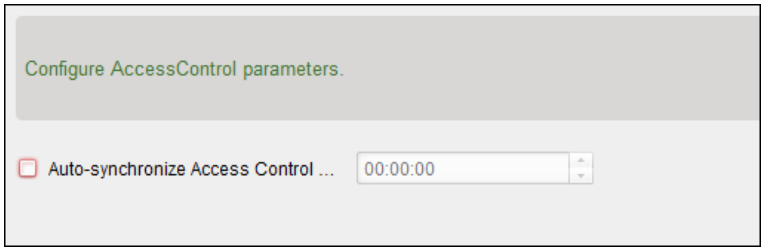
Purpose:

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.



7.3 Access Control Management

Purpose:

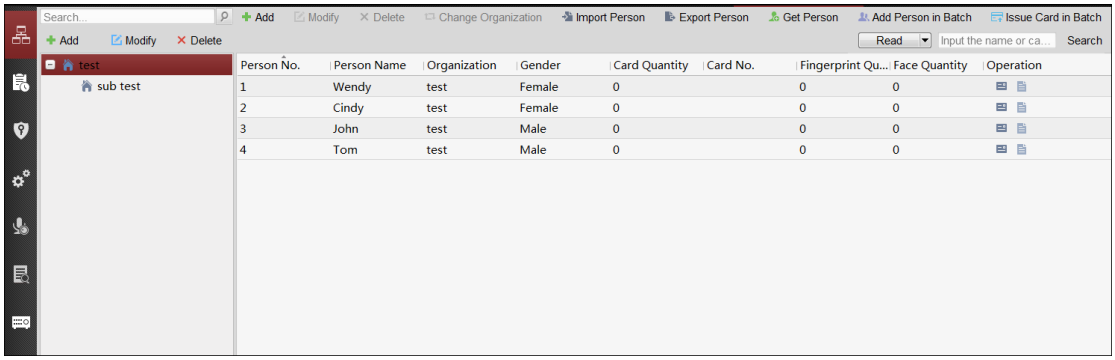
The Access Control module is applicable to access control devices and video intercom. It provides multiple functionalities, including person and card management, permission configuration, access control status management, video intercom, and other advanced functions.

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.

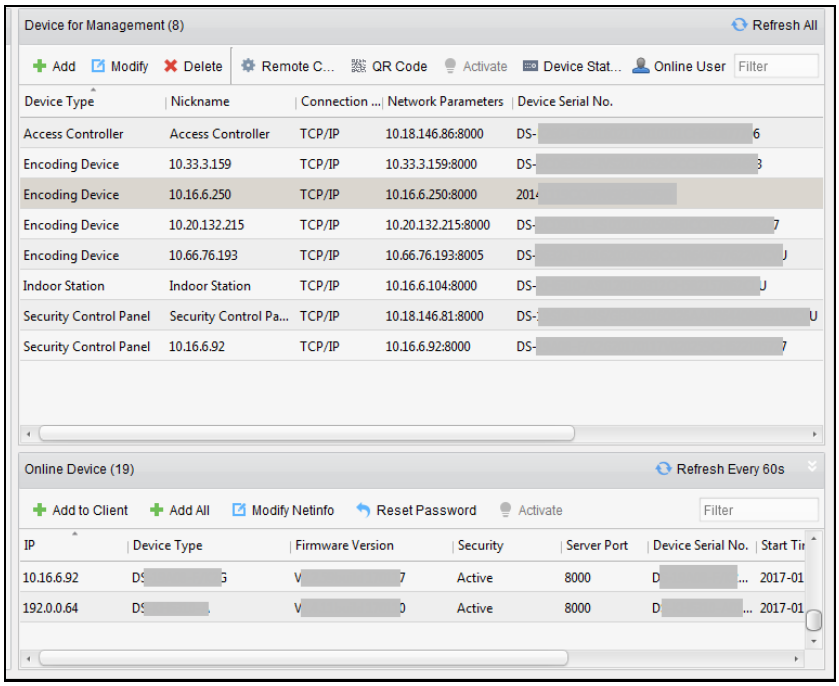
Non-residence: You can set the attendance rule when adding person, while set the access control parameters.

Residence: You cannot set the attendance rule when adding person.

Note: Once the scene is configured, you cannot change it later.

7.3.1 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

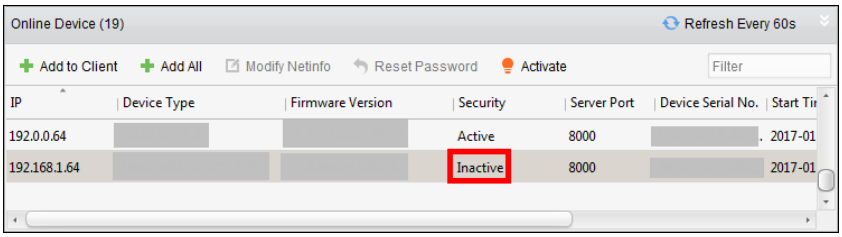
Purpose:

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:

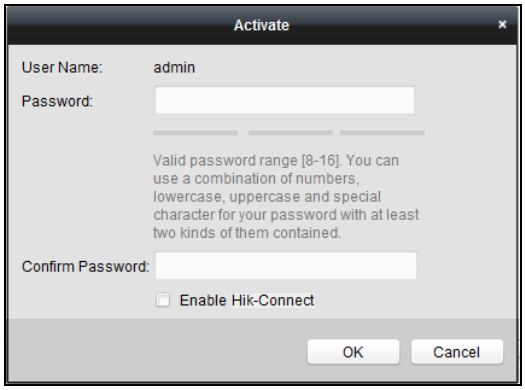
1. Enter the Device Management page.
2. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.



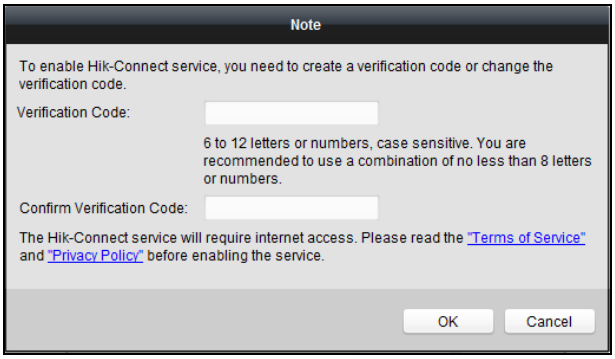
3. Click the **Activate** button to pop up the Activation interface.
4. Create a password in the password field, and confirm the password.

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.



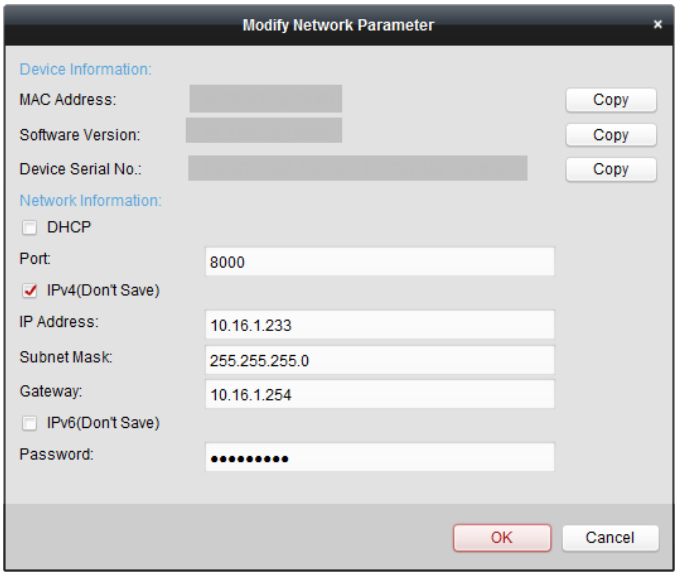
5. (Optional) Enable Hik-Connect service when activating the device if the device supports.
   1) Check **Enable Hik-Connect** checkbox to pop up the Note dialog.



   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.

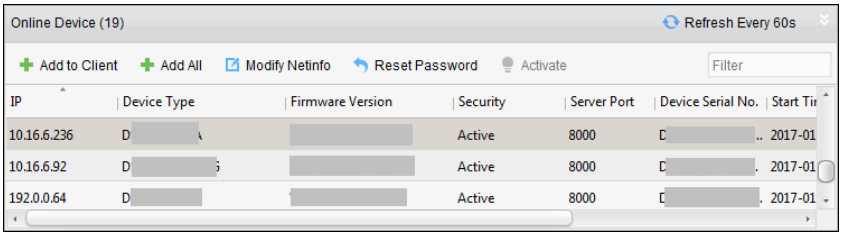


Adding Online Device

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

.

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.

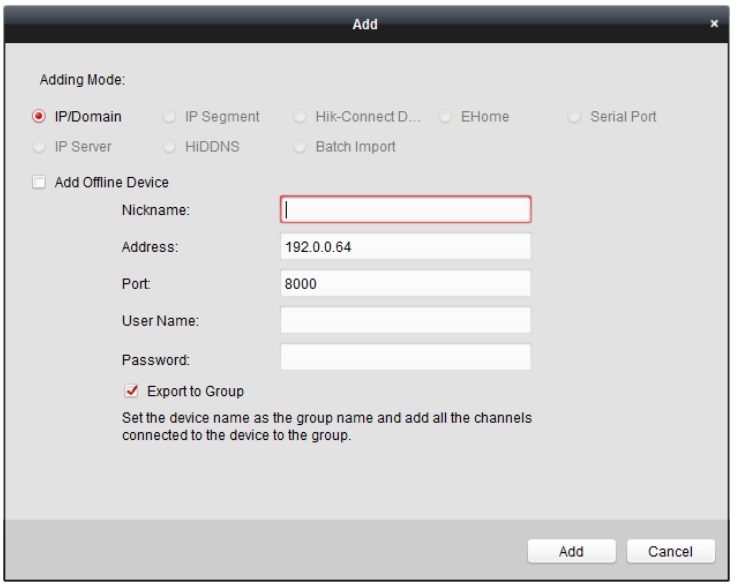
   STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password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



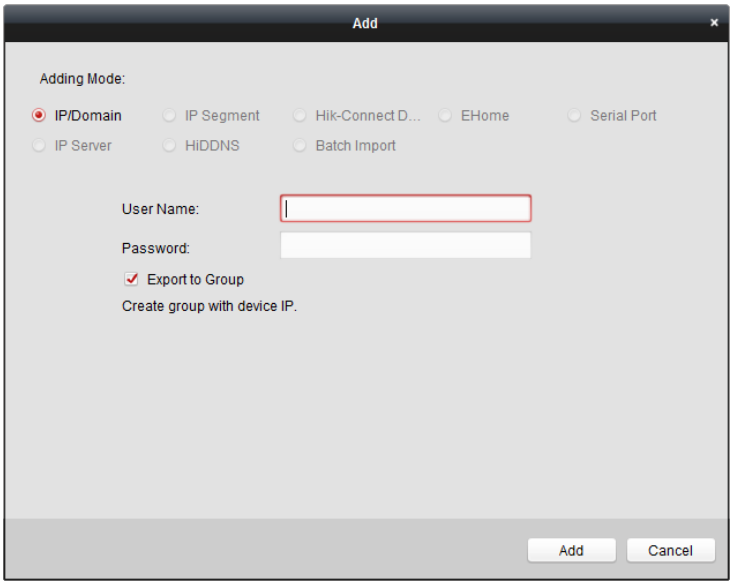
➢ Adding Multiple Online Device

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.

   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. 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.

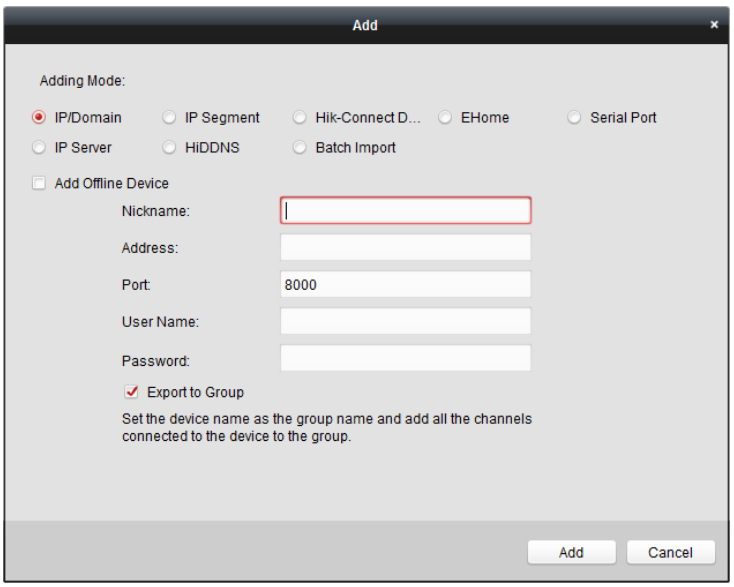
   Note: iVMS-4200 also provides a method to add the offline devices.

   1) Check the **Add Offline Device** checkbox.

2) Input 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.

   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. 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.

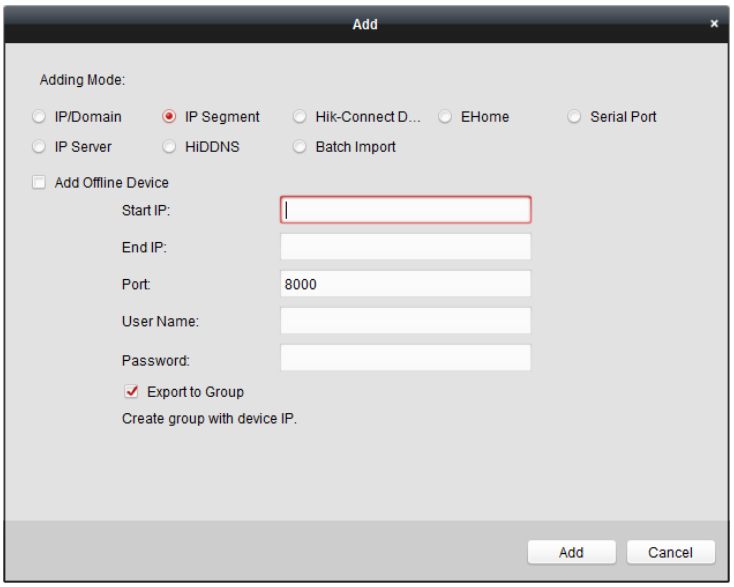
   1) Check the **Add Offline Device** checkbox.

2) Input 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*.

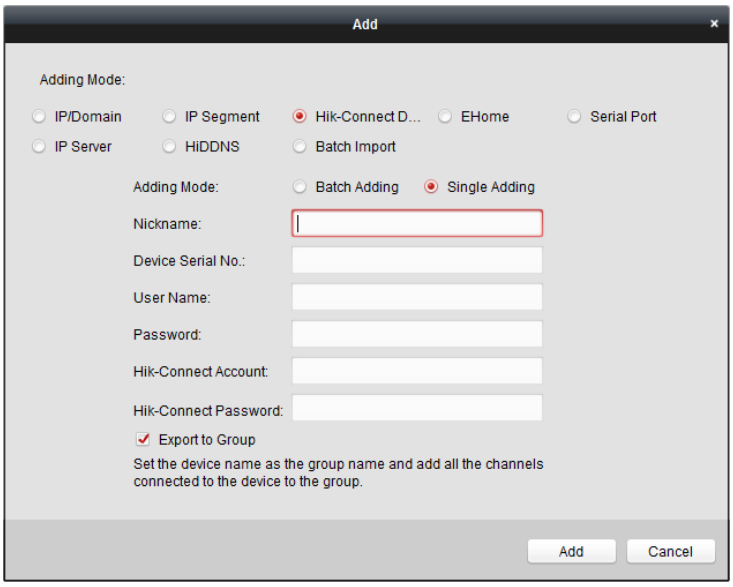
Password: Input the device password.

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.*

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

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

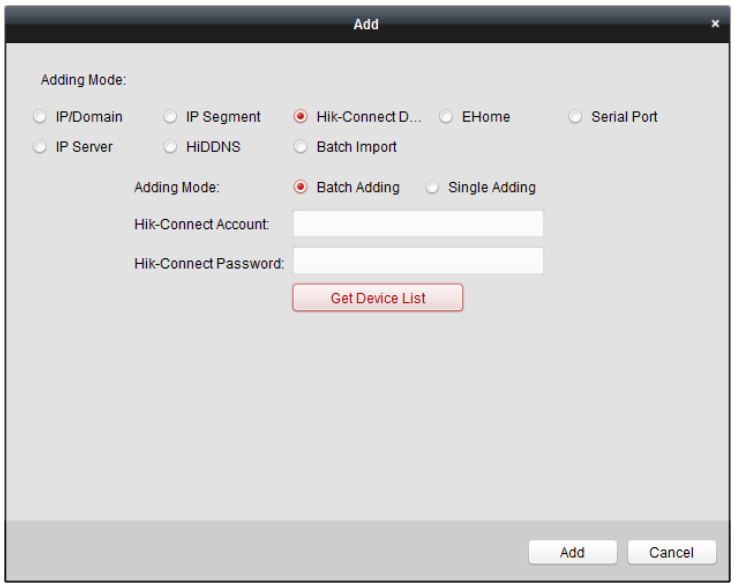
5. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
6. Click **Add** to add the device.



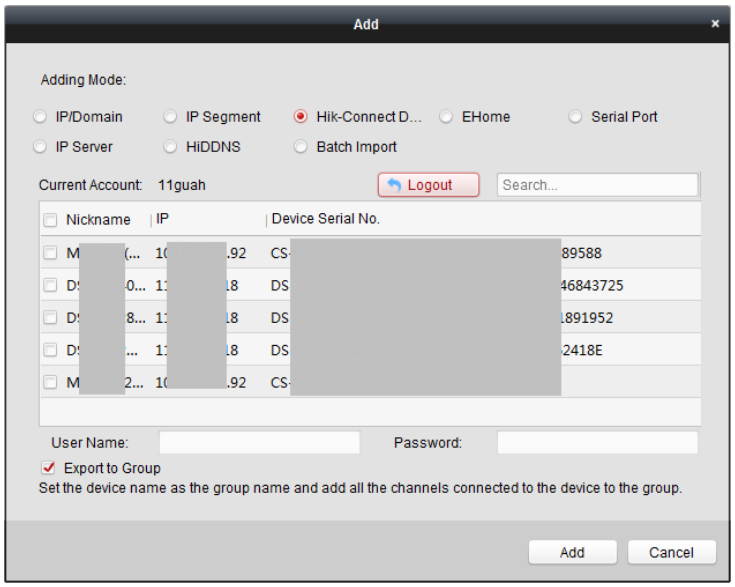
Add Devices in Batch

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

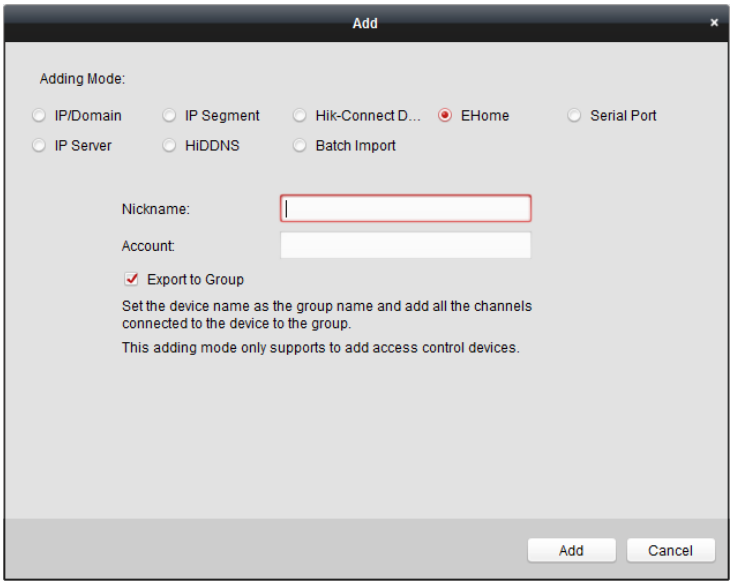
Purpose:

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 7.3.4 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) Input 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.

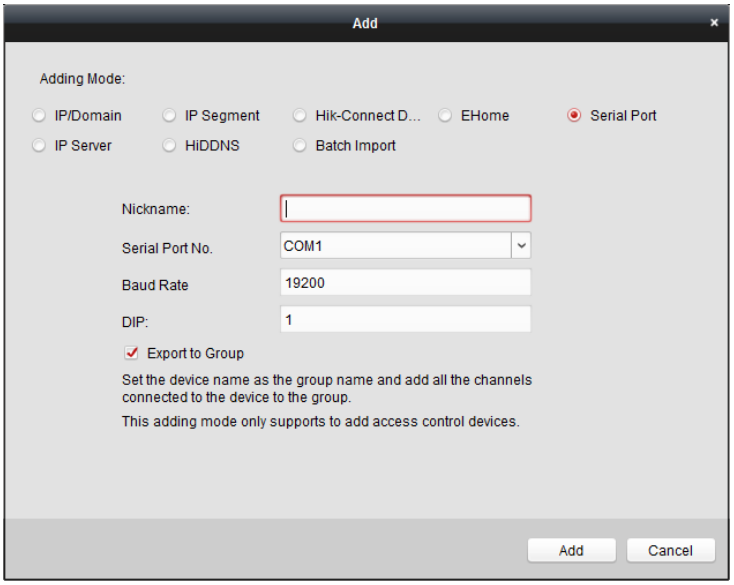
Adding Devices by Serial Port

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.

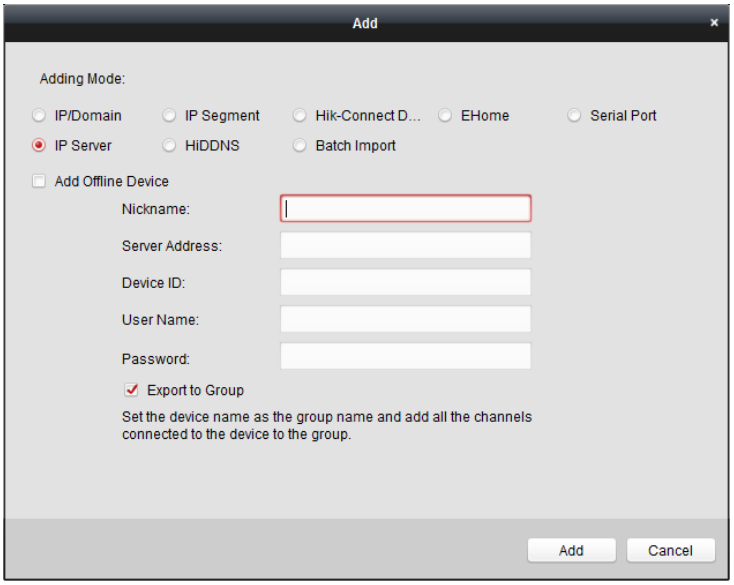
   1) Check the **Add Offline Device** checkbox.
   2) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

   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.

   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. 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) Input the required information, including the device channel number and alarm input number.
   3) Click **Add**.

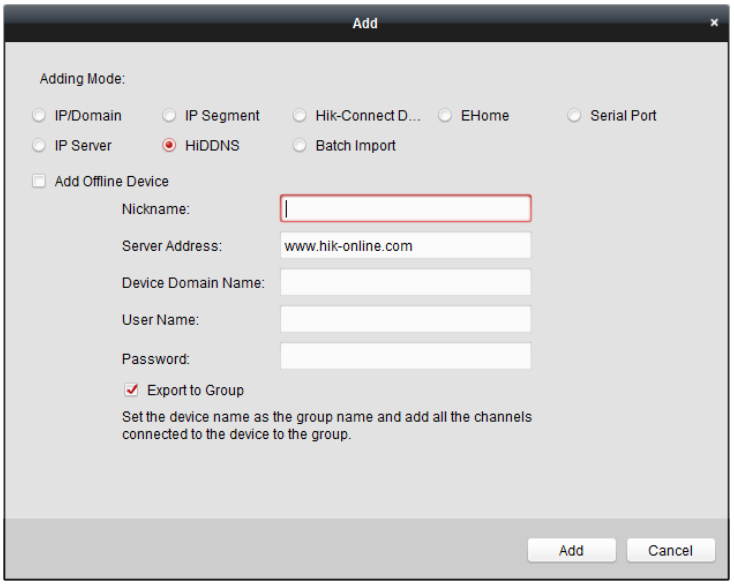
   When the offline device comes online, the software will connect it automatically.

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.

   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. 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) Input 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.

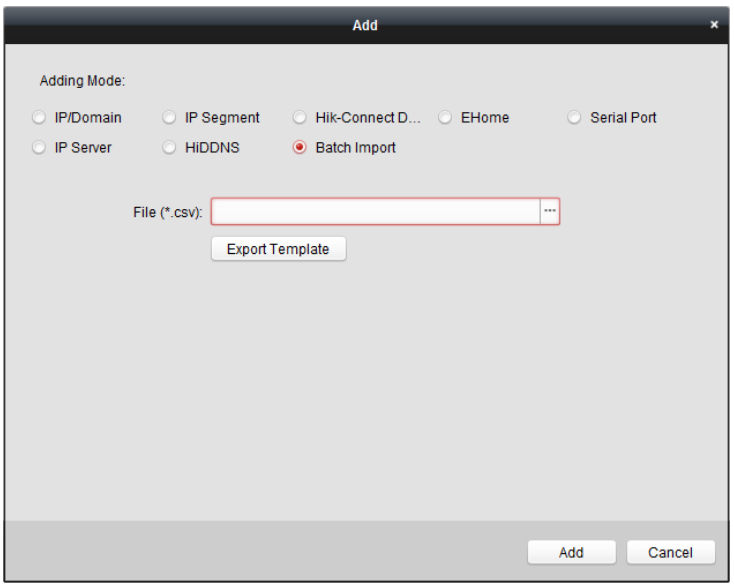
Importing Devices in Batch

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.

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.

- **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.

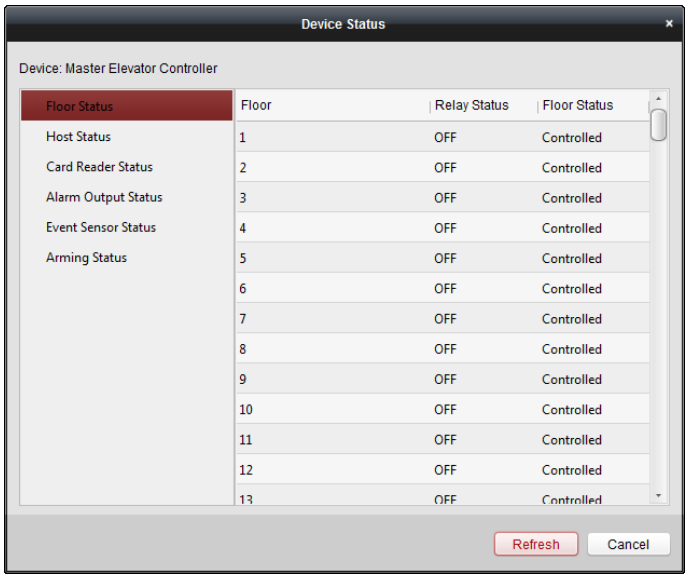
5. Click ··· and select the template file.
6. Click **Add** to import the devices.

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.

7.3.2 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.

- **Floor Status**: The status of the connected floor.
- **Host Status**: The status of the host, including Storage Battery Power Voltage, Whether power storage is in low voltage status, Device Power Supply Status, and Card Added 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 Output Status**: The alarm output status of each port.
- **Event Sensor Status**: The event sensor status of each port.
- **Arming Status:** The status of the device.

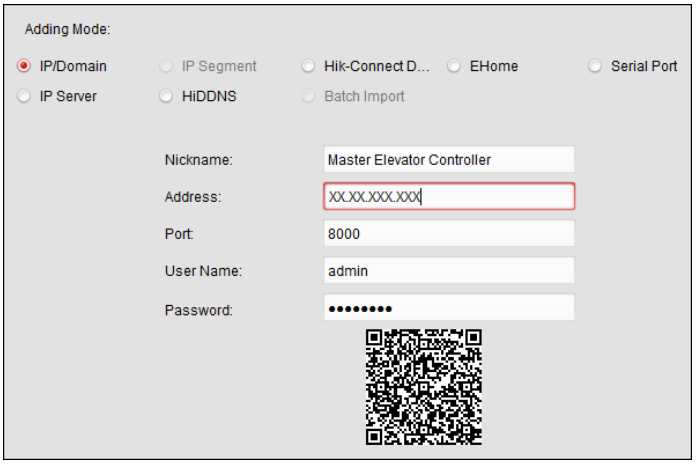
7.3.3 Editing Basic Information

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.

7.3.4 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.

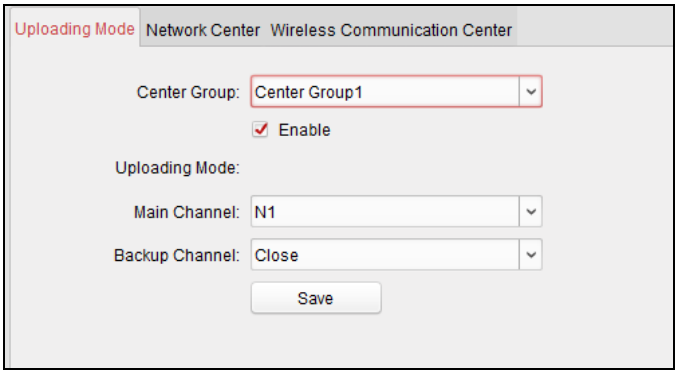
Uploading Mode Settings

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.

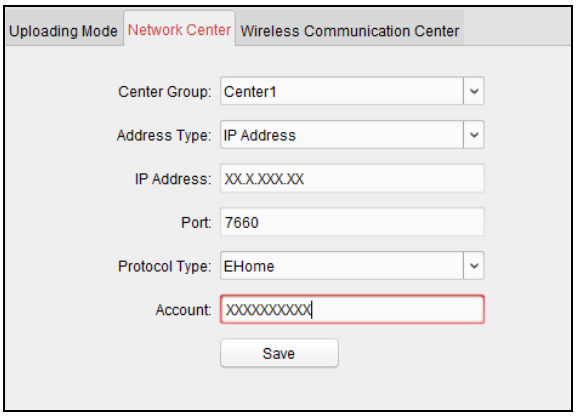
5. Click **Save** button to save parameters.

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 as **IP Address** or **Domain Name.**
4. Input IP address or domain name according to the address type.
5. Input the port No. for the protocol. By default, the port No. is 7660.
6. Select the protocol type as EHome.
7. Set an account name for the network center.

   Note: The account should contain 1 to 32 characters and only letters and numbers are allowed.

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

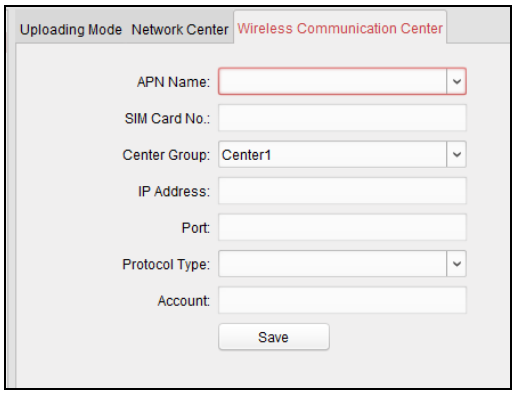
Notes:

- 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 *Editing Time* section in Remote Configuration. For details, refer to *Time* in *7.3.6 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.

7.3.5 RS-485 Settings

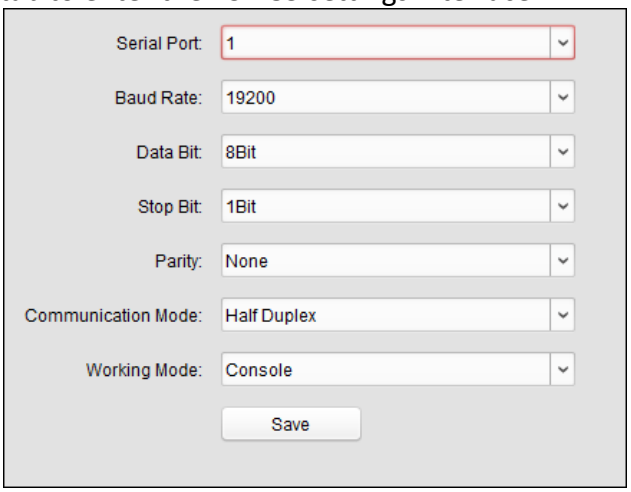
Purpose:

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.

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

Steps:

1. Select the device in the device list, and click **Modify** to pop up the modifying device information window.
2. 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, flow control, communication mode, and working 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.

7.3.6 Remote Configuration

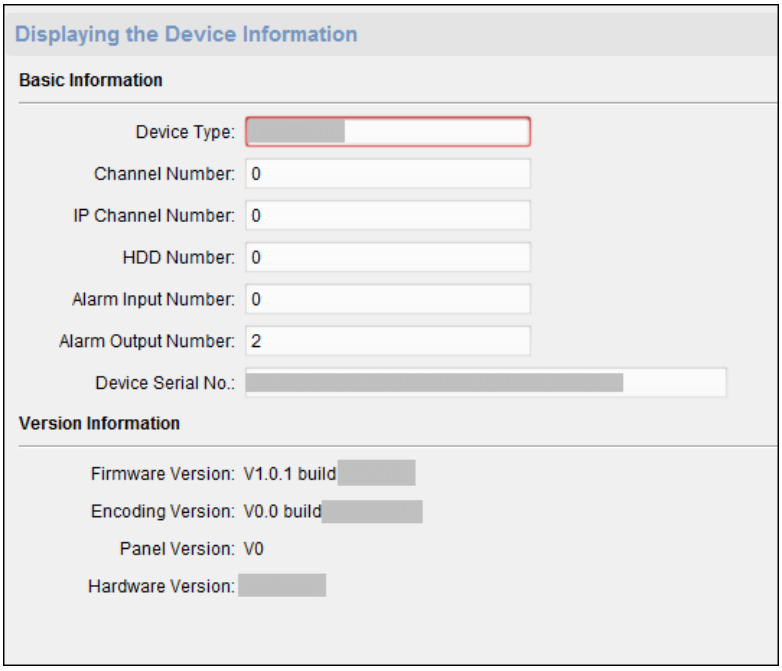
Purpose:

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

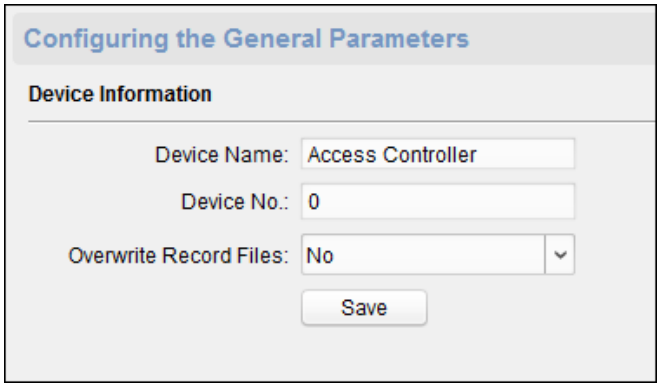
Steps:

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

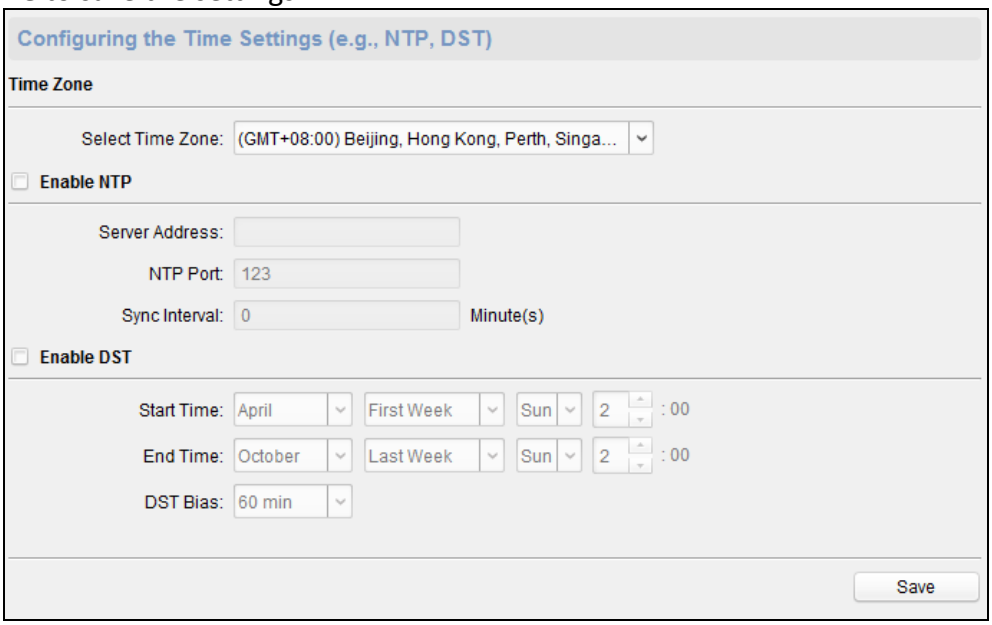
In the Remote Configuration interface, click **System** -> **General** to configure the device name and overwrite record files parameter. Click **Save** to save the settings.



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

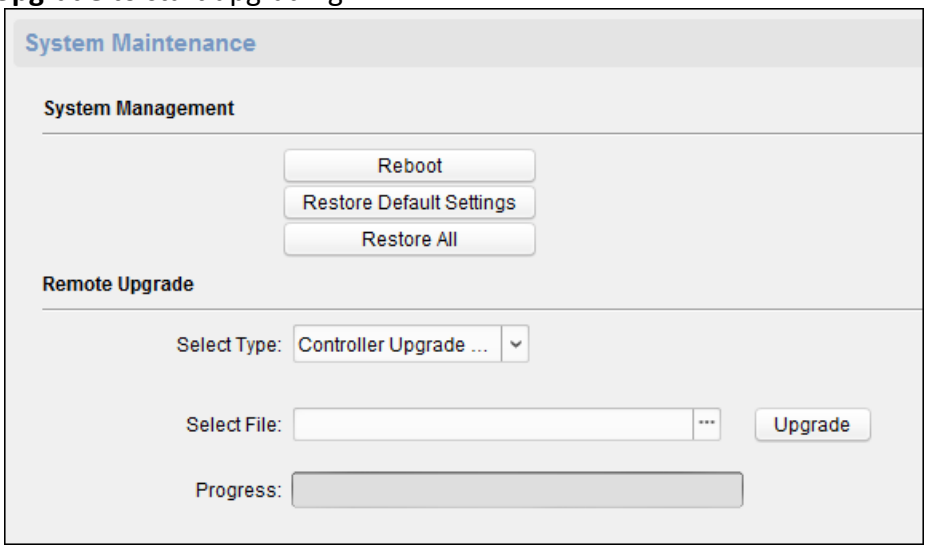
Purpose:

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

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, click ··· to select the upgrade file.
   2) Click **Upgrade** to start upgrading.



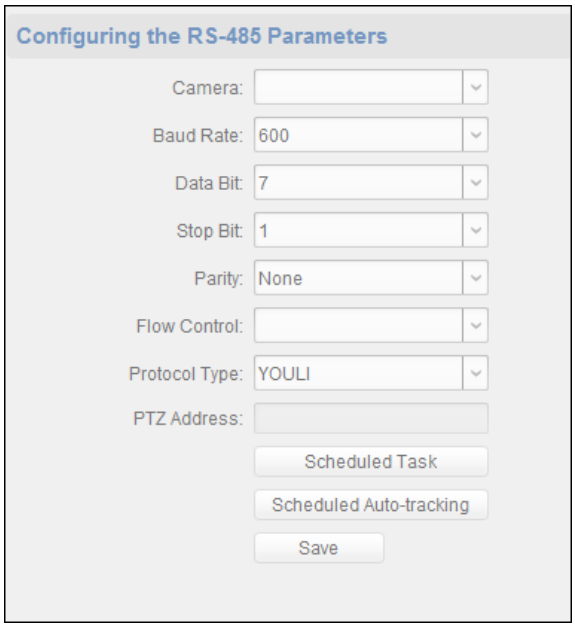
Setting RS-485 Parameters

You can set the device RS-485 parameters to connect peripherals.

Steps:

1. Click **System** –> **RS485** in the Remote Configuration interface.
2. Set the parameters on the page.
3. Click **Save** to save the settings.

   Note: You can also set the RS-485 parameters in Modify window. For details, see 7.3.5 RS-485 Settings.

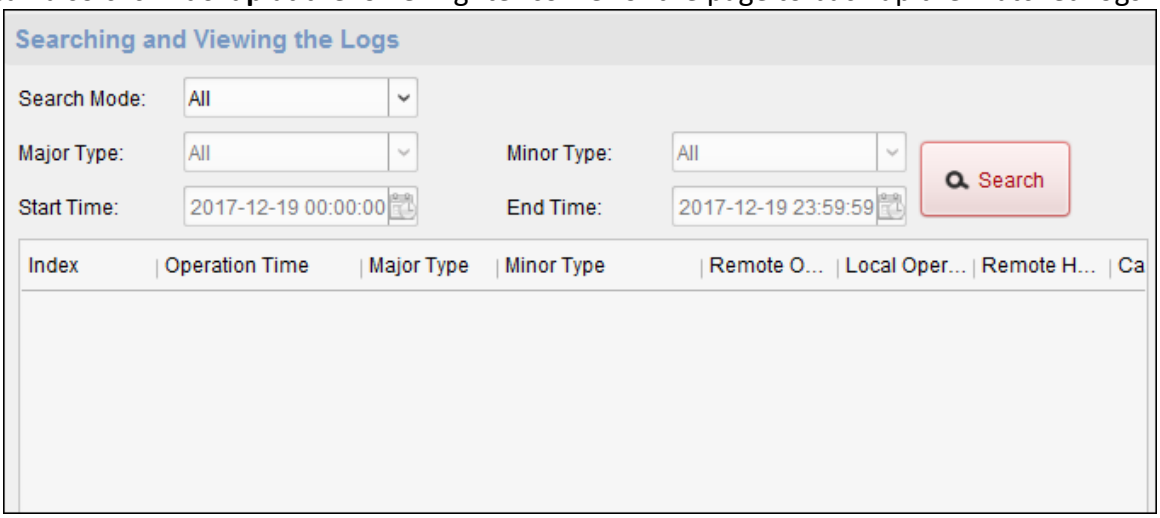


Searching and Viewing Logs

Click **System** –> **Log** and input the search conditions. Click **Search** to search and view the device

logs.

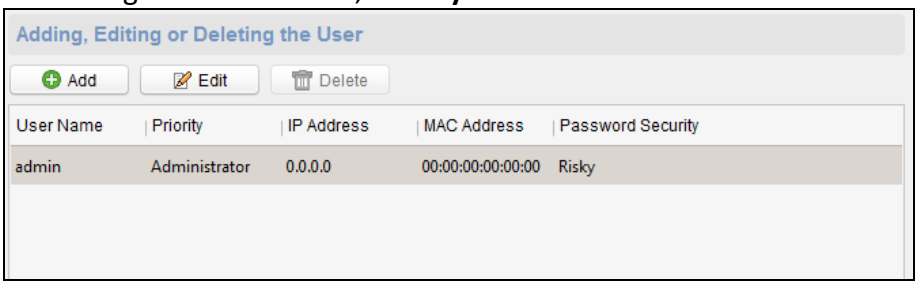
You can also click **Backup** at the lower righter corner of the page to back up the matched logs.



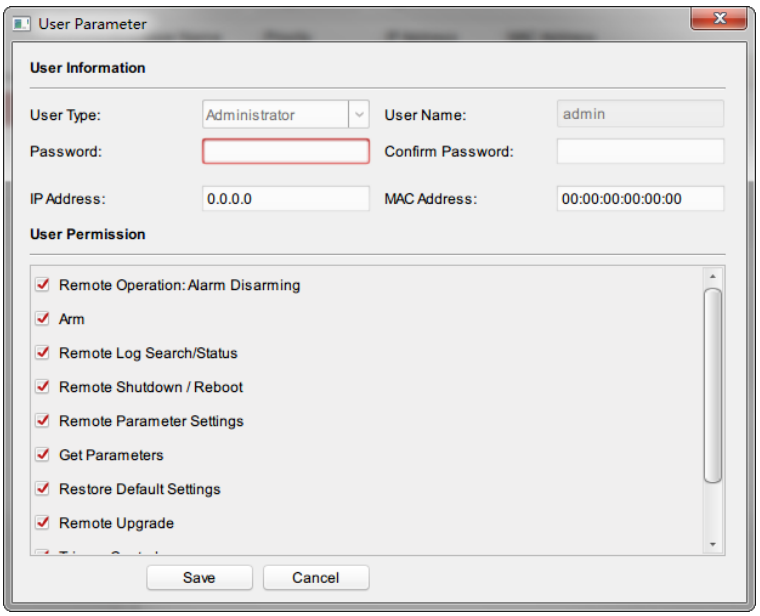
Managing User

Steps:

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



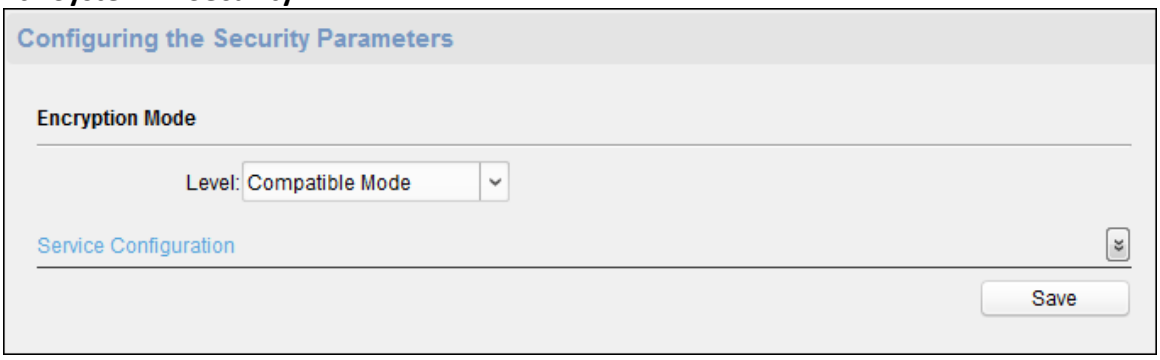
2. Click **Add** to add the user (Do not support by the elevator controller.).
   Or select a user in the user list and click **Edit** to edit the user. You are able to edit the user password, the IP address, the MAC address and the user permission. Cilck **OK** to confirm editing.



Setting Security

Steps:

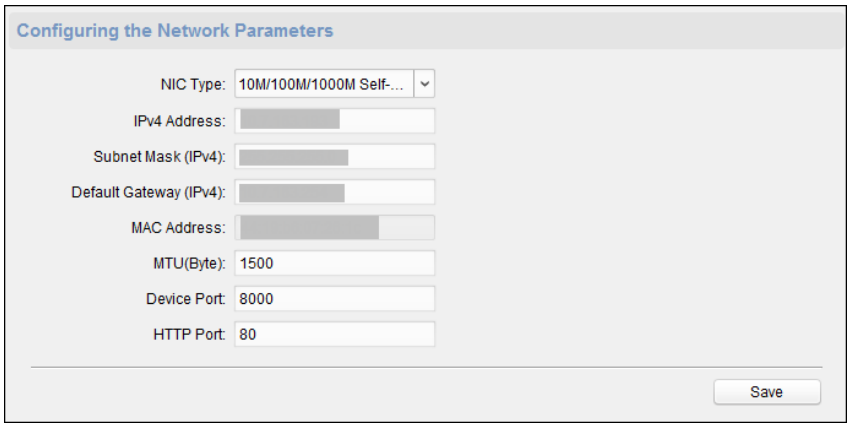
1. Click **System** -> **Security**.



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

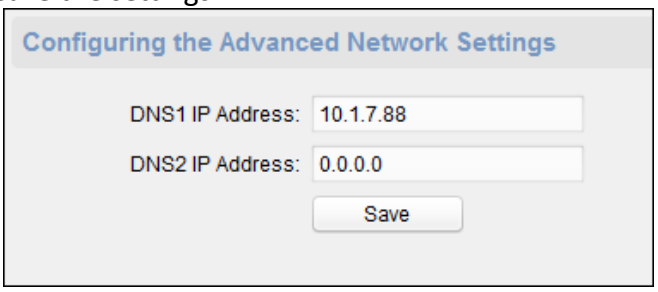
Configuring Network Parameters

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



Configuring Advanced Network

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



7.4 Organization Management

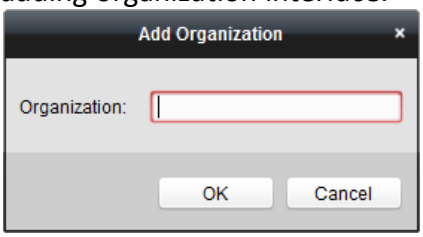
You can add, edit, or delete the organization as desired.

Click tab to enter the Person and Card Management interface.

7.4.1 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.

7.4.2 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 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 person information in batch, etc.

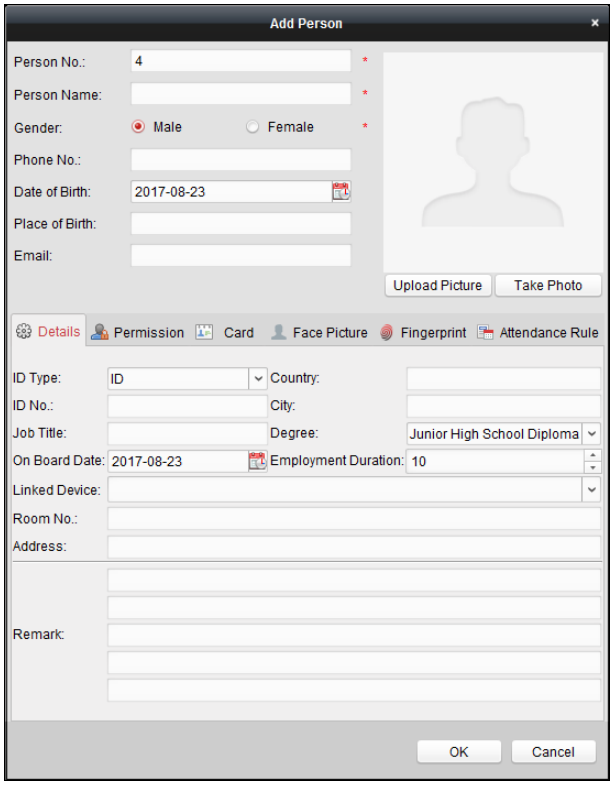
Note: Up to 10,000 persons or cards can be added.

7.5.1 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.

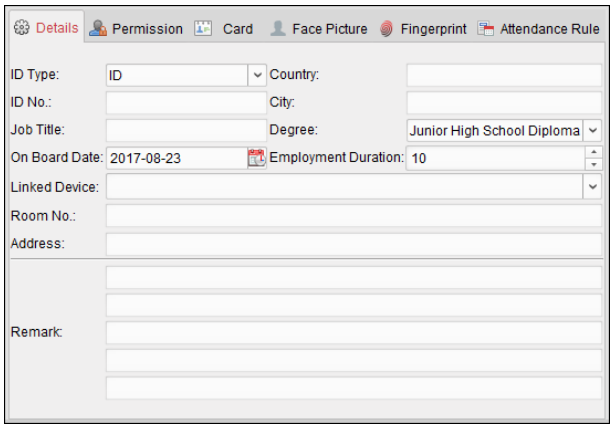


2. The Person No. will be generated automatically and is not editable.
3. Input the basic information including person name, gender, phone No., birthday details, and email address.
4. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
   Note: The picture 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.

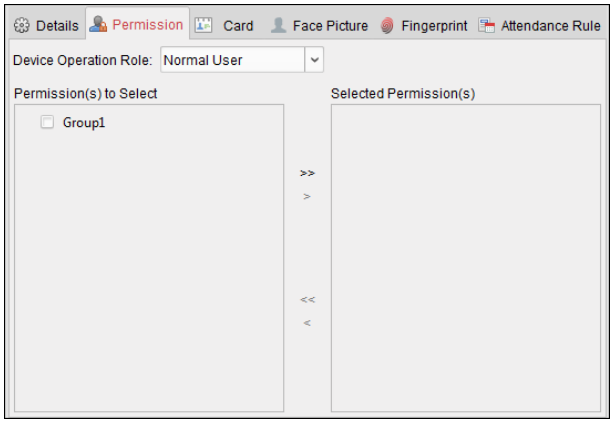
Adding Person (Permission)

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.

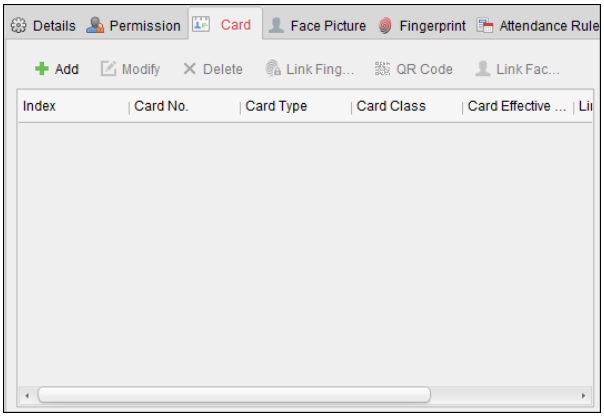
Adding Person (Card)

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

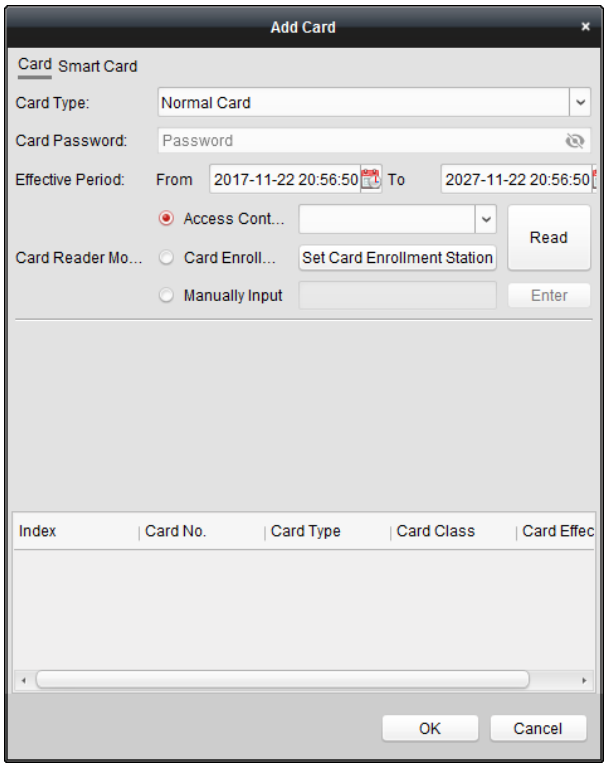
➢ **Adding General Card**

Steps:

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



2. Click **Add** to pop up the Add Card dialog.
3. Click **Card** to enter the Card tab.



4. Select the card type according to actual needs.
   - **Normal Card**

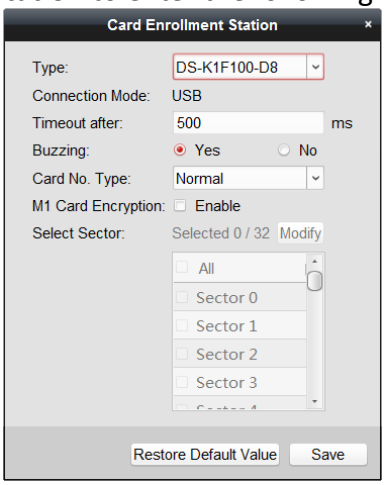
- **Card for Door Extended Opening**: The door will remain open for the configured time period for the card holder.
- **Card in Blocklist**: The card swiping action will be uploaded and the door cannot be opened.
- **Patrol Card**: The card swiping action can used for checking the working status of the 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**.

  Note: The Max. Swipe Times should be between 0 and 255. When setting as 0, it means the card swiping is unlimited.

5. 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.*
6. Click to set the effective time and expiry time of the card.
7. 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 serial port No., the baud rate, the timeout value, the buzzing, or the card No.

type.

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.

8. Click **OK** and the card(s) will be issued to the person.
9. (Optional) You can select the added card and click **Modify** or **Delete** to edit or delete the card.
10. (Optional) You can generate and save the card QR code for QR code authentication.
    1) Select an added card and click **QR Code** to generate the card QR code.
    2) In the QR code pop-up window, click **Download** to save the QR code to the local PC.
    You can print the QR code for authentication on the specified device.
    Note: The device should support the QR code authentication function. For details about setting the QR code authentication function, see the specified device user manual.
11. (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.
12. (Optional) You can click **Link Face Picture** to link the card with the face picture, so that the person can pass the door by scanning the face via the device instead of swiping card when passing the door.
13. Click **OK** to save the settings.

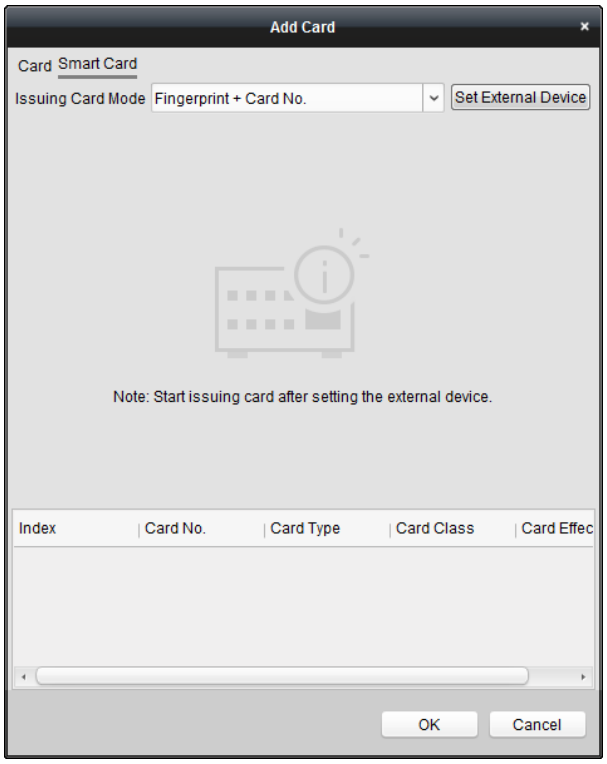
➢ **Adding Smart Card**

Purpose:

You can store fingerprints and ID card infomration in the smart card. When authenticating, after swiping the smart card on the device, you can scan your fingerprint or swipe your ID card on the device. The device will compare the fingerperint or ID card information in the smart card with the ones collected. If you use the smart card for authentication, there is no need to store the fingerprints or ID card information in the device in advance.

Steps:

1. In the Add Person page, set the person basic information.
2. Click **Card** to enter the card tab.
3. Click **Add** to pop up the Add Card dialog.
4. Click **Smart Card** to enter the Smart Card tab.



5. Select an issuing card mode from the dropdown list.
6. Set the external device.
   1) Click **Set External Device** to enter the Set External Device page.
   2) (Optional) Select the issuing card mode again.
   3) Set a card enrollment station.
   4) If you select "Fingerprint + Card No." as the issuing mode, set the fingerprint recorder model.
      If you select "ID Card No. + Card No." as the issuing mode, set the ID card reader model.
      If you select "Fingerprint + ID Card No. + Card No." as the issuing mode, set the fingerprint recorder model and the ID card reader model.
   5) Click **OK** save the settings.
7. Select a card type for the smart card.
   - **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.

Note: The Max. Swipe Times should be between 0 and 255. When setting as 0, it means the card swiping is unlimited.

- **Dismiss Card:** Swipe the card to dismiss alarm.

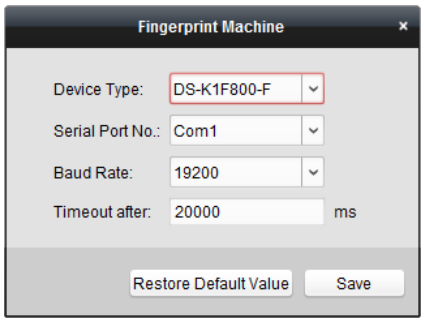
8. Set other parameters of the card.
   1) Set the card password.
   2) Set the card effective date.
   3) Scan your fingerprint and swipe your ID card according to the promt.
   4) Swipe the smart card.
      The added card information will display in the list below.
9. Click **OK** and the card(s) will be issued to the person.
10. (Optional) Select the added card and click **Modify** or **Delete** to edit or delete the card.
11. (Optional) Generate and save the card QR code for QR code authentication.
    1) Select an added card and click **QR Code** to generate the card QR code.
    2) In the QR code pop-up window, click **Download** to save the QR code to the local PC.
       You can print the QR code for authentication on the specified device.
       Note: The device should support the QR code authentication function. For details about setting the QR code authentication function, see the specified device user manual.
12. (Optional) 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.
13. (Optional) Click **Link Face Picture** to link the card with the face picture, so that the person can pass the door by scanning the face via the device instead of swiping card when passing the door.
14. Click **OK** to save the settings.

Adding Person (Fingerprint)

Steps:

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

2. Select **Local Collection** as desired.
3. 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-K1F810-F, DS-K1F820-F, and DS-K1F181-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.

4. Click **Start** button, click to select the fingerprint to start collecting.
5. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.
6. (Optional) You can also click **Remote Collection** to collect fingerprint from the device.
   Note: The function should be supported by the device.
7. (Optional) 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.

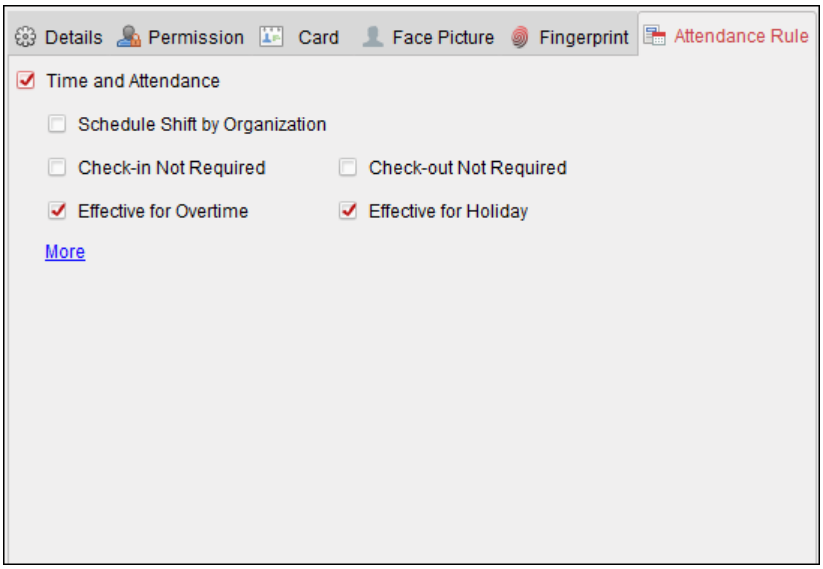
Adding Person (Attendance Rule)

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.



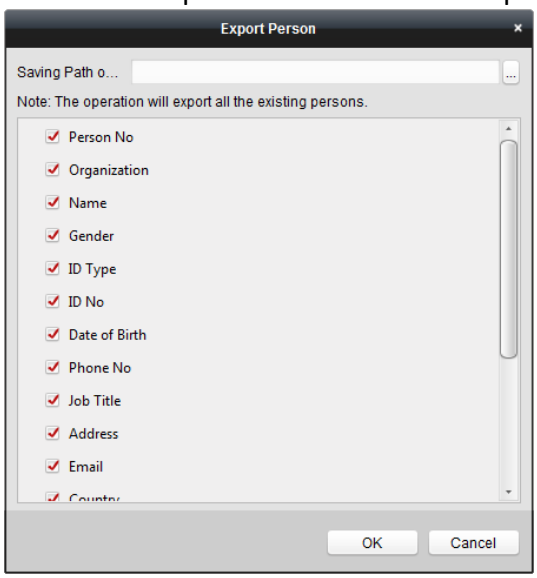
2. If the person joins in the time and attendance, check the **Time and Attendance** checkbox to enable this function for the person. Then the person's card swiping records will be recorded and analyzed for time and attendance.
   For details about Time and Attendance, click **More** to go to the Time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

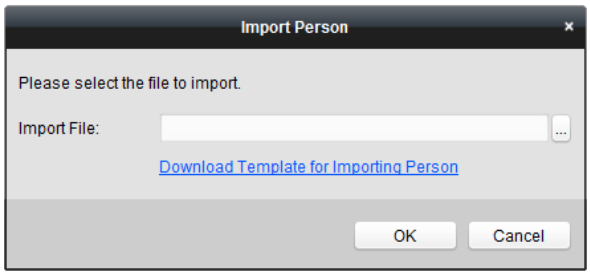
Steps:

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.

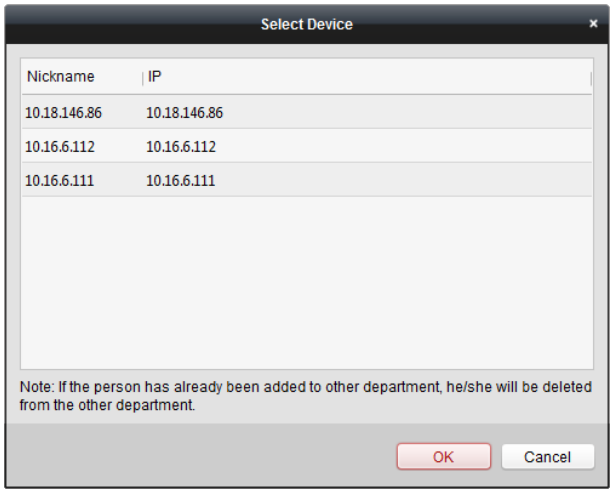
Getting Person Information from Access Control Device

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 can be imported.

7.5.2 Managing Person

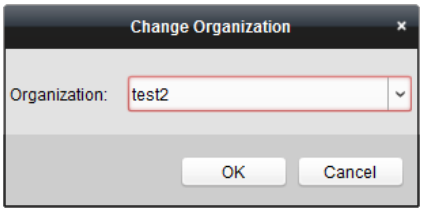
Modifying and Deleting Person

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.

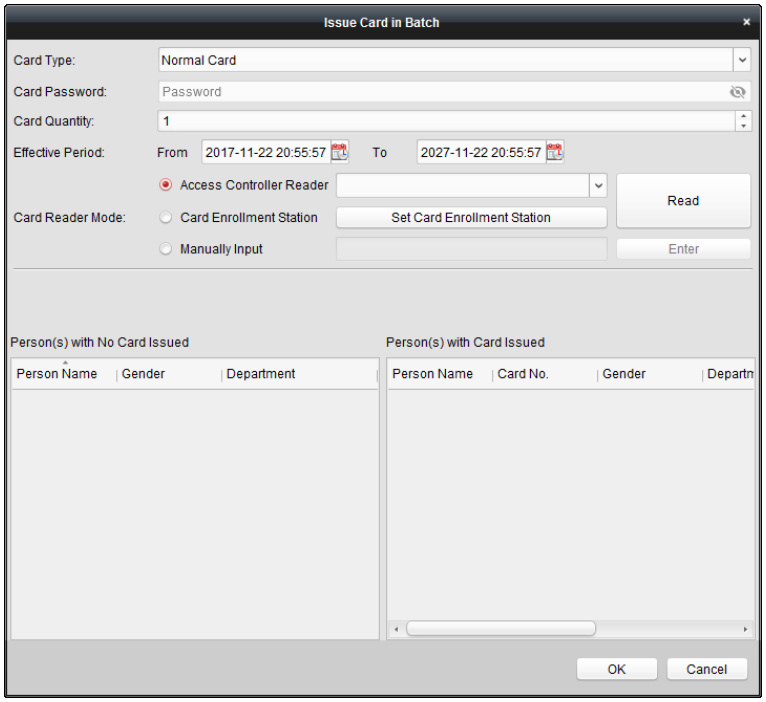
Searching Person

You can input the keyword of card No. or person name in the search field, and click **Search** to search the person.
You can input the card No. by clicking **Read** to get the card No. via the connected card enrollment station.
You can click **Set Card Enrollment Station** in the dropdown list to set the parameters.

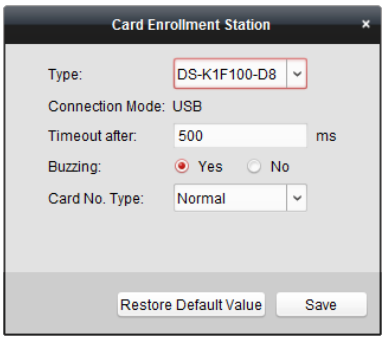
7.5.3 Issuing Card in Batch

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. In the Person(s) with No Card Issued list on the left, select the person to issue card.
   Note: You can click on the Person Name, Gender, and Department column to sort the persons according to actual needs.
7. 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.
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.

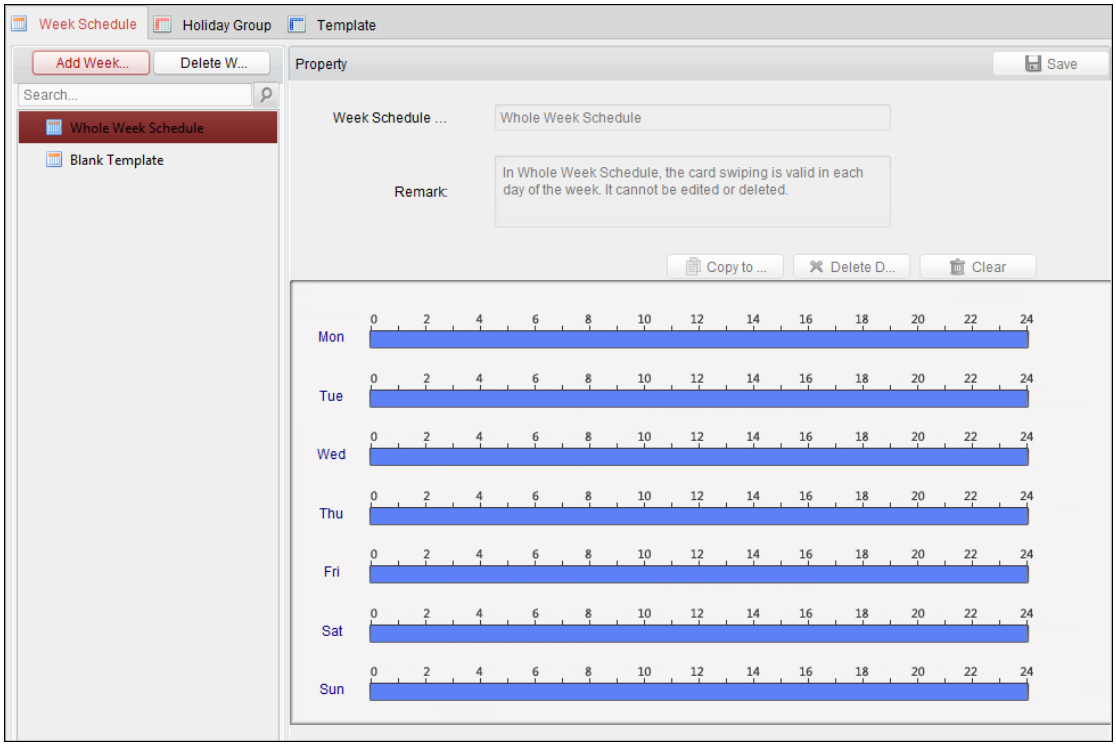
8. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.
9. Click **OK** to save the settings.

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.

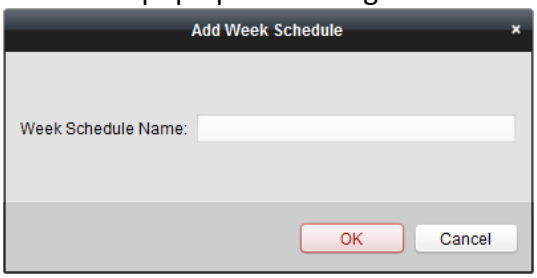
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

- **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

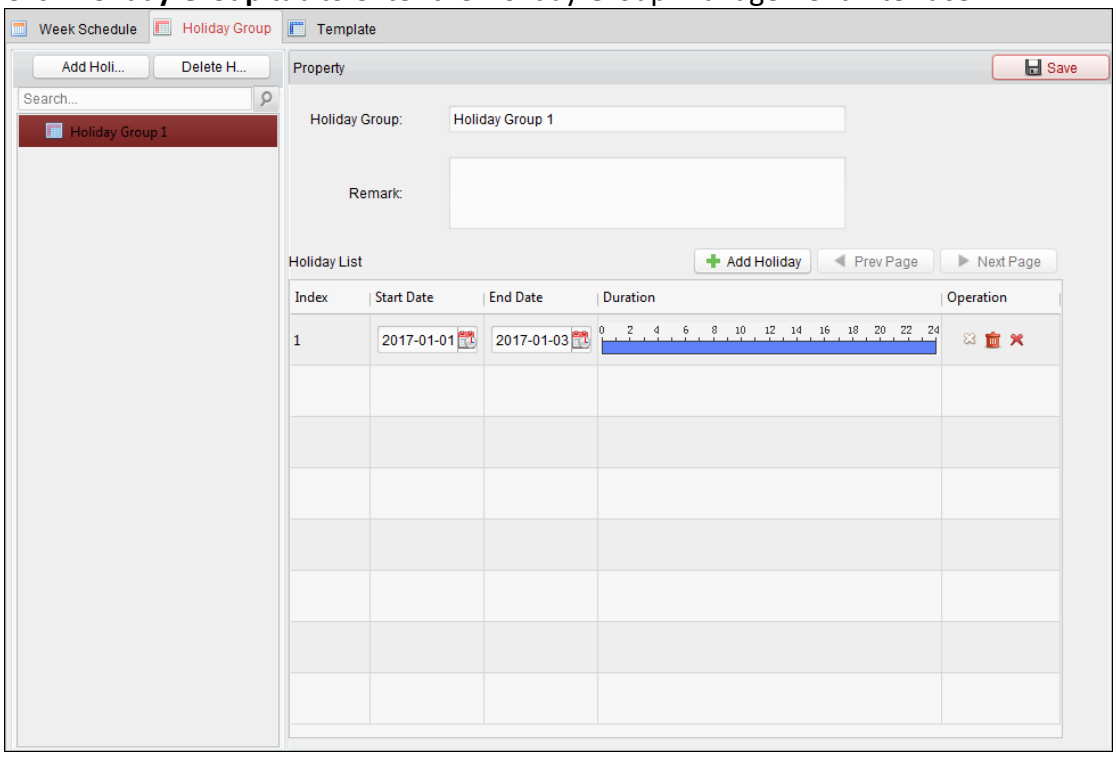
period of time, the configured permission is activated.

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.

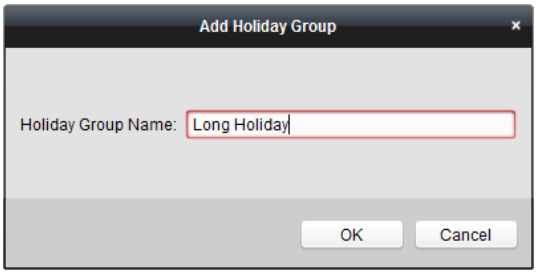
7.6.2 Holiday Group

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.

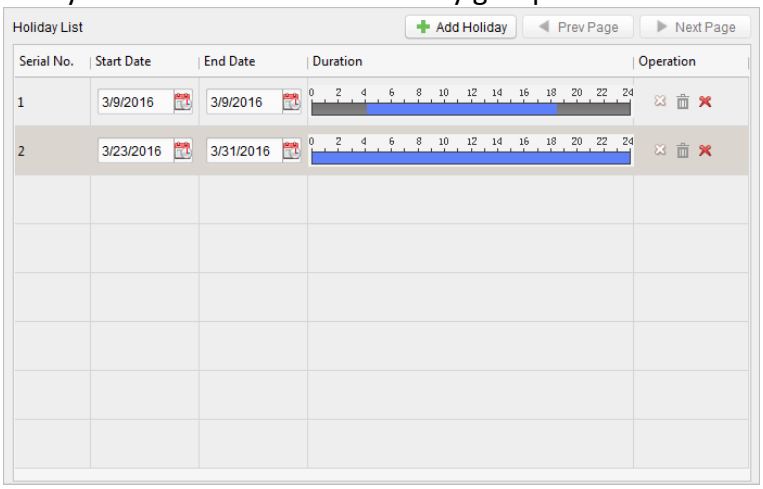


2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.
3. Select the added holiday group and you can edit the holiday group name and input the remark

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.

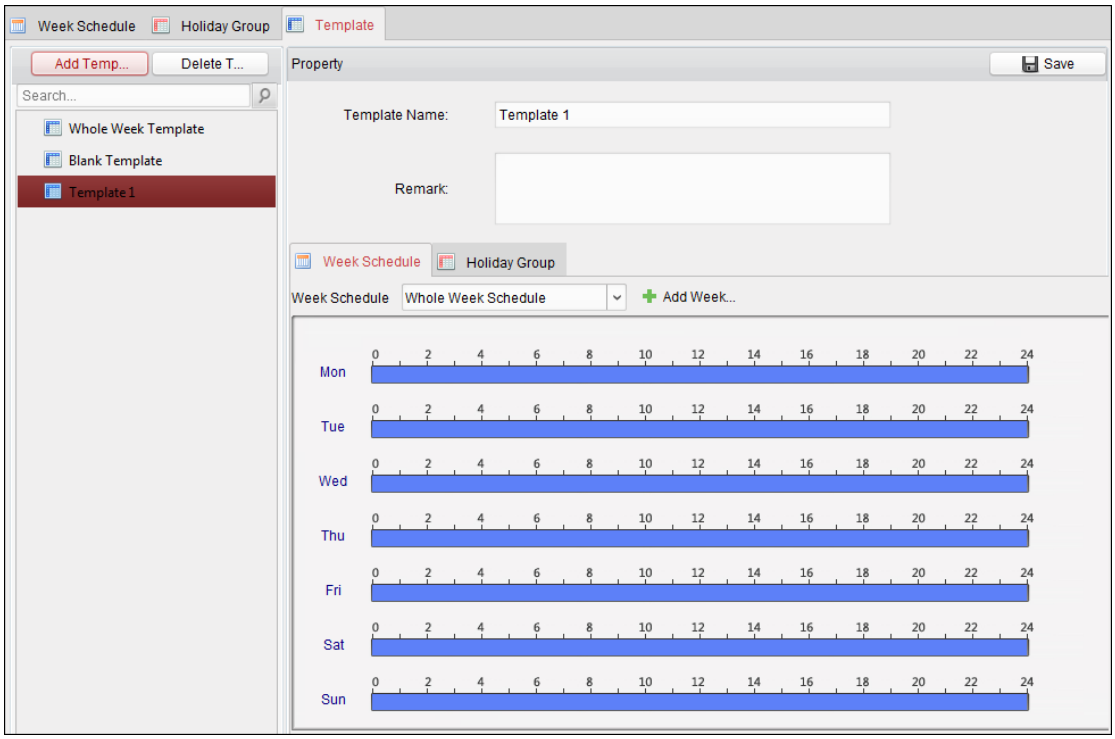
Note: The holidays cannot be overlapped with each other.

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.



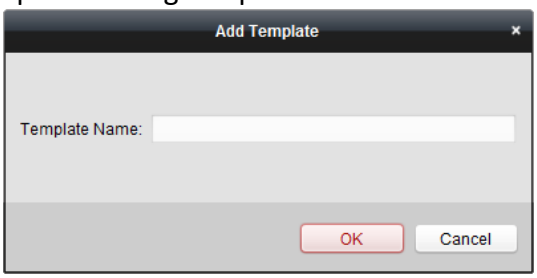
There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

- **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.

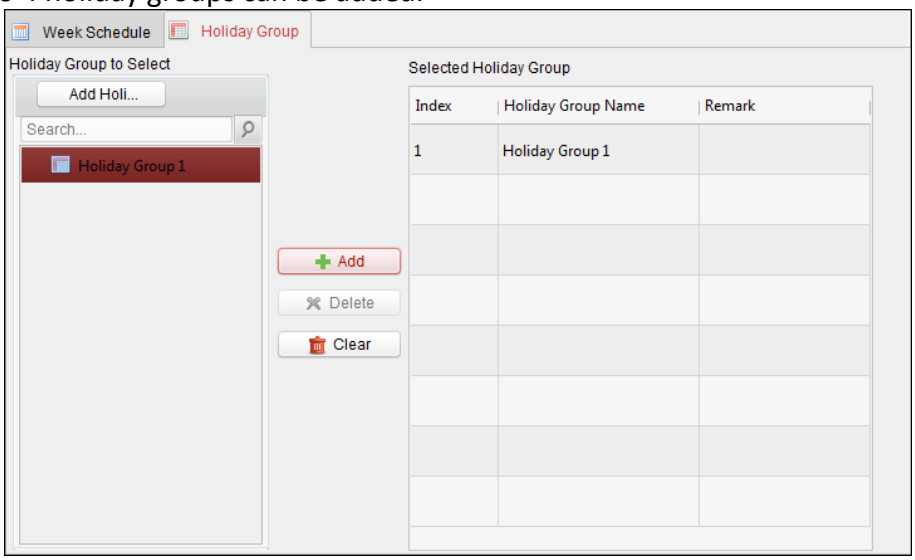
Steps:

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.

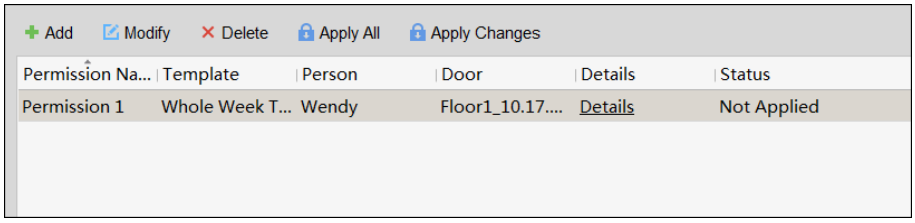


   Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one. For details, refer to *Chapter 7.6.2 Holiday Group.*
   You can click to select an added holiday group in the right-side list and click **Delete** to delete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

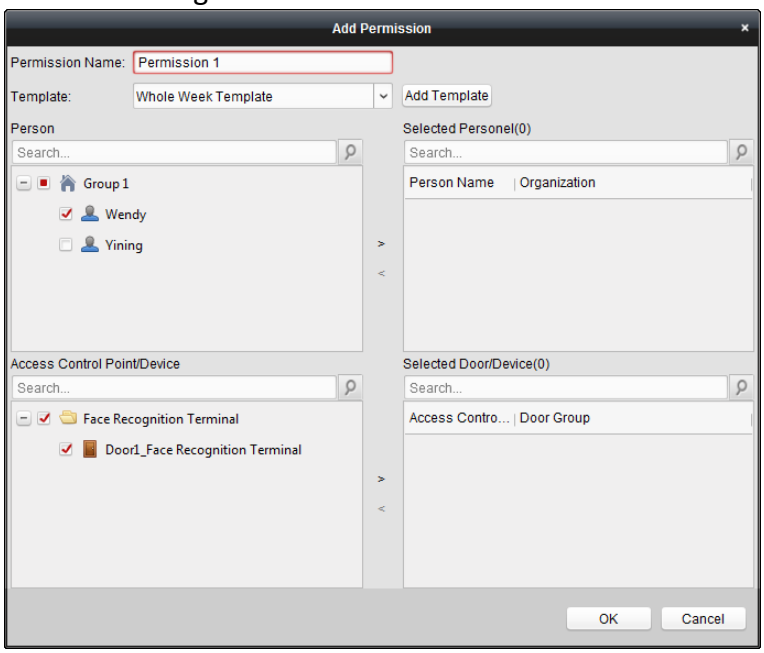
You can assign permission for persons to enter/exist the access control points (doors) in this section.

Notes:

- You can add up to 4 permissions to one access control point of one device.
- You can add up to 128 permissions in total.

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.

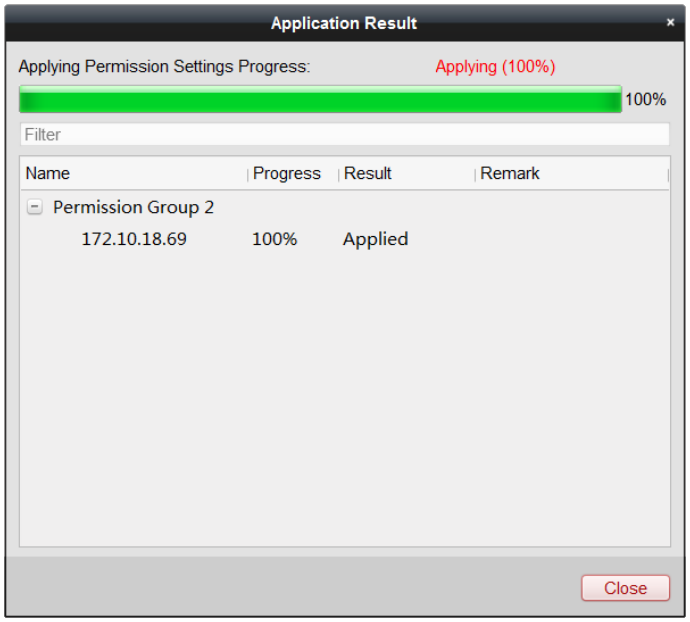
7.7.2 Applying Permission

Purpose:

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

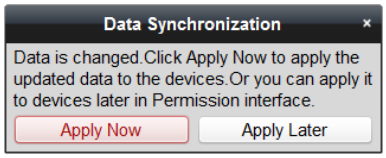
Steps:

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 All** to start applying all the selected permission(s) to the access control device or door station.
   You can also click **Apply Changes** to apply the changed part of the selected permission(s) to the device(s).
3. The following window will pop up, indicating the applying permission result.



Notes:

- When the permission settings are changed, the following hint box will pop up.



  You can click **Apply Now** to apply the changed permissions to the device.

Or you can click **Apply Later** to apply the changes later in the Permission interface.

- The permission changes include changes of schedule and template, permission settings, person's permission settings, and related person settings (including card No., fingerprint, face picture, linkage between card No. and fingerprint, linkage between card No. and fingerprint, card password, card effective period, etc).

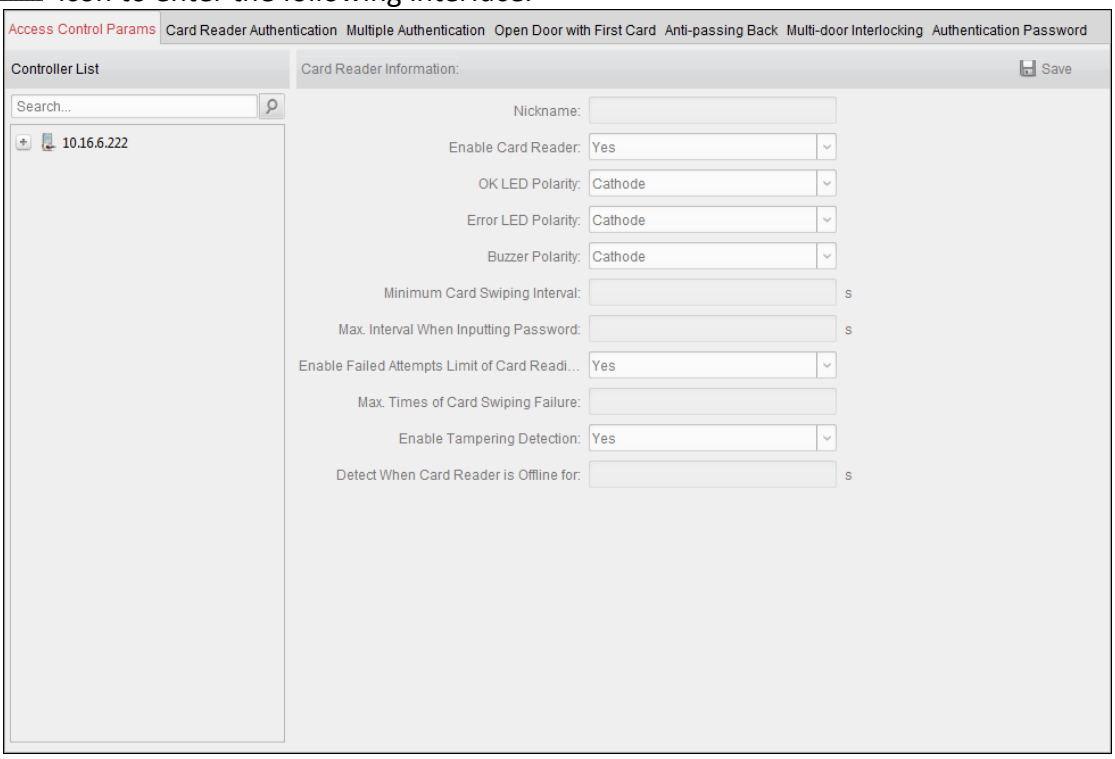
7.8 Advanced Functions

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, opening door with first card 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:

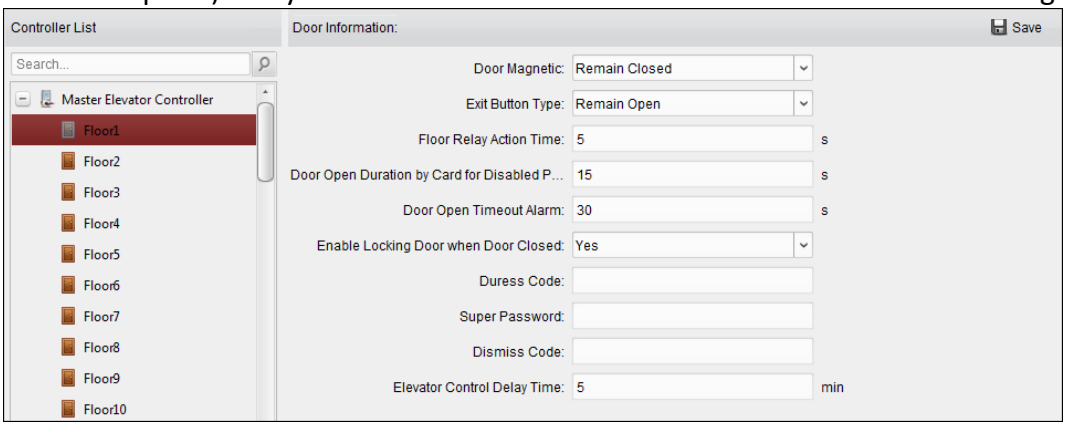
After adding the access control device, you can configure its access control point (Floor)'s parameters, and its card readers' parameters.

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

Floor Parameters

Steps:

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



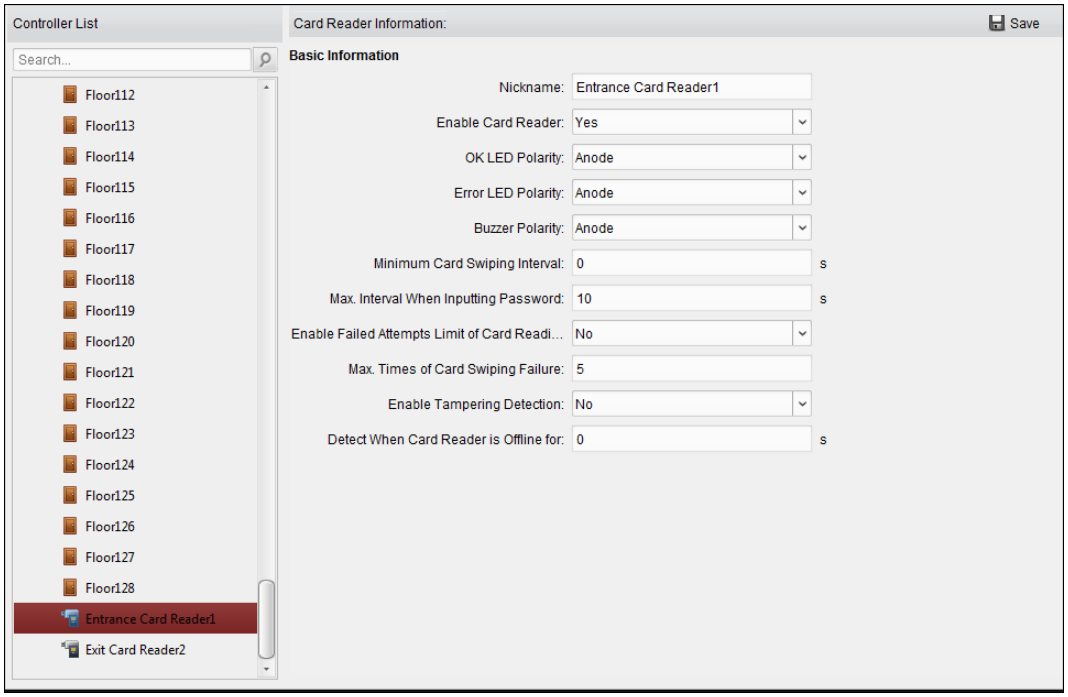
2. You can editing the following parameters:
   - **Door Magnetic**: The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
   - **Exit Button Type**: The Exit Button Type is in the status of **Remain Open** (excluding special conditions).
   - **Floor Relay Action Time**: After swiping the normal card and relay action, the timer for locking the relay starts working.
   - **Door Extended Open Time:** The door magnetic can be enabled with appropriate delay after swiping the card.
   - **Door Open Timeout Alarm**: The alarm can be triggered if the door has not been closed.
   - **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.
   - **Elevator Control Delay Time:** The time duration of the visitor using the elevator.

     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 edit 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.

7.8.2 Card Reader Authentication

Purpose:

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

Steps:

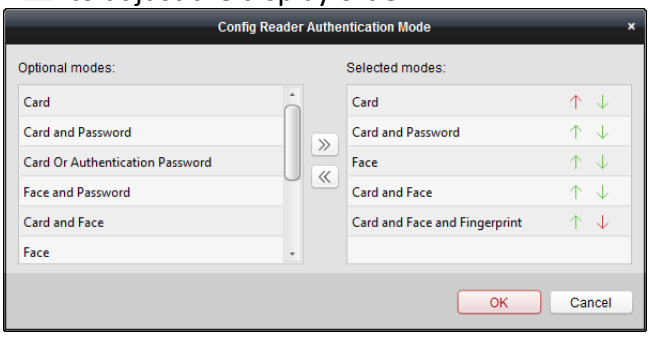
1. Click **Card Reader Authentication** tab and select a card reader on the left.

2. Click **Configuration** button to select the card reader authentication modes for setting the schedule.

   Notes:

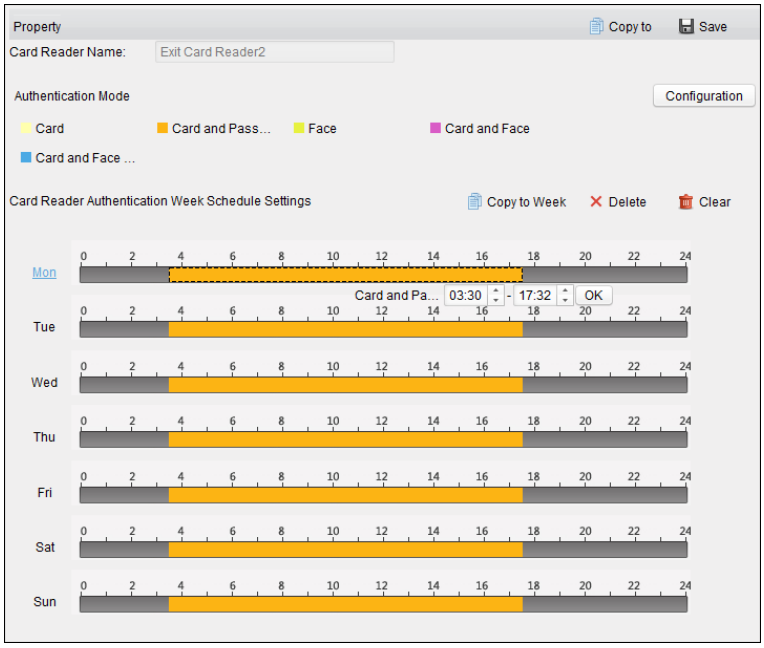
   - The available authentication modes depend on the device type.
   - Password refers to the card password set when issuing the card to the person in *Chapter 7.5 Person Management.*

   1) Select the modes and click » to add to the selected modes list.
      You can click ↑ or ↓ to adjust the display order.

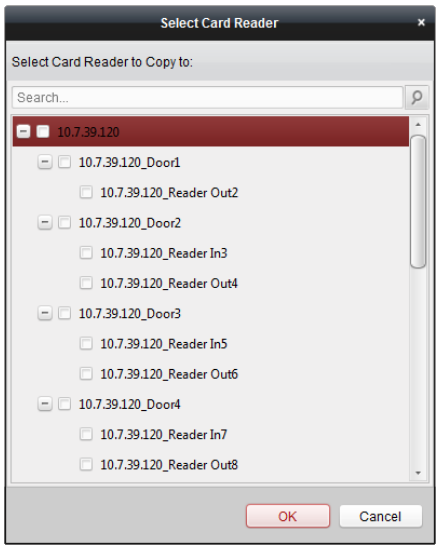


   2) Click **OK** to confirm the selection.

3. After selecting the modes, the selected modes will display as icons.
   Click the icon to select a card reader authentication mode.
4. 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.



5. 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.
6. (Optional) Click **Copy to** button to copy the settings to other card readers.



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

7.8.3 Open Door with First Card

Purpose:

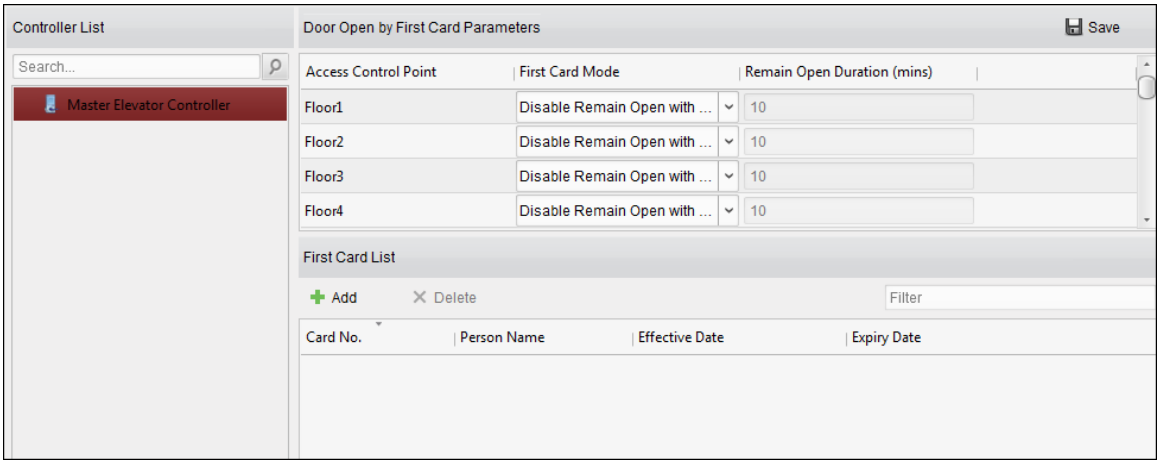
You can set multiple first cards for one access control point. After the first card swiping, it allows multiple persons access the door or other authentication actions. The first card mode contains Remain Open with First Card and Disable Remain Open with First Card.

- **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.
- **Disable Remain Open with First Card:** Disable the function.

  Note: You can swipe the first card again to disable the first card mode.

Steps:

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

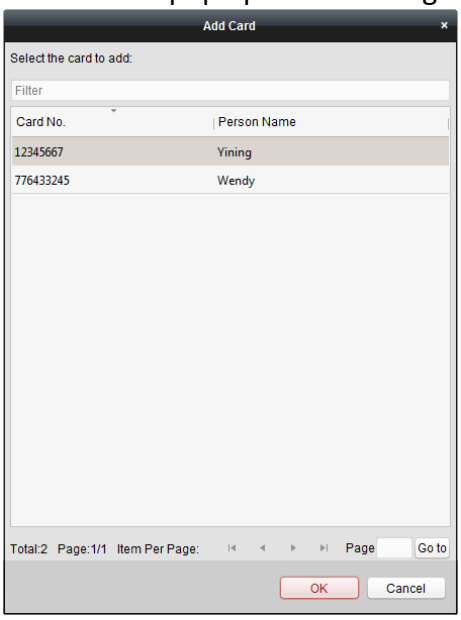


2. Select an access control device from the list on the left.
3. Select the first card mode in the drop-down list for the access control point.
4. (Optional) If you select Remain Open with First Card, you should set remain open duration.

   Notes:

- The Remain Open Duration should be between 0 and 1440 minutes. By default, it is 10 minutes.
- You can swipe the first card again to disable the first card mode.

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



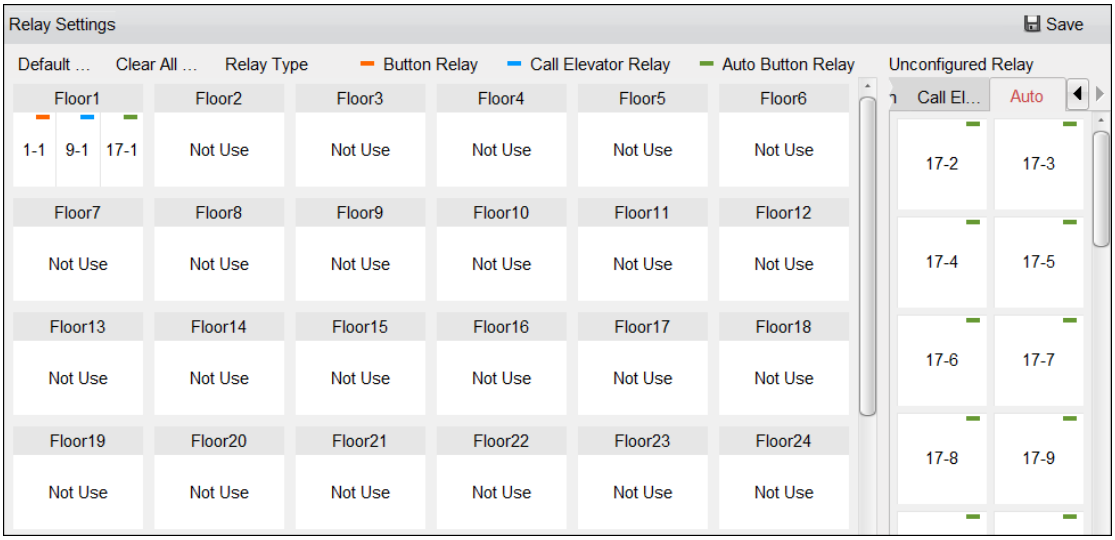
   1) Select the cards to add as first card for the door
      Note: Set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration*.
   2) Click **OK** button to save adding the card.
6. You can click **Delete** button to remove the card from the first card list.
7. Click **Save** to save and take effect of the new settings.

7.8.4 Relay Settings

Purpose:
For elevator controller, you can manage the relationship between the floor and the relay in this chapter.

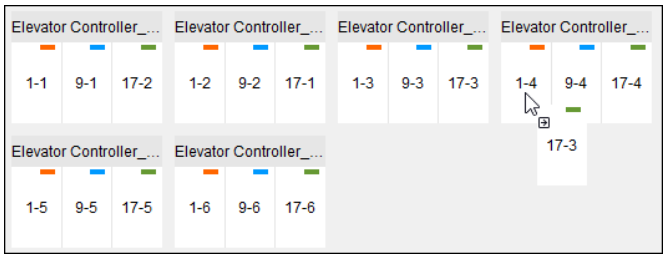
Configuring Relay and Floor

Steps:
1. Click **Relay Settings** tab to enter the Relay Settings interface.



2. Select an elevator controller in the Controller List on the left of the interface.
3. Select an unconfigured relay in the Unconfigured Relay panel on the right of the interface.
   There are three types of unconfigured relays: Button Relay, Call Elevator Relay and Auto Button Relay.
   - **Button Relay:** Control the validity for buttons of each floor.
   - **Call Elevator Relay:** Control to call the elevator to go to the specified floor.
   - **Auto Button Relay:** Control to press the button when the user swipes card inside the elevator. The button of the floor will be pressed automatically according to the user's permission.

4. Click and drag the unconfigured relay from the Unconfigured Relay panel to the coressponding floor in the Floor List panel.
   Or click and drag the relay from the Floor List panel to the Unconfigured Relay panel.
   Or click and drag the relay from one floor to another floor in the Floor List panel.
   When clicking and dragging, if two relays are of the same relay type in the two different floors, the relays will change the place.



5. Click **Save** to apply the settings to the selected device.

   Notes:

   - An elevator controller can link to up to 24 distributed elevator controllers. A distributed elevator controller can link up to 16 relays.
   - Three types of relay are available: Button Relay, Call Elevator Relay and Auto Button Relay. ▬ represents the button relay, ▬ represents the call elevator relay, and ▬ represents the auto button relay.

     Take the fiugre

     as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents the ralay, and the icon ▬ represents the relay type. You can click **Relay Type** to configure the relay type. For details about configuring the relay type, see *Configuring Relay Type*.
   - By default, the relay total amount is the added floor number *3 (three types of relay).
   - Each floor contains up to 3 types of relay. You can click and drag one relay once.
   - If you change the floor number in the door group management, all relays in the Relay Settings interface will restore to the default settings.
   - The action time duration of the call elevator relay and the auto button relay is 1s.

Configuring Relay Type

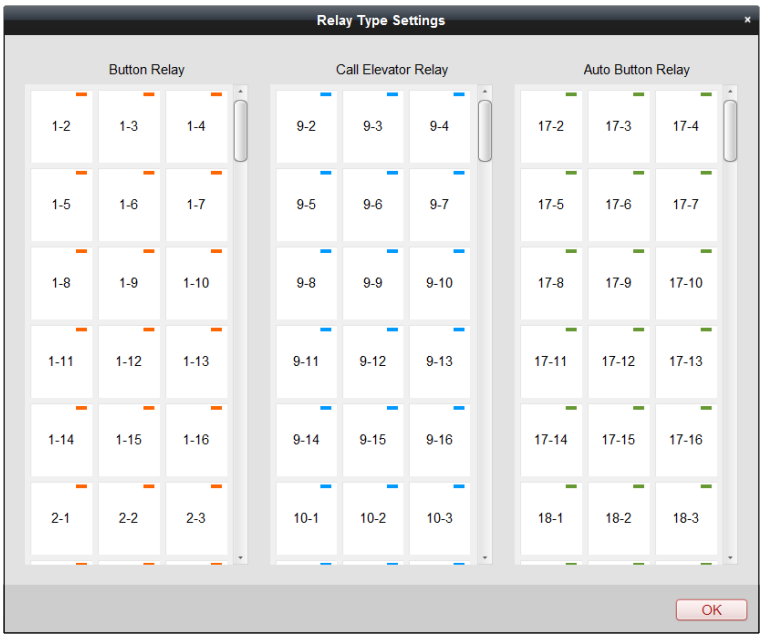
Purpose:

You can change the relay type by following the steps in this section.

Steps:

1. In the Relay Settings interface, click **Relay Type** to pop up the Relay Type Settings window.

   Note: All relays in the Relay Type Settings window are unconfigured relays.



2. Click and drag the relay from one relay type panel to the other one.
3. Click **OK** to save the settings.

Note: Three types of relay are available: Button Relay, Call Elevator Relay and Auto Button Relay. ▬ represents the button relay, ▬ represents the call elevator relay, and ▬ represents the auto button relay.

7.9 Searching Access Control Event

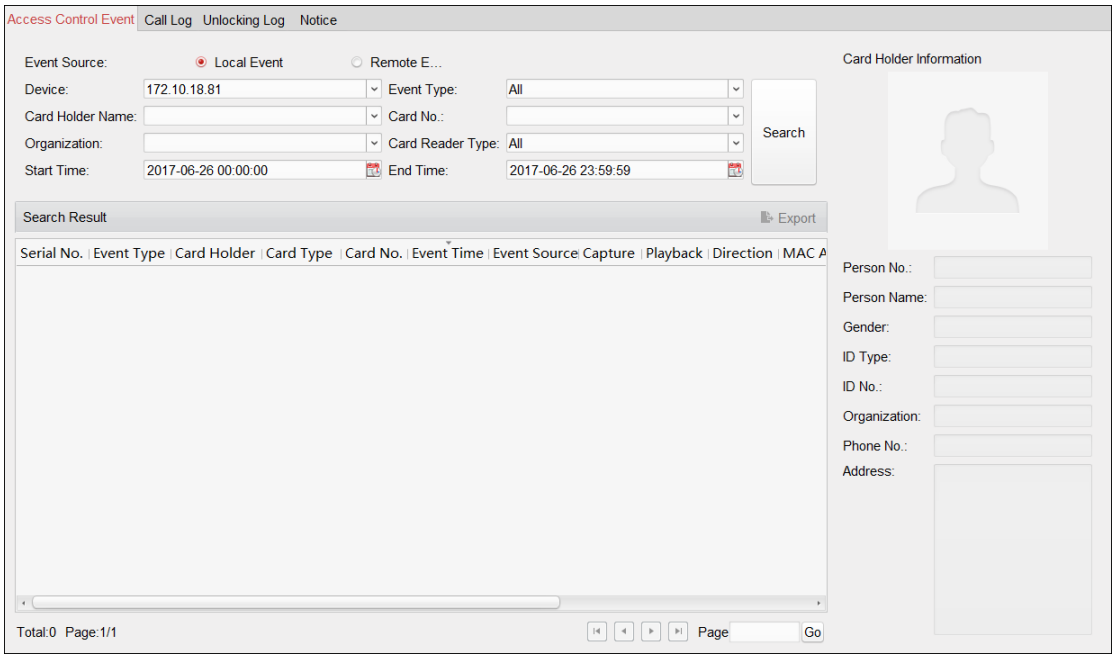
Purpose:

You can search the access control history events including remote event and local event via the client.

Local Event: Search the access control event from the database of the control client.

Remote Event: Search the access control event from the device.

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



7.9.1 Searching Local Access Control Event

Steps:

1. Select the Event Source as **Local Event**.
2. Input the search condition according to actual needs.
3. Click **Search**. The results will be listed below.
4. For the access control event which is triggered by the card holder, you can click the event to view the card holder details, including person No., person name, organization, phone number, contact address and photo.
5. (Optional) If the event contains linked pictures, you can click in the **Capture** column to view the captured picture of the triggered camera when the alarm is trigged.
6. (Optional) If the event contains linked video, you can click in the **Playback** column to view the recorded video file 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*.
7. You can click **Export** to export the search result to the local PC in *.csv file.

7.9.2 Searching Remote Access Control Event

Steps:

1. Select the Event Source as **Remote Event**.
2. Input the search condition according to actual needs.

3. (Optional) You can check **With Alarm Picture** checkbox to search the events with alarm pictures.
4. Click **Search**. The results will be listed below.
5. You can click **Export** to export the search result to the local PC in *.csv file.

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 (floor), 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 7.1 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.

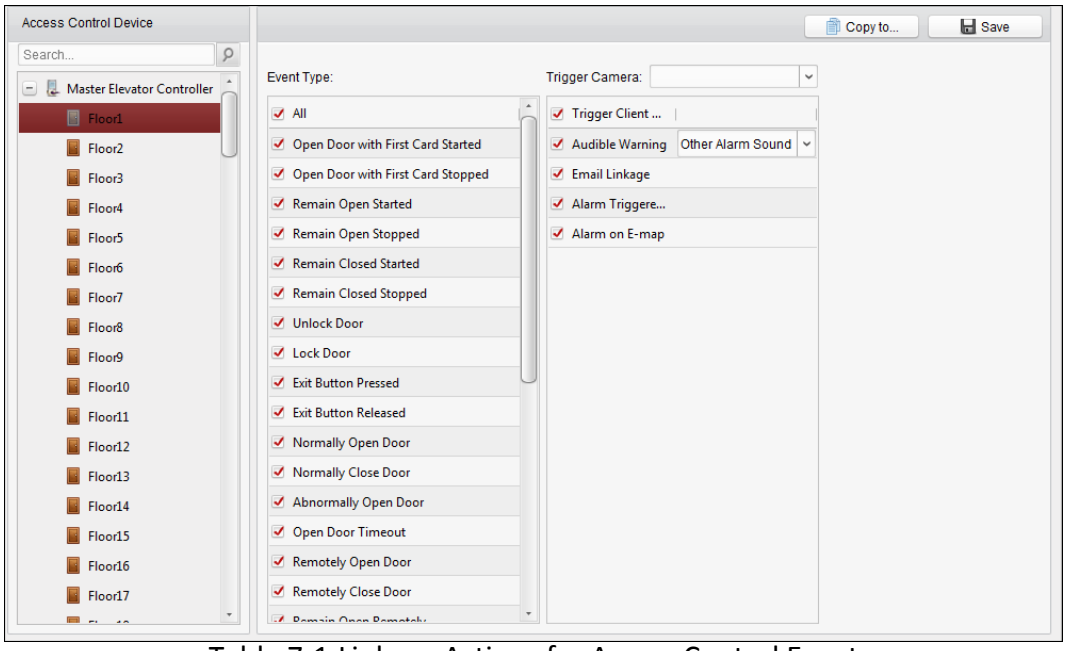
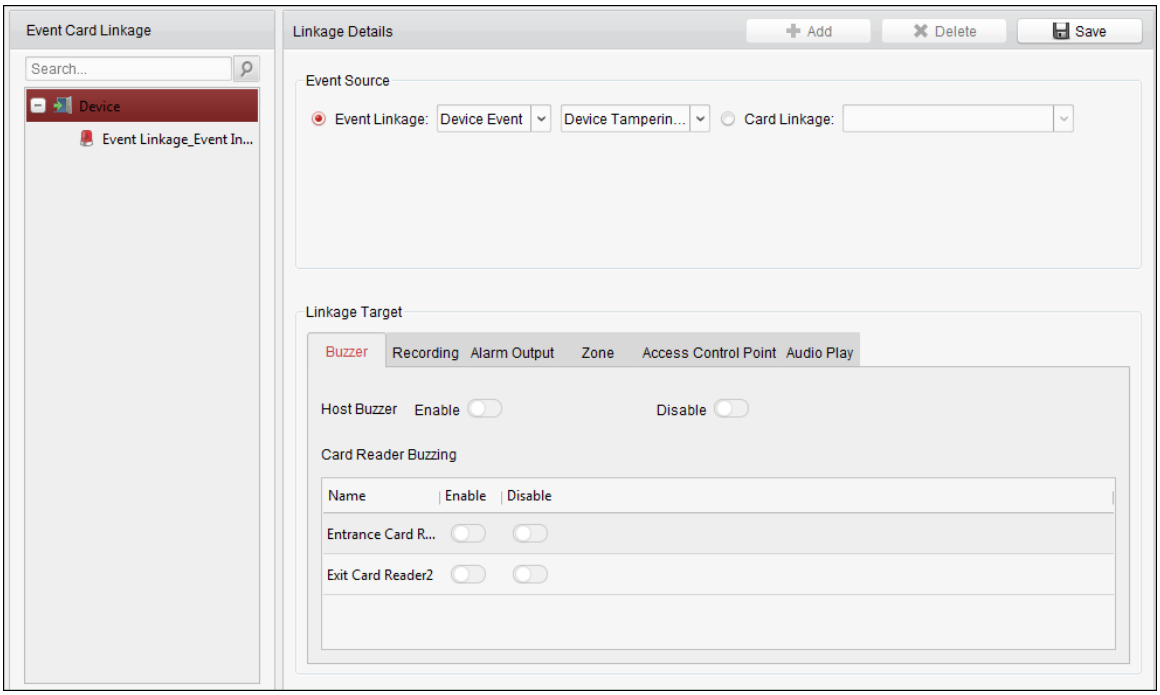


Table 7-1 Linkage Actions for Access Control Event

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 Event Card Linkage

Click **Event Card Linkage** tab to enter the following interface.
Note: The Event Card Linkage should be supported by the device.



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. Select a device on the left and click **Add.**
2. 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 panel.
   - For Door Event, select the detailed event type and select the source door from the panel.
   - For Card Reader Event, select the detailed event type and select the card reader from the panel.
3. Click different tabs to set different parameters. Switch the property from to to enable this function.

   You can set the parameters of buzzer, recording, alarm output, zone, access control point, and audio play.

Linkage Type	Linkage Target	Descriptions
Buzzer	Host Buzzer	The audible warning of controller will be triggered.
	Card Reader Buzzing	The audible warning of card reader will be triggered.

Recording	Capture Status	The real-time capture will be triggered.
Alarm Output	Alarm Output	The alarm output will be triggered for notification.
Access Control Point	Access Control Point	The door status of open, close, remain open, and remain closed will be triggered. ***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.

4. Click **Save** 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 panel for triggering.
5. Click different tabs to set different parameters. Switch the property from to to enable this function.
   You can set the parameters of buzzer, recording, alarm output, zone, access control point, and audio play.

Linkage Type	Linkage Target	Descriptions
Buzzer	Host Buzzer	The audible warning of controller will be triggered.
	Card Reader Buzzing	The audible warning of card reader will be triggered.
Recording	Capture Status	The real-time capture will be triggered.
Alarm Output	Alarm Output	The alarm output will be triggered for notification.
Access Control Point	Access Control Point	The door status of open, close, remain open, and remain closed will be triggered. ***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.

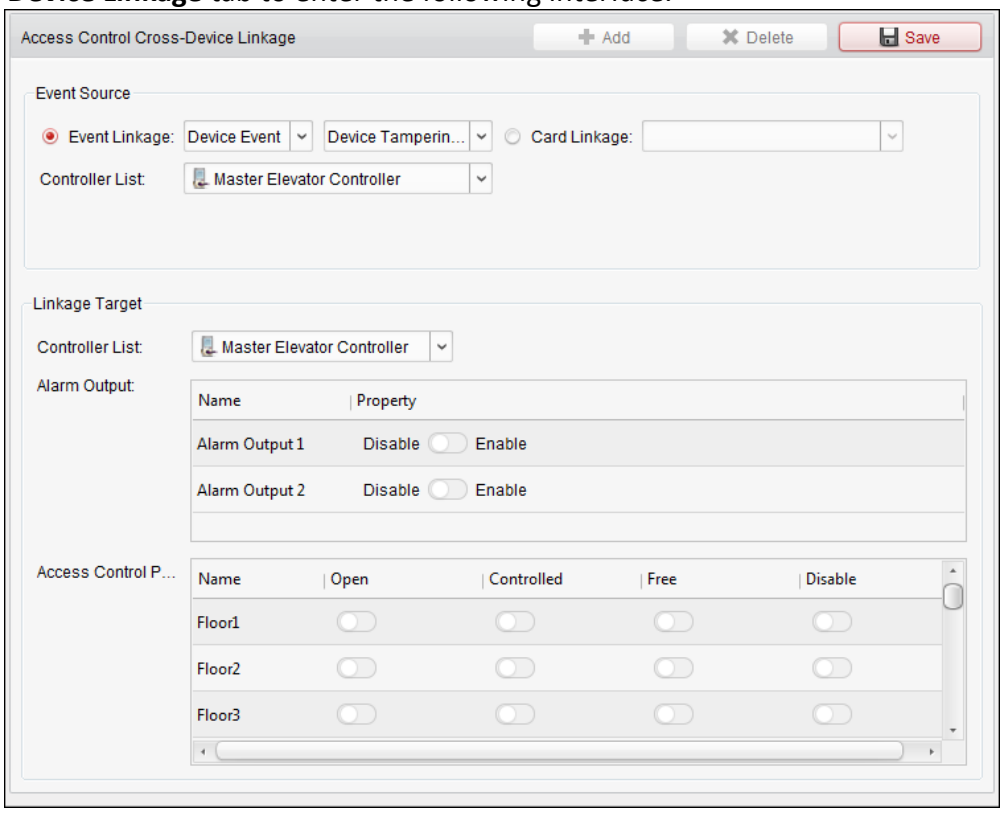
4. Click **Save** to save and take effect of the parameters.

7.10.3 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

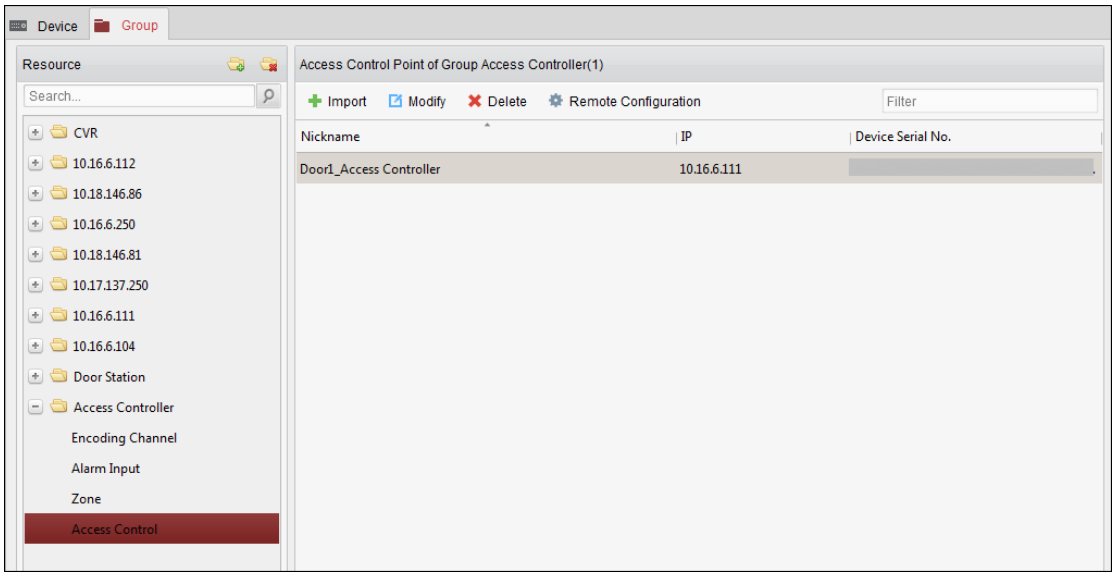
Purpose:

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:

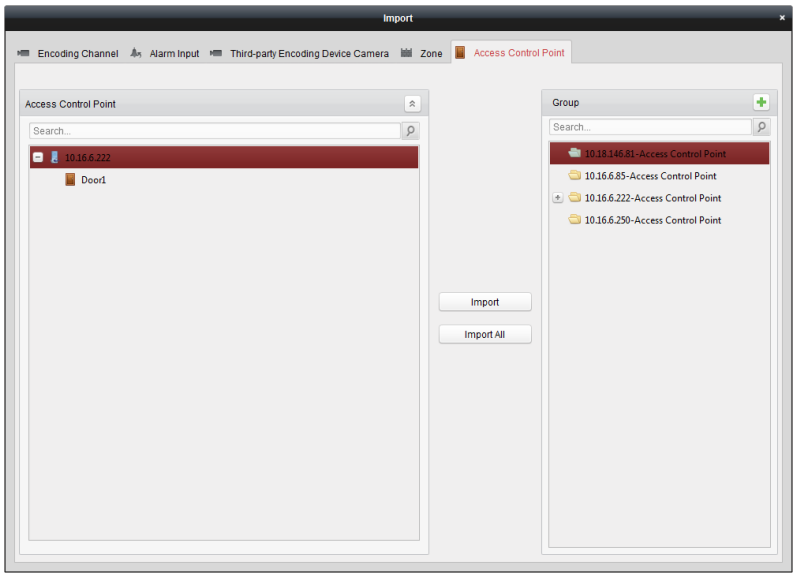
Steps:

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 Controlling Floor Status

Purpose:

You can control the status for a single floor when the device is elevator controller, including opening door, controlled, free, calling elevator, etc.

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 floors of the selected access control group will be displayed on the right of the interface.
3. Click on the Status Information panel to select a floor.
4. Click the following button listed on the **Status Information** panel to control the elevator.
   - **Open Door:** The floor button will be valid for a period of time.
   - **Controlled:** You should swipe the card to press the selected floor button. And the elevator can go to the selected floor.
   - **Free:** The selected floor button will be valid all the time.
   - **Disable:** You cannot go to the selected floor.
   - **Call Elevator (Visitor)**: The elevator will go down to the first floor. The visitor can only press the selected floor button.
   - **Call Elevator (Resident)**: Call the elevator to the selected floor.
5. You can view the anti-control operation result in the Operation Record panel.

Notes:

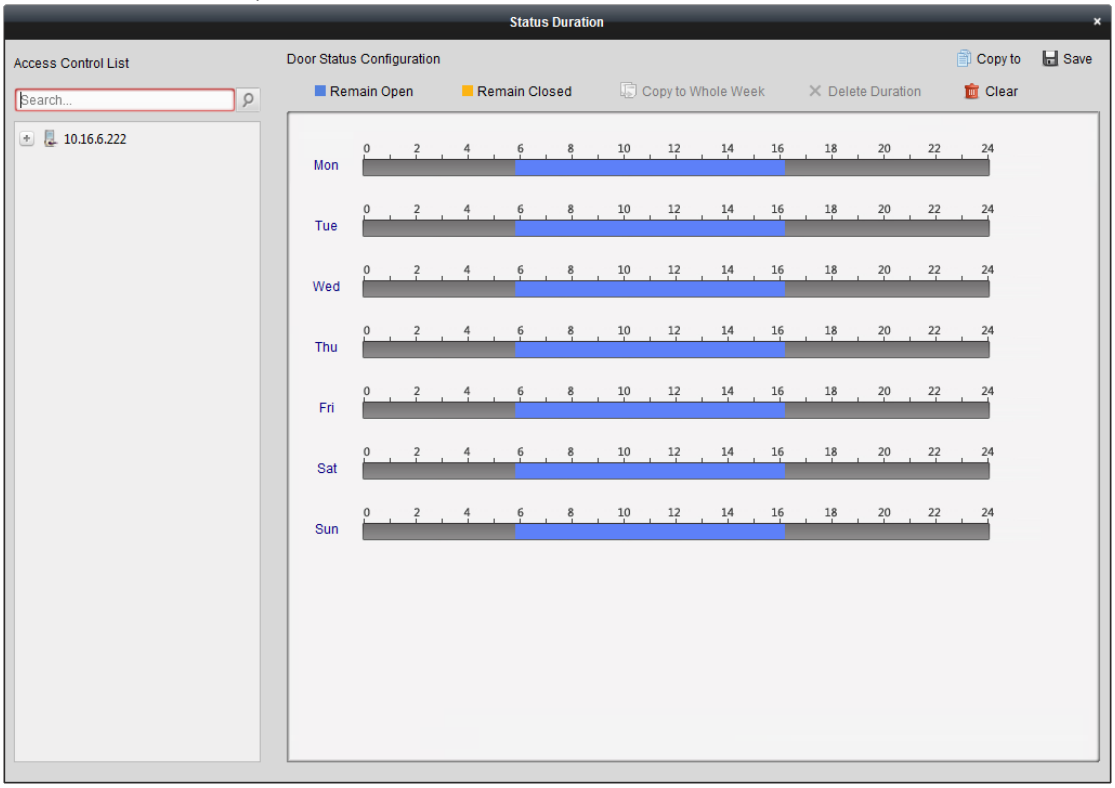
- The elevator cannot be controlled by other client software if the elevator status changes.
- Only one client software can control elevator each time.
- The client software which has controlled the elevator can receive the alarm information and the elevator status. Other clients cannot.

7.11.3 Status Duration Configuration

Purpose:

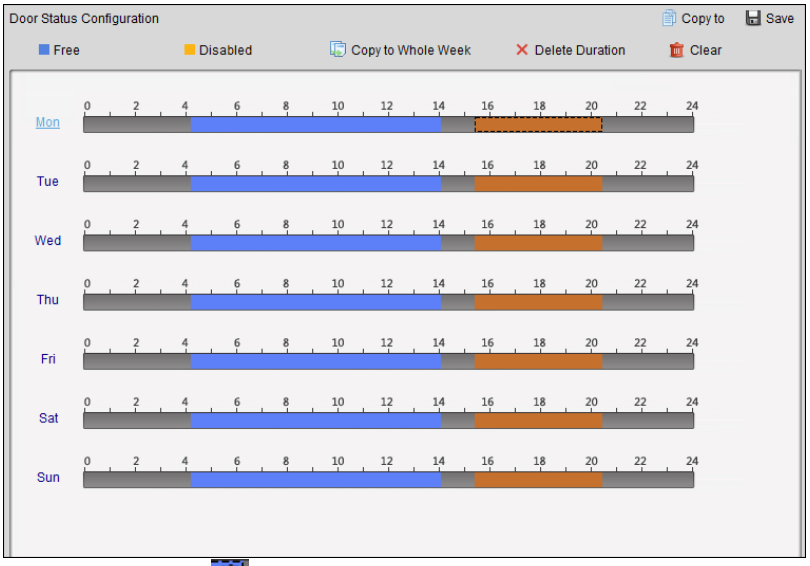
You can schedule weekly time periods for an access control point (floor) to be free or disabled.

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



Steps:

1. Click to select a floor 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 status brush as **Free** or **Disabled**.
      - **Free**: The floor button will be free during the configured time period. The brush is marked as ▬.
      - **Disabled:** You cannot press the floor button 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.

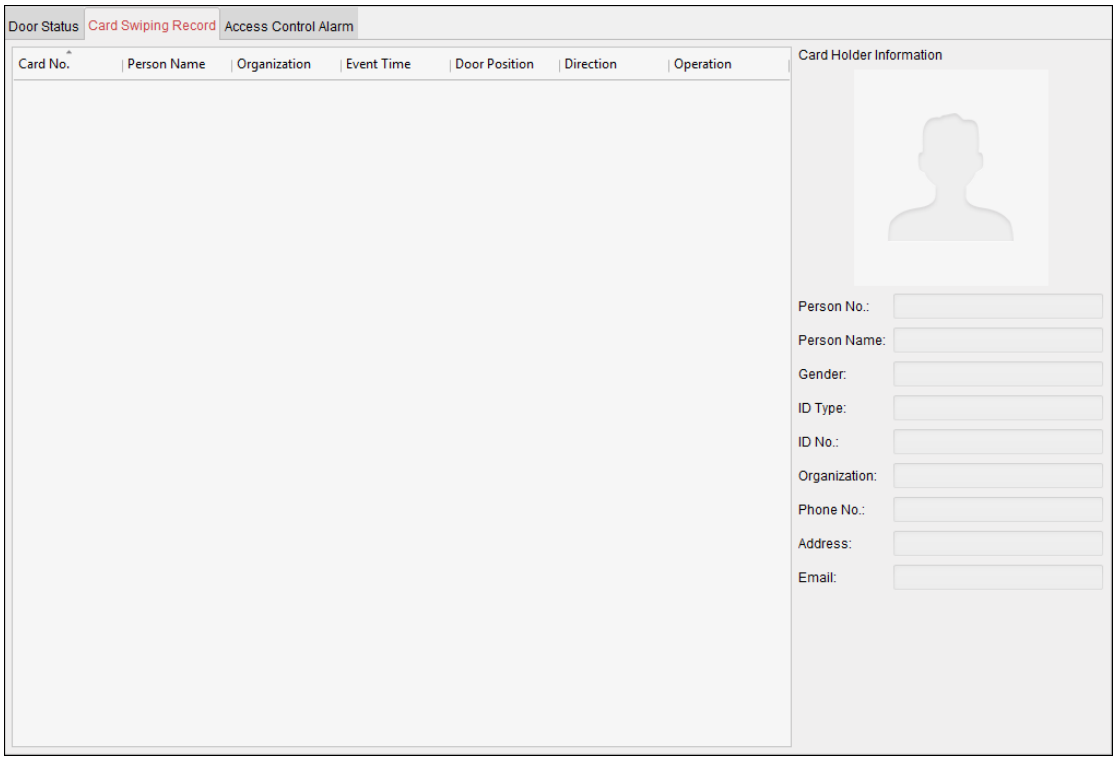


3) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
   When the cursor turns to , you can lengthen or shorten the selected time bar.

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.

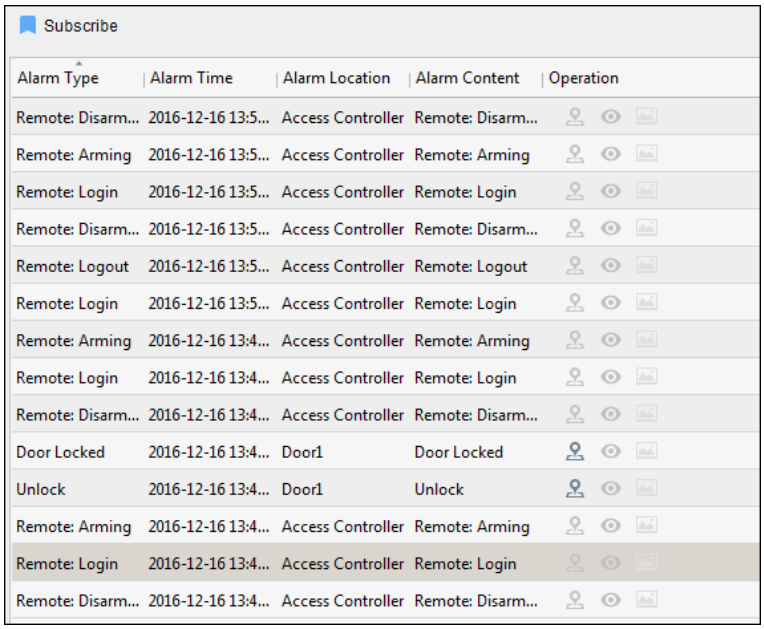
You can also click the event to view the card holder details, including person No., person name, organization, phone, contact address, etc.

7.11.5 Real-time Access Control Alarm

Purpose:

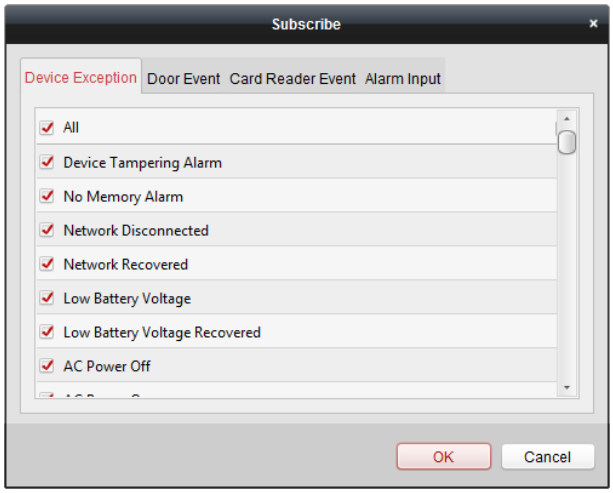
The logs of access control events will be displayed in real time, including device exception, door event, card reader event, and alarm input.

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.

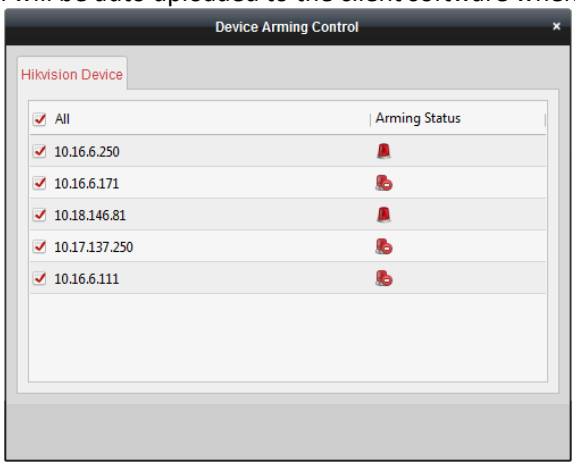
7.12 Arming Control

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.



0100011080316

See Far, Go Further

UD03831B-C