Video Access Control Terminal

User Manual

User Manual

This manual is applied for video access control terminal.

Series	Model
Video Access Control Terminal	DS-K1T501SF

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

Trademarks

Disclaimer

Support

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

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the

applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

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	Standard
DSA-12PFT-12FUK 120100	Dee Van Enterprise Co., Ltd.	BS
DSA-12PFT-12FAU 120100	Dee Van Enterprise Co., Ltd.	AS
DSA-12PFT-12FIN 120100	Dee Van Enterprise Co., Ltd.	IS
DSA-12PFT-12FUS 120100	Dee Van Enterprise Co., Ltd.	IEC
DSA-12PFT-12 FBZ 120100	Dee Van Enterprise Co., Ltd.	NBR

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**

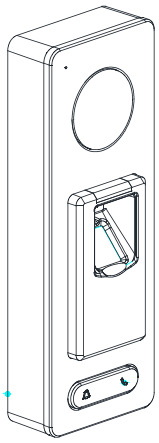
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification 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.
- Please take care of your card and report card loss in time when card is lost.
- If you require a higher security level, use multiple authentication modes.
- Multiple card types are supported. Please select an appropriate card type according to the card performance and the usage scenarios.

Table of Contents

Chapter 1 Overview

1.1 Introduction



DS-K1T501SF is a series video access control terminal with multiple advanced technologies including fingerprint recognition, face detection, Wi-Fi, smart card recognition, and HD camera (2 MP optional). It is equipped with fingerprint recognition module (supporting 1:1 mode and 1:N mode), and supports offline operation.

1.2 Main Features

- Transmission modes of wired network (TCP/TP), Wi-Fi, RS-485, and Wiegand
- Face detection and picture capturing function implemented by built-in camera (2 MP optional)
- 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
- Supports EHome protocol
- Max. 50,000 cards Max. 200,000 access control events records, and Max.3000 fingerprints storage
- Adopts fingerprint module, supporting 1:N mode (fingerprint, card + fingerprint) and 1:1 mode (card + fingerprint)
- Supports multiple authentication modes including card, fingerprint, card + fingerprint, card + password, fingerprint + password, card + fingerprint + password, and so on.
- Supports Mifare card/ QR Code reading
- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, duress card alarm, and so on
- Supports security door control unit connection
- Protection level: IP65
- Data can be permanently saved after power-off

Chapter 2 Appearance

2.1 Appearance of DS-K1T501SF Model

Please refer to the following content for detailed information of the DS-K1T501SF model.

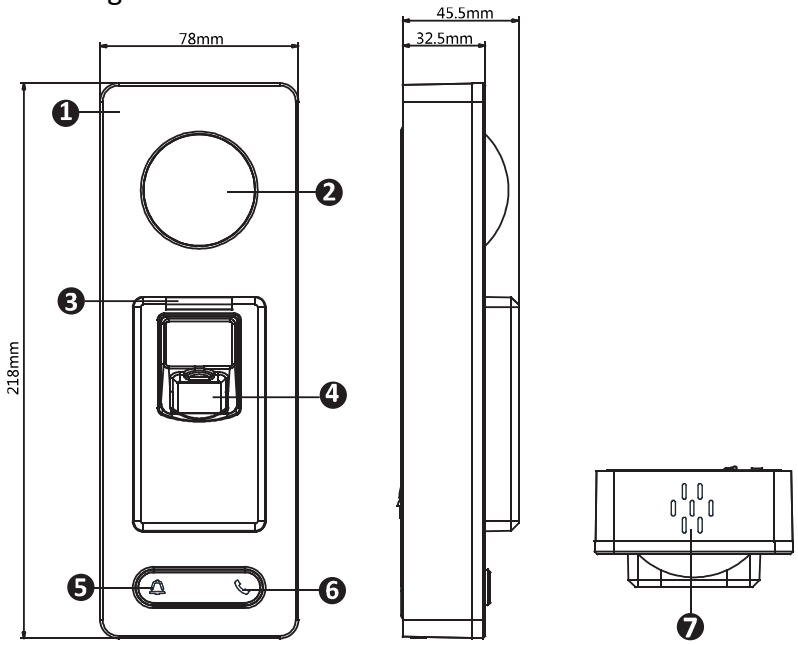
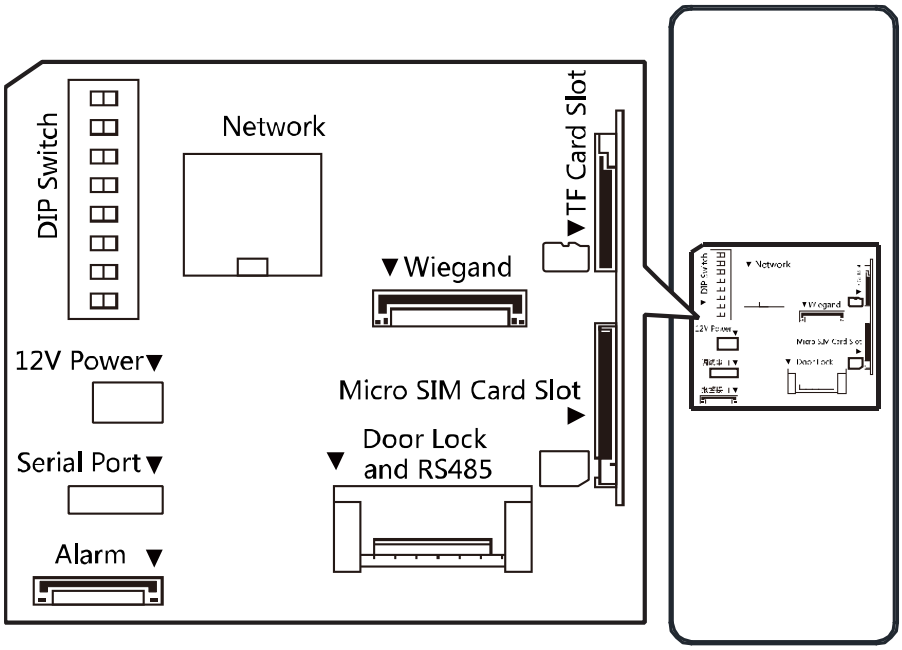


Table 2-1 Description of DS-K1T501SF Series Model

No.	Description
1	Mic
2	Camera
3	LED Indicator
4	Fingerprint Scanner and Card Swiping Area
5	Doorbell Button
6	Voice Talk Button
7	Loud Speaker

2.2 Video Access Control Terminal Connector

The video access control terminal connector is as follows:


DIP Switch
Network
▼TF Card Slot
▼Wiegand
12V Power▼
Micro SIM Card Slot ▶
Serial Port▼
Door Lock
and RS485
Alarm ▼

Chapter 3 Installation

Before You Start:

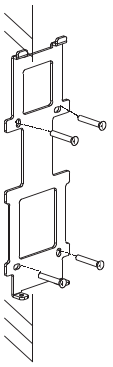
Make sure that the device in the package is in good condition and all the assembly parts are included.

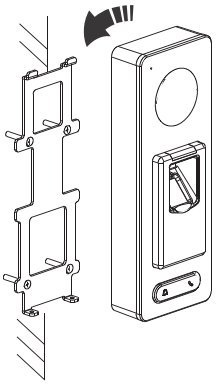
Make sure that the wall is strong enough to withstand three times the weight of the terminal.

Set the DIP address before installation.

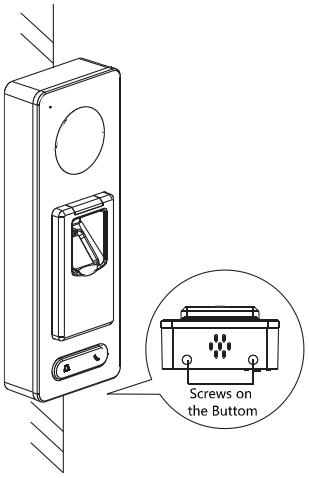
Steps:

1. Connect the cables with the connecter on the rear panel of the device. Route the cables through the cable hole of the mounting plate. The cable holes are on the right side, left side and lower side of the rear cover. If the right/left side cable hole is selected, remove the plastic sheet of the cable hole.
2. Secure the mounting plate on the wall with 4 supplied screws.
3. Connect the corresponding cables.
4. Push the terminal in the mounting plate from bottom up.





5. Tighten the screws on the bottom of the terminal to fix the terminal on the mounting plate and complete the installation.



Chapter 4 Terminal Connection

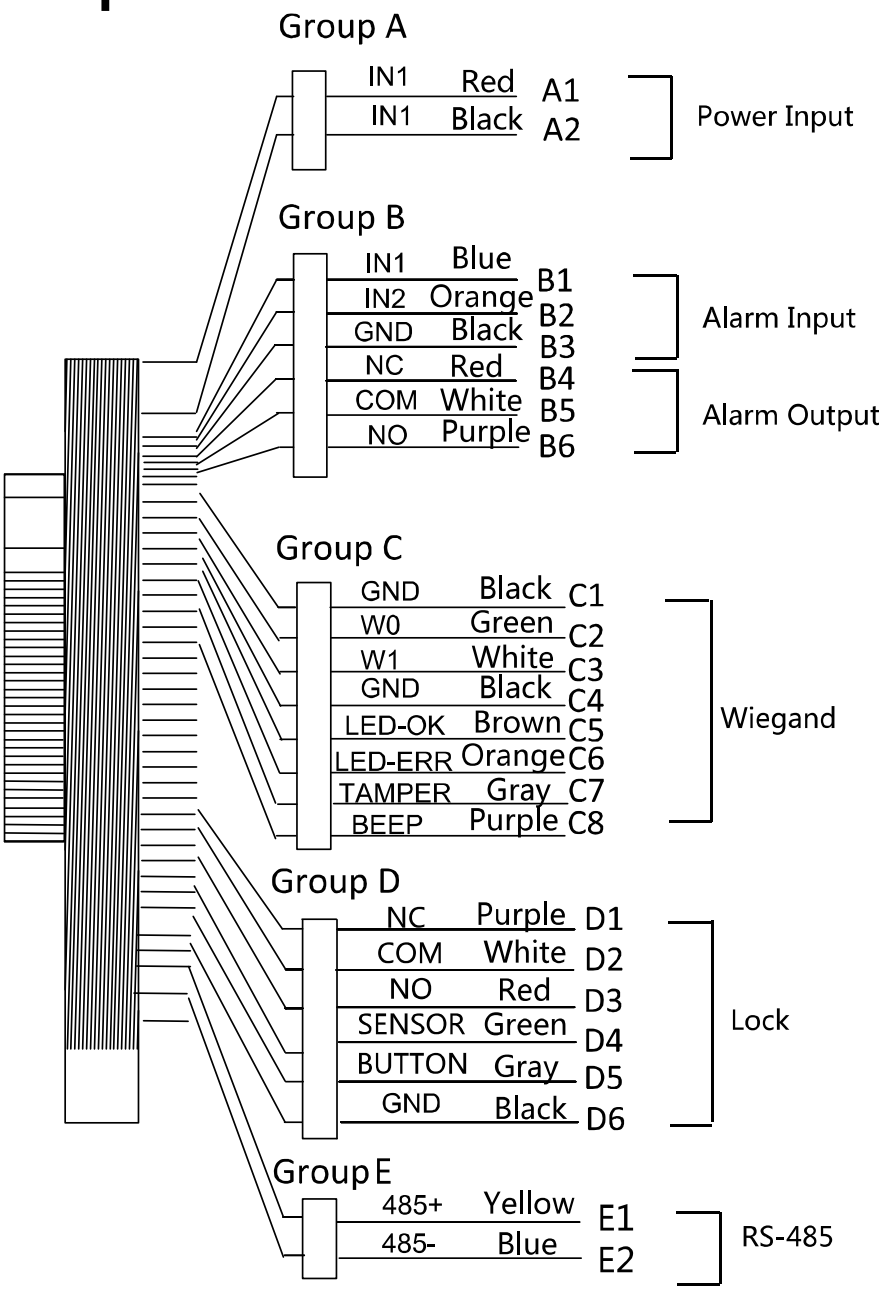
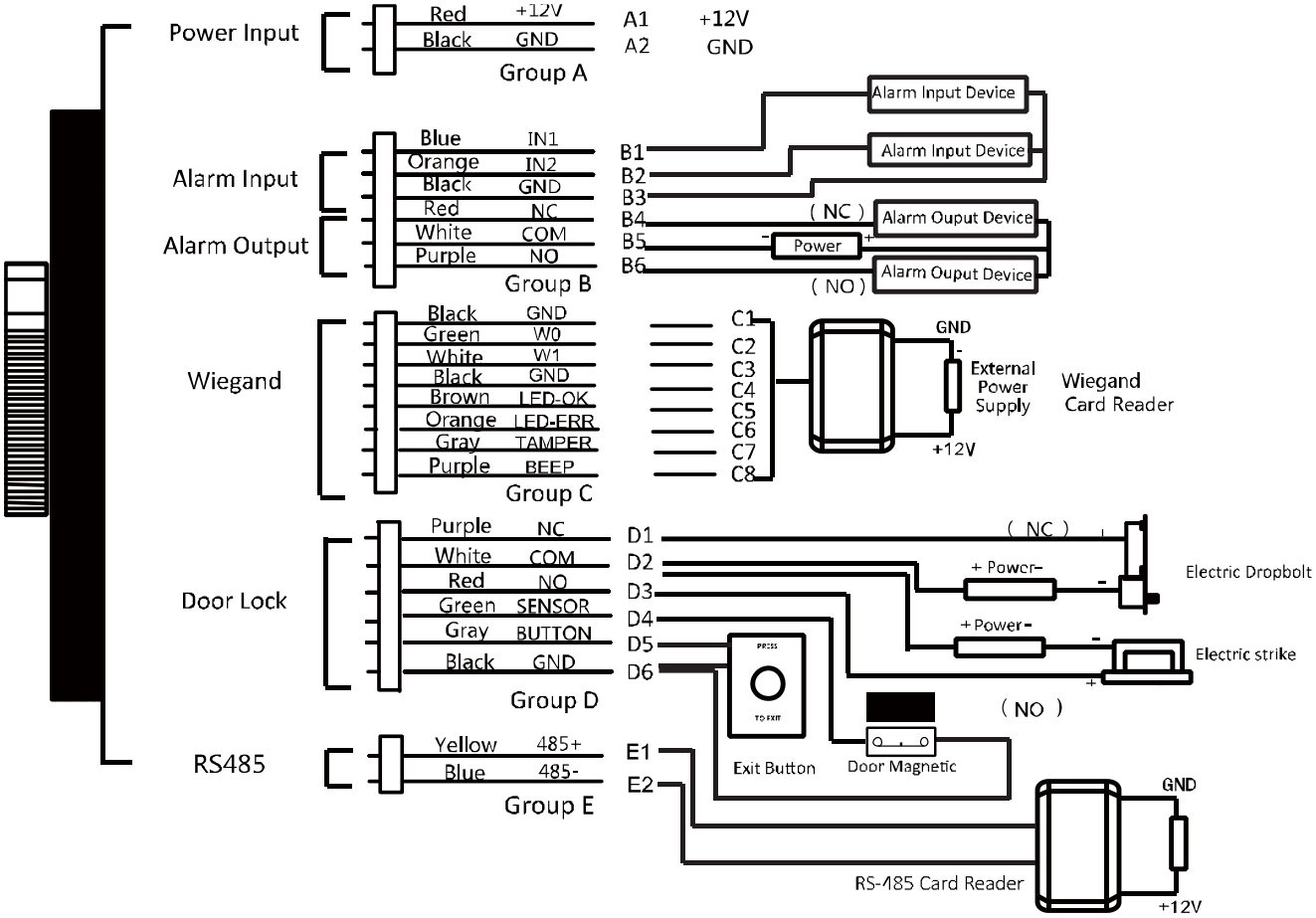


Table 4-1 Terminal Description

Group	No.	Function	Color	Terminal Name	Description
Group A	A1	Power Input	Red	+12V	12V DC Power Supply
	A2		Black	GND	GND
Group B	B1	Alarm Input	Yellow	IN1	Alarm Input 1
	B2		Orange	IN2	Alarm Input 2
	B3		Black	GND	GND
	B4	Alarm Output	Red	NC	Alarm Output Wiring
	B5		White	COM	
	B6		Purple	NO	
Group C	C1	Wiegand	Black	GND	GND
	C2		Green	W0	Wiegand Wiring 0
	C3		White	W1	Wiegand Wiring 1
	C4		Black	GND	GND
	C5		Brown	LED-OK	Wiegand Authenticated
	C6		Orange	LED-ERR	Wiegand Authentication Failed
	C7		Gray	TAMPER	Tampering Alarm Wiring
	C7		Purple	BEEP	Buzzer Wiring
Group D	D1	Lock	Purple	NC	Lock Wiring
	D2		White	COM	
	D3		Red	NO	
	D4		Green	SENSOR	Door Magnetic Signal Input
	D5		Gray	BUTTON	Exit Door Wiring
	D6		Black	GND	GND
Group E	E1	RS-485	Yellow	485 +	RS-485 Wiring
	E2		Blue	485 -	

Chapter 5 Wiring Description

5.1 External Device Wiring Overview



Notes:

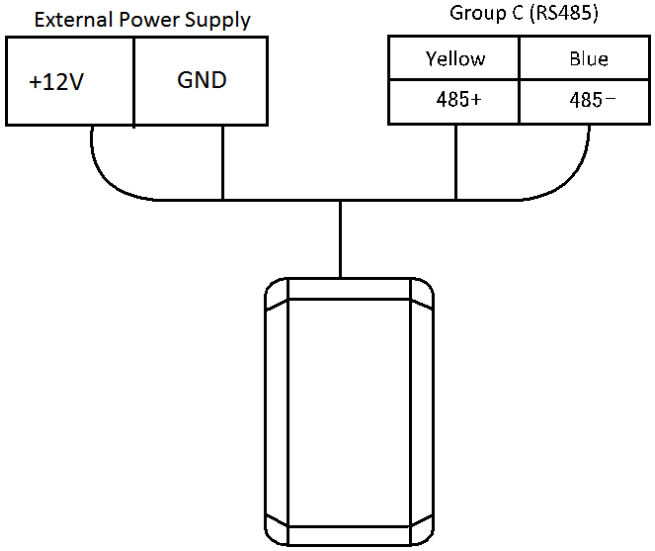
If set the working mode as the controller mode, the terminal can connect the RS-485 card reader or security control unit via RS-485 protocol. For details about wiring of RS-485 card reader, see 5.2 The Wiring of External RS-485 Card Reader.

If set the working mode as the controller mode, the terminal cannot connect the Wiegand card reader.

The security control unit can also connect the external devices. For details, see the specified user manual of security control unit.

5.2 The Wiring of External RS-485 Card Reader

If set the working mode as the controller mode, the DIP switch No.6 should be set as OFF.
If set the working mode as card reader mode, the DIP switch No. from 1 to 4 should be set as OFF.
Set the external card reader's RS-485 DIP switch to 2. For details about DIP switch configuration, see Appendix B DIP Switch Introduction.



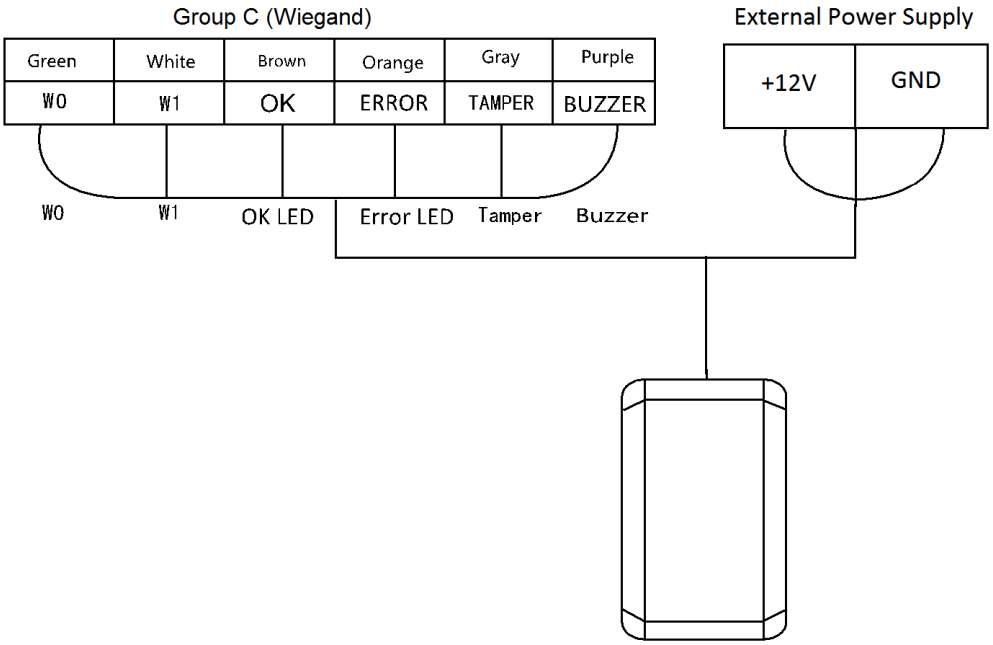
5.3 Card Reader Connection

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.

5.3.1 The Wiring of Wiegand



NOTE

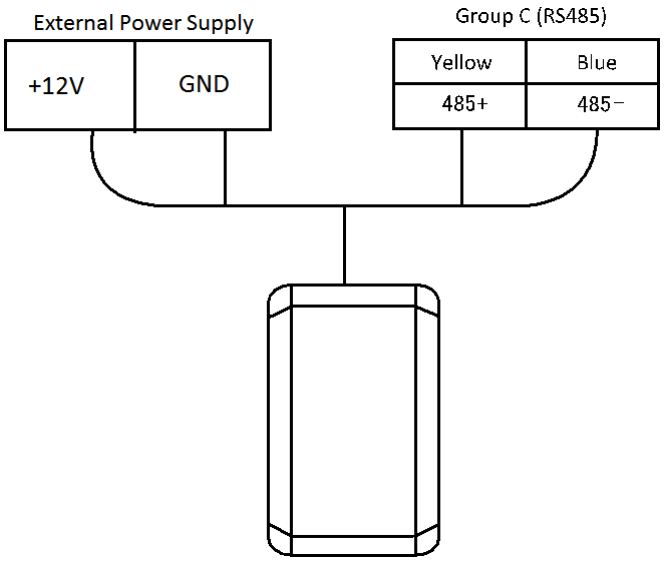
When the access control terminal works as a card reader, you must the **WG_ERR, BUZZER and WG_OK** interfaces if you want to control the LED and buzzer of the Wiegand card reader.

Set the working mode of the terminal as card reader, 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.

5.3.2 The Wiring of RS-485 Output



NOTE

Set the working mode of the terminal as card reader, if the terminal requires working as a card reader.

When the access control terminal works as a RS-485 card reader, you can set the RS-485 address via the DIP switch.

The external power supply and the access control terminal should use the same GND cable.

Chapter 6 Activating the Access Control Terminal

Purpose:

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

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

The default values of the control terminal are as follows.

The default IP address: 192.0.0.64.

The default port No.: 8000.

The default user name: admin.

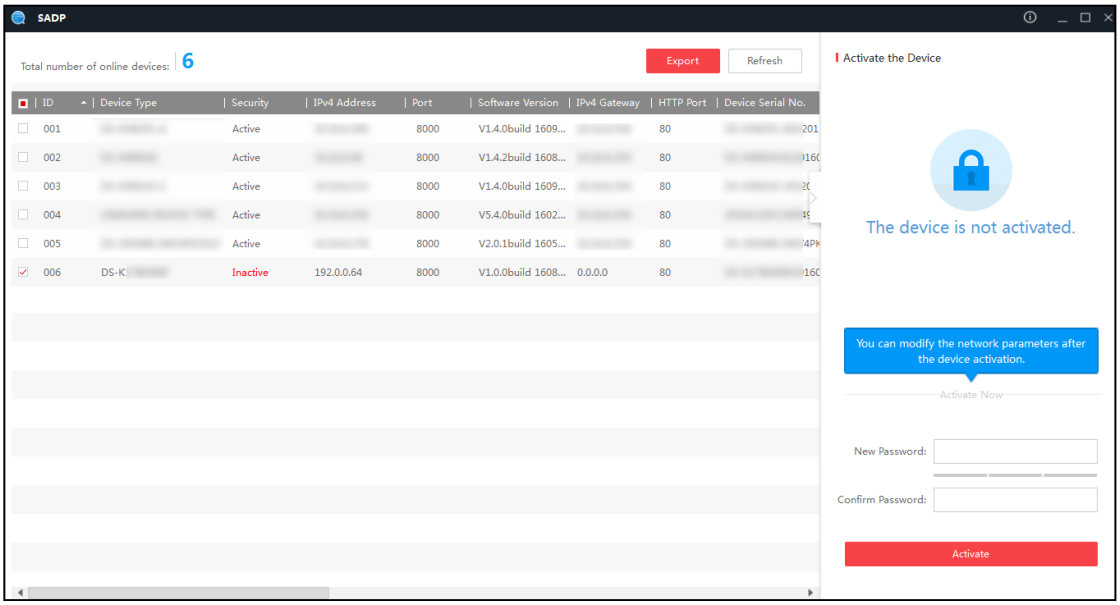
6.1 Activating via SADP Software

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

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

Steps:

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

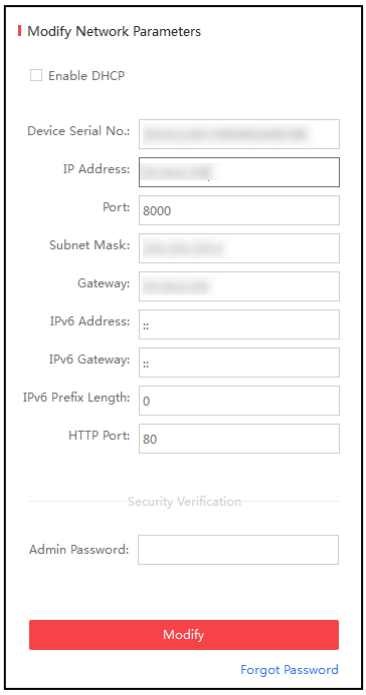


3. Create a password in the password field, and confirm the password.

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

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

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



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

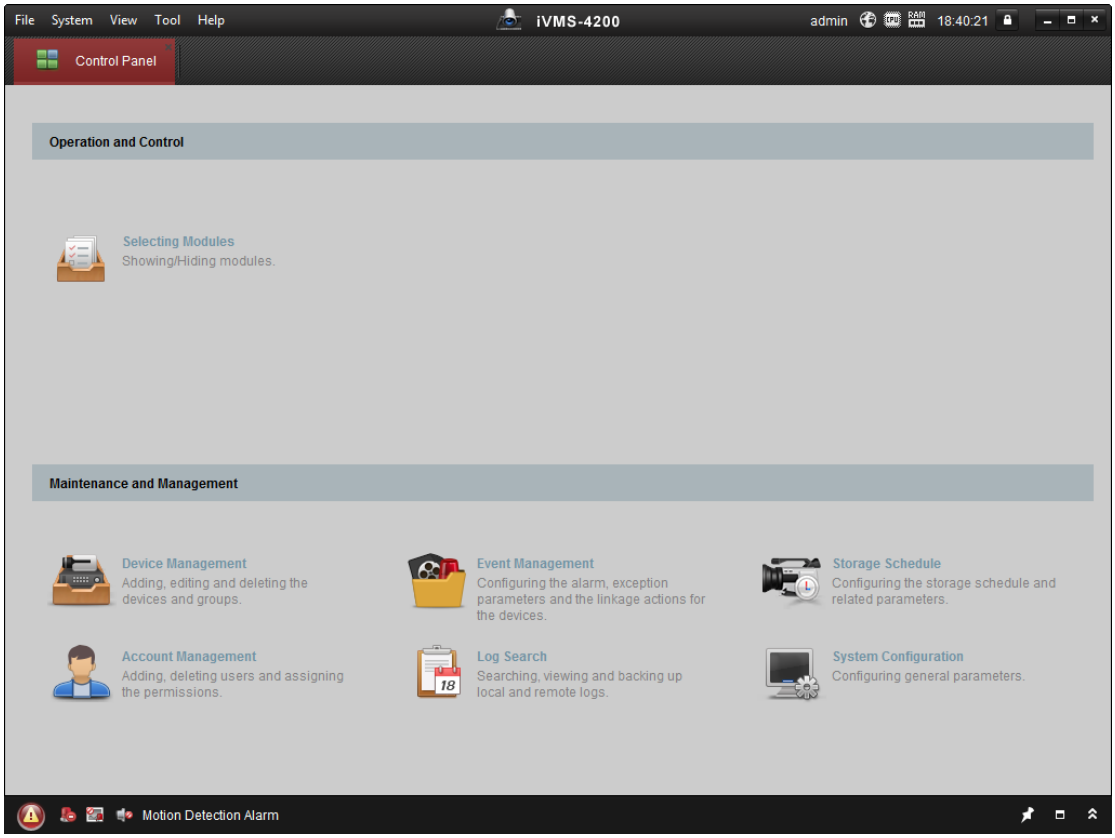
6.2 Activating via Client Software

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

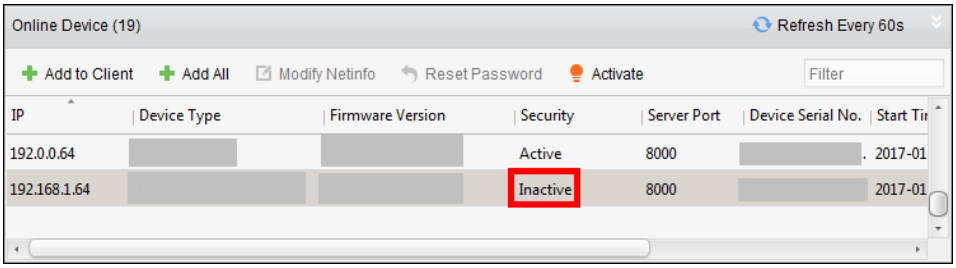
Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

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



2. Click **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.*

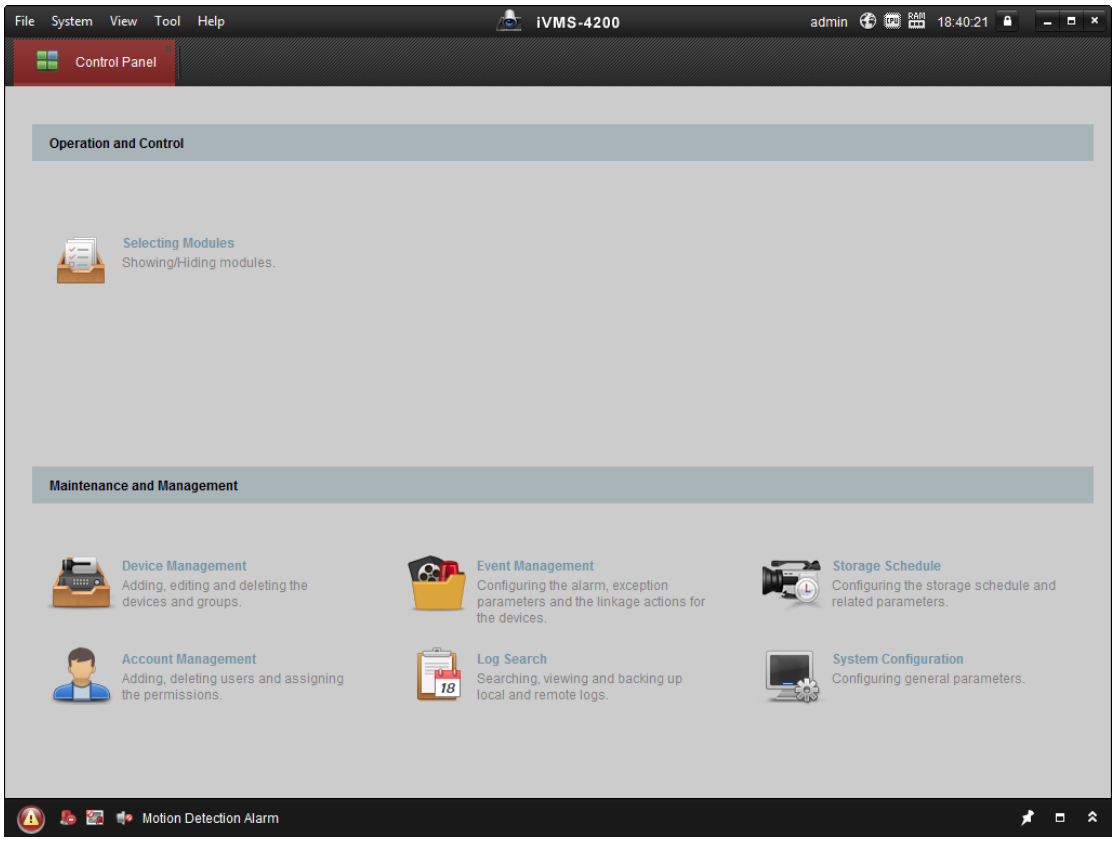
7. Click **OK** button to start activation.
8. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.
9. Change the device IP address to the same network segment with your computer by either modifying the IP address manually.
10. Input the password and click the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

Chapter 7 Client Operation

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

7.1 Function Module

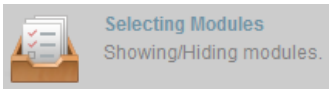
Control Panel of iVMS-4200:



Menu Bar:

File	**Open Image File**	Search and view the captured pictures stored on local PC.
	Open Video File	Search and view the video files recorded on local PC.
	Open Log File	View the backup log files.
	Exit	Exit the iVMS-4200 client software.
System	**Lock**	Lock screen operations. Log in the client again to unlock.
	Switch User	Switch the login user.
	Import System Config File	Import client configuration file from your computer.
	Export System Config File	Export client configuration file to your computer.
	Auto Backup	Set the schedule for backing up the database including person, attendance data, and permission data automatically.
View	**1024*768**	Display the window at size of 1024*768 pixels.

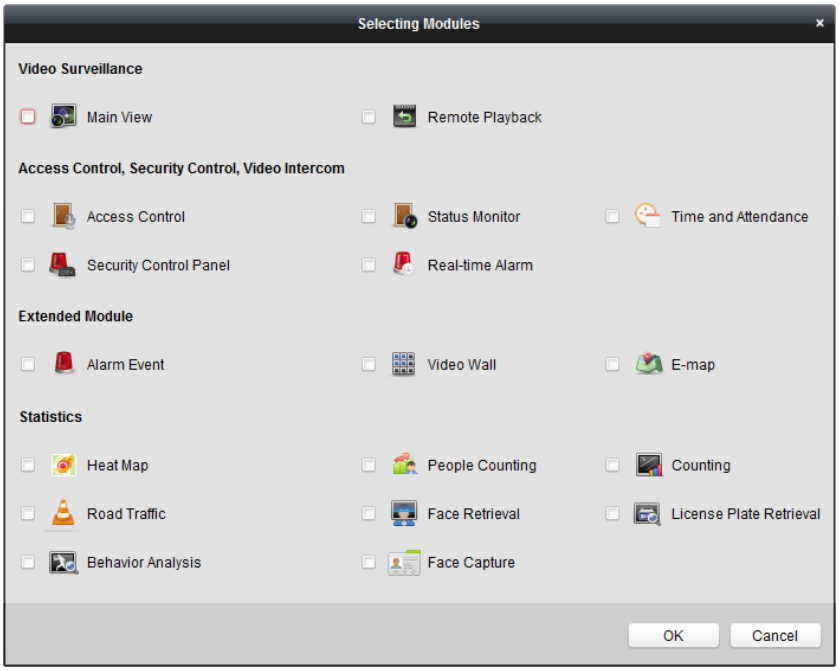
	1280*1024	Display the window at size of 1280*1024 pixels.
	1440*900	Display the window at size of 1440*900 pixels.
	1680*1050	Display the window at size of 1680*1050 pixels.
	Maximize	Display the window in maximum mode.
	Control Panel	Enter Control Panel interface.
	Main View	Open Main View page.
	Remote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

For the first time running the software, you can click 

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

Steps:

1. Click  to pop up the following dialog.



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

Notes:

After adding the access control device in Device Management module, the Access Control, Status, and Time and Attendance module will be displayed on the control panel automatically.

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

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

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

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

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

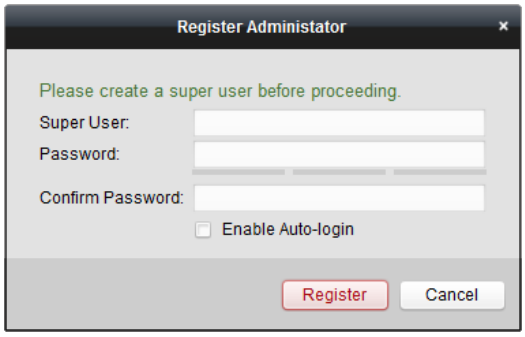
You can check the information, including current user, network usage, CPU usage, memory usage and time, in the upper-right corner of the main page.

7.2 User Registration and Login

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

Steps:

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

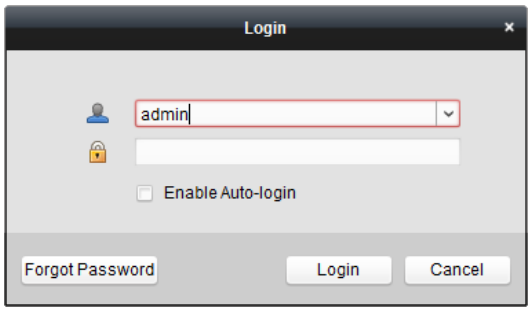


*A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.*
For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters,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

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

Steps:

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



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

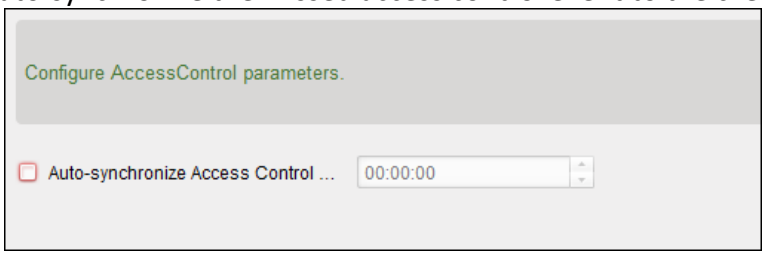
7.3 System Configuration

Purpose:

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

Steps:

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



7.4 Access Control Management

Purpose:

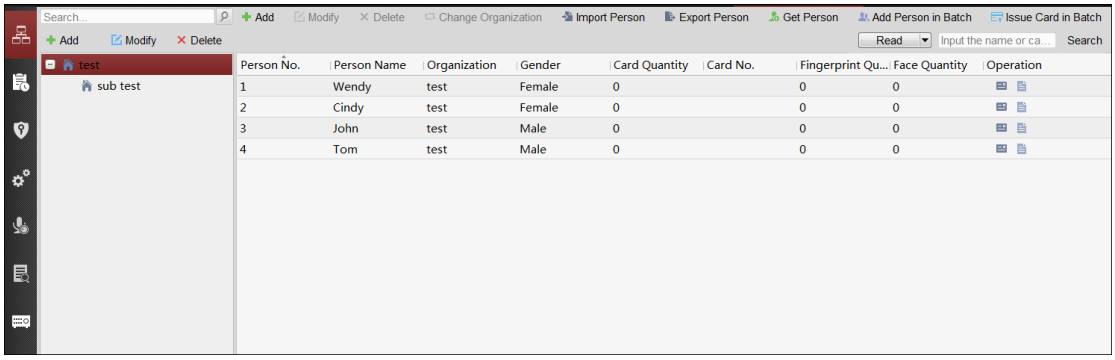
The Access Control module is applicable to access control devices and video intercom. It provides multiple functionalities, including person and card management, permission configuration, access control status management, video intercom, and other advanced functions.

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

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

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

Click  to enter the Access Control module.



Before you start:

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

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.

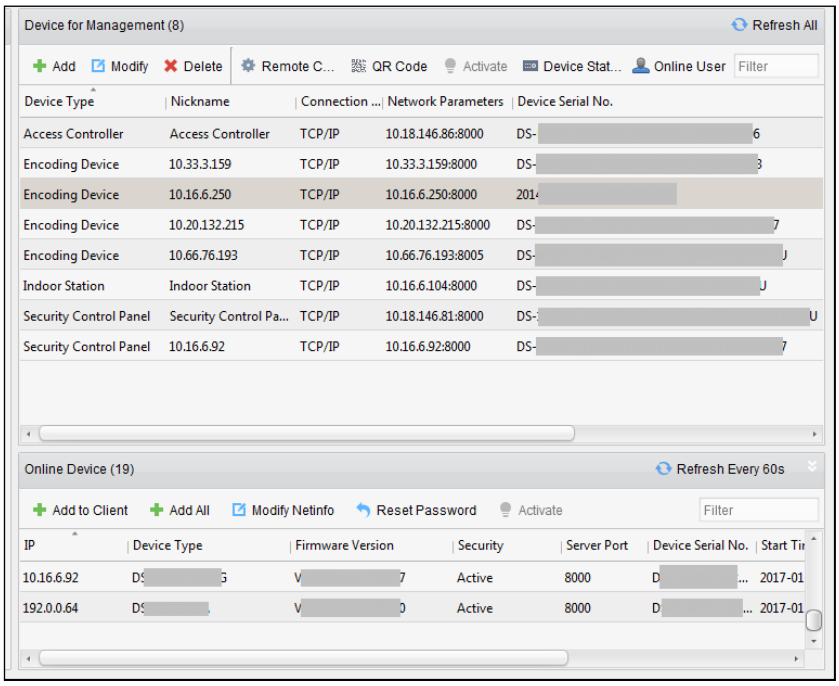
The Access Control module is composed of the following sub modules.

	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.

7. 4. 1 Adding Access Control Device

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



Note: After adding the device, you should check the device arming status in **Tool** – **Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, refer *7.13 Arming Control*.

Creating Password

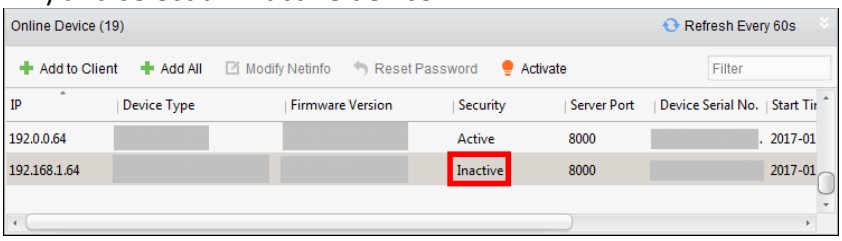
Purpose:

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:

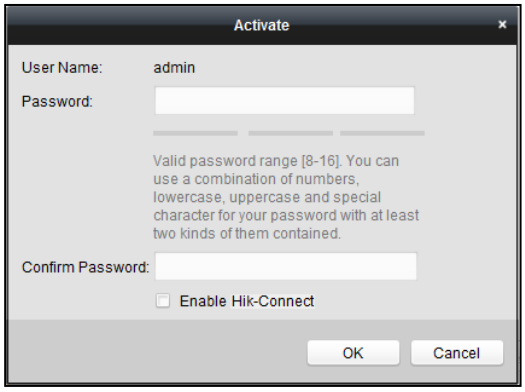
1. Enter the Device Management page.
2. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.



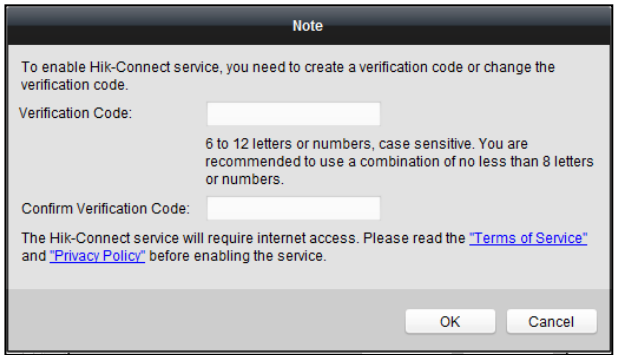
3. Click the **Activate** button to pop up the Activation interface.
4. Create a password in the password field, and confirm the password.

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,*

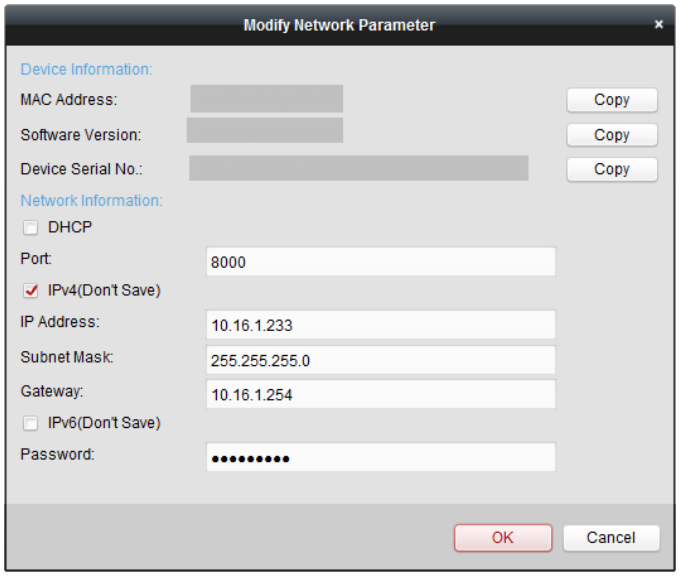
resetting the password monthly or weekly can better protect your product.



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.

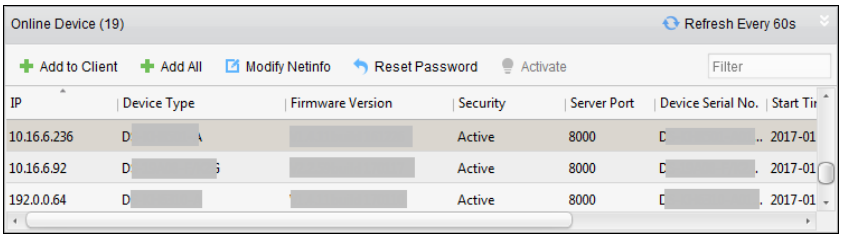


Adding Online Device

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:

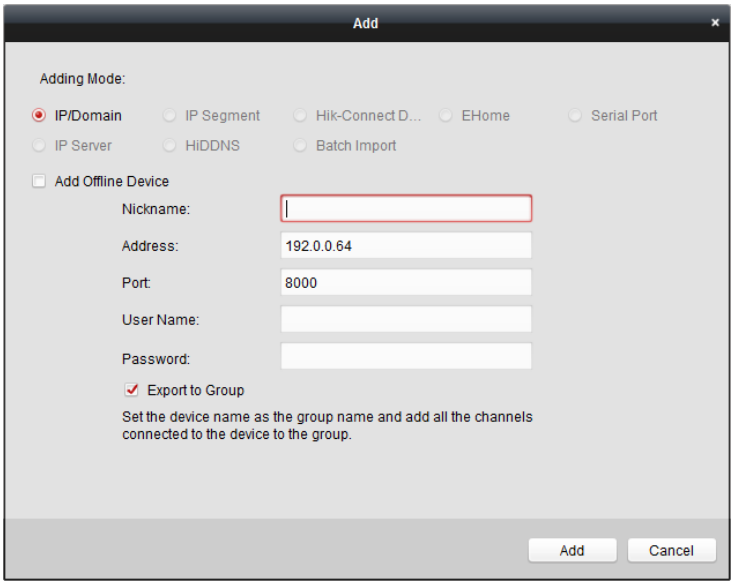
1. Select the devices to be added from the list.
   Note: For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, please refer to *Chapter 6 Activating the Access Control Terminal.*
2. Click **Add to Client** to open the device adding dialog box.
3. Input the required information.
   Nickname: Edit a name for the device as you want.
   Address: Input the device's IP address. The IP address of the device is obtained automatically in this adding mode.
   Port: Input the device port No. The default value is *8000*.
   User Name: Input the device user name. By default, the user name is *admin*.
   Password: Input the device password.

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

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

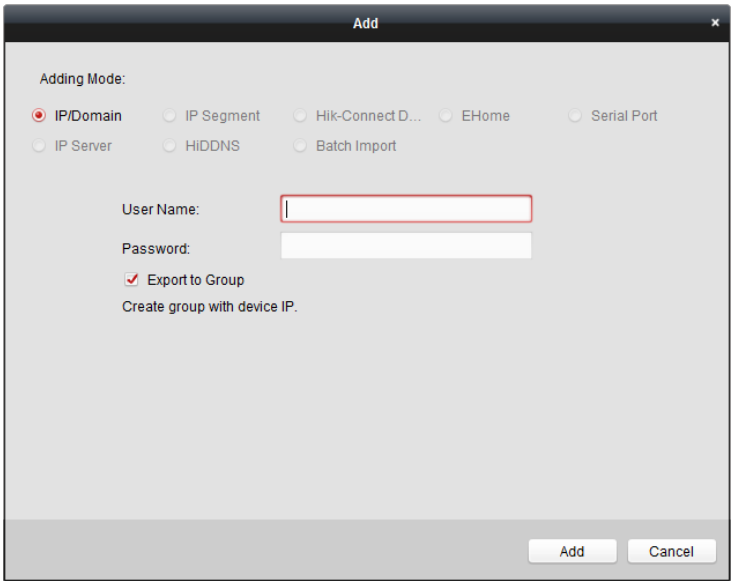


Adding Multiple Online Device

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

Adding All Online Devices

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



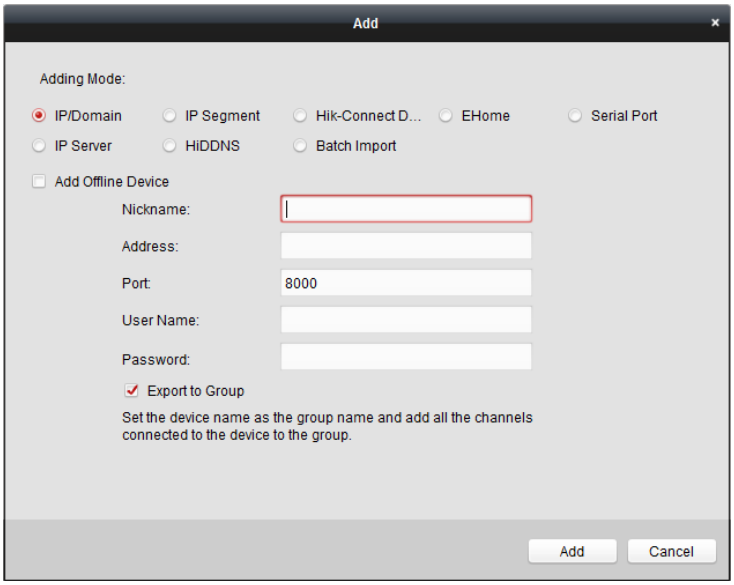
Adding Devices by IP or Domain Name

Steps:

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

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

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



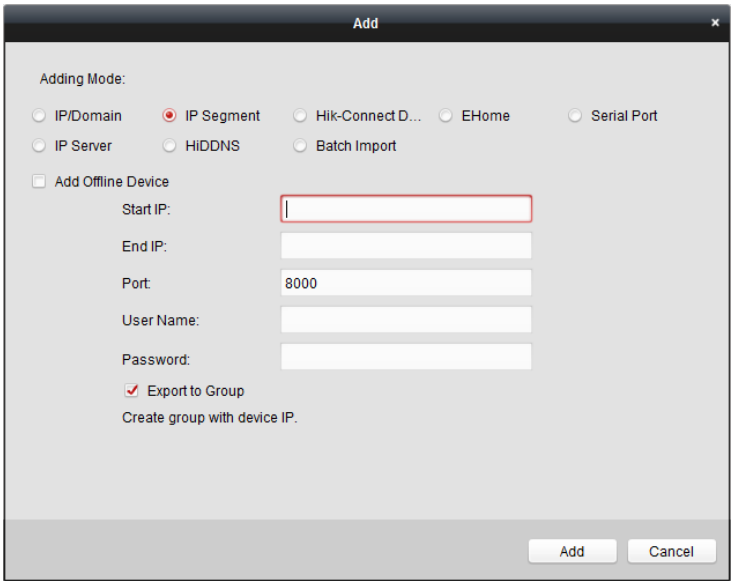
Adding Devices by IP Segment

Steps:

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

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

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



Adding Devices by Hik-Connect Domain

Purpose:

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

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

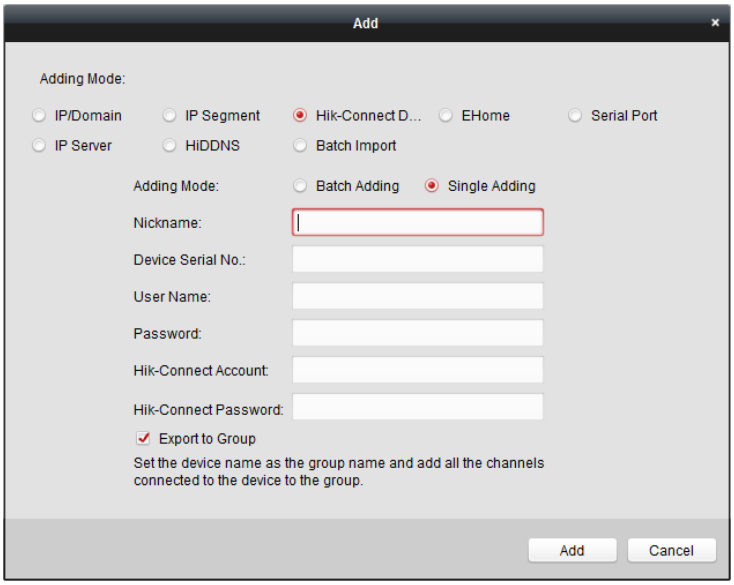
Add Single Device

Steps:

1. Click **Add** to open the device adding dialog.
2. Select **Hik-Connect Domain** as the adding mode.
3. Select **Single Adding**.
4. Input the required information.
   Nickname: Edit a name for the device as you want.
   Device Serial No.: Input the device serial No.
   User Name: Input the device user name. By default, the user name is *admin*.
   Password: Input the device password.

   STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*
   Hik-Connect Account: Input the Hik-Connect account.
   Hik-Connect Password: Input the Hik-Connect password.
5. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the channels of the device to the corresponding group by default.

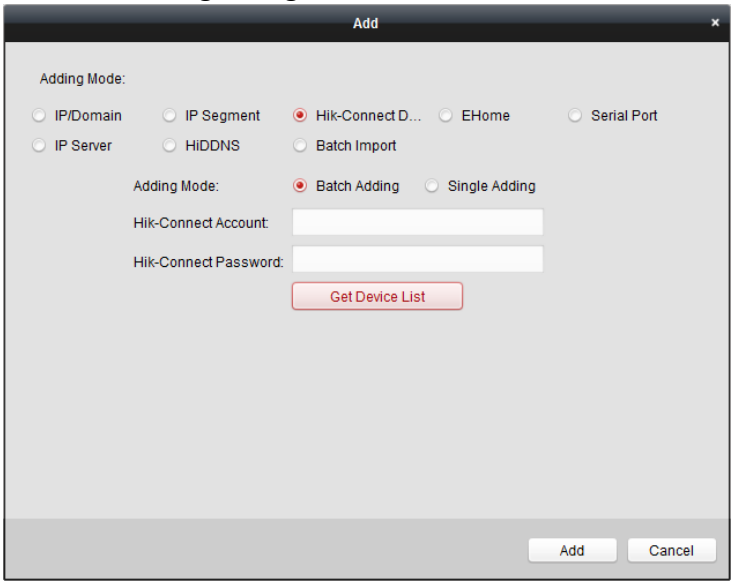
6. Click **Add** to add the device.



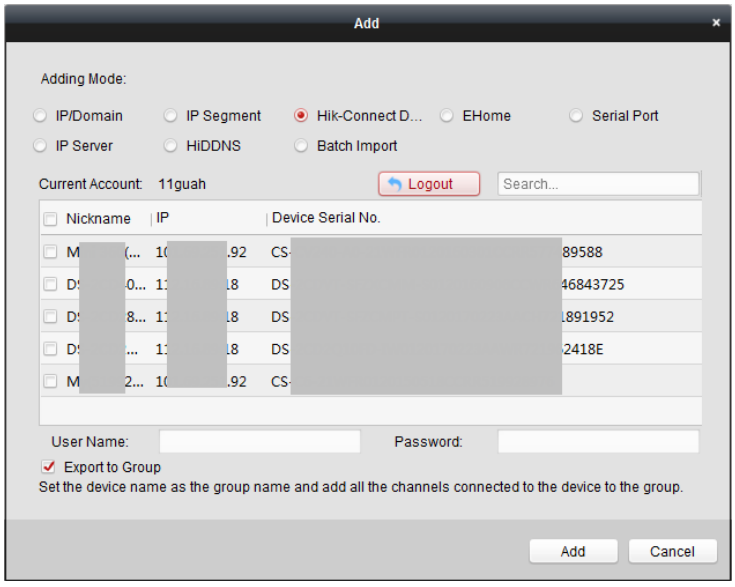
Add Devices in Batch

Steps:

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



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



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

Adding Devices by EHome Account

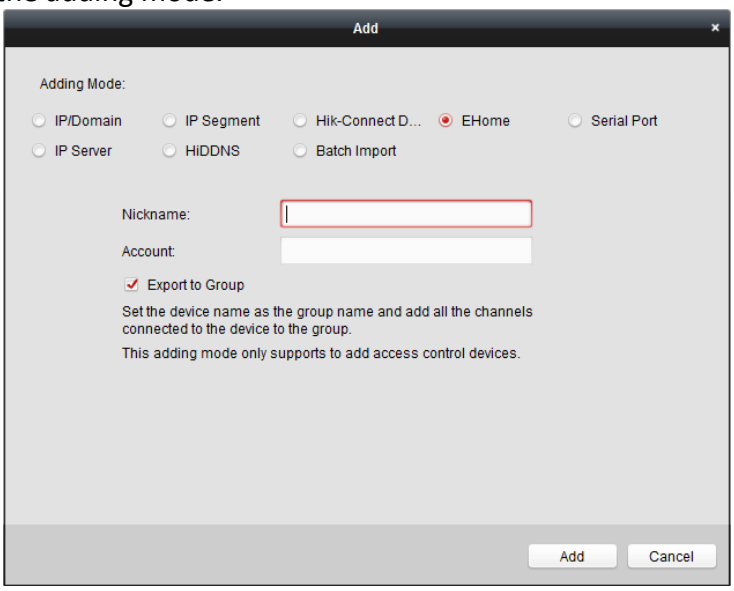
Purpose:

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

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

Steps:

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



3. Input the required information.

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

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

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

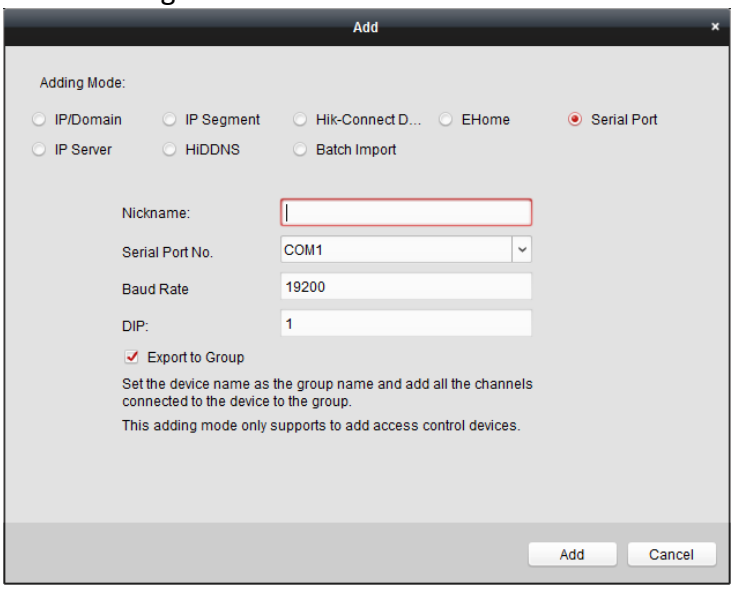
Adding Devices by Serial Port

Purpose:

You can add access control device connected via serial port.

Steps:

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



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

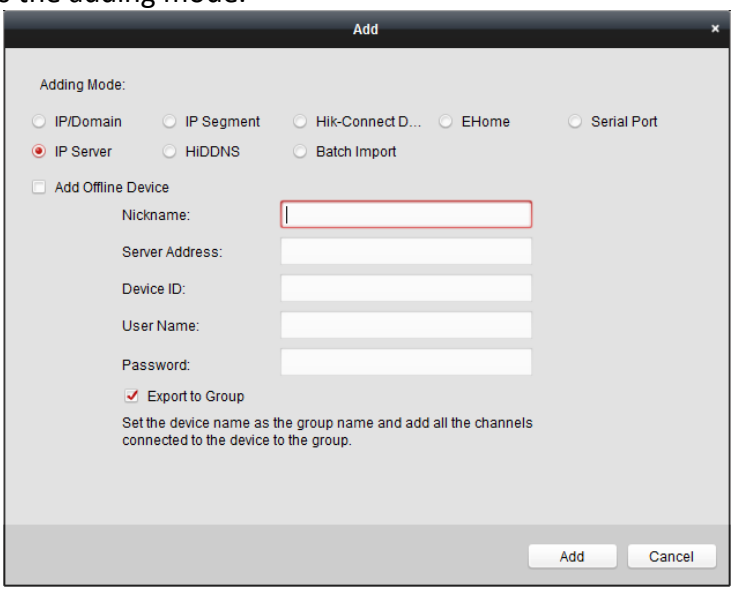
When the offline device comes online, the software will connect it automatically.

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

Adding Devices by IP Server

Steps:

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



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

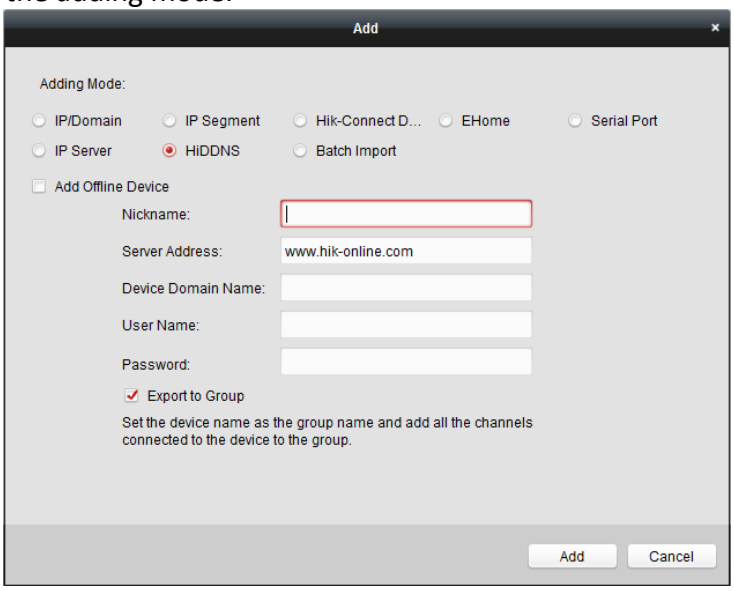
   STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password 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) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

Adding Devices by HiDDNS

Steps:

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



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

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

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

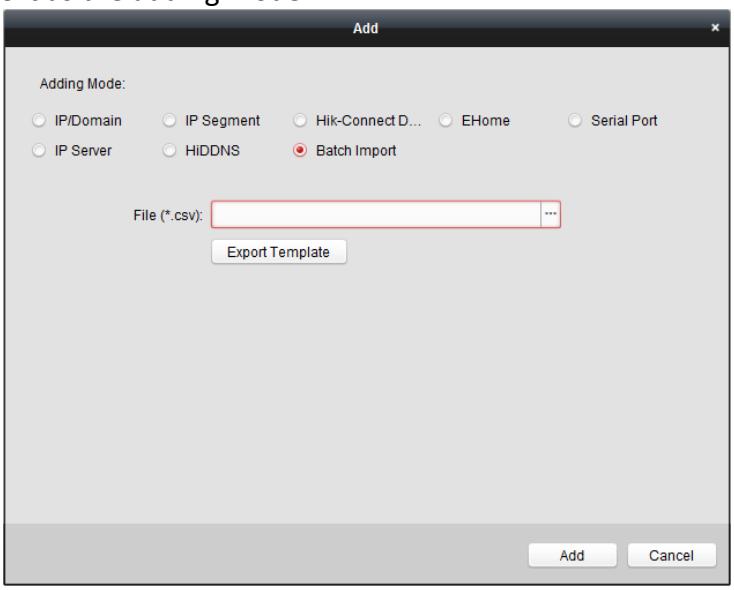
Importing Devices in Batch

Purpose:

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

Steps:

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



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

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

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

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

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

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

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

   Password: Input the device password.

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

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

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

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

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

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

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

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

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

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

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

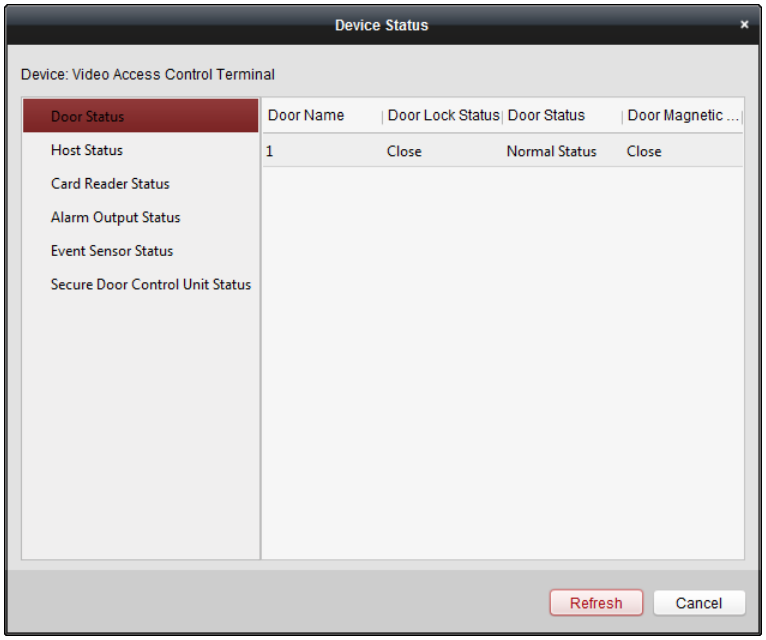
5. Click ··· and select the template file.
6. Click **Add** to import the devices.

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

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

7.4.2 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.

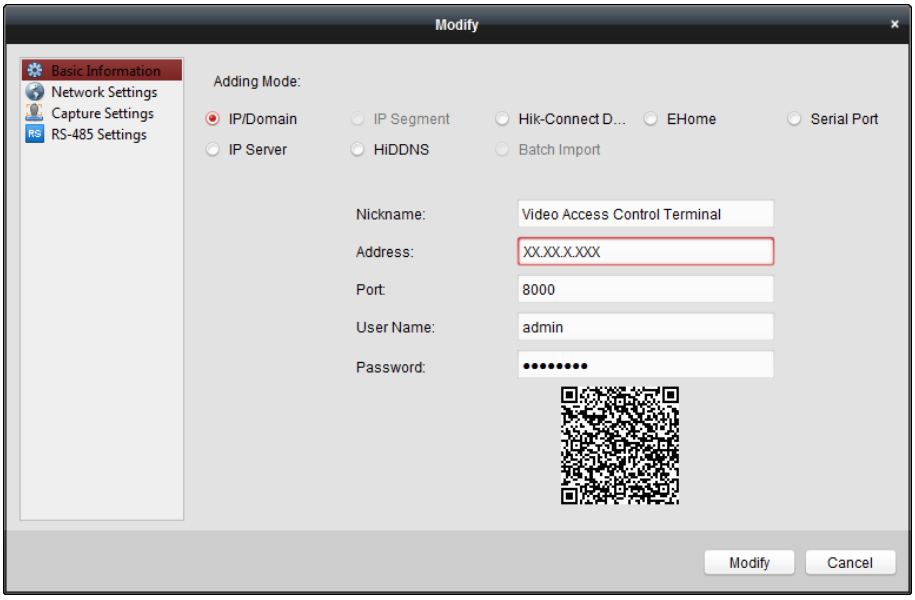
7.4.3 Editing Basic Information

Purpose:

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

Steps:

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



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

7. 4. 4 Network Settings

Purpose:

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

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

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

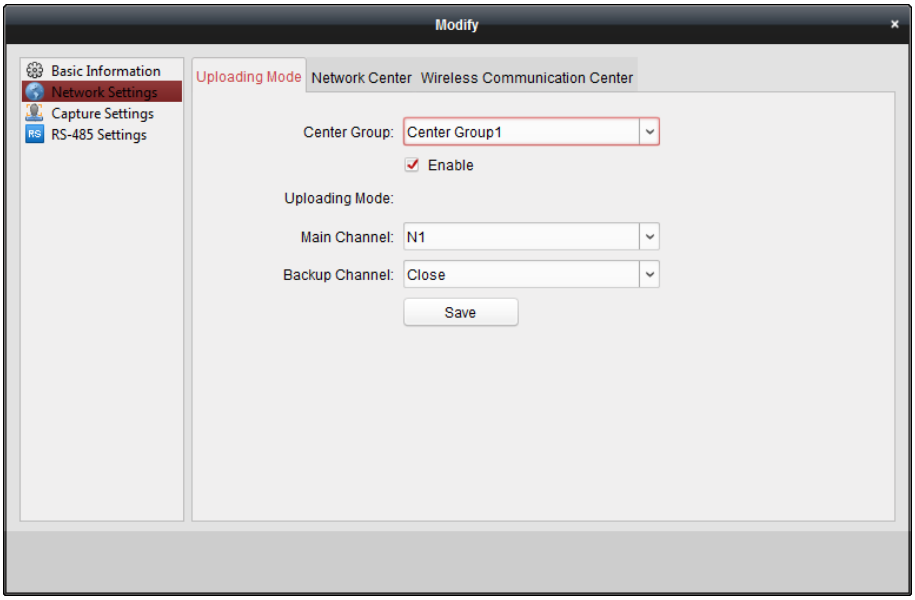
Uploading Mode Settings

Purpose：

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

Steps:

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



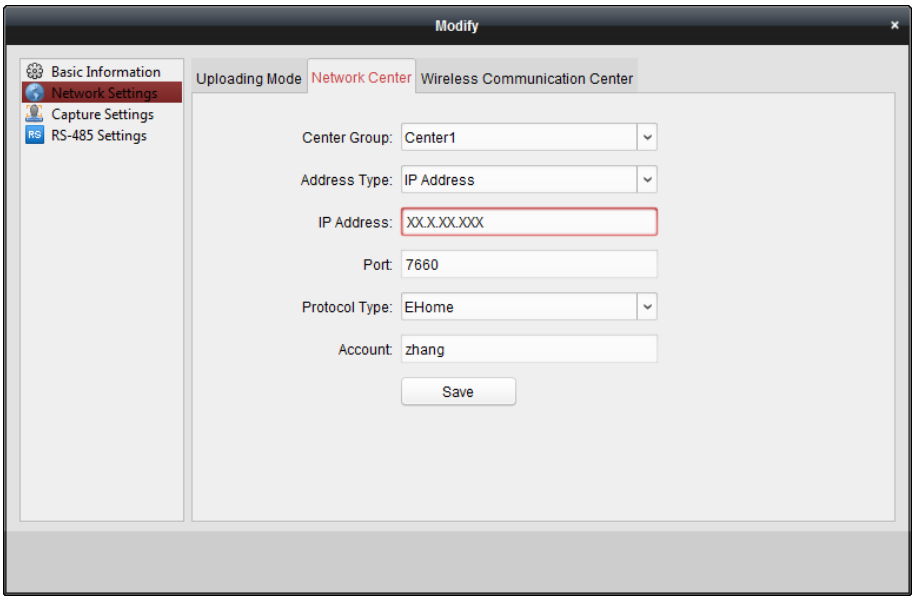
2. Select the center group in the dropdown list.
3. Check the **Enable** checkbox to enable the selected center group.
4. Select the uploading mode in the dropdown list. You can enable **N1/G1** for the main channel and the backup channel, or select **Close** to disable the main channel or the backup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

Network Center Settings

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

Steps:

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



2. Select the center group in the dropdown list.
3. Select the Address Type as **IP Address** or **Domain Name.**

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

Notes:

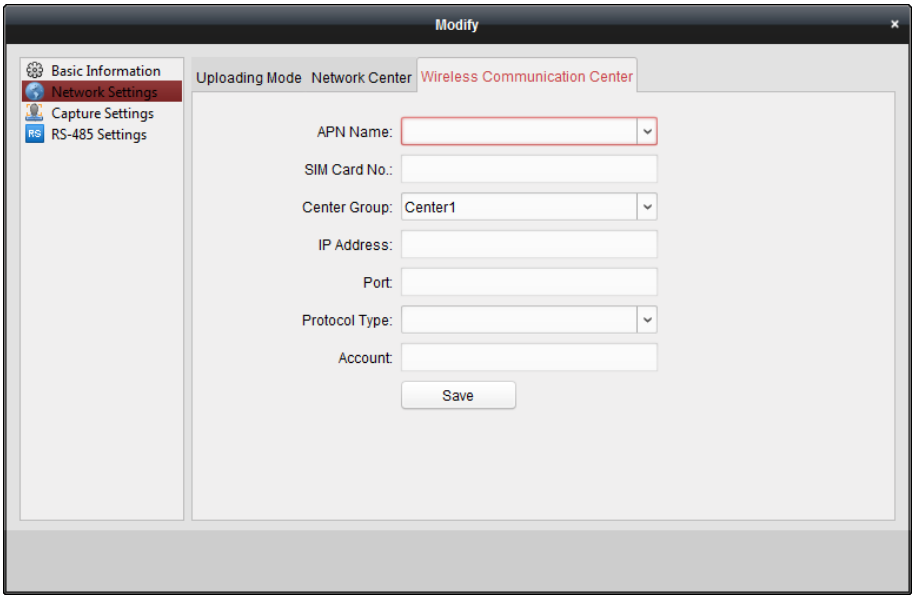
The port No. of the wireless network and wired network should be consistent with the port No. of EHome.

You can set the domain name in Enable NTP area *Editing Time* section in Remote Configuration. For details, refer to *Time* in *7.4.7 Remote Configuration*.

Wireless Communication Center Settings

Steps:

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



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

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

7.4.5 Capture Settings

You can set the parameters of capture linkage and manual capture.

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

Click **Capture Settings** tab to enter the capture settings interface.

Notes:

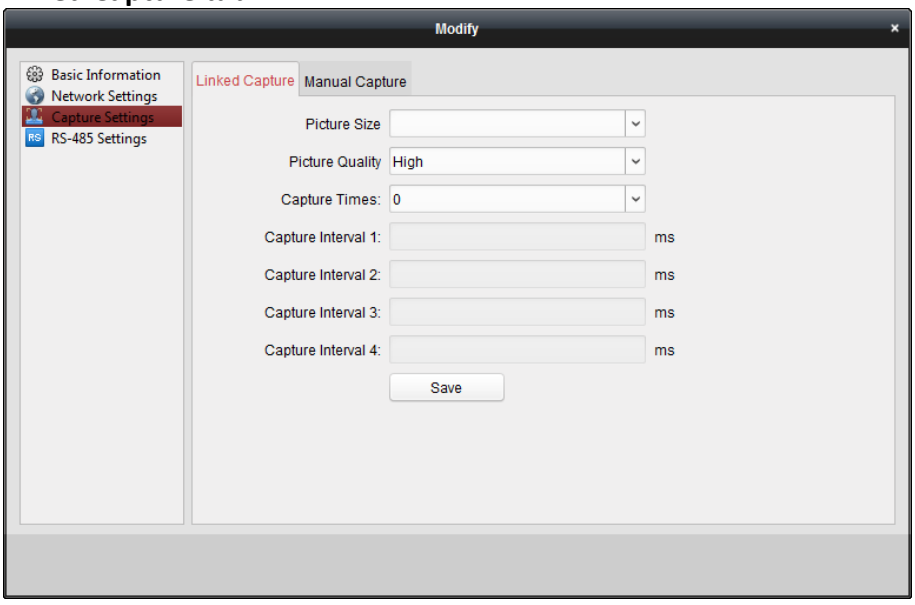
The **Capture Settings** should be supported by the device.

Before setting the capture setting, you should configure the storage server for picture storage.

Linked Capture

Steps:

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

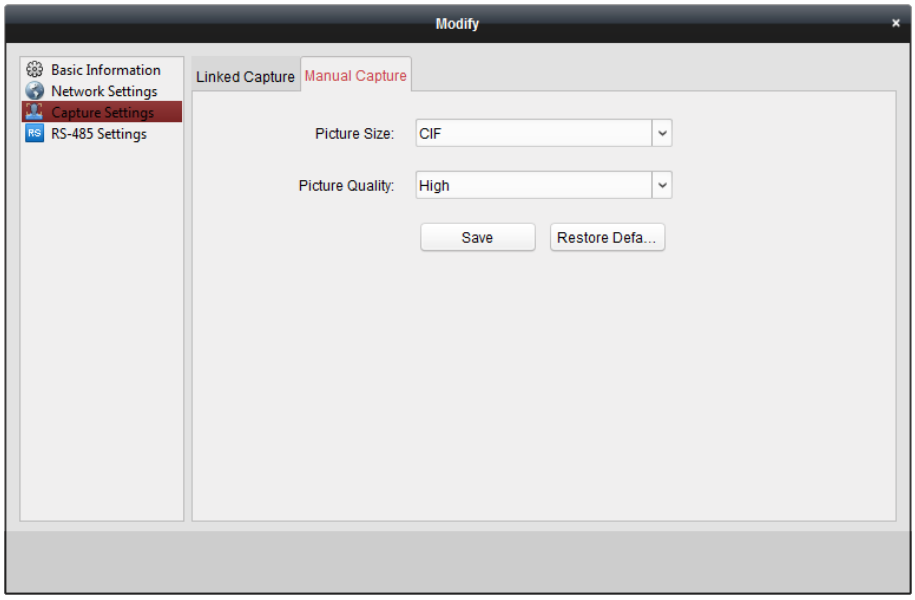


2. Set the picture size and quality.
3. Set the linked capture times once triggered.
4. Set the capture interval according to the capture times.
5. Click **Save** to save the settings.

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.

7. 4. 6 RS-485 Settings

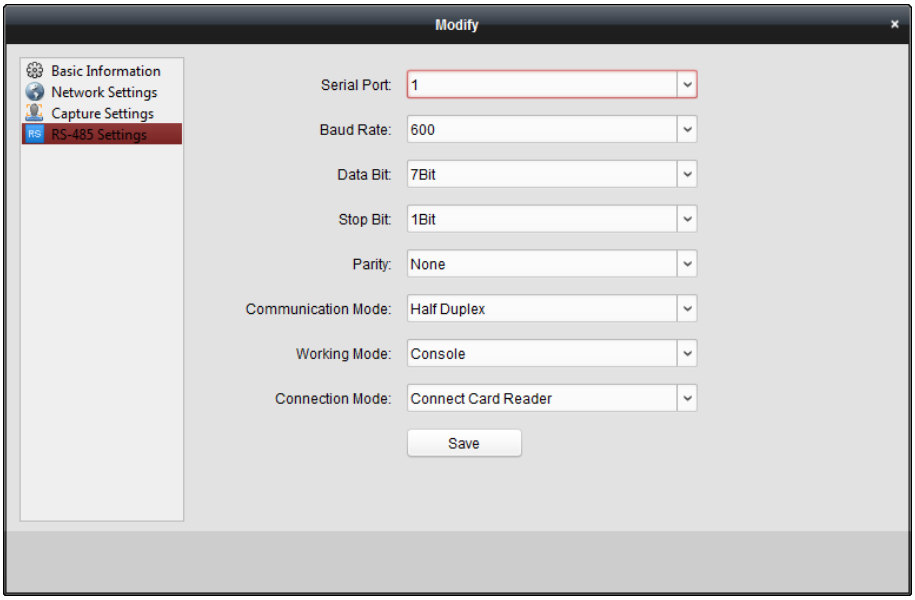
Purpose:

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

7. 4. 7 Remote Configuration

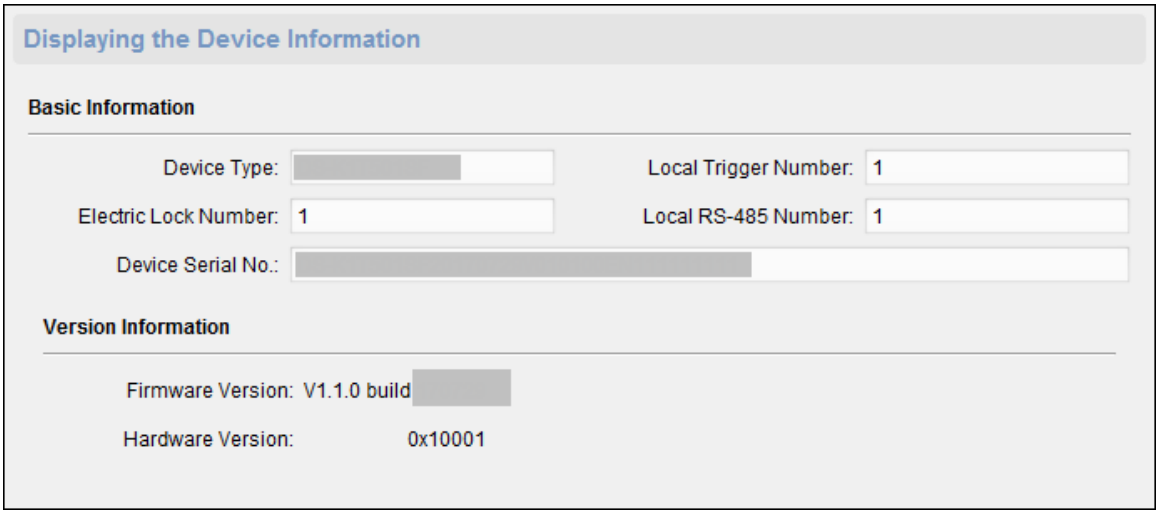
Purpose:

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

Checking Device Information

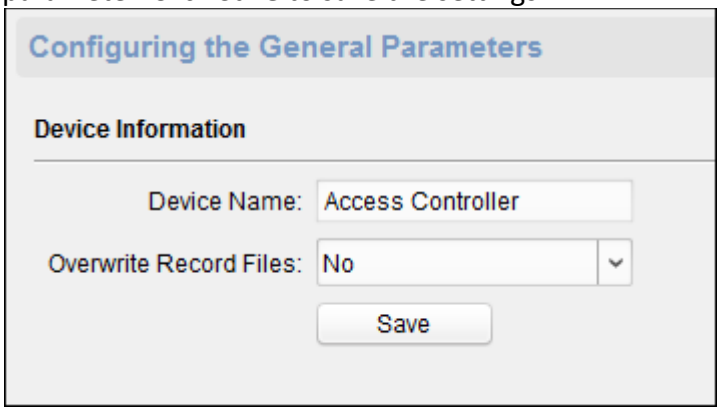
Steps:

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



Editing Device Name

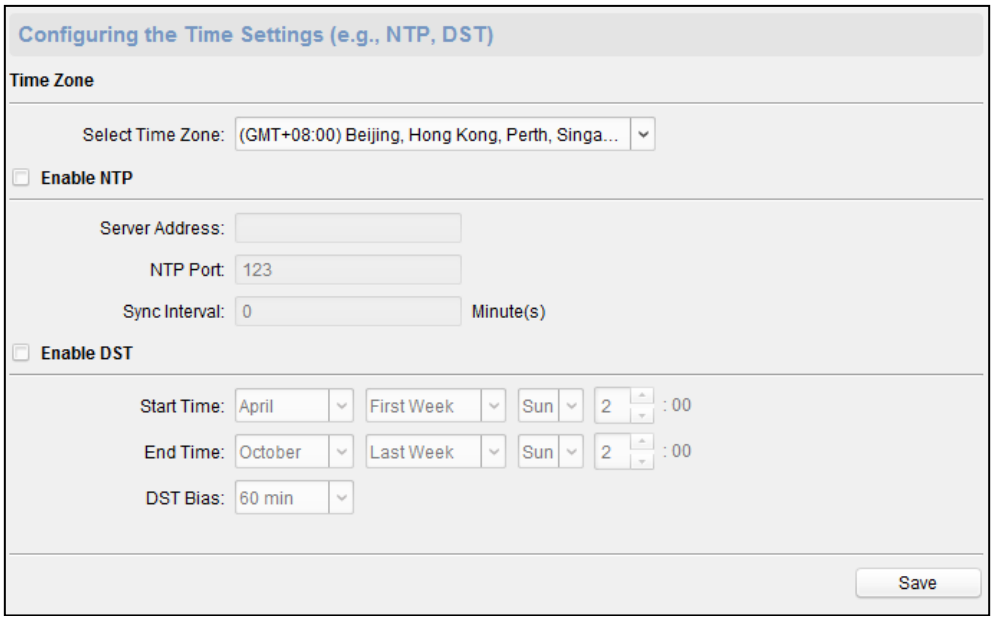
In the Remote Configuration interface, click **System** -> **General** to configure the device name and overwrite record files parameter. Click **Save** to save the settings.



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.



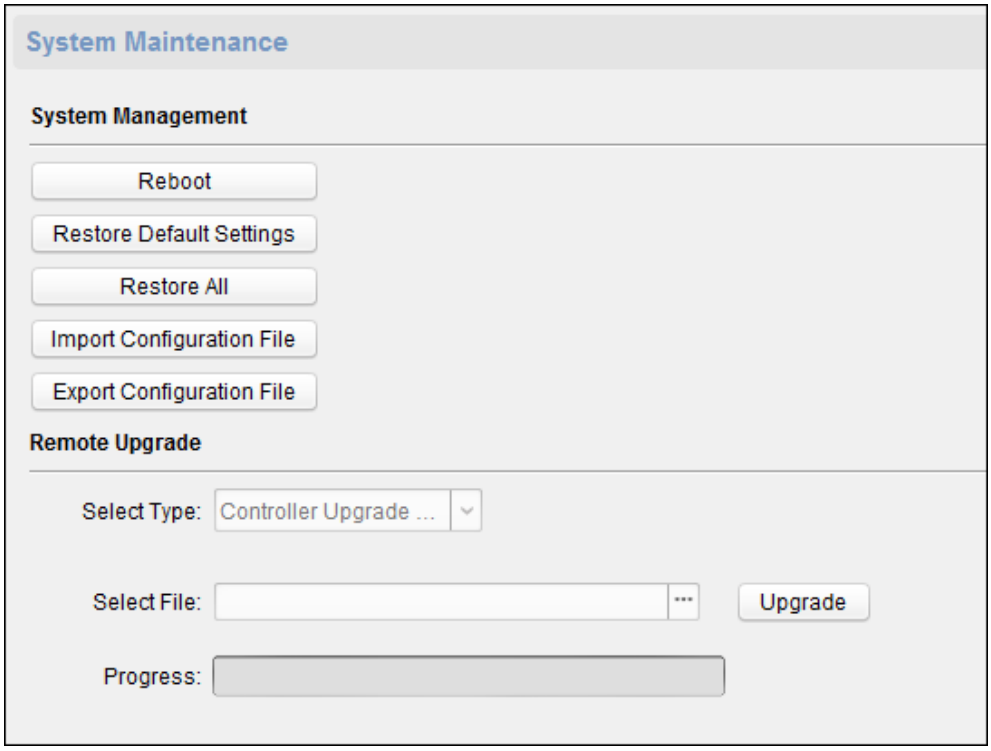
Setting System Maintenance

Purpose:

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

Steps:

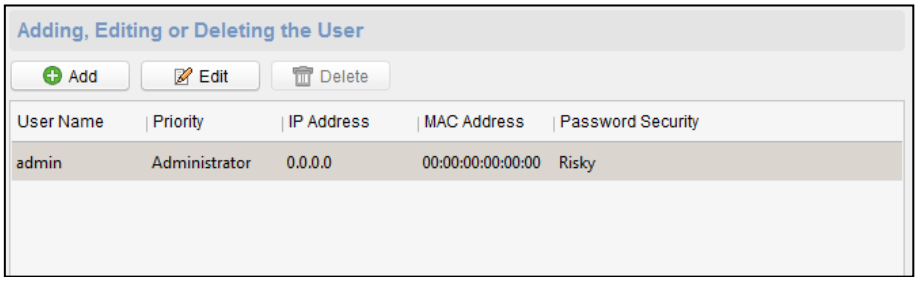
1. In the Remote Configuration interface, click **System** -> **System Maintenance**.
2. Click **Reboot** to reboot the device.
   Or click **Restore Default Settings** to restore the device settings to the default ones, excluding the IP address.
   Or click **Restore All** to restore the device parameters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



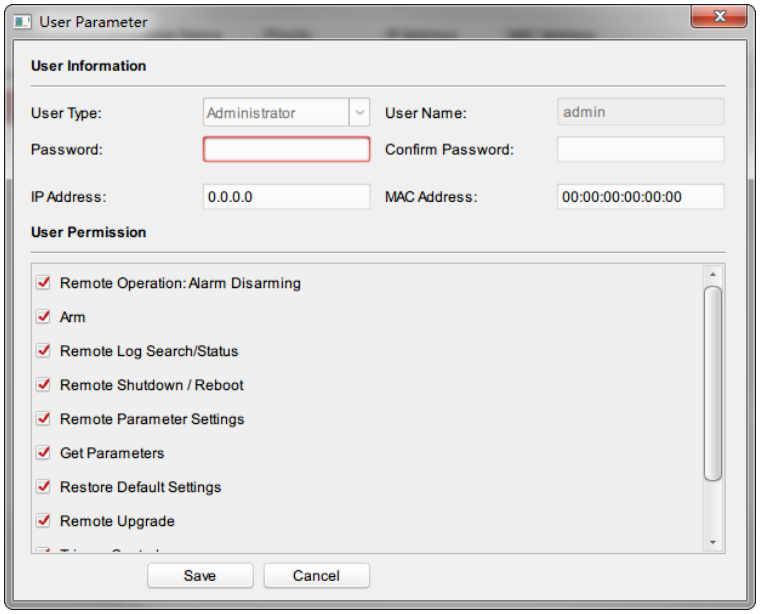
Managing User

Steps:

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



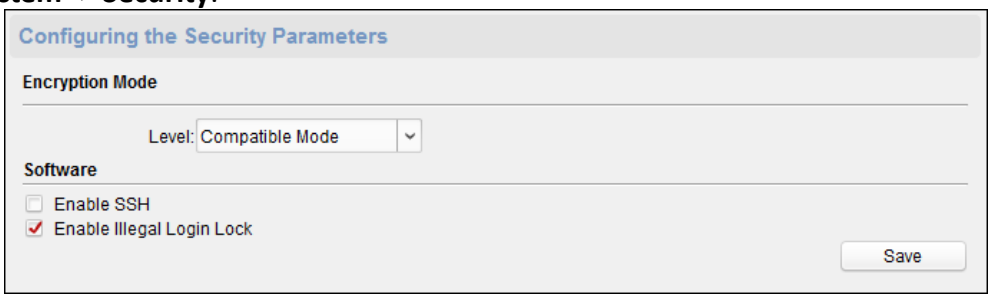
2. Click **Add** to add the user (Do not support by the elevator controller.).
   Or select a user in the user list and click **Edit** to edit the user. You are able to edit the user password, the IP address, the MAC address and the user permission. Cilck **OK** to confirm editing.



Setting Security

Steps:

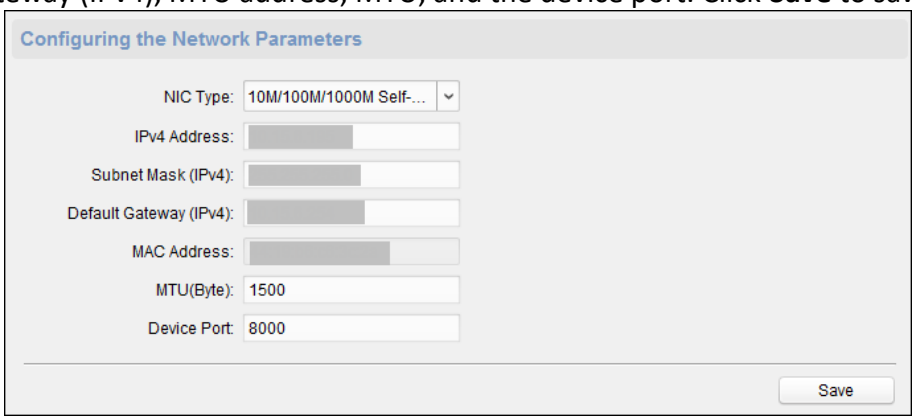
1. Click **System** -> **Security**.



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.



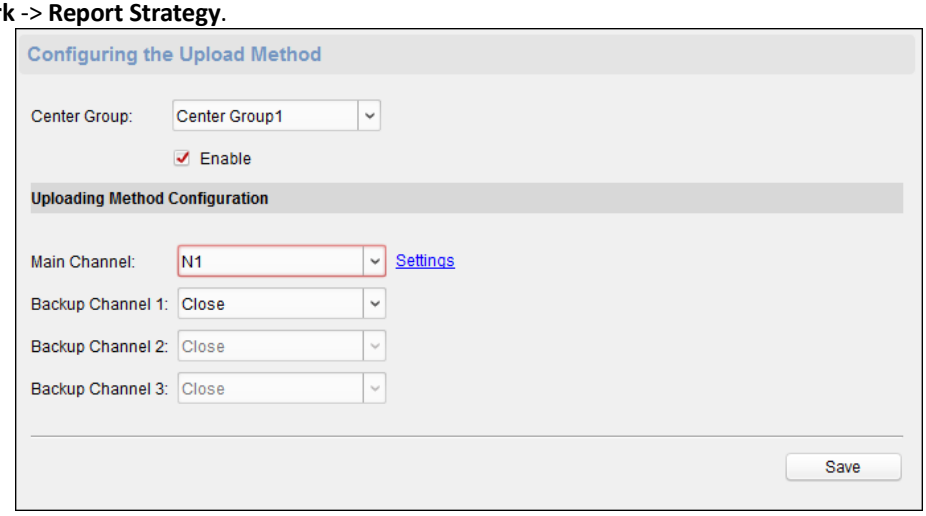
Configuring Upload Method

Purpose：

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

Steps:

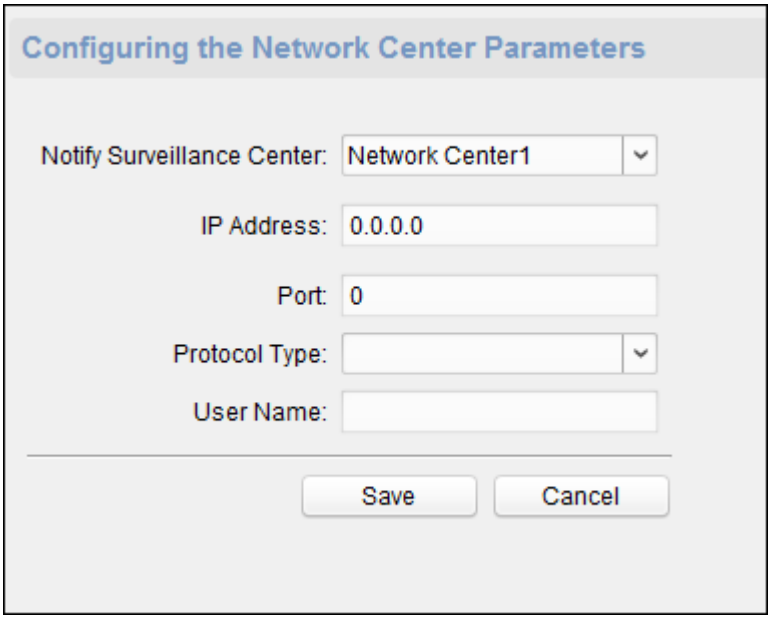
1. Click **Network** -> **Report Strategy**.



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.

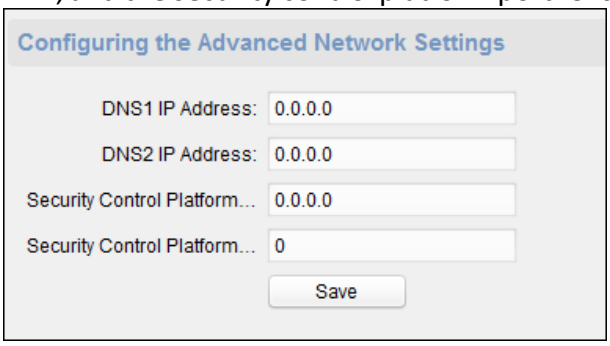
Configuring Network Center

You can set the notify 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 7.4.4 Network Settings.* Click **Save** to save the settings or click



Configuring Advanced Network

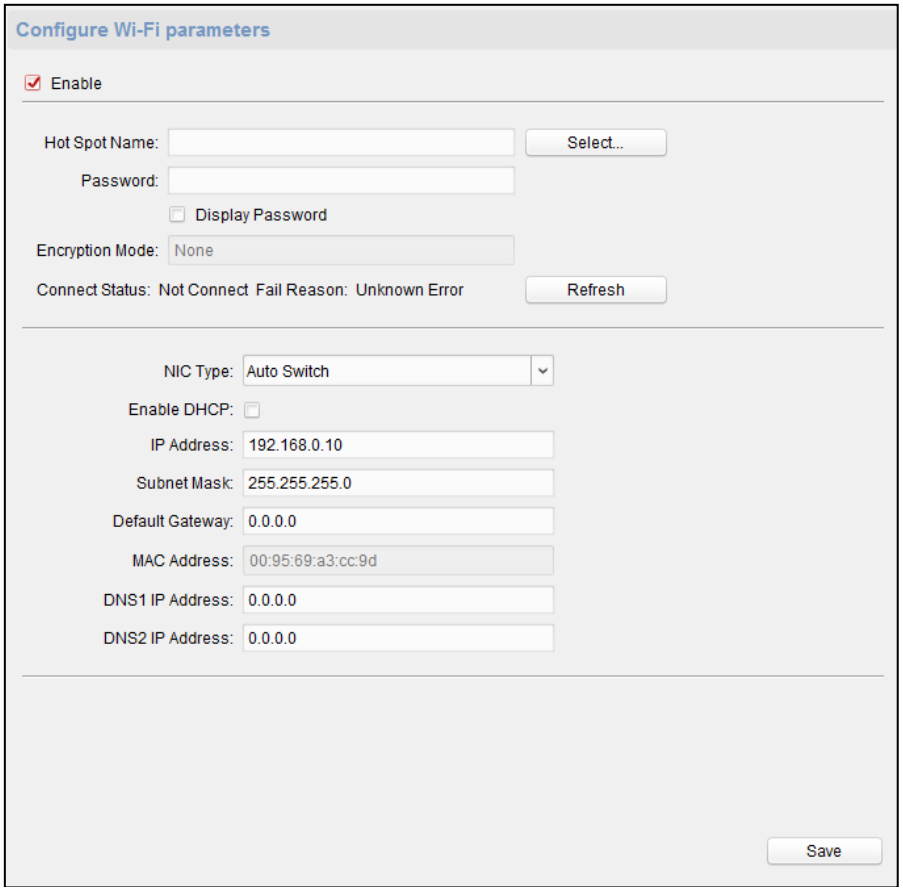
Click **Network** -> **Advanced Settings**. You can configure the DNS IP address 1, the DNS IP address 2, the security control platform IP, and the security control platform port. Click **Save** to save the settings.



Configuring Wi-Fi

Steps:

1. Click **Network** –> **Wi-Fi**.



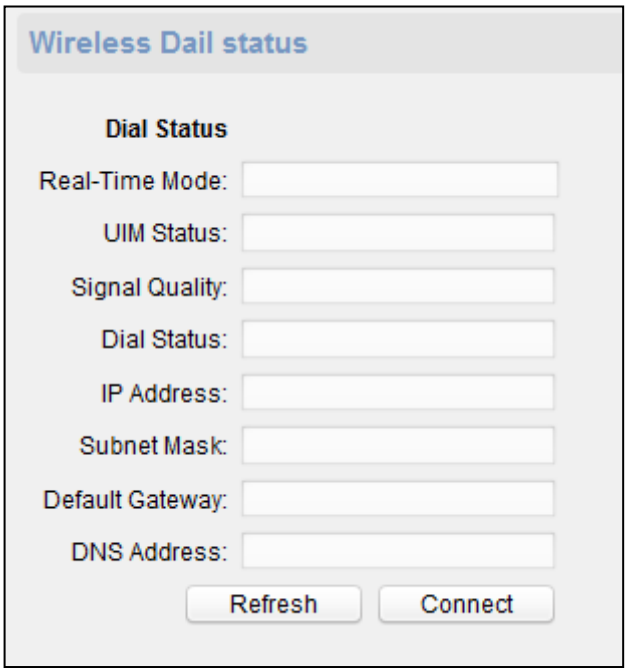
2. Check **Enable** to enable the Wi-Fi function.
3. Input the hot spot name.
   Or you can click **Select…** to select a network.
4. Input the Wi-Fi password.
5. (Optional) Click **Refresh** to refresh the network status.
6. (Optional) Select the NIC Type.

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 Wireless Dail Status

Steps:

1. Click **Network** -> **Wireless Dial**.

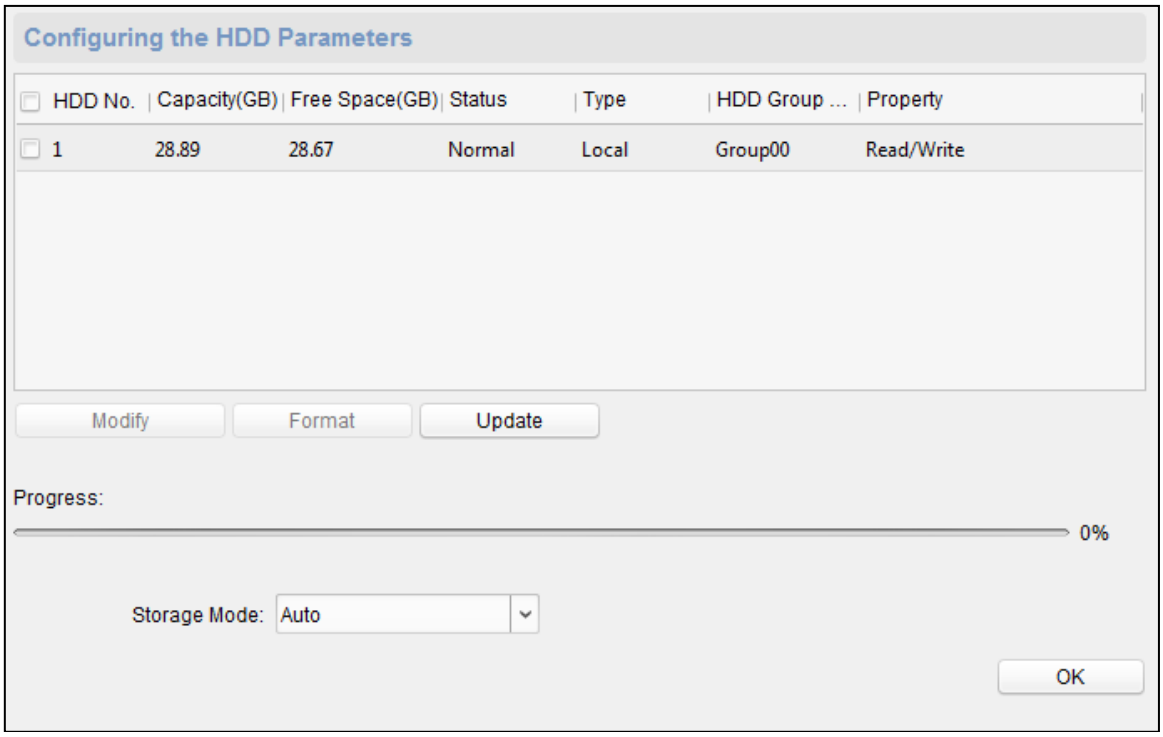


2. Edit the dial status, including the real-time mode, the UIM status, the signal quality, the dial status, the IP address, the subnet mask the default gateway and the DNS address.
3. Click **Conenct** to start connecting.
   Or click **Refresh** to refresh the status.

Configuring HDD Parameters

Steps:

1. Click **Storage** -> **General**.

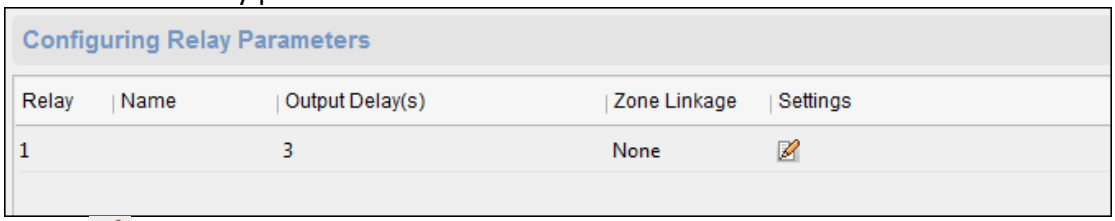


2. Check the HDD (SD card) No., capacity, the free space, the status and so on.
   You can also edit and format the HDD (SD card). Or click **Update** to refresh the data.
3. Select the storage mode.
4. Click **Save** to save the settings.

Configuring Relay Parameters

Steps:

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

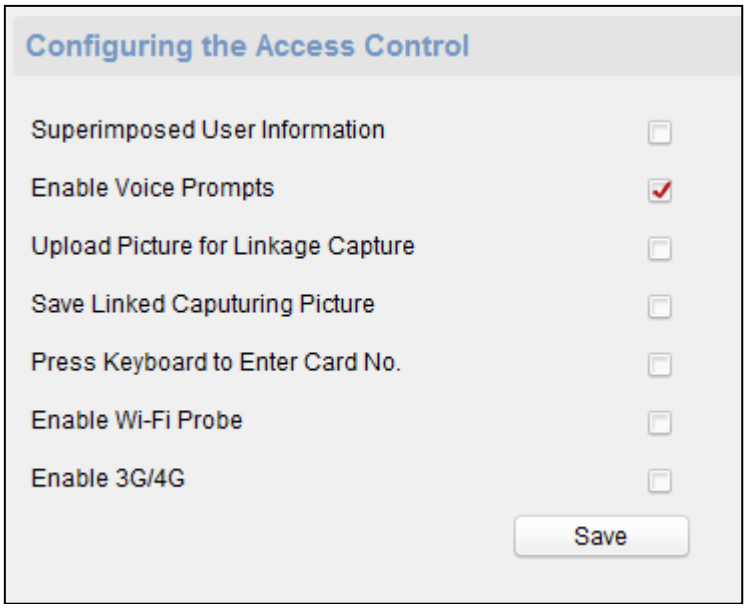


2. Click the  to pop up the Relay Parameters Settings window.
3. Set the relay name and the output delay.
4. Click **Save** to save the paramters.
   Or click **Copy to...** to copy the relay information to other relays.

Configuring Access Control Parameters

Steps:

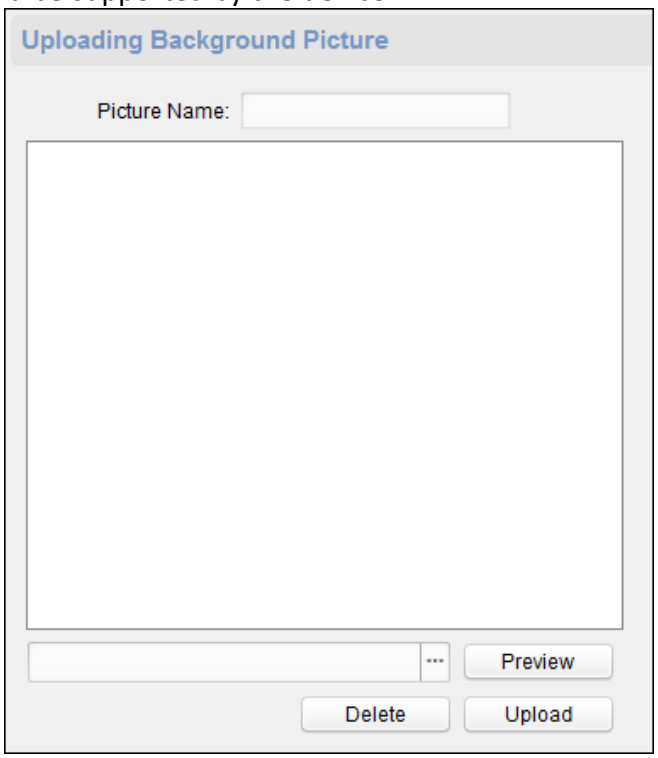
In the Remote Configuration interface, click **Other** -> **Access Control Parameters**. Check **Superimposed user information**, **Enable voice prompts**, **Upload picture to capture whether the linkage**, **Save Linked Captured Pictures**, **Whether to allow key input card number**, **Enable WiFi detect**, and **Enable 3G/4G**. Click **Save** to save the settings.



Uploading Background Picture

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

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.

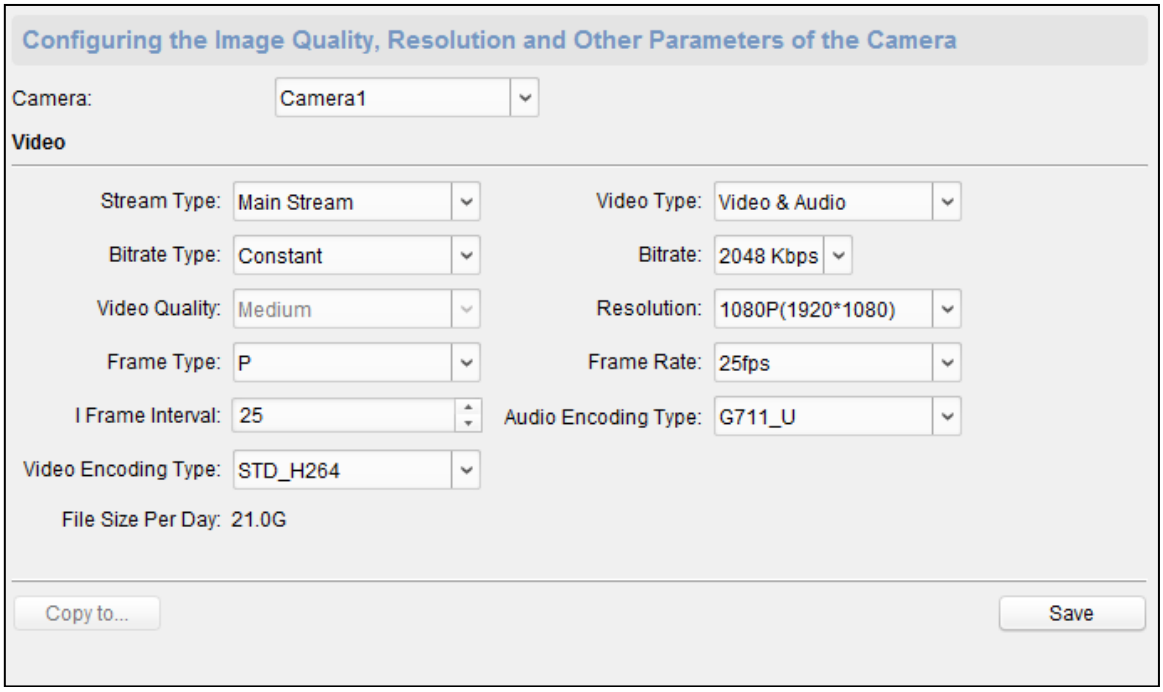
Note: Only devices with video function support this function.

Configuring Video and Audio Parameters

You can set the video compression parameters.

Steps:

1. Click **Image** -> **Video & Audio**.



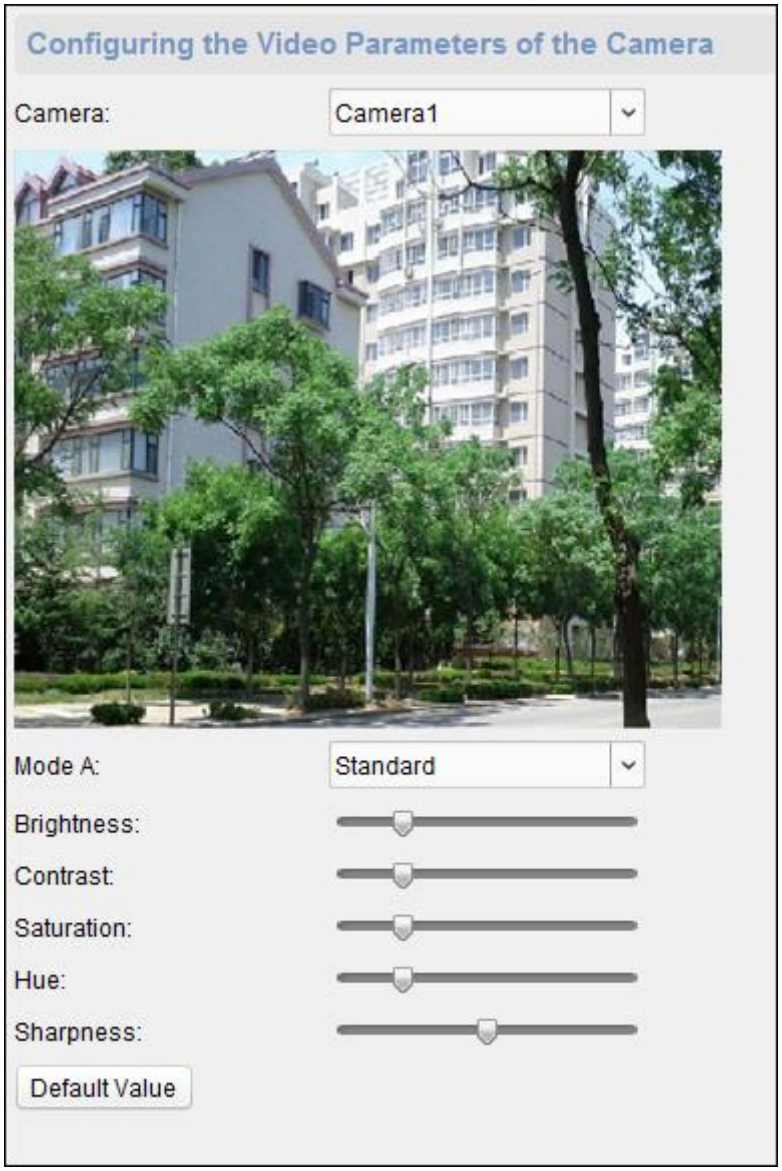
2. Select a camera in the drop-down list.
3. Set the camera video parameters, including the stream type, the bitrate type, the video quality, the frame type , the I frame type, the video encoding type, the video type, the bitrate, the resolution, the frame rate and the audio encoding type.
4. Click **Save** to save the settings.
   Or click **Copy to…** to copy the parameters to other cameras.

Configuring Video Image Parameters

You can set the camera mode, brightness, contrast, saturation, hue, and sharpness.

Steps:

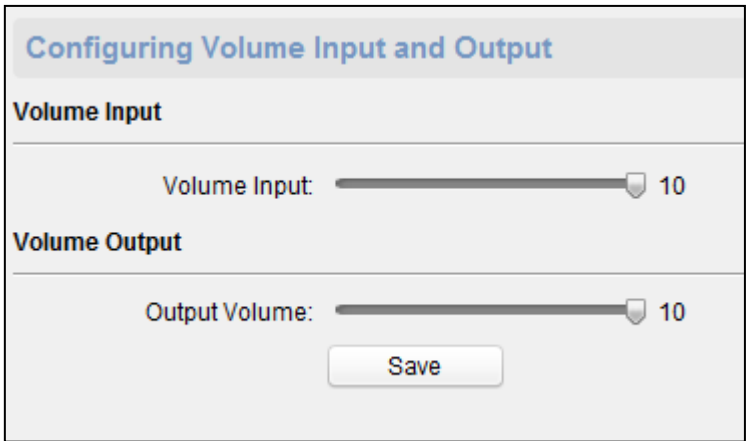
1. Click **Image** -> **Image Settings**.



2. Select a camera in the dropdown list.
3. Set the camera mode, brightness, contrast, saturation, hue, and sharpness.
   Or click **Default Value** to set the parameters to the default values.

Configuring Volume Input and Output

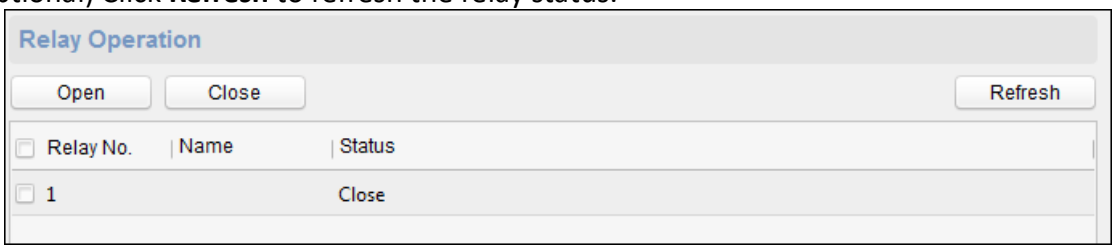
Click **Image** -> **Volume Input/Output**. You can set the volume input and output. Click **Save** to save the settings.



Operating Relay

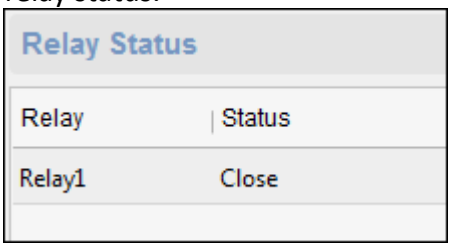
Steps:

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



Viewing Relay Status

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



7.5 Organization Management

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

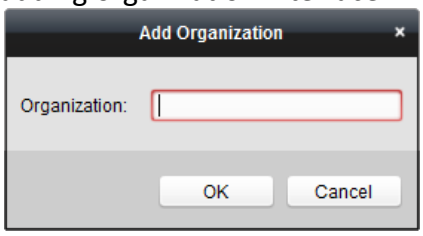
Click  tab to enter the Person and Card Management interface.

7. 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.

7.5.2 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.

7.6 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.

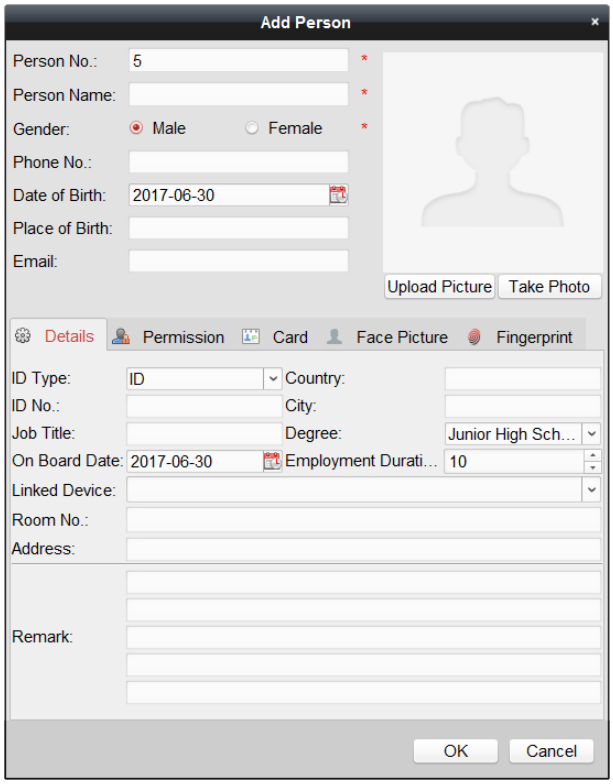
Note: Up to 10,000 persons or cards can be added.

7.6.1 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.

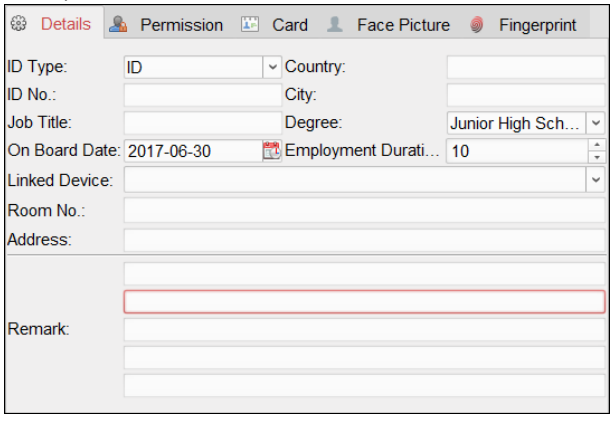


2. The Person No. will be generated automatically and is not editable.
3. Input the basic information including person name, phone No., birthday details, and email address.
4. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
   Note: The picture should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

Adding Person (Detailed Information)

Steps:

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



2. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.

   Linked Device: You can bind the indoor station to the person.

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

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

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

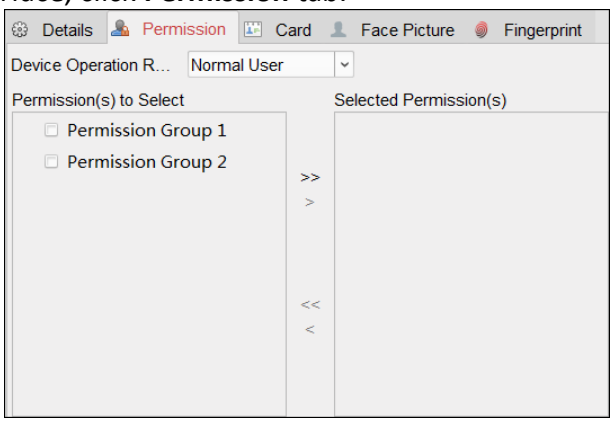
Adding Person (Permission)

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

Note: For setting the access control permission, refer to *Chapter 7.8 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.

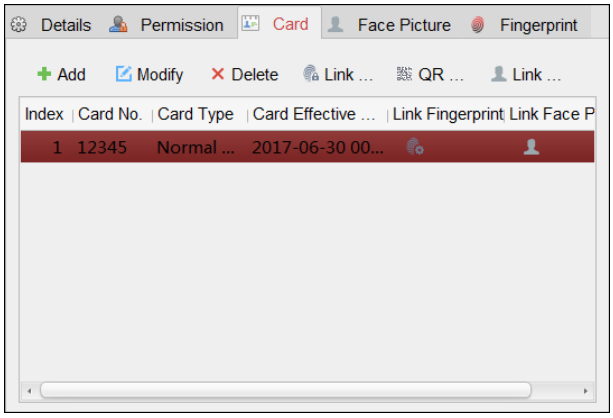
4. Click **OK** to save the settings.

Adding Person (Card)

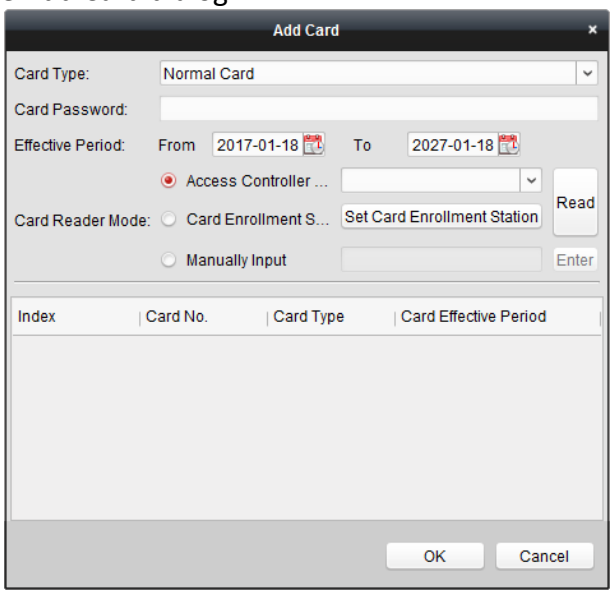
You can add card and issue the card to the person.

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 Door Extended Opening: The door will remain open for the configured time period for the card holder.

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

   Patrol Card: The card swiping action can used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.

   Duress Card: The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.

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

   Visitor Card: The card is assigned for visitors. For the Visitor Card, you can set the **Max. Swipe Times**.

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

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

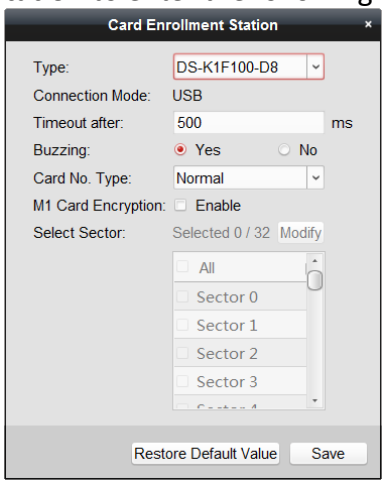
Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to *Chapter 7.9.2 Card 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.
   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.

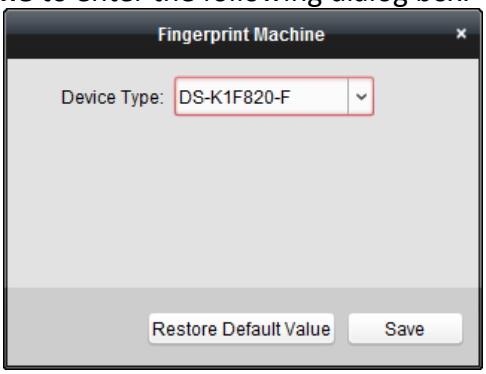
12. Click **OK** to save the settings.

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 DS-K1F820-F as the device type.
   2) 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.

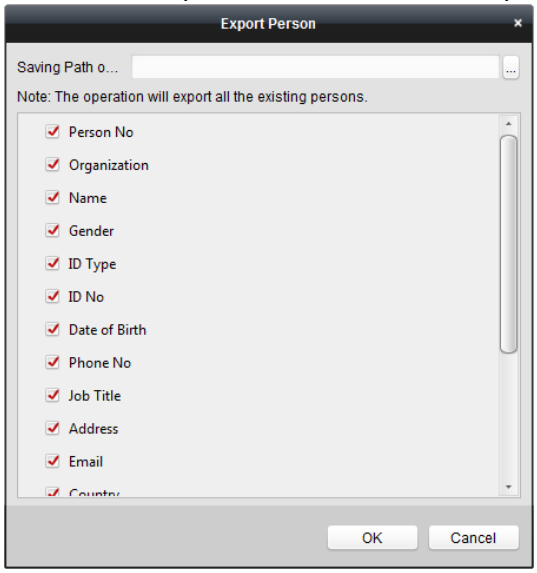
4. Click **Start** button, click to select the fingerprint to start collecting.
5. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.
6. (Optional) You can also click **Remote Collection** to collect fingerprint from the device.
   Note: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

Importing and Exporting Person Information

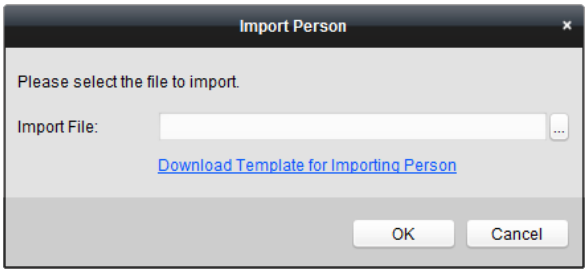
The person information can be imported and exported in batch.

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.

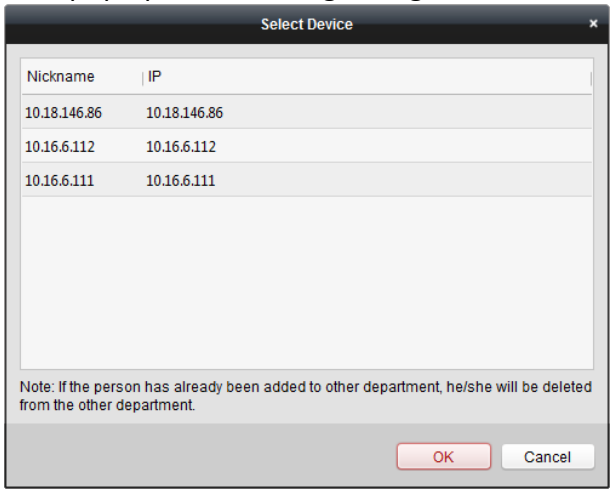
Getting Person Information from Access Control Device

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.
Up to 10000 persons can be imported.

7.6.2 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.

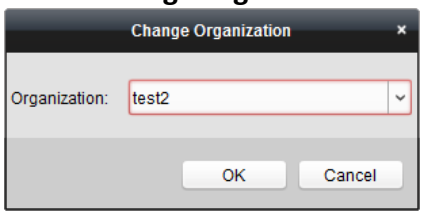
Note: If a card is issued to the current person, the linkage will be invalid after the person is deleted.

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.

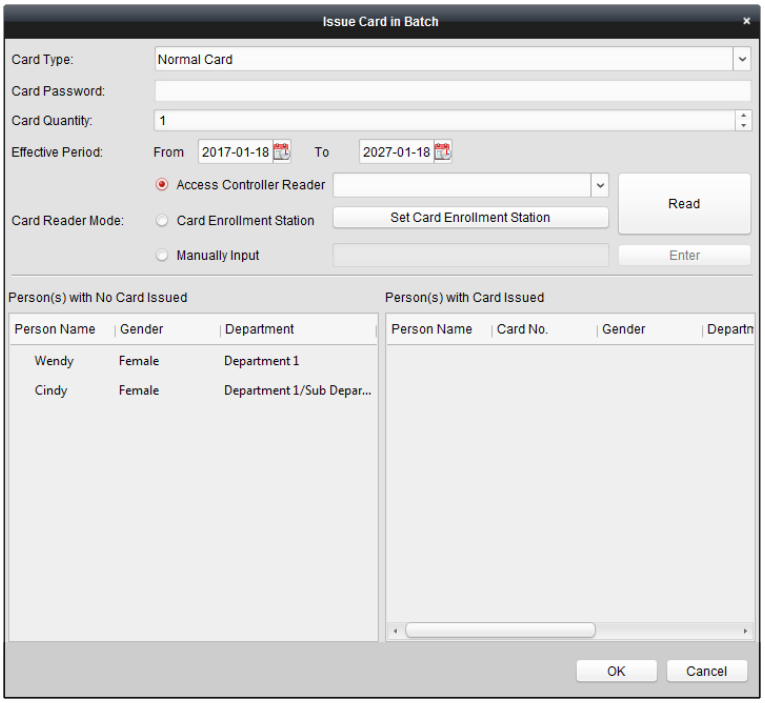
You can click **Set Card Enrollment Station** in the dropdown list to set the parameters.

7. 6. 3 Issuing Card in Batch

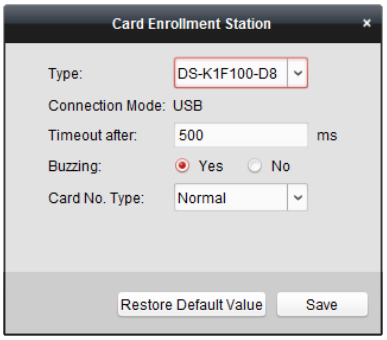
You can issue multiple cards for the person with no card issued in batch.

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 7.9.2 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 and Department column to sort the persons according to actual needs.
7. Select the Card Reader Mode for reading the card No.
   Access Controller Reader: Place the card on the reader of the Access Controller and click **Read** to get the card No.
   Card Enrollment Station: Place the card on the Card Enrollment Station and click **Read** to get the card No.
   Note: The Card Enrollment Station should connect with the PC running the client. You can click **Set Card Enrollment Station** to enter the following dialog.



1) Select the Card Enrollment Station type.
   Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.
2) Set the parameters about the connected card enrollment station.
3) Click **Save** button to save the settings.
   You can click **Restore Default Value** button to restore the defaults.

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

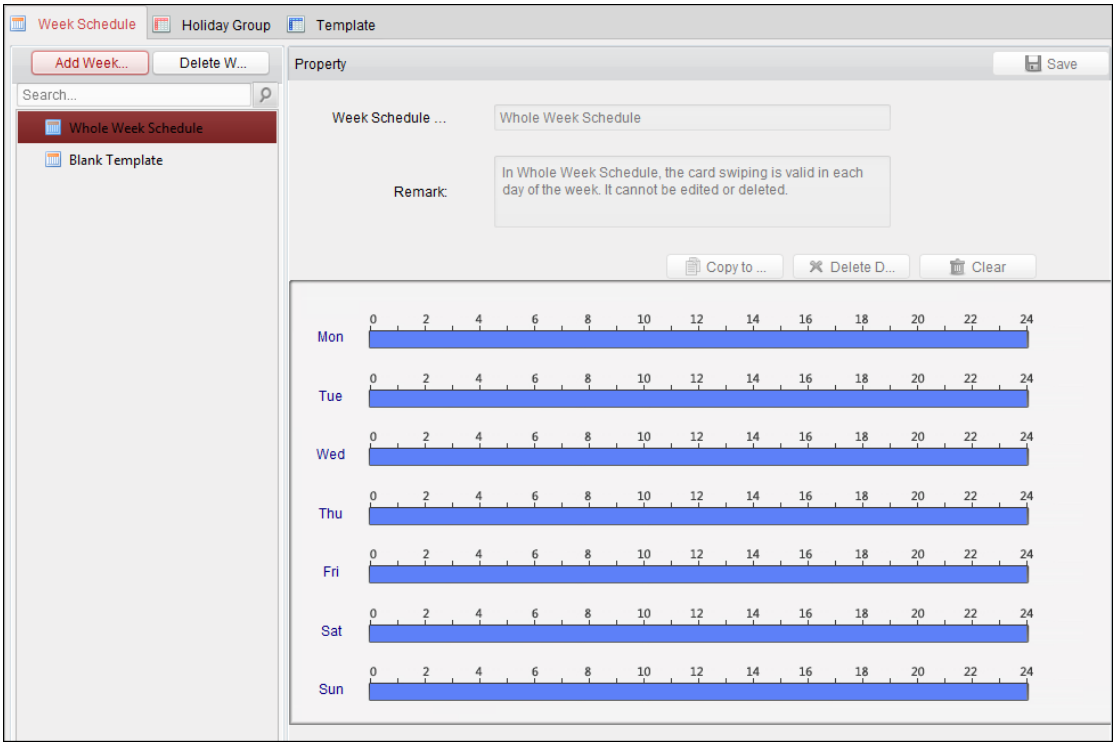
8. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.
9. Click **OK** to save the settings.

7.7 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 7.8 Permission Configuration.*

7.7.1 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.

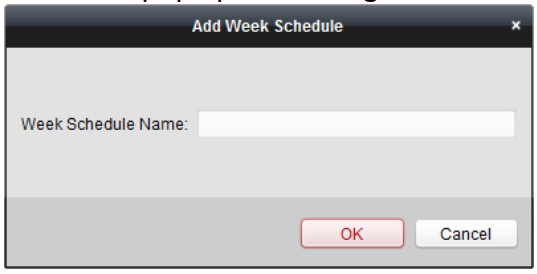
Whole Week Schedule: Card swiping is valid on each day of the week.

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

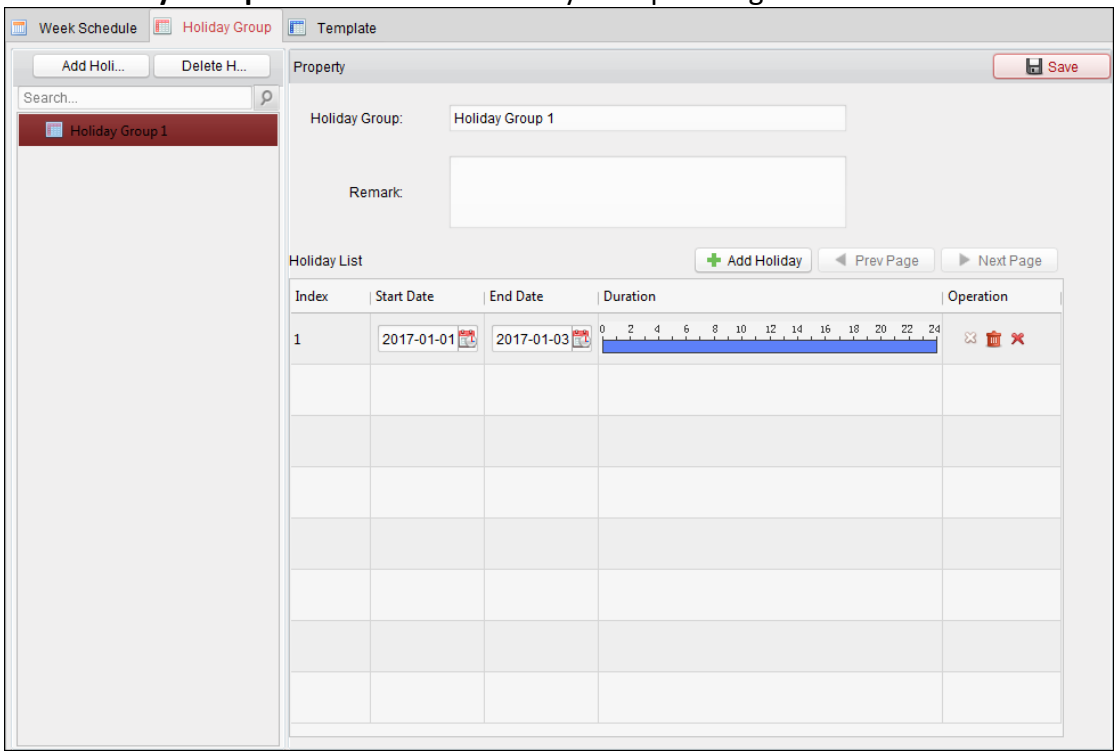
period of time, the configured permission is activated.

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.

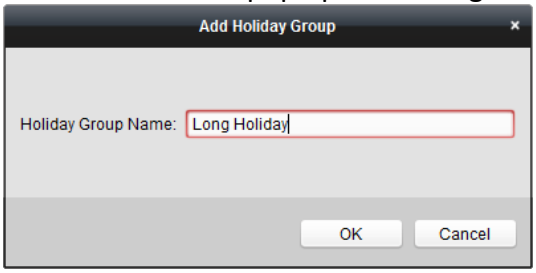
7. 7. 2 Holiday Group

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



Steps:

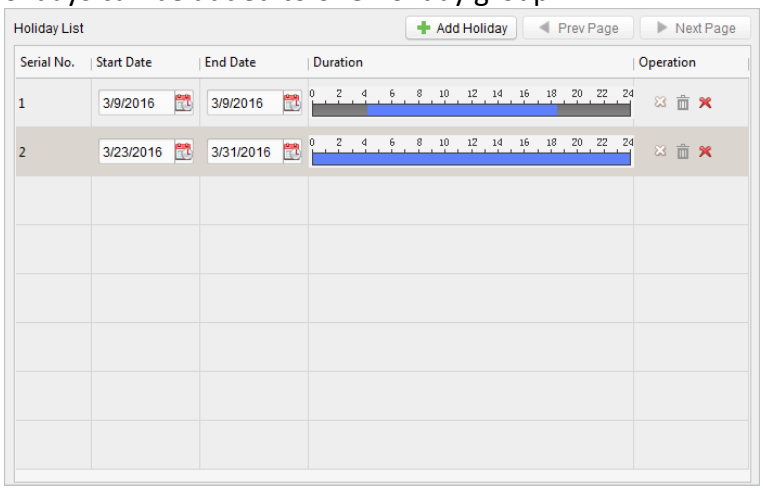
1. Click **Add Holiday Group** button on the left to pop up the adding holiday group interface.



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.

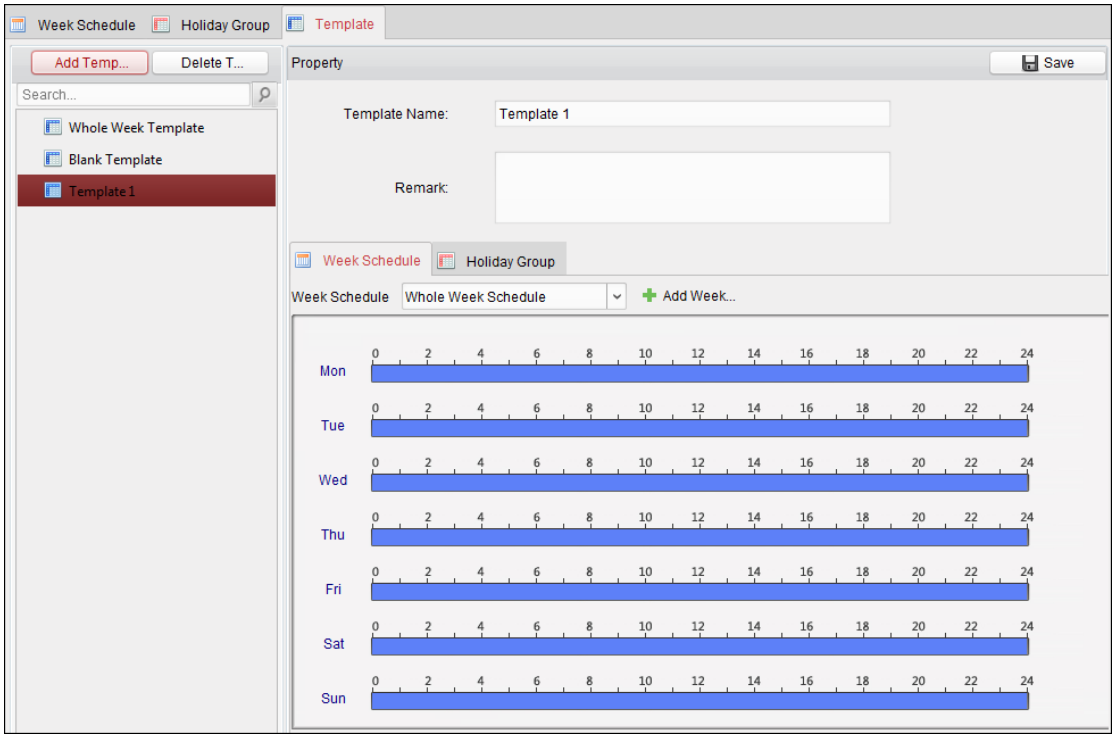
Note: The holidays cannot be overlapped with each other.

7.7.3 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.

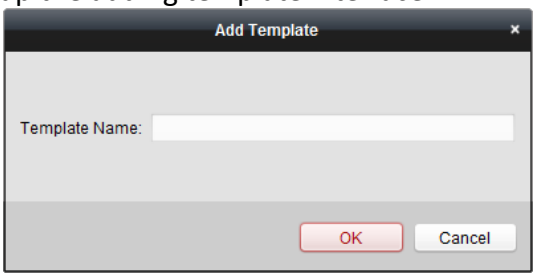
Whole Week Template: The card swiping is valid on each day of the week and it has no holiday group schedule.

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

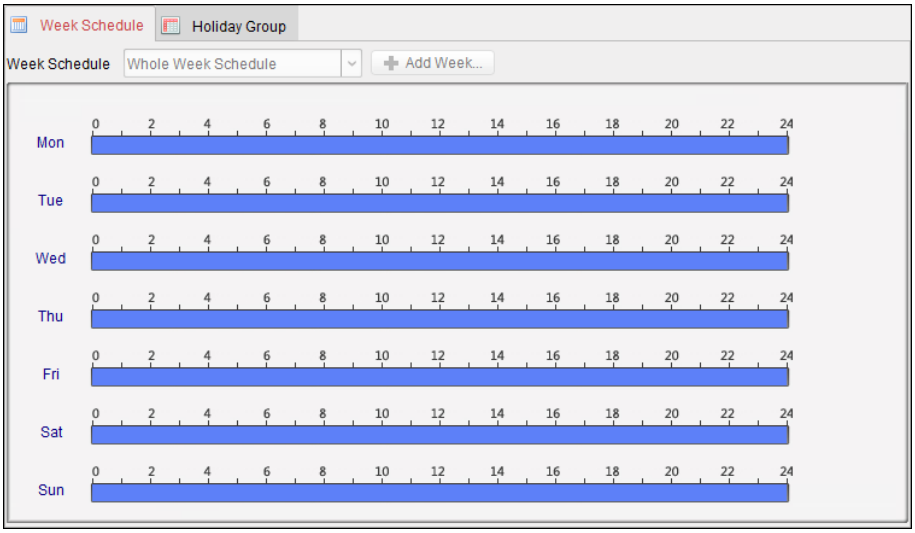
You can define custom templates on your demand.

Steps:

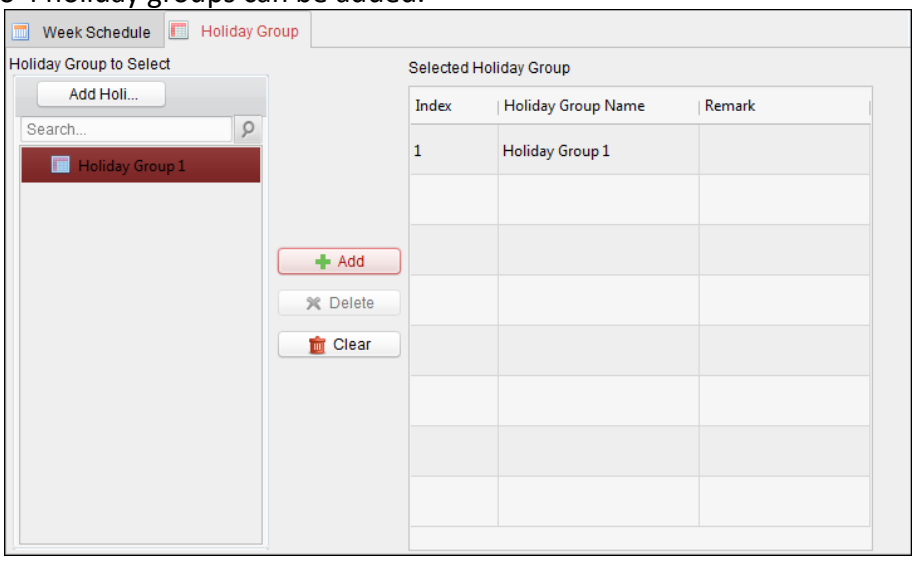
1. Click **Add Template** to pop up the adding template interface.



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 7.7.1 Week Schedule.*



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

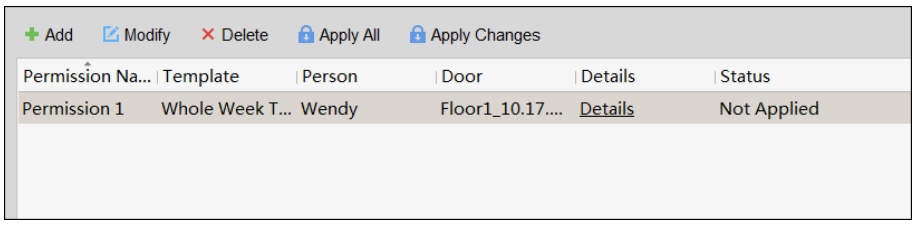


   Click to select a holiday group in the list and click **Add** to add it to the template. You can also click **Add Holiday Group** to add a new one. For details, refer to *Chapter 7.7.2 Holiday Group.*
   You can click to select an added holiday group in the right-side list and click **Delete** to delete it.
   You can click **Clear** to delete all the added holiday groups.
6. Click **Save** button to save the settings.

7.8 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.



7. 8. 1 Adding Permission

Purpose:

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

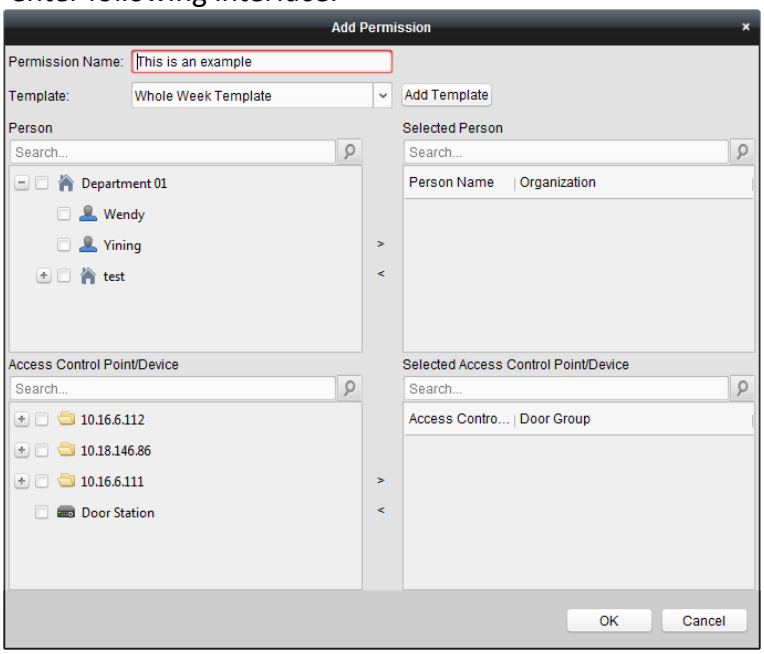
Notes:

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 7.7 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.

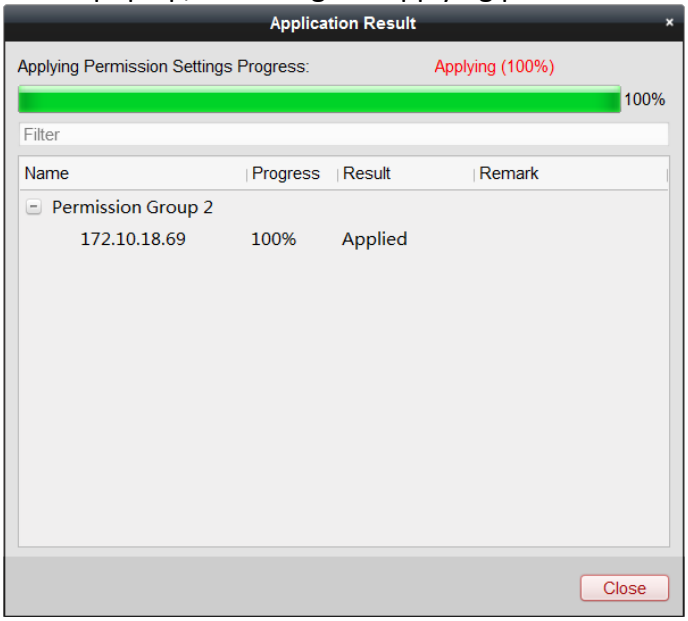
7. 8. 2 Applying Permission

Purpose:

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

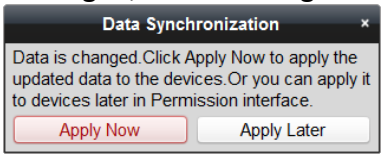
Steps:

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).

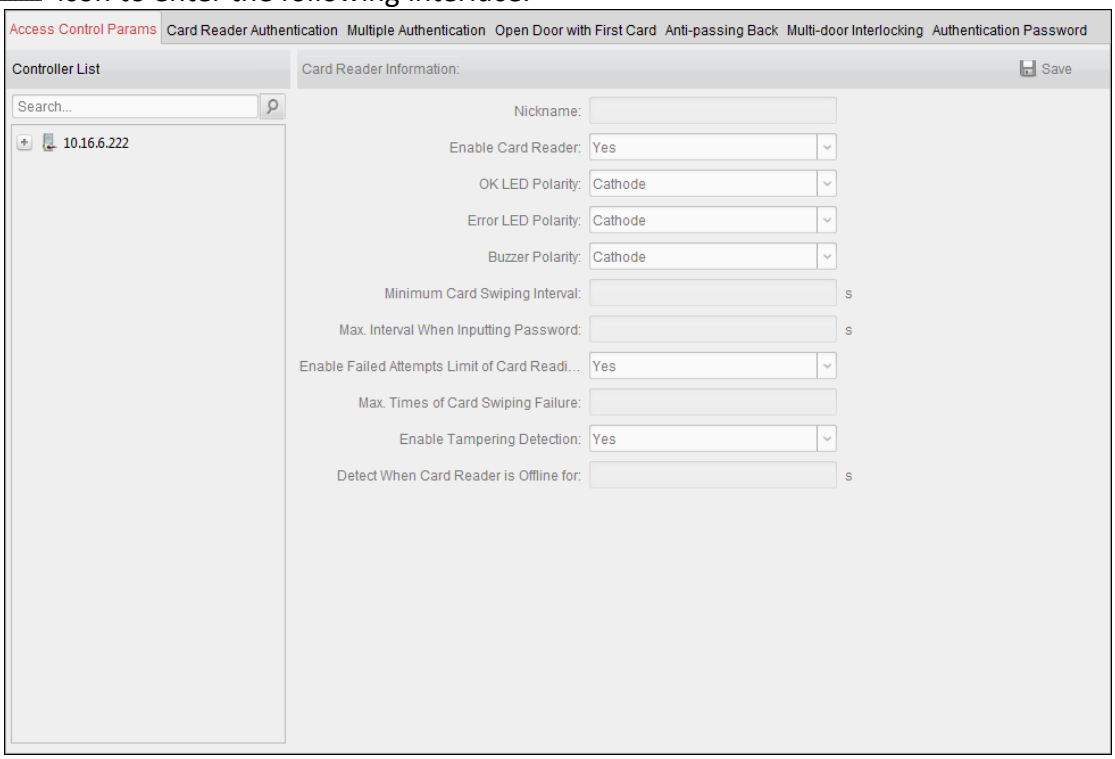
7.9 Advanced Functions

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.



7.9.1 Access Control Parameters

Purpose:

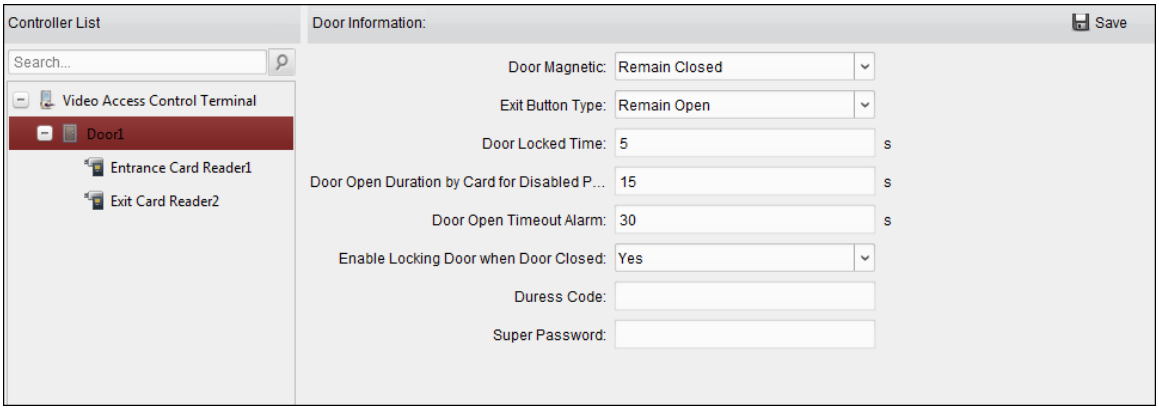
After adding the access control device, you can configure its access control point (door)'s parameters, and its card readers' parameters.

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 Door Extended Opening: The door magnetic can be enabled with appropriate delay after card holder swipes the card.

   Door Open Timeout Alarm: The alarm can be triggered if the door has not been close

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

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

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

   Notes:

   The duress code and Super password should be different.

   The duress code and the super password should be different from the authentication password.

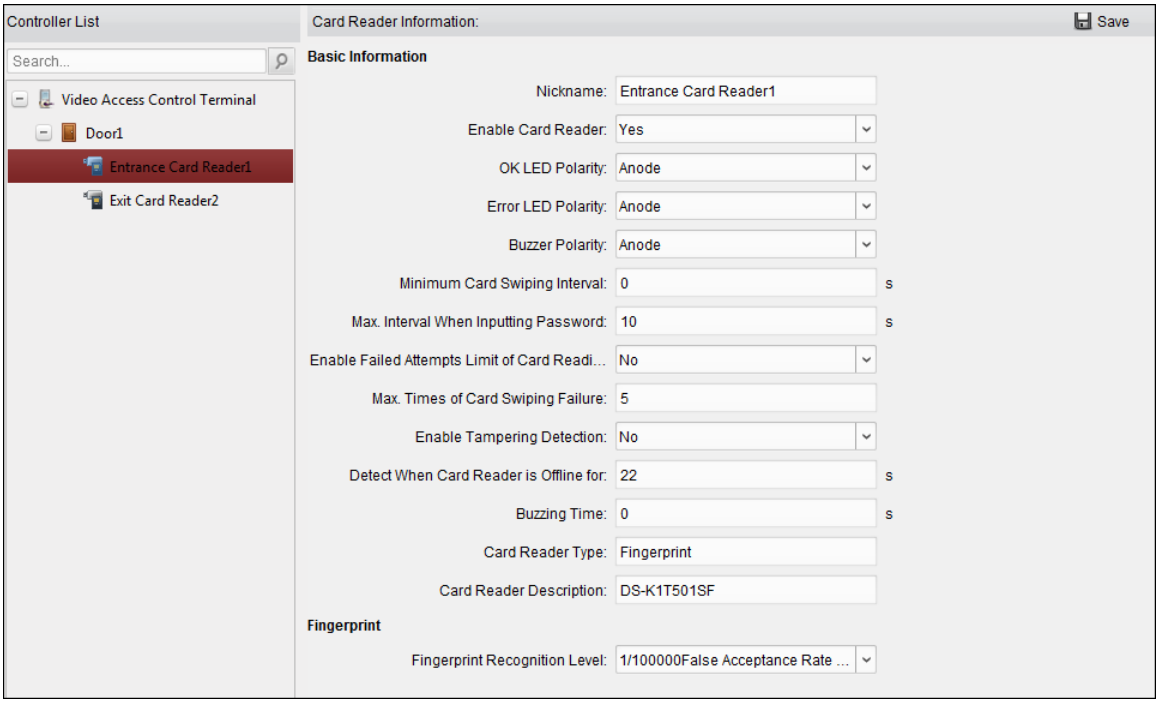
   The duress code and super password should contain 4 to 8 numerics.

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.

7.9.2 Card Reader Authentication

Purpose:

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

Steps:

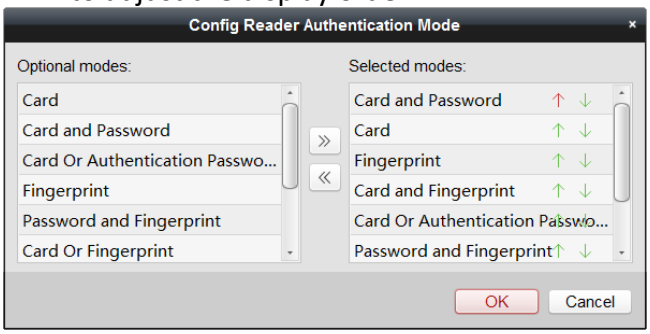
1. Click **Card Reader Authentication** tab and select a card reader on the left.
2. Click **Configuration** button to select the card reader authentication modes for setting the schedule.

   Notes:

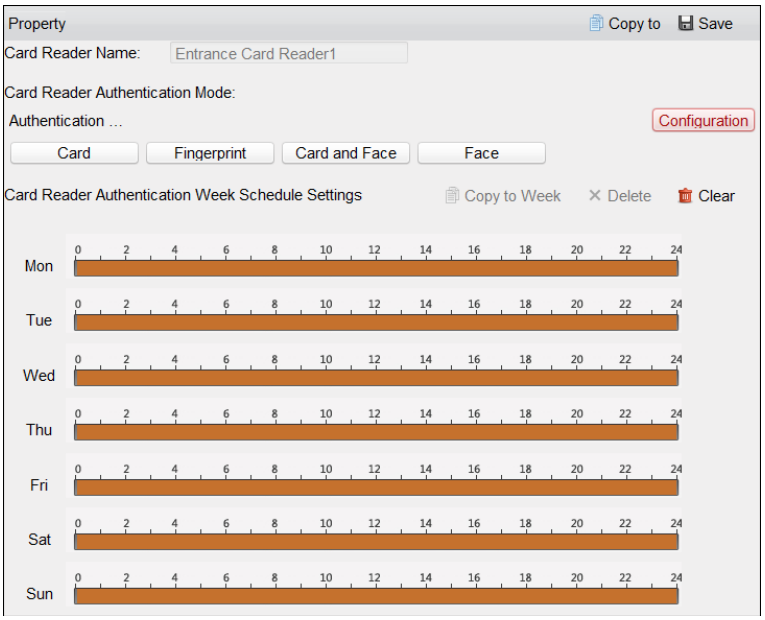
   The available authentication modes depend on the device type.

   Password refers to the card password set when issuing the card to the person in *Chapter 7.6 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.

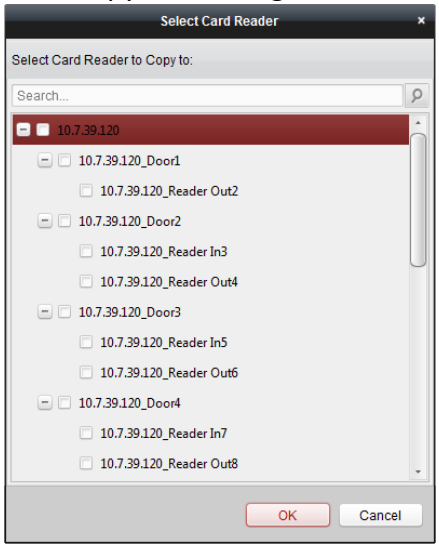


5. Repeat the above step to set other time periods.

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.

7.9.3 Multiple Authentication

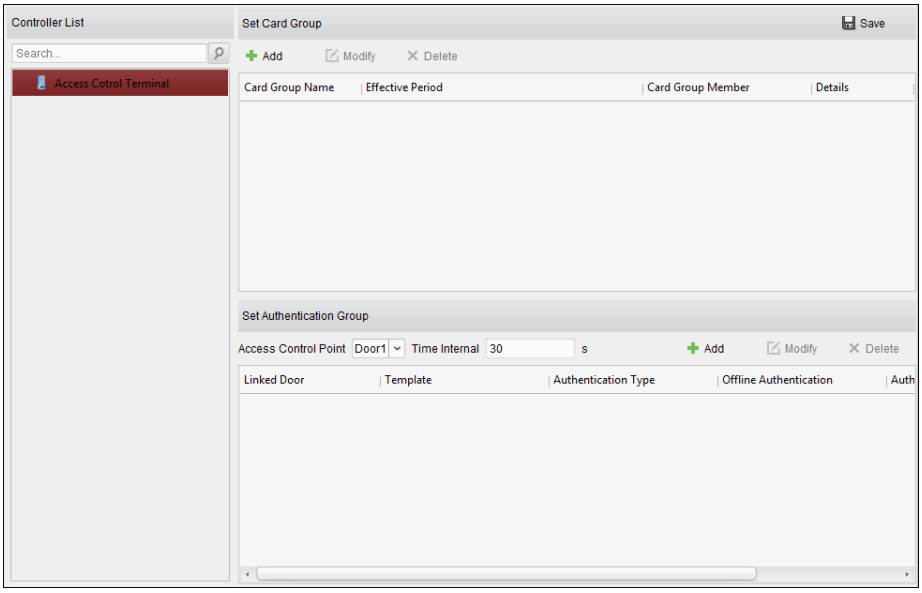
Purpose:

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

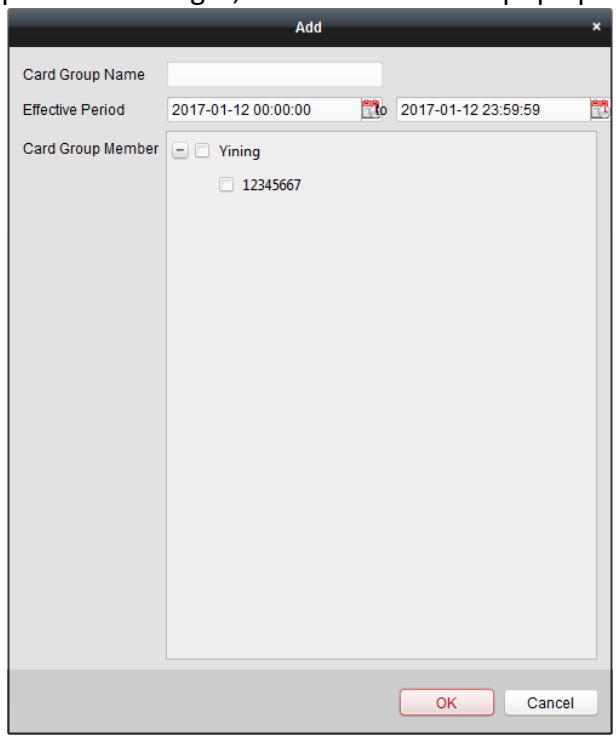
Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.8 Permission Configuration.*

Steps:

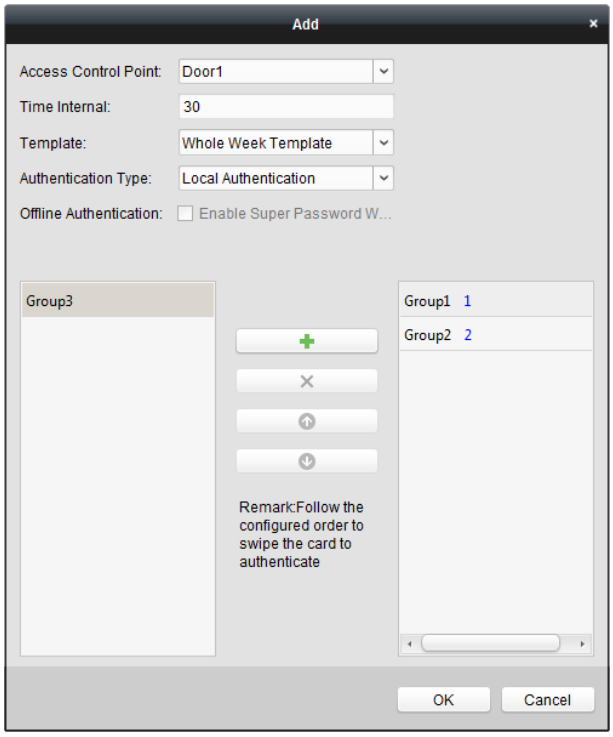
1. Click **Multiple Authentication** tab to enter the following interface.



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 7.7 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.

7.9.4 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.

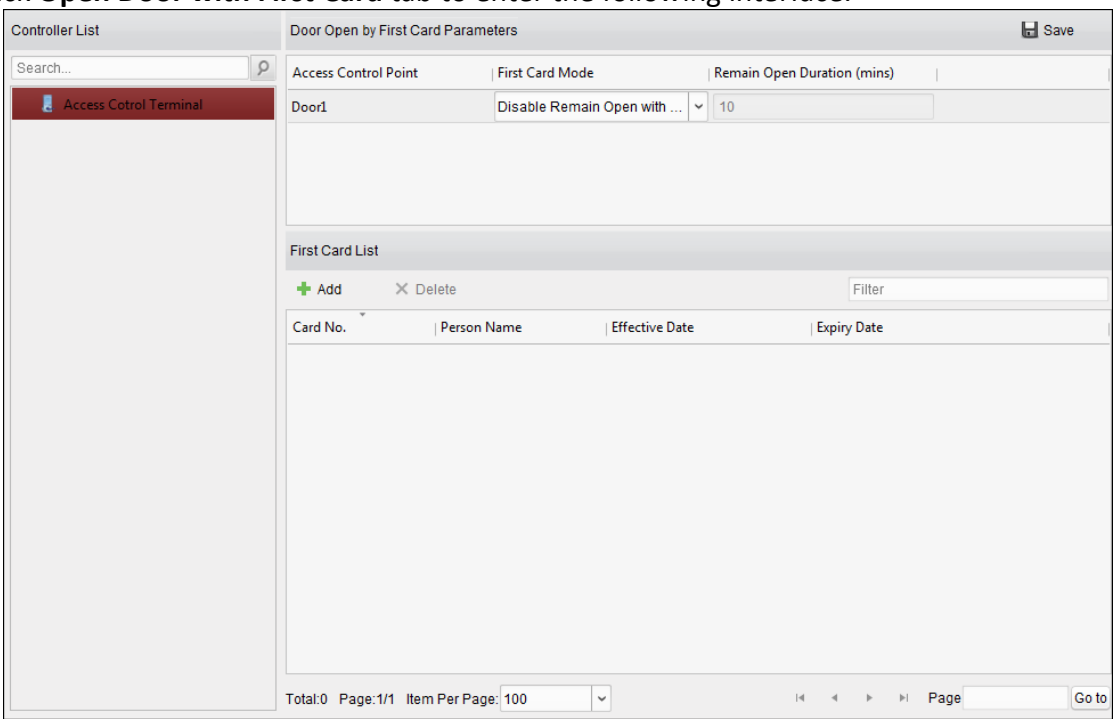
Notes:

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.



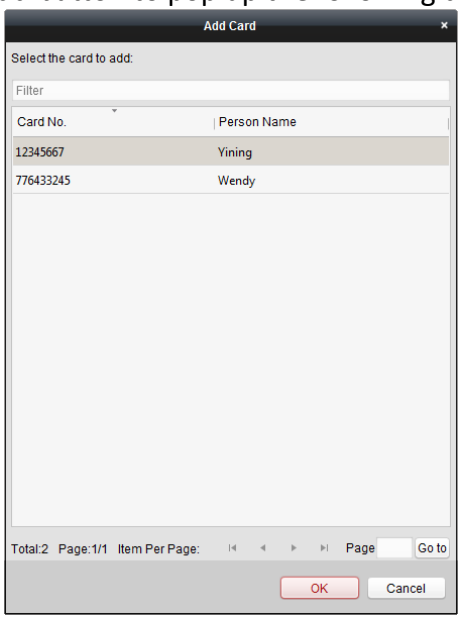
2. Select an access control device from the list on the left.
3. Select the first card mode in the drop-down list for the access control point.
4. (Optional) If you select Remain Open with First Card, you should set remain open duration.

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 7.8 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.

7.9.5 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.

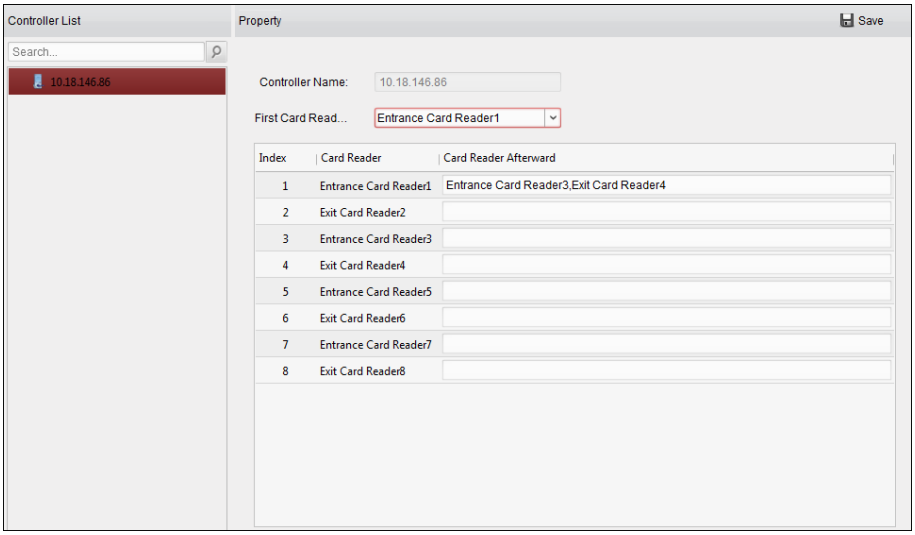
Notes:

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

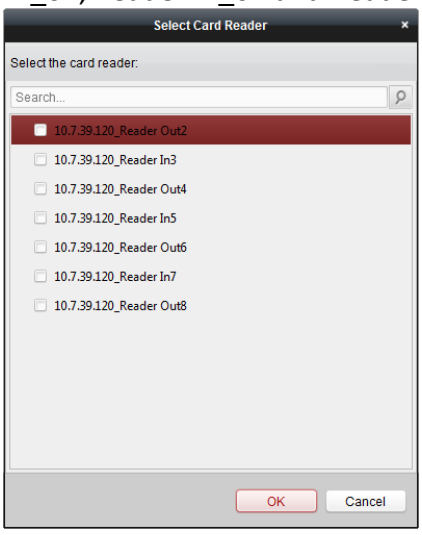
You should enable the anti-passing back function on the access control device first.

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.

7.10 Searching Access Control Event

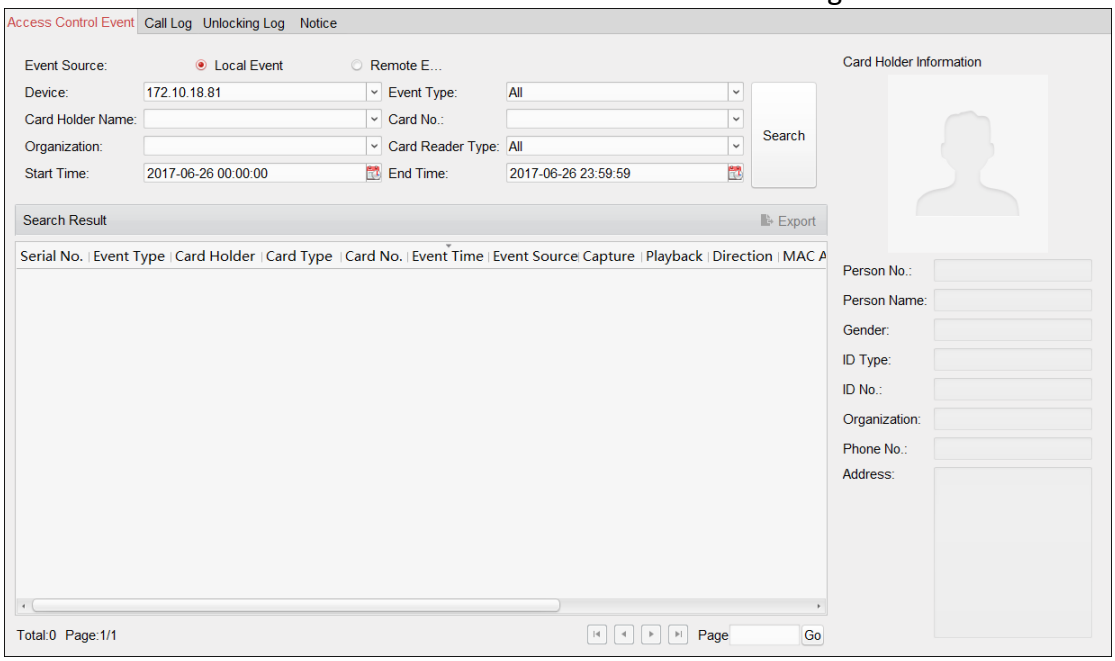
Purpose:

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.



7.10.1 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 7.11.1 Access Control Event Linkage.*
7. You can click **Export** to export the search result to the local PC in *.csv file.

7.10.2 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.

7.11 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.

7. 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.

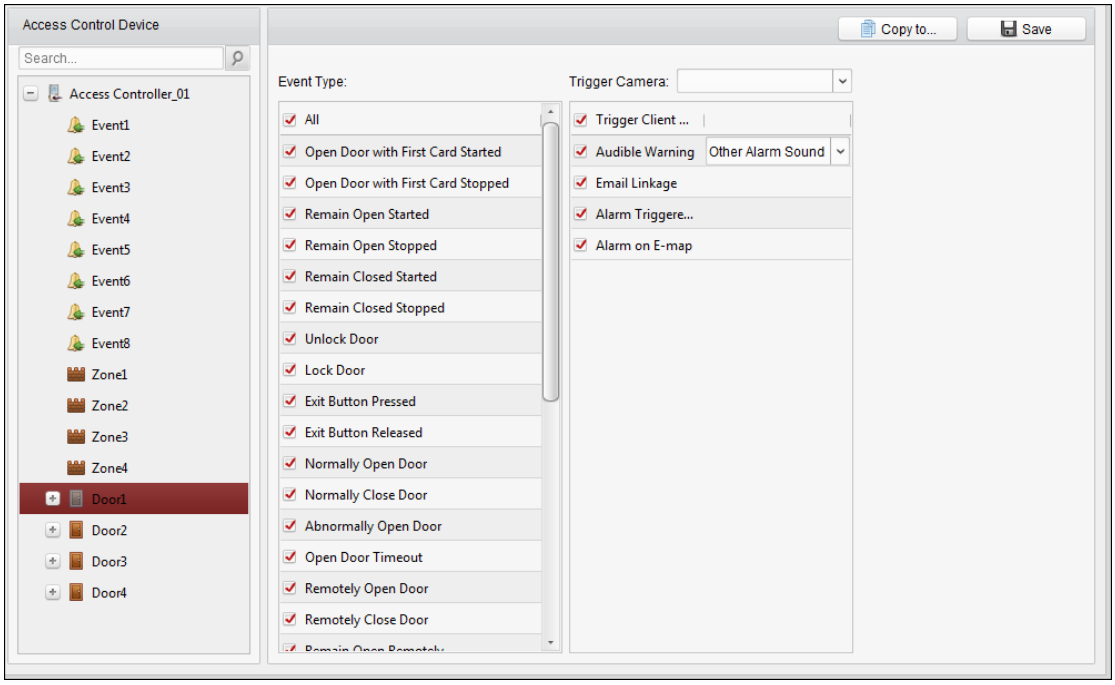
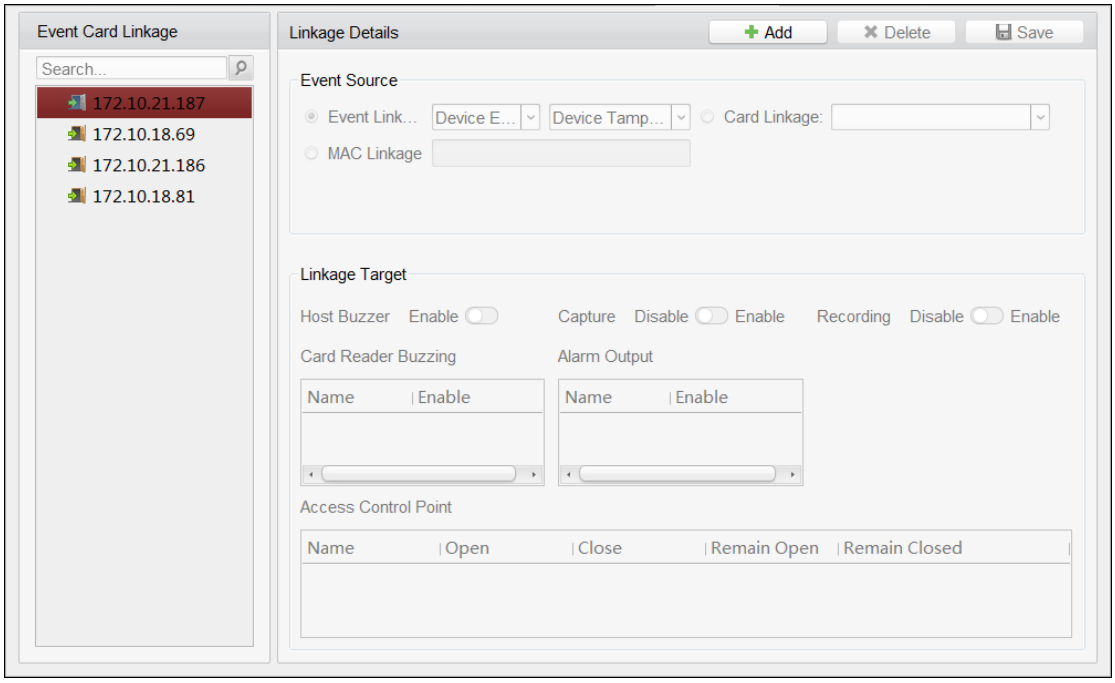


Table 1. 1 Linkage Actions for Access Control Event

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.

7.11.2 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, Card Linkage,** or **MAC 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.

MAC Linkage

Steps:

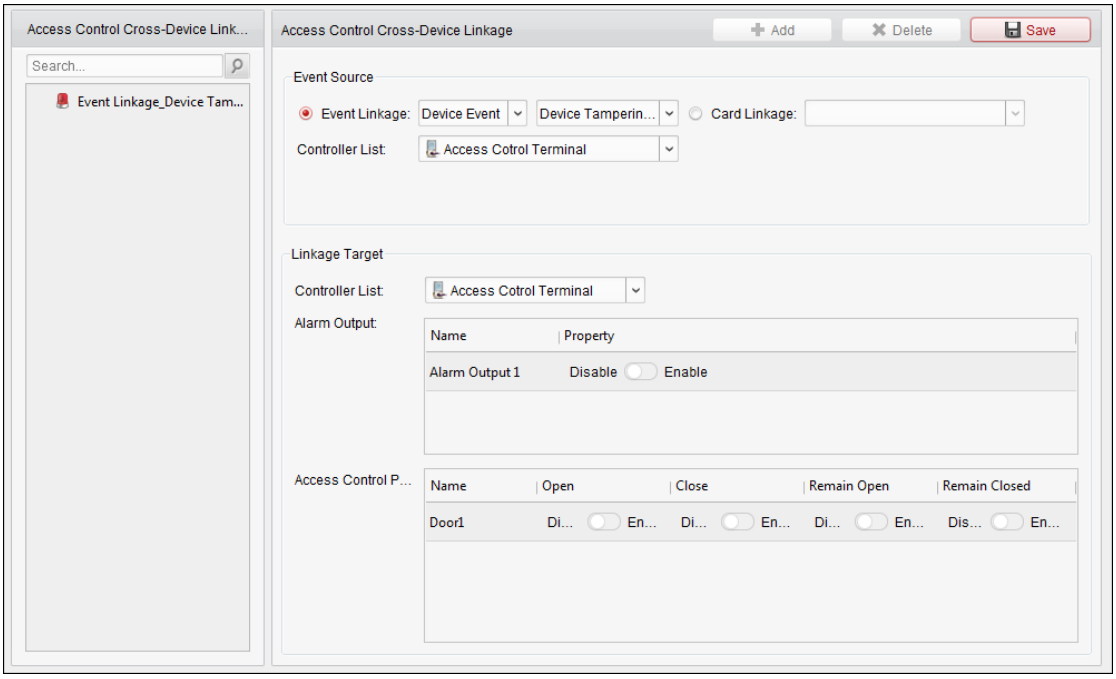
1. Click to select the linkage type as **MAC Linkage**.
2. Input the MAC address of the event source.
   MAC Address Format: AA:BB:CC:DD:EE:FF.
3. Set the linkage target, and switch the property from to  to enable this function.
   Host Buzzer: The audible warning of controller will be triggered.
   Capture: The real-time capture will be triggered.
   Recording: The recording will be triggered.
   Note: The device should support recording.
   Card Reader Buzzing: The audible warning of card reader will be triggered.
   Alarm Output: The alarm output will be triggered for notification.
   Zone: Arm or disarm the zone.
   Note: The device should support zone function.
   Access Control Point: The door status of open, close, remain open, and remain closed will be enabled.
4. Click **Save** button to save and take effect of the parameters.

7.11.3 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.

7.12 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.

7. 12. 1 Access Control Group Management

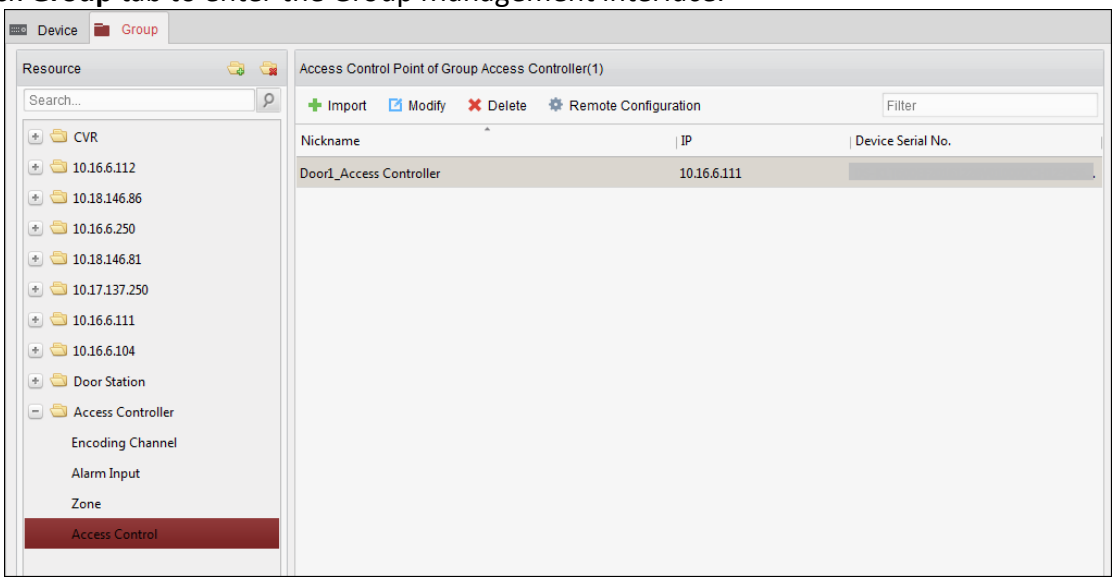
Purpose:

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.

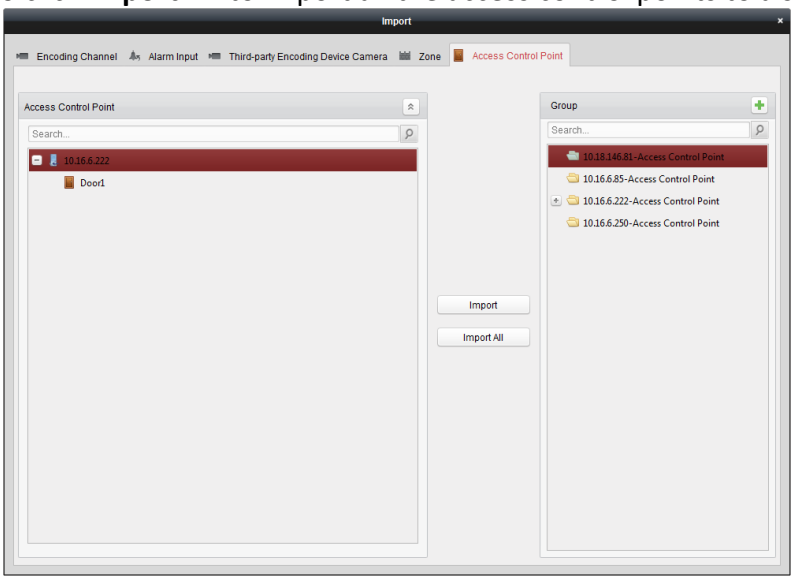
4. Perform the following steps to import the access control points to the group:
   1) Click **Import** on Group Management interface, and then click the **Access Control** tab to open the Import Access Control page.

      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.



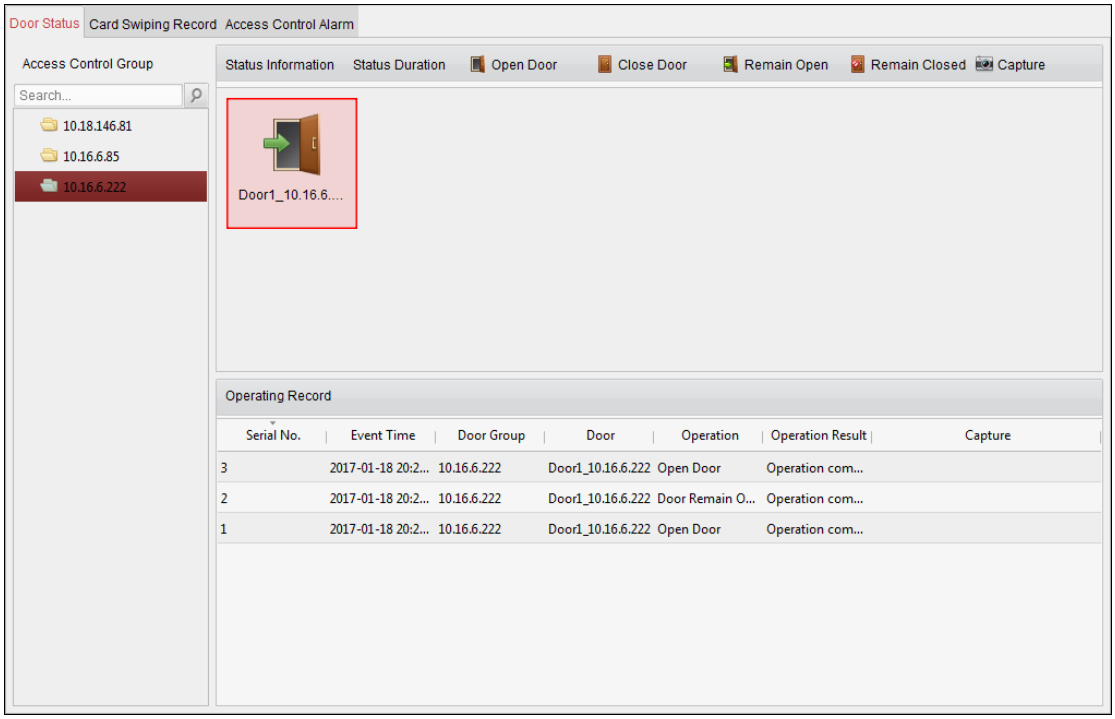
5. After importing the access control points to the group, you can click , or double-click the group/access control point name to modify it.

7. 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 7.12.1 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.

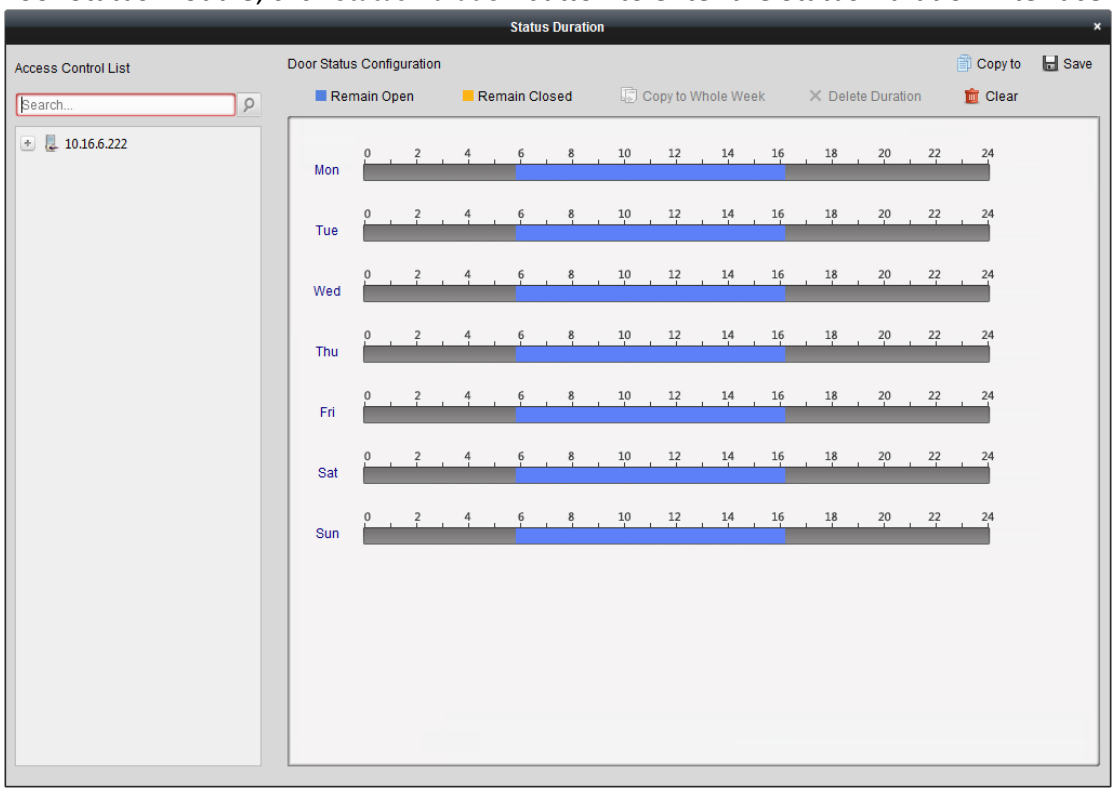
7. 12. 3 Status Duration Configuration

Purpose:

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

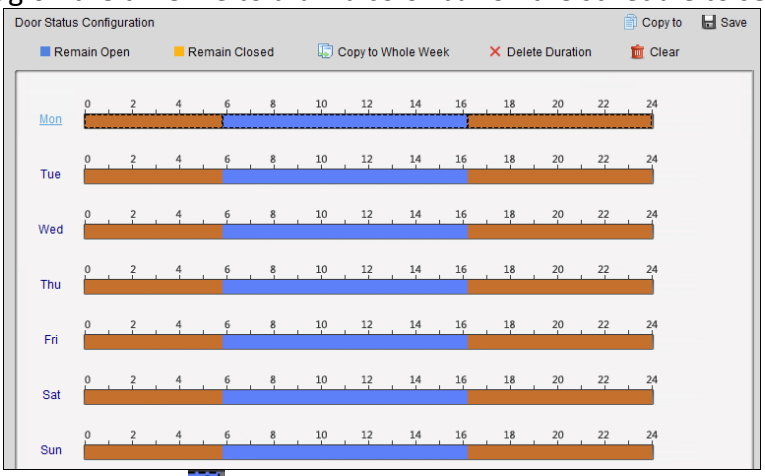
closed.

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.



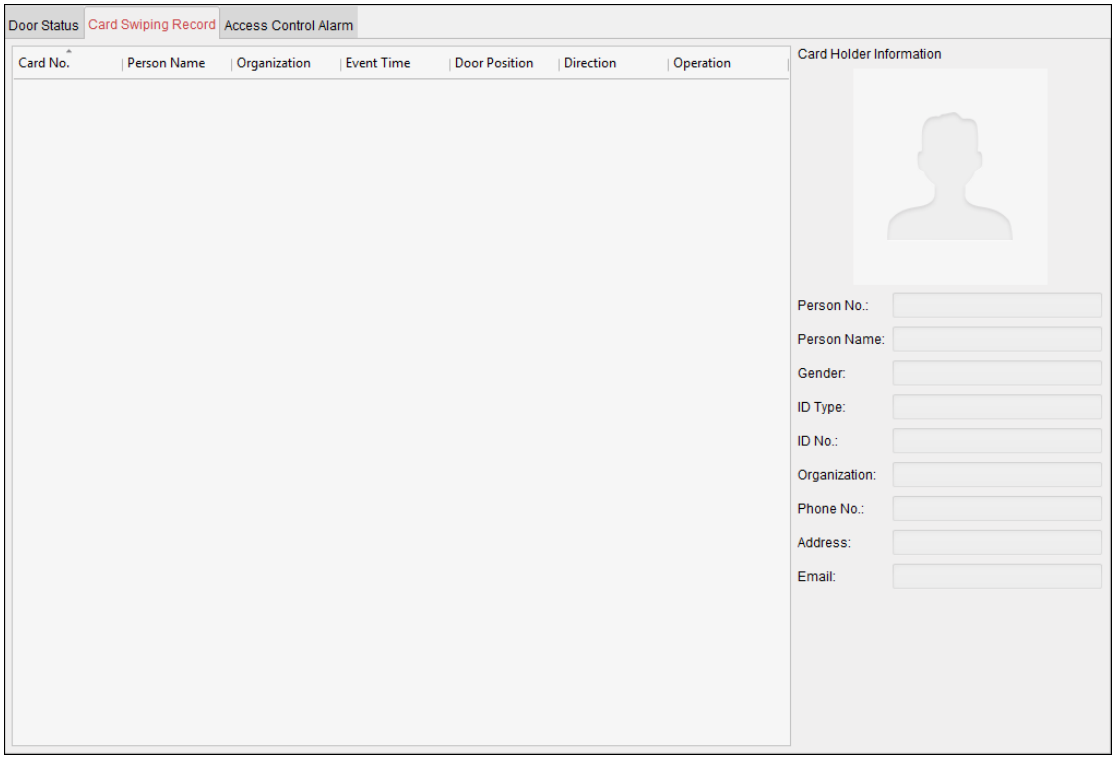
   3) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.

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.

7.12.4 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.

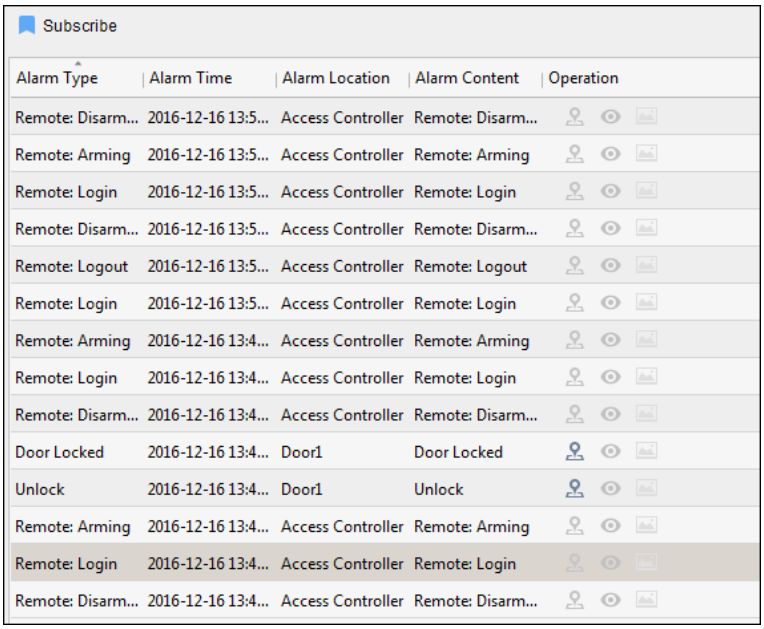
You can also click the event to view the card holder details, including person No., person name, organization, phone, contact address, etc.

7.12.5 Real-time Access Control Alarm

Purpose:

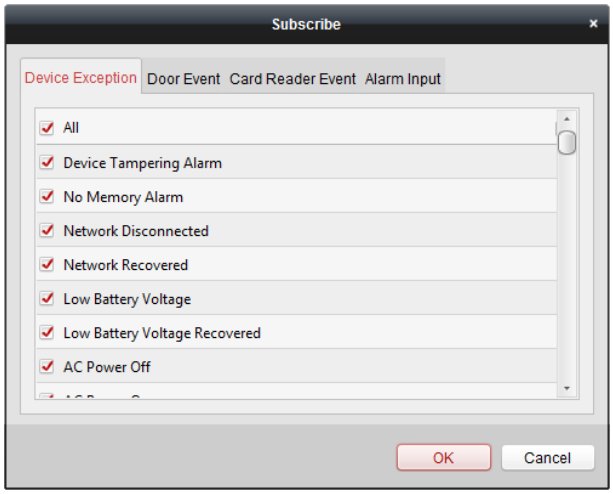
The logs of access control events will be displayed in real time, including device exception, door event, card reader event, and alarm input.

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 7.11.1 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.

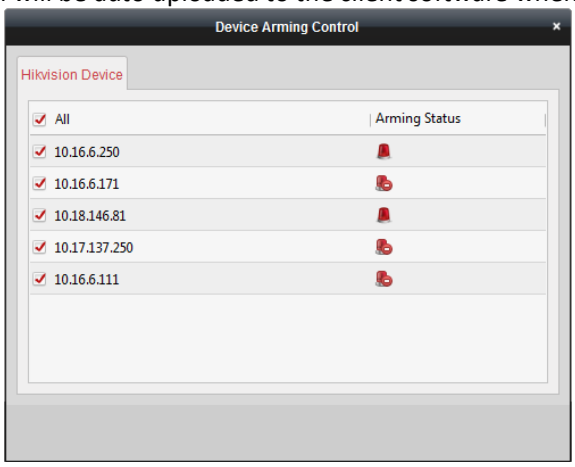
7.13 Arming Control

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.



7.14 Live View and Playback Settings

Purpose:

The parameters for live view and playback, including picture format, pre-play duration, etc., can be set.

Steps:

1. Open the System Configuration page.
2. Click the **Live View and Playback** tab to enter the Live View and Playback Parameter Settings interface.
3. Configure the live view and playback parameters. For details, see *Table 8-1 Live View and Playback Parameters*.
4. Click **Save** to save the settings.

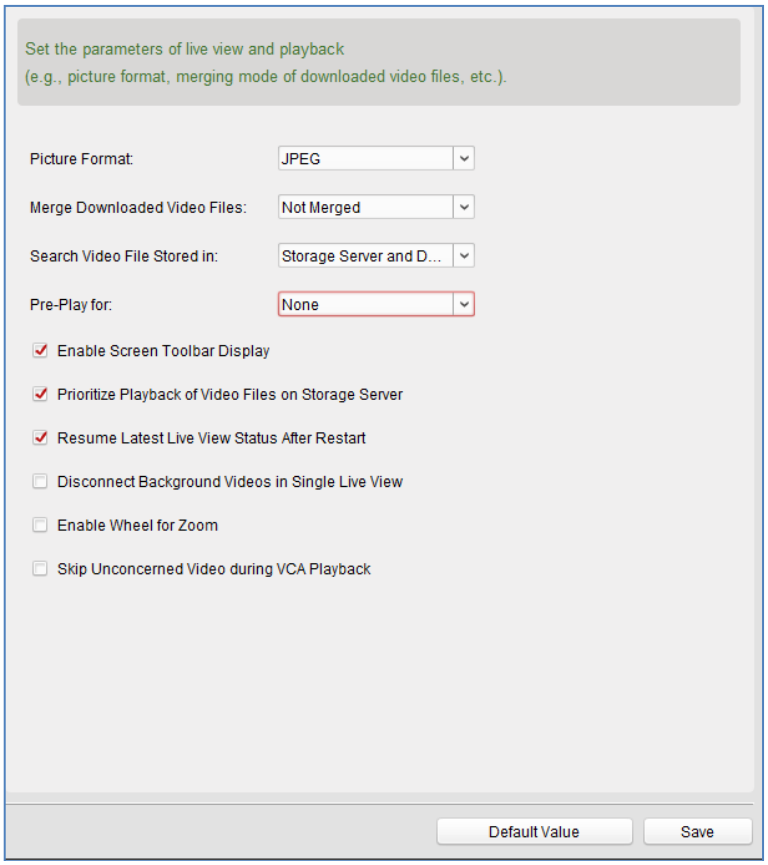


Table 7-1 Live View and Playback Parameters

Parameters	Description
Picture Format	Set the file format for the captured pictures during live view or playback.
Merge Downloaded Video Files	San set the maximum size of merged video file for downloading the video file by date.
Search Video Files Stored in	Set to search the video files stored in the local device, in the storage server, or both in the storage server and local device for playback.
Pre-play for	Set the pre-play time for event playback. ***Note:*** You should set it as None to check the live view and the playback.
Enable Screen Toolbar Display	Show the toolbar on each display window in live view or playback.
Prioritize Playback of Video Files on Storage Server	Play back the video files recorded on the storage server preferentially. Otherwise, play back the video files recorded on the local device.
Resume Latest Live View Status After Restart	Resume the latest live view status after you log into the client again.
Disconnect Background Videos in Single Live View	In multiple-window division mode, double-click a live video to display it in 1-window division mode, and the other live videos will be stopped for saving the resource.

Enable Wheel for Zoom	Enable to use the mouse wheel for zoom in or out of the video in PTZ mode, or for zoom in or restoring of the video in digital zoom mode. In this way, you can directly zoom in or out (or restore) the live video by scrolling the mouse.
Skip Unconcerned Video during VCA Playback	Enable to skip the unconcerned video during VCA playback and the unconcerned video won't be played during VCA playback.

7.15 Live View

Purpose:

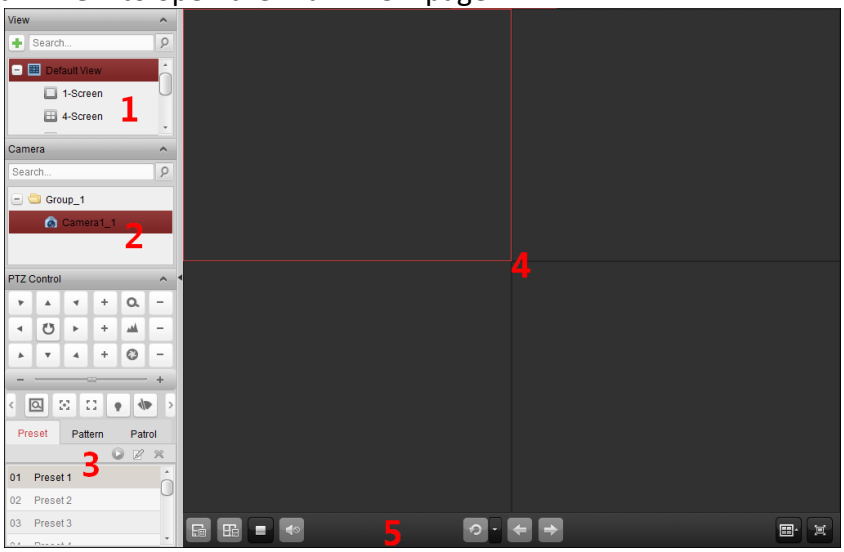
You can view the live video of the added network cameras, video encoders and video intercom device on the Main View page. And some basic operations are supported, including picture capturing, manual recording, PTZ control, etc.

Before you start:

A camera group is required to be defined for live view.

You can set the rotate type if necessary in the Group Management. For details, refer to *User Manual of iVMS-4200 Client Software*.

Click the  icon on the control panel,
or click **View**->**Main View** to open the Main View page.



Main View Page

1 View List
2 Camera List
3 PTZ Control Panel
4 Display Window of Live View
5 Live View Toolbar

Camera Status:

 The camera is online and works properly.

The camera is in live view.
The camera is in recording status.
The camera is offline.

Notes:

If event (e.g., motion detection) is detected for the camera, the camera icon will display as and the group icon will show as .

If the camera is offline, the client can still get the live video via the stream media server if the stream media server is configured. The camera icon will display as .

Live View Toolbar:

On the Main View page, the following toolbar buttons are available:

	Save View	Save the new settings for the current view.
	Save View as	Save the current view as another new view.
	Stop Live View	Stop the live view of all cameras.
	Mute/Audio On	Turn off/on the audio in live view
	Resume/Pause Auto-switch	Click to resume/pause the auto-switch in live view.
	Show/Hide the Menu	Show/Hide the configuration menu of auto-switch. Click again to hide.
	Previous	Go for live view of the previous page.
	Next	Go for live view of the next page.
	Window Division	Set the window division.
	Full Screen	Display the live view in full-screen mode. Press **Esc,** or you can move the mouse to the top of the screen and click **Quit Full Screen** button to exit. You can click **Lock** button to lock the screen, and you can click **Unlock** and input the client admin password to unlock it. For full screen auto-switch, you can click **Previous** or **Next** button to view the previous or next camera.

Right-click on the display window in live view to open the Live View Management Menu:

The following buttons are available on the right-click Live View Management Menu:

Stop Live View	Stop the live view in the display window.
Capture	Capture the picture in the live view process.
Print Captured Picture	Capture the current picture and then print the picture.
Send Email	Capture the current picture and then send an Email notification to one or more receivers. The captured picture can be attached.
Start/Stop Recording	Start/Stop the manual recording. The video file is stored in the PC.
Open PTZ Control	Enable PTZ control function on the display window. Click again to disable the function.
Enable Auto-tracking	Enable the auto-tracking function of the speed dome. Then the speed dome will track the object appearing on the video automatically. This button is only available for the speed dome that supports the auto-tracking function.
Open Digital Zoom	Enable the digital zoom function. Click again to disable the function.
Switch to Instant Playback	Switch to instant playback mode.
Start/Stop Two-way Audio	Click to start/stop the two-way audio with the device in live view.
Start/Stop IP Two-way Audio	Click to start/stop the two-way audio with the camera in live view. This button is only available for the camera that supports the IP two-way audio function.
Enable/Disable Audio	Click to enable/disable the audio in live view.
Camera Status	Display the status of the camera in live view, including the recording status, signal status, connection number, etc.
Remote Configuration	Open the remote configuration page of the camera in live view.
VCA Configuration	Enter the VCA configuration interface of the device if it is VCA device.

	Synchronization	Sync the camera in live view with the PC running the client software.
	Batch Time Sync	Set time synchronization for devices in batch.
	Fisheye Expansion	Enter the fisheye expansion mode. Only available when the device is fisheye camera.
	Start/Stop Speed Dome linkage	Click to start/stop locating or tracking the target according to your demand. Only available when the device is fisheye camera. For details, please refer to *Chapter 2.4.8 Starting Speed Dome Linkage.*
	Unlock Door	Click to remote unlock the door if the device is door station, outer door station or door station (V series).
	Full Screen	Display the live view in full screen mode. Click the icon again to exit.

7.15.1 Starting and Stopping the Live View

Starting Live View for One Camera

Steps:

1. Open the Main View page.
2. Optionally, click the icon in live view toolbar to select the window division mode for live view.
3. Click-and-drag the camera to the display window,
   or double-click the camera name after selecting the display window to start the live view.

Note: You can click-and-drag the video of the camera in live view to another display window if needed.

Starting Live View for Camera Group

Steps:

1. Open the Main View page.
2. Click-and-drag the group to the display window,
   or double-click the group name to start the live view.

Note: The display window number is self-adaptive to the camera number of the group.

Starting Live View in Default View Mode

Purpose:

The video of the added cameras can be displayed in different view modes. 4 frequently-used default view modes are selectable: 1-Screen, 4-Screen, 9-Screen and 16-Screen.

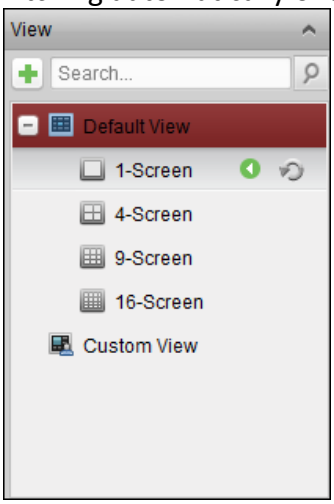
Steps:

1. Open the Main View page.
2. In the View panel, click the icon to expand the default view list.
3. Click to select the default view mode and the video of the added cameras will be displayed in a sequence in the selected view.

Note: Click , and you can save the default view as a custom view.

Move the mouse to the view and the following icons are available:

	Start Instant Playback	Start the instant playback of the view.
	Start Auto-switch	Start switching automatically of the view.



Starting Live View in Custom View Mode

Purpose:

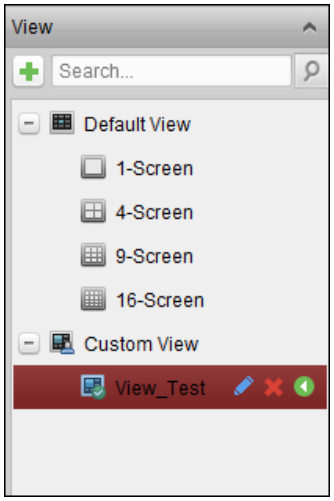
The view mode can also be customized for the video live view.

Steps:

1. Open the Main View page.
2. In the View panel, click the icon to expand the custom view list. If there is custom view available, you can click to start live view of the custom view.
3. Click to create a new view.
4. Input the view name and click **Add**. The new view is of 4-Screen mode by default.
5. Optionally, click the icon in live view toolbar and select the screen layout mode for the new view.
6. Click-and-drag the camera/group to the display window, or double-click the camera/group name in custom view mode to start the live view.
7. Click the icon to save the new view. You can also click to save the view as another custom view.

Move the mouse to the custom view and the following icons are available:

	Edit View Name	Edit the name of the custom view.
	Delete View	Delete the custom view.
	Start Instant Playback	Start the instant playback of the view.



Stopping the Live View

Steps:

1. Select the display window.
2. Click the icon that appears in the upper-right corner when the mouse pointer is over the display window,
   or click **Stop Live View** on the right-click menu to stop the live view of the display window.
   You can also click the button in live view toolbar to stop all the live view.

7.15.2 Manual Recording and Capture

Toolbar in Each Live View Display Window:

In each live view display window, the following toolbar buttons are available:

	Capture	Capture the picture in the live view process. The capture picture is stored in the PC.
	Start/Stop Recording	Start/Stop manual recording. The video file is stored in the PC.
	Switch to Instant Playback	Switch to the instant playback mode.

Manual Recording in Live View

Purpose:

Manual Recording function allows you to record the live video on the Main View page manually and the video files are stored in the local PC.

Steps:

1. Move the mouse pointer to the display window in live view to show the toolbar.
2. Click in the toolbar of the display window or on the right-click Live View Management Menu to start the manual recording. The icon turns to .
3. Click the icon to stop the manual recording.
   A prompt box with the saving path of the video files you just recorded will pop up if all the

operations succeed.

Notes:

During the manual recording, an indicator appears in the upper-right corner of the display window.

The saving path of video files can be set on the System Configuration interface. For details, see *Section 14.2.3 File Saving Path Settings.*

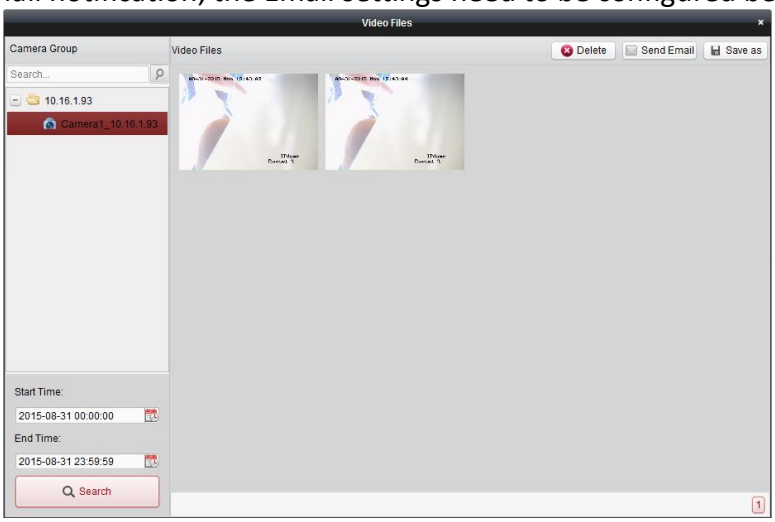
For Hik Cloud P2P device, the manual recording is not supported during live view.

Viewing Local Video Files

Steps:

1. Click **File**->**Open Video File** to open the Video Files page.
2. Select the camera to be searched from the Camera Group list.
3. Click the icon to specify the start time and end time for the search.
4. Click **Search**. The video files recorded between the start time and end time will be displayed.
   Select the video file, and click **Delete**. You can delete the video file.
   Select the video file, and click **Send Email**. You can send an Email notification with the selected video file attached.
   Select the video file, and click **Save as**. You can save a new copy of the video file.

Note: To send an Email notification, the Email settings need to be configured before proceeding.



Double-click the video file and the video file can be played back locally.

The following buttons are available on the local playback page:

CIF/4CIF	Display the video in cif/4cif resolution.
Full Screen	Display the local playback page in full screen mode.
Close	Close the local playback page of the video files.
Pause/Play	Pause/Start the playback of the video files.
Stop	Stop the playback of the video files.
Speed	Set the playback speed.
Single Frame	Play back the video files frame by frame.
Digital Zoom	Enable the digital zoom function. Click again to disable.
Enable/Disable Audio	Click to enable/disable the audio in the local playback.
Capture	Capture the picture in the playback process.

Capturing Picture in Live View

Steps:

1. Move the mouse pointer to the display window in live view to show the toolbar.
2. Click the icon in the toolbar of the display window or on the right-click Live View Management Menu.
   A small window of the captured picture will be displayed to notify whether the capturing operation is done or not.

Note: The saving path of the captured pictures can be set on the System Configuration interface. For details, see *User Manual of iVMS-4200 Client Software.*

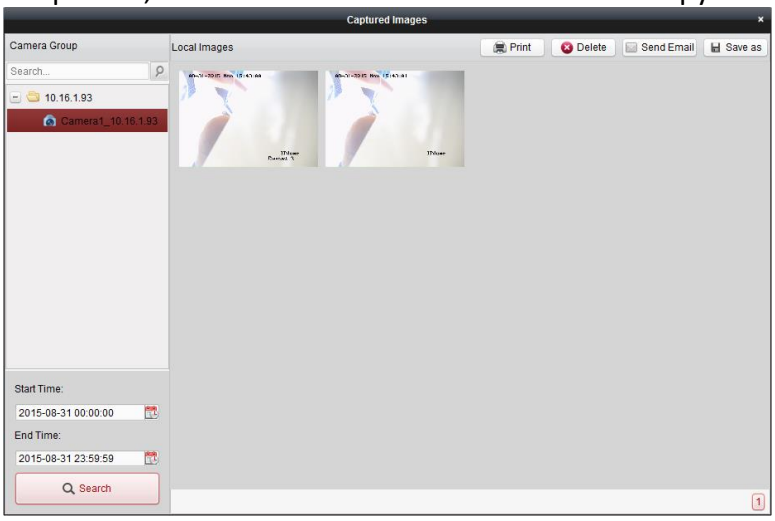
Viewing Captured Pictures

The pictures captured in live view are stored in the PC running the software. You can view the captured pictures if needed.

Steps:

1. Click **File**->**Open Image File** to open the Captured Images page.

2. Select the camera to be searched from the Camera Group list.
3. Click the icon to specify the start time and end time for the search.
4. Click **Search**. The pictures captured between the start time and end time will be displayed.
5. Double-click the captured picture to enlarge it for a better view.
   Select the captured picture, and click **Print**. You can print the selected picture.
   Select the captured picture, and click **Delete**. You can delete the selected picture.
   Select the captured picture, and click **Send Email**. You can send an Email notification with the selected picture attached.
   Select the captured picture, and click **Save as**. You can save a new copy of the selected picture.



7.15.3 Instant Playback

Purpose:

The video files can be played back instantly on the Main View page. Instant playback shows a piece of the video which was remarkable, or which was unclear on the first sight. Thus, you can get an immediate review if needed.

Before you start:

The video files need to be recorded on the storage devices, such as the SD/SDHC cards and HDDs on the DVRs, NVRs, Network Cameras, etc., or on the storage servers.

Steps:

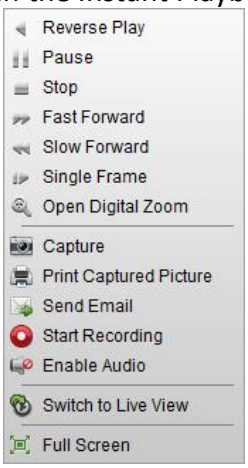
1. Start the live view and move the mouse to the display window to show the toolbar. You can also move the mouse to default view or custom view and click to enable the instant playback of the selected view.
2. Click the icon in the toolbar and a list of time periods pops up.
   30s, 1 min, 3 min, 5 min, 8 min, and 10 min are selectable.
3. Select a time period to start the instant playback.
   Example: If the current time of the live view is 09:30:00, and you select 3 min, then the instant playback will start from 09:27:00.
4. Click the icon again to stop the instant playback and go back for the live view.

Note: During the instant playback, an indicator appears in the upper-right corner of the display window.

On the instant playback page, the following toolbar buttons are available:

	Reverse Playback	Play back the video file reversely.
	Pause/Start Playback	Pause/Start the playback of the video files.
	Stop Playback	Stop the playback of all cameras.
	Slow Forward/Fast Forward	Decrease/Increase the play speed of the playback.
	Single Frame (Reverse)	Play back the video files frame by frame (reversely).

Right-click on the display window to open the Instant Playback Management Menu:



The following buttons are available on the right-click Instant Playback Management Menu:

	Reverse Playback	Play back the video file reversely.
	Pause/Play	Pause/Start the instant playback in the display window.
	Stop	Stop the instant playback and return to the live view mode.
	Fast Forward/Slow Forward	Increase/Decrease the play speed of the instant playback.
	Single Frame (Reverse)	Play back the video file frame by frame (reversely).
	Open Digital Zoom	Enable the digital zoom function. Click again to disable the function.
	Capture	Capture the picture in the instant playback process.
	Print Captured Picture	Capture the current picture and then print the picture.
	Send Email	Capture the current picture and then send an Email notification

		to one or more receivers. The captured picture can be attached.
	Start/Stop Recording	Start/Stop clipping the video files.
	Enable/Disable Audio	Click to turn on/off the audio in instant playback.
	Switch to Live View	Switch to live view mode.
	Full Screen	Display the instant playback in full screen mode. Click again to exit.

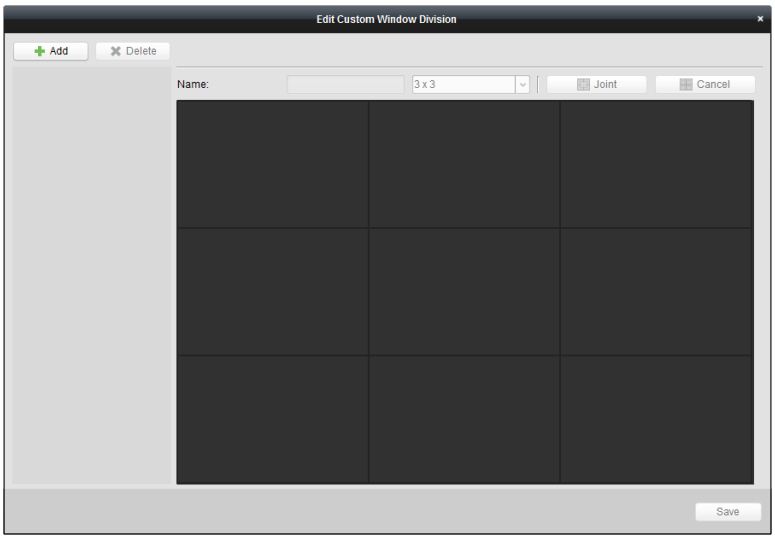
7.15.4 Custom Window Division

Purpose:

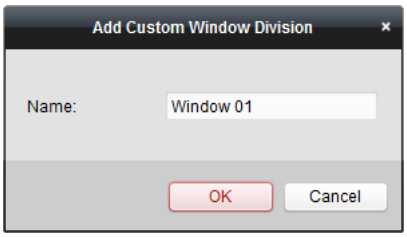
The client software provides multiple kinds of pre-defined window division. You can also set custom window division as desired.

Steps:

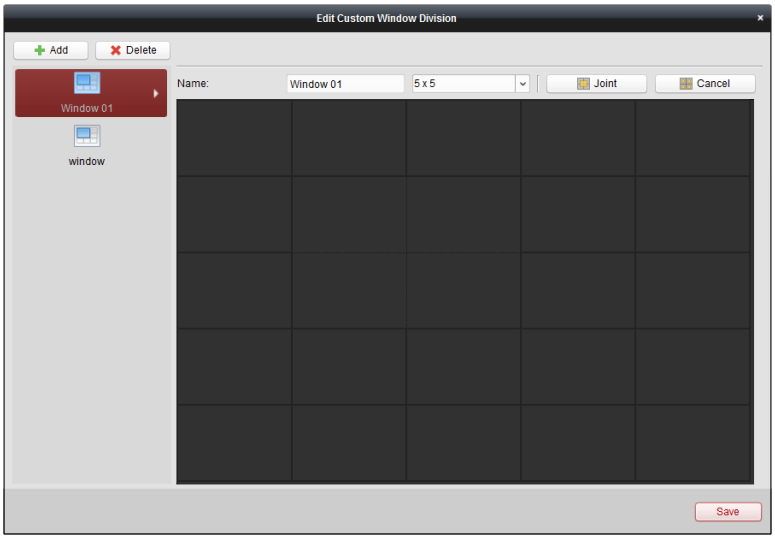
1. Click on the live view toolbar and select Edit to pop up the custom window division dialog box.



2. Click **Add** to open the custom window division adding dialog box.
   Note: Up to 5 custom window divisions can be added.
3. Set a name for the new window division as desired and click **OK** to save the settings.



4. You can edit the name, window division (3x3, 4x4, 5x5) for it.
5. Click-and-drag you mouse to select the adjacent windows, and click **Joint** to joint them as a whole window. You can also click **Cancel** to cancel the jointing.



6. Click **Save** to confirm the settings. Click to back to the Main View page. Then you can click and select the custom window division for playing live video.

Notes:

You can also enter the Remote Playback page and perform the steps above to configure the custom window division.

For remote playback, up to 16 windows can be played back at the same time. The custom window division with more than 16 windows is invalid for playback.

7.15.5 Other Functions in Live View

There are some other functions supported in the live view, including digital zoom, two-way audio, camera status and synchronization.

Auxiliary Screen Preview

The live video can be displayed on different auxiliary screens for the convenient preview of multiple monitoring scenes. Up to 3 auxiliary screens are supported.

Channel-zero

For the channel-zero of the device, you can hold the *Ctrl* key and double-click to display the specific channel. Hold the *Ctrl* key and double-click again to restore.

Two-way Audio

Two-way audio function enables the voice talk of the camera. You can get not only the live video but also the real-time audio from the camera. If the device has multiple two-way audio channels, you can select the channel to start two-way audio.

The two-way audio can be used for only one camera at one time.

Camera Status

The camera status, such as recording status, signal status, connection number, etc., can be detected and displayed for check. The status information refreshes every 10 seconds.

Synchronization

The synchronization function provides a way to synchronize the device clock with the PC which runs the client software.

7.16 Remote Playback

When the video storage devices are the HDDs, Net HDDs, SD/SDHC cards on the local device, or the remote storage server connected, you can set the recording schedule or capture schedule for the cameras for the continuous, alarm triggered or command triggered recording or capture. And the video files can be searched for the remote playback.

7. 16. 1 Storing on Storage Device

Purpose:

You can add storage device to the client for storing the video files and pictures of the added encoding devices and you can search the files for remote playback. The storage device can be storage server, CVR (Center Video Recorder) or other NVR. Here we take the settings of storage server as an example.

Before you start:

The storage server application software needs to be installed and it is packed in the iVMS-4200 software package. When installing the iVMS-4200, check the checkbox **Storage Server** to enable the installation of storage server.

Adding the Storage Server

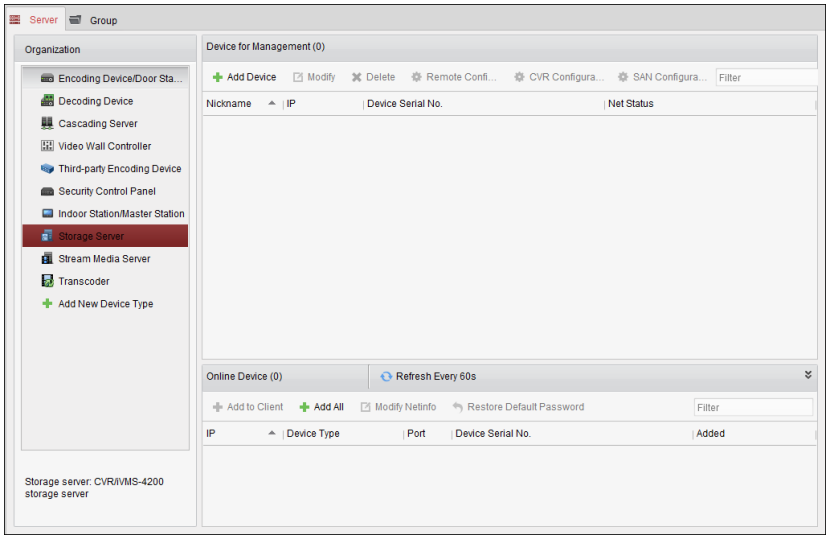
Steps:

1. Click the shortcut icon  on the desktop to run the storage server.

   Notes:

   You can also record the video files on the storage server installed on other PC.

   If the storage server port (value: 8000) is occupied by other service, a dialog box will pop up. You should change the port No. to other value to ensure the proper running of the storage server.
2. Open the Device Management page and click the **Server** tab.
3. Click **Add New Device Type**, select **Storage Server** and click **OK**.
4. Click **Storage Server** on the list to enter the Storage Server Adding interface.



5. Add the storage server.

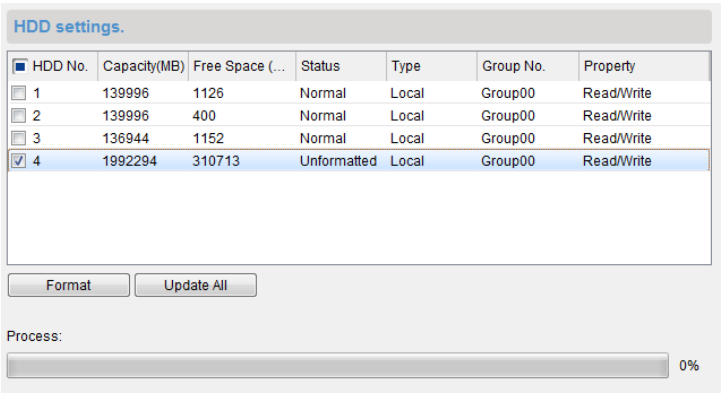
Formatting the HDDs

The HDDs of the storage server need to be formatted for the video file and picture storage.

Steps:

1. Select the added storage server from the list and click **Remote Configuration**.
2. Click **Storage**->**General**, to enter the HDD Formatting interface.
3. Select the HDD from the list and click **Format**. You can check the formatting process from the process bar and the status of the formatted HDD changes from *Unformatted* to *Normal Status*.

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



SAN and CVR Configuration

Purpose:

Client provides SAN configuration and CVR configuration to conveniently set the logical volume and CVR function for CVR device. For detailed introduction about SAN configuration and CVR configuration, refer to the *User Manual* of the CVR.

Note: This function should be supported by the device.

Select the added CVR from the list and click **CVR Configuration** or **SAN Configuration**.

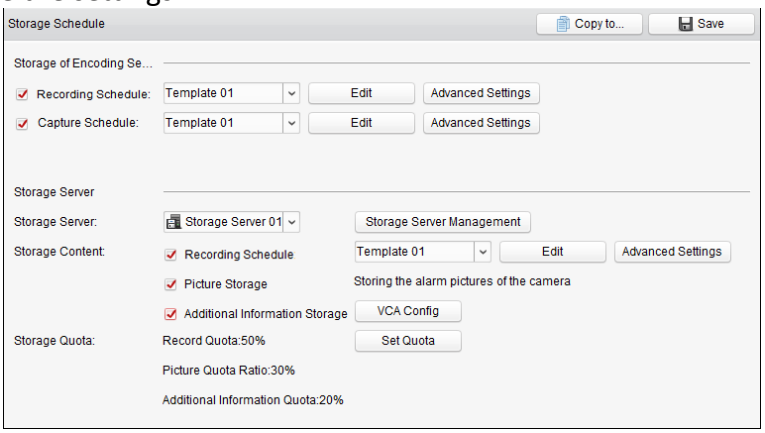
Configuring Storage Schedule

Before you start:

The storage server needs to be added to the client software and the HDDs need to be formatted for the video file storage.

Steps:

1. Open the Storage Schedule page.
2. Select the camera from the Camera Group list.
3. Select the storage server from the **Storage Server** drop-down list.
   Note: You can click **Storage Server Management** to add, edit or delete the storage server.
4. Check the checkbox **Recording Schedule** to enable storing the video files.
   You can also check the checkbox **Picture Storage** to store the alarm pictures of the camera when event occurs.
   For the network cameras with the function of heat map or people counting, the **Additional Information Storage** checkbox is available. You can click **VCA Config** to set the VCA rule for the camera, and check the **Additional Information Storage** checkbox and the heat map, people counting data and road traffic data will be uploaded to the storage server.
   Note: For detailed configuration about setting the VCA rule, please refer to the *User Manual* of the camera.
5. Select the schedule template for recording from the drop-down list.
   If you need to edit or customize the template, see *Configuring Recording Schedule Template.*
6. Click **Advanced Settings** to set the pre-record time, post-record time and other parameters for recording.
7. Click **Set Quota** to enter the HDD management interface of the storage server. You can set the corresponding quota ratio for record, picture and additional information.
   Example: If you set the record quota as 60%, then the 60% of the storage space can be used for storing the video files.
8. Click **Save** to save the settings.



Note: The storage server supports storage of line crossing detection alarm, intrusion detection alarm, region entrance detection alarm, region exiting detection alarm, fast moving detection alarm, people gathering detection alarm, loitering detection alarm, parking detection alarm, object removal detection alarm, and unattended baggage detection alarm recording.

7. 16. 2 Normal Playback

Purpose:

The video files stored on the local device or the storage server can be searched by camera or triggering event, and then can be played back remotely.

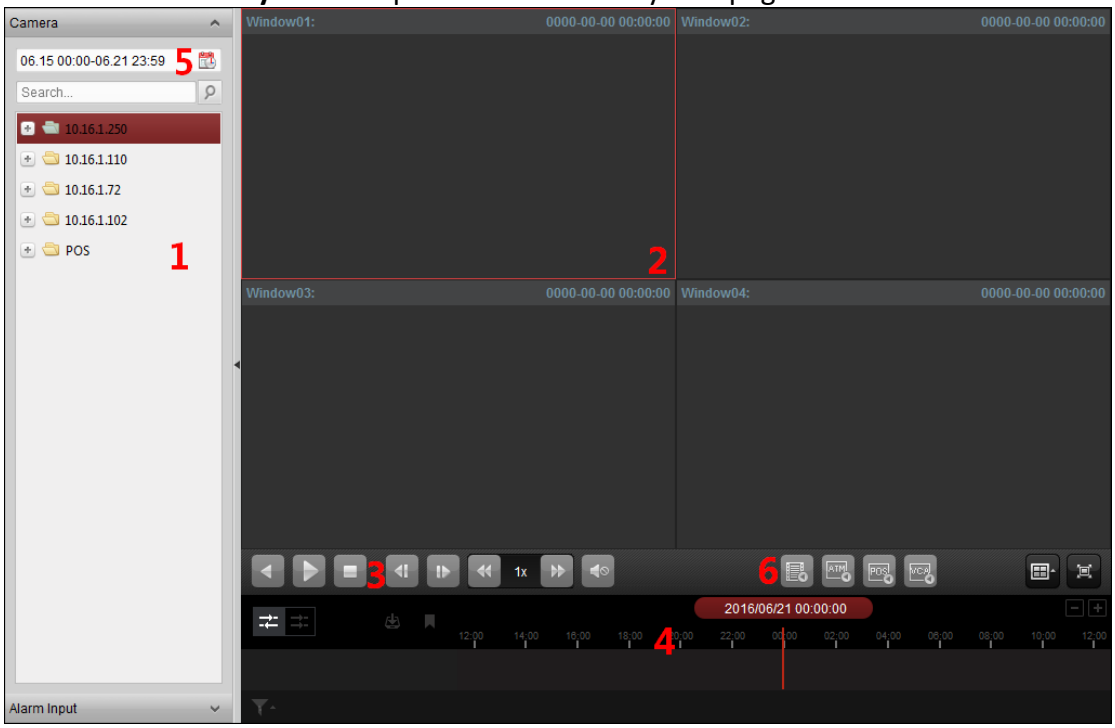
Before you start:

You can set to play back the video files stored in the local device, in the storage server, or both in the storage server and local device. For details, refer to *8.5.1 Storing on Storage Device*.

Optionally, you can set the cameras rotate direction for playback in Group Management. Refer to *Editing the Group/Camera* of *Chapter 8.3 Group Management*.

Click the  icon on the control panel,

or click **View**->**Remote Playback** to open the Remote Playback page.



Remote Playback Page

1 Camera List
2 Display Window of Playback
3 Playback Control Buttons
4 Timeline
5 Calendars
6 Search Condition

Switching Video Stream for Playback

Purpose:

Optionally, you can switch between main stream and sub-stream for playback.

Before you start:

Set the video stream for recording as Dual-Stream.

Note: This function should be support by the device.

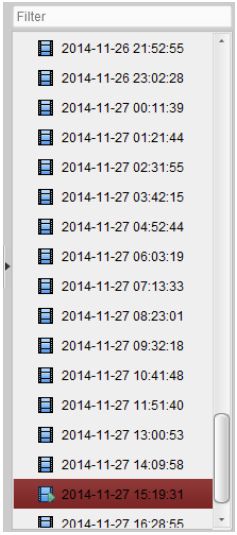
Steps:

1. Enter Group Management interface and open the Modify Camera dialog (refer to *Editing the Group/Camera* of *Chapter 8.3 Group Management*).
2. Set the video stream of the camera to main stream or sub-stream.

Searching Video Files for Normal Playback

Steps:

1. Open the Remote Playback page.
2. Click the calendars icon to activate the calendars dialog.
   Select the start and end date and set the accurate time.
   Click **OK** to save the searching period.
3. Click-and-drag the camera or group to the display window,
   or double-click the camera or group to start the playback.
4. The found video files of the selected group or camera will be displayed on the right of the interface in chronological order. You can filter the results through the **Filter** text field.
   The first video file will be played back automatically by default.



Notes:

Up to 16 cameras can be searched simultaneously.

In the calendar, the date which has scheduled records will be marked with and the date with event records will be marked with .

Playing Back Video Files

After searching the video files for the normal playback, you can play back the video files in the following two ways:

Playback by File List

Select the video file from the search result list, and then click the icon on the video file, or double-click the video file to play the video on the display window of playback.

You can also select a display window and click the icon in the toolbar to play back the corresponding video file.

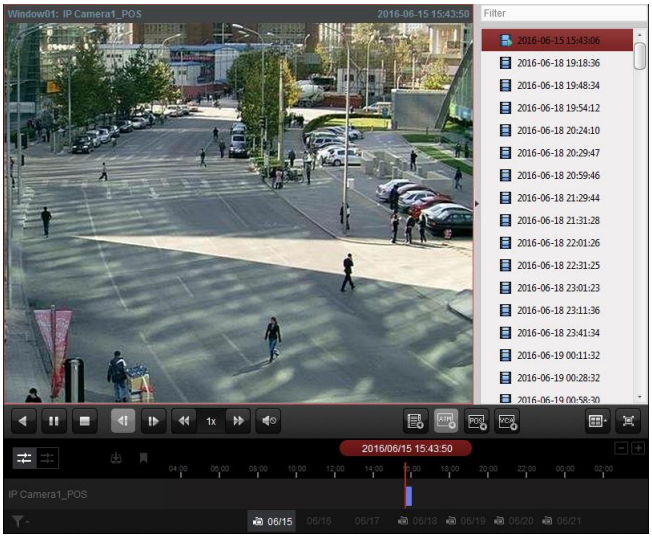
Playback by Timeline

The timeline indicates the time duration for the video file, and the video files of different types are color coded. Click on the timeline to play back the video of the specific time.

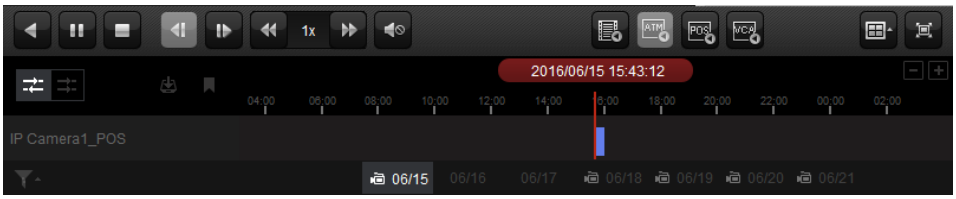
You can click ⊞ or ⊟ to scale up or scale down the timeline bar.

You can drag the timeline bar to go to the previous or the next time period.

You can use the mouse wheel to zoom in or zoom out on the timeline.



Normal Playback Toolbar:

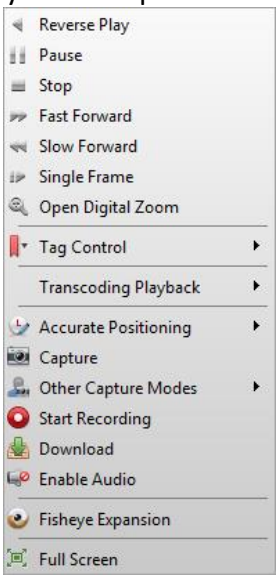


On the Normal Playback page, the following toolbar buttons are available:

	Reverse Playback	Play back the video file reversely.
	Pause/Start Playback	Pause/Start the playback of the video files.
	Stop Playback	Stop the playback of all cameras.
	Single Frame (Reverse)	Play back the video files frame by frame reversely. You can also scroll down the mouse wheel to play the video file frame by frame reversely.
	Single Frame	Play back the video files frame by frame. You can also scroll down the mouse wheel to play the video file frame by frame.
	Slow Forward/Fast Forward	Decrease/Increase the play speed of the playback.
	Volume	Click to turn on/off the audio and adjust the audio volume.
	Event Playback	Search the recordings triggered by event, such as motion detection, video loss or video tampering.
	ATM Playback	Search the recordings of ATM devices.
	POS Playback	Search the recordings which contain POS information.
	VCA Playback	Set the VCA rule to the searched video files that VCA event occurs, including VCA Search, Intrusion and Line Crossing.

	Window Division	Set the window division.
	Full Screen	Display the video playback in full-screen mode. Press **ESC** to exit.
	Async/Sync Playback	Click to play back the video files synchronously/asynchronously.
	Download	Download the video files of the camera and the video files are stored in the PC. You can select to download by file, by date, or by tag.
	Tag	Add default tag for the video file to mark the important video point. You can edit the tag or go to the tag position via the right-click menu.
	Filter	Display the record types as desired. E.g., you can select to display only the event recording.
2016/05/31 10:39:37	**Accurate Positioning**	Set the accurate time point to play back the video file.
09/13 09/14	**Date**	The day that has video files will be marked with .

Right-click on the display window in playback to open the Playback Management Menu:



The following items are available on the right-click Playback Management Menu:

	Reverse Playback	Play back the video file reversely.
/	**Pause/Start**	Pause/Start the playback.
	Stop	Stop the playback.
	Fast Forward	Play back the video file at a faster speed.
	Slow Forward	Play back the video file at a slower speed.
/	**Single Frame (Reverse)**	Play back the video file frame by frame (reversely).
	Open Digital Zoom	Enable the digital zoom function. Click again to disable the function.
	Tag Control	Add default (default tag name *TAG*) or custom tag (customized tag name) for the video file to mark the important video point. You can also edit the tag or go to the tag position conveniently.

Accurate Positioning	Set the accurate time point to play back the video file.
Capture	Capture the picture in the playback process. **Print Captured Picture:** Capture a picture and print it. **Send Email:** Capture the current picture and then send an Email notification to one or more receivers. The captured picture can be attached.
Other Capture Modes	**Custom Capture:** Capture the current picture. You can edit its name and then save it.
Start/Stop Recording	Start/Stop the manual recording. The video file is stored in the PC.
Download	Download the video files of the camera and the video files are stored in the PC. You can select to download by file or by date.
Enable/Disable Audio	Click to enable/disable the audio in playback.
Fisheye Expansion	Enter the fisheye playback mode.
Full Screen	Display the playback in full-screen mode. Click the icon again or press *Esc* key to exit.

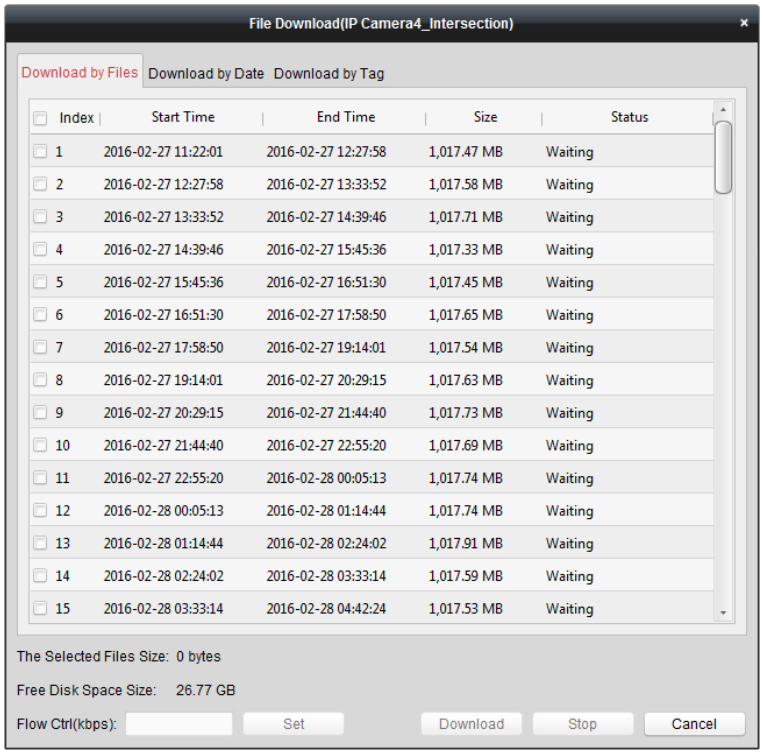
Downloading Video Files

During playback, you can click on the toolbar to download the video files of the camera to the local PC. You can select to download by file, by date, or by tag.

Download by Files

Steps:

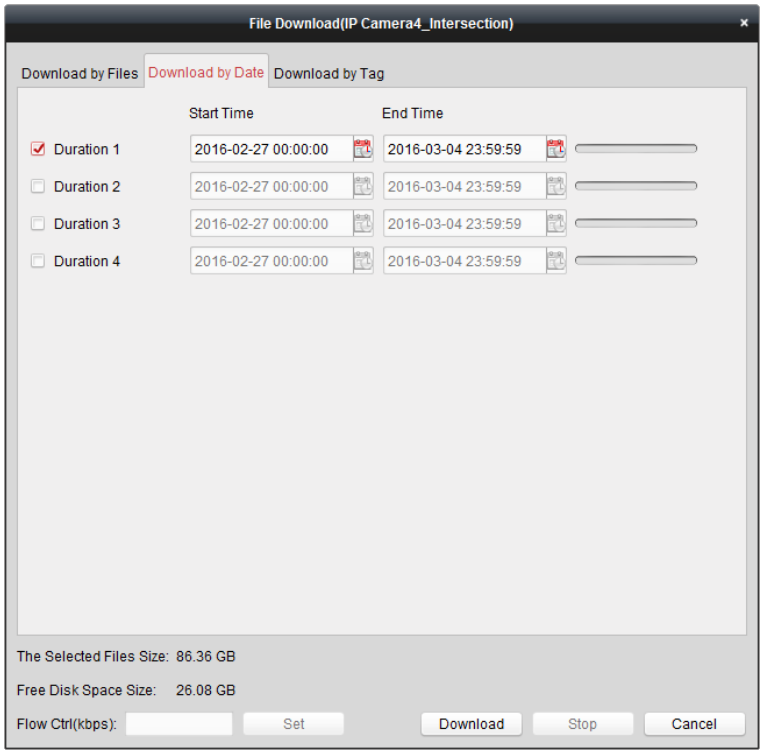
1. Click **Download by Files** tab in the File Download interface. You can view the video files information of selected camera.
2. Check the checkbox of the video file and the total size of the selected files will be shown below.
3. Click **Download** to start downloading the file to the local PC.
   You can input the flow (0 to 32768 kbps) and click **Set** to control the downloading speed.
4. Optionally, you can click **Stop** to stop downloading manually.



Download by Date

Steps:

1. Click **Download by Date** tab in the File Download interface.
2. Check the checkbox of the time duration to enable it, and click to set the start and end time.
3. Click **Download** to start downloading the file to the local PC. The progress bar shows the downloading process.
   You can input the flow (0 to 32768 kbps) and click **Set** to control the downloading speed.
4. Optionally, you can click **Stop** to stop downloading manually.

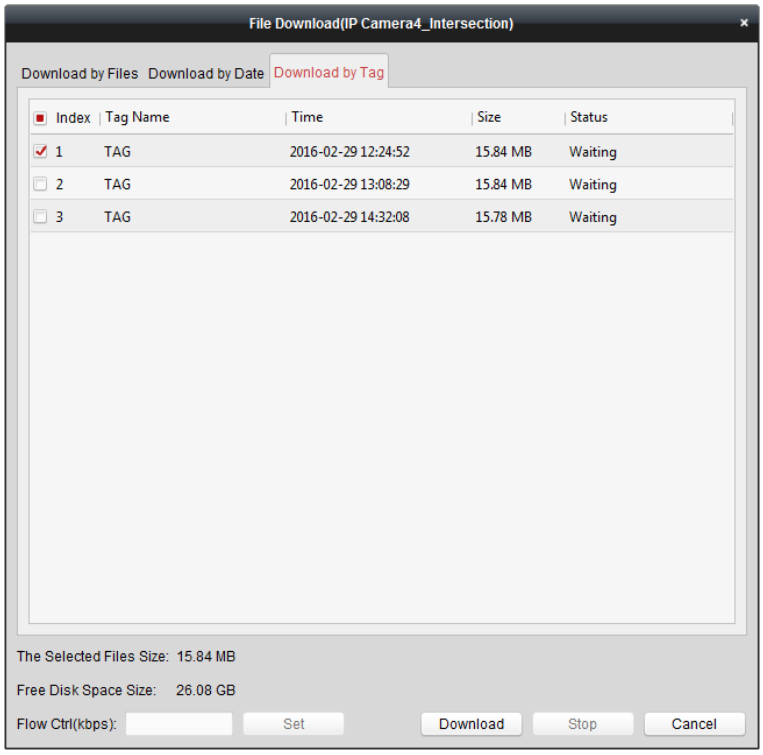


Note: When downloading video file of one time duration, you can set to merge the video files. The video files in the set time duration can be merged for downloading. For configuring merging downloaded video files, refer to *8.2 Live View and Playback Settings*.

Download by Tag

Steps:

1. Click **Download by Tag** tab in the File Download interface. The added tags will be displayed.
2. Check the checkbox of the tag and the total size of the selected files will be shown below.
3. Click **Download** to start downloading the selected file (30 seconds before the selected tag to 30 seconds after the tag) to the local PC. You can input the flow (0 to 32768 kbps) and click **Set** to control the downloading speed.
4. Optionally, you can click **Stop** to stop downloading manually.



7.16.3 Event Playback

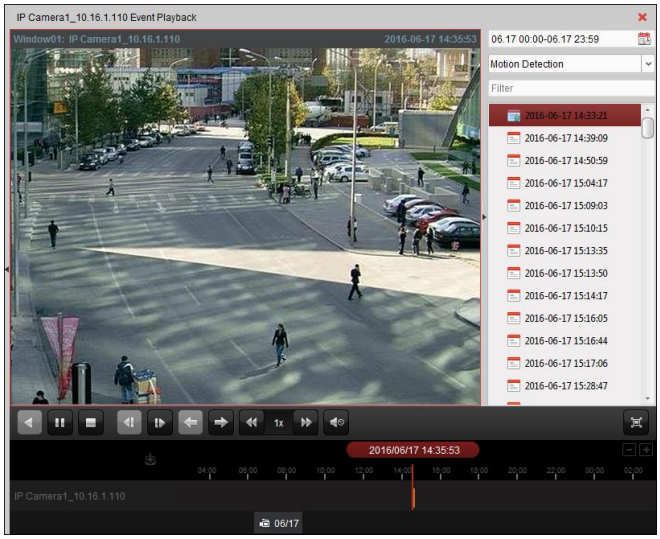
Purpose:

The recordings triggered by event, such as motion detection or VCA detection, can be searched for Event Playback and this function requires the support of the connected device.

Searching Video Files for Event Playback

Steps:

1. Open the Remote Playback page.
2. Select the camera and start the normal playback. Refer to *Chapter 8.5.2 Normal Playback*.
3. Click and the motion detection triggered recording will be searched by default.
4. Click the calendars icon to activate the calendars dialog box.
   Select the start and end date and set the accurate time.
   Click **OK** to save the searching period.
   Note: In the calendar, the date which has scheduled records will be marked with and the date with event records will be marked with .
5. Select the event type from the drop-down list and the found video files will be displayed. You can filter the results by inputting the keyword in the **Filter** text field. Or you can click to go back to the normal playback.
6. Select the video file from the search result list, and then click the icon on the video file, or double-click the video file to play the video on the corresponding display window of playback.



Playing Back Video Files

After searching the recordings triggered by the event, you can play back the video files in the following two ways:

Playback by File List

Select the video file from the search result list, and then click the icon in the toolbar, or click the icon on the video file, or double-click the video file to play the video on the corresponding display window of playback.

Playback by Timeline

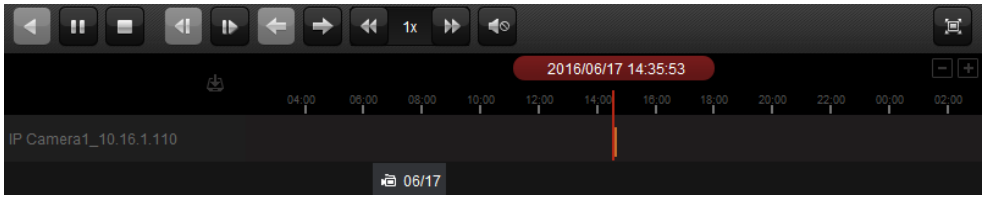
The timeline indicates the time duration for the video file. Click on the timeline to play back the video of the specific time.

You can click or to scale up or scale down the timeline bar.

You can drag the timeline bar to go to the previous or the next time period.

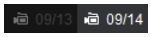
You can use the mouse wheel to zoom in or zoom out on the timeline.

Event Playback Toolbar:



On the Remote Playback page, the following toolbar buttons are available:

	Reverse Playback	Play back the video file reversely.
	Pause/Start Playback	Pause/Start the playback of the video files.
	Stop Playback	Stop the playback of all cameras.
	Single Frame (Reverse)	Play back the video files frame by frame reversely.
	Single Frame	Play back the video files frame by frame.
	Previous Event	Go to the playback of the previous event.
	Next Event	Go to the playback of the next event.
	Slow Forward/Fast Forward	Decrease/Increase the play speed of the playback.
	Volume	Click to turn on/off the audio and adjust the audio volume.

	**Full Screen**	Display the video playback in full screen mode. Press **ESC** to exit.
	**Download**	Download the video files of the camera and the video files are stored in the PC.
	**Accurate Positioning**	Set the accurate time point to play back the video file.
	**Date**	The day that has video files will be marked with  .

Please refer to *Chapter 7.16.2 Normal Playback* for the description of the right-click menu. Some icons may not available for event playback**.**

Note: You can set the pre-play time for event playback in System Configuration. By default, it is 30s. For configuring the pre-play time, refer to *Live View and Playback Settings* in *Chapter 7.16.3 Event Playback*.

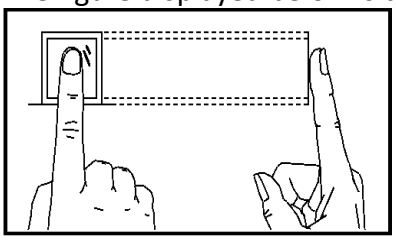
Appendix A Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

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

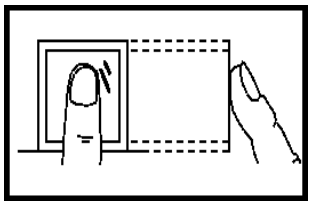


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

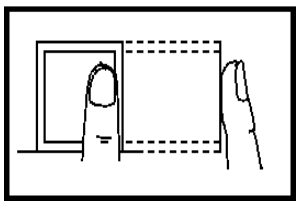
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

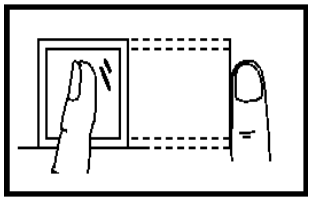
Vertical



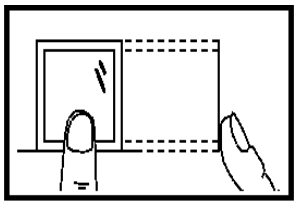
Edge I



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 DIP Switch Introduction

The DIP switch diagram is as follows:

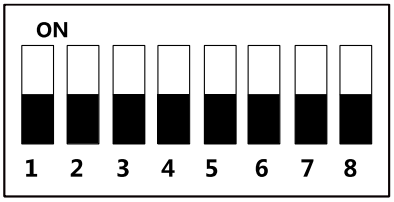


Table 7-2 Description of DIP Switch

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

For example, binary value of the following status is: 0000 1100.

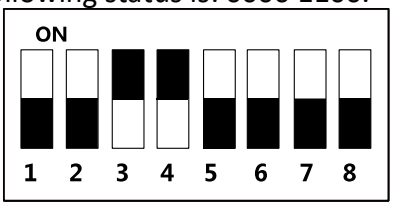


Table 7-3 Description of DIP Switch

No.	Description	DIP Switch Status
1 ~ 4	Address of RS-485	2: Security Module 0: Card Reader
5	RS-485 Direction under the Terminal Mode	1: Upstream; 0: Down Stream
6	Working Method	1: Card Reader; 0: Terminal.
7	Wiegand Protocol (available when No. 6 is 1)	1: Wiegand protocol of 26-bit; 0: Wiegand protocol of 34-bit.
8	Matched Resistance (available for RS-485 protocol)	1: Enable; 0: Disable.

Appendix C Indicator and Buzzer Description

Power on after 10s, the buzzer will beep once. When the device is powered on, the buzzer will beep again (once). The indicator will remain red in this duration.

The buzzer descriptions are as follows:

Type	Description
Beep Once	Card Swiping
	Pressing Button
	After Card Swiping and before Scanning Fingerprint in Multiple Authentications
Fast Beep Twice	Valid Card Swiping
Slow Beep for Three Times	Invalid Card Swiping
Rapid and Continuous Beep	Tampering Alarm
	Buzzer Alarm
Slow and Continuous Beep	Not Encrypted Card Reader

The card reader indicator descriptions are as follows:

Indicator	Description
Flashing Green Once and Flashing Red for 3 Times	Powering On
Continuous Flashing Green	After Card Swiping and before Scanning Fingerprint in Multiple Authentications
Solid Green for 3s	Fingerprint Authentication Completed after Swiping Card in Card Swiping Operation/Multiple Authentications
Solid Red	Working Properly
Flashing Red for 3 Times	Invalid Card Swiping
Continuous Flashing Red	Card Reader Mode Offline and Registration Failure

0200001090312

UD06878B-D