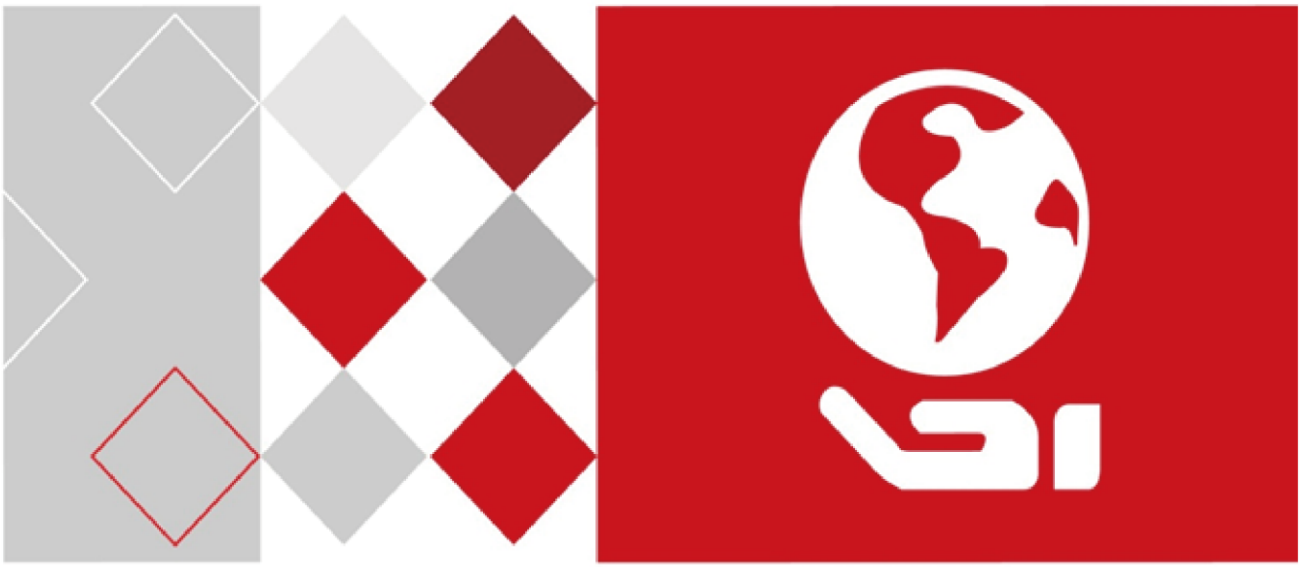
HIKVISION



Access Control Terminal

User Manual

User Manual

©2017 Hangzhou Hikvision Digital Technology Co., Ltd.

This manual is applied for access control terminal.

Series	Model
Standalone Access Control Terminal Fingerprint Access Control Terminal	DS-K1T105E/M
	DS-K1T105E/M-C（with Camera）
	DS-K1T200EF/MF
	DS-K1T200EF/MF-C（with Camera）
	DS-K1T201EF/MF
	DS-K1T201EF/MF-C（with Camera）

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

About this Manual

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

Trademarks

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

Disclaimer

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

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

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

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

Support

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

Regulatory Information

FCC Information

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

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

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

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

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

FCC Conditions

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

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

EU Conformity Statement

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

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

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

Industry Canada ICES-003 Compliance

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

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut
fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Use only power supplies listed in the user instructions:

Model	Manufacturer
KPL-040F-VI	Channel Well Technology Co Ltd.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger

or property loss.
The precaution measure is divided into **Warnings** and **Cautions**:
Warnings: Neglecting any of the warnings may cause serious injury or death.
Cautions: Neglecting any of the cautions may cause injury or equipment damage.

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

Warnings

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Cautions

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.

- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- The device must not be co-located or operating in conjunction with any other antenna or transmitter

Table of Contents

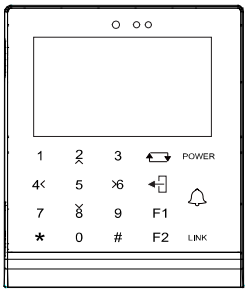
Chapter 1 Overview **1**
1.1 Introduction 1
1.2 Main Features 1
1.2.1 Main Features of DS-K1T105 Series Model 1
1.2.2 Main Features of DS-K1T200/201 Series Model 2
Chapter 2 Appearance **4**
2.1 Appearance of DS-K1T105 Series Model 4
2.2 Appearance of DS-K1T200/201 Series Model 4
2.3 Appearance of Keys 5
Chapter 3 Installation **7**
3.1 Installation of DS-K1T105 Series Device 7
3.2 Installation of DS-K1T200/201 Series Device 8
Chapter 4 Terminal Connection **10**
Chapter 5 Wiring Description **13**
5.1 External Device Wiring Overview 13
5.2 The Wiring of External Card Reader 14
5.2.1 The Wiring of External RS-485 Card Reader 14
5.2.2 The Wiring of External Wiegand Card Reader 14
5.3 The Wiring of Electric Lock and Door Contact 15
5.3.1 The Wiring of Electric Lock 15
5.3.2 The Wiring of Door Contact 15
5.4 The Wiring of Exit Button 16
5.5 The Wiring of Alarm Input 16
5.6 The Wiring of External Alarm Device 17
5.7 Card Reader Connection 17
5.7.1 The Wiring of Wiegand 17
5.7.2 The Wiring of RS-485 Output 18
Chapter 6 Activating Access Control Terminal **19**
6.1 Activating via Device 19
6.2 Activating via SADP Software 20
6.3 Activating via Client Software 21
Chapter 7 Basic Operation **24**
7.1 User Management 25
7.1.1 Adding User 25

7.1.2 Managing User 27
7.2 Communication Settings 29
7.2.3 Network Settings 30
7.2.4 Serial Port Settings 31
7.2.5 Wiegand Settings 31
7.2.6 Wi-Fi Settings 32
7.3 System Settings 33
7.3.1 Setting System 34
7.3.2 Managing Data 35
7.3.3 Restoring Settings 36
7.3.4 Door Settings 37
7.3.5 Setting Camera 37
7.4 Time Settings 38
7.5 Upload/Download Settings 39
7.6 Testing 40
7.7 Log Query Settings 40
7.8 System Information 41
Chapter 8 Client Operation 43
8.1 Function Module 43
8.2 User Registration and Login 46
8.3 System Configuration 47
8.4 Access Control Management 48
8.4.1 Adding Access Control Device 49
8.4.2 Viewing Device Status 63
8.4.3 Editing Basic Information 64
8.4.4 Network Settings 65
8.4.5 Capture Settings 67
8.4.6 RS-485 Settings 68
8.4.7 Wiegand Settings 69
8.4.8 Authenticating M1 Card Encryption 69
8.4.9 Remote Configuration 70
8.5 Organization Management 78
8.5.1 Adding Organization 78
8.5.2 Modifying and Deleting Organization 79
8.6 Person Management 79
8.6.1 Adding Person 79

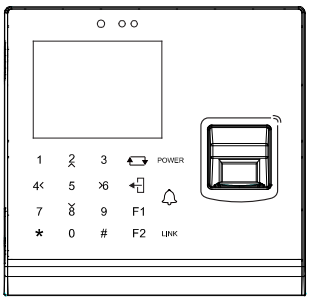
8.6.2 Managing Person 87
8.6.3 Issuing Card in Batch 88
8.7 Schedule and Template 89
8.7.1 Week Schedule 90
8.7.2 Holiday Group 91
8.7.3 Template 92
8.8 Permission Configuration 94
8.8.1 Adding Permission 95
8.8.2 Applying Permission 96
8.9 Advanced Functions 97
8.9.1 Access Control Parameters 97
8.9.2 Card Reader Authentication 100
8.9.3 Multiple Authentication 101
8.9.4 Open Door with First Card 104
8.9.5 Anti-Passing Back 105
8.10 Searching Access Control Event 106
8.10.1 Searching Local Access Control Event 107
8.10.2 Searching Remote Access Control Event 107
8.11 Access Control Event Configuration 108
8.11.1 Access Control Event Linkage 108
8.11.2 Event Card Linkage 109
8.11.3 Cross-Device Linkage 111
8.12 Door Status Management 112
8.12.1 Access Control Group Management 112
8.12.2 Anti-control the Access Control Point (Door) 114
8.12.3 Status Duration Configuration 115
8.12.4 Real-time Card Swiping Record 117
8.12.5 Real-time Access Control Alarm 117
8.13 Arming Control 118
8.14 Time and Attendance 119
8.14.1 Shift Schedule Management 120
8.14.2 Attendance Handling 126
8.14.3 Advanced Settings 130
8.14.4 Attendance Statistics 134
Appendix A Tips for Scanning Fingerprint 139
Appendix B Custom Wiegand Rule Descriptions 140

Chapter 1 Overview

1.1 Introduction



DS-K1T105 is a series of standalone access control terminal with picture capturing function. DS-K1T105 is designed with a 2.8-inch LCD display screen, and HD camera (2 MP optional). It supports face detection, smart card recognition TCP/IP communication method, Wi-Fi communication method, and supports offline operation.



DS-K1T200/201 series and DS-K1T201 Series are optical IP-based fingerprint access control terminal with multiple advanced technologies including fingerprint recognition, face detection, Wi-Fi, smart card recognition, LCD display screen, and picture capturing technology. It is designed with a 2.8-inch LCD display screen, and HD camera (2 MP optional). It is equipped with optical fingerprint recognition module (supporting 1:1 mode and 1:N mode), and supports offline operation.

1.2 Main Features

1.2.1 Main Features of DS-K1T105 Series Model

- Doorbell ringtone settings function
- Touch mode and blue light display technique for keypad
- Stand-alone settings for the terminal
- 2.8-inch LCD display screen
- Transmission modes of wired network (TCP/TP) and Wi-Fi
- Face detection, picture capturing function and QR code authentication implemented by built-in camera (2 MP optional, only supports DS-K1T105E/M -C)

- Supports multiple door opening modes (card, card + password, exit button, etc.)
- Supports RS-485 communication for connecting to external card reader
- Supports working as a card reader, and supports Wiegand interface and RS-485 interface for accessing the controller
- Max. 100,000 valid card No., and Max. 300,000 access control events records storage
- Supports EM card reading (DS-K1T105E/E-C)
- Supports Mifare card reading, including card No. reading, & writing function (DS-K1T105M/M-C)
- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, and duress card alarm
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal
- Data can be permanently saved after power-off.

1.2.2 Main Features of DS-K1T200/201 Series Model

- Doorbell ringtone settings function
- Touch mode and blue light display technique for keypad
- Stand-alone settings for the terminal
- 2.8-inch LCD display screen
- Transmission modes of wired network (TCP/TP) and Wi-Fi
- Face detection, picture capturing function and QR code authentication implemented by built-in camera (2 MP optional, only supports DS-K1T200EF/MF-C and DS-K1T201EF/MF-C)
- Supports RS-485 communication for connecting external card reader
- Supports working as a card reader, and supports Wiegand interface and RS-485 interface for accessing the controller
- Max. 100,000 card No., Max. 300,000 access control events records
- DS-K1T200 series device supports up to 9500 fingerprints storage; DS-K1T201 series device supports up to 5000 fingerprints storage
- Adopts the optical fingerprint module, supporting 1:N mode (fingerprint, card + fingerprint) and 1:1 mode (card + fingerprint)
- Supports multiple authentication modes (card, fingerprint, card + fingerprint, card + password, fingerprint + password, card + fingerprint + password, and so on.)
- Supports EM card reading (DS-K1T200EF/EF-C and DS-K1T201EF/EF-C support the function)
- Supports Mifare card reading, including card No. reading, and sector reading & writing (DS-K1T200MF/MF-C and DS-K1T201MF/MF-C support the function)
- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, duress card alarm, and so on

- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal
- Data can be permanently saved after power-off.

Chapter 2 Appearance

2.1 Appearance of DS-K1T105 Series Model

Please refer to the following content for detailed information of the DS-K1T105 series model.

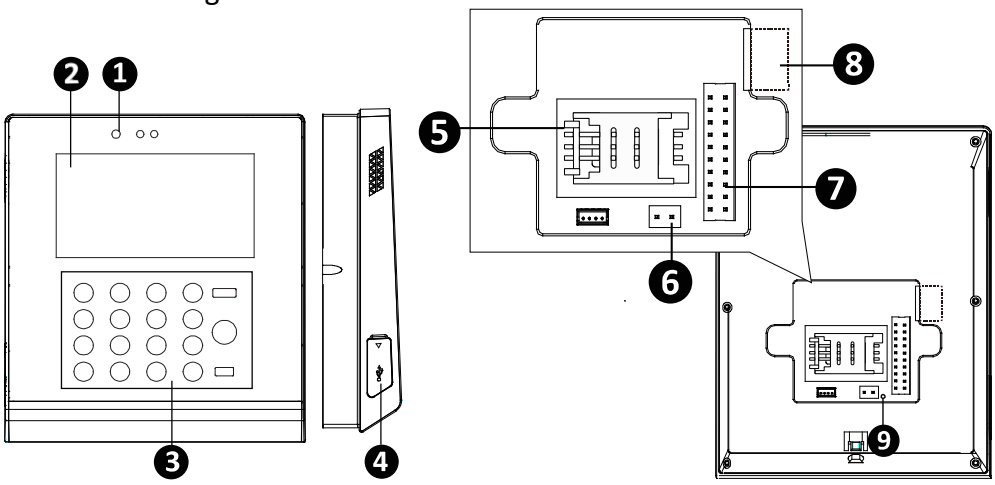


Table 1-1 Description of DS-K1T105 Series Model

No.	Description
1	HD Camera with 2 MP (only DS-K1T105E/M/ -C support)
2	2.8-Inch LCD Display Screen
3	Keypad
4	USB 2.0 Interface
5	PSAM Card Slot
6	Power Interface
7	External Wiring Terminals
8	Ethernet Port
9	Tampering Prevention Switch

2.2 Appearance of DS-K1T200/201 Series Model

Please refer to the following content for detailed information of DS-K1T200 series model

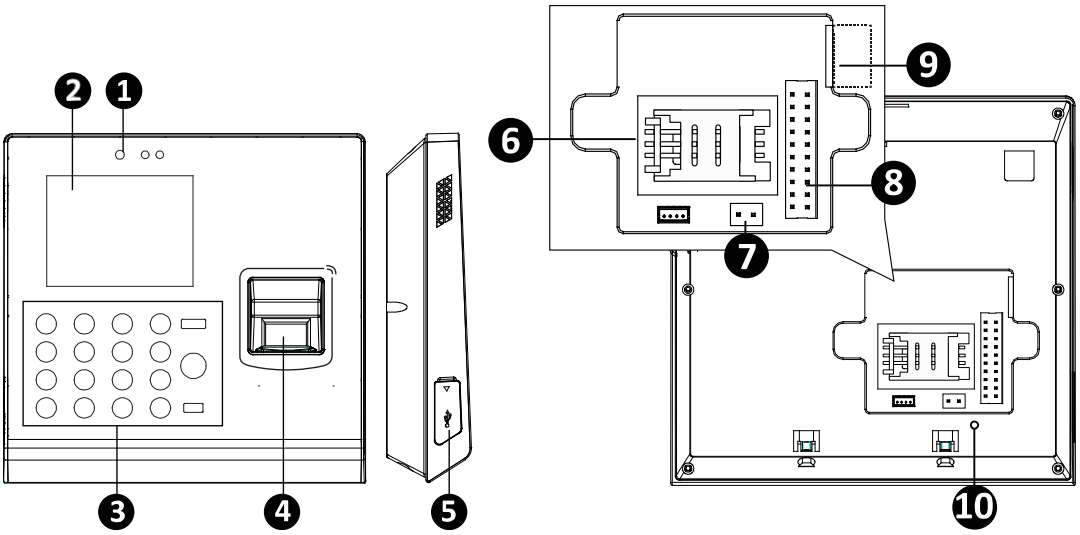


Table 1-2 DS-K1T200/201 Series Fingerprint Access Control Terminal Components

No.	Description
1	HD Camera with 2 MP (only DS-K1T200EF/MF -C support)
2	2.8-Inch LCD Display Screen
3	Keypad
4	Optical Fingerprint Reading Module
5	USB 2.0 Interface
6	PSAM Card Slot
7	Power Interface
8	External Wiring Terminals
9	Ethernet Port
10	Tampering Prevention Switch

2.3 Appearance of Keys

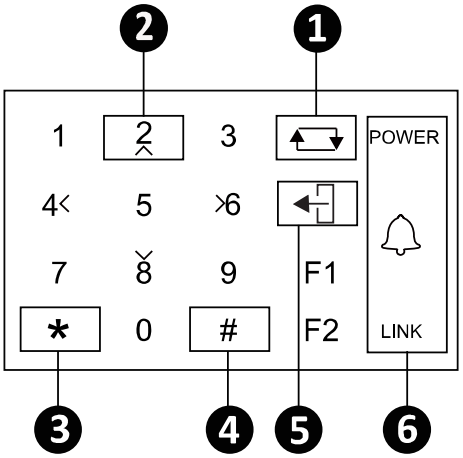


Table 1-3 Description of Keys

<table>
<tr><th>No.</th><th colspan="4">Description</th></tr>
<tr><td>1</td><td colspan="4">Editing Key: Click the key to enter/exit the editing status.</td></tr>
<tr><td>2</td><td colspan="4">Numeric Keys: Enter number in the textbox.
Direction Keys: Select icons in the menu.</td></tr>
<tr><td>3</td><td colspan="4">Exiting Key: Click the key to exit the menu.</td></tr>
<tr><td>4</td><td colspan="4">Confirming Key: Click the key to confirm operations.
Long-press the key to enter the login interface.</td></tr>
<tr><td>5</td><td colspan="4">Deleting Key: Click the key to delete contents in the textbox.</td></tr>
<tr><td rowspan="6">6</td><td rowspan="6">Status Indicator: Indicator for power, ring, and connection status</td><td>POWER</td><td>Power Status</td><td>Solid Blue: Normal Power.
Off：Power Exception.</td></tr>
<tr><td>🔔</td><td colspan="2">Doorbell Ring</td></tr>
<tr><td rowspan="4">LINK</td><td>Normal Card/ Illegal Card</td><td>Normal Card: Solid Blue
Illegal Card: Solid Red</td></tr>
<tr><td rowspan="3">Connection Status</td><td>Off: Network or Wi-Fi Disconnected.</td></tr>
<tr><td>Solid Blue: Network or Wi-Fi connected, but client unarmed.
Flicker Blue: Network or Wi-Fi connected, but client armed.</td></tr>
<tr><td>Flicker blue in the card reader mode.</td></tr>
<tr><td>F1</td><td colspan="4">Long-press the F1 key to enter the QR code authentication mode.</td></tr>
</table>

Note: In the Event Card Interact interface in the iVMS-4200 Client Software, choose the alarm output of Event Bell. You can connect a bell at the alarm output terminal. For details about configuring the Event Bell alarm output, see the *User Manual of iVMS- 4200 Client Software*.

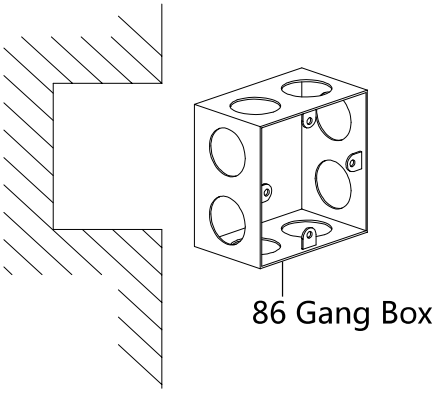
Chapter 3Installation

Note: Make sure that the wall is strong enough to withstand three times the weight of the device.

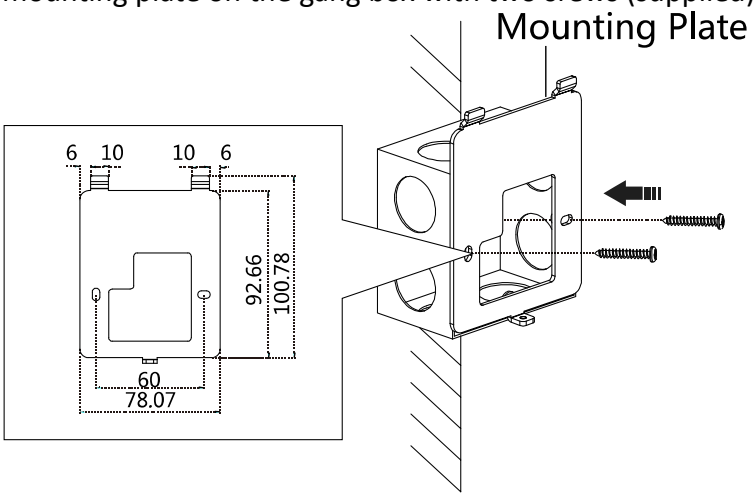
3.1 Installation of DS-K1T105 Series Device

Steps:

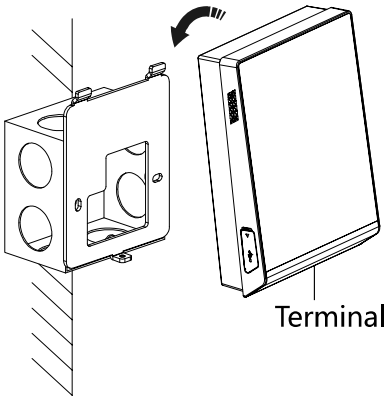
1. Install the 86 gang box into the wall.



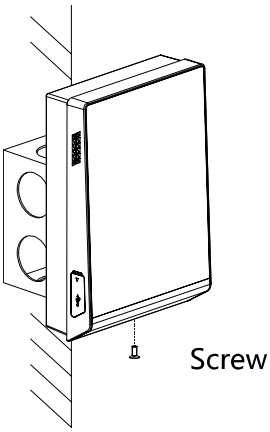
2. Secure the device mounting plate on the gang box with two srews (supplied).



3. Align the terminal with mounting plate.
4. Buckle the terminal on the plate.



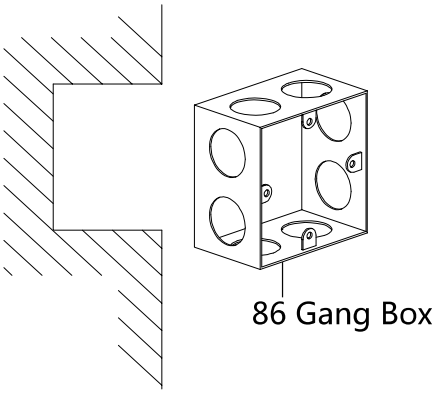
5. Tigten the srew to fix the terminal on the mounting plate and complete the installation.



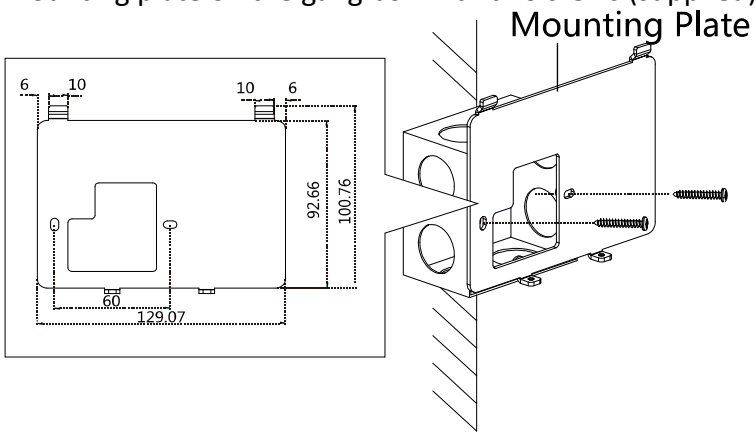
3.2 Installation of DS-K1T200/201 Series Device

Steps:

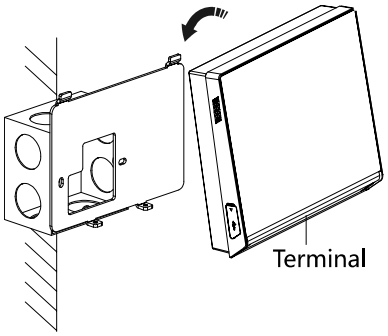
1. Install the 86 gang box into the wall.



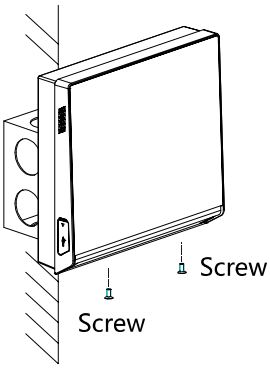
2. Secure the device mounting plate on the gang box with two srews (supplied).



3. Align the terminal with mounting plate.
4. Buckle the terminal on the plate.



5. Tigten the srews to fix the terminal on the mounting plate and complete the installation.



Chapter 4Terminal Connection

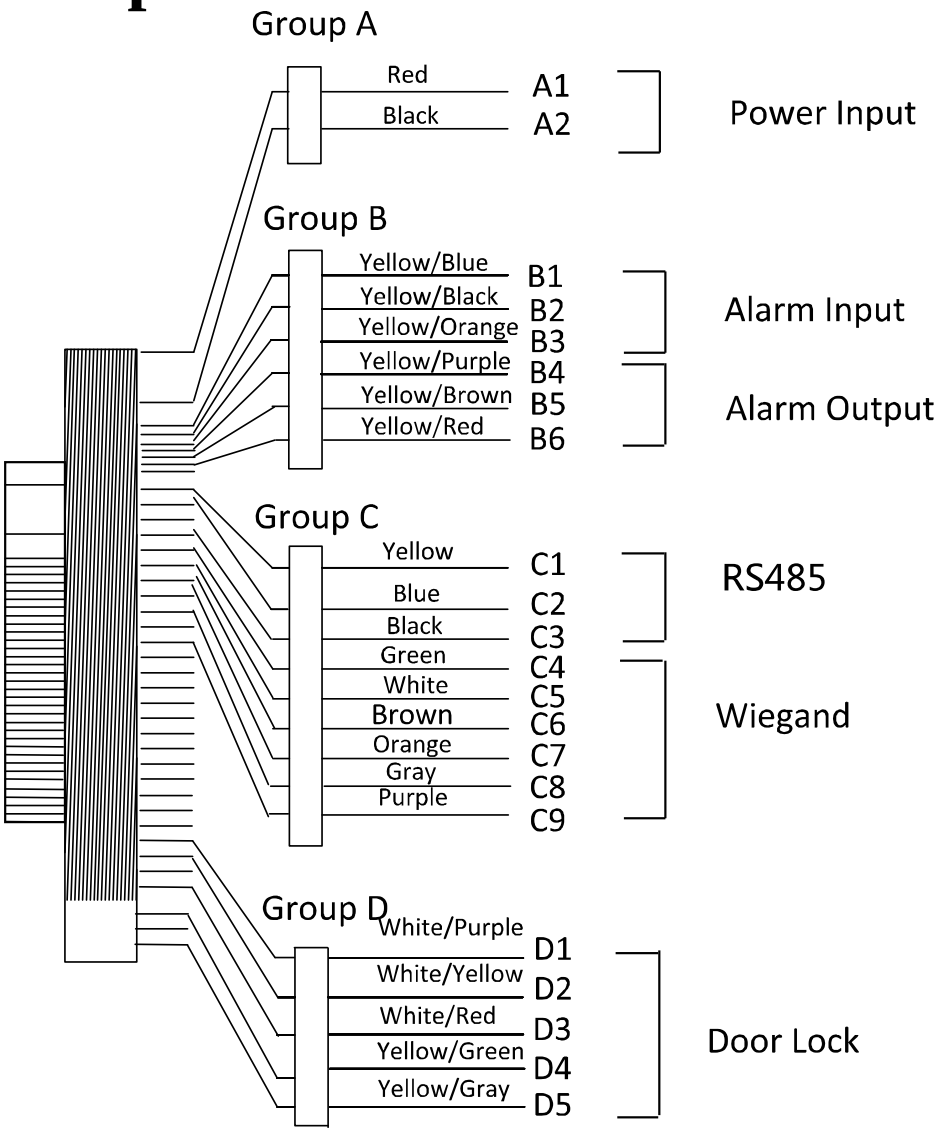


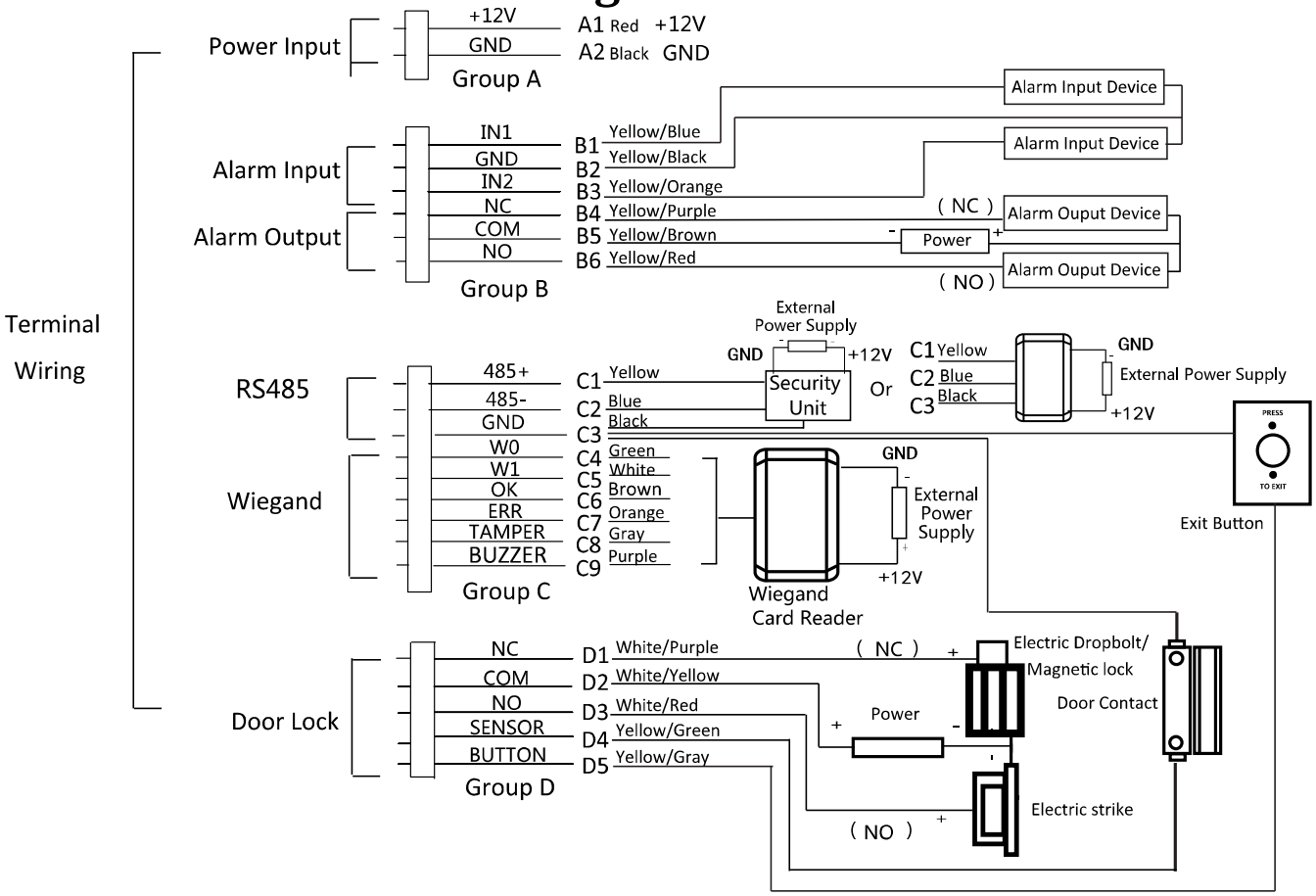
Table 1-4 Terminal Description

Line Group	No.	Function	Color	Terminal Name	Description
Line Group A	A1	Power Input	Red	+12V	12V DC Power Supply
	A2		Black	GND	GND
Line Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Yellow/Black	GND	GND
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Line Group C	C1	RS-485 Communication Port	Yellow	485 +	RS-485 Wiring
	C2		Blue	485 -	
	C3		Black	GND	
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Brown	WG_OK	Indicator of Card Reader Control Output (Valid Card Output)
	C7		Orange	WG_ERR	Indicator of Card Reader Control Output (Invalid Card Output)
	C8		Grey	TAMPER	Tampering Alarm Wiring
	C9		Purple	BUZZER	Buzzer Wiring
Line Group D	D1	Lock	White/Purple	NC	Lock Wiring
	D2		White/Yellow	COM	
	D3		White/Red	NO	
	D4		Yellow/Green	SENSOR	Door Contact Signal Input

Line Group	No.	Function	Color	Terminal Name	Description
	D5		Yellow/Grey	BUTTON	Exit Door Wiring

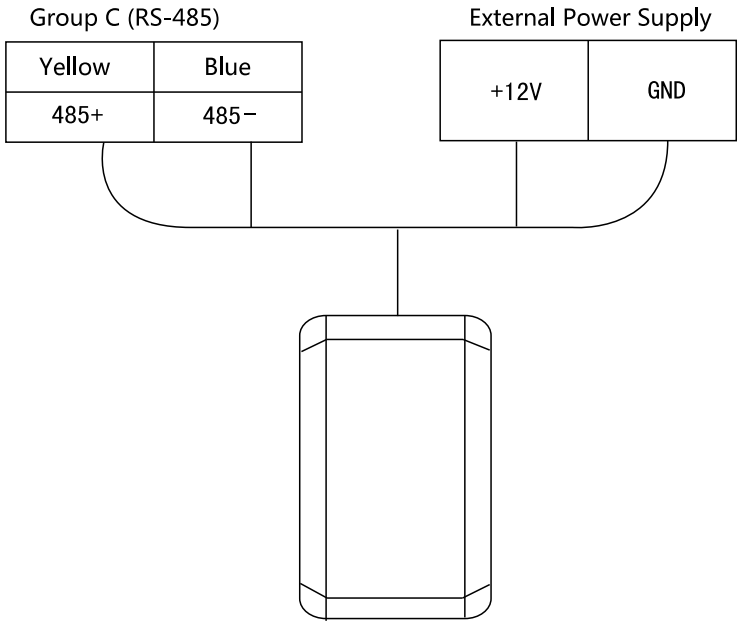
Chapter 5 Wiring Description

5.1 External Device Wiring Overview

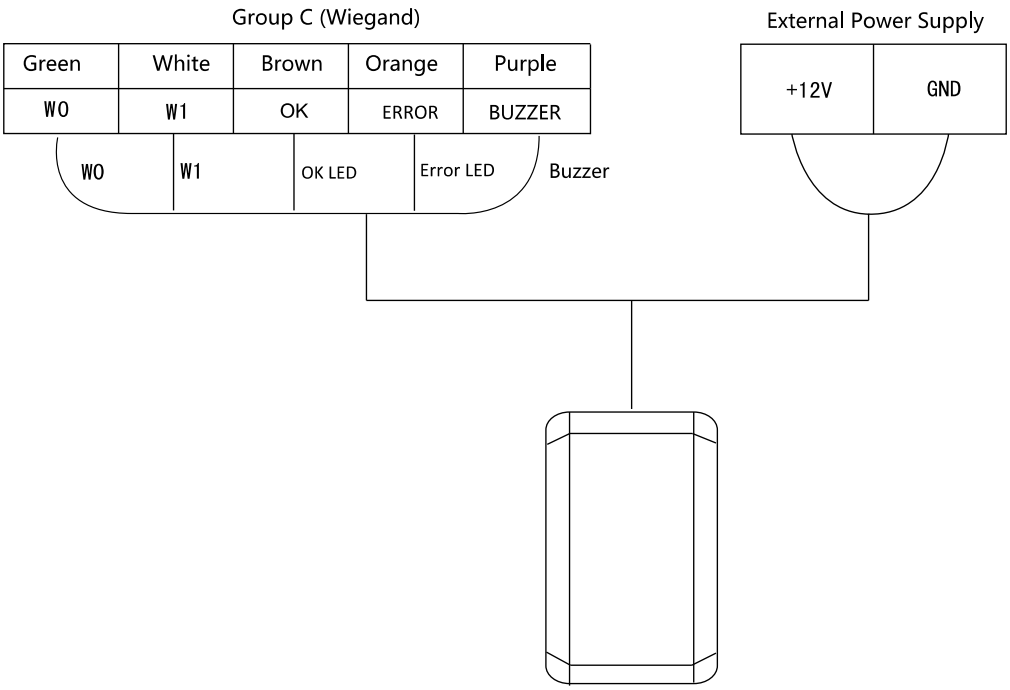


5.2 The Wiring of External Card Reader

5.2.1 The Wiring of External RS-485 Card Reader



5.2.2 The Wiring of External Wiegand Card Reader

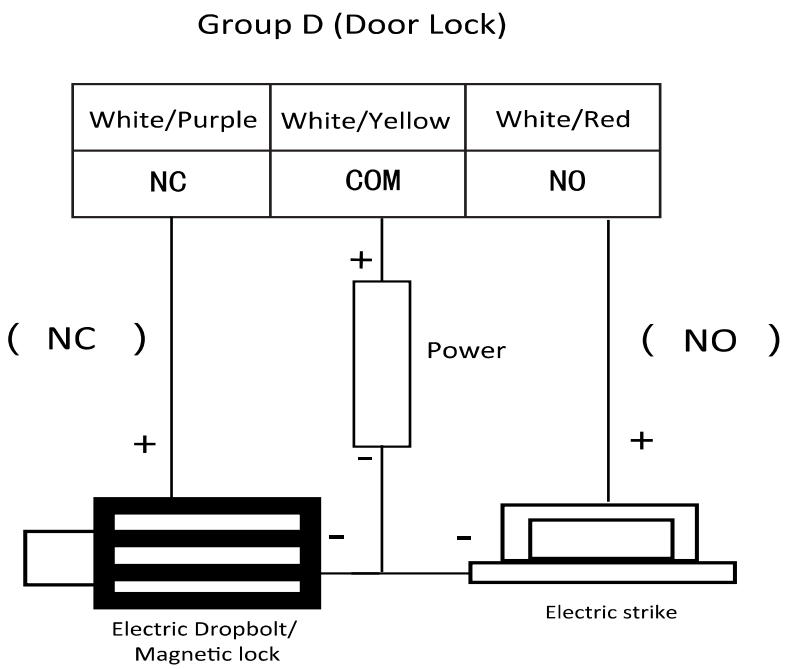


Notes:

- Set the dial-up of the external card reader as 2 when connected to the access control terminal.
- The external power supply and the access control terminal should use the same GND cable.

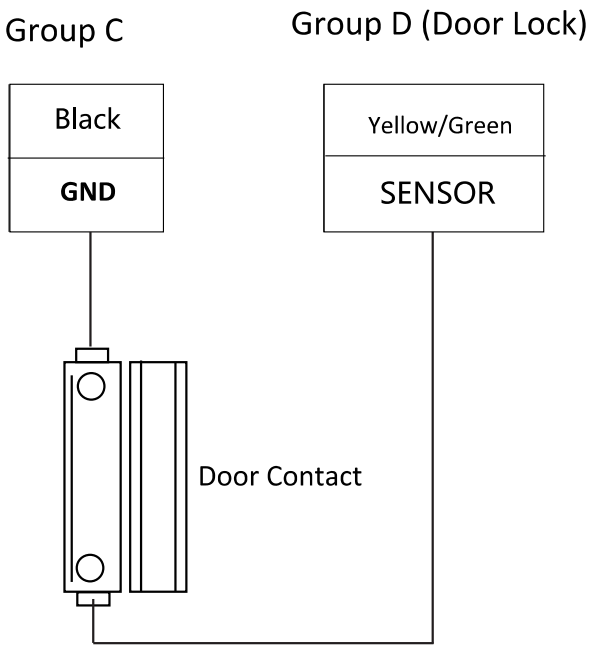
5.3 The Wiring of Electric Lock and Door Contact

5.3.1 The Wiring of Electric Lock

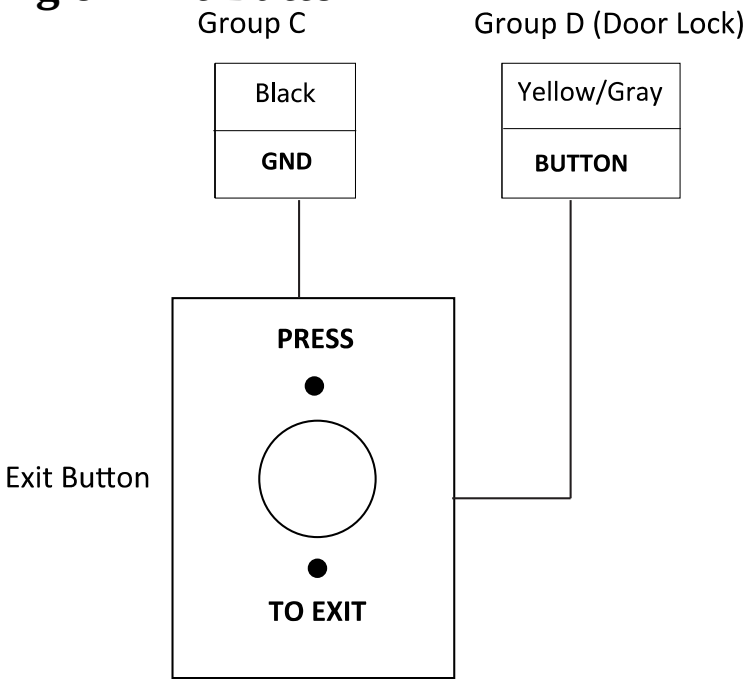


Note: Signal input interface of the door status (DOOR_NC, DOOR_COM, DOOR_NO) is used to recognize whether the door is locked. If the NC interface is connected for opening door, the NO interface can only be connected for locking door.

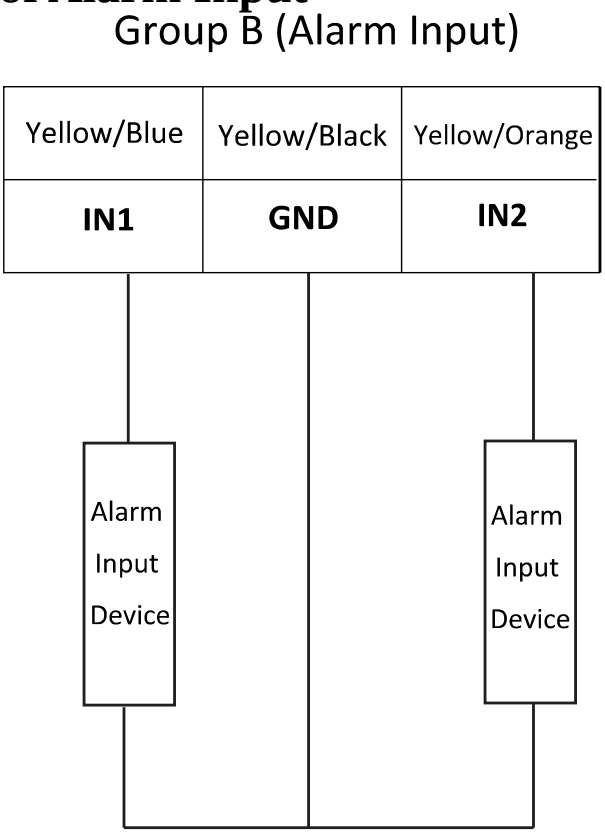
5.3.2 The Wiring of Door Contact



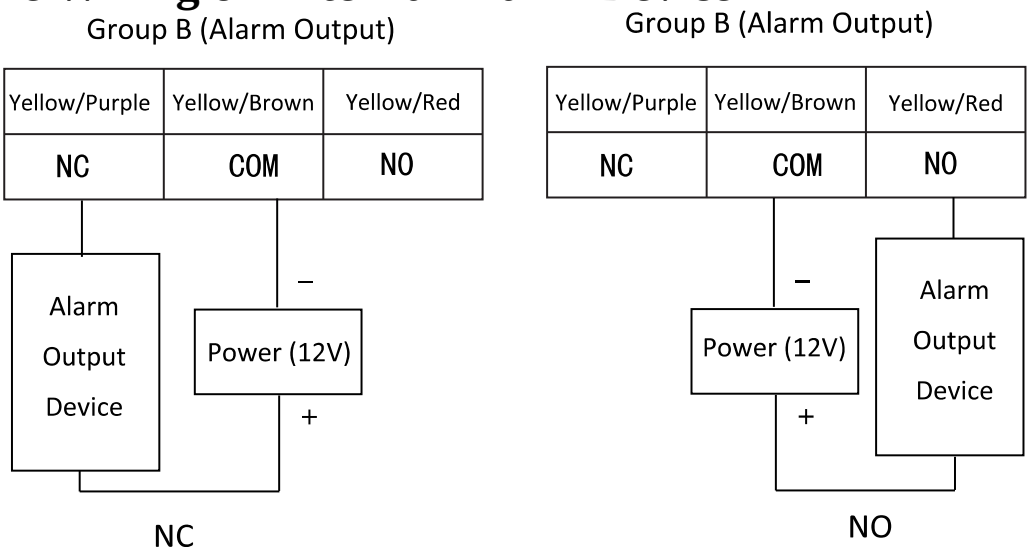
5.4 The Wiring of Exit Button



5.5 The Wiring of Alarm Input



5.6 The Wiring of External Alarm Device

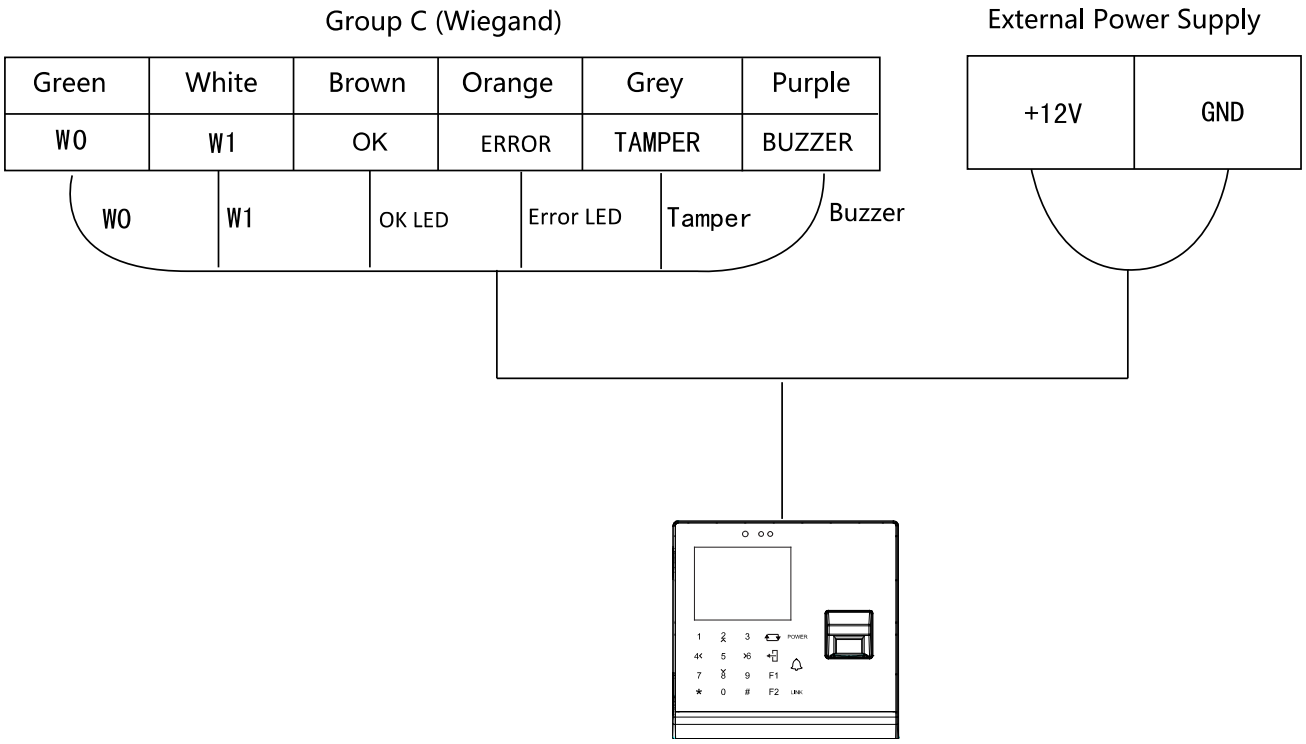


5.7 Card Reader Connection

The access control terminal can be switched into the card reader mode. It can access to the access control as a card reader, and supports Wiegand communication port and RS-485 communication port.

Note: When the access control terminal works as a card reader, it only supports being connected to the controller, but does not support alarm input or output, or the connection of external devices.

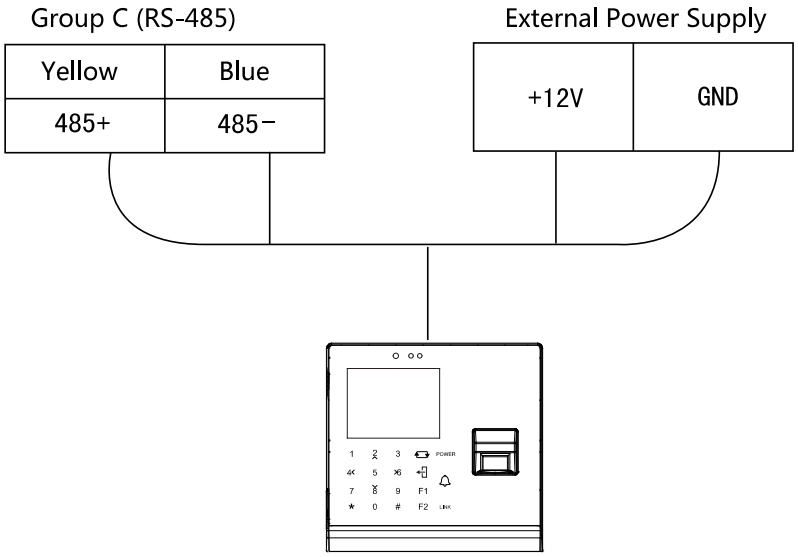
5.7.1 The Wiring of Wiegand



Notes:

- When the access control terminal works as a card reader, you must connect the **WG_ERR, BUZZER and WG_OK** terminals if you want to control the LED and buzzer of the Wiegand card reader.
- Set the working mode of the terminal as card reader, which can be configured in **System Parameter –> Mode Switch,** if the terminal is required to work as a card reader. The card reader mode support to communicate by Wiegand or RS-485.
- The distance of Wiegand communication should be no longer than 80 m.
- The external power supply and the access control terminal should use the same GND cable.

5.7.2 The Wiring of RS-485 Output



Notes:

- Set the working mode of the terminal as card reader, which can be configured in **System Parameter –> Mode Switch,** if the terminal requires working as a card reader.
- When the access control terminal works as a RS-485 card reader, the default RS-485 address is 1. RS-485 address can also be configured in **System Parameter -> Serial Port Settings**.
- The external power supply and the access control terminal should use the same GND cable.

Chapter 6 Activating Access Control Terminal

Purpose:

You are required to activate the terminal first before using it.
Activation via SADP, and Activation via client software are supported.
The default values of the control terminal are as follows.

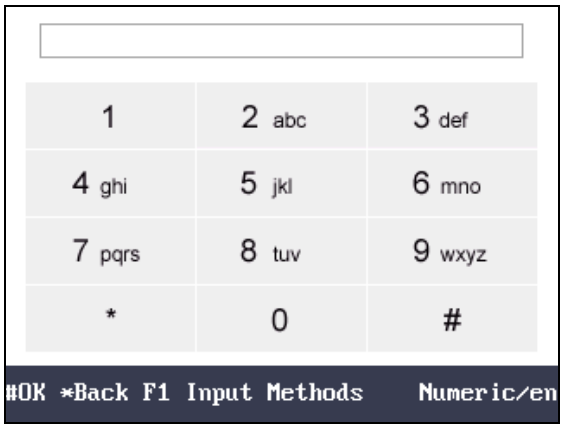
- The default IP address: 192.0.0.64.
- The default port No.: 8000.
- The default user name: admin.

6.1 Activating via Device

If the device is not activated, you can activate the device after it is powering on.

Steps:

1. Use the Up, Down, Left, Right key to move the cursor to the Password textbox and create the password for device activating.
   1) Tap the key (Edit key) to enter the editing mode.



   2) Tap F1 key to switch the input method.
   3) Enter the card number into the textbox.
   4) Tap the key to exit the editing mode.
2. Move the cursor to the Confirm Password textbox and input the password again.

3. Move the cursor to **# Activate** and tap the # key to active the device.

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.*

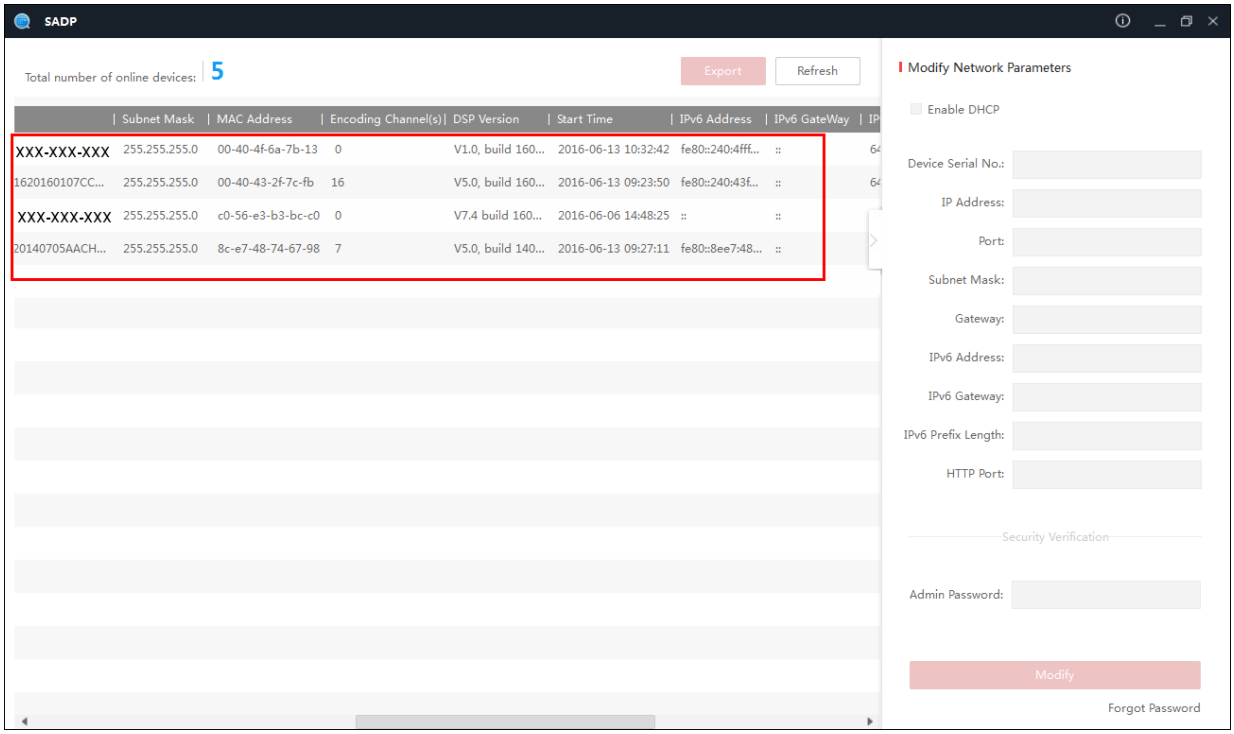
6.2 Activating via SADP Software

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

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

Steps:]

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

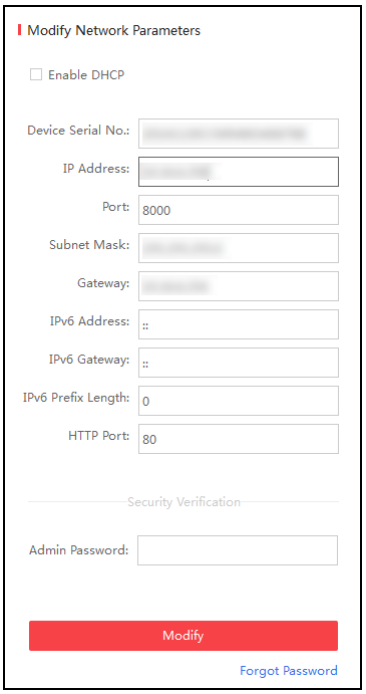


3. Create a password and input the password in the password field, and confirm the password.

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

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

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



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

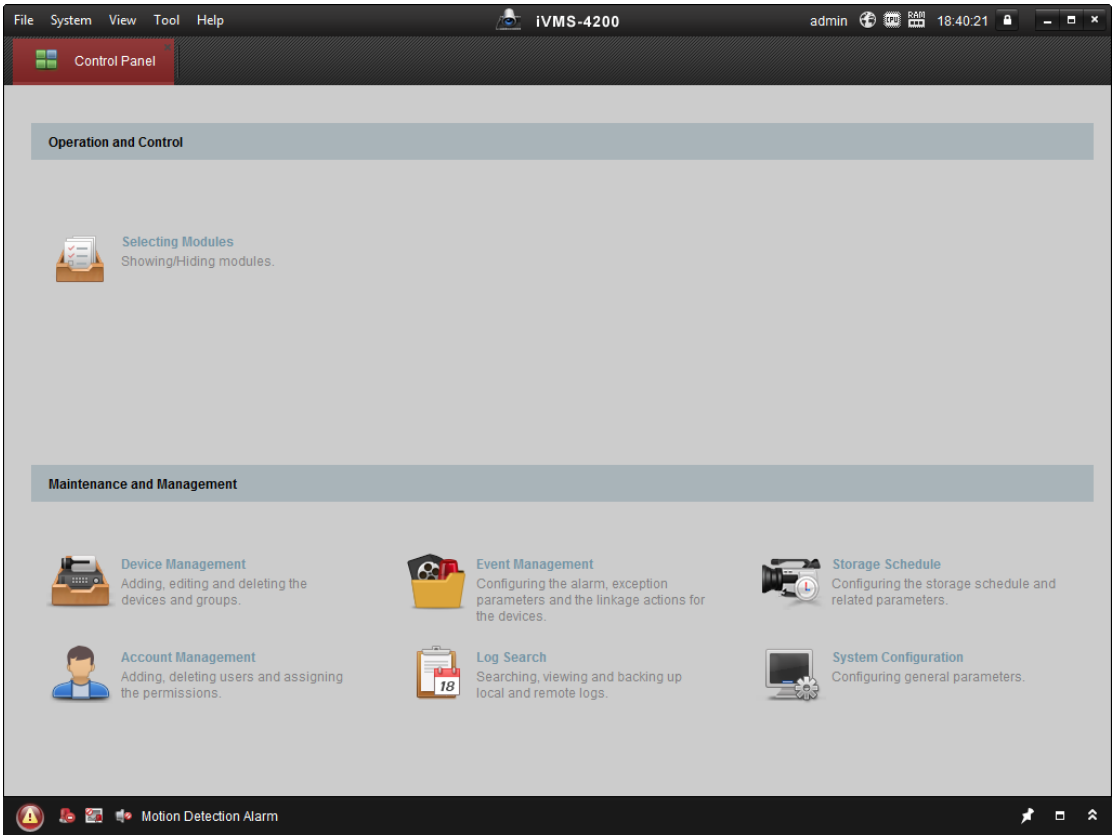
6.3 Activating via Client Software

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

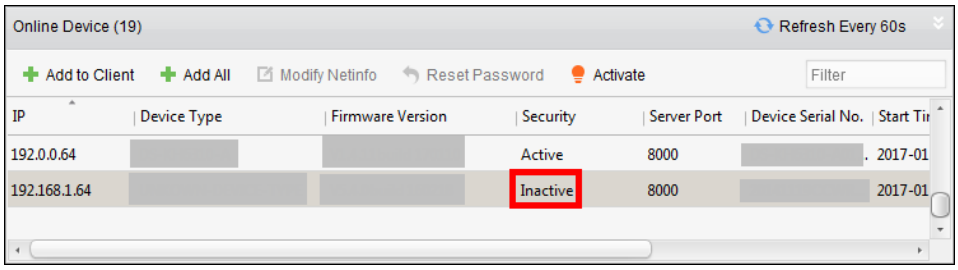
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

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



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



4. Check the device status from the device list, and select an inactive device.
5. Click the **Activate** button to pop up the Activation interface
6. In the pop-up window, create a password in the password field, and confirm the password.

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

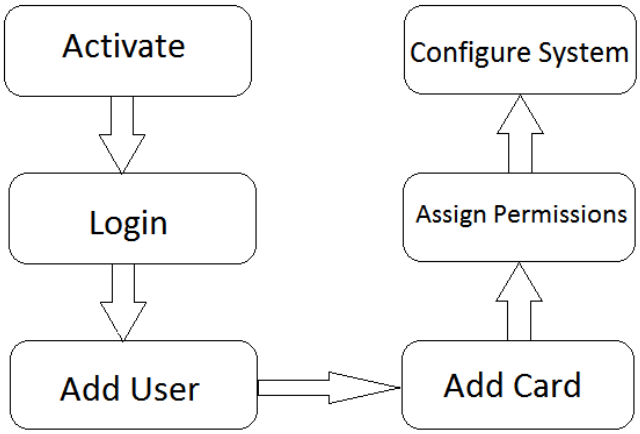
7. Click **OK** button to start activation.
8. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.
9. Change the device IP address to the same network segment with your computer by either modifying the IP address manually.
10. Input the password and click the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

Chapter 7Basic Operation

Before You Start:

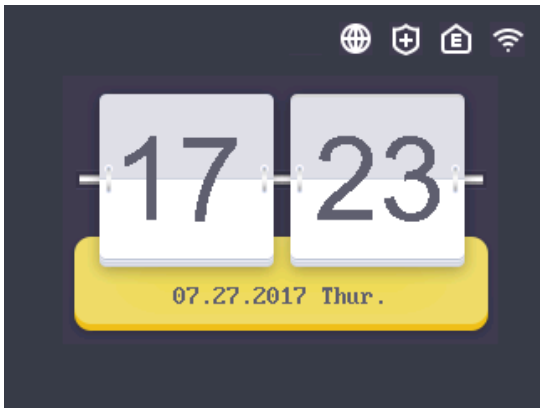
You should activate the device before the first login. Otherwise, after powered on, the system will switch into the Device Activation interface. For detailed information about activation, see Chapter 6 Activating Access Control Terminal.

The working flow is as follows:

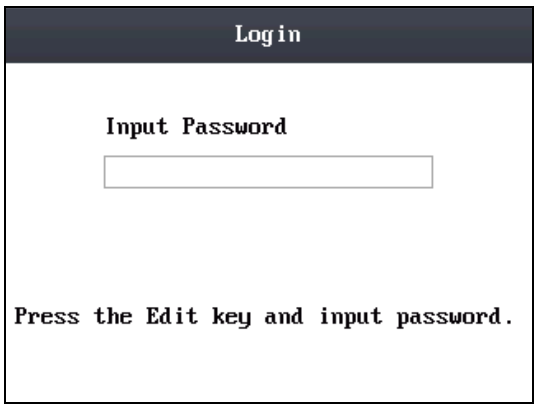


Steps:

1. Power on the device to enter the initial interface.



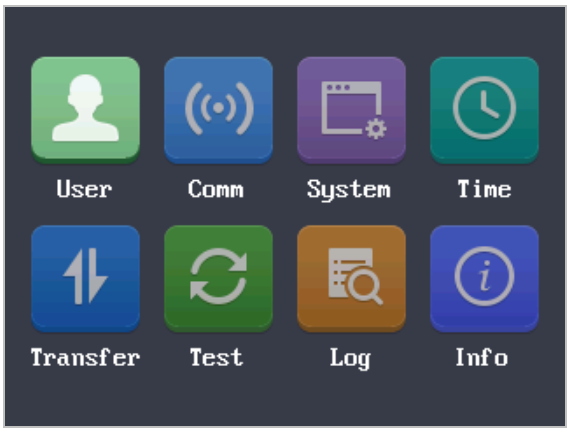
2. Long-tap the **#** key for 3s to enter the password authentication interface.



3. Enter the device password.

1) Tap the key (Edit key) to enter the editing mode.
2) Tap F1 key to switch the input method.
3) Enter the (activation) password into the textbox.
4) Tap the key to exit the editing mode.

4. Tap the # key to confirm the settings. The system will enter the menu operation interface.



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

Note: In the initial interface, the icon , , , and on the upper-right corner represents network is online, network is armed, EHome is online, and Wi-Fi is connected respectively. If there is on the first three icons, it represents network is offline, network is not armed, and EHome is offline respectively. When the Wi-Fi is not connected, the Wi-Fi icon will have no color inside.

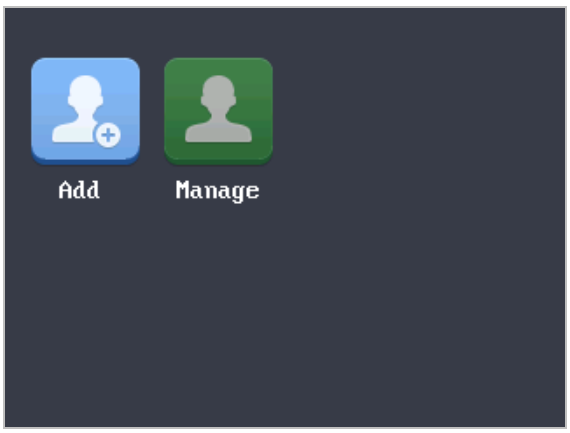
7.1 User Management

Purpose:

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

Use the Up, Down, Left, Right key to move the cursor to **User** (user management) by using the direction keys.

Tap the # key to enter the User interface.



7.1.1 Adding User

Purpose:

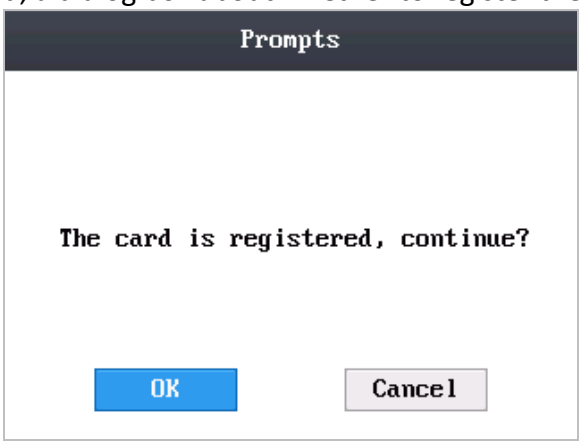
In the **Adding User** menu, you can add users, register card, and record fingerprints optionally for the corresponding person.

Steps:

1. Use the Up, Down, Left, Right key to move the cursor to **Add** (add user) by using the direction keys.
2. Tap the # key to enter the Add interface.

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

   After registering the card, a dialog box about whether to register the fingerprint pops up.



4. Register the fingerprint.
   1) Move the cursor to the **OK** button, and tap the **#** key to enter the fingerprint registration interface.

2) Place the finger on the fingerprint scanner, rise and rest your finger by following the corresponding voice prompts.

Notes:

- The fingerprint registration function only supports device with fingerprint module.
- The same fingerprint cannot be repeatedly registered.
- For the optical access control terminal, you should place your finger twice to register the fingerprint. For details about scanning fingerprints, refer to *Appendix*.

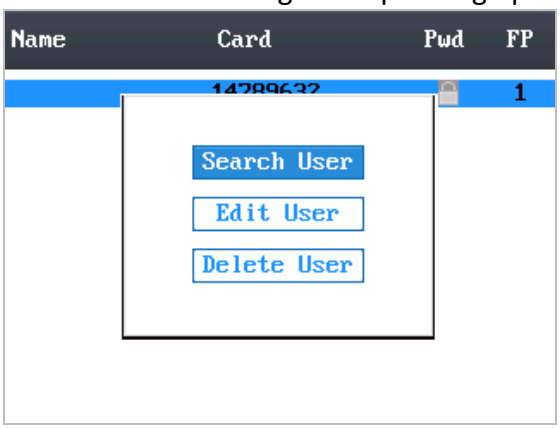
7.1.2 Managing User

Move the cursor to the **Manage** (edit user) by using the direction keys.
Tap the # key to enter the Management interface.

Searching User

Steps:

1. Move the cursor to a user by using the direction keys.
2. Tap the **#** key to pop up an interface for selecting corresponding operations.



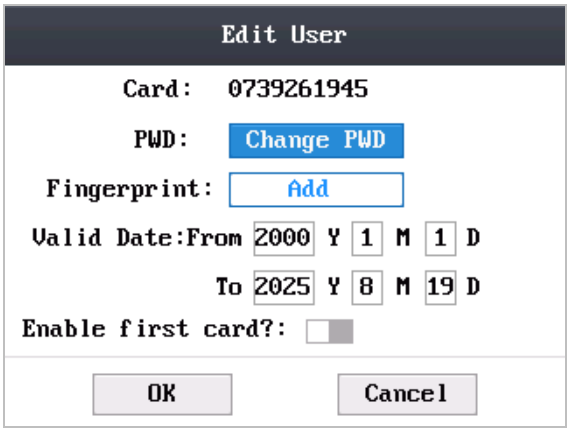
3. Move the cursor to **Search User** by using the direction keys.
4. Tap the **#** key to enter the searching interface.

5. Input the card number to **Input Card No.** textbox.
6. Tap the # key to view the basic information about the card holder.

Editing User

Steps:

1. Move the cursor to a user by using the direction keys.
2. Tap the **#** key to pop up an interface for selecting corresponding operations.
3. Move the cursor to **Edit User**.
4. Tap the **#** key to enter the editing interface.



5. Edit the user information.
   - Adding the Fingerprint.
     Move the cursor to **Add** to enter the fingerprint registration interface. See details in step 4 of adding user.
     Note: DS-K1T105 series model does not support this function.
   - Changing the Password.
     1) Move the cursor to **Change PWD** to enter the password changing interface.
     2) Input a new password.
     3) Confirm the new password.

- Changing the valid date.
  You can set the start/end time of the user's permission.
  Tap the ⇄ key to enter/exit the editing mode.
- Enabling first card
  Tap the **#** key to enable first card.
  Note: After enabling first card, the door remains open during the pre-defined valid duration.

6. Move the cursor to the **OK** button, and tap the **#** key to confirm the settings.

Deleting User

Steps:

1. Move the cursor to a user by using direction keys.
2. Tap the **#** key to pop up an interface for selecting corresponding operations. (Figure 6-9)
3. Move the cursor to **Delete User**, and tap the **#** key to enter the deleting interface.
4. Move the cursor to **Delete User**, **Delete PWD only** or **Delete FP only**.
   Delete User: Delete the user and the overall information.
   Delete PWD only: Only delete the password set by the user.
   Delete FP only: Only delete the fingerprint information of the user.
   Note: DS-K1T105 series model does not support this function.
5. Tap the **#** key to finish the deleting operation.

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

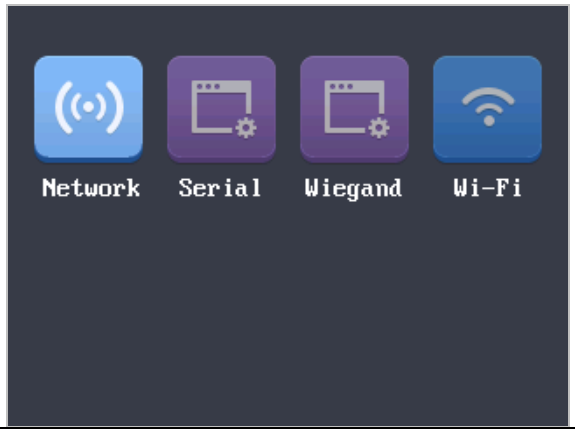
7.2 Communication Settings

Purpose:

On the communication settings interface, you can set network parameters, the serial port, Wiegand parameters, and Wi-Fi.

Steps:

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



Network Settings:	It refers to network parameters of the device, including IP address, subnet mask, and gateway address.
Serial Port Settings:	When the access control terminal works as a RS-485 card reader, serial port parameters include working mode, Baud Rate, and RS-485 address.
Wiegand Settings:	When the access control terminal works as a Wiegand card reader, Wiegand parameters involve the Wiegand direction, and the Wiegand mode.
Wi-Fi:	You can enable the Wi-Fi function.

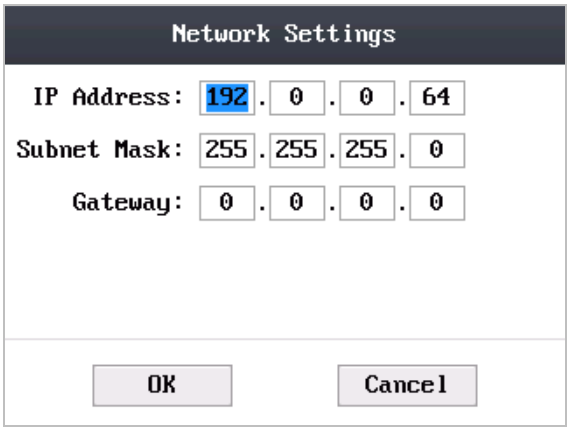
7.2.3 Network Settings

Purpose:

On the network settings interface, you can set network parameters of the device.

Steps:

1. Move the cursor to **Network** (network settings) by using direction keys.
2. Tap the **#** key to enter the network settings interface.



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

   Note: Tap the ⇄ key to enter/exit the editing mode.
4. Move the cursor to the **OK** button, and tap the **#** key.

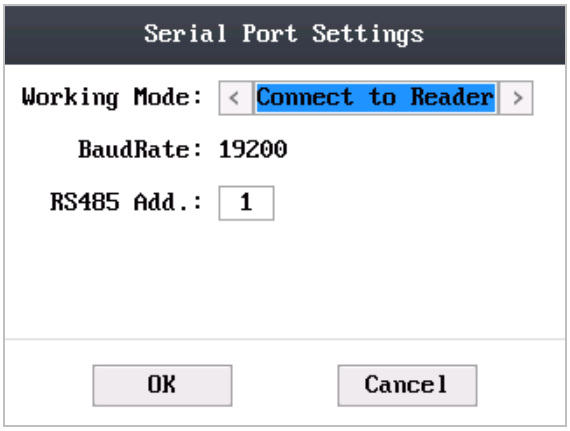
7.2.4 Serial Port Settings

Purpose:

When the access control terminal works as the RS-485 card reader, you should set serial port parameters.

Steps:

1. Move the cursor to **Serial** (serial port settings) by using direction keys on the communication settings interface.
2. Tap the **#** key to enter the serial port settings interface.



3. Modify parameters of the serial port, including working mode, Baud Rate, and RS-485 address.

Working Mode:	● When the access control terminal working as the terminal, set the working mode of the serial port to **Connect to Reader**, **Connect to Client** or **Connect to Unit**. ● If the terminal is worked as the card reader, the serial port is connected to the terminal by default. There is no need to configure the serial port working mode.
Baud Rate:	It will display the Baud Rate configured on the client software.
RS-485 Address:	When the access control terminal works as a card reader, the RS-485 address should be configured.

Notes:

- Tap the ⏎ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the **#** key to switch the mode between "Yes" mode and "No" mode.

4. Move the cursor to the **OK** button, and tap the **#** key.

   Note: Reboot the device after changing the working mode.

7.2.5 Wiegand Settings

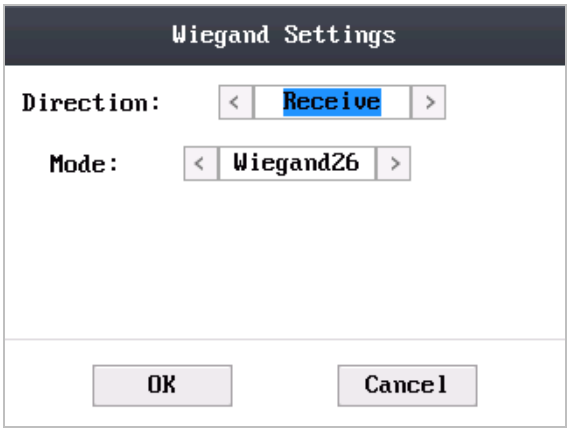
Purpose:

When the access control terminal works as the Wiegand card reader, you should set Wiegand

parameters.

Steps:

1. Move the cursor to **Wiegand** (Wiegand settings) by using direction keys on the communication settings interface.
2. Tap the **#** key to enter the Wiegand settings interface.



3. Edit parameters of the serial port, including the Wiegand direction and the Wiegand mode.

Wiegand Direction:	1) In the terminal mode, select whether to **Receive** or to **Send**. In the **Receive** mode, the mode is self-adaptive and the mode cannot be edited. 2) In the card reader mode, only **Send** is supported.
Wiegand Mode:	The default Wiegand mode is Wigand 34

Notes:

- Tap the ⇄ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the **#** key to switch the mode between “Yes” mode and “No” mode.

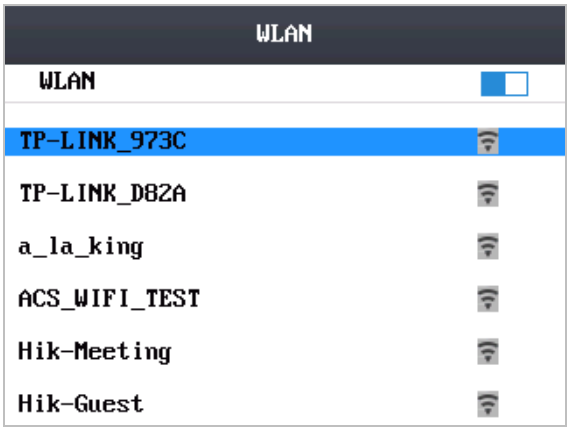
4. Move the cursor to the **OK** button, and tap the **#** key.
   Note: Reboot the device after changing the Direction.

7.2.6 Wi-Fi Settings

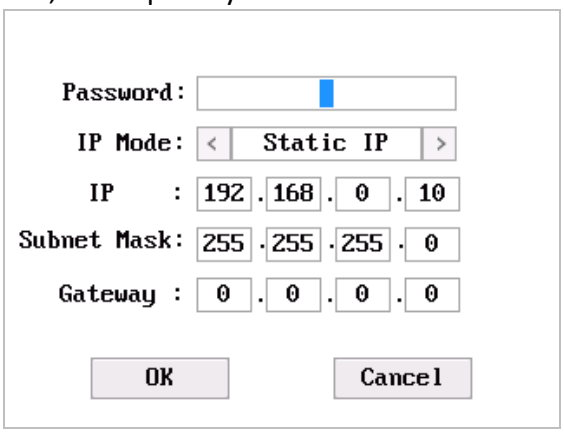
Steps:

1. Move the cursor to **Wi-Fi** (Wi-Fi settings) by using direction keys on the communication settings interface.
2. Tap the **#** key to enter the Wi-Fi settings interface.

3. Move the cursor to and tap the **#** key to enable the WLAN.



4. Move the cursor to a network, and tap **#** key to enter the network connection interface.



5. Input the password of the network. The password supports numbers, letters (uppercase and lowercase) and symbols.
6. Edit the IP mode, IP address, subnet mask, and gateway address.
7. Move the cursor to the **OK** button, and tap the **#** key.

Note: Tap the key to enter and exit the editing mode.

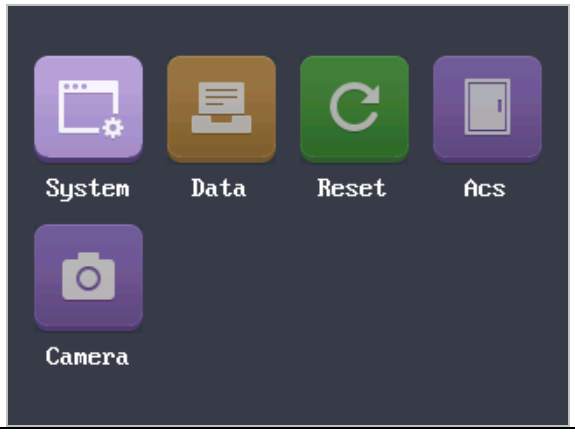
7.3 System Settings

Purpose:

On the system settings interface, you can set system parameters, manage the data, restore default settings, set access control parameters, and set cameras.

Steps:

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



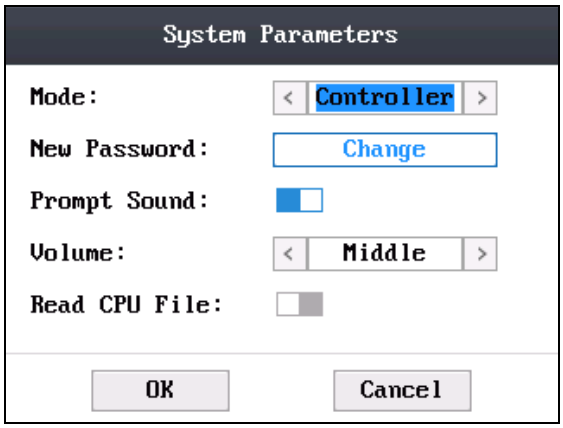
System Parameters:	System parameters of the device include the device running mode, login password, and prompt sound.
Data Management:	It is used to manage the storage data of the device, including Delete Card Parameters, Delete Event Only, and Delete Picture Only.
Restore Settings:	The device can be restored into factory defaults or default settings.
Access Control Settings:	You can set parameters of the access control terminal, including Controller Authentication, Card Reader Authentication, Door Action Time, Delayed Door Alarm, and Anti-passing Back.
Camera Settings:	You can set the camera for the access control terminal (only supported by terminal with the model of -C).

Note: **Camera Settings** will be displayed on the screen when the access control terminal has the function.

7.3.1 Setting System

Steps:

1. Move the cursor to **System** (system parameters) by using direction keys on the system settings interface.
2. Tap the **#** key to enter the system parameters interface.



3. Modify system parameters, including switching the mode, entering the login password, and enabling voice prompts.

Mode:	The device mode can be switched between **Controller** and **Card Reader**. After switching the mode, the system can automatically reboot and enter into the interface of the new mode. ***Notes:*** • If the access control terminal works as a card reader, you should configure the serial port setting and the Wiegand setting. See details in *Chapter 7.2.4 Serial Port Settings* and *Chapter 7.2.5 Wiegand Settings*. • If the access control terminal is in the card reader mode, the terminal works as a card reader to access to the access controller or another access control terminal via RS-485 and Wiegand. • If the access control terminal is in the card reader mode, the terminal will apply the fingerprint via RS-485, the client software and the local. (The fingerprint application function should be supported by the device) • If the access control terminal is in the card reader mode, the terminal supports swiping card and scanning fingerprint. When scan the fingerprint, the bound card No. should contain 10 numbers. Or the fingerprint scanning will be failed.
Login Password:	To change the login password of the device, you should input the old password, create a new password, and confirm it.
Voice Prompts:	After enabling voice prompts, you can hear the voice prompts to notify you the card status when you swipe the card. Otherwise, you will hear the beeper in place of the voice prompts. • Beep three times: legal card. • Beep four times: illegal card.
Volume:	You can adjust the device volume. High, Middle, and Low are available.
Read CPU File:	If the device can be swiped by the CPU card, when enable the function, the device can read the CPU card information. ***Notes:*** ● Only device can recognize CPU card supports the function. ● Tap the key to enter and exit the editing mode. ● Tap the Right/Left direction keys to choose contents. ● Tap the # key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the **#** key.

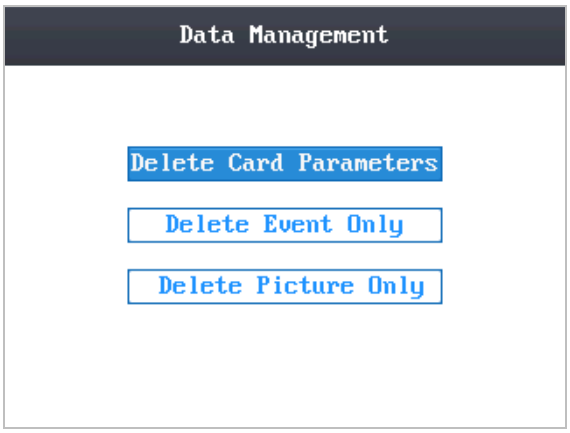
7.3.2 Managing Data

Purpose:

On the data management interface, you can delete the storage data of the device.

Steps:

1. Move the cursor to **Data** (data management) by using direction keys in the system settings Interface.
2. Tap the **#** key to enter the data management interface.



Move the cursor to Delete Card Parameters, Delete Event Only, or Delete Picture Only.
Delete Card Parameters: Delete all cards parameters registered in the device.
Delete Event Only: Delete all access events in the system.
Delete Picture Only: Delete all captured pictures in the system.
Note: This function is only supported by terminal with the model of –C.

3. Tap the **#** key.

7.3.3 Restoring Settings

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

1. Move the cursor to **Reset** (restore settings) by using direction keys on the system settings interface.
2. Tap the **#** key to enter the restore settings interface.

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

5. Move the cursor to the **OK** button, and tap the **#** key.

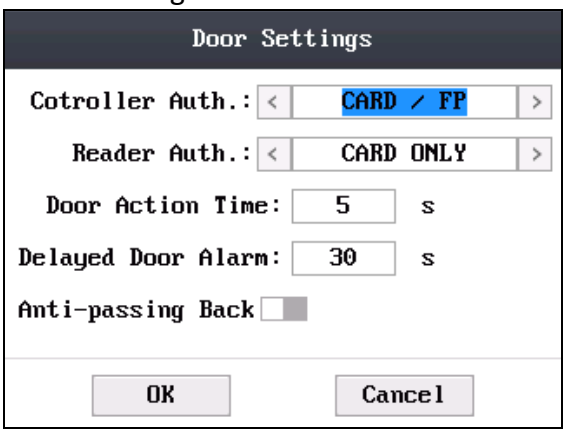
7.3.4 Door Settings

Purpose:

On the door settings interface, you can set door parameters, including Controller Authentication, Card Reader Authentication, Door Action Time, Delayed Door Alarm, and Anti-passing Back.

Steps:

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



3. Edit door parameters.

Controller Authentication:	Set the controller authentication mode for opening the door, that is, Card Only, Fingerprint Only, Card/Fingerprint, Card & Fingerprint, Card & Password, Fingerprint & Password, Card & Fingerprint & Password.
Card Reader Authentication:	Set the card reader authentication mode for opening the door, that is, Card Only, Fingerprint Only, Card/Fingerprint, Card & Fingerprint, Card & Password, Password & Fingerprint, Card & Password & Fingerprint.
Door Action Time:	Set the door action time: 1 ~ 255 s.
Delayed Door Alarm:	Set the delayed door alarm threshold: 1 ~ 255 s.
Anti-Passing Back:	Set whether to enable the function of anti-passing back.

Notes:

- Tap the key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the **#** key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the **#** key.

7.3.5 Setting Camera

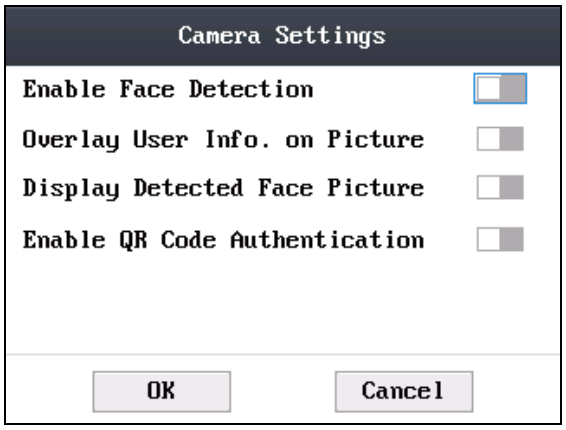
Purpose:

On the camera settings interface, you can set camera parameters.

Note: This function is only supported by terminal with the model of –C.

Steps:

1. Move the cursor to **Camera** (camera settings) by using direction keys in the system settings Interface.
2. Tap the **#** key to enter the camera settings interface.



3. Edit camera parameters.

Enable Face Detection:	If enabling face detection, the device should detect the face when authenticating. Or authentication will be failed.
Overlay User Info. on Picture:	When enabling card No. overlay, captured pictures can be overlaid on the card information.
Display Detected Face Picture:	When enabling to display the picture, captured pictures can display on the screen.
Enable QR Code Authentication:	You can authenticate via QR code. When enabling the function, long-press the F1 key to enter the QR code authentication mode. Place the QR code picture in front of the device camera to authenticate. ***Note:*** • You can generate the card QR code when adding the card to the person. For details, see *Adding User (Card)* in *User Manual of iVMS-4200 Client Software*. • The function should be supported by the device with camera.

Notes:

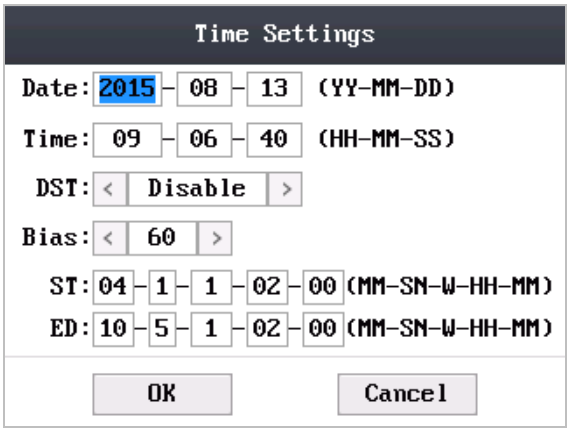
- Tap the key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the **#** key to switch the mode between “Yes” mode and “No” mode.
- The captured pictures can be saved in the SD card.

4. Move the cursor to the **OK** button, and tap the **#** key.

7.4 Time Settings

Steps:

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



3. Edit time parameters.
   Date/Time: Edit the data and the time of the device.
   DST (Daylight Saving Time): When enabling DST, you should set the bias time, the start time, and the end time of DST.

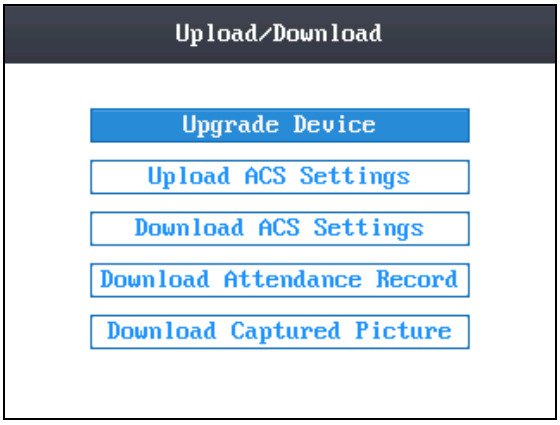
   Notes:
   - Tap the ⏎ key to enter and exit the editing mode.
   - Tap the Right/Left direction keys to choose contents.
   - Tap the **#** key to switch the mode between "Yes" mode and "No" mode.
4. Move the cursor to the **OK** button, and tap the **#** key.

7.5 Upload/Download Settings

Purpose:
On the upload/download interface, you can upgrade the device, upload the door parameters, download access parameters, download captured pictures, and download attendance record.

Steps:

1. Plug a USB disk into the access control terminal.
2. Move the cursor to **Transfer** (upload/download) by using direction keys.
3. Tap the **#** key to enter the upload/download interface.



4. Move the cursor to Device Upgrade, Upload Access Settings, Download Access Settings, Download Attendance Record, or Download Captured Picture.

Upgrade Device:	The system can automatically read the upgrading information from the USB, and upgrade the device. ***Note:*** The upgrading file should be put in the root directory.

Upload ACS Settings:	The system can automatically read the access parameters from the USB, and upload them to the device.
Download ACS Settings:	The system can automatically download access parameters into the USB.
Download Attendance Record:	The system can automatically download attendance records into the USB.
Download Captured Picture:	The system can automatically download captured pictures into the USB. Click the **#** key.

Note: The supported USB format is FAT32.

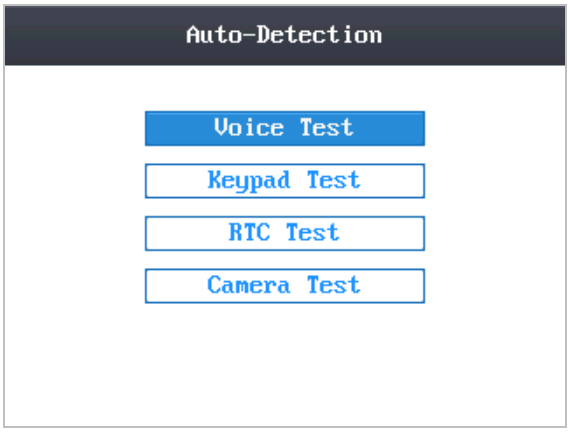
7.6 Testing

Purpose:

On the test interface, you can do voice test, keypad test, RTC test, and camera test.

Steps:

1. Move the cursor to **Test** by using direction keys.
2. Tap the # key to enter the test interface.



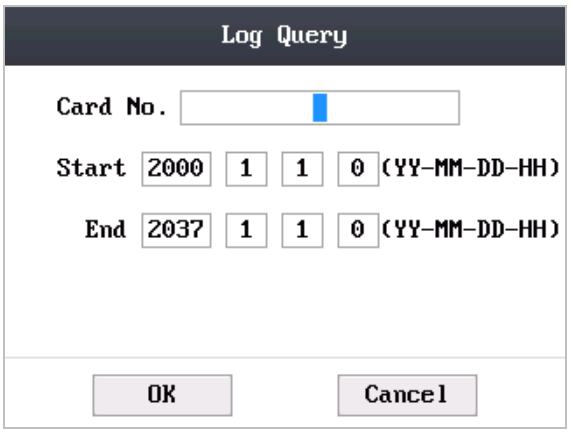
3. Move the cursor to select Voice Test, Keypad Test, RTC Test, or Camera Test to do corresponding test.

Voice Test:	You can hear a voice prompt “Voice prompt succeeds” after click the # key.
Keypad Test:	On the keypad test interface, if the keypad test succeeds, the screen will display corresponding numbers or functions of the keypad you click.
RTC Test:	On the RTC test interface, if the test succeeds, the screen will display the synchronization time.
Camera Test:	On the camera test, if the camera test succeeds, the screen will display the real-time picture the camera captures. ***Note:*** This function is only supported by terminal with the model of –C.

7.7 Log Query Settings

Steps:

1. Move the cursor to **Log** (log query settings) by using direction keys.
2. Tap the **#** key to enter the log query interface.



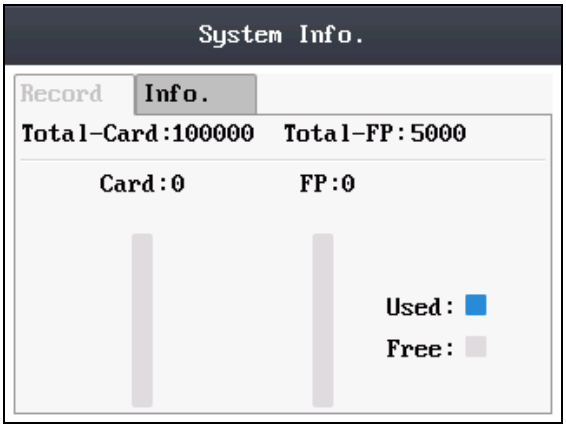
3. Enter the card number.
   - Enter the card number by swiping the card.
     Place the card close to the screen.
   - Input the card number manually.
4. Set the start/end time.
   Tap the ⏎ key to enter and exit the editing mode.
5. Move the cursor to the **OK** button, and tap the **#** key.

Note: On the log query display interface, you can view the card number, swiping time, and card reader ID.

7.8 System Information

Steps:

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



3. Move the cursor to **Record Capacity** or **Information** by using Left/Right direction keys.
   - **Record Capacity**

Card Capacity:	It refers to the maximum amount of cards. ***Note:*** The default maximum card amount is 100,000.
Fingerprint Capacity:	It refers to the maximum amount of fingerprints. ***Notes:*** ● Fingerprint capacity only supports devices with fingerprint registration function. ● The default maximum fingerprint amounts of devices with

	fingerprint registering function are as follows. ● DS-K1T200 series optical device: 9500; DS-K1T201 series optical device: 5000 ● DS-K1T105 series model does not support this function.

- **Device Information**

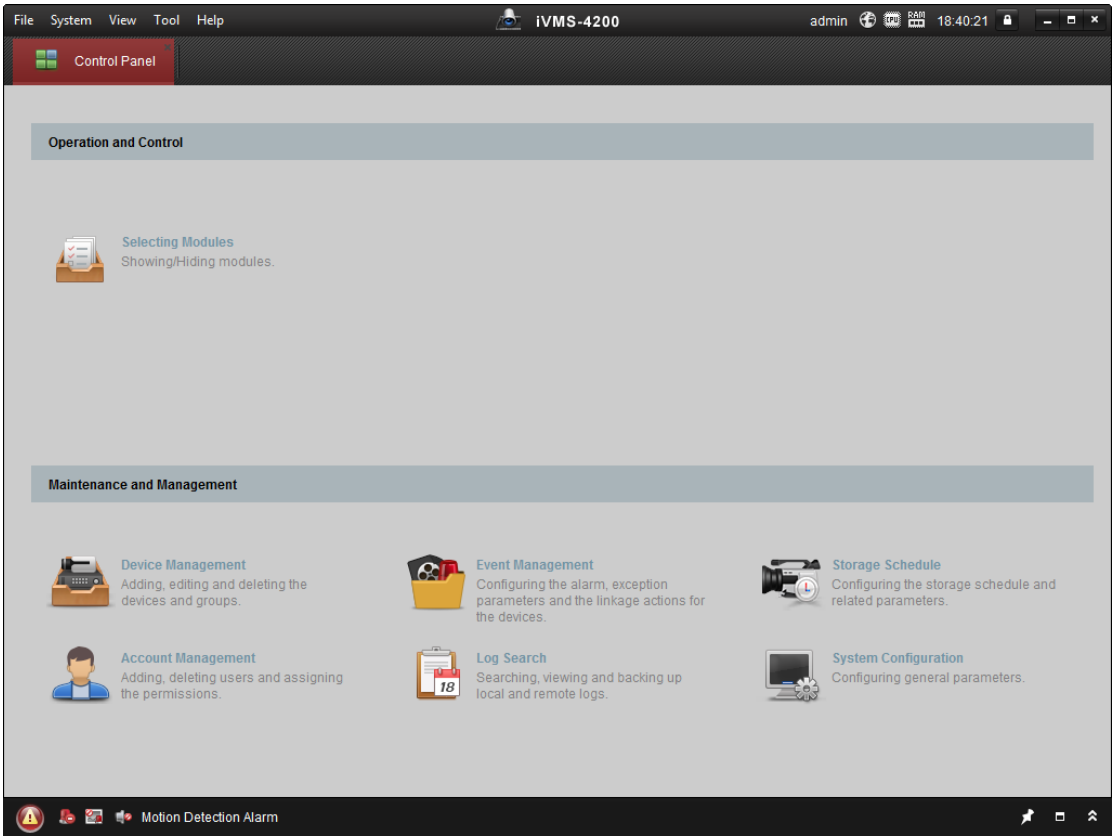
  In the device information interface, you can view the device name, the serial No., Mac address, and so on.

Chapter 8 Client Operation

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

8.1 Function Module

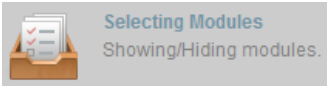
Control Panel of iVMS-4200:



Menu Bar:

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

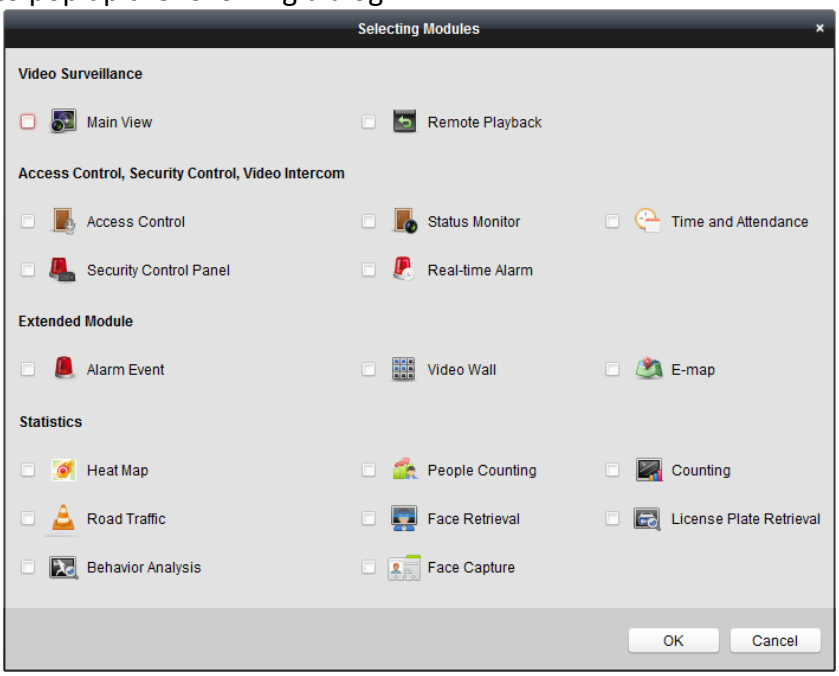
View	**1024*768**	Display the window at size of 1024*768 pixels.
	1280*1024	Display the window at size of 1280*1024 pixels.
	1440*900	Display the window at size of 1440*900 pixels.
	1680*1050	Display the window at size of 1680*1050 pixels.
	Maximize	Display the window in maximum mode.
	Control Panel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

For the first time running the software, you can click 

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

Steps:

1. Click to pop up the following dialog.



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

Notes:

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

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

	The Main View module provides live view of network cameras and video encoders, and supports some basic operations, such as picture capturing, recording, PTZ control, etc.
	The Remote Playback module provides the search, playback, export of video files.
	The Access Control module provides managing the organizations, persons, permissions, and advanced access control functions. Provides video intercom function.
	The Status Monitor module provides monitoring and controlling the door status, viewing the real-time card swiping records and access control events.

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

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

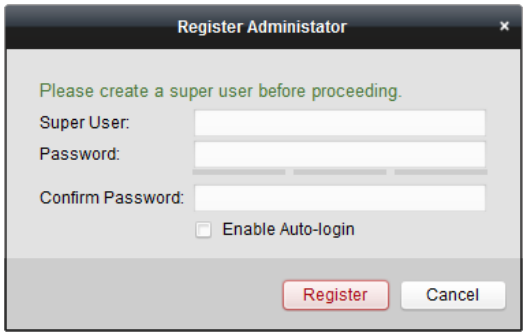
You can check the information, including current user, network usage, CPU usage, memory usage and time, in the upper-right corner of the main page.

8.2 User Registration and Login

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

Steps:

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

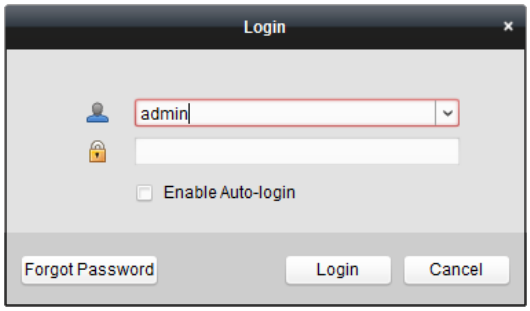


- *A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.*
- *For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case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

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

Steps:

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



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

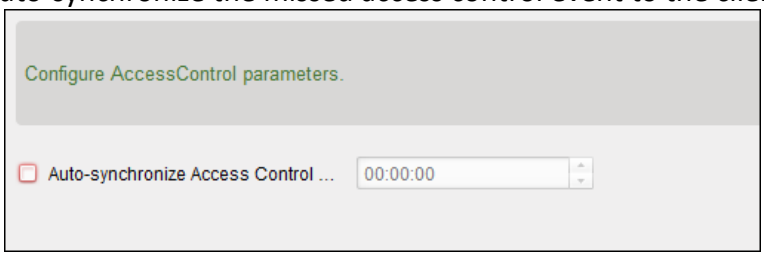
8.3 System Configuration

Purpose:

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

Steps:

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



8.4 Access Control Management

Purpose:

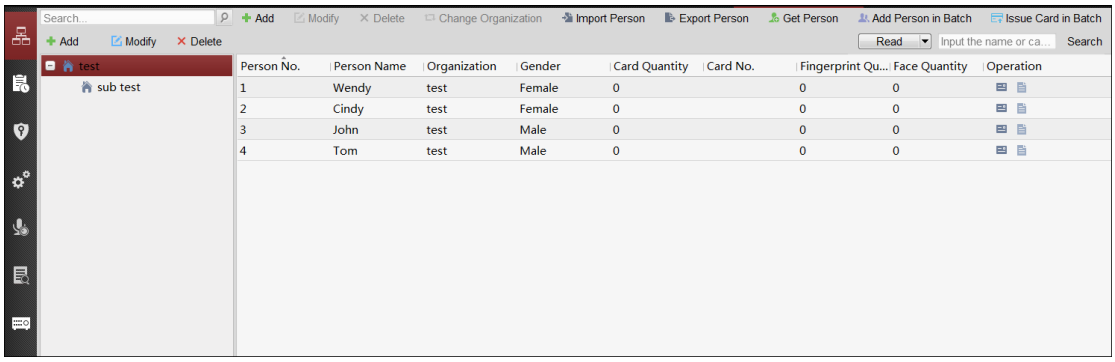
The Access Control module is applicable to access control devices and video intercom. It provides multiple functionalities, including person and card management, permission configuration, access control status management, video intercom, and other advanced functions.

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

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

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

Click to enter the Access Control module.



Before you start:

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

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

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

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

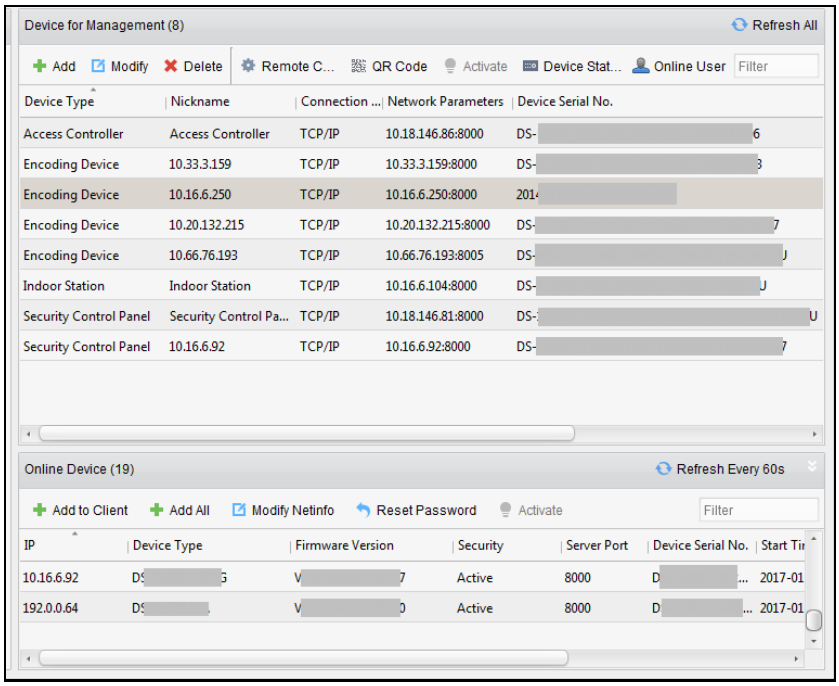
The Access Control module is composed of the following sub modules.

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

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

8.4.1 Adding Access Control Device

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



Note: After adding the device, you should check the device arming status in **Tool – Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, refer *8.13 Arming Control*.

Creating Password

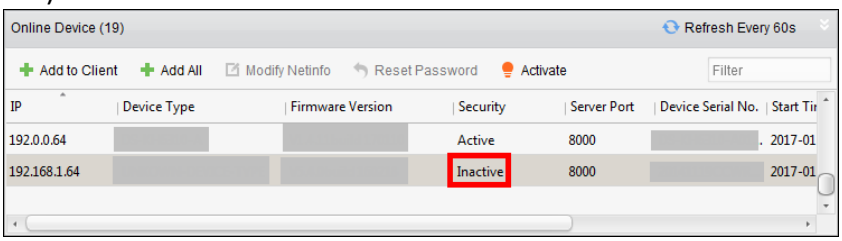
Purpose:

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

Note: This function should be supported by the device.

Steps:

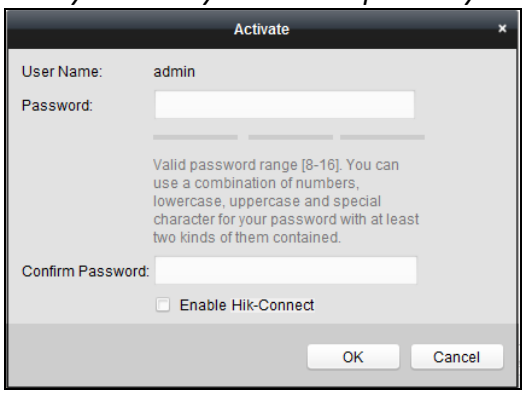
1. Enter the Device Management page.
2. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.



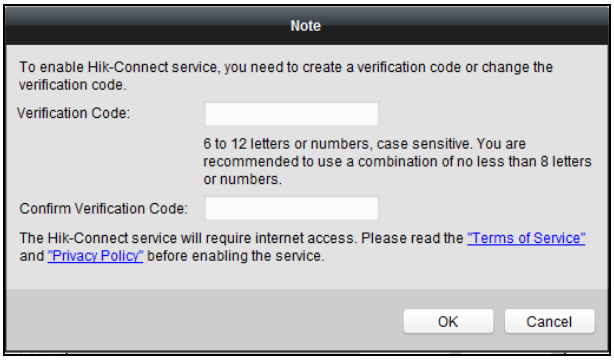
3. Click the **Activate** button to pop up the Activation interface.
4. Create a password in the password field, and confirm the password.

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

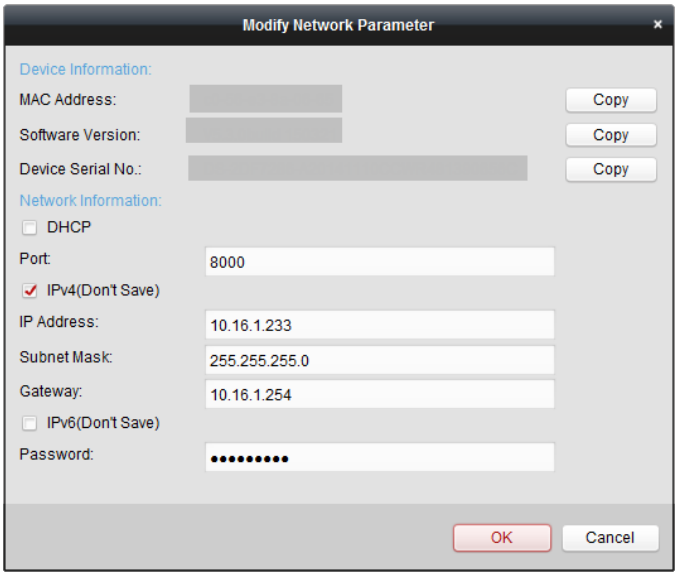
resetting the password monthly or weekly can better protect your product.



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



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

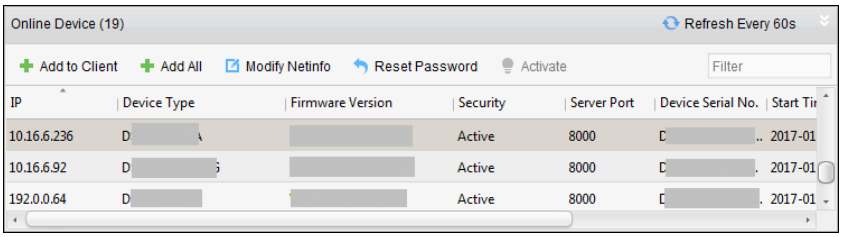


Adding Online Device

Purpose:

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

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



Steps:

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

   Note: For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, please refer to Chapter 6 Activating Access Control Terminal.

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

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

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

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

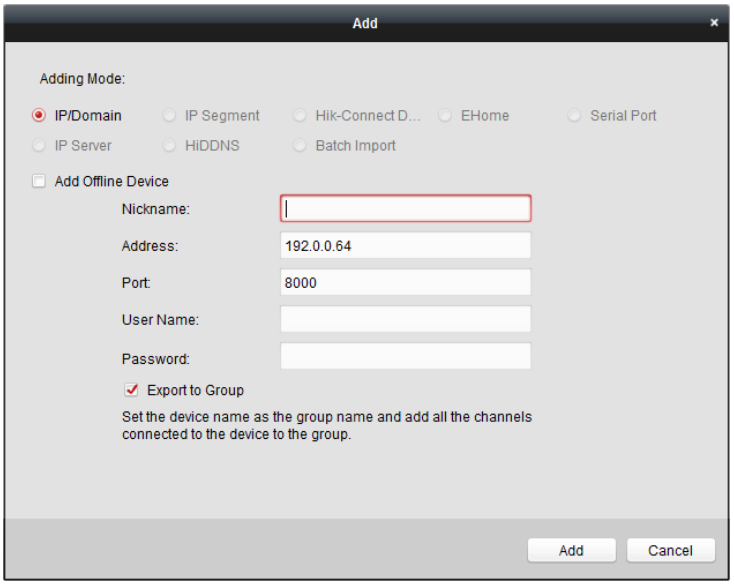
   User Name: Input the device user name. By default, the user name is *admin*.

   Password: Input the device password.

   STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower*

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

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

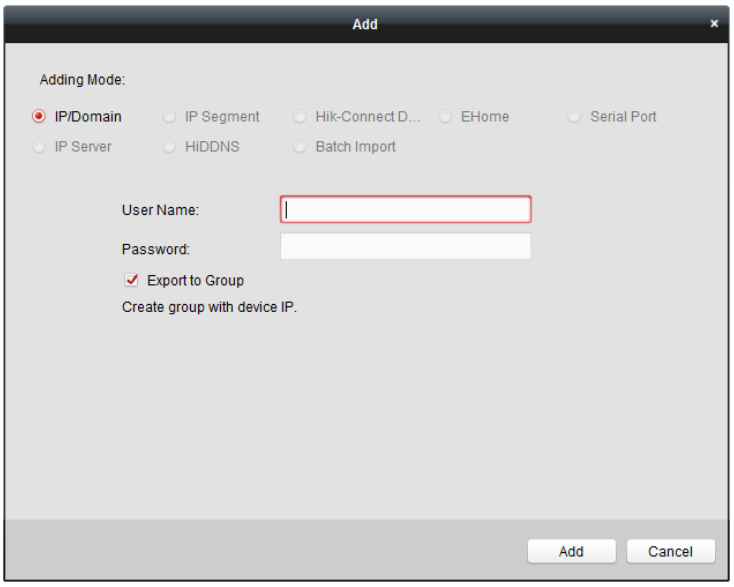


➢ Adding Multiple Online Device

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

➢ Adding All Online Devices

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



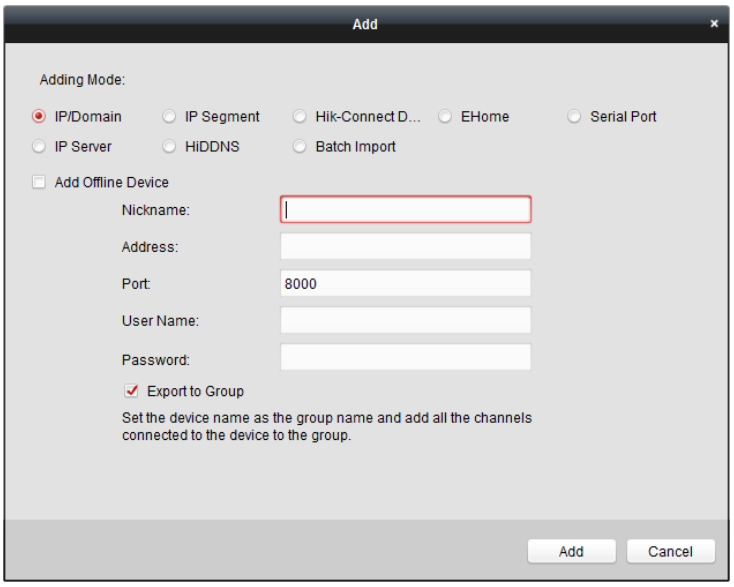
Adding Devices by IP or Domain Name

Steps:

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

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

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



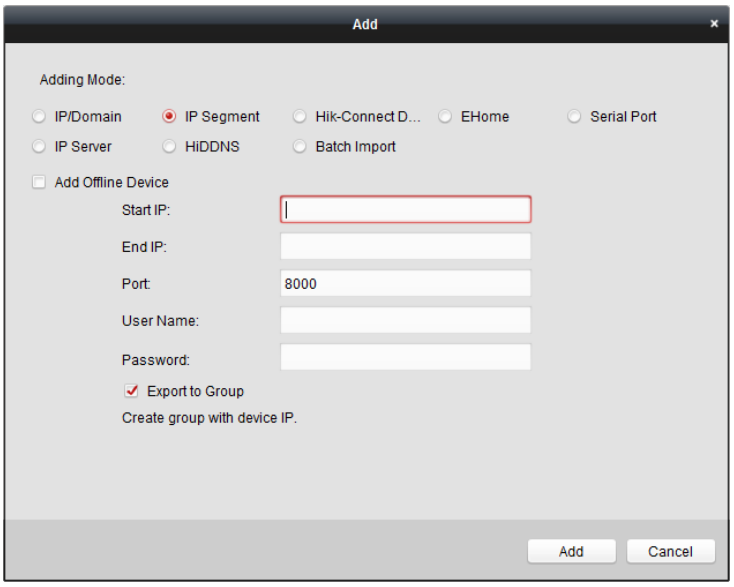
Adding Devices by IP Segment

Steps:

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

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

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



Adding Devices by Hik-Connect Domain

Purpose:

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

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

➢ Add Single Device

Steps:

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

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

   Device Serial No.: Input the device serial No.

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

   Password: Input the device password.

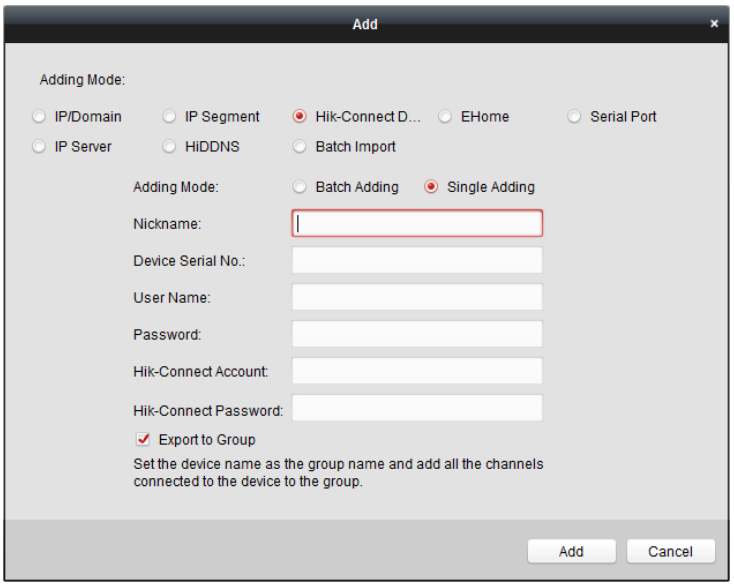
   STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password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

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

   Hik-Connect Password: Input the Hik-Connect password.
5. Optionally, check the **Export to Group** checkbox to create a group by the device name.

   You can import all the channels of the device to the corresponding group by default.

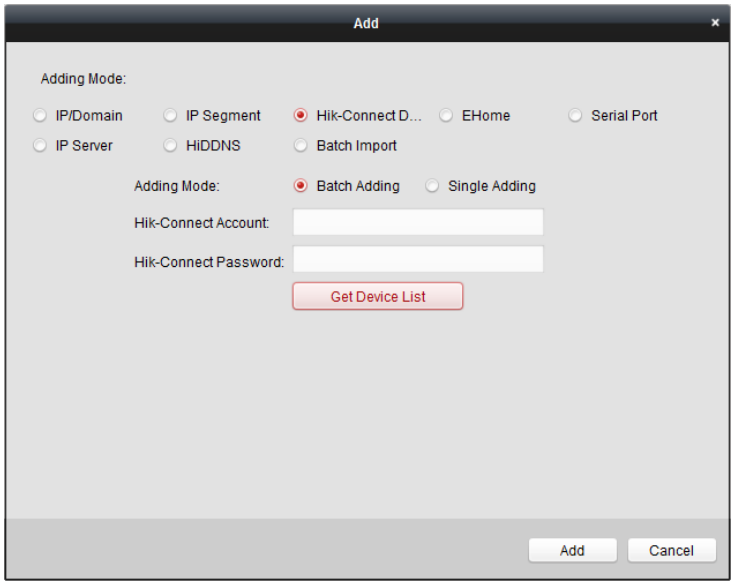
6. Click **Add** to add the device.



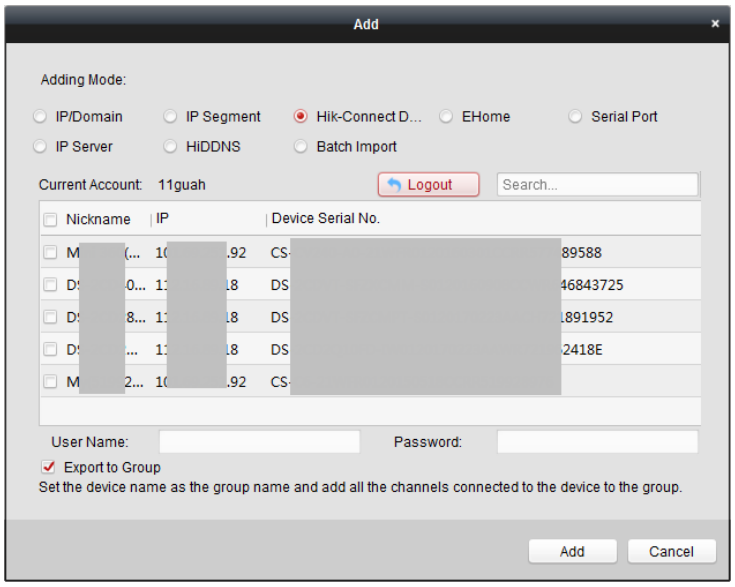
Add Devices in Batch

Steps:

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



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



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

Adding Devices by EHome Account

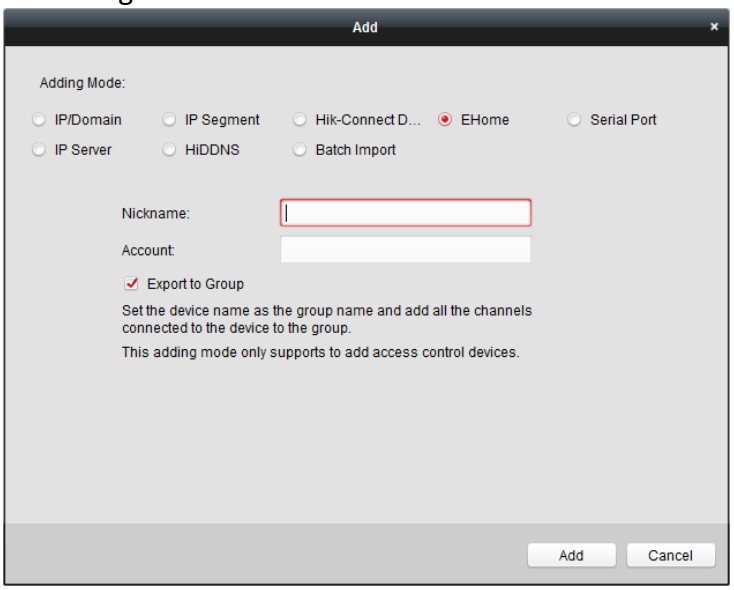
Purpose:

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

Before you start: Set the network center parameter first. For details, refer to *Chapter 8.4.4 Network Settings.*

Steps:

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



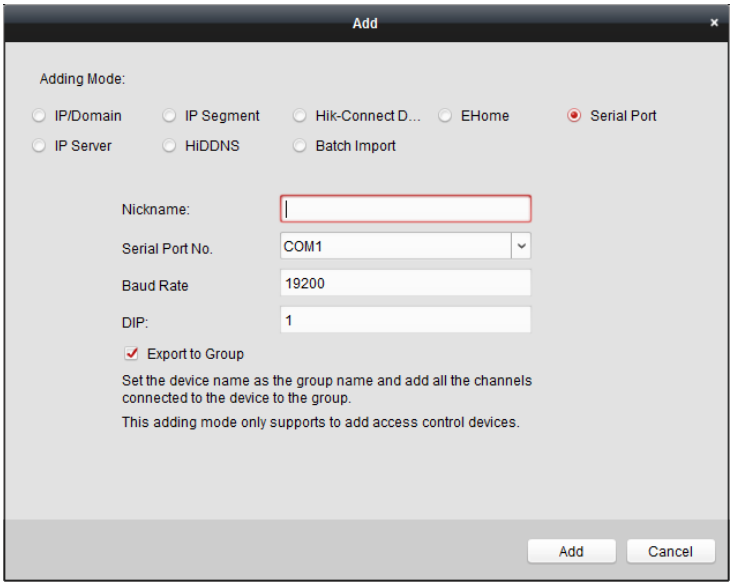
3. Input the required information.

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

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

Adding Devices by Serial Port

Purpose:
You can add access control device connected via serial port.
Steps:
1. Click **Add** to open the device adding dialog box.
2. Select **Serial Port** as the adding mode.



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

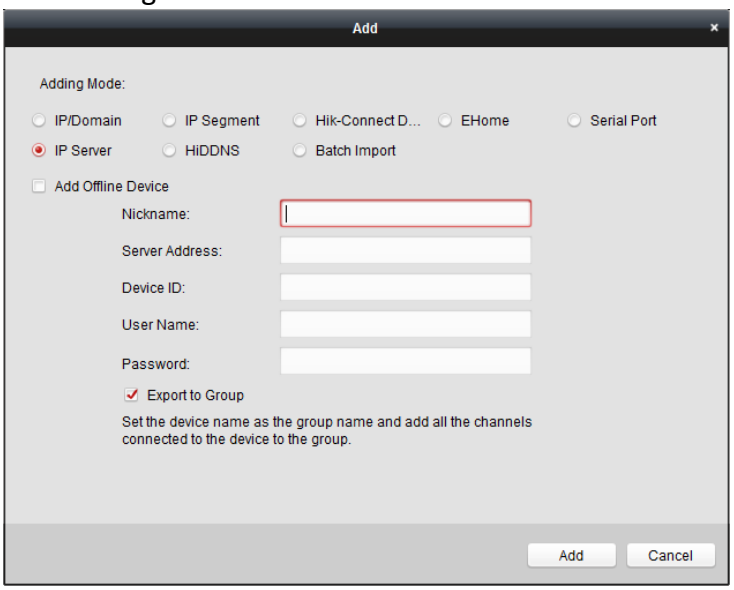
3) Click **Add**.
When the offline device comes online, the software will connect it automatically.

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

Adding Devices by IP Server

Steps:

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



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

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

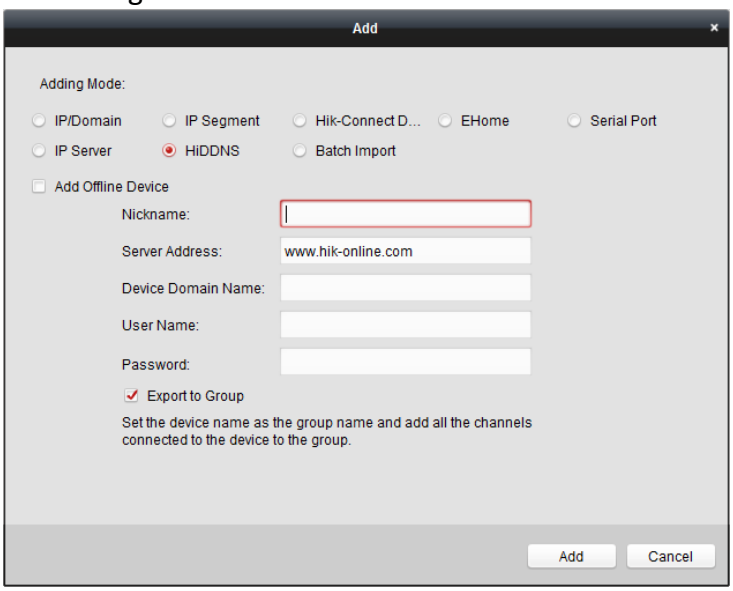
4. Optionally, check the **Export to Group** checkbox to create a group by the device name.
You can import all the channels of the device to the corresponding group by default.
Note: iVMS-4200 also provides a method to add the offline devices.
1) Check the **Add Offline Device** checkbox.
2) Input the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

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

Adding Devices by HiDDNS

Steps:

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



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

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

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

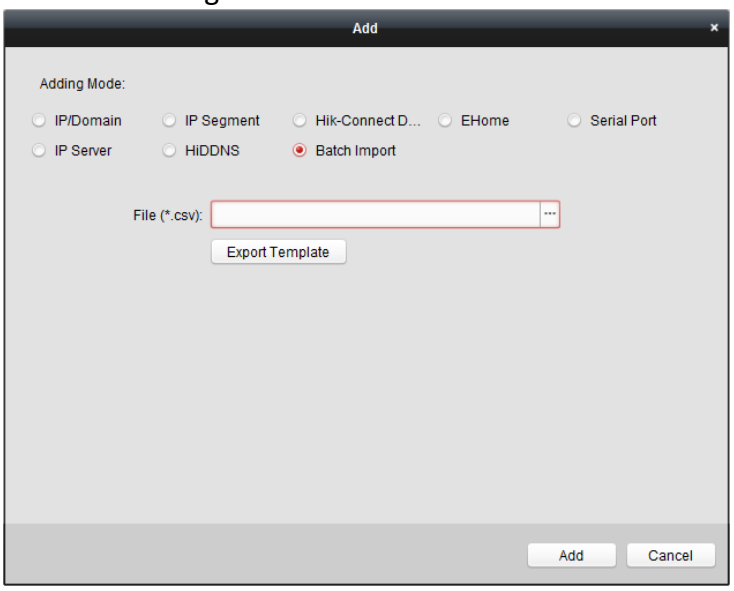
Importing Devices in Batch

Purpose:

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

Steps:

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



3. Click **Export Template** and save the pre-defined template (CSV file) on your PC.
4. Open the exported template file and input the required information of the devices to be added on the corresponding column.
   - **Nickname**: Edit a name for the device as you want.
   - **Adding Mode**: You can input 0, 2, 3, 4, 5, or 6 which indicated different adding modes. 0 indicates that the device is added by IP address or domain name; 2 indicates that the device is added via IP server; 3 indicates that the device is added via HiDDNS; 4 indicates that the device is added via EHome protocol; 5 indicates that the device is added by serial port; 6 indicates that the device is added via Hik-Connect Domain.
   - **Address**: Edit the address of the device. If you set 0 as the adding mode, you should input the IP address or domain name of the device; if you set 2 as the adding mode, you should input the IP address of the PC that installs the IP Server; if you set 3 as the adding mode, you should input *www.hik-online.com*.
   - **Port**: Input the device port No.. The default value is *8000*.
   - **Device Information**: If you set 0 as the adding mode, this field is not required; if you set 2 as the adding mode, input the device ID registered on the IP Server; if you set 3 as the adding mode, input the device domain name registered on HiDDNS server; if you set 4 as the adding mode, input the EHome account; if you set 6 as the adding mode, input the device serial No.
   - **User Name**: Input the device user name. By default, the user name is *admin*.
   - **Password**: Input the device password.

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

- **Add Offline Device**: You can input 1 to enable adding the offline device, and then the software will automatically connect it when the offline device comes online. 0 indicates disabling this function.
- **Export to Group**: You can input 1 to create a group by the device name (nickname). All the channels of the device will be imported to the corresponding group by default. 0 indicates disabling this function.
- **Channel Number**: If you set 1 for Add Offline Device, input the channel number of the device. If you set 0 for Add Offline Device, this field is not required.
- **Alarm Input Number**: If you set 1 for Add Offline Device, input the alarm input number of the device. If you set 0 for Add Offline Device, this field is not required.
- **Serial Port No.:** If you set 5 as the adding mode, input the serial port No. for the access control device.
- **Baud Rate:** If you set 5 as the adding mode, input the baud rate of the access control device.
- **DIP:** If you set 5 as the adding mode, input the DIP address of the access control device.
- **Hik-Connect Account:** If you set 6 as the adding mode, input the Hik-Connect account.
- **Hik-Connect Password:** If you set 6 as the adding mode, input the Hik-Connect password.

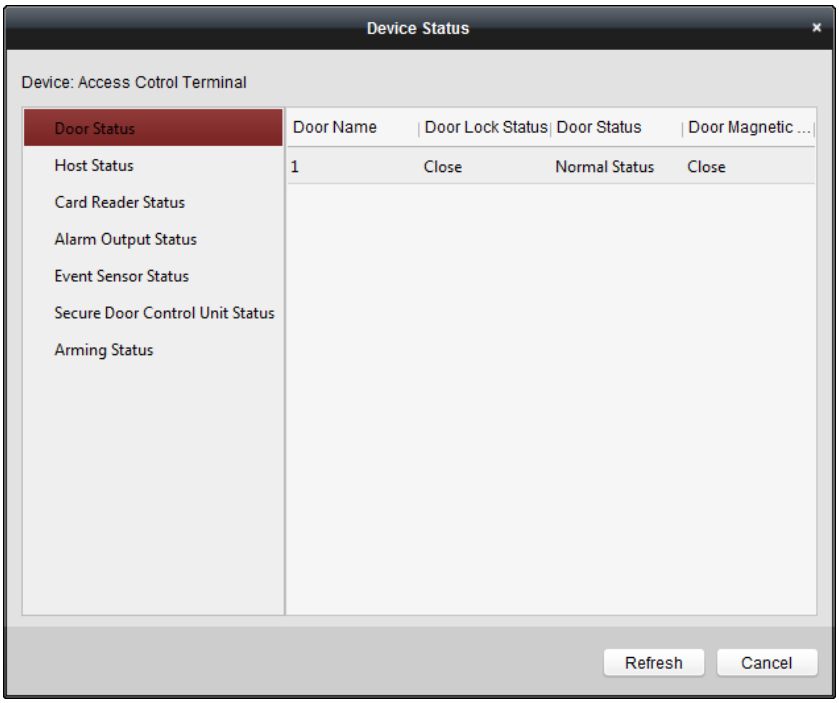
5. Click ··· and select the template file.
6. Click **Add** to import the devices.

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

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

8.4.2 Viewing Device Status

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



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

- **Door Status**: The status of the connected door.
- **Host Status**: The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, and Host Anti-Tamper Status.
- **Card Reader Status**: The status of card reader.
- ***Note:*** If you use the card reader with RS-485 connection, you can view the status of online or offline. If you use the card reader with Wiegand connection, you can view the status of offline.
- **Alarm Output Status**: The alarm output status of each port.
- **Event Sensor Status**: The event sensor status of each port.
- **Secure Door Control Unit Status:** The online status and tamper status of the Secure Door Control Unit.
- **Arming Status:** The status of the device.

8.4.3 Editing Basic Information

Purpose:

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

Steps:

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

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

8.4.4 Network Settings

Purpose:

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

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

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

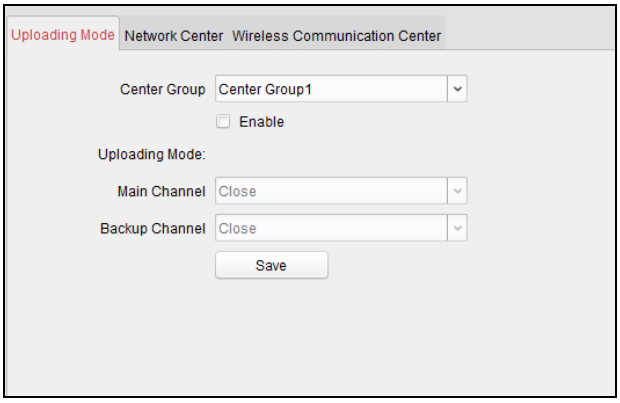
Uploading Mode Settings

Purpose：

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

Steps:

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



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

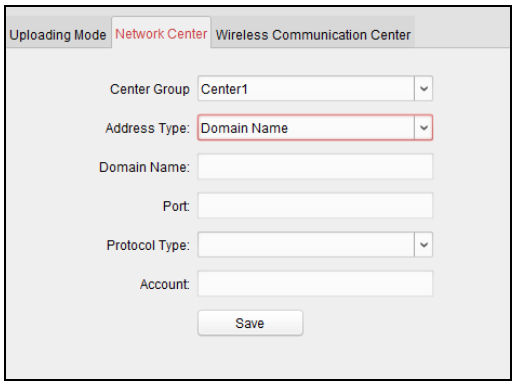
5. Click **Save** button to save parameters.

Network Center Settings

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

Steps:

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



2. Select the center group in the dropdown list.
3. Select the Address Type as **IP Address** or **Domain Name.**
4. Input IP address or domain name according to the address type.
5. Input the port No. for the protocol. By default, the port No. is 7660.
6. Select the protocol type as EHome.
7. Set an account name for the network center.
   Note: The account should contain 1 to 32 characters and only letters and numbers are allowed.
8. Click **Save** button to save parameters.

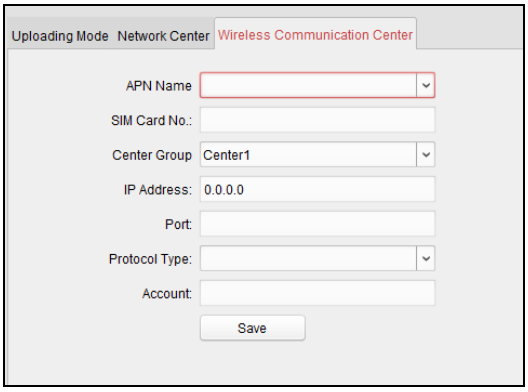
Notes:

- The port No. of the wireless network and wired network should be consistent with the port No. of EHome.
- You can set the domain name in Enable NTP area *Editing Time* section in Remote Configuration. For details, refer to *Time* in *8.4.9 Remote Configuration*.

Wireless Communication Center Settings

Steps:

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



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

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

8.4.5 Capture Settings

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

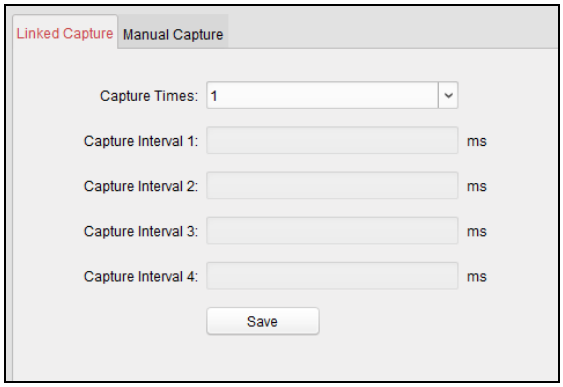
Notes:

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

Linked Capture

Steps:

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

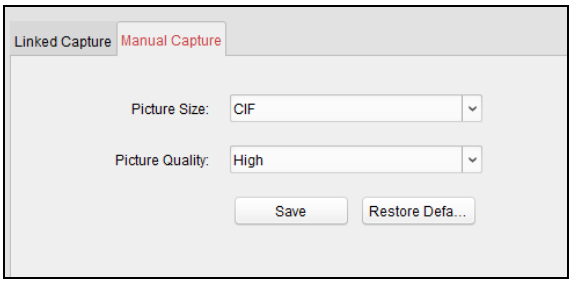


2. Set the picture size and quality.
3. Set the linked capture times once triggered.
4. Set the capture interval according to the capture times.
5. Click **Save** to save the settings.

Manual Capture

Steps:

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



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

8.4.6 RS-485 Settings

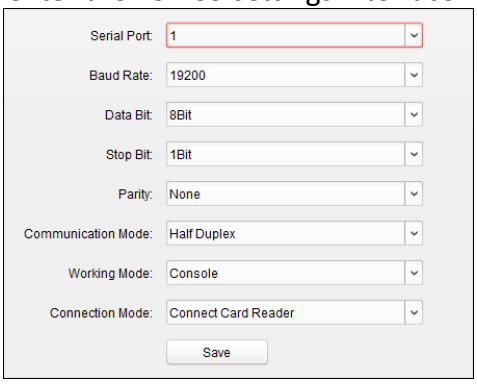
Purpose:

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

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

Steps:

1. Select the device in the device list, and click **Modify** to pop up the modifying device information window.
2. Click **RS-485 Settings** tab to enter the RS-485 settings interface.

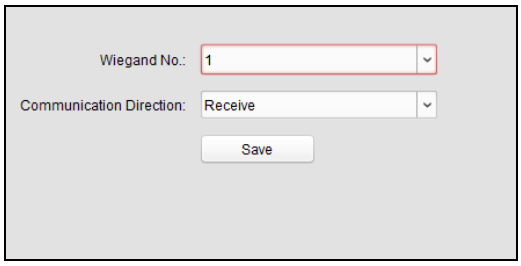


2. Select the serial No. of the port from the dropdown list to set the RS-485 parameters.
3. Set the baud rate, data bit, the stop bit, parity type, communication mode, work mode, and the connection mode in the dropdown list.
4. Click **Save** to save the settings and the configured parameters will be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

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

8.4.7 Wiegand Settings

Purpose:
You can set the Wiegand channel and the communication mode.
Note: The Wiegand Settings should be supported by the device.
Steps:
1. Select the device in the device list, and click **Modify** to pop up the modifying device information window.
2. Click the **Wiegand Settings** tab to enter the Wiegand Settings interface.



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

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

8.4.8 Authenticating M1 Card Encryption

Before you start:
You should use the specified Hikvision card enrollment station to issue card. For details, refer to *Adding Person (Card)* in *Chapter 8.6.1 Adding Person.*
Purpose:
The M1 Card Encryption function increases the authentication security level, which should be applied together with the card enrollment station of our company via the client software or the web client. After issuing the card, you can set the M1 card encryption function on the controller.
Note: The function should be supported by the access control device and the card reader.
Steps:
1. Select the device in the device list, and click **Modify** to pop up the modifying device information window.
2. Click **M1 Card Encryption** tab to enter the M1 Card Encryption interface.
3. In the M1 Card Encryption interface, check **Enable** checkbox to enable the M1 card encryption function.

4. Set the sector ID.
5. Click **Save** to save the settings.

   Note: The sector ID ranges from 1 to 100.

8.4.9 Remote Configuration

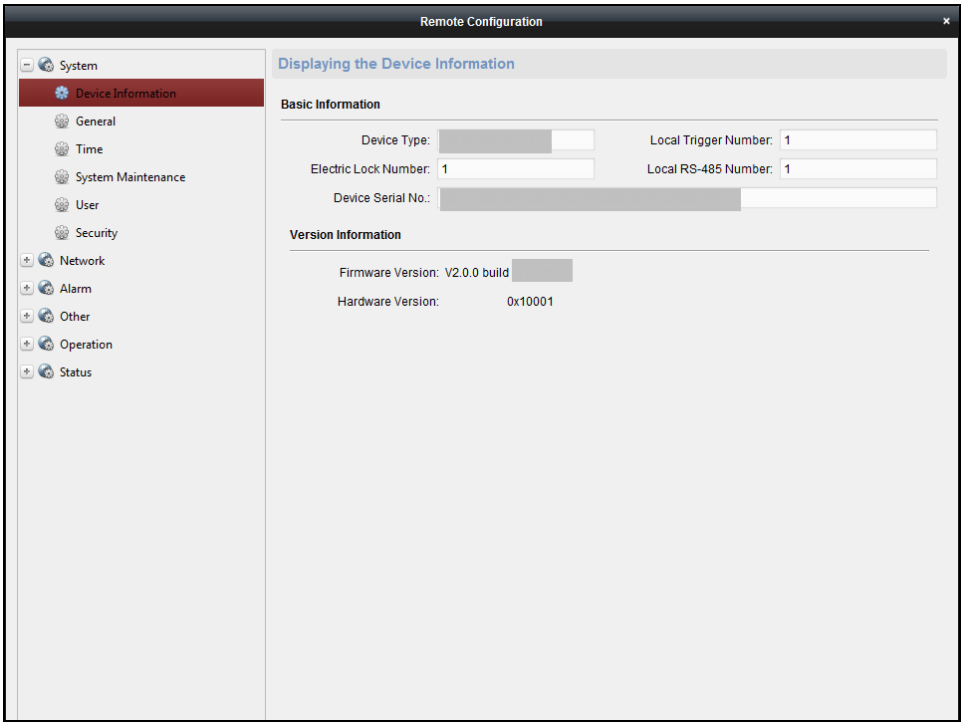
Purpose:

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

Checking Device Information

Steps:

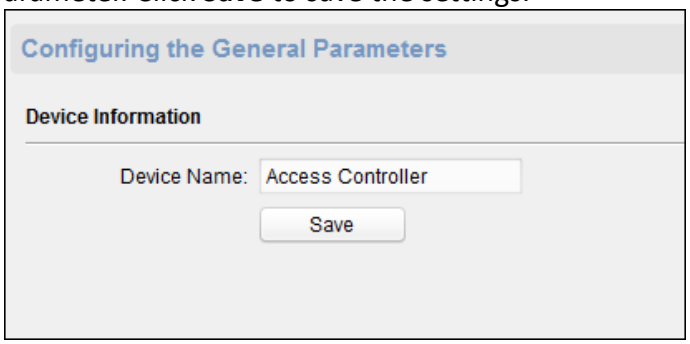
1. In the device list, you can click **Remote Configuration** to enter the remote configuration interface.
2. Click **System** -> **Device Information** to check the device basic information and the device version information.



Editing Device Name

In the Remote Configuration interface, click **System** -> **General** to configure the device name and

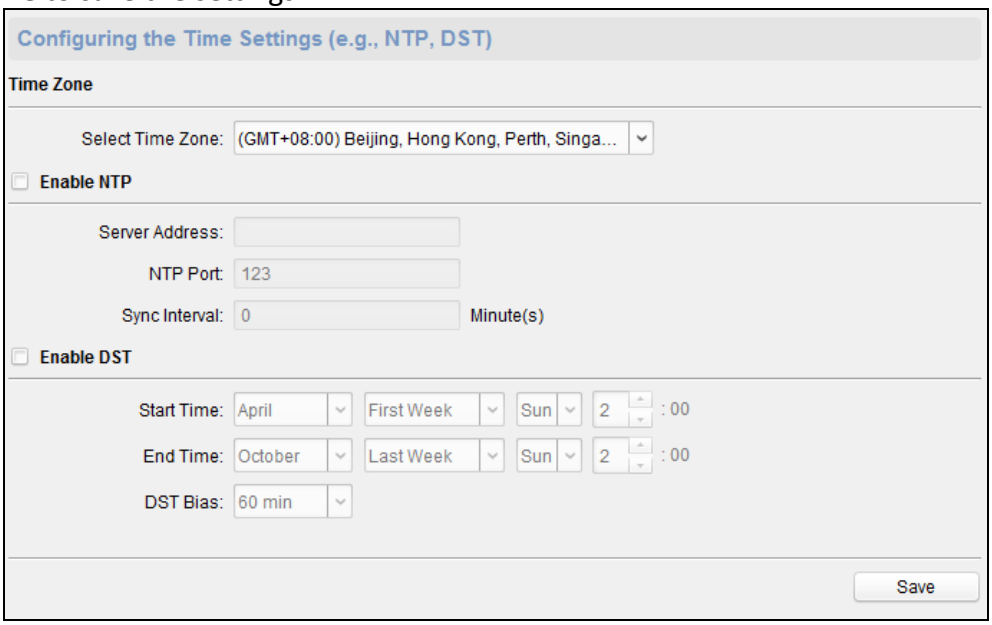
overwrite record files parameter. Click **Save** to save the settings.



Editing Time

Steps:

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



Setting System Maintenance

Purpose:

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

Steps:

1. In the Remote Configuration interface, click **System** -> **System Maintenance**.
2. Click **Reboot** to reboot the device.
   Or click **Restore Default Settings** to restore the device settings to the default ones, excluding the IP address.
   Or click **Restore All** to restore the device parameters to the default ones. The device should be activated after restoring.

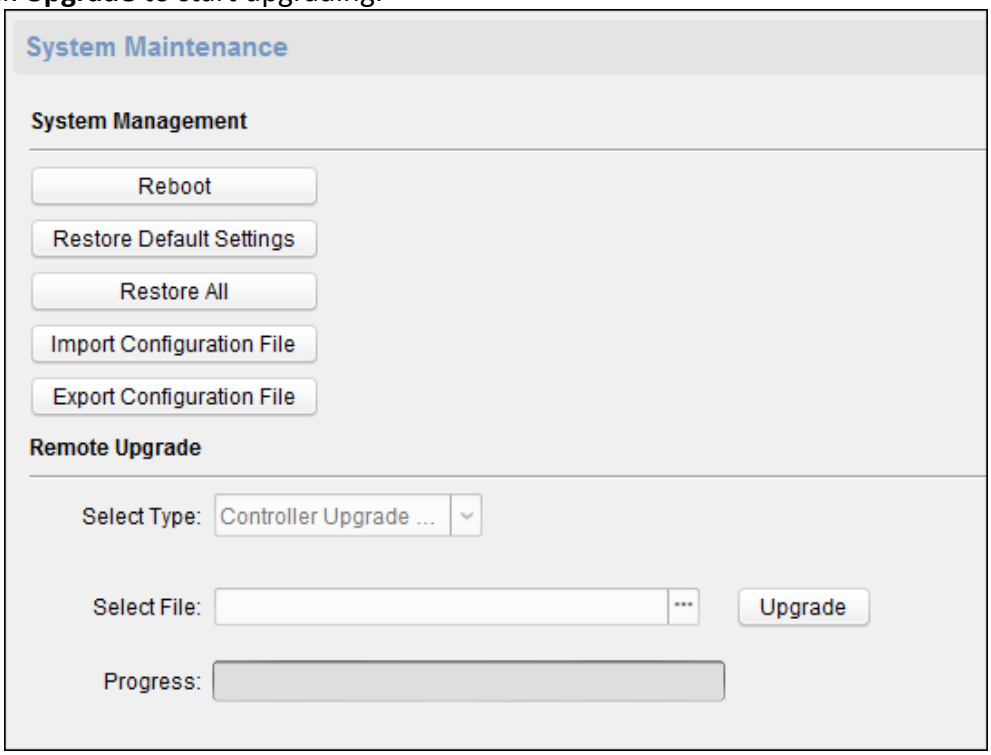
Note: The configuration file contains the device parameters.

Or click **Import Configuration File** to import the configuration file from the local PC to the device.

Or click **Export Configuration File** to export the configuration file from the device to the local PC

Note: The configuration file contains the device parameters.

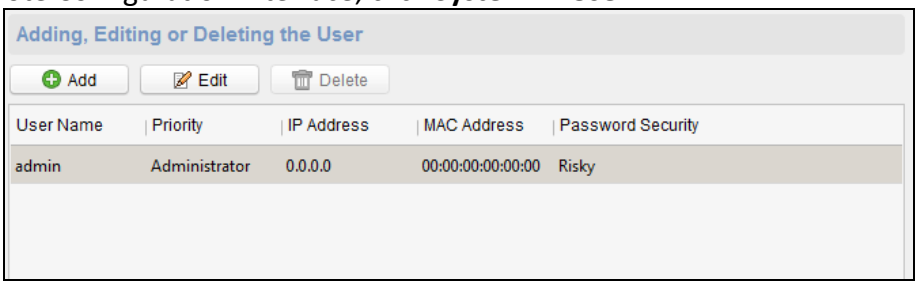
3. You can also remote upgrade the device.
   1) In the Remote Upgrade part, click ··· to select the upgrade file.
   2) Click **Upgrade** to start upgrading.



Managing User

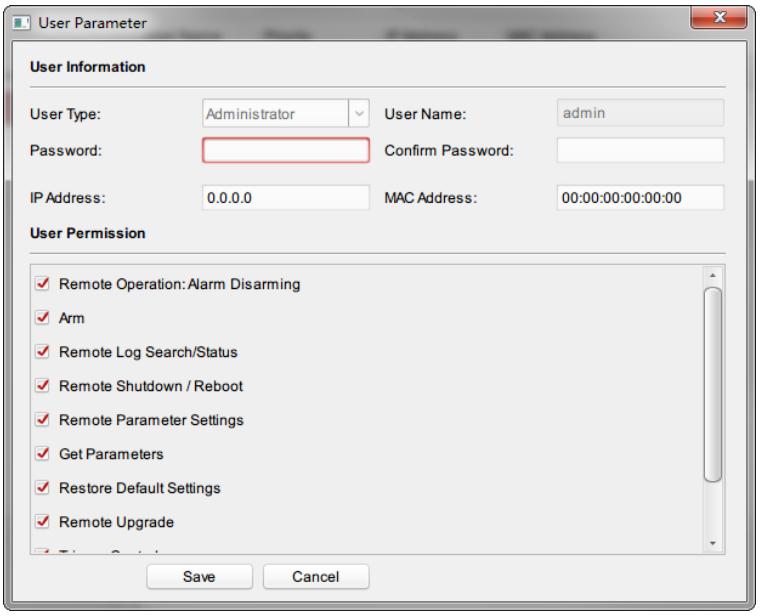
Steps:

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



2. Click **Add** to add the user (Do not support by the elevator controller.).

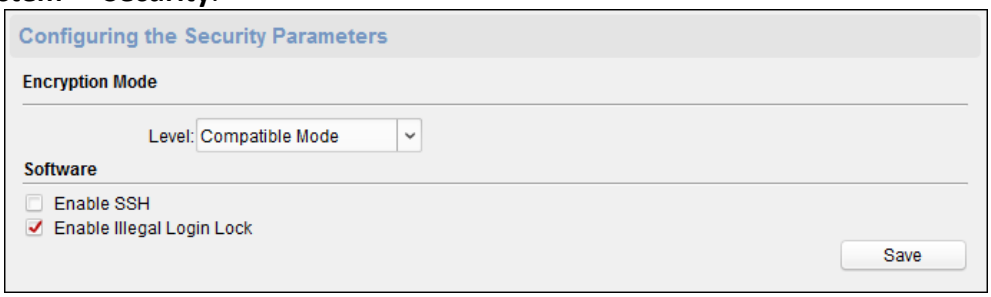
   Or select a user in the user list and click **Edit** to edit the user. You are able to edit the user password, the IP address, the MAC address and the user permission. Cilck **OK** to confirm editing.



Setting Security

Steps:

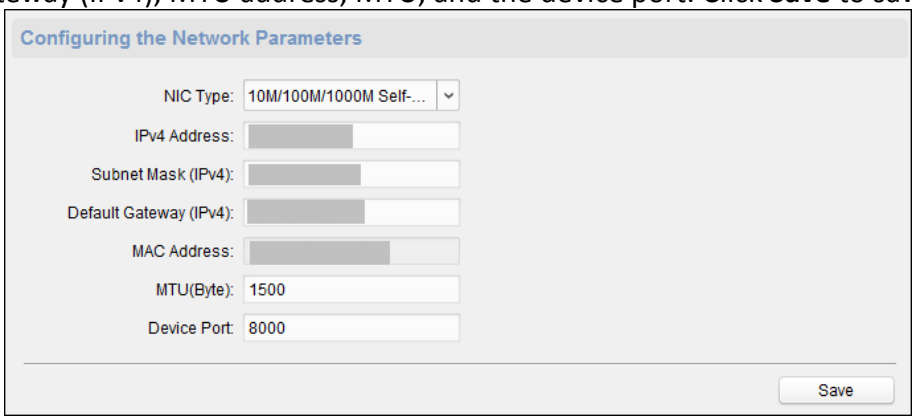
1. Click **System** -> **Security**.



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

Configuring Network Parameters

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



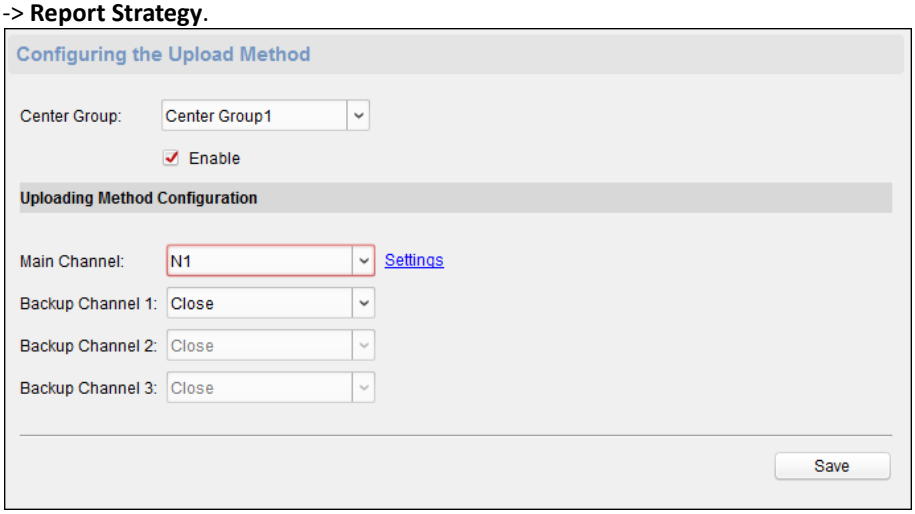
Configuring Upload Method

Purpose：

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

Steps:

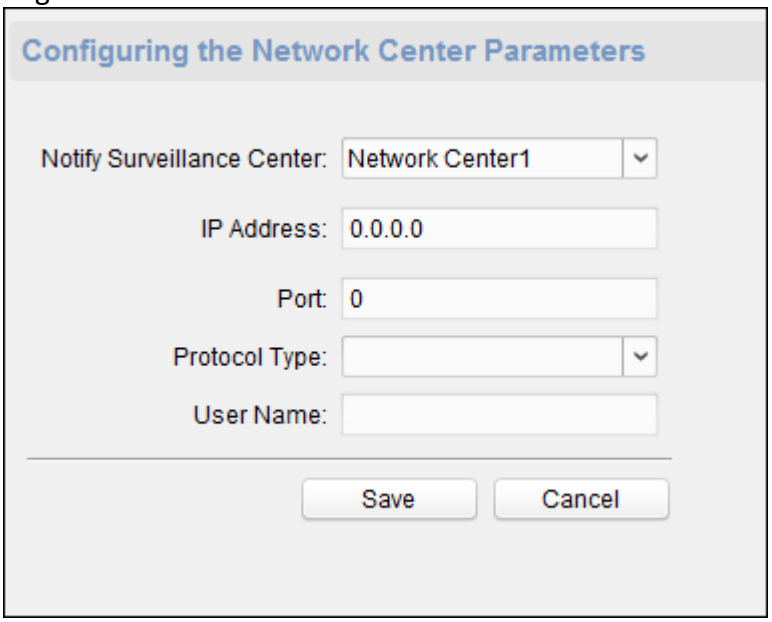
1. Click **Network** -> **Report Strategy**.



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

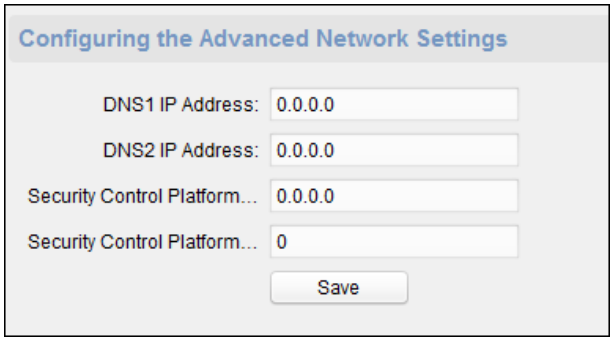
Configuring Network Center

You can set the notify surveillance center, center's IP address, the port No., the Protocol (EHome), and the EHome account user name to transmit data via EHome protocol. For details about EHome protocol's transmission, refer to *Network Center Settings* in *Chapter 8.4.4 Network Settings.* Click **Save** to save the settings or click



Configuring Advanced Network

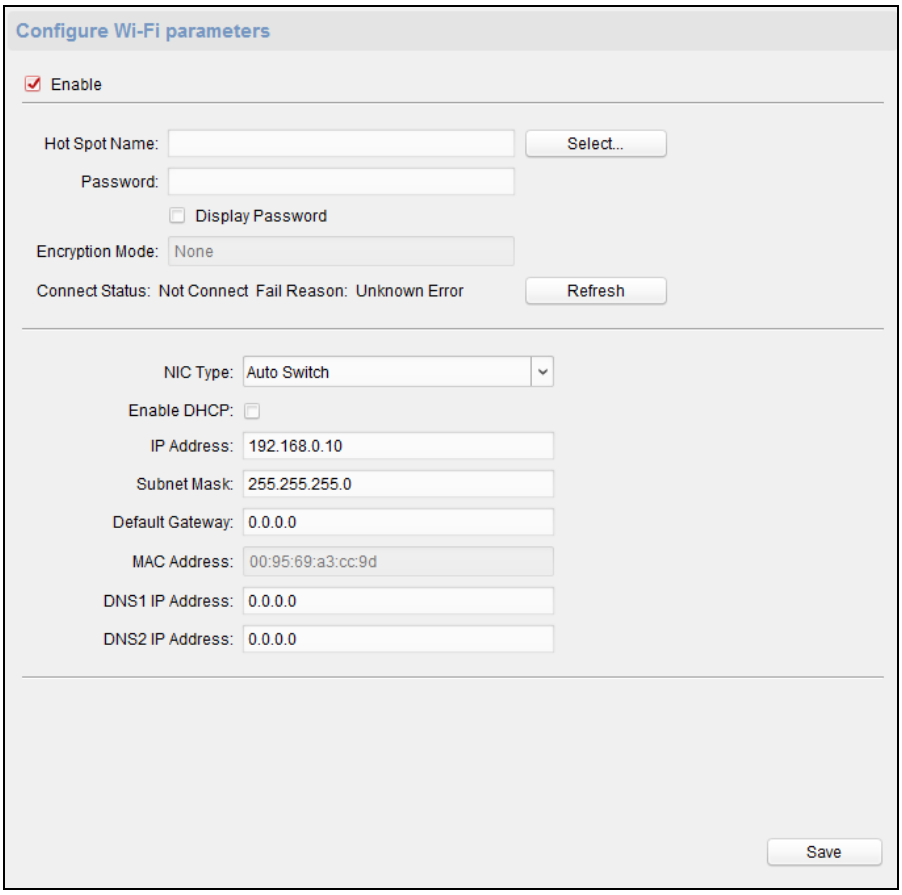
Click **Network** -> **Advanced Settings**. You can configure the DNS IP address 1, the DNS IP address 2, the security control platform IP, and the security control platform port. Click **Save** to save the settings.



Configuring Wi-Fi

Steps:

1. Click **Network –> Wi-Fi**.



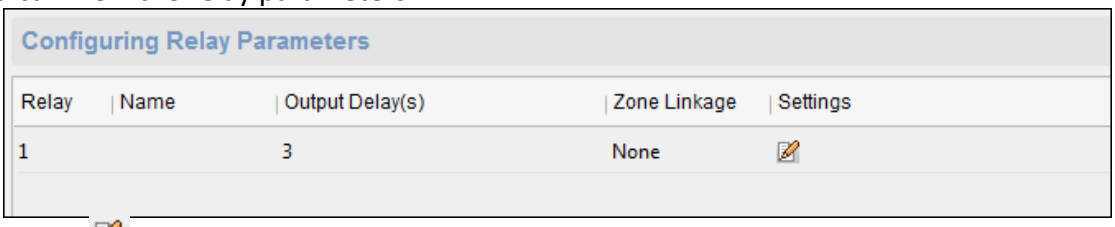
2. Check **Enable** to enable the Wi-Fi function.
3. Input the hot spot name.
   Or you can click **Select...** to select a network.
4. Input the Wi-Fi password.
5. (Optional) Click **Refresh** to refresh the network status.

6. (Optional) Select the NIC Type.
7. (Optional) Select to uncheck **Enable DHCP** and set the IP address, the subnet mask, the default gateway, the MAC address, the DNS1 IP Address, and the DNS2 IP address.
8. Click **Save** to save the settings.

Configuring Relay Parameters

Steps:

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



Configuring Relay Parameters

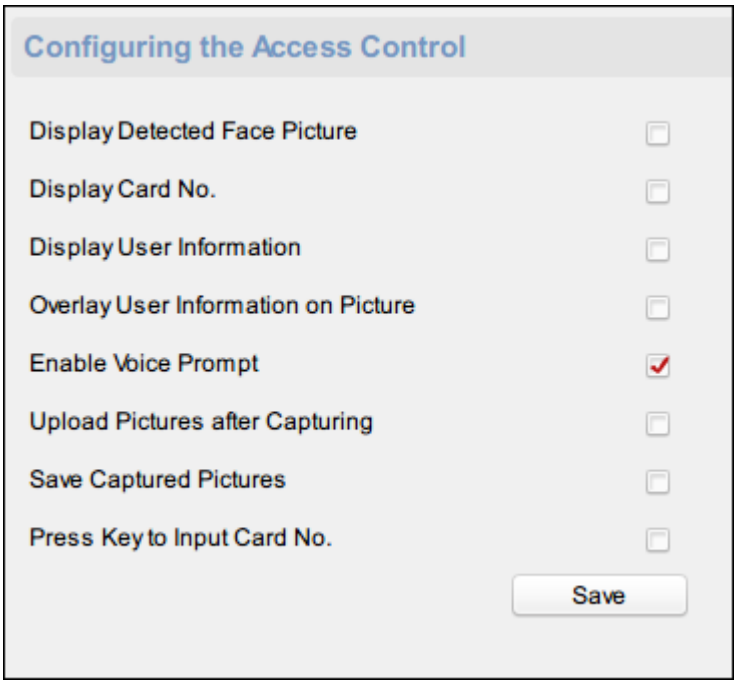
Relay	Name	Output Delay(s)	Zone Linkage	Settings
1		3	None	

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

Configuring Access Control Parameters

Steps:

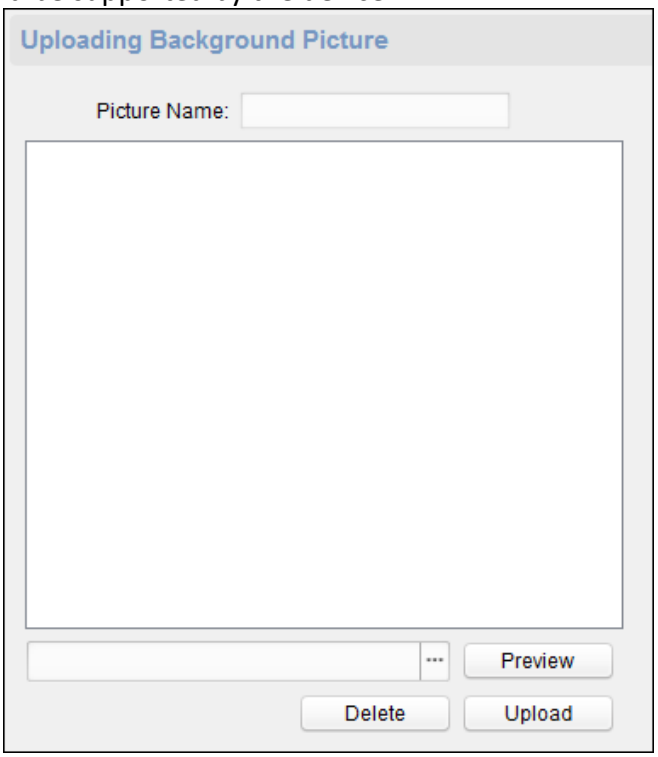
1. In the Remote Configuration interface, click **Other** -> **Access Control Parameters**.
2. Select and check the item as you desired.
   - **Display Detected Face Pictures:** Display face picture when auththenticating.
   - **Display Card No.:** Display the card infomratio when authenticating.
   - **Display User Information:** Display the user infomration when authenticating.
   - **Overlay User Information on Picture:** Display the user infomration on the captured picture.
   - **Enable Voice Prompt:** If check the checkbox, the voicce pormpt is enabled in the device. You can hear the voice prompt when operating in the device.
   - **Upload Pictures after Capturing:** If check the checkbox, the pictures captured by linked camera will be upload to the system automatically.
   - **Save Captured Pictures:** If you check the checkbox, you can save the picture capured by linked camera to the device. You can view the picture in *8.10 Searching Access Control Event*.
   - **Press Key to Input Card No.:** If you check the checkbox, you can input the card No. by pressing the key..
3. Click **Save** to save the settings.



Uploading Background Picture

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

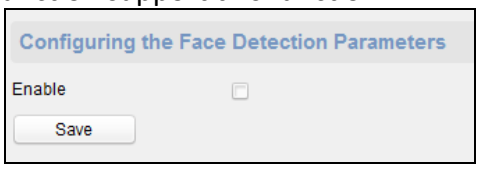
Note: The function should be supported by the device.



Configuring Face Detection Parameters

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

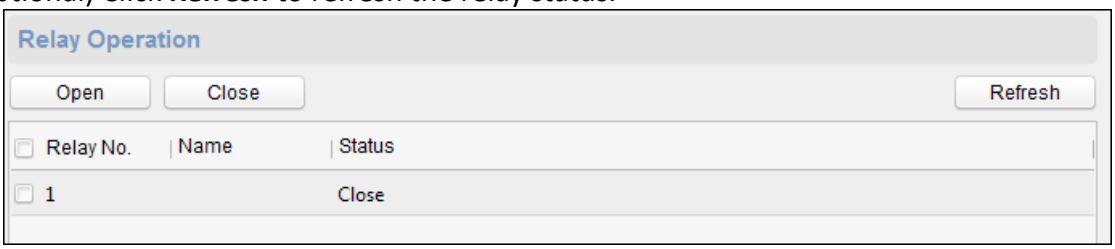
detection function.
After you enable the function, the device should detect the face while authenticating. Or the authentication will be failed.
Note: Only devices with video function support this function.



Operating Relay

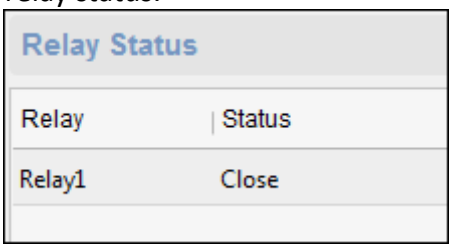
Steps:

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



Viewing Relay Status

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



8.5 Organization Management

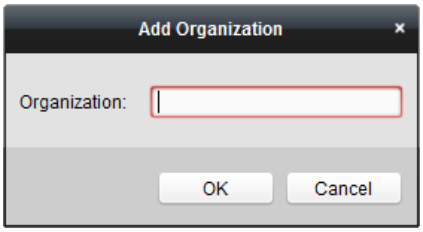
You can add, edit, or delete the organization as desired.

Click tab to enter the Person and Card Management interface.

8.5.1 Adding Organization

Steps:

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



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

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

8.5.2 Modifying and Deleting Organization

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

Notes:

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

8.6 Person Management

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

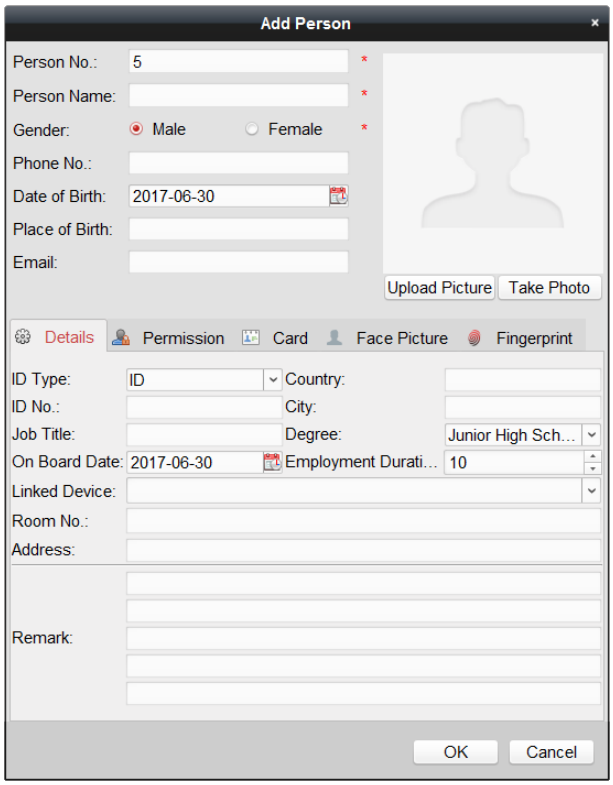
Note: Up to 10,000 persons or cards can be added.

8.6.1 Adding Person

Adding Person (Basic Information)

Steps:

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

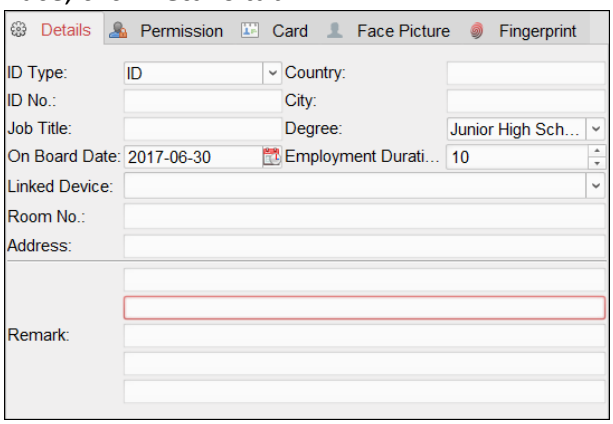


2. The Person No. will be generated automatically and is not editable.
3. Input the basic information including person name, gender, phone No., birthday details, and email address.
4. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
   Note: The picture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

Adding Person (Detailed Information)

Steps:

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



2. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.
   - **Linked Device:** You can bind the indoor station to the person.

Note: If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

- **Room No.:** You can input the room No. of the person.

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

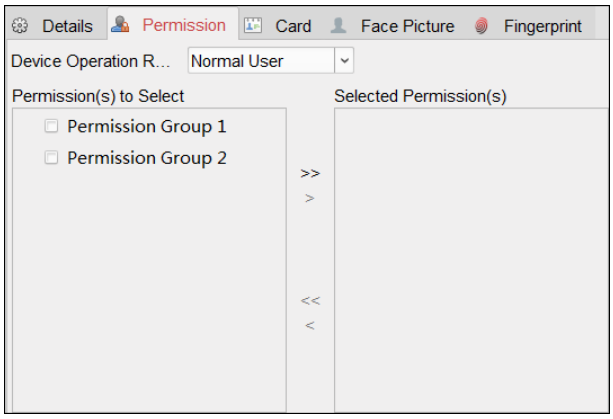
Adding Person (Permission)

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

Note: For setting the access control permission, refer to *Chapter 8.8 Permission Configuration.*

Steps:

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



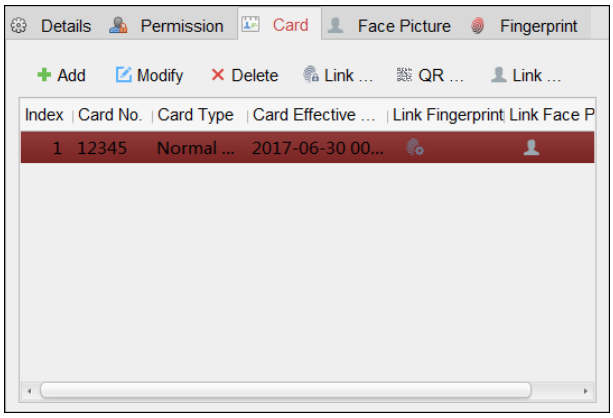
2. In the Device Operation Role field, select the role of operating the access control device.
   Normal User: The person has the permission to check-in/out on the device, pass the access control point, etc.
   Administrator: The person has the normal user permission, as well as permission to configure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

Adding Person (Card)

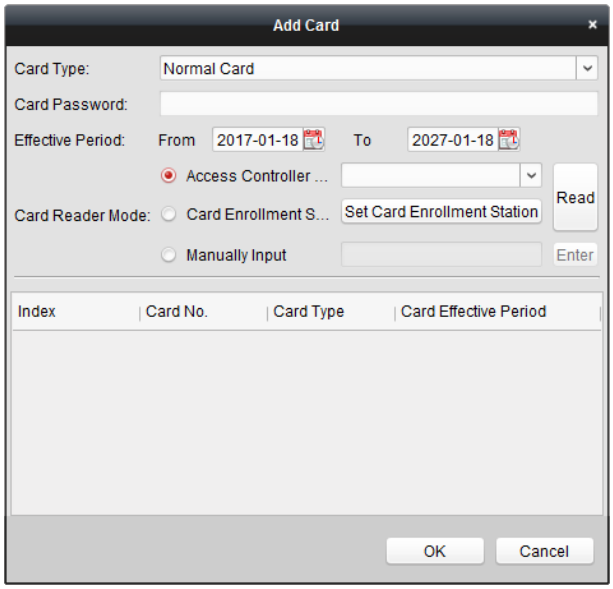
You can add card and issue the card to the person.

Steps:

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



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



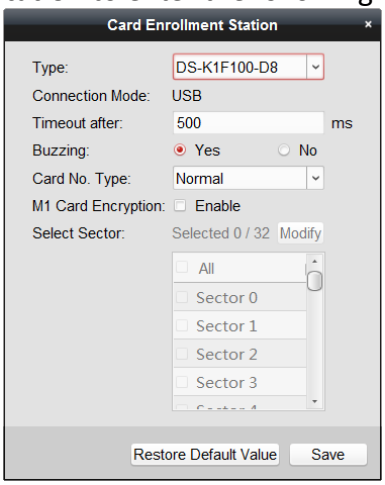
3. Select the card type according to actual needs.
   - **Normal Card**
   - **Card for Disabled Person**: The door will remain open for the configured time period for the card holder.
   - **Card in Blacklist**: The card swiping action will be uploaded and the door cannot be opened.
   - **Patrol Card**: The card swiping action can used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
   - **Duress Card**: The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.
   - **Super Card**: The card is valid for all the doors of the controller during the configured schedule.
   - **Visitor Card**: The card is assigned for visitors. For the Visitor Card, you can set the **Max. Swipe Times**.

     Note: The Max. Swipe Times should be between 0 and 255. When setting as 0, it means the card swiping is unlimited.
4. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, *Chapter 8.9.2 Card Reader Authentication.*

5. Click to set the effective time and expiry time of the card.
6. Select the Card Reader Mode for reading the card No.
   - **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
   - **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.

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



     1) Select the Card Enrollment Station type.

        Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.
     2) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.

        If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.
     3) Click **Save** button to save the settings.

     You can click **Restore Default Value** button to restore the defaults.
   - **Manually Input:** Input the card No. and click **Enter** to input the card No.
7. Click **OK** and the card(s) will be issued to the person.
8. (Optional) You can select the added card and click **Modify** or **Delete** to edit or delete the card.
9. (Optional) You can generate and save the card QR code for QR code authentication.
   1) Select an added card and click **QR Code** to generate the card QR code.
   2) In the QR code pop-up window, click **Download** to save the QR code to the local PC.

      You can print the QR code for authentication on the specified device.

      Note: The device should support the QR code authentication function. For details about setting the QR code authentication function, see the specified device user manual.

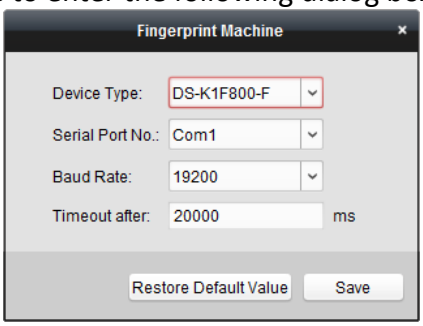
10. (Optional) You can click **Link Fingerprint** to link the card with the person's fingerprint, so that the person can place the finger on the scanner instead of swiping card when passing the door.
11. (Optional) You can click **Link Face Picture** to link the card with the face picture, so that the person can pass the door by scanning the face via the device instead of swiping card when passing the door.
12. Click **OK** to save the settings.

Adding Person (Fingerprint)

Steps:

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

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



   1) Select the device type.
      Currently, the supported fingerprint machine types include DS-K1F800-F, DS-K1F810-F, DS-K1F820-F, and DS-K1F181-F.
   2) For fingerprint machine type DS-K1F800-F, you can set the serial port number, baud rate, and overtime parameters of the fingerprint machine.
   3) Click **Save** button to save the settings.
      You can click **Restore Default Value** button to restore the default settings.

   Notes:

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

value is 19200.

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

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

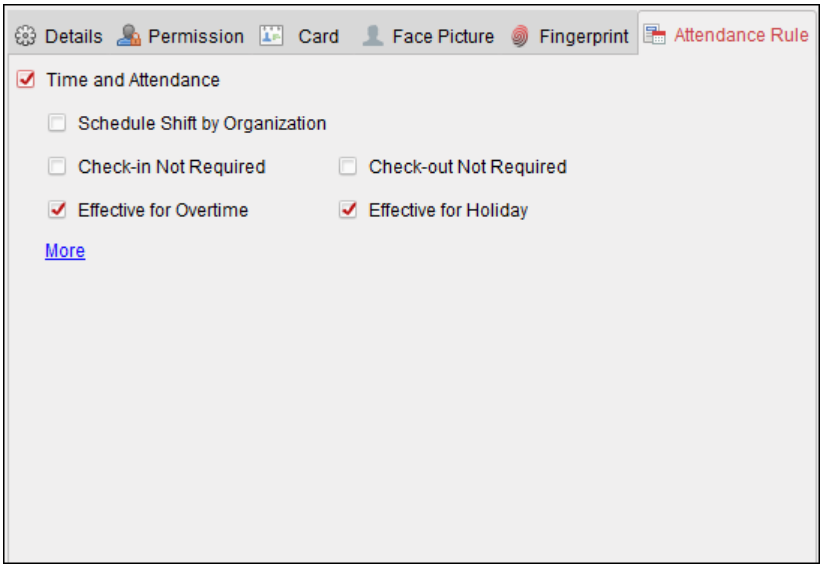
Adding Person (Attendance Rule)

You can set the attendance rule for the person.

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

Steps:

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



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

Importing and Exporting Person Information

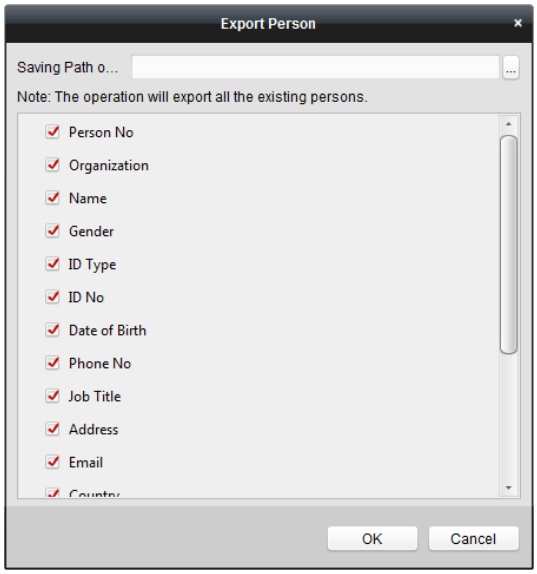
The person information can be imported and exported in batch.

Steps:

1. **Exporting Person:** You can export the added persons' information in Excel format to the local

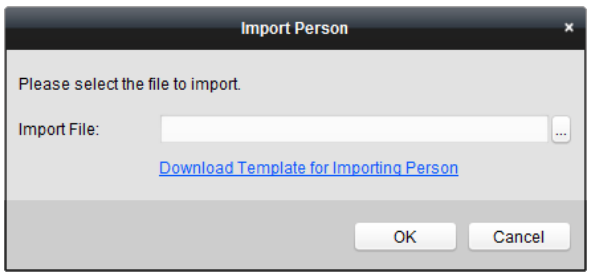
PC.

1) After adding the person, you can click **Export Person** button in the Person and Card tab to pop up the following dialog.
2) Click ... to select the path of saving the exported Excel file.
3) Check the checkboxes to select the person information to export.



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

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



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

Getting Person Information from Access Control Device

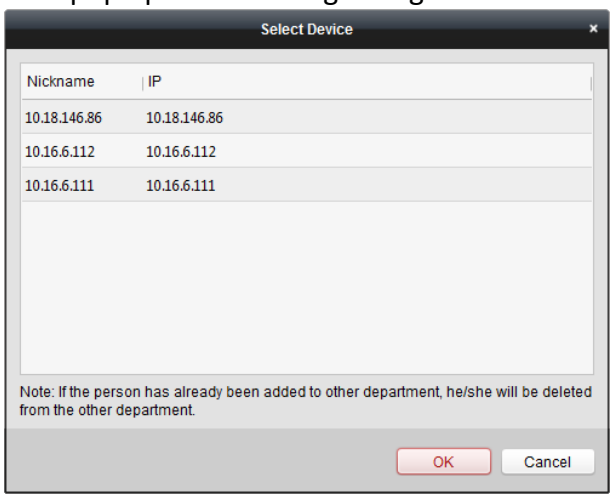
If the added access control device has been configured with person information (including person details, fingerprint, issued card information), you can get the person information from the device and import to the client for further operation.

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

Steps:

1. In the organization list on the left, click to select an organization to import the persons.

2. Click **Get Person** button to pop up the following dialog box.



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

Notes:

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

8.6.2 Managing Person

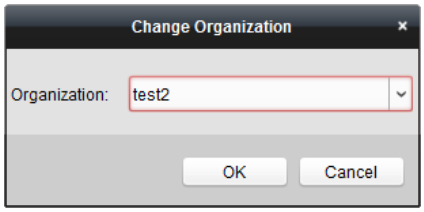
Modifying and Deleting Person

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

Changing Person to Other Organization

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

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



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

Searching Person

You can input the keyword of card No. or person name in the search field, and click **Search** to search the person.

You can input the card No. by clicking **Read** to get the card No. via the connected card enrollment station.

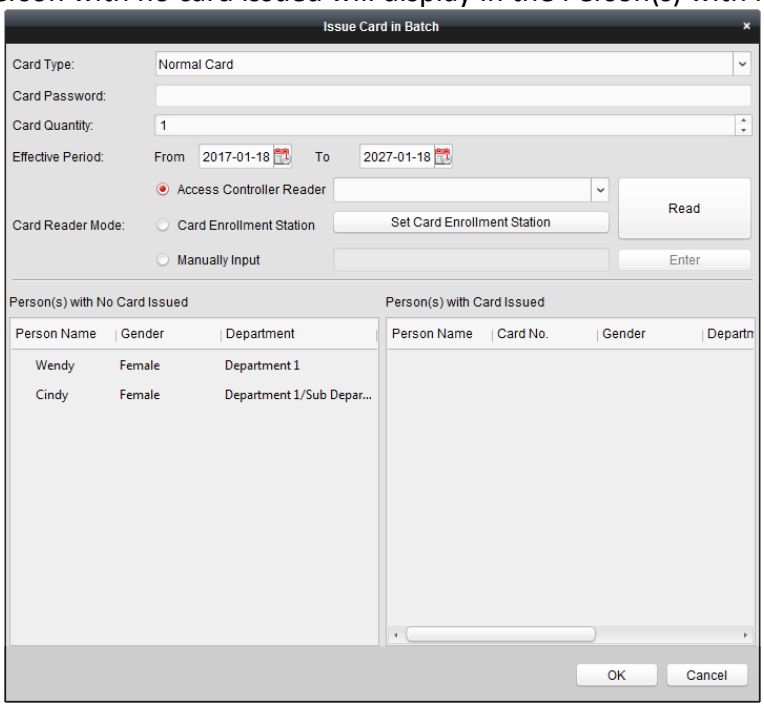
You can click **Set Card Enrollment Station** in the dropdown list to set the parameters.

8.6.3 Issuing Card in Batch

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

Steps:

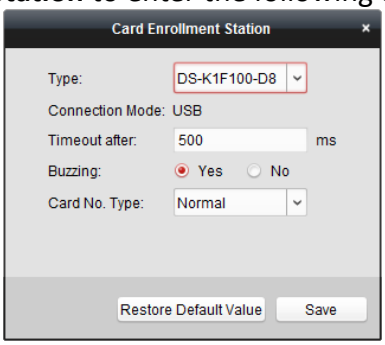
1. Click **Issue Card in Batch** button to enter the following dialog.
   All the added person with no card issued will display in the Person(s) with No Card Issued list.



2. Select the card type according to actual needs.
   Note: For details about the card type, refer to *Adding Person.*
3. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.
   Note: The password will be required when the card holder swiping the card to get enter to or

exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to *Chapter 8.9.2 Card Reader Authentication.*

4. Input the card quantity issued for each person.
   For example, if the Card Quantity is 3, you can read or enter three card No. for each person.
5. Click to set the effective time and expiry time of the card.
6. In the Person(s) with No Card Issued list on the left, select the person to issue card.
   Note: You can click on the Person Name, Gender, and Department column to sort the persons according to actual needs.
7. Select the Card Reader Mode for reading the card No.
   - **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card No.
   - **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card No.
     Note: The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



     1) Select the Card Enrollment Station type.
        Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.
     2) Set the parameters about the connected card enrollment station.
        If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.
     3) Click **Save** button to save the settings.
        You can click **Restore Default Value** button to restore the defaults.
   - **Manually Input:** Input the card No. and click **Enter** to input the card No.
8. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.
9. Click **OK** to save the settings.

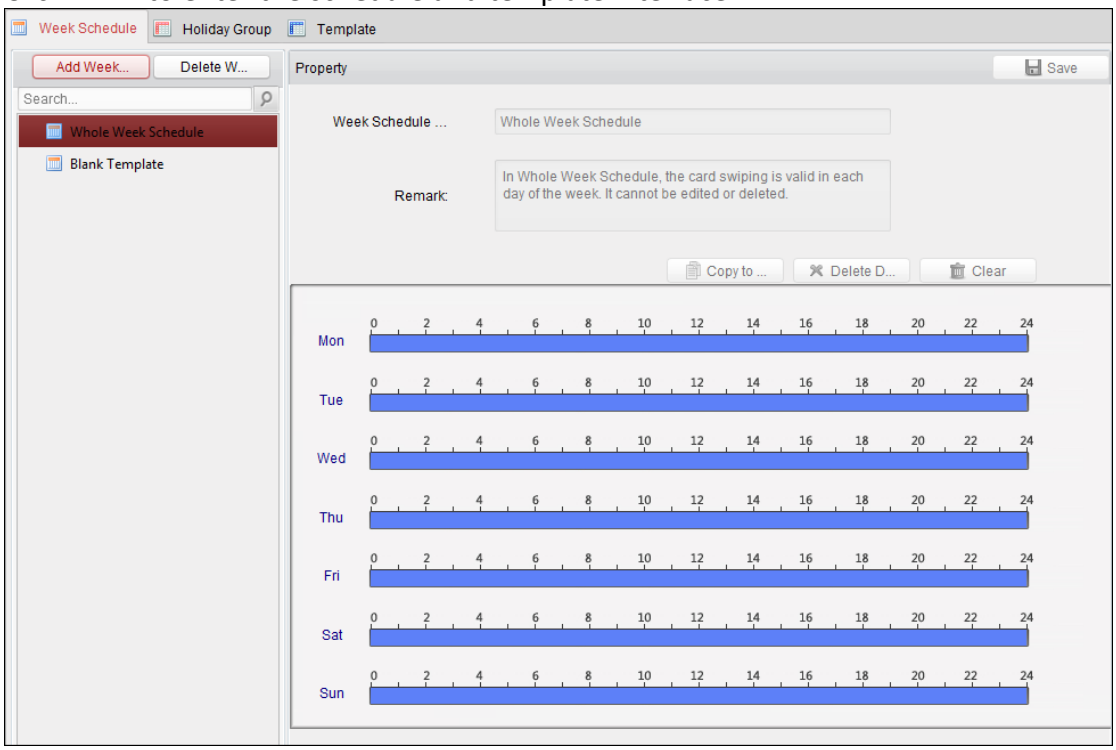
8.7 Schedule and Template

Purpose:

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

template.

Click to enter the schedule and template interface.



You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, please refer to *Chapter 8.8 Permission Configuration.*

8.7.1 Week Schedule

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

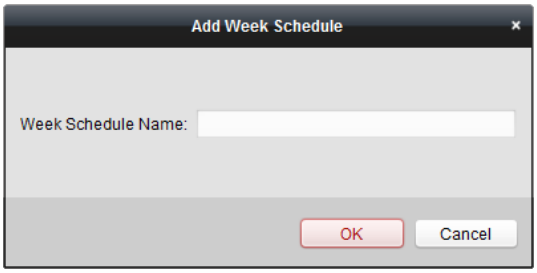
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

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

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

Steps:

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



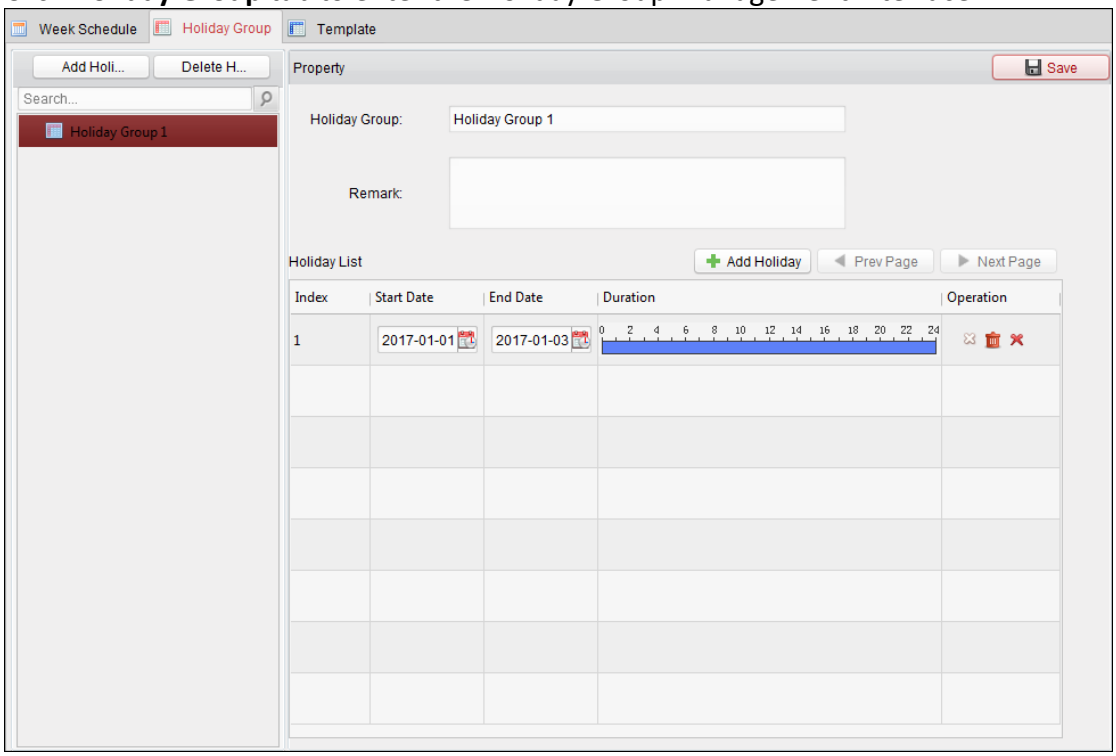
2. Input the name of week schedule and click **OK** button to add the week schedule.
3. Select the added week schedule in the schedule list and you can view its property on the right.

You can edit the week schedule name and input the remark information.

4. On the week schedule, click and drag on a day to draw on the schedule, which means in that period of time, the configured permission is activated.
   Note: Up to 8 time periods can be set for each day in the schedule.
5. When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
   When the cursor turns to , you can lengthen or shorten the selected time bar.
6. Optionally, you can select the schedule time bar,
   and then click **Delete Duration** to delete the selected time bar,
   or click **Clear** to delete all the time bars,
   or click **Copy to Week** to copy the time bar settings to the whole week.
7. Click **Save** to save the settings.

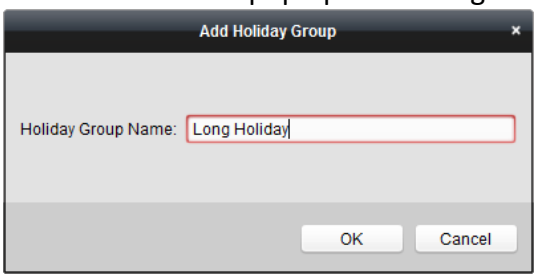
8.7.2 Holiday Group

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

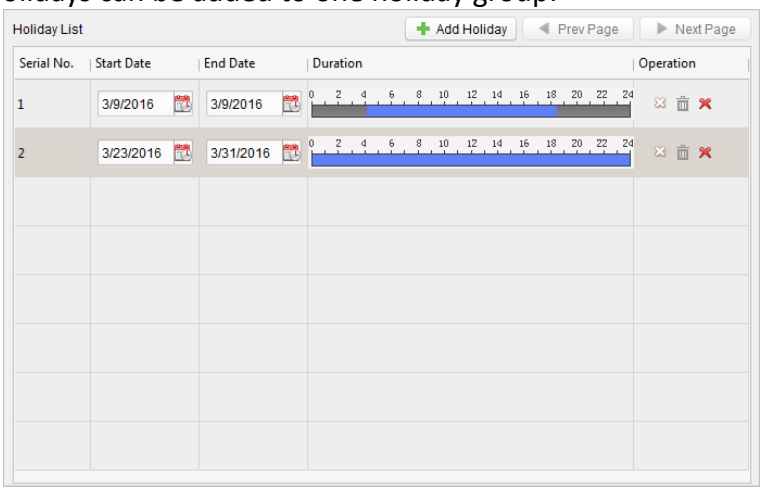


Steps:

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



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



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

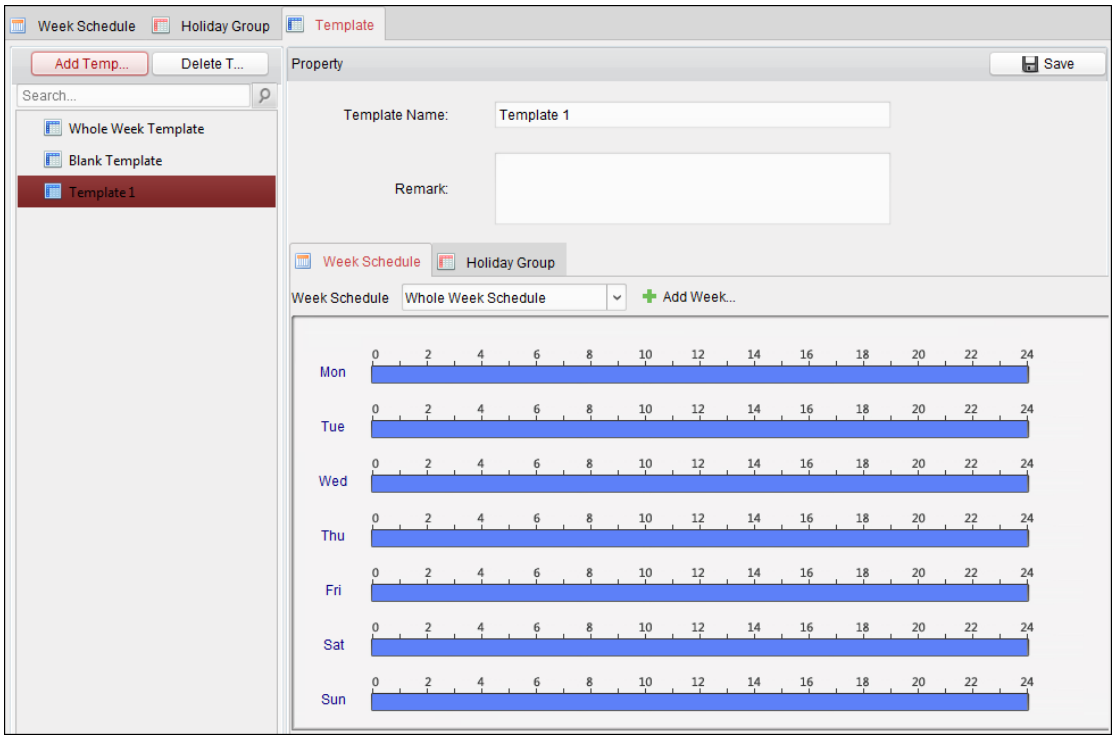
Note: The holidays cannot be overlapped with each other.

8.7.3 Template

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

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

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



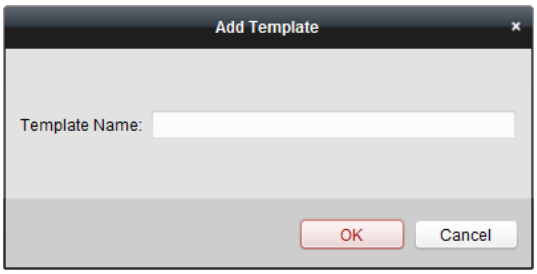
There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

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

You can define custom templates on your demand.

Steps:

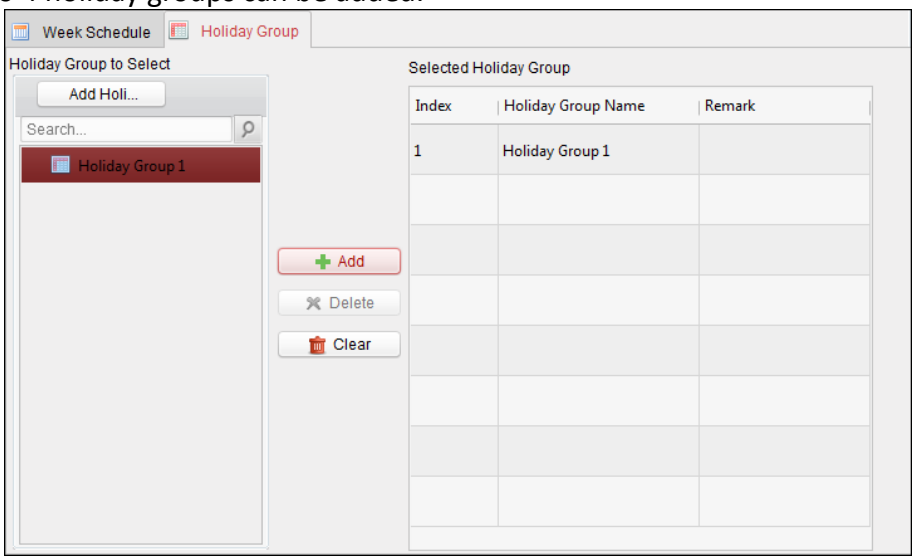
1. Click **Add Template** to pop up the adding template interface.



2. Input the template name in the text filed and click **OK** button to add the template.
3. Select the added template and you can edit its property on the right. You can edit the template name and input the remark information.
4. Select a week schedule to apply to the schedule.
   Click **Week Schedule** tab and select a schedule in the dropdown list.
   You can also click **Add Week Schedule** to add a new week schedule. For details, refer to *Chapter 8.7.1 Week Schedule.*

5. Select holiday groups to apply to the schedule.

   Note: Up to 4 holiday groups can be added.



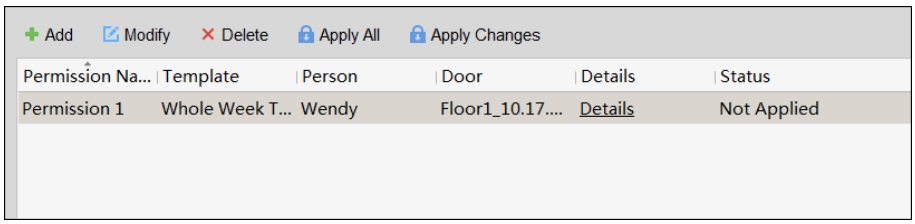
   Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one. For details, refer to *Chapter 8.7.2 Holiday Group.*
   You can click to select an added holiday group in the right-side list and click **Delete** to delete it.
   You can click **Clear** to delete all the added holiday groups.

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

8.8 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.



8.8.1 Adding Permission

Purpose:

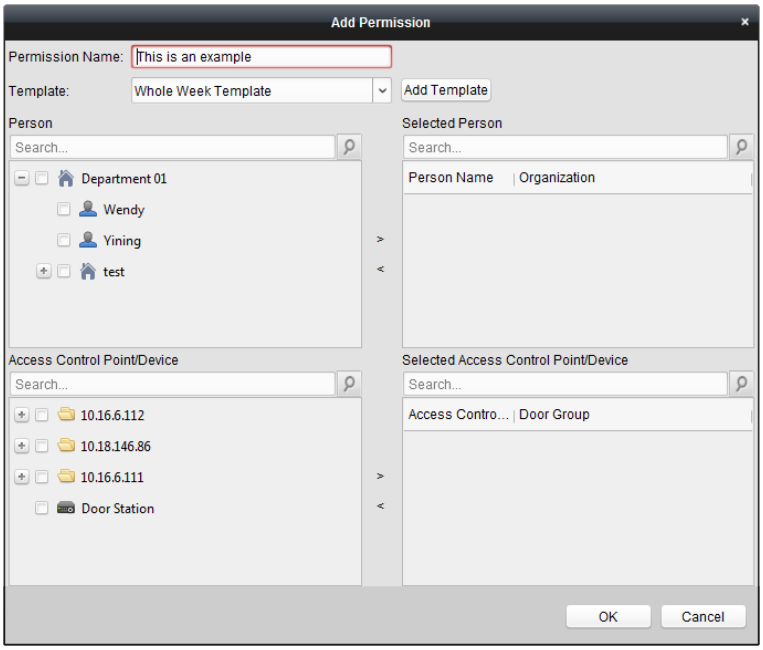
You can assign permission for persons to enter/exist the access control points (doors) in this section.

Notes:

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

Steps:

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



2. In the Permission Name field, input the name for the permission as desired.
3. Click on the dropdown menu to select a template for the permission.
   Note: You should configure the template before permission settings. You can click **Add Template** button to add the template. Refer to *Chapter 8.7 Schedule and Template* for details.
4. In the Person list, all the added persons display.
   Check the checkbox(es) to select person(s) and click **>** to add to the Selected Person list.
   (Optional) You can select the person in Selected Person list and click **<** to cancel the selection.
5. In the Access Control Point/Device list, all the added access control points (doors) and door stations will display.
   Check the checkbox(es) to select door(s) or door station(s) and click **>** to add to the selected list.
   (Optional) You can select the door or door station in the selected list and click **<** to cancel the selection.
6. Click **OK** button to complete the permission adding. The selected person will have the permission to enter/exit the selected door/door station with their linked card(s) or fingerprints.
7. (Optional) after adding the permission, you can click **Details** to modify it. Or you can select the permission and click **Modify** to modify.

You can select the added permission in the list and click **Delete** to delete it.

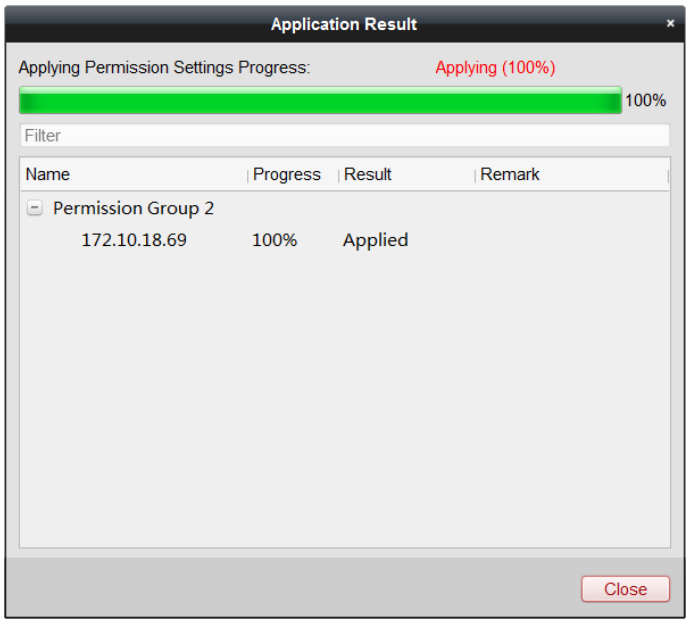
8.8.2 Applying Permission

Purpose:

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

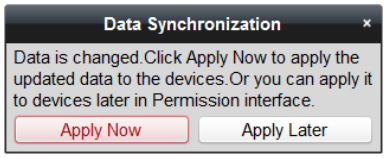
Steps:

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



Notes:

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



  You can click **Apply Now** to apply the changed permissions to the device.
  Or you can click **Apply Later** to apply the changes later in the Permission interface.
- The permission changes include changes of schedule and template, permission settings, person's permission settings, and related person settings (including card No., fingerprint, face picture, linkage between card No. and fingerprint, linkage between card No. and fingerprint, card password, card effective period, etc).

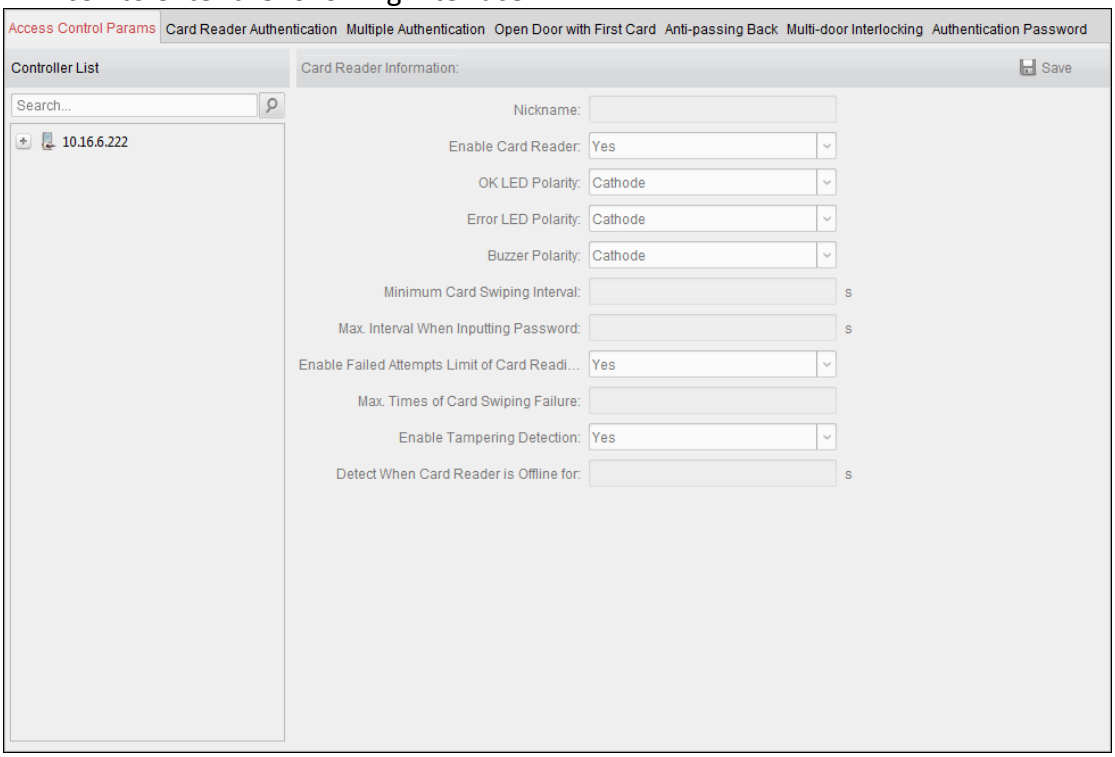
8.9 Advanced Functions

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.



8.9.1 Access Control Parameters

Purpose:

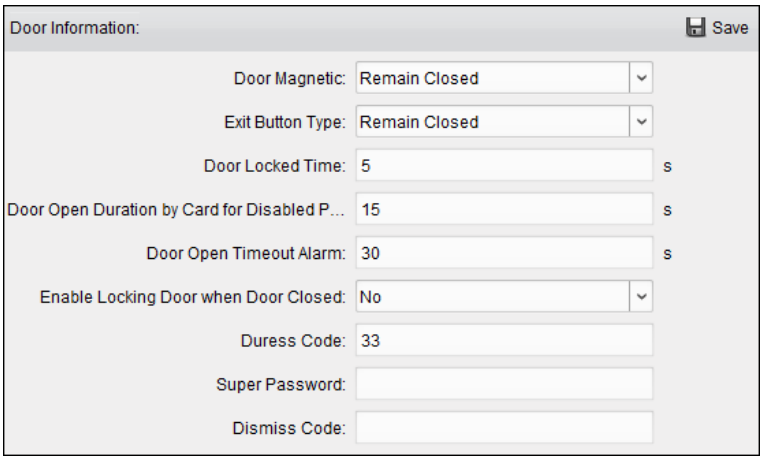
After adding the access control device, you can configure its access control point (door)'s parameters, and its card readers' parameters.

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

Door Parameters

Steps:

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



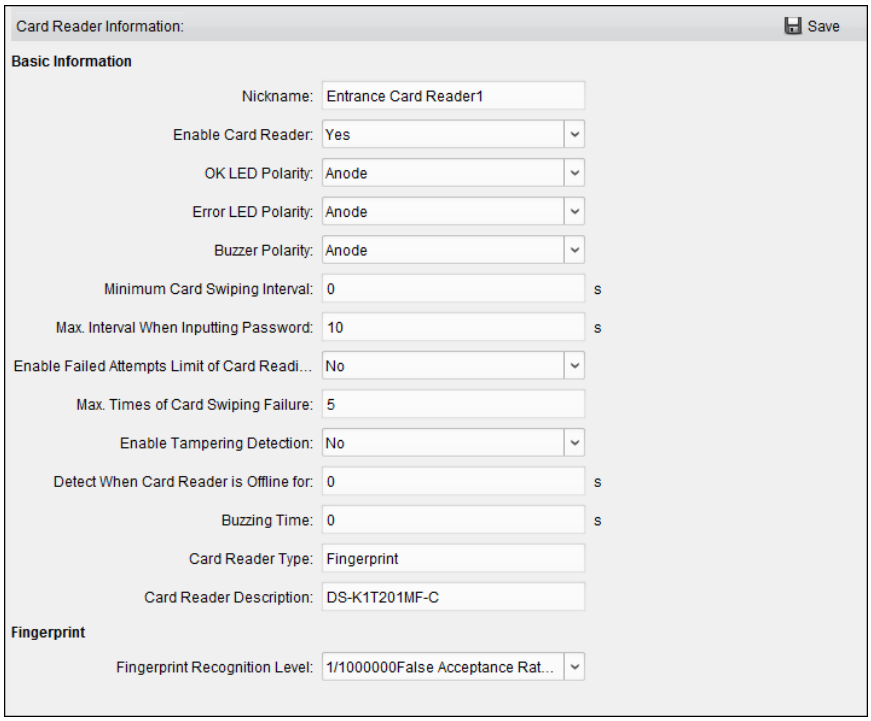
2. You can editing the following parameters:
   - **Door Magnetic**: The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
   - **Exit Button Type**: The Exit Button Type is in the status of **Remain Open** (excluding special conditions).
   - **Door Locked Time**: After swiping the normal card and relay action, the timer for locking the door starts working.
   - **Door Open Duration by Card for 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 has not been close
   - **Enable Locking Door when Door Closed**: The door can be locked once it is closed even if the Door Locked Time is not reached.
   - **Duress Code**: The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.
   - **Super Password:** The specific person can open the door by inputting the super password.
   - **Dismiss Code:** Input the dismiss code to stop the buzzer of the card reader.

     Notes:
     - The duress code, Super password, and dismiss code should be different.
     - The duress code, super password, and the dismiss code should be different from the authentication password.
     - The duress code, super password, and the dismiss code should contain 4 to 8 numerics.
3. Click **Save** button to save parameters.

Card Reader Parameters

Steps:

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



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

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

8.9.2 Card Reader Authentication

Purpose:

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

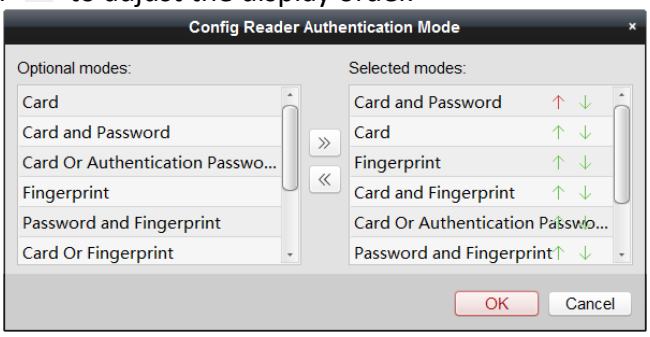
Steps:

1. Click **Card Reader Authentication** tab and select a card reader on the left.
2. Click **Configuration** button to select the card reader authentication modes for setting the schedule.

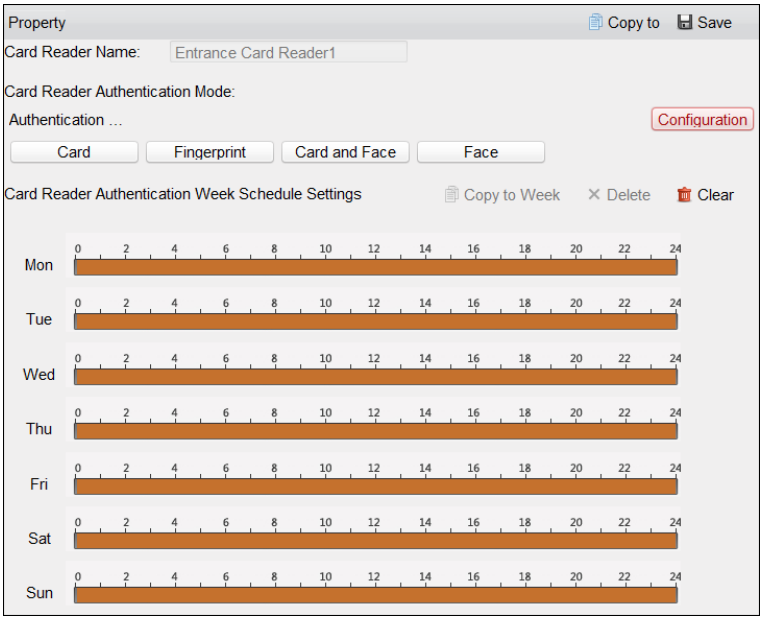
   Notes:

   - The available authentication modes depend on the device type.
   - Password refers to the card password set when issuing the card to the person in *Chapter 8.6 Person Management.*

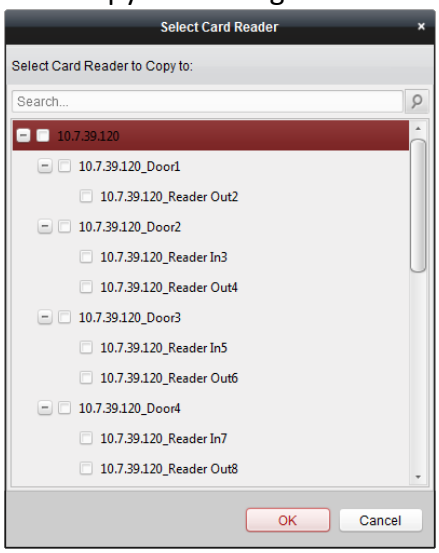
   1) Select the modes and click » to add to the selected modes list.
      You can click ↑ or ↓ to adjust the display order.



   2) Click **OK** to confirm the selection.
3. After selecting the modes, the selected modes will display as icons.
   Click the icon to select a card reader authentication mode.
4. Click and drag your mouse on a day to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.



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



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

8.9.3 Multiple Authentication

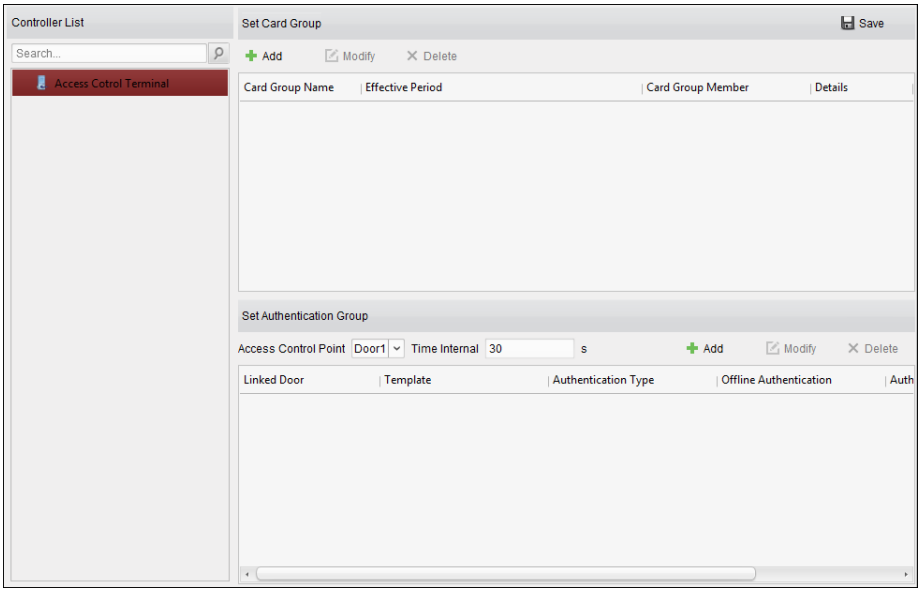
Purpose:

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

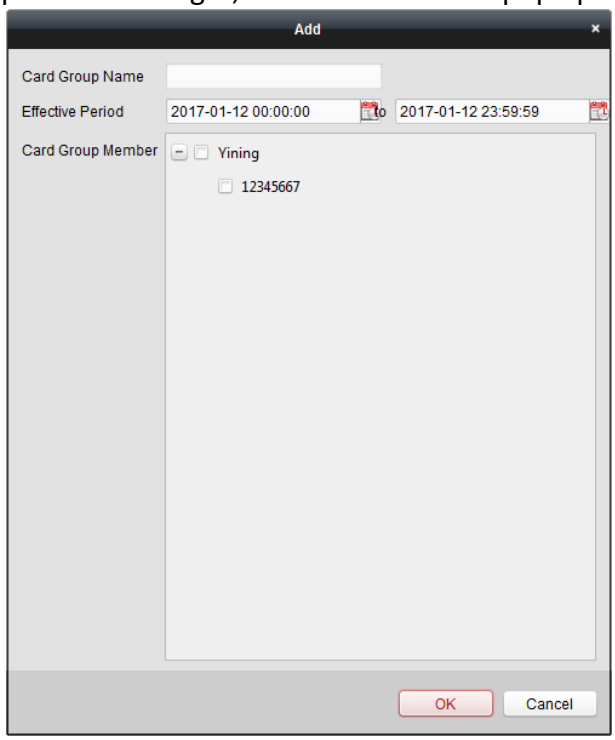
Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 8.8 Permission Configuration.*

Steps:

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

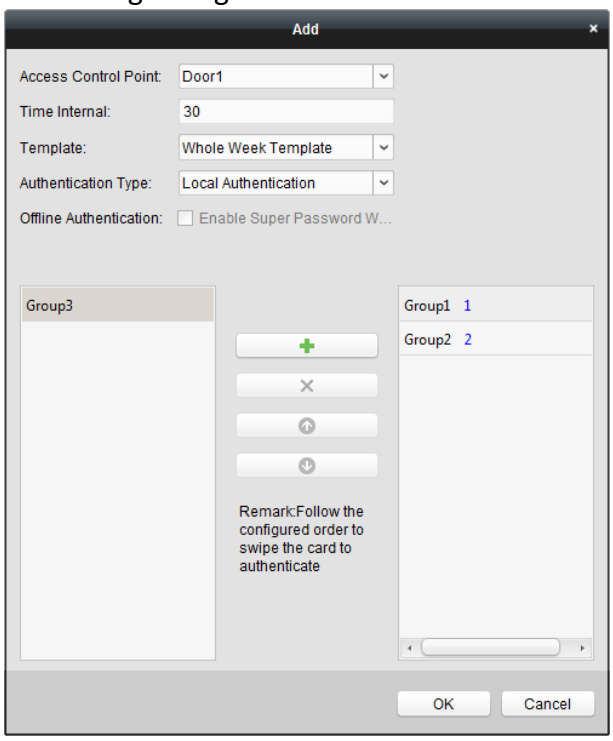


2. Select access control device from the list on the left.
3. In the Set Card Group panel on the right, click **Add** button to pop up the following dialog:



   1) In the Card Group Name field, input the name for the group as desired.
   2) Click to set the effective time and expiry time of the card group.
   3) Check the checkbox(es) to select the card(s) to add the card group.
   4) Click **OK** to save the card group.
4. In the Set Authentication Group panel, select the access control point (door) of the device for multiple authentications.
5. Input the time interval for card swiping.

6. Click **Add** to pop up the following dialog.



1) Select the template of the authentication group from the dropdown list. For details about setting the template, refer to *Chapter 8.7 Schedule and Template*.
2) Select the authentication type of the authentication group from the dropdown list.
   - **Local Authentication:** Authentication by the access control device.
   - **Local Authentication and Remotely Open Door:** Authentication by the access control device and by the client.
     For Local Authentication and Remotely Open Door type, you can check the checkbox to enable the super password authentication when the access control device is disconnected with the client.
   - **Local Authentication and Super Password:** Authentication by the access control device and by the super password.
3) In the list on the left, the added card group will display. You can click the card group and click ✚ to add the group to the authentication group.
   You can click the added card group and click ✕ to remove it from the authentication group.
   You can also click ⬆ or ⬇ to set the card swiping order.
4) Input the **Card Swiping Times** for the selected card group.
   Notes:
   - The Card Swiping Times should be larger than 0 and smaller than the added card quantity in the card group.
   - The upper limit of Card Swiping Times is 16.
5) Click **OK** to save the settings.

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

Notes:

- For each access control point (door), up to 20 authentication groups can be added.
- For the authentication group which certificate type is **Local Authentication**, up to 8 card groups can be added to the authentication group.
- For the authentication group which certificate type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 card groups can be added to the authentication group.

8.9.4 Open Door with First Card

Purpose:

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

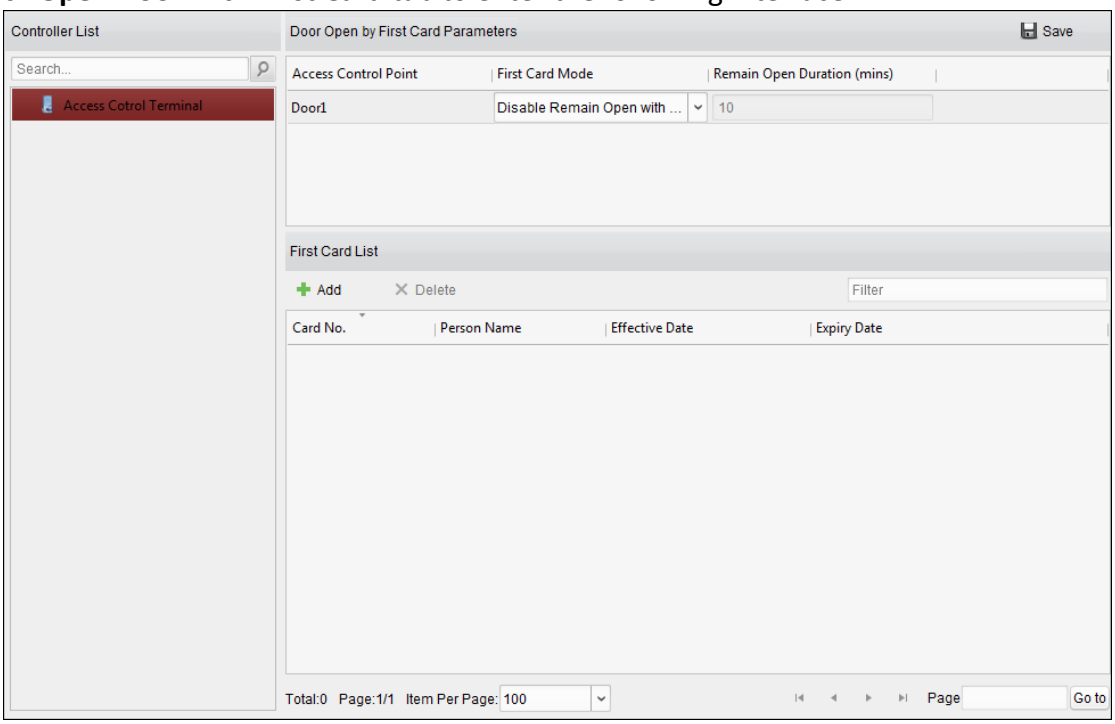
- **Remain Open with First Card:** The door remains open for the configured time duration after the first card swiping until the remain open duration ends.
- **Disable Remain Open with First Card:** Disable the function.

  Notes:

  - The first card authorization is effective only on the current day. The authorization will be expired after 24:00 on the current day.
  - You can swipe the first card again to disable the first card mode.

Steps:

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

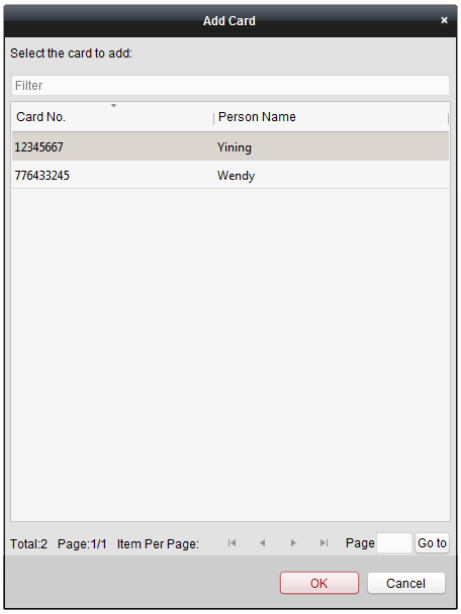


2. Select an access control device from the list on the left.
3. Select the first card mode in the drop-down list for the access control point.
4. (Optional) If you select Remain Open with First Card, you should set remain open duration.

Notes:

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

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



   1) Select the cards to add as first card for the door
      Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 8.8 Permission Configuration.*
   2) Click **OK** button to save adding the card.
6. You can click **Delete** button to remove the card from the first card list.
7. Click **Save** to save and take effect of the new settings.

8.9.5 Anti-Passing Back

Purpose:

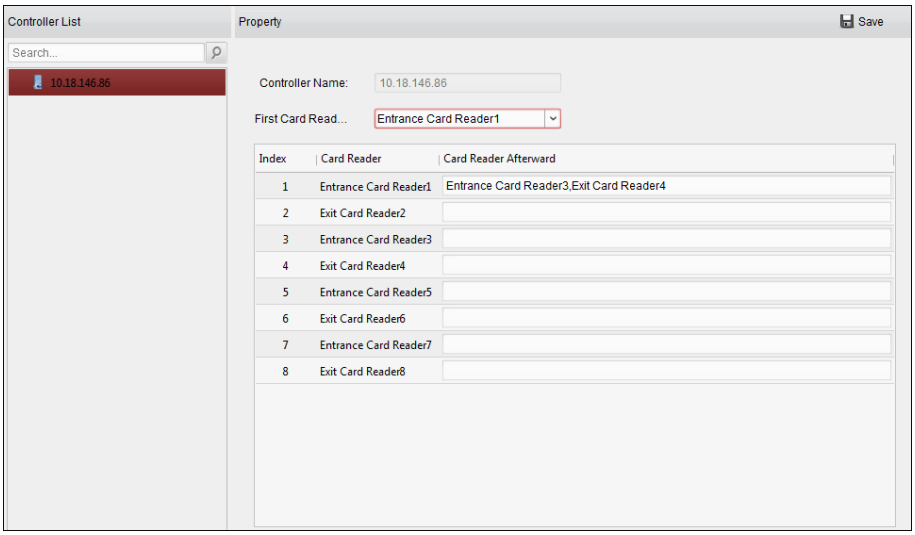
You can set to only pass the access control point according to the specified path and only one person could pass the access control point after swiping the card.

Notes:

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

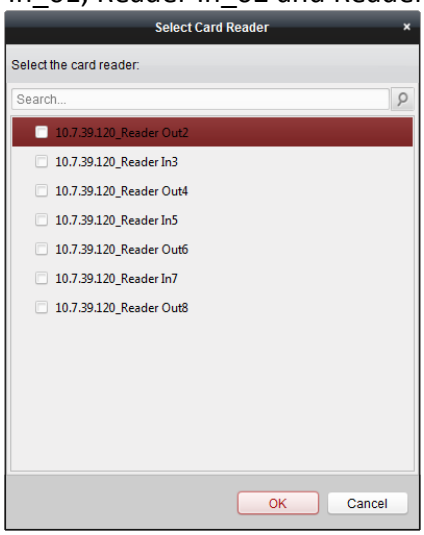
Steps:

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



2. Select an access control device from the device list on the left.
3. In the First Card Reader field, select the card reader as the beginning of the path.
4. In the list, click the text filed of **Card Reader Afterward** and select the linked card readers.

   Example: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.



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

8.10 Searching Access Control Event

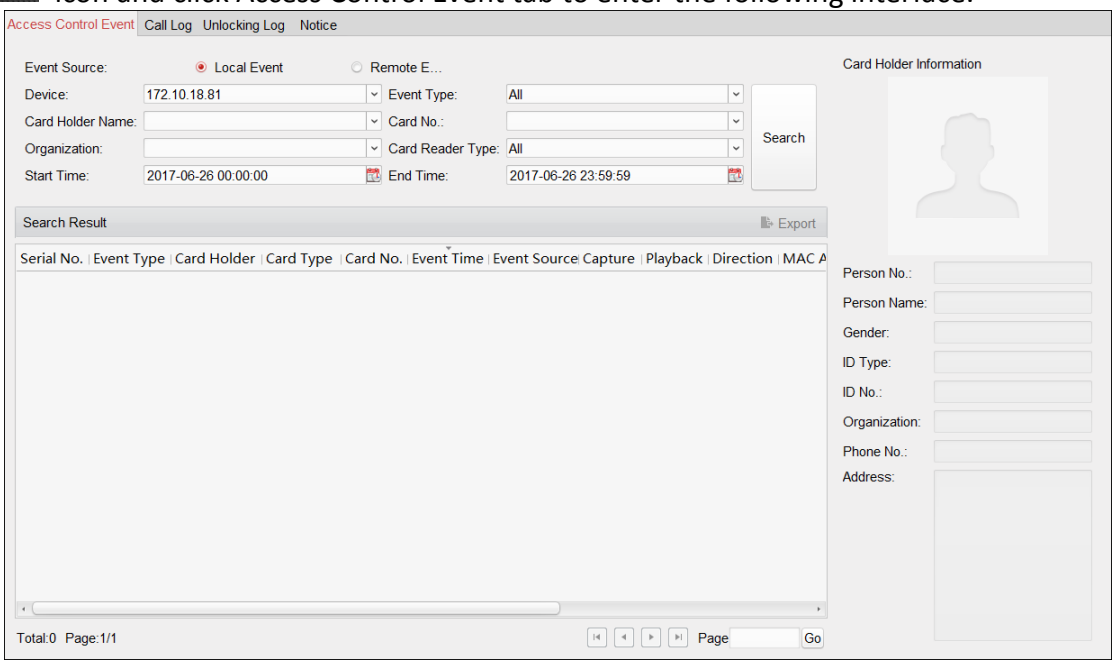
Purpose:

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

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

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

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



8.10.1 Searching Local Access Control Event

Steps:

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

   Note: For setting the triggered camera, refer to *Chapter 8.11.1 Access Control Event Linkage*.
7. You can click **Export** to export the search result to the local PC in *.csv file.

8.10.2 Searching Remote Access Control Event

Steps:

1. Select the Event Source as **Remote Event**.

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

8.11 Access Control Event Configuration

Purpose:

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

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

8.11.1 Access Control Event Linkage

Purpose:

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

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

Steps:

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

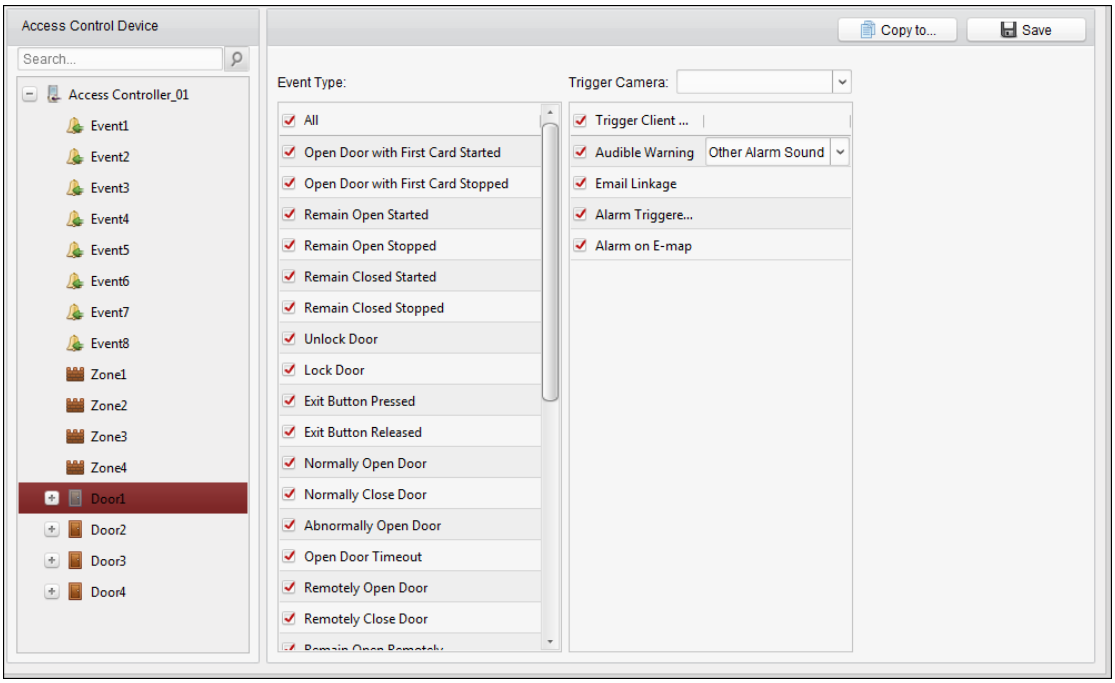
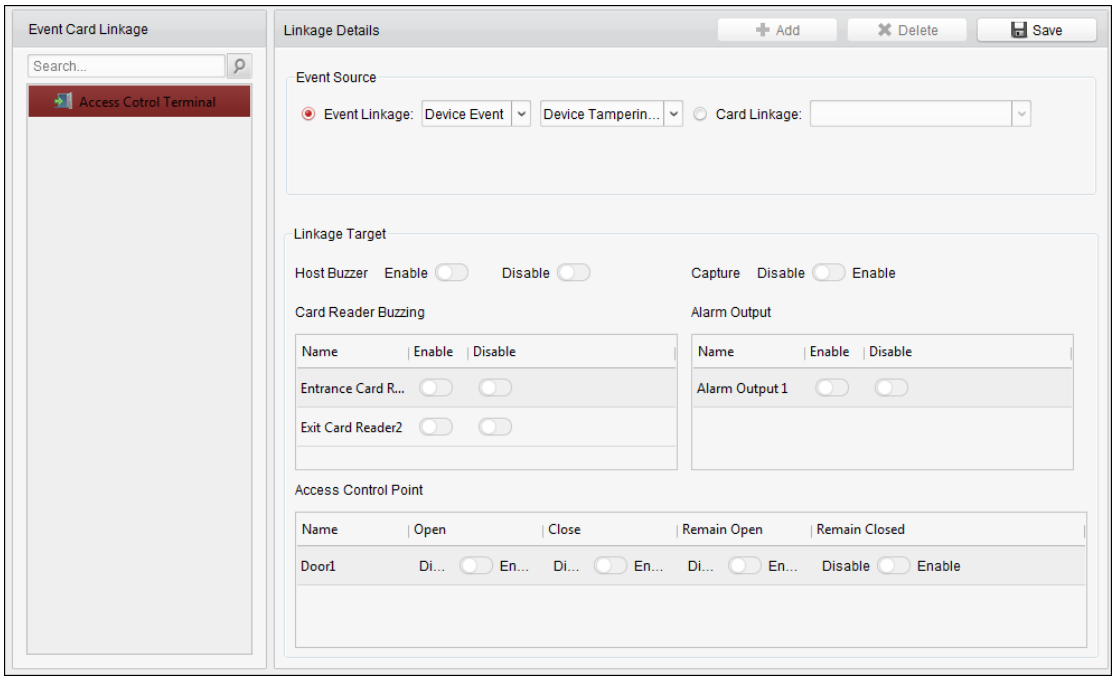


Table 1. 1 Linkage Actions for Access Control Event

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

8.11.2 Event Card Linkage

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



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

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

Event Linkage

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

Steps:

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

     Notes:

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

- The target door and the source door cannot be the same one.

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

Card Linkage

Steps:

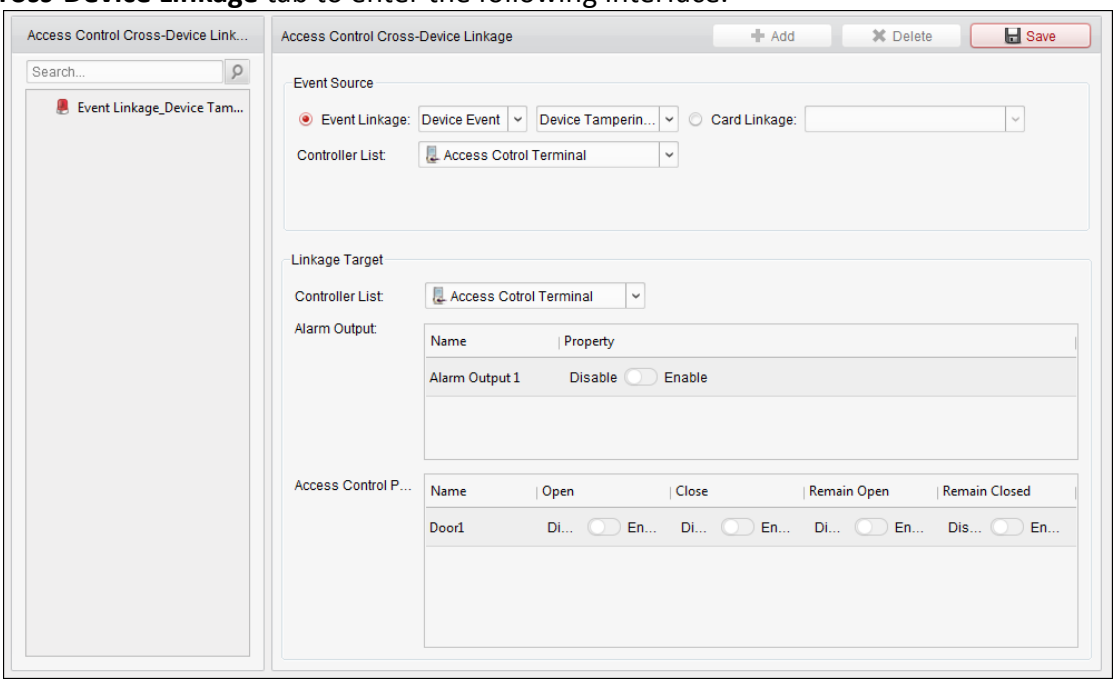
1. Click to select the linkage type as **Card Linkage**.
2. Input the card No. or select the card from the dropdown list.
3. Select the card reader from the table for triggering.
4. Set the linkage target, and switch the property from to to enable this function.
   - **Host Buzzer:** The audible warning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

8.11.3 Cross-Device Linkage

Purpose:

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

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



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

Event Linkage

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

Steps:

1. Click to select the linkage type as **Event Linkage**, select the access control device as event source, and select the event type from the dropdown list.
   - For Device Event, select the detailed event type from the dropdown list.
   - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
   - For Door Event, select the detailed event type and select the door from the table.
   - For Card Reader Event, select the detailed event type and select the card reader from the table.
2. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from to to enable this function.
   - **Alarm Output**: The alarm output will be triggered for notification.
   - **Access Control Point**: The door status of open, close, remain open, and remain close will be triggered.

     Note: The door status of open, close, remain open, and remain close cannot be triggered at the same time.
3. Click **Save** button to save parameters.

Card Linkage

Steps:

1. Click to select the linkage type as **Card Linkage**.
2. Select the card from the dropdown list and select the access control device as event source.
3. Select the card reader from the table for triggering.
4. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from to to enable this function.

   Alarm Output: The alarm output will be triggered for notification.
5. Click **Save** button to save parameters.

8.12 Door Status Management

Purpose:

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

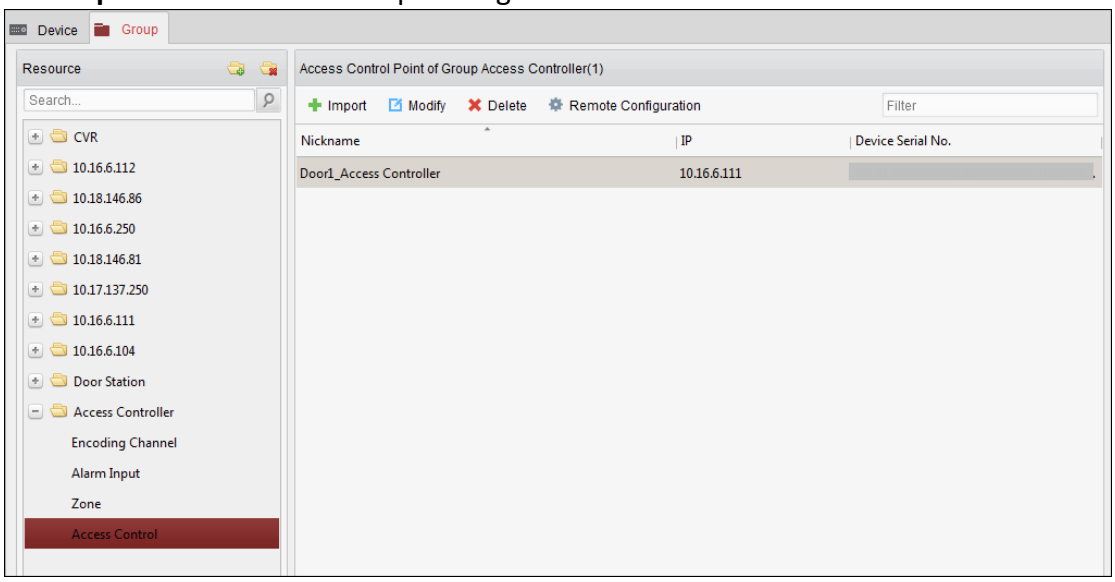
8.12.1 Access Control Group Management

Purpose:

Before controlling the door status and setting the status duration, you are required to organize it

into group for convenient management.
Perform the following steps to create the group for the access control device:
Steps:

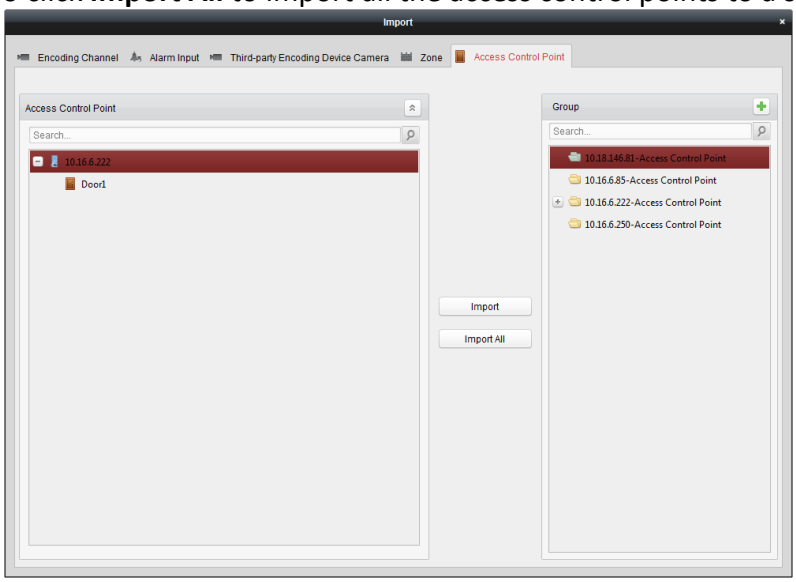
1. Click on the control panel to open the Device Management page.
2. Click **Group** tab to enter the Group Management interface.



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

4. Perform the following steps to import the access control points to the group:
   1) Click **Import** on Group Management interface, and then click the **Access Control** tab to open the Import Access Control page.
   Notes:
   - You can also select **Alarm Input** tab and import the alarm inputs to group.
   - For the Video Access Control Terminal, you can add the cameras as encoding channel to the group.
   2) Select the names of the access control points in the list.
   3) Select a group from the group list.
   4) Click **Import** to import the selected access control points to the group.

You can also click **Import All** to import all the access control points to a selected group.



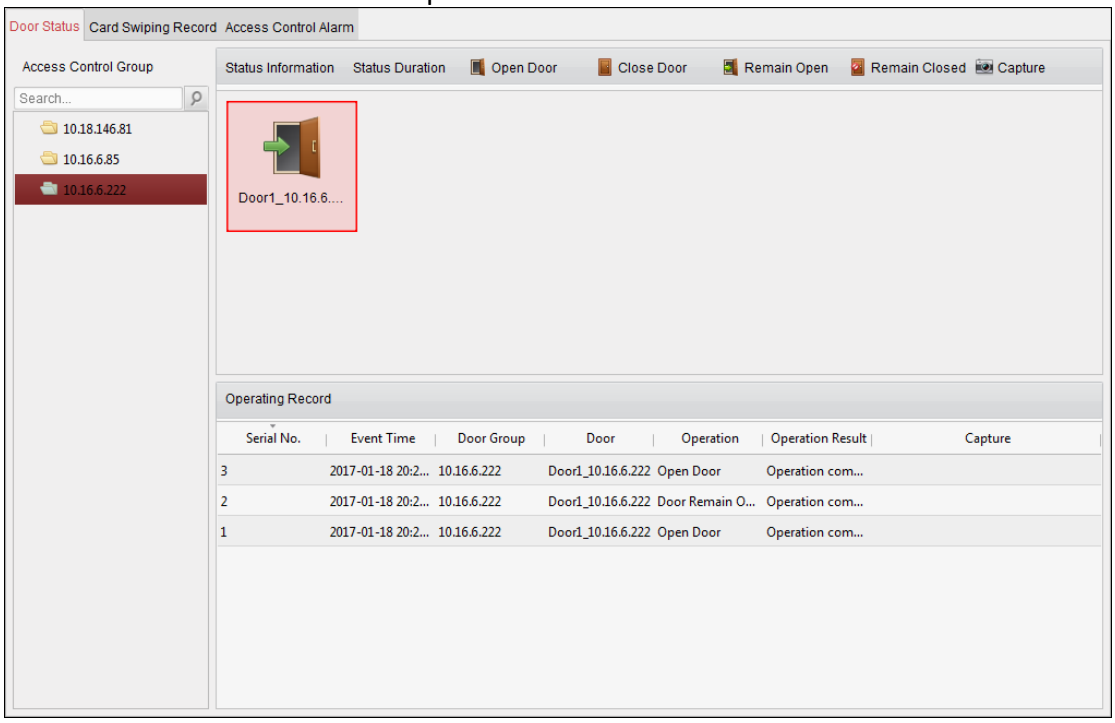
5. After importing the access control points to the group, you can click , or double-click the group/access control point name to modify it.

8.12.2 Anti-control the Access Control Point (Door)

Purpose:

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

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



Steps:

1. Select an access control group on the left. For managing the access control group, refer to *Chapter 8.12.1 Access Control Group Management.*
2. The access control points of the selected access control group will be displayed on the right.

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

   Open Door: Click to open the door once.

   Close Door: Click to close the door once.

   Remain Open: Click to keep the door open.

   Remain Closed: Click to keep the door closed.

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

Notes:

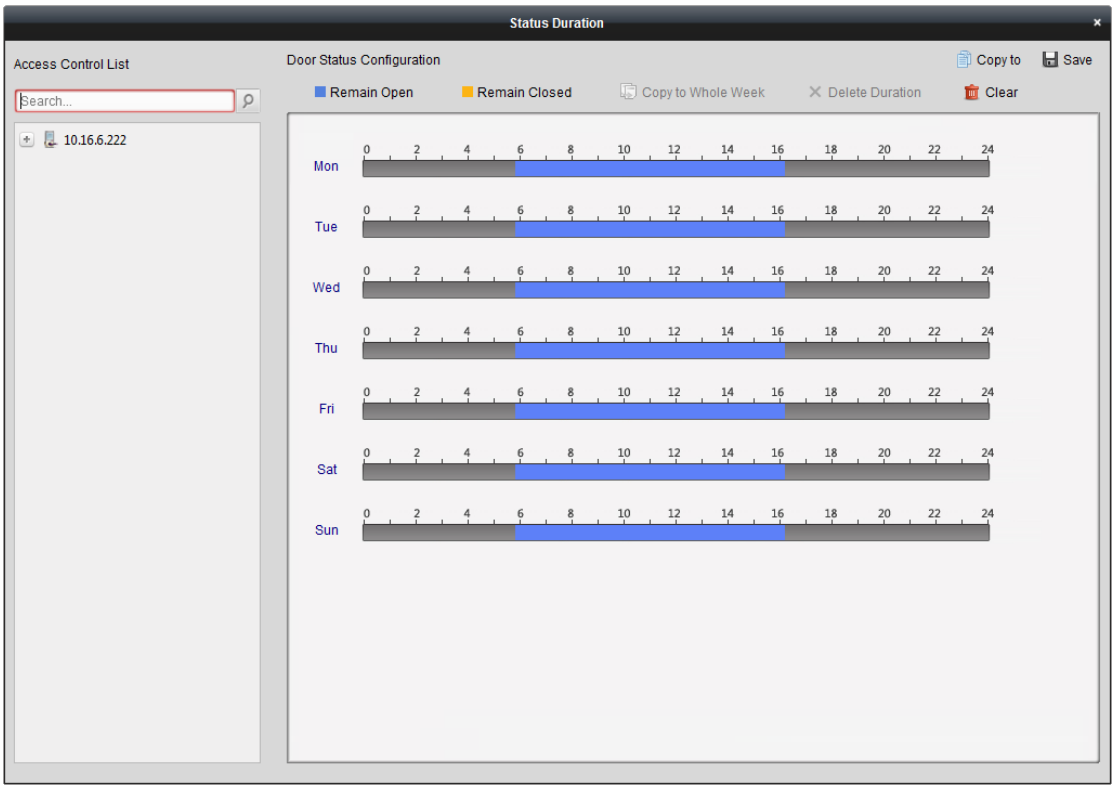
- If you select the status as **Remain Open/Remain Closed**, the door will keep open/closed until a new anti-control command being made.
- The **Capture** button is available when the device supports capture function. And it cannot be realized until the storage server is configured.
- If the door is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

8.12.3 Status Duration Configuration

Purpose:

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

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



Steps:

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

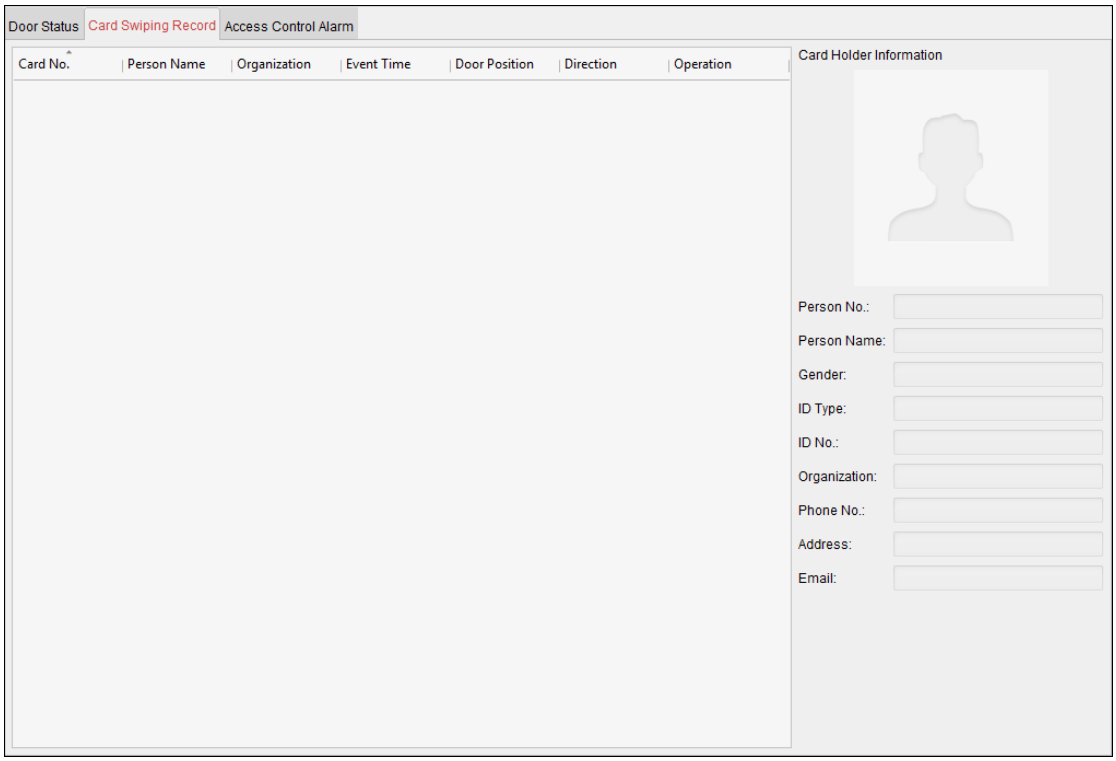
   3) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
      When the cursor turns to , you can lengthen or shorten the selected time bar.
3. Optionally, you can select the schedule time bar and click **Copy to Whole Week** to copy the

time bar settings to the other days in the week.

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

8.12.4 Real-time Card Swiping Record

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



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

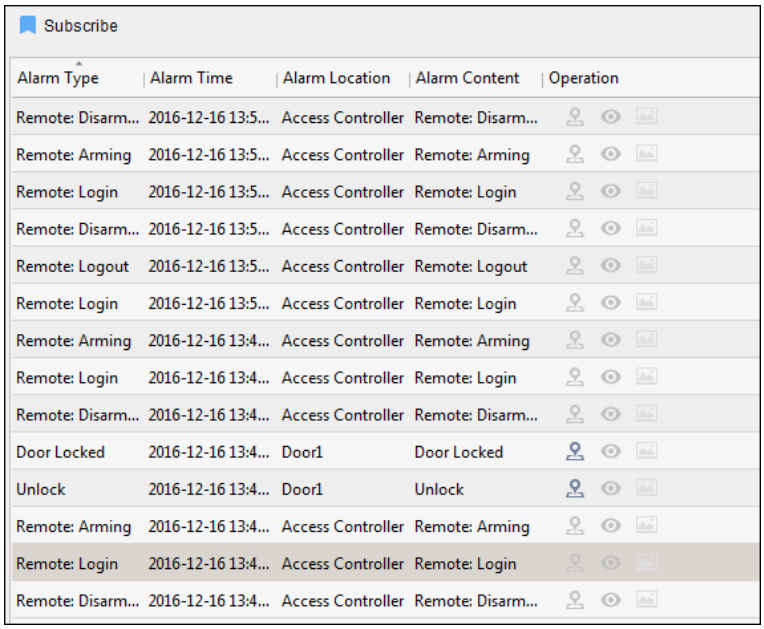
You can also click the event to view the card holder details, including person No., person name, organization, phone, contact address, etc.

8.12.5 Real-time Access Control Alarm

Purpose:

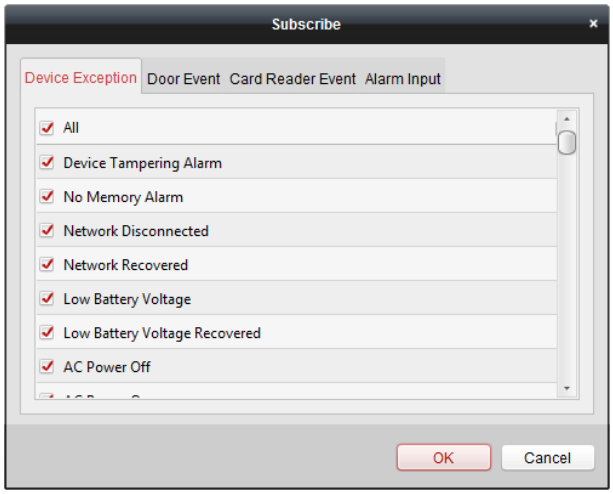
The logs of access control events will be displayed in real time, including device exception, door event, card reader event, and alarm input.

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



Steps:

1. All access control alarms will display in the list in real time.
   You can view the alarm type, alarm time, location, etc.
2. Click to view the alarm on E-map.
3. You can click or to view the live view or the captured picture of the triggered camera when the alarm is trigged.
   Note: For setting the triggered camera, refer to *Chapter 8.11.1 Access Control Event Linkage.*
4. Click **Subscribe** to select the alarm that the client can receive when the alarm is triggered.



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

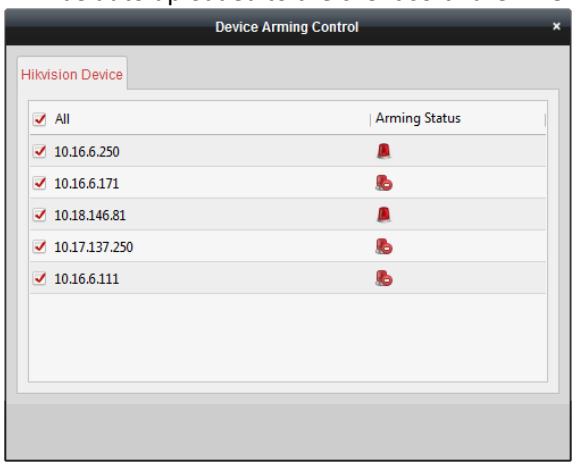
8.13 Arming Control

Purpose:

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

Steps:

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



8.14 Time and Attendance

Purpose:

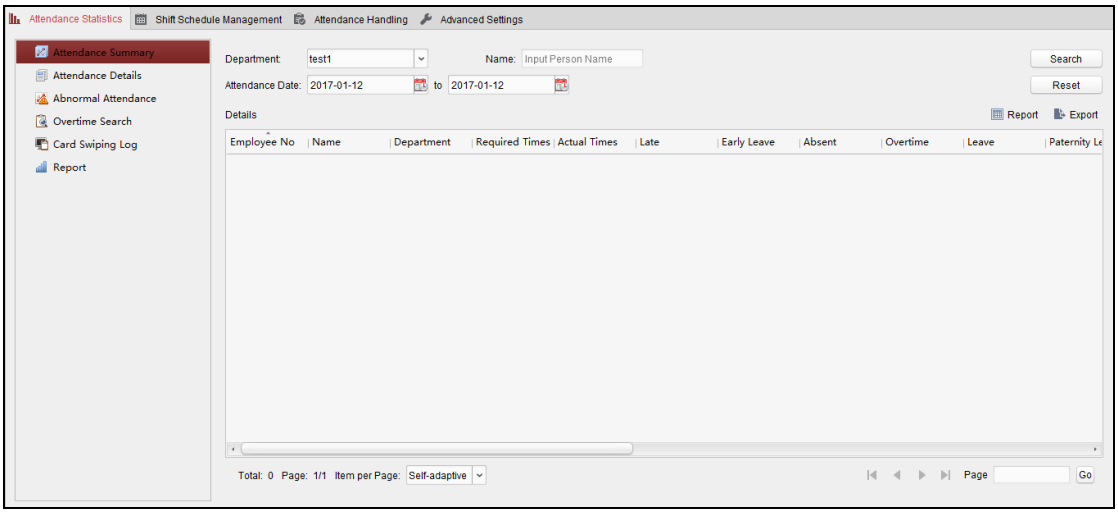
The Time and Attendance module provides multiple functionalities, including shift schedule management, attendance handling, attendance statistics and other advanced functions.

Before you start:

You should add organization and person in Access Control module. For details, refer to *Chapter 8.5.1 Adding Organization* and *Chapter 8.6.1 Adding Person.*

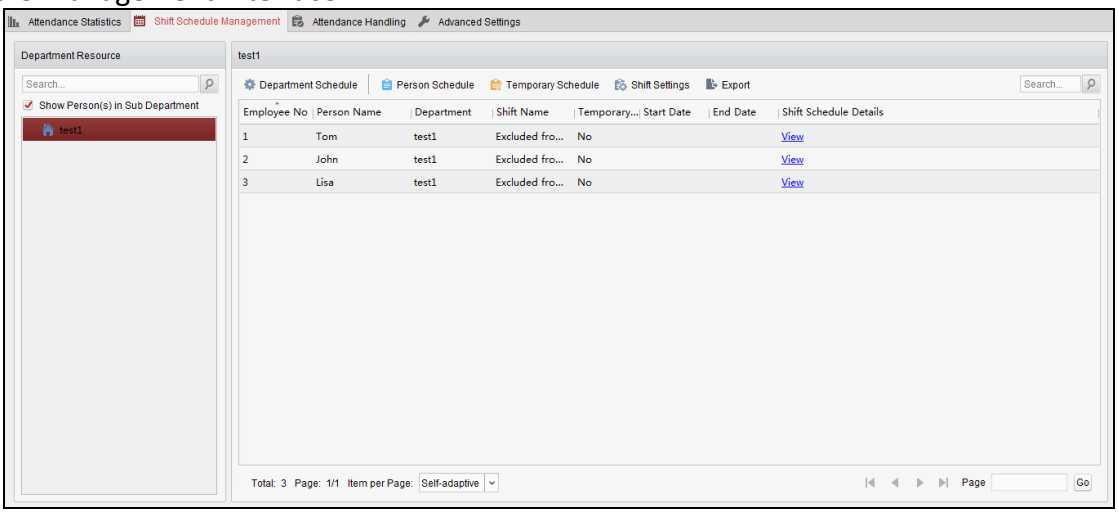
Perform the following steps to access the Time and Attendance module.

Click to enter the Time and Attendance module as follows:



8.14.1 Shift Schedule Management

Open Time and Attendance module and click **Shift Schedule Management** to enter the Shift Schedule Management interface.



Shift Settings

Purpose:

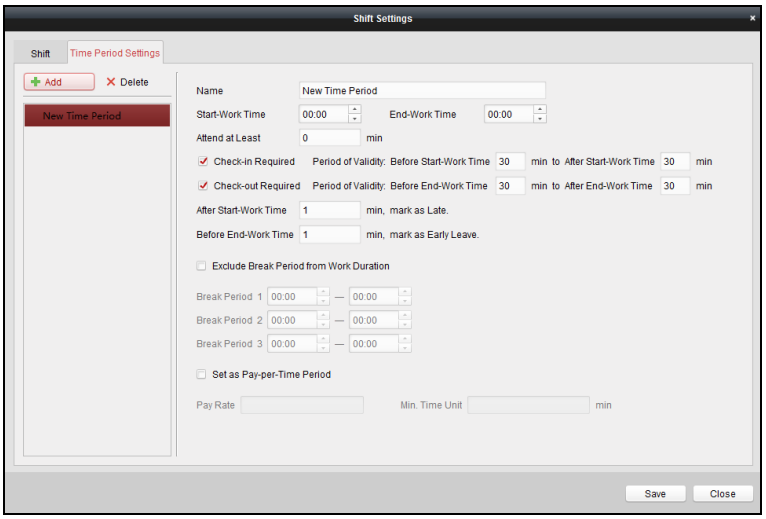
You can add time period and shift for the shift schedule.

Click **Shift Settings** to pop up Shift Settings dialog.

➢ **Adding Time Period**

Steps:

1. Click **Time Period** tab.
2. Click **Add**.



3. Set the related parameters.

   Name: Set the name for time period.

   Start-Work / End-Work Time: Set the start-work time and end-work time.

   Attend at Least: Set the minimum attendance time.

Check-in / Check-out Required: Check the checkboxes and set the valid period for check-in or check-out.

Mark as Late/Mark as Early Leave: Set the time period for late or early leave.

Exclude Break Period from Work Duration: Check the checkbox and set the break period excluded.

Note: Up to 3 break periods can be set.

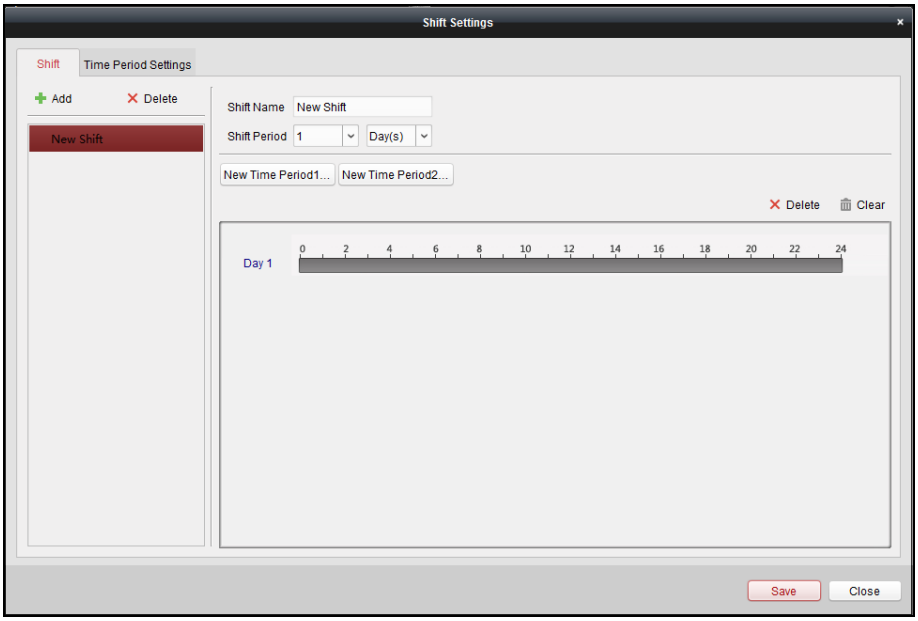
Set as Pay-per-Time Period: Check the checkbox and set the pay rate and minimum time unit.

4. Click **Save** to save the settings.
   The added time period will display on the left panel of the dialog.
   You can also click **Delete** to delete the time period.

➢ **Adding Shift**

Steps:

1. Click **Shift** Tab.
2. Click **Add**.



3. Set the name for shift.
4. Select the shift period from the drop-down list.
5. Configure the shift period with the added time period.
   1) Select the time period.
   2) Click the time bar to apply the time period for the select day.
   You can click the time period on the bar and click ✕ or **Delete** to delete the period.
   You can also click **Clear** to delete all days' time period.
6. Click **Save** to save the settings.
   The added shift will display on the left panel of the dialog.
   You can also click **Delete** on the left panel to delete the shift.

Shift Schedule Settings

Purpose:

After setting the shift, you can set department schedule, person schedule and temporary schedule.

Note: The temporary schedule has higher priority than department schedule and person schedule.

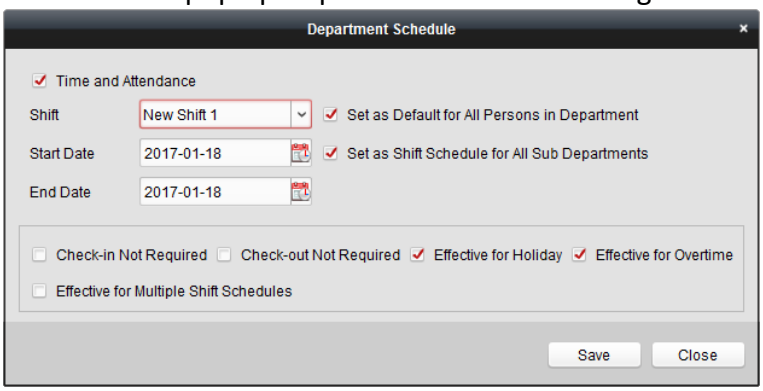
➢ **Department Schedule**

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

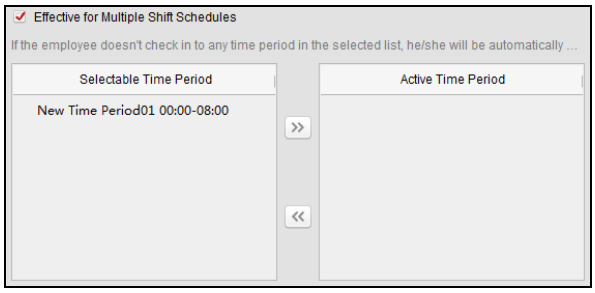
Note: In Time and Attendance module, the department list is the same with the **organization** in Access Control. For setting the organization in Access Control, refer to *Chapter 8.5 Organization Management.*

Steps:

1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Click **Department Schedule** to pop up Department Schedule dialog.



3. Check **Time and Attendance** checkbox.
   All persons in the department expect those excluded from attendance will apply the attendance schedule.
4. Select the shift from the drop-down list.
5. Set the start date and end date.
6. (Optional) Set other parameters for the schedule.
   You can select Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, Effective for Multiple Shift Schedules.
   Notes:
   - Multiple Shift Schedules contains more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.
     Example: If the multiple shift schedules contains three time periods: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three time periods. If the person checks in at 07:50, it will apply the nearest time period 08:00 to 15:00 to the person's attendance.
   - After checking the **Effective for Multiple Shift Schedules** checkbox, you can select the effective time period(s) from the added time periods for the persons in the department.



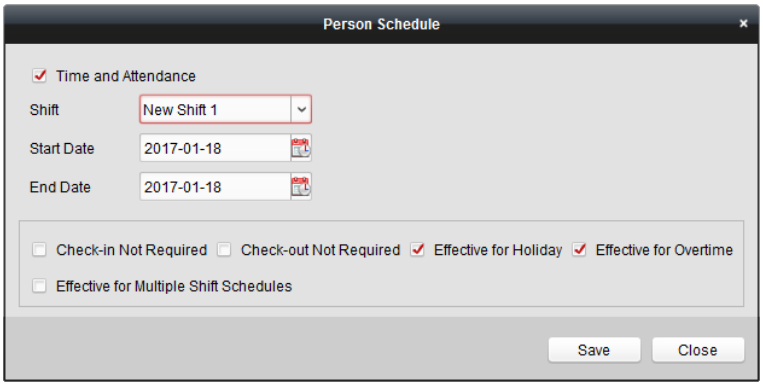
1) In the Selectable Time Period list on the left, click the added time period and click » to add it to the right.
2) (Optional) To remove the selected time period, select it and click «.

7. (Optional) Check **Set as Default for All Persons in Department** checkbox.
   All persons in the department will use this shift schedule by default.
8. (Optional) If the selected department contains sub department(s), the Set as **Shift Schedule for All Sub Departments** checkbox will display. You can check it to apply the department schedule to its sub departments.
9. Click **Save** to save the settings.

➢ **Person Schedule**

Steps:

1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **Person Schedule** to pop up Person Schedule dialog.

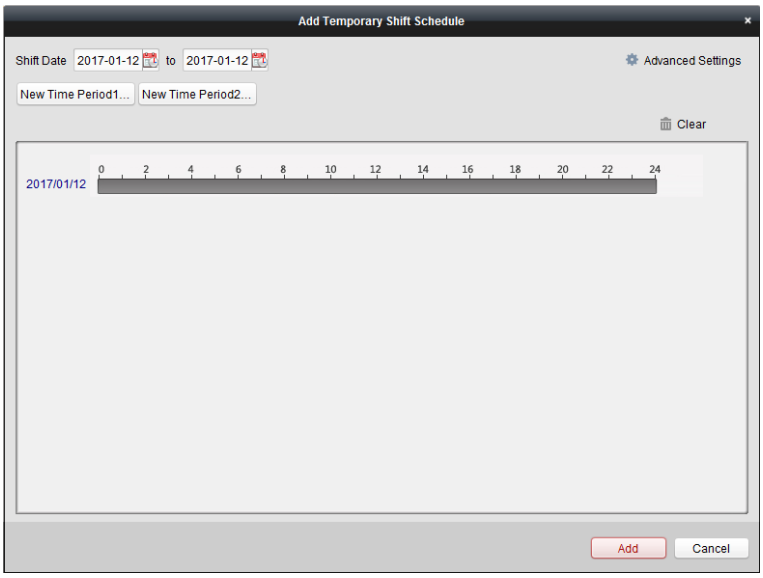


4. Check **Time and Attendance** checkbox.
   The configured person will apply the attendance schedule.
5. Select the shift from the drop-down list.
6. Set the start date and end date.
7. (Optional) Set other parameters for the schedule.
   You can select Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, Effective for Multiple Shift Schedules.
8. Click **Save** to save the settings.

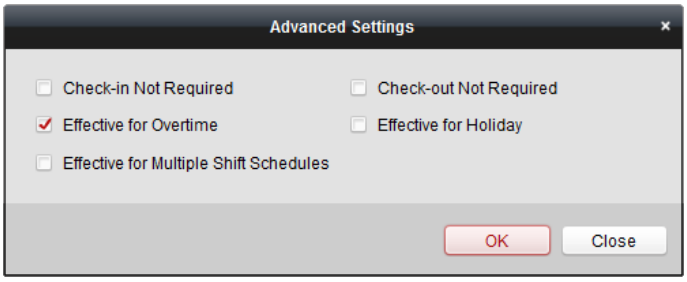
➢ **Temporary Schedule**

Steps:

1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **Temporary Schedule** to pop up Temporary Schedule dialog.



4. Click to set the shift date.
5. Configure the shift date with the added time period.
   1) Select the time period.
   2) Click the time bar to apply the time period for the select date.
   You can click the time period on the bar and click to delete the period.
   You can also click **Clear** to delete all days' time period.
6. You can click **Advanced Settings** to advanced attendance rules for the temporary schedule.

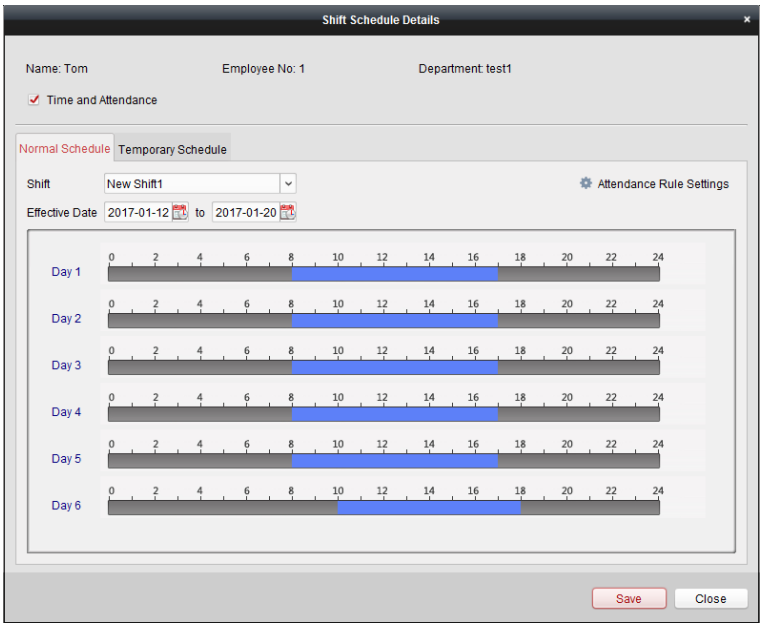


7. Click **Add** to save the settings.

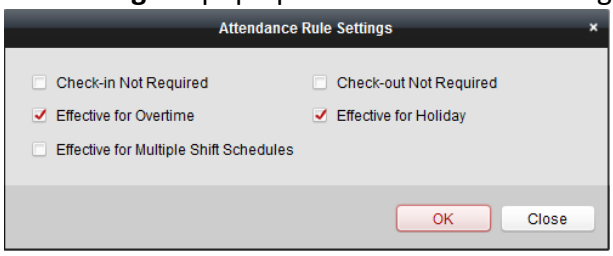
➢ Checking Shift Schedule Details

Steps:

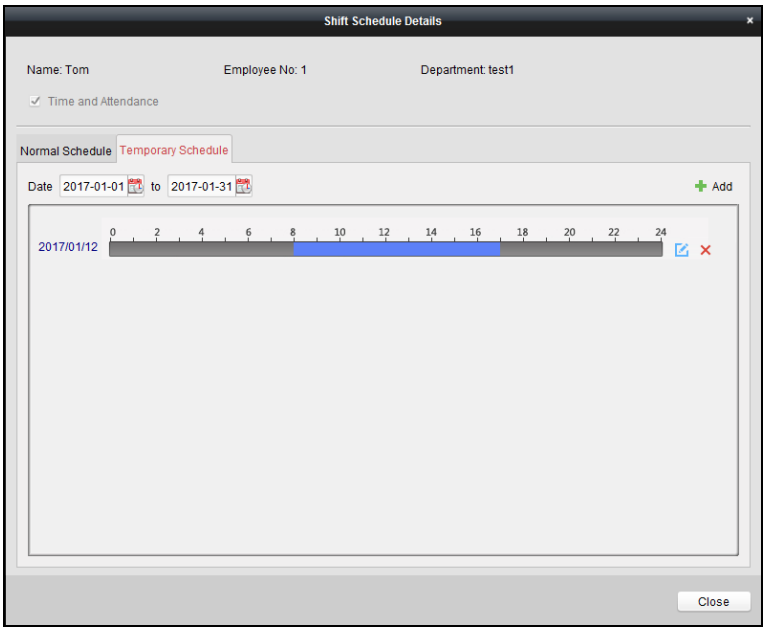
1. On the Shift Schedule Management interface, select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **View** to pop up Shift Schedule Details dialog.
   You can check the shift schedule details.



4. Click **Normal Schedule** tab.
   You can check and edit the normal schedule details.
   1) Select the shift from the drop-down list.
   2) Click **Attendance Rule Settings** to pop up Attendance Rule Settings dialog.



   You can check the attendance rules as desired and click **OK** to save the settings.
   3) Click to set the effective date.
   4) Click **Save** to save the settings.
5. (Optional) Click **Temporary Schedule** tab.



You can check and edit the temporary schedule details.

(Optional) Click **Add** to add temporary schedule for the selected person.

(Optional) Click to edit the time period.

(Optional) Click to delete the temporary schedule.

➢ **Exporting Shift Schedule Details**

On the Shift Schedule Management interface, select the department on the left panel and click **Export** to export all persons' shift schedule details to local PC.

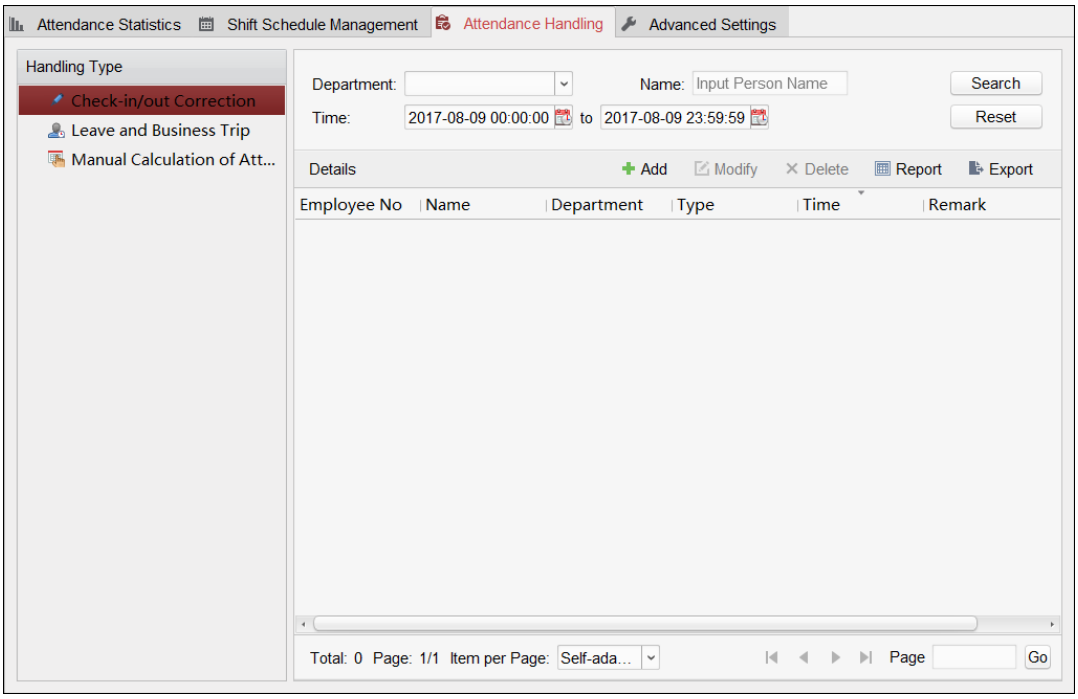
Note: The exported details are saved in *.csv format.

8.14.2 Attendance Handling

Purpose:

You can handle the attendance, including check-in correction, check-out correction, leave and business trip, and manual calculation of attendance.

Open Time and Attendance module and click **Attendance Handling** to enter the Attendance Handling interface.



Check-in/out Correction

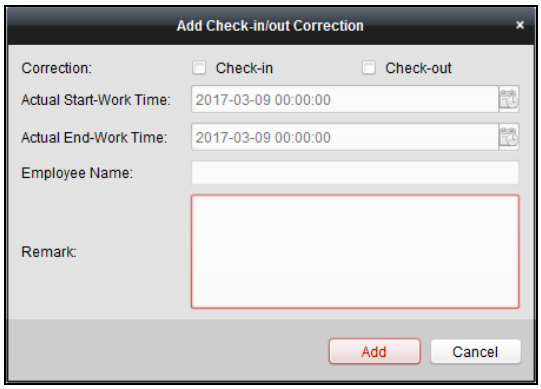
Purpose:

You can add, edit, delete, search the check-in/out correction and generate the related report. You can also export the check-in/out correction details to local PC.

➢ Add Check-in/out Correction

Steps:

1. Click **Check-in/out Correction** tab.
2. Click **Add** to pop up Add Check-in/out Correction dialog.



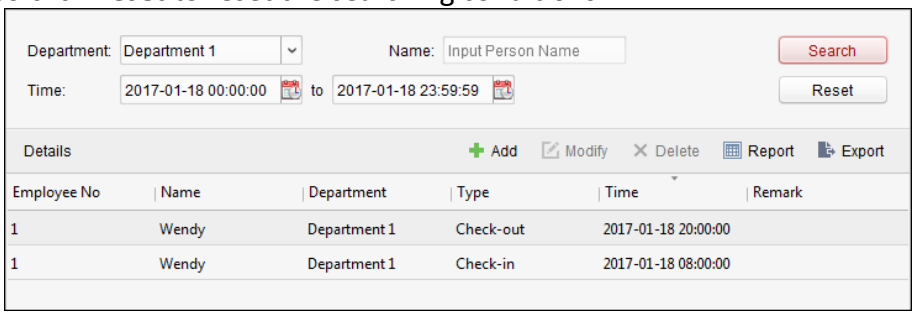
3. Set the check-in/out correction parameters.
   For Check-in Correction: Check **Check-in** checkbox and set the actual start-work time.
   For Check-out Correction: Check **Check-out** checkbox and set the actual end-work time.
4. Click **Employee Name** field and select the person.
   You can also input the keyword and click to search the person you want.
5. (Optional) Input the remark information as desired.
6. Click **Add** to add the check-in/out correction.

The added check-in/out correction will display on the Attendance Handling interface.
(Optional) Select the check-in/out correction and click **Modify** to edit the correction.
(Optional) Select the check-in/out correction and click **Delete** to delete the correction.
(Optional) Click **Report** to generate the check-in/out correction report.
(Optional) Click **Export** to export the check-in/out correction details to local PC.
Note: The exported details are saved in *.csv format.

➢ **Search Check-in/out Correction**

Steps:

1. Click **Check-in/out Correction** tab.
2. Set the searching conditions.
   Department: Select the department from the drop-down list.
   Name: Input the person name.
   Time: Click to set the specified time as time range.
3. Click **Search** to search the check-in/out corrections.
   The check-in/out correction details will display on the list.
   You can also click **Reset** to reset the searching conditions.



Leave and Business Trip

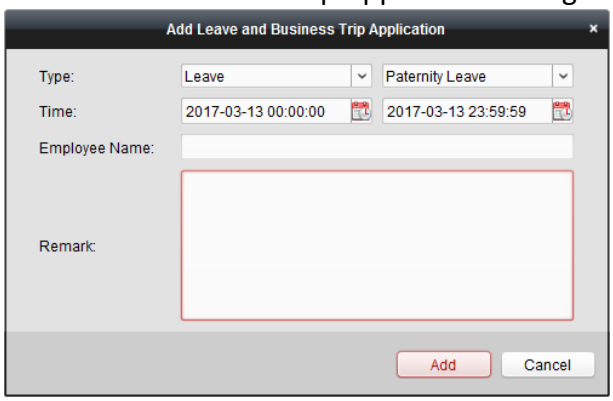
Purpose:

You can add, edit, delete, search the leave and business trip and generate the related report. You can also export the leave and business trip details to local PC.

➢ **Add Leave and Business Trip**

Steps:

1. Click **Leave and Business Trip** tab.
2. Click **Add** to pop up Add Leave and Business Trip Application dialog.



3. Select the leave and business trip type from the Type drop-down list.
   You can configure the leave type in Advanced Settings. For details, refer to *Chapter 0 Leave Type Settings*.
4. Click to set the specified time as time range.
5. Click **Employee Name** field and select the person for this application.
   You can also input the keyword and click to search the person you want.
6. (Optional) Input the remark information as desired.
7. Click **Add** to add the leave and business trip.
   The added leave and business trip will display on the Attendance Handling interface.
   (Optional) Select the leave and business trip and click **Modify** to edit the leave or business trip.
   (Optional) Select the leave and business trip and click **Delete** to delete the leave or business trip.
   (Optional) Click **Report** to generate the leave or business trip report.
   (Optional) Click **Export** to export the leave or business trip details to local PC.
   Note: The exported details are saved in *.csv format.

➢ **Search Leave and Business Trip**

Steps:

1. Click **Leave and Business Trip** tab.
2. Set the searching conditions.
   Department: Select the department from the drop-down list.
   Name: Input the person name.
   Time: Click to set the specified time as time range.
3. Click **Search** to search the leave and business trips.
   The leave and business trip details will display on the list.
   You can also click **Reset** to reset the searching conditions.

Manual Calculation of Attendance

Purpose:

You can calculate the attendance result manually if needed by specifying the start time and end time.

Steps:

1. Click **Manual Calculation of Attendance** tab.
2. Set the start time and end time for calculation.
3. Click **Calculate** to start.

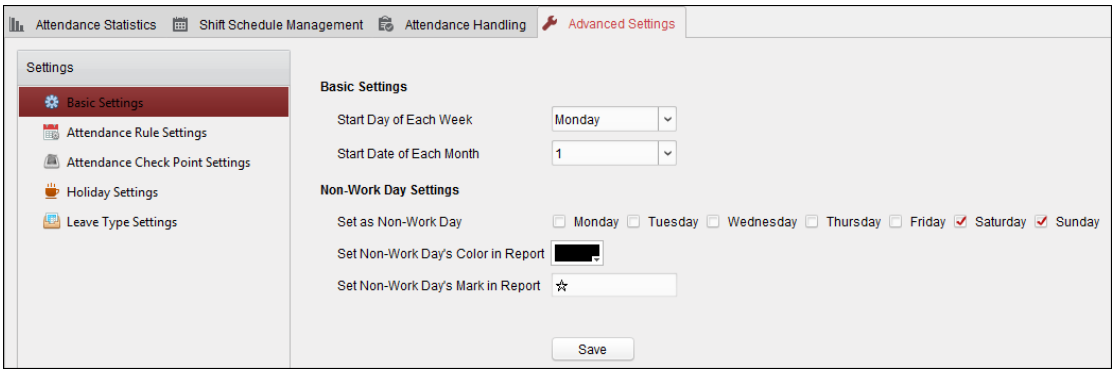
Note: It can only calculate the attendance data within three months.

8.14.3 Advanced Settings

Purpose:

You can configure the basic settings, attendance rule, attendance check point, holiday settings and leave type for attendance.

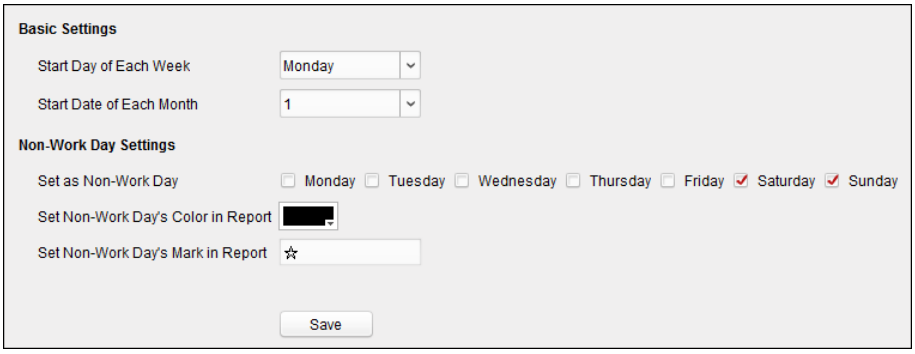
Open Time and Attendance module and click **Advanced Settings** to enter the Advanced Settings interface.



Basic Settings

Steps:

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

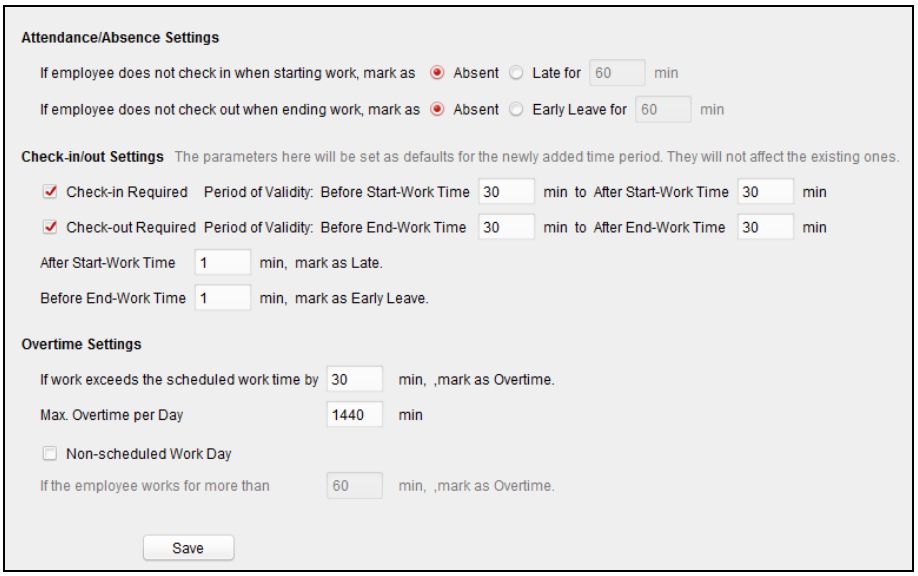


2. Set the basic settings.
   Start Day of Each Week: You can select one day as the start day of each week.
   Start Date of Each Month: You can select one day as the start date of each month.
3. Set the non-work day settings.
   Set as Non-Work Day: Check the checkbox(es) to set the selected day(s) as non-work day.
   Set Non-Work Day's Color in Report: Click the color filed and select the color to mark the non-work day in report.
   Set Non-Work Day's Mark in Report: Input the mark as non-work day in report.
4. Click **Save** to save the settings.

Attendance Rule Settings

Steps:

1. Click **Attendance Rule Settings** tab to enter the Attendance Rule Settings interface.



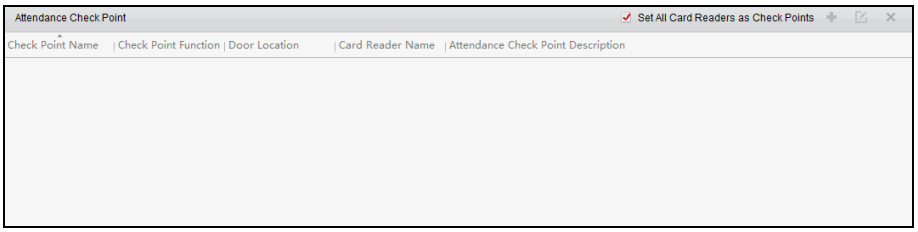
2. Set the attendance or absence settings.
   If employee does not check in when starting work, you can mark as **Absent** or **Late** and set the late time.
   If employee does not check out when ending work, you can mark as **Absent** or **Early Leave** and set the early leave duration.
3. Set the Check-in/out Settings.
   You can check the checkbox of **Check-in Required** or **Check-out Required** and set the valid period.
   You can also set the late rule or early leave rule.
   Note: The parameters here will be set as default for the newly added time period. It will not affect the existed one(s).
4. Set the overtime settings.
   You can set the overtime rule and set the maximum overtime for each day.
   (Optional) You can check **Non-scheduled Work Day** checkbox and set the overtime rule for non-work day.
5. Click **Save** to save the settings.

Attendance Check Point Settings

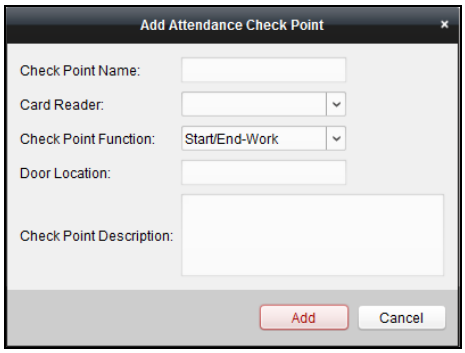
You can set the card reader(s) of the access control point as the attendance check point, so that the card swiping on the card reader(s) will be valid for attendance.

Steps:

1. Click **Attendance Check Point Settings** tab to enter the Attendance Check Point Settings interface.



2. Click ✚ to pop up Add Attendance Check Point dialog.



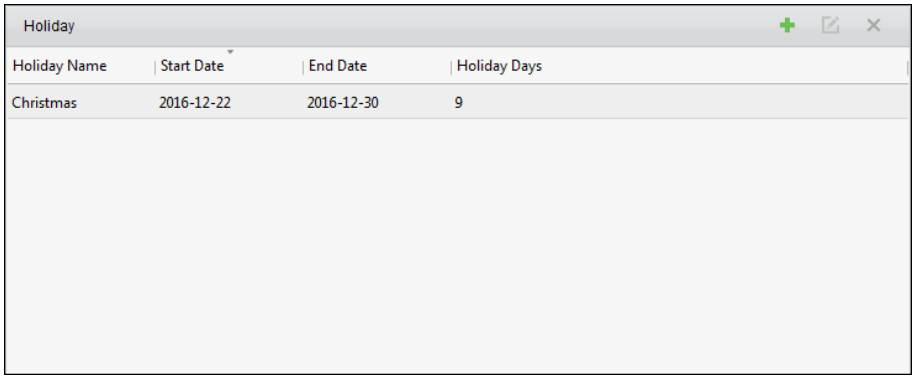
3. Set the related information.
   Check Point Name: Input a name for check point.
   Card Reader: Select the card reader from the drop-down list.
   Check Point Function: Select the function for check point.
   Door Location: Input the door location.
   Check Point Description: Set the description information for check point.
4. Click **Add** to add the attendance check point.
   The added attendance check point will display on the list.
5. (Optional) Check **Set All Card Readers as Check Points** checkbox.
   You can use all the card readers as check points.
   Note: If this checkbox is unchecked, only the card readers in the list will be added as attendance check points.

You can also edit or delete the card readers.
Click to edit the card reader.
Click to delete the card reader.

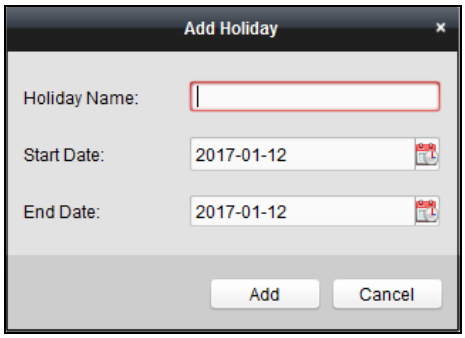
Holiday Settings

Steps:

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



2. Click to pop up Add Holiday dialog.



3. Set the related parameters.
   Holiday Name: Input the name for the holiday.
   Start Date / End Date: Click to specify the holiday date.
4. Click **Add** to add the holiday.
   The added holiday will display on the list.

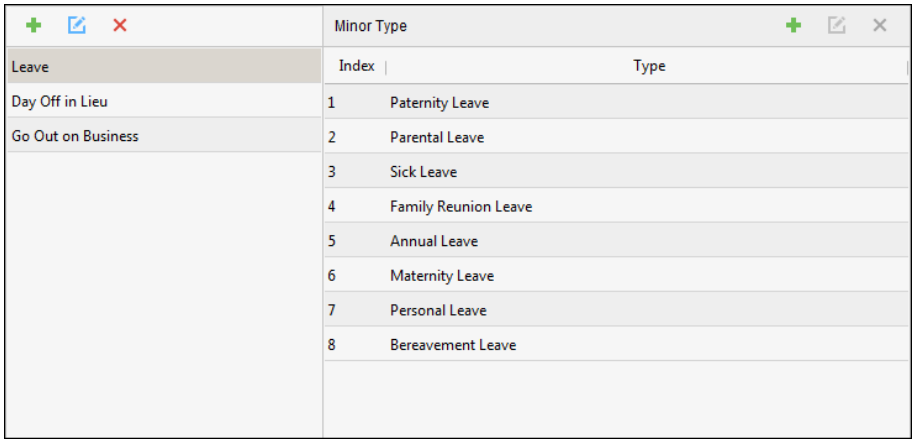
You can also edit or delete the holiday.
Click to edit the holiday.
Click to delete the holiday.

Leave Type Settings

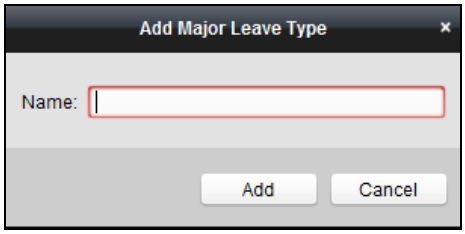
Purpose

Steps:

1. Click **Leave Type Settings** tab to enter the Leave Type Settings interface.



2. Add the major leave type.
   1) Click on the left panel to pop up the Add Major Leave Type dialog.

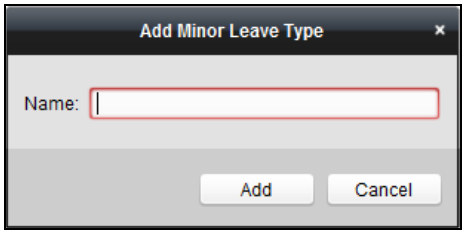


   2) Input the name for major leave type.
   3) Click **Add** to add the major leave type.

   You can also edit or delete the major leave type.
   Click to edit the major leave type.

Click ✕ to delete the major leave type.

3. Add the minor leave type.
   1) Select the major leave type.
      The minor leave type belonging to this major leave type will display on the right panel.
   2) Click ✚ on the right panel to pop up the Add Minor Leave Type dialog.



   3) Input the name for minor leave type.
   4) Click **Add** to add the minor leave type.

   You can also edit or delete the major leave type.
   Click ✎ to edit the minor leave type.
   Click ✕ to delete the minor leave type.

8.14.4 Attendance Statistics

Purpose:
After calculating attendance data, you can check the attendance summary, attendance details, abnormal attendance, overtime, card swiping logs and reports based on the calculated attendance data.

Notes:

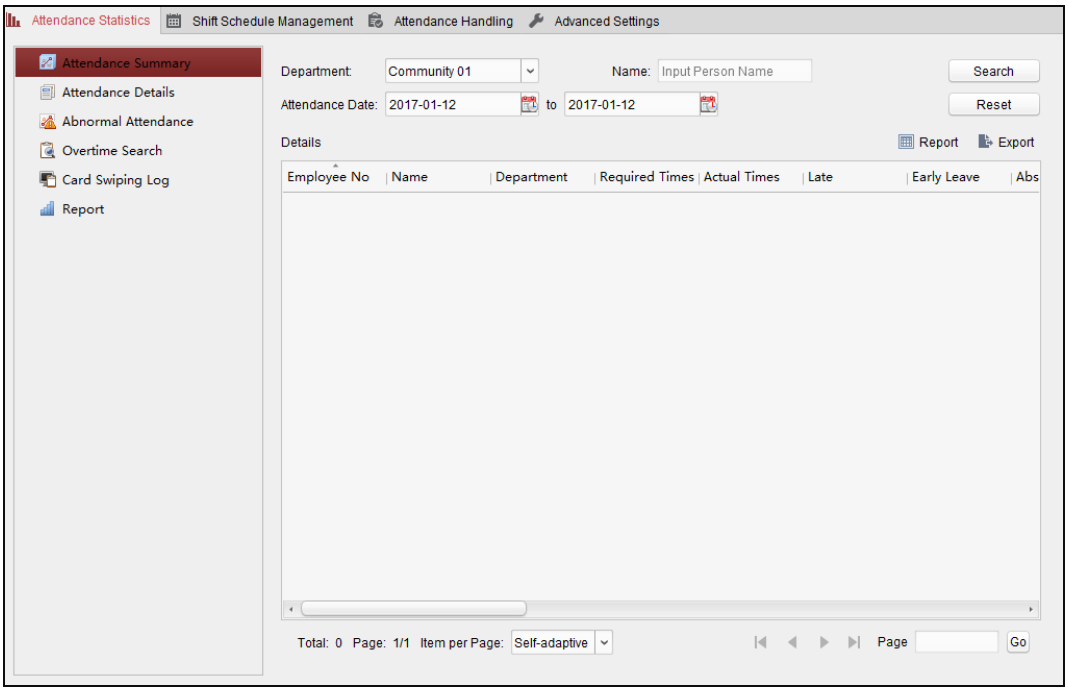
- The client automatically calculates the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to *Manual Calculation of Attendance* in *Chapter 8.14.2 Attendance Handling*.

Attendance Summary

Purpose:
You can get all the attendance information statistics of the employees in the specified time period.

Steps:

1. In the Time and Attendance module, click **Attendance Statistics** tab to enter the Attendance Statistics page.
2. Click **Attendance Summary** item on the left panel to enter the Attendance Summary interface.

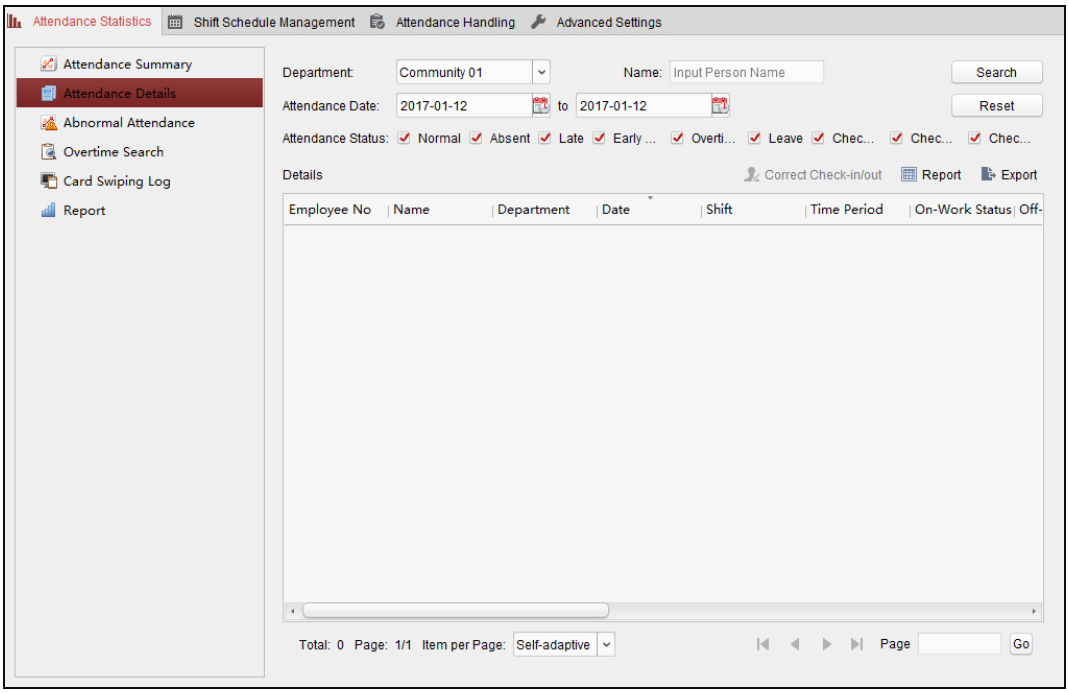


3. Set the search conditions, including department, employee name and attendance date.
   (Optional) You can click **Reset** to reset all the configured search conditions.
4. Click **Search** to start searching and the matched results will list on this page.
   (Optional) Click **Report** to generate the attendance report.
   (Optional) Click **Export** to export the results to the local PC.

Attendance Details

Steps:

1. In the Attendance Statistics page, click **Attendance Details** item on the left panel to enter the Attendance Details interface.



2. Set the search conditions, including department, employee name, attendance date and status.
   (Optional) You can click **Reset** to reset all the configured search conditions.
3. Click **Search** to start searching and the matched results will list on this page.
   (Optional) You can select a result item in the list and click **Correct Check-in/out** to correct the check-in or check-out status.
   (Optional) Click **Report** to generate the attendance report.
   (Optional) Click **Export** to export the results to the local PC.

Abnormal Attendance

You can search and get the statistics of the abnormal attendance data, including No., name and department of the employees, abnormal type, start/end time and date of attendance. For detailed operations, refer to *Chapter 0 Purpose:*

After calculating attendance data, you can check the attendance summary, attendance details, abnormal attendance, overtime, card swiping logs and reports based on the calculated attendance data.

Notes:

- The client automatically calculates the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to *Manual Calculation of Attendance* in *Chapter 8.14.2 Attendance Handling*.

Attendance Summary.

Overtime Search

You can search and get the overtime status statistics of the selected employee in the specified time period. And you can check the detailed overtime information, including No., name and department of the employees, attendance date, overtime duration and overtime type. For detailed operations, refer to *Chapter 0 Purpose:*

After calculating attendance data, you can check the attendance summary, attendance details, abnormal attendance, overtime, card swiping logs and reports based on the calculated attendance data.

Notes:

- The client automatically calculates the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to *Manual Calculation of Attendance* in *Chapter 8.14.2 Attendance Handling*.

Attendance Summary.

Card Swiping Log

You can search the card swiping logs used for the attendance statistics. After searching the logs, you can check the card swiping details, including name and department of the employees, card swiping time, card reader authentication mode and card No.. For detailed operations, refer to

Chapter 0 Purpose:

After calculating attendance data, you can check the attendance summary, attendance details, abnormal attendance, overtime, card swiping logs and reports based on the calculated attendance data.

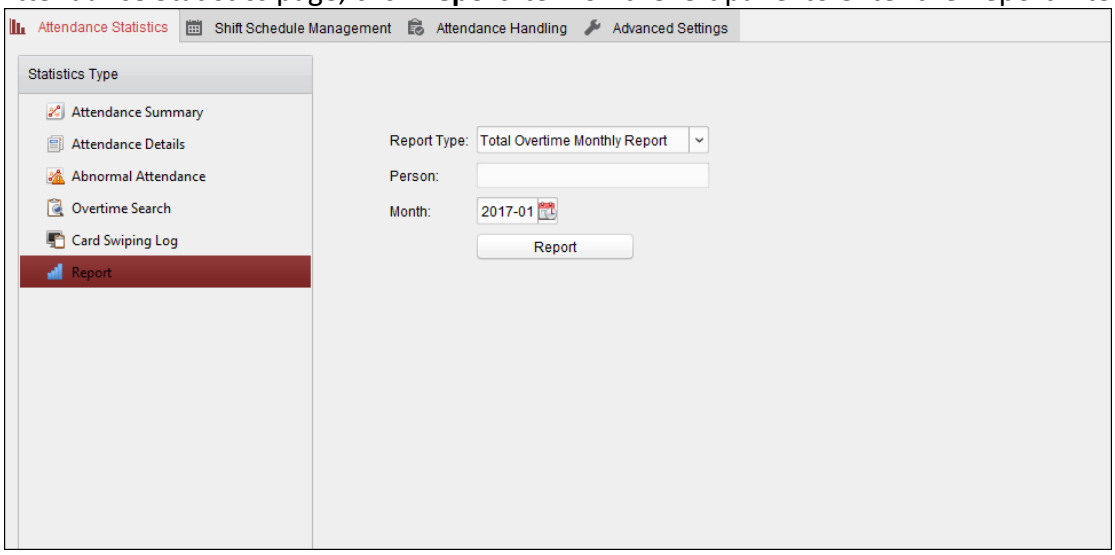
Notes:

- The client automatically calculates the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to *Manual Calculation of Attendance* in *Chapter 8.14.2 Attendance Handling*.

Attendance Summary.

Report

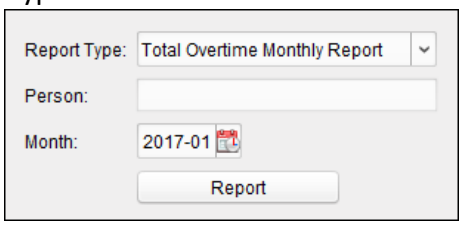
In the Attendance Statistics page, click **Report** item on the left panel to enter the Report interface.



➢ Generating Total Overtime Monthly Report

Steps:

1. Click in the Report Type field to unfold the drop-down list and select **Total Overtime Monthly Report** as the report type.



2. Click **Person** field to select the person.
3. Click to specify a month.
4. Click **Report** to start generating the matched total overtime monthly report.

➢ Generating Overtime Details Monthly Report

Select **Overtime Details Monthly Report** as the report type. You can generate overtime details

monthly report. For detailed operations, refer to *Generating Total Overtime Monthly Report.*

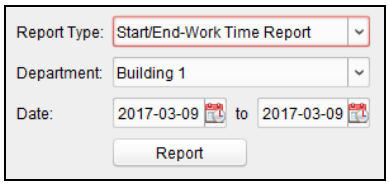
➢ Generating Attendance Monthly Report

Select **Attendance Monthly Report** as the report type. You can generate attendance monthly report. For detailed operations, refer to *Generating Total Overtime Monthly Report.*

➢ Generating Start/End-Work Time Report

Steps:

1. Click in the report type field to unfold the drop-down list and select **Start/End-Work Time Report** as the report type.



2. Click **Department** field to select the department.
3. Click to specify the start date and end date of a date period.
4. Click **Report** to start generating the matched total overtime monthly report.

➢ Generating Department Attendance Report

Set the report type as **Department Attendance Report** and you can generate department attendance report. For detailed operations, refer to *Generating Start/End-Work Time Report* above.

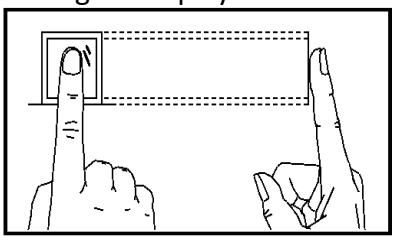
Appendix A Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

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

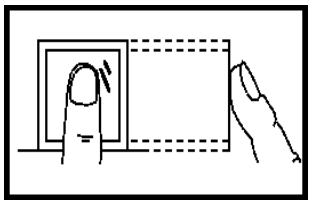


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

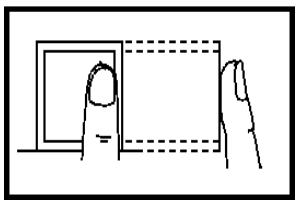
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

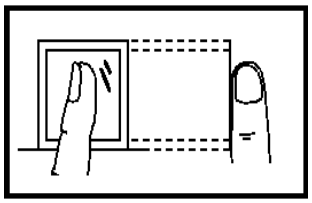
Vertical



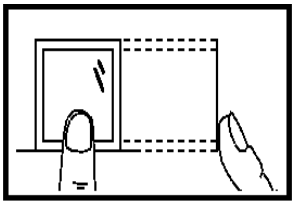
Edge I



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.

Appendix B Custom Wiegand Rule Descriptions

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

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

Wiegand Data = Valid Data + Parity Data

Total Length: Wiegand data length.

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

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

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

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

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

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

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

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

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

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

0200001071027

UD05944B

www.hikvision.com