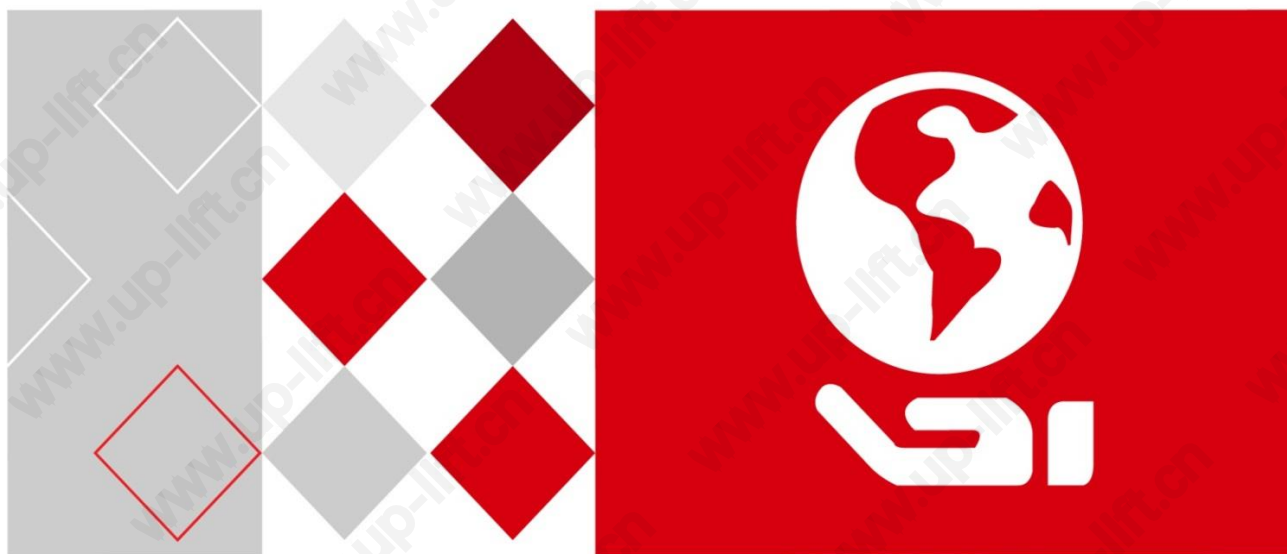


HIKVISION



Master Elevator Controller

User Manual

UD03831B

User Manual

This user manual is intended for users of the models below:

Name	Model
Master 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.

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

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

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

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

FCC Conditions

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

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

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.



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



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



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.

Contents

Chapter 1	Overview.....	1
1.1	Introduction	1
1.2	Main Features	1
Chapter 2	Appearance.....	2
2.1	Device Appearance Introduction	2
2.2	Indicator Information.....	3
Chapter 3	Installation.....	4
Chapter 4	Device Wiring.....	5
Chapter 5	Activation.....	7
5.1	Activating Device via Web Client	7
5.2	Activating Device via SADP Tool.....	7
5.3	Activating Device via Client Software	9
Chapter 6	Web Client Operation	11
6.1	Overview	11
6.1.1	Introduction	11
6.1.2	Running Environment	11
6.2	Login/Logout Web Client	11
6.2.1	Login.....	11
6.2.2	Logout	12
6.3	Setting Device via Web Client	13
6.3.3	System Settings	13
6.3.4	Network Settings.....	15
6.3.5	System Maintenance.....	16
6.3.6	Elevator Control Settings	16
Chapter 7	Client Operation	20
7.1	Overview of iVMS-4200 Client Software.....	20
7.1.1	Description.....	20
7.1.2	Running Environment	20
7.1.3	Client Performance	20
7.2	User Registration and Login	21
7.2.1	User Registration.....	21
7.2.2	Login.....	21
7.2.3	Function Modules	22
7.3	Basic Configuration	25
7.3.1	Work Flow	25
7.3.2	Card Reader Configuration.....	25
7.3.3	Fingerprint Machine Configuration	26
7.3.4	Storage Server Configuration	26
7.4	Device Management.....	28
7.4.1	Access Control Device Management.....	28
7.4.2	Door Group Management.....	33
7.4.3	Editing Access Control Device	35
7.4.4	Deleting Device	38
7.4.5	Time Synchronization	39
7.4.6	Viewing Device Status.....	39
7.4.7	Remote Configuration.....	40
7.4.8	Network Settings (Do Not Support by Elevator Control Device).....	46
7.4.9	Capture Settings (Do Not Support by Elevator Control Device).....	48
7.4.10	RS-485 Settings (Do Not Support by Elevator Control Device)	50
7.5	Person Management.....	50

7.5.1	Department Management	51
7.5.2	Person Management.....	52
7.6	Card Management	57
7.6.1	Empty Card.....	57
7.6.2	Normal Card.....	59
7.6.3	Lost Card	62
7.7	Relay Management	63
7.7.1	Configuring Relay and Floor.....	63
7.7.2	Configuring Relay Type.....	65
7.8	Schedule Template.....	65
7.8.1	Week Schedule.....	66
7.8.2	Holiday Group	67
7.8.3	Schedule Template	68
7.9	Permission Configuration.....	70
7.9.1	Adding Permission	71
7.9.2	Applying Permission.....	72
7.9.3	Importing/Exporting Permission.....	73
7.9.4	Searching Access Control Permission.....	74
7.10	Advanced Functions.....	75
7.10.1	Card Type	75
7.10.2	Card Reader Authentication.....	77
7.10.3	Open Door with First Card	79
7.11	Linkage Configuration	80
7.11.1	Event Card Linkage	80
7.11.2	Client Linkage.....	81
7.12	Attendance Management	83
7.12.1	Attendance Configuration	83
7.12.2	Attendance Statistic	95
7.13	Access Control System Maintenance	95
7.13.1	Door Status Management.....	95
7.13.2	Account Management.....	98
7.13.3	Event and Alarm Management	99
7.13.4	Log Management	102
7.13.5	People Counting Statistics.....	103
7.13.6	System Maintenance.....	104
Chapter 8	Appendix.....	106
8.1	Tips for Scanning Fingerprint.....	106
8.2	Device Dimension	107
8.3	Access Controller Model List.....	108

Chapter 1 Overview

1.1 Introduction

The elevator controller contains master elevator controller and distributed elevator controller. It can be applied to buildings, public areas and so on. The master 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 master elevator controller by the web client, iVMS-4200 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 master elevator controlling via the web client, the iVMS-4200 client software, or other systems.
- Connectable to the Third party system.
- Supports managing the floor status through the master elevator controller. The floor status includes "Disable", "Controlled", and "Free".
- Linkage of the distributed elevator controller and reporting the alarm event to the system.

Chapter 2 Appearance

2.1 Device Appearance Introduction

The device appearance introduction is shown as follows:

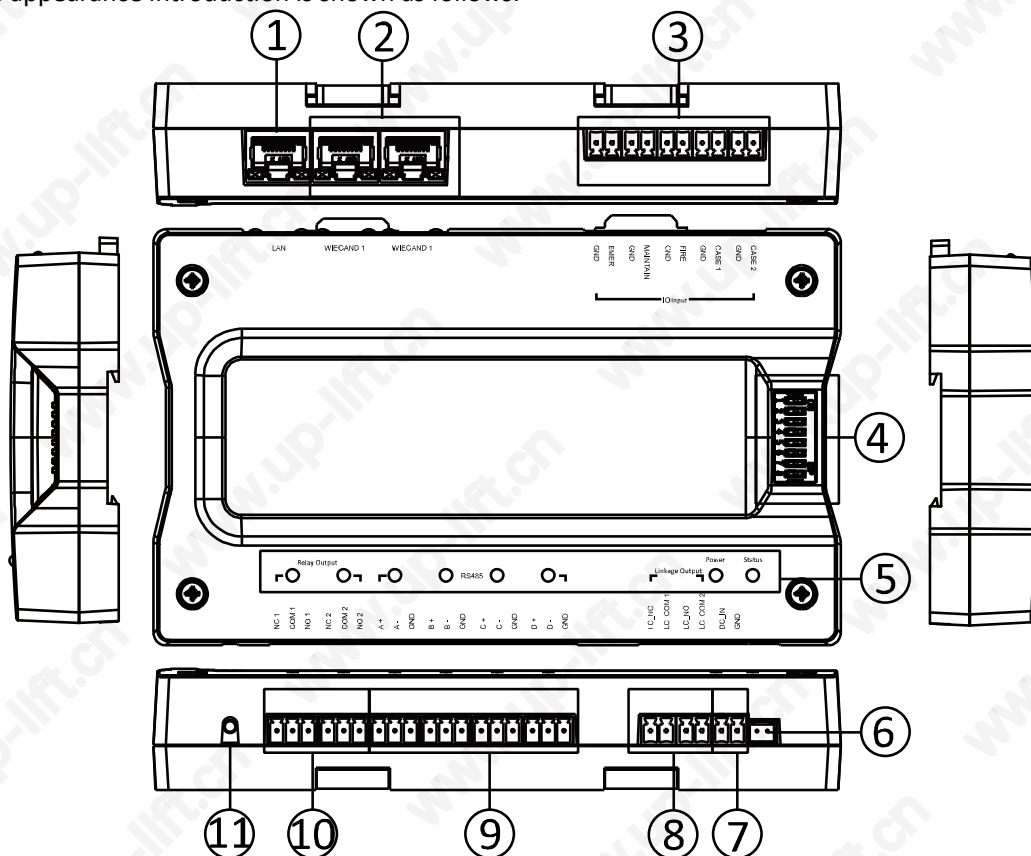


Table 2. 1 Device Appearance Description

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	Off
Relay NO	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

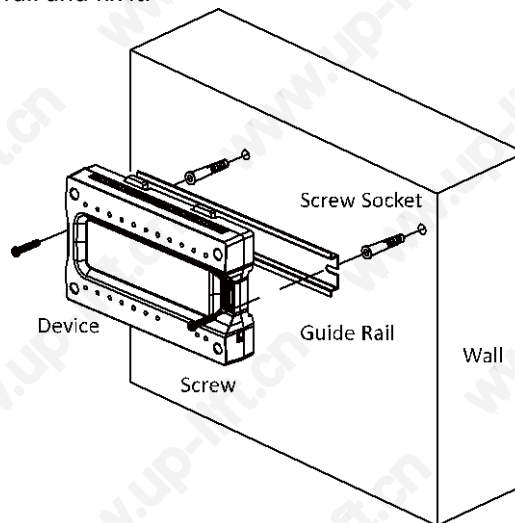
Chapter 3 Installation

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:

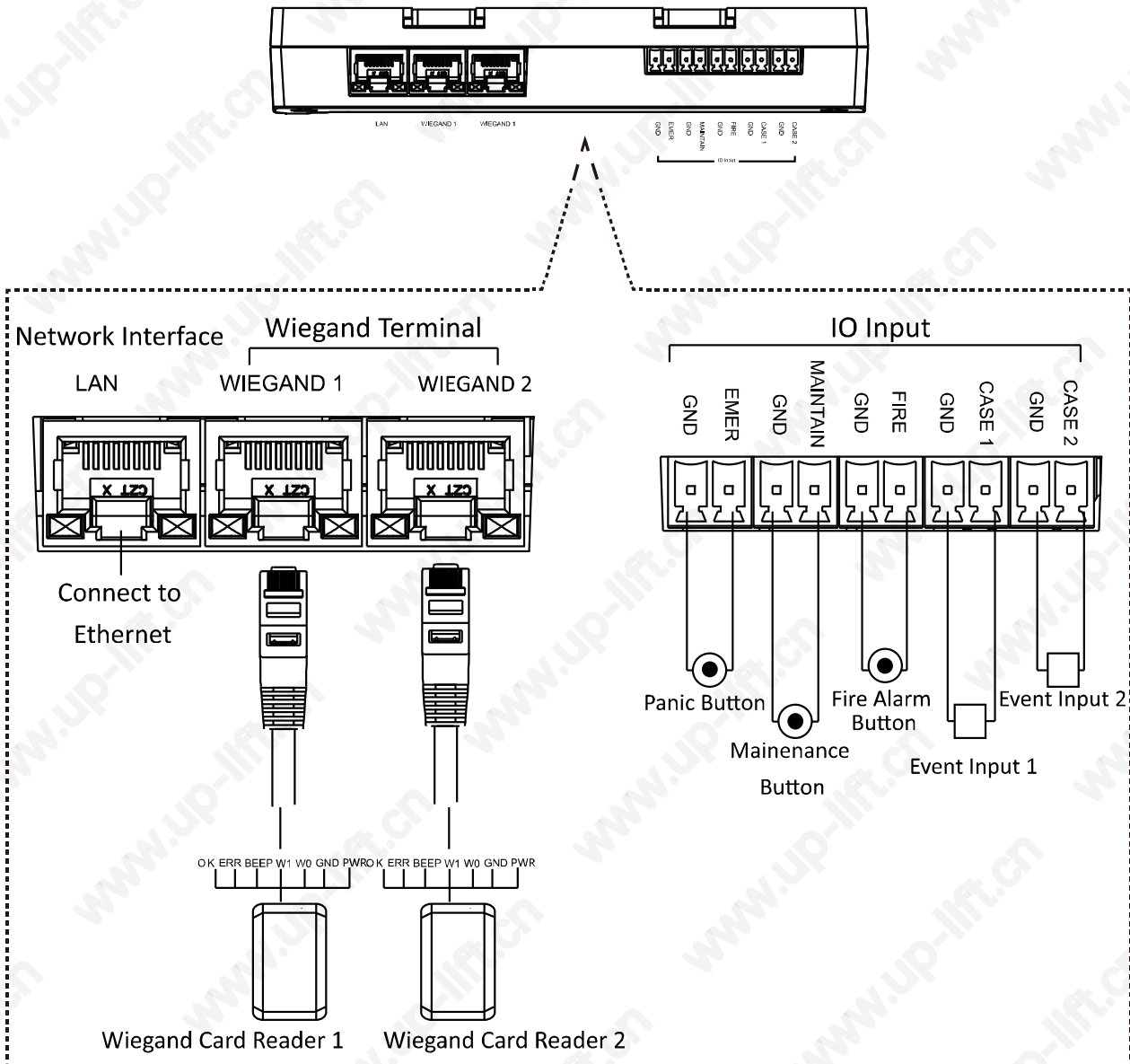
1. Drill holes on the wall or other places according to the holes on the guide rail.
2. Insert the screw sockets of the set screws (supplied) in the drilled holes.
3. Secure the guide rail on the wall or other places with the screws (supplied).
4. Push the device to the guide rail and fix it.



Chapter 4 Device Wiring

When the panic button, the maintenance button, fire alarm button, and the event alarm are triggered, the master 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:

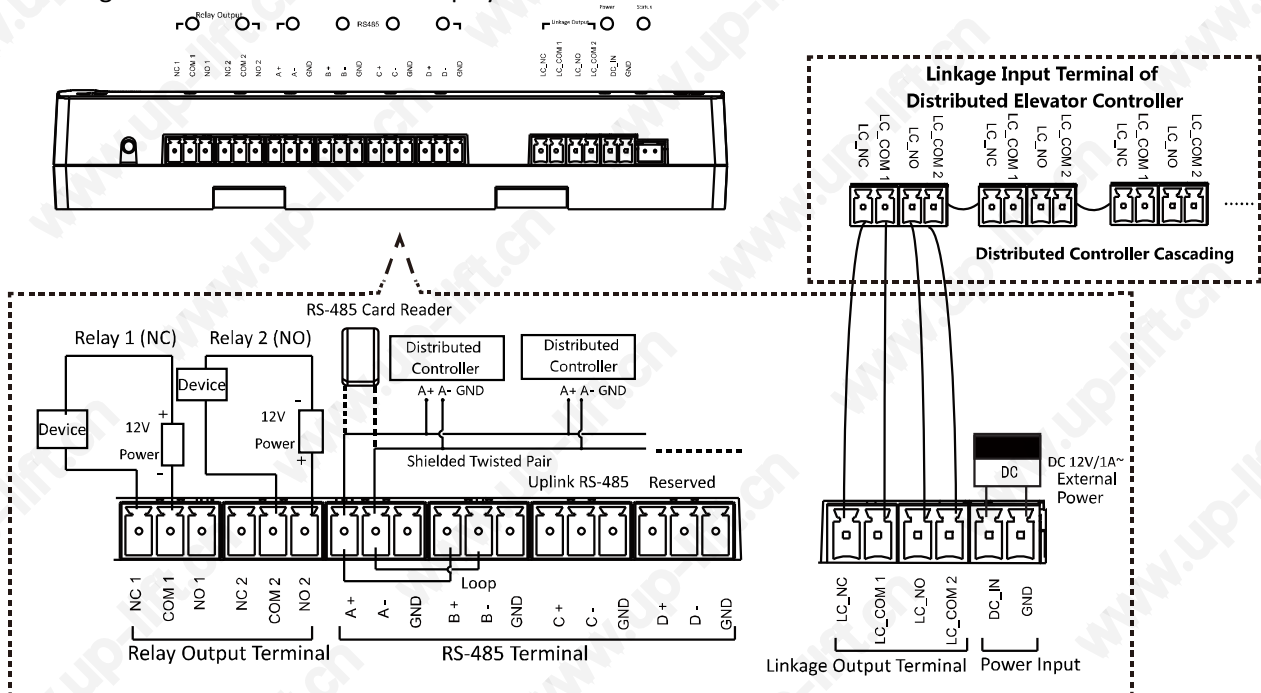
- When the panic button is triggered, all relays keep connected. It is valid for all floors.
- When the fire alarm button is triggered, all relays keep disconnected. It is invalid for all floors.
- When the maintenance button is triggered, all relays keep disconnected. It is invalid for all floors.

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:



Note: Each master 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.

Chapter 5 Activation

Purpose:

You should activate the device before the first login.

Activation via the Web client, the SADP tool and the iVMS-4200 Client Software are supported.

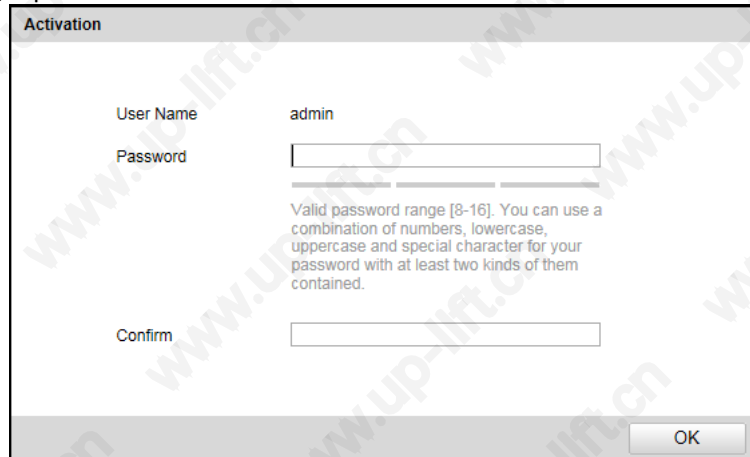
The default values of the terminal are as follows:

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

5.1 Activating Device via Web Client

Steps:

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



3. Input the password 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 **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 Device via SADP Tool

Purpose:

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

Steps:

1. Get the SADP software from the supplied disk or the official website. Install and run the software.

Total number of online devices: 6

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
001	DS-7208HGH-SH	Active	10.16.1.72	8000	V3.3.0build 1508...	10.16.1.254	80	DS-7208HGH-SH08
002	DS-7104N-SN/N	Active	10.16.1.28	8000	V3.0.19build 160...	10.16.1.254	N/A	DS-7104N-SN/N042
003	DS_8106THFH_E2	Active	10.16.1.248	8000	V3.0.0build 1408...	10.16.1.254	N/A	DS_8106THFH_E207
004		Active	10.16.1.250	8000	V5.4.0build 1602...	10.16.1.254	80	20141119CCWR45
005	DS-2CD864FWD-E	Active	10.16.1.102	8000	V5.1.0build 1312...	10.16.1.254	80	DS-2CD864FWD-E2
006	DS-K1A801MF	Inactive	192.0.0.64	8000	V1.0.0build 1607...	0.0.0.0	80	DS-K1A801MF2016

Modify Network Parameters

☐ Enable DHCP

Device Serial No.:

IP Address:

Port:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port:

Security Verification:

Admin Password:

Modify

[Forgot Password](#)

- Check the inactive device from the device list.
- Create a password in the right side of the interface 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.

Total number of online devices: 6

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
001	DS-7208HGH-SH	Active	10.16.1.72	8000	V3.3.0build 1508...	10.16.1.254	80	DS-7208HGH-SH08
002	DS-7104N-SN/N	Active	10.16.1.28	8000	V3.0.19build 160...	10.16.1.254	N/A	DS-7104N-SN/N042
003	DS_8106THFH_E2	Active	10.16.1.248	8000	V3.0.0build 1408...	10.16.1.254	N/A	DS_8106THFH_E207
004	UNKNOWN-DEVICE-TYPE	Active	10.16.1.250	8000	V5.4.0build 1602...	10.16.1.254	80	20141119CCWR45
005	DS-2CD864FWD-E	Active	10.16.1.102	8000	V5.1.0build 1312...	10.16.1.254	80	DS-2CD864FWD-E2
006	DS-K1A801MF	Inactive	192.0.0.64	8000	V1.0.0build 1607...	0.0.0.0	80	DS-K1A801MF2016

1. Check the inactive device.

2. Create a new password and confirm the new password

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

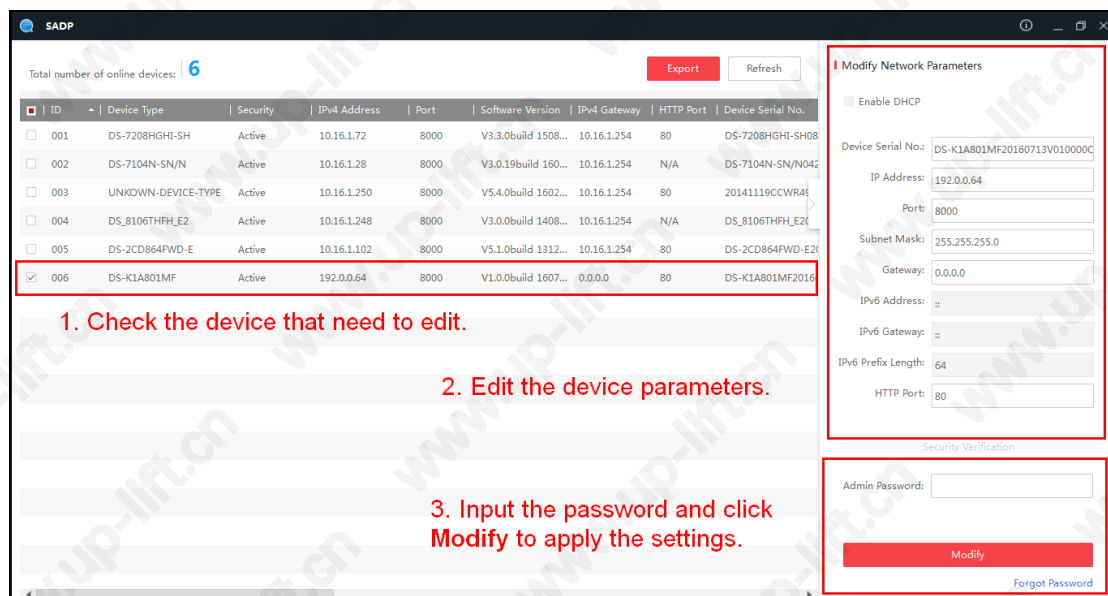
New Password:

Confirm Password:

Activate

- Click **Activate**. The device will be active.
Or click **Fresh** to fresh the device status.
- Check the device and manually edit the device IP address, Port No., Subnet Mask, Gateway, etc.
Or check **DHCP** to enable DHCP.
- Input the password and click **Modify** to apply the settings.

Note: The device IP segment should be the same with the PC's.



5.3 Activating Device via Client Software

Purpose:

The iVMS-4200 Access Control Client is a client-based access control system for management of access control devices.

Steps:

1. Install and run the software.



2. Click **Device Management** icon to enter the Device Management interface.

Device Managed (0)

+

Add Device

Edit

Delete

Bulk Time...

Status

Remote Co...

Attendance...

Refresh

Filter

Name	Type	Connection M...	IP	Port	Baud Rate	Dial-up	Connection St...	Refresh

Online Devices (1)

+

Add to Client

+

Add All Device

🔧

Edit Networkk...

↺

Reset P...

🔴

Activate

Filter

Name	Type	IP	Port	Activated	Added
44-19-b6-c5-cb-a6	Access Controller_DS-K1A801MF	192.0.0.64	8000	No	No

3. Select an inactive device from the device list.
4. Click **Activate** to pop up the Activation interface.



Activate Device [X]

Password:

The password (8 to 16 characters)
should contain two or more of the
following character types: numeric, low...

Confirm Pas...

OK Cancel

5. Create a password and confirm the new password.



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

6. Click **OK** to start activate.
7. Click  to configure the device IP address, mask address, gateway address, port No.
8. Input the password and click **OK** to apply.

Note: The device IP segment should be the same with the PC.

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

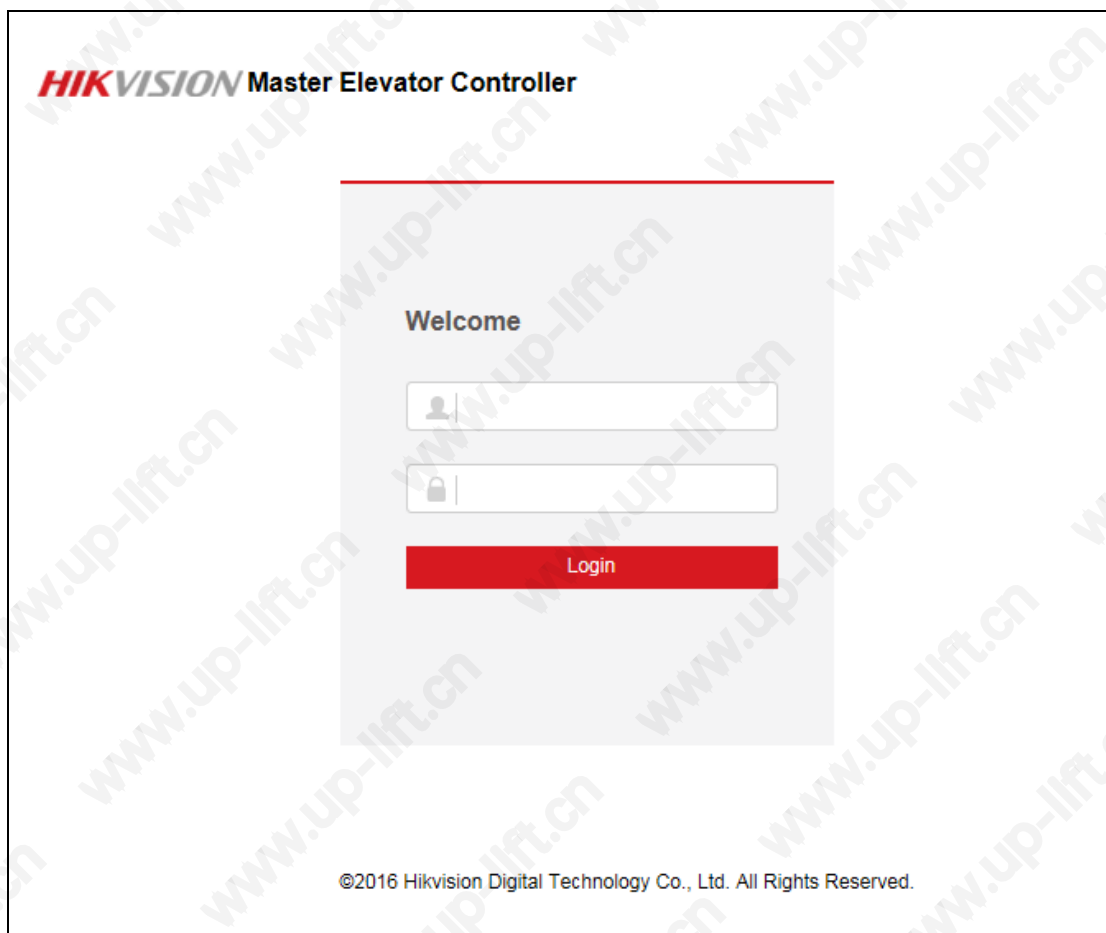
Before you start:

Make sure the device is activated. For details, refer to 5.1 Activating Device via Web Client.

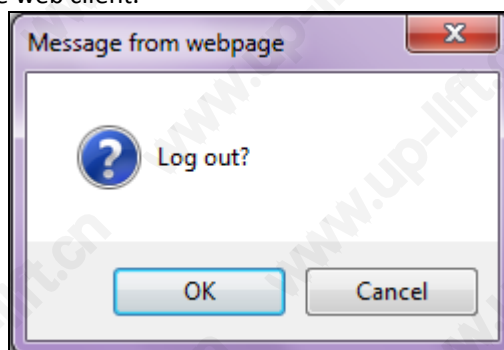
6.2.1 Login

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:

- Activate the device before logging in. For details, refer to 5.1 Activating Device via Web Client.
- 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 interface.
2. Click **Yes** in the pop-up dialog box to log out.

6.3 Setting Device via Web Client

6.3.3 System Settings

Managing Device Information

Steps:

1. Click **System Settings** → **Device Information** to enter the Device Information interface.

HIKVISION Master Elevator Controller admin | Logout

System Settings

- Device Information
- Controller Working Status

Network Settings

- TCP/IP Settings
- Port Settings

System Maintenance

- System Maintenance

Elevator Control Settings

- Remote Control
- Floor Parameters
- Add/Delete Card Permission

Device Information

Basic Information

Device Name	Access Controller
Model	DS-K2210
Number of Alarm Output	2
Case	5
Serial No.	123456788
Floor Number	0

Version Information

Software Version	V1.0.0 build 20161130
Hardware Version	V2.0
Device Language	EN

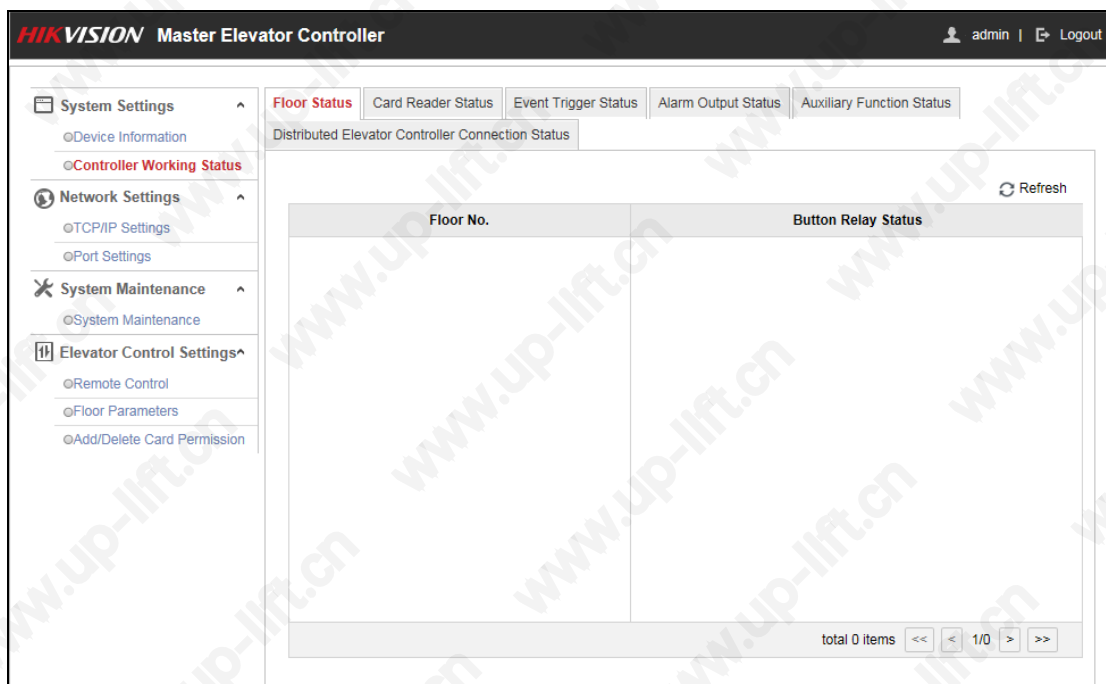
Save

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 interface.



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
	Master Controller Tamper-Proof
Distributed Elevator Controller Connection Status	Distributed Elevator Controller No.
	Status: Online, Offline

6.3.4 Network Settings

Setting TCP/IP

Steps:

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

HIKVISION Master Elevator Controller

admin | Logout

System Settings

- Device Information
- Controller Working Status

Network Settings

- TCP/IP Settings**
- Port Settings

System Maintenance

- System Maintenance

Elevator Control Settings

- Remote Control
- Floor Parameters
- Add/Delete Card Permission

TCP/IP Settings

Basic Settings

NIC Type: Auto

IPv4 Address: 10.15.5.192

Subnet Mask: 255.255.255.0

Default Gateway: 10.15.5.254

MAC Address: aa-bb-01-cc-02-dd

MTU: 1500

Advanced Settings

DNS Server Address 1:

DNS Server Address 2:

Save

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 interface.

HIKVISION Master Elevator Controller

admin | Logout

System Settings

- Device Information
- Controller Working Status

Network Settings

- TCP/IP Settings
- Port Settings**

System Maintenance

- System Maintenance

Elevator Control Settings

- Remote Control
- Floor Parameters
- Add/Delete Card Permission

Port Settings

Device Port No.: 8000

HTTP Port No.: 80

Save

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

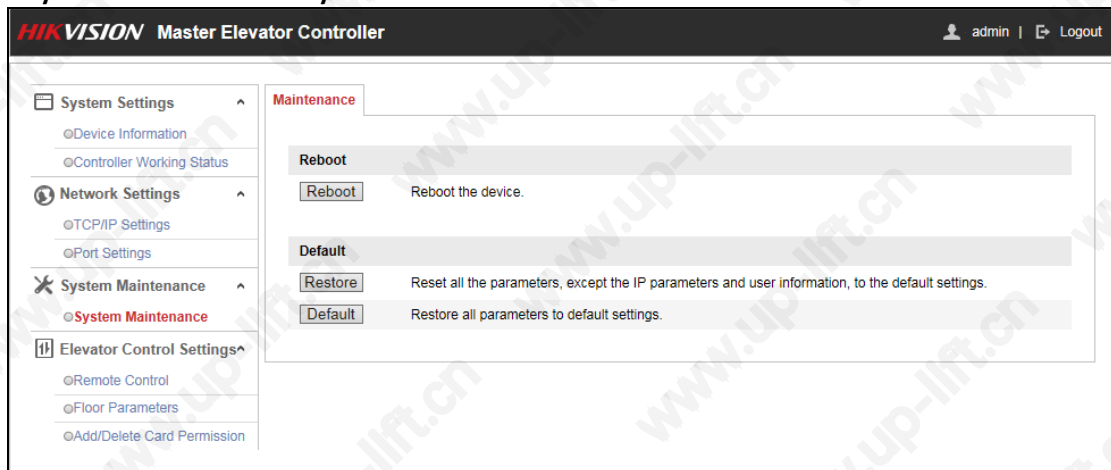
Notes:

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

6.3.5 System Maintenance

Steps:

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



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.

6.3.6 Elevator Control Settings

Setting Remote Control

Steps:

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



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 go 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

The time duration of the visitor using the elevator.

Time:

The default delay time is 5s.

Disabled Person:

The door can be open with appropriate delay after disabled person swipes the card.

First Card:

The default time duration is 15s.

Set the door open duration for the function of Open Door with First Card.

The default time duration is 10min.

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

Adding and Deleting Card Permission

Adding Card Permission

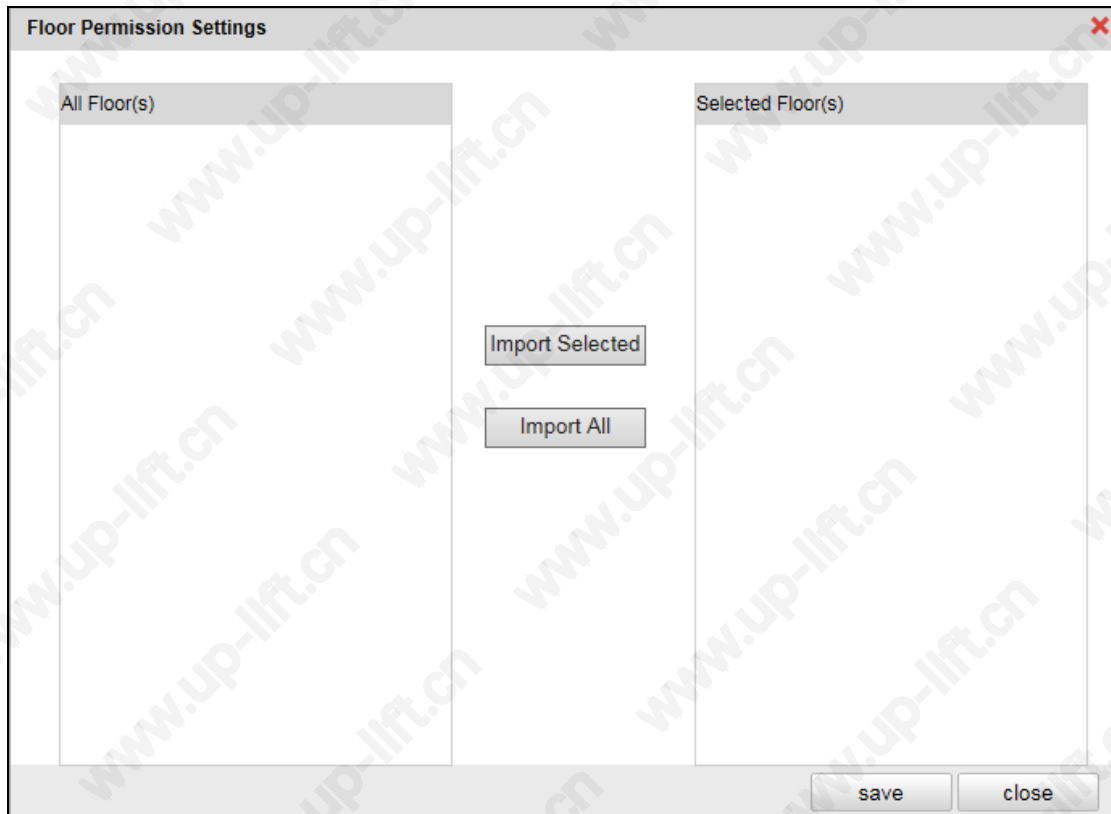
- Click **Elevator Settings -> Add/Delete Card Permission -> Adding Card Permission** to enter the Adding Card Permission interface.

- Input the card No.
Or check the **Auto Obtain** checkbox, and swipe the card on the external card reader to get the card No.
- Select a card type in the drop-down list.
You can select from normal card, card for disabled person, card in blacklist, 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 Disabled Person	The door will remain open for the configured time period for the card holder.
Card in Blacklist	The card swiping action will be uploaded and the floor button cannot be controlled.
Patrol Card	The card swiping action can be 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.

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

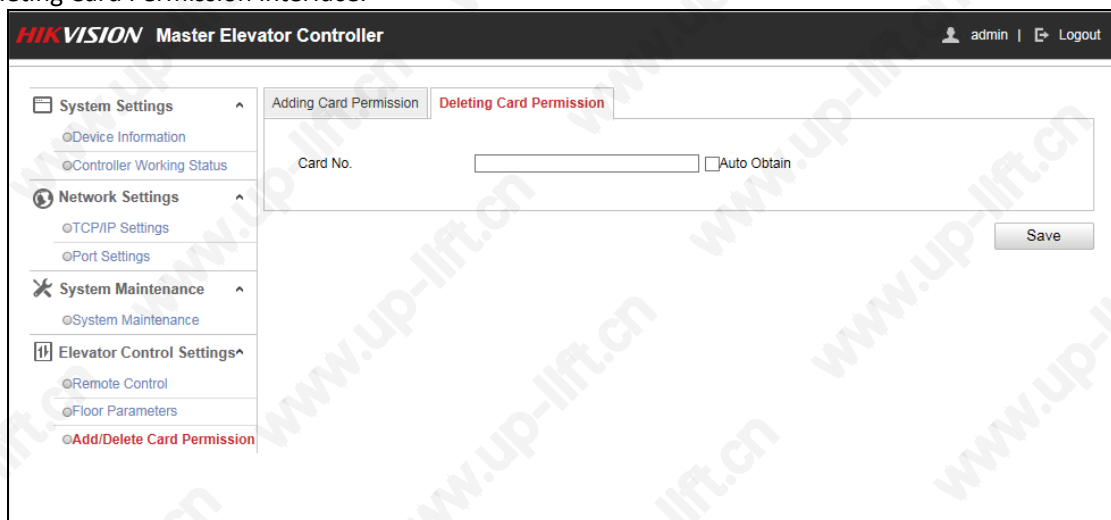


5. Check the floor checkbox(es) in the All Floor(s) list. And click **Import Selected Item** to import the selected floors to the Selected Floor(s) list.
6. Click **Save** to save the settings and the window will be automatically exited. The configured card will contain the selected floors permissions.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



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

7.1 Overview of iVMS-4200 Client Software

7.1.1 Description

The iVMS-4200 Access Control Client is a client-based access control system for management of access control devices. With intuitive and easy-to-use operations, it provides multiple functionalities, including access control device management, person/card management, permission configuration, door status management, attendance management, event search, etc.

This user manual describes the function, configuration and operation steps of iVMS-4200 Access Control Client. To ensure the properness of usage and stability of the client, please refer to the contents below and read the manual carefully before installation and operation.

7.1.2 Running Environment

Operating System: Microsoft Windows 7/Windows 2008 R2/Windows 8.1/Windows 10 (32-bit or 64-bit), Windows XP SP3 (32-bit)

CPU: Intel Pentium IV 3.0 GHz or above

Memory: 2G or above

Video Card: RADEON X700 Series or above

GPU: 256 MB or above

Notes:

- For high stability and good performance, these above system requirements must be met.
- The software does not support 64-bit operating system; the above mentioned 64-bit operating system refers to the system which supports 32-bit applications as well.

7.1.3 Client Performance

The client performance is shown as follows:


Client Performance	Quantity
User Account	Up to 16 user accounts (including super user) supported
Access Control Device	Up to 16 access control devices supported
Access Control Point	Up to 64 access control points (doors) supported
Person	Up to 2,000 persons supported
Card	Up to 2,000 cards supported
Department	Up to 10 levels of departments supported

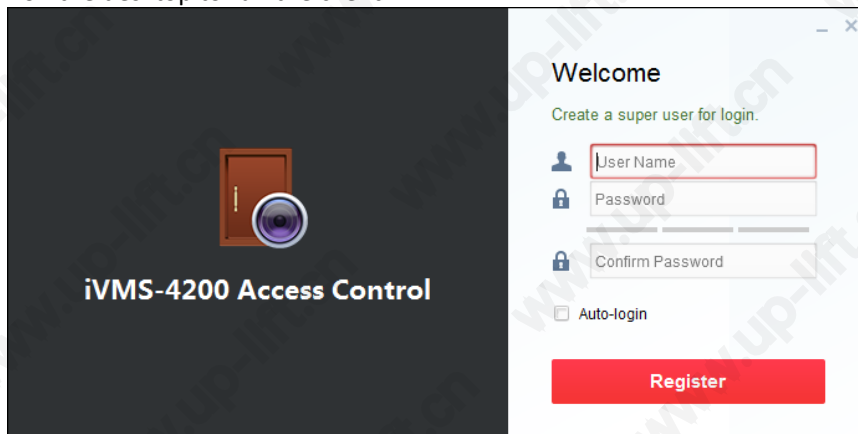
7.2 User Registration and Login

For the first time using the client software, you need to register a super user to login.

7.2.1 User Registration

Steps:

1. Double-click  on the desktop to run the client.



2. Input the super user name, password and confirm password in the pop-up window.
3. Optionally, check the checkbox **Auto-login** to log in to the software automatically.
4. Click **Register**. Then, you can log in to the software as the super user.



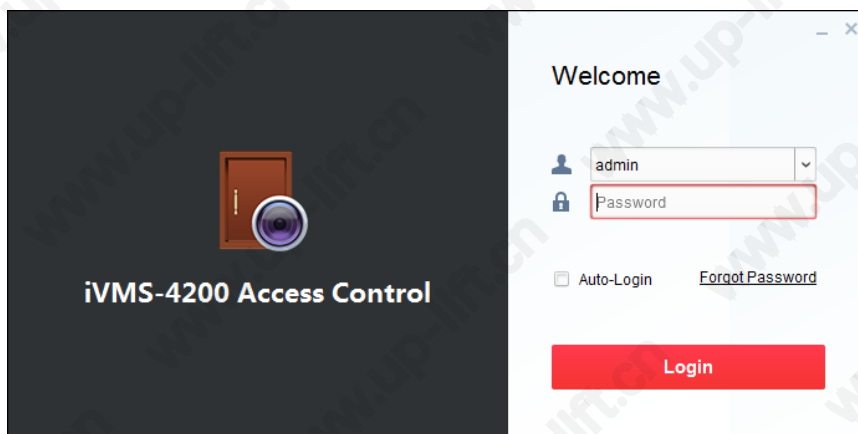
- ◆ A user name cannot contain any of the following characters: / \ : * ? " ' < > | . And the length of the password cannot be less than 8 characters.
- ◆ For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper 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 Access Control Client after registration, you can log in to the client software with the registered user name and password.

7.2.2 Login

Steps:

1. Input the user name and password you registered.



2. Optionally, check the checkbox **Auto-login** to log in to the software automatically.
3. Optionally, if you forget your password, please click **Forgot Password** and remember the encrypted string in the pop-up window. Contact your dealer and send the encrypted string to him to reset your password.
4. Click **Login**.

7.2.3 Function Modules

After login, the control panel of the Access Control Client is shown as follows:

Control Panel of iVMS-4200 Access Control Client:



Menu Bar:

File	Exit	Exit the iVMS-4200 Access Control Client.
System	Lock	Lock screen operations. Log in the client again to unlock.
	Switch User	Switch the login user.
	Import Parameters	Import client configuration file from your computer.
	Export Parameters	Export client configuration file to your computer.
	Auto Backup	Back up the database including person, attendance data, and permission data automatically.
View	Device Management	Open the Device Management page.
	Attendance Configuration	Open the Attendance Configuration page.
	Attendance Statistics	Open the Attendance Statistics page.
	Person Management	Open the Person Management page.
	Card Management	Open the Card Management page.
	Template	Open the Template page.
	Access Control Permission	Open the Access Control Permission page.
	Advanced Function	Open the Advanced Function page.
	Status Monitor	Open the Status Monitor page.
	Linkage Configuration	Open the Linkage Configuration page.
	Door Group Management	Open the Door Group Management page.
	Account Management	Open the Account Management page.
	Event Management	Open the Event Management page.
	Log Search	Open the Log Search page.
	Control Panel	Enter Control Panel interface.
Tools	Search Access Control Permission	Search the added access control permission.
	Card Reader	Configure the card reader parameters.
	Fingerprint Machine	Configure the fingerprint machine parameters.
	Storage Server	Configure the storage server parameters.
	System Configuration	Enter the System Configuration page.
	People Counting	Enter the People Counting page.
	Apply Parameters	Apply the settings on the client to the corresponding access control device.
	Arming Settings	Set the arming status of access control devices.
Help	User Manual (F1)	Click to open the User Manual; you can also open the User Manual by pressing F1 on your keyboard.
	Language	Select the language for the client software and reboot the software to activate the settings.
	About	View the basic information of the client software.

The iVMS-4200 Access Control Client is composed of the following function modules:



Device Management

The Device Management module provides adding, editing, and deleting of access controllers.














Person Management

The Person Management module provides adding, editing, and deleting of person and departments.



Card Management

The Card Management module provides adding, editing, and deleting the card information.

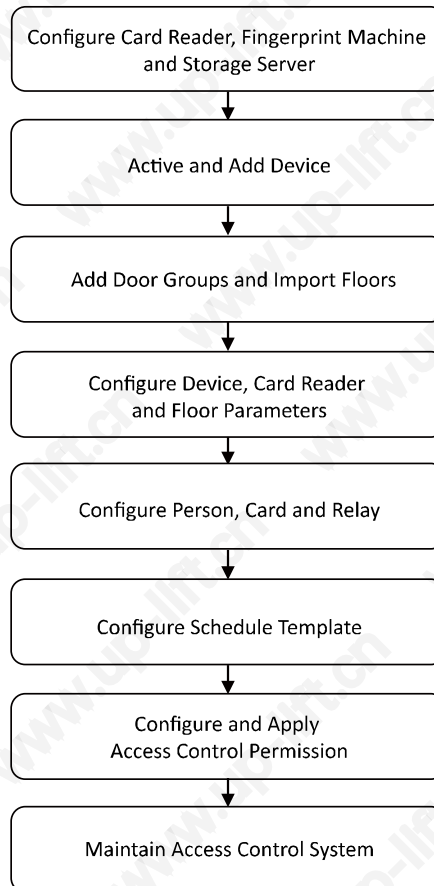
	Template		The Template module provides adding, deleting, and editing of duration, week plan, and holiday.
	Access Permission	Control	The Access Control Permission module provides adding, deleting, and applying the access control permissions.
	Advanced Function		The Advanced Function module provides configuration of advanced functions including access control type, anti-passing back, multiple interlocking, etc..
	Linkage Configuration		The Linkage Configuration module provides event alarm, event card, and client linkage configuration.
	Attendance Configuration		The Attendance Configuration module provides shift schedule settings including attendance rule, attendance check point, holiday schedule, etc.
	Attendance Statistics		The Attendance Statistics module provides calculating and analyzing the attendance results.
	Status Monitor		The Status Monitor module displays access control status and provides anti-control function.
	Door Management	Group	The Door Group Management module provides adding, editing, and deleting the access control group.
	Account Management		The Account Management module provides adding, editing, and deleting the user and assigning permission.
	Event Management		The Event Management module provides setting the search condition to search the access control event.
	Log Search		The Log Search module provides searching the configuration logs and control logs.

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

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

7.3 Basic Configuration

7.3.1 Work Flow



7.3.2 Card Reader Configuration

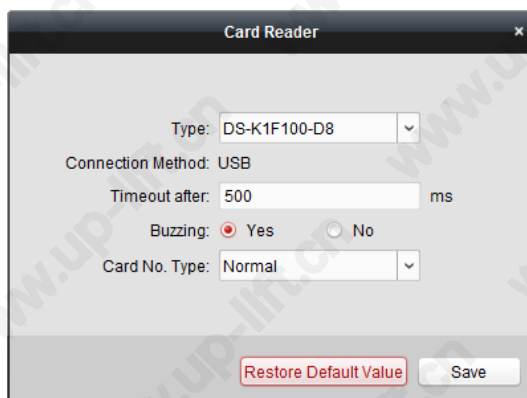
Purpose:

The Card Reader should connect with the PC running the client to read the card No.. You should configure the card reader before setting the card.

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

Steps:

1. Click **Tool->Card Reader** on the menu to pop up the card reader configuration dialog box.



2. Set the parameters about the connected card reader.
3. Click **Save** button to save the settings.
You can click **Restore Default Value** button to restore the defaults.

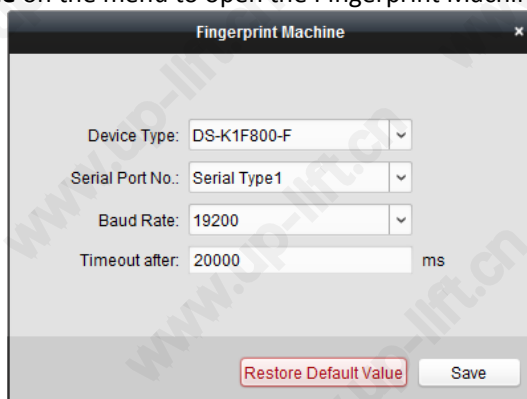
7.3.3 Fingerprint Machine Configuration

Purpose:

The fingerprint machine should connect with the PC to run the client for collecting the fingerprint.

Steps:

1. Click **Tool->Fingerprint Machine** on the menu to open the Fingerprint Machine Configuration page.



2. Select the device type.
Currently, the supported fingerprint machine types include DS-K1F800-F, DS-K1F300-F, and DS-K1F810-F.
3. For fingerprint machine type DS-K1F800-F, you can set the serial port number, baud rate, and overtime parameters of the fingerprint machine.
4. 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.
- The baud rate should be set according to the external fingerprint card reader. The default value is 19200.
- Overtime 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.

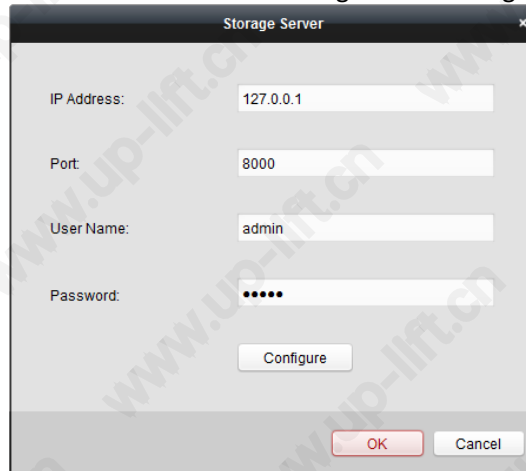
7.3.4 Storage Server Configuration

Purpose:

You should configure the storage server before capturing the pictures for the storage of captured pictures.

Steps:

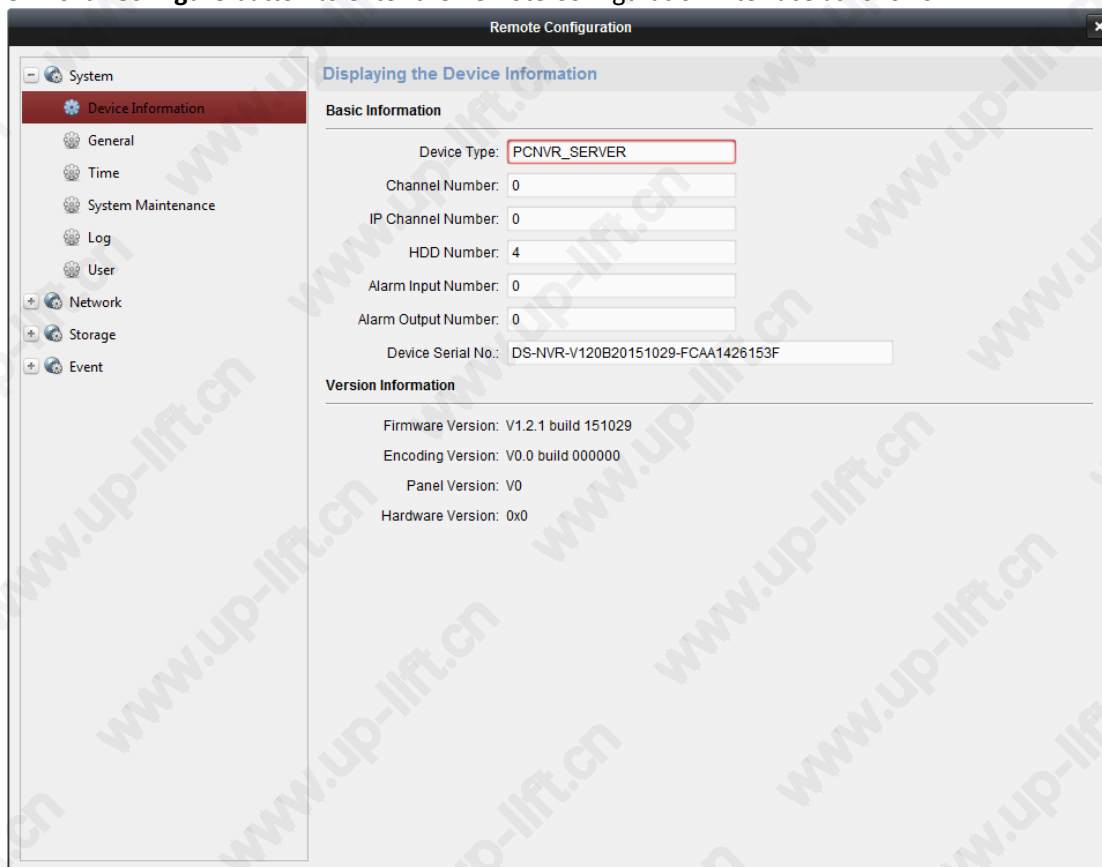
1. Click **Tool->Storage Server** on the menu to enter the storage server configuration interface.



The 'Storage Server' dialog box contains the following fields and buttons:

- IP Address: 127.0.0.1
- Port: 8000
- User Name: admin
- Password: (masked with dots)
- Buttons: Configure, OK, Cancel

2. Input the storage server parameters including IP address, port No., user name, and password.
3. Click **Configure** button to enter the Remote Configuration interface as follows.



The 'Remote Configuration' interface displays the following information:

- System** (selected in the left sidebar)
- Device Information** (selected in the left sidebar)
- Displaying the Device Information** (title)
- Basic Information**
 - Device Type: PCNVR_SERVER
 - Channel Number: 0
 - IP Channel Number: 0
 - HDD Number: 4
 - Alarm Input Number: 0
 - Alarm Output Number: 0
 - Device Serial No.: DS-NVR-V120B20151029-FCAA1426153F
- Version Information**
 - Firmware Version: V1.2.1 build 151029
 - Encoding Version: V0.0 build 000000
 - Panel Version: V0
 - Hardware Version: 0x0

4. Format the HDDs of the storage server for the video file and picture storage.
 - 1) Click **Storage->General**, to enter the HDD Formatting interface.
 - 2) Select the HDD from the list and click **Format**. You can check the formatting process from the process bar and the status of the formatted HDD changes from *Unformatted* to *Normal Status*.

Note: Formatting the HDDs is to pre-allocate the disk space for storage and the original data of the formatted HDDs will not be deleted.

Configuring the HDD Parameters

<input type="checkbox"/> HDD No.	Capacity(GB)	Free Space(GB)	Status	Type	HDD Group No.	Property
<input type="checkbox"/> D	180.00	153.45	Unformatted	Local	Group00	Read/Write
<input type="checkbox"/> E	185.75	185.65	Unformatted	Local	Group00	Read/Write
<input checked="" type="checkbox"/> P	50.00	36308.20	Unformatted	Local	Group00	Read/Write
<input type="checkbox"/> Z	3071.87	430.12	Unformatted	Local	Group00	Read/Write

Format Update

Progress:
0%

5. After formatting of the HDD, you can set the picture storage quota in the Remote Configuration interface.

Storage Mode: ▾

Total Capacity: 3487.62 GB

Quota Ratio For Record: %

Quota Ratio For Picture: %

Quota Ratio For Additiona... %

Save

Click **Save** to save the storage server remote configuration settings.

6. After formatting the HDD and setting the quota, click **OK** to save the settings.

7.4 Device Management

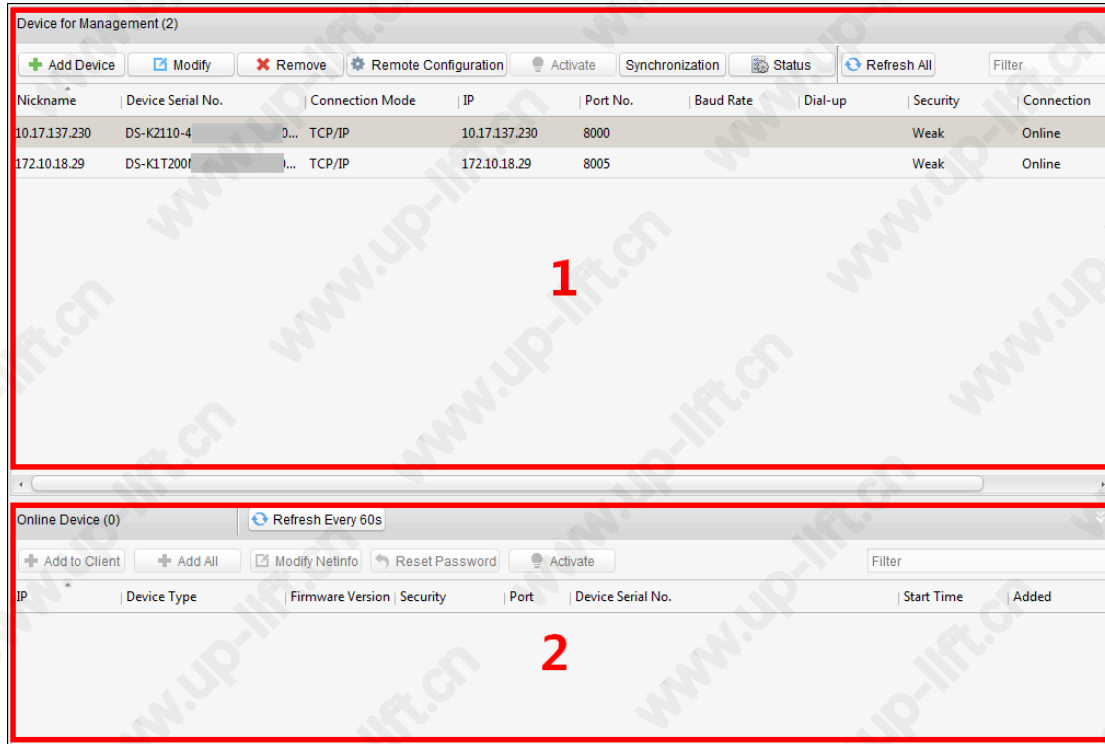
Purpose:

After running the iVMS-4200 Access Control Client, the access control device should be added to the client for the remote configuration and management.

7.4.1 Access Control Device Management



Click **Device Management** icon on the control panel to enter the access control device management interface.



The interface is divided into two parts: Device Management area and Online Device Detection area.

- **Device Management**

Manage the access control devices, including adding, editing, deleting, and batch time synchronizing functions.

- **Online Device Detection**

Automatically detect online devices in the same subnet with the client, and the detected devices can be added to the client in an easy way.

Note: The client can manage up to 16 access control devices and 64 access control points.

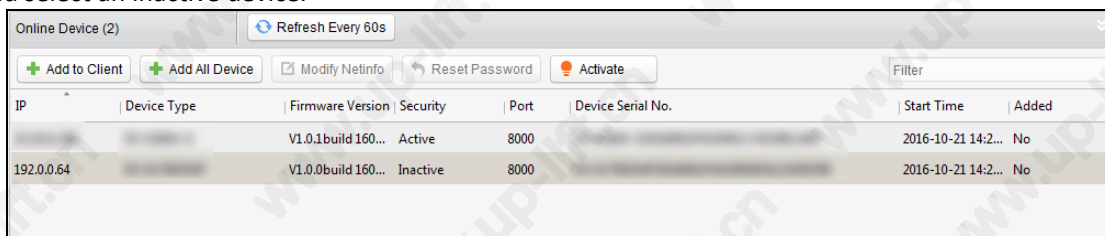
Activating Device and Creating Password

Purpose:

If the access control device is not activated, you are required to create the password to activate them before they can be added to the software and work properly.

Steps:

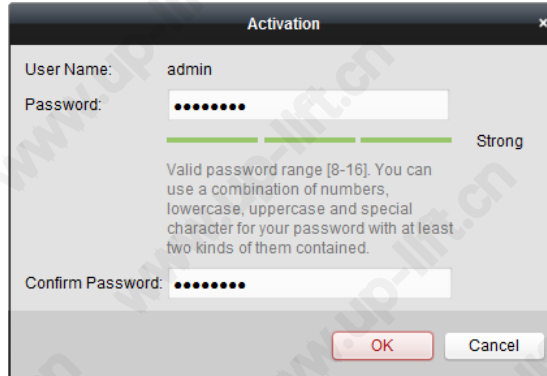
1. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.



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



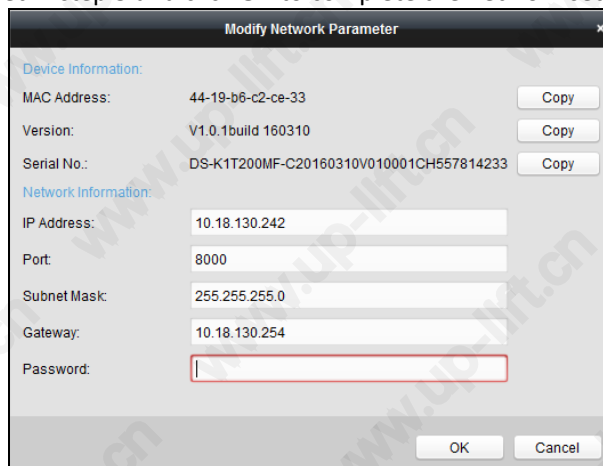
STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password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



The 'Activation' dialog box contains the following fields and text:

- User Name:** admin
- Password:** A text field with 8 dots, followed by a green progress bar and the label 'Strong'.
- Confirm Password:** A text field with 8 dots.
- Text below password fields:** Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.
- Buttons:** OK and Cancel.

4. Click **OK** to create the password for the device. A "The device is activated." window pops up when the password is set successfully.
 5. Edit the device's network parameters:
 - 1) 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.
- 2) Input the password set in step 3 and click **OK** to complete the network settings.



The 'Modify Network Parameter' dialog box contains the following sections and fields:

- Device Information:**
 - MAC Address:** 44-19-b6-c2-ce-33 (Copy button)
 - Version:** V1.0.1build 160310 (Copy button)
 - Serial No.:** DS-K1T200MF-C20160310V010001CH557814233 (Copy button)
- Network Information:**
 - IP Address:** 10.18.130.242
 - Port:** 8000
 - Subnet Mask:** 255.255.255.0
 - Gateway:** 10.18.130.254
 - Password:** A text field with a red border.
- Buttons:** OK and Cancel.

- 3) Click **OK** to save the settings.

Adding Online Devices

Purpose:

The active online access control devices in the same local subnet with the client 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.

Online Device (2)

Refresh Every 60s

+ Add to Client

+ Add All Device

Modify NetInfo

Reset Password

Activate

Filter

IP	Device Type	Firmware Version	Security	Port	Device Serial No.	Start Time	Added
		V1.0.1build 160...	Active	8000		2016-10-21 14:4...	No
192.0.0.64		V1.0.0build 160...	Inactive	8000		2016-10-21 14:2...	No

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 3.1.1 *Activating Device and Creating Password*.

2. Click **Add to Client** to open the device adding dialog box.



The 'Add Device' dialog box contains the following fields and controls:

- Nickname:** A text input field with a red border.
- Connection Method:** A dropdown menu currently set to 'TCP/IP'.
- IP Address:** A text input field containing '10.16.6.151'.
- Port:** A text input field containing '8000'.
- User Name:** A text input field.
- Password:** A text input field.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.

3. Input the required information.

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

Connection Type: Select TCP/IP as the connection type.

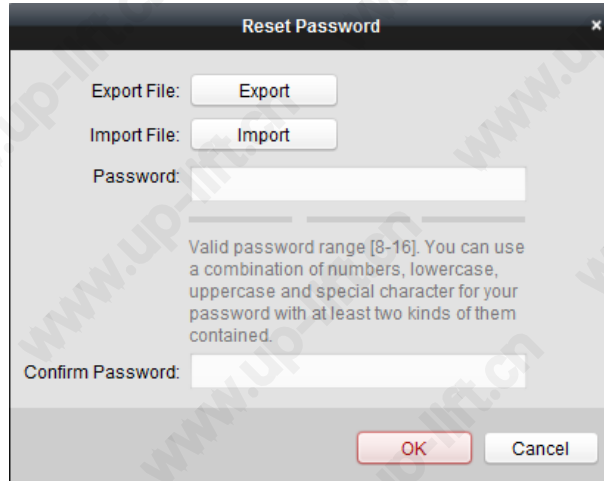
IP Address: Input the device's IP address. The IP address of the device is obtained automatically in this adding mode.

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.

4. Click **Add** to add the device to the client.
5. (Optional) Click and hold *Ctrl* key to select multiple devices. You can
 - 1) Click **Add to Client** to open the device adding dialog box.
 - 2) In the pop-up message box, enter the user name and password for the devices to be added.
6. (Optional) Add all online devices to the client software. You can
 - 1) Click **Add All**
 - 2) Click **OK** in the pop-up message box.
 - 3) Enter the user name and password for the devices to be added.
7. You can select the device from the list and click **Reset Password** to reset the device password.



Reset Password

Export File:

Import File:

Password:

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm Password:

Perform the following steps to reset the device password.

- 1) Click **Export** to save the device file on your PC.
- 2) Send the file to our technical engineers.
- 3) Our technical engineer will send you a file or an eight-digit number to you.
 - If you receive a file from the technical engineer, select **Import File** from Key Importing Mode drop-down list and click to import the file.
 - If you receive an eight-digit number from the technical engineer, select **Input Key** from Key Importing Mode drop-down list and input the number.
- 4) Input new password in text fields of **Password** and **Confirm Password**.
- 5) Click **OK** to reset the password.



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

Adding Access Control Device Manually

Steps:

1. Click **Add Device** on the Device for Management panel to enter the Add Device interface.



Add Device

Nickname:

Connection Method:

IP Address:

Port:

User Name:

Password:

2. Input the device name.
3. Select the connection type in the dropdown list: TCP/IP, COM port (1 to 5), or EHome protocol.

TCP/IP: Connect the device via the network.

COM1 to COM5: Connect the device via the COM port.

EHome: Connect the device via EHome Protocol.

Note: For connection type of EHome protocol, please set the network center parameter first. For details, refer to 3.2.2 Network Center Settings.

- Set the parameters of connecting the device.

If you select the connection type as TCP/IP, you should input the device **IP Address**, **Port No.**, **User Name**, and **Password**.

If you select the connection type as COM port, you should input the **Baud Rate** and **Dial-up** value.

If you select the connection type as EHome, you should input the **Account**.

- Click **Add** button to finish adding.

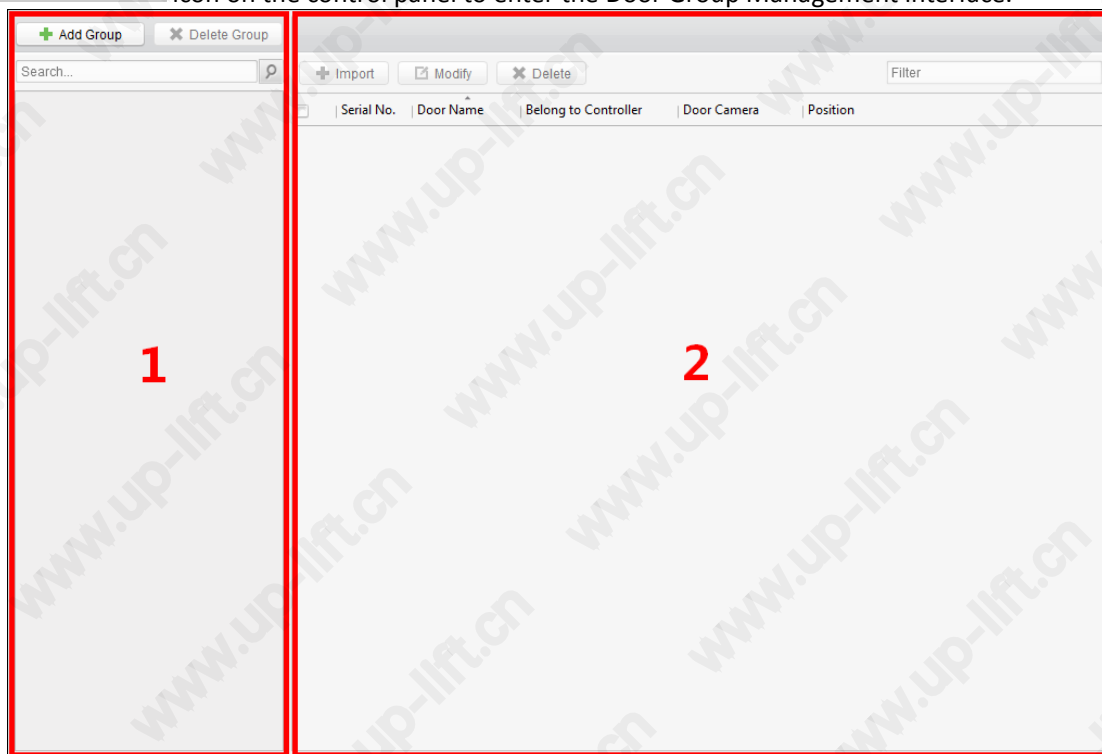
7.4.2 Door Group Management

Purpose:

After adding the access control device, you can add the access control points (floor) to different groups to realize the centralized management.



Click **Door Group Management** icon on the control panel to enter the Door Group Management interface.



The interface is divided into two parts: Group Management area and Access Control Point Management area.

1. Group Management

The access control points can be added to different groups to realize the centralized management.

2. Access Control Point Management

Manage the specific access control point (door) under the group, including importing, editing and deleting access control point.

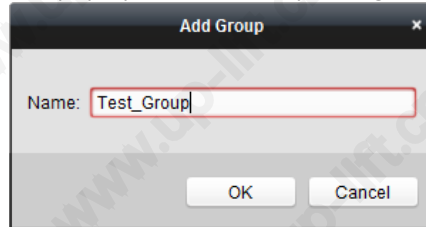
Access Control Group Management

Adding Group

Before you can manage the doors, you need to create groups first.


Steps:

1. Click **Add Group** button on the left to pop up the Add Group dialog.



2. Input the group name in the text field and click **OK** button to finish adding.

Editing Group

After adding the group, you can move the mouse to the group name and click  to pop up the Edit Group dialog box.

Or you can double click the group to edit the group name.

Deleting Group

You can move the mouse to the group name and click  to delete the selected group.

Or you can click to select the group and click **Delete Group** to delete it.

Note: All the access control points in the group will be deleted.

Access Control Point (Floor) Management

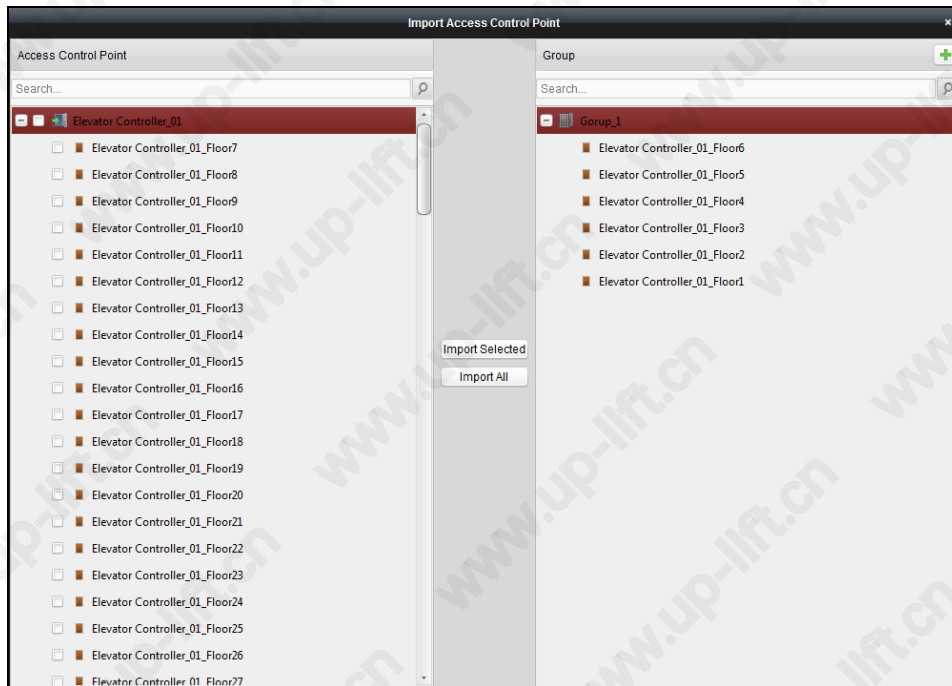
Purpose:

After adding the group, you can import the access control point of the added access control device to the group.

Importing Access Control Point (Floor)

Steps:

1. Select the added group, and click **Import Selected** button to pop up Import Access Control Point (Floor).



2. Select the floors to import from the access control point (floor) list on the left.
3. Select an added group to import the access control point (floor) on the right.
4. Click **Import Selected** button to import the selected access control points (floors) or you can click **Import All** to import all the available access control points (floors) to the selected group.
5. (Optional) You can click button on the upper-right corner of the window to create a new group. Move the mouse to the added group or access control point and click or to edit or delete it.

Note: Up to 64 access control points (floors) can be imported to the door group.

Editing Access Control Point (Floor)

Steps:

1. Check the checkbox to select the imported access control point in the list and click **Edit** button to edit the access control point.
2. You can edit the access control point name and the position.
3. You can view the card reader under the selected access control point.
4. Click **OK** to save the settings.

Deleting Access Control Point (Floor)

Check the checkbox to select the imported access control point and click **Delete** button to delete the selected access control point.

7.4.3 Editing Access Control Device

Purpose:

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

Click to select the added access control device from the list, and then click **Modify** button to enter the Edit Access Controller interface.

Notes:

- After editing the device, you can click **Apply Parameters** to apply the configured parameters to the device to take effect.
- You can also click **Read Parameters** to get the device parameters from the device itself.

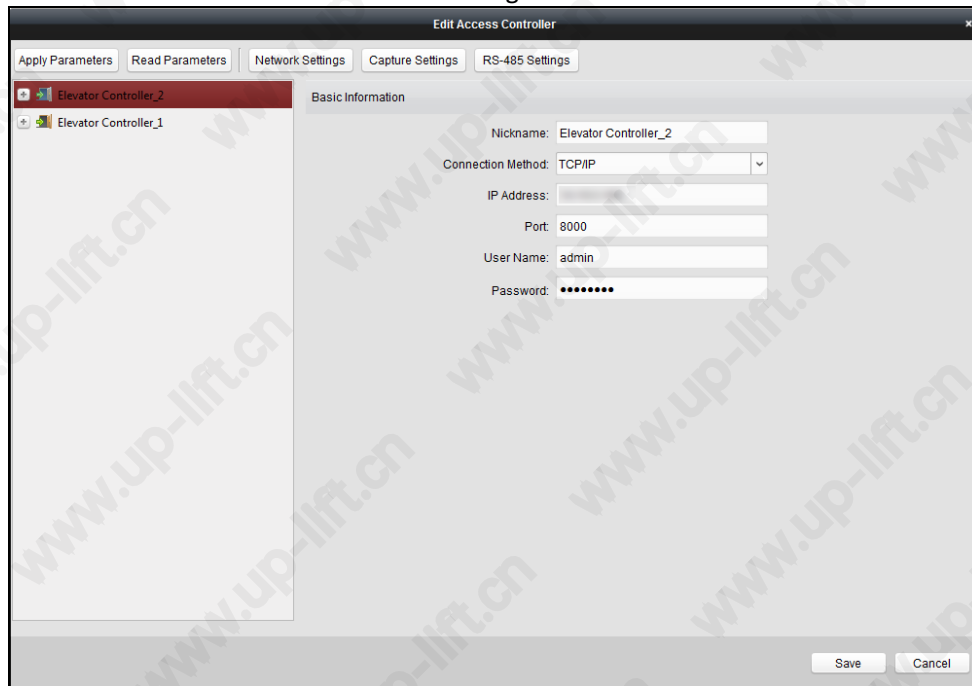
Editing Basic Information

Purpose:

You can configure the device basic information including IP address, port No., etc.

Steps:


1. In the device list on the left, select the access control device and you can edit its basic parameters on your demand, which are the same as the ones when adding the device.

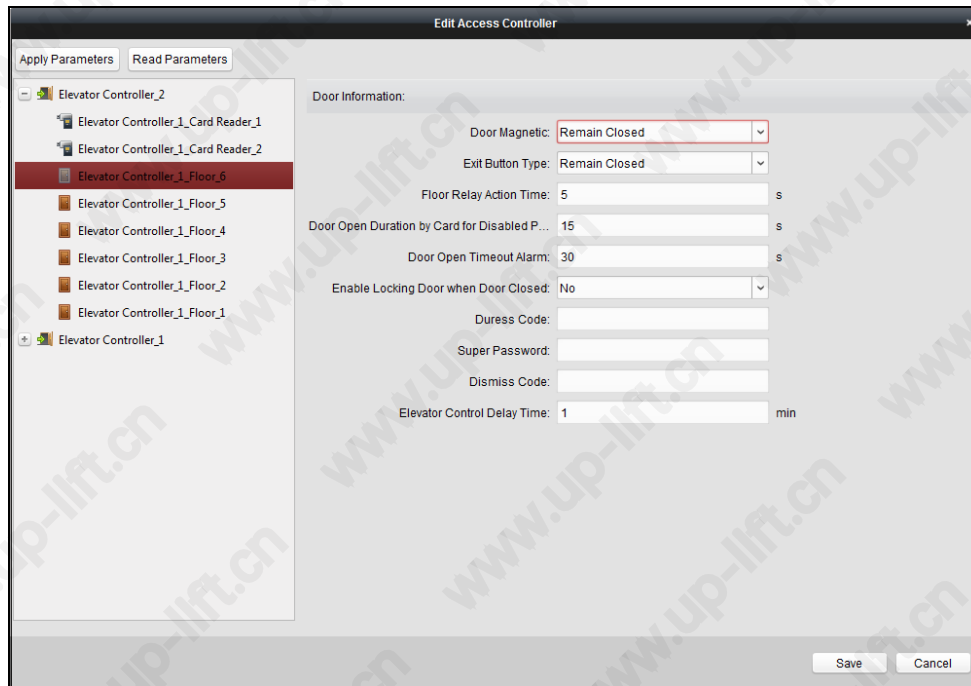


2. Click **Save** button to save the settings.
3. You can click **Apply Parameters** button to apply the updated parameters to the local memory of the device.

Editing Door (Floor) Information

Steps:

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



2. You can edit the following parameters:

Door Magnetic:

The Door Magnetic is in the status of **Normal 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:

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.

Door Open Duration by Card for Disabled Person:

The door magnetic can be enabled with appropriate delay after disabled person swipes the card.

Door Open Timeout Alarm:

The alarm can be triggered if the door is not closed.

Note: If the Door Open Timeout Alarm value is 0, the alarm is not enabled.

Enable Locking Door when Door Closed (Do Not Support by Elevator Control Device):

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.

Note: The Duress Code, Super Code, and Dismiss Code should be different.

Elevator Control Delay Time:

The time duration of the visitor using the elevator.

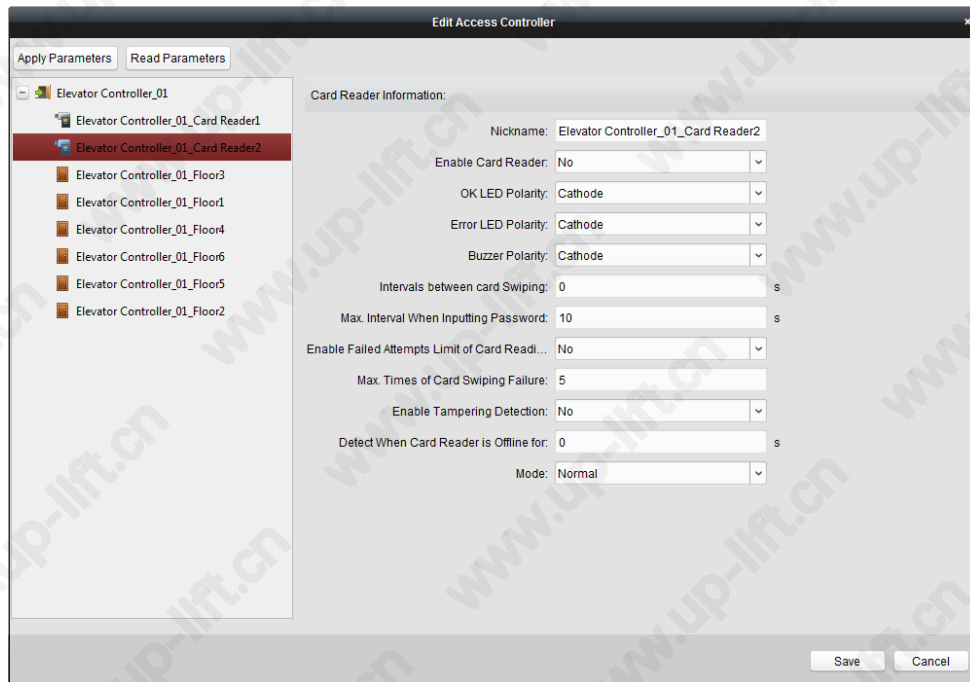
3. Click **Save** button to save the parameters.

4. Click **Apply Parameters** button to apply the updated parameters to the local memory of the device.

Editing Card Reader Information

Steps:

1. In the device list, select a card reader. You can edit the card reader information on the right.



2. Edit the following parameters:

Nickname:	Edit the card reader name.
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.
Interval between Card Swiping:	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.
Mode:	Select the card reader mode as normal mode (reading card) or issuing card mode (getting the card No.).
	Normal: Normal card reading mode.
	Card Issuing: Swipe the card on the card enrollment station to read the card No. The system will fill the card No. to the place that needs it.

3. Click the **Save** button to save parameters.

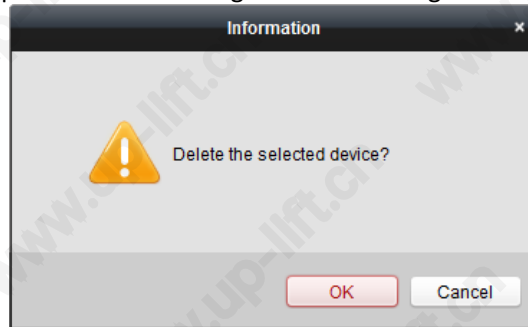
4. Click **Apply Parameters** button to apply the updated parameters to the local memory of the device.

7.4.4 Deleting Device

Steps:

1. In the device list, click to select a single device, or select multiple devices by pressing **Ctrl** button on your keyboard and clicking them one by one.

- Click **Remove** button to delete the selected device(s).
- Click **OK** button in the pop-up confirmation dialog to finish deleting.



7.4.5 Time Synchronization

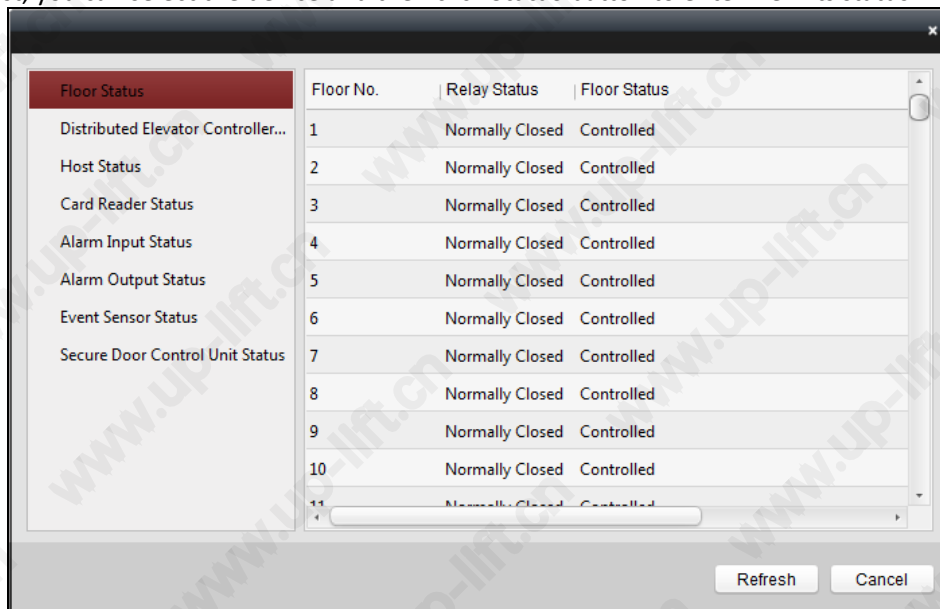
Steps:

- In the device list, click to select a single device, or select multiple devices by pressing *Ctrl* button on your keyboard and clicking them one by one.
- Click **Synchronization** button to start time synchronization.
A message box will pop up on the lower-right corner of the screen when the time synchronization is completed.

7.4.6 Viewing Device Status

Purpose:

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



Floor Status:

The floor relay status and the floor status.

Distributed Elevator Controller Status:

The distributed elevator controller status and its tamper-proof status.

Host Status:

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

Card Reader Status:	The status of card reader.
Alarm Input Status:	The alarm input status of each port.
Alarm Output Status:	The alarm output status of each port.
Event Sensor Status:	The event status of each port.
Secure Door Control Unit Status:	The online status and tamper status of the Secure Door Control Unit.

7.4.7 Remote Configuration

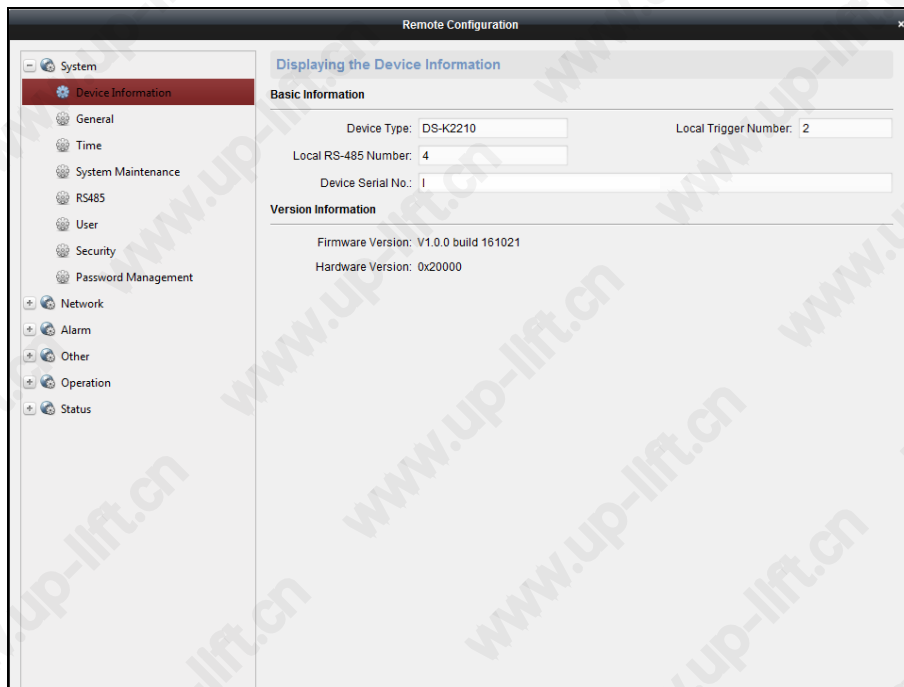
Purpose:

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




Editing Time

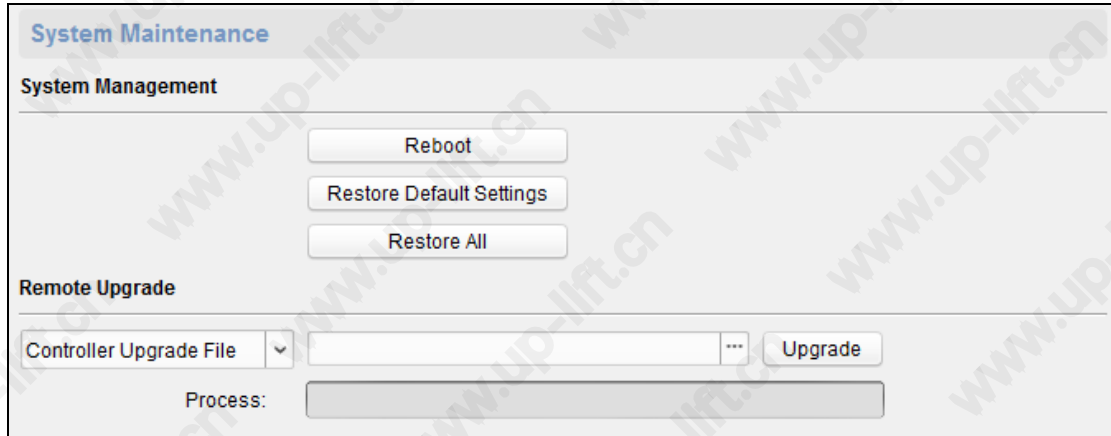
Steps:

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 start time, end time and the bias.
4. Click **Save** to save the settings.

System Maintenance Settings

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.
3. In the Remote Upgrade part, select a upgrade file type in the dropdown list. Click  to select the upgrade file. Click **Upgrade** to start upgrading.
You are able to select Controller Upgrade File, Card Reader Upgrade File and Distributed Controller Upgrade File in the drop-down list.

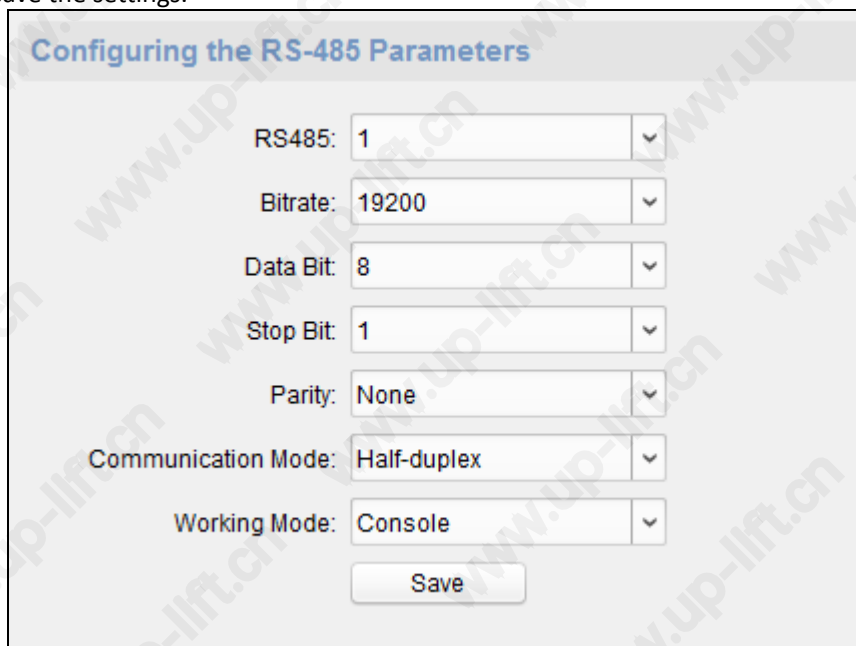


The screenshot shows a web interface titled "System Maintenance". Under the "System Management" section, there are three buttons: "Reboot", "Restore Default Settings", and "Restore All". Below this is the "Remote Upgrade" section, which includes a "Controller Upgrade File" dropdown menu, a file selection button (three dots), an "Upgrade" button, and a "Process:" progress bar.

Configuring RS-485 Parameters

Steps:

1. In the Remote Configuration interface, click **System** -> **RS485**.
2. Configure the RS-485 parameters, including the RS-485, the bitrate, the data bit, the stop bit, the parity, the communication mode and the working mode.
3. Click **Save** to save the settings.



The screenshot shows a web interface titled "Configuring the RS-485 Parameters". It contains several dropdown menus for configuration: "RS485" (set to 1), "Birate" (set to 19200), "Data Bit" (set to 8), "Stop Bit" (set to 1), "Parity" (set to None), "Communication Mode" (set to Half-duplex), and "Working Mode" (set to Console). A "Save" button is located at the bottom.

Managing User

Steps:

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

Adding, Editing or Deleting the User

User Name	Priority	IP Address	MAC Address	Password Security
admin	Administrator	0.0.0.0	00:00:00:00:00:00	Risky

- 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. Click **OK** to confirm editing.

User Parameter

User Information

User Type: Administrator
 User Name: admin
 Password: Confirm Password:
 IP Address: 0.0.0.0 MAC Address: 00:00:00:00:00:00

User Prission

- ☒ Remote Operation: Alarm Disarming
- ☒ Arm
- ☒ Remote Log Search/Status
- ☒ Remote Shutdown / Reboot
- ☒ Remote Parameter Settings
- ☒ Get Parameters
- ☒ Restore Default Settings
- ☒ Remote Upgrade

OK Cancel

Setting Security

Steps:

- Click **System** -> **Security**.
- Select the encryption mode in the dropdown list. You are able to select Compatible Mode or Encryption Mode.
- (Optional) You can check **Enable Telnet** in the Software part.
- Click **Save** to save the settings.

Configuring Network Parameters

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

Configuring the Network Parameters

NIC Type: 10M/100M/1000M Self... ▾

IPv4 Address: 10.15.5.192

Subnet Mask (IPv4): 255.255.255.0

Default Gateway (IPv4): 10.15.5.254

MAC Address: aa:bb:01:cc:02:dd

MTU(Byte): 1500

Device Port: 8000

HTTP Port: 80

Save

Configuring Advanced Network

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

Configuring the Advanced Network Settings

DNS Server Address1: 0.0.0.0

DNS Server Address2: 0.0.0.0

Alarm Host IP: 0.0.0.0

Alarm Host Port: 0

Save


Configuring Trigger Parameters

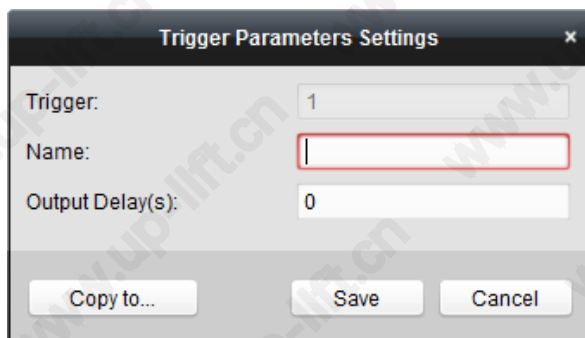
Steps:

1. Click **Alarm** -> **Trigger**. You can check the trigger parameters.

Configuring the Trigger Parameters

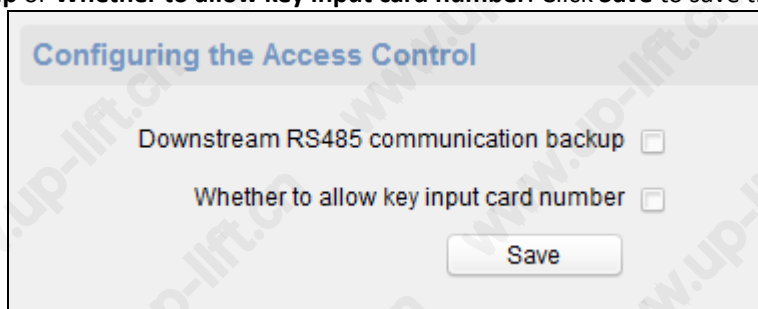
Trigger	Name	Output Delay(s)	Settings
1		0	
2		0	

2. Click the icon  to enter the Trigger Parameters Settings window. You can configure the trigger name and the output delay.
3. Click **Save** to save the parameters.
4. (Optional) Click **Copy to...** to copy the trigger information to other triggers.




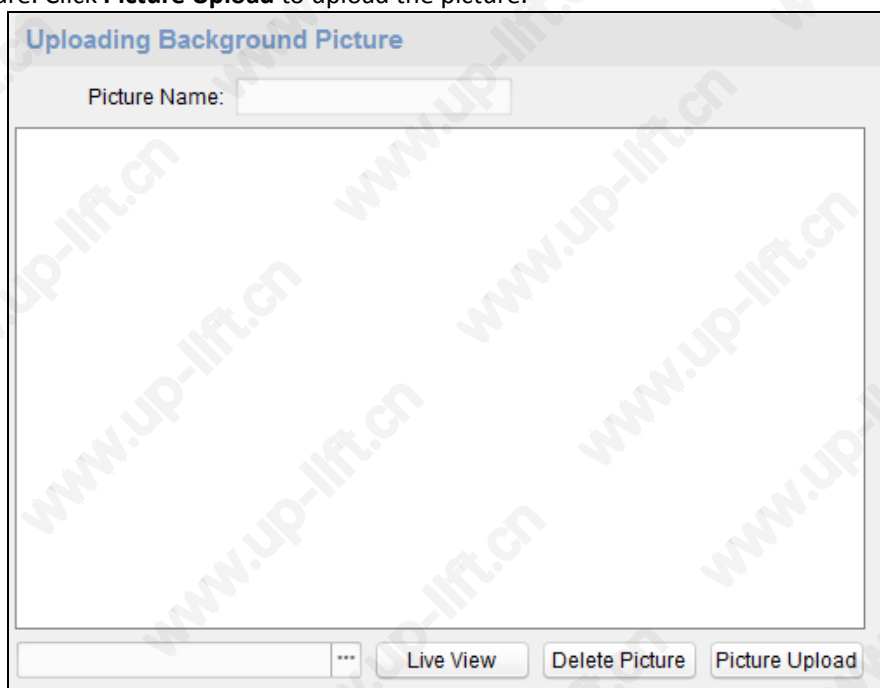
Configuring Access Control

In the Remote Configuration interface, click **Other** -> **Access Control Parameters**. Check **Downstream RS485 communication backup** or **Whether to allow key input card number**. Click **Save** to save the settings.



Uploading Backgroup Picture

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



Operating Trigger

Steps:

1. Click **Operation** -> **Trigger**. You can check the trigger status.

2. Check the trigger and click **Open** or **Close** to open/close the trigger.

Trigger Operation		
<input type="button" value="Open"/> <input type="button" value="Close"/>		
<input type="checkbox"/> Trigger No.	Name	Status
<input type="checkbox"/> 1		Close
<input type="checkbox"/> 2		Close

Checking Status

Click **Status** -> **Alarm** or **Status** -> **Trigger** to check the trigger status.

Trigger Status	
Trigger	Status
Trigger1	Close
Trigger2	Close

7.4.8 Network Settings (Do Not Support by Elevator Control Device)

Purpose:

In the Edit Access Controller interface, select the access control device and click **Network Settings** button to enter the Network Settings interface. You can set the uploading mode, and set the network center and wireless communication center.

Uploading Mode Settings

Steps:

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

The screenshot shows a window titled "Network Settings" with three tabs: "Uploading Mode Settings" (selected), "Network Center Settings", and "Wireless Communication Center Settings". The "Uploading Mode Settings" tab contains the following fields:

- Center Group: A dropdown menu with "Center Group1" selected.
- ☐ Enable
- Report Type: A dropdown menu.
- Uploading Mode Settings:
 - Main Channel: A dropdown menu with "Close" selected.
 - Backup Channel: A dropdown menu with "Close" selected.
- A "Save" button at the bottom right.

2. Select the center group in the dropdown list.
3. Check the **Enable** checkbox to enable the selected center group.
4. Select the report type in the dropdown list.

5. Select the uploading mode in the dropdown list. You can enable N1/G1 for the main channel and the backup channel, or select off 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.
6. Click **Save** button to save parameters.

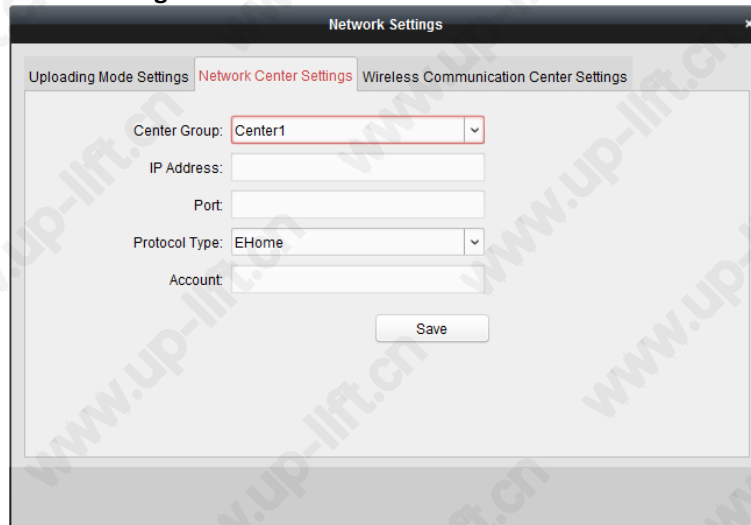
Network Center Settings

Purpose:

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

Steps:

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



The screenshot shows a 'Network Settings' dialog box with three tabs: 'Uploading Mode Settings', 'Network Center Settings' (selected), and 'Wireless Communication Center Settings'. The 'Network Center Settings' tab contains the following fields: 'Center Group' (a dropdown menu with 'Center1' selected), 'IP Address' (a text input field), 'Port' (a text input field), 'Protocol Type' (a dropdown menu with 'EHome' selected), and 'Account' (a text input field). A 'Save' button is located at the bottom right of the form area.

2. Select the center group in the dropdown list.
3. Input IP address and port No.
4. Select the protocol type as EHome.
5. Set an account name for the network center.

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

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

Note: The port number of the wireless network and wired network should be consistent with the port number of EHome.

Wireless Communication Center Settings

Steps:

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

The screenshot shows a 'Network Settings' window with three tabs: 'Uploading Mode Settings', 'Network Center Settings', and 'Wireless Communication Center Settings'. The 'Wireless Communication Center Settings' tab is active. It contains the following fields:

- APN Name: A dropdown menu.
- SIM Card No.: A text input field.
- Center Group: A dropdown menu with 'Center1' selected.
- IP Address: A text input field.
- Port: A text input field.
- Protocol Type: A dropdown menu with 'EHome' selected.
- Account: A text input field.

A 'Save' button is located at the bottom right of the form.

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.
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 number of the wireless network and wired network should be consistent with the port number of EHome.

7.4.9 Capture Settings (Do Not Support by Elevator Control Device)

Purpose:

In the Edit Access Controller interface, select the access control device and click **Capture Settings** button to enter the capture settings interface. You can set the parameters of capture linkage and manual capture.

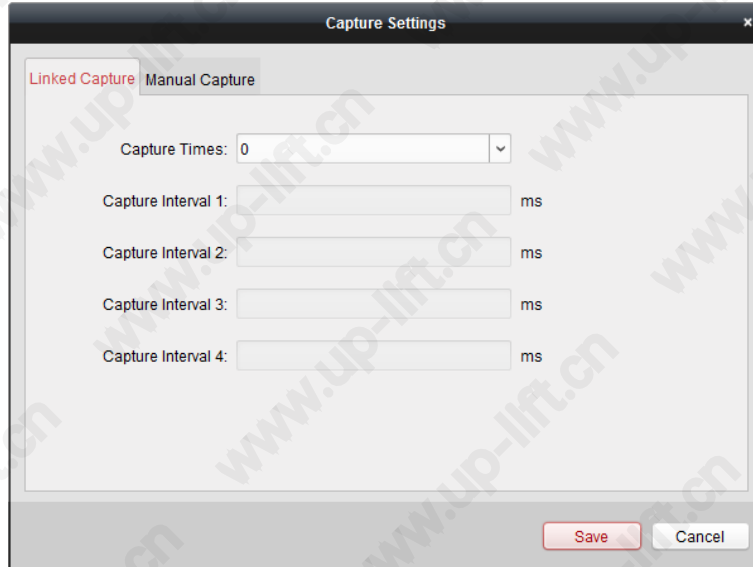
Notes:

- The **Capture Settings** should be supported by the device.
- Before setting the capture setting, you should configure the storage server for picture storage. For details, refer to *Section 7.3.4 Storage Server Configuration*.

Linked Capture

Steps:

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

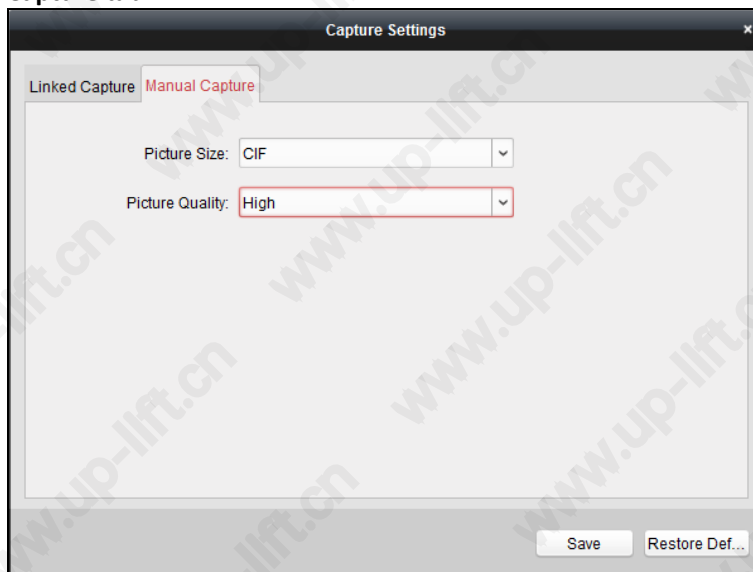


2. Set the linked capture times once triggered.
Set the capture interval according to the capture times.
3. Click **Save** to save the settings.

Manual Capture

Steps:

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



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

7.4.10 RS-485 Settings (Do Not Support by Elevator Control Device)

Purpose:

You can set the RS-485 parameters including the serial port No., the baud rate, the data bit, the stop bit, the parity type, the communication mode, and work mode.

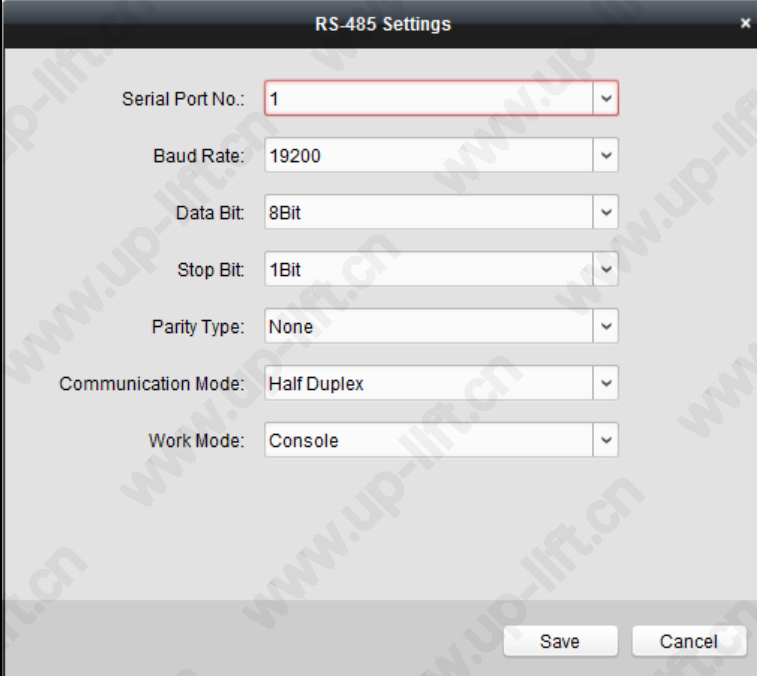
Note: The RS-485 Settings should be supported by the device.

Steps:

1. In the Edit Access Controller interface, select the access control device and click the **RS-485 Settings** button to enter the RS-485 Settings interface.

Note: The **RS-485 Settings** button is available when the device supports RS-485 port.

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

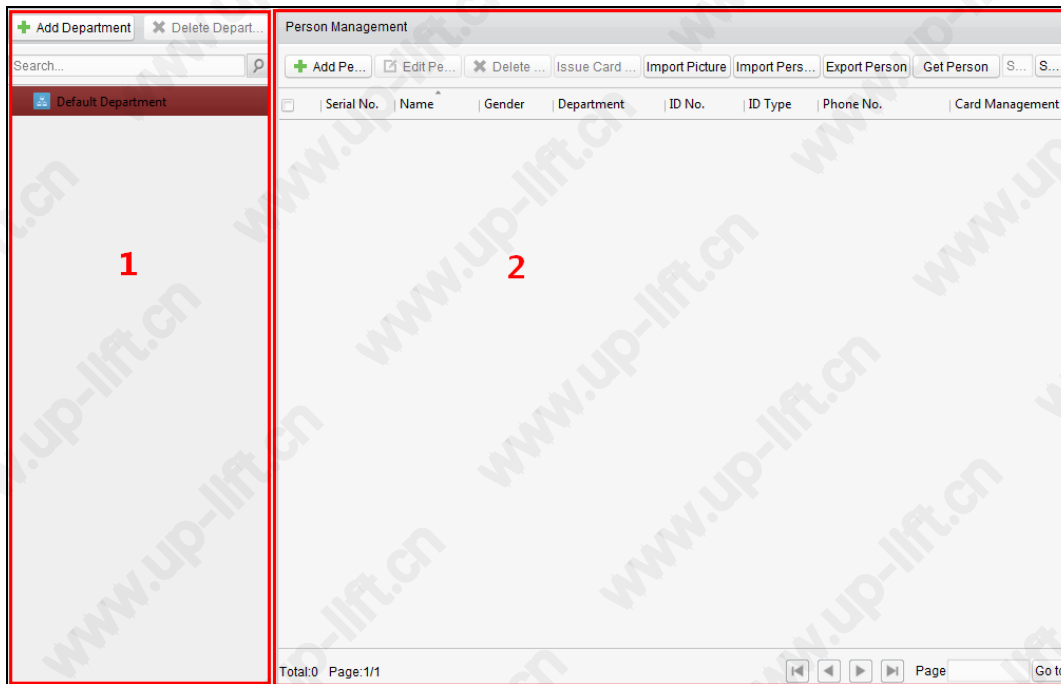


7.5 Person Management



Click [Person Management](#) icon on the control panel to enter the Person Management interface.

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



The interface is

divided into two parts: Department Management and Person Management.

1. Department Management

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

2. Person Management

After adding the department, you can add the person to the department for further management.

7.5.1 Department Management

Adding Department

Steps:

1. In the department list on the left, the Default Department already exists in the client as the parent department of all departments.
2. Select the upper department and click **Add Department** button to pop up the adding department interface to add the lower department.

3. Input the Department Name as desired.
4. Click **OK** to save the adding.

Notes:

- You can add multiple levels of departments according to the actual needs. Click a department as the upper-level department and click **Add Department** button, and then the added department will be the sub-department of it.
- Up to 10 levels can be created.

Editing and Deleting Department

You can double-click the added department to edit its name.

You can click to select a department, and click **Delete Department** button to delete it.

Notes:

- The lower-level departments will be deleted as well if you delete a department.
- Make sure there is no person added under the department, or the department cannot be deleted.

7.5.2 Person Management

Purpose:

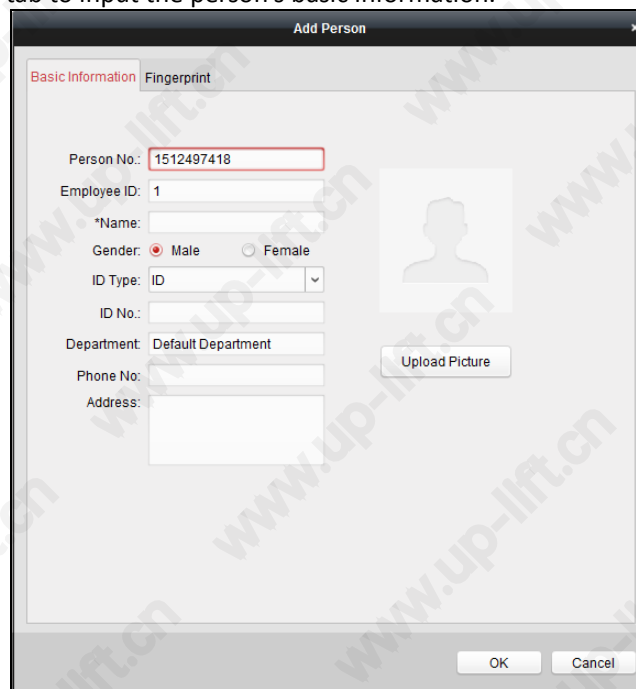
After adding the department, you can add person to the department and manage the added person such as issuing card in batch, importing and exporting person information in batch, etc..

Note: Up to 2000 persons can be added.

Adding Person (Basic Information)

Steps:

1. Select a department in the department list and click **Add Person** to pop up the adding person interface.
2. Click **Basic Information** tab to input the person's basic information.

The screenshot shows a software window titled "Add Person" with a close button (X) in the top right corner. Inside the window, there are two tabs: "Basic Information" (which is selected and highlighted in red) and "Fingerprint". The "Basic Information" tab contains a form with the following fields: "Person No." (containing "1512497418" and highlighted with a red border), "Employee ID:" (containing "1"), "*Name:" (empty), "Gender:" (with radio buttons for "Male" (selected) and "Female"), "ID Type:" (a dropdown menu showing "ID"), "ID No.:" (empty), "Department:" (containing "Default Department"), "Phone No.:" (empty), and "Address:" (empty). To the right of these fields is a placeholder for a person's picture and a button labeled "Upload Picture". At the bottom of the dialog box are "OK" and "Cancel" buttons.

3. The Person No. will be generated automatically and is not editable.
4. Edit the basic information, including the employee ID, the person name, the gender, the ID type, the ID No., the phone No., and the address.
5. 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, or *.jpeg format.
6. Click **OK** to finish adding.

Adding Person (Fingerprint)

Purpose:

Before inputting the fingerprint, you should connect the fingerprint machine to the PC and set its parameters first. For details, refer to 8.4.3 *Fingerprint Machine Configuration*.

Steps:

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



2. Click **Start** button, click to select the fingerprint to start collecting.
3. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.
You can select the registered fingerprint and click **Delete** to delete it.
You can click **Delete All** to clear all fingerprints.
Note: For details about scanning the fingerprint, see *Section 8.1 Tips for Scanning Fingerprint*.
4. Click **OK** to save the fingerprints.

Editing and Deleting Person

You can double-click the added person to edit its basic information and fingerprint.
Or you can check the checkbox to select the person and click **Edit Person** to edit it.
You can click to select a person, and click **Delete Person** to delete it.

Note: If a card is associated with the current person, the association will be invalid after the person is deleted.

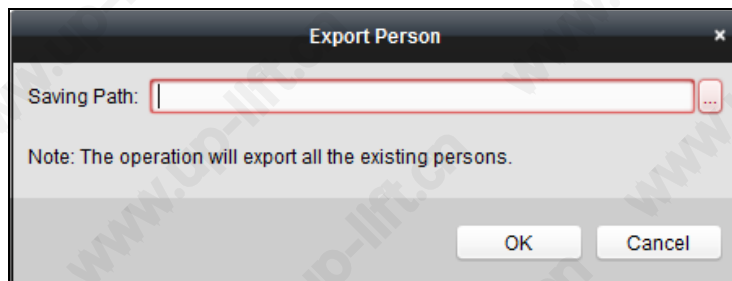
Importing and Exporting Person Information


Purpose:

The person information can be imported and exported in batch.

Steps:

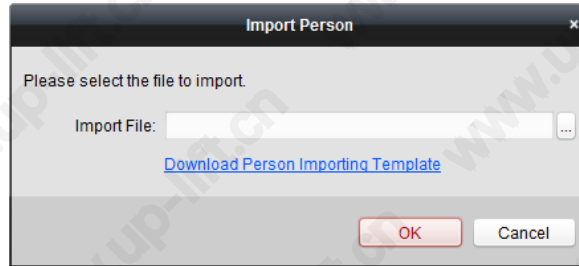
1. After adding the person, you can click **Export Person** button to export all the added person information to the local PC including person No., person name, gender, ID type, ID No., Department, telephone No., and contact address.



Click  to select the path of saving the exported Excel file.

Click **OK** to start exporting.

2. To import the Excel file with person information in batch from the local PC, click **Import Person** button.



You can click **Download Person Importing Template** to download the template first.

Input the person information to the downloaded template.

Click  to select the Excel file with person information.

Click **OK** to start importing.

Getting Person Information from Access Control Device (Do Not Support by Elevator Control Device)

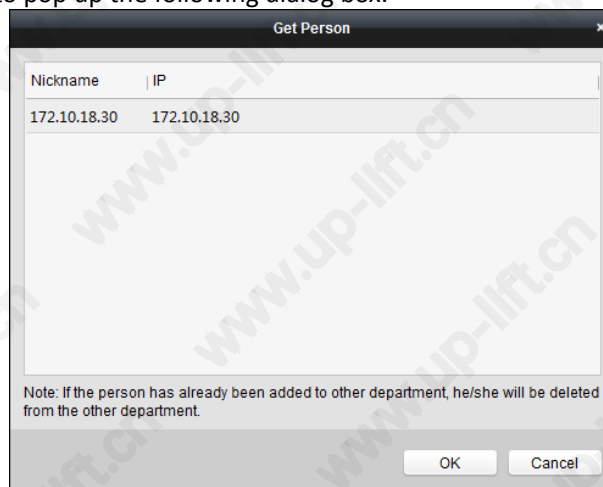
Purpose:

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 method of which is TCP/IP when adding the device.

Steps:

1. In the department list on the left, click to select a department to import the persons to.
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 department.
- After getting the person information, if the person has issued card, the card information will be added to the Card Managment module of the client as well.
- 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.

Importing Person Picture

Purpose:

After adding the person information to the client, you can also import person picture to the client in batch.

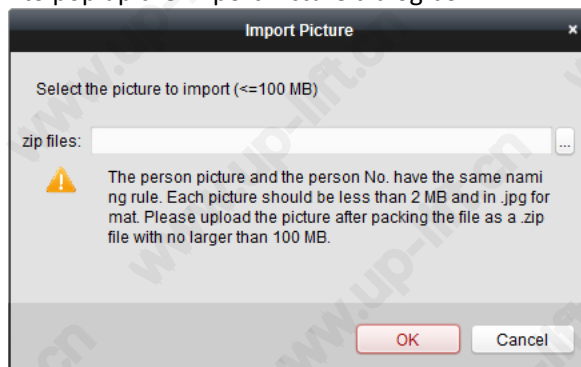
Before you start:

The person pictures to import should be named after the corresponding person No. As a result, you can export the persons information to get the No. of the persons first.

After naming the pictures after the person No., you can import the pictures in batch.

Steps:

1. Click **Import Picture** button to pop up the Import Picture dialog box..




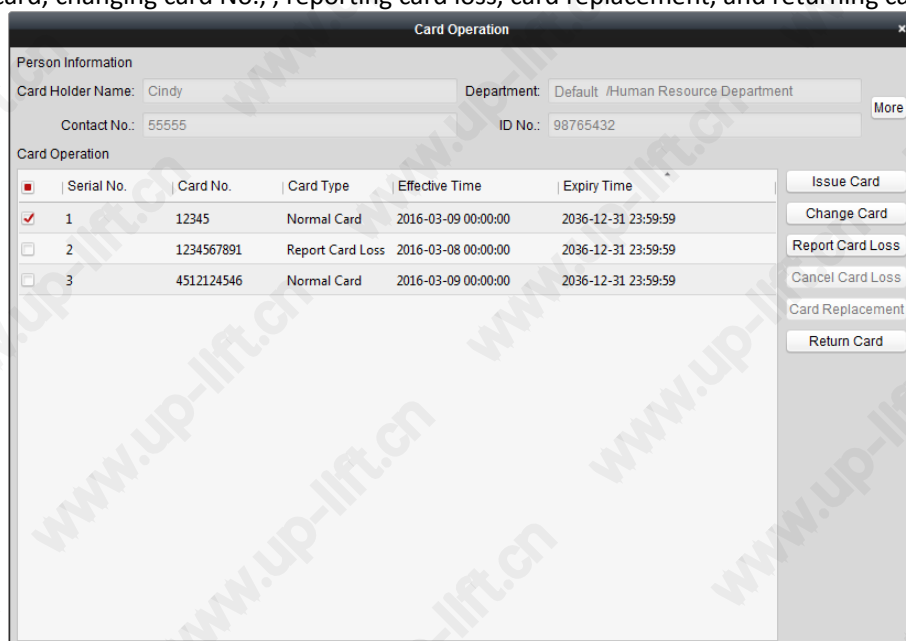
2. Click  to select the package with person pictures and click **OK** to start importing.

Notes:

- The picture name should be the same with the person's person No..
- Each picture should be less than 2 MB and should be in .jpg format.
- The package file should be .zip file.
- The package file should be less than 100 MB.

Card Operation**Purpose:**

After adding the person and card, you can select the person and click  in the Card field for further operation such as issuing card, changing card No., , reporting card loss, card replacement, and returning card.



You can click **More** to view the person details.

For details about these operation, please refer to *Chapter 4.2 Card Management*.

Issuing Card in Batch**Purpose:**

After adding the card information to the client, you can issuing card for the person in batch. For details about adding the card, please refer to *4.2 Card Management*.

Steps:

1. Check the checkbox to select the person for issuing card.
2. Click **Issur Card in Batch** button to enter the following interface.

Issue Card in Batch

Effective Time: 2016-03-08 00:00:00 Expiry Time: 2036-12-31 23:59:59

Open card for the following persons:

Serial No.	Person Name	Department	Telephone No.	Card No.
1	Wendy	Human Resour...	987654321	
2	Cindy	Human Resour...	55555	

OK Cancel

3. Click to set the effective time and expiry time of the card. Click **OK** to save the time settings.
4. In the person list, you can view the selected person details including person name, department, and telephone number.
Click to select card to be issued to the person.

Select Card

Please select card to change.

Search

Serial No.	Card No.
1	1234567891
2	4512124546

Total:2 Page:1/1

Page Go to

OK Cancel

Select the card from the card list and click **OK** to save the settings.
You can input the card No. and click **Search** button to search the card.

5. Click **OK** to complete the card issuing.

7.6 Card Management



Click **Card Management** on the control panel to enter the card management interface.

Serial No.	Card No.
1	123456789

There are three card types: Empty Card, Normal Card, and Lost Card.

Empty Card: A card has not been issued with a person.

Normal Card: A card is issued with a person and is under normal using.

Lost Card: A card is issued with a person and is reported as lost.

7.6.1 Empty Card

Click **Empty Card** tab to manage the empty card first.

Adding

Card

Before you start:

When inputting the card No. when adding the card, you can get the card No. via the following two ways:

- You can get the card No. by the connected card reader. Make sure a card reader is connected to the PC and is configured already. Refer to *Section 7.3.2 Card Reader Configuration*.
- You can also get the card No. by scanning the card on the card reader of the access control device. For this situation, please set the mode as **Card Reader Mode** in Editing Access Controller. For details, refer to 7.4.3

Editing Access Control Device.

The detected card No. will be inputted in the Card No. field automatically.
Perform the following steps to add empty card.

Steps:

1. Click **Add Card** button to pop up the Add Card dialog box.
2. Two adding methods are supported.

✧ Adding Single Card

Select **Single Adding** as the adding mode and input the card No..

Note: Up to 20 digits are allowed in the card No.

The screenshot shows a dialog box titled 'Add Card'. It has two radio buttons under 'Adding Method:': 'Single Adding' (which is selected) and 'Batch Adding'. Below this is a text input field labeled 'Enter Card No.:'. At the bottom right are 'OK' and 'Cancel' buttons.

✧ Batch Adding Cards

Select **Batch Adding** as the adding mode. Input the start card No. and the end card No..

Notes:

- The start card No. and the last card No. should be the with same length. E.g., the last card No. is 234, then the start card No. should be like 028.
- For batch adding, the card No. should contain 1 to 10 digits and letters are not allowed.

The screenshot shows the same 'Add Card' dialog box, but now 'Batch Adding' is selected. It has two text input fields: 'Start Card No.: ' and 'End Card No.: '. At the bottom right are 'OK' and 'Cancel' buttons.

3. Click **OK** button to finish adding.
4. You can check the checkbox of the added card and click **Delete** to delete the card.

Issuing Card

Purpose:

After adding the card to the client, you can issue it to the corresponding added person. You can also issuing the cards to persons in batch. For details, refer to 7.5.2 *Person Management*.

Steps:

1. Click an added empty card in the list and click **Issue Card** button to issue the card with a person.
You can also double click the empty card in the card list to enter the **Issue Card** interface as follows.

2. Input the password of the card itself. 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 4.7.2 Card Reader Authentication.
3. Click to set the effective time and expiry time of the card. Click **OK** to save the time settings.
4. Click to select a person and select a fingerprint for the card.
Note: To select the person's fingerprint, you are required to import the fingerprint first. For details, refer to 7.5.2 Person Management.
5. Click **OK** to finish issuing card.

Notes:

- The issued card will disappear from the Empty Card list, and you can check the card information in the Normal Card list.
- Up to 2000 cards can be added.
- For details about scanning the fingerprint, see the Section 8.1 Tips for Scanning Fingerprint.

7.6.2 Normal Card

Purpose:

After adding the empty card to the client and issue the card to the person, the card will be displayed in the Normal Card list.

Click **Normal Card** tab in the card management interface to show the Normal Card list. You can view all the issued card information, including card No., card holder, and the department of the card holder.

Empty Card Normal Card Lost Card

Normal Card List

Change Card Return Card Report Card... Set Password Import Export Search... Search

<input checked="" type="checkbox"/>	Serial No.	Card No.	Type	Card Holder Name	Department
<input checked="" type="checkbox"/>	1	123456789	Normal Card	Wendy	Default Department

Editing

Card

You can double click the normal card in the list to edit the card linked person information.

Modify Card Linked Information

Card No.: 634364535 Card Password:

Effective Time: 2016-08-17 00:00:00 Expiry Time: 2036-12-31 23:59:59

Please choose person node to issue card.

Search...

Default Department

resit

cindy

Please choose responding fingerprint for card:

OK Cancel

You can edit the card effective time and expiry time, and you can change the person and select the corresponding fingerprint to issue the card again.

Note: To select the person's fingerprint, you are required to import the fingerprint first. For details, refer to 7.5 Person Management.

Changing Card

Purpose:

You can change the linked card for the card holder.

Steps:

1. Check the checkbox to select a normal card and click **Change Card** button to change the associated card for card holder.

Change Card

Old Card No.: 12352

Card Status: Normal Card

Card Holder No.: 2016030817552595

Card Holder Name: Wendy

New Card No.:

OK Cancel

2. In the pop-up window, click ... and select another card in the popup window to replace the current card.
3. Click **OK** to save the changes.

Note: After changing the card, the original card will turn to empty card and you can find it in the Empty Card tab page.

Returning Card

Purpose:

You can return the card from normal card to empty status and cancel the linkage between the card and the person.

Steps:

1. Check the checkbox to select an issued card and click **Return Card** button to cancel the association of the card.
2. Click **OK** to confirm the operation.
Then the card will disappear from the Normal Card list, and you can find it in the Empty Card list.

Reporting Card Loss

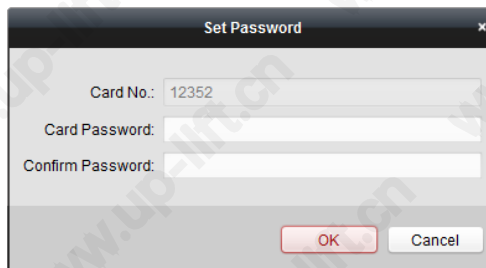
Steps:

1. Check the checkbox to select an issued card and click **Report Card Loss** button to set the card as the Lost Card, that is, an invalid card.
2. Click **OK** to confirm the operation.
Then the card will disappear from the Normal Card list, and you can find it in the Lost Card list.

Setting Card Password

Steps:

1. Check the checkbox to select an issued card and click **Set Password** button to set the password for the card.



The 'Set Password' dialog box contains three input fields: 'Card No.' with the value '12352', 'Card Password:', and 'Confirm Password:'. At the bottom right, there are 'OK' and 'Cancel' buttons.

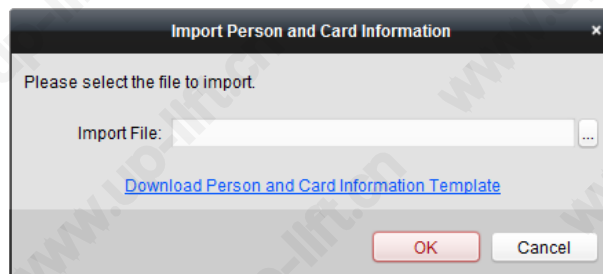
2. Input the card password and confirm the password. The card password should contain 4 to 8 digits.
3. Click **OK** to save the settings.

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 of **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to 7.10.2 *Card Reader Authentication*.

Importing and Exporting Cards

Steps:


1. To import the card and person information from the local PC, click **Import** button to pop up the following dialog box.



The 'Import Person and Card Information' dialog box displays the text 'Please select the file to import.' Below this is an 'Import File:' label followed by a text input field and a file selection icon (three dots). A blue hyperlink 'Download Person and Card Information Template' is positioned below the input field. At the bottom right, there are 'OK' and 'Cancel' buttons.

Click **Download Person and Card Information Template** to download the template for importing. In the template file, input the card holder name and the corresponding card No..


Note: The Card No. should be 1 to 20 digits

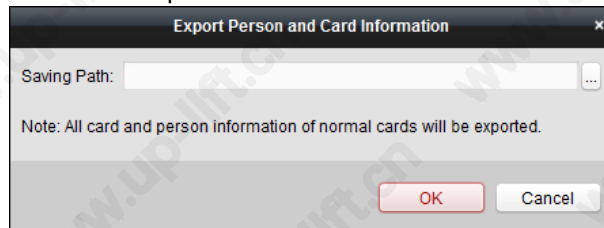
Click  to select the template file with card and person information.

Click **OK** to start importing.

2. To export all the normal card information to the local PC, click **Export** button to pop up the following dialog

box.

Click  to select the path to save the exported file.



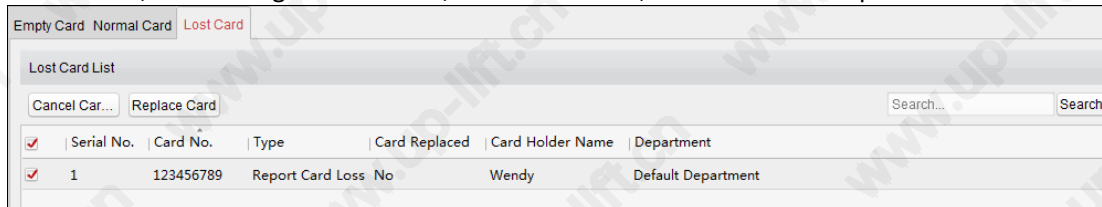
Click **OK** to start exporting. All the normal cards with card holder name and card No. will be exported to the Excel file.

7.6.3 Lost Card

Purpose:

You can manage the card which is reported as lost, including canceling card loss and replacing card.

Click **Lost Card** tab in the card management interface to show the Lost Card list. You can view all the lost card information, including card No., card holder, and the department of the card holder.



Canceling

Card Loss

Purpose:

If the lost card is found, you can cancel the loss for the card and the lost card will turn to normal card.

Steps:

1. Check the checkbox to select the lost card in the list.
2. Click **Cancel Card Loss** button to resume the card to the normal card.
3. Click **OK** to confirm the operation.

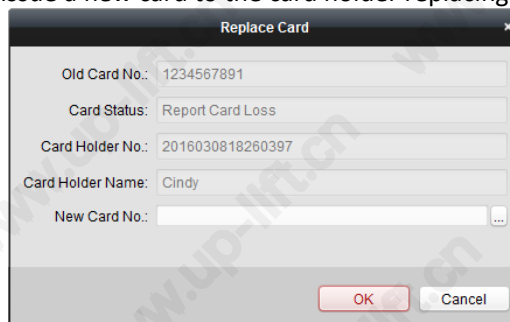
Card Replacement


Purpose:

If the lost card cannot be found any more, you can replace the lost card with a new card.

Steps:

1. Check the checkbox to select the lost card in the list.
2. Click **Replace Card** button to issue a new card to the card holder replacing for the lost card.



3. Click  button to select another card in the popup window as the new card and the predefined permissions of the lost card will be copied to the new one automatically.
4. Click **OK** to save the changes.

7.7 Relay Management

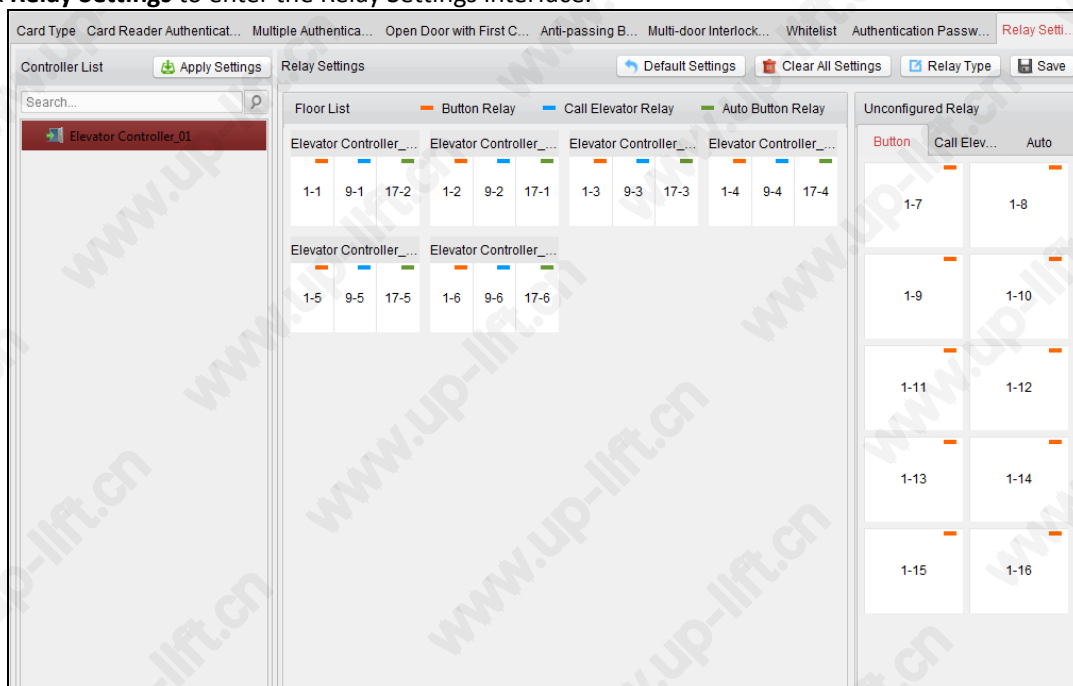
Purpose:

You can manage the relationship between the floor and the relay in this chapter.

7.7.1 Configuring Relay and Floor

Steps:

1. In the Control Panel, click the icon  to enter the Advanced Function module.
2. Click **Relay Settings** to enter the Relay Settings interface.



3. Select an elevator controller in the Controller List on the left of the interface.
4. 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.






5. Click and drag the unconfigured relay from the Unconfigured Relay panel to the corresponding 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.




6. Click **Apply Settings** 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 Relay.  represents the button relay,  represents the call elevator relay, and  represents the auto button relay.



Take the figure as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents the relay, 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 *Section 7.7.2 Configuring Relay Type*.

- By default, the relay total amount is the added floor number X 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.

7.7.2 Configuring Relay Type

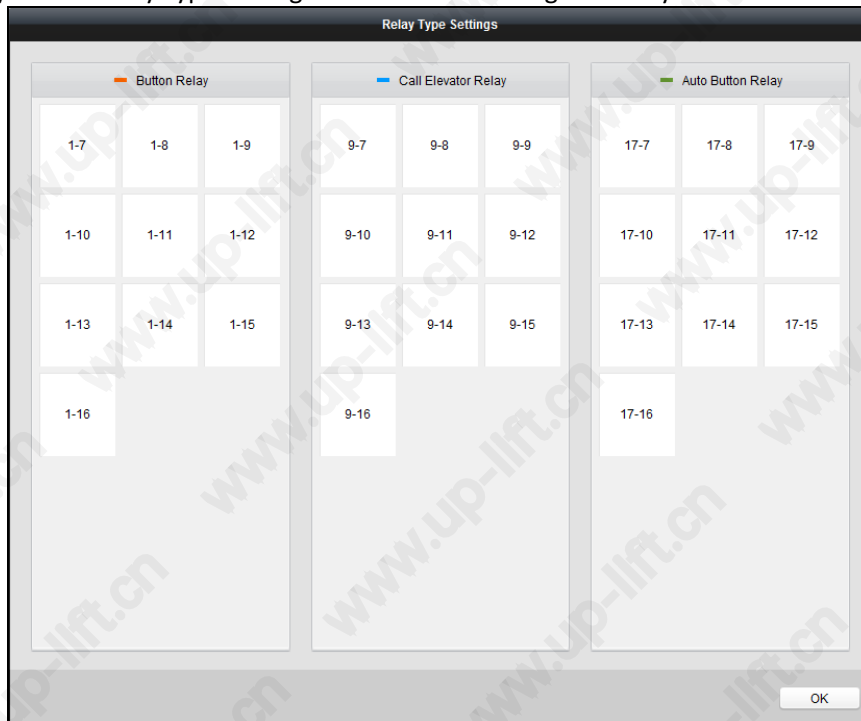
Purpose:

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

Steps:

1. In the Relay Settings interface, click the button **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 Relay. ■ represents the button relay, ■ represents the call elevator relay, and ■ represents the auto button relay.

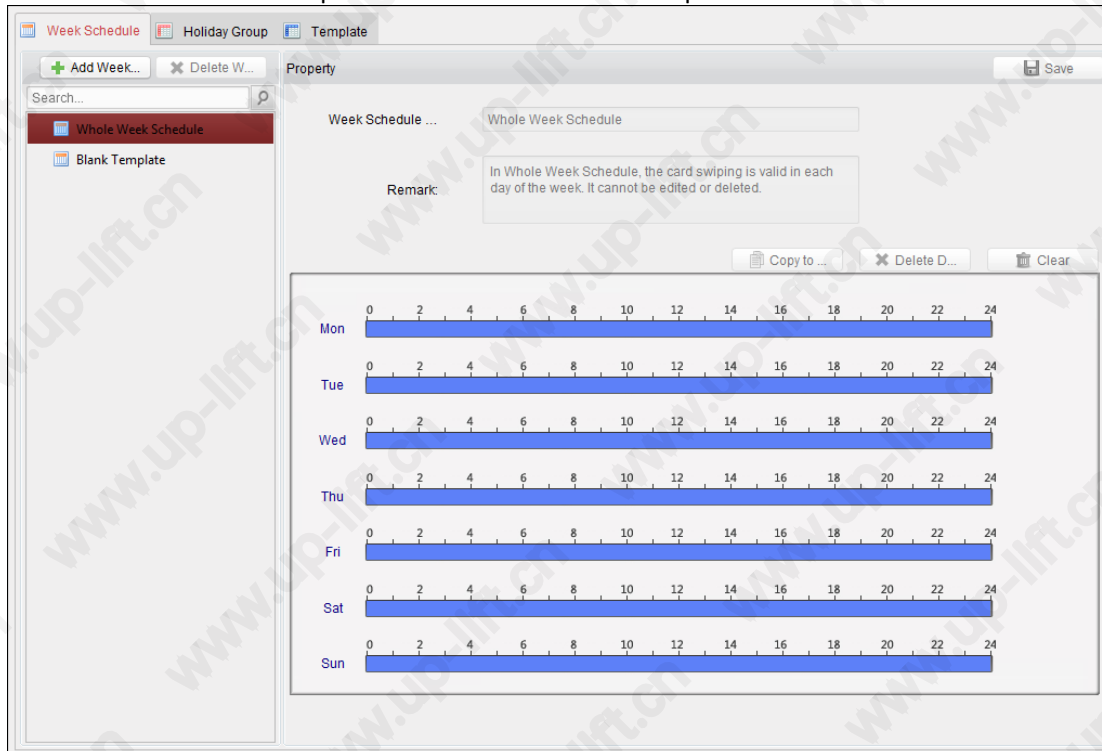
7.8 Schedule Template

Purpose:

You can configure the schedule 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 schedule template.



Click **Template** on the control panel to enter the schedule template interface.



You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, please refer to [7.9 Permission Configuration](#)

7.8.1 Week Schedule

Click **Week Schedule** tab to enter the Week Schedule Management interface.

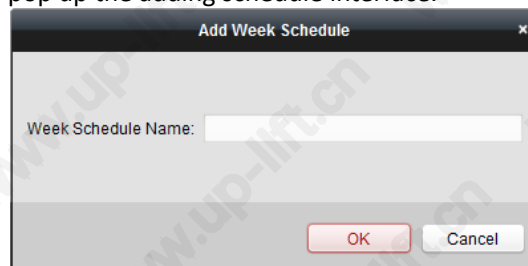
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

- **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 define custom schedules on your demand.

Steps:

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



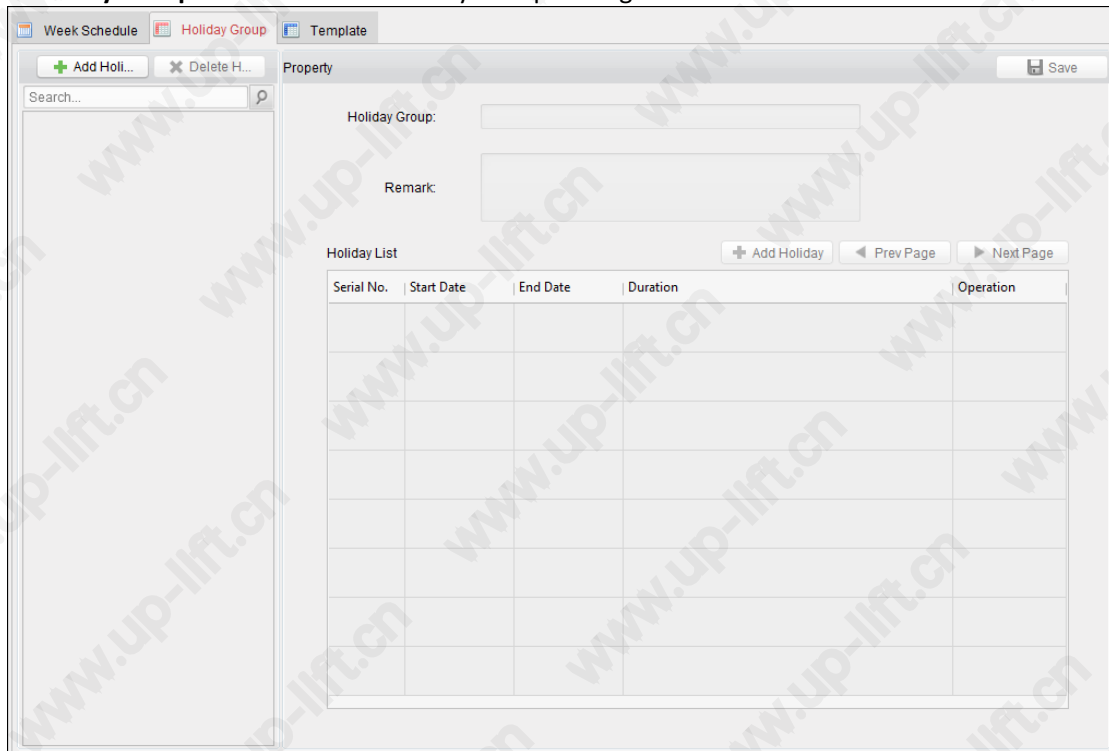
2. Input the name of week schedule and click **OK** button to add the week schedule.
3. Select the added week schedule in the schedule list on the left and you can view its property on the right.
4. You can edit the week schedule name and input the remark information.

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

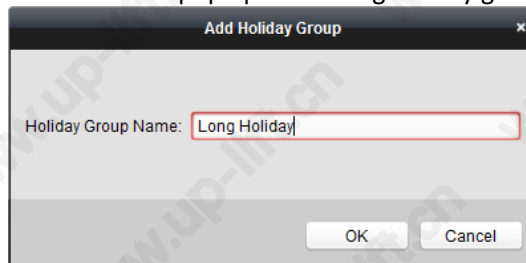
7.8.2 Holiday Group

Steps:

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



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








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

Serial No.	Start Date	End Date	Duration	Operation
1	3/9/2016	3/9/2016	0 2 4 6 8 10 12 14 16 18 20 22 24	
2	3/23/2016	3/31/2016	0 2 4 6 8 10 12 14 16 18 20 22 24	

- 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.

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

Note: The holidays cannot be overlapped with each other.

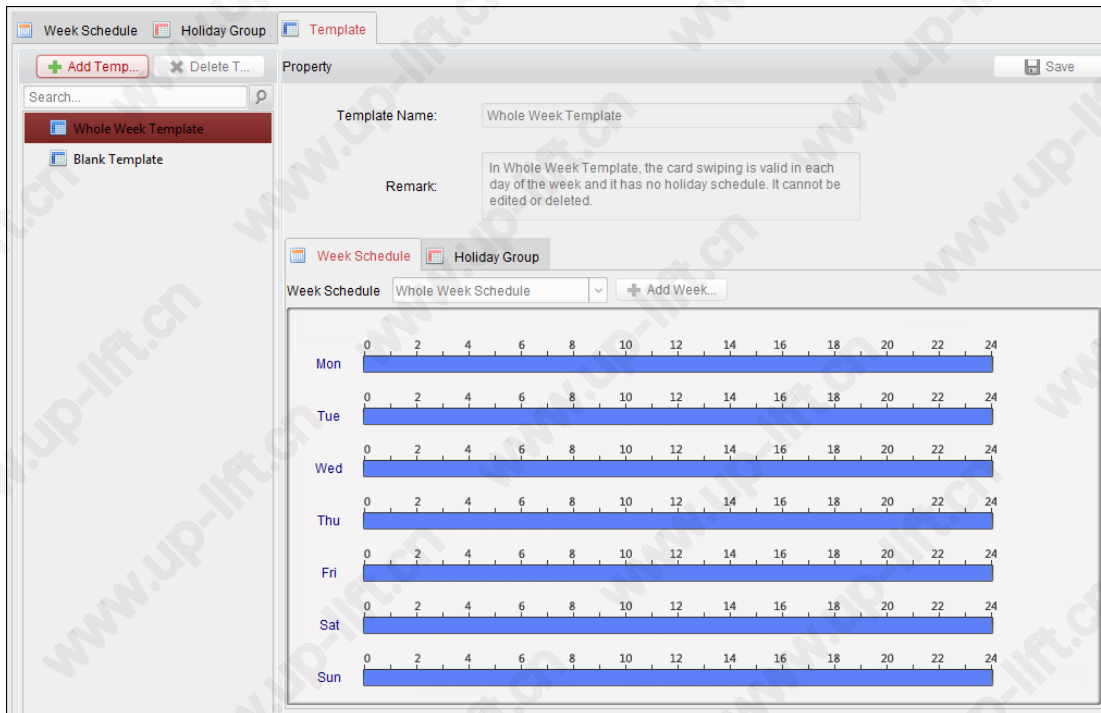
7.8.3 Schedule Template

Purpose:

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

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

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

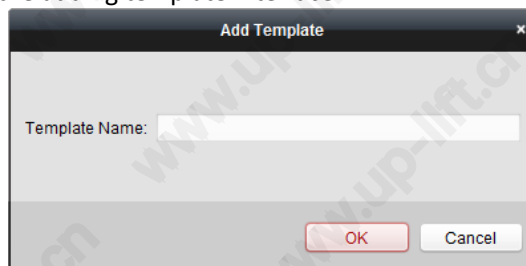


There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

- **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 field 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 4.3.1 Week Schedule.

5. Select holiday groups to apply to the schedule.

Note: Up to 4 holiday groups can be added.

Serial No.	Holiday Group Name	Remark
1	Long Holiday	

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 4.3.2 *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.

7.9 Permission Configuration



Click [Access Control Permission](#) icon on the control panel to enter the Access Control Permission interface.

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.

<input type="checkbox"/>	Serial No.	Person Name	Department	Access Control	Door Group	Template	Status
<input type="checkbox"/>	1	Cindy		10.16.6.111_Door1	test	Whole Week Template	Not Applied
<input type="checkbox"/>	2	Cindy		172.10.18.25_Door1		Whole Week Template	Applied
<input type="checkbox"/>	3	Cindy		172.10.18.25_Door2		Whole Week Template	Applied
<input type="checkbox"/>	4	Cindy		172.10.18.25_Door3		Whole Week Template	Applied
<input type="checkbox"/>	5	Cindy		172.10.18.25_Door4		Whole Week Template	Applied
<input type="checkbox"/>	6	Jess		10.16.6.111_Door1	test	Whole Week Template	Not Applied
<input type="checkbox"/>	7	Jess		172.10.18.25_Door1		Whole Week Template	Applied
<input type="checkbox"/>	8	Jess		172.10.18.25_Door2		Whole Week Template	Applied
<input type="checkbox"/>	9	Jess		172.10.18.25_Door3		Whole Week Template	Applied
<input type="checkbox"/>	10	Jess		172.10.18.25_Door4		Whole Week Template	Applied
<input type="checkbox"/>	11	John		10.17.137.230_Door1	test	Whole Week Template	Not Applied
<input type="checkbox"/>	12	John		10.16.6.111_Door1	test	Whole Week Template	Not Applied
<input type="checkbox"/>	13	John		172.10.18.25_Door1		Whole Week Template	Applied
<input type="checkbox"/>	14	John		172.10.18.25_Door2		Whole Week Template	Applied
<input type="checkbox"/>	15	John		172.10.18.25_Door3		Whole Week Template	Applied
<input type="checkbox"/>	16	John		172.10.18.25_Door4		Whole Week Template	Applied
<input type="checkbox"/>	17	Marry		10.16.6.111_Door1	test	Whole Week Template	Not Applied
<input type="checkbox"/>	18	Marry		172.10.18.25_Door1		Whole Week Template	Applied
<input type="checkbox"/>	19	Marry		172.10.18.25_Door2		Whole Week Template	Applied
<input type="checkbox"/>	20	Marry		172.10.18.25_Door3		Whole Week Template	Applied

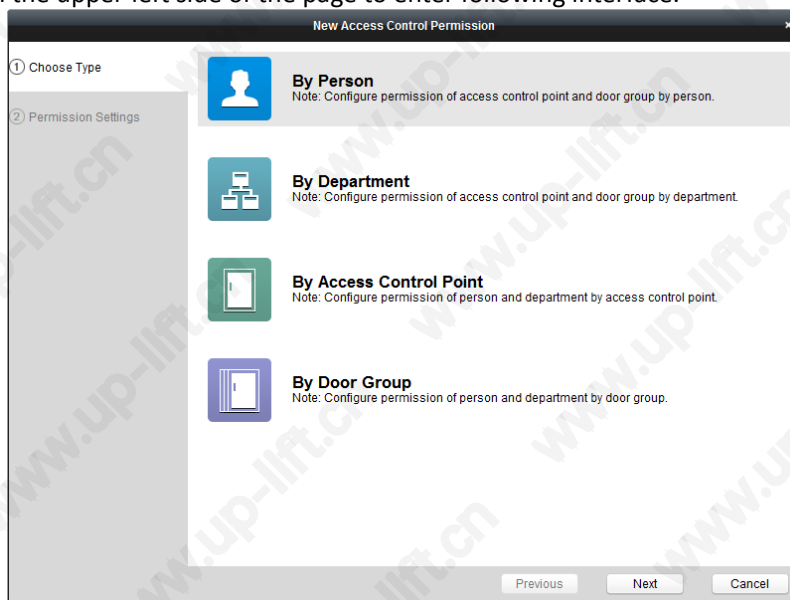
7.9.1 Adding Permission

Purpose:

You can assign permission for people/department to enter/exist the control points (floors) in this section.

Steps:

1. Click **Add** icon on the upper-left side of the page to enter following interface.



The dialog box titled "New Access Control Permission" has a close button (X) in the top right corner. It contains two main sections: "1 Choose Type" and "2 Permission Settings". Under "1 Choose Type", there are four options, each with an icon and a note:

- By Person** (Person icon): Note: Configure permission of access control point and door group by person.
- By Department** (Briefcase icon): Note: Configure permission of access control point and door group by department.
- By Access Control Point** (Floor icon): Note: Configure permission of person and department by access control point.
- By Door Group** (Door icon): Note: Configure permission of person and department by door group.

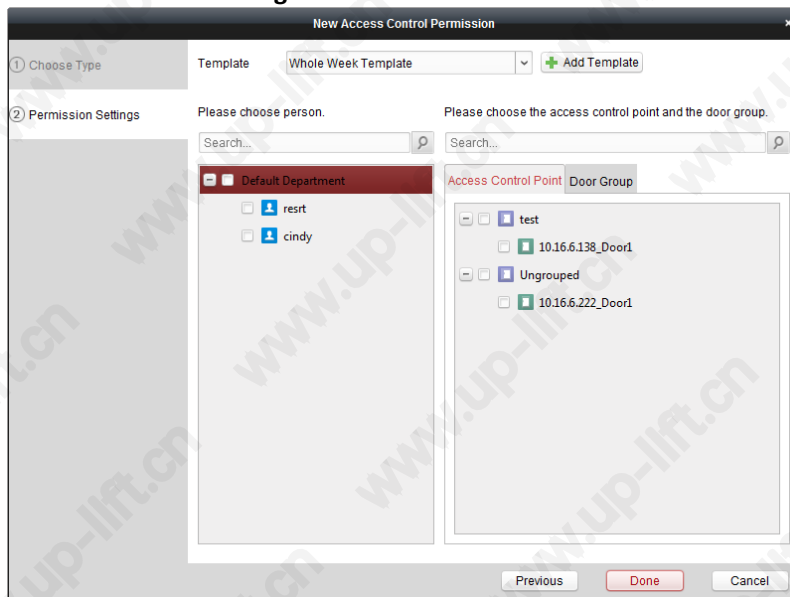
At the bottom of the dialog box, there are three buttons: "Previous", "Next", and "Cancel".

2. Select the permission type.

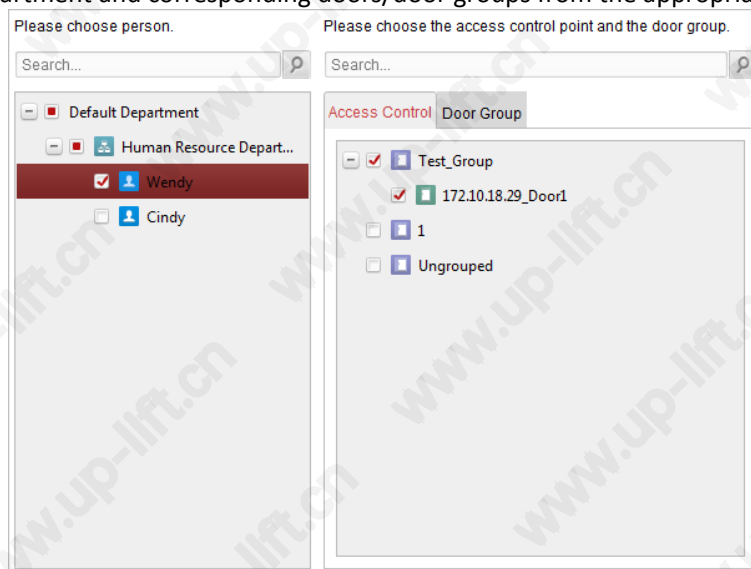
- **By Person:** You can select people from the list to enter/exit the door.
- **By Department:** You can select departments from the list to enter/exit the door. Once the permission is allocated, all the people in this department will have the permission to access the door.
- **By Access Control Point (Floor):** You can select floors from the floor list for people to enter/exit.
- **By Door Group:** You can select groups from the floor list for people to enter/exit. The permission will take effect on the floor in this group.

Note: The Door Group Permission will be available after the door group is added. For details about the door group, refer to 7.4.2 Door Group Management.

- Click **Next** to enter the **Permission Settings** interface.



- Click on the dropdown menu to select a schedule template for the permission.
Note: The schedule template must be configured before any permission settings. You can click **Add Template** button to add the schedule template. Refer to 7.8 Schedule Template for details.
- Select people/department and corresponding doors/door groups from the appropriate lists.



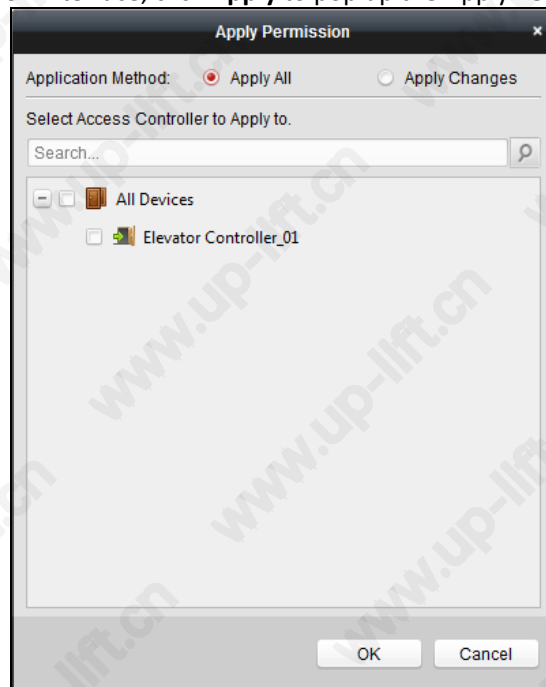
- Click **Finish** button to complete the permission adding.
- (Optional) You can double click **Template** column of the added permission in the list to edit its permission schedule template.
You can select the added permission in the list and click **Delete** to delete it.

7.9.2 Applying Permission

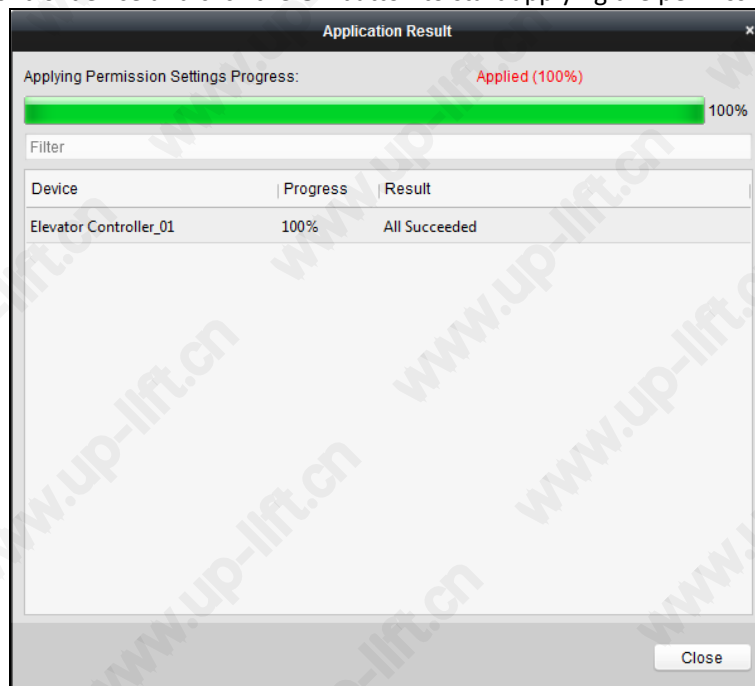
You can apply the added permission to the access control to take effect.

Steps:

1. In the Access Control Permission interface, click **Apply** to pop up the Apply Permission window.



2. Select the Applying Method.
 - **Apply All:** Apply all the permission settings in the list to the selected access control device.
 - **Apply Changes:** Apply the changed permissions to the selected access control device.
3. Select an access control device and click the **OK** button to start applying the permission to the device.



7.9.3 Importing/Exporting Permission

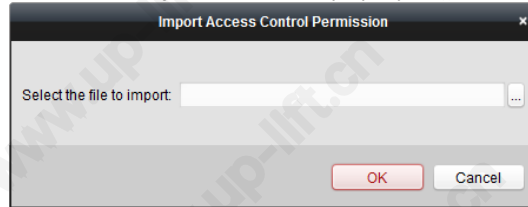
Purpose:


You can also export the added permissions information to the local PC and import the permissions in batch from the local PC.

Steps:

Task 1

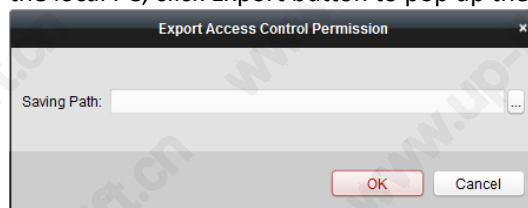
1. To import the permission in batch, click **Import** button to pop up the following dialog box.




2. Click  to select the package file containing the permission information.
3. Click **OK** to start importing.

Task 2

1. To export the permissions to the local PC, click **Export** button to pop up the following dialog box.



2. Click , input the permission file name as desired and select the saving path of the exported package file containing the permission information.
3. Click **OK** to start exporting.

Note: The exported permission file is not editable.

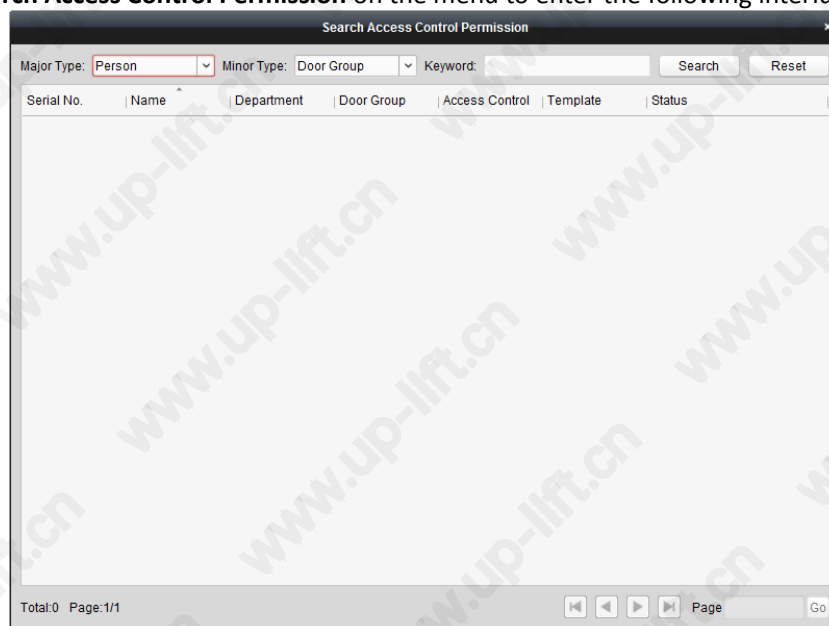
7.9.4 Searching Access Control Permission

Purpose:

You can search the added access control permission via the client.

Steps:

1. Click **Tool->Search Access Control Permission** on the menu to enter the following interface.



2. Set the major type as the main search condition from the dropdown list. You can set it as by person, department, door group, or access control point.
3. Set the minor type as the second search condition from the dropdown list. You can set it as by door group or access control point.
4. You can also input the keyword of the permission.
5. Click **Search** to start searching the result.
You can click **Reset** to set the search condition to the default value.

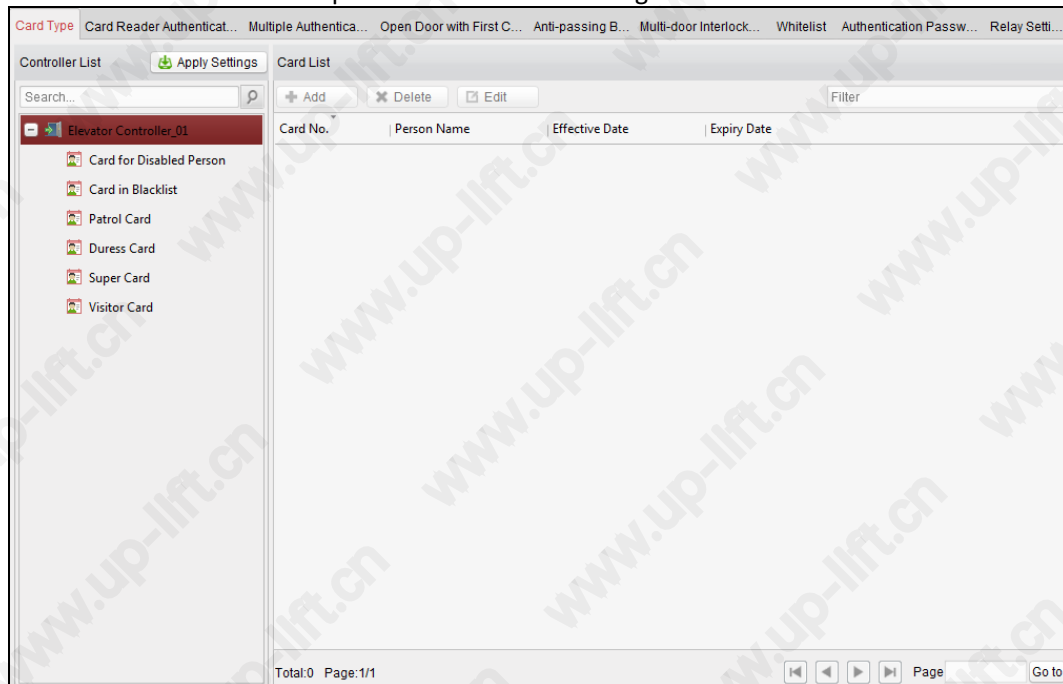
7.10 Advanced Functions

Purpose:

After configuring the person, card, template, status duration, alarm linkage, and access permission, the advanced functions of the Access Control Client can be configured, such as access control type, authentication password and first card.



Click **Advanced Function** icon on the control panel to enter the following interface.



7.10.1 Card Type

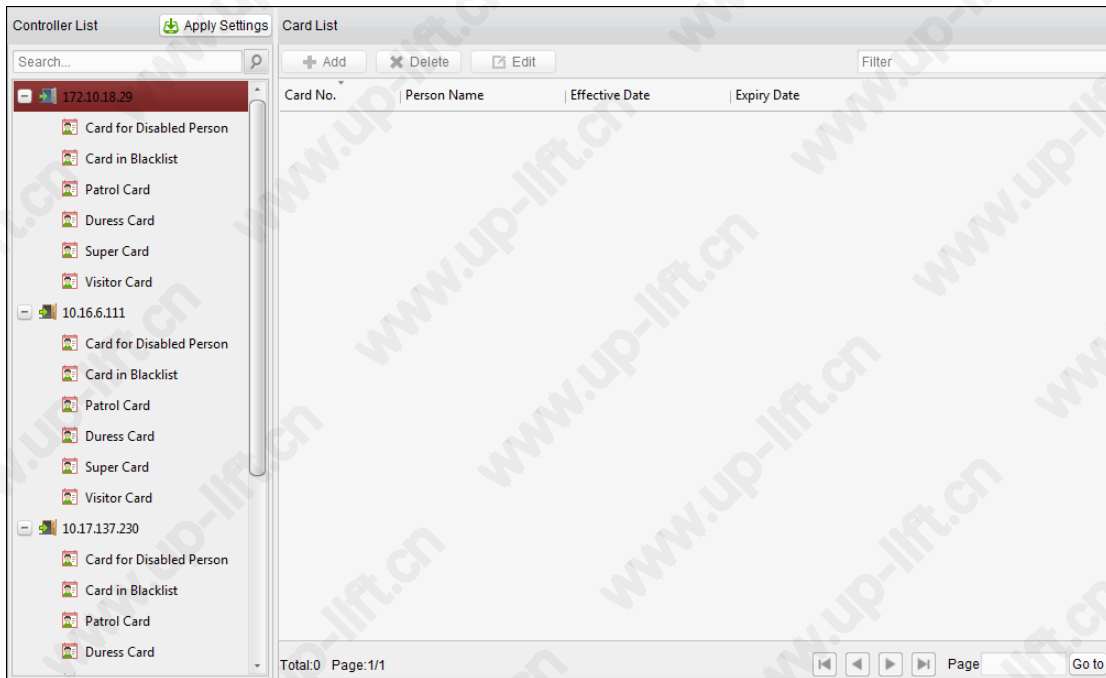
Purpose:

The added cards can be assigned with different card type for the corresponding usage.

Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *4.6 Permission Configuration*

Steps:

1. Click **Card Type** tab and select a card type.



Card for Disabled Person: The door will remain open for the configured time period for the card holder.

Card in Blacklist: The card swiping action will be uploaded and the door cannot be opened.

Patrol Card: The card swiping action can be 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.

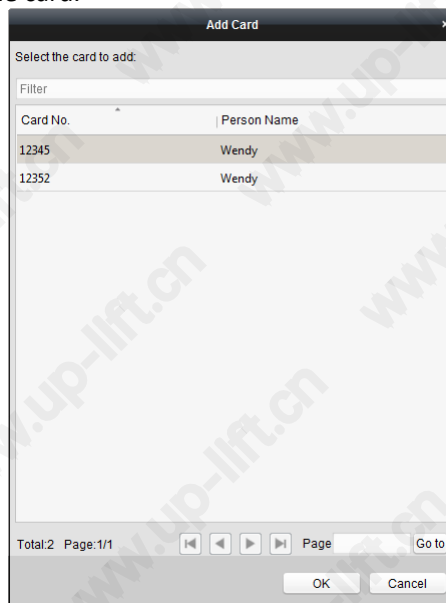
Super Card: The card is valid for all the doors of the controller during the configured schedule.

Visitor Card: The card is assigned for visitors.

Notes:

- The available card types depend on the access control device type.
- If the card is not assigned as any of the above card types, it is assigned as normal card by default.

- Click **Add** and select the available card.



- Click **OK** to confirm assigning the card(s) to the selected card type.
- For the Visitor Card, you can click the added card and click **Edit** to edit the Max. Swipe Times, card Effective Time and Expiry Time.

The screenshot shows a dialog box titled "Edit Visitor Card". It has four input fields: "Card No." with the value "12345", "Max. Swipe Times" with the value "0", "Effective Time" with the value "2016-03-09 00:00:00", and "Expiry Time" with the value "2036-12-31 23:59:59". At the bottom right, there are two buttons: "OK" and "Cancel".

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

5. Click **Apply Settings** button to take effect of the new settings.
6. (Optional) You can click **Delete** to remove the card from the card type and the card can be available for being re-assigned.

7.10.2 Card Reader Authentication

Purpose:

You can set the passing rules for the card reader.

Steps:

1. Click **Card Reader Authentication** tab and select a card reader in the Controller List on the left.
2. Select a card reader authentication mode. The available authentication modes depends on the card reader type:
 - **Card and Password:** The door can open by both inputting the card password and swiping the card.
 - **Fingerprint:** The door can open by only inputting the fingerprint.
 - **Card:** The door can open by only swiping the card.
 - **Card or Fingerprint:** The door can open by inputting the fingerprint or swiping the card.
 - **Password and Fingerprint:** The door can open by both inputting the card password and inputting the fingerprint.
 - **Card and Fingerprint:** The door can open by both inputting the fingerprint and swiping the card.
 - **Card, Password and Fingerprint:** The door can open by inputting the fingerprint, inputting the card password, and swiping the card.
 - **Employee ID and Password:** The door can open by inputting the employee ID and the card password.
3. Click and drag your mouse on a day to draw a color bar on the schedule. It means in that period of time, the card reader authentication is valid.

Property [Copy to] [Save]

Card Reader Name:

Card Reader Authentication Mode:

Authentication Mode: ☒ Card and P... ☐ Card or Aut... ☐ Fingerprint ☐ Card ☐ Card or Fin... ☐ Password a... ☐ Card and Fi... ☐ Card, Pass... ☐ Employee I...

Card Reader Authentication Week Schedule Settings [Copy to Week] [Delete] [Clear]

Day	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	[Schedule bar with segments: grey, yellow, red, orange]												
Tue	[Schedule bar with segments: grey, yellow, red, orange]												
Wed	[Schedule bar with segments: grey, yellow, red, orange]												
Thu	[Schedule bar with segments: grey, yellow, red, orange]												
Fri	[Schedule bar with segments: grey, yellow, red, orange]												
Sat	[Schedule bar with segments: grey, yellow, red, orange]												
Sun	[Schedule bar with segments: grey, yellow, red, orange]												

- Repeat the above steps 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.
You can click **Delete** button to delete the selected time period
Or click **Clear** button to delete all the configured time periods.
- (Optional) Click **Copy to** button at the upper right corner to copy the settings to other card readers.

Select Card Reader [X]

Select Card Reader to Copy to:

Search...

- ☒ Elevator Controller_01
- ☐ Elevator Controller_01_Card Reader2

[OK] [Cancel]

- Click **Save** button to save parameters.
- Click **Apply Settings** button to take effect of the new settings.

7.10.3 Open Door with First Card

Purpose:

The door remains open for the configured time duration after the first card swiping until the remain open duration ends.

Steps:

1. Click **Open Door with First Card** tab and select an access control device from the Controller List on the left of the interface.
2. Check the checkbox of the **Enable First Card Remain Open** field to enable this function.
3. In the **Remain Open Duration** (min), input the time duration for remaining open the door.
Note: The Remain Open Duration should be between 0 and 1440 minutes. By default, it is 10 minutes.
4. In the First Card list, Click **Add** button to pop up the following dialog box.

5. Select the cards to add as first card for the floor and click the **OK** button.

Note: Please set the card permission and apply the permission settings to the access control device first. For details, refer to *7.9 Permission Configuration*

Or you can click the **Delete** button to remove the card from the first card list.

- Click **Save** and then click **Apply Settings** button to take effect of the new settings.

7.11 Linkage Configuration



Click **Linkage Configuration** on the control panel to enter the Linkage Configuration interface.

You can set alarm linkage modes of the access control device, including event alarm linkage, event card linkage, and client linkage.

7.11.1 Event Card Linkage

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

Purpose:



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

Steps:

- In the Linkage Configuration interface, click **Event Card Linkage** tab to enter the following interface.

- Select the access control device from the list on the left.
- Click **Add** button to add a new linkage.
- Click to select the linkage type as **Event Linkage**, and select the event type from the dropdown list.
 - For Device Event, select the detailed event type from the dropdown list.
 - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the



table.

- For Door Event, select the detailed event type and select the door from the table.
 - For Card Reader Event, select the detailed event type and select the card reader from the table.
5. Set the linkage target, and switch the property from  to  to trigger the linkage.
 - **Host Buzzer:** The audible warning of controller will be triggered.
 - **Card Reader Buzzing:** The audible warning of the card reader will be triggered.
 - **Alarm Output:** The alarm output will be triggered for notification.
 - **Door:** The door status of open, closed, remain open, and remain closed will be triggered.

Note: The door status of open, closed, remain open, and remain closed cannot be triggered at the same time.
 6. Click **Save** button to save parameters.
 7. Click **Apply Settings** to apply the updated parameters to the local memory of the device to take effect.

Card Linkage

Steps:

1. Click to select the linkage type as **Card Linkage**.
2. Input the card No. or select the card from the dropdown list.
3. Select the card reader from the table for triggering.
4. Set the linkage target, and switch the property from  to  to trigger the linkage.
 - Host Buzzer:** The audible warning of controller will be triggered.
 - Card Reader Buzzing:** The audible warning of card reader will be triggered.
 - Alarm Output:** The alarm output will be triggered for notification.
 - Door:** The door status of open, closed, remain open, and remain closed will be triggered.

Note: The door status of open, closed, remain open, and remain closed cannot be triggered at the same time.
5. Click **Save** button to save parameters.
6. Click **Apply Settings** to apply the updated parameters to the local memory of the device to take effect.

7.11.2 Client Linkage

Purpose:

You can assign other access control device linkage actions to the trigger by setting up a rule in client linkage.

Event Linkage

Purpose:

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. In the Linkage Configuration interface, click **Client Linkage** tab to enter the following interface.

- Click the **Add** button to add a new client linkage.
- 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.
- Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from ☐ to ☒ to trigger the linkage.
 - Alarm Output:** The alarm output will be triggered for notification.
 - Door:** 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.
- Click **Save** button to save parameters.

Card Linkage

Steps:

- Click to select the linkage type as **Card Linkage**.
- Select the card from the dropdown list and select the access control device as event source.
- Select the card reader from the table for triggering.

- Set the linkage target, select the access control device from the dropdown list as the linkage target, and

switch the property from  to  to trigger the linkage.

Alarm Output: The alarm output will be triggered for notification.

Note: The elevator controller does not support linking the door.

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

7.12 Attendance Management

Purpose:

After adding the device and person, you can set the person shift, set the holiday, manage the person attendance and view the card swiping log.

7.12.1 Attendance Configuration



Click **Attendance Configuration** icon on the control panel to enter the Attendance Configuration interface.

- **Shift Group Management:** Adding, editing, and deleting shift groups for attendance management.
- **Shift Management:** Adding, editing, and deleting the attendance rule and attendance shift.
- **Holiday Management:** Adding, editing, and deleting the holidays for attendance.
- **Shift Schedule Management:** Adding, editing, and deleting the normal and advanced shift schedule.
- **Attendance Check Point Management:** Adding, editing, and deleting the attendance check point.
- **Adjustment Management:** Setting the attendance adjustment reasons and managing the adjustment form.
- **Card Swiping Record Search:** Searching the card swiping log.
- **Parameter Configuration:** Setting the attendance parameters, recalculating and rearranging the attendance data.
- **Data Management:** Calculating the attendance data during the configured period, and supporting exporting or importing the data.

Shift Group Management

Purpose:

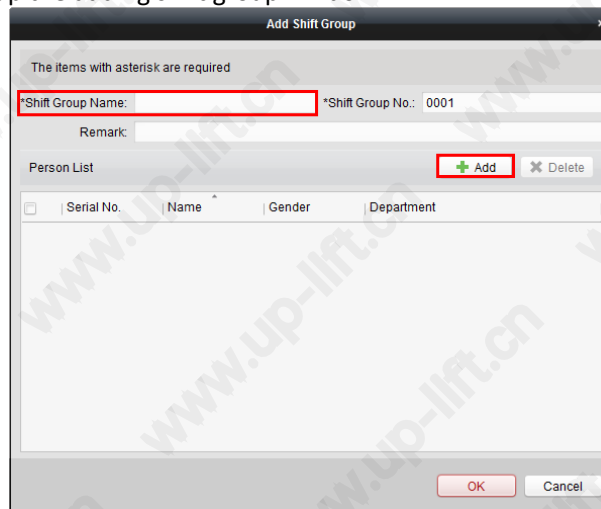
On the shift group management interface, you can add, edit, and delete shift groups for attendance management.

Steps:

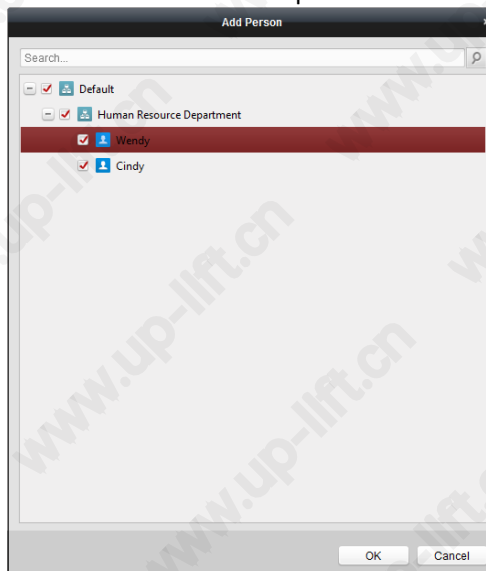
- Click **Shift Group** tab to enter the following page.

+ Add Modify Delete					
<input type="checkbox"/>	Serial No.	Shift Group Name	Shift Group No.	People Counting	Remark

- Click **Add** button to pop up the adding shift group window.



- Enter the shift group name, and add **Add** button on the person list area to pop up the person adding window.



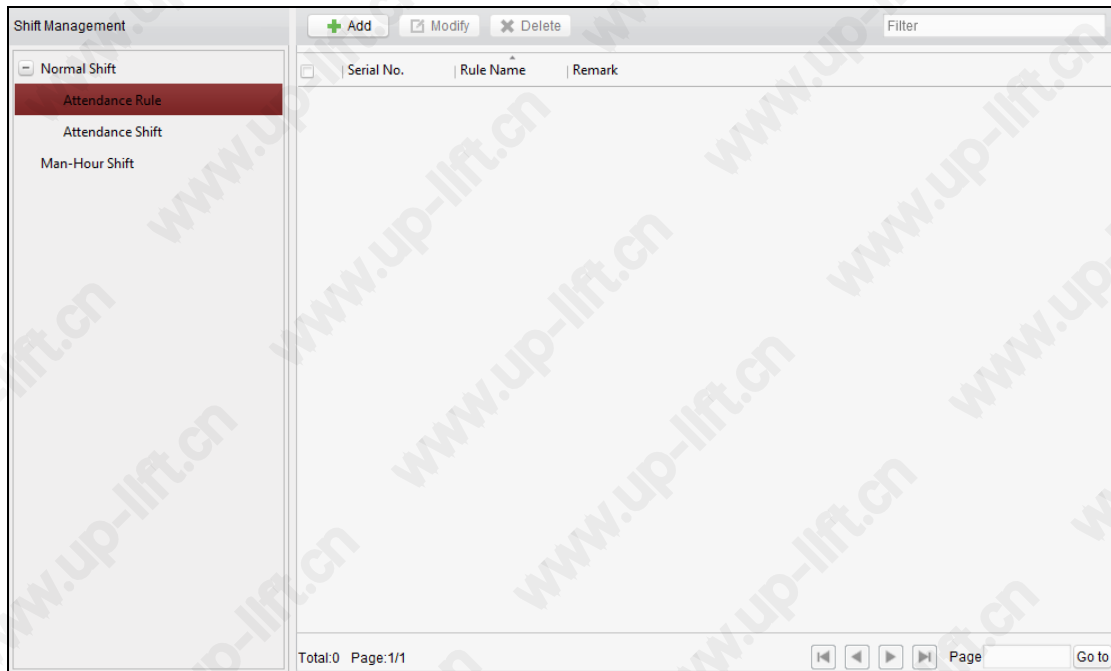
- Check the checkbox to select the person and click **OK** button and return to the shift group settings interface. To delete the added person, check the person from the person list, and click **Delete** button.
- Click **OK** button to complete the operation.
- You can edit or delete the added shift groups by clicking **Edit** or **Delete** button.

Notes:

- After deleting the shift group, the shift schedule of the shift group will be deleted as well. For details about shift schedule, refer to *Section 1401440.0 Shift Schedule Management*.
- If the person has been added to one shift group, he/she cannot be added to other shift groups.
- After deleting the person from the shift group, the person's attendance date will be deleted as well. If the attendance result has been calculated, the person's attendance result will be deleted.

Shift Management

Click **Shift** tab to enter the shift management interface.



There are two kinds of shifts in this interface: **Normal Shift**, and **Man-Hour Shift**.

Normal Shift

✧ Setting Attendance Rule

Steps:

1. Click **Attendance Rule** to set the rule for the attendance management.
2. Click **Add** button to pop up the following dialog box.

3. Set a rule name.
4. Set detailed parameters for the attendance rule according to actual needs.
5. Click **OK** to save the rule.
6. (Optional) You can edit or delete the rule by clicking **Edit** or **Delete** button.

Notes:

- After deleting the rule, the normal attendance shift which has enabled the rule will be deleted as well.
- If the shift which has enabled the rule has already set the shift schedule, the shift will not be deleted.

✧ Setting Attendance Shift

Steps:

1. Click **Attendance Shift** to set the normal attendance shift.

- Click **Add** button to pop up the attendance shift setting window.

- Set a shift name.
- Set on-work duration for the shift, and select the attendance rule from the dropdown list.
- Click **OK** button to complete the operation.
- (Optional) You can edit or delete the shift by clicking **Edit** or **Delete** button.
Note: After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to 5.1.4 Shift Schedule Management.

Man-Hour Shift

Steps:

- Click **Man-Hour Shift** to set the man-hour shift details.
- Click **Add** button to pop up the man-hour shift setting window.

- Set a shift name, and daily work duration.
- (Optional) Check the checkbox of latest on-work time, and set the latest on-work time.
- (Optional) Set the durations excluded from man-hour duration.
- Click **OK** button to complete the operation.
- (Optional) You can edit or delete the shift by clicking **Edit** or **Delete** button.

Note: After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to Section 36377600.0.1073774594 Shift Schedule Management.

Holiday Management

Steps:

1. Click **Holiday** tab to enter the holiday management interface.

Serial No.	Holiday Name	Holiday Days	Remark

2. Click **Add** button to pop up the holiday setting window.

The items with asterisk are required

*Holiday Name:

Remark:

Date List

Serial No.	Date	Week

OK Cancel

3. Click **Add** button to pop-up holiday adding window.

The items with asterisk are required

*Start Date: 3/10/2016

*End Date: 3/10/2016

*Select by Week

☐ Monday ☐ Tuesday ☐ Wed ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

☐ All

OK Cancel

4. Set the start date and end date, select the date of week, and click **OK** button.
5. Click **OK** to save the settings.

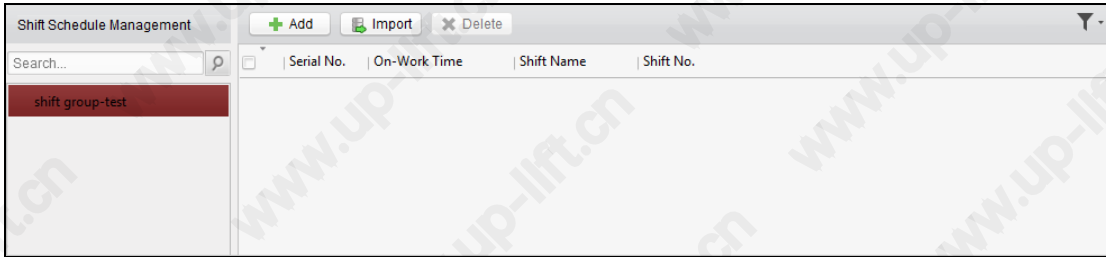
Shift Schedule Management

Purpose:

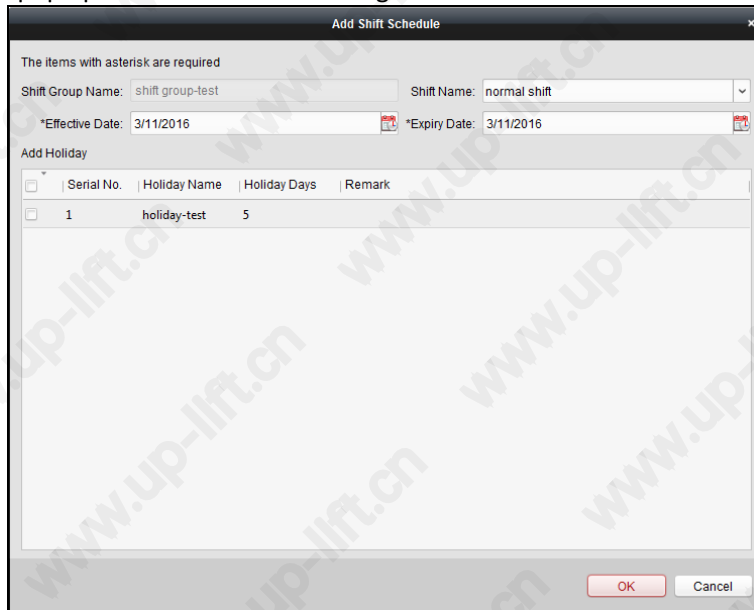
After setting the shift group and the corresponding shift and shift rule, you can set the shift schedule for the shifts.

Steps:

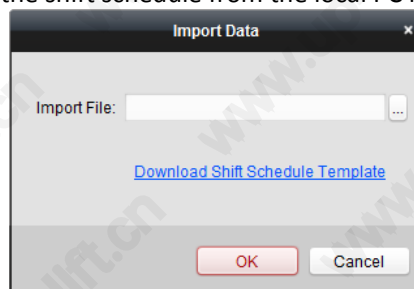
1. Click **Shift Schedule** tab to enter the shift schedule management interface.



2. Select the shift group from the list on the left.
3. Click **Add** button to pop up the shift schedule settings window.



4. Select the shift name from the drop-down list and set the start data and end data.
Note: The effective date of the shift schedule cannot be earlier than the current data.
 (Optional) You can check the checkbox of holiday to add the holiday shift.
 Click **OK** button to complete the operation.
5. Click **OK** to save the settings.
6. You can also click **Import** to import the shift schedule from the local PC in batch.



Click **Download Shift Schedule Template** to download the template and you can input the Shift Group No., Date, and Shift No. in the template.

Click ... to select the file for importing

Click **OK** to start importing.

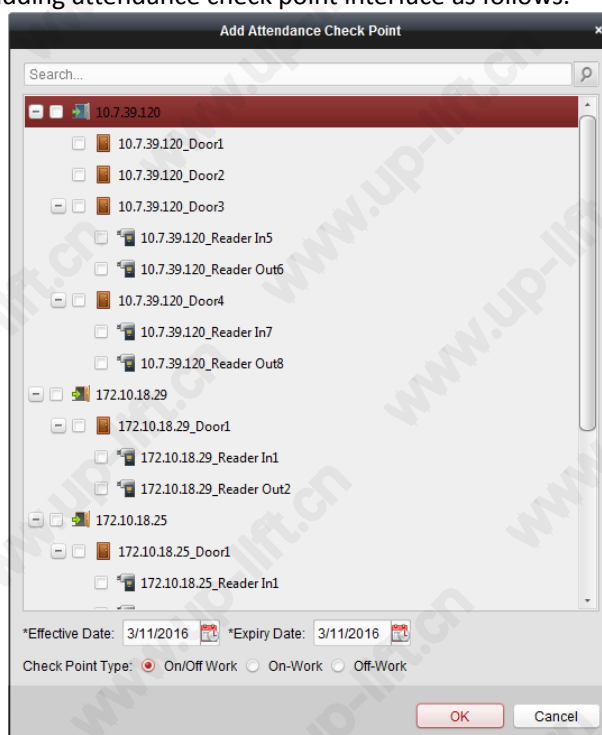
Attendance Check Point Management

Steps:

1. Click **Attendance Check Point** tab to enter the attendance check point management interface.

+ Add ✎ Modify ✕ Delete			Filter					
<input type="checkbox"/>	Serial No.	Check Point Name	Check Point Type	Effective Date	Expiry Date	Door Position	Reader Name	Description
<input type="checkbox"/>	1	10.7.39.120_10.7.39.120_...	On/Off-Work	2016-03-10	2016-03-10		10.7.39.120_Reader ...	
<input type="checkbox"/>	2	10.7.39.120_10.7.39.120_...	On/Off-Work	2016-03-10	2016-03-10		10.7.39.120_Reader L...	
<input type="checkbox"/>	3	10.7.39.120_10.7.39.120_...	On/Off-Work	2016-03-10	2016-03-10		10.7.39.120_Reader L...	
<input type="checkbox"/>	4	10.7.39.120_10.7.39.120_...	On/Off-Work	2016-03-10	2016-03-10		10.7.39.120_Reader ...	
<input type="checkbox"/>	5	172.10.18.25_172.10.18....	On/Off-Work	2016-03-10	2016-03-10		172.10.18.25_Reader...	
<input type="checkbox"/>	6	172.10.18.25_172.10.18....	On/Off-Work	2016-03-10	2016-03-10		172.10.18.25_Reader...	

2. Click **Add** to pop up the adding attendance check point interface as follows.



Check the select the card reader of the access control point and set the start date and end date.

Select the check point type.

Click **OK** to save the adding.

The added check points will be displayed in the attendance check point list.

3. You can check the checkbox of a check point, and click **Edit** button to pop up the attendance check point editing window.

You can edit the attendance check point name, start date, end date, and check point type, controller name, door position, and card reader name.

Click **OK** button to complete the operation.

4. You can check the checkbox of a check point and click **Delete** button to delete the added check point.

Adjustment Management

Purpose:

In this module, you can manage the adjustment reason in **Reason Management** and manage the adjustment application form in **Form Management**.

Reason Management

✧ Leave

You can add, edit, and delete reasons for leave on the leave interface.

Steps:

1. Click **Adjustment** tab to enter the adjustment management interface.
2. Click **Leave** tab to enter the leave interface.

+ Add <input checked="" type="checkbox"/> Modify <input checked="" type="checkbox"/> Delete Filter		
<input type="checkbox"/>	Serial No.	Adjustment Reason
<input type="checkbox"/>	1	Sick Leave
<input type="checkbox"/>	2	Personal Leave
<input type="checkbox"/>	3	Paternity Leave
<input type="checkbox"/>	4	Parental Leave
<input type="checkbox"/>	5	Maternity Leave
<input type="checkbox"/>	6	Family Reunion Leave
<input type="checkbox"/>	7	Bereavement Leave
<input type="checkbox"/>	8	Annual Leave

3. Click **Add** button to pop up the adjustment reason adding dialog box.

Adjustment Reason

The items with asterisk are required

Adjustment Type:

*Adjustment Reason:

OK Cancel

4. Enter the adjustment reason, and click **OK** button to save the adding.

Notes:

- The default adjustment reasons include leave for personal affairs, sick leave, marriage leave, funeral leave, home leave, annual leave, maternity leave, and paternity leave. These pre-defined reasons cannot be edited or deleted.
- You can check the checkbox of a reason and click **Edit** button to edit the reason, and click **Delete** button to delete the reason.

✧ **Leave in Lieu**

Steps:

1. Click **Leave in Lieu** tab to enter the leave-in-lieu interface.

+ Add <input checked="" type="checkbox"/> Modify <input checked="" type="checkbox"/> Delete Filter		
<input type="checkbox"/>	Serial No.	Adjustment Reason
<input type="checkbox"/>	1	Overtime Exchange Holiday
<input type="checkbox"/>	2	Business Trip Exchange Holiday

2. Click **Add** button to pop up the adjustment reason adding dialog box.

Adjustment Reason

The items with asterisk are required

Adjustment Type:

*Adjustment Reason:

OK Cancel

3. Enter the adjustment reason, and click **OK** button.

Notes:

- The default adjustment reasons for leave in lieu include overtime, and business trip. These pre-defined reasons cannot be edited or deleted.
- You can check the checkbox of a reason and click **Edit** button to edit the reason, and click **Delete** button to delete the reason.

✧ **Overtime**

Steps:

1. Click **Overtime** tab to enter the overtime interface.

+ Add <input checked="" type="checkbox"/> Modify <input checked="" type="checkbox"/> Delete Filter	
Serial No.	Adjustment Reason
<input type="checkbox"/> 1	Workday Overtime
<input type="checkbox"/> 2	Work Demand
<input type="checkbox"/> 3	Off Day Overtime
<input type="checkbox"/> 4	Holiday Overtime

2. Click **Add** button to pop up the adjustment reason adding dialog box.
3. Enter the adjustment reason, and click **OK** button.

Notes:

- The default adjustment reasons for overtime include work requirement, working day overtime, rest day overtime, and holiday overtime. These pre-defined reasons cannot be edited or deleted.
- You can check the checkbox of a reason and click **Edit** button to edit the reason, and click **Delete** button to delete the reason.

✧ Card Replacement

Steps:

1. Click **Card Replacement** tab to enter the following interface.

+ Add <input checked="" type="checkbox"/> Modify <input checked="" type="checkbox"/> Delete Filter	
Serial No.	Adjustment Reason
<input type="checkbox"/> 1	Shift Rearrangement
<input type="checkbox"/> 2	Forget to Swipe Card
<input type="checkbox"/> 3	Device Fault
<input type="checkbox"/> 4	Card Loss
<input type="checkbox"/> 5	Business Trip

2. Click **Add** button to pop up the adjustment reason adding dialog box.
3. Enter the adjustment reason, and click **OK** button.

Notes:

- The default adjustment reasons for card replacing include forget to swipe card, attendance card lost, device fault, shift adjustment, and business trip. These pre-defined reasons cannot be edited or deleted.
- You can check the checkbox of a reason and click **Edit** button to edit the reason, and click **Delete** button to delete the reason.

Form Management

✧ Enabled List

Steps:

1. Click **Enabled List** tab to enter the enabled adjustment application form interface.

+ Add <input checked="" type="checkbox"/> Disable <input checked="" type="checkbox"/> Delete Filter								
<input checked="" type="checkbox"/>	Serial No.	Form No.	Person Name	Department	Start Time	End Time	Adjustment Type	Adjustmen
<input checked="" type="checkbox"/>	1	20160311162...	Cindy	Dafault /Human...	2016-03-11 00:00:00	2016-03-11 23:59:59	Leave	Personal Le
<input type="checkbox"/>	2	20160311162...	Wendy	Default /Human...	2016-03-11 00:00:00	2016-03-11 23:59:59	Leave	Personal Le
<input type="checkbox"/>	3	20160311162...	Cindy	Default /Human...	2016-03-11 00:00:00	2016-03-11 23:59:59	Leave	Personal Le
<input type="checkbox"/>	4	20160311162...	Wendy	Default /Human...	2016-03-11 00:00:00	2016-03-11 23:59:59	Leave	Personal Le

2. Click **Add** button to add an attendance management form.

Adjustment Type: ☒ Leave ☐ Leave in Lieu ☐ Overtime ☐ Card Replacement

Adjustment Reason: Personal Leave

Please choose person.

+ Add - Delete

Serial No.	Name	Gender	Department
------------	------	--------	------------

Duration: 2016-03-21 00:00:00 — 2016-03-21 23:59:59

OK Cancel

3. Select the adjustment type: leave, leave in lieu, overtime, and card replacement.

Leave, Leave in Lieu, and Overtime

- 1) Select the adjustment reason from the drop-down list.
- 2) Click **Add** button to pop up the person adding window.

Select Adding Type: ☐ By Department ☒ By Shift Group

Search...

All

shift group-test

Wendy

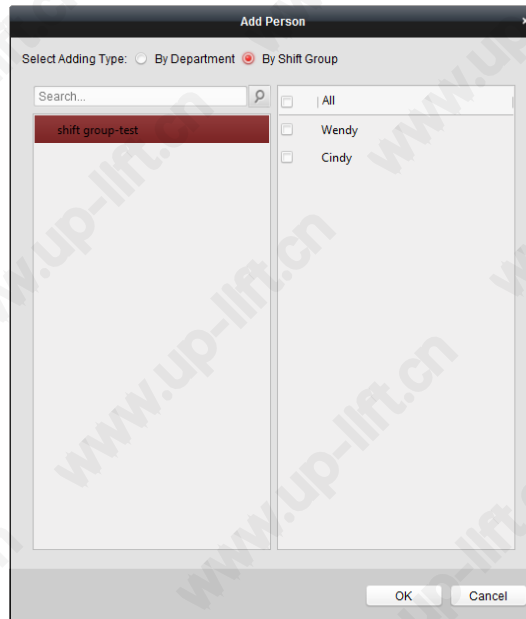
Cindy

OK Cancel

- 3) Select the adding type as by department or by shift group. Select the person and click **OK** button.
- 4) Set the time duration.

Card Replacement

- 1) Select the adjustment reason from the drop-down list.
- 2) Click **Add** button to pop up the person adding window.



- 3) Select the adding type as by department or by shift group. Select the person and click **OK** button.
- 4) Set the date, attendance shift type, and card replacing time.
4. Click **OK** button to complete the operation

✧ Disabled List

Steps:

1. In the Enabled List interface, check the checkbox of a piece of enabled list and click **Disable** button to disable the list.
2. Click **Disabled List** tab and the disabled adjustment application form will be listed on the disabled interface.

Delete									
	Serial No.	Form No.	Person Name	Department	Start Time	End Time	Adjustment Type	Adjustmen	
<input checked="" type="checkbox"/>	1	20160310132...	Wendy	默认部门/Human...	2016-03-10 00:00:00	2016-03-10 23:59:59	Leave	Personal Le	
<input type="checkbox"/>	2	20160310132...	Cindy	默认部门/Human...	2016-03-10 00:00:00	2016-03-10 23:59:59	Leave	Personal Le	

3. You can check the checkbox and click **Delete** to delete the disabled list.

Searching Card Swiping Record

Click **Card Swiping Record** tab to enter the card swiping log searching and viewing interface.

Search by: Department	Department: Human Resource	Name:	Search						
Search Scope: All	Start Time: 2016-08-15 00:00:00	End Time: 2016-08-15 23:59:59	Reset						
Card Swiping Record			Export						
<input type="checkbox"/>	Serial No.	Person Name	Card No.	Card Swiping Time	Department	Check Point Name	Card Reader Name	Door Name	Controller Name

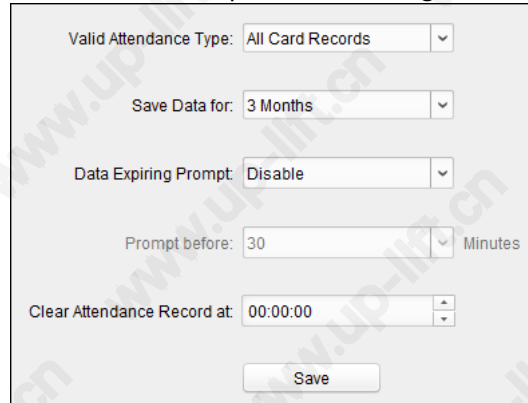
You can search

the card swiping log by two query types: **By Shift Group**, and **By Department**.
 Input other search conditions and click **Search** to start query the card swiping log.
 You can click **Export** to export the card swiping records to the local PC.

Parameters Configuration

Steps:

1. Click **Parameters Configuration** tab to enter the parameters configuration interface.



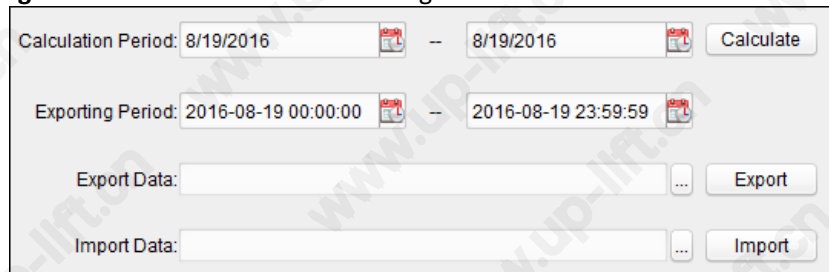
The screenshot shows the 'Parameters Configuration' window. It contains several settings: 'Valid Attendance Type' is set to 'All Card Records'; 'Save Data for' is set to '3 Months'; 'Data Expiring Prompt' is set to 'Disable'; 'Prompt before' is set to '30' minutes; and 'Clear Attendance Record at' is set to '00:00:00'. A 'Save' button is at the bottom.

2. Select the valid attendance type and data saving time.
3. Select to enable or disable the data expiring prompt function. If enabled, you can set the time for the prompt before the data is expired.
4. Set the time to clear the attendance records.
5. Click **Save** to save the parameters.

Data Management

Steps:

1. Click **Data Management** tab to enter the data management interface.



The screenshot shows the 'Data Management' window. It includes fields for 'Calculation Period' (8/19/2016 to 8/19/2016) with a 'Calculate' button. Below that is 'Exporting Period' (2016-08-19 00:00:00 to 2016-08-19 23:59:59). There are also fields for 'Export Data' and 'Import Data', each with a file selection icon and a corresponding button ('Export' and 'Import').

2. Select the date and time period for calculation and click **Calculate** to start calculating the attendance data.
3. After calculation, you can also export the attendance data to the local PC. Select the period for exporting the attendance data, click ... and select the saving path for the exported data file, and then click **Export** to start exporting.
4. You can also import the attendance data to the client. Click ... to select the data file to import and then click **Import** to start importing.

7.12.2 Attendance Statistic



Click **Attendance Statistics** icon on the control panel to enter the Attendance Statistics interface.

On the Attendance Statistics interface, you can search the attendance statistic, attendance result statistics, and attendance rate statistics.

You can input the search condition including shift type, department, start date, and end date, and click **Search** button to search the attendance data.

You can click **Reset** to reset the search condition to the default value.

After searching, you can click **Export** to export the searching report to the local PC.

7.13 Access Control System Maintenance

7.13.1 Door Status Management

Purpose:

You can anti-control the door via the client and set the door status duration.

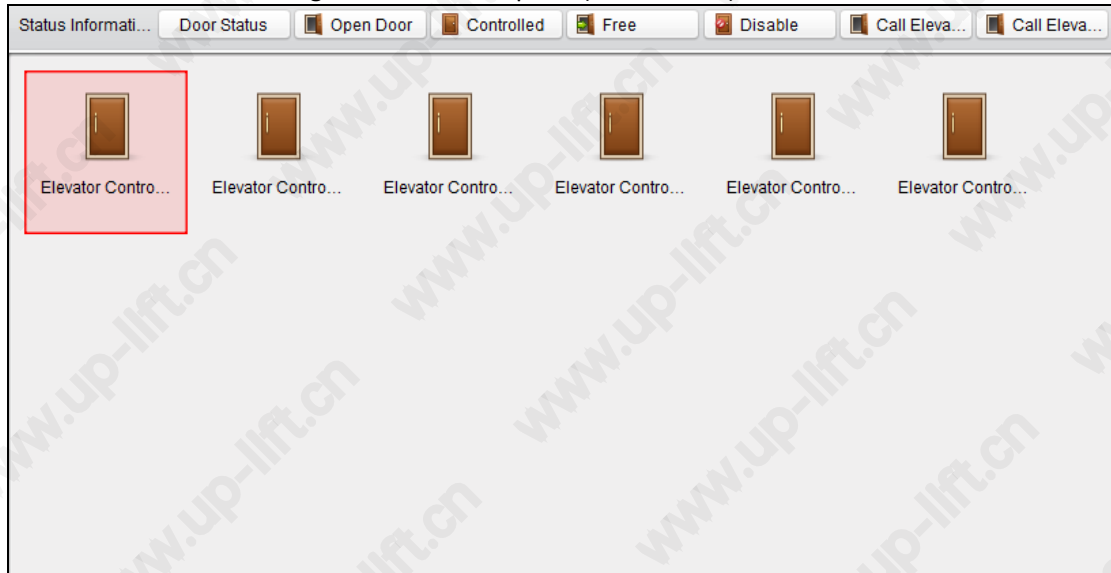


Click **Status Monitor** icon on the control panel to enter the Status Monitor interface.

Anti-control the Access Control Point (Floor)

Purpose:

You can control the status for a single access control point (floor button).

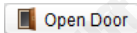


Steps:

1. Select an access control group on the left. For managing the access control group, refer to *Section 7.4.2 Door Group Management*.
2. The access control points of the selected access control group will be displayed on the right of the interface.

3. Click icon  on the Status Information panel to select an access control point (floor).

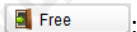
4. Click the following button listed on the **Status Information** panel to control the elevator.



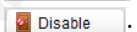
Open Door: The floor button will be valid for a period of time.



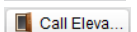
Controlled: You should swipe the card to press the selected floor button. And the elevator can go to the selected floor.



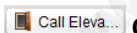
Free: The selected floor button will be valid all the time.



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 Log panel.

Notes:

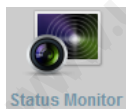
- The elevator cannot be controlled by other client software if the elevator status changes.
- Only one client software can control elevator each time.
- The client software which has controlled the elevator can receive the alarm information and the elevator status. Other client software cannot.

Status Duration Configuration

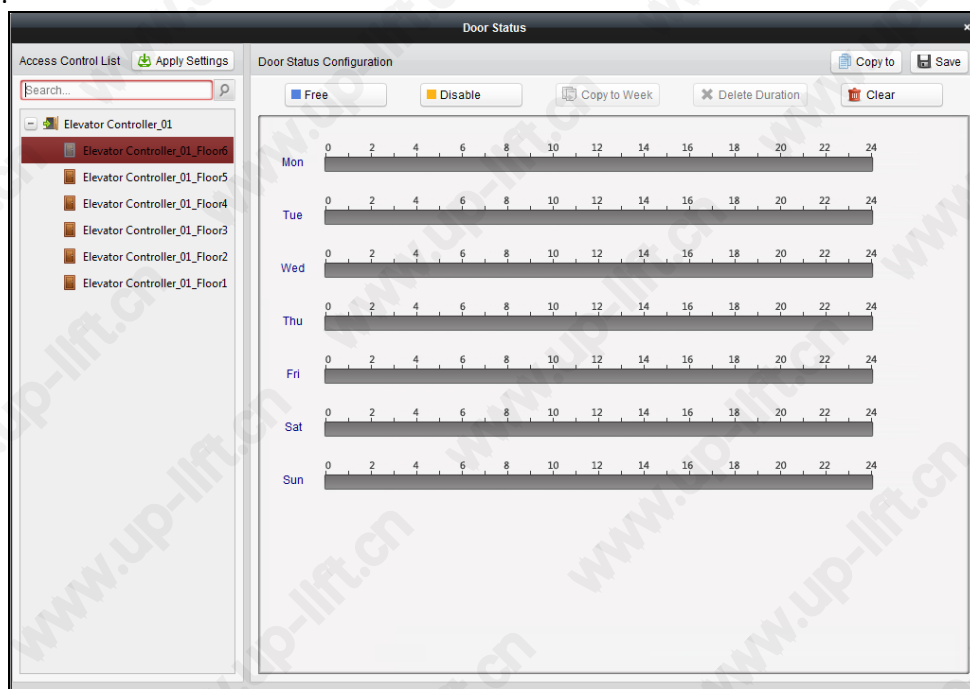
Purpose:

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

Steps:



1. Click **Status Monitor** icon on the control panel and click **Status Duration** button to enter the Status Duration interface.



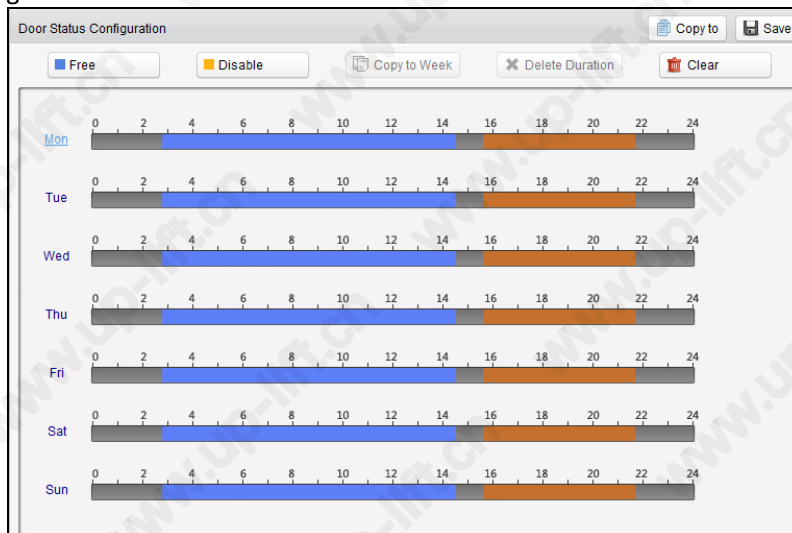
2. Click to select a floor from the access control list on the left of the pop-up window.
3. On the Door Status Configuration panel on the right, draw a schedule for the selected floor.

- 1) Select a door status brush as **Free** or **Disable**.


Free: The floor button will be free during the configured time period. The brush is marked as ■.


Disable: 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.



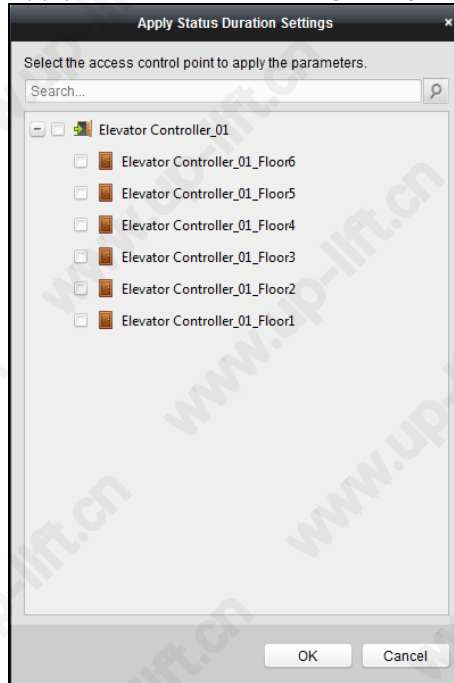
Note: The min. segment of the schedule is 30min.

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.

4. Optionally, you can select the schedule time bar and click **Copy to Week** to copy the time bar settings to the whole week.

5. 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.
6. Click **Save** to save the settings.
7. You can click **Copy to** button to copy the schedule to other doors.
8. Click **Apply Settings** to pop up the Apply Status Duration Setting dialog box.



9. Select a control point and click **OK** to apply the settings to access control point (floor).
Note: The door status duration settings will take effect after applying the settings to the access control point (floor).

7.13.2 Account Management

Purpose:

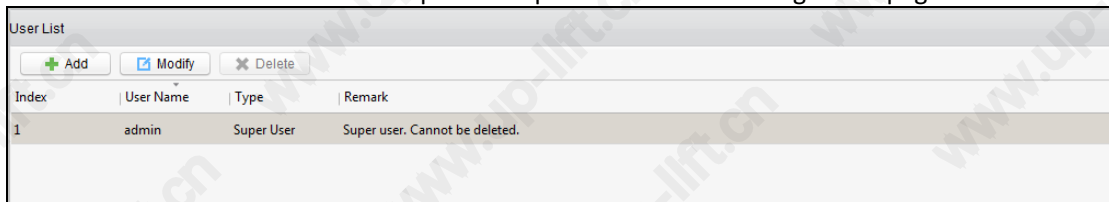
Multiple user accounts can be added to the client software, and you are allowed to assign different permissions for different users if needed.

Adding the User

Steps:



1. Click **Account Management** icon on the control panel to open the Account Management page.



Note: The user account you registered to log in to the software is set as the super user.

2. Open the Account Management page.
3. Click **Add** to open the Add User dialog box.

4. Input the user name, password and confirm password as desired. The software will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.
5. Check the checkboxes to assign the permissions for the created user.
6. Click **OK** to save the settings.

Note: Up to 16 user accounts can be added to the client.



- ◆ A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 8 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.

Managing the User

Purpose:

After created successfully, the user account is added to the user list on the Account Management page. You can edit or delete the information of the user accounts.

To edit the information of the user, select the user from the list, and click **Modify**.

To delete the information of the user, select the user from the list, and click **Delete**.

Note: The super user cannot be deleted and its permission cannot be modified.

7.13.3 Event and Alarm Management

Purpose:

In this section, you are able to check the real-time events and alarms, and view the event report of the access control point.

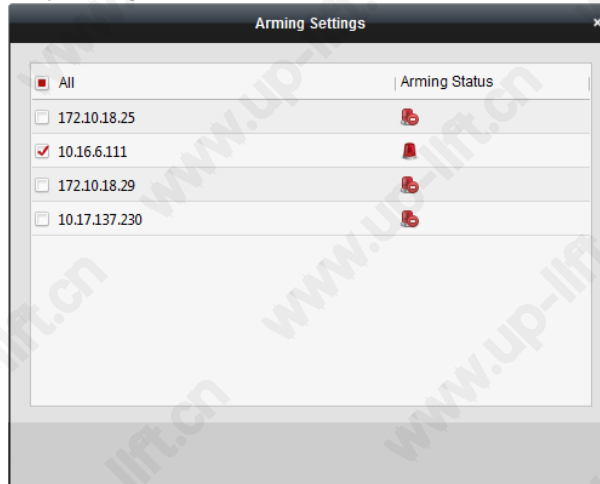
Real-Time Access Control Event and Alarm

Purpose:

You can view the real-time alarm and event information received by the client.



Before you start:

Before you can receive the alarm information from the device, you need to click **Tool -> Arming Settings** and arm the device by checking the corresponding checkbox.



Note: The device will be armed by default after being added to the client.

After enabling the arming control of the access control device, the client can receive the alarms and events once triggered.

Click the icon  in Alarms and Events Toolbar to show the Alarms and Events panel. Or click  to display the Alarm Event interface.



You can view real-time access event (such as swiping to open the door, unrecognized card number, duration group error, etc.) information and other operation events in Alarm Event interface.

Note: If you cannot receive the event and alarm information of the access control device, you can check the arming status of the device in **Tool -> Arming Settings**.

Alarm Information								
Serial No.	Event Type	Card Holder	Card Type	Card No.	Event Time	Event Source	Capture	Direction
20	No card No.			2929558121	2016-08-19 13:5...	10.16.6.138_Entrance Card Reader1		Enter
19	No card No.			0916181063	2016-08-19 13:5...	10.16.6.138_Entrance Card Reader1		Enter
18	No card No.			45321	2016-08-19 13:5...	10.16.6.138_Entrance Card Reader1		Enter
17	No card No.			1234	2016-08-19 13:5...	10.16.6.138_Entrance Card Reader1		Enter
16	Remotely Arming				2016-08-19 13:0...	10.16.6.138		
15	Remotely Login				2016-08-19 13:0...	10.16.6.138		
14	Device Tampering ...				2016-08-19 13:0...	10.16.6.138		
13	External Power Sup...				2016-08-19 13:0...	10.16.6.138		
12	Device Tampering ...				2016-08-04 09:5...	10.16.6.138		
11	External Power Sup...				2016-08-04 09:5...	10.16.6.138		

You can click the card swiping event to view the card holder information.

You can click to view the captured alarm pictures if the storage server is configured. For configuring the storage server, please refer to *Section 7.3.4 Storage Server Configuration*.

Event Management


Purpose:


You can search historical access event according to the search conditions (such as event type, name of the person, card No. or start/end time).



Click **Event Management** icon on the control panel to enter the interface.

Return on the control panel to enter the information.

Event Type: Start Time: 

Card Holder Name: End Time: 


Card No.: Card Type:

Search Result

Serial ...	Event Type	Card Holder	Card Type	Card No.	Event Time	Event Source	Capture

Total:0 Page:1/1

Card Holder Information



Person No.:

Name:

Gender:

ID Type:

ID No.:

Department:

Phone No.:

Address:

Steps:

1. Enter the search condition (event type/card holder /card No./start & end time).
2. Click **Search** to get the search results.
3. View the event information in the event list.

- Click an event to view the information of the card holder on the **Card Holder Information** panel on the left side of the page.
- You can click **Export** button to export the search results to the local PC.

7.13.4 Log Management

Purpose:

The log files of the Access Control Client and the devices that connected to the Access Control Client can be searched for checking.



Click **Log Search** icon on the control panel to open the Log Search page.

Search Condition		Search Result																																																																																			
Log Type: <input checked="" type="radio"/> Configuration Log <input type="radio"/> Control Log Operation Type: All Start Time: 2016-03-19 00:00:00 End Time: 2016-03-21 23:59:59 <input type="button" value="Search"/>		<div style="text-align: right;"><input type="button" value="Export"/></div> <table border="1"> <thead> <tr> <th>Serial No.</th> <th>Operation Type</th> <th>Time</th> <th>Content</th> </tr> </thead> <tbody> <tr><td>5</td><td>Data Import/Export</td><td>2016-03-21 11:10:02</td><td>Export Person</td></tr> <tr><td>6</td><td>Data Import/Export</td><td>2016-03-21 10:25:19</td><td>Export Person and Card Information.</td></tr> <tr><td>7</td><td>Data Import/Export</td><td>2016-03-21 10:20:14</td><td>Export Person and Card Information.</td></tr> <tr><td>8</td><td>Login</td><td>2016-03-21 09:39:56</td><td>User Login</td></tr> <tr><td>9</td><td>Login</td><td>2016-03-20 18:06:20</td><td>Logout</td></tr> <tr><td>10</td><td>Data Import/Export</td><td>2016-03-20 18:02:23</td><td>Export Person and Card Information.</td></tr> <tr><td>11</td><td>Login</td><td>2016-03-20 15:06:52</td><td>User Login</td></tr> <tr><td>12</td><td>Login</td><td>2016-03-20 15:04:43</td><td>Logout</td></tr> <tr><td>13</td><td>Man-Hour Shift</td><td>2016-03-20 12:48:21</td><td>Add Man-Hour Attendance Shift:man</td></tr> <tr><td>14</td><td>Normal Shift</td><td>2016-03-20 12:15:52</td><td>Add Normal Attendance Shift:00111</td></tr> <tr><td>15</td><td>Attendance Rule</td><td>2016-03-20 12:15:28</td><td>Add Normal Shift Attendance Rule:1212</td></tr> <tr><td>16</td><td>Password Authentication</td><td>2016-03-20 11:51:31</td><td>Download Password Authentication</td></tr> <tr><td>17</td><td>Password Authentication</td><td>2016-03-20 11:51:27</td><td>Add Password Authentication:12373</td></tr> <tr><td>18</td><td>Card Reader Authentication</td><td>2016-03-20 11:51:11</td><td>Save Card Reader Permission</td></tr> <tr><td>19</td><td>Card Reader Authentication</td><td>2016-03-20 11:51:02</td><td>Card reader authentication downloading operation</td></tr> <tr><td>20</td><td>Card Reader Authentication</td><td>2016-03-20 11:50:55</td><td>Copied the card reader authentication</td></tr> <tr><td>21</td><td>Login</td><td>2016-03-20 11:29:21</td><td>User Login</td></tr> <tr><td>22</td><td>Login</td><td>2016-03-20 11:28:19</td><td>Logout</td></tr> <tr><td>23</td><td>Login</td><td>2016-03-20 11:24:50</td><td>User Login</td></tr> </tbody> </table>				Serial No.	Operation Type	Time	Content	5	Data Import/Export	2016-03-21 11:10:02	Export Person	6	Data Import/Export	2016-03-21 10:25:19	Export Person and Card Information.	7	Data Import/Export	2016-03-21 10:20:14	Export Person and Card Information.	8	Login	2016-03-21 09:39:56	User Login	9	Login	2016-03-20 18:06:20	Logout	10	Data Import/Export	2016-03-20 18:02:23	Export Person and Card Information.	11	Login	2016-03-20 15:06:52	User Login	12	Login	2016-03-20 15:04:43	Logout	13	Man-Hour Shift	2016-03-20 12:48:21	Add Man-Hour Attendance Shift:man	14	Normal Shift	2016-03-20 12:15:52	Add Normal Attendance Shift:00111	15	Attendance Rule	2016-03-20 12:15:28	Add Normal Shift Attendance Rule:1212	16	Password Authentication	2016-03-20 11:51:31	Download Password Authentication	17	Password Authentication	2016-03-20 11:51:27	Add Password Authentication:12373	18	Card Reader Authentication	2016-03-20 11:51:11	Save Card Reader Permission	19	Card Reader Authentication	2016-03-20 11:51:02	Card reader authentication downloading operation	20	Card Reader Authentication	2016-03-20 11:50:55	Copied the card reader authentication	21	Login	2016-03-20 11:29:21	User Login	22	Login	2016-03-20 11:28:19	Logout	23	Login	2016-03-20 11:24:50	User Login
Serial No.	Operation Type	Time	Content																																																																																		
5	Data Import/Export	2016-03-21 11:10:02	Export Person																																																																																		
6	Data Import/Export	2016-03-21 10:25:19	Export Person and Card Information.																																																																																		
7	Data Import/Export	2016-03-21 10:20:14	Export Person and Card Information.																																																																																		
8	Login	2016-03-21 09:39:56	User Login																																																																																		
9	Login	2016-03-20 18:06:20	Logout																																																																																		
10	Data Import/Export	2016-03-20 18:02:23	Export Person and Card Information.																																																																																		
11	Login	2016-03-20 15:06:52	User Login																																																																																		
12	Login	2016-03-20 15:04:43	Logout																																																																																		
13	Man-Hour Shift	2016-03-20 12:48:21	Add Man-Hour Attendance Shift:man																																																																																		
14	Normal Shift	2016-03-20 12:15:52	Add Normal Attendance Shift:00111																																																																																		
15	Attendance Rule	2016-03-20 12:15:28	Add Normal Shift Attendance Rule:1212																																																																																		
16	Password Authentication	2016-03-20 11:51:31	Download Password Authentication																																																																																		
17	Password Authentication	2016-03-20 11:51:27	Add Password Authentication:12373																																																																																		
18	Card Reader Authentication	2016-03-20 11:51:11	Save Card Reader Permission																																																																																		
19	Card Reader Authentication	2016-03-20 11:51:02	Card reader authentication downloading operation																																																																																		
20	Card Reader Authentication	2016-03-20 11:50:55	Copied the card reader authentication																																																																																		
21	Login	2016-03-20 11:29:21	User Login																																																																																		
22	Login	2016-03-20 11:28:19	Logout																																																																																		
23	Login	2016-03-20 11:24:50	User Login																																																																																		
Total:23 Page:1/1		<div> <input type="button" value="First"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Last"/> </div> Page <input type="text" value="1"/> Go to <input type="button" value="Go"/>																																																																																			

Searching Configuration Logs

Purpose:

The operation logs via the Access Control Client can be searched by time.

Steps:



- Click **Log Search** icon on the control panel to open the Log Search page.

Serial No.	Operation Type	Time	Content
5	Data Import/Export	2016-03-21 11:10:02	Export Person
6	Data Import/Export	2016-03-21 10:25:19	Export Person and Card Information.
7	Data Import/Export	2016-03-21 10:20:14	Export Person and Card Information.
8	Login	2016-03-21 09:39:56	User Login
9	Login	2016-03-20 18:06:20	Logout
10	Data Import/Export	2016-03-20 18:02:23	Export Person and Card Information.
11	Login	2016-03-20 15:06:52	User Login
12	Login	2016-03-20 15:04:43	Logout
13	Man-Hour Shift	2016-03-20 12:48:21	Add Man-Hour Attendance Shift:man
14	Normal Shift	2016-03-20 12:15:52	Add Normal Attendance Shift:00111
15	Attendance Rule	2016-03-20 12:15:28	Add Normal Shift Attendance Rule:1212
16	Password Authentication	2016-03-20 11:51:31	Download Password Authentication
17	Password Authentication	2016-03-20 11:51:27	Add Password Authentication:12373
18	Card Reader Authentication	2016-03-20 11:51:11	Save Card Reader Permission
19	Card Reader Authentication	2016-03-20 11:51:02	Card reader authentication downloading operation
20	Card Reader Authentication	2016-03-20 11:50:55	Copied the card reader authentication
21	Login	2016-03-20 11:29:21	User Login
22	Login	2016-03-20 11:28:19	Logout
23	Login	2016-03-20 11:24:50	User Login

- Open the Log Search page.
- Select the radio button of Configuration Logs.
- Select the Operation Type of log files. For configuration log, the operation type includes department management, card management, access control permission configuration, etc..
- Click to specify the start time and end time.
- Click **Search**. The matched log files will display on the right.
You can check the operation time, log type and other information of the logs.
- You can click **Export** to export the search result to the local PC.

Note: Please narrow the search condition if there are too many log files.

Searching Control Logs

Purpose:

The logs of controlling access control point via the client can be searched by time.

Steps:

- Open the Log Search page.
- Select the radio button of Control Logs.
- Select the Operation Type of log files. For control log, the operation type includes opening door, closing door, remaining open, remaining closed, and capture.
- Click to specify the start time and end time.
- Click **Search**. The matched log files will display on the right.
You can check the operation time, log type and other information of the logs.
- You can click **Export** to export the search result to the local PC.

Note: Please narrow the search condition if there are too many log files.

7.13.5 People Counting Statistics

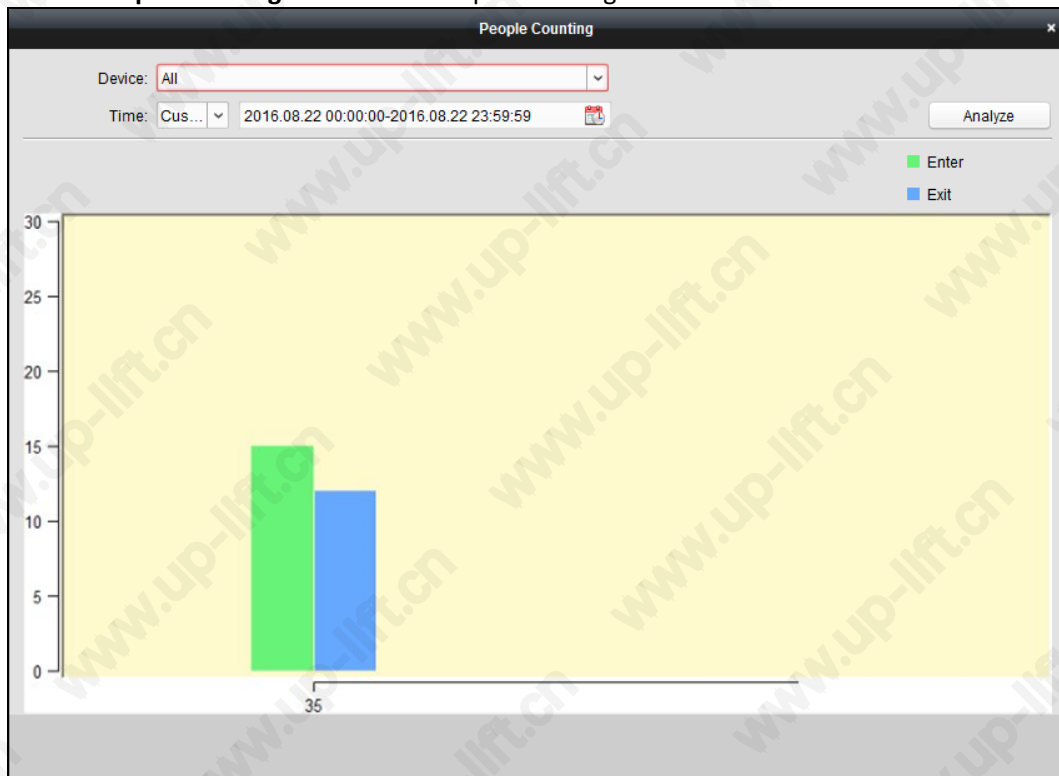
Purpose:

You can view the people amount of entering and exiting of the added access control device(s) and the data can

be displayed in histogram.

Steps:

1. Click **Tool** -> **People Counting** to enter the People Counting interface as follows.



2. In the device field, check to select the access control device for people counting.
Note: Up to eight access control devices can be selected for people counting statistics at the same time.
3. Set the time period for the statistics.
 - For setting the time period as **Daily**, you can click to select the date for people counting.
 - For setting the time period as **Weekly**, you can click to select the date, and person during the week of that date can be counted for people counting.
 - For setting the time period as **Monthly**, you can click to select the month for people counting.
 - For setting the time period as **Annually**, you can click to select the year for people counting.
 - For setting the time period as **Custom**, you can click to set the start time and end time for people counting.
4. Click **Analyze** to display the statistics.

7.13.6 System Maintenance

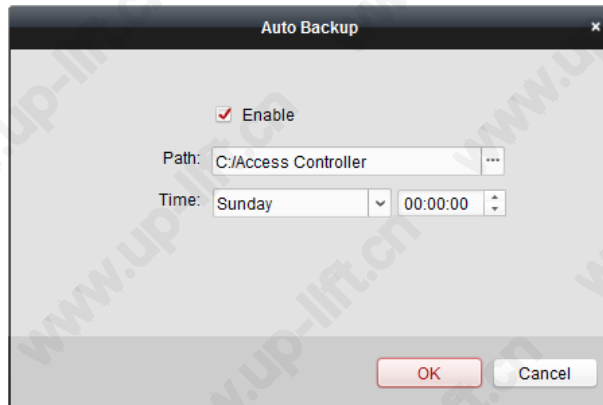
Auto Backup Settings

Purpose:

You can set to enable the auto backup function to back up the client database automatically such as person, attendance data, permission data, etc.

Steps:

1. Click **System** -> **Auto Backup** to open the Auto Backup window as follows.

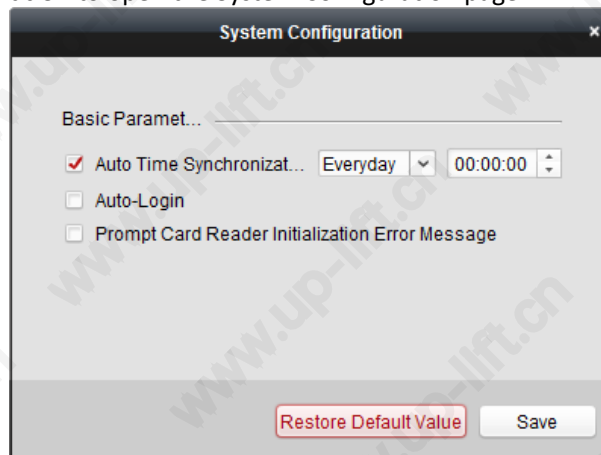


2. Check the **Enable** checkbox to enable the Auto Backup function.
3. Click to set the path for saving the backed file.
4. Set the date and time for backing up the database.
5. Click **OK** to save the settings.

System Configuration

Steps:

1. Click **Tool->System Configuration** to open the System Configuration page.



2. Check the checkbox to enable Automatic Time Synchronization.
The Automatic Time Synchronization can operate auto time adjustment to all access control devices added to the Access Control Client according to specified period and time.
Select the matched day and input the time to operate the time adjustment.
3. You can check the checkbox to enable auto-login.
4. You can click the checkbox to enable the message prompt when the card reader initialization is error.
5. Click **Save** button to save the settings.

Note: You can click **Restore Default Value** button to restore the defaults of the general settings.

Chapter 8 Appendix

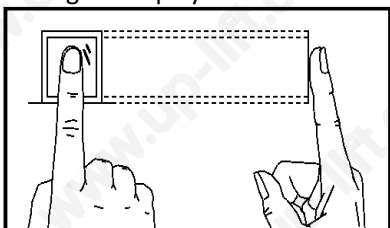
8.1 Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

The figure displayed below is the correct way to scan your finger:

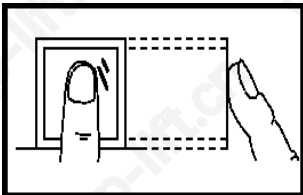


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

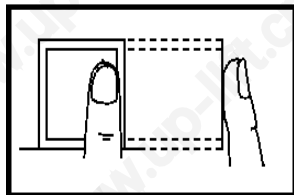
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

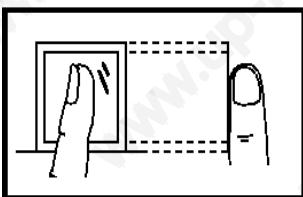
Vertical



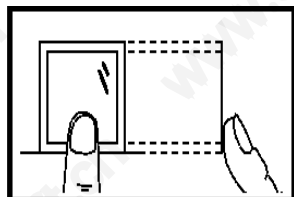
Edge I



Side



Edge II



Environment

The scanner should avoid direct high light, high temperature, humid conditions and rain.

When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again after drying the finger.

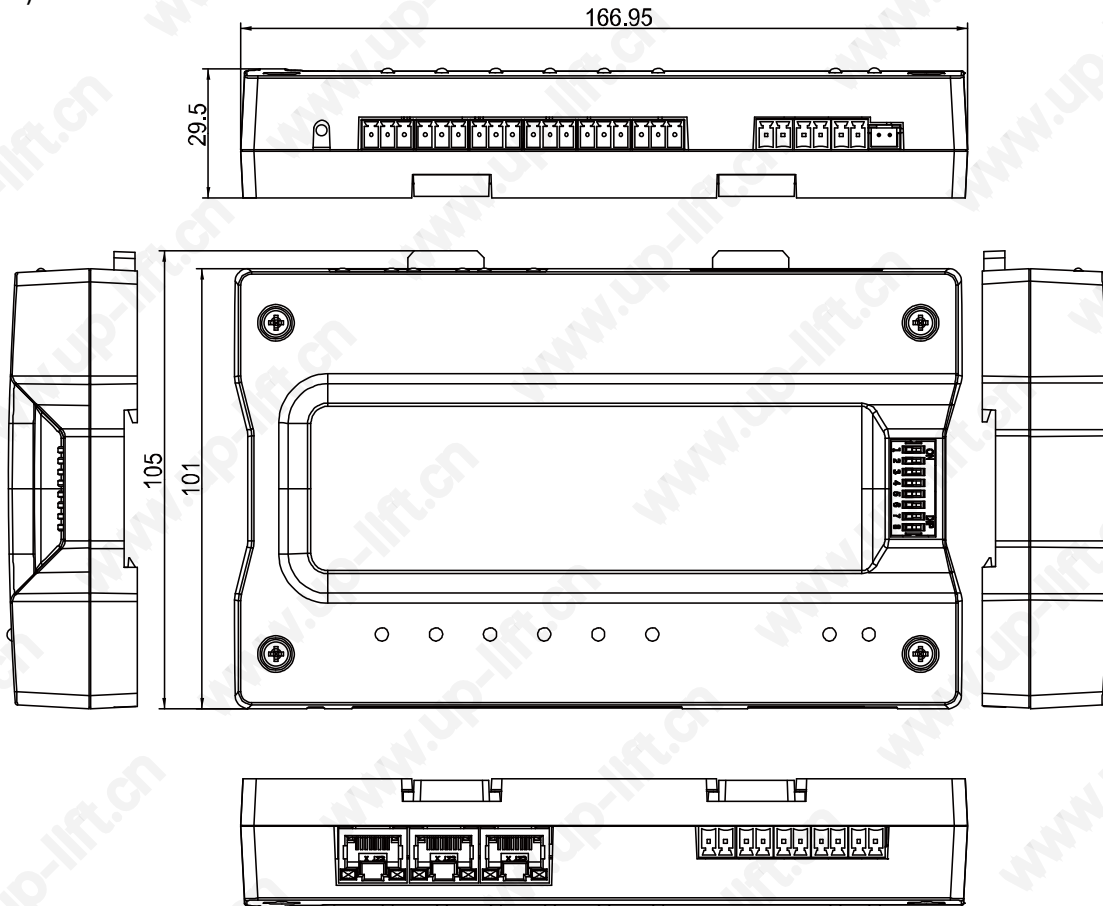
Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

8.2 Device Dimension

The device dimension is shown as follows:
(Unit:mm)



8.3 Access Controller Model List

The client software supports the access controller in the following list:

Available Access Controller Model
DS-K2601
DS-K2602
DS-K2604
DS-K2601-G
DS-K2602-G
DS-K2604-G
DS-GJZA6201
DS-GJZA6202
DS-GJZA6204
DS-K2110-DK
DS-K2110-2DK
DS-K2110-4DK
DS-K1T200EF/MF/CF
DS-K1T200EF/MF/CF-C
DS-K1T300EF/MF/CF
DS-K1T300EF/MF/CF-C
DS-K1T105E/M/C
DS-K1T105E/M/C-C
DS-K2210（梯控主机）
DS-K2202（梯控定制主机）

0100001070116