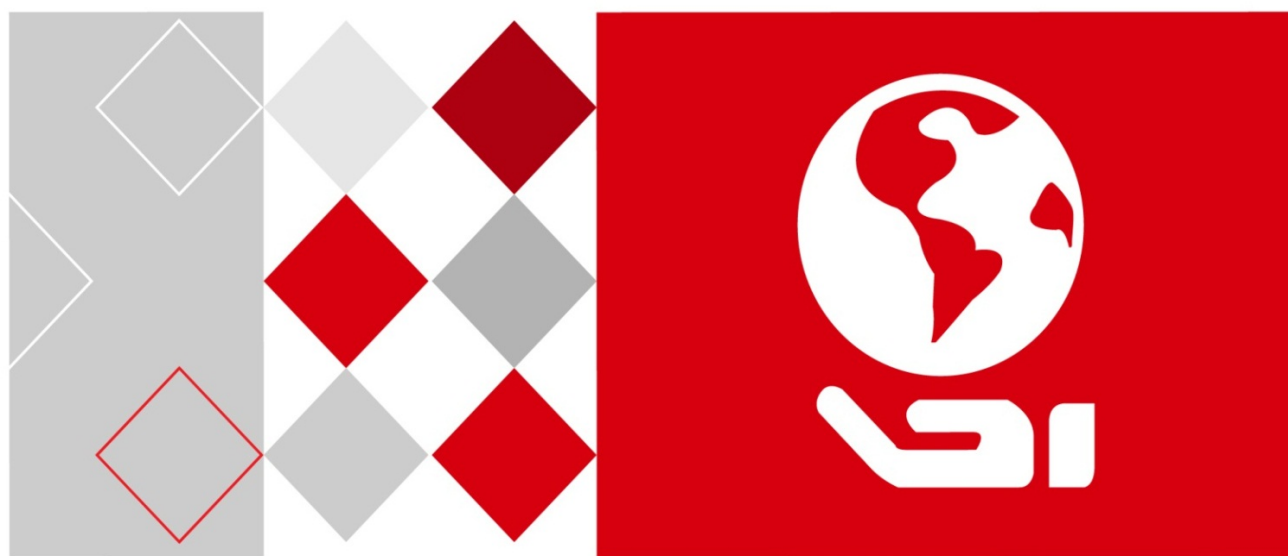


---

**HIKVISION**



CORPORATION

**Elevator Controller**

**Ness User Manual**

*Ness Version 1.0*



## **User Manual**

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

Name	Model
Master Elevator Controller	DS-K2210 (Ness Part No. 104-064A)
Distributed Elevator Controller	DS-K2M0016 – Ness Part No. 104-064B

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.

Modifications have been made to this manual by Ness Corporation Australia to suit the Australian market and to assist in Ness customers understanding the product easier.

### **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](http://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](http://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.

	
<b>Warnings</b> Follow these safeguards to prevent serious injury or death.	<b>Cautions</b> 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.

# Contents

<b>Chapter 1</b>	<b>Overview</b> .....	<b>1</b>
1.1	Introduction .....	1
1.2	Main Features .....	1
	<b>Appearance Master Controller</b> .....	<b>2</b>
	Device Appearance .....	2
	Indicator Information .....	3
	Installation Master Controller .....	4
	Device Wiring Master Controller .....	5
	<b>Appearance Distributed Controller</b> .....	<b>7</b>
	Device Appearance .....	7
	Indicator Information .....	8
	<b>Installation Distributed Controller</b> .....	<b>8</b>
	<b>Device Wiring Distributed Controller</b> .....	<b>9</b>
<b>Chapter 2</b>	<b>Activation</b> .....	<b>12</b>
2.1	Activating Device via Web Client .....	12
2.2	Activating Device via SADP Tool .....	13
2.3	Activating Device via Client Software .....	15
<b>Chapter 3</b>	<b>Web Client Operation</b> .....	<b>17</b>
3.1	Overview .....	17
3.1.1	Introduction .....	17
3.2	Login/Logout Web Client .....	17
3.2.1	Login .....	17
3.2.2	Logout .....	18
3.3	Setting Device via Web Client .....	18
3.3.3	System Settings .....	18
3.3.4	Network Settings .....	20
3.3.5	System Maintenance .....	21
3.3.6	Elevator Control Settings .....	22
<b>Chapter 4</b>	<b>Client Operation</b> .....	<b>26</b>
4.1	Overview of iVMS-4200 Client Software .....	26
4.1.1	Description .....	26
4.1.2	Running Environment .....	26
4.1.3	Client Performance .....	26
4.2	User Registration and Login .....	27
4.2.1	User Registration .....	27
4.2.2	Login .....	27
4.2.3	Function Modules .....	28
4.3	Basic Configuration .....	31
7.3.1	Work Flow .....	31
4.4	Device Management .....	31
4.4.1	Access Control Device Management .....	31
4.4.2	Door Group Management .....	36
4.4.3	Editing Access Control Device .....	39
4.4.4	Deleting Device .....	42

4.4.5	<u>Time Synchronization</u> .....	42
4.4.6	<u>Viewing Device Status</u> .....	43
4.4.7	<u>Remote Configuration</u> .....	43
4.5	<b>Person Management</b> .....	<b>52</b>
4.5.1	<u>Organisation Management</u> .....	52
4.5.2	<u>Person Management</u> .....	53
4.6	<u>Card Management (Adding Card / Person)</u> .....	53
4.6.1	<u>Empty Card (Adding Person / Access Level)</u> .....	55
4.6.2	<u>Adding Card</u> .....	56
4.6.3	<u>Adding Fingerprint</u> .....	60
4.7	<u>Relay Management</u> .....	48
4.7.1	<u>Configuring Relay and Floor</u> .....	48
4.7.2	<u>Configuring Relay Type</u> .....	50
	<b>Schedule Template</b> .....	<b>67</b>
	<u>Week Schedule</u> .....	67
	<u>Holiday Group</u> .....	69
	<u>Schedule Template</u> .....	70
4.8	<u>Permission Configuration</u> .....	75
	<u>Adding Permission</u> .....	75
	<u>Applying Permission</u> .....	76
4.9	<u>Advanced Functions</u> .....	77
4.9.1	<u>Card Type</u> .....	77
4.9.2	<u>Card Reader Authentication</u> .....	80
4.9.3	<u>Open Door with First Card</u> .....	86
	<b>Door / Floor Status Management</b> .....	<b>91</b>
	<b>Status Duration Configuration (Auto Unlocking of Floors)</b> .....	<b>92</b>
	<b>Appendix</b> .....	<b>94</b>
	<u>Tips for Scanning Fingerprint</u> .....	94
	<u>Device Dimension</u> .....	95
	<u>Access Controller Model List</u> .....	96

---

# Chapter 1 Overview

## 1.1 Introduction

The elevator control Interface is designed to interface between Access Control System and / or Video Intercom system and the building elevators.

It consists of two parts.

1. Master Elevator Controller (DS-K2210A – Ness Part No 104-064), one required per lift car and
2. Distributed Elevator Controller (DS-K2M0016A – Ness Part No. 104-064B). Each Distributed Elevator Controller can manage 16 Floors. Up to 8 Distributed Elevator Controller can be connected to each Master Elevator Controller, therefore supporting up to 128 floors.

Card readers are connected to the Master Elevator Controller via RS485 or via Wiegand data. 2 Card readers can connect to each Master Elevator Controller.

You can control the master elevator controller by the web client and iVMS-4200 client software.

It requires iVMS4200 Client Software to program.

## 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.

# Master Controller

## 1.3 Device Appearance Introduction

The device appearance introduction is shown as follows:

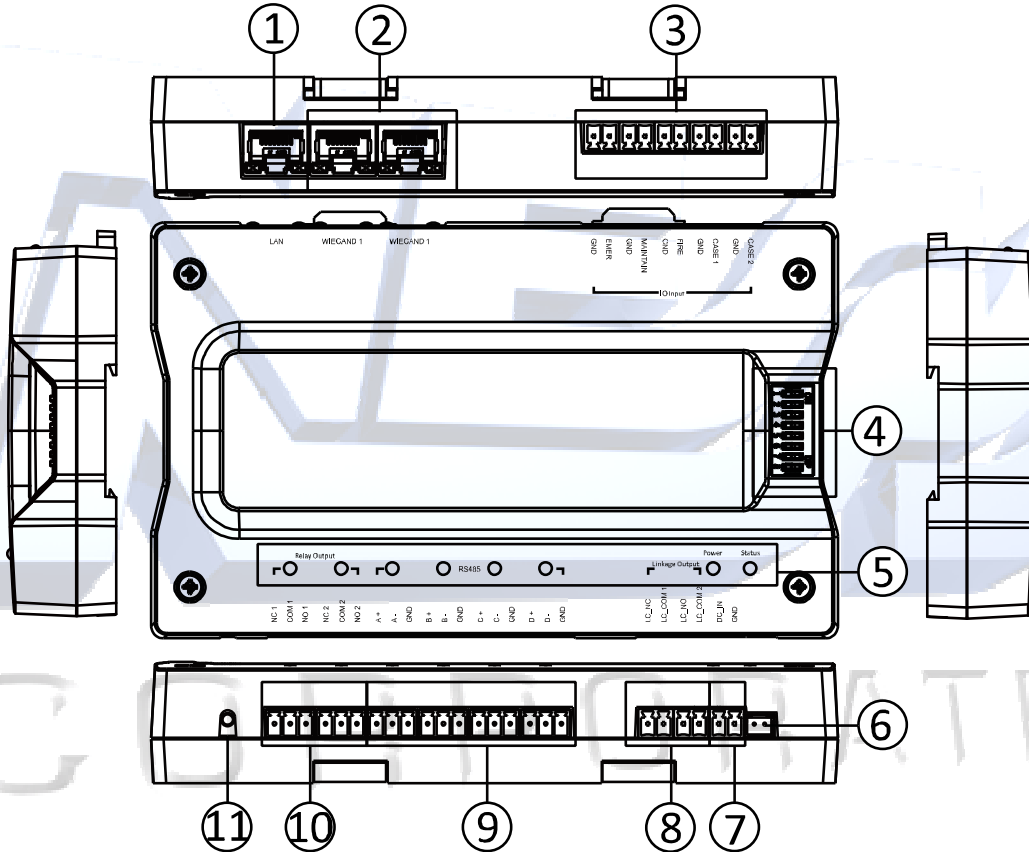


Table 1. 1 Device Appearance Description

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



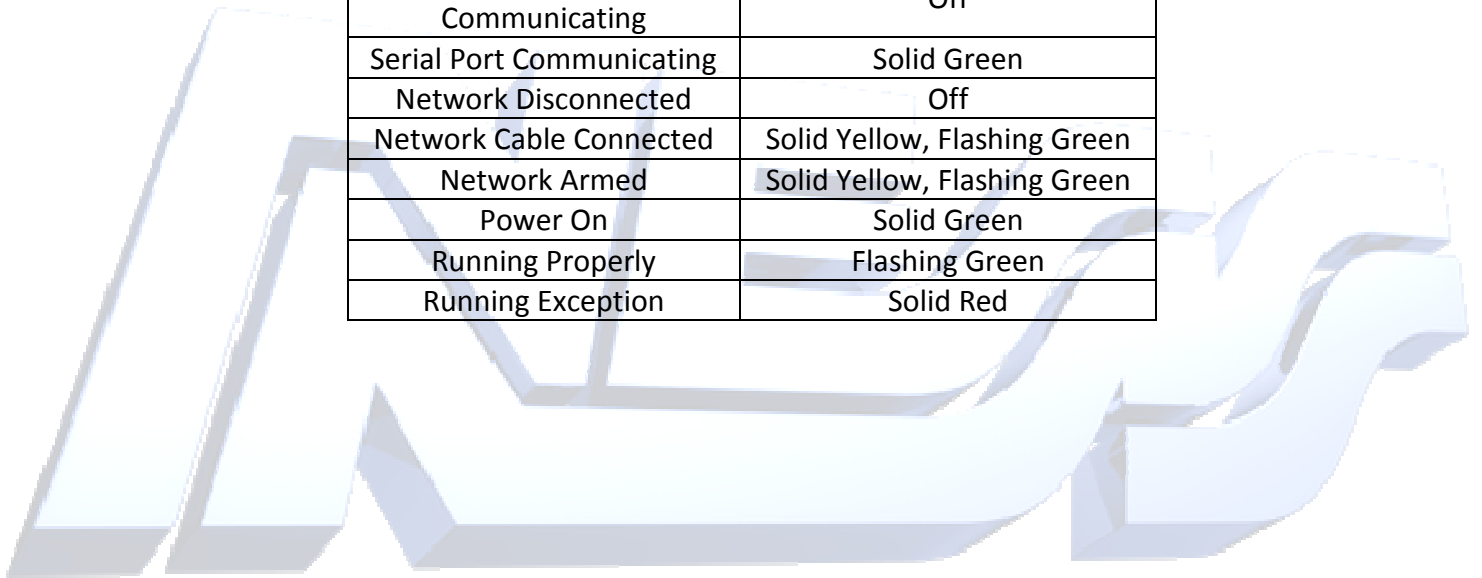
---

## 1.4 Indicator Information

The indicator information is as follows:

Table 1. 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



C O R P O R A T I O N

---

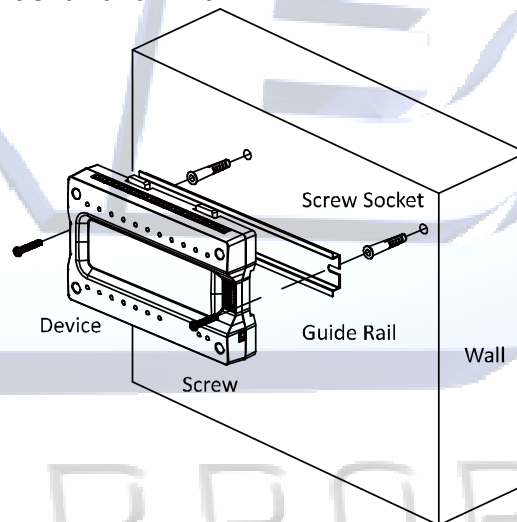
# Installation – Master Controller

## ***Before your start:***

- The controllers mount via a DIN / Guide Rail (Supplied)
- The minimum bearing weight of the wall or other places should be three times heavier than the device weight.
- Check before you installing.

## ***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.

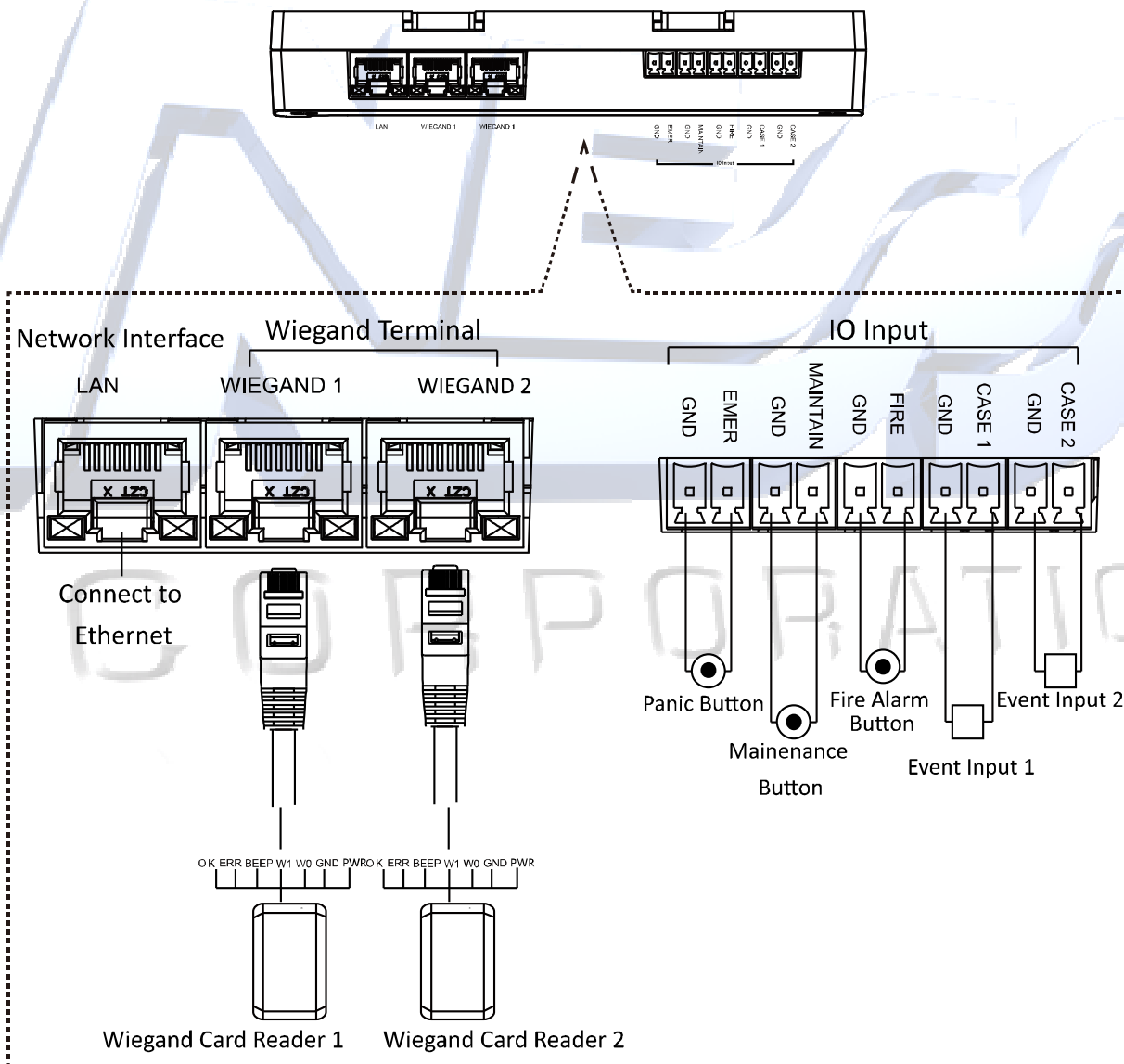


# Device Wiring – Master Controller

## Master Controller

When the panic button, the maintenance button, fire alarm button, and the event alarm(s) are triggered, or authorized Access card is presented to the lift card reader, the master elevator controller will control the distributed controller(s) to perform the linked actions via the linkage output.

The wiring of the device upper side is as follows:



**Notes:**

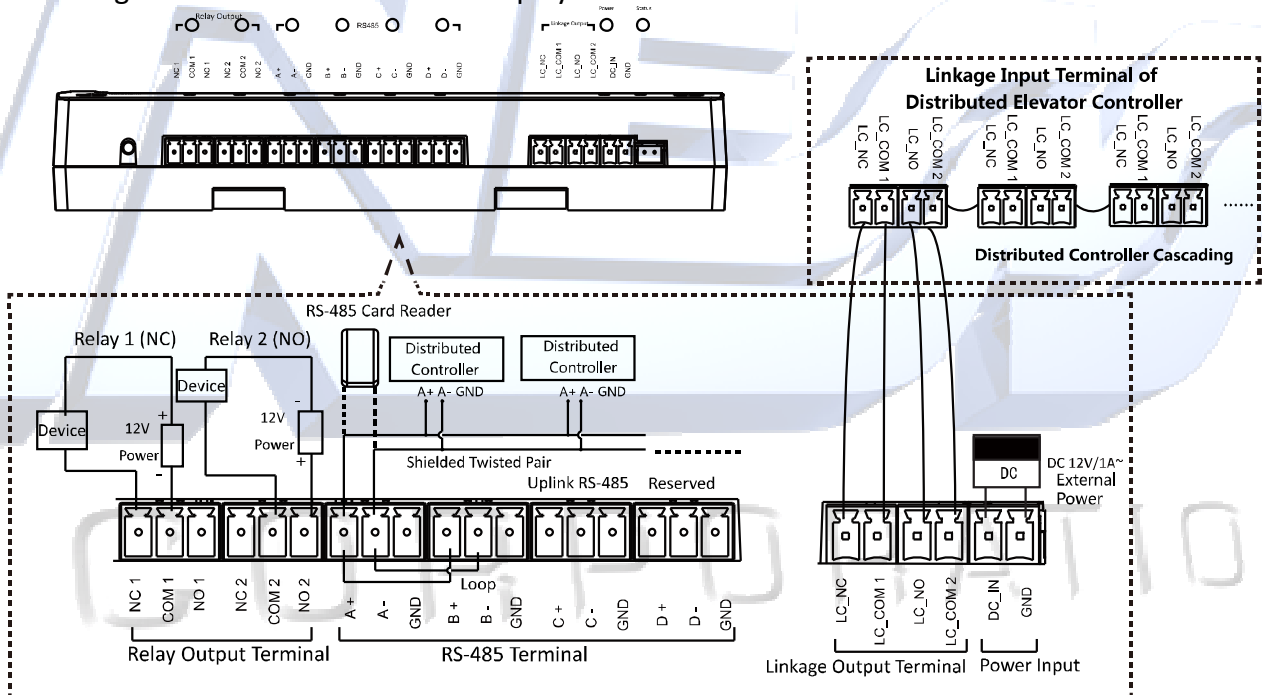
- When the panic / Emergency button is triggered, all relays will activate to grant access to all floors. In normal operation ‘Emer to Gnd’ is left open.
- When the fire alarm button (or maintenance button) is triggered, it locks out all floors from being activated. In normal operation ‘Fire to Gnd’ and ‘Maintain to Gnd’ are left open.

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.

**Note:** Make sure the following connections are made between the Master Elevator Controller and Distributed Controllers.

#### Connections.

1. RS485 Link.
2. Linkage Output Terminals of Master Controller to Linkage Input Terminals of the Distributed Controllers.

# Distributed Elevator Controller

## Main Features

- RS-485 communication with the master elevator controller.
- DIP switch settings for device address.
- Connectable with up to 16 relays to control the floor buttons in the elevator. Three types of relays are supported: Button Relay, Call Elevator Relay and Auto Button Relay.
- Remote control of the distributed elevator controlling via the web client, the iVMS-4200 client software, or other systems through the master elevator controller.
- Linkage of the master elevator controller to report the event to the system.

## Device Appearance Introduction

The device appearance introduction is shown as follows:

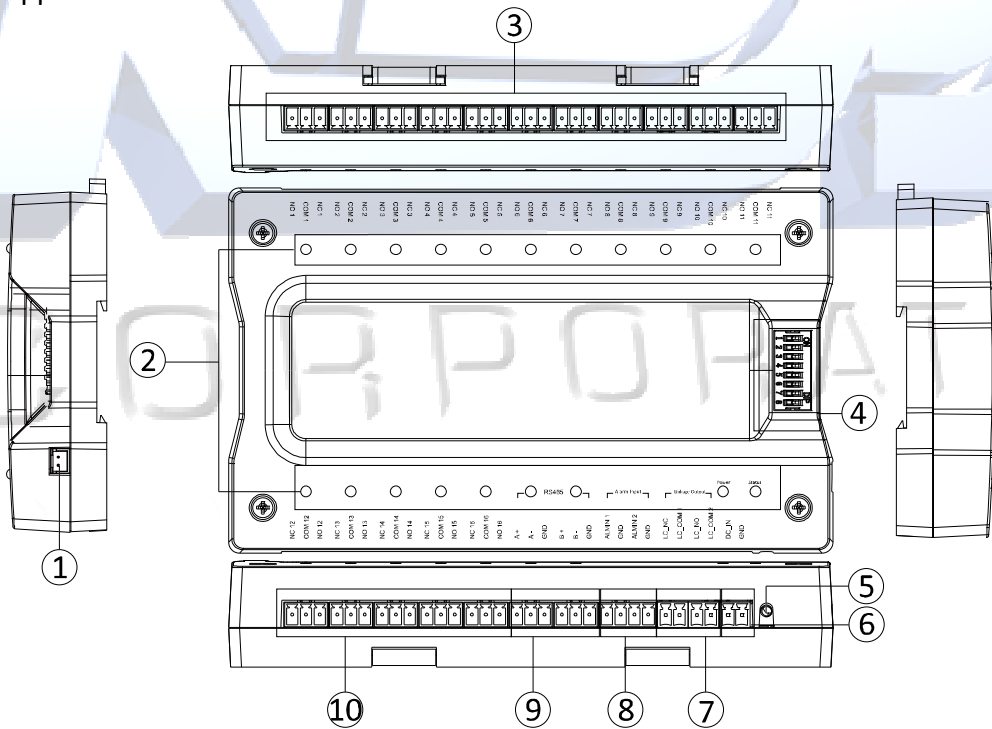


Table 1. 3 Device Appearance Description

No.	Description
1	Tamper-Proof Interface
2	Indicator
3	Relay Terminal
4	DIP Switch
5	GND Thread Interface

6	Power Input (12VDC)
7	Linkage Output Terminal
8	Alarm Input Terminal
9	RS-485 Terminal
10	Relay Terminal

## Indicator Introduction

The indicator information is as follows:

Table 1. 4 Indicator Description

Description	Indicator
Relay NC Closed	Off
Relay NO Closed	Solid Green
Serial Port Not Communicating	Off
Serial Port Communicating	Solid Green
Power On	Solid Green
Running Properly	Flashing Green
Running Exception	Solid Red

## 1.5 DIP Switch Introduction

The DIP Switches set the address of the Distributed Elevator Controllers, which therefore set what floors / outputs they will respond to from the Master Elevator Controller.

The DIP Switches on the Master Controllers are left to the OFF position.

The DIP Switches of the Distributed Elevator Controllers need to be set as per below.

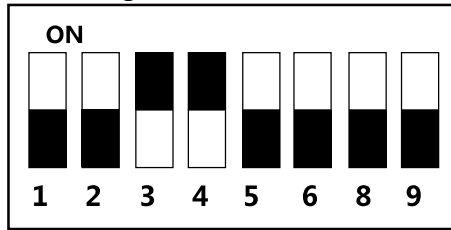
The DIP switch module is shown below. The No. of DIP switch from left to right is 1 to 8.



Table 1. 5 Description of DIP Switch

Icon	Description
	Represent 1 in binary mode
	Represent 0 in binary mode

For example, binary value of the following status is: 0011 0000.

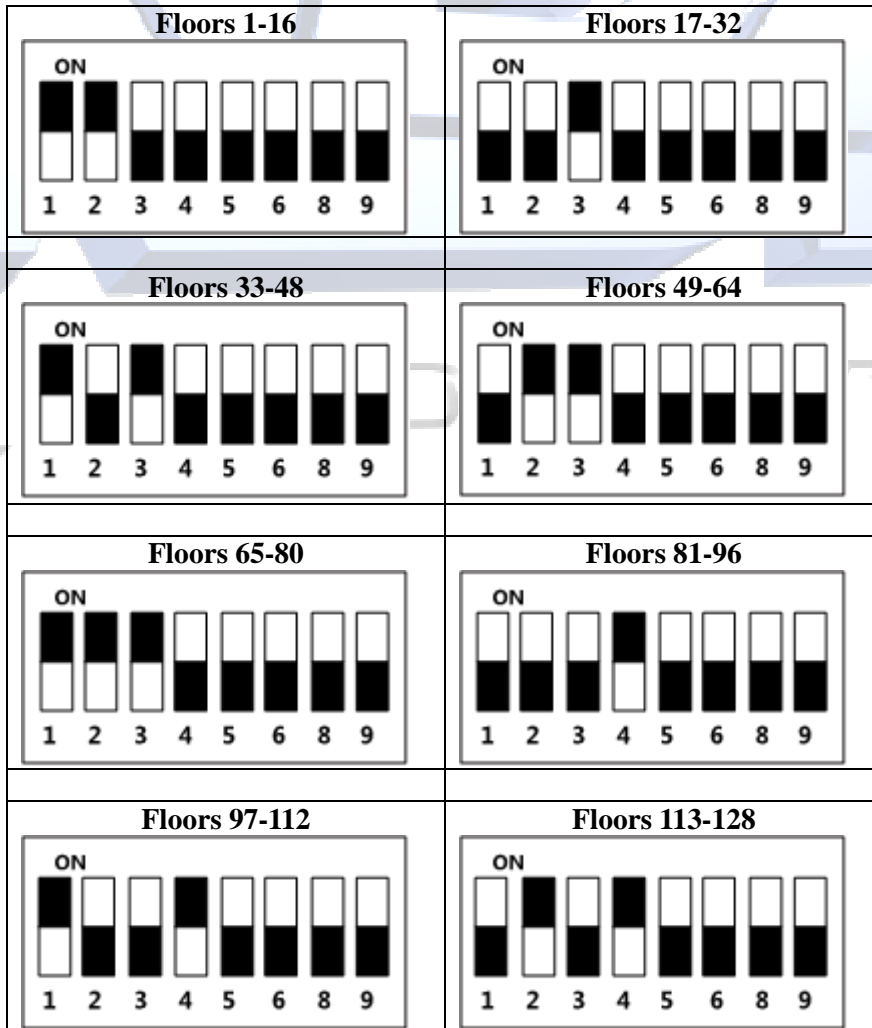


DIP Switch Module

Table 1. 6 Description of DIP Switch Address

No.	Description
1 to 6	Address of Distributed Elevator Controller
7	Reserved
8	NO/NC Status Reversal

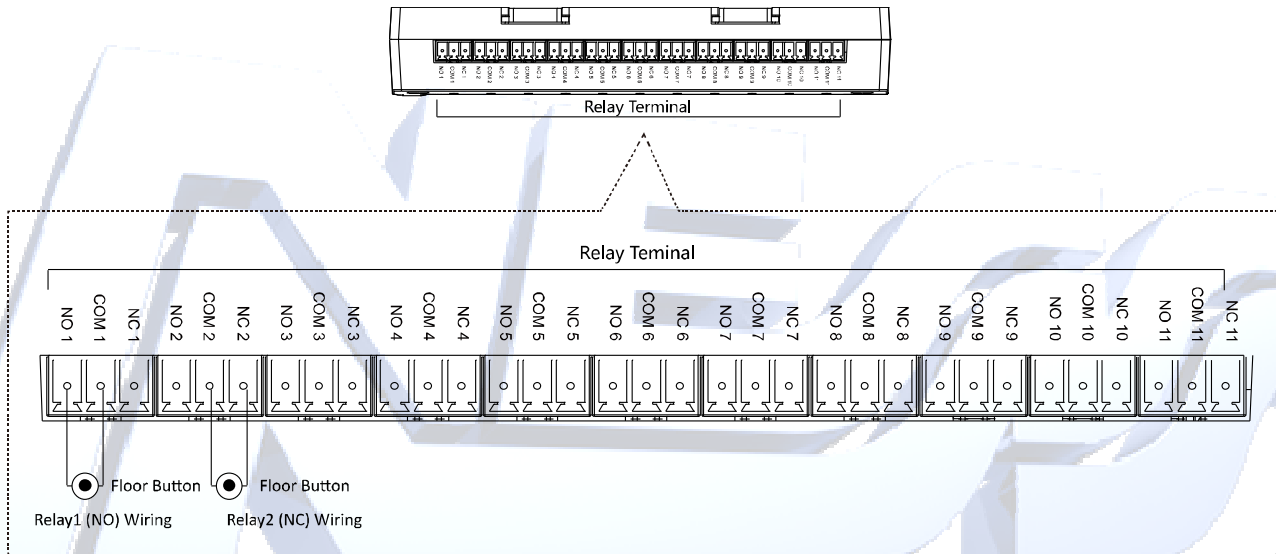
Distributed Controller DIP Switch settings for Floor Relay control



# Device Wiring – Distributed Controller

## Distributed Controller

The wiring of the device upper side is as follows:

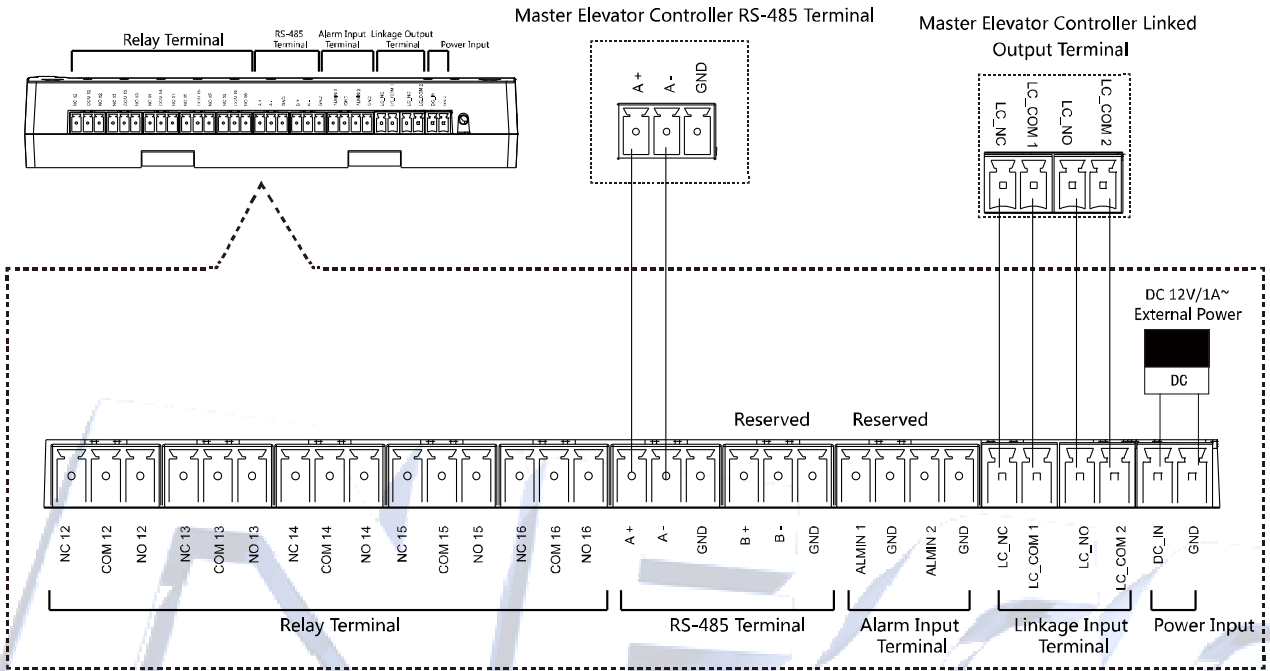


**Notes:**

- **Relay NO Wiring:** Wire the call elevator distributed controller and the call elevator relay, or wire the auto button distributed controller and the auto button relay to make sure the call elevator control and the auto button elevator control is invalid when powering off. The elevator will not stay between floors.
- **Relay NC Wiring:** Wire the button distributed controller and the button relay to make sure all buttons are valid when powering off.

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





**Notes:**

- Up to 16 relays can be connected.  
Relay No. = Distributed Controller Dial-up No. + Relay Serial No.

C O R P O R A T I O N

---

# Chapter 2 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.

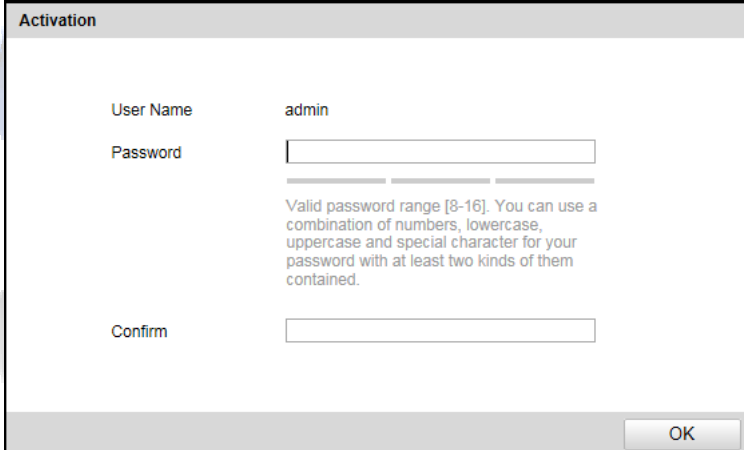
The default values of the terminal are as follows:

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

## 2.1 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.



Activation

User Name admin

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

OK

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.

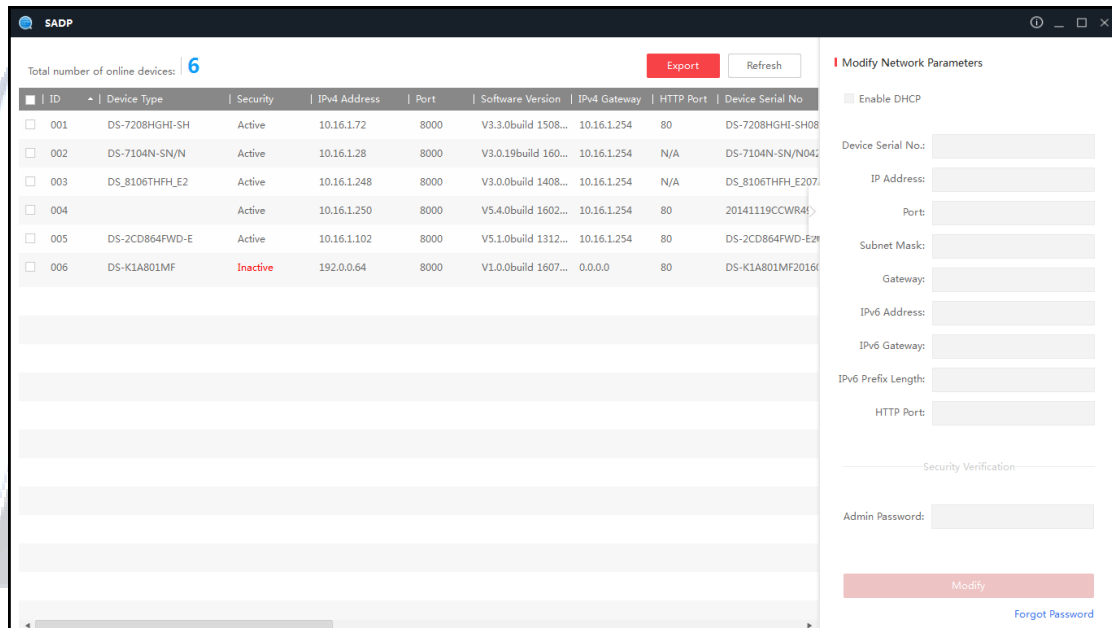
## 2.2 Activating Device via SADP Tool

### 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.



2. Check the inactive device from the device list.
3. 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.

SADP

Total number of online devices: **6** Export Refresh

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
<input type="checkbox"/>	001 DS-7208HGH-SH	Active	10.16.1.72	8000	V3.3.0build 1508...	10.16.1.254	80	DS-7208HGH-SH08
<input type="checkbox"/>	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
<input type="checkbox"/>	003 DS_8106THFH_E2	Active	10.16.1.248	8000	V3.0.0build 1408...	10.16.1.254	N/A	DS_8106THFH_E21
<input type="checkbox"/>	004 UNKOWN-DEVICE-TYPE	Active	10.16.1.250	8000	V5.4.0build 1602...	10.16.1.254	80	20141119CCWR45
<input type="checkbox"/>	005 DS-2CD864FWD-E	Active	10.16.1.102	8000	V5.1.0build 1312...	10.16.1.254	80	DS-2CD864FWD-E21
<input checked="" type="checkbox"/>	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**

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.

SADP

Total number of online devices: **6** Export Refresh

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
<input type="checkbox"/>	001 DS-7208HGH-SH	Active	10.16.1.72	8000	V3.3.0build 1508...	10.16.1.254	80	DS-7208HGH-SH08
<input type="checkbox"/>	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
<input type="checkbox"/>	003 UNKOWN-DEVICE-TYPE	Active	10.16.1.250	8000	V5.4.0build 1602...	10.16.1.254	80	20141119CCWR45
<input type="checkbox"/>	004 DS_8106THFH_E2	Active	10.16.1.248	8000	V3.0.0build 1408...	10.16.1.254	N/A	DS_8106THFH_E21
<input type="checkbox"/>	005 DS-2CD864FWD-E	Active	10.16.1.102	8000	V5.1.0build 1312...	10.16.1.254	80	DS-2CD864FWD-E21
<input checked="" type="checkbox"/>	006 DS-K1A801MF	Active	192.0.0.64	8000	V1.0.0build 1607...	0.0.0.0	80	DS-K1A801MF2016

**1. Check the device that need to edit.**

**2. Edit the device parameters.**

Modify Network Parameters

Enable DHCP

Device Serial No.: DS-K1A801MF20160713V010000C

IP Address: 192.0.0.64

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 64

HTTP Port: 80

Security Verification

Admin Password:

Modify

[Forgot Password](#)

**3. Input the password and click Modify to apply the settings.**

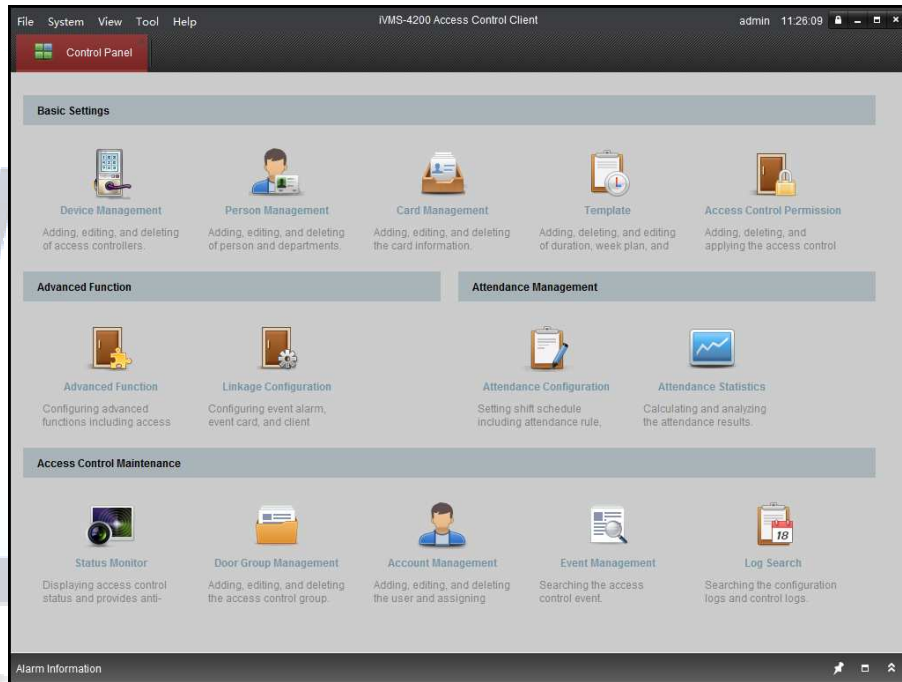
## 2.3 Activating Device via Client Software

### **Purpose:**

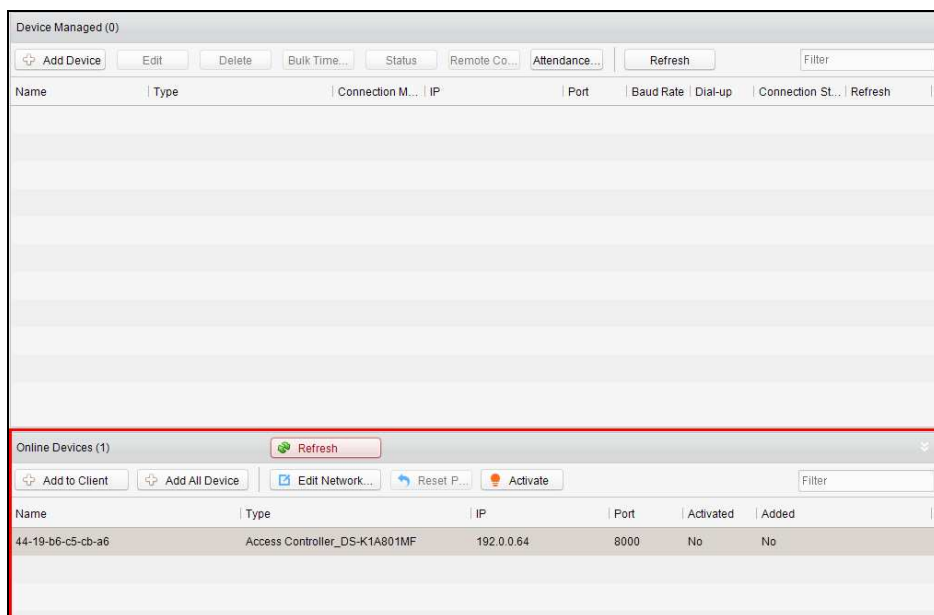
The iVMS-4200 Access Control Client is a client-based access control system for management of access control devices.

### **Steps:**

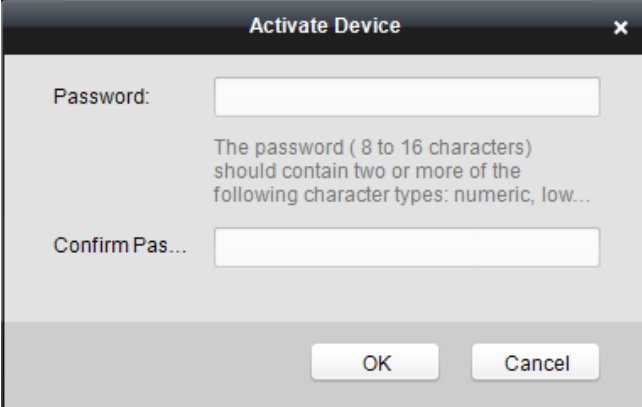
1. Install and run the software.



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



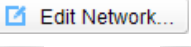
3. Select an inactive device from the device list.
4. Click **Activate** to pop up the Activation interface.



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  **Edit Network...** 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 3 Web Client Operation

## 3.1 Overview

### 3.1.1 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.

### 3.1.2 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

## 3.2 Login/Logout Web Client

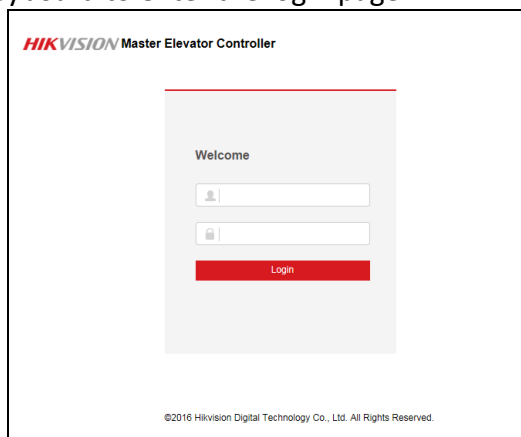
### *Before you start:*

Make sure the device is activated. For details, refer to 2.1 Activating Device via Web Client.

### 3.2.1 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 2.1 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.

### 3.2.2 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.

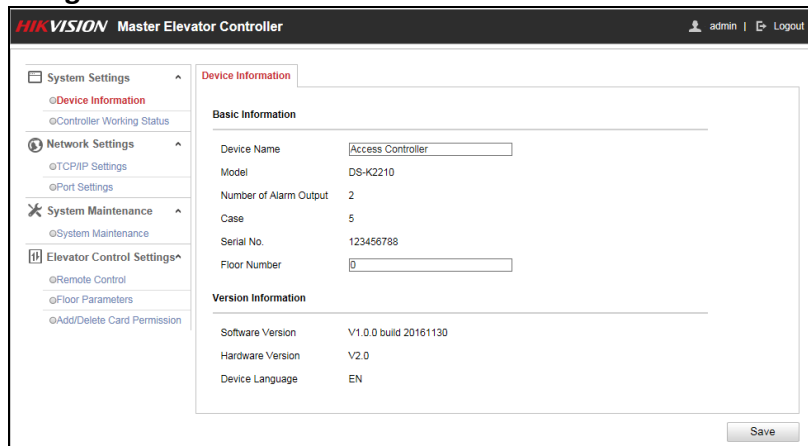
## 3.3 Setting Device via Web Client

### 3.3.3 System Settings

#### Managing Device Information

**Steps:**

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



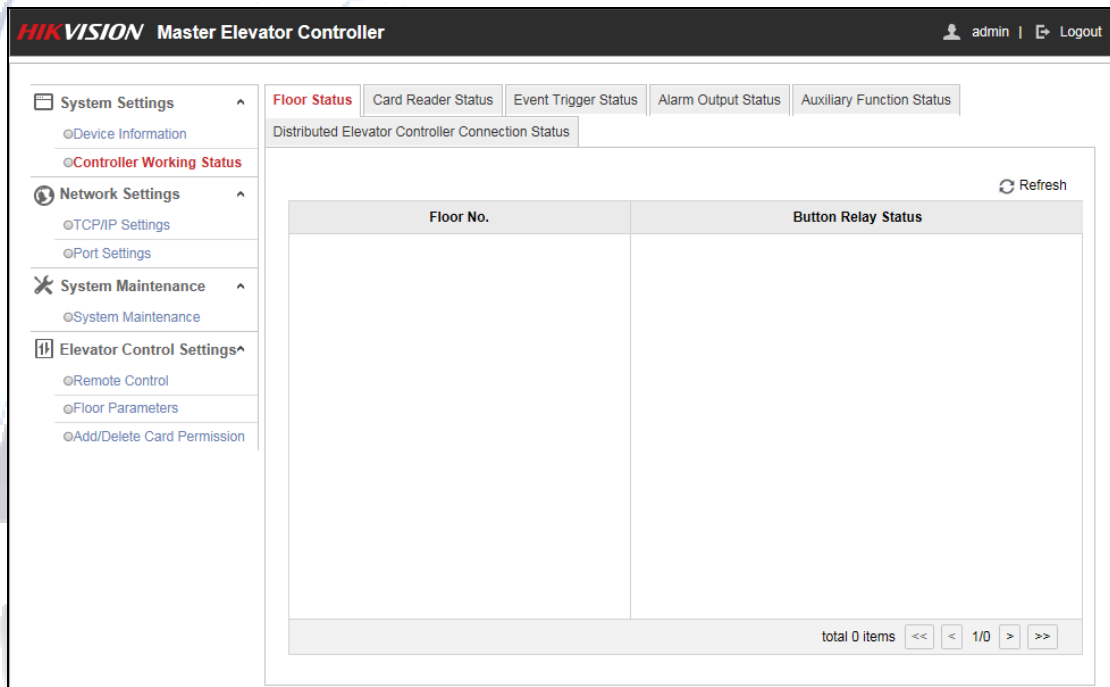


2. Check the device basic information (including the device name, the device type, the alarm output No., the case, the device serial No. and the floor number) and the version information (including the software version, the device language, and the hardware version).
3. (Optional) Edit the device name 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 3. 1.

Table 3. 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

### 3.3.4 Network Settings

#### Setting TCP/IP

##### Steps:

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

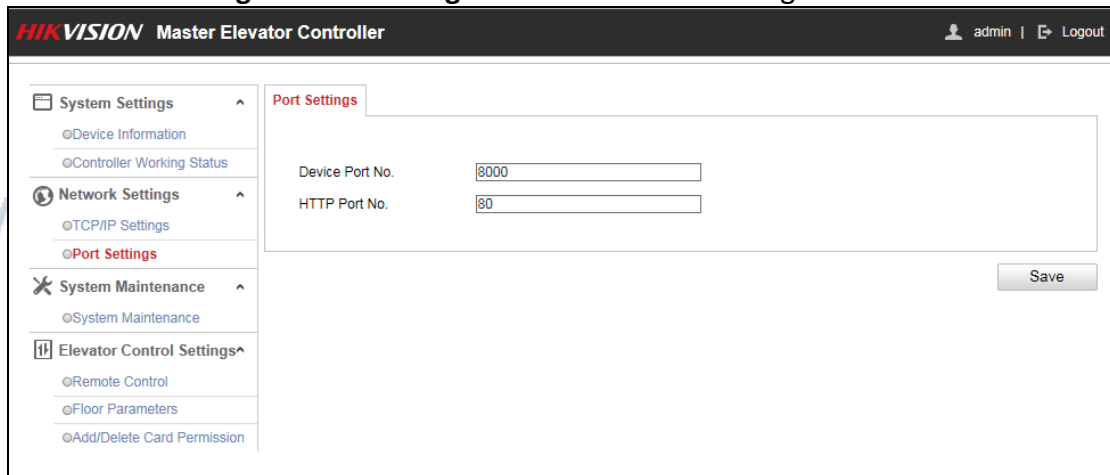
The screenshot shows the HIKVISION Master Elevator Controller web interface. The top bar displays 'HIKVISION Master Elevator Controller' and 'admin | Logout'. The left sidebar has 'Network Settings' selected, with sub-items 'TCP/IP Settings' (highlighted), 'Port Settings', 'System Maintenance', and 'Elevator Control Settings'. The main content area is titled 'TCP/IP Settings' and is divided into 'Basic Settings' and 'Advanced Settings'. Under 'Basic Settings', there are fields for NIC Type (set to '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), and MTU (1500). Under 'Advanced Settings', there are two empty input fields for DNS Server Address 1 and DNS Server Address 2. A 'Save' button is located at the bottom right of the settings area.

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.



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

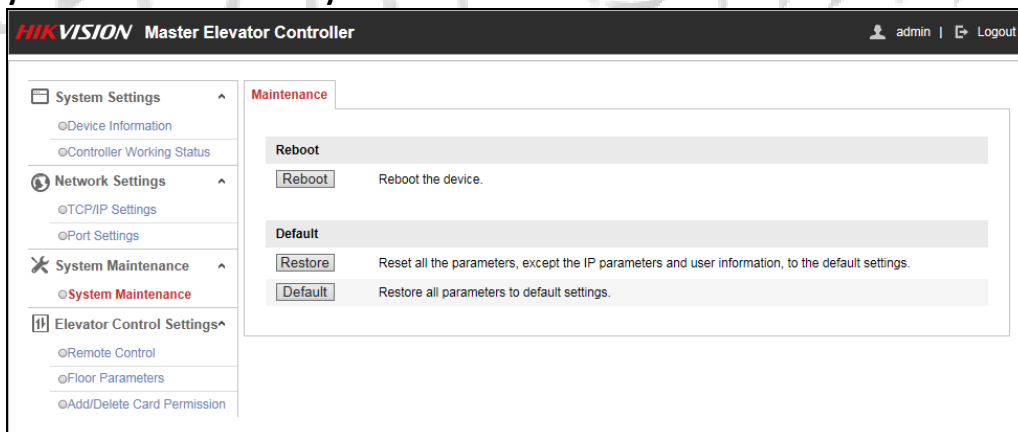
### Notes:

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

## 3.3.5 System Maintenance

### Steps:

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



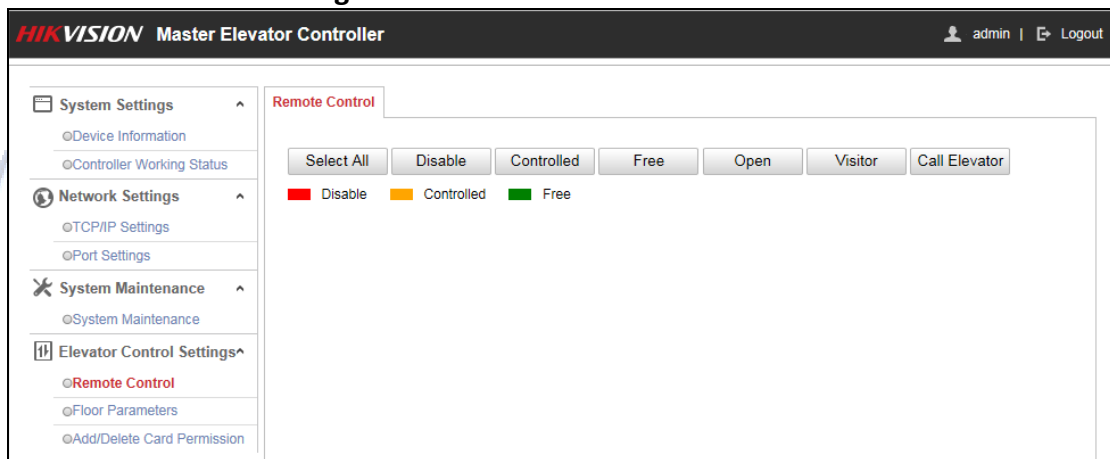
2. Click **Reboot** to remotely reboot the device.  
Or click **Restore** to reset all parameters, except the IP parameters and user parameters and user information to the default settings.  
Or click **Default** to reset all parameters to the default settings.

## 3.3.6 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.

The screenshot shows the 'Floor Parameters Settings' interface. The sidebar on the left lists various settings categories: System Settings (Device Information, Controller Working Status), Network Settings (TCP/IP Settings, Port Settings), System Maintenance (System Maintenance), and Elevator Control Settings (Remote Control, Floor Parameters, Add/Delete Card Permission). The 'Floor Parameters' section is active. The main area contains the following fields:

- Floor Parameters Settings**
  - Floor No.: Input field with value '1' and a warning icon and text 'Floor No. range 1-0'.
  - Floor Name: Input field.
  - Open Door with First Card: Dropdown menu with 'yes' selected.
- Time Settings**
  - Floor Relay Action Time: Input field with 's' unit.
  - Elevator Control Delay Time: Input field with 'min' unit.
  - Disabled Person: Input field with 's' unit.
  - First Card: Input field with 'min' unit.

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

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 / Floor remains open for the configured time duration after the first card swiping until the remain open duration ends.

**Floor Relay Action Time:** The relay closed time duration after swiping the normal card. It refers to the available using duration of the elevator button after assigning the permission to the card.  
The default action time is 5s.

**Elevator Control Delay Time:** The time duration of the visitor using the elevator.  
The default delay time is 5s.

**Disabled Person:** The door can be open with appropriate delay after disabled person swipes the card.  
The default time duration is 15s.

**First Card:** Set the door open duration for the function of Open Door with First Card.  
The default time duration is 10min.

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

## Adding and Deleting Card Permission

### Adding Card Permission

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

The screenshot shows the HIKVISION Master Elevator Controller web interface. The top navigation bar includes the HIKVISION logo, the title 'Master Elevator Controller', and user information 'admin | Logout'. A left sidebar contains a menu with categories: System Settings (Device Information, Controller Working Status), Network Settings (TCP/IP Settings, Port Settings), System Maintenance (System Maintenance), and Elevator Control Settings (Remote Control, Floor Parameters, Add/Delete Card Permission). The main content area is titled 'Adding Card Permission' and contains the following form elements:
 

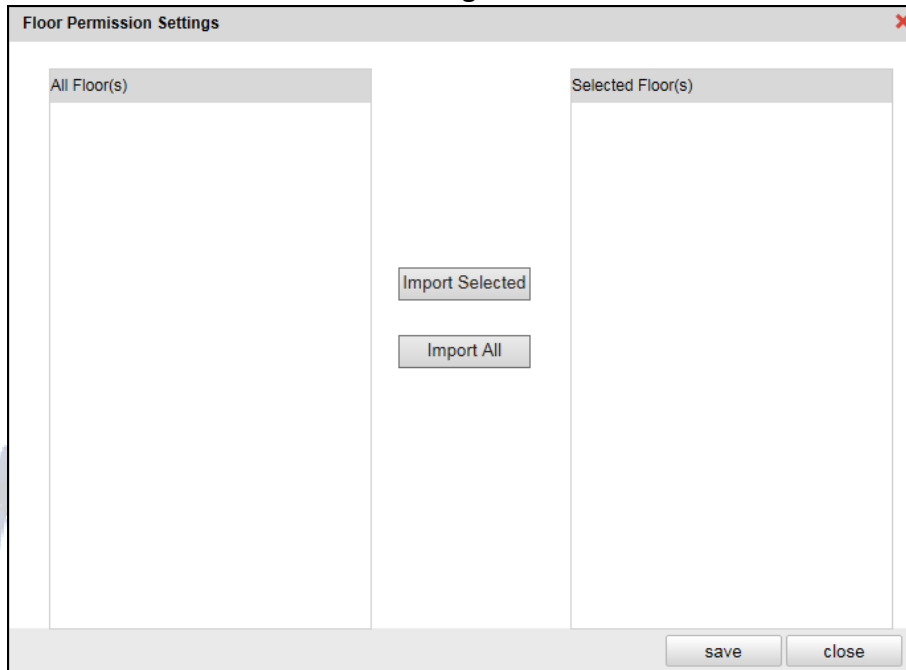
- Card No.:** A text input field.
- Auto Obtain:** A checkbox.
- Card Type:** A dropdown menu currently set to 'Normal Card'.
- Floor Permission:** A link labeled 'Settings'.
- Save:** A button at the bottom right of the form.

2. Input the card No.  
Or check the **Auto Obtain** checkbox, and swipe the card on the external card reader to get the card No.
3. Select a card type in the drop-down list.  
You can select from normal card, card for 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 3. 2.

Table 3. 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 be opened by swiping the duress card when there is a 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.

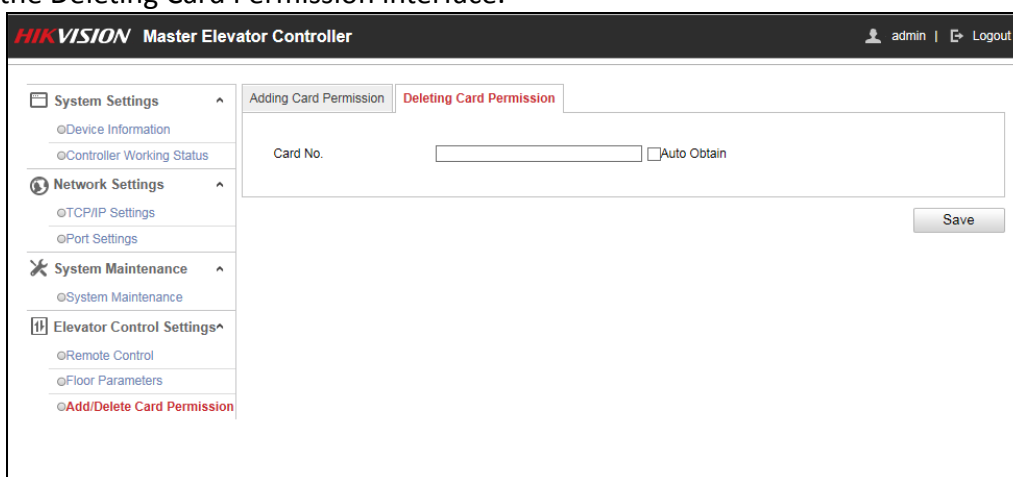


4. Check the floor checkbox(es) in the All Floor(s) list. And click **Import Selected Item** to import the selected floors to the Selected Floor(s) list.
5. Click **Save** to save the settings and the window will be automatically exited. The configured card will contain the selected floors permissions.
6. 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 4 Client Operation

## 4.1 Overview of iVMS-4200 Client Software

### 4.1.1 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.

### 4.1.2 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.

### 4.1.3 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




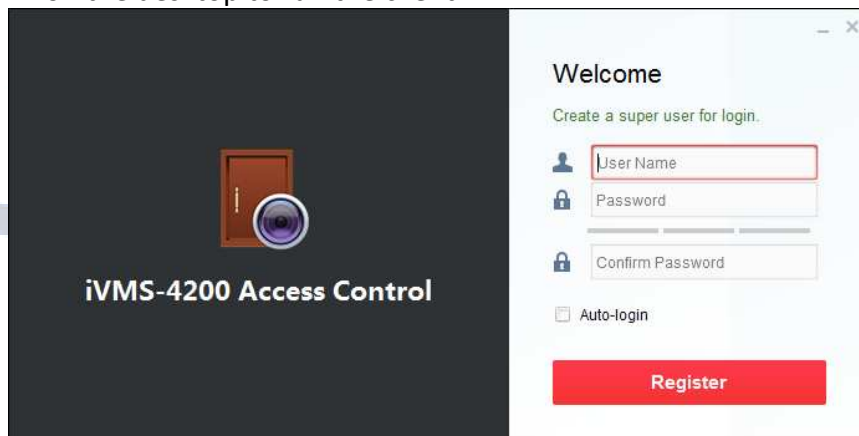
## 4.2 User Registration and Login

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

### 4.2.1 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.



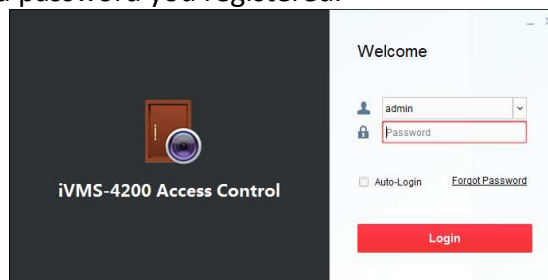
- ◆ A user name cannot contain any of the following characters: / \ : \* ? " < > |. And the length of the password cannot be less than 8 characters.
- ◆ For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case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

### 4.2.2 Login

**Steps:**

1. Input the user name and password you registered.

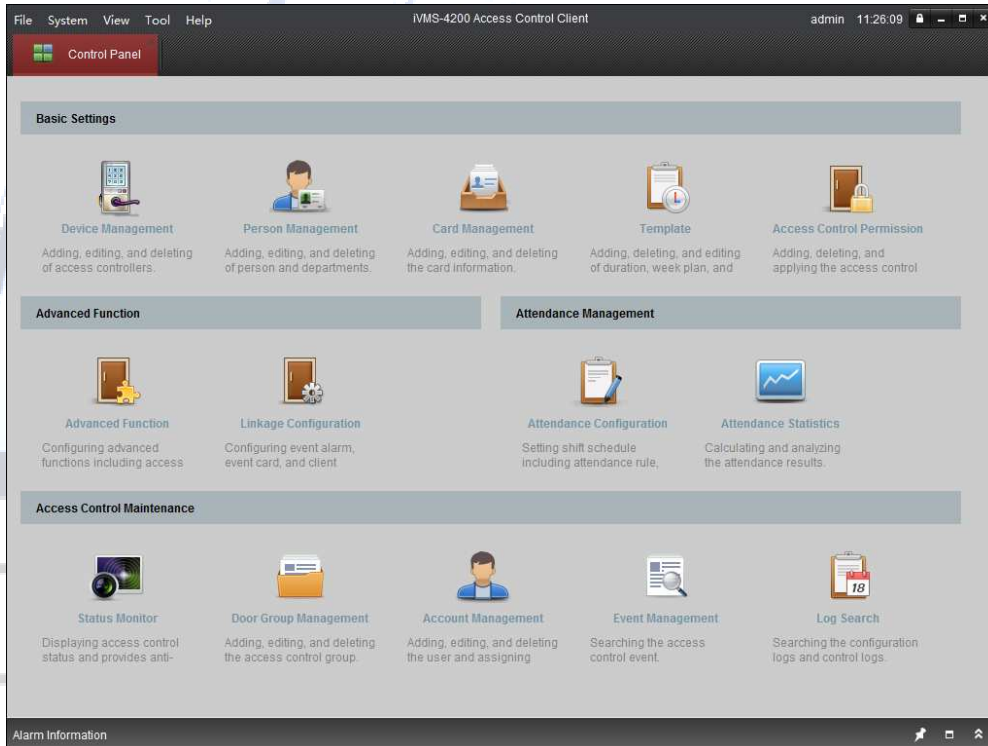


2. Optionally, check the checkbox **Auto-login** to log in to the software automatically.
3. Optionally, if you forget your password, please click **Forgot Password** and remember the encrypted string in the pop-up window. Contact your dealer and send the encrypted string to him to reset your password.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

### 4.2.3 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:**

<b>File</b>	<b>Exit</b>	Exit the iVMS-4200 Access Control Client.
<b>System</b>	<b>Lock</b>	Lock screen operations. Log in the client again to unlock.
	<b>Switch User</b>	Switch the login user.
	<b>Import Parameters</b>	Import client configuration file from your computer.
	<b>Export Parameters</b>	Export client configuration file to your computer.
	<b>Auto Backup</b>	Back up the database including person, attendance data, and permission data automatically.
<b>View</b>	<b>Device Management</b>	Open the Device Management page.

	<b>Attendance Configuration</b>	Open the Attendance Configuration page.
	<b>Attendance Statistics</b>	Open the Attendance Statistics page.
	<b>Person Management</b>	Open the Person Management page.
	<b>Card Management</b>	Open the Card Management page.
	<b>Template</b>	Open the Template page.
	<b>Access Control Permission</b>	Open the Access Control Permission page.
	<b>Advanced Function</b>	Open the Advanced Function page.
	<b>Status Monitor</b>	Open the Status Monitor page.
	<b>Linkage Configuration</b>	Open the Linkage Configuration page.
	<b>Door Group Management</b>	Open the Door Group Management page.
	<b>Account Management</b>	Open the Account Management page.
	<b>Event Management</b>	Open the Event Management page.
	<b>Log Search</b>	Open the Log Search page.
	<b>Control Panel</b>	Enter Control Panel interface.
<b>Tools</b>	<b>Search Access Control Permission</b>	Search the added access control permission.
	<b>Card Reader</b>	Configure the card reader parameters.
	<b>Fingerprint Machine</b>	Configure the fingerprint machine parameters.
	<b>Storage Server</b>	Configure the storage server parameters.
	<b>System Configuration</b>	Enter the System Configuration page.
	<b>People Counting</b>	Enter the People Counting page.
	<b>Apply Parameters</b>	Apply the settings on the client to the corresponding access control device.
<b>Help</b>	<b>Arming Settings</b>	Set the arming status of access control devices.
	<b>User Manual (F1)</b>	Click to open the User Manual; you can also open the User Manual by pressing <b>F1</b> on your keyboard.
	<b>Language</b>	Select the language for the client software and reboot the software to activate the settings.
	<b>About</b>	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 Control Permission

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 Group Management

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.

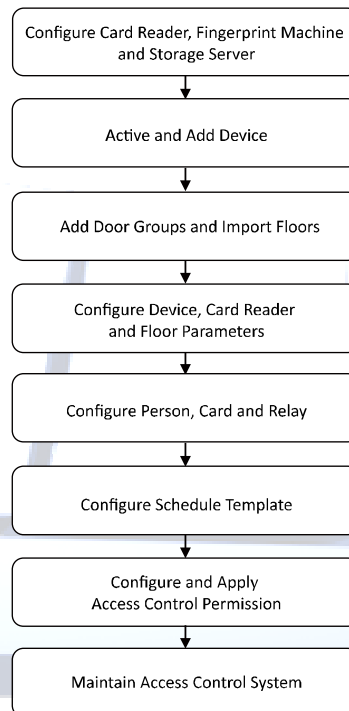
The function modules are easily accessed by clicking the navigation buttons on the control panel or by selecting the function module from the **View** menu.

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

---

## 4.3 Basic Configuration

### 4.3.1 Work Flow



## 4.4 Device Management

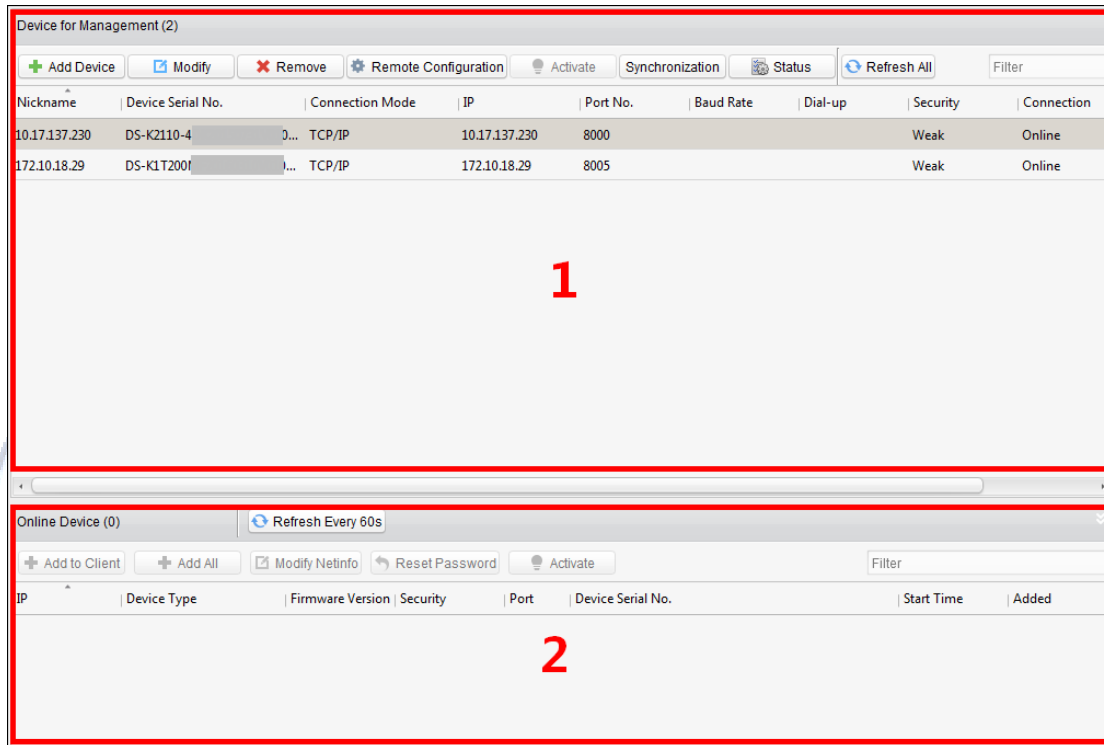
### **Purpose:**

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

### 4.4.1 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.

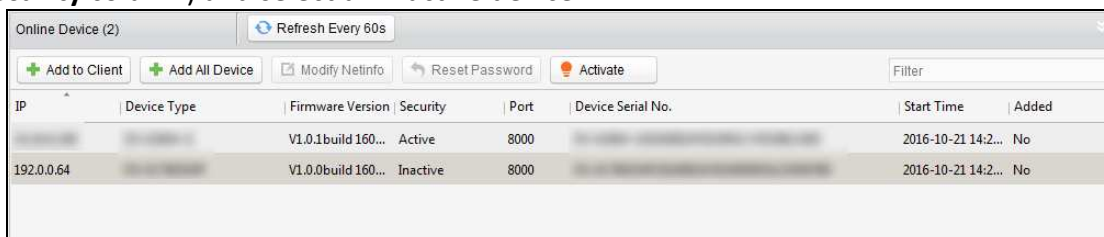
### Activating Device and Creating Password

**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.

Activation

User Name: admin

Password: .....

Strong

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: .....

OK 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.

Modify Network Parameter

Device Information:

MAC Address: 44-19-b6-c2-ce-33 Copy

Version: V1.0.1build 160310 Copy

Serial No.: DS-K1T200MF-C20160310V010001CH557814233 Copy

Network Information:

IP Address: 10.18.130.242

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 10.18.130.254

Password: |


OK Cancel

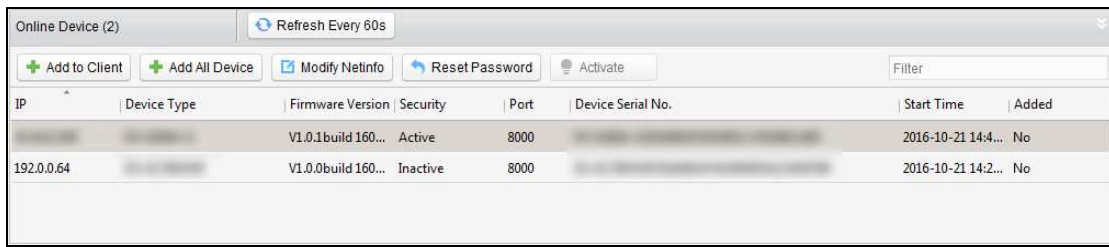
- 3) Click **OK** to save the settings.

## 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.



IP	Device Type	Firmware Version	Security	Port	Device Serial No.	Start Time	Added
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.



**Add Device**

Nickname:

Connection Method: TCP/IP

IP Address: 10.16.6.151

Port: 8000

User Name:

Password:

Add Cancel

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.



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.

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 *Error! Reference source not found.*
4. 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.**
5. Click **Add** button to finish adding.

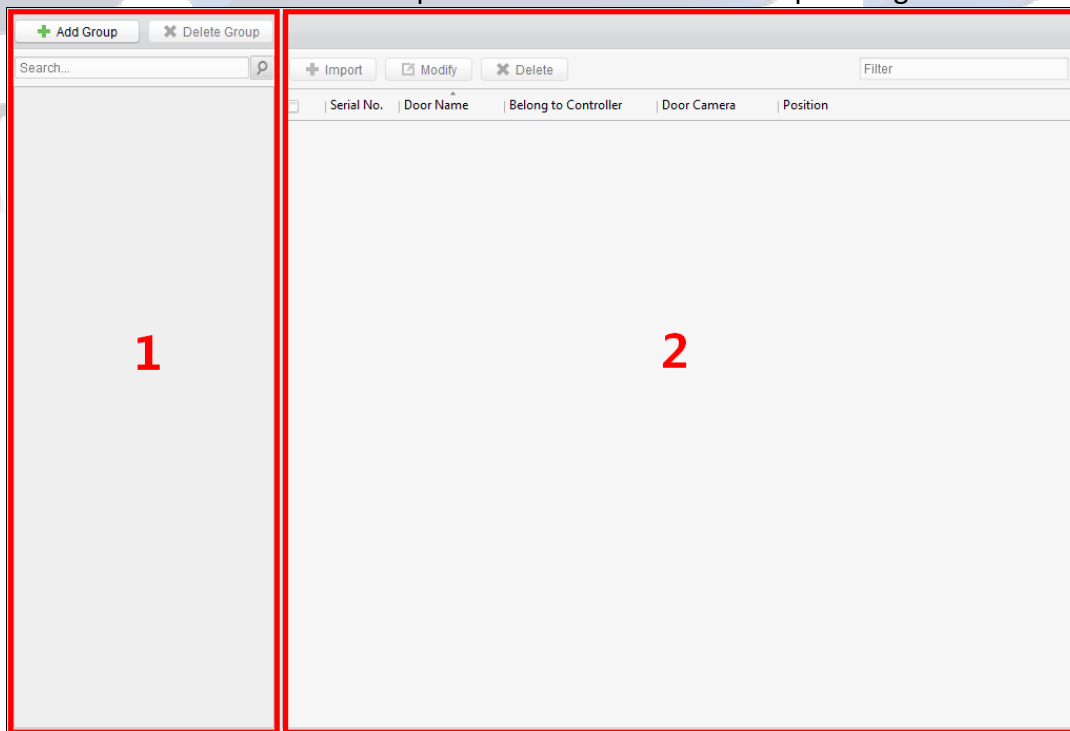
## 4.4.2 Door Group Management

### **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.

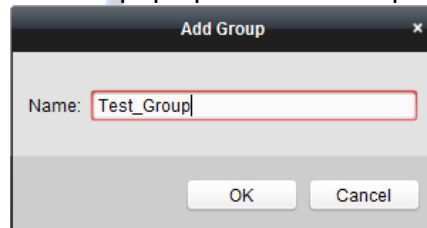
### Access Control Group Management

#### 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

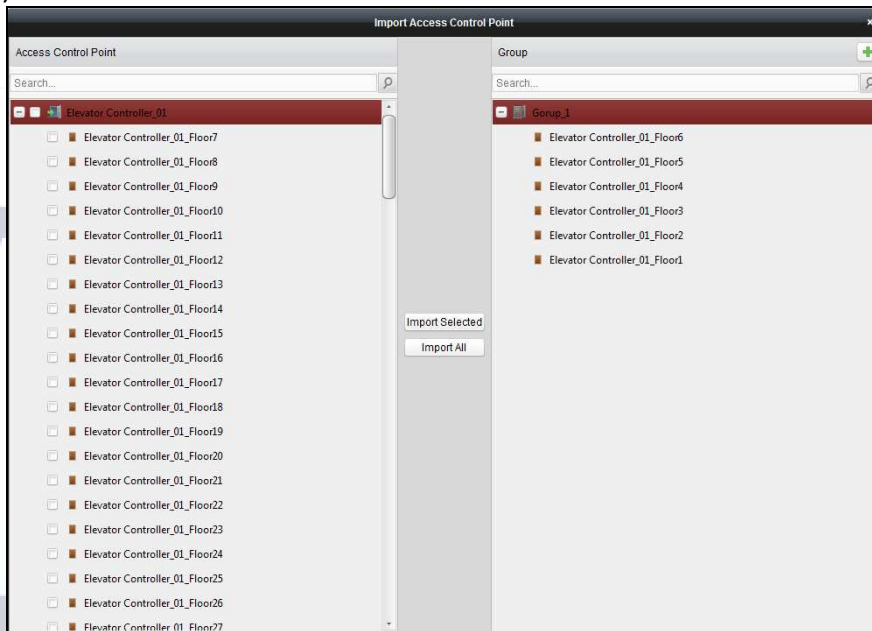
### Purpose:




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.

---

## 4.4.3 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.

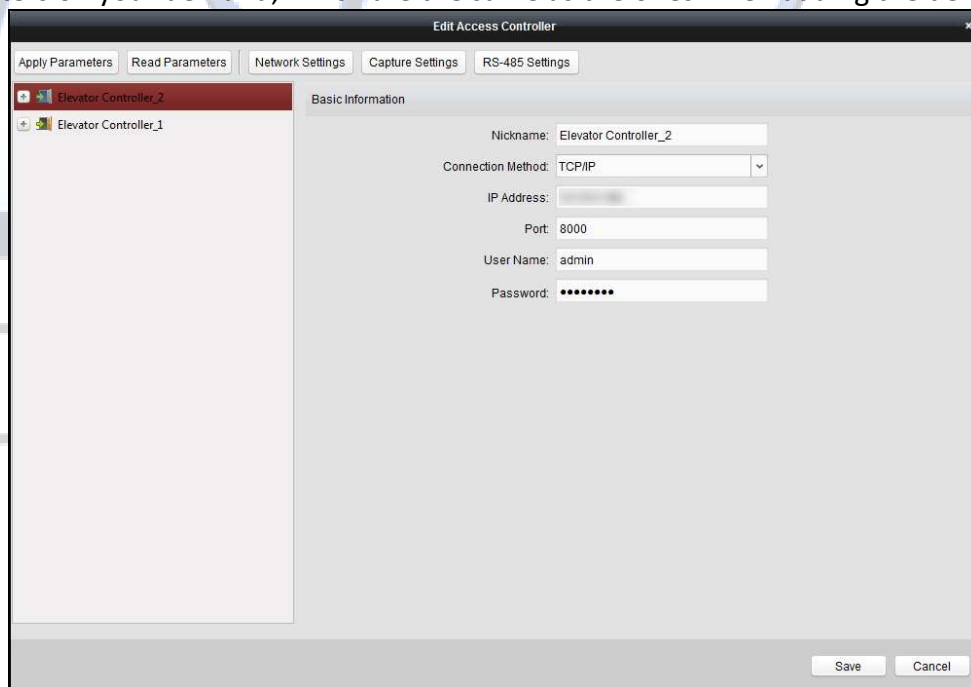
### **Editing Basic Information**

#### **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.

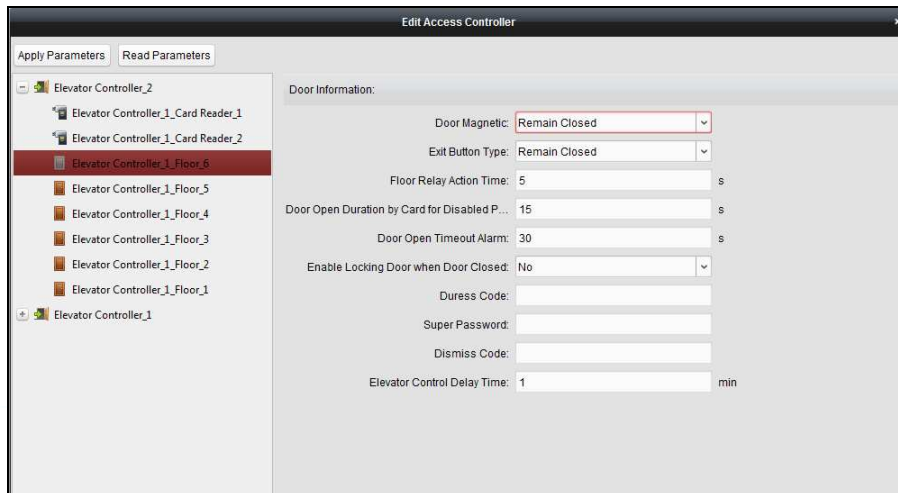


2. Click **Save** button to save the settings.
3. You can click **Apply Parameters** button to apply the updated parameters to the local memory of the device.

### **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.

**Time:**

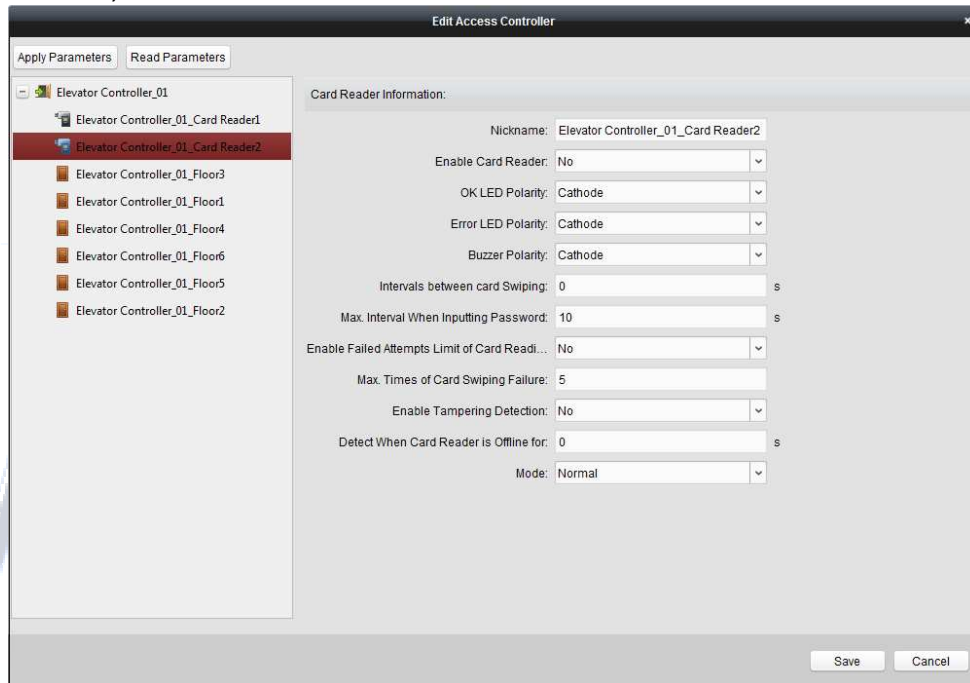
3. Click **Save** button to save the parameters.

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:

<b>Nickname:</b>	Edit the card reader name.
<b>Enable Card Reader:</b>	Select <b>Yes</b> to enable the card reader.
<b>OK LED Polarity:</b>	Select the OK LED Polarity of the card reader mainboard.
<b>Error LED Polarity:</b>	Select the Error LED Polarity of the card reader mainboard.
<b>Buzzer Polarity:</b>	Select the Buzzer LED Polarity of the card reader mainboard.
<b>Interval between Card Swiping:</b>	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.
<b>Max. Interval When Inputting Password:</b>	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.
<b>Enable Failed Attempts Limit of Card Reading:</b>	Enable to report alarm when the card reading attempts reach the set value.
<b>Max. Times of Card Swiping Failure:</b>	Set the max. failure attempts of reading card.
<b>Enable Tampering Detection:</b>	Enable the anti-tamper detection for the card reader.
<b>Detect When Card Reader is Offline for:</b>	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.

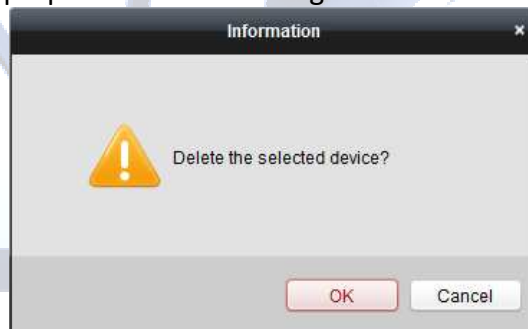
**Card Issuing:** Swipe the card on the card enrollment station to read the card No. The system will fill the card No. to the place that needs it.

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.

#### 4.4.4 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.
2. Click **Remove** button to delete the selected device(s).
3. Click **OK** button in the pop-up confirmation dialog to finish deleting.



#### 4.4.5 Time Synchronization

**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.
2. 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.

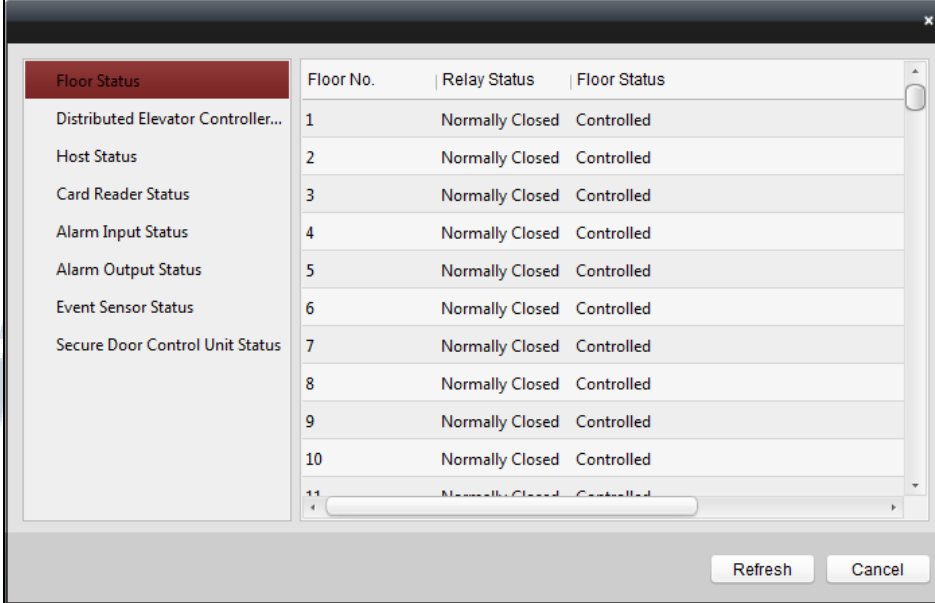


---

## 4.4.6 Viewing Device Status

### **Purpose:**

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



The screenshot shows a dialog box titled 'Floor Status'. On the left is a sidebar with a tree view containing the following items: 'Floor Status' (selected), 'Distributed Elevator Controller...', 'Host Status', 'Card Reader Status', 'Alarm Input Status', 'Alarm Output Status', 'Event Sensor Status', and 'Secure Door Control Unit Status'. The main area of the dialog is a table with three columns: 'Floor No.', 'Relay Status', and 'Floor Status'. The table contains 11 rows of data, all showing 'Normally Closed' for Relay Status and 'Controlled' for Floor Status. At the bottom right of the dialog are 'Refresh' and 'Cancel' buttons.

Floor No.	Relay Status	Floor Status
1	Normally Closed	Controlled
2	Normally Closed	Controlled
3	Normally Closed	Controlled
4	Normally Closed	Controlled
5	Normally Closed	Controlled
6	Normally Closed	Controlled
7	Normally Closed	Controlled
8	Normally Closed	Controlled
9	Normally Closed	Controlled
10	Normally Closed	Controlled
11	Normally Closed	Controlled

- 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.

## 4.4.7 Remote Configuration

### **Purpose:**

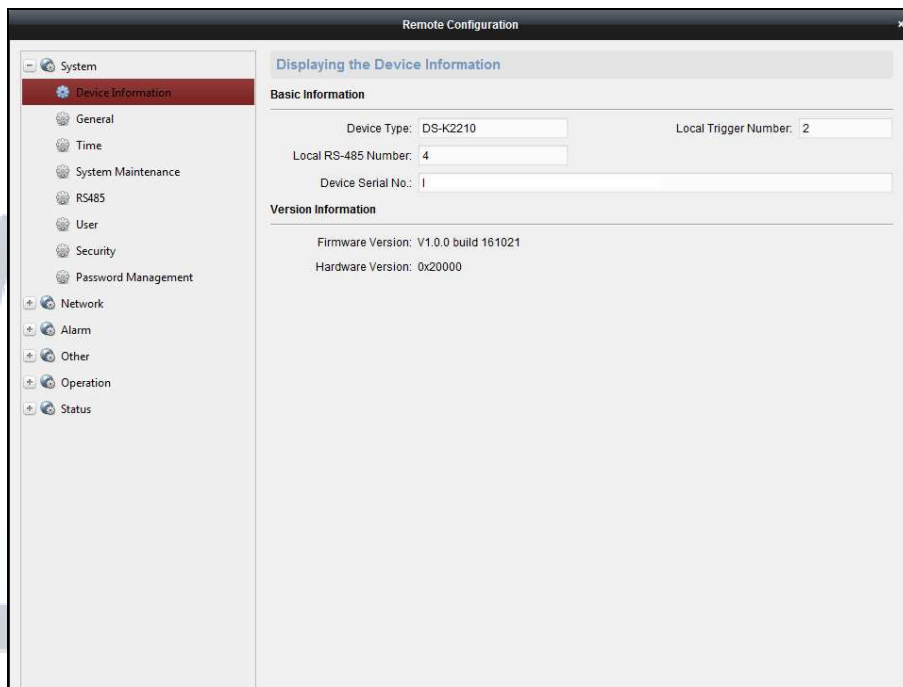
In the device list, select the device and click **Remote Configuration** button to enter the remote configuration interface. You can set the detailed parameters of the selected device.

---

## Checking Device Information

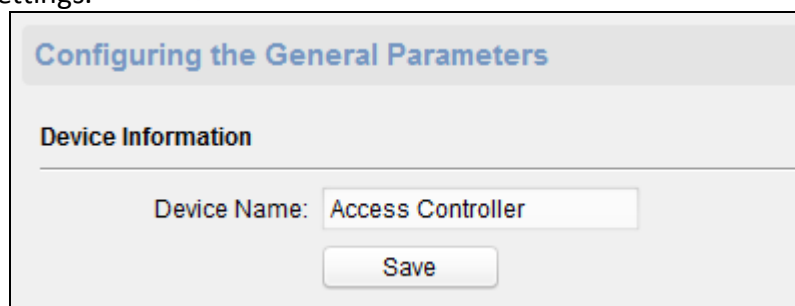
### Steps:

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

### Configuring the Time Settings (e.g., NTP, DST)

**Time Zone**

Select Time Zone: (GMT) Dublin, Edinburgh, London ▼

**Enable NTP**

Server Address:

NTP Port:

Sync Interval:  Minute(s)

**Enable DST**

Start Time: January ▼ First Week ▼ Sun ▼ 0  : 00

End Time: January ▼ First Week ▼ Sun ▼ 0  : 00

DST Bias:

## 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.

### System Maintenance

**System Management**

**Remote Upgrade**

Controller Upgrade File ▼

Process:

---

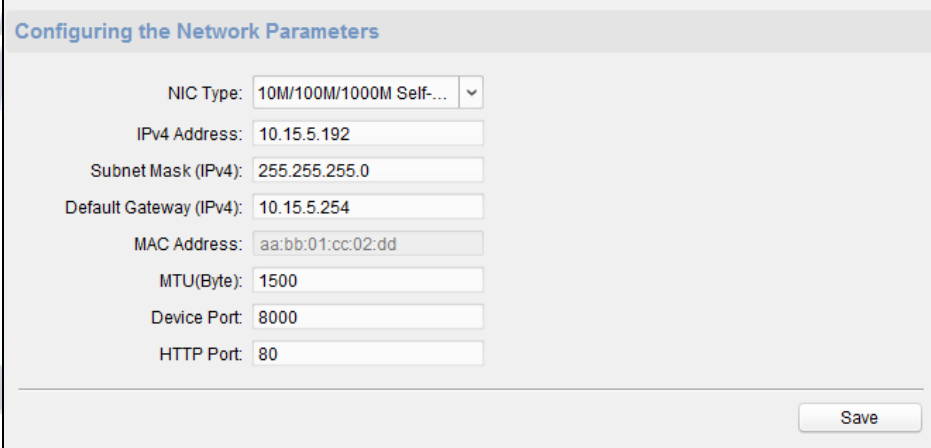
## Setting Security

### Steps:

1. Click **System** -> **Security**.
2. Select the encryption mode in the dropdown list. You are able to select Compatible Mode or Encryption Mode.
3. (Optional) You can check **Enable Telnet** in the Software part.
4. 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

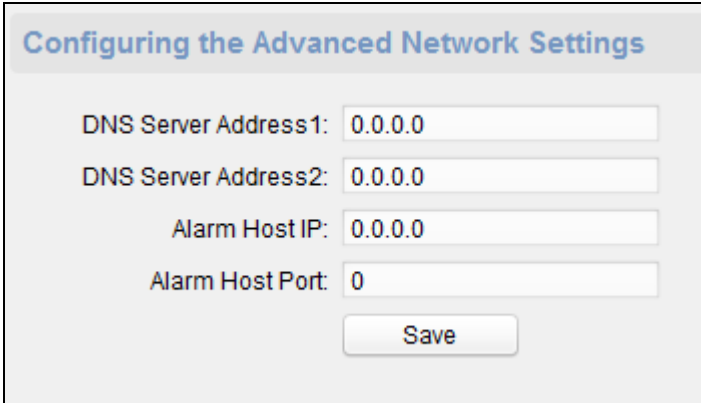
Device Port: 8000

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


---

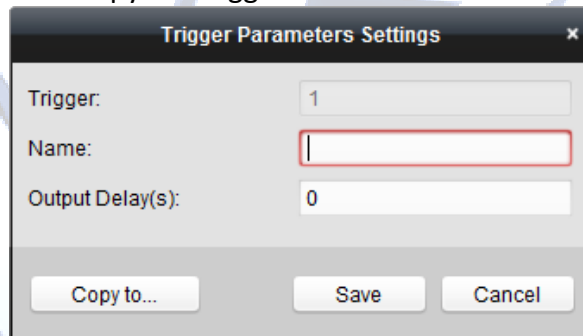
## Configuring Trigger Parameters

### 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.



The dialog box titled "Trigger Parameters Settings" contains the following fields and buttons:

- Trigger: 1
- Name:
- Output Delay(s): 0
- Buttons: Copy to..., Save, Cancel

C O R P O R A T I O N

---

## 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"/>	
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

## 4.5 Relay Management

### Purpose:

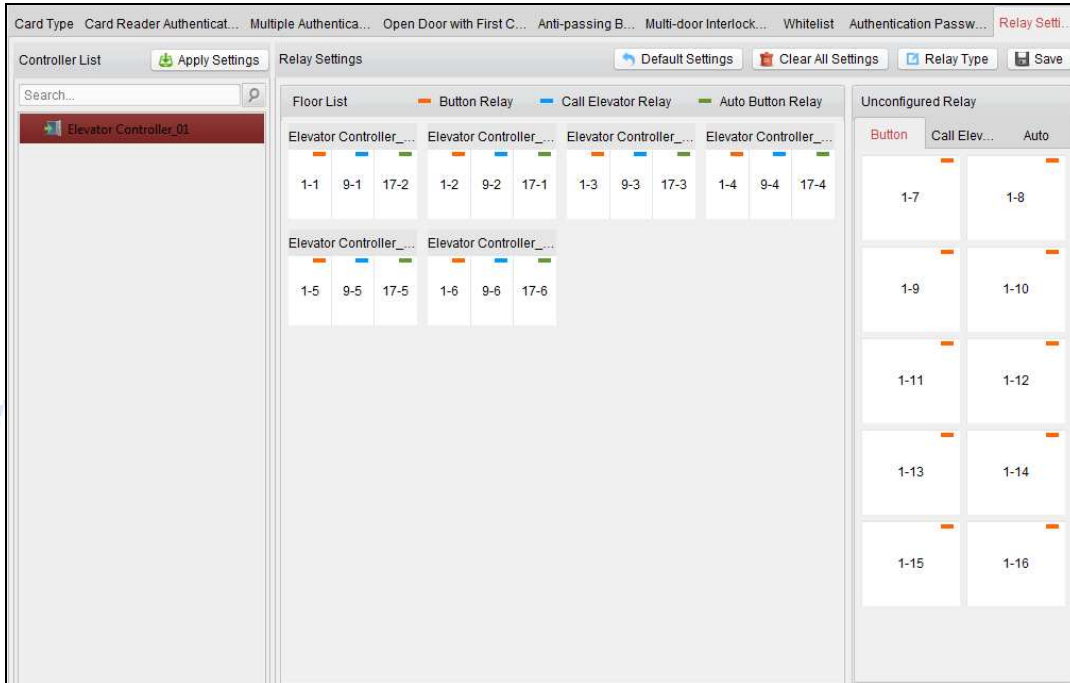
You can manage the relationship between the floor and the relay in this chapter.

### 4.5.1 Configuring Relay and Floor

### Steps:



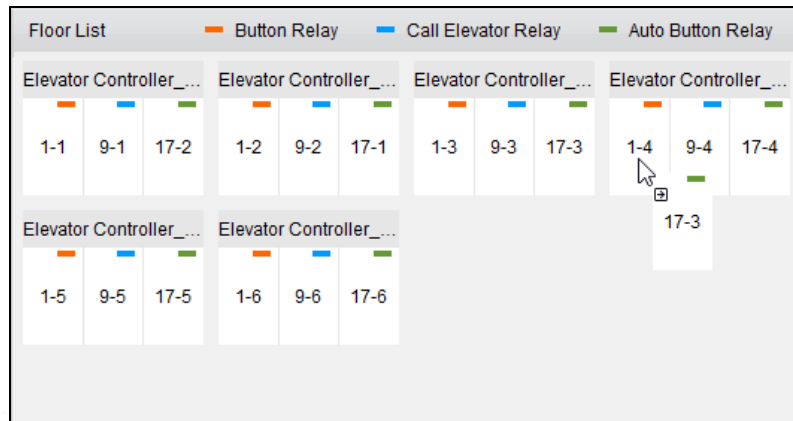
1. In the Control Panel, click the icon Advanced Function to enter the Advanced Function module.
2. Click **Relay Settings** to enter the Relay Settings interface.



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.



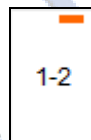
5. Click and drag the unconfigured relay from the Unconfigured Relay panel to the corresponding floor in the Floor List panel.  
Or click and drag the relay from the Floor List panel to the Unconfigured Relay panel.  
Or click and drag the relay from one floor to another floor in the Floor List panel.  
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 4.5.2 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.

## 4.5.2 Configuring Relay Type

**Purpose:**

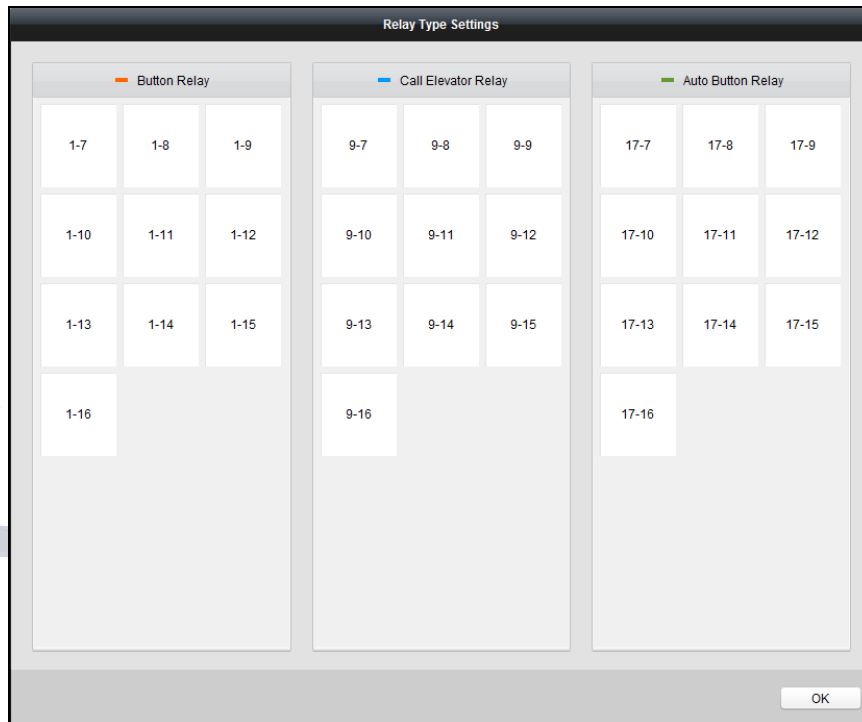
You can change the relay type by following the steps in this section.

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

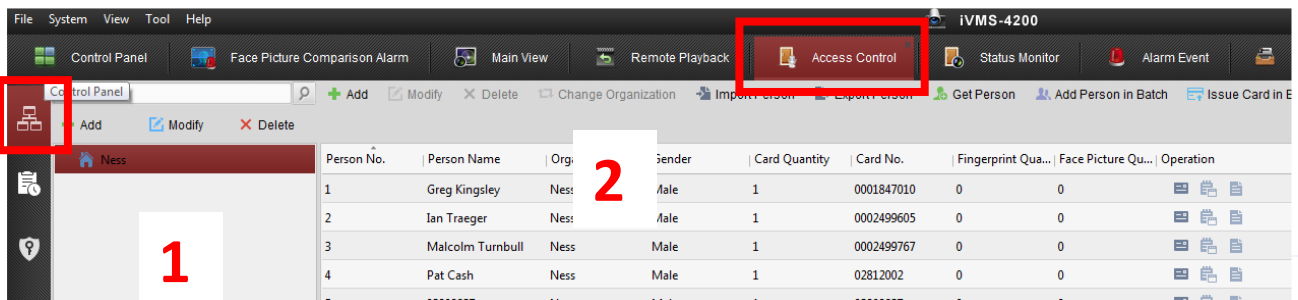
**Note:** Three types of relay are available: Button Relay, Call Elevator Relay and Auto Relay. ■ represents the button relay, ■ represents the call elevator relay, and ■ represents the auto button relay.

C O R P O R A T I O N

## 4.6 Person and Card Management

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

From the 'Access Control' Module, Click  tab to enter the Person and Card Management interface.



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

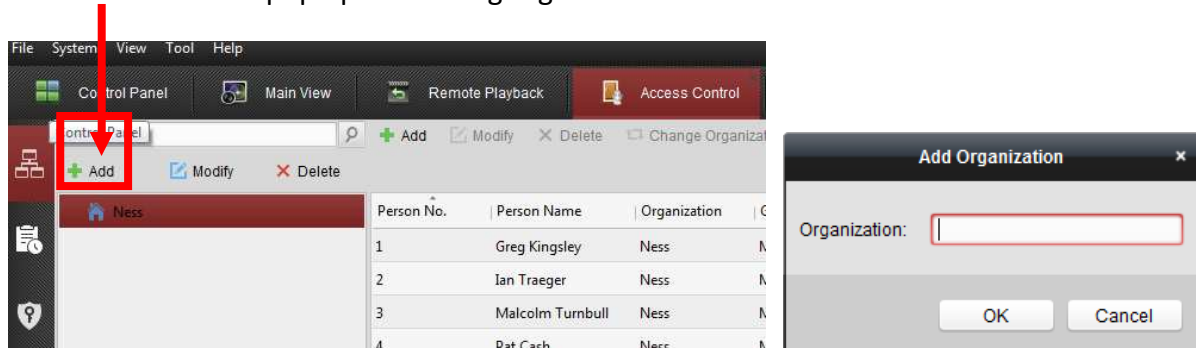
1	<b>Organization Management</b>	You can add, edit, or delete the organization as desired.
2	<b>Person Management</b>	After adding the organization, you can add the person to the organization and issue card to persons for further management.

### Organization Management

#### Adding Organization

##### Steps:

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



2. Input the Organization Name as desired.
3. Click **OK** to save the adding.

4. You can add multiple levels of organizations according to the actual needs.  
To add sub organizations, select the parent organization and click **Add**.  
Repeat *Step 2* and *3* to add the sub organization.  
Then the added organization will be the sub-organization of the upper-level organization.

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

### Modifying and Deleting Organization

You can select the added organization and click **Modify** to modify its name.

You can select an organization, and click **Delete** button to delete it.

**Notes:**

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

## 4.6.3 Person Management

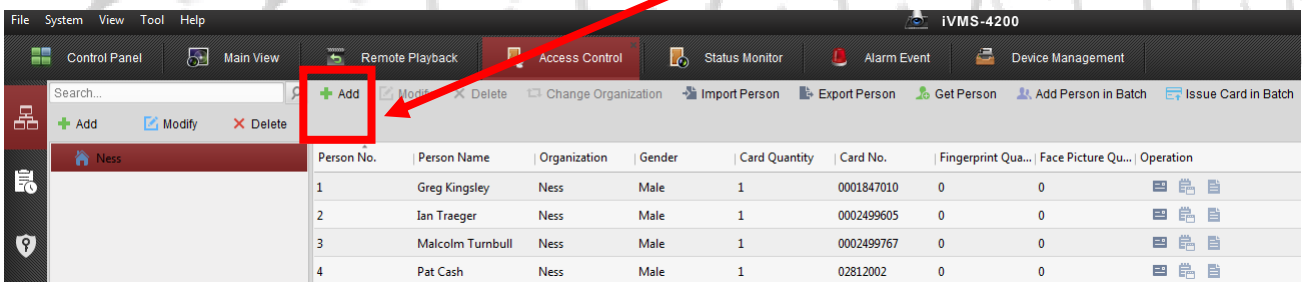
After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting person's information in batch, etc.

**Note:** Up to 2,000 persons or cards can be added.

### Adding Person / Card

**Steps:**

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



1. The Person No. will be generated automatically and is not editable.
2. Input the persons information as required. (i.e. Person name, gender, phone No., date of Birth, and email etc to suit the client’s actual needs. This is database information for the customer and will work without this information)
3. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.  
**Note:** The picture should be in \*.jpg format.  
(Optional) You can also click **Take Photo** to take the person’s photo with the PC camera.
4. Click **OK** to finish adding.

### Adding Person (Detailed Information)

#### Steps:

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

2. Input the detailed information of the person, including person’s ID type, ID No., country, etc., according to actual needs.
  - **Linked Device:** You can bind the Intercom indoor station to the person.  
**Note:** If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will

display and you are required to select the door station to communicate with the analog indoor station.

- **Room No.:** You can input the room No. of the person, as used with the Apartment Intercom System. .

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

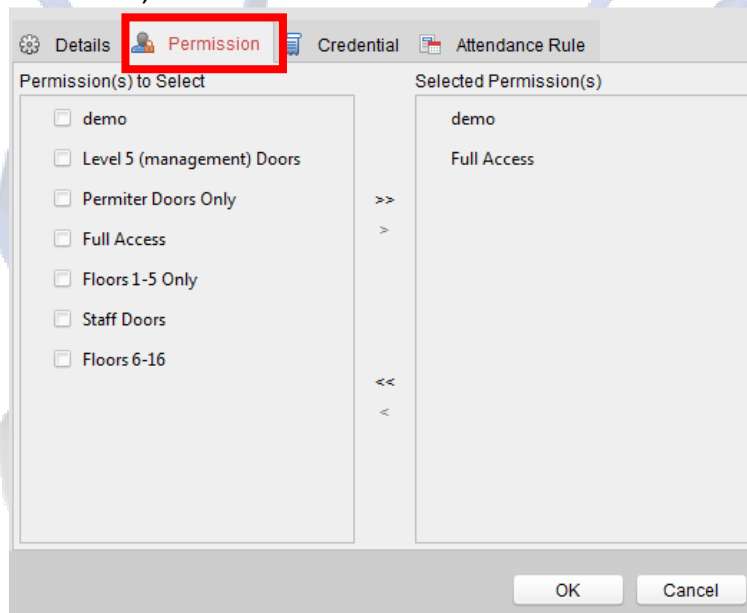
### Adding Person (Permission / Access Levels)

**Note:** Before Permissions can be set to a user, they first need to be set. For setting the access control permission, so they can be used, refer to *Chapter Error! Reference source not found. Error! Reference source not found.*

Once access permissions are created, you can assign the permissions (ie. What doors the user can access during what times) to the person when adding person.

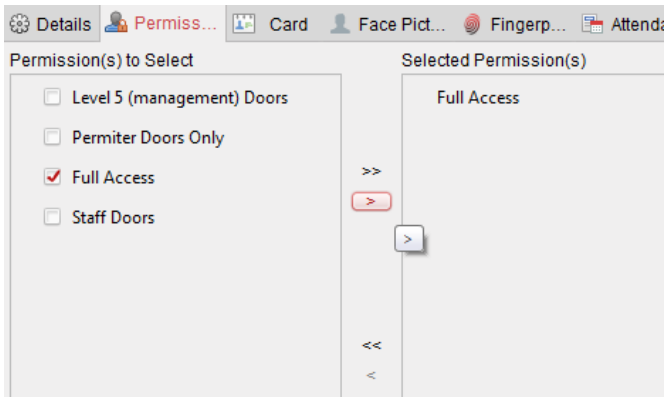
#### Steps:

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



2. In the 'Permission(s) to Select list', all the configured permissions are displayed. Check the permission(s) checkbox(es) and click > to add to the Selected Permission(s) list. (Optional) You can click >> to add all the displayed permissions to the Selected Permission(s) list.





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

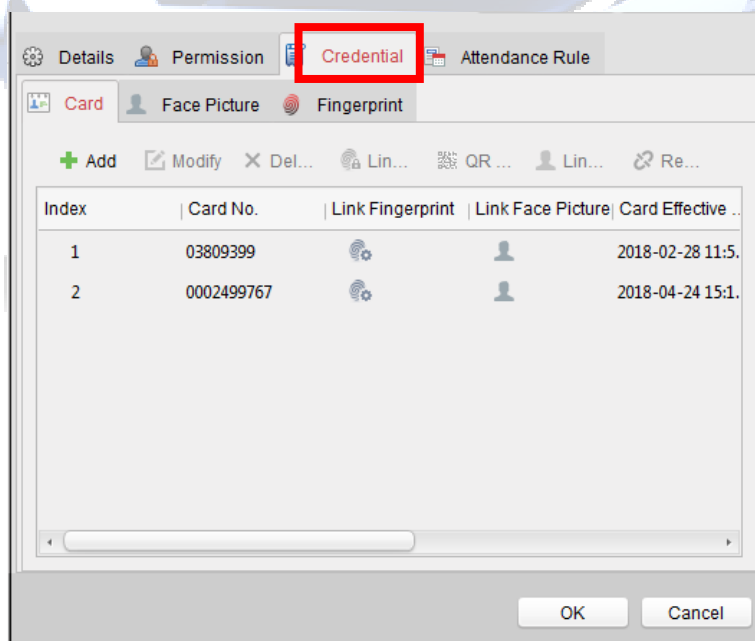
3. Click **OK** to save the settings.

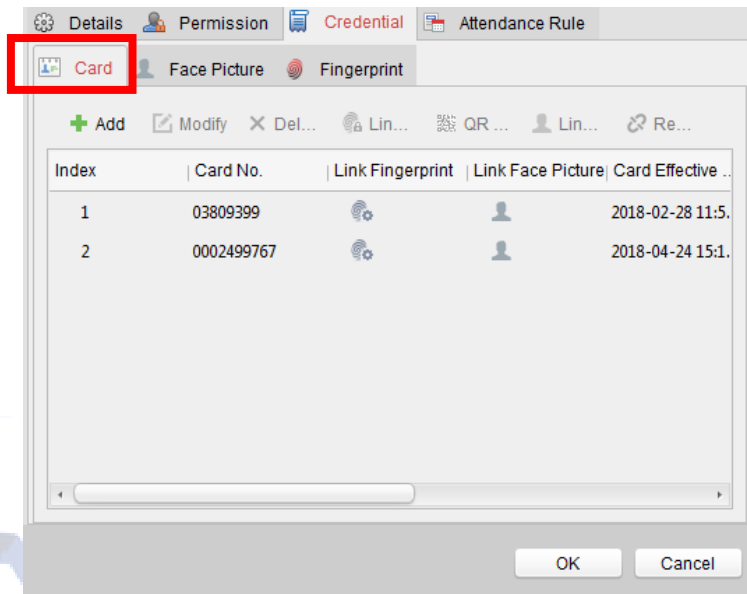
### Adding Person (Card / Credential)

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

#### Steps:

1. In the Add Person interface, click **Credential** tab, then click “Card” tab to add an Access Card.





C O R P O R A T I O N

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

3. Select the card type according to actual needs.

- **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 door cannot be opened.
- **Patrol Card:** The card swiping action can be used for checking the working status of the Guard Patrol. The access permission of the Guard Patrol staff is configurable.
- **Duress Card:** The door can be opened by swiping the duress card when there is a duress. At the same time, the client can report the duress event.
- **Super Card:** The card is valid for all the doors of the controller during the configured schedule.
- **Visitor Card:** The card is assigned for visitors. For the Visitor Card, you can set the **Max. Swipe Times**.

**Notes for Visitor Card:**


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

4. Input the password (PIN No) of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

**Note:** The password will be required when the card holder swipes the card to get enter to or



exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, *Chapter 4.9.4 Card Reader Authentication*.

5. Click  to set the effective time and expiry time of the card.

Effective Period: From 2018-02-28 10:40:21  To 2028-02-28 10:40:21 

6. Select the **Card Reader Mode** for reading the card No.

A card can be entered into the system in 3 different ways.

1. Via the Controllers card reader (any reader on the system)
2. Via an Enrollement reader connected via a USB port to the clients PC running iVMS4200 software. (e.g. DS-K1F180-D8E)

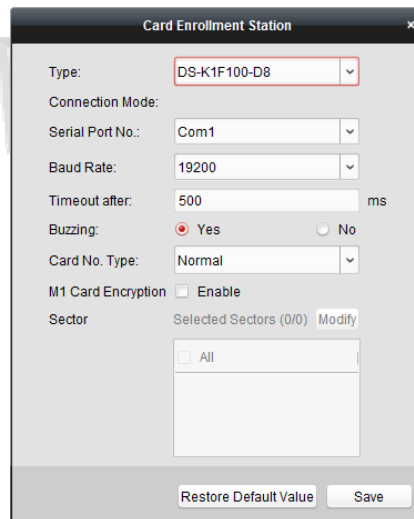


3. Manually entering the full card Number (e.g. 8 digits – 3 Digit Site code followed by 5 digit card No.)

- **Access Controller Reader:** Select “Read” and then place the card on the reader of the Access Controller to get the card No.

**Card Enrollment Station:** Select “Read” and then place the card on the Card Enrollment Station to get the card No.

**Note:** The Card Enrollment Station should connect with the PC running the client. You first need to click **Set Card Enrollment Station** to enter the following dialog to set it up before reading a card.



The screenshot shows a dialog box titled "Card Enrollment Station" with the following fields and options:

- Type: DS-K1F100-D8 (dropdown menu)
- Connection Mode: (empty dropdown menu)
- Serial Port No.: Com1 (dropdown menu)
- Baud Rate: 19200 (dropdown menu)
- Timeout after: 500 ms (text input)
- Buzzing: Yes (radio button selected), No (radio button)
- Card No. Type: Normal (dropdown menu)
- M1 Card Encryption: Enable (checkbox, unchecked)
- Sector: Selected Sectors (0/0) Modify (text input with "All" button)
- Buttons: Restore Default Value, Save

- 1) Select the Card Enrollment Station type.
- 2) **Note:** Currently, the supported card reader types include DS-K1F100-D8E and **DS-K1F180-D8E**
- 3) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.
- 4) If using standard 26 Bit Wiegand Cards, then set the Card No. Type to Wiegand.

---

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

5) Click **Save** button to save the settings.

You can click Restore Default Value button to restore the defaults.

### **Understanding Card Markings.**

Depending on the card vendor, there may be a 10 Digit Card No, 8 Digit (with comma after the first 3 digits) or both 10 and 8 Digit numbers on the card.

There are usually two sets of numbers on the 125kHz EM4100 RFID cards. Key fobs usually only have a single 10-digit or Single 8-digit number.

e.g.



The number on the right, "**comma format**": (e.g. 123, 45678)

- This is usually the Cards **26 Bit Wiegand Number**. It consists of a 3 Digit Site Code (0-255) and then a 5 Digit Card No (0-65,535).
- According to the Wiegand 26 spec, this is the badge number in this format.

The number on the left, "**10-digit format**": (e.g. 0123456789)

- If the Card Reader is set to output **37 Bit Wiegand**, then often this is the associated Card No.

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

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

## Adding Person (Fingerprint)

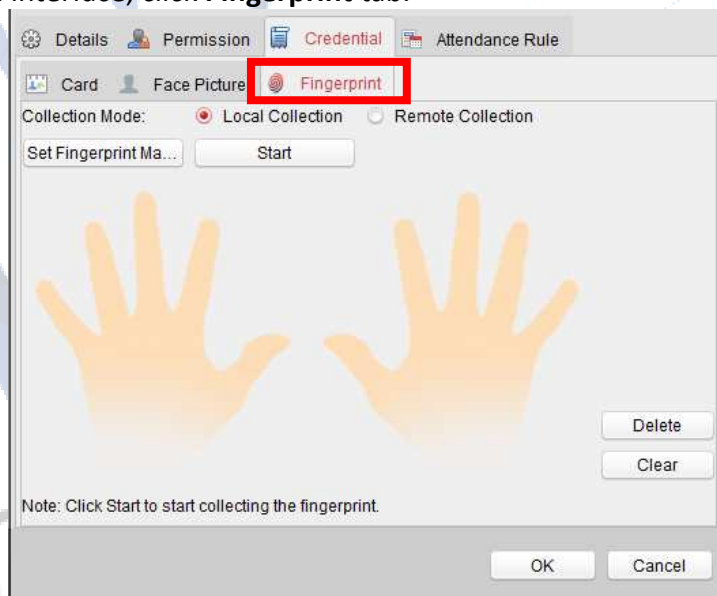
To program Fingerprint into the system, you require a Fingerprint Registration Terminal.



**DS-K1F820-F**

### Steps:

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



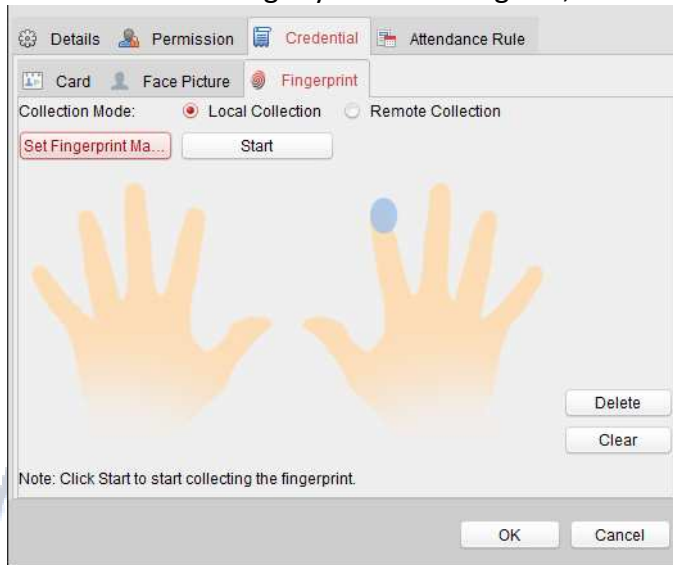
2. Before inputting the fingerprint, you should connect the fingerprint machine to the PC and set its parameters first.

Click **Set Fingerprint Machine** to enter the following dialog box.



- 1) Select the device type: **DS-K1F820-F**
- 2) Click **Save** button to save the settings.  
You can click **Restore Default Value** button to restore the default settings.

3. Click on the first Finger you wish to register,



4. Click **Start** button, click to select the fingerprint to start collecting.

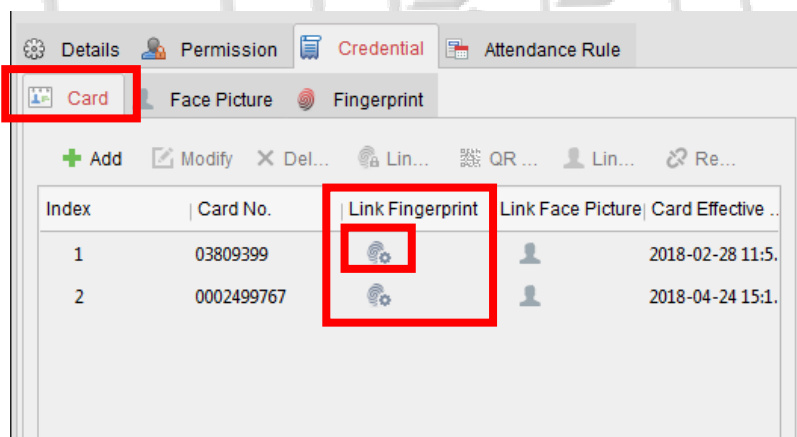
5. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.

6. Click **Stop** button can stop collecting.

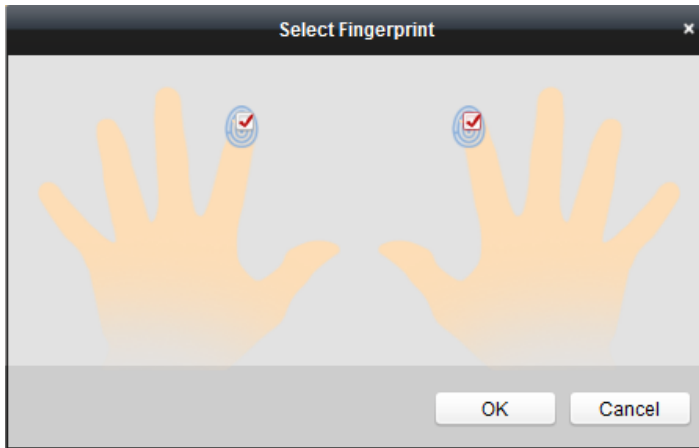
7. After collecting the fingerprint, click 'Card' in the Add Person window to enter the Card tab. You can select the registered fingerprint and click **Delete** to delete it. You can click **Clear** to clear all fingerprints.

8. Click **OK** to save the fingerprints.

9. Click **Link Fingerprint** to link the fingerprint to the card.



Select the Fingerprints you wish to link to the added card and then click "OK".



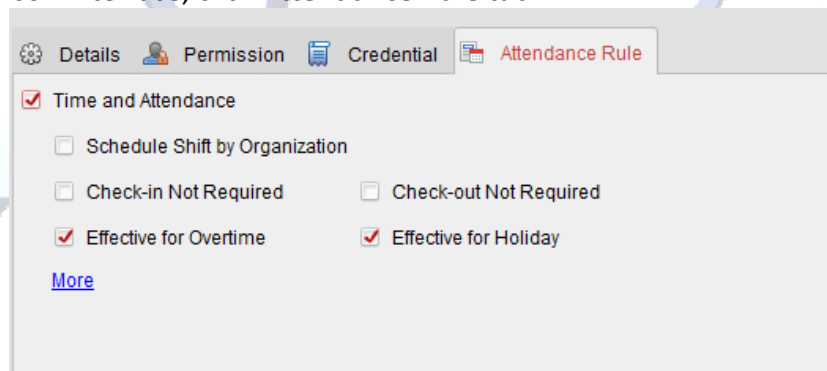
### Adding Person (Attendance Rule)

You can set the attendance rule for the person.

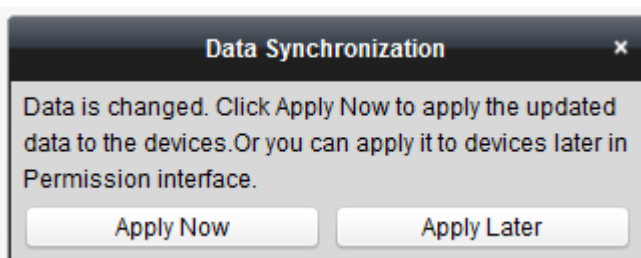
**Note:** This tab page will display when you select **Non-Residence** mode in the application scene when running the software for the first time.

#### Steps:

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



2. If the person joins in the time and attendance, check the **Time and Attendance** checkbox to enable this function for the person. Then the person's card swiping records will be recorded and analyzed for time and attendance.  
For details about Time and Attendance, click **More** to go to the Time and Attendance module.
3. Click **OK** to save the settings.
4. Once the person's details have been saved, if the changes affect the access to doors / readers etc, then a 'Data Synchronise' dialog box will open to allow you to download / synchronize the changes into the controller.




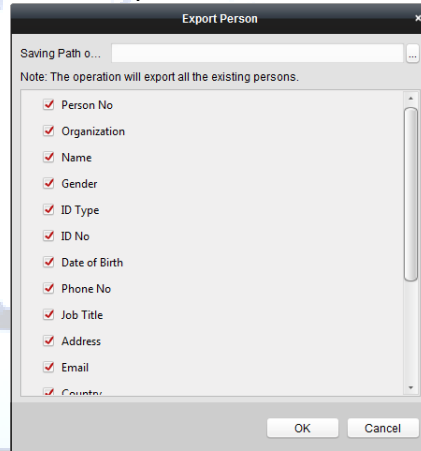
- 
5. Click 'apply now' to download the changes to the controller(s)

## Importing and Exporting Person Information

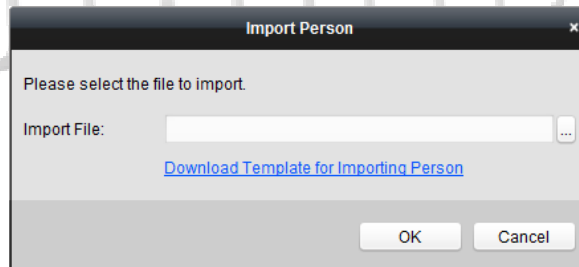
The person information can be imported and exported in batch.


### Steps:

1. **Exporting Person:** You can export the added persons' information in Excel format to the local PC.
  - 1) After adding the person, you can click **Export Person** button in the Person and Card tab to pop up the following dialog.
  - 2) Click  to select the path of saving the exported Excel file.
  - 3) Check the checkboxes to select the person information to export.



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



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

To bulk add cards into the system, export the file, modify it with all the card numbers you want to add and then import it into the system.

## Getting Person Information from Access Control Device

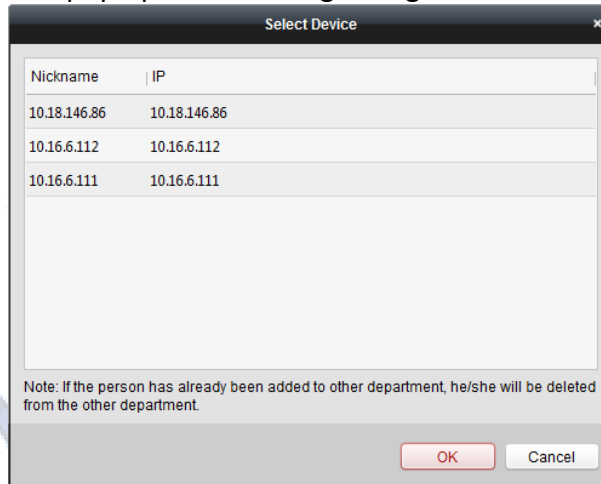
If the added access control device has been configured with person information (including person details, fingerprint, issued card information), you can get the person information from the device

and import to the client for further operation.

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

**Steps:**

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





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

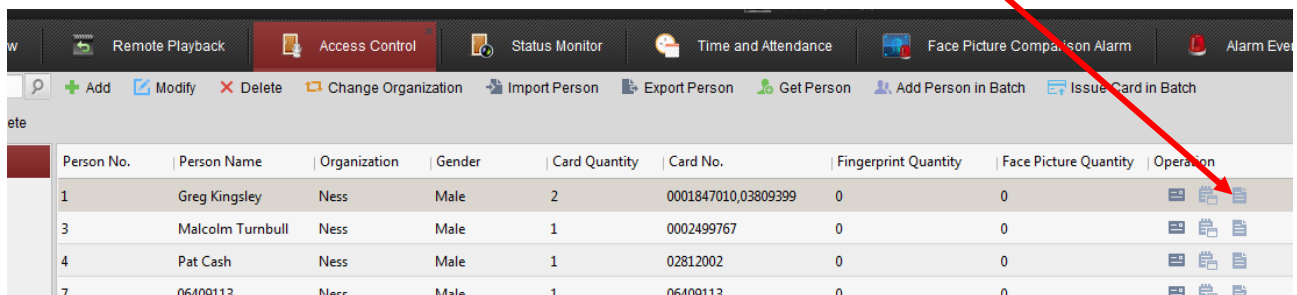
**Notes:**


- The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- The gender of the persons will be **Male** by default.
- Up to 10,000 persons with up to 5 cards each can be imported.

## Managing Person

### Modifying and Deleting Person

To modify the person information and attendance rule, click  or  in the Operation column, or select the person and click **Modify** to open the editing person dialog.



You can click  to view the person's card swiping records.

Serial No.	Event Type	Card Holder	Card Type	Card No.
1	Legal Card Authe...	Greg Kingsley	Normal Card	03809399
2	Legal Card Authe...	Greg Kingsley	Normal Card	03809399
3	Legal Card Authe...	Greg Kingsley	Normal Card	03809399
4	Legal Card Authe...	Greg Kingsley	Normal Card	03809399
5	Legal Card Authe...	Greg Kingsley	Normal Card	03809399
6	Legal Card Authe...	Greg Kingsley	Normal Card	03809399

To delete the person, select a person and click **Delete** to delete it.

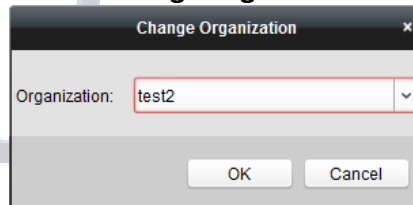
**Note:** If a card is issued to the current person, the linkage will be invalid after the person is deleted.

## Changing Person to Other Organization

You can move the person to another organization if needed.

### Steps:

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



A dialog box titled "Change Organization" with a close button (X) in the top right corner. It contains a label "Organization:" followed by a dropdown menu showing "test2". At the bottom, there are two buttons: "OK" and "Cancel".

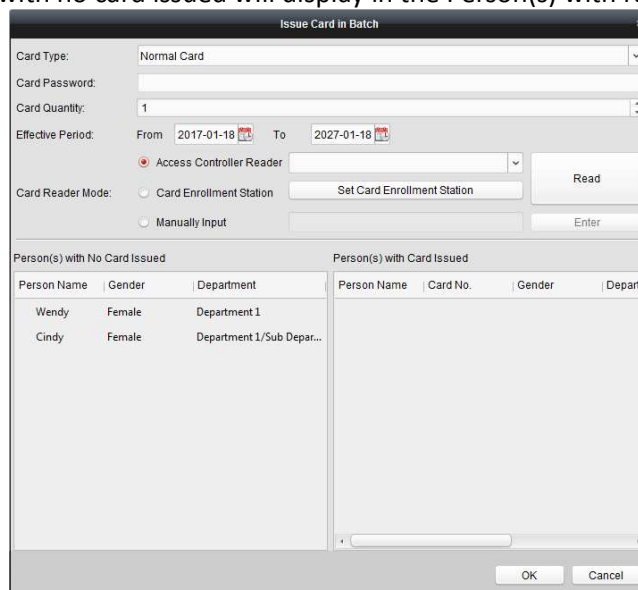
2. Select the organization to move the person to.
3. Click **OK** to save the settings.

## Issuing Card in Batch

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

### Steps:

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



A dialog box titled "Issue Card in Batch" with a close button (X) in the top right corner. It contains several fields: "Card Type:" (Normal Card), "Card Password:" (empty), "Card Quantity:" (1), "Effective Period:" (From 2017-01-18 To 2027-01-18), "Card Reader Mode:" (Access Controller Reader selected), and "Person(s) with No Card Issued" and "Person(s) with Card Issued" tables. The "Person(s) with No Card Issued" table has columns: Person Name, Gender, Department. It lists Wendy (Female, Department 1) and Cindy (Female, Department 1/Sub Depart...). The "Person(s) with Card Issued" table has columns: Person Name, Card No., Gender, Departm. At the bottom, there are "OK" and "Cancel" buttons.



---

2. Select the card type according to actual needs.


**Note:** For details about the card type, refer to *Adding Person*.

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

**Note:** The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to *Chapter 4.9.4 Card Reader Authentication*.

4. Input the card quantity issued for each person.

For example, if the Card Quantity is 3, you can read or enter three card No. for each person.

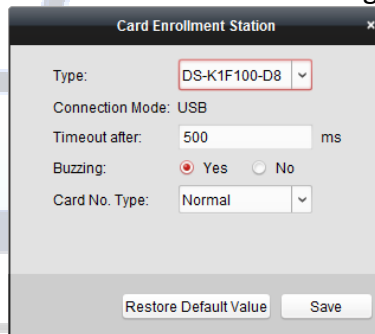
5. Click  to set the effective time and expiry time of the card.

6. Select the Card Reader Mode for reading the card No.

- **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.

- **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.

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



1) Select the Card Enrollment Station type.

2) Currently, the supported card reader types include DS-K1F100-D8E and **DS-K1F180-D8E**

3) Set the parameters about the connected card enrollment station.

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

4) Click **Save** button to save the settings.

You can click **Restore Default Value** button to restore the defaults.

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

7. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.


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

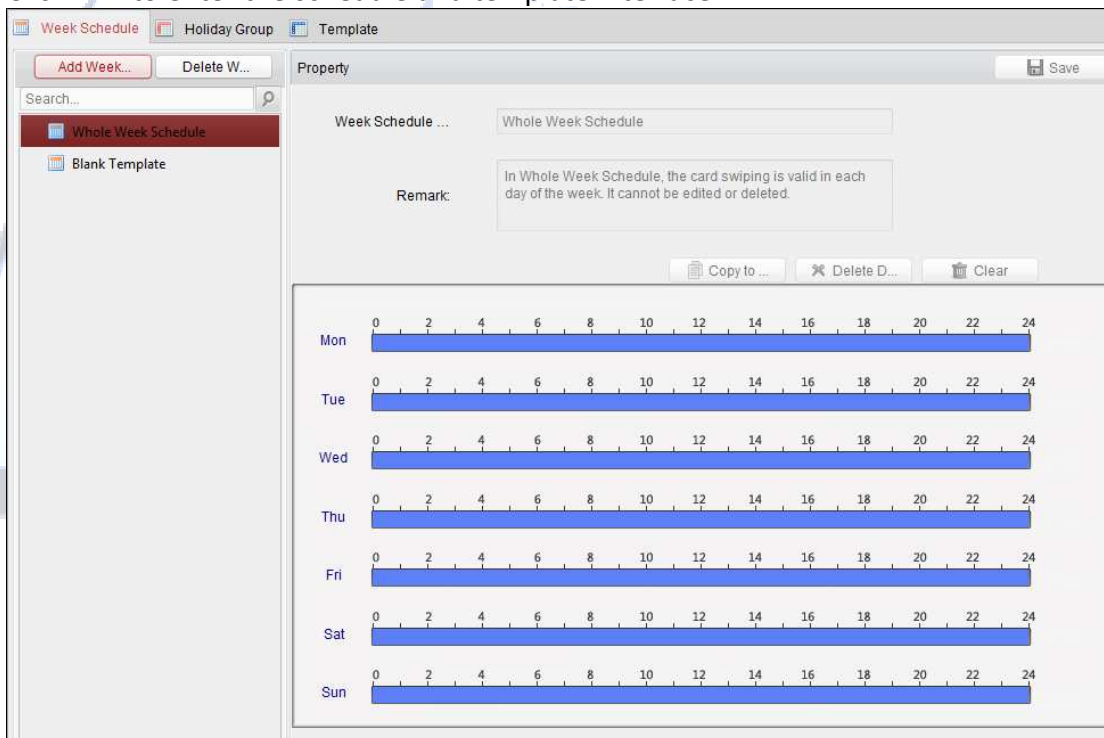
## 4.7 Schedule and Template

### Purpose:

Schedules allow you to set what times and day's events will occur. E.g. Door Auto unlocking, what times card holder can access doors etc.

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

Click  to enter the schedule and template interface.



You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, please refer to *Chapter Error! Reference source not found. Error! Reference source not found.*

### Week Schedule

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

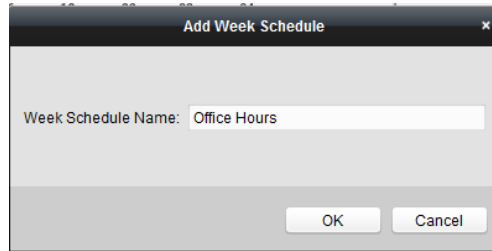
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

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

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


**Steps:**

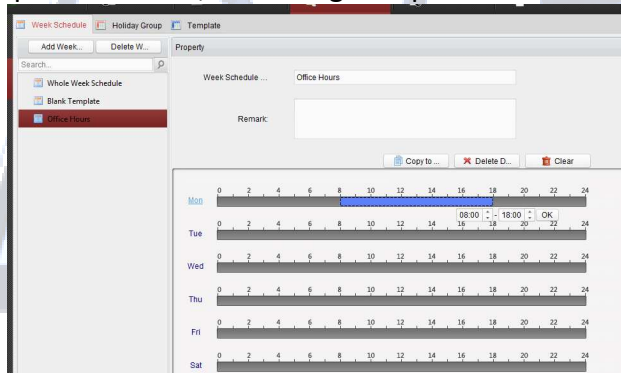
1. Click **Add Week Schedule** button to pop up the adding schedule interface.



2. Input a name of week schedule (e.g. Office Access Hours) and click **OK** button to add the week schedule.
3. Select the 'added week schedule' in the schedule list and you can view its property on the right.



You can edit the week schedule name and input the remark / comment information for future reference.

4. On the week schedule, click and drag on a day to draw on the schedule, which means in that period of time, the configured permission is activated. 



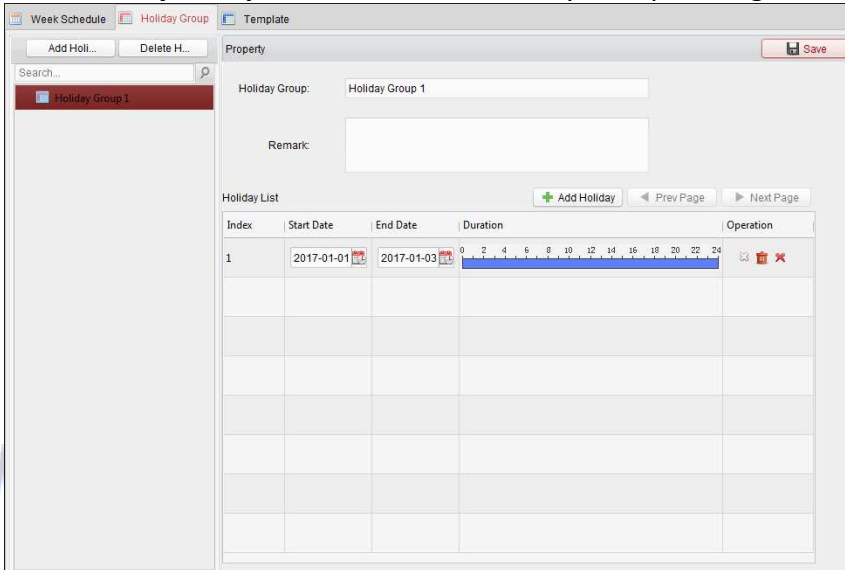
e.g.

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

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

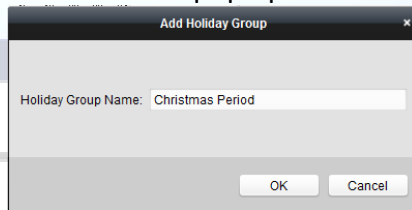
# Holiday Group

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



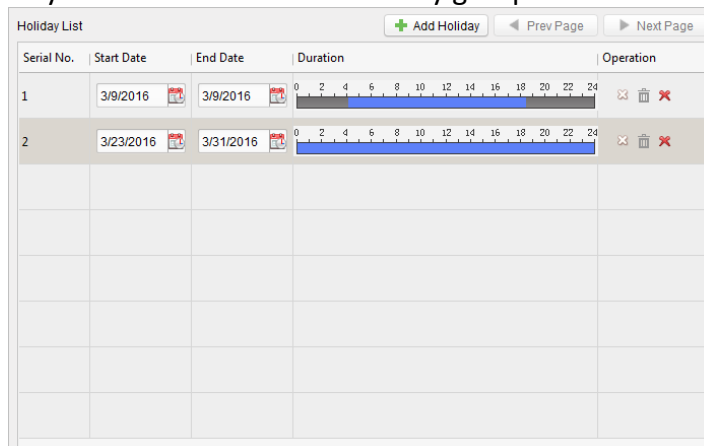
**Steps:**

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




2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.
3. Select the added holiday group and you can edit the holiday group name and input the remark information.
4. Click **Add Holiday** icon on the right to add a holiday period to the holiday list and configure the duration of the holiday.


**Note:** Up to 16 holidays can be added to one holiday group.






1) On the period schedule, click and drag to draw the period, which means in that period of time, the configured permission is activated.

**Note:** Up to 8 time durations can be set for each period in the schedule.

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

3) When the cursor turns to , you can lengthen or shorten the selected time bar.

4) Optionally, you can select the schedule time bar, and then click  to delete the selected time bar, or click  to delete all the time bars of the holiday, or click  to delete the holiday directly.

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

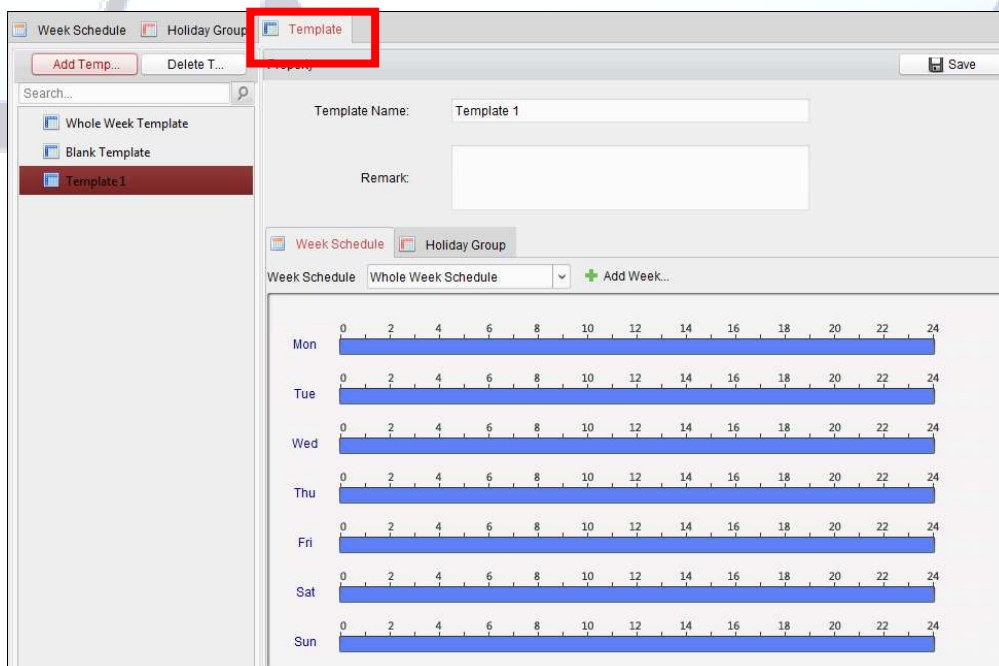
**Note:** The holidays cannot be overlapped with each other.

## Schedule Template

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

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

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



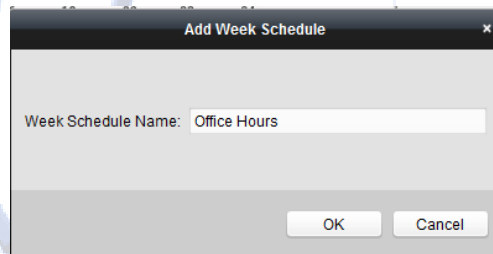
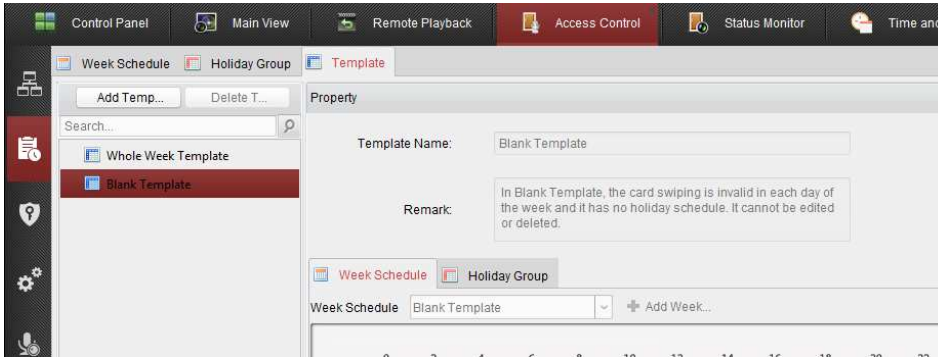
There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

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

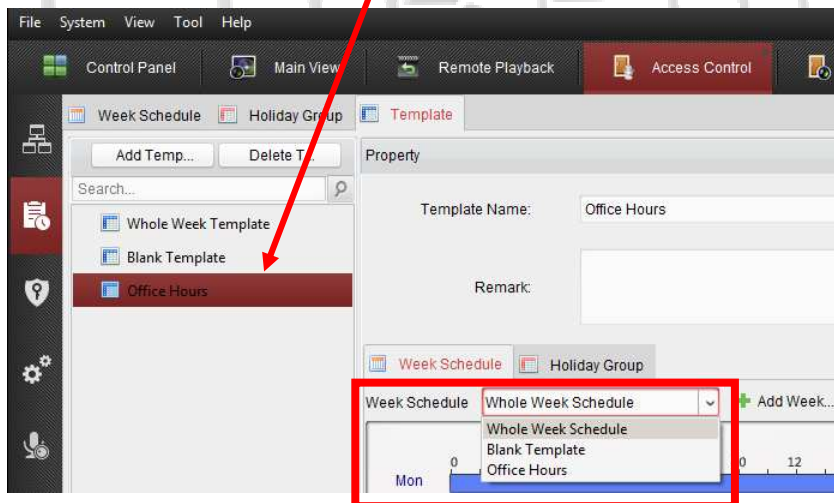
You can define custom templates on your demand.

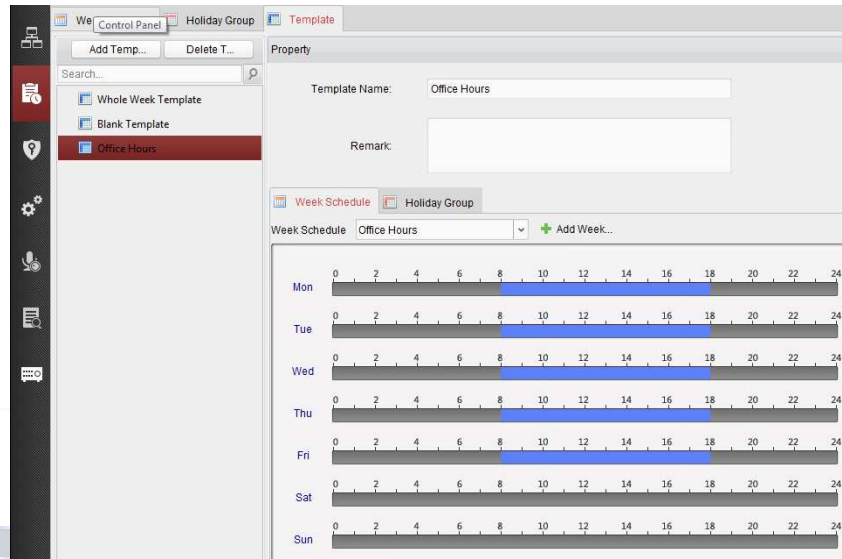
**Steps:**

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



2. Input the template name (for future use that makes easier reference in the future) in the text field and click **OK** button to add the template.
3. Select the added template (from the left hand window) and you can edit its property on the right. You can edit the template name and input the remark information.
4. Select a week schedule to apply to the schedule. Click **Week Schedule** tab and select a schedule in the dropdown list.

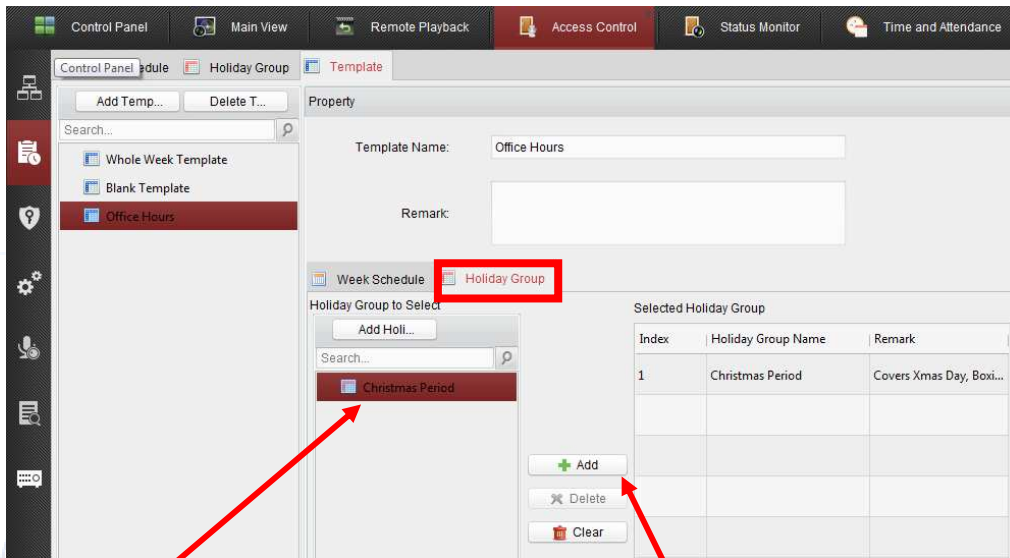






You can also click **+ Add Week Schedule** to add a new week schedule. For details, refer to *Chapter Error! Reference source not found. Error! Reference source not found.*

5. Select holiday groups to apply to the schedule.

**Note:** Up to 4 holiday groups can be added.



Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one from this screen. For details, refer to *Chapter 5 When the cursor turns to *, you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.

When the cursor turns to , you can lengthen or shorten the selected time bar.

8. 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.
9. Click **Save** to save the settings.



---

### **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.

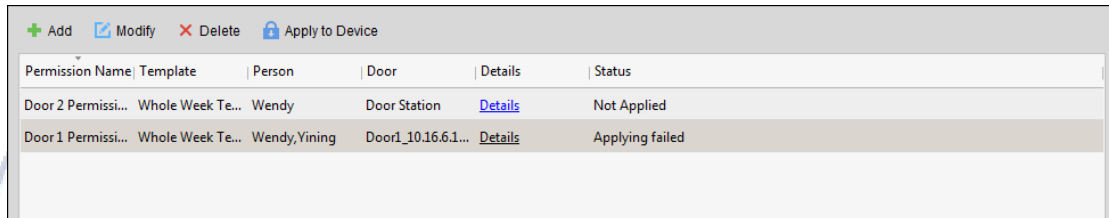
Click **Save** button to save the settings.



## 4.8 Permission Configuration

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

Click  icon to enter the Access Control Permission interface.



Permission Name	Template	Person	Door	Details	Status
Door 2 Permissi...	Whole Week Te...	Wendy	Door Station	<a href="#">Details</a>	Not Applied
Door1 Permissi...	Whole Week Te...	Wendy,Yining	Door1_10.16.6.1...	<a href="#">Details</a>	Applying failed

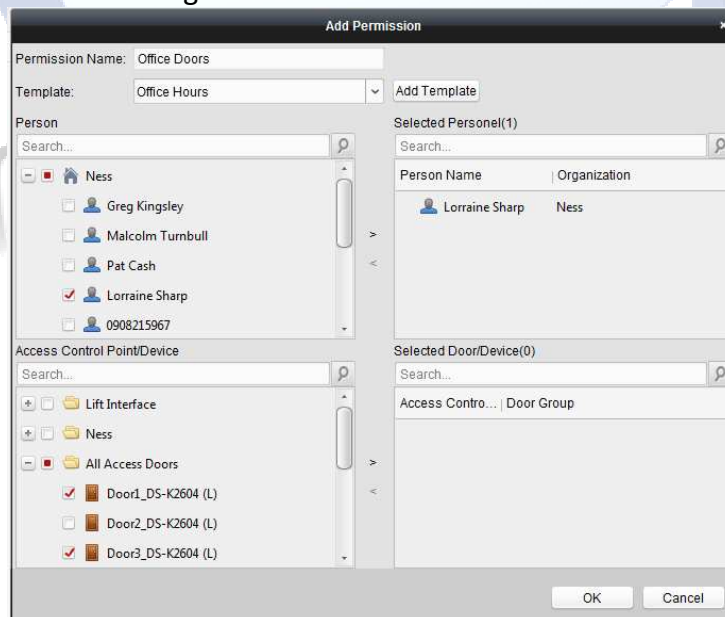
### Adding Permission

#### Purpose:

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

#### Steps:

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



The 'Add Permission' dialog box contains the following information:

- Permission Name: Office Doors
- Template: Office Hours
- Person list: Lorraine Sharp (selected)
- Selected Personnel(1): Lorraine Sharp, Ness
- Access Control Point/Device list: Door1\_DS-K2604 (L), Door2\_DS-K2604 (L), Door3\_DS-K2604 (L) (all selected)
- Selected Door/Device(0):

2. In the Permission Name field, input the name for the permission as desired.
  3. Click on the dropdown menu to select a template for the permission. (e.g. Office Hours)
- Note:** You should configure the Schedule Template before permission settings. You can click **Add Template** button from this screen to add the template. Refer to *Chapter 4.5 Error! Not a valid bookmark self-reference.* for details.
- In the Person list, all the added persons are displayed. Select the persons for this Permission

Group.

**Note:** Once Permissions are added, you can also assign the persons to their permissions from the Add / Modify persons Card section. Refer to [Chapter 7.5.2 Adding Person \(Permission / Access Levels\)](#) for details.

4. Check the checkbox(s) to select person(s) and click > to add to the Selected Person list.  
(Optional) You can select the person in Selected Person list and click < to cancel the selection.
5. In the Access Control Point/Device list, all the added access control points (doors) and door stations will display.  
Check the checkbox(s) to select door(s) or door station(s) the person(s) will have access to and click > to add to the selected list.  
(Optional) You can select the door or door station in the selected list and click < to cancel the selection.
6. Click **OK** button to complete the permission adding. The selected person will have the permission to enter/exit the selected door/door station with their linked card(s).
7. (Optional) after adding the permission, you can click **Details** to modify it. Or you can select the permission and click **Modify** to modify.  
You can select the added permission in the list and click **Delete** to delete it.

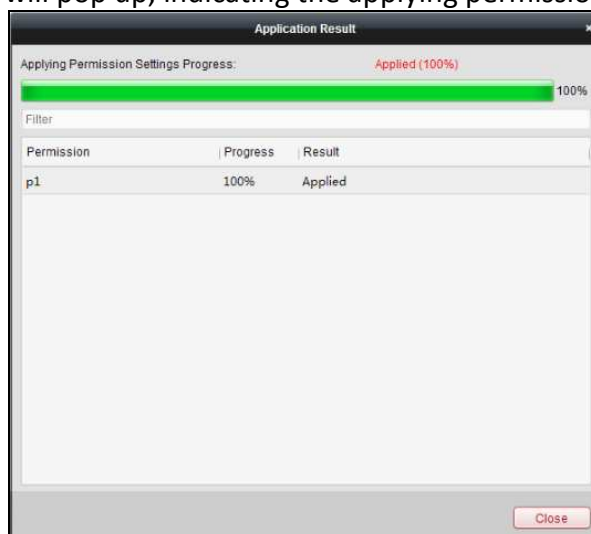
## Applying Permission

### **Purpose:**

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

### **Steps:**

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




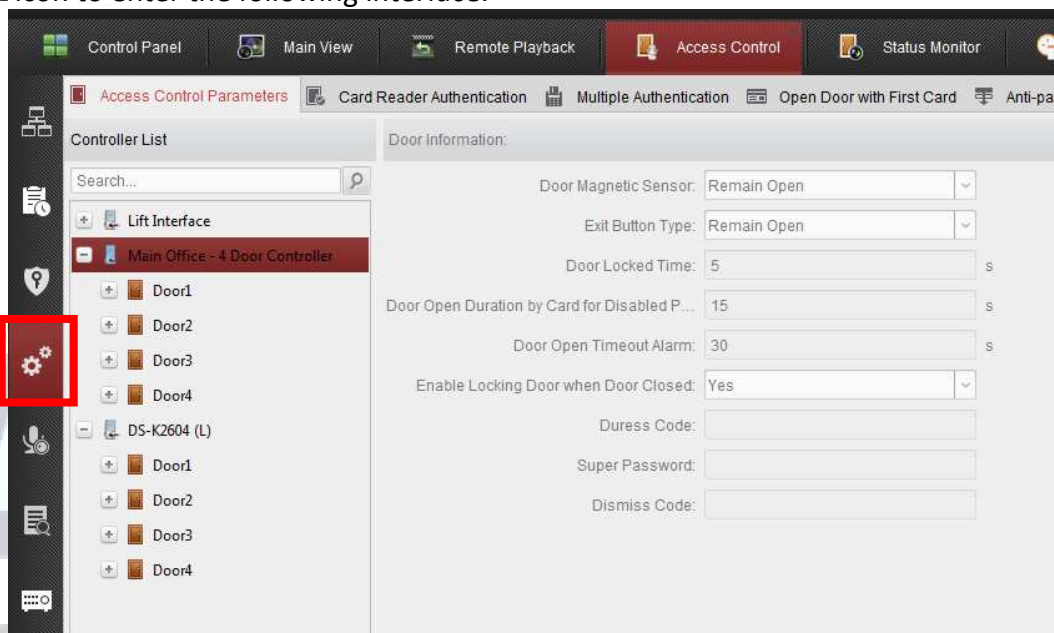
## 4.9 Advanced Functions

### **Purpose:**

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

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

Click  icon to enter the following interface.



### **Access Control Parameters**


### **Purpose:**

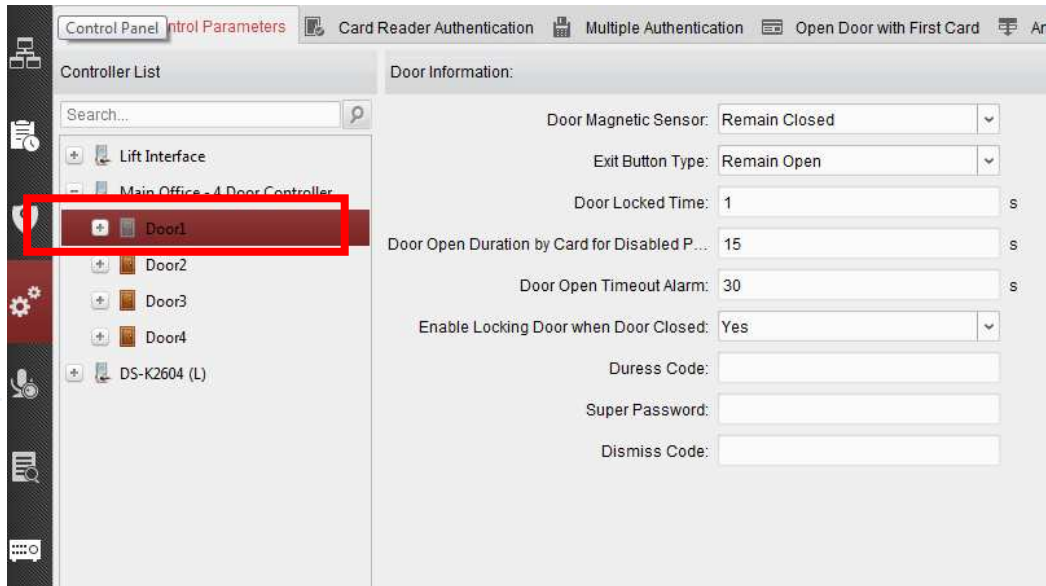
After adding the access control device, you can configure its access control point (door)'s parameters, and its card readers' parameters.

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

### **Door Parameters**

### **Steps:**

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



6. You can editing the following parameters:

**Door Magnetic:** (reed switch for monitoring the state (open/close) of the door. When using door monitoring with a N/C Reed Switch, then select '**Remain Closed**'. If not monitoring the state of the door with a N/C Reed switch then have it set to "**Remain Open**" (Normally Open condition).

**Exit Button Type:** Sets the "Request to Exit Button Type" : If the exit button has a Normally Open contact then set this to "**Remain Open**" and if it uses a Normally Closed contact then set this to "**Remain Close**".

**Door Locked Time:** This is the time the door lock Output will stay activated for (Door unlocked for) after a valid Card read.

**Door Open Duration by Card for Disabled Person:** This is the time the door lock Output will stay activated for (Door unlocked for) after a valid Card read by a user assigned as disabled.

**Door Open Timeout Alarm:** The alarm can be triggered if the door has not been closed (i.e. Door open too long). The time set here sets how long the door can remain opened for after a valid card read, or Request to Exit button activation before the door open timeout alarm will activate.

**Enable Locking Door when Door Closed:** The door can be locked once it is closed even if the Door Locked Time is not reached.

**Duress Code:** The door can open by inputting the duress code when there is duress. At the same time, the client software can receive the duress event.

**Super Password:** The specific person can open the door by inputting the super password.

**Dismiss Code:** Input the dismiss code to stop the buzzer of the card reader.

**Notes:**


- The duress code, Super password, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The duress code, super password, and the dismiss code should contain 4 to 8 digits.

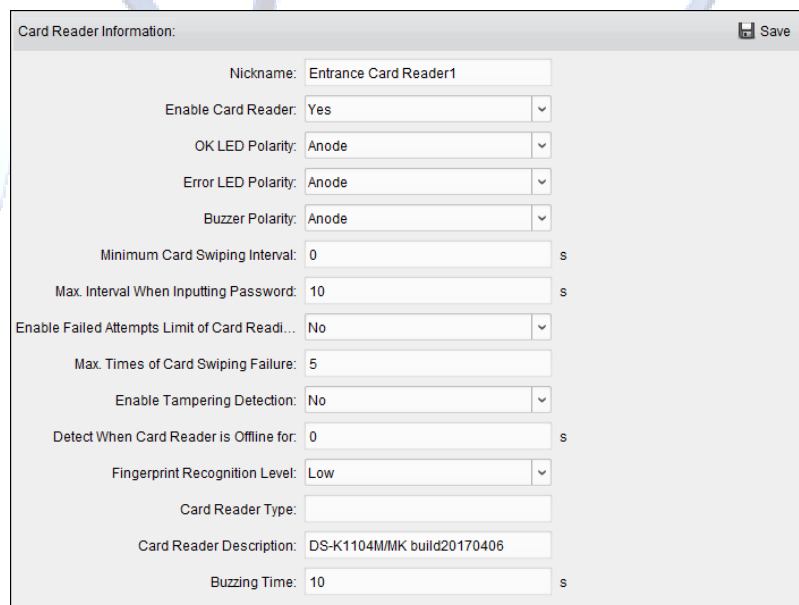
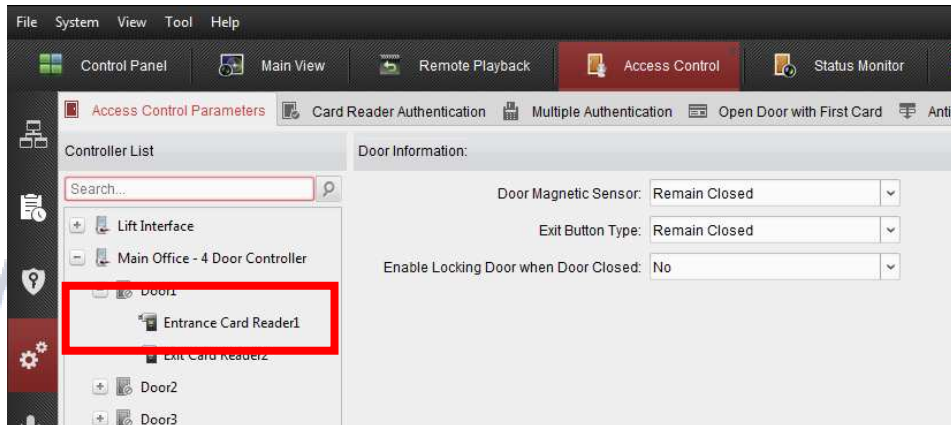
7. Click **Save** button to save parameters.

---

## Card Reader Parameters

### Steps:

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



6. You can editing the following parameters:

**Nickname:** Edit the card reader name as desired. (e.g. Front Door Entry Reader)

**Enable Card Reader:** Select **Yes** to enable the card reader.

**OK LED Polarity:** Select the OK LED Polarity of the card reader main board.

**Error LED Polarity:** Select the Error LED Polarity of the card reader main board.

**Buzzer Polarity:** Select the Buzzer LED Polarity of the card reader main board.

**Minimum Card Swiping Interval:** This sets the minimum time between card Reads. If a card is read after another less than this set time, 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. (Used with RS485 Readers)

**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. (Used with RS485 Readers).

**Fingerprint Recognition Level:** Sets the Fingerprint level for when Fingerprint readers are used.

**Card Reader Type:** If a RS485 reader is used, this field will automatically be filled by the system showing the type of reader.

**Card Reader Description:** If a RS485 reader is used, this field will automatically be filled by the system showing the description of the reader.

**Buzzer Time:** sets how long the reader buzzer will pulse for if programmed to pulse.

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

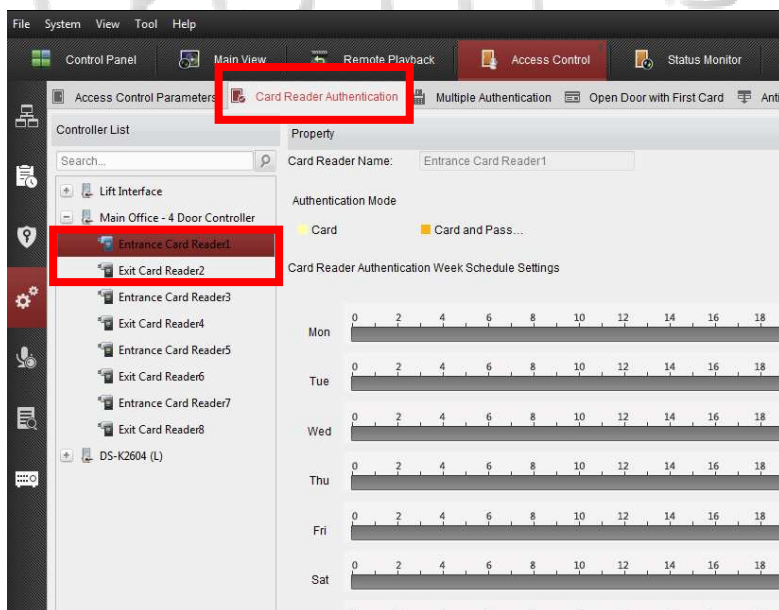
## 4.9.4 Card Reader Authentication

### **Purpose:**

You can set what credential is required and during what time for access to be granted. E.g. Card only during office hours and Card AND Code after hours. This is set for each controller entry point.

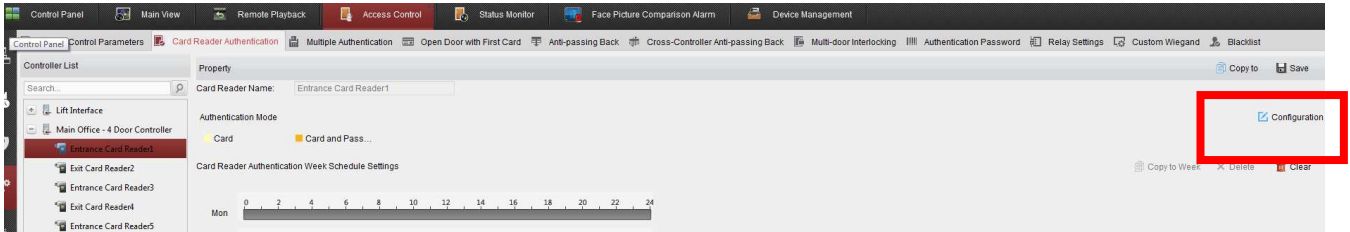
### **Steps:**

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



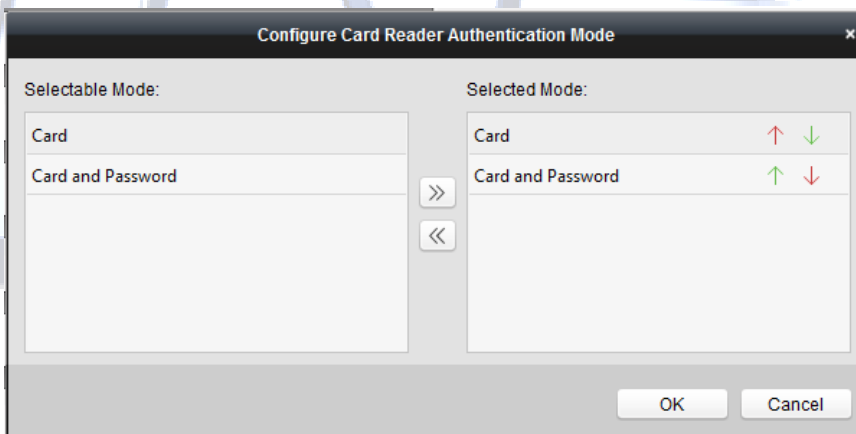
2. Select a card reader authentication mode. The available authentication modes depend on the card reader type:

To see what available options you have for the selected Controller and Reader, click on 'Configure' on the top right of the screen.

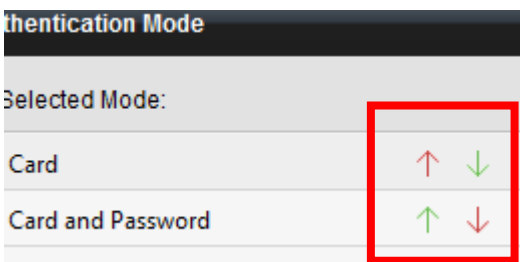


All available options for your Controller and Reader will be displayed on the left hand window in the 'Selectable Mode' column. Select the option you want to use from the 'Selectable Mode'

column and then select click on the  to add them to the 'Selected Mode'.

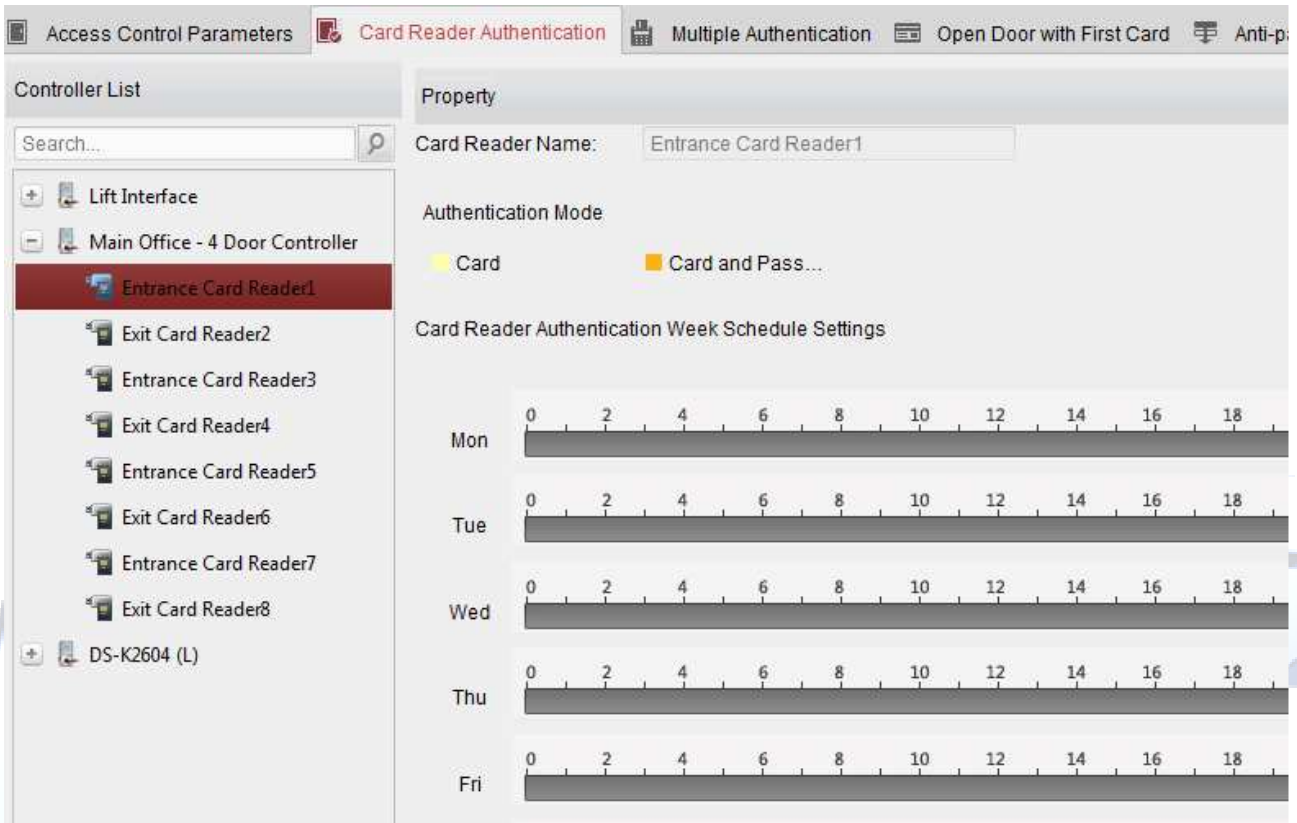


Once selected, you can then set them in the required order they will appear in the settings page by using the up and down arrows options.





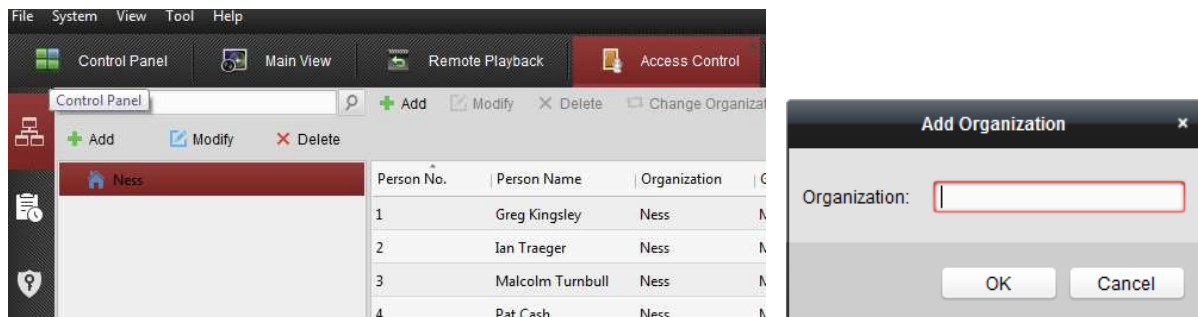
They will then display in the order you selected.



The following possible options are dependent on the Controller and Reader you have.

- **Card:** The door can be unlocked by presenting a Valid Card only.
  - **Card and Password:** The door can open by both inputting the card password and swiping the card.
- Note:** Here the password refers to the password set when issuing the card to the person.
- Chapter 1* In the organization list on the left, you should add a top organization as the parent organization of all organizations.

Click **Add** button to pop up the adding organization interface.



5. Input the Organization Name as desired.
6. Click **OK** to save the adding.
7. You can add multiple levels of organizations according to the actual needs.

To add sub organizations, select the parent organization and click **Add**.  
 Repeat *Step 2* and *3* to add the sub organization.  
 Then the added organization will be the sub-organization of the upper-level organization.

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

### Modifying and Deleting Organization

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

**Notes:**

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

Person Management.

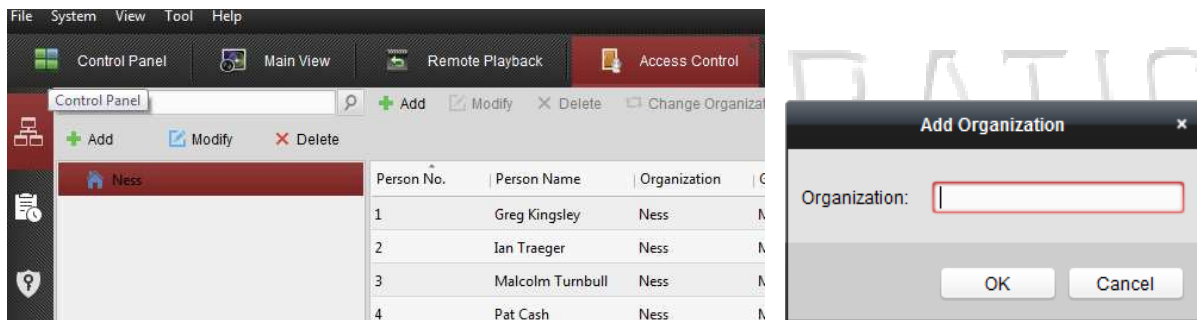
- **Card or Authentication Password:** The door can open by inputting the authentication password (PIN ONLY) or swiping the card.

**Note:** Here the authentication password refers to the password set to open the door.  
 Refer to *Chapter Error! Reference source not found. Error! Reference source not found.*

- **Fingerprint:** The door can open by only inputting the fingerprint.
- **Card or Fingerprint:** The door can open by inputting the fingerprint or swiping the card.
- **Password and Fingerprint:** The door can open by both inputting the card password and inputting the fingerprint.

**Note:** Here the password refers to the card password set when issuing the card to the person. Refer to *Chapter 1 In the organization list on the left, you should add a top organization as the parent organization of all organizations.*

Click **Add** button to pop up the adding organization interface.



8. Input the Organization Name as desired.
9. Click **OK** to save the adding.
10. You can add multiple levels of organizations according to the actual needs.

To add sub organizations, select the parent organization and click **Add**.  
 Repeat *Step 2* and *3* to add the sub organization.  
 Then the added organization will be the sub-organization of the upper-level organization.

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

### Modifying and Deleting Organization

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

**Notes:**

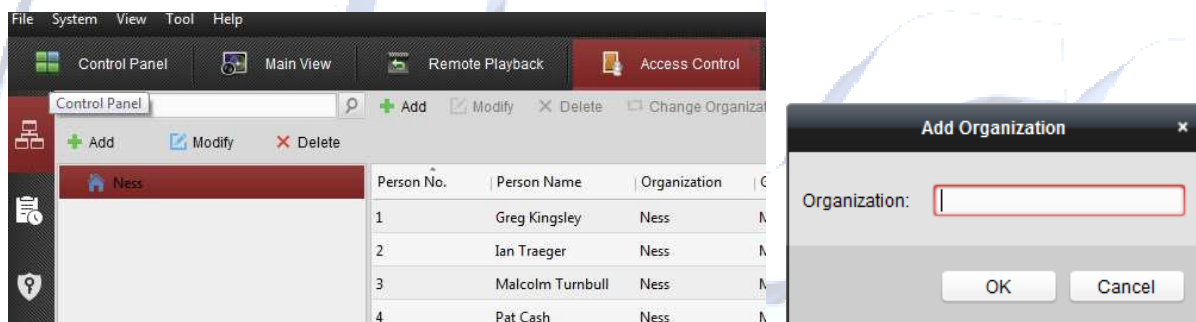
- The lower-level organizations will be deleted as well if you delete an organization.
- Make sure there is no person added under the organization, or the organization cannot be deleted.

Person Management.

- **Card and Fingerprint:** The door can open by both inputting the fingerprint and swiping the card.
- **Card, Password and Fingerprint:** The door can open by inputting the fingerprint, inputting the card password, and swiping the card.

**Note:** Here the password refers to the card password set when issuing the card to the person. Refer to *Chapter 1 In the organization list* on the left, you should add a top organization as the parent organization of all organizations.

Click **Add** button to pop up the adding organization interface.



11. Input the Organization Name as desired.
12. Click **OK** to save the adding.
13. You can add multiple levels of organizations according to the actual needs.

To add sub organizations, select the parent organization and click **Add**.

Repeat *Step 2* and *3* to add the sub organization.

Then the added organization will be the sub-organization of the upper-level organization.

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

### **Modifying and Deleting Organization**

**You can select the** added organization and click **Modify** to modify its name.

You can select an organization, and click **Delete** button to delete it.

**Notes:**

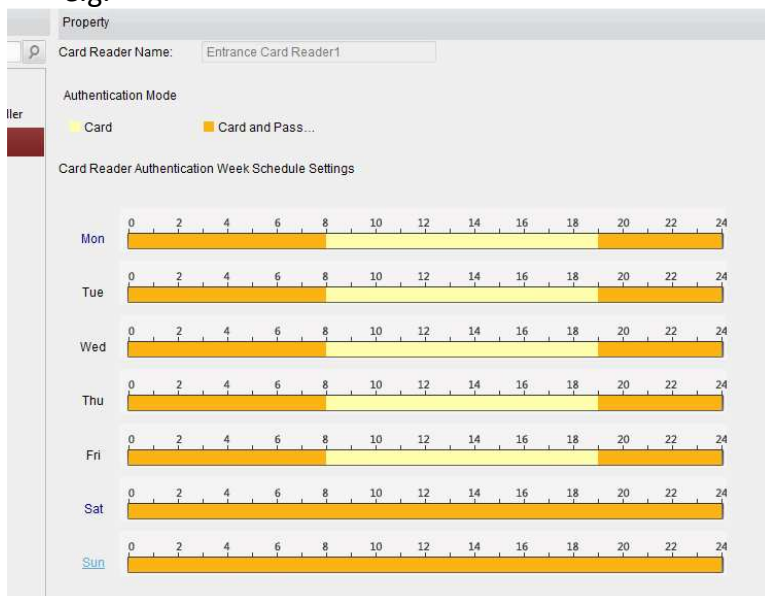
The lower-level organizations will be deleted as well **if** you delete an organization.

**Make sure** there is no person added under the organization, or the organization cannot be deleted.

Person Management.

3. Select the required method for unlocking the door lock and then “click and drag” your mouse on a day to draw a color bar on the schedule. The ‘drawn / selected’ hours means in that period of time, the card reader authentication is valid.

e.g.

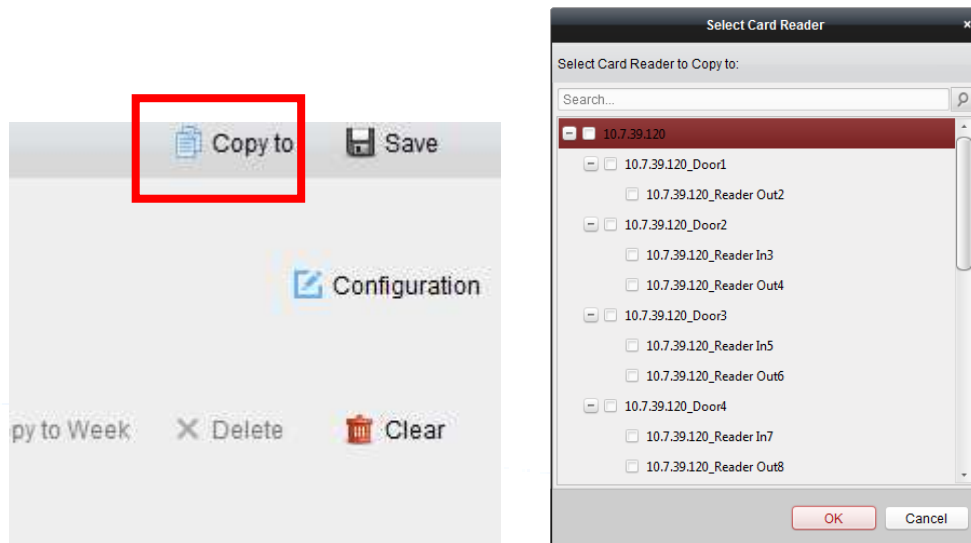


- Repeat the above step to set other time periods.  
Or you can select a configured day and click **Copy to Week** button (from the top right of the window) to copy the same settings to the whole week.  
(Optional) You can click **Delete** button to delete the selected time period or click **Clear** button to delete all the configured time periods.



(Optional) 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 to copy the settings to other card readers.



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

## 4.9.5 Open Door with First Card

### **Purpose:**

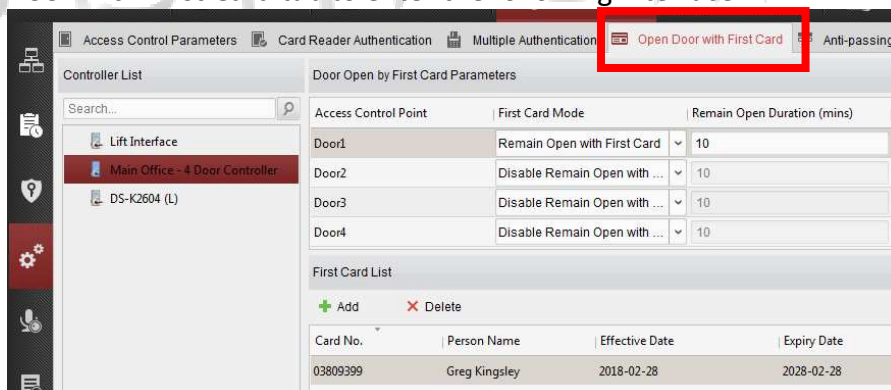
You can set multiple first cards for one access control point. After the first card is presented to the programmed reader, it allows multiple persons access through this control door point or other authentication actions.

The first card mode contains Remain Open with First Card or Disable Remain Open with First Card.

**Remain Open with First Card:** The door remains open for the configured time duration after the first card is presented until 'the remain open duration' expires.

### **Steps:**

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

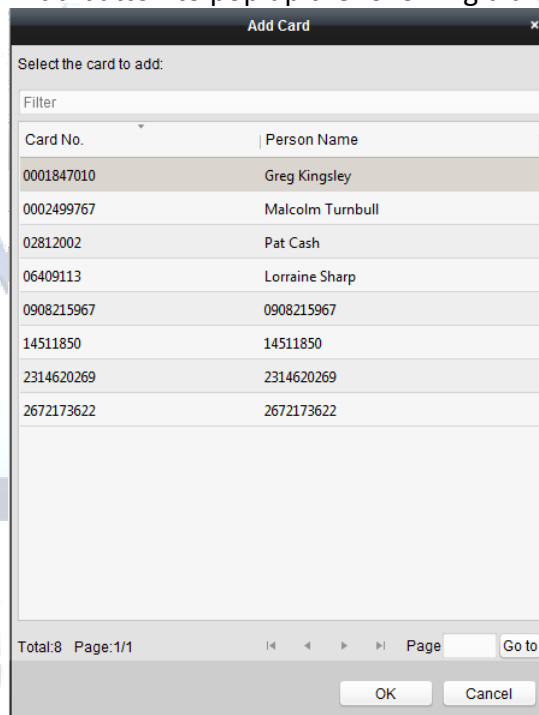


- Select an access control device from the list on the left.
- Select the first card mode in the drop-down list for the access control point.
- (Optional) If you select Remain Open with First Card, you should set the 'remain open duration'.

**Notes:**

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

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



A. Select the cards to add as first card for the door

- a. **Note:** Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter Error! Reference source not found. Error! Reference source not found..*

B. Click **OK** button to save adding the card.

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

---

# Door Status Management

## Purpose:

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

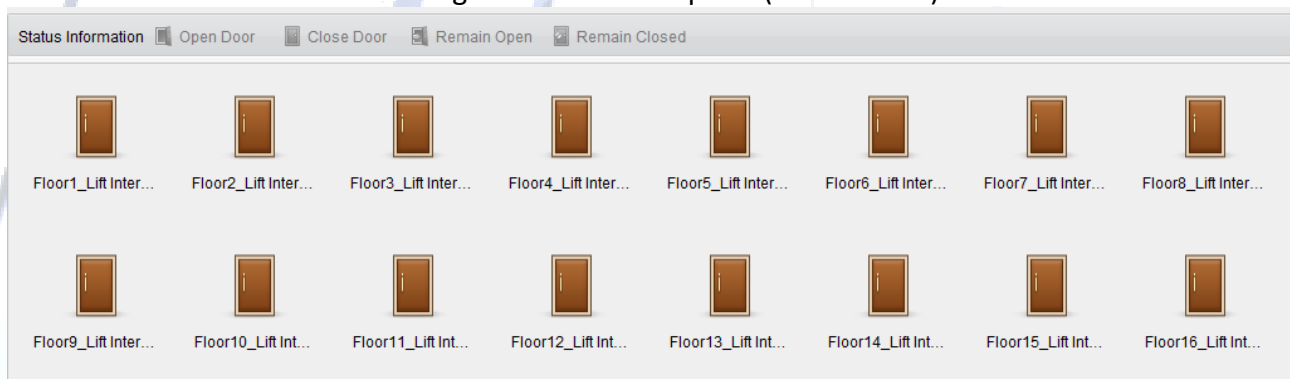


Click **Status Monitor** icon on the control panel to enter the Status Monitor interface.

## 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 4.4.2 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

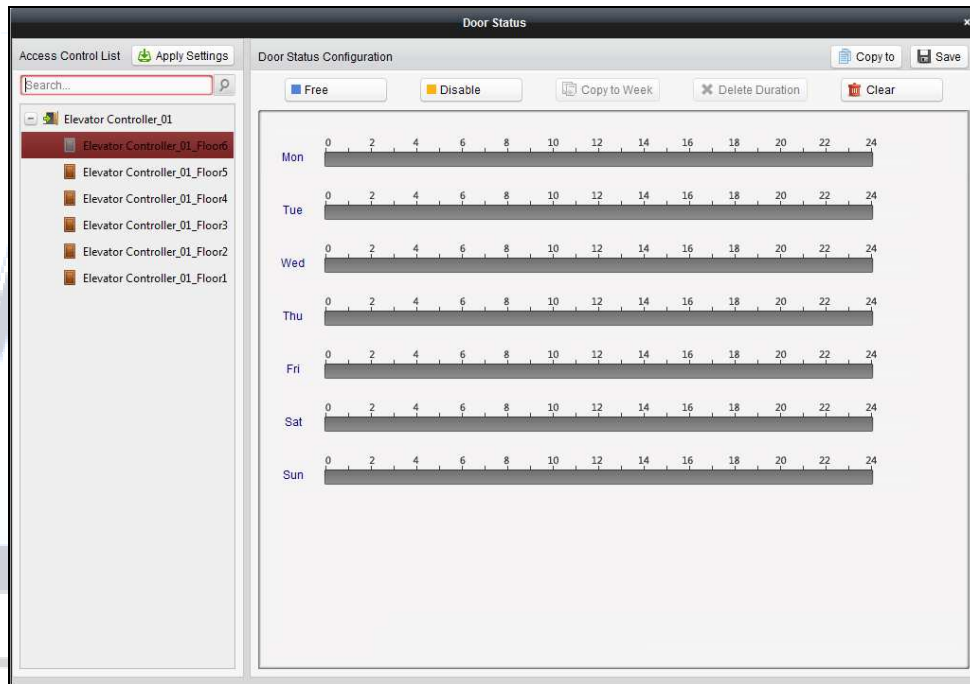
## Purpose:

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

## Steps:

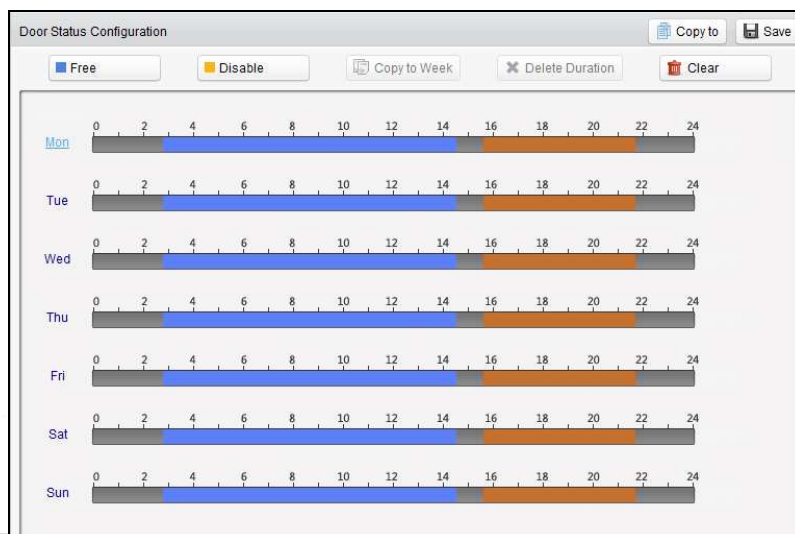


- Click **Status Monitor** icon on the control panel and click **Status Duration** button to enter the Status Duration interface.





- Click to select a floor from the access control list on the left of the pop-up window.
- On the Door Status Configuration panel on the right, draw a schedule for the selected floor.
  - 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 **Free**.
    - Disable:** You cannot press the floor button during the configured duration. The brush is marked as **Disable**.
  - Click and drag on the timeline to draw a colour bar on the schedule to set the duration.



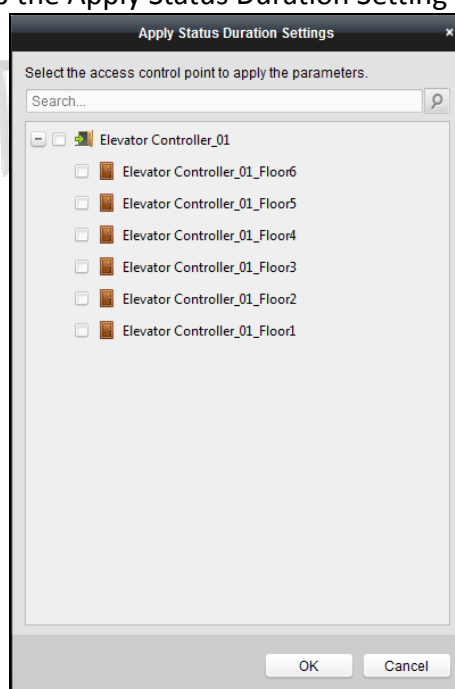


**Note:** The min. segment of the schedule is 30min.

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.

- Optionally, you can select the schedule time bar and click **Copy to Week** to copy the time bar settings to the whole week.
- 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.
- Click **Save** to save the settings.
- You can click **Copy to** button to copy the schedule to other doors.
- Click **Apply Settings** to pop up the Apply Status Duration Setting dialog box.



- 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).

---

# Appendix

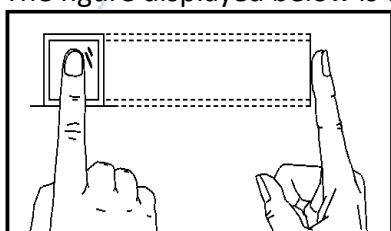
## 4.10 Tips for Scanning Fingerprint

### Recommended Finger

Forefinger, middle finger or the third finger.

### Correct Scanning

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

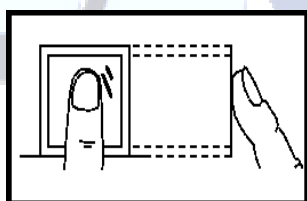


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

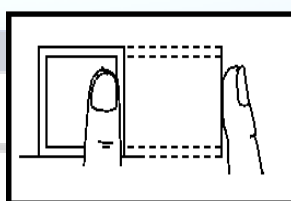
### Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

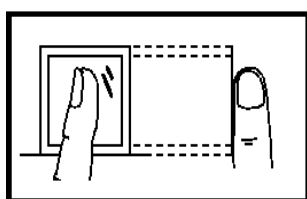
#### Vertical



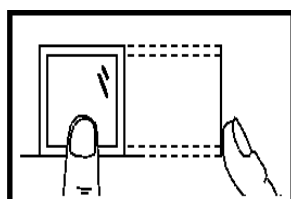
#### Edge I



#### 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.

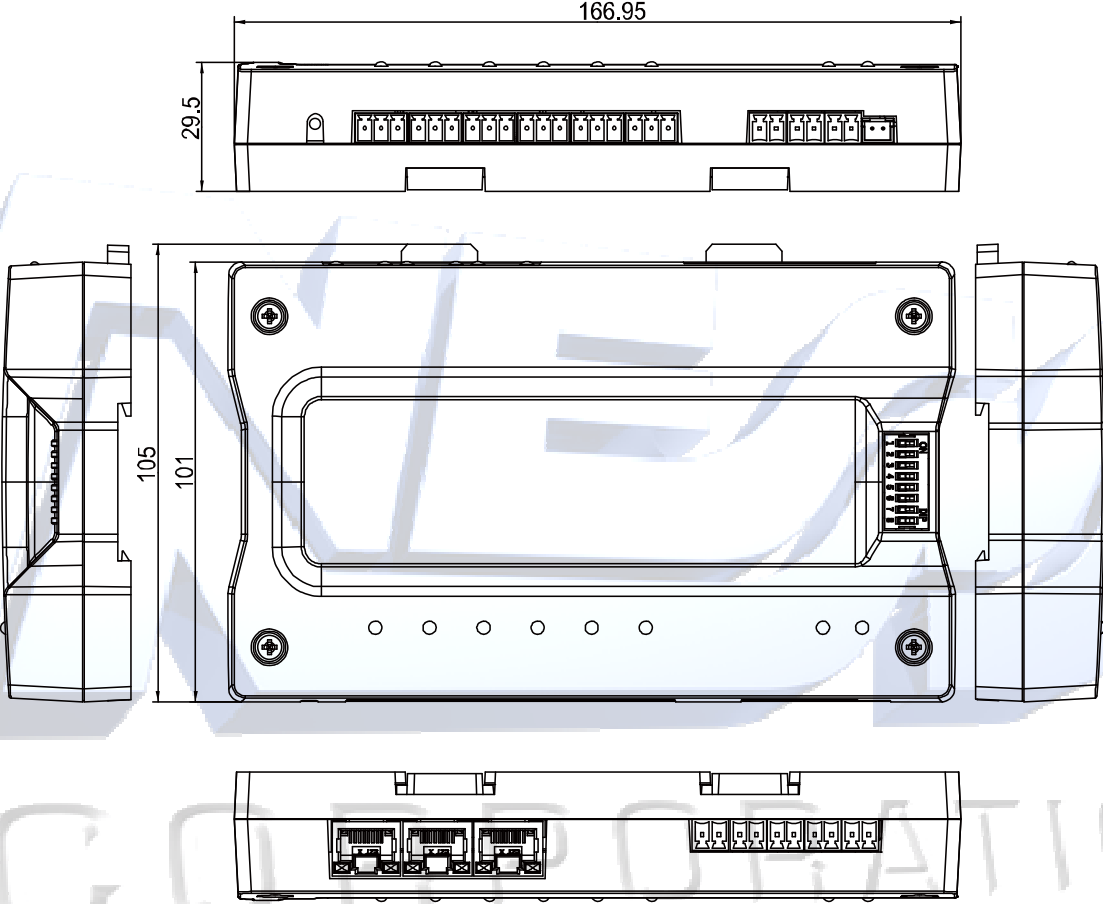
### Others

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.

# 4.11 Device Dimension

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



---

## 4.12 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
DS-K2202

0100001070116



First Choice for Security Professionals

This manual has been modified by Ness Corporation for our valued customers.



[www.nesscorporation.com](http://www.nesscorporation.com)

[www.hikvision.com](http://www.hikvision.com)