iVMS-4200 Client Software

User Manual

V2.5.2

UD03324B

User Manual

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to iVMS-4200 Client Software.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

Contents

Chapter 1 Overview

1.1 Description

iVMS-4200 is a versatile video management software for the DVRs, NVRs, IP cameras, encoders, decoders, VCA device, security control panel, video intercom device, etc. It provides multiple functionalities, including real-time live view, video recording, remote search and playback, file backup, alarm receiving, etc., for the connected devices to meet the needs of monitoring task. With the flexible distributed structure and easy-to-use operations, the client software is widely applied to the surveillance projects of medium or small scale.

We also provide Access Control System module which can manage the access controllers. For the detailed configuration of the access control system, please refer to *Chapters 19 to 24*.

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

1.2 Running Environment

Operating System: Microsoft Windows 7/Windows 8.1/Windows 10 (32-bit or 64-bit),
Microsoft Windows XP SP3 (32-bit),
Microsoft Windows 2008 R2/Windows Server 2012 (64-bit).

CPU: Intel Pentium IV 3.0 GHz or above

Memory: 2G or above

Video Card: RADEON X700 Series or above

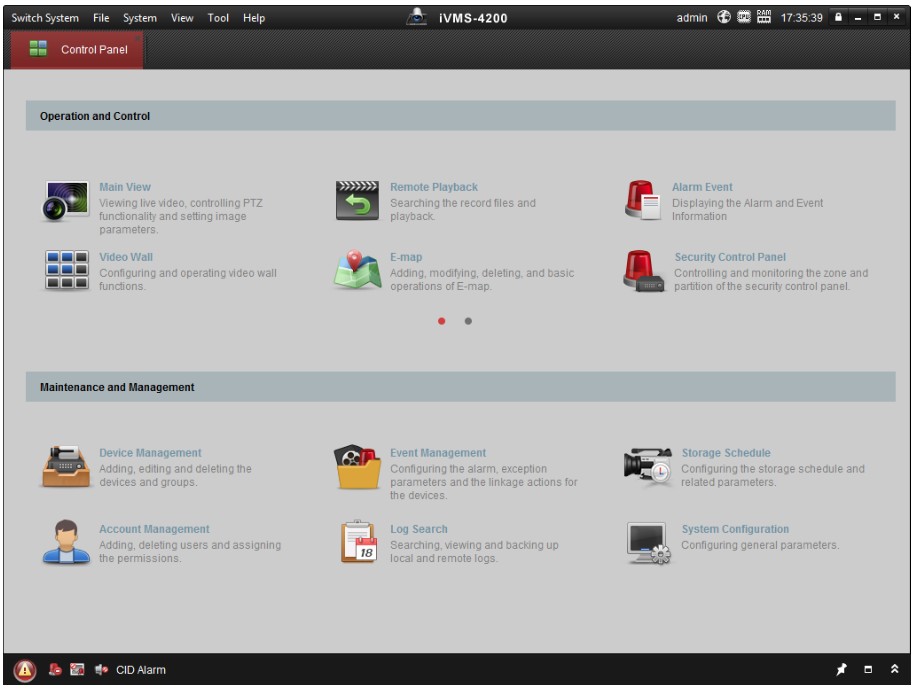
GPU: 256 MB or above

Notes:

- For high stability and good performance, these above system requirements must be met.
- The software does not support 64-bit operating system; the above mentioned 64-bit operating system refers to the system which supports 32-bit applications as well.
- Hardware decoding function is only supported by operating systems the version of which is after Windows XP.

1.3 Function Modules

Control Panel of iVMS-4200:



Operation and Control

Main View
Viewing live video, controlling PTZ functionality and setting image parameters.

Remote Playback
Searching the record files and playback.

Alarm Event
Displaying the Alarm and Event Information

Video Wall
Configuring and operating video wall functions.

E-map
Adding, modifying, deleting, and basic operations of E-map.

Security Control Panel
Controlling and monitoring the zone and partition of the security control panel.

Maintenance and Management

Device Management
Adding, editing and deleting the devices and groups.

Event Management
Configuring the alarm, exception parameters and the linkage actions for the devices.

Storage Schedule
Configuring the storage schedule and related parameters.

Account Management
Adding, deleting users and assigning the permissions.

Log Search
Searching, viewing and backing up local and remote logs.

System Configuration
Configuring general parameters.

Menu Bar:

Switch System	**Video Management System**	Go to Video Management System interface for live view, playback, device management, event management, etc..
	Access Control System	Go to Access Control System for access controller management, permission settings, door status management, event search, attendance, etc..
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.
	Import from Access Control Client	Import the access control data (including access control devices, access control points, alarm inputs, and cameras of access control terminal) of the iVMS-4200 Access Control Client to the iVMS-4200 Client Software.
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.

	Video Wall	Open Video Wall page.
	E-map	Open E-map page.
	Security Control Panel	Open Security Control Panel page.
	Video Intercom	Open Video Intercom 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 Wizard**	Open the guide for the client configuration.
	Open Video Wall Wizard	Open the guide for the video wall 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.

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 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 Security Control Panel module provides operations such as arming, disarming, bypass, group bypass, and so on for both the partitions and zones.

The Video Intercom module provides video intercom with iVMS-4200 via indoor station, group management, card management and notice management.

The Statistics module provides functions of heat map, people counting statistics, counting statistics, road traffic, face retrieval, license plate retrieval, behavior analysis, and face capture statistics.

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.

1.4 Updates Instruction

Multiple newly-designed functions are offered in the latest iVMS-4200 client software. You can get a brief view of the updates instruction from the following contents.

- **High DPI Compatible**

  Compatible with High DPI Screen.
- **POS Playback**

  Support searching the video files which contain POS information.
- **Communication with Access Control Client**

  Support communication with the iVMS-4200 Access Control Client, and it provides further functions after importing the access control devices, including access control event configuration, displaying access control point on E-map, alarm/event linkage, and so on.
- **Display Zone and Access Control Point on E-map**

  Support displaying the zone of security control panel and access control point of access control device on the E-map.
- **New Structure of System Configuration**

  Provide new structure in System Configuration module.
- **Set Icon on Live View and Playback Toolbar**

  Set the icon display on the toolbar of live view and playback window.
- **Frame Extracting for High-speed Playback**

  When play back the video in high-speed (8x speed and above), you can disable this function to make the image of playback more fluent to view the details.
- **Prioritize to View Latest Alarm**

  Set to view the latest alarm in priority when viewing the alarm information in the pop-up alarm window.

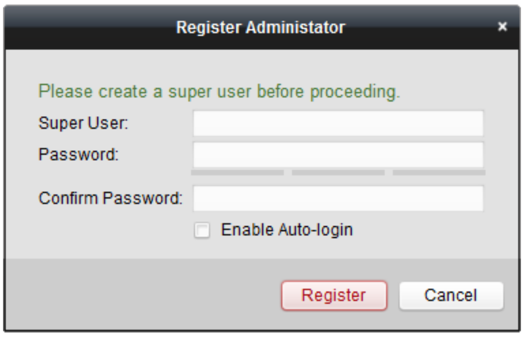
- **Customize Alarm Sound**
  Support custom alarm sound as desired.
- **Search Video File in 31 Days**
  Support searching video files during up to 30 days.
- **Provide Player**
  Provide Player in the installation directory to view the downloaded video file.
- **Provide Attendance Management for Access Control System**
  Provide attendance management including shift, shift group, holiday, shift schedule, attendance adjustment, and attendance statistics.

Chapter 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.



Register Administator

Please create a super user before proceeding.

Super User:

Password:

Confirm Password:

□ Enable Auto-login

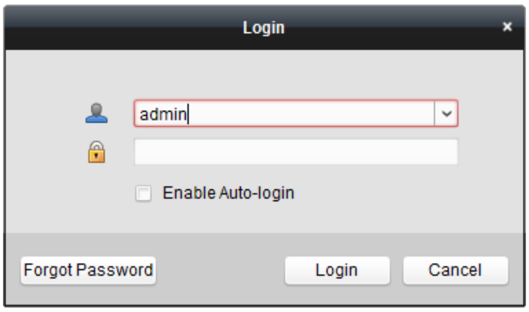
- *A user name cannot contain any of the following characters: / \ : * ? “ < > |. And the length of the password cannot be less than 6 characters.*
- *For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case 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, a wizard will pop up to guide you to add the device and do some basic settings. For detailed configuration about the wizard, please refer to the *Quick Start Guide of iVMS-4200*.

Chapter 3 Device Management

3.1 Adding the Device

Purpose:

After running the iVMS-4200, devices including network cameras, video encoders, DVRs, NVRs, decoder, security control panel, video intercom device, etc., should be added to the client for the remote configuration and management, such as live view, playback, alarm settings, etc.

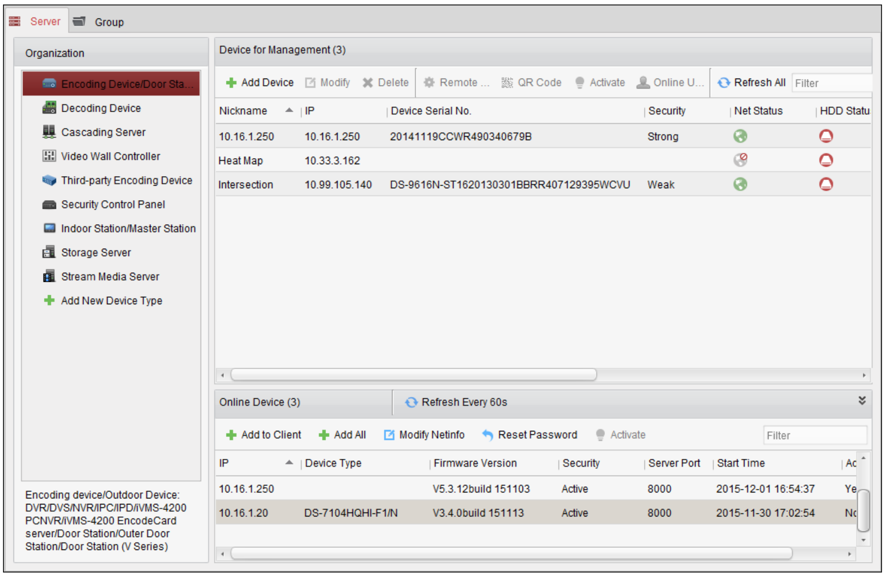
Perform the following steps to enter the Device Adding interface.

Steps:

1. Click the icon on the control panel,

   or click **Tools**->**Device Management** to open the Device Management page.
2. Click the **Server** tab.
3. Click **Encoding Device/Door Station** to enter Encoding Device/Door Station Adding interface.

   Note: Here we take the adding of encoding device as an example.



Nickname	IP	Device Serial No.	Security	Net Status	HDD Statu
10.16.1.250	10.16.1.250	20141119CCWR490340679B	Strong	●	○
Heat Map	10.33.3.162			⊘	○
Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR407129395WCVU	Weak	●	○

IP	Device Type	Firmware Version	Security	Server Port	Start Time	Ac
10.16.1.250		V5.3.12build 151103	Active	8000	2015-12-01 16:54:37	Ye
10.16.1.20	DS-7104HQHI-F1/N	V3.4.0build 151113	Active	8000	2015-11-30 17:02:54	No

Encoding device/Outdoor Device: DVR/DVS/NVR/IPC/IPD/iVMS-4200 PCNVR/iVMS-4200 EncodeCard server/Door Station/Outer Door Station/Door Station (V Series)

You can add the device in the following ways:

- By detecting the online devices, see *Section 3.1.2 Adding Online Devices.*
- By specifying the device IP address or domain name, see *Section 3.1.3 Adding Devices Manually.*
- By specifying an IP segment, see *Section 3.1.4 Adding Devices by IP Segment*.
- By IP Server, see *Section 3.1.5 Adding Devices by IP Server.*
- By HiDDNS, see *Section 3.1.6 Adding Devices by HiDDNS.*
- Adding Devices in batch, see *Section 3.1.7 Batch Adding Devices.*

3.1.1 Creating the Password

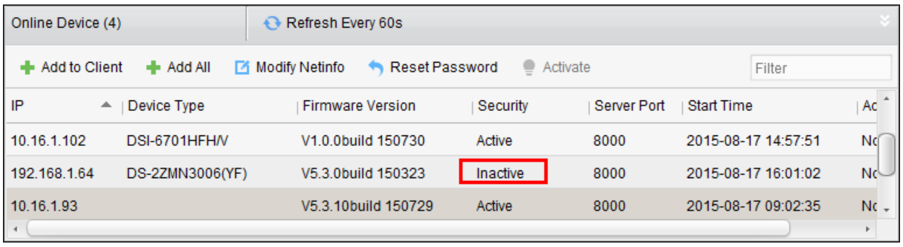
Purpose:

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:

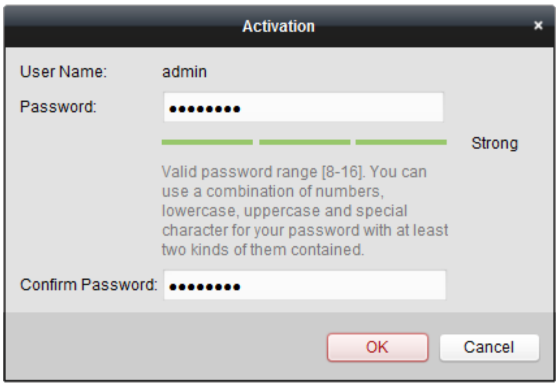
1. Enter the Device Management page.
2. On the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.



IP	Device Type	Firmware Version	Security	Server Port	Start Time	Ac
10.16.1.102	DSI-6701HFH/V	V1.0.0build 150730	Active	8000	2015-08-17 14:57:51	Nc
192.168.1.64	DS-2ZMN3006(YF)	V5.3.0build 150323	Inactive	8000	2015-08-17 16:01:02	Nc
10.16.1.93		V5.3.10build 150729	Active	8000	2015-08-17 09:02:35	Nc

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

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



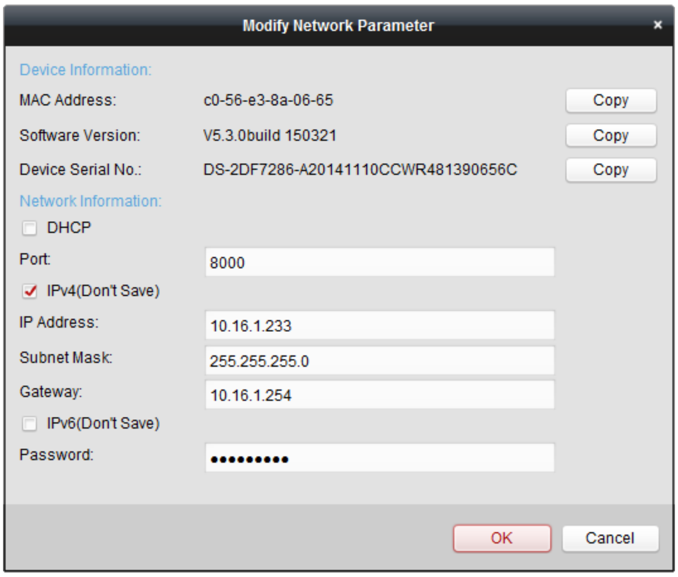
User Name: admin

Password: ••••••••

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

Confirm Password: ••••••••

5. Click **OK** to create the password for the device. A “The device is activated.” window pops up when the password is set successfully.
6. 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.
7. 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.
8. Input the password set in step 4 and click **OK** to complete the network settings.



Device Information:

MAC Address: c0-56-e3-8a-06-65

Software Version: V5.3.0build 150321

Device Serial No.: DS-2DF7286-A20141110CCWR481390656C

Network Information:

□ DHCP

Port: 8000

☑ IPv4(Don't Save)

IP Address: 10.16.1.233

Subnet Mask: 255.255.255.0

Gateway: 10.16.1.254

□ IPv6(Don't Save)

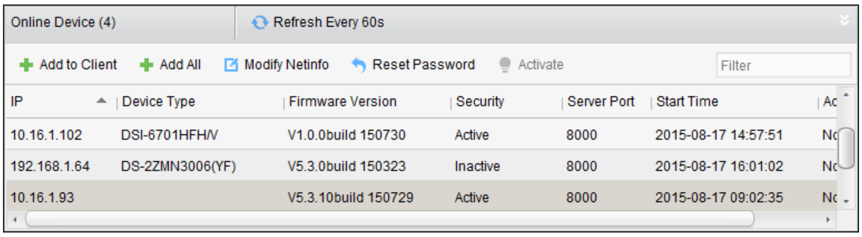
Password: ●●●●●●●●●

3.1.2 Adding Online Devices

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.



IP	Device Type	Firmware Version	Security	Server Port	Start Time	Ac
10.16.1.102	DSI-6701HFH/V	V1.0.0build 150730	Active	8000	2015-08-17 14:57:51	Nc
192.168.1.64	DS-2ZMN3006(YF)	V5.3.0build 150323	Inactive	8000	2015-08-17 16:01:02	Nc
10.16.1.93		V5.3.10build 150729	Active	8000	2015-08-17 09:02:35	Nc

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 3.1.1 Creating the Password*.

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.

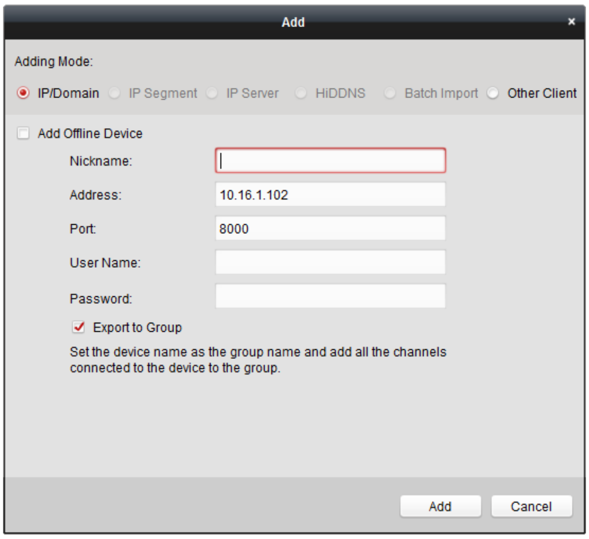
   Port: Input the device port No.. The default value is *8000*.

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

   Password: Input the device password.

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

4. Optionally, you can check the checkbox **Export to Group** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default.
   Note: iVMS-4200 also provides a method to add the offline devices. Check the checkbox **Add Offline Device**, input the required information and the device channel number and alarm input number, and then click **Add**. When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.



Add

Adding Mode:

● IP/Domain ○ IP Segment ○ IP Server ○ HiDDNS ○ Batch Import ○ Other Client

□ Add Offline Device

Nickname:

Address: 10.16.1.102

Port: 8000

User Name:

Password:

☑ Export to Group

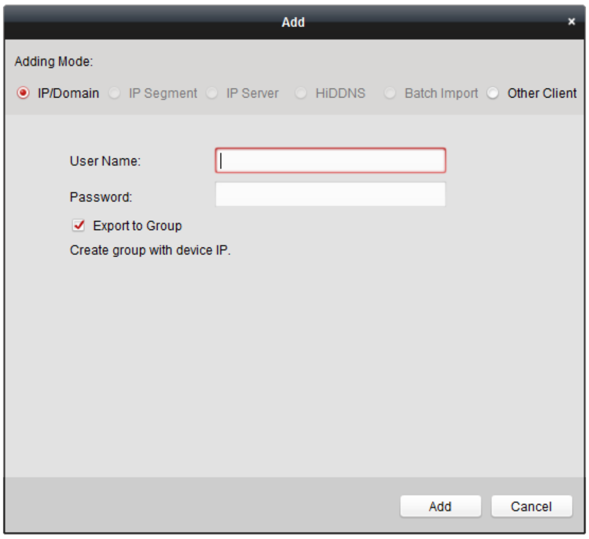
Set the device name as the group name and add all the channels connected to the device to the group.

Add Multiple Online Devices

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.

Add All the 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 Mode:

○ IP/Domain ○ IP Segment ○ IP Server ○ HiDDNS ○ Batch Import ● Other Client

User Name:

Password:

☑ Export to Group

Create group with device IP.

Modify Network Information

Select the device from the list, click **Modify Netinfo**, and then you can modify the network information of the selected device.

Note: You should enter the admin password the device in the **Password** field of the pop-up window to modify the parameters.

Reset Password

According to the different devices, the software provides three different methods for restoring the default password or resetting the password.

Select the device from the list, click **Reset Password**.

Option 1:

If the window with security code field pops up, input the security code, and then you can restore the default password of the selected device.

Note: The security code is returned after you send the data and serial No. of the device to the manufacturer.

Option 2:

If the window with import file and export file buttons pops up, perform the following steps to restore the default password:

1. Click **Export** to save the device file on your PC.
2. Send the file to our technical engineers.
3. Click **Import** and select the file received from the technical engineer.
4. Click **OK** to restore the default password of the device.

- *The default password (12345) for the Admin account is for first-time log-in purposes only. You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.*
- *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.*

Option 3:

If the window with import file and export file buttons, password and confirm password field pops up, follow the steps below to reset the password:

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

⚠

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

Option 4:

If the dialog with Generate buttons, password and confirm password field pops up, follow the steps below to reset the password:

1. Click **Generate** to pop up the QR Code dialog.
2. Click **Download** and select a saving path to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone.
3. Send the picture to our technical engineers and you will receive an eight-digit number from the technical engineer
4. Select **Input Key** from Key Importing Mode drop-down list and input the number.
5. Input new password in text fields of **Password** and **Confirm Password**.
6. Click **OK** to reset the password.

⚠

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

Synchronizing the Password

Purpose:

You can reset the password for the NVR or HDVR and use the new password as the password of the connected network cameras and encoders.

Note: This function should be supported by the device.

Steps:

1. Select a device on the Online Device panel and click **Reset Password**.
2. Perform the password reset steps and check **Use New Password as Camera Password** checkbox.
3. Click **OK** to save the settings.

3.1.3 Adding Devices Manually

Steps:

1. Click **Add Device** 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*.

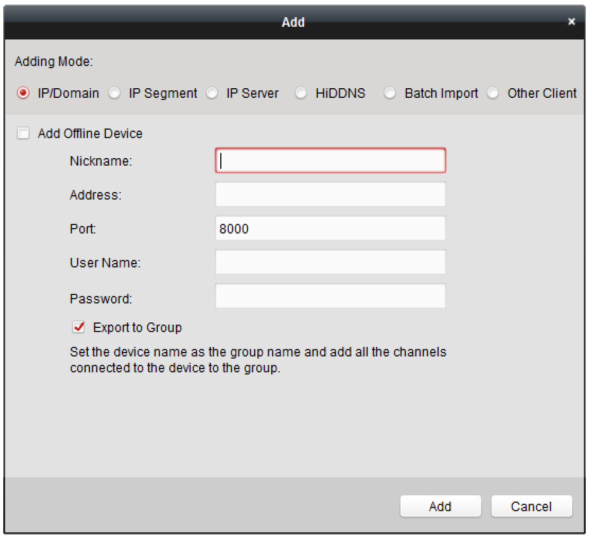
   User Name: Input the device user name. By default, the user name is *admin*.

   Password: Input the device password.

   ⚠

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Optionally, you can check the checkbox **Export to Group** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default.

   Note: iVMS-4200 also provides a method to add the offline devices. Check the checkbox **Add Offline Device**, input the required information and the device channel number and alarm input number, and then click **Add**. When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.



Add

Adding Mode:

● IP/Domain ○ IP Segment ○ IP Server ○ HiDDNS ○ Batch Import ○ Other Client

□ Add Offline Device

Nickname:

Address:

Port: 8000

User Name:

Password:

☑ Export to Group

Set the device name as the group name and add all the channels connected to the device to the group.

3.1.4 Adding Devices by IP Segment

Steps:

1. Click **Add Device** 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*.

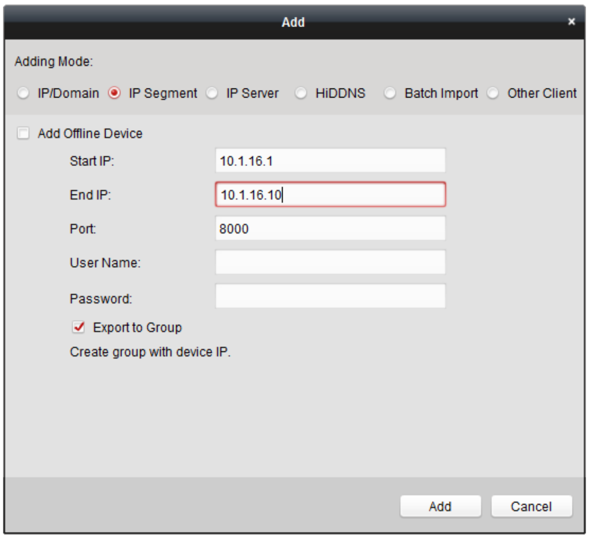
   User Name: Input the device user name. By default, the user name is *admin*.

   Password: Input the device password.

   ⚠

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Optionally, you can check the checkbox **Export to Group** to create a group by the device IP. All the channels of the device will be imported to the corresponding group by default.

   Note: iVMS-4200 also provides a method to add the offline devices. Check the checkbox **Add Offline Device**, input the required information and the device channel number and alarm input number, and then click **Add**. When the offline device comes online, the software will connect it automatically.
5. Click **Add**, and the device of which the IP address is between the start IP and end IP will be added to the device list.



Adding Mode:

○ IP/Domain ● IP Segment ○ IP Server ○ HiDDNS ○ Batch Import ○ Other Client

□ Add Offline Device

Start IP: 10.1.16.1

End IP: 10.1.16.10

Port: 8000

User Name:

Password:

☑ Export to Group

Create group with device IP.

3.1.5 Adding Devices by IP Server

Steps:

1. Click **Add Device** 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.

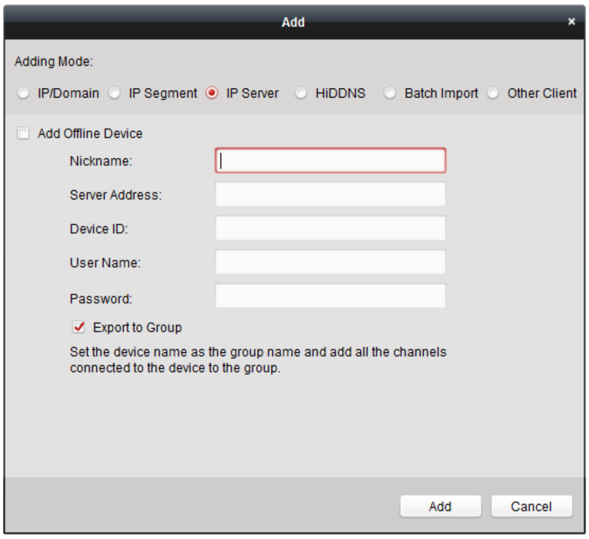
   Device ID: Input the device ID registered on the IP Server.

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

   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Optionally, you can check the checkbox **Export to Group** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default.

   Note: iVMS-4200 also provides a method to add the offline devices. Check the checkbox **Add Offline Device**, input the required information and the device channel number and alarm input number, and then click **Add**. When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.



Adding Mode:

○ IP/Domain ○ IP Segment ● IP Server ○ HiDDNS ○ Batch Import ○ Other Client

□ Add Offline Device

Nickname:

Server Address:

Device ID:

User Name:

Password:

☑ Export to Group

Set the device name as the group name and add all the channels connected to the device to the group.

3.1.6 Adding Devices by HiDDNS

Steps:

1. Click **Add Device** 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*.

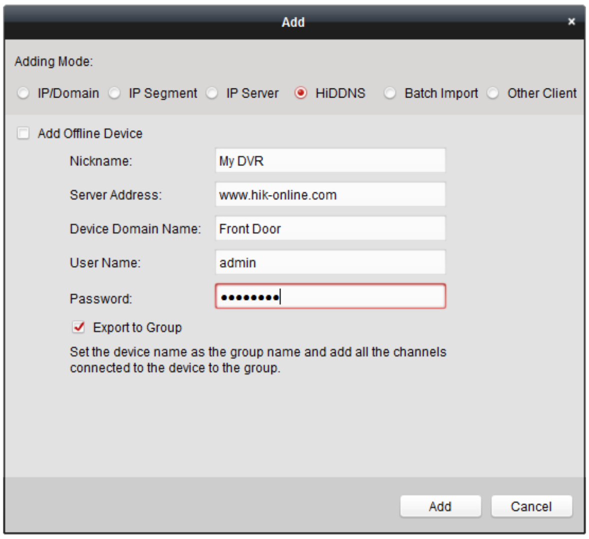
   Device Domain Name: Input the device domain name registered on HiDDNS server.

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

   Password: Input the device password.

   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Optionally, you can check the checkbox **Export to Group** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default.

   Note: iVMS-4200 also provides a method to add the offline devices. Check the checkbox **Add Offline Device**, input the required information and the device channel number and alarm input number, and then click **Add**. When the offline device comes online, the software will connect it automatically.
5. Click **Add** to add the device.



Adding Mode:

○ IP/Domain ○ IP Segment ○ IP Server ● HiDDNS ○ Batch Import ○ Other Client

□ Add Offline Device

Nickname: My DVR

Server Address: www.hik-online.com

Device Domain Name: Front Door

User Name: admin

Password: ••••••••

☑ Export to Group

Set the device name as the group name and add all the channels connected to the device to the group.

3.1.7 Batch Adding Devices

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 Device** 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, or 3 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.

   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.

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

   Password: Input the device password.

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

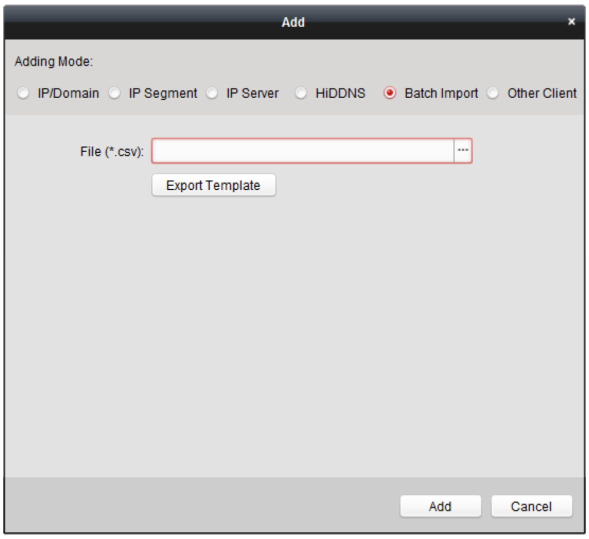
Add Offline Device: You can input 1 to enable adding the offline device, and then the software will automatically connect it when the offline device comes online. 0 indicates disabling this function.

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.

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



Add

Adding Mode:

○ IP/Domain ○ IP Segment ○ IP Server ○ HiDDNS ● Batch Import ○ Other Client

File (*.csv):

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.

Select device from the list, click **Modify**/**Delete**, and then you can modify/delete the information of the selected device.

Select device from the list, click **Remote Configuration**, and then you can do some remote configurations of the selected device if needed. For detailed settings about the remote configuration, please refer to the *User Manual* of the devices.

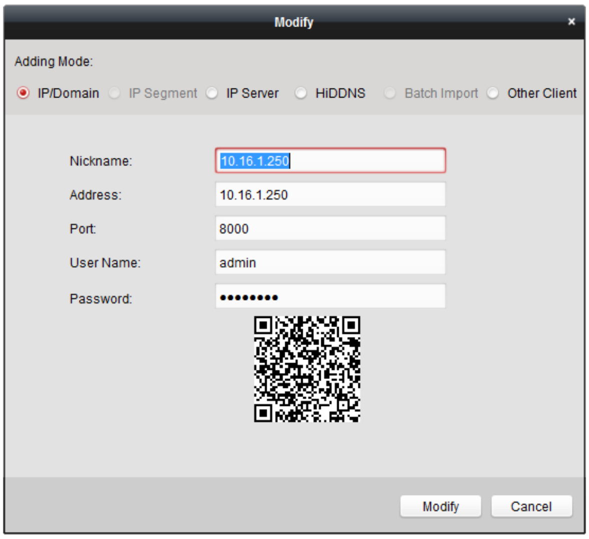
3.1.8 QR Code of Encoding Devices

Purpose:

For encoding devices, the QR code of the devices can be generated. You can add the device to your mobile client software by using the mobile client software to scan the QR code. For adding the devices to your mobile client software, please refer to the *User Manual* of the mobile client software.

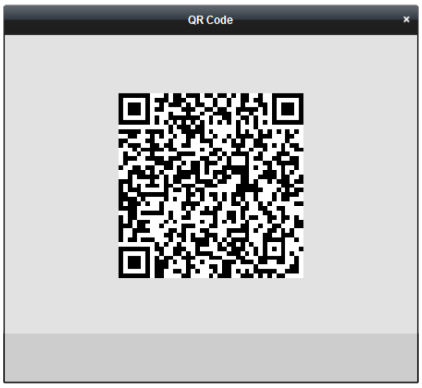
Check the QR Code

On the device list, double-click a device, the information and QR code of the device will be displayed. Or you can click to select a device and click **QR Code** to pop up the QR code window of the device. You can also click and hold the Ctrl key to select multiple devices, and click **QR Code** to pop up the QR code window of the devices. In this way, you can add multiple devices at the same time by scanning the QR code.



Adding Mode:
● IP/Domain ○ IP Segment ○ IP Server ○ HiDDNS ○ Batch Import ○ Other Client

Nickname: 10.16.1.250
Address: 10.16.1.250
Port: 8000
User Name: admin
Password: ••••••••



3.1.9 Checking Device’s Online Users

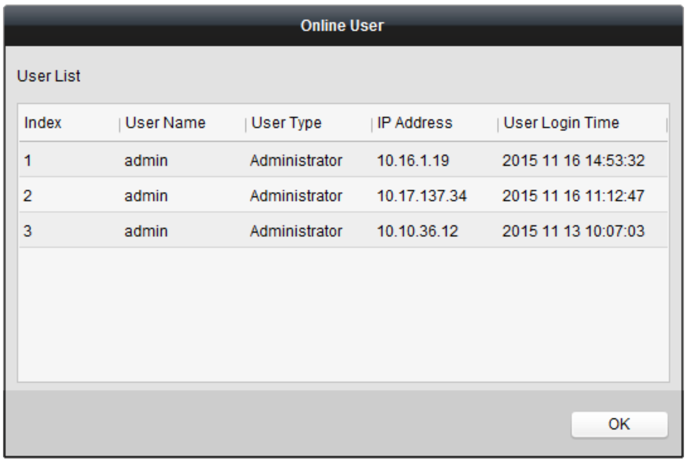
Purpose:

When any user accesses the device, the client can record and show the connection information, including user name, user type, user’s IP address, and login time.

Note: This function should be supported by the device.

Steps:

1. Click to select an added and online device.
2. Click **Online Users** to pop up the Online Users dialog.



Index	User Name	User Type	IP Address	User Login Time
1	admin	Administrator	10.16.1.19	2015 11 16 14:53:32
2	admin	Administrator	10.17.137.34	2015 11 16 11:12:47
3	admin	Administrator	10.10.36.12	2015 11 13 10:07:03

3. Check the information of the users that log into the device.
4. Click **OK** to close the dialog.

3.2 Group Management

Purpose:

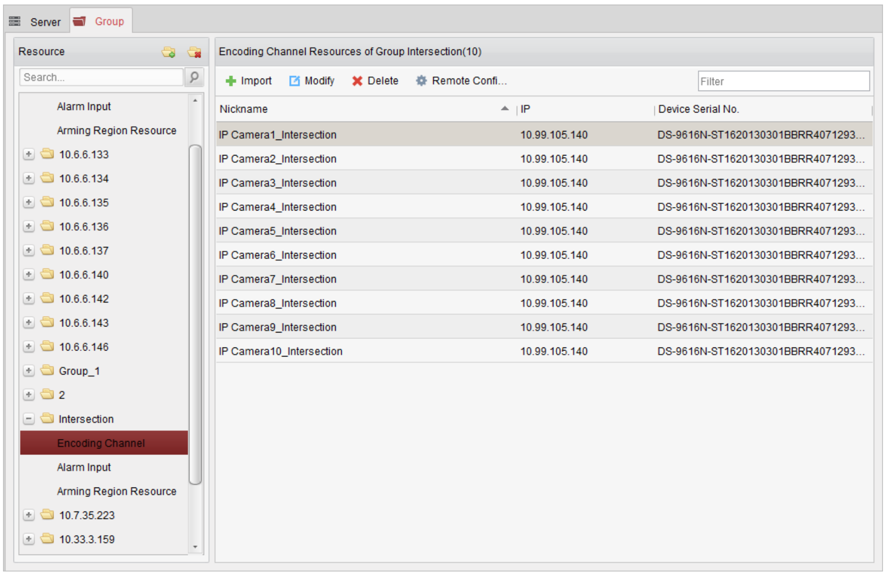
The devices added should be organized into groups for a convenient management. You can get the live view, play back the video files, and do some other operations of the device through the group.

Before you start:

Devices need to be added to the client software for group management.

Perform the following steps to enter the Group Management interface:

1. Open the Device Management page.
2. Click the **Group** tab to enter the Group Management interface.



Encoding Channel Resources of Group Intersection(10)

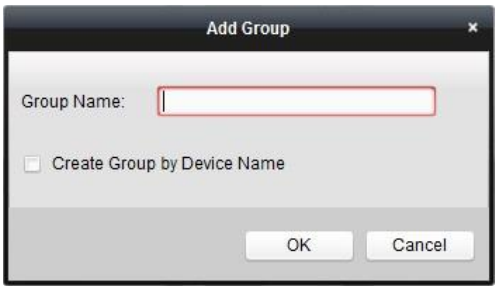
Nickname	IP	Device Serial No.
IP Camera1_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera2_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera3_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera4_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera5_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera6_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera7_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera8_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera9_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...
IP Camera10_Intersection	10.99.105.140	DS-9616N-ST1620130301BBRR4071293...

Adding the Group

Steps:

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.



Group Name:

□ Create Group by Device Name

Importing Encoding Device to Group

Steps:

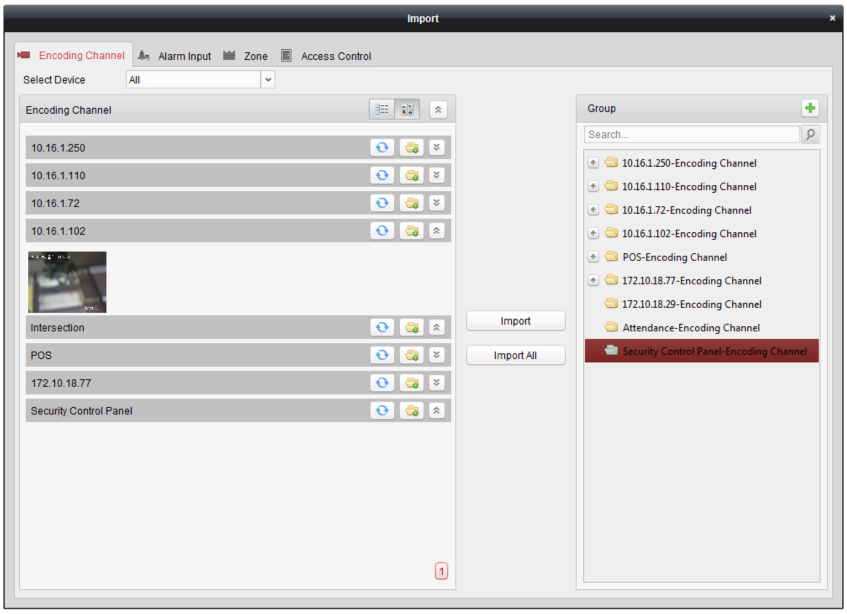
1. Click **Import** on Group Management interface, and then click the **Encoding Channel** tab to open the Import Encoding Channel page.

   Note: You can also select **Alarm Input** tab and import the alarm inputs to group.
2. Select the thumbnails/names of the cameras in the thumbnail/list view.
3. Select a group from the group list.
4. Click **Import** to import the selected cameras to the group.

   You can also click **Import All** to import all the cameras to a selected group.

Notes:

- You can also click the icon + on the Import Encoding Channel page to add a new group.
- Up to 256 cameras can be added to one group.


Import
Encoding Channel
Alarm Input
Zone
Access Control
Select Device
All
Encoding Channel
10.16.1.250
10.16.1.110
10.16.1.72
10.16.1.102
Intersection
POS
172.10.18.77
Security Control Panel
1
Import
Import All
Group
Search...
10.16.1.250-Encoding Channel
10.16.1.110-Encoding Channel
10.16.1.72-Encoding Channel
10.16.1.102-Encoding Channel
POS-Encoding Channel
172.10.18.77-Encoding Channel
172.10.18.29-Encoding Channel
Attendance-Encoding Channel
Security Control Panel-Encoding Channel

The following buttons are available on the Import Encoding Channel page:

	List View	View the camera in list view.
	Thumbnail View	View the camera in thumbnail view.
	Refresh	Refresh the latest information of added cameras.
	Import	Create a group named as *device name-Encoding Channel (Alarm Input)* and import the device to group.
	Collapse/Expand	Collapse/Expand the thumbnails of cameras.

Modifying the Group/Camera

Steps:

1. Select the group/camera from the group list on the Import page.

   Move the mouse to the camera/group and click ✎, or double-click the group/camera name to open Modify Group/Camera dialog box.
2. Edit the group/camera information, including the group/camera name, the stream type, etc.

   Video Stream: Select the stream for the live view or playback of the camera as desired.

Rotate Type: Select the rotate type for the live view or playback of the camera as desired.

Protocol Type: Select the transmission protocol for the camera.

Stream Media Server: Configure to get stream of the camera via stream media server. You can select and manage the available stream media server.

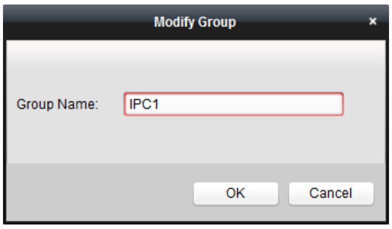
Copy to…: Copy the configured parameters to other camera(s).

Refresh: Get a new captured picture for the live view of the camera.

Note: For video stream and protocol type, the new settings will take effect after you reopen the live view of the camera.

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

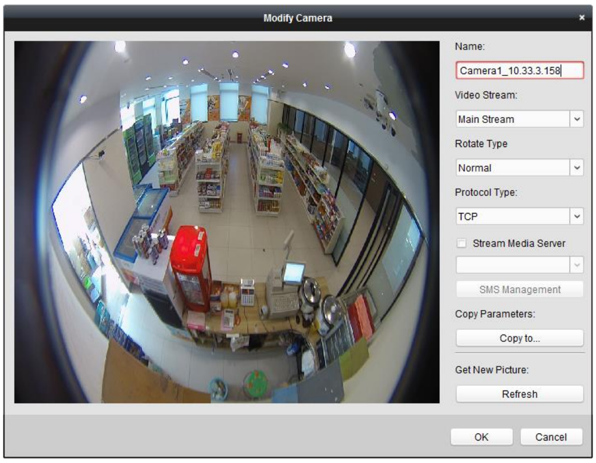
   You can also double click the encoding channel on the Resource list in the Group Management interface after encoding channels encoded, or select the encoding channel and click Modify to open the Modify Camera dialog box.



Modify Group ×

Group Name: IPC1

OK Cancel



Modify Camera ×

Name: Camera1_10.33.3.158

Video Stream: Main Stream

Rotate Type: Normal

Protocol Type: TCP

□ Stream Media Server

SMS Management

Copy Parameters: Copy to...

Get New Picture: Refresh

OK Cancel

Notes:

For the IP channel of NVR which supports decoding function:

- After decoding and displaying on video wall, there will be a new channel in the Encoding Channel Resources list whose protocol type is decoding on video wall.
- After closing the corresponding roaming window, the new channel will be removed from the Encoding Channel Resources list.

Removing Cameras from the Group

Steps:

1. Select the camera from the group list on the Import Encoding Channel page.
2. Move the mouse to the camera and click ✖ to remove the camera from the group.

   You can also select the camera on the Group Management interface, and then click **Delete** to remove the camera from the group.
3. Select the group from the group list on the Import Encoding Channel page, move the mouse to the group and click ✖ and you can remove all the cameras from the group.

Deleting the Group

Steps:

1. Select the group on the Group Management interface

2. Click **Delete Group**, or move the mouse to the group and click the icon ✖, the selected group and the resource under it will be deleted.

Chapter 4 Live View

Purpose:

For the surveillance task, 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.

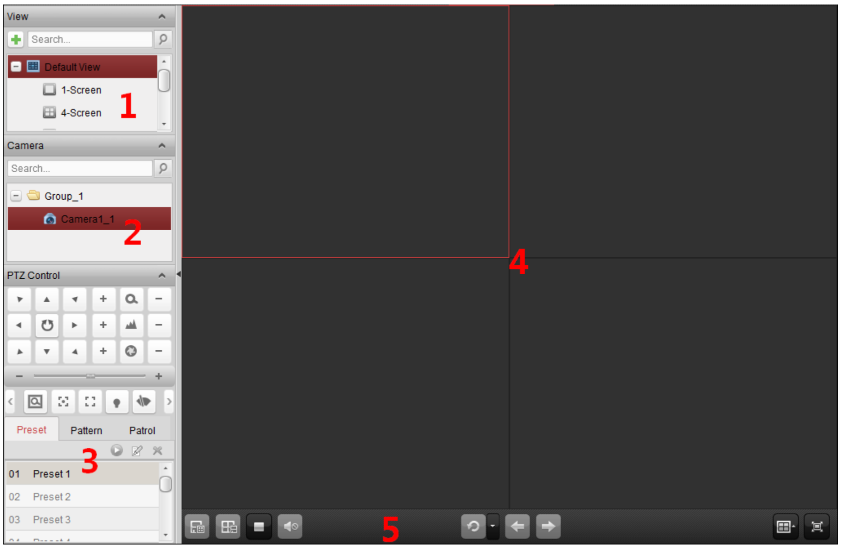
Before you start:

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 *Modifying the Group/Camera* of *Chapter 3.2 Group Management*.

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.

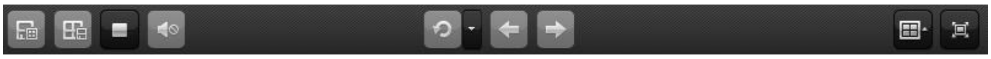
The camera is offline.

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 . For configuring the stream media server of the camera, refer to *Chapter 11 Forwarding Video Stream through Stream Media Server.*

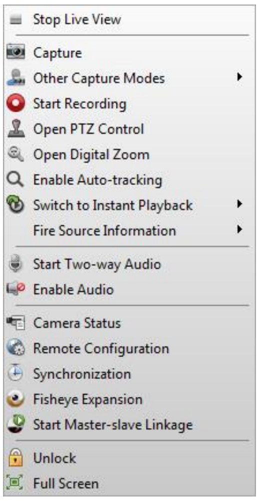
Live View Toolbar:



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.
	Other Capture Modes	**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. **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.
	Open PTZ Control	Enable PTZ control function on the display window. Click again to disable the function.
	Open Digital Zoom	Enable the digital zoom function. 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.
	Switch to Instant Playback	Switch to instant playback mode.
	Fire Source Information	For thermal camera, click to display the fire source region, display the maximum temperature information, locate the maximum temperature region, or display the fire source target.
	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.
	Fisheye Expansion	Enter the fisheye expansion mode. Only available when the device is fisheye camera. For details, please refer to *Chapter 4.7 Live View in Fisheye Mode.*
	Start/Stop Master-slave Linkage	Click to start/stop locating or tracking the target according to your demand. Only available when the device is fisheye camera or box/bullet camera. For details, please refer to *Chapter 4.8 Starting Master-slave Linkage.*
	Unlock	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.

4.1 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.

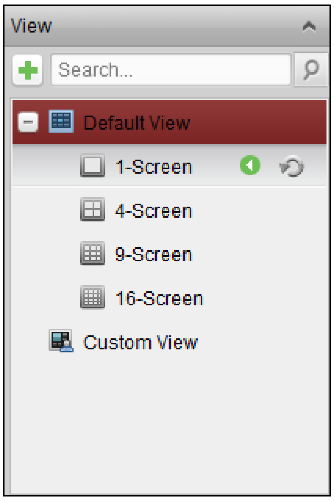
Steps:

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. For details, please refer to *Chapter 4.2 Auto-switch in Live View*.



Starting Live View in Custom View Mode

Purpose:

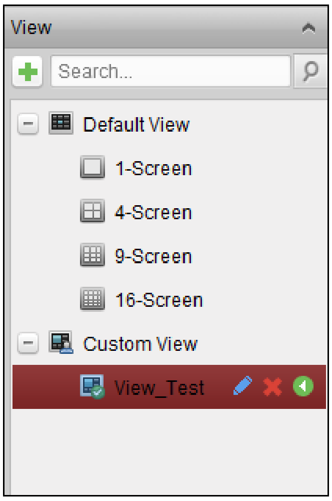
The view mode can also be customized for the video live view.

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.

4.2 Auto-switch in Live View

Camera Auto-switch

Purpose:

The video stream of the cameras from the same group will switch automatically in a selected display window in camera auto-switch.

Steps:

1. Open the Main View page.
2. Select a display window for camera auto-switch.
3. Click the icon ▾ in the toolbar and select or customize the switching interval.
4. Select a group and click the icon ↻ on the group node.
5. You can click the icon ⏸/↻ to pause/resume the camera auto-switch.
6. You can click ← or → to view the live video of previous or next camera.

Single View Auto-switch

Purpose:

The video of all the cameras on the camera list will switch automatically in a selected default view in single view auto-switch.

Steps:

1. Open the Main View page.
2. Click the icon ▾ in the toolbar and select or customize the switching interval.
3. Select a default view and click the icon ↻ on the selected view node.
4. You can click the icon ⏸/↻ to pause/resume the single view auto-switch.
5. You can click ← or → to view the live video of previous or next camera.

Multi-view Auto-switch

Purpose:

The custom views will switch automatically in multi-view auto-switch. The custom views need to be added before proceeding.

Steps:

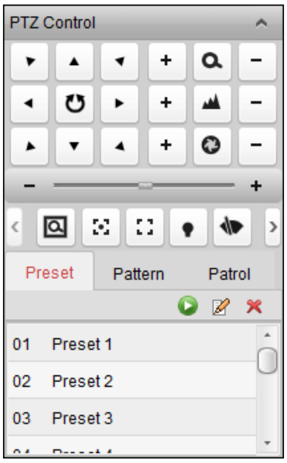
1. Open the Main View page.
2. Click the icon ▾ in the toolbar and select the switching interval.
3. Click the icon ↻ on the custom view node.
4. You can click the icon ⏸/↻ to pause/resume the multi-view auto-switch.

5. You can click or to view the live video of previous or next camera.

4.3 PTZ Control in Live View

The software provides PTZ control for cameras with pan/tilt/zoom functionality. You can set the preset, patrol and pattern for the cameras on the PTZ Control panel. And you can also open window PTZ control for the operations of PTZ cameras.

Click the icon to expand the PTZ Control panel.



01 Preset 1
02 Preset 2
03 Preset 3

The following buttons are available on the PTZ Control panel:

Zoom

Focus

Iris

3D Positioning

Auxiliary Focus

Lens Initialization

Light

Wiper

Manual Tracking

Menu

One-touch Patrol

One-touch Park

Notes:

- For the analog speed dome, you can click ☰ to display its local menu. For detailed operation of the menu, please refer to the *User Manual* of the speed dome.
- For the speed dome with auto-tracking function, you can enable the auto-tracking (via right-click menu) for it and then click to manually track the target by clicking on the video.
- For the one-touch patrol function, you can click and the speed dome will start patrol from the predefined preset No.1 to preset No.32 in order after a period of inactivity (park time). For setting the park time, please refer to the *User Manual* of the speed dome.
- For the speed dome with one-touch park function, you can enable the one-touch park by clicking and the speed dome will save the current view to the preset No.32. The device starts to park at preset No. 32 automatically after a period of inactivity (park time). For setting the parking time, please refer to the *User Manual* of the speed dome.

Configuring the Preset

A preset is a predefined image position which contains information of pan, tilt, focus and other parameters.

Perform the following steps to add a preset:

1. Click the **Preset** button to enter the PTZ preset configuration panel.
2. Click the direction buttons and other buttons on the PTZ control panel to steer the camera to the desired view.
3. Select a PTZ preset number from the preset list and click ✎.
4. Input the name of the preset in the pop-up dialog box.
5. Click **OK** to save the settings.

To call a configured preset, double-click the preset, or select the preset and click the icon ▶.

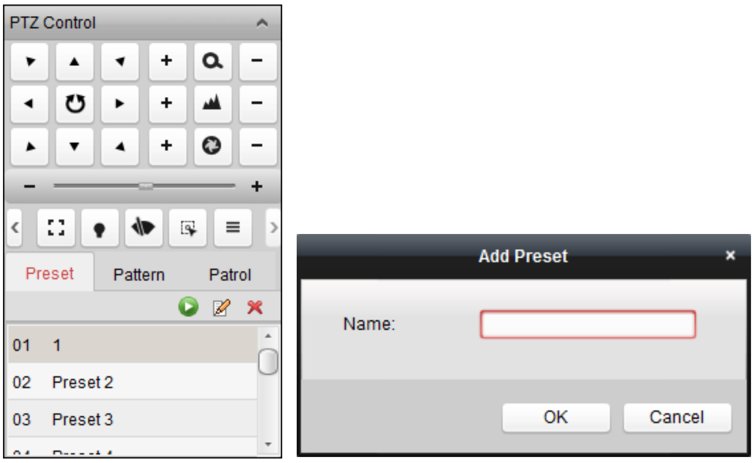
You also perform the following steps to call the preset.

Steps:

1. Click to select a live view window.
2. For preset 1 to 9, click the corresponding number key (e.g., 4) to call the preset.
   For other presets, click "[", number keys (e.g., 124), and "]" to call the preset.

To modify a configured preset, select the preset from the list and click the icon ✎.

To delete a configured preset, select the preset from the list and click the icon ✖.

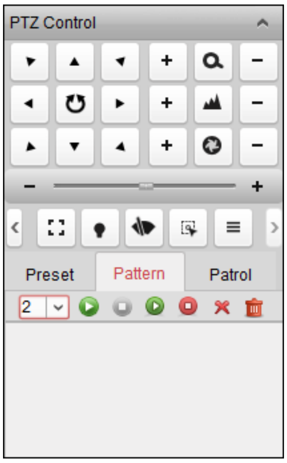


Configuring the Pattern

A pattern is a memorized, repeating series of pan, tilt, zoom, and preset functions.

Perform the following steps to add a pattern:

1. Click the **Pattern** button to enter the PTZ pattern configuration panel.
2. Click ▶ to start recording of this pattern path.
3. Use the direction buttons to control the PTZ movement.
4. Click ■ to stop and save the pattern recording.
5. Click the icon ▶ to call the pattern. To stop calling the pattern, click ■.
6. (Optional) You can click ✖ to delete the selected pattern.
   Click 🗑 to delete all the patterns.



Configuring the Patrol

A patrol is a scanning track specified by a group of user-defined presets, with the scanning speed between two presets and the dwell time at the preset separately programmable.

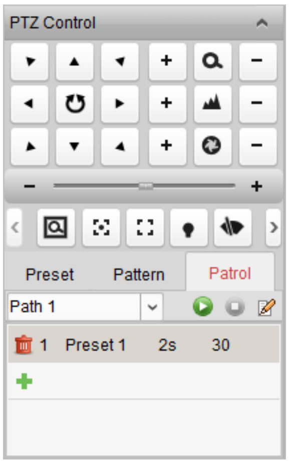
Before you start:

Two or more presets for one PTZ camera need to be added.

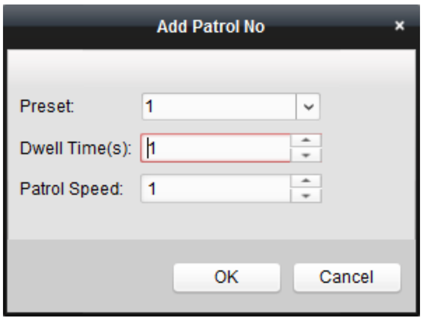
Perform the following steps to add and call a patrol:

1. Click the **Patrol** button to enter the PTZ patrol configuration panel.
2. Select a track number from the drop-down list.
3. Click ✚ to add a preset, and set the dwell time and patrol speed for the preset.
4. Repeat the above operation to add other presets to the patrol.
5. Optionally, you can click ✎ or 🗑 to edit or delete a preset in the patrol path.
6. Click the icon ▶ to call the patrol. To stop calling the patrol, click ⏹.

Note: The preset dwell time can be set to 1 to 30 sec, and the patrol speed can be set to level 1 to 40.



1	Preset 1	2s	30



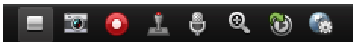
Preset: 1

Dwell Time(s): 1

Patrol Speed: 1

4.4 Manual Recording and Capture

Toolbar in Each Live View Display Window:



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

■	**Stop Live View**	Stop the live view in the display window.
📷	**Capture**	Capture the picture in the live view process. The capture picture is stored in the PC.
● R	**Start/Stop Recording**	Start/Stop manual recording. The video file is stored in the PC.
🕹	**Open/Close PTZ Control**	Start/Stop PTZ mode for speed dome. Click and drag in the view to perform the PTZ control.
🎤	**Start/Stop Two-way Audio**	Click to start/stop the two-way audio with the device in live view.
🔍	**Open/Close Digital Zoom**	Enable the digital zoom function. Click again to disable the function.
↻	**Switch to Instant Playback**	Switch to the instant playback mode.
⚙	**Remote Configuration**	Open the remote configuration page of the camera in live view.

Note: You can customize the icons and the icons' order as desired in System Configuration. For details, refer to *Chapter 17.2.5 Toolbar Settings.*

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 R.
3. Click the icon R 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 R 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 17.2.4 File Saving Path Settings.*
- For Hik Cloud P2P device, the manual recording is not supported during live view.

Viewing Local Video Files

Steps:

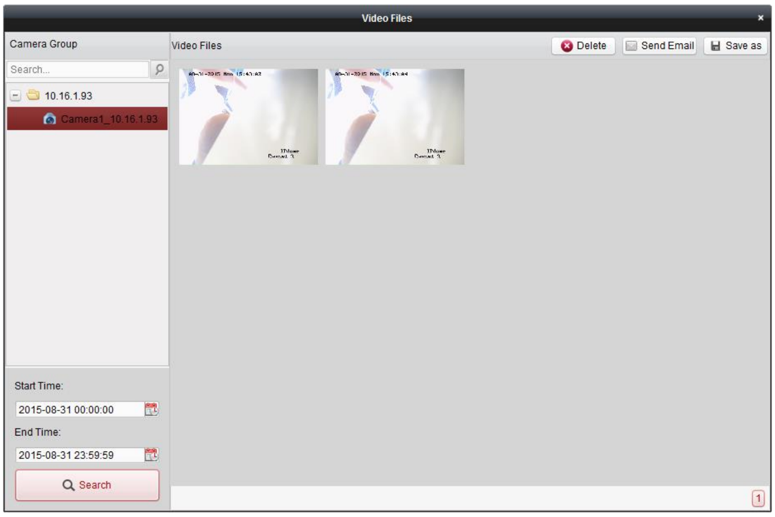
1. Click **File**->**Open Video File** to open the Video Files page.
2. Select the camera to be searched from the Camera Group list.
3. Click the icon 📅 to specify the start time and end time for the search.
4. Click **Search**. The video files recorded between the start time and end time will be displayed.

   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.

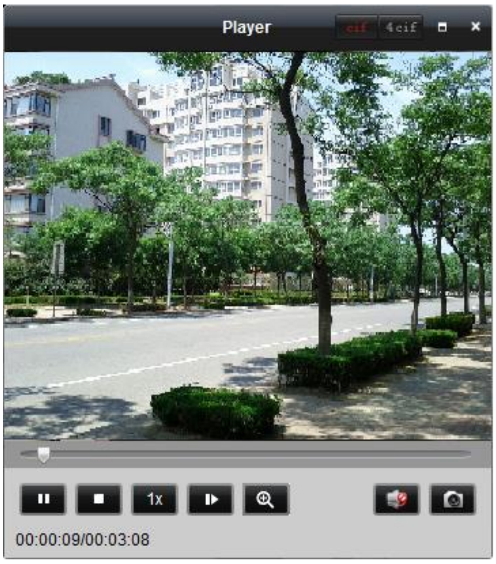
Note: To send an Email notification, the Email settings need to be configured before proceeding. For details, see *Section 17.2.8 Email Settings*.



Start Time: 2015-08-31 00:00:00

End Time: 2015-08-31 23:59:59

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	**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.
1x	**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 *Section 17.2.4 File Saving Path Settings.*

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:

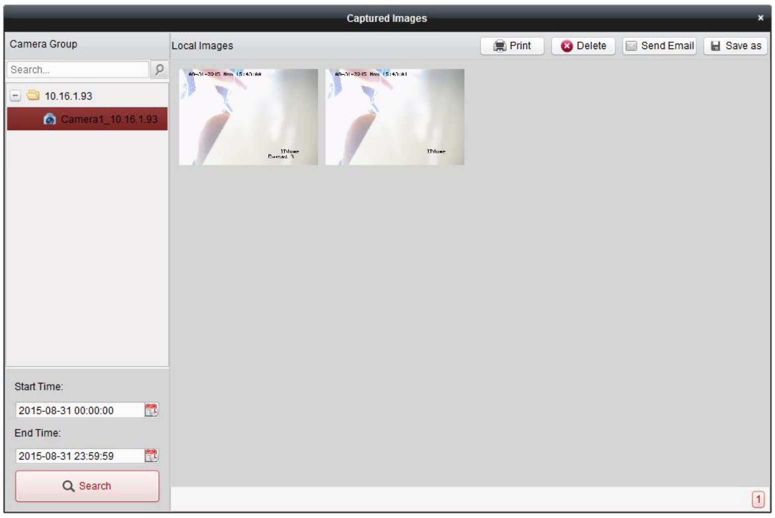
1. Click **File**->**Open Image File** to open the Captured Images page.
2. Select the camera to be searched from the Camera Group list.
3. Click the icon to specify the start time and end time for the search.
4. Click **Search**. The pictures captured between the start time and end time will be displayed.
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.



Start Time: 2015-08-31 00:00:00

End Time: 2015-08-31 23:59:59

4.5 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.

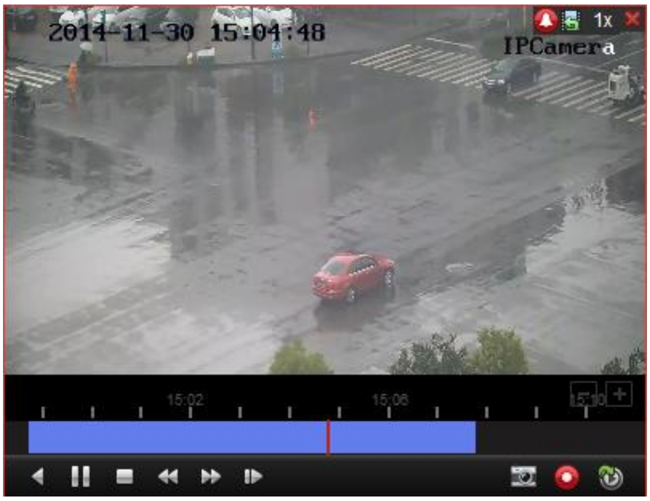
Before you start:

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.

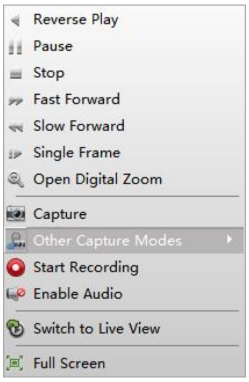
Note: During the instant playback, an indicator ▣ appears in the upper-right corner of the display window.



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.
	Other Capture Modes	**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. **Custom Capture:** Capture the current picture. You can edit its name and then save it.
●	**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.

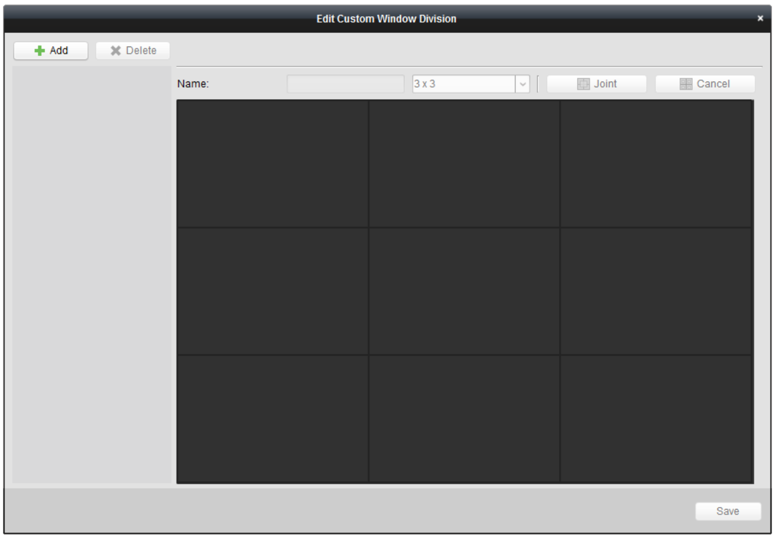
4.6 Custom Window Division

Purpose:

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

Steps:

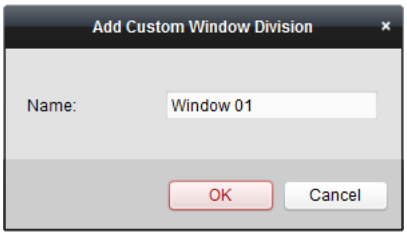
1. Click ⊞ on the live view toolbar and select Edit to pop up the custom window division dialog box.



2. Click **Add** to open the custom window division adding dialog box.

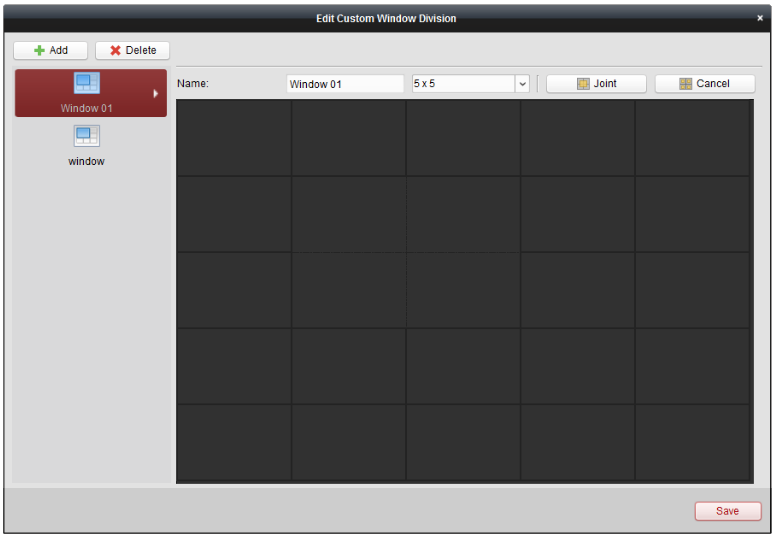
   Note: Up to 5 custom window divisions can be added.

3. Set a name for the new window division as desired and click **OK** to save the settings.



Name: Window 01

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.



Name: Window 01 5 x 5

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.

4.7 Live View in Fisheye Mode

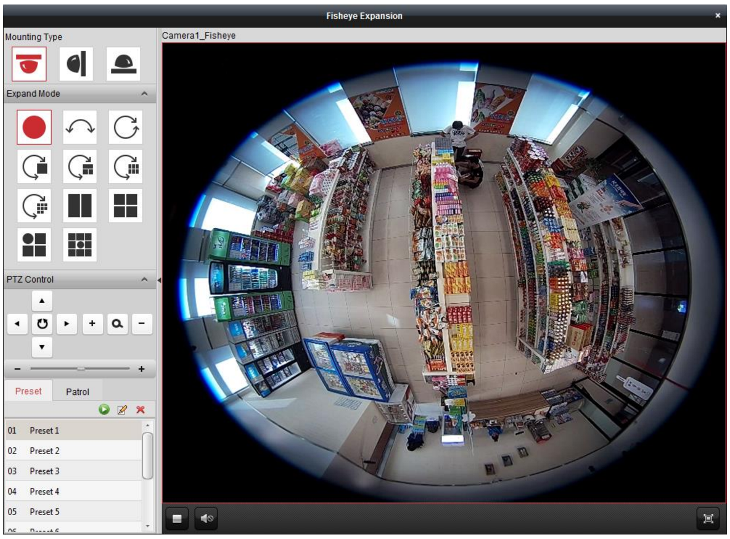
Purpose:

The live video of the camera can be played in fisheye expansion mode.

Steps:

1. Start the live view (refer to *Chapter 4.1 Starting and Stopping the Live View*).
2. Right-click on the video and select **Fisheye Expansion** to enter the Fisheye Expansion window.
3. Select the mounting type of the fisheye camera according to the actual mounting position.
4. You can select the expand mode for live view as desired.

   Note: For some devices, you can select the mounting type of the device and the related expand mode will be listed.



- **Fisheye:** In the Fisheye view mode, the whole wide-angle view of the camera is displayed. This view mode is called Fisheye because it approximates the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.
- **Panorama/Dual-180° Panorama/360° Panorama:** In the Panorama view mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.
- **PTZ:** The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view, and it supports the electronic PTZ function, which is also called e-PTZ.
  Note: Each PTZ view is marked on the Fisheye view and Panorama view with a specific navigation box. You can drag the navigation box on the Fisheye view or Panorama view to adjust the PTZ view, or drag the PTZ view to adjust the view to the desired angle.

5. You can right click on the window and select **Capture** to capture the picture in the live view process. The capture picture is stored in the PC.
6. Right-click on a playing window and you can switch the selected window to full-screen mode Press *ESC* key on the keyboard or right-click on the window and select **Quit Full Screen** to exit the full-screen mode.

PTZ Control

In PTZ mode, you can use the PTZ control to adjust the PTZ window.

Note: The PTZ panel varies according to different devices.

- Select a PTZ window, and click one of the direction buttons to adjust the view angle.
  Note: Click-and-drag the No. label in the fisheye or panorama window will change the view angle of the PTZ window as well.
- Select a PTZ window, and click ⟳ to start auto-scan, and click it again to stop auto-scan.
- − ——— + : Drag the slider to adjust the speed for PTZ movement.
- + 🔍 − : Zoom in or zoom out the selected PTZ window by clicking + or −. Or you can scroll the mouse wheel to zoom in or zoom out.

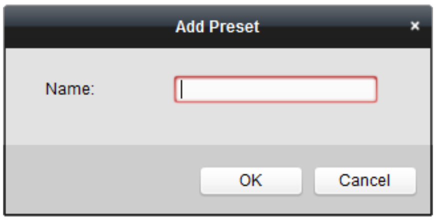
Preset

Note: The preset is only supported by specific fisheye camera.

A preset is a user-defined monitor position/point. You can simply call the preset No. to change the monitor scene to the defined position. Please follow the steps below to configure the preset.

Steps:

1. Click **Preset** tab to enter the preset configuration interface.
2. Select a PTZ window, and adjust the scene to the place you want to mark as a preset.
3. Click ✎, input the preset name, and click **OK** to save a preset.



Name:

4. (Optional) Click ▶ to call the configured preset.
5. (Optional) Click ✖ to delete the configured preset.

Patrol

Note: The preset is only supported by specific fisheye camera.

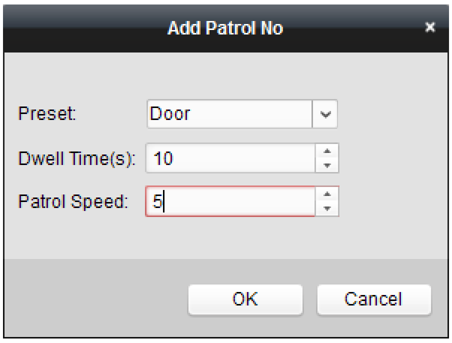
A patrol is a scanning track specified by a group of user-defined presets, with the scanning speed between two presets and the dwell time at the preset separately programmable. Please follow the steps below to configure the patrol.

Note:

At least 2 presets have to be configured before you configure the patrol.

Steps:

1. Click patrol tab to enter the patrol configuration interface.
2. Select a path No. from the drop-down list.
3. Click ✚ to add the configured presets, and set the dwell time and patrol speed for the preset.
4. Repeat the above operation to add other presets to the patrol.



Preset: Door

Dwell Time(s): 10

Patrol Speed: 5

5. Click ▶ to start the patrol, and click ■ to stop patrol.
6. Optionally, you can click ✎ or 🗑 to edit or delete a preset in the patrol path.

Notes:

- Up to 256 presets can be configured.
- Up to 32 patrols can be set.
- The dwell time ranges from 1 to 120s.
- The patrol speed ranges from 1 to 40.

4.8 Starting Master-slave Linkage

Purpose:

The fisheye camera and box/bullet camera support master-slave linkage function so as to locate or tracking the target according to your demand.

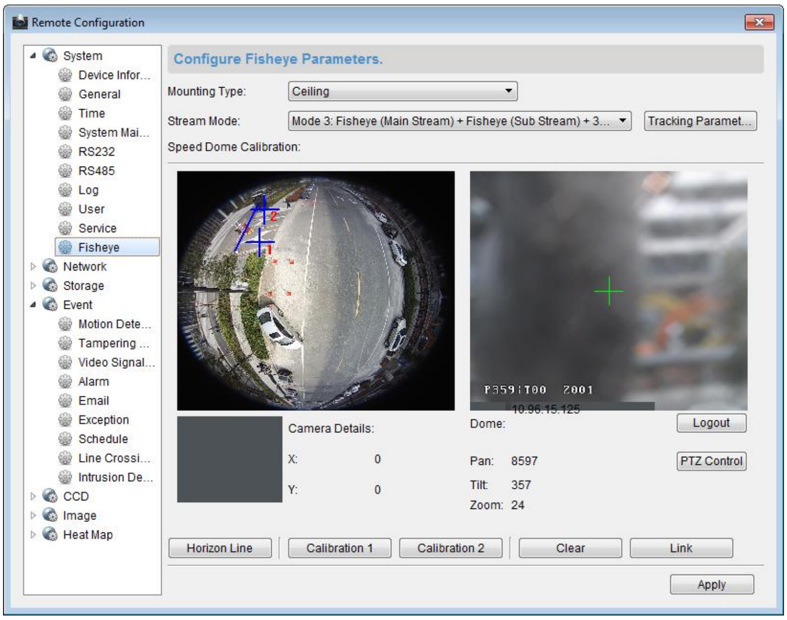
Notes:

- This function in only supported by the specific fisheye or box/bullet camera.
- A speed dome with the auto-tracking function is required to be installed near the camera.

Master-slave Linkage for Fisheye Camera

Steps:

1. Right click on the panorama view of fisheye camera and select **Remote Configuration** to enter the Remote Configuration interface.
2. Click **Fisheye** menu to enter the following interface.



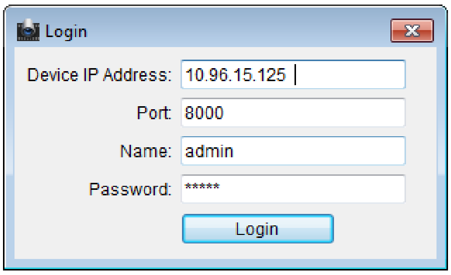
Mounting Type: Ceiling

Stream Mode: Mode 3: Fisheye (Main Stream) + Fisheye (Sub Stream) + 3...

Camera Details:
X: 0
Y: 0

Dome:
Pan: 8597
Tilt: 357
Zoom: 24

3. Select the mounting type of the speed dome, and select the stream mode for the fisheye camera.
4. Click **Login** to add the speed dome.



Device IP Address: 10.96.15.125

Port: 8000

Name: admin

Password: *****

Input the device IP address, port No., user name, password, and click **Login**.

5. Click **PTZ Control**, and use the direction arrows to adjust the speed dome to a horizontal position.

   Note: If the speed dome is adjusted to the horizontal position, the tilt degree is close to 0.

6. Click **Horizon Line** to set a horizon line, and a message of “Setting horizontal line succeeded”

pops up if the line is set.

7. Move the No.1 calibration cross to the middle area of the fisheye camera, and you will see a small picture under the fisheye camera. Use the PTZ to adjust the speed dome to the same position, and click **Calibration 1** to finish a calibration setting.
8. Move the No.2 calibration cross to the second position, and use the PTZ to adjust the speed dome to the same position, and click **Calibration 2** to finish the second calibration setting.

   Note: You can click **Clear** to delete the configured calibrations.
9. Click **Link** to link the speed dome to the fisheye camera.
10. Click **Tracking Parameters** to select the tracking method.

    Notes:

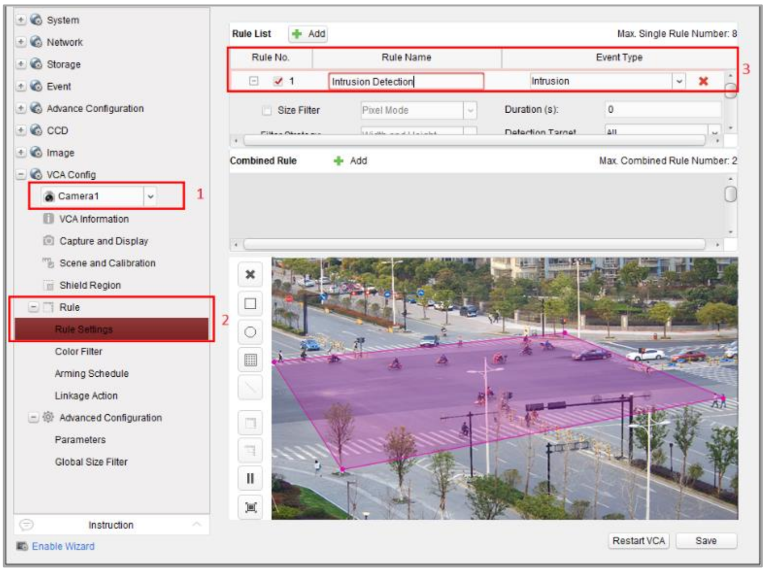
    - The speed dome linkage works as the linkage method of the intrusion detection and line crossing detection if any of those alarms is triggered.
    - Right click on the live view window of fisheye camera, and go to Remote Config >Event >Intrusion/Line Crossing to check the checkbox **Smart Tracking** to enable the tracking function.
11. Click **Save** to save the settings
12. (Optional) You can also right click on the panorama view and select **Start Master-slave Linkage**. Then you can make the speed dome to track target manually by clicking the target on the live view of fisheye camera.

    Note: If you want to see the speed dome linkage, you should add the speed dome to the software (*Section 3.1 Adding the Device*) and start live view (*Section 4.1 Starting and Stopping the Live View*) of it.

Master-slave Linkage for Box/Bullet Camera

Steps:

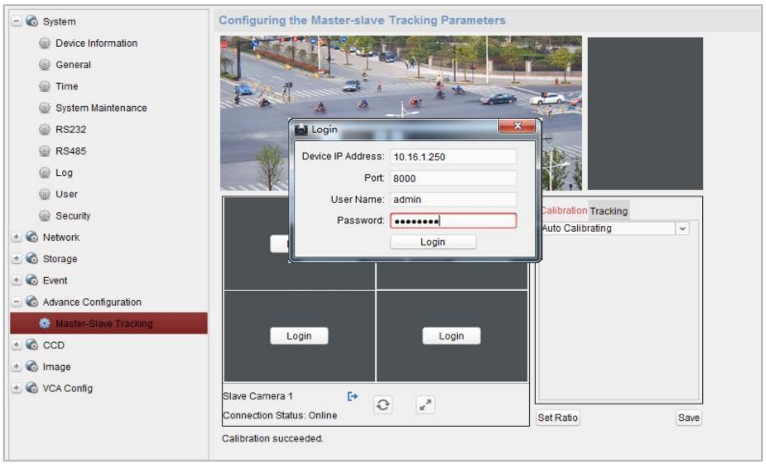
1. Enter **Remote Configuration** -> **VCA Config** -> **Rule** -> **Rule Settings**.
2. Select Camera No.1, and click + of Rule List to add rule.
3. Select **Intrusion** as Event Type, and then click ○ to draw the zone of intrusion rule and click **Save** to save the settings.



Rule No.	Rule Name	Event Type
☑ 1	Intrusion Detection	Intrusion

Size Filter: Pixel Mode; Duration (s): 0

4. Login the speed dome.
   1) In the Remote Configuration interface, select **Advanced Configuration**->**Master-Slave Tracking** to show the login interface.
   2) Click **Login** button to pop up the speed dome login dialog box.
   3) Input the required information.

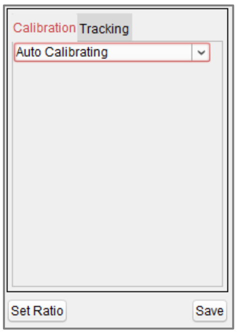


Configuring the Master-slave Tracking Parameters

Device IP Address: 10.16.1.250
Port: 8000
User Name: admin
Password: ••••••••

Slave Camera 1
Connection Status: Online
Calibration succeeded.

5. Click **PTZ**, and use the direction arrows to adjust the speed dome to a horizontal position.
6. Click to select the calibration tab page.

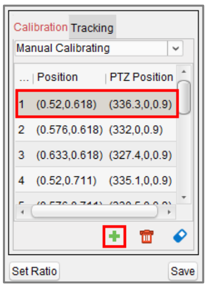


For Auto Calibrating:

1) Select **Auto Calibrating** from the calibration list.
2) Perform the calibration operation.
   Move and zoom in/out the speed dome to make sure the live views of dome and camera is mostly the same.
3) Click **Save** to save the calibration settings.

For Manual Calibrating:

1) Select **Manual Calibrating** from the calibration list.
2) Select No. 1 from the list and click ✚, a blue cross appears in the center of the live view page, and the digital zoom view of the selected site appears on the right.
3) Select No. 2 to No. 4, and repeat the step above to add the manual calibration sites.



...	Position	PTZ Position
1	(0.52,0.618)	(336.3,0,0.9)
2	(0.576,0.618)	(332,0,0.9)
3	(0.633,0.618)	(327.4,0,0.9)
4	(0.52,0.711)	(335.1,0,0.9)

4) Perform the calibration operation.
   Adjust the distances between the four calibration sites evenly in the live view page.
   Select calibration site No. 1 and the digital zoom view of site No. 1 appears on the right.
   Move and zoom in/out the speed dome to make sure the live views of dome and the digital zoom view of selected site is mostly the same.
   Click to save the current site position information.
   Select No. 2 to No. 4, and repeat the steps above to save the site position information.
   Click **Save** to save the calibration settings.

7. Right-click on the live view window of camera to show the menu and click **Enable Master-slave Tracking.**
8. When configured VCA rule is triggered by target, the speed dome performs the automatic master-slave tracking and the target frame turns from green into red.

4.9 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.

Digital Zoom

Use the left key of mouse to drag a rectangle area in the lower-right/upper-left direction, and then the rectangle area will zoom in/out. You can also use the mouse wheel for zooming in or restoring of the video in digital zoom mode.

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.

Chapter 5 Remote Storage Schedule Settings and 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.

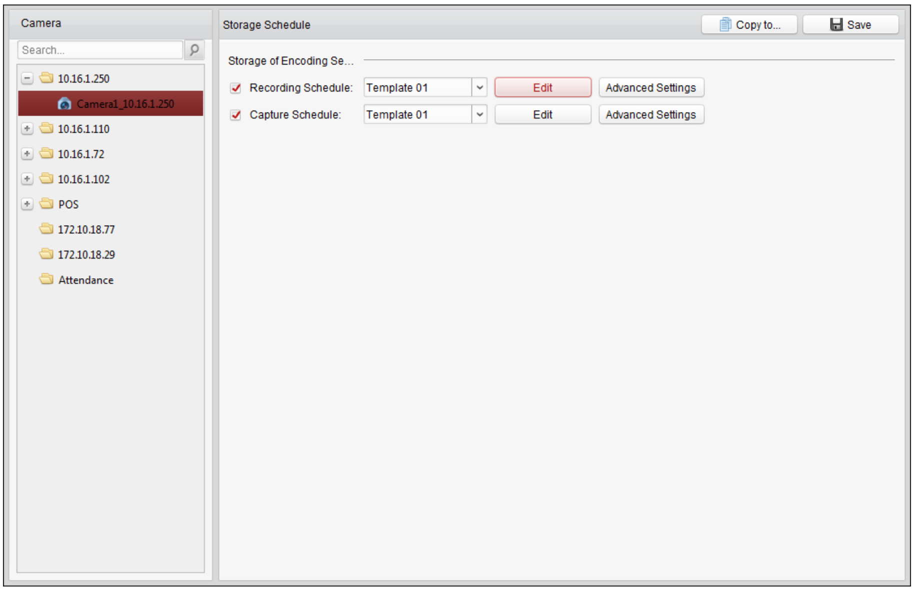
5.1 Remote Storage

Purpose:

The video files and captured pictures can be stored on the HDDs, Net HDDs, SD/SDHC cards on the local device, or the storage server connected.

Click the icon on the control panel,

or click **Tool**->**Storage Schedule** to open the Storage Schedule page.



Storage of Encoding Se...

☑ Recording Schedule: Template 01

☑ Capture Schedule: Template 01

5.1.1 Storing on Storage Device on the DVR, NVR, or Network Camera

Purpose:

Some local devices, including the DVRs, NVRs, and Network Cameras, provide storage devices such as the HDDs, Net HDDs and SD/SDHC cards for video files. You can set a recording schedule or capture schedule for the channels of the local devices.

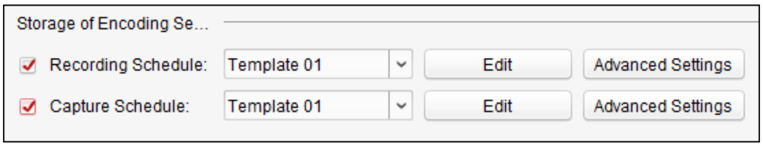
Note: The pictures captured through the capture schedule are stored on the local device and can be searched on the remote configuration page of the device.

Before you start:

The newly installed storage devices need to be formatted. Go to the remote configuration page of the device, click **Storage**->**General**, select the HDD or SD/SDHC card, and click **Format** to initialize the selected storage device.

Steps:

1. Open the Recording Schedule page.
2. Select the camera in the Camera Group list.
3. Check the checkbox **Recording Schedule/Capture Schedule** under **Storage of Encoding Server** to enable device local recording or capture.

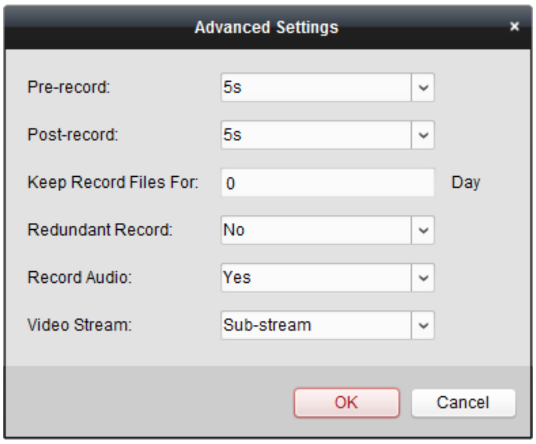


Storage of Encoding Se...

☑ Recording Schedule: Template 01 | Edit | Advanced Settings

☑ Capture Schedule: Template 01 | Edit | Advanced Settings

4. Select the record or capture schedule template from the drop-down list.
   All-day Template: for all-day continuous recording.
   Weekday Template: for working-hours continuous recording from 8:00 AM to 8:00 PM.
   Event Template: for the event triggered recording.
   Template 01 to 08: fixed templates for specific schedules. You can edit the templates if needed.
   Custom: can be customized as desired.
   If you need to edit or customize the template, see *Configuring Recording Schedule Template.*
5. Click **Advanced Settings** to set the recording parameters. For details, see *Table 5.1 Advanced Recording Settings* and *Table 3.2 Advanced Capture Settings*.
   Note: The displayed items vary with the devices.
6. Optionally, click **Copy to…** to copy the recording schedule settings to other channels.
7. Click **Save** to save the settings.



Advanced Settings

Pre-record: 5s

Post-record: 5s

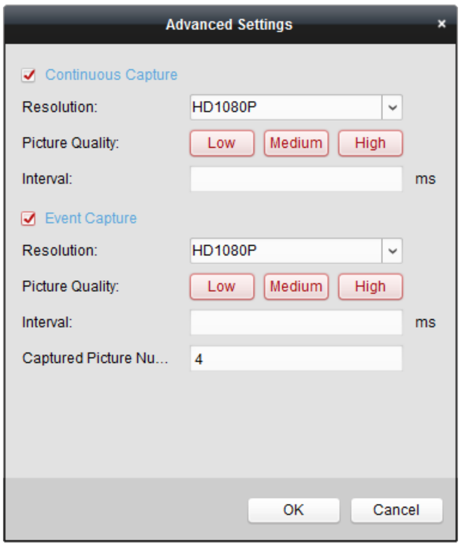
Keep Record Files For: 0 Day

Redundant Record: No

Record Audio: Yes

Video Stream: Sub-stream

OK | Cancel



Advanced Settings

☑ Continuous Capture

Resolution: HD1080P

Picture Quality: Low | Medium | High

Interval: ms

☑ Event Capture

Resolution: HD1080P

Picture Quality: Low | Medium | High

Interval: ms

Captured Picture Nu... 4

OK | Cancel

Table 5. 1 Advanced Recording Settings

Parameters	Descriptions
Pre-record	Normally used for the event triggered record, when you want to record before the event happens
Post-record	After the event finished, the video can also be recorded for a certain time.
Keep Record Files for	The time for keeping the video files in the storage device, once exceeded, the

	files will be deleted. The files will be saved permanently if the value is set as *0*.
Redundant Record	Save the video files not only in the R/W HDD but also in the redundant HDD.
Record Audio	Record the video files with audio or not.
Video Stream	Select the stream type for the recording. ***Note:*** For specific type of devices, you can select Dual-Stream for recording both main stream and sub-stream of the camera. In this mode, you can switch the stream type during remote playback. Refer to *Chapter 5.2.1 Normal Playback* for stream switch during playback.

Table 5. 2 Advanced Capture Settings

Parameters	Descriptions
Resolution	Select the resolution for the continuous or event captured pictures.
Picture Quality	Set the quality for the continuous or event captured pictures.
Interval	Select the interval which refers to the time period between two capturing actions.
Captured Picture Number	Set the picture number for event capture.

Configuring Recording Schedule Template

Perform the following steps to configure the recording schedule template:

If **Template 01 to 08** is selected from the drop-down list, start from step 1;

If **Custom** is selected from the drop-down list, start from step 2.

1. Click **Edit** to enter the Templates Management interface. Select the template to be set and you can edit the template name.
2. Set the time schedule for the selected template.

   ✎ Schedule Recording refers to normal schedule record. The schedule time bar is marked with 🟦.

   ✎ Event Recording refers to the schedule record for the event. The schedule time bar is marked with 🟧.

   ✎ Command refers to the schedule record triggered by command. The schedule time bar is marked with 🟩.

   Note: Record triggered by command is only available for the ATM transactions when the ATM DVR is added to iVMS-4200.

   When the cursor turns to ✎, you can set the time period.

   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,

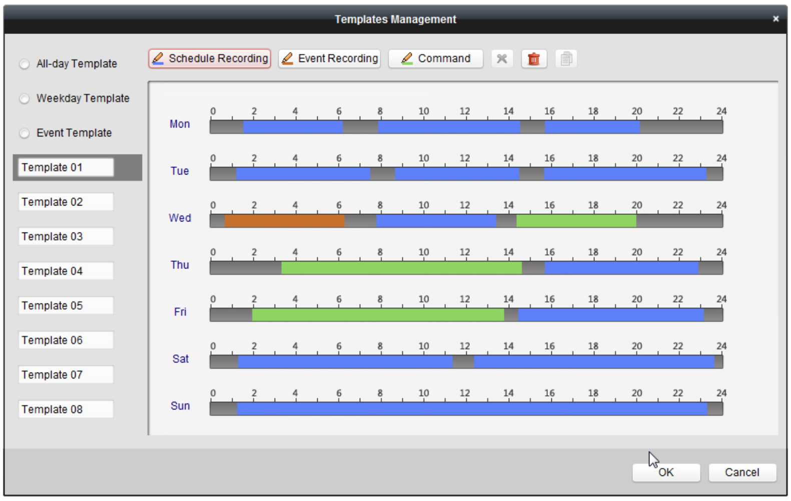
   and then click the icon ✖ to delete the selected time bar,

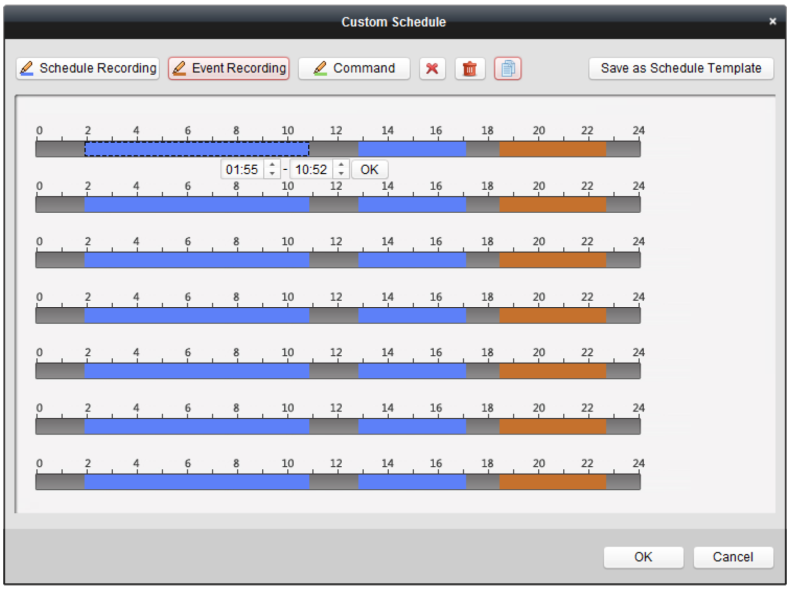
   or click the icon 🗑 to delete all the time bars,

   or click the icon 📋 to copy the time bar settings to the other dates.
4. Click **OK** to save the settings.

   You can click **Save as Schedule Template** on the Custom Schedule interface, and then the custom template can be saved as template 01 to 08.

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





5.1.2 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

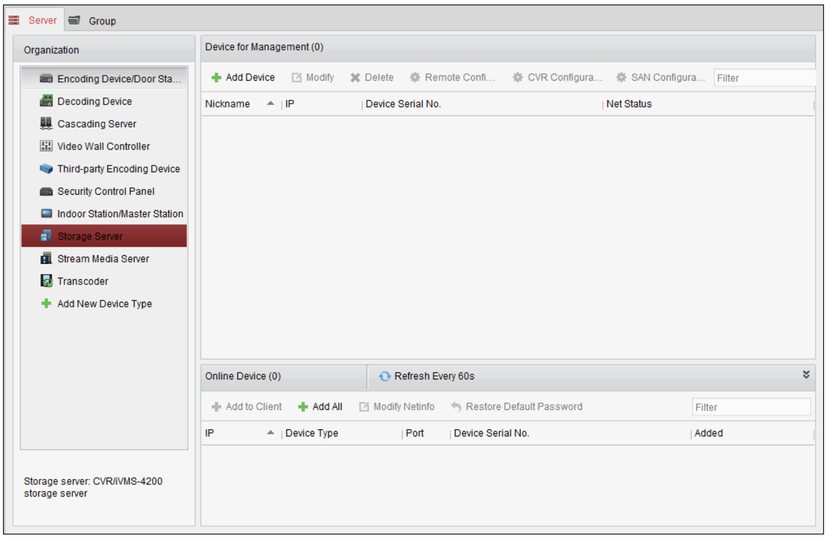
Steps:

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. You can add the storage server in the following ways:

- By detecting the online storage server, see *Section 3.1.2 Adding Online Devices.*
- By specifying the storage server IP address or domain name, see *Section 3.1.3 Adding Devices Manually.*
- By specifying an IP segment, see *Section 3.1.4 Adding Devices by IP Segment*.
- By IP Server, see Section *3.1.5 Adding Devices by IP Server.*

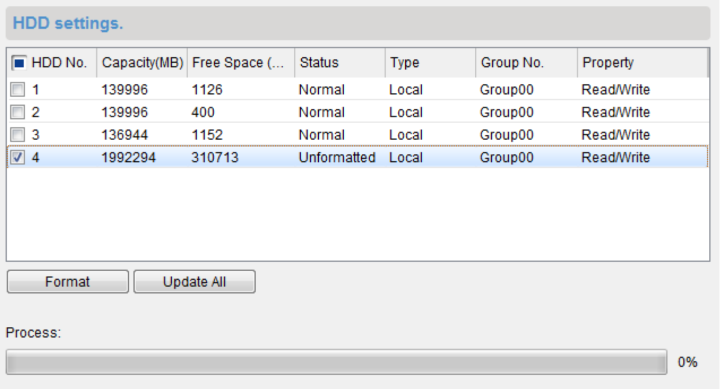
Formatting the HDDs

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.



HDD settings.

■ HDD No.	Capacity(MB)	Free Space (...	Status	Type	Group No.	Property
□ 1	139996	1126	Normal	Local	Group00	Read/Write
□ 2	139996	400	Normal	Local	Group00	Read/Write
□ 3	136944	1152	Normal	Local	Group00	Read/Write
☑ 4	1992294	310713	Unformatted	Local	Group00	Read/Write

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.

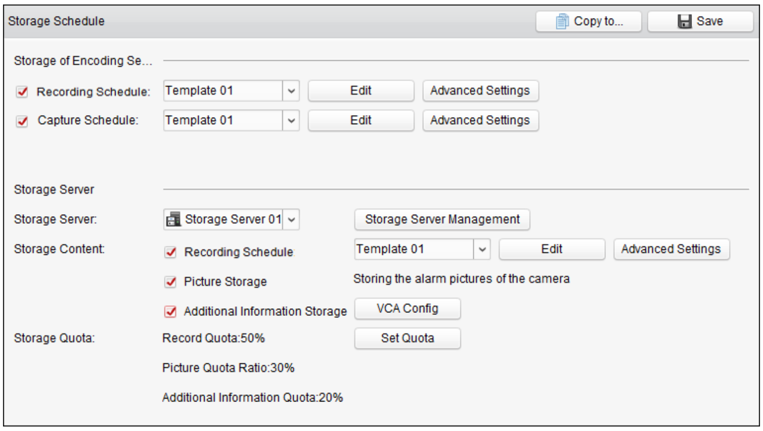
   You can also check the checkbox **Picture Storage** to store the alarm pictures of the camera when event occurs.

   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. Please refer to *Chapter 18.1 Heat Map, Chapter 18.2 People Counting Statistics* and *Chapter 18.4 Road Traffic* for checking the data.

   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.



Storage Schedule — Copy to... — Save

Storage of Encoding Se...

☑ Recording Schedule: Template 01 — Edit — Advanced Settings

☑ Capture Schedule: Template 01 — Edit — Advanced Settings

Storage Server

Storage Server: Storage Server 01 — Storage Server Management

Storage Content: ☑ Recording Schedule — Template 01 — Edit — Advanced Settings

☑ Picture Storage — Storing the alarm pictures of the camera

☑ Additional Information Storage — VCA Config

Storage Quota: Record Quota:50% — Set Quota

Picture Quota Ratio:30%

Additional Information Quota:20%

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. For details, refer to *Chapter 6 Event Management.*

5.2 Remote Playback

Purpose:

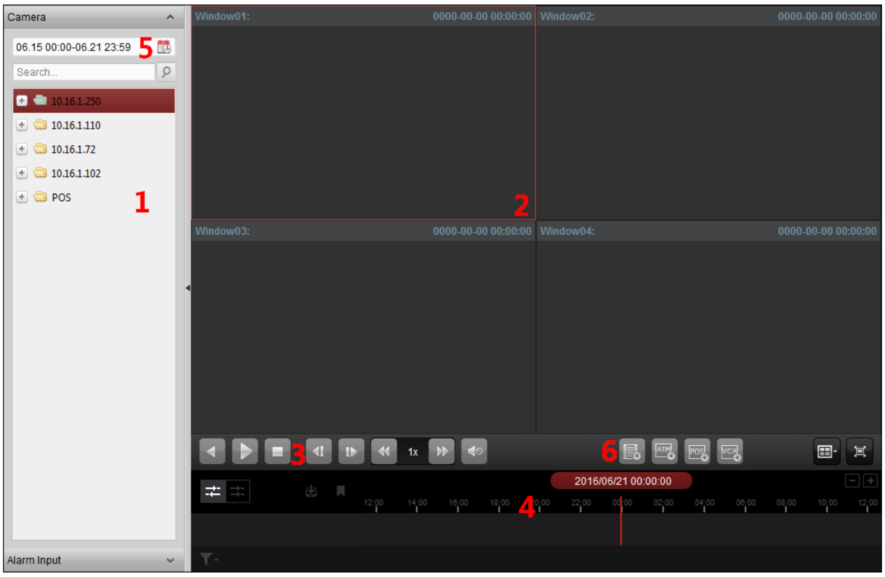
The video files stored on the local device or the storage server can be searched by camera or triggering event, and then can be played back remotely.

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 *17.2.2 Live View and Playback Settings*. Optionally, you can set the cameras rotate direction for playback in Group Management. Refer to *Modifying the Group/Camera* of *Chapter 3.2 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

5.2.1 Normal Playback

Purpose:

The video files can be searched by camera or group name for the Normal Playback.

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, refer to *step 5* of *Chapter 5.1.1 Storing on Storage Devices on the DVRs, NVRs, or Network Cameras* for details.

Note: This function should be support by the device.

Steps:

1. Enter Group Management interface and open the Modify Camera dialog (refer to *Modifying the Group/Camera* of *Chapter 3.2 Group Management*).
2. Set the video stream of the camera to main stream or sub-stream.

Searching Video Files for Normal Playback

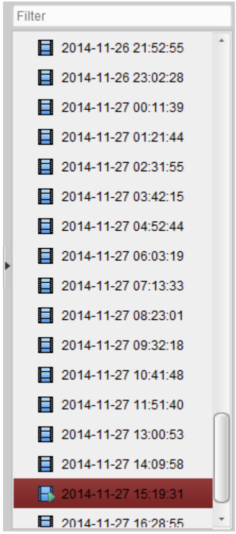
Steps:

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.



Filter

- 2014-11-26 21:52:55
- 2014-11-26 23:02:28
- 2014-11-27 00:11:39
- 2014-11-27 01:21:44
- 2014-11-27 02:31:55
- 2014-11-27 03:42:15
- 2014-11-27 04:52:44
- 2014-11-27 06:03:19
- 2014-11-27 07:13:33
- 2014-11-27 08:23:01
- 2014-11-27 09:32:18
- 2014-11-27 10:41:48
- 2014-11-27 11:51:40
- 2014-11-27 13:00:53
- 2014-11-27 14:09:58
- 2014-11-27 15:19:31
- 2014-11-27 16:28:55

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.

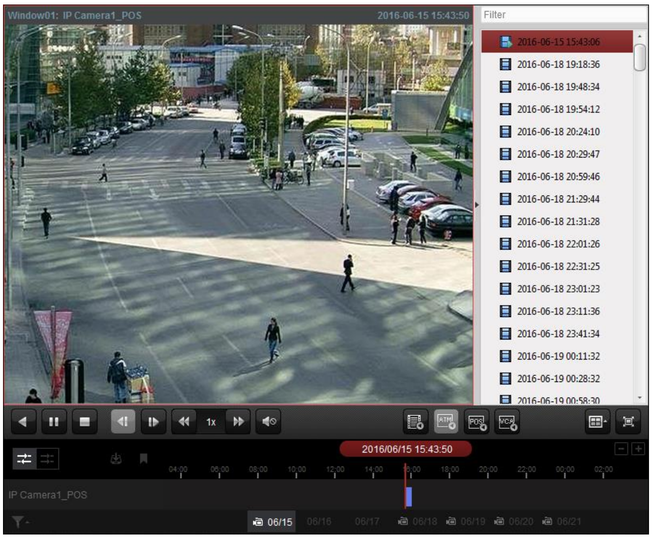
  You can also select a display window and click the icon ▶ in the toolbar to play back the corresponding video file.
- **Playback by Timeline**

  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.

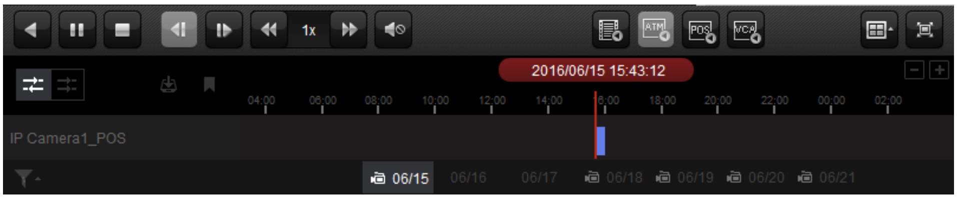
  You can drag the timeline bar to go to the previous or the next time period.

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



2016-06-15 15:43:06
2016-06-18 19:18:36
2016-06-18 19:48:34
2016-06-18 19:54:12
2016-06-18 20:24:10
2016-06-18 20:29:47
2016-06-18 20:59:46
2016-06-18 21:29:44
2016-06-18 21:31:28
2016-06-18 22:01:26
2016-06-18 22:31:25
2016-06-18 23:01:23
2016-06-18 23:11:36
2016-06-18 23:41:34
2016-06-19 00:11:32
2016-06-19 00:28:32
2016-06-19 00:58:30

Normal Playback Toolbar:

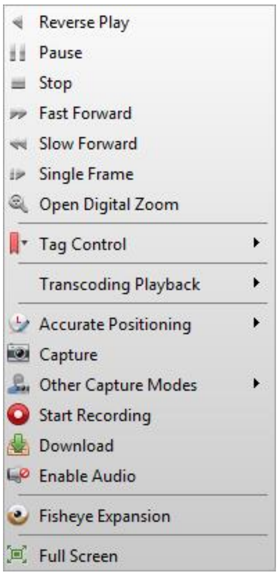


On the Normal Playback page, the following toolbar buttons are available:

◀	**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	**ATM Playback**	Search the recordings of ATM devices.
POS	**POS Playback**	Search the recordings which contain POS information.
VCA	**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.
	Other Capture Modes	**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.

		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. For details, please refer to *Chapter 5.2.8 Fisheye Playback*.
▣	**Full Screen**	Display the playback in full-screen mode. Click the icon again or press *Esc* key to exit.

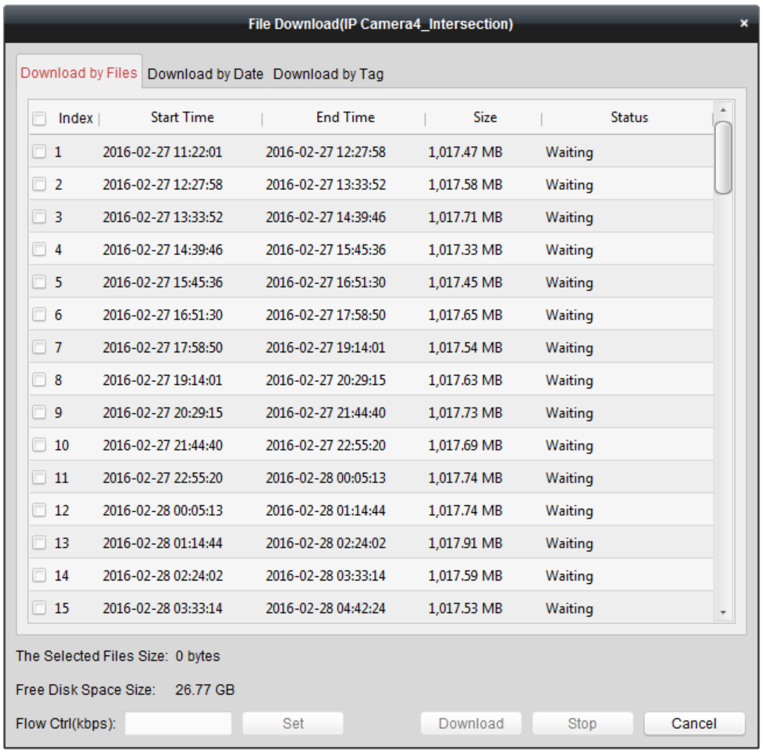
Downloading Video Files

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.



□ Index	Start Time	End Time	Size	Status
□ 1	2016-02-27 11:22:01	2016-02-27 12:27:58	1,017.47 MB	Waiting
□ 2	2016-02-27 12:27:58	2016-02-27 13:33:52	1,017.58 MB	Waiting
□ 3	2016-02-27 13:33:52	2016-02-27 14:39:46	1,017.71 MB	Waiting
□ 4	2016-02-27 14:39:46	2016-02-27 15:45:36	1,017.33 MB	Waiting
□ 5	2016-02-27 15:45:36	2016-02-27 16:51:30	1,017.45 MB	Waiting
□ 6	2016-02-27 16:51:30	2016-02-27 17:58:50	1,017.65 MB	Waiting
□ 7	2016-02-27 17:58:50	2016-02-27 19:14:01	1,017.54 MB	Waiting
□ 8	2016-02-27 19:14:01	2016-02-27 20:29:15	1,017.63 MB	Waiting
□ 9	2016-02-27 20:29:15	2016-02-27 21:44:40	1,017.73 MB	Waiting
□ 10	2016-02-27 21:44:40	2016-02-27 22:55:20	1,017.69 MB	Waiting
□ 11	2016-02-27 22:55:20	2016-02-28 00:05:13	1,017.74 MB	Waiting
□ 12	2016-02-28 00:05:13	2016-02-28 01:14:44	1,017.74 MB	Waiting
□ 13	2016-02-28 01:14:44	2016-02-28 02:24:02	1,017.91 MB	Waiting
□ 14	2016-02-28 02:24:02	2016-02-28 03:33:14	1,017.59 MB	Waiting
□ 15	2016-02-28 03:33:14	2016-02-28 04:42:24	1,017.53 MB	Waiting

The Selected Files Size: 0 bytes

Free Disk Space Size: 26.77 GB

Flow Ctrl(kbps):

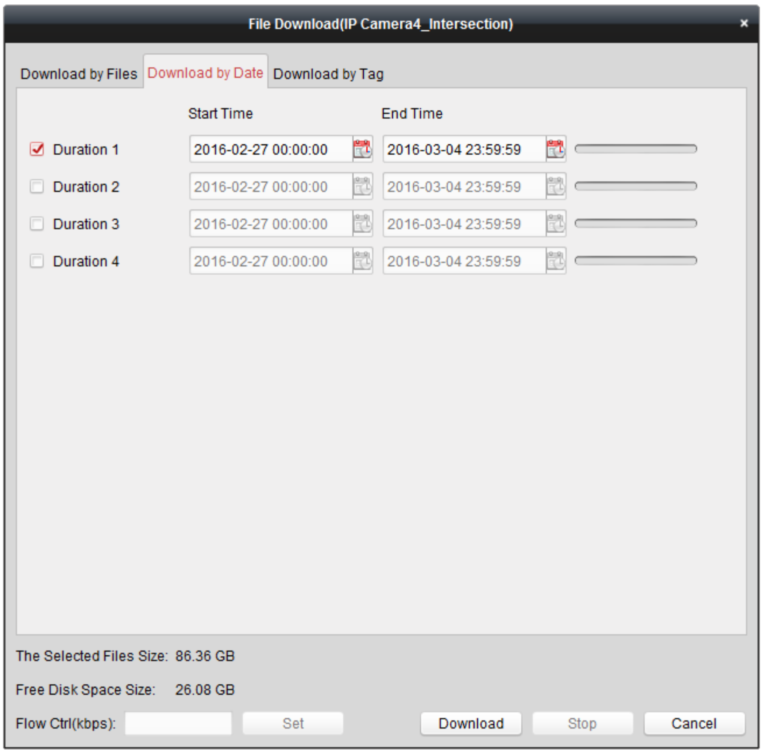
Download by Date

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.



	Start Time	End Time
☑ Duration 1	2016-02-27 00:00:00	2016-03-04 23:59:59
□ Duration 2	2016-02-27 00:00:00	2016-03-04 23:59:59
□ Duration 3	2016-02-27 00:00:00	2016-03-04 23:59:59
□ Duration 4	2016-02-27 00:00:00	2016-03-04 23:59:59

The Selected Files Size: 86.36 GB

Free Disk Space Size: 26.08 GB

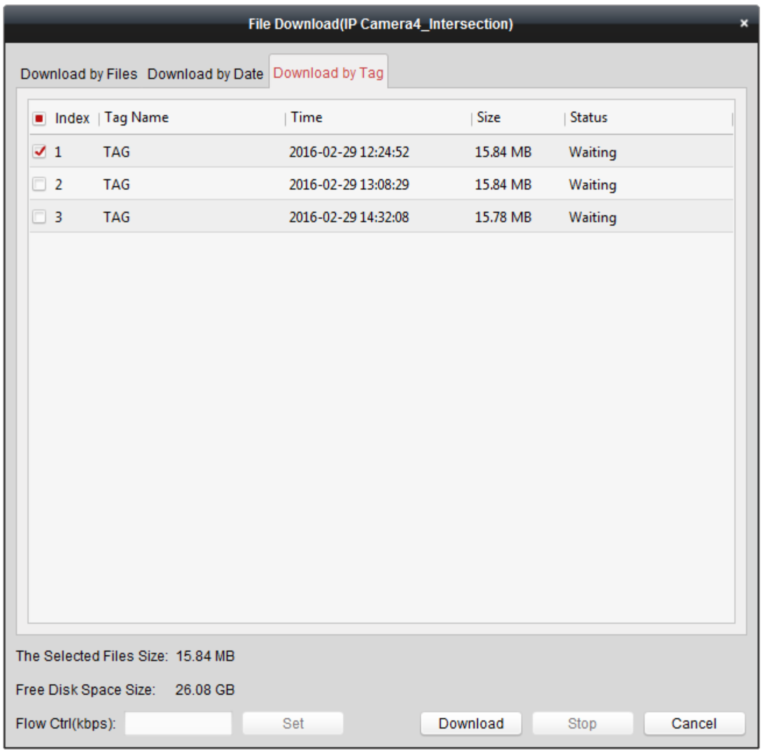
Flow Ctrl(kbps):

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 *17.2.2 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.



■ Index	Tag Name	Time	Size	Status
☑ 1	TAG	2016-02-29 12:24:52	15.84 MB	Waiting
☐ 2	TAG	2016-02-29 13:08:29	15.84 MB	Waiting
☐ 3	TAG	2016-02-29 14:32:08	15.78 MB	Waiting

The Selected Files Size: 15.84 MB

Free Disk Space Size: 26.08 GB

Flow Ctrl(kbps):

5.2.2 Alarm Input Playback

Purpose:

When the alarm input is triggered and the linked video can be searched for Alarm Input Playback and this function requires the support of the connected device.

Searching Video Files for Alarm Input Playback

Steps:

1. Open the Remote Playback page.
2. Click ⌄ to show the Alarm Input panel on the left.
3. (Optional) Click the calendars icon 📅 to activate the calendars dialog.
   Select the start and end date and set the accurate time, and click **OK**.
4. Click-and-drag the alarm input to the display window,
   or double-click the alarm input to start the playback.
5. The found video files of the selected alarm input will be displayed on the right of the interface.
   You can filter the results through the **Filter** text field.

Playing Back Video Files

After searching the video files triggered by alarm input, 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.

Please refer to *Chapter 5.2.1 Normal Playback* for the description of the playback control toolbar and right-click menu. Some icons may not available for Alarm Input playback**.**

5.2.3 Event Playback

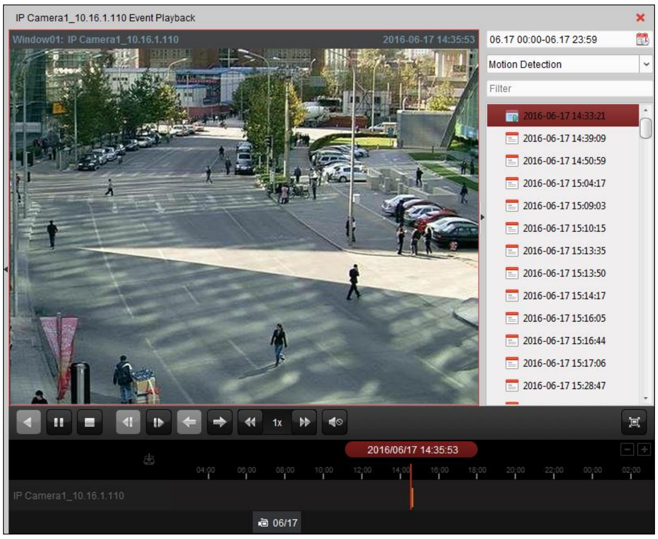
Purpose:

The recordings triggered by event, such as motion detection, VCA detection or behavior analysis, 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 5.2.1 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.



IP Camera1_10.16.1.110 Event Playback

Window01: IP Camera1_10.16.1.110 2016-06-17 14:35:53

06.17 00:00-06.17 23:59

Motion Detection

Filter

2016-06-17 14:33:21
2016-06-17 14:39:09
2016-06-17 14:50:59
2016-06-17 15:04:17
2016-06-17 15:09:03
2016-06-17 15:10:15
2016-06-17 15:13:35
2016-06-17 15:13:50
2016-06-17 15:14:17
2016-06-17 15:16:05
2016-06-17 15:16:44
2016-06-17 15:17:06
2016-06-17 15:28:47

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**

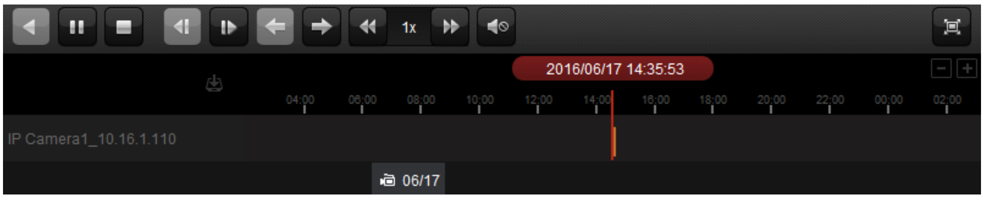
  The timeline indicates the time duration for the video file. Click on the timeline to play back the video of the specific time.

  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.
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 📼.

Please refer to *Chapter 5.2.1 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 *17.2.2 Live View and Playback Settings*.

5.2.4 ATM Playback

Purpose:

Search the video files for ATM DVR.

Note: This function should be supported by the device and the device should be configured with transaction rules. For details, please refer to the *User Manual* of the device.

Searching Video Files for ATM Playback

Steps:

1. Open the Remote Playback page.
2. Select the camera of the ATM DVR and start the normal playback. Refer to *Chapter 5.2.1 Normal Playback.*
3. Click ATM to enter the ATM playback interface.
4. Enter the search conditions.

   ☑ By Card Nu... : Input the card number that is contained in the ATM information.

   □ All ▾ : Check the checkbox and select the transaction type for query, and input the related transaction amount.

   File Type: Select the type of the video file to be searched.
5. 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.
6. Click **Search** and the matched files will be displayed. You can filter the results through the Filter text field.
7. Double-click a file for playback. Or you can click ✕ to go back to the normal playback.

Playing Back Video Files

After searching the recordings, 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 zoom in or zoom out 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.

Please refer to *Chapter 5.2.1 Normal Playback* for the description of the playback control toolbar and right-click menu. Some icons may not available for ATM playback**.**

5.2.5 POS Playback

Purpose:

Search the video files which contain POS information.

Note: This function should be supported by the device and the device should be configured with POS text overlay. For details, please refer to the User Manual of the device.

Searching Video Files for POS Playback

Steps:

1. Open the Remote Playback page.
2. Select the camera and start the normal playback. Refer to *Chapter 5.2.1 Normal Playback.*
3. Click POS to enter the POS playback interface.
4. Enter the search conditions.

   Keywords: Input the keywords that are contained in the POS information. You can input up to 3 keywords by separating each one with a comma.

   Filter: If you input more than one keyword for query, you can select “or(|)” to search the POS information containing any of the keywords, or select “and(&)” to search the POS information containing all of the keywords.

   Case Sensitive: Check the checkbox to search the POS information with case-sensitivity.

7. 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.

5. Click **Search** and the matched files will be displayed. You can filter the results through the **Filter** text field.
6. Double-click a file for playback. Or you can click ✖ to go back to the normal playback.

Playing Back Video Files

After searching the recordings, 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 zoom in or zoom out the timeline bar. You can also use the mouse wheel to zoom in or zoom out on the timeline.

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

Please refer to *Chapter 5.2.1 Normal Playback* for the description of the playback control toolbar, right-click menu and downloading record files. Some icons may not be available for POS playback.

5.2.6 Synchronous Playback

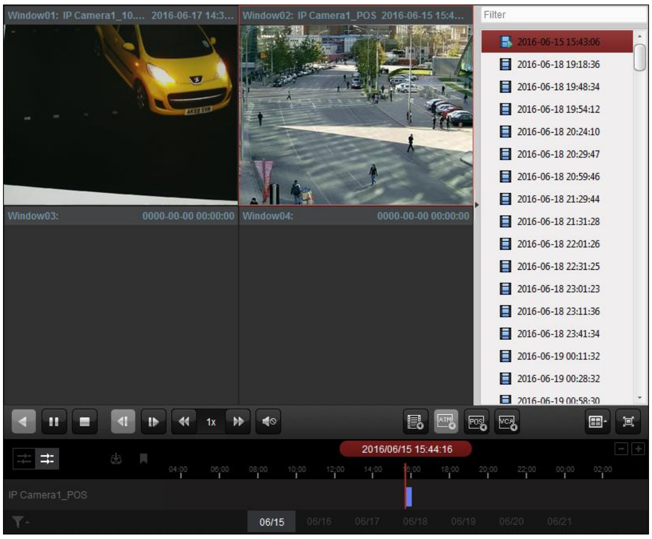
Purpose:

In synchronous playback, the video files can be played back in synchronization.

Note: Video files from up to 16 cameras can be played back simultaneously.

Steps:

1. Search the video files for the normal playback (*Section 3.2.1 Normal Playback*). At least two cameras are during playback.
2. Click in the toolbar to enable the synchronous playback. The camera under playback will start synchronous playback.



Window01: IP Camera1_10.... 2016-06-17 14:3...
Window02: IP Camera1_POS 2016-06-15 15:4...
Window03: 0000-00-00 00:00:00
Window04: 0000-00-00 00:00:00
Filter
1x
ATM
POS
VCA
2016/06/15 15:44:16
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
IP Camera1_POS
06/15
06/16
06/17
06/18
06/19
06/20
06/21

2016-06-15 15:43:06
2016-06-18 19:18:36
2016-06-18 19:48:34
2016-06-18 19:54:12
2016-06-18 20:24:10
2016-06-18 20:29:47
2016-06-18 20:59:46
2016-06-18 21:29:44
2016-06-18 21:31:28
2016-06-18 22:01:26
2016-06-18 22:31:25
2016-06-18 23:01:23
2016-06-18 23:11:36
2016-06-18 23:41:34
2016-06-19 00:11:32
2016-06-19 00:28:32
2016-06-19 00:58:30

3. To disable the synchronous playback, click the icon .

5.2.7 VCA Playback

Purpose:

You can set VCA rule to the searched video files and find the video that VCA event occurs, including VCA Search, Intrusion and Line Crossing. This function helps to search out the video that you may be more concerned and mark it with red color.

- **VCA Search**: Get all the related motion detection events that occurred in the pre-defined region.
- **Intrusion Detection:** Detect whether there are people, vehicles and other moving objects intruding into the pre-defined region.
- **Line Crossing Detection**: Bi-directionally detect people, vehicles and other moving objects that cross a virtual line.

Note: For some devices, you can filter the searched video files by setting the advanced attributes, such as the gender and age of the human and whether he/she wears glasses.

Steps:

1. Open the Remote Playback page.
2. Select the camera and start the normal playback. Refer to *Chapter 5.2.1 Normal Playback*.
3. Click to enter the VCA playback interface.

4. Select the VCA Type, draw the detection region and set the sensitivity.

   Notes:

   - For VCA Search, click , and then click and move on the playback window to set the grid rectangle as the detection region. Or you can click to set all the area shot by the camera as the detection region.
   - For Intrusion, click and then click on the playback window to set the vertex for the detection region.
   - For Line Crossing, click and then click-and-drag on the playback window to set the detection line.

     Note: For Intrusion and Line Crossing, you can click **Advanced Attributes** and check the checkbox to filter the searched video files by setting the target characters, such as the gender and age of the human and whether he/she wears glasses. This function should be supported by the device.
   - To delete the drawn region or line, click to remove it.

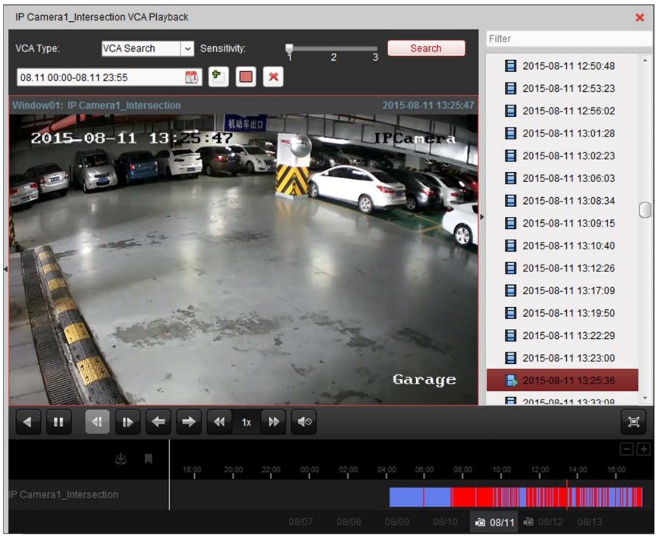
5. Click the calendars icon to activate the calendars dialog box.

   Select the start and end date and set the accurate time.

   Click **OK** to save the searching period.

6. Click **Search** and the VCA events occurred in the defined area will be red marked on the timeline. By default, the playback speed of concerned video will be 1X, and the playback speed of unconcerned video will be 8X.

   Note: You can set to skip the unconcerned video during VCA playback in System Configuration and the unconcerned video won't be played during VCA playback. Refer to *17.2.2 Live View and Playback Settings.*



IP Camera1_Intersection VCA Playback

VCA Type: VCA Search

Sensitivity: 1 2 3

08.11 00:00-08.11 23:55

Window01: IP Camera1_Intersection 2015-08-11 13:25:47

2015-08-11 12:50:48
2015-08-11 12:53:23
2015-08-11 12:56:02
2015-08-11 13:01:28
2015-08-11 13:02:23
2015-08-11 13:06:03
2015-08-11 13:08:34
2015-08-11 13:09:15
2015-08-11 13:10:40
2015-08-11 13:12:26
2015-08-11 13:17:09
2015-08-11 13:19:50
2015-08-11 13:22:29
2015-08-11 13:23:00
2015-08-11 13:25:36
2015-08-11 13:33:08

Playing Back Video Files

After searching the recordings, 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 zoom in or zoom out 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.

Please refer to *Chapter 5.2.1 Normal Playback* for the description of the playback control toolbar and right-click menu. Some icons may not available for VCA playback**.**

5.2.8 Fisheye Playback

Purpose:

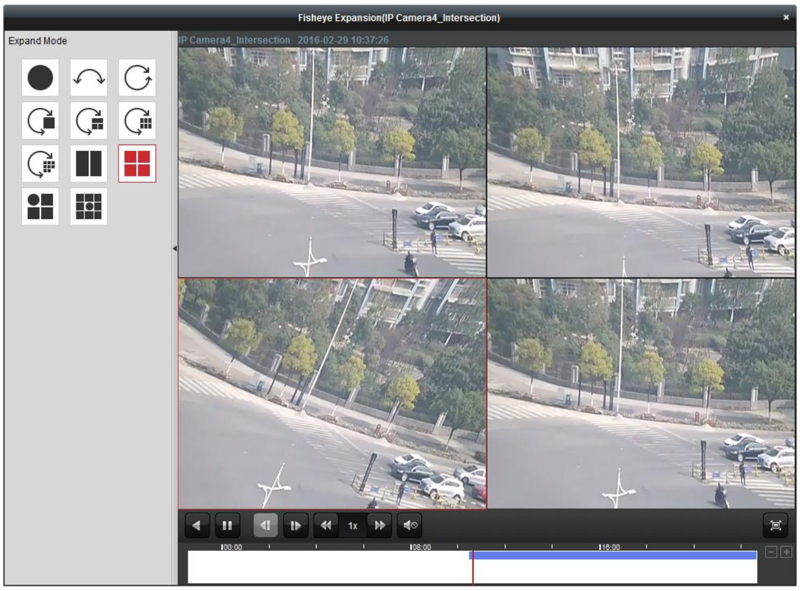
The video files can be played back in fisheye expansion mode.

Steps:

1. Open the Remote Playback page.
2. Select the camera and start the normal playback. Refer to *Chapter 5.2.1 Normal Playback*.
3. Right-click on the playback video and select **Fisheye Expansion** to enter the Fisheye Expansion Mode.

   Note: The mounting type of fisheye expansion in playback is set according to the mounting type in live view. For details, please refer to *Chapter 4.7 Live View in Fisheye Mode.*
4. You can select the expand mode for playback as desired.
   - **Fisheye:** In the Fisheye view mode, the whole wide-angle view of the camera is displayed. This view mode is called Fisheye because it approximates the vision of a fish’s convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.
   - **Panorama/Dual-180° Panorama/360° Panorama:** In the Panorama view mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.
   - **PTZ:** The PTZ view is the close-up view of some defined area in the Fisheye view or Panorama view, and it supports the electronic PTZ function, which is also called e-PTZ.

     Note: Each PTZ view is marked on the Fisheye view and Panorama view with a specific navigation box. You can drag the navigation box on the Fisheye view or Panorama view to adjust the PTZ view, or drag the PTZ view to adjust the view to the desired angle.


Fisheye Expansion(IP Camera4_Intersection)
Expand Mode
IP Camera4_Intersection 2016-02-29 10:37:26
1x
00:00
08:00
16:00

Right-click on a playing window and you can switch the selected window to full-screen mode.

Press *ESC* key on the keyboard or right-click on the window and select **Quit Full Screen** to exit the full-screen mode.

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.
◀❙	**Single Frame (Reverse)**	Play back the video files frame by frame reversely.
❙▶	**Single Frame**	Play back the video files 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.
⛶	**Full Screen**	Display the video playback in full-screen mode. Press **ESC** to exit.

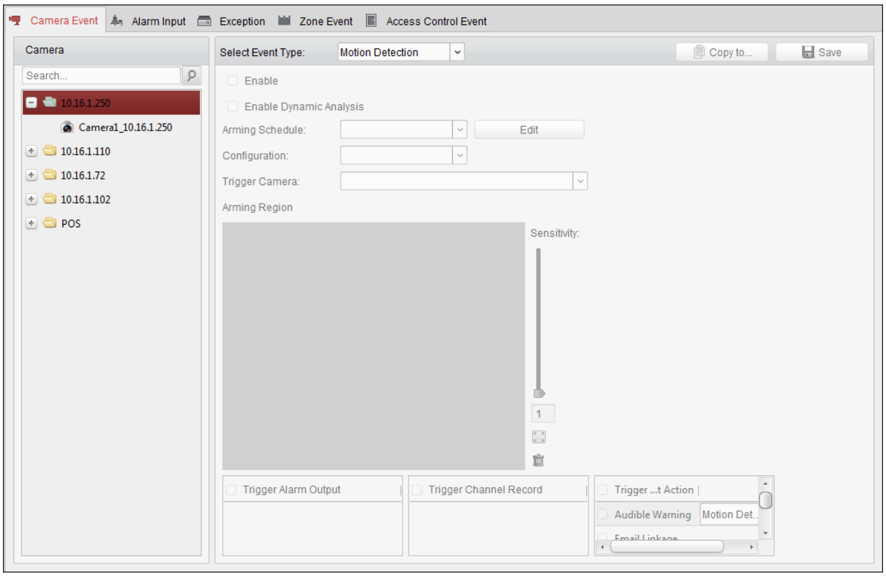
Chapter 6 Event Management

Purpose:

In iVMS-4200 client software, rules can be set up for triggers and linkage actions. You can assign linkage actions to the trigger by setting up a rule. For example, when motion is detected, an audible warning appears or other linkage actions happen.

Click the icon on the control panel,

or click **Tool**->**Event Management** to open the Event Management page.



Select Event Type: Motion Detection

You can set different linkage actions for the following triggers:

Note: The event detection should be supported by the device before you can configure it.

- Camera Event
- Alarm Input
- Exception
- Zone Event (For details, please refer to *Chapter 13.2 Zone Event Configuration.*)
- Access Control Event (For details, please refer to *Chapter 15.4 Access Control Event Configuration.*)

Note: The event types of Camera Event vary according to different devices. Here we take the configuration of some event types as examples. For other types, please refer to the *User Manual* of the device.

6.1 Configuring Motion Detection Alarm

Purpose:

A motion detection alarm is triggered when the client software detects motion within its defined area. The linkage actions, including alarm output, channel record and client action can be set.

Note: The configuration varies according to different devices. For details, please refer to the *User Manual* of the devices.

Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Motion Detection** as the event type.
3. Check the checkbox **Enable** to enable the function of motion detection. Check the checkbox **Enable Dynamic Analysis** to mark the detected objects with green rectangles in live view and playback.
4. Select the arming schedule template from the drop-down list.

   All-day Template: For all-day continuous arming.

   Weekday Template: For working-hours continuous arming from 8:00 AM to 8:00 PM.

   Template 01 to 09: Fixed templates for special schedules. You can edit the templates if needed.

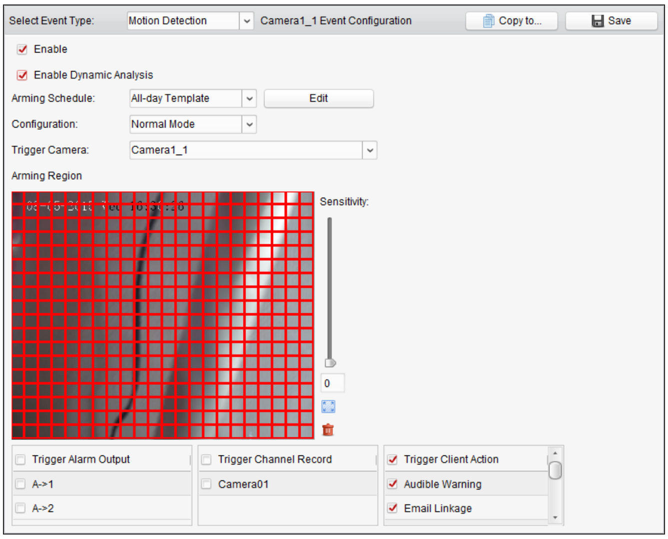
   Custom: Can be customized as desired.

   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
5. Select the Configuration as desired.

   Note: For some camera, you can select **Normal** or **Expert** as the configuration type. Expert mode is mainly used to configure the sensitivity and proportion of object on area of each area for different day/night switch. For details, please refer to the *User Manual* of the device.
6. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when motion detection alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
7. Click-and-drag the mouse to draw a defined area for the arming region.

   You can click the icon to set the whole video area as detection area, or click the icon to clear all the detection area.
8. Drag the slider on the sensitivity bar to adjust the motion detection sensitivity. The larger the value is, the more sensitive the detection is.
9. Check the checkboxes to activate the linkage actions. For details, see *Table 6.1 Linkage Actions for Motion Detection Alarm*.
10. Optionally, click **Copy to…** to copy the event parameters to other channels.
11. Click **Save** to save the settings.



Select Event Type: Motion Detection

Camera1_1 Event Configuration

☑ Enable

☑ Enable Dynamic Analysis

Arming Schedule: All-day Template

Configuration: Normal Mode

Trigger Camera: Camera1_1

Arming Region

Sensitivity: 0

□ Trigger Alarm Output
□ A->1
□ A->2

□ Trigger Channel Record
□ Camera01

☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage

Table 6. 1 Linkage Actions for Motion Detection Alarm

Linkage Actions	Descriptions

Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

Configuring Arming Schedule Template

Perform the following steps to configure the arming schedule template:

If **Template 01 to 09** is selected in the drop-down list, start from step 1;

If **Custom** is selected in the drop-down list, start from step 2.

Steps:

1. Click **Edit** to enter the Templates Management interface. Select the template to be set and you can edit the template name.
2. Set the time schedule for the selected template.

   When the cursor turns to ✎, you can set the time period.

   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,

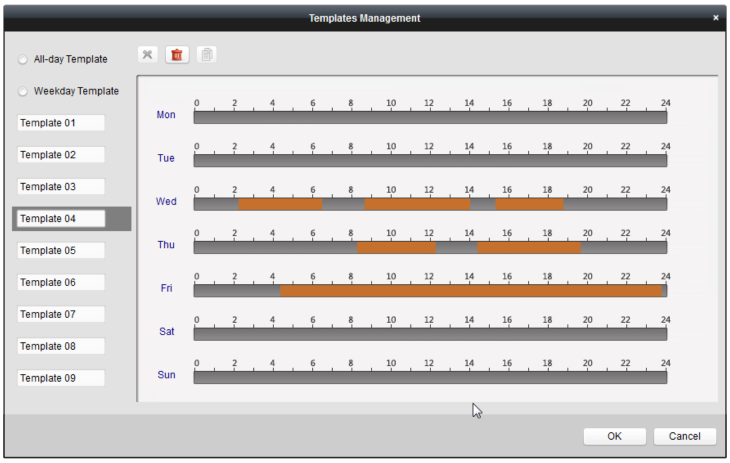
   and then click the icon ✖ to delete the selected time bar,

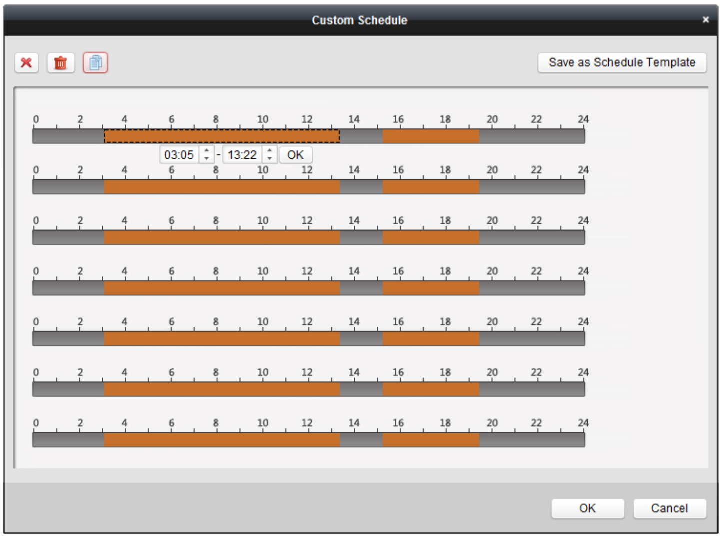
   or click the icon 🗑 to delete all the time bars,

   or click the icon 📋 to copy the time bar settings to the other dates.
4. Click **OK** to save the settings.

   You can click **Save as Schedule Template** on the Custom Schedule interface, and then the custom template can be saved as template 01 to 09.

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





6.2 Configuring Video Tampering Alarm

Purpose:

A video tampering alarm is triggered when the camera is covered and the monitoring area cannot be viewed. The linkage actions, including alarm output and client action can be set.

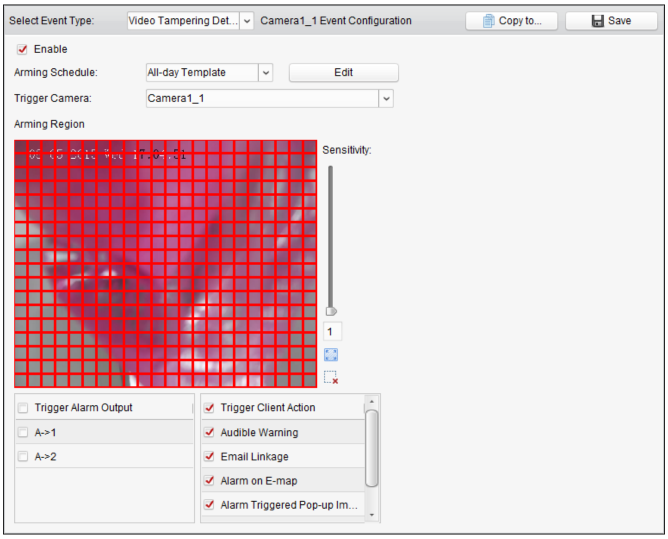
Steps:

1. Open the Event Management page and click the **Camera Event** tab.
2. Select the camera to be configured and select **Video Tampering Detection** as the event type.
3. Check the checkbox **Enable** to enable the function of video tampering.
4. Select the arming schedule template from the drop-down list.

   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when video tampering alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
6. Click-and-drag the mouse to draw a defined area for the arming region.

   You can click the icon to set the whole video area as detection area, or click the icon to clear the detection area.
7. Drag the slider on the sensitivity bar to adjust the tampering alarm sensitivity.
8. Check the checkboxes to activate the linkage actions. For details, see *Table 6.2 Linkage Actions for Tampering Alarm*.
9. Optionally, click **Copy to…** to copy the event parameters to other cameras.
10. Click **Save** to save the settings.



Select Event Type: Video Tampering Det... Camera1_1 Event Configuration

☑ Enable

Arming Schedule: All-day Template

Trigger Camera: Camera1_1

Arming Region

Sensitivity: 1

☐ Trigger Alarm Output

☐ A->1

☐ A->2

☑ Trigger Client Action

☑ Audible Warning

☑ Email Linkage

☑ Alarm on E-map

☑ Alarm Triggered Pop-up Im...

Table 6. 2 Linkage Actions for Tampering Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.3 Configuring PIR Alarm

Purpose:

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector's field of view. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

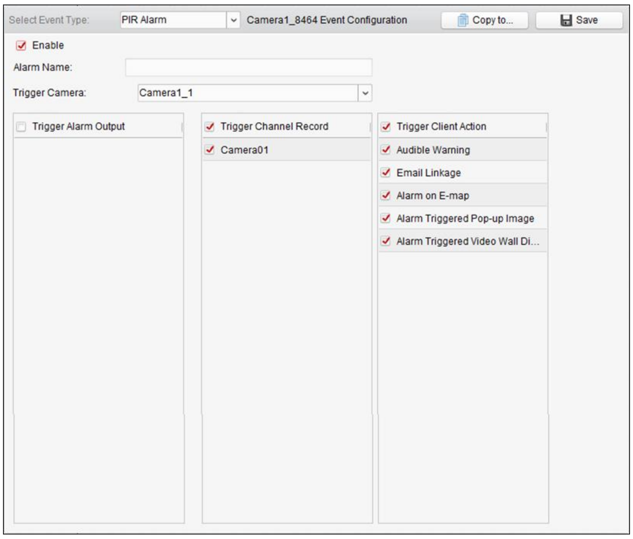
Note: The PIR Alarm function requires the support of connected device.

Steps:

1. Open the Event Management page and click the **Camera Event** tab.
2. Select the camera to be configured and select **PIR Alarm** as the event type.
3. Check the checkbox **Enable** to enable the function of PIR alarm.
4. Input a descriptive name of the alarm.
5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when PIR alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*

6. Check the checkboxes to activate the linkage actions. For details, see *Table 6.3 Linkage Actions for PIR Alarm*.
7. Optionally, click **Copy to**… to copy the event parameters to other channels.
8. Click **Save** to save the settings.



Select Event Type: PIR Alarm
Camera1_8464 Event Configuration

☑ Enable

Alarm Name:

Trigger Camera: Camera1_1

☐ Trigger Alarm Output

☑ Trigger Channel Record
☑ Camera01

☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage
☑ Alarm on E-map
☑ Alarm Triggered Pop-up Image
☑ Alarm Triggered Video Wall Di...

Table 6. 3 Linkage Actions for PIR Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.4 Configuring Video Loss Alarm

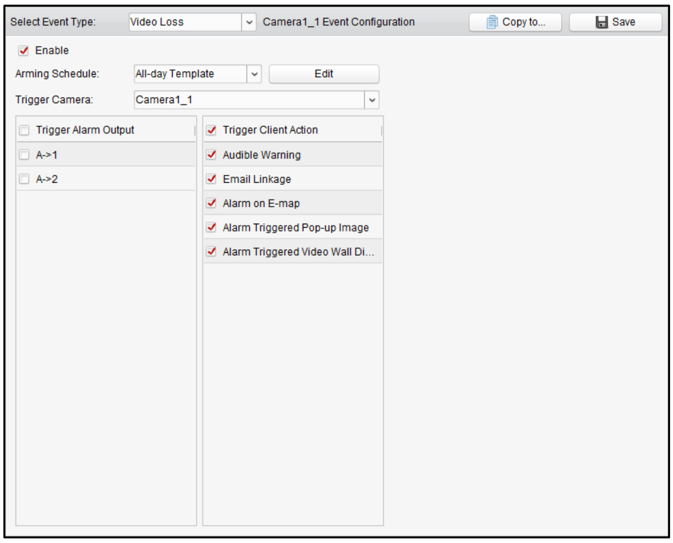
Purpose:

When the client software cannot receive video signal from the front-end devices, the video loss alarm will be triggered. The linkage actions, including alarm output and client action can be set.

Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Video Loss** as the event type.

3. Check the checkbox **Enable** to enable the function of video loss alarm.
4. Select the arming schedule template from the drop-down list.
   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when video loss alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
6. Check the checkboxes to activate the linkage actions. For details, see *Table 6.4 Linkage Actions for Video Loss Alarm*.
7. Optionally, click **Copy to...** to copy the event parameters to other cameras.
8. Click **Save** to save the new settings.



Select Event Type: Video Loss

Camera1_1 Event Configuration

☑ Enable

Arming Schedule: All-day Template

Trigger Camera: Camera1_1

□ Trigger Alarm Output
□ A->1
□ A->2

☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage
☑ Alarm on E-map
☑ Alarm Triggered Pop-up Image
☑ Alarm Triggered Video Wall Di...

Table 6. 4 Linkage Actions for Video Loss Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.5 Configuring Audio Exception Alarm

Purpose:

The abnormal sounds, such as the silence detection, environment noise detection, and current noise detection, can be detected.

Enabling the **Audio Input Detection** can detects the exceptions of audio input condition.

Enabling the **Sudden Increase of Sound Intensity** can detects the sudden increase of the sound intensity, and it consists of the following two settings.

- Sensitivity: Range [1 to 100], the smaller the value the more severe the change should be to trigger the detection.
- Sound Intensity Threshold: Range [1 to 100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

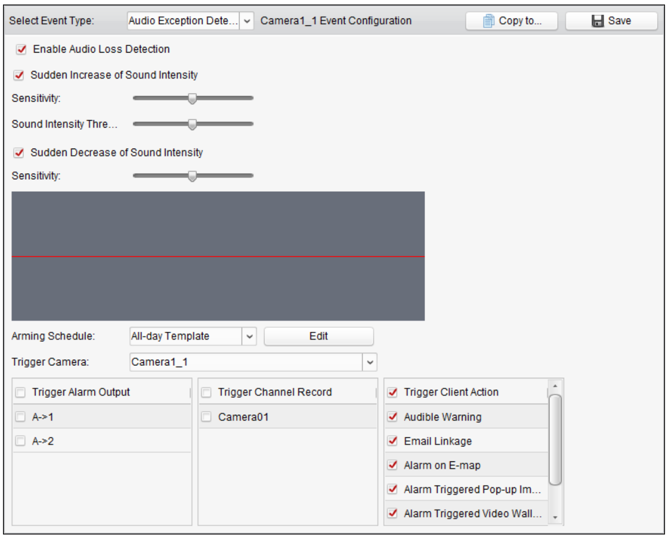
Enabling the **Sudden Decrease of Sound Intensity** can detects the sudden decrease of the sound intensity, by which you can find the abnormal silent. E.g.: The electric generator makes loud noise when it's working, while it should be paid attention if the loud noise drops suddenly.

You can set the sensitivity level [0 to 100] according to the actual environment.

Note: The Audio Exception function requires the support of connected device.

Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Audio Exception Detection** as the event type.
3. Check the related checkbox to enable the related function of audio detection alarm.
4. Set the sensitivity and sound intensity threshold.
5. Select the arming schedule template from the drop-down list.
   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
6. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when audio exception alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
7. Check the checkboxes to activate the linkage actions. For details, see *Table 6.5 Linkage Actions for Audio Detection Alarm.*
8. Optionally, click **Copy to...** to copy the event parameters to other cameras.
9. Click **Save** to save the new settings.



Select Event Type: Audio Exception Dete... Camera1_1 Event Configuration

☑ Enable Audio Loss Detection

☑ Sudden Increase of Sound Intensity

Sensitivity:

Sound Intensity Thre...

☑ Sudden Decrease of Sound Intensity

Sensitivity:

Arming Schedule: All-day Template

Trigger Camera: Camera1_1

☐ Trigger Alarm Output
☐ A->1
☐ A->2

☐ Trigger Channel Record
☐ Camera01

☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage
☑ Alarm on E-map
☑ Alarm Triggered Pop-up Im...
☑ Alarm Triggered Video Wall...

Table 6. 5 Linkage Actions for Audio Detection Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.6 Configuring Defocus Detection Alarm

Purpose:

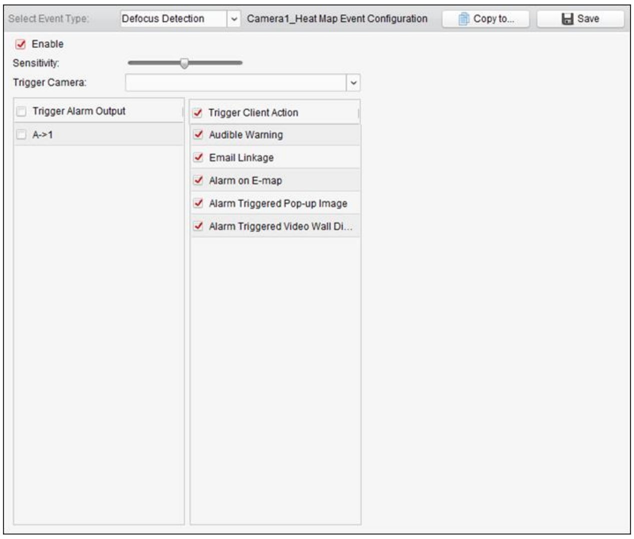
The image blur caused by defocus of the lens can be detected and a series of alarm action can be triggered.

Note: The Defocus Detection function requires the support of connected device.

Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Defocus Detection** as the event type.
3. Check the checkbox **Enable** to enable the function of defocus detection alarm.
4. You can set the sensitivity level [0 to 100] according to the actual environment.
5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when defocus alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
6. Check the checkboxes to activate the linkage actions. For details, see *Table 6.6 Linkage Actions for Defocus Detection Alarm*.
7. Optionally, click **Copy to…** to copy the event parameters to other cameras.
8. Click **Save** to save the new settings.



Select Event Type: Defocus Detection

Camera1_Heat Map Event Configuration

☑ Enable

Sensitivity:

Trigger Camera:

□ Trigger Alarm Output

□ A->1

☑ Trigger Client Action

☑ Audible Warning

☑ Email Linkage

☑ Alarm on E-map

☑ Alarm Triggered Pop-up Image

☑ Alarm Triggered Video Wall Di...

Table 6. 6 Linkage Actions for Defocus Detection Alarm

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. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.7 Configuring Face Detection Alarm

Purpose:

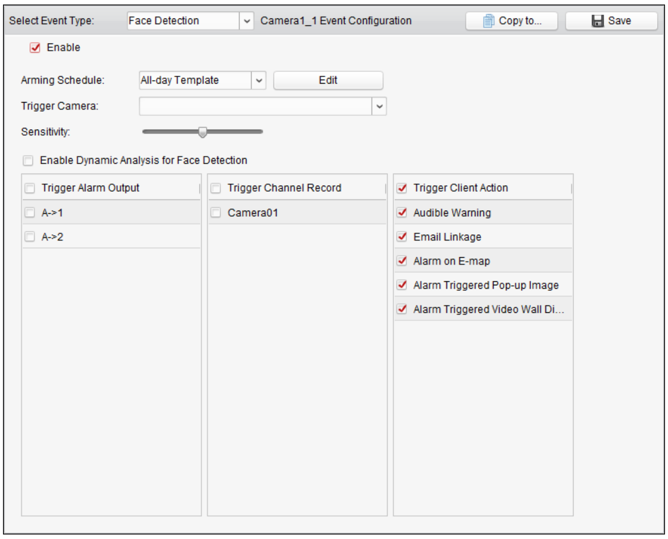
The camera will detect human faces within the monitoring area automatically if the function is enabled. A series of alarm action will be triggered if the alarm is triggered.

Note: The Face Detection function requires the support of connected device.

Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Face Detection** as the event type.
3. Check the checkbox **Enable** to enable the function of face detection alarm.
4. Select the arming schedule template from the drop-down list.
   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when face detection alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
6. Set the sensitivity for face detection.

7. Check the checkbox **Enable Dynamic Analysis for Face Detectio**n if you want the detected face get marked with rectangle in the live view.
8. Check the checkboxes to activate the linkage actions. For details, see *Table 6.7 Linkage Actions for Face Detection Alarm*.
9. Optionally, click **Copy to…** to copy the event parameters to other cameras.
10. Click **Save** to save the new settings.


Select Event Type: Face Detection

Camera1_1 Event Configuration

☑ Enable

Arming Schedule: All-day Template

Trigger Camera:

Sensitivity:

□ Enable Dynamic Analysis for Face Detection

□ Trigger Alarm Output	□ Trigger Channel Record	☑ Trigger Client Action
□ A->1	□ Camera01	☑ Audible Warning
□ A->2		☑ Email Linkage
		☑ Alarm on E-map
		☑ Alarm Triggered Pop-up Image
		☑ Alarm Triggered Video Wall Di...

Table 6. 7 Linkage Actions for Face Detection Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.8 Configuring Line Crossing Detection Alarm

Purpose:

This function can be used for detecting people, vehicles and objects crossing a pre-defined virtual line. The crossing direction can be set as bidirectional, from left to right or from right to left. And a series of linkage method will be triggered if any object is detected.

Note: This line crossing detection function requires the support of connected device.

Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Line Crossing Detection** as the event type.
3. Check the checkbox **Enable** to enable the function.

   Note: For the specific speed dome, you can click **Lock** to prevent the speed dome from moving automatically during the configuration.
4. Select the arming schedule template from the drop-down list.

   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when line crossing detection alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
6. Configure the arming region.

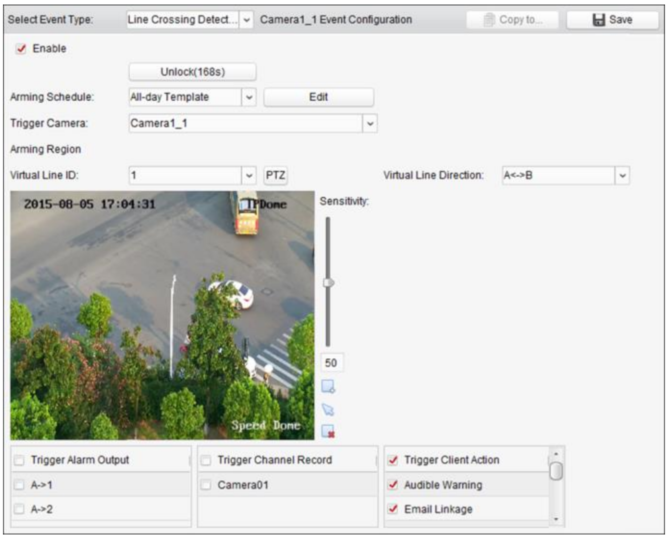
   Virtual Line ID: Click the drop-down list to choose an ID for the virtual line.

   Note: For some specific speed dome, you can click **PTZ** to move the speed dome to the desired scene which corresponds to a virtual line ID. In this way, you can configure the different line crossing detection alarms for multiple views.

   Virtual Line Direction: You can select the directions as A<->B, A ->B, and B->A.

   - **A<->B**: When an object going across the line with both directions can be detected and alarms are triggered.
   - **A->B**: Only the object crossing the virtual line from the A side to the B side can be detected.
   - **B->A**: Only the object crossing the virtual line from the B side to the A side can be detected.
7. Set the sensitivity [1 to 100].
8. Click and draw a virtual line on the preview window. Optionally, you can click and drag the virtual line to adjust its position, click to delete the selected line.

   Note: Select another virtual line ID and draw another one. Up to 4 lines can be drawn.
9. Check the checkboxes to activate the linkage actions. For details, see *Table 6.8 Linkage Actions for Line Crossing Detection Alarm*.
10. Optionally, click **Copy to...** to copy the event parameters to other cameras.
11. Click **Save** to save the settings.



Select Event Type: Line Crossing Detect... Camera1_1 Event Configuration

☑ Enable

Arming Schedule: All-day Template

Trigger Camera: Camera1_1

Arming Region

Virtual Line ID: 1

Virtual Line Direction: A<->B

Sensitivity: 50

□ Trigger Alarm Output	□ Trigger Channel Record	☑ Trigger Client Action
□ A->1	□ Camera01	☑ Audible Warning
□ A->2		☑ Email Linkage

Table 6. 8 Linkage Actions for Line Crossing Detection Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.9 Configuring Intrusion Detection Alarm

Purpose:

You can set a detection area in the surveillance scene for Intrusion and once the area is been entered longer than the set time duration, a set of alarm action is triggered.

Note: The Intrusion Detection function requires the support of connected device.

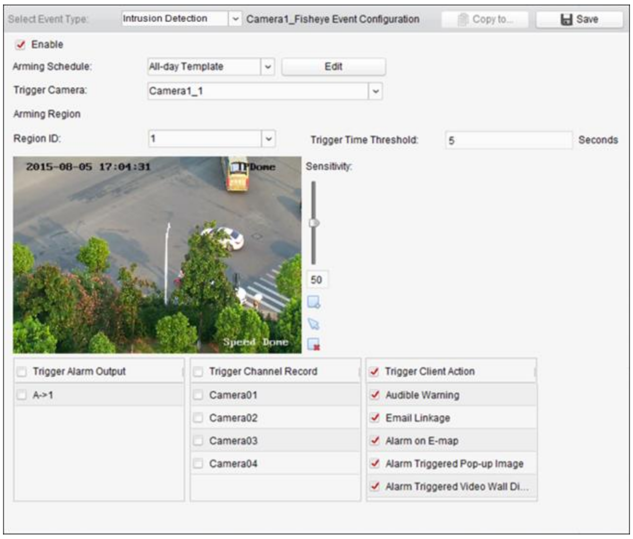
Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Intrusion Detection** as the event type.
3. Check the checkbox **Enable** to enable the function of intrusion detection alarm.

   Note: For the specific speed dome, you can click **Lock** to prevent the speed dome from moving automatically during the configuration.
4. Select the arming schedule template from the drop-down list.

   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.

5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when intrusion detection alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
6. Configure the arming region.
   - **Region ID:** Click the drop-down list to choose a region ID for the arming region.
     Note: For some specific speed dome, you can click **PTZ** to move the speed dome to the desired scene which corresponds to a region ID. In this way, you can configure the different Intrusion detection alarms for multiple views.
   - **Trigger Time Threshold:** Range [0 to 10s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.
   - **Sensitivity:** Range [1 to 100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
7. Click and draw a quadrangle on the preview window. Optionally, you can click and drag the quadrangle to adjust its position, or click to delete the selected region.
   Notes:
   - When you draw the quadrangle, click on the preview window to set the vertex to set the quadrangle.
   - Select another region ID and draw another one. Up to 4 quadrangles can be drawn.
8. Check the checkboxes to activate the linkage actions. For details, see *Table 6.9 Linkage Actions for Intrusion Alarm*.
9. Optionally, click **Copy to...** to copy the event parameters to other cameras.
10. Click **Save** to save the new settings.



Select Event Type: Intrusion Detection
Camera1_Fisheye Event Configuration

☑ Enable
Arming Schedule: All-day Template
Trigger Camera: Camera1_1
Arming Region
Region ID: 1
Trigger Time Threshold: 5 Seconds
Sensitivity: 50

□ Trigger Alarm Output
□ A->1

□ Trigger Channel Record
□ Camera01
□ Camera02
□ Camera03
□ Camera04

☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage
☑ Alarm on E-map
☑ Alarm Triggered Pop-up Image
☑ Alarm Triggered Video Wall Di...

Table 6. 9 Linkage Actions for Intrusion Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can

	select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.10 Configuring Scene Change Alarm

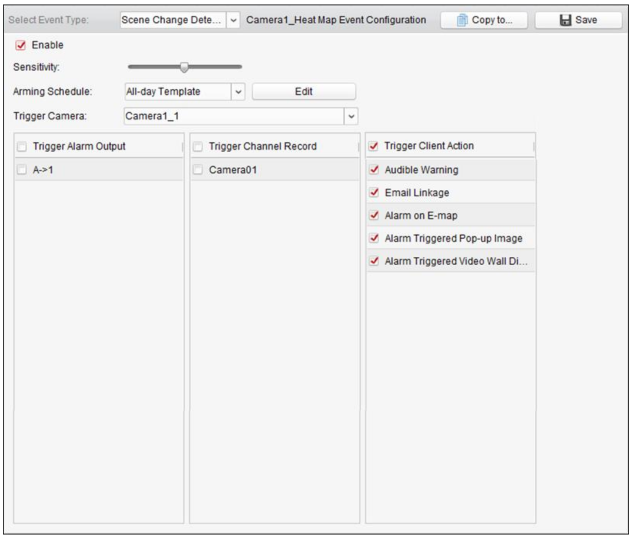
Purpose:

Scene change detection is used to detect the change of surveillance environment affected by the external factors; such as the intentional rotation of the camera.

Note: The Scene Detection function requires the support of connected device.

Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Scene Detection** as the event type.
3. Check the checkbox **Enable** to enable the function of audio detection alarm.
   Sensitivity: Range [1 to 100]. The higher the sensitivity, the easier the change of scene can trigger the alarm.
4. Select the arming schedule template from the drop-down list.
   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when scene change alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*
6. Check the checkboxes to activate the linkage actions. For details, see *Table 6.10 Linkage Actions for Scene Change Alarm*.
7. Optionally, click **Copy to…** to copy the event parameters to other cameras.
8. Click **Save** to save the new settings.



Select Event Type: Scene Change Dete...

Camera1_Heat Map Event Configuration

☑ Enable

Sensitivity:

Arming Schedule: All-day Template

Trigger Camera: Camera1_1

□ Trigger Alarm Output
□ A->1

□ Trigger Channel Record
□ Camera01

☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage
☑ Alarm on E-map
☑ Alarm Triggered Pop-up Image
☑ Alarm Triggered Video Wall Di...

Table 6. 10 Linkage Actions for Scene Change Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.11 Configuring VCA Detection Alarm

Purpose:

When the VCA alarm of the connected device occurs, a series of linkage actions can be triggered.

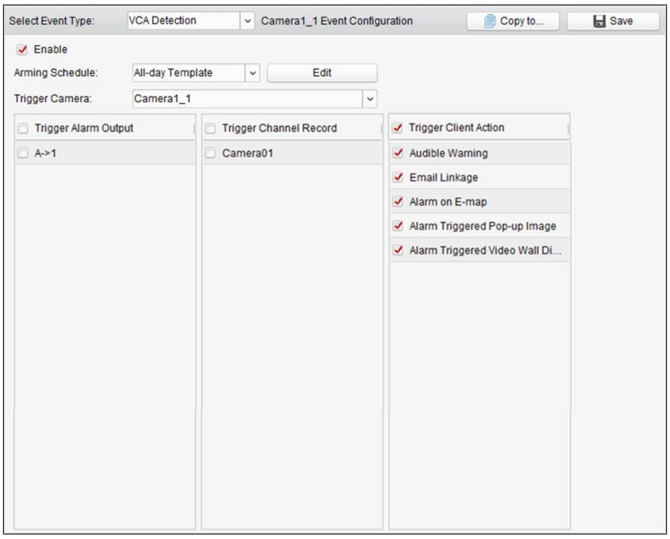
Note: The VCA Detection function requires the support of connected device.

Steps:

1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **VCA Detection** as the event type.
3. Check the checkbox **Enable** to enable the function of VCA Detection alarm.
4. Select the arming schedule template from the drop-down list.
   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
5. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when VCA detection alarm 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. For details, refer to *Chapter 5.1 Remote Storage.*

6. Check the checkboxes to activate the linkage actions. For details, see *Table 6.11 Linkage Actions for VCA Detection Alarm*.
7. Optionally, click **Copy to…** to copy the event parameters to other cameras.
8. Click **Save** to save the new settings.



Select Event Type: VCA Detection

Camera1_1 Event Configuration

☑ Enable

Arming Schedule: All-day Template

Trigger Camera: Camera1_1

□ Trigger Alarm Output
□ A->1

□ Trigger Channel Record
□ Camera01

☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage
☑ Alarm on E-map
☑ Alarm Triggered Pop-up Image
☑ Alarm Triggered Video Wall Di...

Table 6. 11 Linkage Actions for VCA Detection Alarm

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image of the triggered camera pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.12 Configuring Alarm Input Linkage

Purpose:

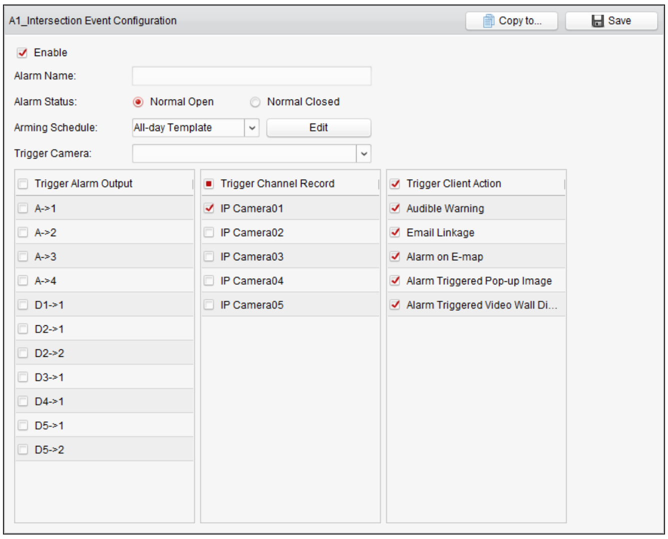
When a device's alarm input port receives a signal from an external alarm device, such as smoke detector, doorbell, etc., the alarm input linkage actions are triggered for notification.

Before you start:

Add the alarm inputs to the client, click **Import** on the Group Management interface, click the **Alarm Input** tab and import alarm inputs into groups for management.

Steps:

1. Open the Event Management page and click the **Alarm Input** tab.
2. Select the alarm input channel to be configured.
3. Check the checkbox **Enable**.
4. Input a descriptive name of the alarm.
5. Set the alarm status according to the alarm input device.
6. Select the arming schedule template from the drop-down list.
   If you need to edit or customize the template, see *Configuring Arming Schedule Template*.
7. Select the triggered camera. The image or video from the triggered camera will pop up or be displayed on the Video Wall when alarm input 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. For details, refer to *Chapter 5.1 Remote Storage.*
8. Check the checkboxes to activate the linkage actions. For details, see *Table 6.12 Linkage Actions for Alarm Input*.
9. Optionally, click **Copy to…** to copy the event parameters to other alarm inputs.
10. Click **Save** to save the settings.



A1_Intersection Event Configuration

Copy to... Save

☑ Enable

Alarm Name:

Alarm Status: ● Normal Open ○ Normal Closed

Arming Schedule: All-day Template Edit

Trigger Camera:

□ Trigger Alarm Output
□ A->1
□ A->2
□ A->3
□ A->4
□ D1->1
□ D2->1
□ D2->2
□ D3->1
□ D4->1
□ D5->1
□ D5->2

■ Trigger Channel Record
☑ IP Camera01
□ IP Camera02
□ IP Camera03
□ IP Camera04
□ IP Camera05

☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage
☑ Alarm on E-map
☑ Alarm Triggered Pop-up Image
☑ Alarm Triggered Video Wall Di...

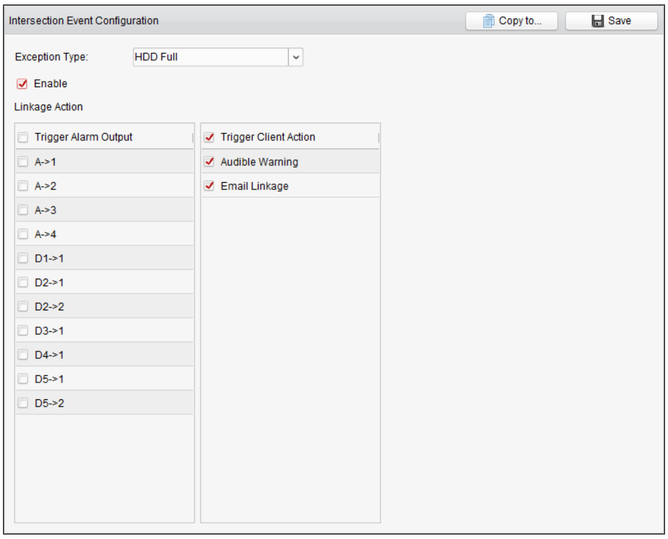
Table 6. 12 Linkage Actions for Alarm Input

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled.
Channel Record	Start the recording of the selected cameras when alarm is triggered.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.
Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

6.13 Configuring Device Exception Linkage

Steps:

1. Open the Event Management page and click the **Exception** tab.
2. Select the device to be configured.
3. Select the device exception type, including HDD full, HDD exception, illegal login, device offline, etc.
4. Check the checkbox **Enable**.
5. Check the checkboxes to activate the linkage actions. For details, see *Table 6.13 Linkage Actions for Device Exception*.
6. Optionally, click **Copy to...** to copy the event parameters to other devices.
7. Click **Save** to save the settings.



Exception Type: HDD Full

☑ Enable

Linkage Action

□ Trigger Alarm Output
□ A->1
□ A->2
□ A->3
□ A->4
□ D1->1
□ D2->1
□ D2->2
□ D3->1
□ D4->1
□ D5->1
□ D5->2

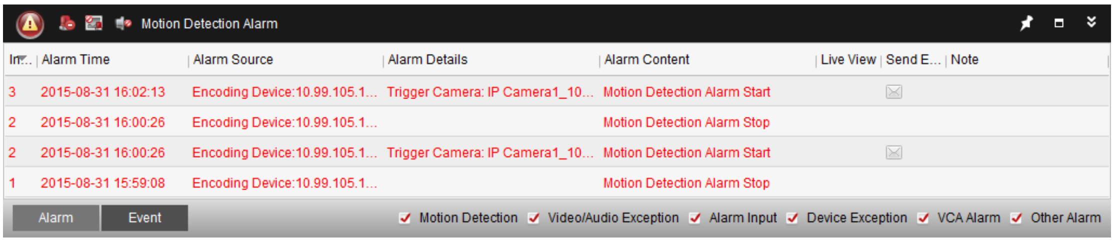
☑ Trigger Client Action
☑ Audible Warning
☑ Email Linkage

Table 6. 13 Linkage Actions for Device Exception

Linkage Actions	Descriptions
Alarm Output	Enable the alarm output function. Select the alarm output port and the external device connected to the port can be controlled. ***Note:*** Alarm Output is not available for Device Offline exception.
Audible Warning	The client software gives an audible warning when alarm is triggered. You can select the alarm sound for audible warning. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
Email Linkage	Send an email notification of the alarm information to one or more receivers.

6.14 Viewing Alarm and Event Information

The information of recent alarms and events can be displayed. Click the icon ⏶ in Alarms and Events Toolbar to show the Alarms and Events panel.



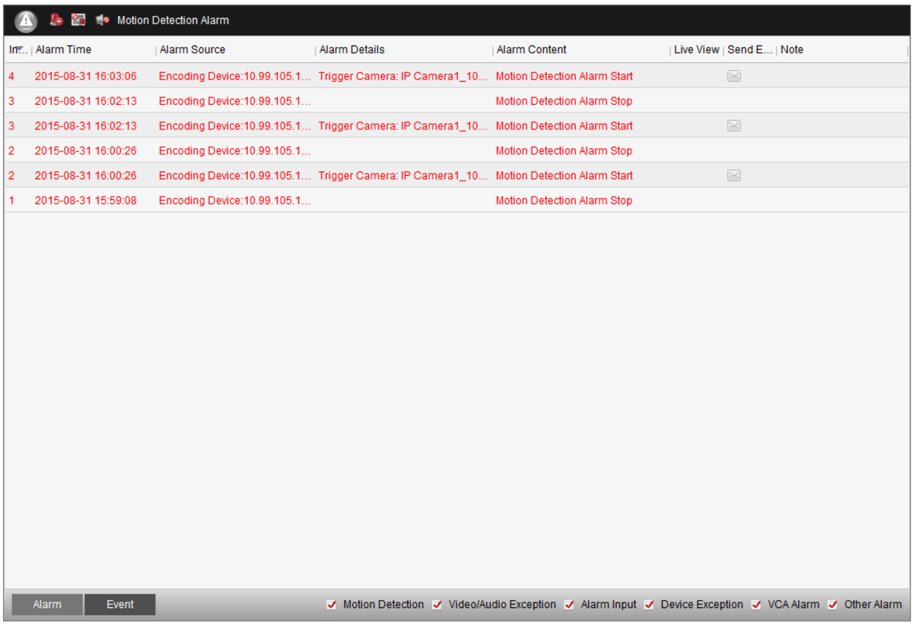
Motion Detection Alarm

Im...	Alarm Time	Alarm Source	Alarm Details	Alarm Content	Live View	Send E...	Note
3	2015-08-31 16:02:13	Encoding Device:10.99.105.1...	Trigger Camera: IP Camera1_10...	Motion Detection Alarm Start		✉	
2	2015-08-31 16:00:26	Encoding Device:10.99.105.1...		Motion Detection Alarm Stop			
2	2015-08-31 16:00:26	Encoding Device:10.99.105.1...	Trigger Camera: IP Camera1_10...	Motion Detection Alarm Start		✉	
1	2015-08-31 15:59:08	Encoding Device:10.99.105.1...		Motion Detection Alarm Stop			

Alarm
Event
☑ Motion Detection ☑ Video/Audio Exception ☑ Alarm Input ☑ Device Exception ☑ VCA Alarm ☑ Other Alarm

You can click □ to display the Alarm Event interface.

Or click icon on the control panel to enter the Alarm Event interface.

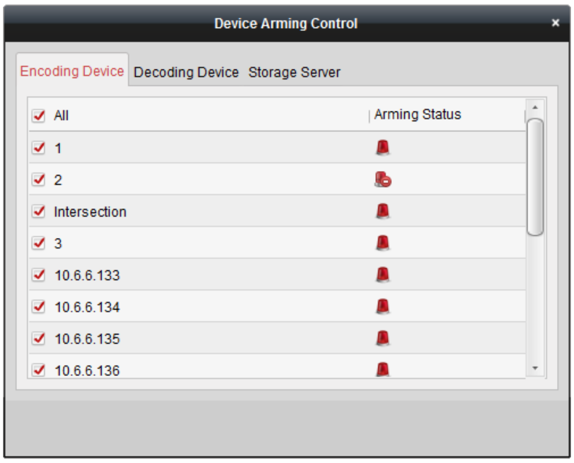


Motion Detection Alarm

Im...	Alarm Time	Alarm Source	Alarm Details	Alarm Content	Live View	Send E...	Note
4	2015-08-31 16:03:06	Encoding Device:10.99.105.1...	Trigger Camera: IP Camera1_10...	Motion Detection Alarm Start		✉	
3	2015-08-31 16:02:13	Encoding Device:10.99.105.1...		Motion Detection Alarm Stop			
3	2015-08-31 16:02:13	Encoding Device:10.99.105.1...	Trigger Camera: IP Camera1_10...	Motion Detection Alarm Start		✉	
2	2015-08-31 16:00:26	Encoding Device:10.99.105.1...		Motion Detection Alarm Stop			
2	2015-08-31 16:00:26	Encoding Device:10.99.105.1...	Trigger Camera: IP Camera1_10...	Motion Detection Alarm Start		✉	
1	2015-08-31 15:59:08	Encoding Device:10.99.105.1...		Motion Detection Alarm Stop			

Alarm
Event
☑ Motion Detection ☑ Video/Audio Exception ☑ Alarm Input ☑ Device Exception ☑ VCA Alarm ☑ Other Alarm

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



Device Arming Control

☑ All	Arming Status
☑ 1	🔔
☑ 2	🔔
☑ Intersection	🔔
☑ 3	🔔
☑ 10.6.6.133	🔔
☑ 10.6.6.134	🔔
☑ 10.6.6.135	🔔
☑ 10.6.6.136	🔔

On the Alarms and Events panel, the following toolbar buttons are available:

	Clear Info	Clear the information of alarms and events displayed on the list.
	Enable/Disable Alarm Triggered Pop-up Image	Click to enable/disable image pop-up when alarms occur.
	Enable/Disable Audio	Click to enable/disable the audio warning for the alarm.
	Auto Hide/Lock	Click to hide automatically/lock the Alarms and Events panel.

▣	**Maximize**	Maximize the Alarms and Events panel in a new tab page.
⏫ ⏬	**Show/Hide**	Click to show/hide the Alarms and Events panel.

6.14.1 Viewing Alarms Information

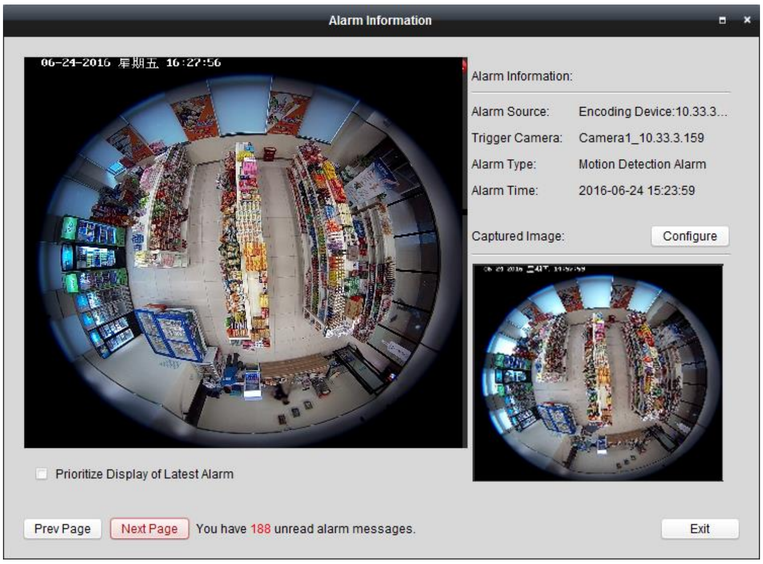
Different alarm types can be displayed on the panel: Motion Detection, Video/Audio Exception, Alarm Input, Device Exception, VCA Alarm and Other Alarm. You can check the checkbox to enable the displaying of that type alarm.

Before you start:

To display the alarms, the event parameters need to be configured.

Steps:

1. Click the **Alarm** tab.
2. Check the checkboxes of different alarm types.
3. When an alarm occurs, the icon ⚠ twinkles to call attention. The alarm information, including the time, source, details and content will be displayed.
4. Click ▶ to get a live view of the alarm triggered camera.



Alarm Information

06-24-2016 星期五 16:27:56

Alarm Information:

Alarm Source: Encoding Device:10.33.3...

Trigger Camera: Camera1_10.33.3.159

Alarm Type: Motion Detection Alarm

Alarm Time: 2016-06-24 15:23:59

Captured Image:

□ Prioritize Display of Latest Alarm

You have 188 unread alarm messages.

You can view the live video of the triggered camera. You can click **Prev Page** or **Next Page** button to view the next alarm information.

Notes:

- The **Picture Storage** should be checked for storing the alarm pictures of the camera on the storage server. You can click **Configure** to set the parameters. For details, please refer to *Chapter 5.1.2 Storing on Storage Device*.
- The **Prioritize Display of Latest Alarm** is unchecked by default.
  You can check this checkbox to switch to view the latest triggered alarm. The alarm window is in 4-window division. The latest alarm will replace the earliest alarm window of the displayed four windows.

5. Click ✉ to send an email notification of the alarm to one or more receivers if the email settings are properly configured (*Section 17.2.6 Email Settings*).
6. Click ▦ to display the video of alarm triggered camera on the Video Wall. You can enter the Video Wall interface to check the alarm triggered video playing on the screen which set as the

alarm window. The physical video wall also displays the video.

Note: You should add decoding device and configure the video wall. For details, please refer to *Chapter 12 Decoding and Displaying Video on Video Wall*.

Click under the **Note** column to input the description for the alarm.

7. To clear the alarm information, click the icon, or right-click on an alarm log and then click **Clear**.

6.14.2 Viewing Events Information

Purpose:

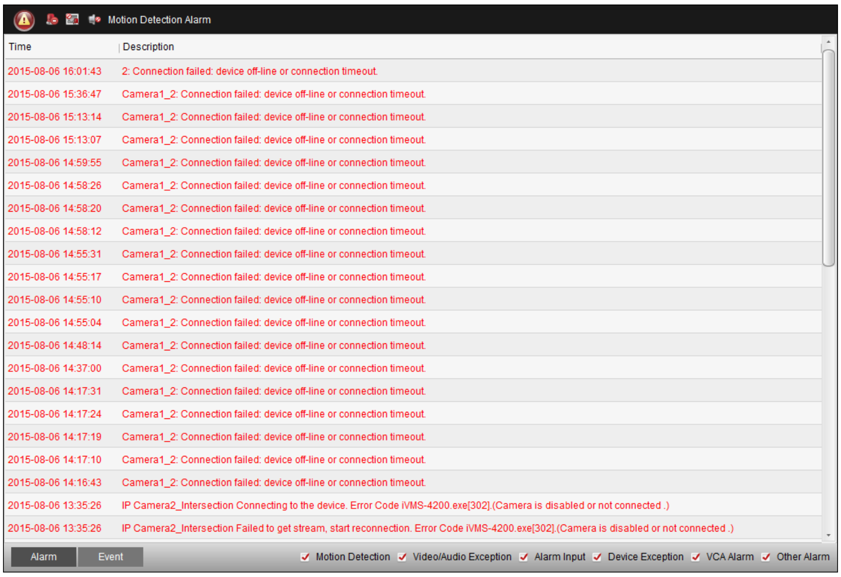
The abnormal events of the client software, such as the live view failure, device disconnection, can also be displayed.

Steps:

1. Click the **Event** tab.

   The event information, including the time and detailed description will be displayed.

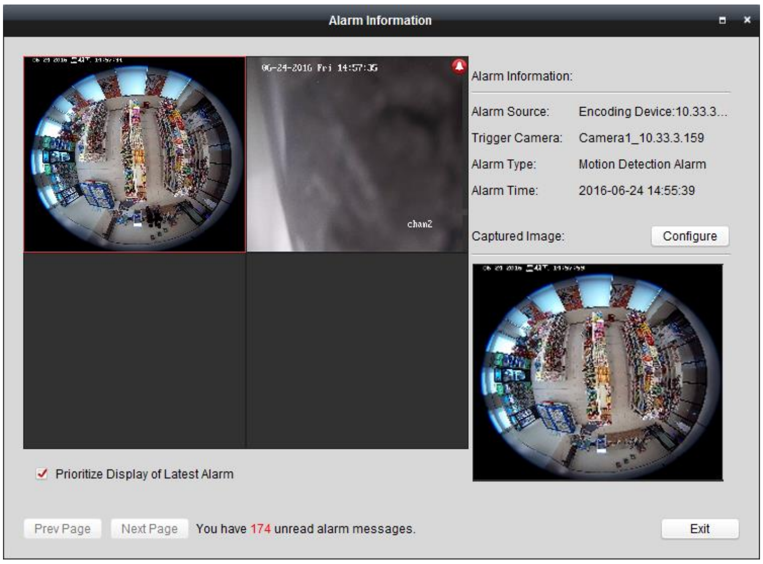
2. To clear the event information, click the icon, or right-click on the event log and then click **Clear**.



Time	Description
2015-08-06 16:01:43	2: Connection failed: device off-line or connection timeout.
2015-08-06 15:36:47	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 15:13:14	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 15:13:07	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:59:55	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:58:26	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:58:20	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:58:12	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:55:31	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:55:17	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:55:10	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:55:04	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:48:14	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:37:00	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:17:31	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:17:24	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:17:19	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:17:10	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 14:16:43	Camera1_2: Connection failed: device off-line or connection timeout.
2015-08-06 13:35:26	IP Camera2_Intersection Connecting to the device. Error Code iVMS-4200.exe[302].(Camera is disabled or not connected .)
2015-08-06 13:35:26	IP Camera2_Intersection Failed to get stream, start reconnection. Error Code iVMS-4200.exe[302].(Camera is disabled or not connected .)

6.14.3 Viewing Pop-up Alarm Information

After enabling the event linkage of **Alarm Triggered Pop-up Image**, and enabling the **Enable Alarm Triggered Pop-up Image** function on the client, the alarm image will pop up when the corresponding event/alarm is triggered.



Alarm Information:

Alarm Source: Encoding Device:10.33.3...

Trigger Camera: Camera1_10.33.3.159

Alarm Type: Motion Detection Alarm

Alarm Time: 2016-06-24 14:55:39

Captured Image:

☑ Prioritize Display of Latest Alarm

You have 174 unread alarm messages.

You can view the live video of the triggered camera. In the right panel, the alarm picture displays.

Notes:

- The **Picture Storage** should be checked for storing the alarm pictures of the camera on the storage server. You can click **Configure** to set the parameters. For details, please refer to *Chapter 5.1.2 Storing on Storage Device*.
- The **Prioritize Display of Latest Alarm** is checked by default and the alarm window is in 4-window division. The latest alarm will replace the earliest alarm window of the displayed four windows.

  You can uncheck this checkbox to switch to view the current triggered alarm. You can click **Prev Page** or **Next Page** button to view the next alarm information.

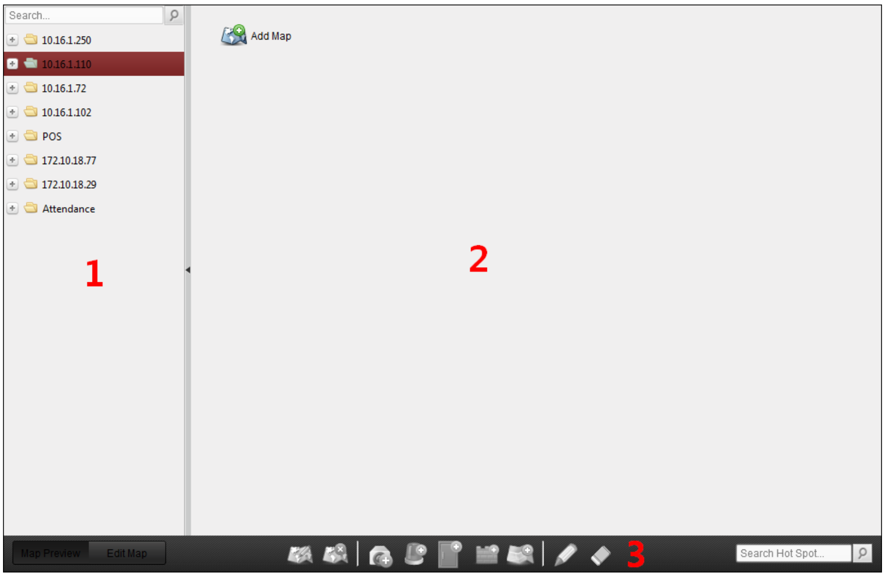
Chapter 7 E-map Management

Purpose:

The E-map function gives a visual overview of the locations and distributions of the installed cameras, alarm input devices, zones, and access control points. You can get the live view of the cameras on the map, and you will get a notification message from the map when alarm is triggered. You can also control the access control points on the E-map such as opening and closing door.

Click the icon on the control panel,

or click **View**->**E-map** to open the E-map page.



E-map Page

1 Group List

2 Map Display Area

3 E-map Toolbar

7.1 Adding an E-map

Purpose:

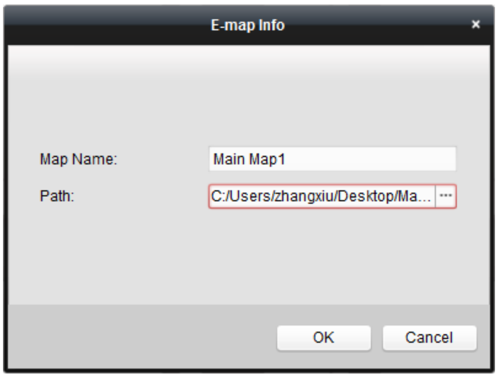
An E-map needs to be added as the parent map for the hot spots and hot regions.

Steps:

1. Open the E-map page.
2. Select a group for which you want to add a map.
3. Click the icon in the Map Display Area to open the map adding dialog box.
4. Input a descriptive name of the added map as desired.
5. Click the icon and select a map file from the local path.
6. Click **OK** to save the settings.

Notes:

- The picture format of the map can only be *.png, *.jpg or *.bmp.
- Only one map can be added to a group.

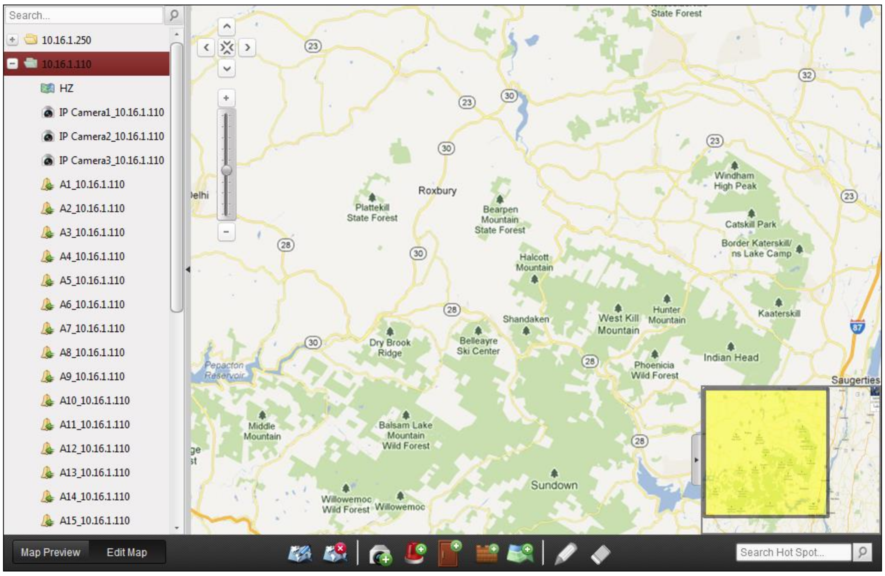


Map Name: Main Map1

Path: C:/Users/zhangxiu/Desktop/Ma...

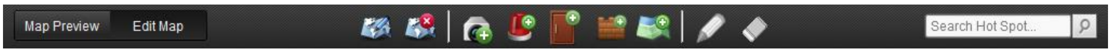
OK Cancel

The map added is displayed in the Map Display Area. Use the mouse wheel or click + or −, to zoom in or zoom out on the map. You can click-and-drag the yellow window in the lower-right corner or use the direction buttons and zoom bar to adjust the map area for view.

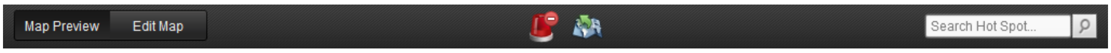


Click the button **Edit Map** or **Map Preview** in the E-map toolbar to enter the map editing mode or map preview mode.

E-map Toolbar in Map Editing Mode:



E-map Toolbar in Map Preview Mode:



On the E-map page, the following toolbar buttons are available:

Modify Map Modify the map information, including the map name and file path.

Delete Map Delete the current map.

Add Camera Add a camera as the hot spot on the map.

Add Alarm Input Add an alarm input sensor as the hot spot on the map.

Add Access Control Point Add an access control point as the hot spot on the map.

Add Zone Add a zone as the hot spot on the map.

Add Hot Region Add a map as the hot region on the current map.

Modify Modify the information of the selected hot spot or hot region.

Delete	Delete the selected hot spot or hot region.
Clear Alarm Info	Clear the alarm information displayed on the map.
Back to Parent Map	Go back to the parent map.

7.2 The Hot Spot Function

Purpose:

The cameras and alarm inputs can be added on the map and are called the hot spots. The hot spots show the locations of the cameras and alarm inputs, and you can also get the live view and alarm information of the surveillance scenarios through the hot spots.

Notes:

- For managing and previewing the access control point hot spot, please refer to *Chapter 15.5 Displaying Access Control Point on E-map*.
- For managing and previewing the zone hot spot, please refer to *Chapter 13.4 Displaying Zone on E-map.*

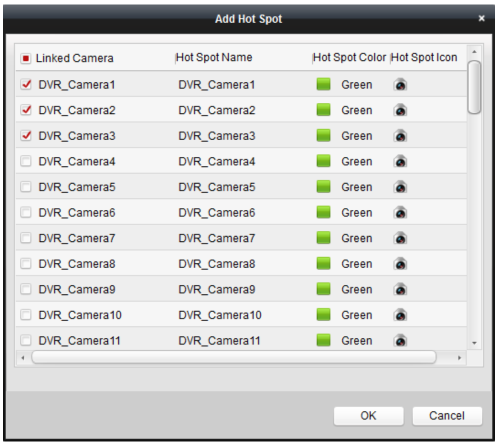
7.2.1 Adding Hot Spots

Adding Cameras as Hot Spots

Steps:

1. Click the **Edit Map** button in the E-map toolbar to enter the map editing mode.
2. Click the icon in the toolbar to open the Add Hot Spot dialog box.
3. Check the checkboxes to select the cameras to be added.
4. Optionally, you can edit hot spot name, select the name color and select the hot spot icon by double-clicking the corresponding field.
5. Click **OK** to save the settings. The camera icons are added on the map as hot spots and the icons of added cameras changes from to in the group list. You can click-and-drag the camera icons to move the hot spots to the desired locations.

   You can also click-and-drag the camera icons from the group list to the map directly to add the hot spots.



Add Hot Spot

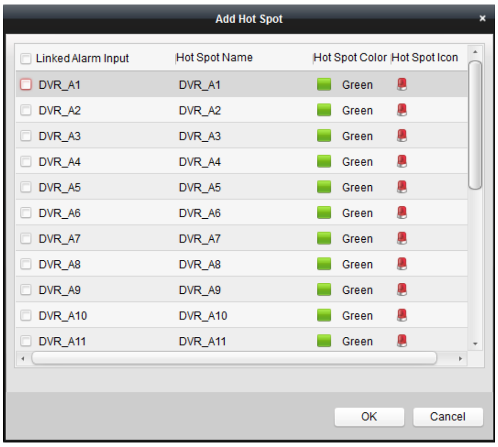
■ Linked Camera	Hot Spot Name	Hot Spot Color	Hot Spot Icon
☑ DVR_Camera1	DVR_Camera1	🟩 Green	●
☑ DVR_Camera2	DVR_Camera2	🟩 Green	●
☑ DVR_Camera3	DVR_Camera3	🟩 Green	●
□ DVR_Camera4	DVR_Camera4	🟩 Green	●
□ DVR_Camera5	DVR_Camera5	🟩 Green	●
□ DVR_Camera6	DVR_Camera6	🟩 Green	●
□ DVR_Camera7	DVR_Camera7	🟩 Green	●
□ DVR_Camera8	DVR_Camera8	🟩 Green	●
□ DVR_Camera9	DVR_Camera9	🟩 Green	●
□ DVR_Camera10	DVR_Camera10	🟩 Green	●
□ DVR_Camera11	DVR_Camera11	🟩 Green	●

Adding Alarm Inputs as Hot Spots

Steps:

1. Click the **Edit Map** button in the E-map toolbar to enter the map editing mode.
2. Click the icon in the toolbar to open the Add Hot Spot dialog box.
3. Check the checkboxes to select the alarm inputs to be added.
4. Optionally, you can edit hot spot name, select the name color and select the hot spot icon by double-clicking the corresponding field.
5. Click **OK** to save the settings. The alarm input icons are added on the map as hot spots and the icons of added alarm inputs changes from to in the group list. You can click-and-drag the alarm input icons to move the hot spots to the desired locations.

   You can also click-and-drag the alarm input icons from the alarm input list to the map directly to add the hot spot.



□ Linked Alarm Input	Hot Spot Name	Hot Spot Color	Hot Spot Icon
□ DVR_A1	DVR_A1	🟩 Green	🚨
□ DVR_A2	DVR_A2	🟩 Green	🚨
□ DVR_A3	DVR_A3	🟩 Green	🚨
□ DVR_A4	DVR_A4	🟩 Green	🚨
□ DVR_A5	DVR_A5	🟩 Green	🚨
□ DVR_A6	DVR_A6	🟩 Green	🚨
□ DVR_A7	DVR_A7	🟩 Green	🚨
□ DVR_A8	DVR_A8	🟩 Green	🚨
□ DVR_A9	DVR_A9	🟩 Green	🚨
□ DVR_A10	DVR_A10	🟩 Green	🚨
□ DVR_A11	DVR_A11	🟩 Green	🚨

7.2.2 Modifying Hot Spots

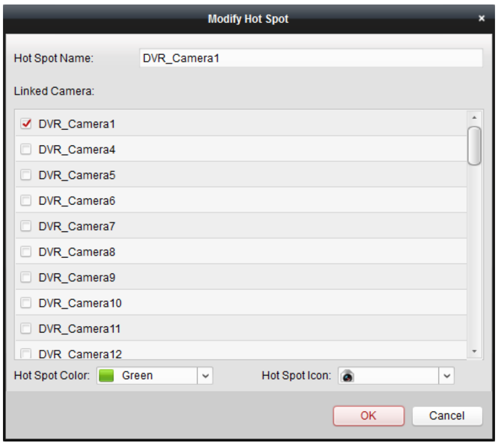
Purpose:

You can modify the information of the added hot spots on the map, including the name, the color, the icon, etc.

Steps:

1. Click the **Edit Map** button in the E-map toolbar to enter the map editing mode.
2. Select the hot spot icon on the map and then click in the toolbar, right-click the hot spot icon and select **Modify**, or double-click the hot spot icon on the map to open the Modify Hot Spot dialog box.
3. You can edit the hot spot name in the text field and select the color, the icon and the linked camera or alarm input.
4. Click **OK** to save the new settings.

   To delete the hot spot, select the hot spot icon and click in the toolbar, or right-click the hot spot icon and select **Delete**.



Modify Hot Spot

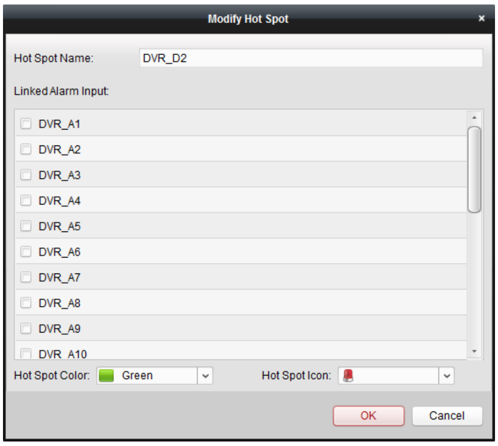
Hot Spot Name: DVR_Camera1

Linked Camera:

- ☑ DVR_Camera1
- ☐ DVR_Camera4
- ☐ DVR_Camera5
- ☐ DVR_Camera6
- ☐ DVR_Camera7
- ☐ DVR_Camera8
- ☐ DVR_Camera9
- ☐ DVR_Camera10
- ☐ DVR_Camera11
- ☐ DVR_Camera12

Hot Spot Color: 🟩 Green

Hot Spot Icon:



Modify Hot Spot

Hot Spot Name: DVR_D2

Linked Alarm Input:

- ☐ DVR_A1
- ☐ DVR_A2
- ☐ DVR_A3
- ☐ DVR_A4
- ☐ DVR_A5
- ☐ DVR_A6
- ☐ DVR_A7
- ☐ DVR_A8
- ☐ DVR_A9
- ☐ DVR_A10

Hot Spot Color: 🟩 Green

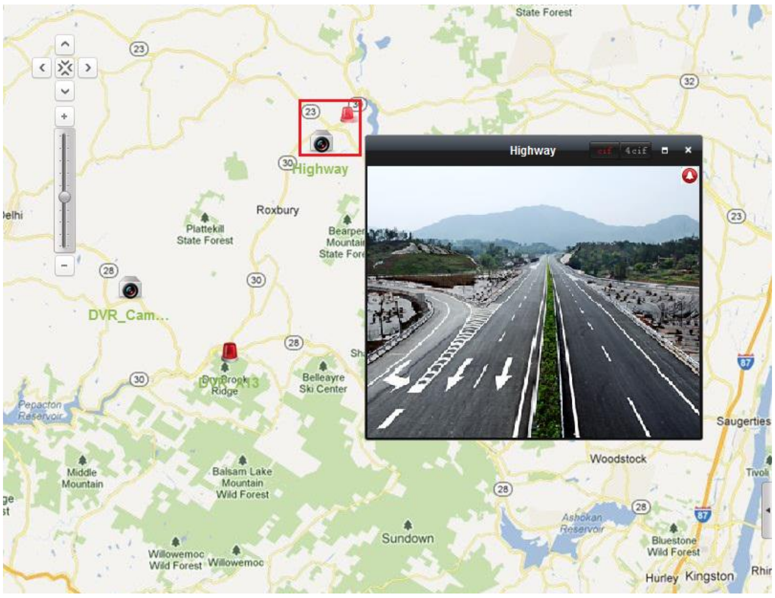
Hot Spot Icon:

7.2.3 Previewing Hot Spots

Steps:

1. Click the **Map Preview** button in the E-map toolbar to enter the map preview mode.
2. Double-click the camera hot spots or right-click it and select **Live View**, and you can get the live view of the cameras.
3. If there is any alarm triggered, an icon 🚨 will appear and twinkle near the hot spot. Click the alarm icon, and then you can check the alarm information, including alarm type and triggering time.

Note: To display the alarm information on the map, the Alarm on E-map functionality needs to be set as the alarm linkage action. For details, refer to *Chapter 6 Event Management*.



7.3 The Hot Region Function

Purpose:

The hot region function links a map to another map. When you add a map to another map as a hot region, an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

Note: A map can only be added as the hot region for one time.

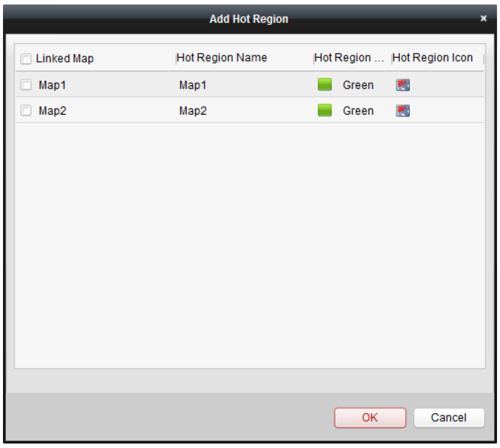
7.3.1 Adding Hot Regions

Before you start:

Add a map to another group.

Steps:

1. Click the **Edit Map** button in the E-map toolbar to enter the map editing mode.
2. Select an added map as the parent map.
3. Click the icon in the toolbar to open the Add Hot Region dialog box.
4. Check the checkbox to select the child map to be linked.
5. Optionally, you can edit the hot region name, and select the hot region color and icon by double-clicking the corresponding field.
6. Click **OK** to save the settings. The child map icons are added on the parent map as the hot regions. You can click-and-drag the child map icons to move the hot regions to desired locations.



□ Linked Map	Hot Region Name	Hot Region ...	Hot Region Icon
□ Map1	Map1	🟩 Green	
□ Map2	Map2	🟩 Green	

7.3.2 Modifying Hot Regions

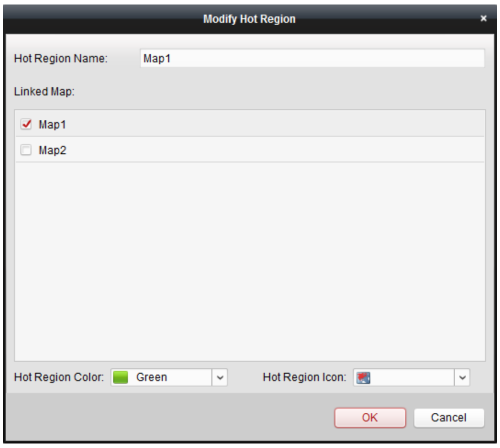
Purpose:

You can modify the information of the hot regions on the parent map, including the name, the color, the icon, etc.

Steps:

1. Click the **Edit Map** button in the E-map toolbar to enter the map editing mode.
2. Select the hot region icon on the parent map and then click in the toolbar, right-click the hot spot icon and select **Modify**, or double-click the hot region icon to open the Modify Hot Region dialog box.
3. You can edit the hot region name in the text field and select the color, the icon and the linked child map.
4. Click **OK** to save the new settings.

   To delete the hot region, select the hot region icon and click in the toolbar, or right-click the hot spot icon and select **Delete**.



Modify Hot Region

Hot Region Name: Map1

Linked Map:

☑ Map1

□ Map2

Hot Region Color: 🟩 Green

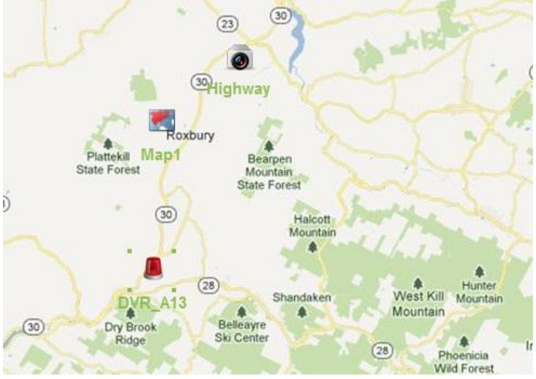
Hot Region Icon:

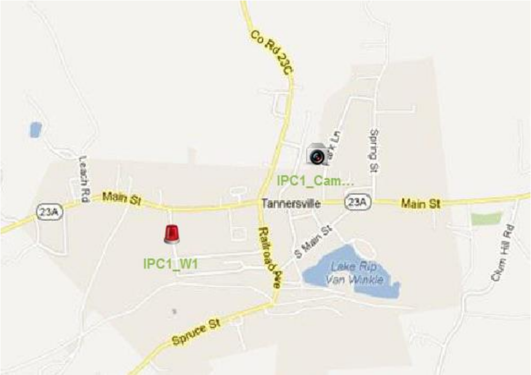
7.3.3 Previewing Hot Regions

Steps:

1. Click the **Map Preview** button in the E-map toolbar to enter the map preview mode.
2. Click the hot region icon to go to the linked child map.
3. The hot spots can also be added on the hot regions.
4. You can click the icon in the toolbar to go back to the parent map.

   You can also click the icon in the toolbar to clear the alarm information.





Chapter 8 Hik Cloud P2P

Purpose:

The client software also supports to register a Hik Cloud P2P account, log into your Hik Cloud P2P and manage the devices which support the Hik Cloud P2P service.

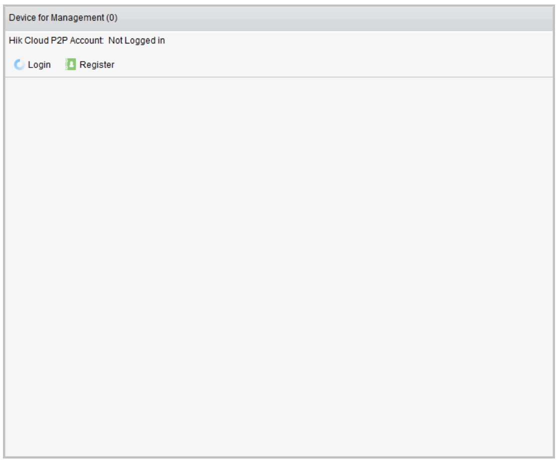
8.1 Registering a Hik Cloud P2P Account

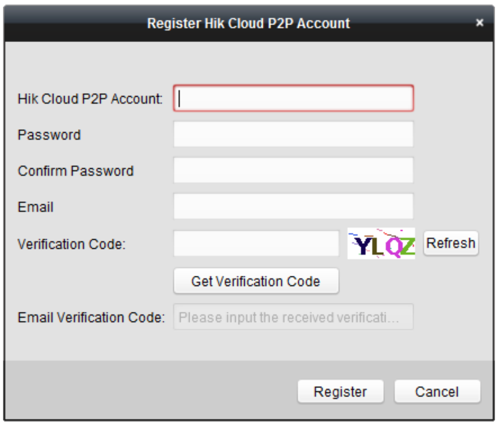
Purpose:

If you do not have a Hik Cloud P2P account, you can register one.

Steps:

1. Open the Device Management page and click the **Server** tab.
2. Click **Add New Device Type**, select **Hik Cloud P2P Device** and click **OK**.
3. Click **Hik Cloud P2P Device** on the list and then click **Register**.


Device for Management (0)
Hik Cloud P2P Account: Not Logged in
Login
Register



4. Enter the required information to register an account.

   Hik Cloud P2P Account: Edit a user name for your account as desired.

   Password and **Confirm**: Enter the password for your account and confirm it.

   Email: Enter your email account to register the account.

   Verification Code: Enter the verification code shown in the picture. If it is not clear, you can click **Refresh** to get a new one.

   Email Verification Code: Click **Get Verification Code** and enter the verification code received by your email.

   - *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.*

5. Click **Register** to get a Hik Cloud P2P account.

8.2 Logging into Hik Cloud P2P Account

Steps:

1. Click **Login** and enter the Hik Cloud P2P account and password.
2. Click **Login** to log into your account.

   Notes:

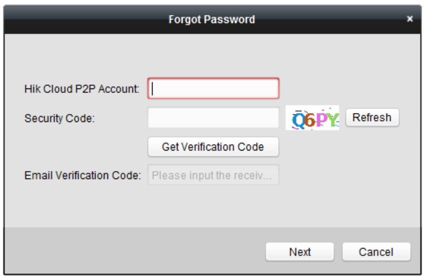
   - The software will login the Hik Cloud P2P account automatically next time.
   - If you forget your password, click **Forgot Password** to verify your account and reset your password.

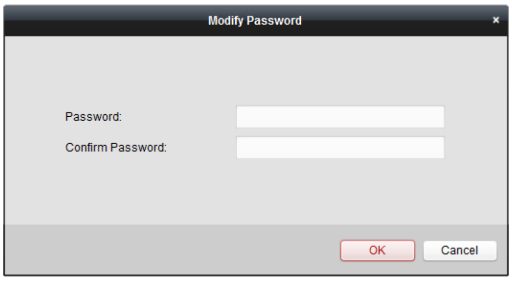
     Hik Cloud P2P Account: Edit user name of your account.

     Security Code: Enter the security code shown in the picture. If it is not clear, you can click **Refresh** to get a new one.

     Email Verification Code: Click **Get Verification Code** and enter the verification code received by your email.

     Password and **Confirm**: Click **Next** and enter a new password for your account and confirm it.





- ◆ *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.*

3. After login, you can click **Login** to switch to another account or click **Logout** to log out of your Hik Cloud P2P account.

8.3 Device Management

Steps:

1. Click **Add Device** and input the serial No. and verification code of the device.

   Notes:

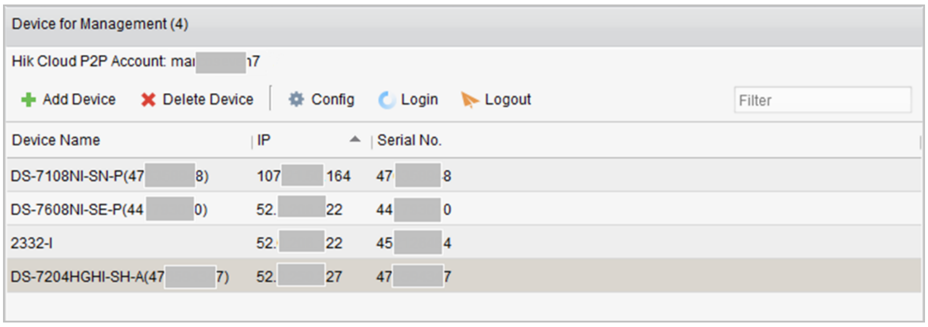
   - Only the device that supports the Hik Cloud P2P service can be added.
   - The serial No. and the verification code is marked on the label of you device.
   - The device can only be added to one Hik Cloud P2P account.
2. Click **OK** to add the device and the successfully added device will list on the device management

interface.

Note: A group named as your account name is created by default, you can import the cameras of the added devices to the default group or other groups. For group management, please refer to *Chapter 3.2 Group Management.*

3. For live view, please refer to *Chapter 4 Live View*; for playback, please refer to *Chapter 5.2 Remote Playback*; for e-map settings, please refer to *Chapter 7 E-map Management.*
4. Click to select a device and click **Config** to pop up the remote configuration interface of the device. You can do some remote configurations for the device. For detailed settings about the remote configuration, please refer to the *User Manual* of the device.

   Note: This function should be suported by the device.
5. If you want delete the device, select the device(s) and click **Delete Device**. You can also enter the keyword of the device name in the **Filter** field to filter the required devices.



Device for Management (4)

Hik Cloud P2P Account: mai[redacted]7

Device Name	IP	Serial No.
DS-7108NI-SN-P(47[redacted]8)	107[redacted]164	47[redacted]8
DS-7608NI-SE-P(44[redacted]0)	52.[redacted]22	44[redacted]0
2332-I	52.[redacted]22	45[redacted]4
DS-7204HGHI-SH-A(47[redacted]7)	52.[redacted]27	47[redacted]7

Chapter 9 VCA Devices Management

Purpose:

The VCA (Video Content Analysis) devices can be added to the client for VCA configuration, including VCA resource allocation, rule settings, VQD (Video Quality Diagnostics), etc.

Allocating VCA Resource

Before you start: You should add the VCA device to the software. Please refer to *Chapter 3.1 Adding the Device* for adding the VCA device as Encoding Device.

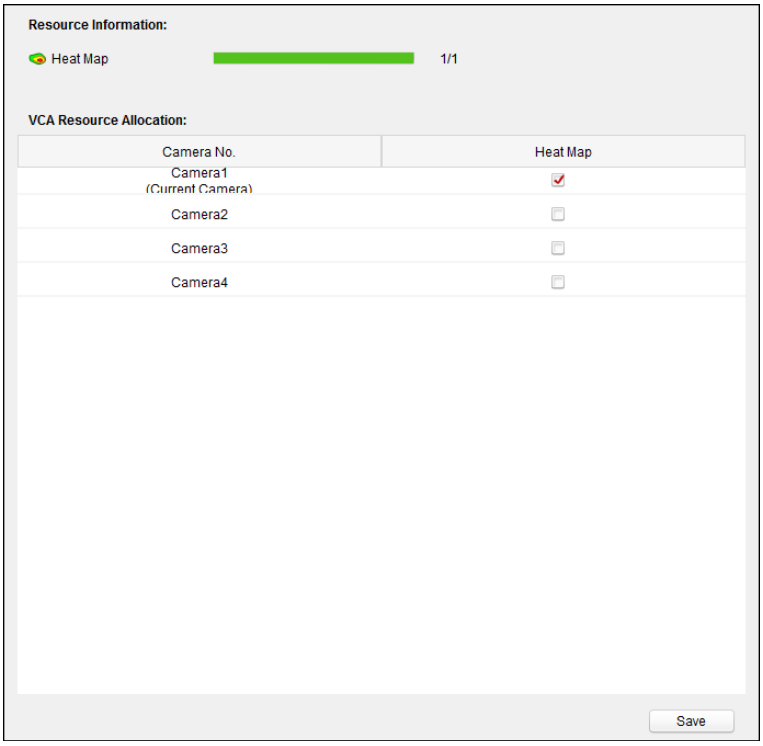
Purpose: Before you can set the VCA configuration for the added device, you need to configure the VCA resource of the device which means to enable the VCA function of the corresponding cameras.

Option 1

Steps:

1. In the Device Management Configuration interface, select **Server** tab.
2. Click to select the VCA device and click **Remote Configuration** to activate the Remote Configuration window.
3. In the Remote Configuration window, click **VCA Config** to expand the VCA configuration list. In the camera dropdown list, select **VCA Resource Allocation** to allocate the VCA resource.
4. In the Resource Information area, you can view the VCA type and VCA resource usage of the device.

   Example: In the figure shown below, the VCA type of the device is Heat Map and four cameras are available for configuring VCA settings. The camera1 has been enabled with VCA function.



Resource Information:

Heat Map 1/1

VCA Resource Allocation:

Camera No.	Heat Map
Camera1 (Current Camera)	☑
Camera2	□
Camera3	□
Camera4	□

5. In the VCA Resource Allocation panel, check ☑ checkbox to enable the VCA function of the camera.

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

Configuring VCA Settings

After allocating the VCA resource, you can configure the VCA settings for the camera.

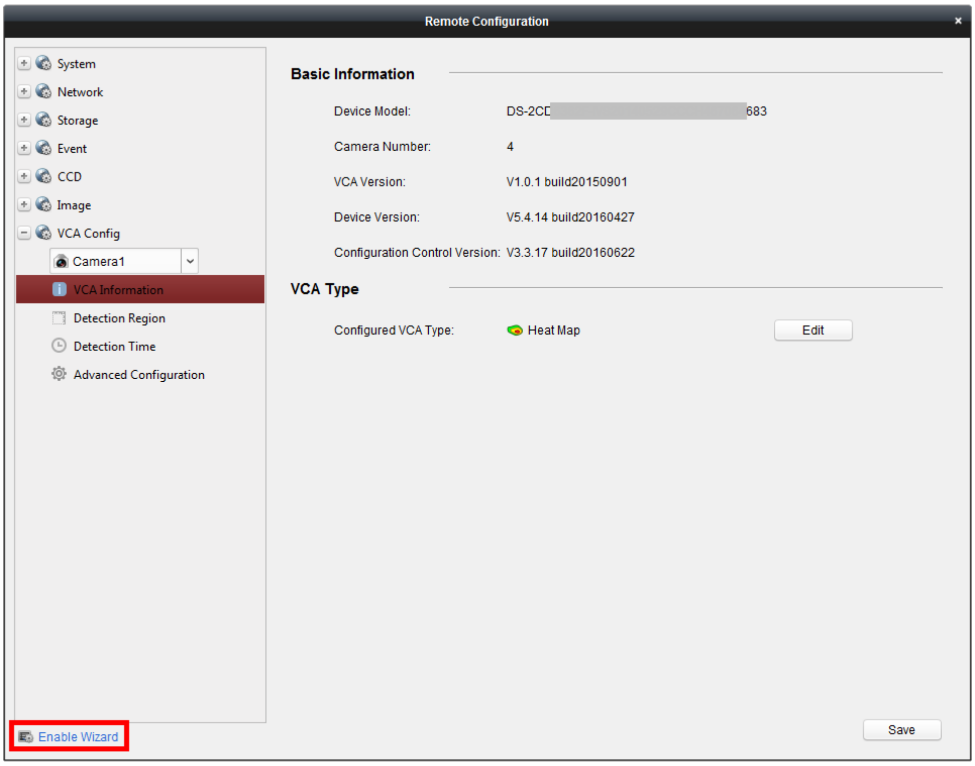
Steps:

1. In the Device Management Configuration interface, select **Server** tab.
2. Click to select the VCA device and click **Remote Configuration** to activate the Remote Configuration window.
3. In the Remote Configuration window, click **VCA Config** to expand the VCA configuration list.

   Note: The VCA configuration list varies according to different VCA devices.

You can set the VCA configuration for the camera according to the provided instruction.

Click **Enable Wizard** and the wizard will guide you to set the quick VCA configuration for the camera.



Basic Information

Device Model: DS-2CD[redacted]683

Camera Number: 4

VCA Version: V1.0.1 build20150901

Device Version: V5.4.14 build20160427

Configuration Control Version: V3.3.17 build20160622

VCA Type

Configured VCA Type: Heat Map

Chapter 10 Transcoder Management

Purpose:

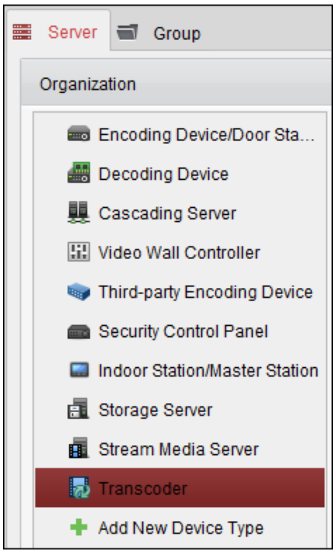
Transcoder is designed for real-time transcoding of different streams. With the use of transcoder, streams and control signals from different manufactures and different surveillance systems can be effectively integrated and standardized. iVMS-4200 client software supports to add transcoder and configure the transcoding function for it.

10.1 Adding Encoding Device to the Transcoder

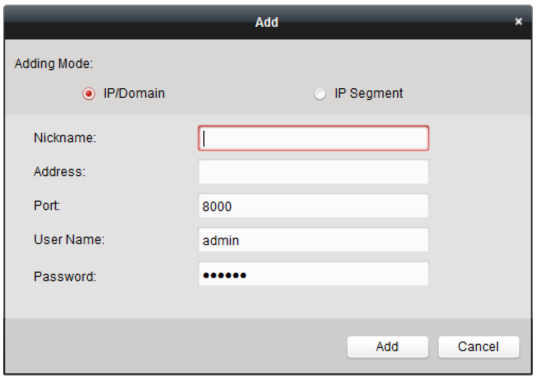
10.1.1 Adding the Transcoder to the Client Software

Steps:

1. Click the icon on the control panel to enter the Device Management interface and click the **Server** tab.
2. Click **Add New Device Type** on the Organization list and select **Transcoder**.
3. Click **OK** to save the settings, and the added transcoder type is displayed on the Organization list.



4. Click **Transcoder** and click **Add Device** to add the transcoder to the management list of the software.



Add

Adding Mode:

● IP/Domain ○ IP Segment

Nickname:

Address:

Port: 8000

User Name: admin

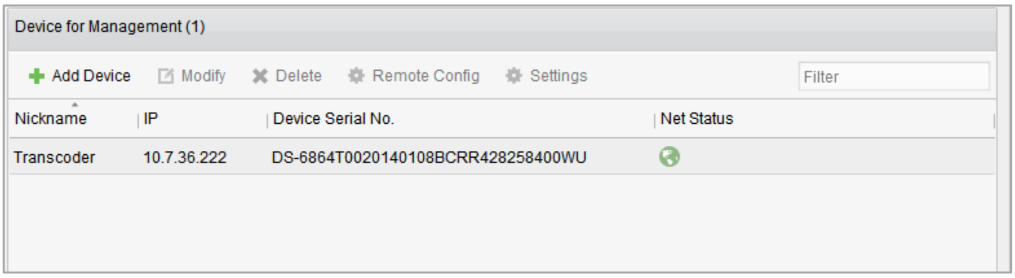
Password: ••••••

Select the adding mode by IP/Domain or by IP segment, and configure the corresponding settings for the device.

For the detailed configuration about the adding modes, please refer to the following sections:

- By specifying the device IP/Domain address, see *Section 3.1.3 Adding Devices Manually.*
- By specifying an IP segment, see *Section 3.1.4 Adding Devices by IP Segment*.

5. The successfully added transcoder can be viewed in the list:



Device for Management (1)

Nickname	IP	Device Serial No.	Net Status
Transcoder	10.7.36.222	DS-6864T0020140108BCRR428258400WU	●

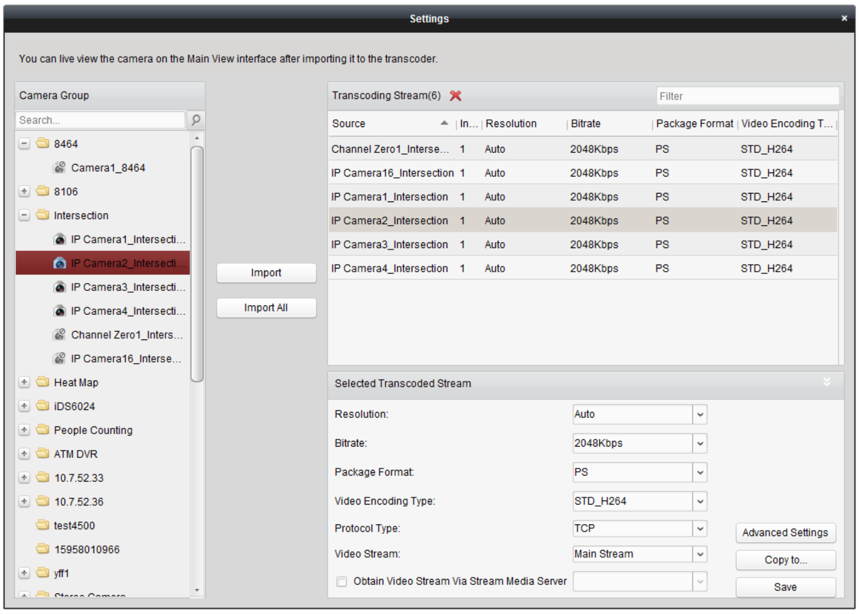
10.1.2 Importing the Encoding Channel to the Transcoder

Before you start:

The cameras of encoding devices should be organized into groups before being imported to the transcoder. For detailed configuration, please refer to *Chapter 3.2 Group Management*.

Steps:

1. On the Device Management interface, select a transcoder from the device list and click **Settings** to enter the transcoder settings interface.
2. Select a group or a camera from the Group list and click the **Import** button to import the selected camera or the cameras of the group, or click **Import All** to import the cameras of all groups to the transcoder on the right.
3. Optionally, you can click to select the stream and click ✖ to remove it from the transcoding list.



You can live view the camera on the Main View interface after importing it to the transcoder.

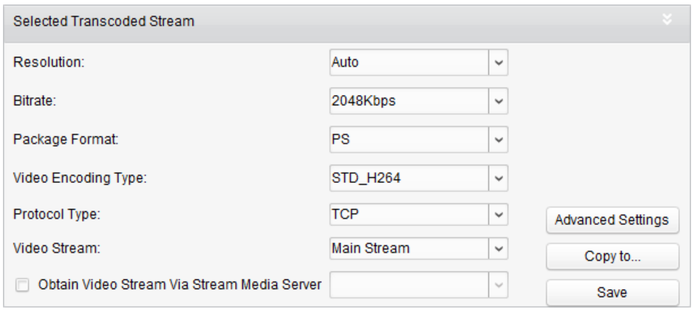
Source	In...	Resolution	Bitrate	Package Format	Video Encoding T...
Channel Zero1_Interse...	1	Auto	2048Kbps	PS	STD_H264
IP Camera16_Intersection	1	Auto	2048Kbps	PS	STD_H264
IP Camera1_Intersection	1	Auto	2048Kbps	PS	STD_H264
IP Camera2_Intersection	1	Auto	2048Kbps	PS	STD_H264
IP Camera3_Intersection	1	Auto	2048Kbps	PS	STD_H264
IP Camera4_Intersection	1	Auto	2048Kbps	PS	STD_H264

Resolution: Auto
Bitrate: 2048Kbps
Package Format: PS
Video Encoding Type: STD_H264
Protocol Type: TCP
Video Stream: Main Stream
□ Obtain Video Stream Via Stream Media Server

10.2 Configuring the Transcoded Stream Parameters

Steps:

1. On the Transcoder Settings interface, select a stream from the list and you can configure its parameters in the Selected Transcoded Stream area.



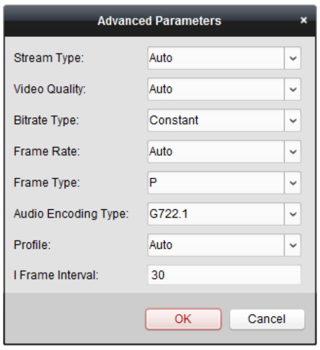
Resolution: Auto
Bitrate: 2048Kbps
Package Format: PS
Video Encoding Type: STD_H264
Protocol Type: TCP
Video Stream: Main Stream
□ Obtain Video Stream Via Stream Media Server

2. Configure the parameters of the transcoded stream as needed, including the resolution, bitrate, package format, video encoding type, protocol type and video stream from the drop-down list.
3. (Optional) Check the checkbox of **Obtain Video Stream Via Stream Media Server** if you want to use the stream media server to forward the video stream.

   Note: You should add a stream media server to the client before you can select the stream media server.
4. Click **Advanced Settings** to enter the advanced settings of the selected transcoded stream.

   (1) Edit the parameters of the transcoded stream on demands, including the stream type, video quality, bitrate type, frame rate, frame type, audio encoding type, profile and I frame interval.

   You can also remain the default parameters of the stream.

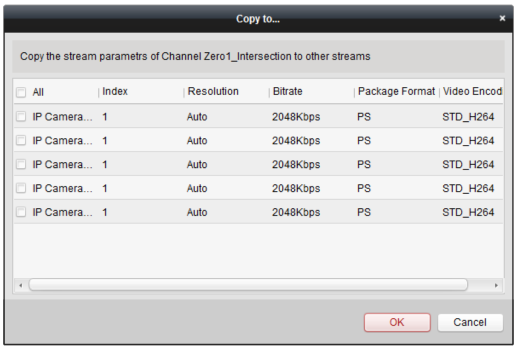


Advanced Parameters

Stream Type:	Auto
Video Quality:	Auto
Bitrate Type:	Constant
Frame Rate:	Auto
Frame Type:	P
Audio Encoding Type:	G722.1
Profile:	Auto
I Frame Interval:	30

(2) Click **OK** to save the settings.

5. (Optional) Click the **Copy to** on the Selected Transcoded Stream settings area to copy the settings of the current stream to other stream(s).



Copy to...

Copy the stream parametrs of Channel Zero1_Intersection to other streams

□ All	Index	Resolution	Bitrate	Package Format	Video Encod
□ IP Camera...	1	Auto	2048Kbps	PS	STD_H264
□ IP Camera...	1	Auto	2048Kbps	PS	STD_H264
□ IP Camera...	1	Auto	2048Kbps	PS	STD_H264
□ IP Camera...	1	Auto	2048Kbps	PS	STD_H264
□ IP Camera...	1	Auto	2048Kbps	PS	STD_H264

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

10.3 Operating the Transcoded Stream

Purpose:

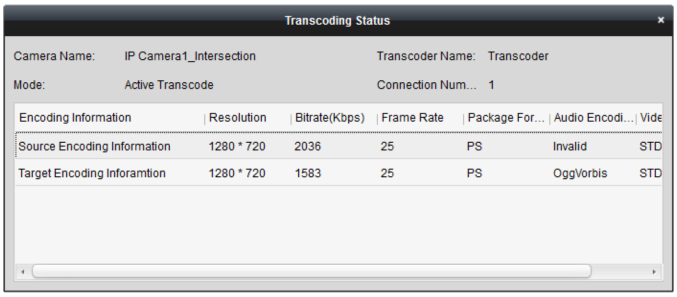
After successfully transcoding, the live view of the camera uses transcoded stream.

Steps:

1. Enter the Main View interface and select a transcoded camera for live view. For detailed configuration, please refer to *Chapter 4 Live View*.

   Note: If the camera is in live view before transcoding, please stop the live view first and then start the live view again to view the live video of the camera via transcoded stream.

2. During the live view, you can right-click on the camera node and select **Transcoding Status** to view the transcoding status.



Transcoding Status

Camera Name: IP Camera1_Intersection   Transcoder Name: Transcoder

Mode: Active Transcode   Connection Num... 1

Encoding Information	Resolution	Bitrate(Kbps)	Frame Rate	Package For...	Audio Encodi...	Vide
Source Encoding Information	1280 * 720	2036	25	PS	Invalid	STD
Target Encoding Inforamtion	1280 * 720	1583	25	PS	OggVorbis	STD

3. For e-map settings, please refer to *Chapter 7 E-map Management*; for displaying on video wall, please refer to *Chapter 12 Decoding and Displaying Video on Video Wall*.

   Note: Displaying the transcoded stream on video wall should be supported by the decoder.

Chapter 11 Forwarding Video Stream through Stream Media Server

Purpose:

There is always a limit of the device remote access number. When there are many users wanting to get remote access to the device to get the live view, you can add the stream media server and get the video data stream from the stream media server, thus to lower the load of the device.

11.1 Adding the Stream Media Server

Before you start:

The stream media 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 **Stream Media Server** to enable the installation of stream media server.

Steps:

1. Click the shortcut icon on the desktop to run the stream media server.

   Notes:

   - You can also forward the video through the stream media server installed on other PC.
   - If the stream media server port (value: 554) 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 stream media server.

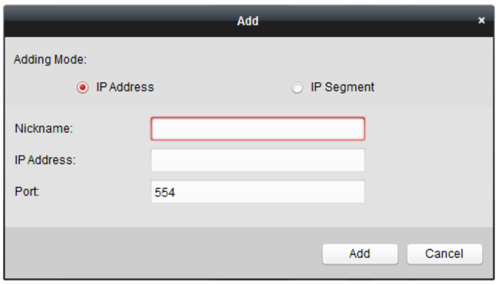
2. Open the Device Management page and click the **Server** tab.
3. Click **Add New Device Type**, select **Stream Media Server** and click **OK**.
4. Click **Stream Media Server** on the list and then click **Add Device**.

   You can add the stream media server in the following two ways:

   - **Adding Stream Media Server by IP Address**

     Perform the following steps to add the stream media server:

     1) Select **IP Address** as the adding mode.
     2) Input the nickname and IP address of the stream media server. The default port value is *554*.
     3) Click **Add** to add the stream media server to the client software.



Adding Mode:

● IP Address ○ IP Segment

Nickname:

IP Address:

Port: 554

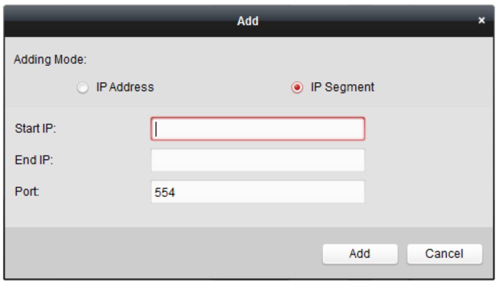
   - **Adding Stream Media Server by IP Segment**

     Perform the following steps to add the stream media server by IP segment:

     1) Select **IP Segment** as the adding mode.

2) Input the start IP and end IP. The default port value is *554*.

3) Click **Add** to add the stream media server to the client software. The steam media server of which the IP address is between the start IP and end IP will be added to the client.



Add

Adding Mode:

○ IP Address ● IP Segment

Start IP:

End IP:

Port: 554

Add Cancel

Note: For one client, up to 16 stream media servers can be added.

11.2 Adding Cameras to Stream Media Server to Forward Video Stream

Purpose:

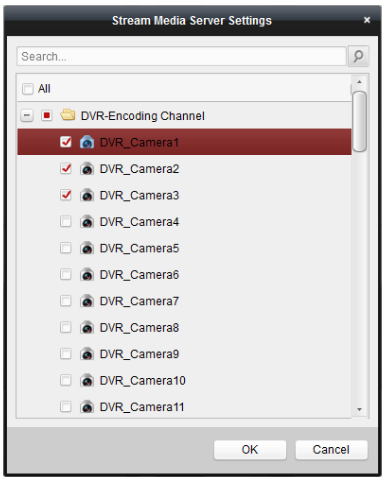
To get the video stream of a camera via stream media server, you need to connect the camera to the stream media server.

Steps:

1. Select the stream media server from the list.
2. Click **Configure** to enter the Stream Media Server Settings interface.
3. Select the cameras of which the video stream is to be forwarded via the stream media server.
4. Click **OK** to save the new settings.
5. Go the Main View page and start the live view of the cameras again. You can check the channel number of the video stream forwarded through or sent from the stream media server.

Notes:

- For one stream media server, up to 64 channels of video stream can be forwarded through it and up to 200 channels of video stream can be sent to clients from it.
- If the camera is offline, the client can still get the live video via the stream media server.



Stream Media Server Settings

Search...

□ All

DVR-Encoding Channel

☑ DVR_Camera1

☑ DVR_Camera2

☑ DVR_Camera3

□ DVR_Camera4

□ DVR_Camera5

□ DVR_Camera6

□ DVR_Camera7

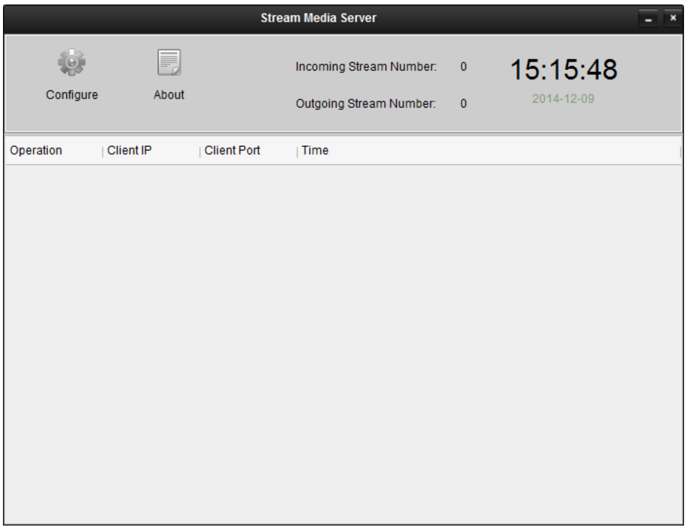
□ DVR_Camera8

□ DVR_Camera9

□ DVR_Camera10

□ DVR_Camera11

OK Cancel



Stream Media Server

Configure About

Incoming Stream Number: 0

Outgoing Stream Number: 0

15:15:48

2014-12-09

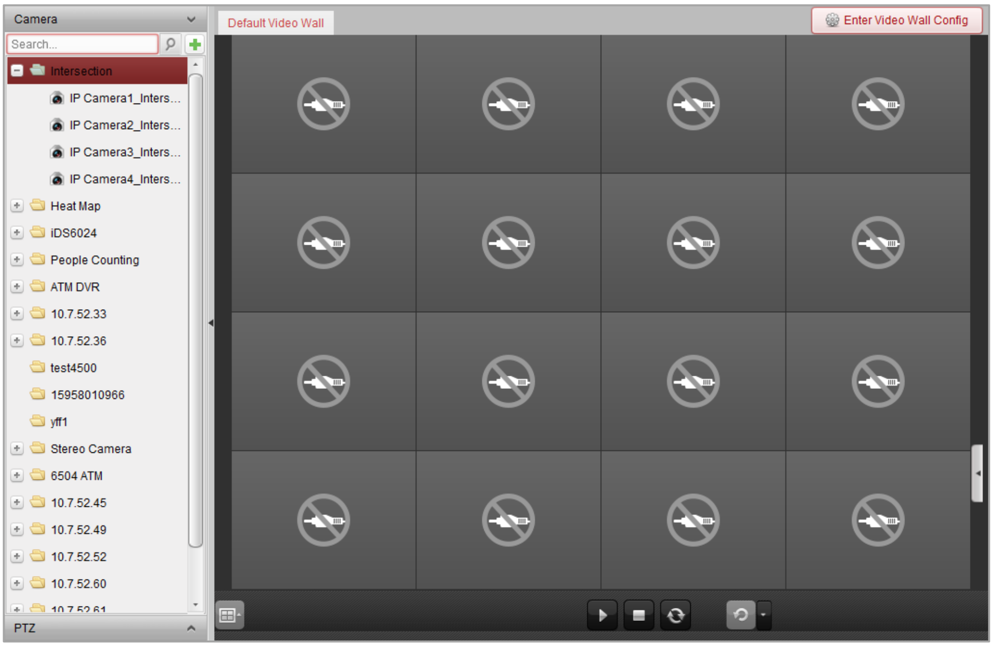
Operation	Client IP	Client Port	Time

Chapter 12 Decoding and Displaying Video on Video Wall

Purpose:

The Video Wall module provides the video decoding functionality, and the decoded video can be displayed on the Video Wall for an attention-grabbing performance.

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



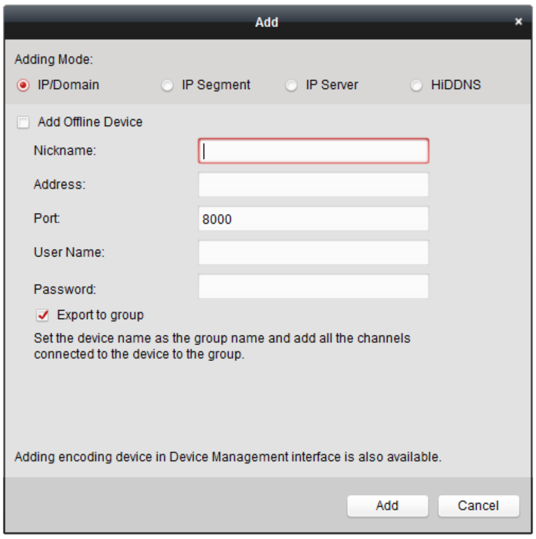
12.1 Adding the Encoding Device

Purpose:

You should add the encoding device for decoding and displaying on the video wall. If you do not add the encoding devices in the Device Management page, you can add them in Video Wall page.

Steps:

1. In the Camera area, click to activate the adding device window.



Adding Mode: ● IP/Domain ○ IP Segment ○ IP Server ○ HiDDNS

□ Add Offline Device

Nickname:

Address:

Port: 8000

User Name:

Password:

☑ Export to group

Set the device name as the group name and add all the channels connected to the device to the group.

Adding encoding device in Device Management interface is also available.

2. Select the adding mode and configure the corresponding settings for the device.

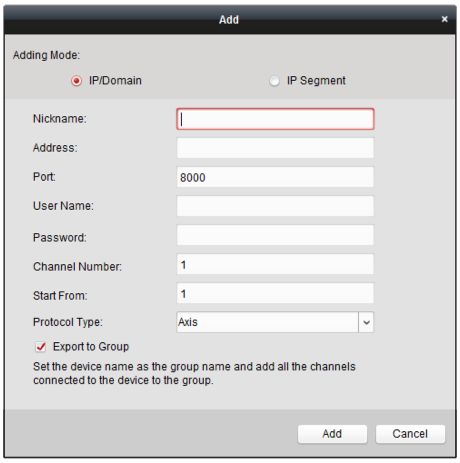
   For the detailed configuration about the 4 adding modes, please refer to the following sections:

   - By specifying the device IP address, see *Section 3.1.3 Adding Devices Manually.*
   - By specifying an IP segment, see *Section 3.1.4 Adding Devices by IP Segment*.
   - By IP Server, see *Section 3.1.5 Adding Devices by IP Server.*
   - By HiDDNS, see *Section 3.1.6 Adding Devices by HiDDNS.*

(Optional) If you want to add the third-party encoding device, please perform the following steps:

1. Go to the Device Management page and click the **Server** tab.
2. Click **Add New Device Type**, select **Third-party Encoding Device** and click **OK**.
3. Select Third-party Encoding Device in the organization panel and click **Add Device** to activate the Add Device window.
   - For IP/Domain: Edit the nickname, IP address/domain name, port No., user name, password, channel number, start from and protocol for the device.
   - For IP Segment: Edit the start IP, end IP, port No., user name, password, channel number, start from and protocol for the device.

Note: If you edit 4 in **Start From** field, it means that the starting channel No. is 4.



Adding Mode: ● IP/Domain ○ IP Segment

Nickname:

Address:

Port: 8000

User Name:

Password:

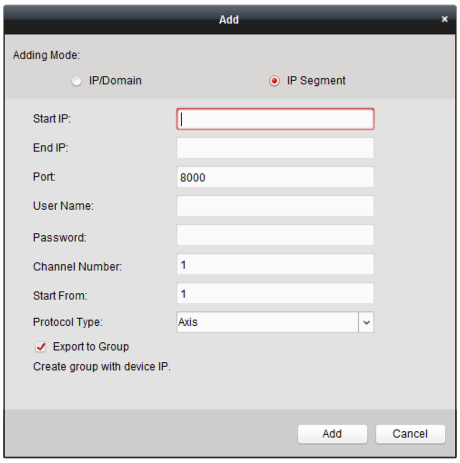
Channel Number: 1

Start From: 1

Protocol Type: Axis

☑ Export to Group

Set the device name as the group name and add all the channels connected to the device to the group.



Adding Mode: ○ IP/Domain ● IP Segment

Start IP:

End IP:

Port: 8000

User Name:

Password:

Channel Number: 1

Start From: 1

Protocol Type: Axis

☑ Export to Group

Create group with device IP.

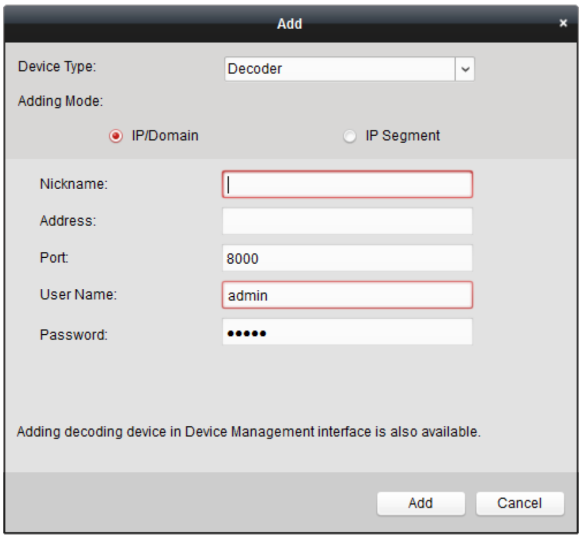
12.2 Adding the Decoding Device

Purpose:

To decode the video of the encoding device and display the decoded video on the Video Wall, the decoding device needs to be added to the client.

Steps:

1. Click **Enter Video Wall Config** to enter the decoding device and video wall configuration interface.
2. In the Decoding Output area, click ⊞ to activate the Quick Adding of Decoding Device window.



Device Type: Decoder

Adding Mode:

● IP/Domain ○ IP Segment

Nickname:

Address:

Port: 8000

User Name: admin

Password: •••••

Adding decoding device in Device Management interface is also available.

3. Set the device type as **Decoder** or **Cascading Server**.

   Note: To added cascading server here, please enter the Device Management page and click the **Server** tab. Click **Add New Device Type**, select **Cascading Server** and click OK.

   For **Decoder**, there are two adding modes available. Select the adding mode and configure the corresponding settings for the device.

   For the detailed configuration about the two adding modes, please refer to the following sections:

   - By specifying the device IP address or domain, see *Section 3.1.3 Adding Devices Manually.*
   - By specifying an IP segment, see *Section 3.1.4 Adding Devices by IP Segment*.

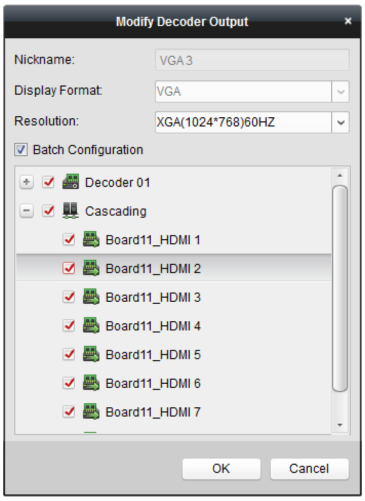
   For **Cascading Server**, you can add the device via IP address. For detailed configuration, see *Section 3.1.3 Adding Devices Manually.*

Edit the Output of the Decoding Device

Steps:

1. In the Decoding Output area, click ⊞ before the decoding device to list the outputs of it.
2. Double-click an output and you can edit the parameters for it. Or you can right-click a decoding output in the video wall area and select **Decoding Output Configuration** to edit its parameters.

   Note: For HDMI and VGA outputs, the resolution can be configured; for BNC output, the video standard can be configured.
3. (Optional) you can check the checkbox of **Batch Configuration** and select other outputs to copy the settings to.
4. Click **OK** to save the settings.



Modify Decoder Output

Nickname: VGA 3

Display Format: VGA

Resolution: XGA(1024*768)60HZ

☑ Batch Configuration

- ☑ Decoder 01
- ☑ Cascading
  - ☑ Board11_HDMI 1
  - ☑ Board11_HDMI 2
  - ☑ Board11_HDMI 3
  - ☑ Board11_HDMI 4
  - ☑ Board11_HDMI 5
  - ☑ Board11_HDMI 6
  - ☑ Board11_HDMI 7

Notes:

With the extension HDMI output board, NVR also supports decoding function:

- It can link with the video inputs and display them on the video wall without through decoding device.
- It can realize the video wall display, windowing and roaming of images of the cameras directly via the HDMI outputs.
- You can also edit the parameters of the decoding output.
- For details, please refer to the *User Manual* of the NVR.

12.3 Configuring Video Wall Settings

Purpose:

After the encoding device and decoding device have been added, the parameters of Video Wall need to be configured for video display.

12.3.1 Linking Decoding Output with Video Wall

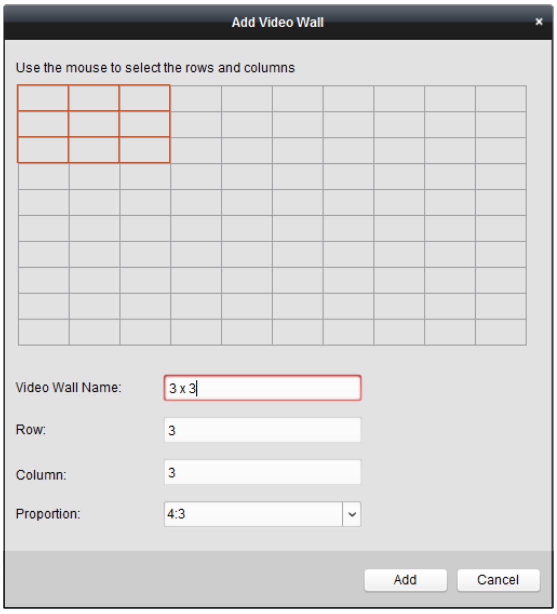
Steps:

1. Click **Enter Video Wall Config** to enter the decoding device and video wall configuration interface.
2. A default video wall view with the window division of 4*4 is provided. You can edit the default video wall or add a new video wall as desired.

   Task 1: Add a Video Wall

   1) Right-click the video wall and select **Add Video Wall**, or click + to activate the Add Video Wall window.

   2) Enter the name, row number, column number and proportion of the video wall.



Use the mouse to select the rows and columns

Video Wall Name: 3 x 3

Row: 3

Column: 3

Proportion: 4:3

3) Click **Add**.

Task 2: Edit a Video Wall

1) Right-click the video wall and select **Modify Video Wall** to edit it.

2) In the pop-up window, you can edit the name, row number, column number and proportion of the video wall.

Note: You can also drag your mouse to set the needed video wall.

3) Click **Modify** to save the settings.

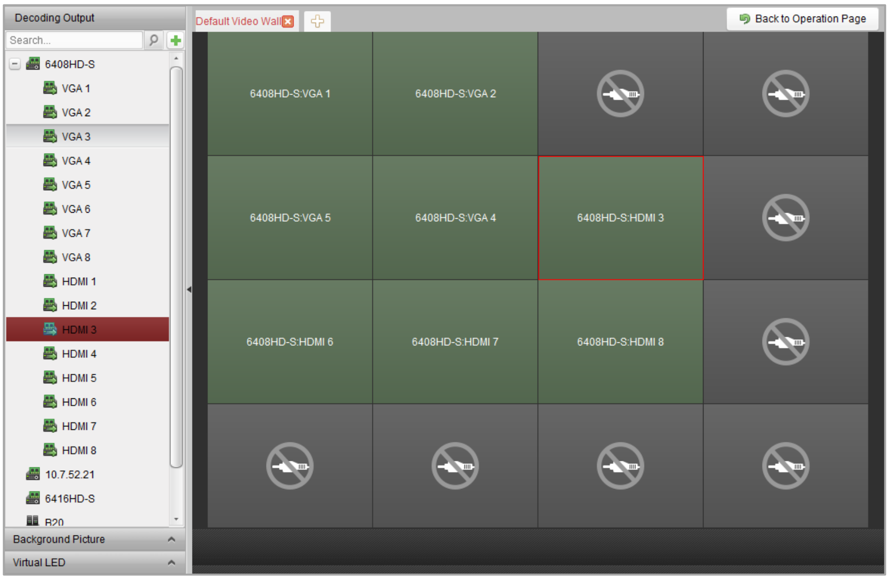
Task 3: Delete a Video Wall

To delete the video wall, right-click the video wall and select **Delete Video Wall**, or click ☒ of the video wall.

3. Click-and-drag the decoding output on the left-side list to the display window of video wall, to configure the one-to-one correspondence. You can also click and hold the *Ctrl* or *Shift* key to select multiple outputs and then drag them to the video wall for configuring linkage in batch. You can click ☒ in the upper-right corner of the display window to release the linkage.

Notes:

- Up to 4 video walls can be added to the client software.
- The total number of the display windows of the video wall should be no more than 100.
- The ranges of the row number and column number are both between 1 and 10.



12.3.2 Multi-Screen Display

Purpose:

For DS-6400HDI-T series decoder, you can joint multiple screens as a whole window. In this way, the decoded video of one camera can be shown on the jointed window.

Before you start:

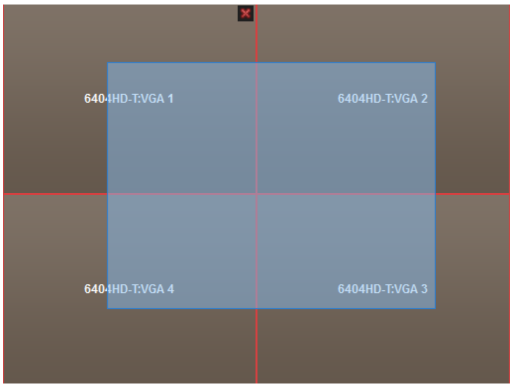
You should add DS-6400HDI-T series decoding device to the client. Please refer to *Chapter 12.2 Adding the Decoding Device* for detailed configuration about adding decoding device.

Steps:

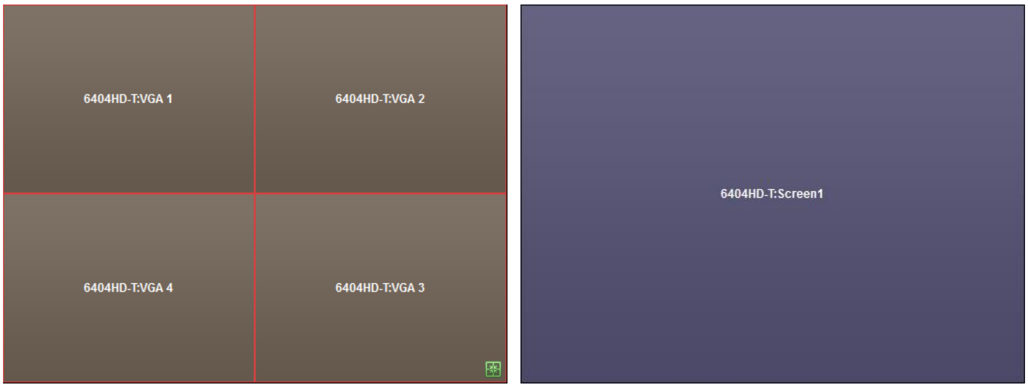
1. Perform the step 3 of *Chapter 10.3.1 Linking Decoding Output with Video Wall* to configure the linkage between the decoder and video wall.
2. Click-and-drag you mouse to select the adjacent display windows for jointing.

   Notes:

   - You can only joint the same output interfaces as a whole window. E.g., you can only joint 4 VGA interfaces or HDMI interfaces.
   - BNC interface does not support jointing.

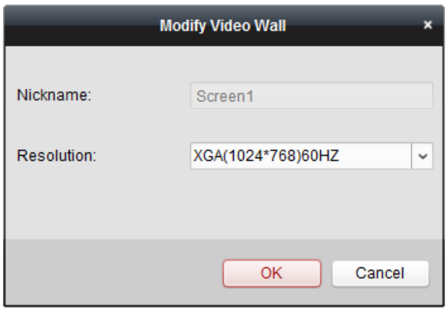


3. Click to confirm jointing the screens.



4. (Optional) You can set the resolution for the jointed window by right-clicking on it and select **Decoding Output Configuration**.

   To cancel the multi-screen display, click ✖ in the upper-right corner of the display window.


Modify Video Wall

Nickname: Screen1

Resolution: XGA(1024*768)60HZ

12.3.3 Configuring Background

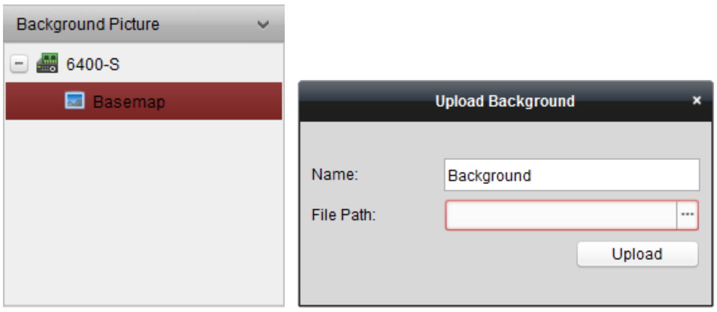
Purpose:

You can upload pictures for showing as the background of the video window.

Note: The function should be supported by the decoding device.

Steps:

1. Click ⌃ to expand the Background Picture panel.
2. Select a background picture and double-click (or right-click and select **Background Configuration**) it to activate the background uploading window.



Upload Background

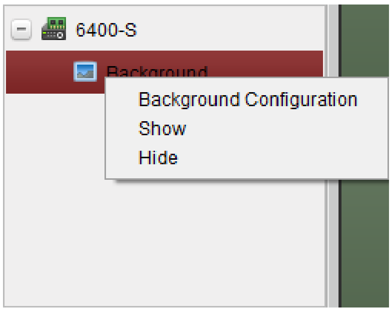
Name: Background

File Path:

3. Set a user-defined name for the background picture and click … to select a picture file.
4. Click **Upload** to upload the picture.
5. Click and drag the configured background picture to the desired position of the video wall.
6. You can move the window when the cursor becomes ✋ and adjust its size when the cursor becomes directional arrow. Right-click on the background picture and select **Show** or **Hide** to

show or hide the background picture.

Note: The picture will be displayed on the physical video wall after you upload the background.



12.3.4 Configuring Virtual LED

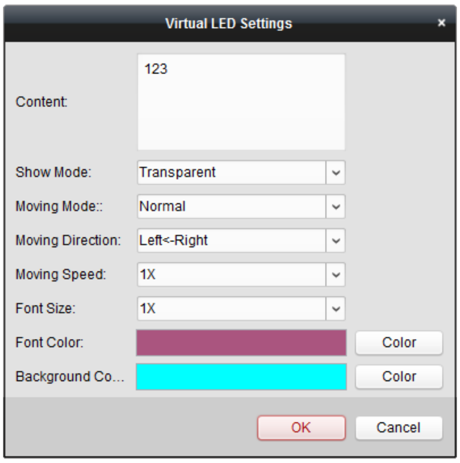
Purpose:

You can display the required contents on the video wall by using virtual LED.

Note: The function should be supported by the decoding device.

Steps:

1. Click **Enter Video Wall Config** to enter the configuration interface.
2. Click ⌃ to display the Virtual LED panel, click ⊞ to expand the added video wall controller.
3. Click-and-drag the virtual LED to the video wall.
4. You can move the window when the cursor becomes ✋ and adjust its size when the cursor becomes directional arrow.
5. Right-click the virtual LED in the panel and select Virtual LED Settings to set the parameters for it.
   - **Content**: Set the content that you want to display on the video wall.
   - **Show Mode**: Select the mode of the virtual LED as desired.
   - **Moving Mode**: Set the scrolling effect for the displayed text.
   - **Moving Direction**: Set the scrolling direction for the displayed text.
   - **Moving Speed**: Set the moving speed for the displayed text.
   - **Font Size**: Set the size of the displayed text.
   - **Font Color**: Set the color of the displayed text by clicking Color.
   - **Background Color**: Set the color of the background by clicking Color


Virtual LED Settings

Content: 123

Show Mode: Transparent

Moving Mode:: Normal

Moving Direction: Left<-Right

Moving Speed: 1X

Font Size: 1X

Font Color: 🟪 Color

Background Co... 🟦 Color

12.4 Displaying Video on Video Wall

Purpose:

After the settings of the encoding device, decoding device and video wall, the video stream from the encoding devices can be decoded and displayed on the Video Wall.

Notes:

- After enable decoding and displaying, the captured picture of the video from the encoding device displays on the Video Wall interface. And the real-time live view is shown on the physical video wall.
- For some kinds of decoder, the video stream from the signal source (which refers to the video signal (e.g., PC) connected to the decoder via the local interfaces) can also be displayed on the video wall. For detailed configuration, please refer to the *User Manual* of the device.

12.4.1 Decoding and Displaying

Steps:

1. Click **Back to Operation Page** to go back to the Video Wall Operation interface.
2. Click to save the linkage settings for the current scene. Or click (beside) and select a scene to save the settings for.

   Notes:

   - Scene settings are only supported by the cascading server. For setting the decoder, please skip step 2 and 3.
   - 8 scenes can be set for a video wall. Each scene can be configured with different linkage settings and window divisions.
   - For editing the name of a scene, select a scene and click to define a new name for it. You can also click to clear all the settings for the scene.
3. Select a scene which is configured with linkage settings and click to enable the scene.
4. Click-and-drag the camera on the left-side list to the display window of video wall. The video stream from the camera will be decoded and displayed on the Video Wall. You can also select a decoding window and then double-click a camera to decode and display the video. You can also click and hold the *Ctrl* or *Shift* key to select multiple cameras and then drag them to the video wall.

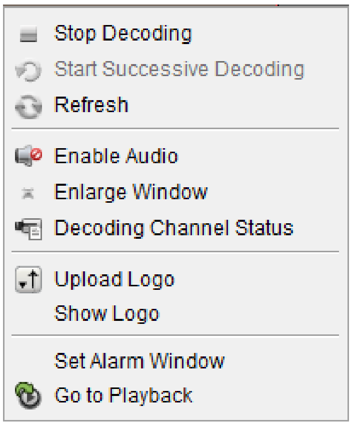
   Note: For DS-6400HDI-T decoder, you can select the signal source on the Signal Source panel for video wall display.
5. Select a playing window and click the icon to get a preview of the video in the lower-right corner of the screen. Or you can directly drag a camera to the preview window for live view. You can also double-click the preview window to get a full-screen view.

   Note: You can move the mouse to the window and click in the lower-right corner to stop decoding.
6. (Optional) Select a decoding window and click to set the window division for it. Click to save the settings for the current scene. Or click (beside) and select a scene to save the settings for.
7. If the decoded camera supports PTZ control, you can click beside **PTZ** to activate the PTZ

control panel. For detailed configuration, please refer to *Chapter 4.3 PTZ Control in Live View.*

8. Right-click on a playing window to activate the decoding management menu, as shown below:

   Note: The menu differs depending on the devices.



Stop/Start Decoding: Stop/Start the decoding.

Start/Pause Successive Decoding: Start/Pause the cycle decoding. This function is only supported by decoder.

Refresh: Refresh the decoding.

Open/Close Digital Zoom: Enable/Disable digital zoom.

Enable Audio: Turn on/off the audio of the decoding video.

Enlarge Window: Display the window in full-screen mode.

Decoding Channel Status: View the status of the decoding channel, such as decoding status, stream type.

Upload Logo: Upload a picture as the logo to the video window and set the display parameters for it. After setting, the logo shows in the defined position of the window on physical video wall.

Show/Hide Logo: Show/Hide the logo.

Stick on Top: Always stick the window on the top layer. This function is only supported by cascading server.

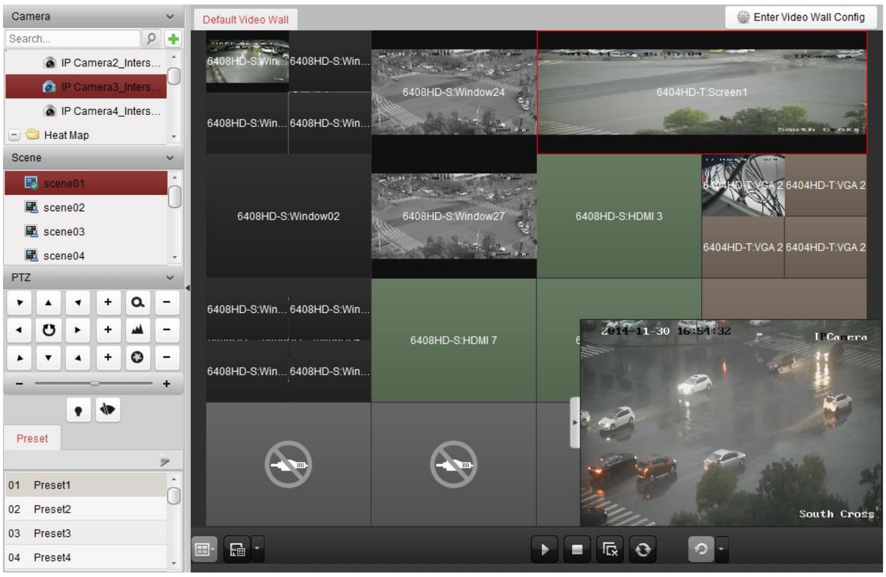
Stick at Bottom: Always stick the window at the bottom layer. This function is only supported by cascading server.

Lock: Lock the window to disable the roaming function.

Set Alarm Window: Display the video triggered by event or alarm input on Video Wall.

Decoding Delay: Set the delay degree of the decoding according to the actual needs. This function is only supported by cascading server.

Go to Playback: Enter the playback mode. This function is only supported by decoder.



Icon	Description
▶	Start all the decoding
■	Stop all the decoding
⧉	Stop all the roaming windows
⟳	Refresh all the decoding windows
⟲ ▾	Set cycle decoding and switching interval

12.4.2 Windowing and Roaming Settings

Purpose:

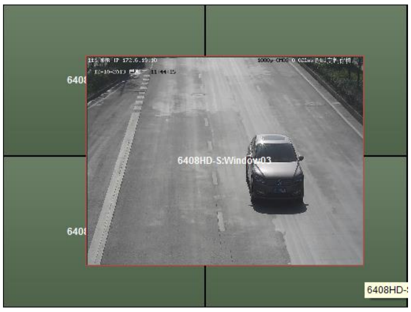
Windowing is to open a new window on the screen(s). The window can be within a screen or span multiple screens. You can move the playing window within the video wall as desired and this function is called roaming.

Note: The windowing and roaming function should be supported by the decoding device.

Steps:

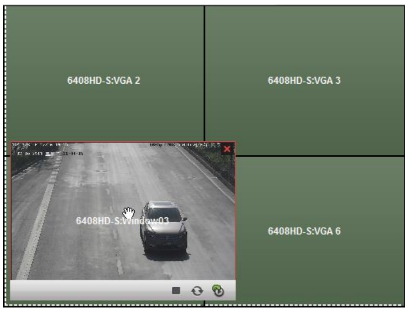
1. Click-and-drag on a screen which links to a decoding output to open a window. The window can be within a screen or span multiple screens. If you want to open a window on the opened window, click-and-drag and hold the *Ctrl* key to create one. And for the locked window (refer to step 6), you can click-and-drag to create a new window on it.

   Note: At least one camera should be selected before opening window.

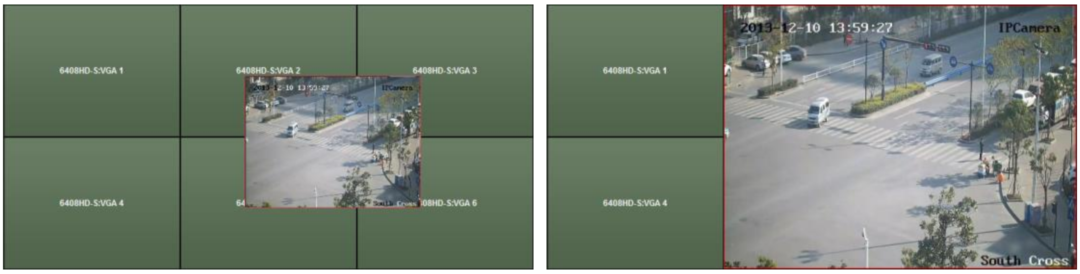


2. You can move the window when the cursor becomes ✋ and adjust its size when the cursor becomes directional arrow. You can also hold the *Shift* key to scale the window in proportion.

3. During moving the window, the dotted borders will display. The window will be adjusted to align with the borders if it is moved to the location near the dotted borders.



4. Double-click the window and it will enlarge to fill the spanning screens and display on the top layer. You can double-click again to restore.



5. (Optional) Select a window and click ⊞ to set the window division for it. Click ▦ to save the settings for it.
6. Right-click on a window and select **Lock** in the right-click menu to disable the roaming function, and the 🔒 icon shows on the top-right corner of the window. In this way, the window cannot be moved and resized. You can right-click on the window and select **Unlock** in the right-click menu to recover the roaming function.
7. Right-click on a window and select **Stop Decoding** in the right-click menu, or move the mouse to the window and click ☒ in the upper-right corner to stop the decoding of the window and it will be closed. You can also click ☒ to close all the roaming windows.
8. The window only shows a captured picture of the decoded video. You can right-click on a window and select **Refresh** in the right-click menu, or move the mouse to the window and click ⟳ in the lower-right corner to capture a latest picture of the decoded video and display on the window.
9. If you want to view the specific area of the video in details, you can right-click on a window and select **Open Digital Zoom** (if available) in the right-click menu and the cursor becomes 🔍. Use the mouse to drag on the video to realize digital zoom. You can check the effect on the physical video wall
10. Select a playing window and click the icon ◂ to get a preview of the video in the lower-right corner of the screen. Or you can directly drag a camera to the preview window for live view. You can also double-click the preview window to get a full-screen view.
11. Right-click on a playing window and you can control decoding management via the right-click menu.

12.4.3 Configuring Playback

Purpose:

The video file is supported to be played back on the video wall.

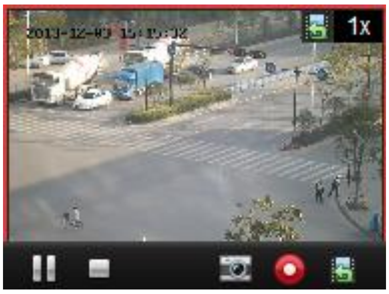
Note: Playback function is only supported by decoder.

Steps:

1. Click-and-drag the camera on the left-side list to the display window of video wall, or you can open a window if supported.
2. Move the mouse to the window and click in the upper-right corner. Or you can right-click on the window and select **Go to Playback** in the right-click menu.
3. If there is video file of current day, the video file will be played back automatically. If not, you can set the search condition on the search panel which shows in the left area of the interface (click to show more search options, and then click the icon to specify the start time and end time for the search), and click **Search** to find the video file.
4. Right-click on the playback window and you can control the playback through the right-click menu, such as pause, stop, fast forward, slow forward, capture, start recording and full-screen playback.

   Note: The saving path for the captured pictures and recorded files can be configured on System Configuration page. Please refer to *Chapter 17.2.4 File Saving Path Settings* for detailed settings.

When you move the mouse to the screen, the icons will display as shown below.



Icon	**Description**
⏸	Pause the playback
■	Stop the playback
📷	Capture the playback video
●	Record the playback video
⇄	Back to live view mode
⇄ 1x	Playback speed.

12.4.4 Configuring Cycle Decoding

Purpose:

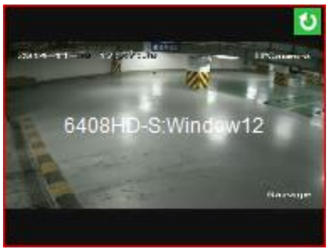
The cycle decoding refers that you can configure multiple video streams of encoding devices to one decoding output and you can set the switching interval for the decoding.

Note: The cycle decoding is only supported by decoder.

Steps:

1. Click ▪ beside ↻ and set the switching interval for the cycle decoding.
2. Click-and-drag the camera on the left-side list to the display window of video wall, or you can open a window if supported.

   Note: The cycle decoding is not supported by the signal source of DS-6400HDI-T.
3. Move the mouse to the group node and click ↻ to start cycle decoding (the decoding output under cycle decoding will be marked with ↻). Right-click on the window and you can control decoding management via the right-click menu.



12.5 Configuring Video Wall Controller

Purpose:

The client provides the function of managing the added video wall controller.

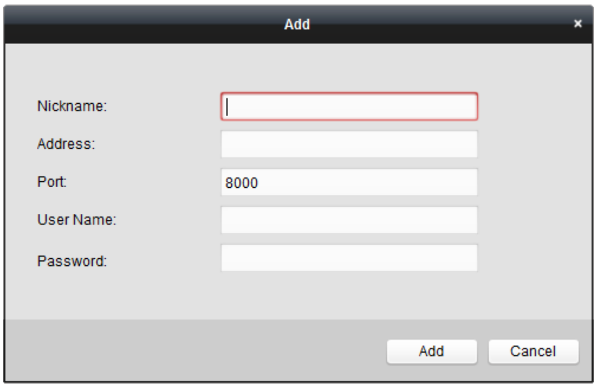
12.5.1 Adding the Video Wall Controller

Purpose:

You should add the video wall controller to the client for management.

Steps:

1. Go to the Device Management page and click the **Server** tab.
2. Click **Add New Device Type**, select **Video Wall Controller** and click **OK**.
3. Select Video Wall Controller in the organization panel and click **Add Device** to activate the Add Device window.
4. Edit the nickname, IP address/domain name, port No., user name and password for the device.
5. Click **Add** to save the settings.



Add

Nickname:	
Address:	
Port:	8000
User Name:	
Password:	

6. For edit the output, please refer to *Chapter 12.2 Adding the Decoding Device*.

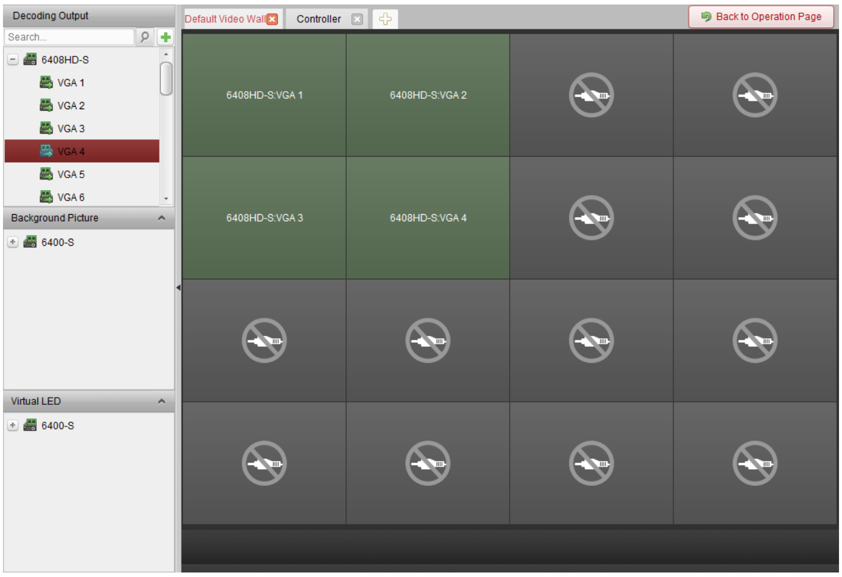
12.5.2 Linking Output with Video Wall

Steps:

1. Click **Enter Video Wall Config** to enter the configuration interface.
2. A default video wall with the added video wall controller name is provided. You can edit the default video wall as desired. For details, please refer to *Chapter 12.3.1 Linking Decoding Output with Video Wall*.
3. Click-and-drag the output of the added video wall controller on the left-side list to the display window of video wall, to configure the one-to-one correspondence. You can also click and hold the *Ctrl* or *Shift* key to select multiple outputs and then drag them to the video wall for configuring linkage in batch. You can click ☒ in the upper-right corner of the display window to release the linkage.
4. For background settings, please refer to the *Section 12.3.3 Configuring Background*.

Notes:

- The total number of the display windows of the video wall should be no more than 100.
- The ranges of the row number and column number are both between 1 and 10.



12.5.3 Configuring Virtual LED

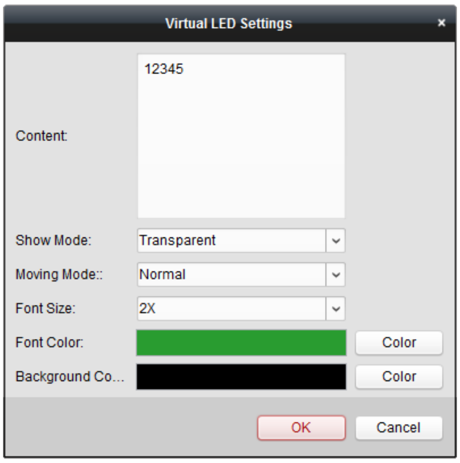
Purpose:

You can display the required contents on the video wall by using virtual LED.

Steps:

1. Click **Enter Video Wall Config** to enter the configuration interface.
2. Click ▲ to display the Virtual LED panel, click ⊞ to expand the added video wall controller.
3. Click-and-drag the virtual LED to the video wall.
4. You can move the window when the cursor becomes ✋ and adjust its size when the cursor becomes directional arrow.
5. Right-click the virtual LED in the panel and select Virtual LED Settings to set the parameters for it.

- **Content**: Set the content that you want to display on the video wall.
- **Show Mode**: Select the mode of the virtual LED as desired.
- **Moving Mode**: Set the scrolling effect for the displayed text.
- **Font Size**: Set the size of the displayed text.
- **Font Color**: Set the color of the displayed text by clicking **Color**.
- **Background Color**: Set the color of the background by clicking **Color**


Virtual LED Settings

Content: 12345

Show Mode: Transparent

Moving Mode:: Normal

Font Size: 2X

Font Color: 🟩

Background Co... ■

12.5.4 Configuring Video Wall Screens

Purpose:

The screens of the video wall can be configured, including screen type, opening screen, closing screen, input source and image parameters.

Steps:

1. Click **Back to Operation Page** to go back to the Video Wall Operation interface.
2. Click to activate the Screen Control window.
3. Click-and-drag on the video wall to select the screens and configure the parameters for them.

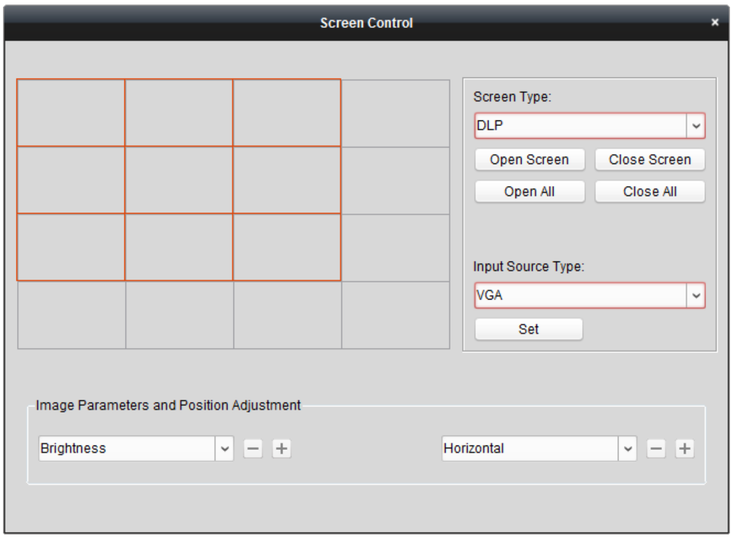
   Screen Type: Select the type for the selected screens for different screen type adopting different communication protocols.

   Open Screen/Close Screen: Open or close the selected screens.

   Open All/Close All: Open or close all the screens.

   Input Source Type: Select the input source for the screen and click **Set** to save the settings.

   Image Parameters and Position Adjustment: Select brightness or contrast and click + or − to adjust the image parameters. Select horizontal or vertical and click + or − to adjust the image position on the screen.



12.5.5 Displaying Video on Video Wall

Purpose:

After adding the video wall controller and linking the output with the video wall, the video stream from the encoding devices or the signal source can be displayed on the video wall.

Notes:

- Encoding devices refer to the devices connected to iVMS-4200 client via network.
- Decoding module should be connected to the video wall controller before the video of the encoding devices can be decoded and displayed.
- Signal source refers to the video signal (e.g., analog camera) connected to the video wall controller via the local interfaces of the controller.
- After enable decoding and displaying, the captured picture of the video from the encoding device displays on the Video Wall interface. And the real-time live view is shown on the physical video wall.
- For signal source, no captured pictures displaying on the output window. You can check the live video on the physical video wall.

Steps:

1. Click **Back to Operation Page** to go back to the Video Wall Operation interface.
2. Select a scene which is configured with linkage settings and click ▶ to enable the scene.
3. Click-and-drag the camera or signal source on the left-side list to the display window of video wall. The video stream from the camera or signal source will be displayed on the Video Wall. You can also select a decoding window and then double-click a camera to decode and display the video. You can also click and hold the *Ctrl* or *Shift* key to select multiple cameras and then drag them to the video wall.
4. Or you can select a camera or signal source, then click-and-drag on a screen which links to an output to open a window. The window can be within a screen or span multiple screens. If you want to open a window on the opened window, click-and-drag and hold the *Ctrl* key to create one. For details, please refer to *Chapter 12.4.2 Windowing and Roaming Settings*.
5. Select a playing window and click the icon ◂ to get a preview of the video in the lower-right corner of the screen. Or you can directly drag a camera to the preview window for live view. You

can also double-click the preview window to get a full-screen view.

6. Click to save the current settings as a scene. Or click (beside) and select a scene or create a new scene to save the settings for.

   Notes:

   - 32 scenes can be set for a video wall controller.
   - For editing the name of a scene, select a scene and click to define a new name for it. You can also click to clear all the settings for the scene. For calling a scene, select a scene and click to enable the scene.

7. Right-click on a playing window to activate the decoding management menu.

   Note: The menu differs depending on the devices. Please refer to *Chapter 12.4.1 Decoding and Displaying* for detailed introduction.

8. For displaying the video files of the encoding device on the video wall, please refer to *Chapter 12.4.3 Configuring Playback*.

12.5.6 Configuring Plan

Purpose:

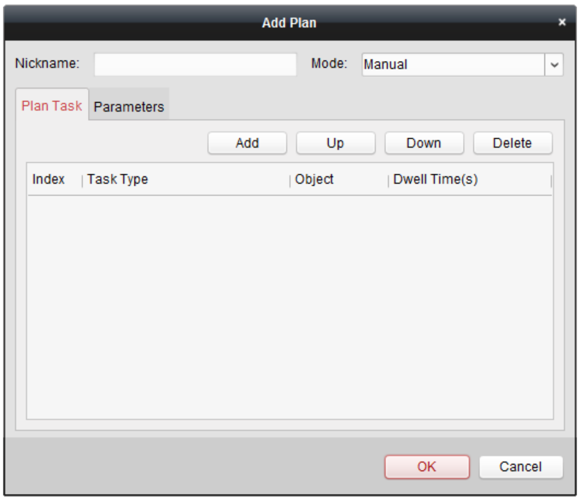
The plan function of video wall controller provides the switching the configured scene(s) and turning on or off the screens at a certain time. You can also set the time schedule for switching the operations (such as scene, close screens) and the plan can also be auto-switched.

Before you start: Scene(s) should be added for the video wall controller. Please refer to *Chapter 12.5.5 Displaying Video on Video Wall* for adding scenes.

Steps:

1. Click **Back to Operation Page** to go back to the Video Wall Operation interface.
2. Click to display the Plan panel, click **Add Plan** or right-click on the panel and select **Add Plan** to pop up the Add Plan window.

   Note: Up to 16 plans can be added to a video wall controller.



Mode: Manual

3. Set the parameters for the plan:

   Nickname: Edit a name for the plan as desired.

   Mode: Select the mode to execute the plan. Manual, Auto and Auto-switch are selectable.

   - Manual: Automatically execute the plan until you stop calling the plan manually.
   - Auto: Execute the plan according to the configured start time and execution times in

Parameters panel.

- Auto-switch: Execute the plan according to the configured time schedule and execution times in Parameters panel.

Plan Task: Set the operations for the plan. The plan will be execute the added operations in order.

- Add: Add an operation for the plan. If you select the **Task Type** as Display Scene, you can select the configured scene in the Scene drop-down list and set the dwell time. If you select the **Task Type** as Open Screen or Close Screen, you can select the screen type for opening or closing and set the dwell time.
- Up: Move the selected operation up.
- Down: Move the selected operation down.
- Delete: Remove the selected operation.

Parameters:

If you select Auto as the mode, you can set the Start Time and Execution Times. E.g., you set the Start Time as 2014-06-04 00:00:00 and Execution Times as 4, then the plan will be executed from 2014-06-04 00:00:00 and continuously for 4 times before stopping.

If you select Auto-switch as the mode, you can set the Weekday Settings and Execution Times. E.g., you set the Weekday Settings as 10:30:00 of Mon and 08:30:00 of Wed, and Execution Times as 6, the plan will be executed from 10:30:00 of Monday and continuously for 6 times, then from 08:30:00 of Wednesday and continuously for 6 times. The next week, the plan will be executed at the configured time.

4. Click **OK** to save the settings.
5. To call a plan, select a plan and click ▶ to enable the plan. For editing the plan, select a plan and click ✎ to edit the settings for it. You can also click ■ to clear all the settings for the plan. To stop the plan, right-click a plan and select **Stop Plan**.

   Note: Please stop the plan before you want to configure the video wall controller.

Chapter 13 Security Control Panel

Purpose:

The Security Control Panel module provides remote control and configuration via the iVMS-4200 client software.

- Before remote configure and control the security control panel, you are required to add the device to the software first. Refer to *Chapter 13.1 Device Management*.
- For setting the event linkage of the zone, refer to *Chapter 13.2 Zone Event Management*.
- For remote control of security control panel via the iVMS-4200 client software, refer to *Chapter 13.3 Remote Control.*
- For managing the zones on E-map, please refer to *Chapter 13.4 Displaying Zone on E-map.*

13.1 Device Management

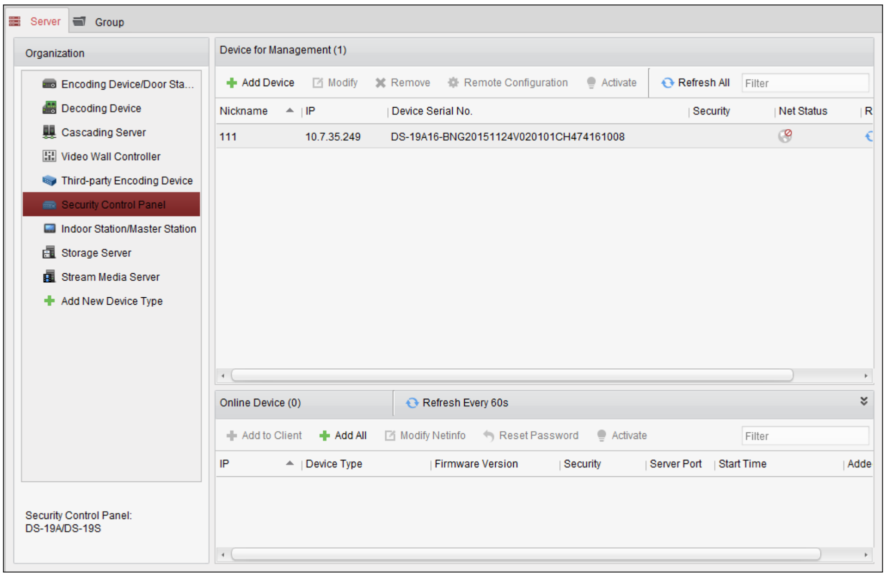
Purpose:

In this section, you can add the security control panel for further configuration.

13.1.1 Adding Security Control Panel

Steps:

1. Click the icon on the control panel to enter the Device Management interface and click the **Server** tab.



Nickname	IP	Device Serial No.	Security	Net Status	R
111	10.7.35.249	DS-19A16-BNG20151124V020101CH474161008			

IP	Device Type	Firmware Version	Security	Server Port	Start Time	Adde

Security Control Panel:
DS-19A/DS-19S

2. Click **Add New Device Type** on the Organization list and select **Security Control Panel**.
3. Click **OK** to save the settings, and the added security control panel type is displayed on the Organization list.
4. Click **Security Control Panel** and click **Add Device** to add the security control panel to the management list of the software.

5. You can add the active online devices in the same local subnet with the client software, or select the adding mode by IP/Domain, by IP segment, by IP Server, or by HiDDNS, and configure the corresponding settings for the device.

   Note: For activating the device, see *Chapter 3.1.1 Creating the Password*.

   For the detailed configuration about the adding modes, please refer to the following chapters:

   - By adding the online devices, see *Chapter 3.1.2 Adding Online Devices*.
   - By specifying the device IP/Domain address, see *Chapter 3.1.3 Adding Devices Manually.*
   - By specifying an IP segment, see *Chapter 3.1.4 Adding Devices by IP Segment*.
   - By IP Server, see *Section 3.1.5 Adding Devices by IP Server.*
   - By HiDDNS, see *Section 3.1.6 Adding Devices by HiDDNS.*

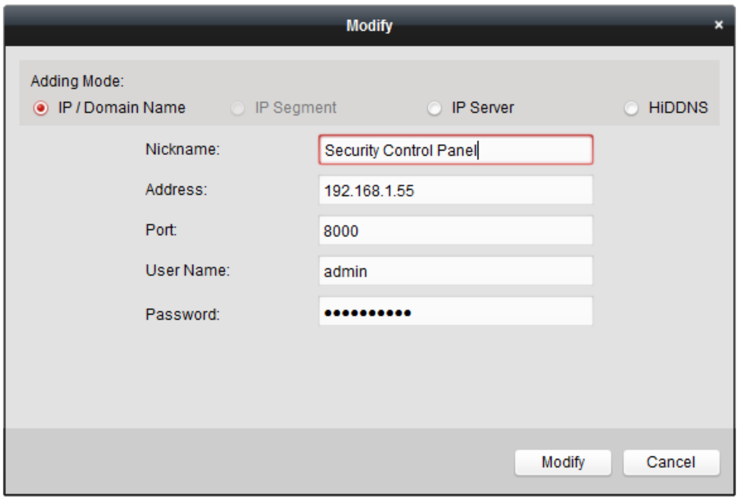
13.1.2 Editing Security Control Panel

Purpose:

You can edit the device information in this section, including the device name, address and port number.

Steps:

1. On the **Device Management** interface, click and select a security control panel in the device list.
2. Click the **Modify** button on the upper side of the list to enter the device modify interface.



Modify

Adding Mode:
● IP / Domain Name ○ IP Segment ○ IP Server ○ HiDDNS

Nickname: Security Control Panel
Address: 192.168.1.55
Port: 8000
User Name: admin
Password: ••••••••••

3. Edit the device information according to the adding mode.
4. Click **Modify** to save the changes.

13.1.3 Deleting Security Control Panel

Select device from the list, click **Remove**, and then you can delete the information of the selected device.

13.2 Zone Event Configuration

Purpose:

For security control panel, you can configure its zones linkage including siren, trigger, client linkage, and triggered cameras.

Steps:

1. Click the icon on the control panel,

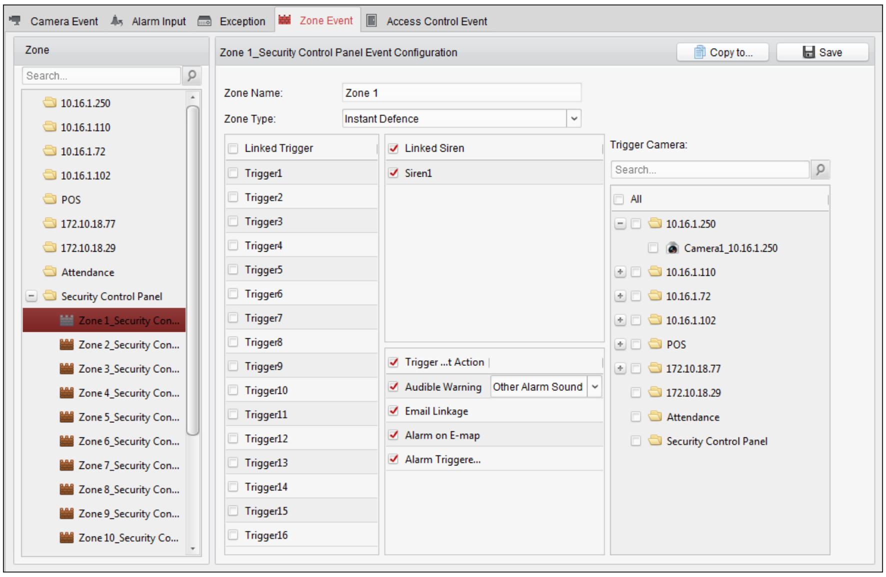
   or click **Tool**->**Event Management** to open the Event Management page.
2. Click the **Zone Event** tab.

   Note: The Zone Event tab is available when the device type of Security Control Panel is added.
3. Select the security control panel and zone to be configured.
4. You can edit the zone name and zone type.
5. Select the linked trigger on the **Linked Trigger** panel.
6. Select the linked siren on the **Linked Siren** panel.
7. Check the checkboxes to activate the linkage actions. For details, see *Table 13.1 Linkage Actions for Zone Event*.
8. Select the triggered camera to be triggered in the camera list for popping up image or displaying on the video wall when the alarm is triggered.

   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. For details, refer to *Chapter 5.1 Remote Storage.*

   Note: Up to four cameras can be set as triggered camera.
9. Optionally, click **Copy to...** to copy the event parameters to other zones.
10. Click **Save** to save the settings.

Note: The zone should be disarmed before configuring the zone event linkage.



Zone 1_Security Control Panel Event Configuration

Zone Name: Zone 1

Zone Type: Instant Defence

☑ Linked Siren

☑ Siren1

☑ Audible Warning Other Alarm Sound

☑ Email Linkage

☑ Alarm on E-map

☑ Alarm Triggere...

Table 13. 1 Linkage Actions for Zone 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. For setting the alarm sound, please refer to *Chapter 17.2.7 Alarm Sound Settings.*
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.

Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered.

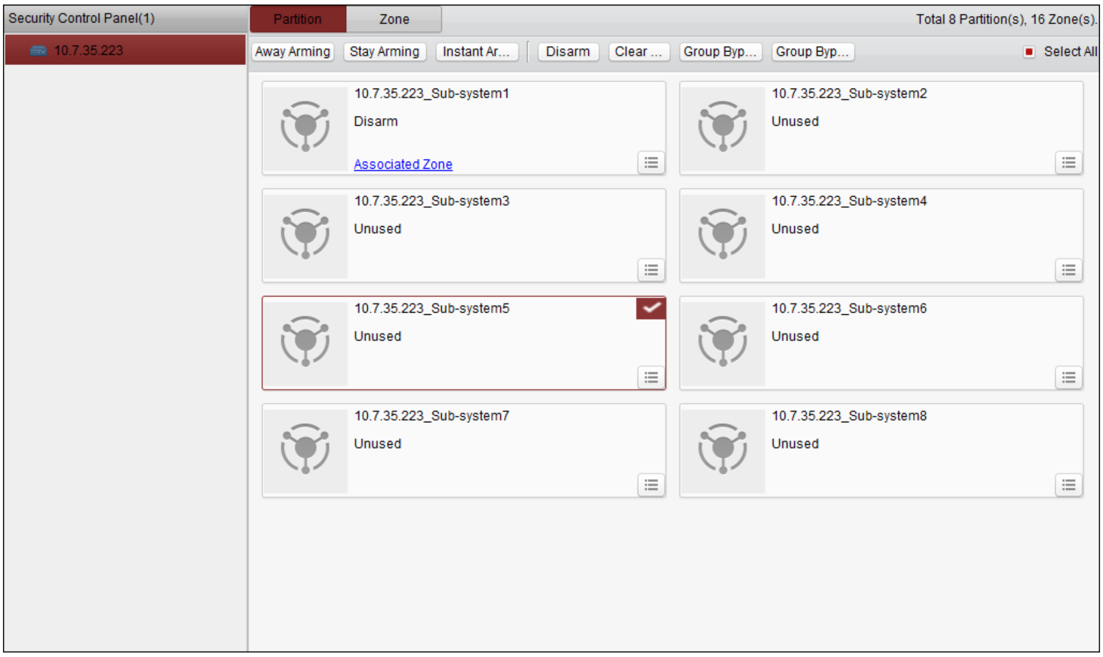
13.3 Remote Control

Purpose:

In this section, you can control the panel remotely to implement operations such as arming, disarming, bypass, group bypass, and so on for both the partitions and zones.

Click the icon on the control panel,

or click **View->Security Control Panel** to open the Security Control Panel page.



The added security control panels are listed in the Security Control Panel on the left. Select one for further operations.

13.3.1 Partition System Remote Control

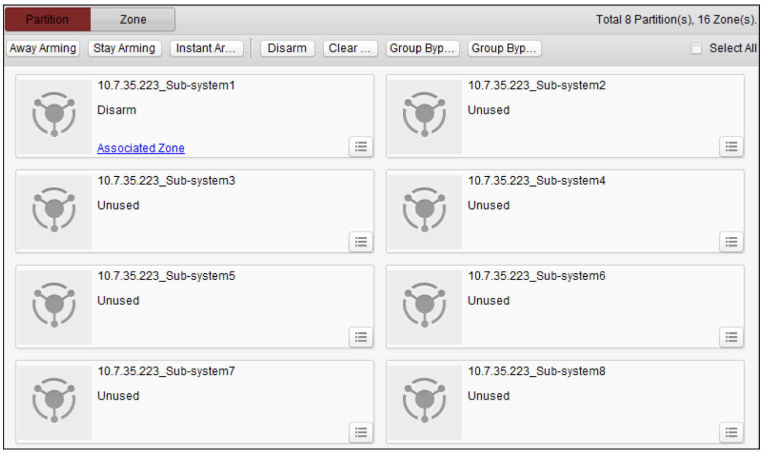
Purpose:

In this section, you can remotely implement operations of away arming, stay arming, instant arming, disarming, clearing alarm, group bypass, and recovering group bypass for the configured partitions.

Steps:

1. On the **Partition** page, click to select one or more partitions to be controlled, or check the check box of **Select All** on the upper-right side of the page to select all partitions.
2. Click the operations buttons (away arming, stay arming, instant arming, disarming, clearing alarm, group bypass, and group bypass recovery) on the upper side of the page.

   Note: You can also click the icon to get the operation menu for each partition.



Total 8 Partition(s), 16 Zone(s).

10.7.35.223_Sub-system1
Disarm
Associated Zone

10.7.35.223_Sub-system2
Unused

10.7.35.223_Sub-system3
Unused

10.7.35.223_Sub-system4
Unused

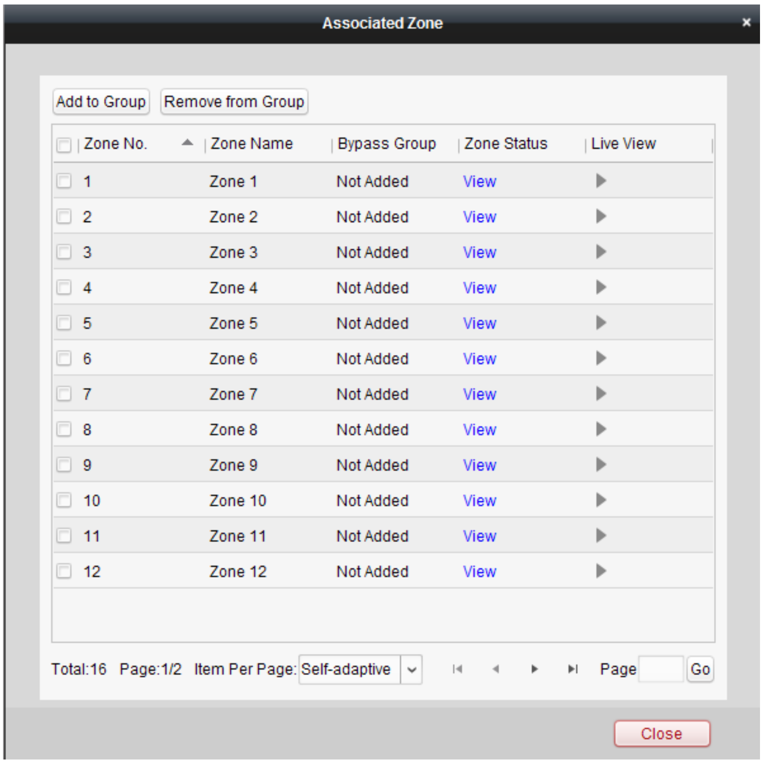
10.7.35.223_Sub-system5
Unused

10.7.35.223_Sub-system6
Unused

10.7.35.223_Sub-system7
Unused

10.7.35.223_Sub-system8
Unused

3. Click **Associated Zone** to view the zones of the current partition.



□ Zone No.	Zone Name	Bypass Group	Zone Status	Live View
□ 1	Zone 1	Not Added	View	▶
□ 2	Zone 2	Not Added	View	▶
□ 3	Zone 3	Not Added	View	▶
□ 4	Zone 4	Not Added	View	▶
□ 5	Zone 5	Not Added	View	▶
□ 6	Zone 6	Not Added	View	▶
□ 7	Zone 7	Not Added	View	▶
□ 8	Zone 8	Not Added	View	▶
□ 9	Zone 9	Not Added	View	▶
□ 10	Zone 10	Not Added	View	▶
□ 11	Zone 11	Not Added	View	▶
□ 12	Zone 12	Not Added	View	▶

Total:16 Page:1/2 Item Per Page: Self-adaptive Page Go

You can add/remove the selected zones into/from the group.

Click **View,** and you can view the status of the zone.

Click ▶ to view the live view of the zone's triggered camera.

Note: You can set the triggered camera of the zone in Event Management. Refer to *Chapter 13.2 Zone Event Configuration*.

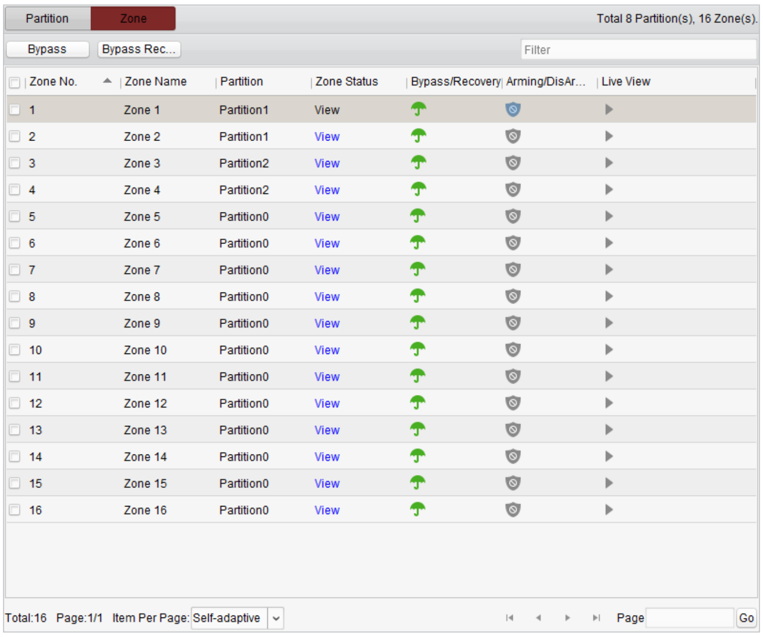
13.3.2 Zone Remote Control

Purpose:

In this section, you can remotely implement bypass, or recovering bypass for the zones.

Steps:

1. Click **Zone** tag to enter the interface.



Total 8 Partition(s), 16 Zone(s).

□	Zone No.	Zone Name	Partition	Zone Status	Bypass/Recovery	Arming/DisAr...	Live View
□	1	Zone 1	Partition1	View	☂	🛡	▶
□	2	Zone 2	Partition1	View	☂	🛡	▶
□	3	Zone 3	Partition2	View	☂	🛡	▶
□	4	Zone 4	Partition2	View	☂	🛡	▶
□	5	Zone 5	Partition0	View	☂	🛡	▶
□	6	Zone 6	Partition0	View	☂	🛡	▶
□	7	Zone 7	Partition0	View	☂	🛡	▶
□	8	Zone 8	Partition0	View	☂	🛡	▶
□	9	Zone 9	Partition0	View	☂	🛡	▶
□	10	Zone 10	Partition0	View	☂	🛡	▶
□	11	Zone 11	Partition0	View	☂	🛡	▶
□	12	Zone 12	Partition0	View	☂	🛡	▶
□	13	Zone 13	Partition0	View	☂	🛡	▶
□	14	Zone 14	Partition0	View	☂	🛡	▶
□	15	Zone 15	Partition0	View	☂	🛡	▶
□	16	Zone 16	Partition0	View	☂	🛡	▶

Total:16 Page:1/1 Item Per Page: Self-adaptive

2. Click and select one or more zones to be controlled.
3. Click **Bypass**/**Bypass Recovery** on the upper side of the page to control the selected zones.
4. Click **View,** and you can view the status of the zone.
5. Click the ☂/↑ icon to bypass or recover a zone separately.

   ↑: The zone is bypassed.

   ☂: The zone is recovered.
6. Click the 🛡/⊘ icon to arm or disarm the zone.

   ⊘: Click to disarm the zone.

   🛡: Click to arm the zone.
7. Click ▶ icon to view the live view of the zone's triggered camera.

   Note: You can set the triggered camera of the zone in Event Management. Refer to *Chapter 13.2 Zone Event Configuration*.

13.4 Displaying Zone on E-map

Purpose:

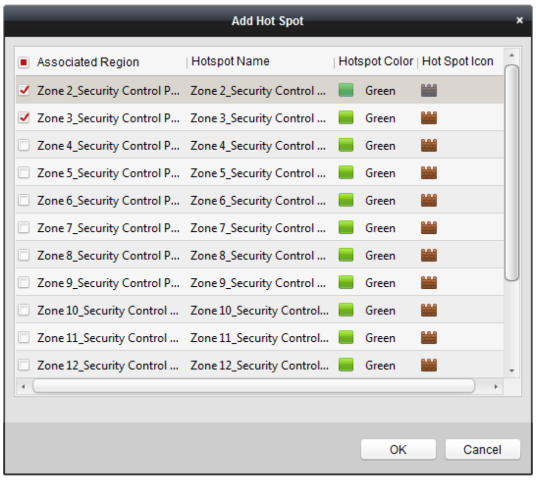
You can add the zone on the E-map, and when the alarm in the zone is triggered, you can view the alarm notification on the E-map and check the alarm details.

Note: For detailed operations of E-map, please refer to *Chapter 7 E-map Management*.

Adding Zones as Hot Spots

Steps:

1. Click the **Edit Map** button in the E-map toolbar to enter the map editing mode.
2. Click the icon ⊕ in the toolbar to open the Add Hot Spot dialog box.



■	Associated Region	Hotspot Name	Hotspot Color	Hot Spot Icon
☑	Zone 2_Security Control P...	Zone 2_Security Control ...	🟩 Green	
☑	Zone 3_Security Control P...	Zone 3_Security Control ...	🟩 Green	
□	Zone 4_Security Control P...	Zone 4_Security Control ...	🟩 Green	
□	Zone 5_Security Control P...	Zone 5_Security Control ...	🟩 Green	
□	Zone 6_Security Control P...	Zone 6_Security Control ...	🟩 Green	
□	Zone 7_Security Control P...	Zone 7_Security Control ...	🟩 Green	
□	Zone 8_Security Control P...	Zone 8_Security Control ...	🟩 Green	
□	Zone 9_Security Control P...	Zone 9_Security Control ...	🟩 Green	
□	Zone 10_Security Control ...	Zone 10_Security Control...	🟩 Green	
□	Zone 11_Security Control ...	Zone 11_Security Control...	🟩 Green	
□	Zone 12_Security Control ...	Zone 12_Security Control...	🟩 Green	

3. Check the checkboxes to select the zones to be added.
4. Optionally, you can edit hot spot name, select the name color and select the hot spot icon by double-clicking the corresponding field.
5. Click **OK** to save the settings. The zone icons are added on the map as hot spots and the icons of added zones change from to in the group list. You can click-and-drag the zone icons to move the hot spots to the desired locations.

   You can also click-and-drag the zone icons from the group list to the map directly to add the hot spots.

Modifying Hot Spots

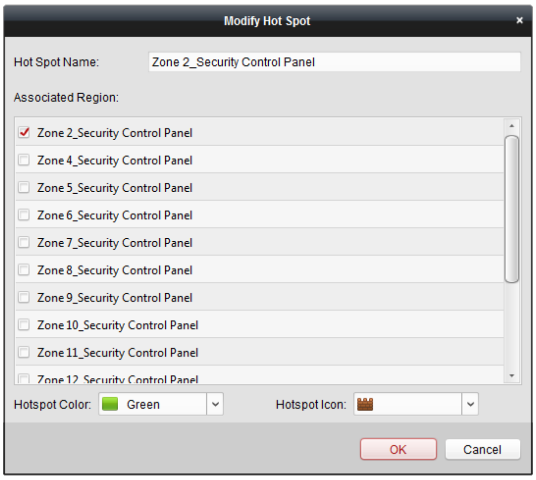
Purpose:

You can modify the information of the added hot spots on the map, including the name, the color, the icon, etc.

Steps:

1. Click the **Edit Map** button in the E-map toolbar to enter the map editing mode.
2. Select the hot spot icon on the map and then click in the toolbar, right-click the hot spot icon and select **Modify**, or double-click the hot spot icon on the map to open the Modify Hot Spot dialog box.
3. You can edit the hot spot name in the text field and select the color, the icon and the linked zone.
4. Click **OK** to save the new settings.

   To delete the hot spot, select the hot spot icon and click in the toolbar, or right-click the hot spot icon and select **Delete**.



Modify Hot Spot

Hot Spot Name: Zone 2_Security Control Panel

Associated Region:

- ☑ Zone 2_Security Control Panel
- □ Zone 4_Security Control Panel
- □ Zone 5_Security Control Panel
- □ Zone 6_Security Control Panel
- □ Zone 7_Security Control Panel
- □ Zone 8_Security Control Panel
- □ Zone 9_Security Control Panel
- □ Zone 10_Security Control Panel
- □ Zone 11_Security Control Panel
- □ Zone 12_Security Control Panel

Hotspot Color: 🟩 Green

Hotspot Icon:

Previewing Hot Spots

Steps:

1. Click the **Map Preview** button in the E-map toolbar to enter the map preview mode.
2. If there is any alarm triggered in the zone, an icon will appear and twinkle near the hot spot. Click the alarm icon, or you can right click the zone icnon and select **Display Alarm Information**, to check the alarm information, including alarm type and triggering time.

   Note: To display the alarm information on the map, the Alarm on E-map functionality needs to be set as the alarm linkage action. For details, refer to *Chapter 13.2 Zone Event Configuration.*
3. To clear the alarm inforatiom displayed on the map, click on the toobar, or right click the zone icnon and select **Clear Alarm Information** to clear the alarms of the selected zone.

Chapter 14 Video Intercom

Purpose:

The Video Intercom module provides remote control and configuration via the iVMS-4200 client software.

- Before remote configure and control the video intercom, you are required to add the device to the software first. Refer to *Chapter 14.1 Device Management*.
- For the live view of video intercom via the iVMS-4200 client software, refer to *Chapter 14.2 Live View.*
- For the picture storage on Storage Server, refer to *Chapter 14.3 Picture Storage.*
- For remote control of video intercom, please refer to *Chapter 14.4* to *14.8*.

14.1 Device Management

Purpose:

Device management includes device activation, adding device, editing device, deleting device and remote configuration.

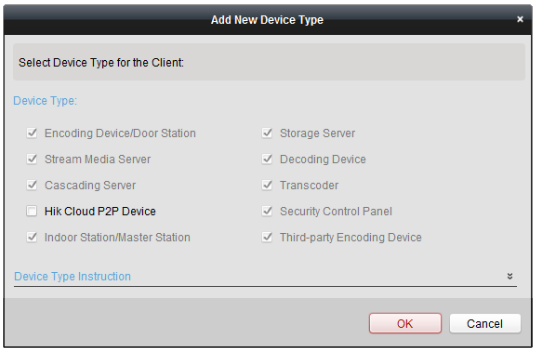
After running the iVMS-4200, door stations, indoor stations, master stations and other video intercom devices should be added to the client for remote configuration and management.

Steps:

1. Click the icon on the control panel, or click **Tools->Device Management** to open the Device Management page.
2. Click the **Server** tab.

   To add indoor station or master station:

   1) Click **Add New Device Type** to enter add new device type interface.
   Select **Indoor Station/Master Station** and click **OK**.



Add New Device Type

Select Device Type for the Client:

Device Type:

☑ Encoding Device/Door Station ☑ Storage Server
☑ Stream Media Server ☑ Decoding Device
☑ Cascading Server ☑ Transcoder
□ Hik Cloud P2P Device ☑ Security Control Panel
☑ Indoor Station/Master Station ☑ Third-party Encoding Device

Device Type Instruction

OK Cancel

   2) In the Server tab, Indoor Station/Master Station will display, select **Indoor Station/Master Station** and click **Add Device** to add the indoor station and master station.

   To add door station:

   In the Server tab, select **Encoding Device/Door Station** to add door station.

   Note: Up to 16 door stations can be added, and up to 512 indoor stations or master stations can be added.

3. You can add the active online devices in the same local subnet with the client software, or select

the adding mode by IP/Domain, or by IP segment, and configure the corresponding settings for the device.

Note: For activating the device, see *Chapter 3.1.1 Creating the Password*.

For the detailed configuration about the adding modes, please refer to the following chapters:

- By adding the online devices, see *Chapter 3.1.2 Adding Online Devices*.
- By specifying the device IP/Domain address, see *Chapter 3.1.3 Adding Devices Manually.*
- By specifying an IP segment, see *Chapter 3.1.4 Adding Devices by IP Segment*.

Add Multiple Online Devices

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.

Add All the 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.

Modify Network Information

Select the device from the list, click **Modify Netinfo**, and then you can modify the network information of the selected device.

Note: You should enter the admin password of the device in the **Password** field of the pop-up window to modify the parameters.

Restore Default Password

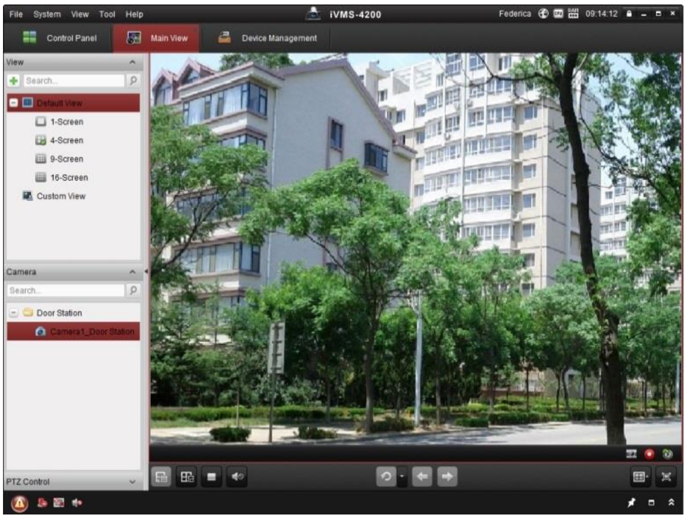
Select the device from the list, click **Restore Default Password**, input the security code, and then you can restore the default password of the selected device.

Note: The security code is returned after you send the data and serial No. of the device to the manufacturer.

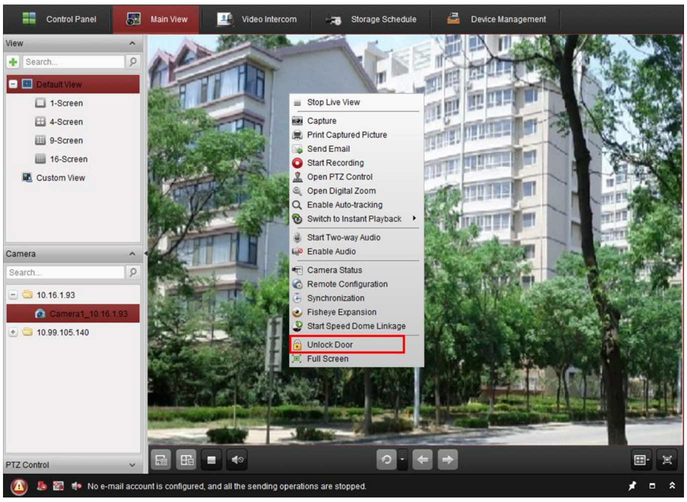
14.2 Live View

Steps:

1. Enter the main view interface of iVMS-4200 client software to display the live view of door station (V Series).



2. Right click on the live view interface to display the menu and select **Unlock Door** to remote unlock the door.



14.3 Picture Storage

When the device is under armed status, it will auto capture after unlocking the door. If the storage server is installed together with iVMS-4200 client software, the captured picture will be uploaded to the storage server.

Note: The device refers to V Series door station and D Series door station.

14.4 Group Management

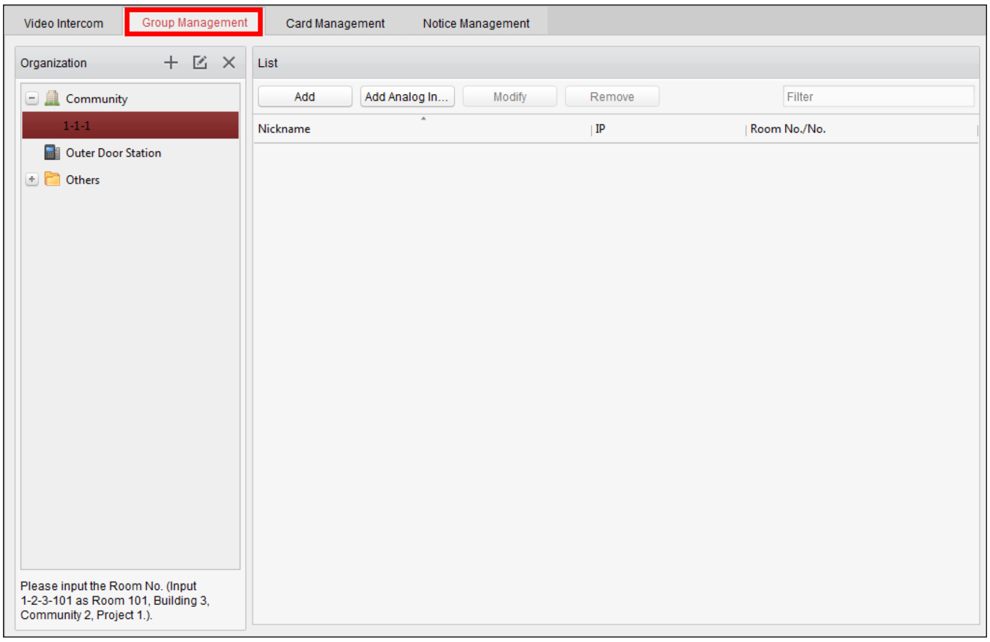
Click the icon on the control panel,

or click **View**->**Video Intercom** to open the Intercom page.

Click **Group Management** tab to add, edit, and delete groups. Three group types can be selected: building, outer door station and other. Here we take the building as an example.

Steps:

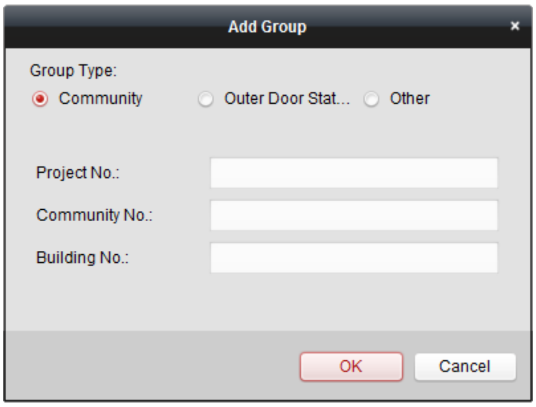
1. The group of the community is listed on the left, as shown in the figure below.



Please input the Room No. (Input 1-2-3-101 as Room 101, Building 3, Community 2, Project 1.).

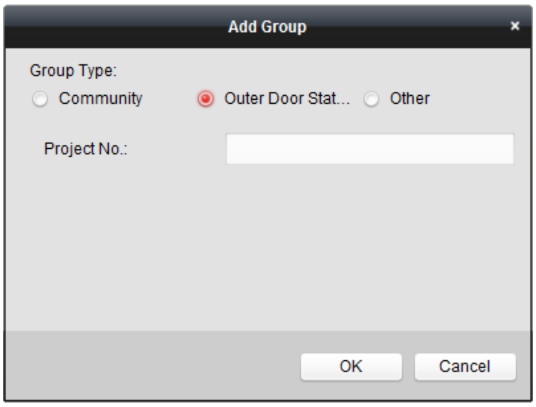
2. Select the group type and click + to add group, input the corresponding information accordingly.

- Select group type as **Community** and then Input the Project No., Community No., and Building No. to set the community structure, as shown in the figure below.



Group Type:
● Community ○ Outer Door Stat... ○ Other

- Select group type as **Outer Door Station** and then input the outer door station name (Range: 1 to 9) to set the outer door station, as shown in the figure below.



Group Type:
○ Community ● Outer Door Stat... ○ Other

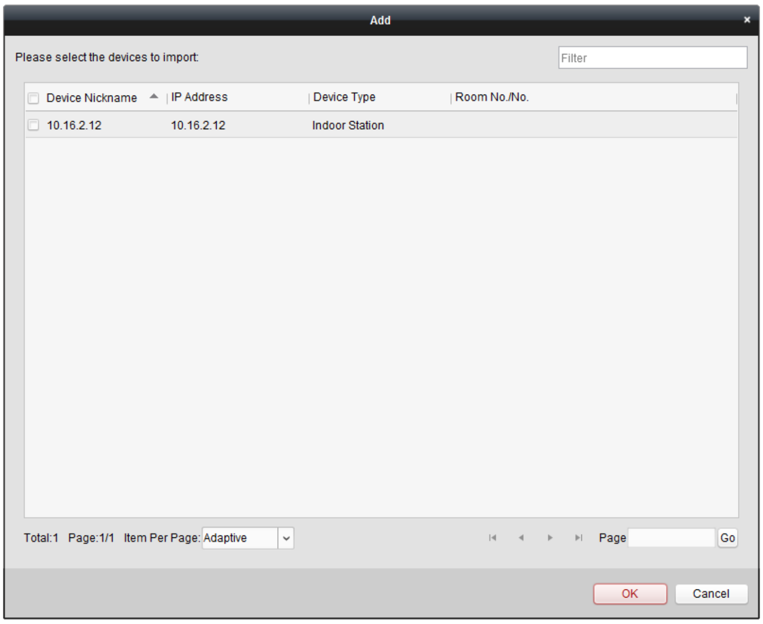
- Select group type as **Other** and then input the group name. For example, you can set group as administrator, entrance guard and cleaning staff, etc.

Note: You can add group to **Other** and set different groups to assign cards to staff other than residents, such as administrator, security guard and cleaning staff, etc. So you can assign corresponding cards and configure their different permissions.

3. After setting the community, you can add devices to the list on the right.

- **Adding Network Video Intercom Device:**

  1) Select the added community in the organization list and click **Add** to enter the following interface. The video intercom devices added to the client software will be listed, as shown in the figure below.

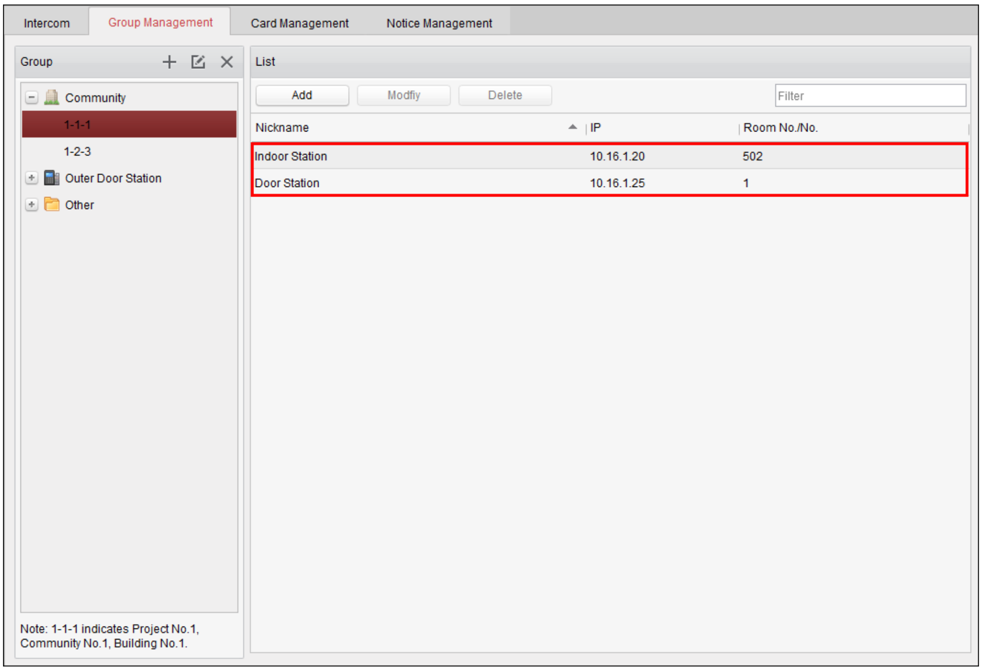


Please select the devices to import:

□ Device Nickname	IP Address	Device Type	Room No./No.
□ 10.16.2.12	10.16.2.12	Indoor Station	

  2) Check the checkboxes of devices and input the Room No. of indoor stations and door station No. to assign the devices to the community.

  3) Click **OK** to save the setting.

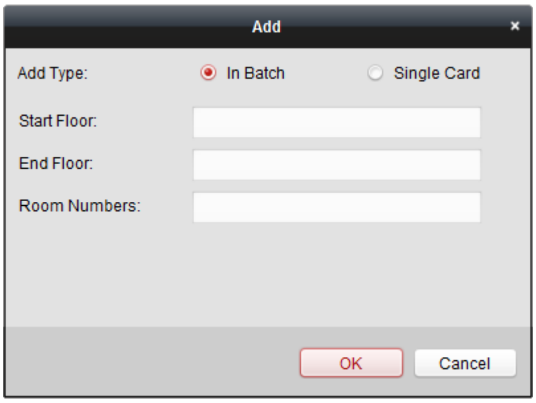


Nickname	IP	Room No./No.
Indoor Station	10.16.1.20	502
Door Station	10.16.1.25	1

Note: 1-1-1 indicates Project No.1, Community No.1, Building No.1.

- **Adding Analog Indoor Station**

1) Select the added community in the organization list and click **Add Analog Indoor Station** to enter the following interface.



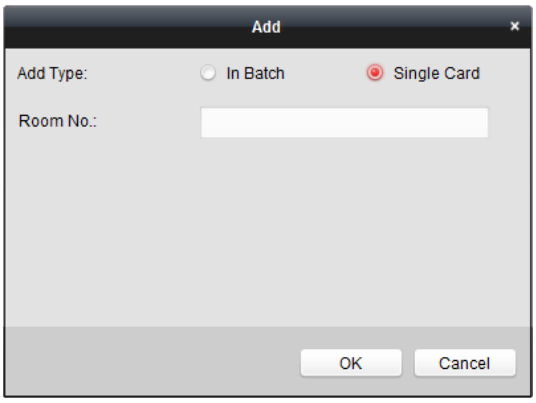
Add

Add Type: ● In Batch ○ Single Card

Start Floor:

End Floor:

Room Numbers:



Add

Add Type: ○ In Batch ● Single Card

Room No.:

2) You can select the adding method as **Single Adding** or **Batch Adding**.

For Single Adding, you are required to input the room No. for the analog indoor station to add.

For Batch Adding, you are required to input:

Start Floor: The start floor No. for the analog indoor stations to add.

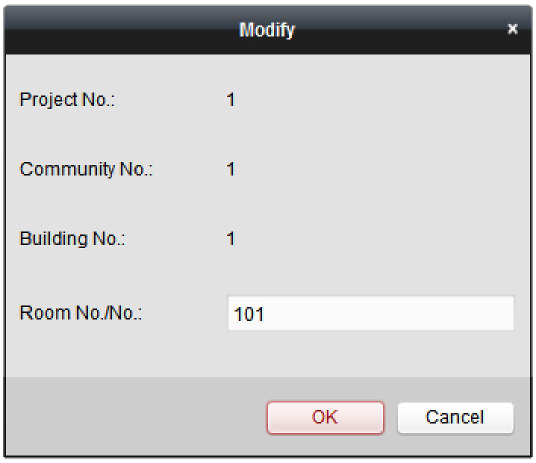
End Floor: The start floor No. for the analog indoor stations to add.

Room Number: The number of the rooms of each floor.

Note: For configuring the floor No. and Room No. of the analog indoor station, please refer to the *User Manual* of the analog indoor station.

3) Click **OK** to add the analog indoor station(s).

2. Select the indoor station or door station and click **Modify** to modify the room No. or the door station No.. If you want to delete the assigned device, select the device and click **Remove** to delete it.



Modify

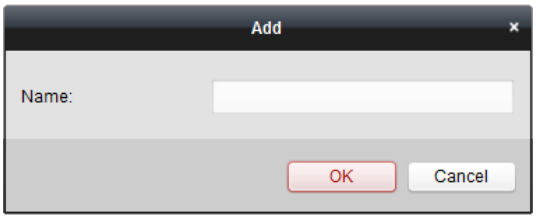
Project No.: 1

Community No.: 1

Building No.: 1

Room No./No.: 101

3. To add person in other groups, you should select a sub group from **Other** and then click **Add** to add a person.

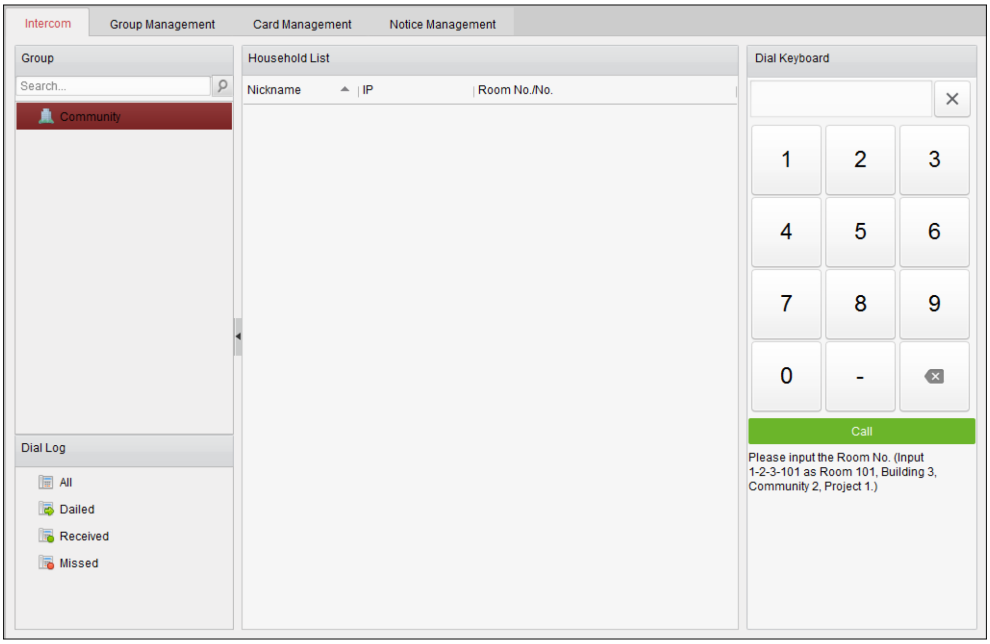


Input the name of the added person, and click **OK** to save the settings.

After adding the person, select the person and click **Modify** to modify the person's name. If you want to delete the assigned person, select the person and click **Remove** to delete it.

14.5 Intercom

Click **Intercom** tab to open the Intercom page.



Please input the Room No. (Input 1-2-3-101 as Room 101, Building 3, Community 2, Project 1.)

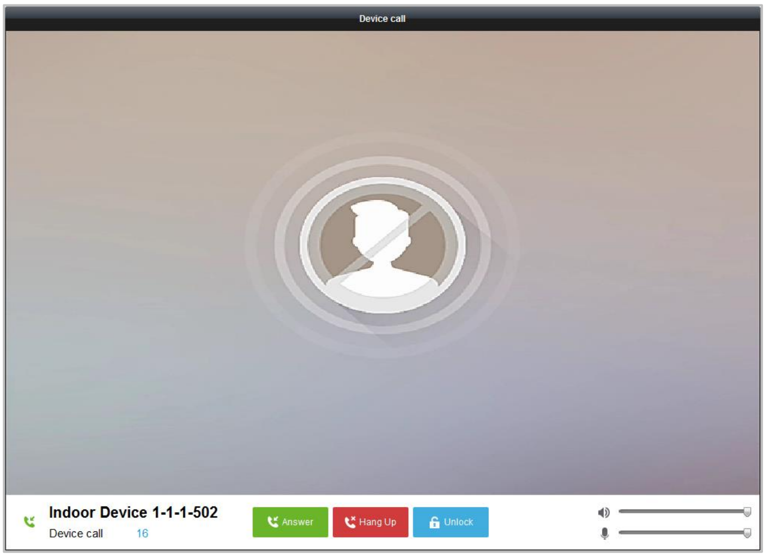
14.5.1 Video Intercom with iVMS-4200 via Indoor Station

Purpose:

When the indoor station has been added to the client software, the video intercom with iVMS-4200 via indoor station can be realized.

Steps:

1. Add the indoor station to the iVMS-4200 client software.
2. Make sure the SIP Server IP of the indoor station is not configured (or abnormal).
3. Press **Center** on the main interface of the indoor station.



Note: When the SIP server IP of the indoor station is configured, press **Center** on the main interface of the indoor station to call the master station.

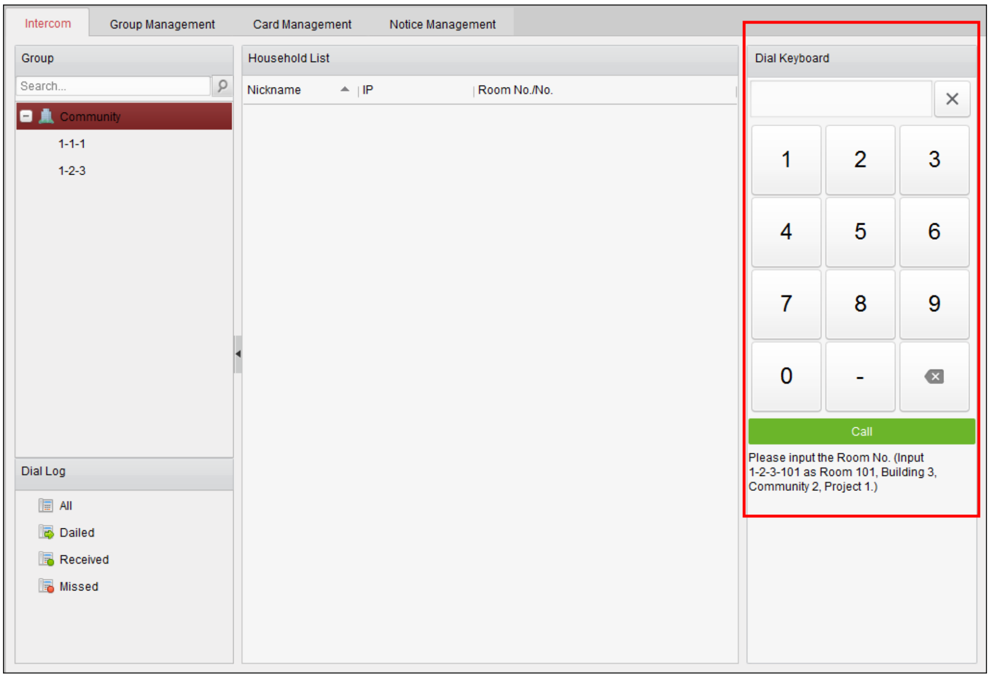
14.5.2 Video Intercom with Indoor Station via iVMS-4200

Enter **Control Panel**-> **Video Intercom**-> **Intercom** tab page.

Three ways of video calling indoor stations via iVMS-4200 can be realized.

Calling Resident by Room No.

1. Input the room No. of the indoor station in the dial keyboard on the right.



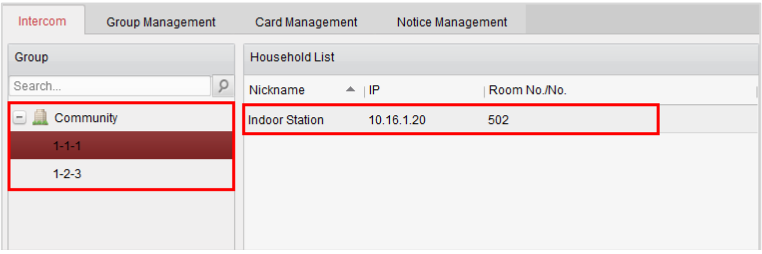
Please input the Room No. (Input 1-2-3-101 as Room 101, Building 3, Community 2, Project 1.)

Note: The room No. should be in correct format. For example, 1-2-3-101 as Room 101, Building No.3, Community No.2, Project No.1.

2. Click Call to start video call with the indoor station.

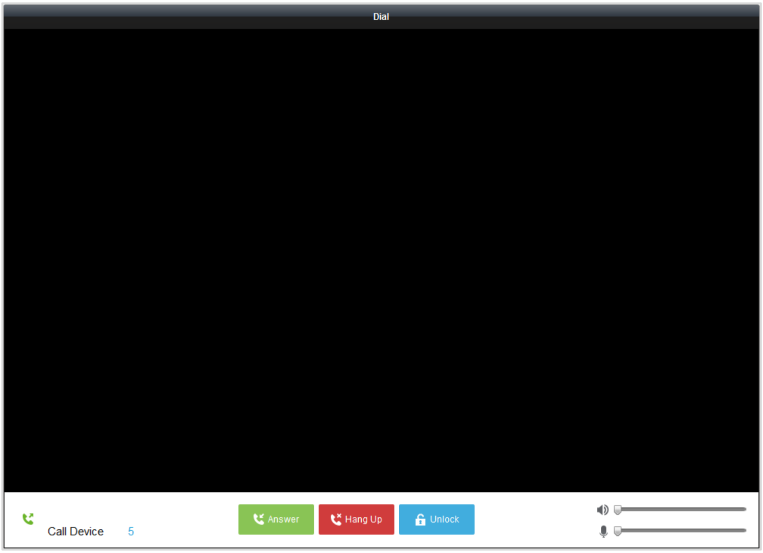
Calling Resident from Community

1. Select the community from the groups on the left.



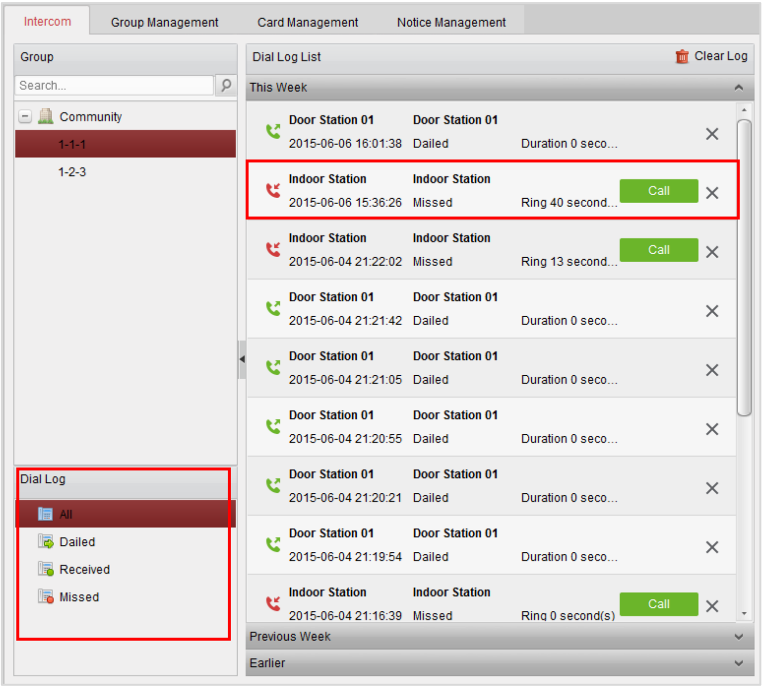
Nickname	IP	Room No./No.
Indoor Station	10.16.1.20	502

2. Double click the added resident from the resident list to call the resident.
3. The video call from client software with resident will be realized.



Calling Resident from Call Log

1. Click the dial log on the below and select the log type to enter the dial log interface.



Door Station 01 2015-06-06 16:01:38	Door Station 01 Dailed	Duration 0 seco...	
Indoor Station 2015-06-06 15:36:26	Indoor Station Missed	Ring 40 second...	Call
Indoor Station 2015-06-04 21:22:02	Indoor Station Missed	Ring 13 second...	Call
Door Station 01 2015-06-04 21:21:42	Door Station 01 Dailed	Duration 0 seco...	
Door Station 01 2015-06-04 21:21:05	Door Station 01 Dailed	Duration 0 seco...	
Door Station 01 2015-06-04 21:20:55	Door Station 01 Dailed	Duration 0 seco...	
Door Station 01 2015-06-04 21:20:21	Door Station 01 Dailed	Duration 0 seco...	
Door Station 01 2015-06-04 21:19:54	Door Station 01 Dailed	Duration 0 seco...	
Indoor Station 2015-06-04 21:16:39	Indoor Station Missed	Ring 0 second(s)	Call

2. Click the Call button from the call logs to start video call with the indoor station.

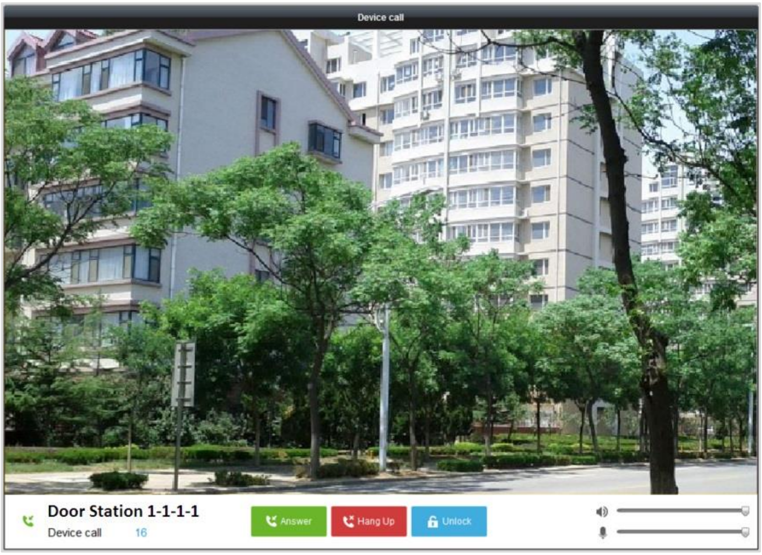
14.5.3 Video Intercom with iVMS-4200 via Door Station

Purpose:

When the door station has been added to the client software, the video intercom with iVMS-4200 via door station can be realized.

Steps:

1. Add the door station to the iVMS-4200 client software.
2. Make sure the SIP Server IP of the door station is not configured (or abnormal).
3. Press **Calling Center Key** on the door station.



Notes:

- When the SIP server IP of door station is configured, press **Calling Center Key** of the door station to call the master station.
- You can press the **Unlock** key to remote unlock the door station via iVMS-4200 while video call is started by the door station. Answering the video call is optional for remote unlocking the door station.

14.5.4 Call Log

Steps:

1. Enter **Control Panel**-> **Operation and Control**-> **Video Intercom**-> **Intercom tab** page.
2. Click to select the log type from the dial log and the selected dial logs will be listed in the dial log list.
3. Click **Call** button to start video call with the indoor station.
4. Click Clear Log to clear all logs (optional).

14.6 Card Management

Purpose:

You can add unauthorized cards to the community and then you can assign the cards to the corresponding indoor station and outdoor stations.

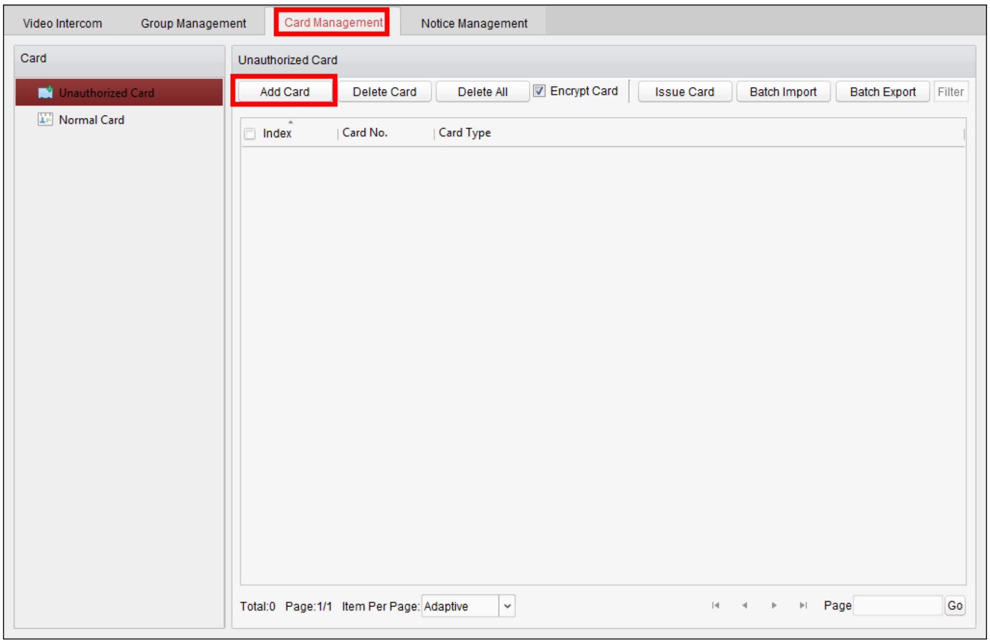
For example, if there are 3 residents living in Room 401, you can assign 3 cards to No. 401 Indoor Station.

For each indoor station, you can assign multiple cards, and you can assign these cards to the door station from same building.

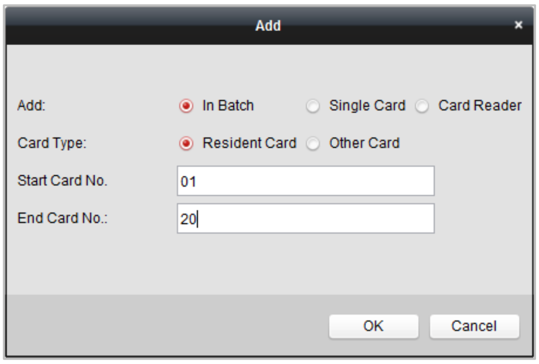
14.6.1 Adding Card

Steps:

1. Select **Card Management** to enter the card management tab page.



2. Select **Unauthorized Card** and click **Add Card** to add unauthorized cards.



Add: ● In Batch ○ Single Card ○ Card Reader

Card Type: ● Resident Card ○ Other Card

Start Card No. 01

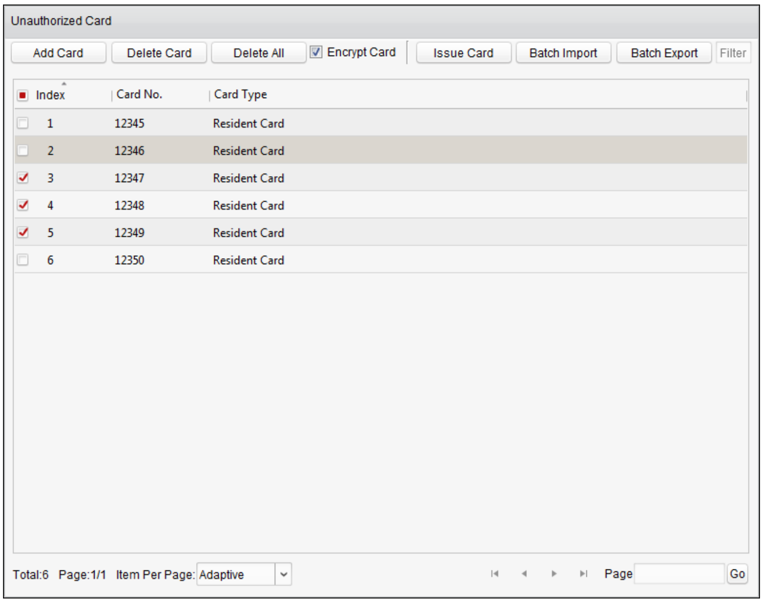
End Card No.: 20

3. Select adding mode to add cards in batch, add single card or with card reader. You can select card type as resident card or other card.

Note: To add cards with card reader, a card reader is required (purchased separately). For setting the card reader type, please refer to *Chapter 17.2.7 Video Intercom Settings.*

4. Input the start card No. and end card No., click **OK** to accomplish the adding.

   The added cards information are listed in the unauthorized card interface, as shown in the figure below.



■ Index	Card No.	Card Type
□ 1	12345	Resident Card
□ 2	12346	Resident Card
☑ 3	12347	Resident Card
☑ 4	12348	Resident Card
☑ 5	12349	Resident Card
□ 6	12350	Resident Card

Total:6 Page:1/1 Item Per Page: Adaptive

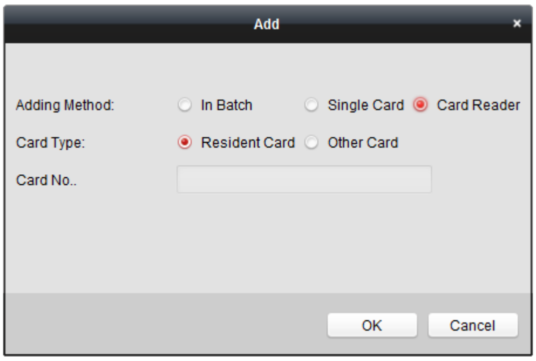
5. To delete the unauthorized card, you can check to select the card and click **Delete Card** to delete the selected unauthorized card, or click **Delete All** to clear all the added unauthorized cards.

14.6.2 Encrypting Card

You can encrypt the card to improve the card security and prevent it from being copied.

Steps:

1. Connect the card reader with the PC for reading the card information.
2. Check the **Encrypt Card** checkbox and click **Add Card** button to add unauthorized cards.
3. Select the adding method as **Card Reader** and select the card type to add.



Adding Method: ○ In Batch ○ Single Card ● Card Reader

Card Type: ● Resident Card ○ Other Card

Card No..

4. Get the card No. with the connected card reader.
5. Click **OK** to add the card and the added card will be encrypted.

Note: Enabling the card encryption can improve the card security to prevent it from being copied. But at the same time, the default key of all the available sectors of the card is modified.

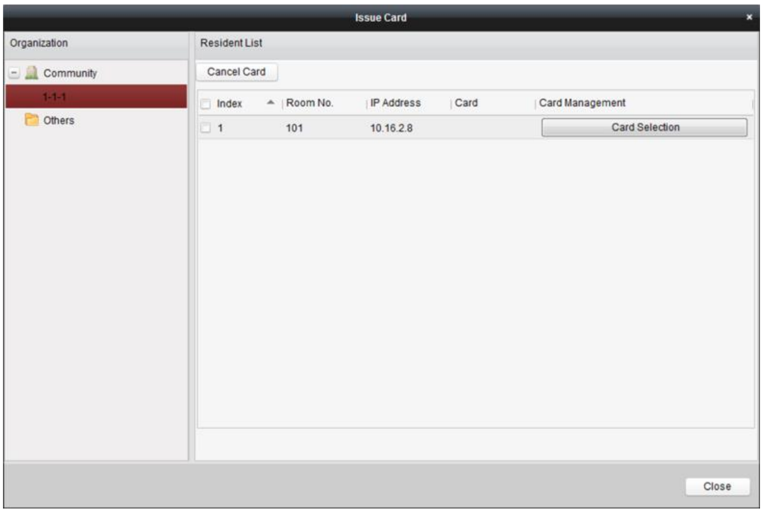
14.6.3 Issuing Card

Click **Issue Card** to enter the issue card interface.

To Assign Resident Cards:

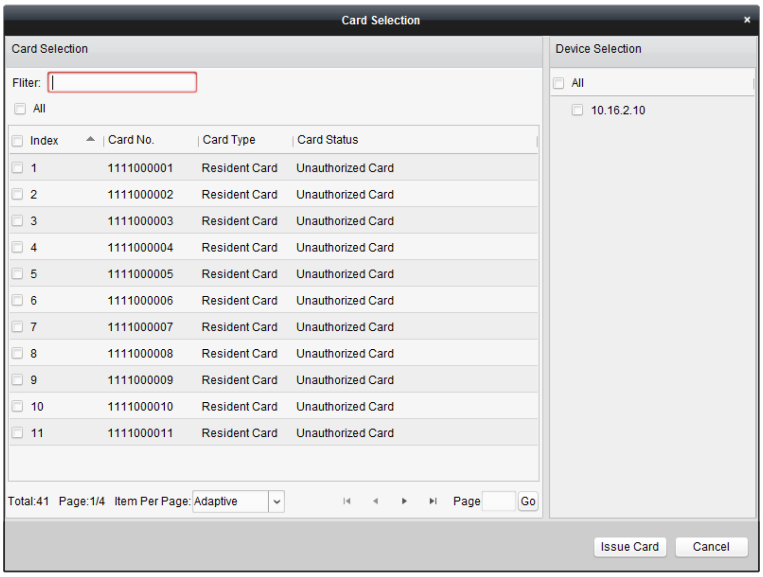
Steps:

1. Select **Community** from the group list and the indoor stations of the community will be listed in the resident list.



Index	Room No.	IP Address	Card	Card Management
1	101	10.16.2.8		Card Selection

2. Click **Card Selection** to assign cards to the indoor station. You can assign multiple cards to one indoor station.
3. Check the checkboxes of the cards you need to assign to the indoor station, and check the checkbox of door stations, doorphones and outer door stations (only resident cards can be assigned to indoor stations).
4. Click **Issue Card** to complete the card issuing operation.

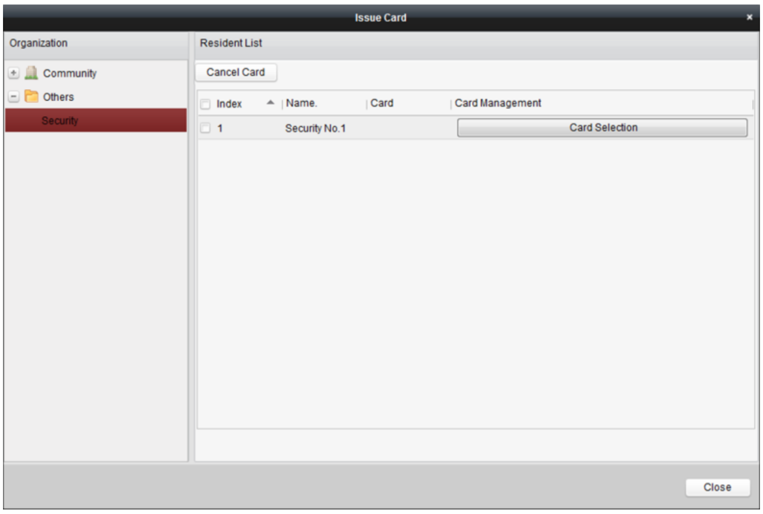


□ Index	Card No.	Card Type	Card Status
□ 1	1111000001	Resident Card	Unauthorized Card
□ 2	1111000002	Resident Card	Unauthorized Card
□ 3	1111000003	Resident Card	Unauthorized Card
□ 4	1111000004	Resident Card	Unauthorized Card
□ 5	1111000005	Resident Card	Unauthorized Card
□ 6	1111000006	Resident Card	Unauthorized Card
□ 7	1111000007	Resident Card	Unauthorized Card
□ 8	1111000008	Resident Card	Unauthorized Card
□ 9	1111000009	Resident Card	Unauthorized Card
□ 10	1111000010	Resident Card	Unauthorized Card
□ 11	1111000011	Resident Card	Unauthorized Card

To Assign Other Cards:

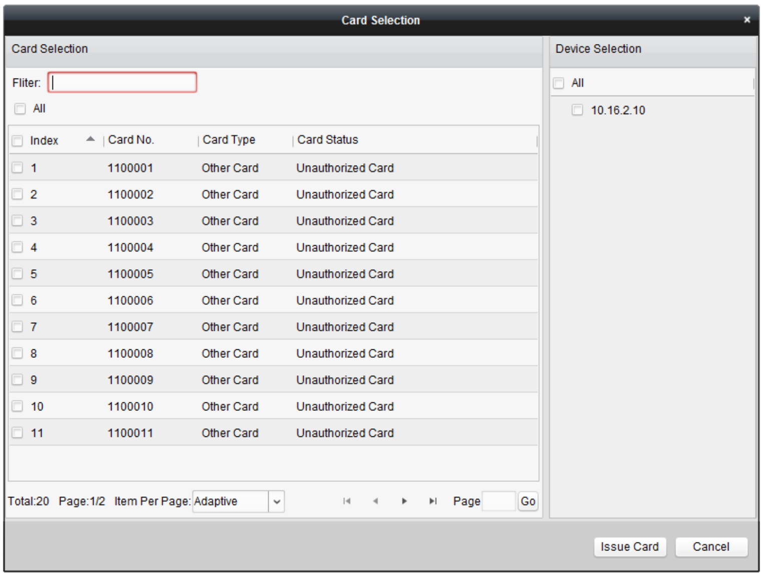
Steps:

1. Select **Other** from the group list and the added persons of the community will be listed in the resident list.



□ Index	Name.	Card	Card Management
□ 1	Security No.1		Card Selection

2. Click **Card Selection** to assign cards to the organization. You can assign multiple cards to one person.
3. Check the checkboxes of the cards you need to assign to the person, and check the checkbox of door stations, doorphones and outer door stations (only other cards can be assigned to person).
4. Click **Issue Card** to complete the card issuing operation.



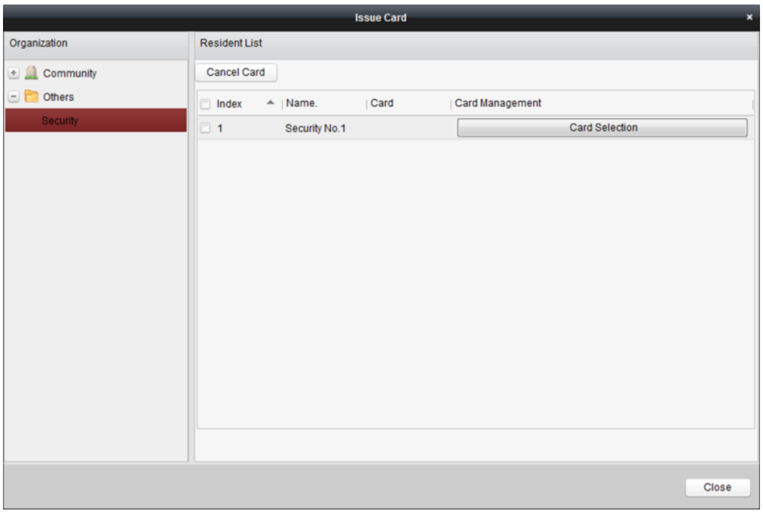
□ Index	Card No.	Card Type	Card Status
□ 1	1100001	Other Card	Unauthorized Card
□ 2	1100002	Other Card	Unauthorized Card
□ 3	1100003	Other Card	Unauthorized Card
□ 4	1100004	Other Card	Unauthorized Card
□ 5	1100005	Other Card	Unauthorized Card
□ 6	1100006	Other Card	Unauthorized Card
□ 7	1100007	Other Card	Unauthorized Card
□ 8	1100008	Other Card	Unauthorized Card
□ 9	1100009	Other Card	Unauthorized Card
□ 10	1100010	Other Card	Unauthorized Card
□ 11	1100011	Other Card	Unauthorized Card

Total:20 Page:1/2 Item Per Page: Adaptive

To Delete Cards:

Steps:

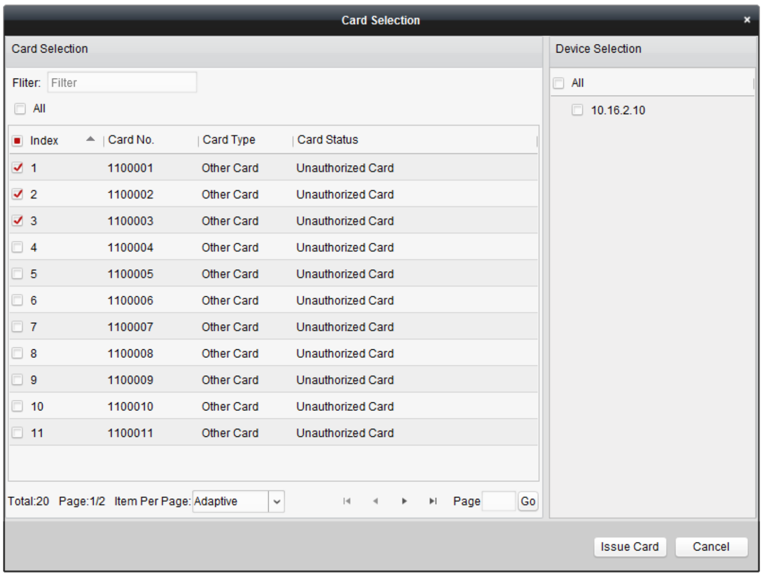
1. Click **Issur Card** to enter the card issuing interface.



□ Index	Name.	Card	Card Management
□ 1	Security No.1		Card Selection

2. Select the **Community** from groups to delete normal cards, and select **Other** from groups to delete other cards.

3. To cancel certain cards or single card, click the **Card Selection** to enter the card selection interface.



Card Selection

Card Selection

Filter: Filter

□ All

☒ Index	Card No.	Card Type	Card Status
☑ 1	1100001	Other Card	Unauthorized Card
☑ 2	1100002	Other Card	Unauthorized Card
☑ 3	1100003	Other Card	Unauthorized Card
□ 4	1100004	Other Card	Unauthorized Card
□ 5	1100005	Other Card	Unauthorized Card
□ 6	1100006	Other Card	Unauthorized Card
□ 7	1100007	Other Card	Unauthorized Card
□ 8	1100008	Other Card	Unauthorized Card
□ 9	1100009	Other Card	Unauthorized Card
□ 10	1100010	Other Card	Unauthorized Card
□ 11	1100011	Other Card	Unauthorized Card

Total:20 Page:1/2 Item Per Page: Adaptive Page Go

Device Selection

□ All

□ 10.16.2.10

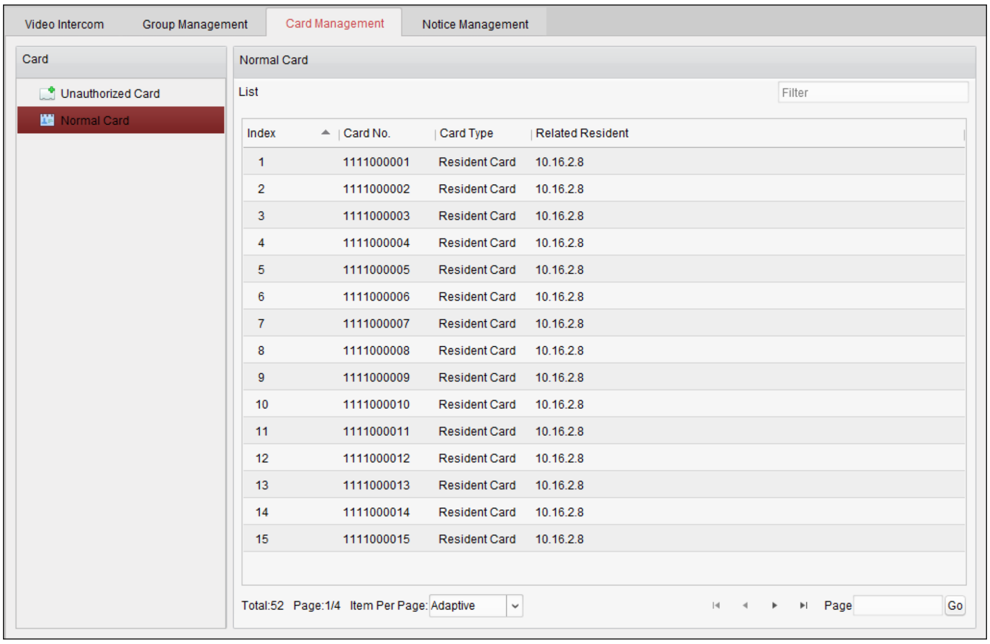
4. Cancel the checkbox(es) of assigned cards and check the checkbox(es) of door station(s) to cancel the card(s).
5. Click **Issue Card** to accomplish the operation.

Notes:

- You can cancel card from single or certain door stations by cancelling the checkboxes from the device list.
- To cancel all issued cards, check the checkboxes of Room No./name, and click **Cancel Card** to cancel all cards issued to the device. The card state will be reset to unauthorized card.

Normal Card

Click **Normal Card** to display normal card list. After issuing cards, the issued cards will be listed in the normal card list, as shown in the figure below.



Normal Card

List

Filter

Index	Card No.	Card Type	Related Resident
1	1111000001	Resident Card	10.16.2.8
2	1111000002	Resident Card	10.16.2.8
3	1111000003	Resident Card	10.16.2.8
4	1111000004	Resident Card	10.16.2.8
5	1111000005	Resident Card	10.16.2.8
6	1111000006	Resident Card	10.16.2.8
7	1111000007	Resident Card	10.16.2.8
8	1111000008	Resident Card	10.16.2.8
9	1111000009	Resident Card	10.16.2.8
10	1111000010	Resident Card	10.16.2.8
11	1111000011	Resident Card	10.16.2.8
12	1111000012	Resident Card	10.16.2.8
13	1111000013	Resident Card	10.16.2.8
14	1111000014	Resident Card	10.16.2.8
15	1111000015	Resident Card	10.16.2.8

Total:52 Page:1/4 Item Per Page: Adaptive Page Go

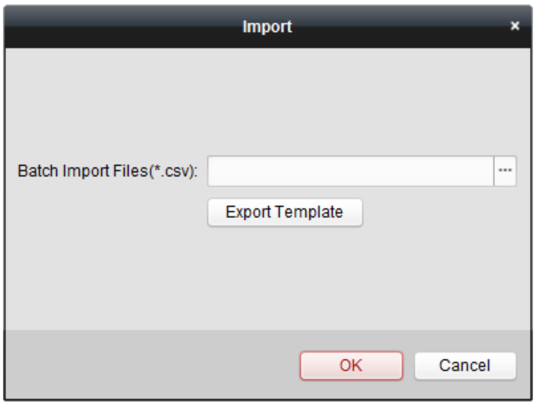
Notes:

- To assign the cards with card issuer, please connect the card reader DS-K1F100-D8 (purchased separately) to PC via USB interface. Open iVMS-4200 and enter the directory of **Video Intercom->Card Management->Unauthorized Card->Add Card**. Swipe the unauthorized card in turn and the card No. will be read and added to the device automatically.
- After issuing each card via iVMS-4200, the device plays the voice prompt: Issuing card finished.

14.6.4 Batch Importing Unauthorized Cards

Steps:

1. Click **Batch Import** to enter the batch import interface, as shown in the figure below.



2. Click **Export Template** to export the template of the batch import file.
3. Fill in the template of the batch import file and save it.
4. Click ⋯ to select the batch import file and click **Open**.
5. Click **OK** to start importing the batch import file.

14.6.5 Batch Exporting Unauthorized Cards

Steps:

1. After adding unauthorized cards, and click **Batch Export**.
2. Select the saving file path and click **Save**.
3. After batch exporting the unauthorized cards, the excel will be generated in the saving directory.

14.7 Notice Management

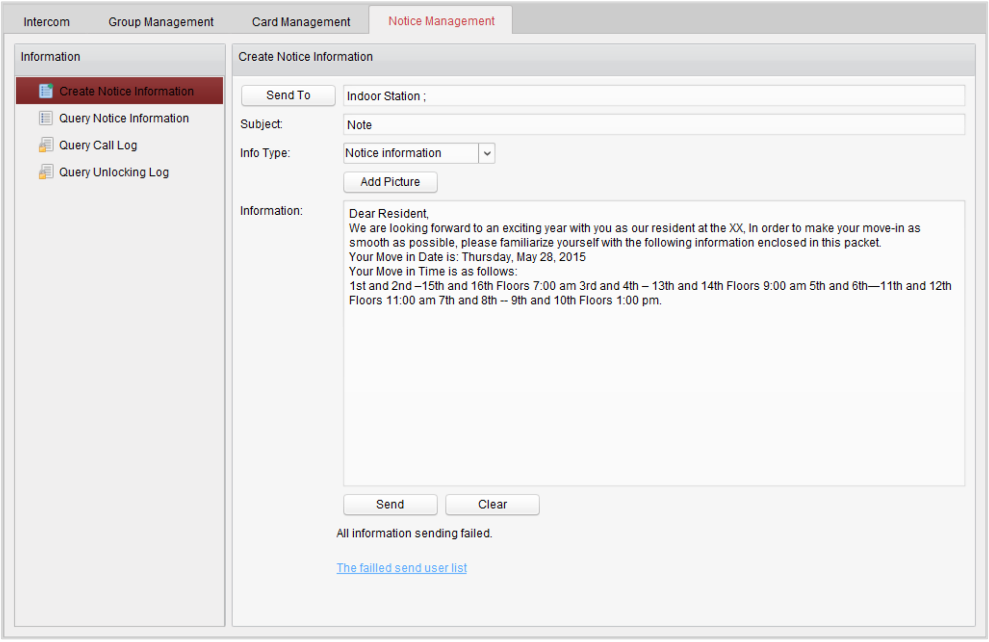
14.7.1 Create Notice Information

Purpose:

You can create notice information and send it to residents.

Steps:

1. Click **Create Notice Information** to enter the create notice information interface.



Create Notice Information

Send To: Indoor Station ;

Subject: Note

Info Type: Notice information

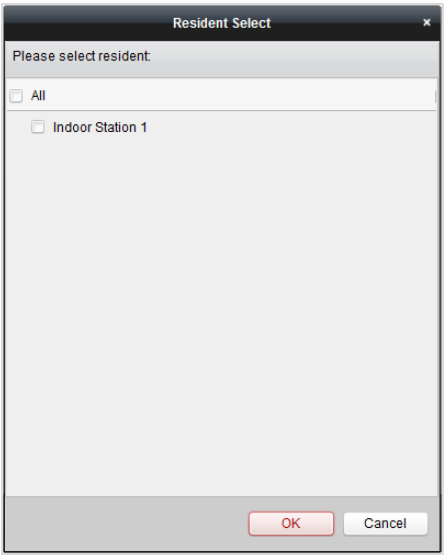
Information:

Dear Resident,
We are looking forward to an exciting year with you as our resident at the XX, In order to make your move-in as smooth as possible, please familiarize yourself with the following information enclosed in this packet.
Your Move in Date is: Thursday, May 28, 2015
Your Move in Time is as follows:
1st and 2nd –15th and 16th Floors 7:00 am 3rd and 4th – 13th and 14th Floors 9:00 am 5th and 6th—11th and 12th Floors 11:00 am 7th and 8th -- 9th and 10th Floors 1:00 pm.

All information sending failed.

The failled send user list

2. Click **Send To** to enter the resident select interface.



3. Select the resident to send the notice information, and click **OK**.
4. Input the subject, select the info type and add the picture (optional).
5. Input the information and click **Send** to send the notice.

Notes:

- No more than 63 letters (including space) can be input in the field of subject.
- No more than 1023 letters (including space) can be input in the field of information.
- Only picture with size smaller than 512KB and with format of jpg. can be added to the notice, and no more than 6 pictures can be added to the same notice information.

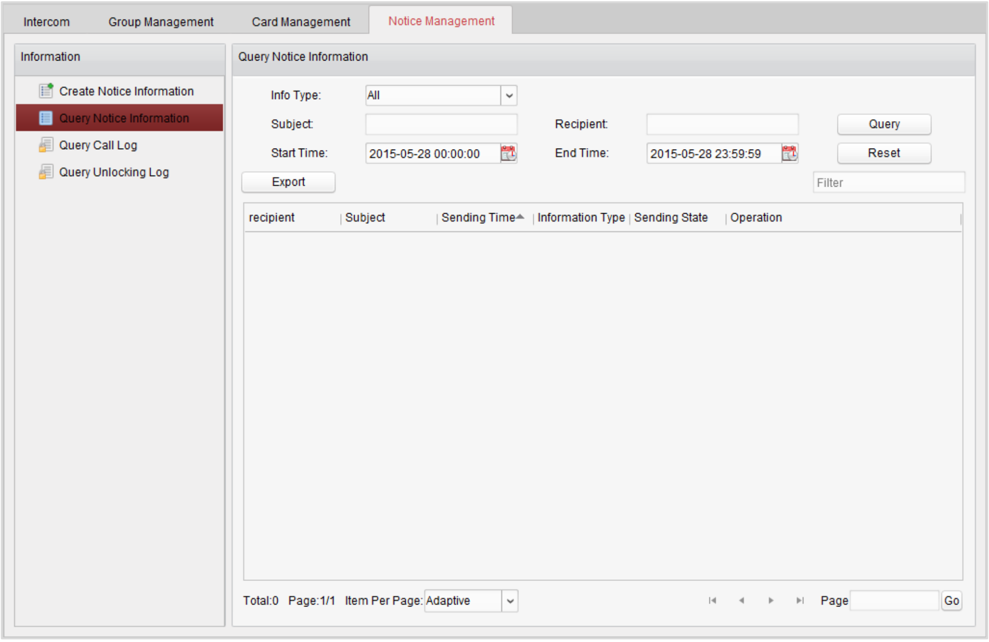
14.7.2 Query Notice Information

Purpose:

You can search the notice information send to residents.

Steps:

1. Select **Query Notice Information** to enter query notice information interface.
2. Select the info type, input the subject, recipient, and set the start time and end time.



Info Type: All

Subject:

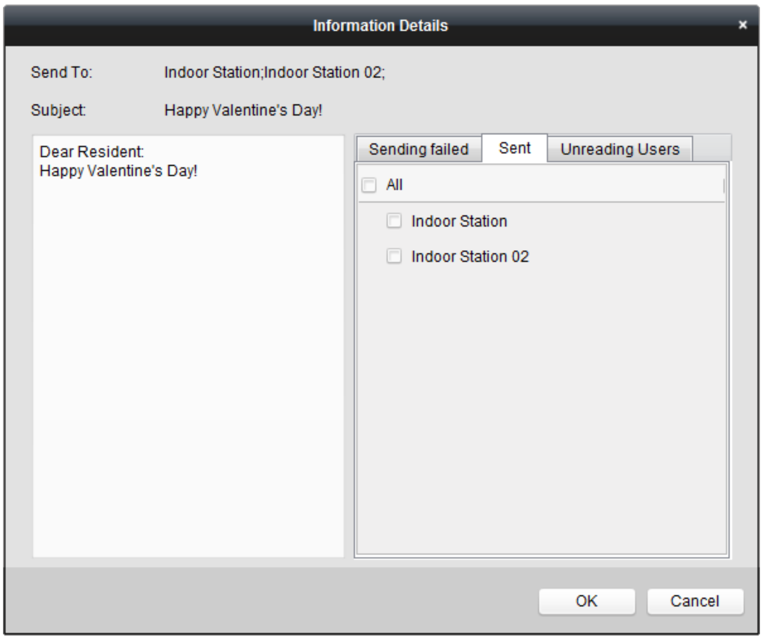
Recipient:

Start Time: 2015-05-28 00:00:00

End Time: 2015-05-28 23:59:59

Total:0 Page:1/1 Item Per Page: Adaptive

3. Click **Query** to search the notice information.
4. Click ⚙ to view the detailed information of selected notice. You can resend the notice information failed to be received or unread by residents.



Send To: Indoor Station;Indoor Station 02;

Subject: Happy Valentine's Day!

Dear Resident:
Happy Valentine's Day!

□ All

□ Indoor Station

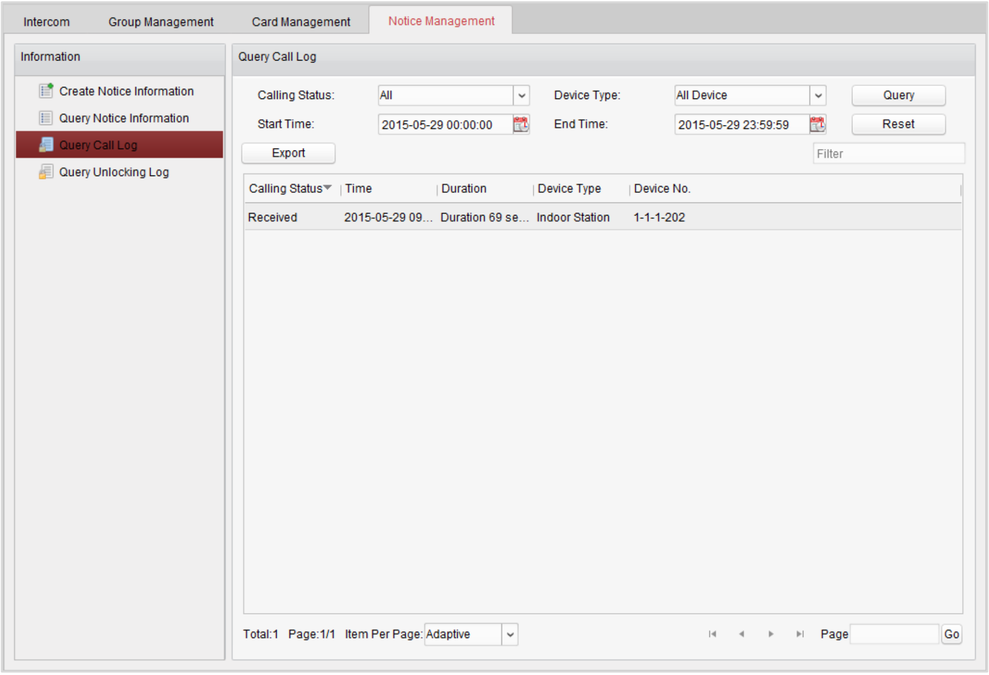
□ Indoor Station 02

5. Click **Export** to export the notice information.

14.7.3 Query Call Logs

Steps:

1. Click **Query Call Logs** to enter query call logs interface.
2. Select the calling status, device type, and set the start time and end time.
3. Click **Query** to search the calling log.



Calling Status: All

Device Type: All Device

Start Time: 2015-05-29 00:00:00

End Time: 2015-05-29 23:59:59

Calling Status	Time	Duration	Device Type	Device No.
Received	2015-05-29 09...	Duration 69 se...	Indoor Station	1-1-1-202

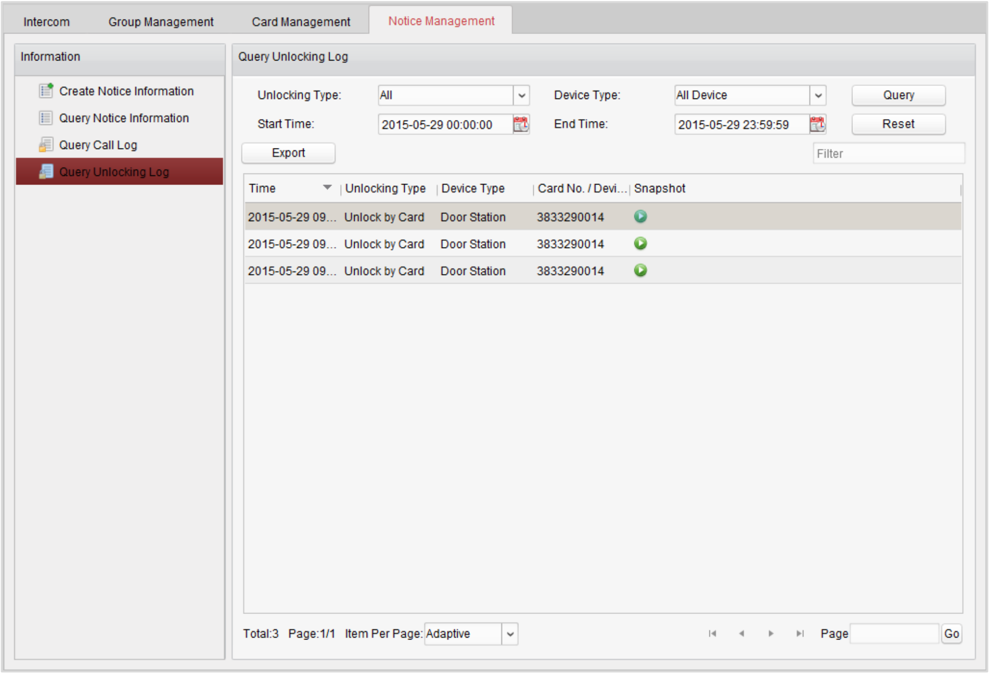
Total:1 Page:1/1 Item Per Page: Adaptive

4. Click **Export** to export the calling logs.

14.7.4 Query Unlocking Log

Steps:

1. Click **Query Unlocking Logs** to enter query unlocking logs interface.
2. Select the unlocking type, device type, and set the start time and end time.



Unlocking Type: All
Device Type: All Device
Start Time: 2015-05-29 00:00:00
End Time: 2015-05-29 23:59:59

Time	Unlocking Type	Device Type	Card No. / Devi...	Snapshot
2015-05-29 09...	Unlock by Card	Door Station	3833290014	●
2015-05-29 09...	Unlock by Card	Door Station	3833290014	●
2015-05-29 09...	Unlock by Card	Door Station	3833290014	●

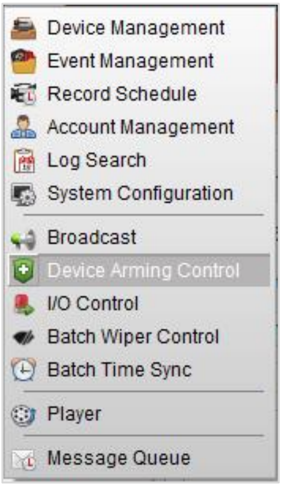
Total:3 Page:1/1 Item Per Page: Adaptive Page Go

3. Click **Query** to search the unlocking log.
4. Click **Export** to export the unlocking logs.

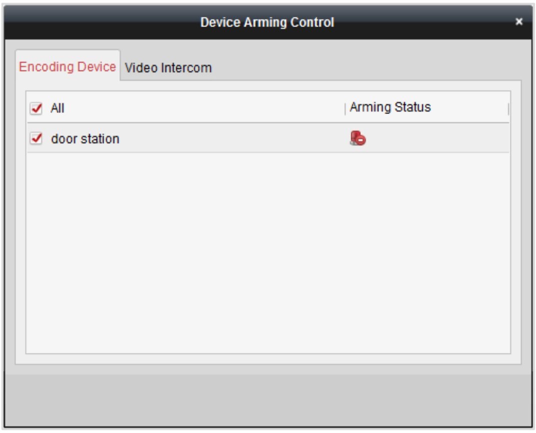
14.8 Device Arming Control

Steps:

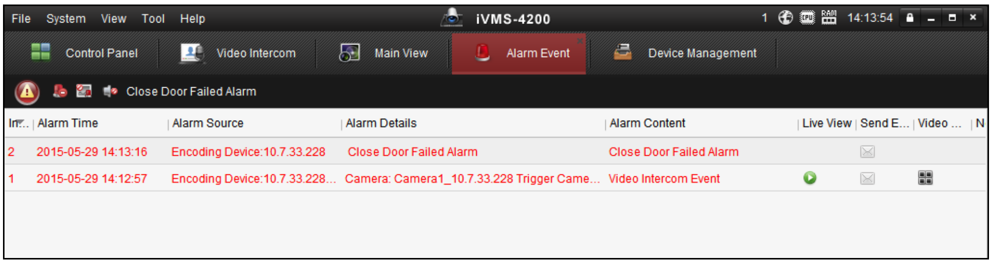
1. Select **Tool**->**Device Arming Control** to enter the device arming control interface.



2. Set the arming status of the device as armed, and the alarm information will be auto uploaded to the client software when alarm occurs.



☑ All	Arming Status
☑ door station	



In...	Alarm Time	Alarm Source	Alarm Details	Alarm Content	Live View	Send E...	Video ...	N
2	2015-05-29 14:13:16	Encoding Device:10.7.33.228	Close Door Failed Alarm	Close Door Failed Alarm				
1	2015-05-29 14:12:57	Encoding Device:10.7.33.228...	Camera: Camera1_10.7.33.228 Trigger Came...	Video Intercom Event				

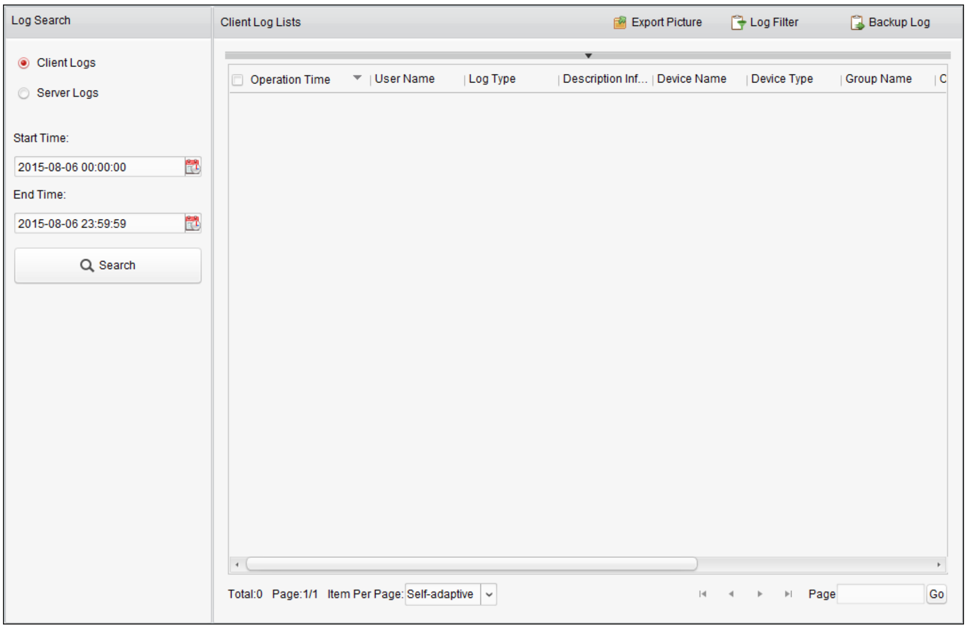
Note: After adding the device to the client software, it will be armed automatically.

Chapter 15 Log Management

Purpose:

The log files of the client software are stored on the local PC and can be searched for checking. 2 types of log files are provided: client logs and server logs. The client logs refer to the log files of the client and are stored on the local PC; the server logs refer to the log files of the connected devices and are stored on the local device.

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



● Client Logs
○ Server Logs

Start Time: 2015-08-06 00:00:00

End Time: 2015-08-06 23:59:59

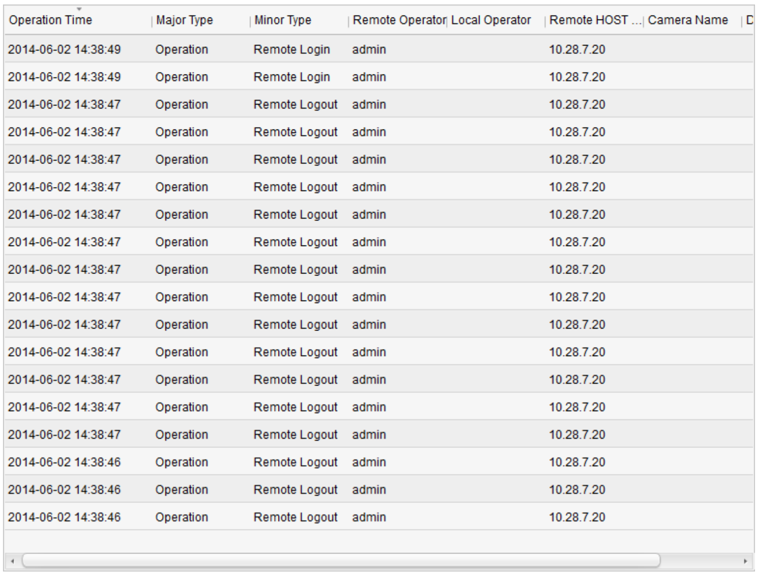
Total:0 Page:1/1 Item Per Page: Self-adaptive

Searching Log Files

Steps:

1. Open the Log Search page.
2. Select the log type. If **Server Logs** is selected, then click to specify the device for search.
3. Click the icon to specify the start time and end time.
4. Click **Search**. The log files between the start time and end time will be displayed on the list. You can check the operation time, type and other information of the logs.

Note: Please narrow the time range or filter the log type for search if there are too many log files.



Operation Time	Major Type	Minor Type	Remote Operator	Local Operator	Remote HOST ...	Camera Name	D
2014-06-02 14:38:49	Operation	Remote Login	admin		10.28.7.20		
2014-06-02 14:38:49	Operation	Remote Login	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:47	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:46	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:46	Operation	Remote Logout	admin		10.28.7.20		
2014-06-02 14:38:46	Operation	Remote Logout	admin		10.28.7.20		

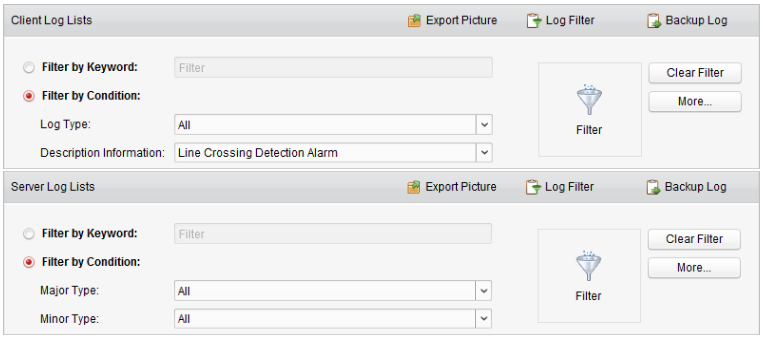
Filtering Log Files

Purpose:

After searched out successfully, the log files can be filtered by the keyword or condition, and thus you can find the logs as you want.

Steps:

1. Click **Log Filter** or the icon ▼ on the Log Search page to expand the Log Filter panel.
2. Select **Filter by Keyword**, and then input keyword for filtering in the text field.
   Or select **Filter by Condition**, and then specify log type in the drop-down list.
3. Optionally, you can click **More…** to filter the log files more accurately.
4. Click **Filter** to start filtering. You can click **Clear Filter** the cancel the filtering.



Client Log Lists

○ Filter by Keyword: Filter

● Filter by Condition:

Log Type: All

Description Information: Line Crossing Detection Alarm

Server Log Lists

○ Filter by Keyword: Filter

● Filter by Condition:

Major Type: All

Minor Type: All

Backing up Log Files

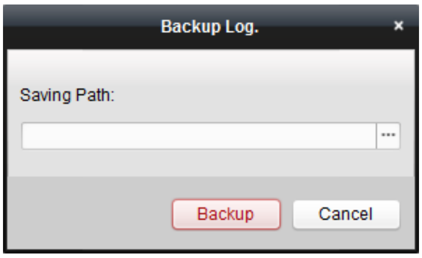
Purpose:

The log files, including the client logs and server logs, can be exported for backup.

Steps:

1. Set the condition and search the log file.
2. Click **Backup Log** to open the Backup Log dialog box.
3. Click the icon ..., select a local saving path and set a name for the file.
4. Click **Backup** to export the selected log file for backup.

You can click **File→Open Log File** to check the information of the backup log files on local PC.



Exporting Picture

Purpose:

The alarm pictures, which are stored in the storage server, can be exported to the local PC.

Steps:

1. Select the alarm pictures.
2. Click **Export Picture** to open the Export Picture dialog box.
3. Click the icon ···, select a local saving path and set a name for the file.
4. Click **Export** to export the selected pictures.

Chapter 16 Account Management and System Configuration

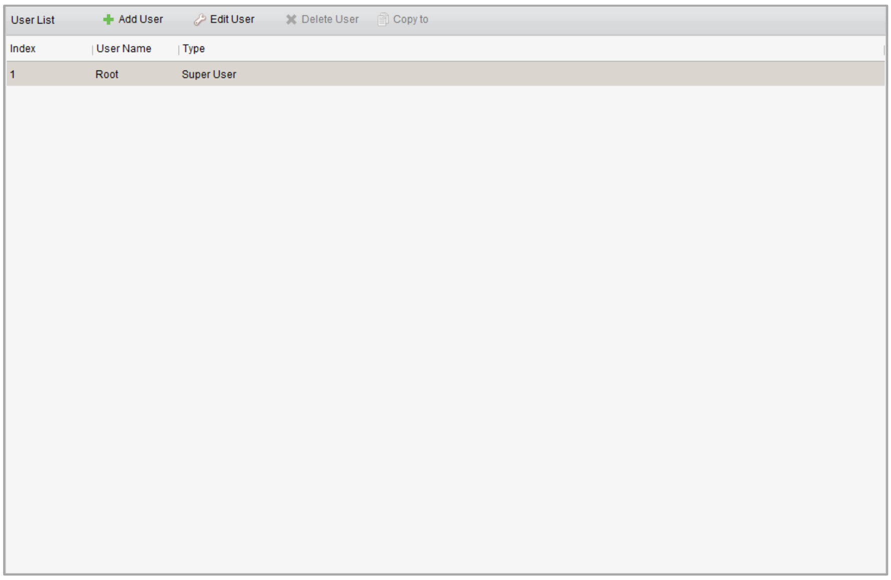
16.1 Account Management

Purpose:

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

Click the icon on the control panel,

or click **Tool**->**Account Management** to open the Account Management page.



Index	User Name	Type
1	Root	Super User

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

Adding the User

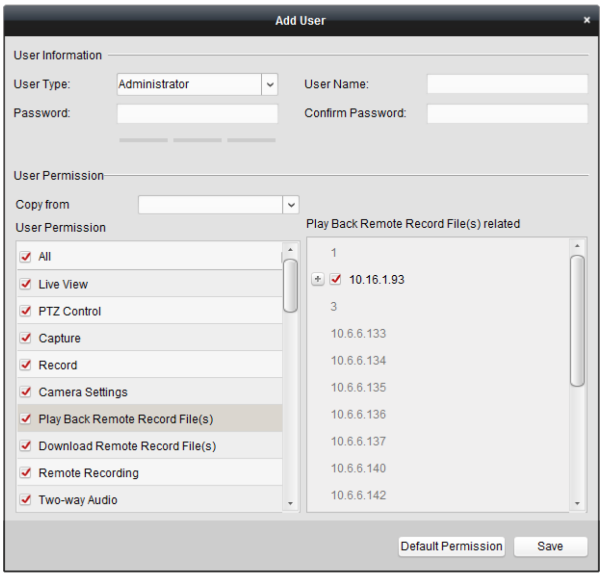
Steps:

1. Open the Account Management page.
2. Click **Add User** to open the Add User dialog box.
3. Select the user type from the drop-down list. 2 types of user accounts are selectable:
   Administrator: The administrator account has all permissions by default, and can modify the passwords and permissions of all operators and its own account.
   Operator: The operator account has no permission by default and you can assign the permissions manually. An operator can only modify the password of its own account.
4. Input the user name, password and confirm password as desired. The software will judge password strength automatically, and we highly recommend you to use a strong password to ensure your data security.
5. Check the checkboxes to assign the permissions for the created user. Optionally, you can select a user in the **Copy from** drop-down list, to copy the permissions of the selected user.

6. Optionally, you can click **Default Permission** to restore the default permissions of this user.
7. Click **Save** to save the settings.

- *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.*

Note: Up to 50 user accounts can be added for the client software.



Add User

User Information

User Type: Administrator

User Name:

Password:

Confirm Password:

User Permission

Copy from

User Permission

☑ All
☑ Live View
☑ PTZ Control
☑ Capture
☑ Record
☑ Camera Settings
☑ Play Back Remote Record File(s)
☑ Download Remote Record File(s)
☑ Remote Recording
☑ Two-way Audio

Play Back Remote Record File(s) related

1
☑ 10.16.1.93
3
10.6.6.133
10.6.6.134
10.6.6.135
10.6.6.136
10.6.6.137
10.6.6.140
10.6.6.142

Managing the User

Purpose:

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

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

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

For super and administrator user, you can click **Copy to** to copy the permissions to other user(s).

Note: The super user cannot be deleted and only the password of the super user can be edited.

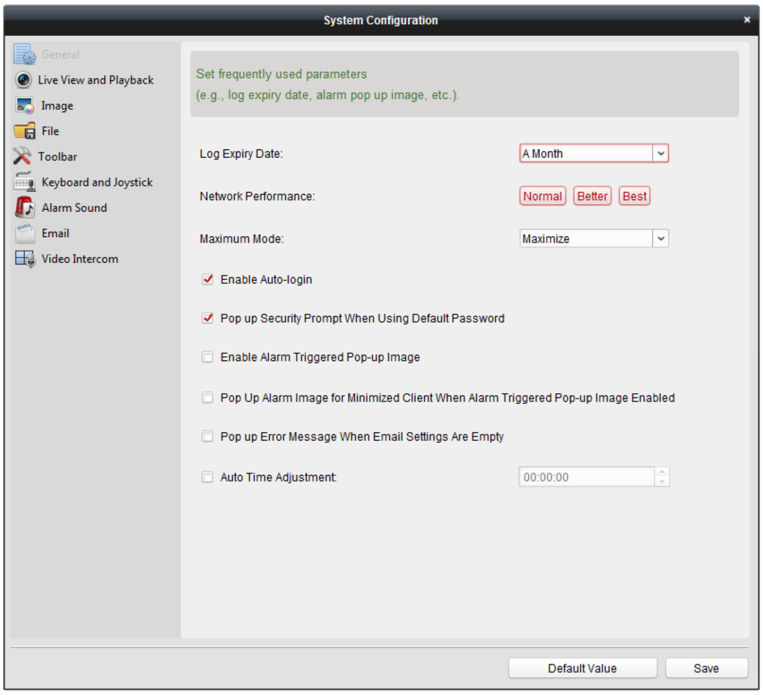
16.2 System Configuration

Purpose:

The general parameters, live view and playback parameters, image parameters, file saving paths, icon of live view and playback toolbar settings, keyboard and joystick shortcuts, alarm sounds, email settings and video intercom parameters can be configured.

Click the icon on the control panel,

or click **Tool**->**System Configuration** to open the System Configuration page.



Set frequently used parameters
(e.g., log expiry date, alarm pop up image, etc.).

Log Expiry Date: A Month

Network Performance: Normal Better Best

Maximum Mode: Maximize

☑ Enable Auto-login

☑ Pop up Security Prompt When Using Default Password

□ Enable Alarm Triggered Pop-up Image

□ Pop Up Alarm Image for Minimized Client When Alarm Triggered Pop-up Image Enabled

□ Pop up Error Message When Email Settings Are Empty

□ Auto Time Adjustment: 00:00:00

Note: You can click **Default Value** to restore the defaults of all the system configurations.

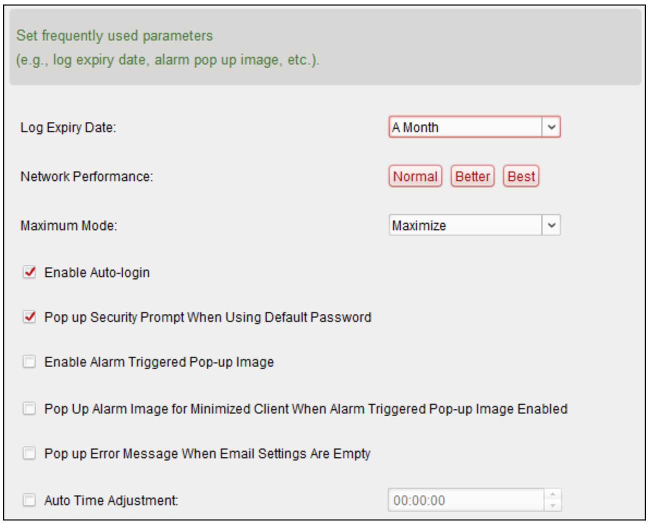
16.2.1 General Settings

Purpose:

The frequently-used parameters, including the log expired time, network performance, etc., can be set.

Steps:

1. Open the System Configuration page.
2. Click the **General** tab to enter the General Settings interface.
3. Configure the general parameters. For details, see *Table 17.1 General Parameters*.
4. Click **Save** to save the settings.



Set frequently used parameters
(e.g., log expiry date, alarm pop up image, etc.).

Log Expiry Date: A Month

Network Performance: Normal Better Best

Maximum Mode: Maximize

☑ Enable Auto-login

☑ Pop up Security Prompt When Using Default Password

□ Enable Alarm Triggered Pop-up Image

□ Pop Up Alarm Image for Minimized Client When Alarm Triggered Pop-up Image Enabled

□ Pop up Error Message When Email Settings Are Empty

□ Auto Time Adjustment 00:00:00

Table 16. 1 General Parameters

Parameters	Descriptions
Log Expiry Date	The time for keeping the log files, once exceeded, the files will be deleted.
Network Performance	The current network conditions. It can be set as Normal, Better or Best.
Maximum Mode	Select Maximize or Full Screen as the maximum mode. For selecting Maximize, the software will be maximized and the taskbar will display. For selecting Full Screen, the software will be displayed in full-screen mode.
Enable Auto-login	Log into the client software automatically.
Pop up Security Prompt When Using Default Password	If the default password of the added device has not been changed, the prompt will pop up for notification.
Enable Alarm Triggered Pop-up Image	Enable the image pop-up when alarms occur. You can also click or to enable/disable the image pop-up in Alarm Event interface.
Pop Up Alarm Image for Minimized Client When Alarm Triggered Pop-up Image Enabled	Enable the alarm image popping up when the client is minimized if the Alarm Triggered Pop-up Image function is enabled. For enabling the Alarm Triggered Pop-up Image, refer to *Chapter 6 Event Management*.
Pop Up Error Message When Email Settings Are Empty	Set whether the client prompts the error message if the email is not configured. For setting the email, refer to *Chapter 17.2.8 Email Settings*.
Auto Time Adjustment	Adjust the time automatically at a specified time point.

16.2.2 Live View and Playback Settings

Purpose:

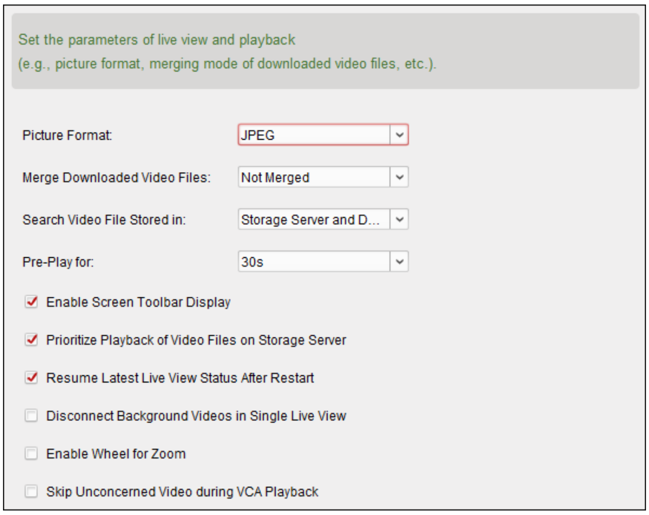
The parameters for live view and playback, including picture format, pre-play duration, etc., can be set.

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 17.2 Live View and Playback Parameters*.
4. Click **Save** to save the settings.



Set the parameters of live view and playback
(e.g., picture format, merging mode of downloaded video files, etc.).

Picture Format: JPEG

Merge Downloaded Video Files: Not Merged

Search Video File Stored in: Storage Server and D...

Pre-Play for: 30s

☑ Enable Screen Toolbar Display

☑ Prioritize Playback of Video Files on Storage Server

☑ Resume Latest Live View Status After Restart

☐ Disconnect Background Videos in Single Live View

☐ Enable Wheel for Zoom

☐ Skip Unconcerned Video during VCA Playback

Table 16. 2 Live View and Playback Parameters

Parameters	Descriptions
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. By default, it is 30s.
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.

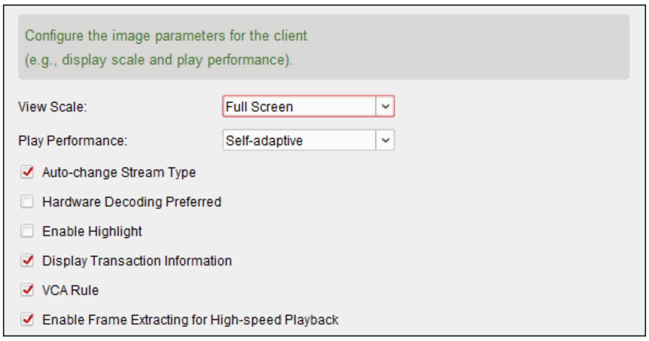
16.2.3 Image Settings

Purpose:

The image parameters of the software can be configured, such as view scale, play performance, etc.

Steps:

1. Open the System Configuration page.
2. Click the **Image** tab to enter the Image Settings interface.
3. Configure the image parameters. For details, see *Table 17.3 Image Parameters*.
4. Click **Save** to save the settings.



Configure the image parameters for the client
(e.g., display scale and play performance).

View Scale: Full Screen

Play Performance: Self-adaptive

☑ Auto-change Stream Type
□ Hardware Decoding Preferred
□ Enable Highlight
☑ Display Transaction Information
☑ VCA Rule
☑ Enable Frame Extracting for High-speed Playback

Table 16. 3 Image Parameters

Parameters	Descriptions
View Scale	The view scale of the video in live view or playback. It can be set as Full Screen, 4:3, 16:9 or Original Resolution.
Play Performance	The play performance of the live video. It can be set as Shortest Delay or Self-adaptive.
Auto-change Stream Type	Change the video stream (main stream or sub-stream) automatically in live view according to the size of the display window.
Hardware Decoding Preferred	Set to enable decoding by hardware for live view and playback. Hardware Decoding can provide better decoding performance and lower CPU usage when playing the HD videos during live view or playback.
Enable Highlight	Mark the detected objects with green rectangles in live view and playback.
Display Transaction Information	Display the transaction information in the live view.
VCA Rule	Display the VCA rule in the live view.
Enable Frame Extracting for High-speed Playback	When play back the video in high-speed (8x speed and above), you can disable this function to make the image of playback more fluent to view the details.

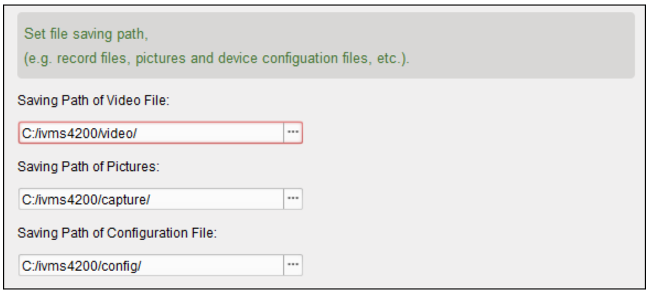
16.2.4 File Saving Path Settings

Purpose:

The video files from manual recording, the captured pictures and the system configuration files are stored on the local PC. The saving paths of these files can be set.

Steps:

1. Open the System Configuration page.
2. Click the **File** tab to enter the File Saving Path Settings interface.
3. Click the icon ··· and select a local path for the files.
4. Click **Save** to save the settings.



Set file saving path,
(e.g. record files, pictures and device configuation files, etc.).

Saving Path of Video File: C:/ivms4200/video/

Saving Path of Pictures: C:/ivms4200/capture/

Saving Path of Configuration File: C:/ivms4200/config/

16.2.5 Toolbar Settings

Purpose:

The icons and the order on the toolbar in the live view and playback window can be customized. You can set to display what icons and set the icon order.

Steps:

1. Open the System Configuration page.
2. Click the **Toolbar** tab to enter the Toolbar Settings interface.
3. Click to select the icon to display on the toolbar. You can drag the icon to set the icon order when displaying on the toolbar.

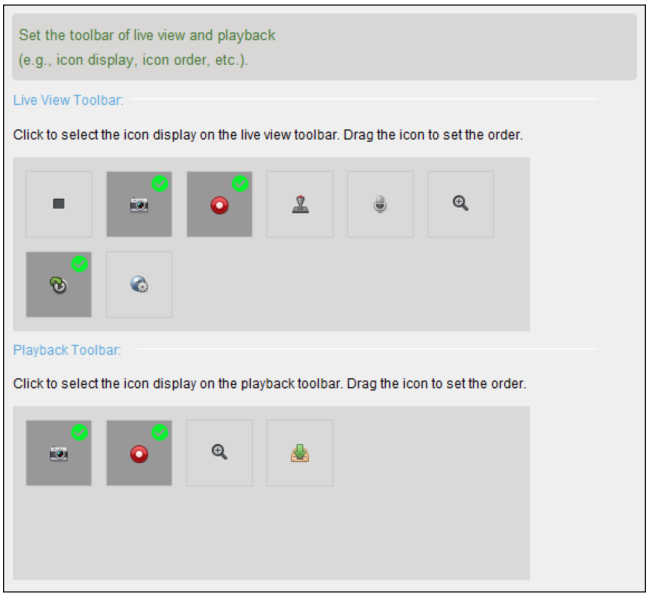
Icons on Live View Toolbar

Stop Live View	Stop the live view in the display window.
Capture	Capture the picture in the live view process. The capture picture is stored in the PC.
Record	Start manual recording. The video file is stored in the PC.
PTZ Control	Start PTZ mode for speed dome. Click and drag in the view to perform the PTZ control.
Two-way Audio	Start the two-way audio with the device in live view.
Digital Zoom	Enable the digital zoom function. Click again to disable the function.
Instant Playback	Switch to the instant playback mode.
Remote Configuration	Open the remote configuration page of the camera in live view.

Icons on Playback Toolbar

Capture	Capture the picture in the live view process. The capture picture is stored in the PC.
Record	Start manual recording. The video file is stored in the PC.
Digital Zoom	Enable the digital zoom function. Click again to disable the function.
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.

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



Set the toolbar of live view and playback (e.g., icon display, icon order, etc.).

Live View Toolbar:

Click to select the icon display on the live view toolbar. Drag the icon to set the order.

Playback Toolbar:

Click to select the icon display on the playback toolbar. Drag the icon to set the order.

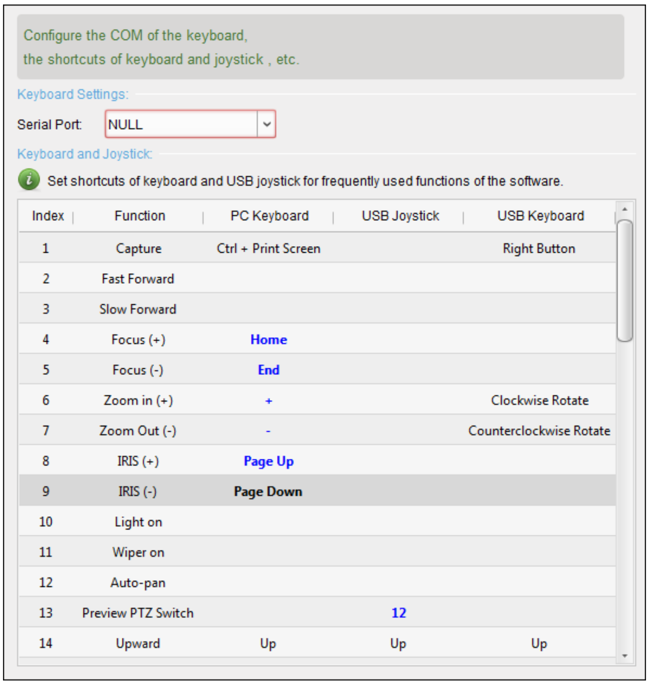
16.2.6 Keyboard and Joystick Shortcuts Settings

Purpose:

The keyboard can be connected to the client and be used to control the PTZ cameras. You can set the shortcuts for keyboard and joystick to get quick and convenient access to the commonly used actions.

Steps:

1. For keyboard: Select the COM port from the drop-down list if the keyboard is connected to the PC installed with the client.
2. For keyboard and joystick:
   1) Select a certain function from the list.
   2) Double-click the item field under the PC Keyboard, USB Joystick or USB Keyboard column.
   3) Select the compound keys operation or number from the drop-down list to set it as the shortcuts for the function of the keyboard or USB joystick.
3. Click **Save** to save the settings.



Configure the COM of the keyboard, the shortcuts of keyboard and joystick , etc.

Keyboard Settings:

Serial Port: NULL

Keyboard and Joystick:

Set shortcuts of keyboard and USB joystick for frequently used functions of the software.

Index	Function	PC Keyboard	USB Joystick	USB Keyboard
1	Capture	Ctrl + Print Screen		Right Button
2	Fast Forward			
3	Slow Forward			
4	Focus (+)	Home		
5	Focus (-)	End		
6	Zoom in (+)	+		Clockwise Rotate
7	Zoom Out (-)	-		Counterclockwise Rotate
8	IRIS (+)	Page Up		
9	IRIS (-)	Page Down		
10	Light on			
11	Wiper on			
12	Auto-pan			
13	Preview PTZ Switch		12	
14	Upward	Up	Up	Up

16.2.7 Alarm Sound Settings

Purpose:

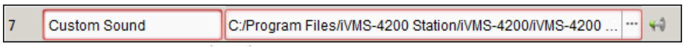
When the alarm, such as motion detection alarm, video exception alarm, etc., is triggered, the client can be set to give an audible warning and the sound of the audible warning can be configured.

Steps:

1. Open the System Configuration page.
2. Click the **Alarm Sound** tab to enter the Alarm Sound Settings interface.
3. There are six pre-defined alarm sound type in the list. You can click the icon … and select the audio files from the local path for different alarms.
4. You can also click **Add** button to add customized alarm sound.

   Double click the Type field to customize the alarm sound name as desired.

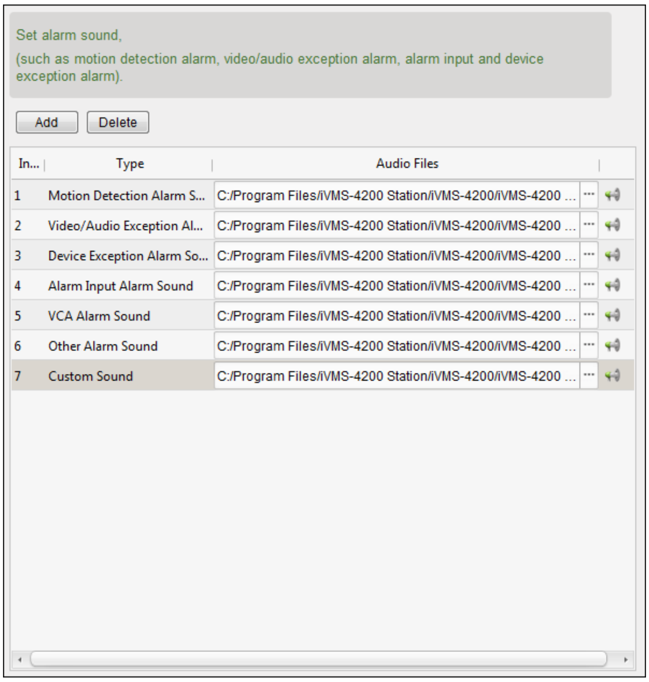
   Click the icon … and select the audio files from the local path for different alarms.



7	Custom Sound	C:/Program Files/iVMS-4200 Station/iVMS-4200/iVMS-4200 ...

5. Optionally, you can click the icon 🔈 for a testing of the audio file.
6. You can select the added custom alarm sound and click **Delete** to delete it.
7. Click **Save** to save the settings.

Note: The format of the audio file can only be *wav.



Set alarm sound,
(such as motion detection alarm, video/audio exception alarm, alarm input and device exception alarm).

In...	Type	Audio Files
1	Motion Detection Alarm S...	C:/Program Files/iVMS-4200 Station/iVMS-4200/iVMS-4200 ...
2	Video/Audio Exception Al...	C:/Program Files/iVMS-4200 Station/iVMS-4200/iVMS-4200 ...
3	Device Exception Alarm So...	C:/Program Files/iVMS-4200 Station/iVMS-4200/iVMS-4200 ...
4	Alarm Input Alarm Sound	C:/Program Files/iVMS-4200 Station/iVMS-4200/iVMS-4200 ...
5	VCA Alarm Sound	C:/Program Files/iVMS-4200 Station/iVMS-4200/iVMS-4200 ...
6	Other Alarm Sound	C:/Program Files/iVMS-4200 Station/iVMS-4200/iVMS-4200 ...
7	Custom Sound	C:/Program Files/iVMS-4200 Station/iVMS-4200/iVMS-4200 ...

16.2.8 Email Settings

Purpose:

An email notification can be sent when a system alarm occurs. To send the email to some specified receivers, the settings of the email need to be configured before proceeding.

Steps:

1. Open the System Configuration page.
2. Click the **Email** tab to enter the Email Settings interface.
3. Input the required information.

   Server Authentication (Optional): If your email server requires authentication, check this checkbox to use authentication to log into the server and enter the login user name and password of your email account.

   SMTP Server: Input the SMTP Server address.

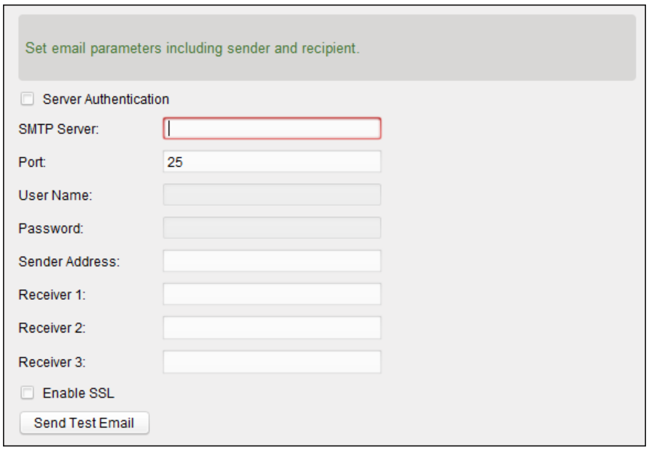
   Port: Input the communication port of email service. The port is 25 by default.

   User Name: Input the user name of the sender email address if **Server Authentication** is checked.

   Password: Input the password of the sender Email address if **Server Authentication** is checked.

   Sender Address: Input the email address of the sender.

   Receiver 1 to 3: Input the email address of the receiver. Up to 3 receivers can be set.
4. Optionally, you can check the checkbox **Enable SSL** to increase the security of email sending.
5. Optionally, you can click **Send Test Email** to send an email to the receiver for test.
6. Click **Save** to save the settings.



Set email parameters including sender and recipient.

☐ Server Authentication

SMTP Server:

Port: 25

User Name:

Password:

Sender Address:

Receiver 1:

Receiver 2:

Receiver 3:

☐ Enable SSL

16.2.9 Video Intercom Settings

Purpose:

You can configure the video intercom parameters accordingly.

Steps:

1. Open the System Configuration page.
2. Click the **Video Intercom** tab to enter the Video Intercom Settings interface.
3. Input the required information.

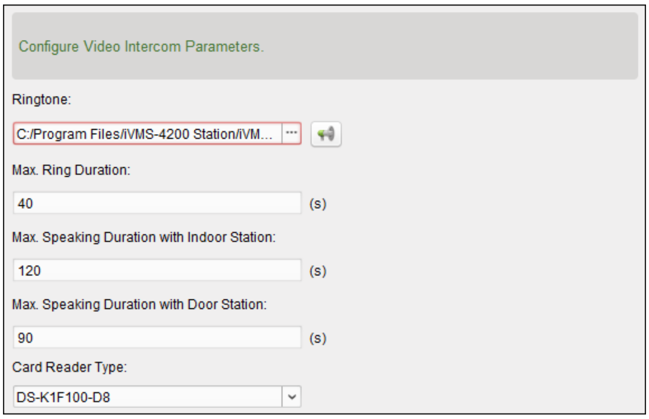
   Ringtone: Click the icon ⋯ and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click the icon 📢 for a testing of the audio file.

   Max. Ring Duration: Input the maximum duration of the ringtone.

   Max. Speaking Duration with Indoor Station: Input the maximum duration of speaking with the indoor station.

   Max. Speaking Duration with Door Station: Input the maximum duration of speaking with the door station.
4. Select the card reader mode in the dropdown list according to the connected card reader type for reading the card information when adding the card.

   Currently, the supported card reader models include: DS-K1F100-D8 and DS-K1F100-D8E.
5. Click **Save** to save the settings.



Configure Video Intercom Parameters.

Ringtone: C:/Program Files/iVMS-4200 Station/iVM...

Max. Ring Duration: 40 (s)

Max. Speaking Duration with Indoor Station: 120 (s)

Max. Speaking Duration with Door Station: 90 (s)

Card Reader Type: DS-K1F100-D8

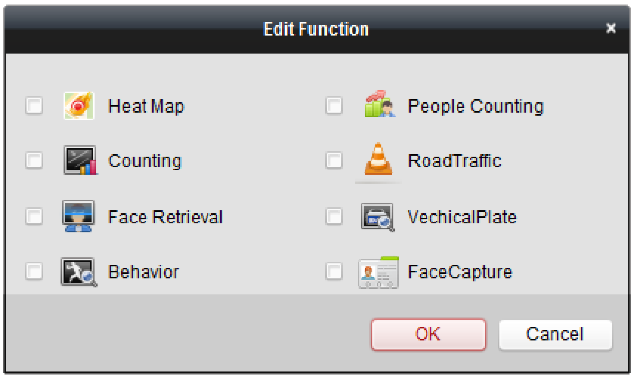
Chapter 17 Statistics

Purpose:

In Statistics, it provides eight modules for data statistics via the software: Heat Map, People Counting, Counting, Road Traffic, Face Retrieval, License Plate Retrieval, Behavior Analysis, and Face Capture.

Click the icon on the control panel to open the Edit Function page to select the statistics functions.

Check the modules checkboxes and click **OK** to list the selected modules on the control panel.



The Heat Map module provides the display of the heat map statistics.

The People Counting module provides the display of the people counting statistics.

The Counting module provides the display of the counting statistics.

The Road Traffic module provides the display of the road traffic data.

Face Retrieval module provides the query of the picture of face.

License Plate Retrieval module provides the query of the license plate number.

Behavior Analysis module provides the query of behavior analysis.

Face Capture module provides the data search and statistics for captured faces pictures.

17.1 Heat Map

Purpose:

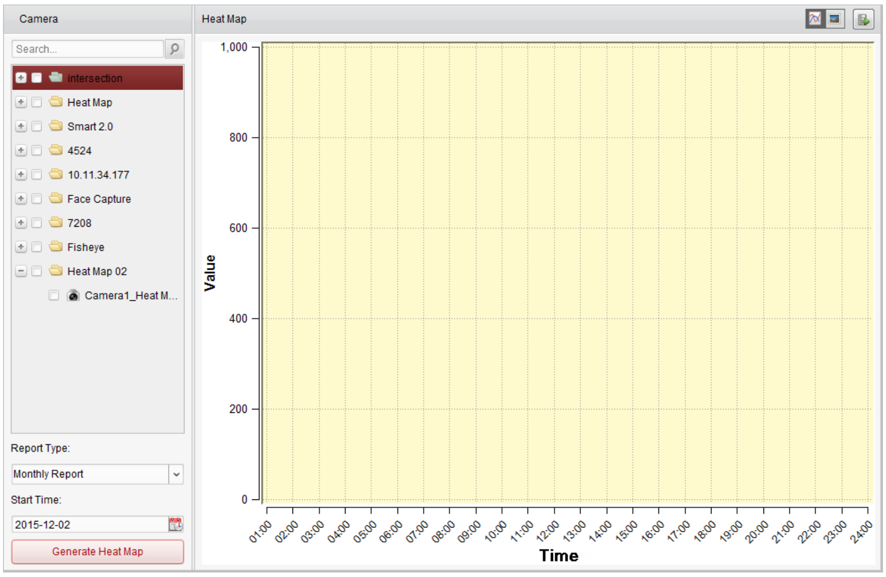
Heat map is a graphical representation of data represented by colors or the heat map data can be displayed in line chart. The heat map function of the camera usually be used to analyze the visit times and dwell time of customers in a configured area.

Before you start:

Please add a heat map network camera to the software and properly configure the corresponding area. The added camera should have been configured with heat map rule.

Note: The heat map network camera should be added to the software as Encoding Device, please refer to *Chapter 3.1 Adding the Device* for detailed configuration. For configuring heat map rule, please refer to the *User Manual* of the heat map network camera.

Click the icon on the control panel to open the Heat Map page.



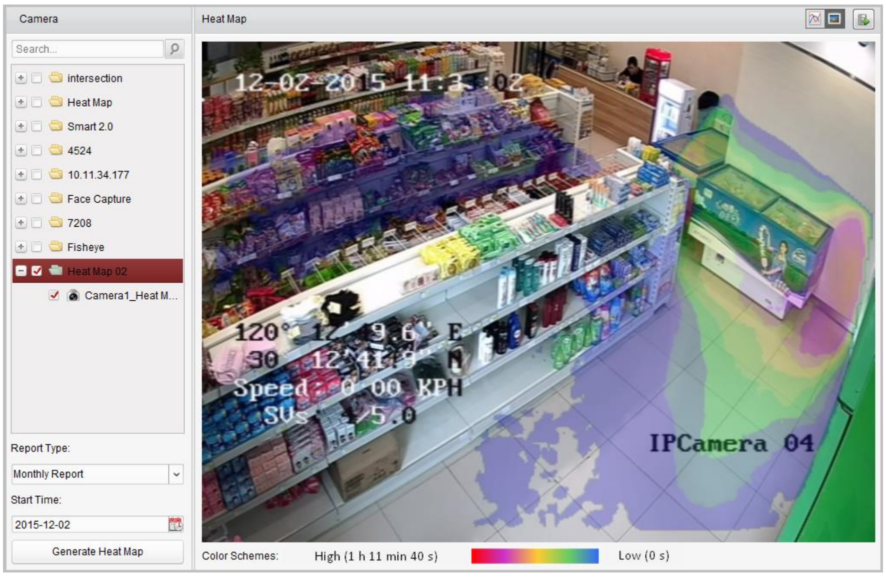
Report Type: Monthly Report

Start Time: 2015-12-02

Steps:

1. Open the Heat Map page.
2. Click to select a heat map camera in the area panel.
3. Select the report type as needed and set the start time.
4. Click **Generate Heat Map** and the heat map of the camera displays. You can click or to display the statistics in line chart or picture mode.

   In picture mode, the red color block (255, 0, 0) indicates the most welcome area, and blue color block (0, 0, 255) indicates the less-popular area.
5. (Optional) Click to save the detailed data of heat map to your PC.



Report Type: Monthly Report

Start Time: 2015-12-02

Color Schemes: High (1 h 11 min 40 s) Low (0 s)

17.2 People Counting Statistics

Purpose:

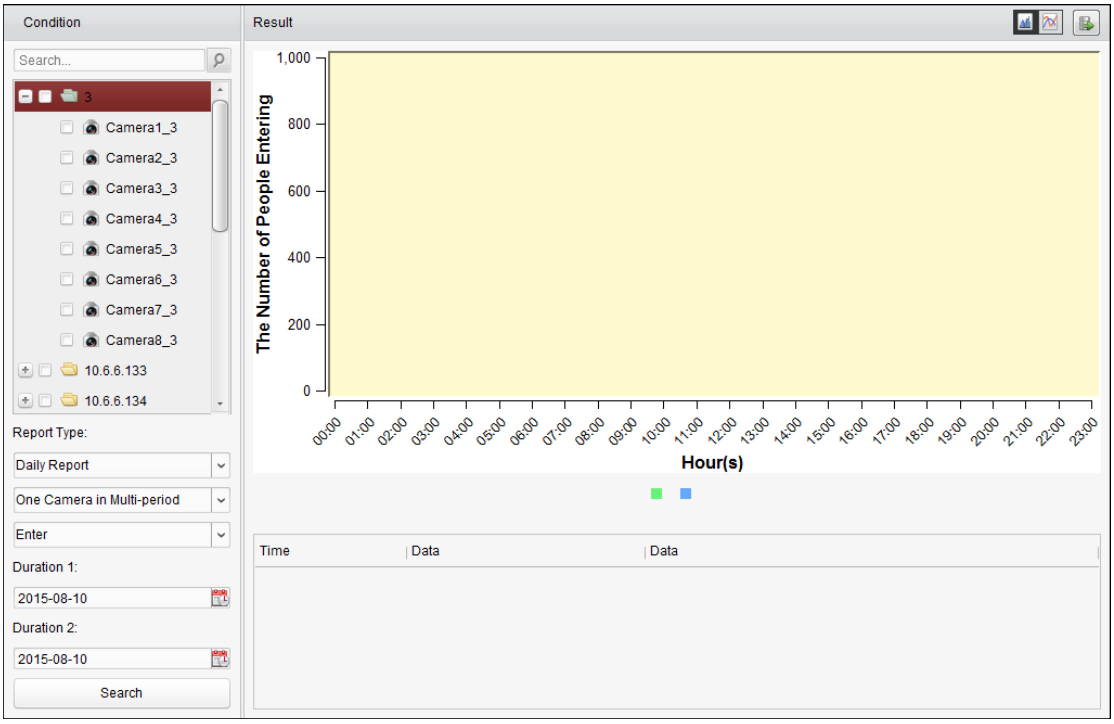
You can check the people counting statistics of the added people counting device and the statistics can be displayed in line chart or histogram. The detailed data can be exported for local storage.

Before you start:

Please add a people counting device to the software and properly configure the corresponding area. The added device should have been configured with people counting rule.

Note: The people counting device should be added to the software as Encoding Device, please refer to *Chapter 3.1 Adding the Device* for detailed configuration. For configuring people counting rule, please refer to the *User Manual* of the people counting device.

Click the icon on the control panel to open the People Counting page.



Steps:

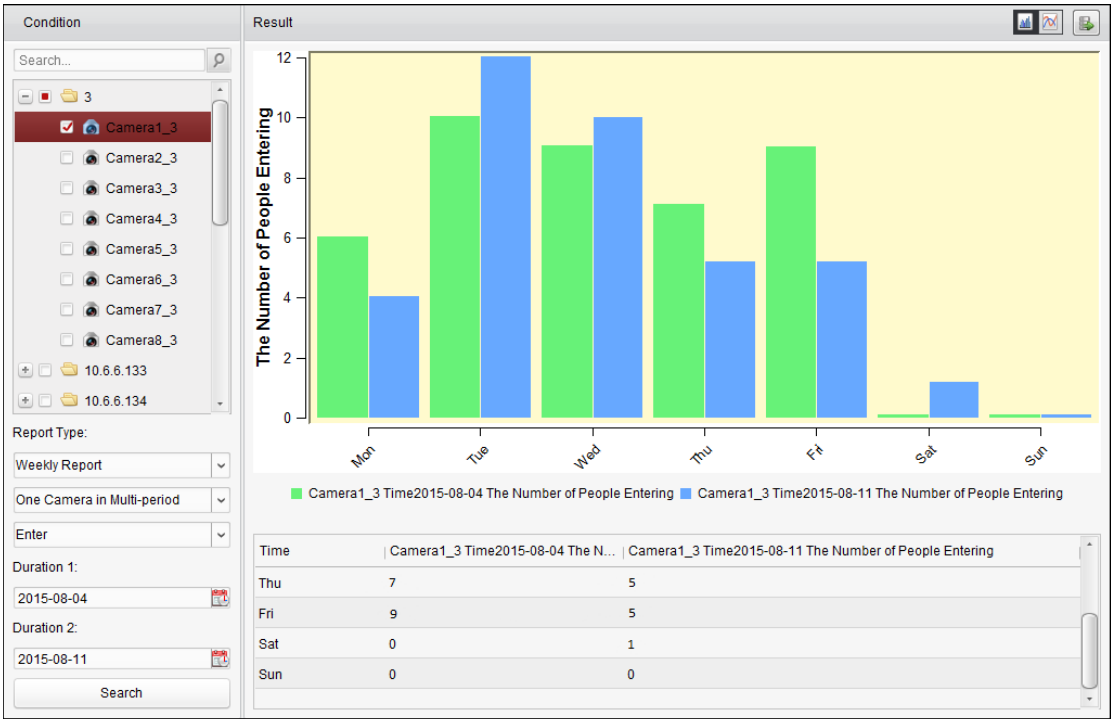
1. Open the People Counting page.
2. Select the report type as needed and set the time.
   1) Select daily report, weekly report, monthly report or annual report as the time type for the report.
   2) Select One Camera in Multi-period or One Camera in One Period as the statistics type.
      - **One Camera in Multi-period:** One camera can be selected for generating the statistics for it of the two time periods.
      - **One Camera in One Period:** One camera can be selected for generating the statistics for it of one time period.
   3) Select Enter, Exit, or Enter and Exit as the data type.
      - **Enter:** The people entered will be counted.
      - **Exit:** The people exited will be counted.

- **Enter and Exit:** Both people entered and exited will be counted.

4) Set the time period(s).

3. Select the camera for generating the report.
4. Click **Search** and the statistics displays on the right panel. The detailed data for each hour, day or month will be also displayed.

   By default, the statistics are shown in histogram form. You can switch it to line chart by clicking the .
5. (Optional) Click to save the detailed data of people counting to your PC.



Report Type:

Weekly Report

One Camera in Multi-period

Enter

Duration 1:

2015-08-04

Duration 2:

2015-08-11

Time	Camera1_3 Time2015-08-04 The N...	Camera1_3 Time2015-08-11 The Number of People Entering
Thu	7	5
Fri	9	5
Sat	0	1
Sun	0	0

17.3 Counting Statistics

Purpose:

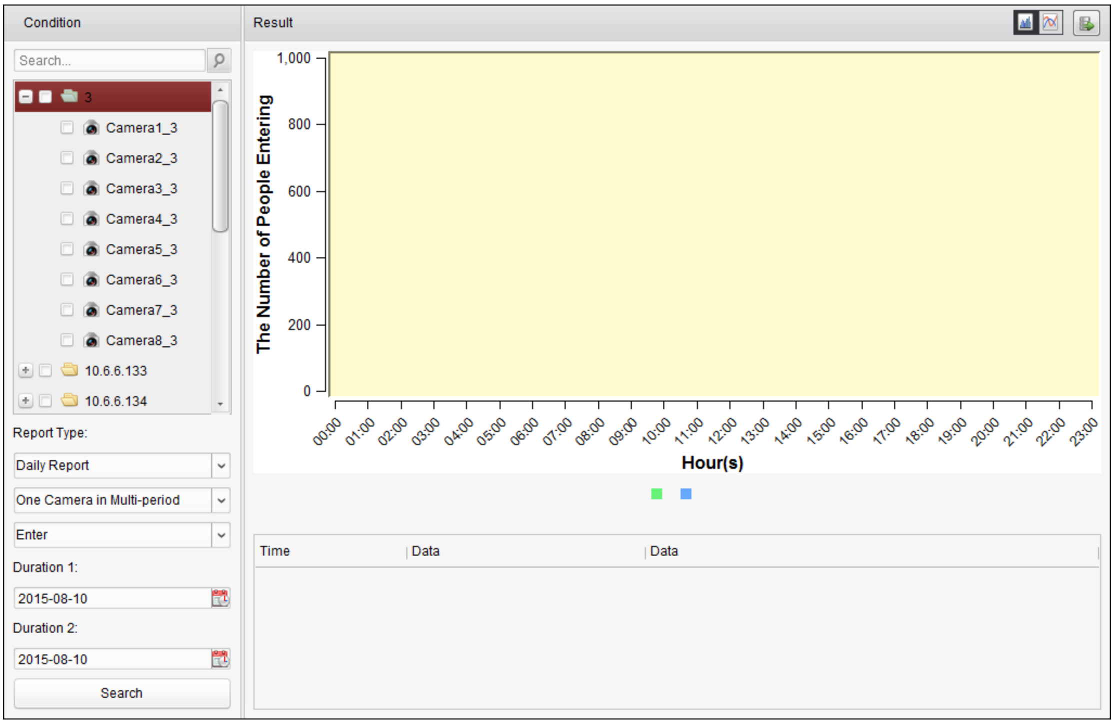
You can check the counting statistics of the added counting device and the statistics can be displayed in line chart or histogram. The detailed data can be exported for local storage.

Before you start:

Please add a counting device to the software and properly configure the corresponding area. The added device should have been configured with counting settings.

Note: The counting device should be added to the software as Encoding Device, please refer to *Chapter 3.1 Adding the Device* for detailed configuration. For configuring counting settings, please refer to the *User Manual* of the counting device.

Click the icon on the control panel to open the Counting page.



Report Type: Daily Report

One Camera in Multi-period

Enter

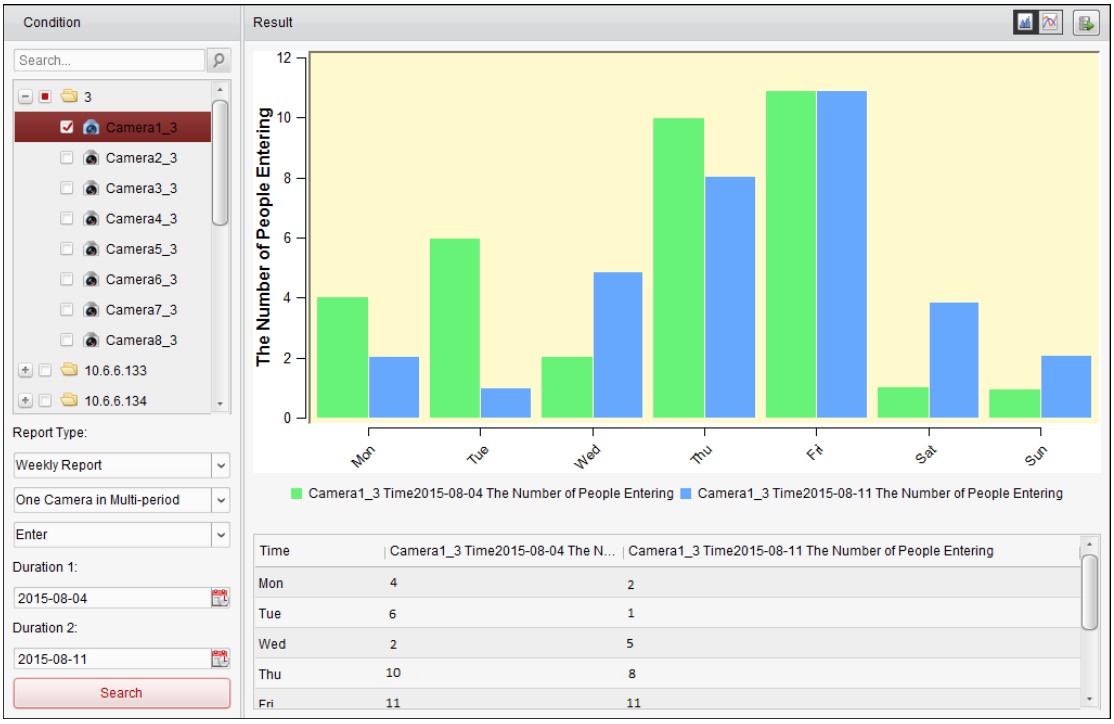
Duration 1: 2015-08-10

Duration 2: 2015-08-10

Steps:

1. Open the Counting page.
2. Select the report type as needed and set the time.
    1) Select daily report, weekly report, monthly report or annual report as the time type for the report.
    2) Select One Camera in Multi-period or One Camera in One Period as the statistics type.
        - **One Camera in Multi-period:** One camera can be selected for generating the statistics for it of the two time periods.
        - **One Camera in One Period:** One camera can be selected for generating the statistics for it of one time period.
    3) Select Enter, Exit, or Enter and Exit as the data type.
        - **Enter:** The people entered will be counted.
        - **Exit:** The people exited will be counted.
        - **Enter and Exit:** Both people entered and exited will be counted.
    4) Set the time period(s).
3. Select the camera for generating the report.
4. Click **Search** and the statistics displays on the right panel. The detailed data for each hour, day or month will be also displayed.

   By default, the statistics are shown in histogram form. You can switch it to line chart by clicking the 📈.
5. (Optional) Click 📤 to save the detailed data of counting to your PC.



Report Type:

Weekly Report

One Camera in Multi-period

Enter

Duration 1:

2015-08-04

Duration 2:

2015-08-11

Time	Camera1_3 Time2015-08-04 The N...	Camera1_3 Time2015-08-11 The Number of People Entering
Mon	4	2
Tue	6	1
Wed	2	5
Thu	10	8
Fri	11	11

17.4 Road Traffic

Purpose:

If you add road traffic monitoring device, the captured pictures of the detected vehicle or license plate can be searched and checked. Three types are available for searching the corresponding pictures.

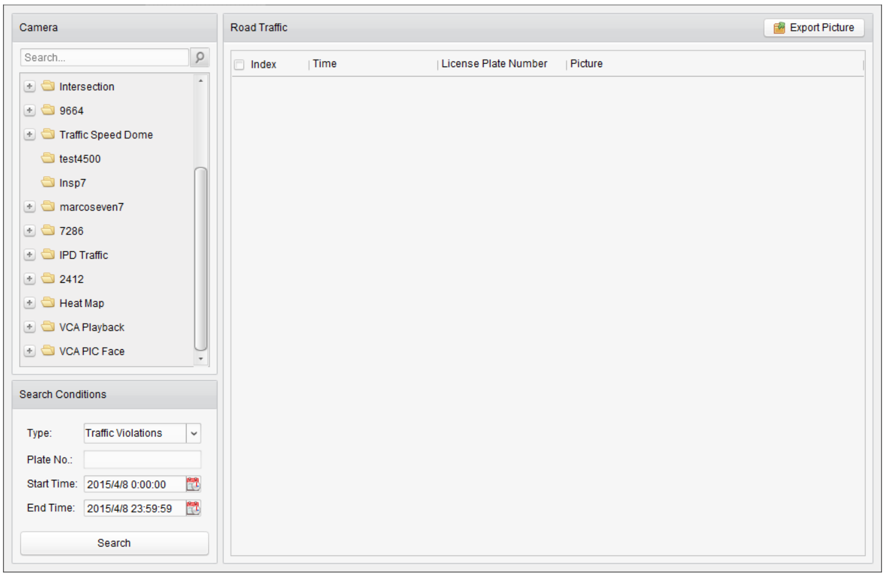
- **Vehicle Detection:** The passed vehicle can be detected and the picture of its license plate can be captured; besides, the vehicle color, vehicle logo and other information can be recognized automatically.
- **Mixed-traffic Detection:** The pedestrian, motor vehicle and non-motor vehicle can be detected, and the picture of the object (for pedestrian/non-motor vehicle/motor vehicle without license plate) or license plate (for motor vehicle with license plate) can be searched.
- **Traffic Violations:** The captured pictures of the vehicle that violates the traffic rules (such as illegal parking and congestion) can be checked.

Before you start:

1. Please add a road traffic monitoring device to the software and properly configure the corresponding area. The added device should have been configured with corresponding settings for capturing pictures.
2. For Traffic Violations, the Storage Server should be added to software and you must configure the Storage Server for the device and check the checkbox of **Picture Storage** and **Additional Information Storage**. For details, please refer to *Chapter 5.1.2 Storing on Storage Device*.
3. For Vehicle Detection and Mixed-traffic Detection, if no storage server is configured, the software will search the related pictures from the storage device of the local device.

Note: The road traffic monitoring device should be added to the software as Encoding Device, please refer to *Chapter 3.1 Adding the Device* for detailed configuration. For configuring capture settings, please refer to the *User Manual* of the device.

Click the icon on the control panel to open the Road Traffic page.



Camera

Search...

- Intersection
- 9664
- Traffic Speed Dome
- test4500
- Insp7
- marcoseven7
- 7286
- IPD Traffic
- 2412
- Heat Map
- VCA Playback
- VCA PIC Face

Search Conditions

Type: Traffic Violations

Plate No.:

Start Time: 2015/4/8 0:00:00

End Time: 2015/4/8 23:59:59

Search

Road Traffic

Export Picture

☐ Index	Time	License Plate Number	Picture

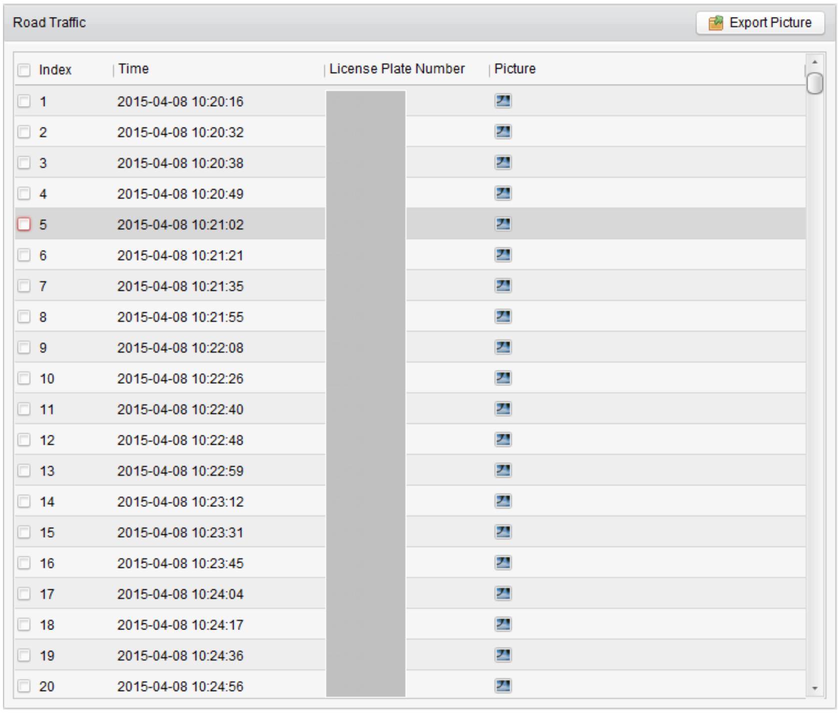
Steps:

1. Open the Road Traffic page.
2. Click to select a road traffic monitoring camera in the camera panel.
3. Set the search condition for finding the related pictures.

   Type: Select the query type and the pictures triggered by the event type can be found.

   Plate No.: Input the license plate number for searching the pictures.

   Start Time/End Time: Click to set the start time and end time.
4. Click **Search** and the found picture items will list.



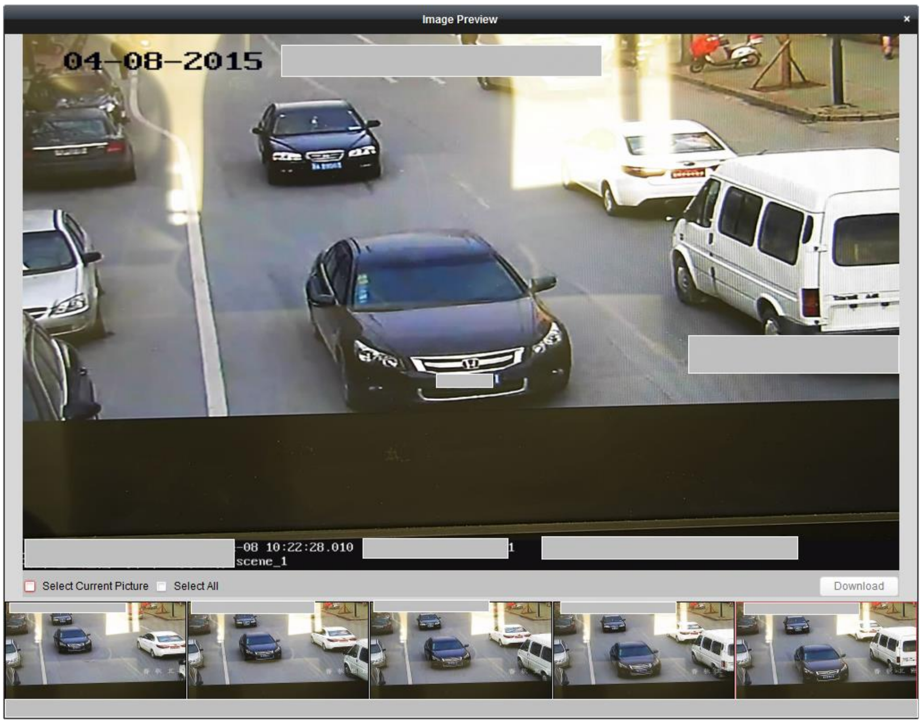
Road Traffic

Export Picture

☐ Index	Time	License Plate Number	Picture
☐ 1	2015-04-08 10:20:16	[redacted]	🖼
☐ 2	2015-04-08 10:20:32	[redacted]	🖼
☐ 3	2015-04-08 10:20:38	[redacted]	🖼
☐ 4	2015-04-08 10:20:49	[redacted]	🖼
☐ 5	2015-04-08 10:21:02	[redacted]	🖼
☐ 6	2015-04-08 10:21:21	[redacted]	🖼
☐ 7	2015-04-08 10:21:35	[redacted]	🖼
☐ 8	2015-04-08 10:21:55	[redacted]	🖼
☐ 9	2015-04-08 10:22:08	[redacted]	🖼
☐ 10	2015-04-08 10:22:26	[redacted]	🖼
☐ 11	2015-04-08 10:22:40	[redacted]	🖼
☐ 12	2015-04-08 10:22:48	[redacted]	🖼
☐ 13	2015-04-08 10:22:59	[redacted]	🖼
☐ 14	2015-04-08 10:23:12	[redacted]	🖼
☐ 15	2015-04-08 10:23:31	[redacted]	🖼
☐ 16	2015-04-08 10:23:45	[redacted]	🖼
☐ 17	2015-04-08 10:24:04	[redacted]	🖼
☐ 18	2015-04-08 10:24:17	[redacted]	🖼
☐ 19	2015-04-08 10:24:36	[redacted]	🖼
☐ 20	2015-04-08 10:24:56	[redacted]	🖼

5. Click to view the captured pictures and the related information. You can check the

checkbox of **Select Current Picture** or **Select All** and click **Download** to save the pictures to your PC.



6. (Optional) Check the checkbox(es) to select the picture items and click **Export Picture** to save the pictures to your PC.

17.5 Face Retrieval

Purpose:

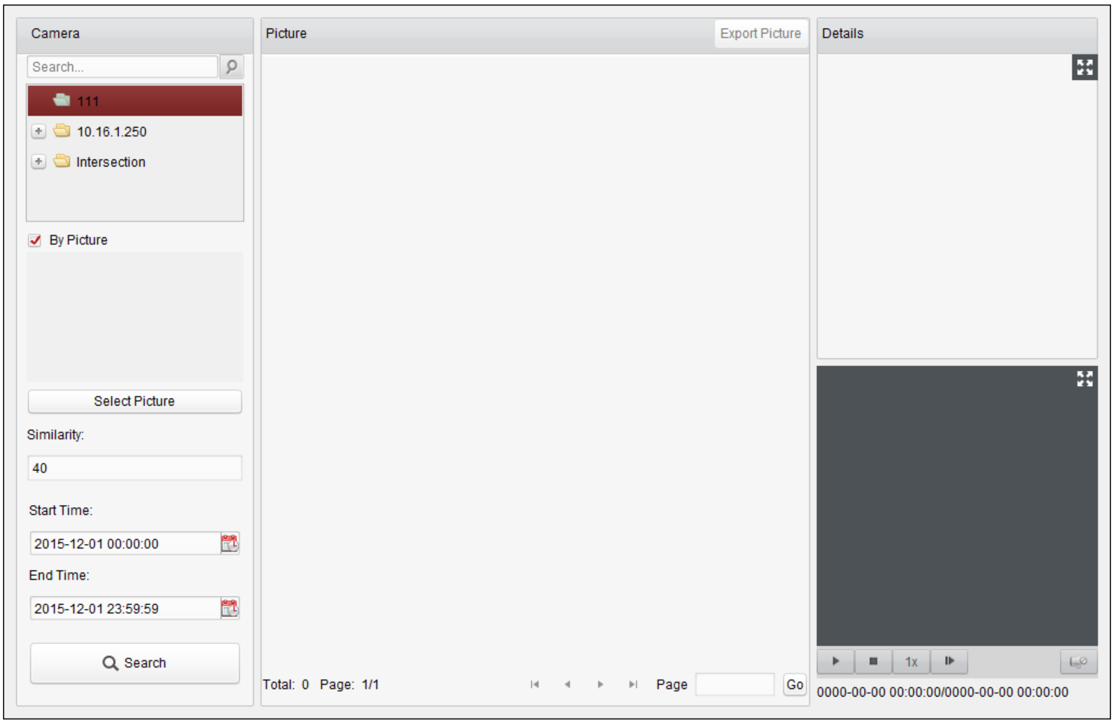
When the connected device (NVR or HDVR) supports face search, you can search the related picture and play the picture related video file.

Before you start:

Please add the device to the software and properly configure the corresponding settings. For detailed settings, please refer to the *User Manual* of the device.

Note: The device should be added to the software as Encoding Device, please refer to *Chapter 3.1 Adding the Device* for detailed configuration.

Click the icon on the control panel to open the Face Retrieval page.



Similarity: 40

Start Time: 2015-12-01 00:00:00

End Time: 2015-12-01 23:59:59

Total: 0 Page: 1/1

0000-00-00 00:00:00/0000-00-00 00:00:00

Steps:

1. Open the Face Retrieval page.
2. Click to select a device in the camera panel.

   Note: This function should be supported by the connected device (NVR or HDVR).
3. Set the corresponding search condition.
   - (Optional) You can check the checkbox of **By Picture**, click **Select Picture** to upload the pictures from your PC and click to select a detected face from uploaded picture for matching the captured face pictures.
   - Set the similarity level.

     Example: If you set the similarity as 40, the captured pictures have no less than 40% similarity with the uploaded face picture will list.
   - Click 📅 to set the start time and end time for searching the captured face pictures or video files.
4. Click **Search** to start searching. The search results of the pictures are displayed in list.
5. You can click on a picture from the list to check the detailed information.

   You can click ⛶ to show the large picture, and click ⛶ to restore.
6. To save the pictures to your PC:
   1) Click **Export Picture** and check the checkboxes to select the pictures to export. You can also click **Select All** to choose all the searched pictures.
   2) Click **Export**, and select a local saving path for the pictures.
   3) Click **Back** to leave the picture export mode.
7. Click ▶ to play the picture's related video file in the view window on the bottom right.

   You can click ⛶ to show the large video, and click ⛶ to restore.

   You can click 1x to adjust the play speed of the playback, click ▶| to play back the video files frame by frame, click 🔇 to enable the audio, double-click the playback window to maximize the window.

17.6 License Plate Retrieval

Purpose:

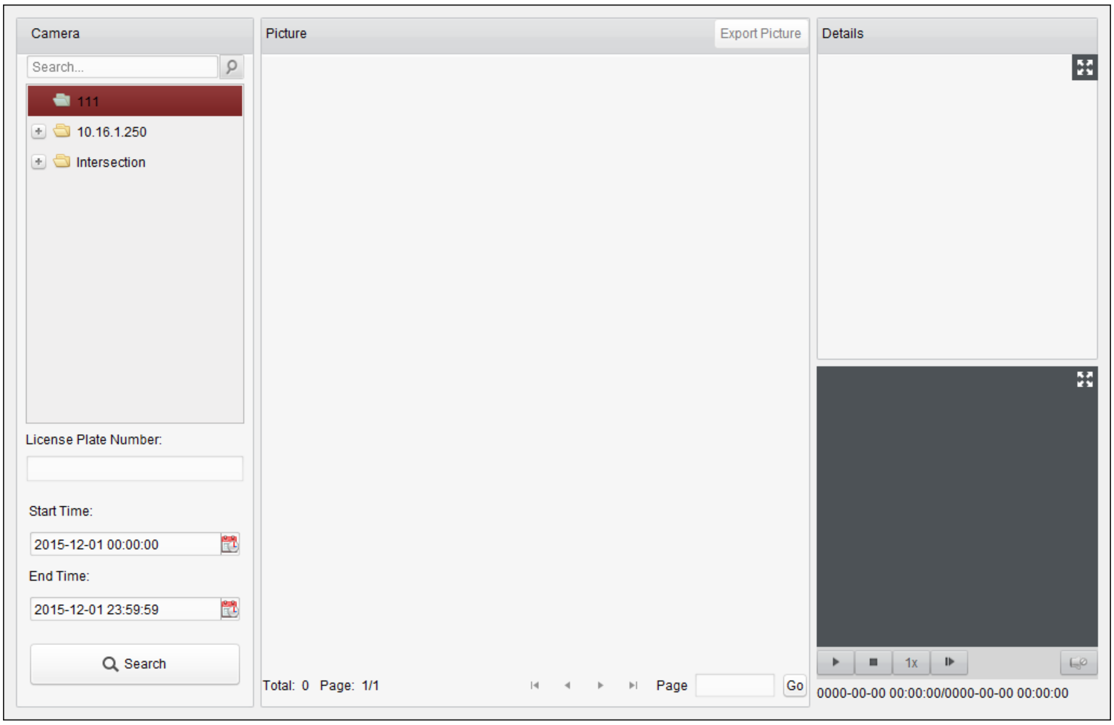
When the connected device (NVR or HDVR) supports license plate search, you can search the related picture and play the picture related video file.

Before you start:

Please add the device to the software and properly configure the corresponding settings. For detailed settings, please refer to the *User Manual* of the device.

Note: The device should be added to the software as Encoding Device, please refer to *Chapter 3.1 Adding the Device* for detailed configuration.

Click the icon on the control panel to open the License Plate Retrieval page.



Start Time: 2015-12-01 00:00:00

End Time: 2015-12-01 23:59:59

Steps:

1. Open the License Plate Retrieval page.
2. Click to select a device in the camera panel.

   Note: This function should be supported by the connected device (NVR or HDVR).
3. Set the corresponding search condition.
   - (Optional) Input the license plate number in the field for search.
   - Click to set the start time and end time for searching the matched license plate pictures.
4. Click **Search** to start searching. The search results of the pictures are displayed in list.
5. You can click on a picture from the list to check the detailed information.

   You can click to show the large picture, and click to restore.
6. To save the pictures to your PC:

   1) Click **Export Picture** and check the checkboxes to select the pictures to export. You can also click **Select All** to choose all the searched pictures.

2) Click **Export**, and select a local saving path for the pictures.

3) Click **Back** to leave the picture export mode.

7. You can click ▶ to play the picture's related video file in the view window on the bottom right. You can click ⛶ to show the large video, and click ⛶ to restore.
   You can click 1x to adjust the play speed of the playback, click ▶ to play back the video files frame by frame, click 🔊 to enable the audio, double-click the playback window to maximize the window.

17.7 Behavior Analysis

Purpose:

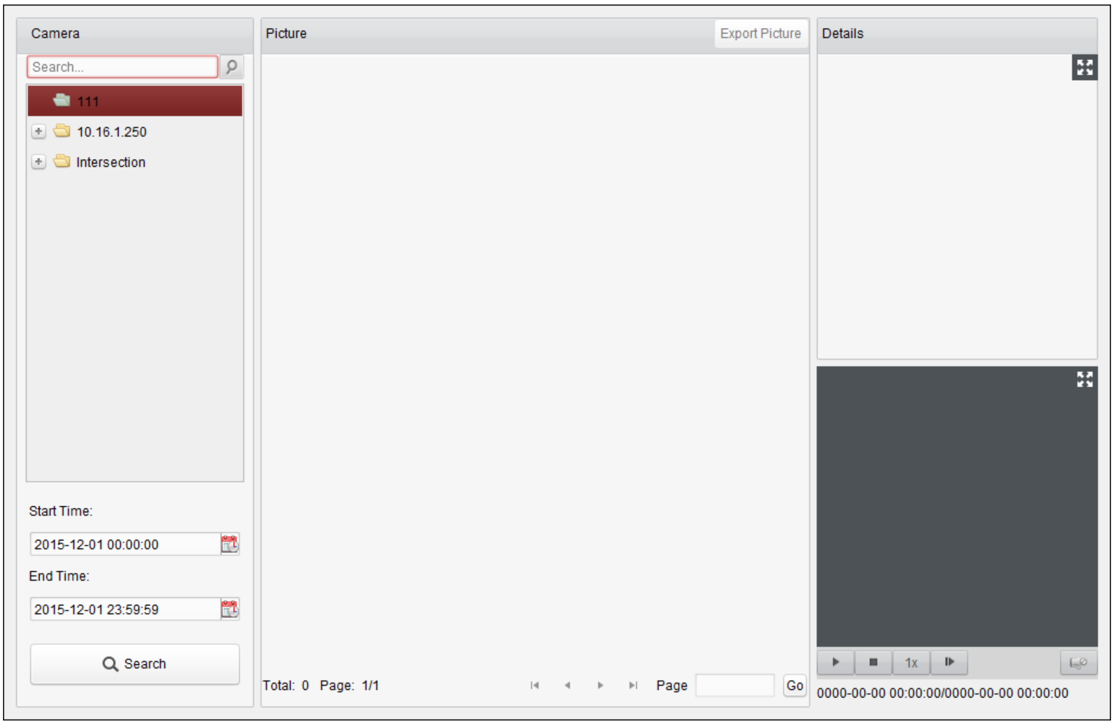
When the connected device (NVR or HDVR) supports behavior search, you can search the related picture and play the picture related video file.

Before you start:

Please add the device to the software and properly configure the corresponding settings. For detailed settings, please refer to the *User Manual* of the device.

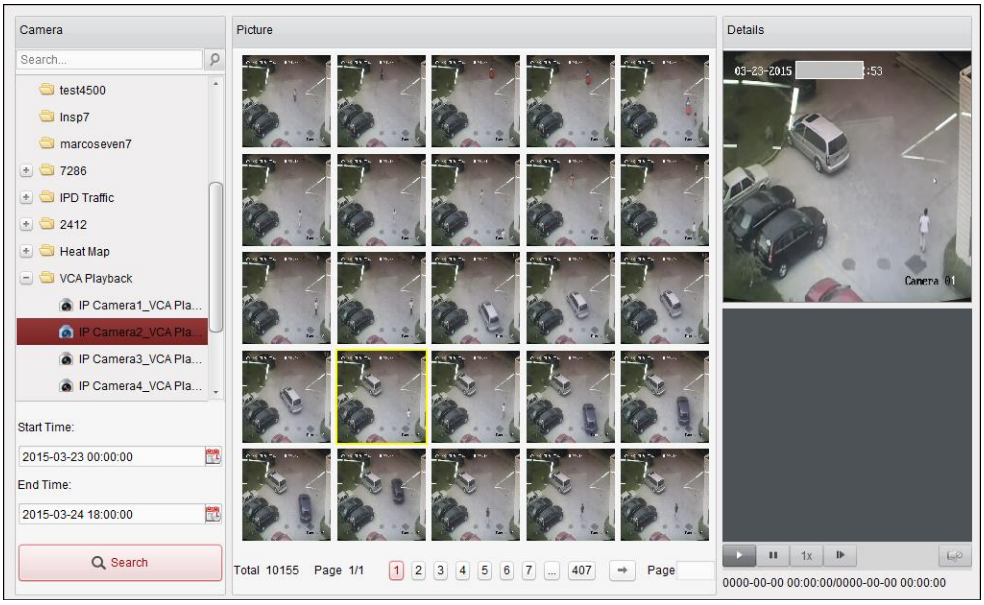
Note: The device should be added to the software as Encoding Device, please refer to *Chapter 3.1 Adding the Device* for detailed configuration.

Click the icon on the control panel to open the Behavior Analysis page.



Steps:

1. Open the Behavior Analysis page.
2. Click to select a device in the camera panel.
   Note: This function should be supported by the connected device (NVR or HDVR).
3. Click 📅 to set the start time and end time for searching the matched pictures.
4. Click **Search** to start searching. The search results of the pictures are displayed in list.



Start Time: 2015-03-23 00:00:00

End Time: 2015-03-24 18:00:00

Total 10155 Page 1/1 1 2 3 4 5 6 7 ... 407

0000-00-00 00:00:00/0000-00-00 00:00:00

5. You can click on a picture from the list to check the detailed information.

   You can click ⛶ to show the large picture, and click ⛶ to restore.

6. To save the pictures to your PC:

   1) Click **Export Picture** and check the checkboxes to select the pictures to export. You can also click **Select All** to choose all the searched pictures.

   2) Click **Export**, and select a local saving path for the pictures.

   3) Click **Back** to leave the picture export mode.

7. Click ▶ to play the picture's related video file in the view window on the bottom right.

   You can click ⛶ to show the large video, and click ⛶ to restore.

   You can click 1x to adjust the play speed of the playback, click ▶ to play back the video files frame by frame, click 🔇 to enable the audio, double-click the playback window to maximize the window.

17.8 Face Capture

Purpose:

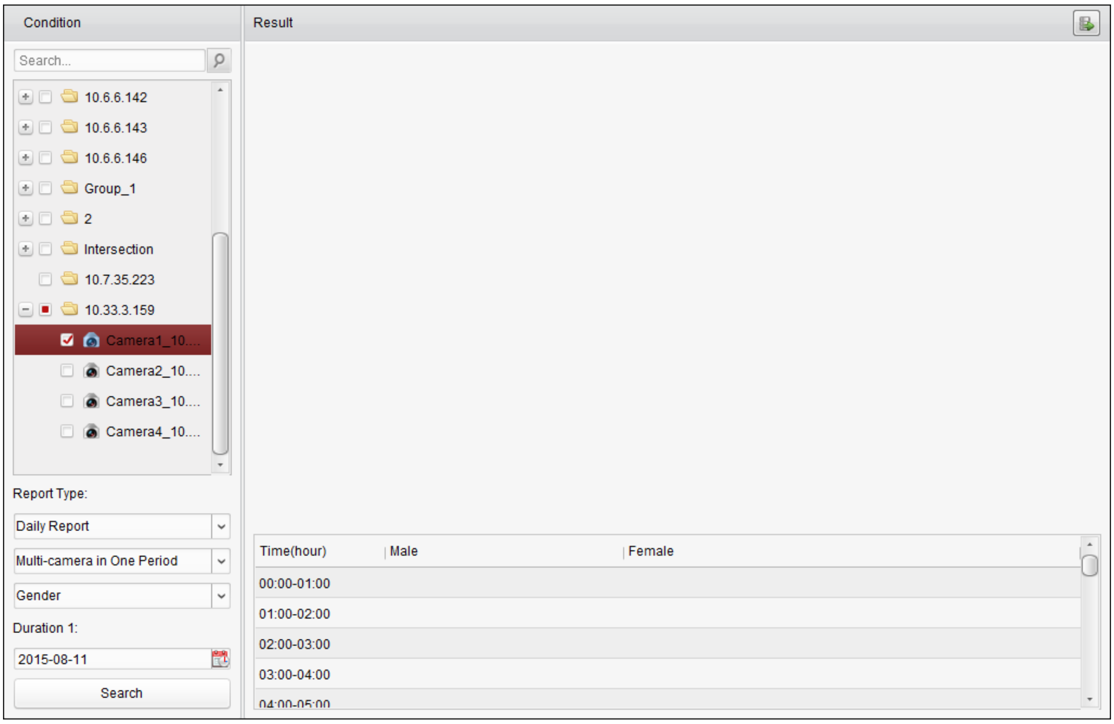
You can check the captured faces statistics of the added face capture device and the statistics can be displayed in table, line chart, pie chart or histogram. The detailed data can be exported for local storage.

Before you start:

Please add the face capture device to the software and properly configure the corresponding settings. For detailed settings, please refer to the *User Manual* of the device.

Note: The face capture device should be added to the software as Encoding Device, please refer to *Chapter 3.1 Adding the Device* for detailed configuration.

Click the 🪪 icon on the control panel to open the Face Capture page.



Condition

Search...

- 10.6.6.142
- 10.6.6.143
- 10.6.6.146
- Group_1
- 2
- Intersection
- 10.7.35.223
- 10.33.3.159
  - ☑ Camera1_10....
  - □ Camera2_10....
  - □ Camera3_10....
  - □ Camera4_10....

Report Type:

Daily Report

Multi-camera in One Period

Gender

Duration 1:

2015-08-11

Search

Result

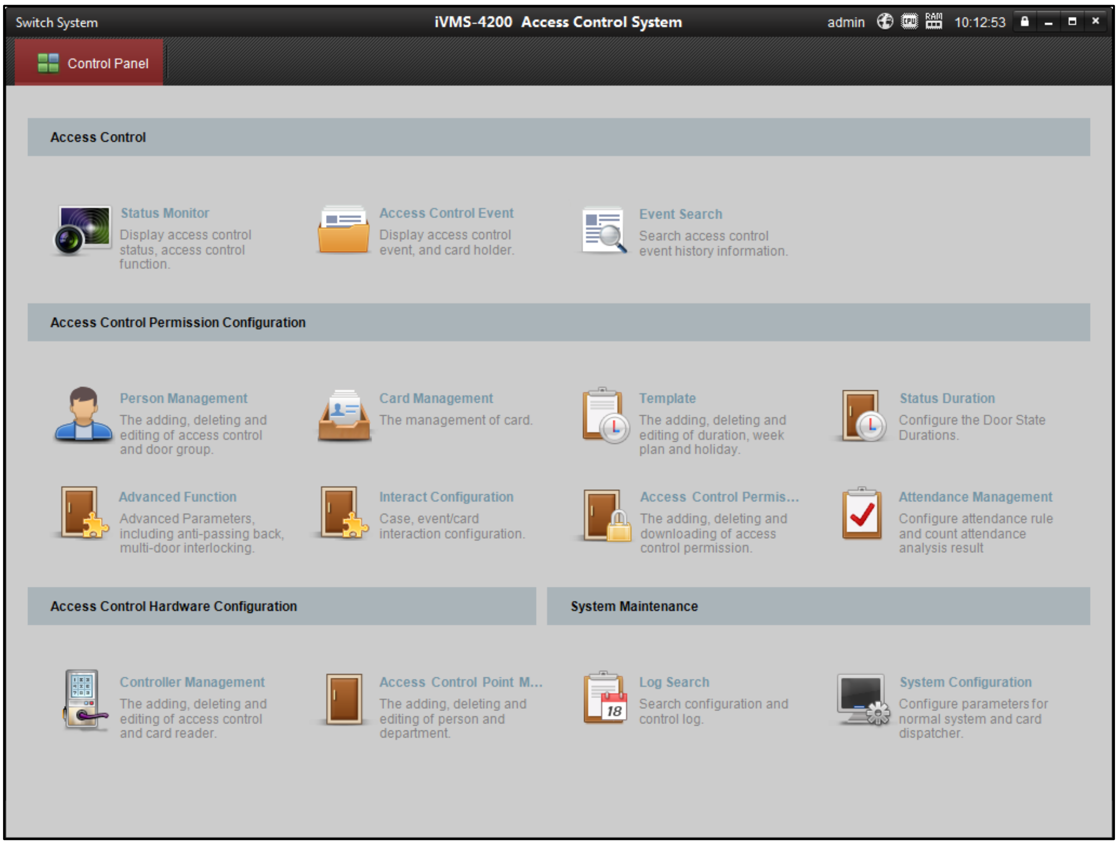
Time(hour)	Male	Female
00:00-01:00		
01:00-02:00		
02:00-03:00		
03:00-04:00		
04:00-05:00		

Steps:

1. Open the Face Capture page.
2. Select the report type as needed and set the time.
   1) Select daily report, weekly report, monthly report or annual report as the time type for the report.
   2) Select Multi-camera in One Period as the statistics type.
      Multi-camera in One Period: Multiple cameras can be selected for generating the statistics for them of one time period.
   3) Select Age, Gender or Number of People as the data type.
   4) Set the time period.
3. Select the cameras for generating the report.
4. Click **Search** and the statistics displays on the right panel. The detailed data for each hour, day or month will be also displayed.
   For Age and Gender statistics, the statistics are shown in pie chart.
   For Number of People statistics, the statistics are shown in histogram form by default. You can switch it to line chart by clicking the .
5. (Optional) Click to save the detailed data of captured face pictures to your PC.

Chapter 18 Overview of Access Control System

Click **Switch System**-> **Access Control System** on the menu bar to enter the Access Control System.



Access Control

Status Monitor
Display access control status, access control function.

Access Control Event
Display access control event, and card holder.

Event Search
Search access control event history information.

Access Control Permission Configuration

Person Management
The adding, deleting and editing of access control and door group.

Card Management
The management of card.

Template
The adding, deleting and editing of duration, week plan and holiday.

Status Duration
Configure the Door State Durations.

Advanced Function
Advanced Parameters, including anti-passing back, multi-door interlocking.

Interact Configuration
Case, event/card interaction configuration.

Access Control Permis...
The adding, deleting and downloading of access control permission.

Attendance Management
Configure attendance rule and count attendance analysis result

Access Control Hardware Configuration

Controller Management
The adding, deleting and editing of access control and card reader.

Access Control Point M...
The adding, deleting and editing of person and department.

System Maintenance

Log Search
Search configuration and control log.

System Configuration
Configure parameters for normal system and card dispatcher.

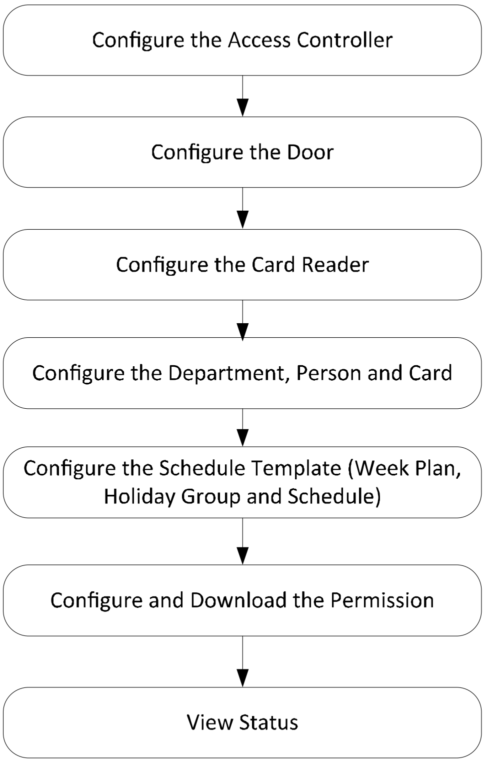
18.1 Description

The Access Control System is a client of configuring permission of door access. It provides multiple functionalities, including access controller management, person/card management, permission configuration, door status management, attendance management, event search, etc.

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

18.2 Configuration Flow

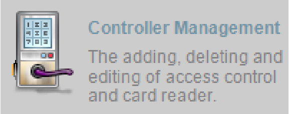
Refer to the following flow chart for the configuration order.



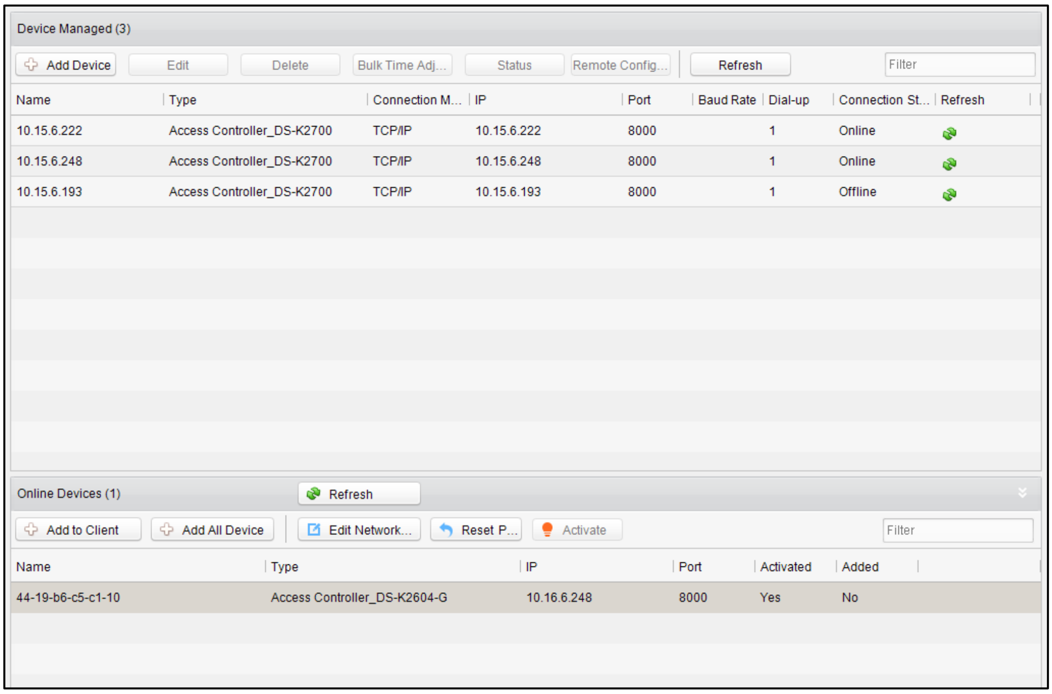
Configure the Access Controller
Configure the Door
Configure the Card Reader
Configure the Department, Person and Card
Configure the Schedule Template (Week Plan, Holiday Group and Schedule)
Configure and Download the Permission
View Status

Chapter 19 Device Management

19.1 Controller Management


Controller Management
The adding, deleting and editing of access control and card reader.

Click the icon to enter the controller management interface.



Device Managed (3)

Name	Type	Connection M...	IP	Port	Baud Rate	Dial-up	Connection St...	Refresh
10.15.6.222	Access Controller_DS-K2700	TCP/IP	10.15.6.222	8000		1	Online	⟳
10.15.6.248	Access Controller_DS-K2700	TCP/IP	10.15.6.248	8000		1	Online	⟳
10.15.6.193	Access Controller_DS-K2700	TCP/IP	10.15.6.193	8000		1	Offline	⟳

Online Devices (1)

Name	Type	IP	Port	Activated	Added
44-19-b6-c5-c1-10	Access Controller_DS-K2604-G	10.16.6.248	8000	Yes	No

The interface is divided into 2 parts: device management and online device detection.

Device Management:

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

Online Device Detection:

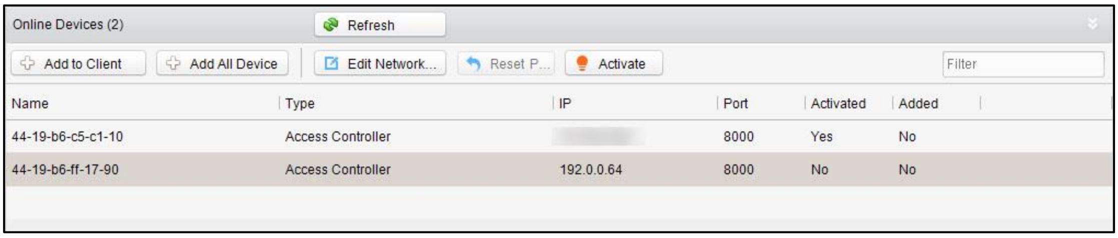
Automatically detect online devices in the same subnet with the access control server, and the detected devices can be added to the server in an easy way.

Note: The control client can manage up to 16 access controllers

19.1.1 Device Activation

Steps:

1. In the Controller Management interface, select an inactive device that in the Online Devices list.

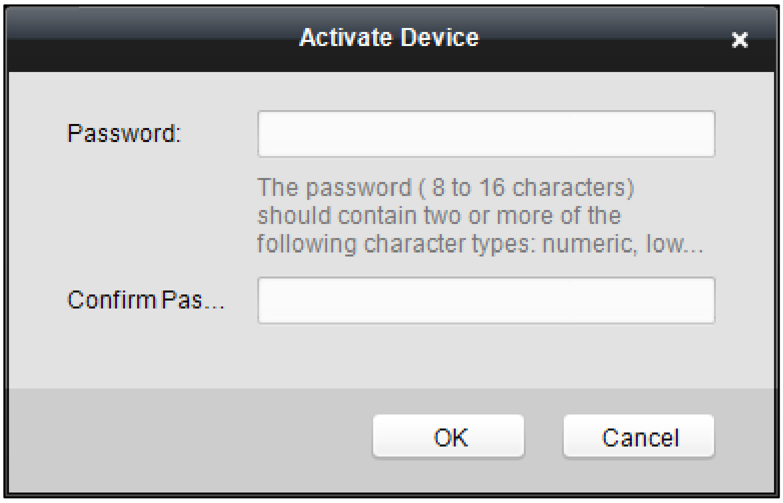


Name	Type	IP	Port	Activated	Added
44-19-b6-c5-c1-10	Access Controller	[redacted]	8000	Yes	No
44-19-b6-ff-17-90	Access Controller	192.0.0.64	8000	No	No

2. Click Activate.

3. Create a password and confirm the password of the device.

4. Click OK. The device will be activated.



Password:

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

Confirm Pas...

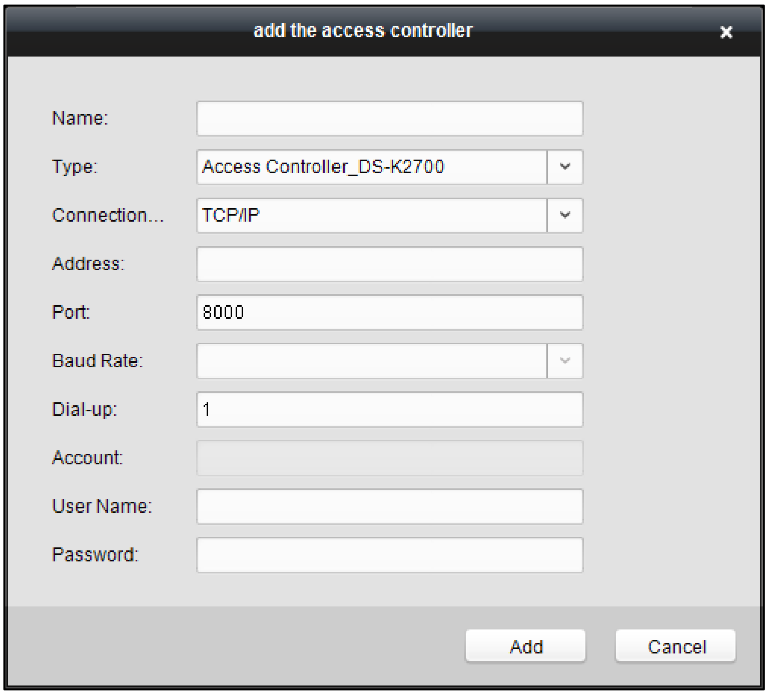
__STRONG PASSWORD RECOMMENDED__– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters and maximum 16 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

19.1.2 Device Management

Adding Controller

Steps:

1. Click Add Device to enter the add access controller interface.



add the access controller

Name:

Type: Access Controller_DS-K2700

Connection…: TCP/IP

Address:

Port: 8000

Baud Rate:

Dial-up: 1

Account:

User Name:

Password:

2. Input the device name.
3. Select the access controller type in the dropdown list.
4. Select the connection mode in the dropdown list: TCP/IP, or COM port.

   TCP/IP: Connect the device via the network.
5. Set the parameters of connecting the device.

   If you choose to connect the device via network, you should input the IP address and port No. of the device, and set the Dial-up value to 1.
6. Click the Add button to finish adding.

   Notes:

   - Up to 1 access control point and up to 2 card readers can be added to each access control terminal.
   - Add the access control point and the card reader to the DS-K2700 Access Controller after adding the DS-K27M01, DS-K27M02 or DS-K27M04 Distributed Access Controller.
   - Ehome is not supported.

   Or you are able to select the detected online device in the Online Devices list and click Add to Client. Input the device user name and the password to add the device to the Device Managed list.

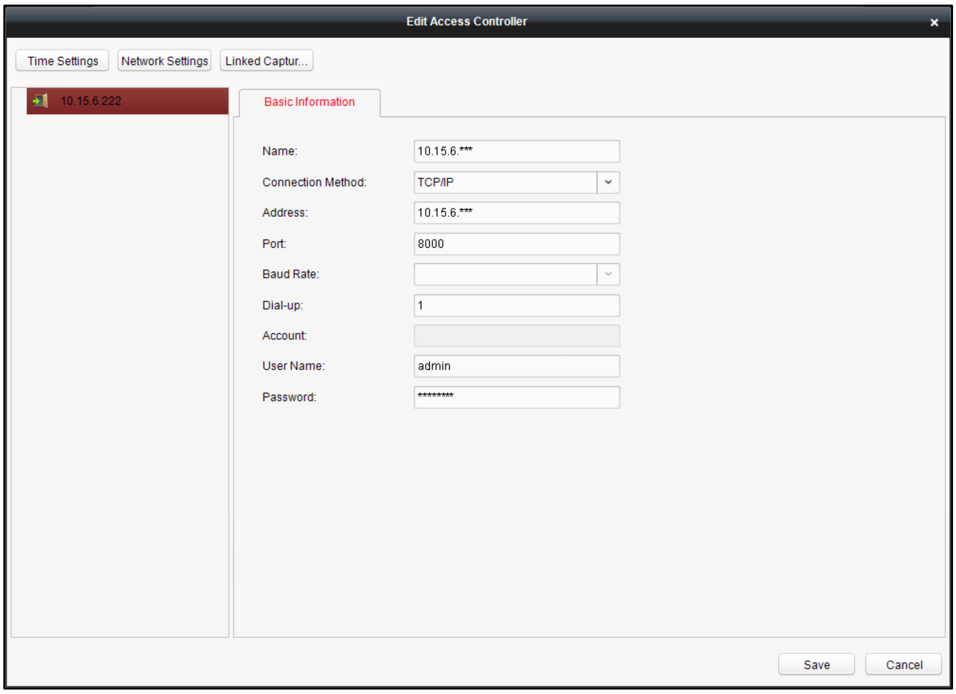
Editing Device (Basic Information)

Purpose:

After adding the device, some advanced parameters can be configured in the editing device interface, e.g. downloading hardware parameters, reading hardware parameters, time synchronizing, configuring access point, etc.

Steps:

1. In the device list, select a device and click Edit to edit the device information.



Edit Access Controller

Time Settings | Network Settings | Linked Captur...

10.15.6.222

Basic Information

Name: 10.15.6.***

Connection Method: TCP/IP

Address: 10.15.6.***

Port: 8000

Baud Rate:

Dial-up: 1

Account:

User Name: admin

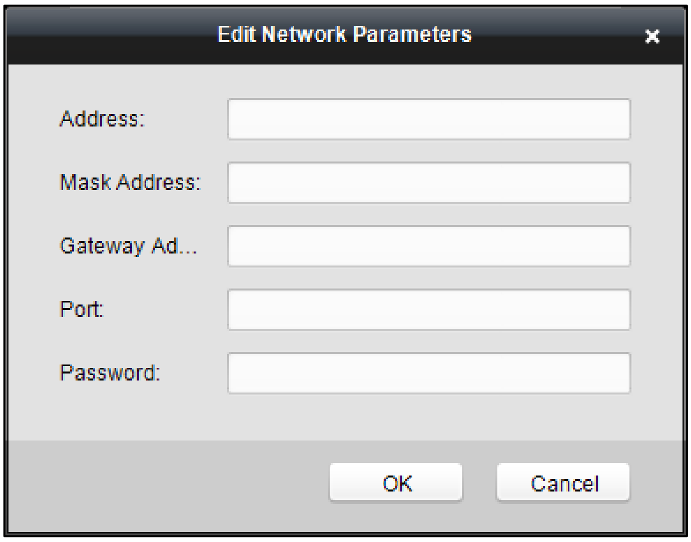
Password: ********

Save | Cancel

2. Edit the basic parameters of the device on your demand, which are the same as the ones when adding the device.

3. Click Save to finish editing.

   Or in the Online Devices list, select a device and click Edit Network... to edit the device IP Address, Mask Address, Gateway Address, Port No. Input the device password and click OK to finish editing.



Edit Network Parameters

Address:

Mask Address:

Gateway Ad...

Port:

Password:

OK | Cancel

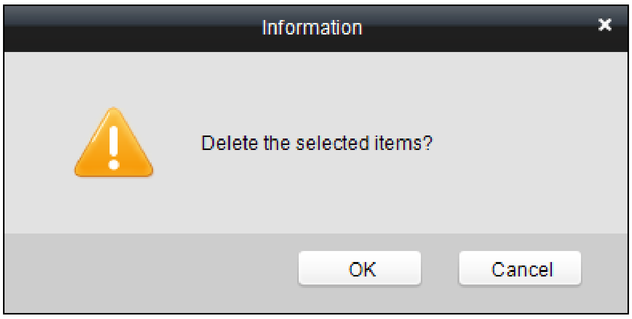
Deleting Device

Steps:

1. In the Device Managed list, select a device by clicking it, or select multiple devices by pressing Ctrl button on your keyboard and clicking them one by one.

2. Click Delete to delete the selected device(s).

3. Click OK in the popup confirmation dialog to finish deleting.



Delete the selected items?

Resetting Password

Steps:

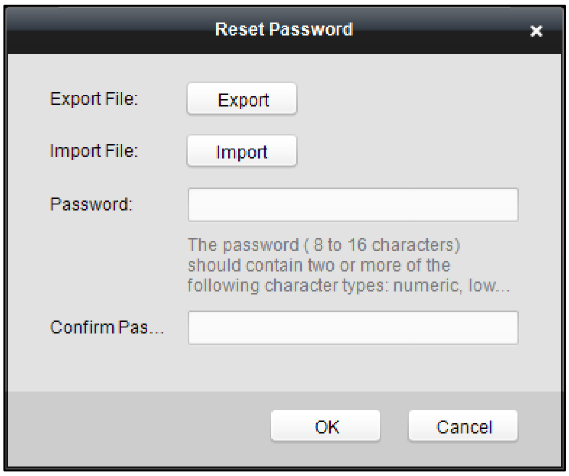
1. In the Online Devices list, select an online device and click Reset P... .

2. Click Export in the pop-up window to export the device security code.

3. Send the security code to our technical supporters to get the encrypted security code of the device.

4. Click Import to import the encrypted security code.

5. Click OK to finishing resetting.



Export File:

Import File:

Password:

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

Confirm Pas...

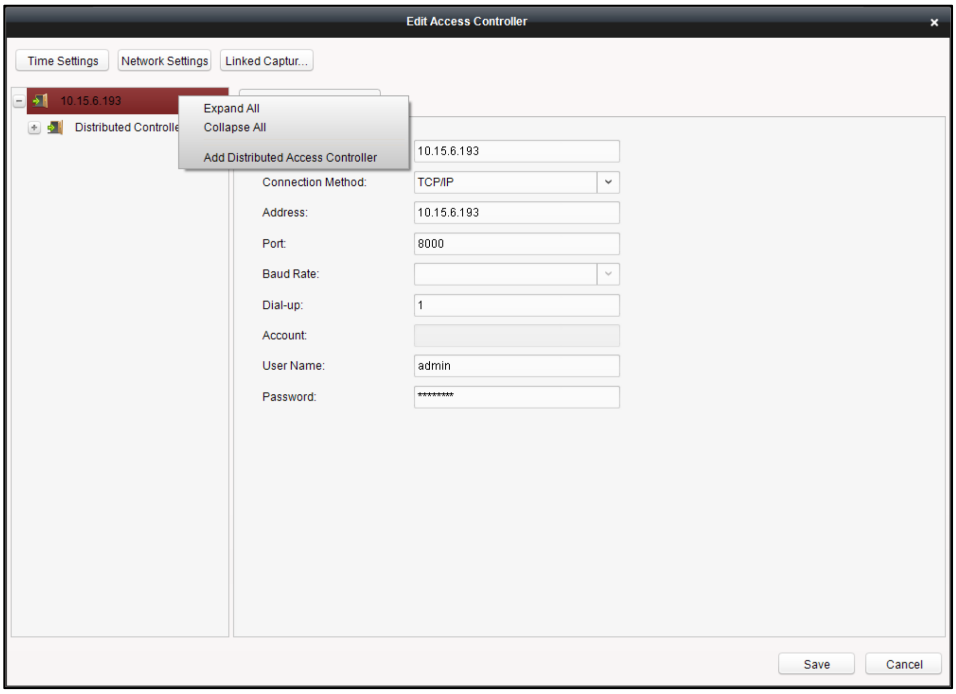
Manually Registering Distributed Access Controller

Steps:

1. In the Device Managed list, double click an online device, or select an online device and click Edit to enter the Edit Access Controller interface.

2. Right click a target access controller in the device list to open the right-click menu.

3. Click **Add Distributed Access Controller**.



10.15.6.193

Connection Method: TCP/IP

Address: 10.15.6.193

Port: 8000

Baud Rate:

Dial-up: 1

Account:

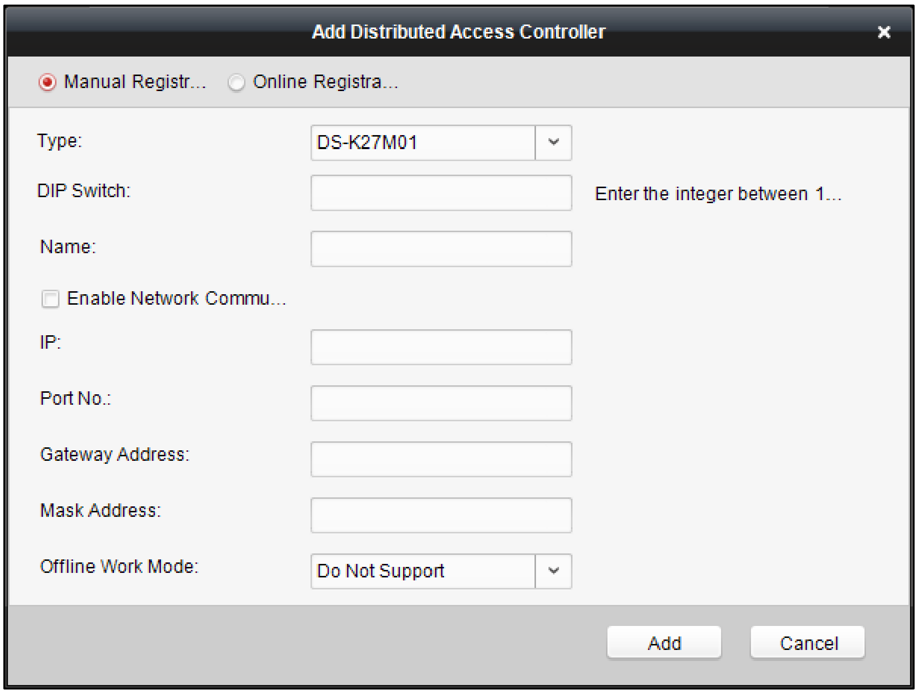
User Name: admin

Password: ********

4. Select Manual Registration in the Add Distributed Access Controller window, and configure the distributed controller type, the DIP switch and the name.
   If check **Enable Network Communication**, you are able to configure the port No., the gateway address, the mask address and the distributed controller offline work mode.
   If you do not check **Enable Network Communication**, only configure the type, the DIP switch and the name to add the distributed controller.

5. Click Add and click OK in the pop-up window. The added distributed access controller will be displayed in the device list in the Edit Access Controller interface.

6. Click the Hardware Par... (Hardware Parameters Downloading) button to download information to the device.



Add Distributed Access Controller

● Manual Registr... ○ Online Registra...

Type: DS-K27M01

DIP Switch: Enter the integer between 1...

Name:

□ Enable Network Commu...

IP:

Port No.:

Gateway Address:

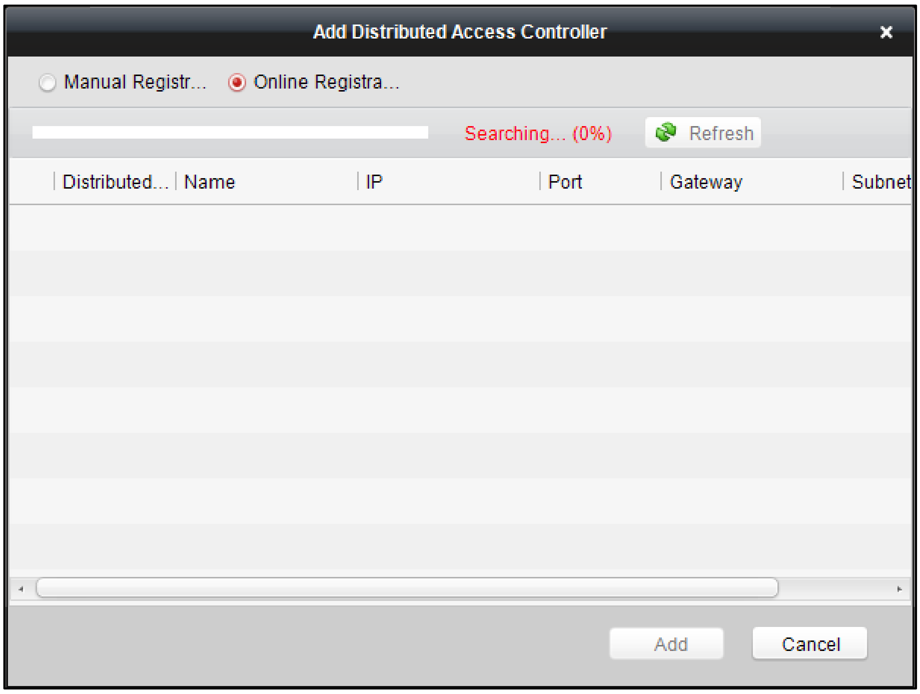
Mask Address:

Offline Work Mode: Do Not Support

Registering Distributed Access Controller Online

Steps:

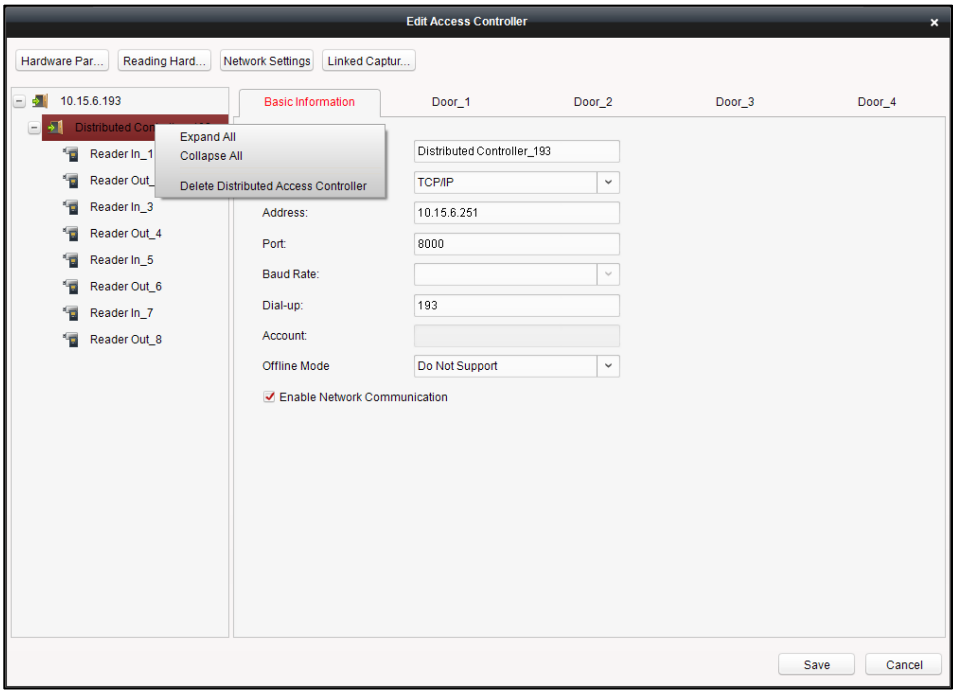
1. In the Add Distributed Access Controller window, click Online Registration.
2. Click Refresh. The software will search the online distributed access controller. The result will be displayed in the list, including the device No., name, IP address, gateway and subnet mask.
3. Select a distributed access controller and click Add.
4. Click OK in the pop-up window. The distributed access controller will be added to the access controller.
5. Click the Hardware Par... (Hardware Parameters Downloading) button to download information to the device.



Logout Distributed Access Controller

Steps:

1. In the Edit Access Controller interface, right click a target distributed assess controller in the device list to open the right-click menu.
2. Click **Delete Distributed Access Controller**.
3. Click OK in the pop-up window to confirm deleting. All related information of the distributed access controller will be also deleted.
4. Click the Hardware Par... (Hardware Parameters Downloading) button to download information to the device.



Distributed Controller_193

TCP/IP

Address: 10.15.6.251

Port: 8000

Baud Rate:

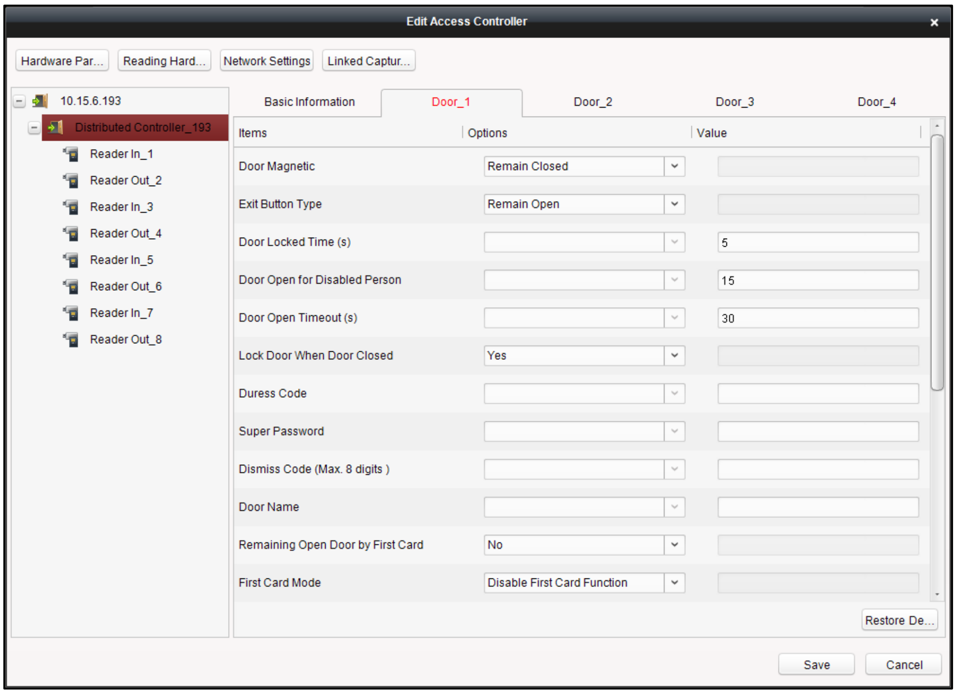
Dial-up: 193

Account:

Offline Mode: Do Not Support

☑ Enable Network Communication

Editing Distributed Access Controller (Door Information)



Items	Options	Value
Door Magnetic	Remain Closed	
Exit Button Type	Remain Open	
Door Locked Time (s)		5
Door Open for Disabled Person		15
Door Open Timeout (s)		30
Lock Door When Door Closed	Yes	
Duress Code		
Super Password		
Dismiss Code (Max. 8 digits)		
Door Name		
Remaining Open Door by First Card	No	
First Card Mode	Disable First Card Function	

Steps:

1. In the editing interface, select a distributed access controller and click **Door_1/Door_2/...** to edit the information of the selected door.
   1) **Door Magnetic**: The Door Magnetic is in the status of **Remain Closed** (excluding special conditions).
   2) **Exit Button Type**: The Exit Button Type is in the status of **Remain Open** (excluding special conditions).
   3) **Door Locked Time(s)**: After swiping the normal card and relay action, the timer for locking

the door starts working.

4) **Door Open for Disabled Person:** The door magnetic can be enabled with appropriate delay after disabled person swipes the card.

5) **Door Open Timeout(s)**: The alarm can be triggered if the door has not been close

6) **Enable Lock Door when Door Close**: This function has not been supported yet.

7) **Duress Code**: The door can open by inputting the duress code when there is a duress. At the same time, the access system can report the duress event.

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

9) **Dismiss Code (Max. 8 digits):** The alarm can be dismissed by entering the configured dismiss code.

10) **Door Name:** You are able to edit the door name.

11) **Remaining Open Door by First Card:** Select Yes or No.

12) **First Card Mode:** Select the first card mode, including Disable First Card Function, Remain Open by First Card Mode and First Card Authorization Mode.

13) **Remaining Open Duration Time (Minute):** Configure the remaining open duration for the first card.

14) **Connected to Distributed Controller:** Connect the door to the distributed access controller or not.

15) **Distributed Controller No.:** Configure the distributed access controller No.

16) **Distributed Controller Door No.:** Configure the distributed access controller door No.

17) **Distributed Controller Network Status:** Configure the distributed access controller status.

18) **Lock Input Detection:** Select enable or disable the function.

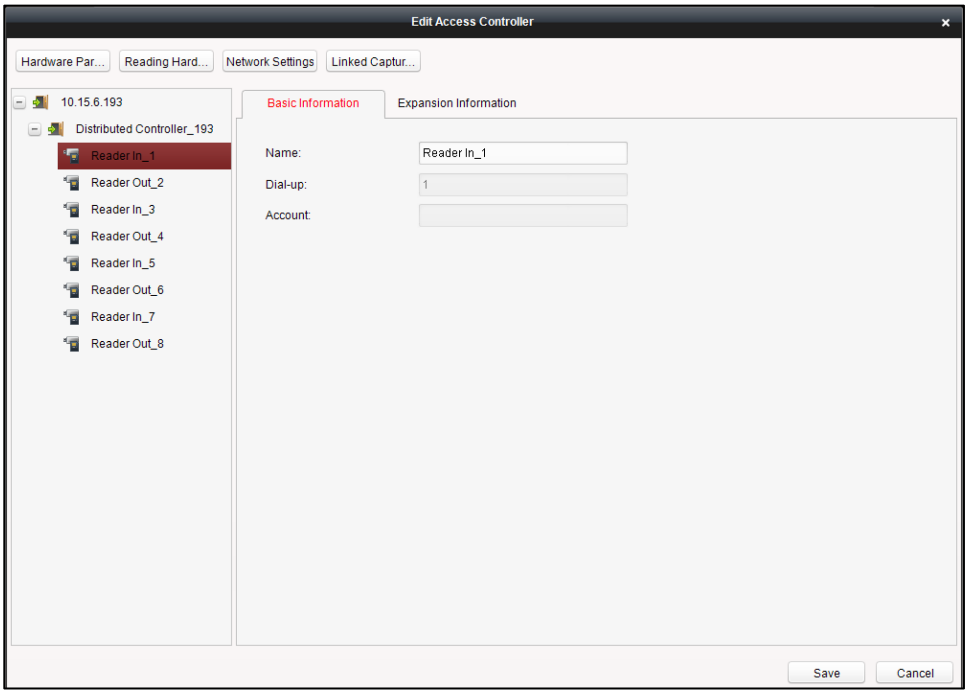
19) **Lock Input Type:** Select to remaining open or close the door.

20) **Door Control Terminal Work Mode:** Select Open/Short Circuit Attempts Alarm or Normal mode.

21) **Exit Button:** Select to enable or disable the exit button.

2. Click the **Restore Default Value** to restore all parameters into default settings.
3. Click the Save button to save parameters.
4. Click the Hardware Par... (Hardware Parameters Downloading) button to download information to the device.

Editing Distributed Access Controller (Card Reader Information)



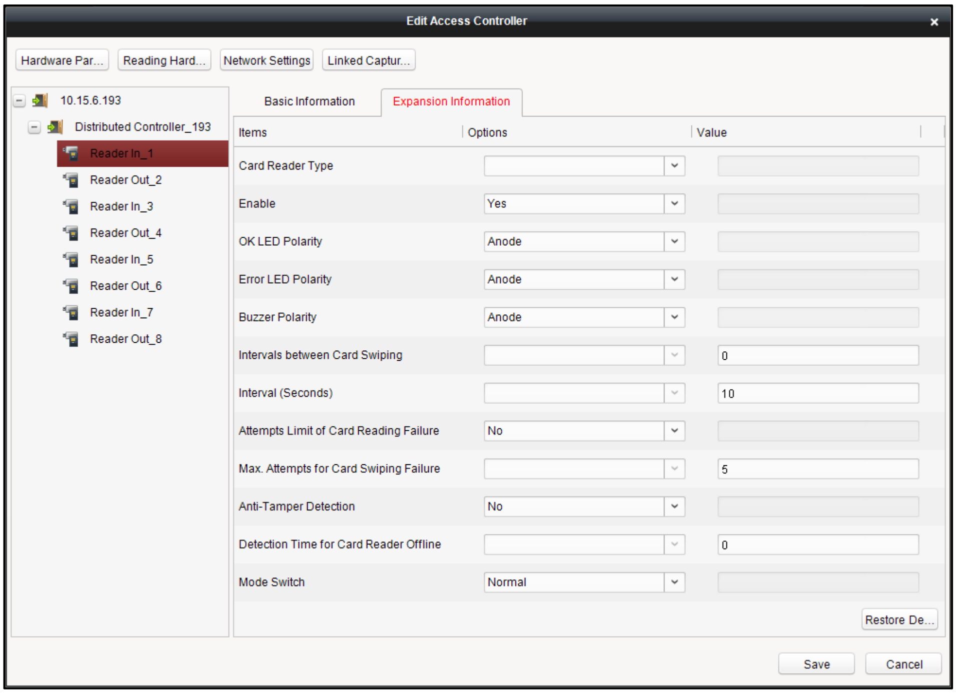
Name: Reader In_1

Dial-up: 1

Account:

Steps:

1. In the device list, select a card reader name to enter into the card reader basic information editing interface.
2. Click **Basic Information** to edit the basic information about the card reader.
3. Click **Expansion Information** to edit the expansion information of the card reader.



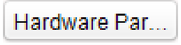
Items	Options	Value
Card Reader Type		
Enable	Yes	
OK LED Polarity	Anode	
Error LED Polarity	Anode	
Buzzer Polarity	Anode	
Intervals between Card Swiping		0
Interval (Seconds)		10
Attempts Limit of Card Reading Failure	No	
Max. Attempts for Card Swiping Failure		5
Anti-Tamper Detection	No	
Detection Time for Card Reader Offline		0
Mode Switch	Normal	

The Expansion Information includes:

1) **Card Reader Type:** You cannot select the card reader type. Viewing the card reader type is available.
2) **Enable: Yes** refers to card swiping is available on the card reader. No
3) **OK LED Polarity:** Select the polarity.

4) **Error LED Polarity:** Select the polarity.
5) **Buzzer Polarity:** Select the buzzer polarity.
6) **Intervals between Card Swiping:** It is invalid to swipe the same card again in the configured time duration. Available configured time duration is from 0 to 255s. (If set the time duration to 0, the function is not enabled.)
7) **Interval (Seconds):** The maximum interval between entering two characters of the password. After inputting a character, if you do not enter the next character in the configured interval, all characters will be cleared.
8) **Attempts Limit of Card Reading Failure:** If select "Yes", when the operation of card reading failed exceeds the configured attempts, the controller will generate an alarm event.
9) **Max. Attempts for Card Swiping Failure:** The maximum attempts for card swiping failed.
10) **Anti-Tamper Detection:** If select "Yes", when the card reader is tampered or removed, the controller will generate an alarm.
11) **Detection Time for Card Reader Offline:** If the card reader does not respond to the controller in the configured time duration, the card reader will be in the offline mode.
12) **Mode Switch:** Switch the card reader mode. Support the normal mode and the Card Enrollment mode.

4. Click the button to save parameters.

5. Click the  (Hardware Parameters Downloading) button to download information to the device.

Bulk Time synchronization

Steps:

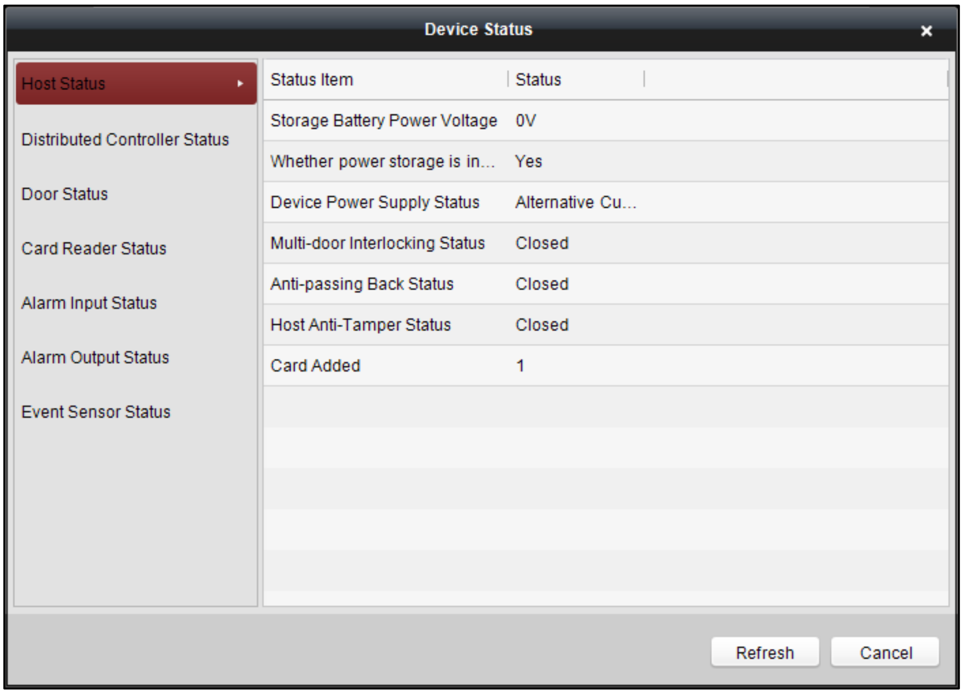
1. In the device list, select a device by clicking it, or select multiple devices by pressing **Ctrl** button on your keyboard and clicking them one by one.

2. Click the button to start time synchronization.

   A message box will pop up on the lower-right corner of the screen when the time synchronization is compeleted.

Status

In the device list, you can click button to enter view the status.



Status Item	Status
Storage Battery Power Voltage	0V
Whether power storage is in...	Yes
Device Power Supply Status	Alternative Cu...
Multi-door Interlocking Status	Closed
Anti-passing Back Status	Closed
Host Anti-Tamper Status	Closed
Card Added	1

1) **Host Status**: The status of the host, including Storage Battery Power Voltage, Whether power storage is in low voltage status, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, Host Anti-Tamper Status and Card Added.

2) **Distributed Controller Status:** Display the distributed access controller status, including the distributed access controller No., offline status, tampering status, device power supply status, fire alarm, storage battery power voltage, Whether power storage is in low voltage status and Serial No.

3) **Door Status**: The status of the connected door. The door status includes Normal Status, Remain Closed and Remain Open.

Note: Normal Status refers to the default value. You are able to configure Remain Closed and Remain Open via the remote open settings and the schedule template setting.

4) **Card Reader Status**: The status of card reader.

5) **Alarm Input Status**: The alarm input status of each port.

6) **Alarm Output Status**: The alarm output status of each port.

7) **Event Sensor Status**: The event status of each port.

Remote Configuration

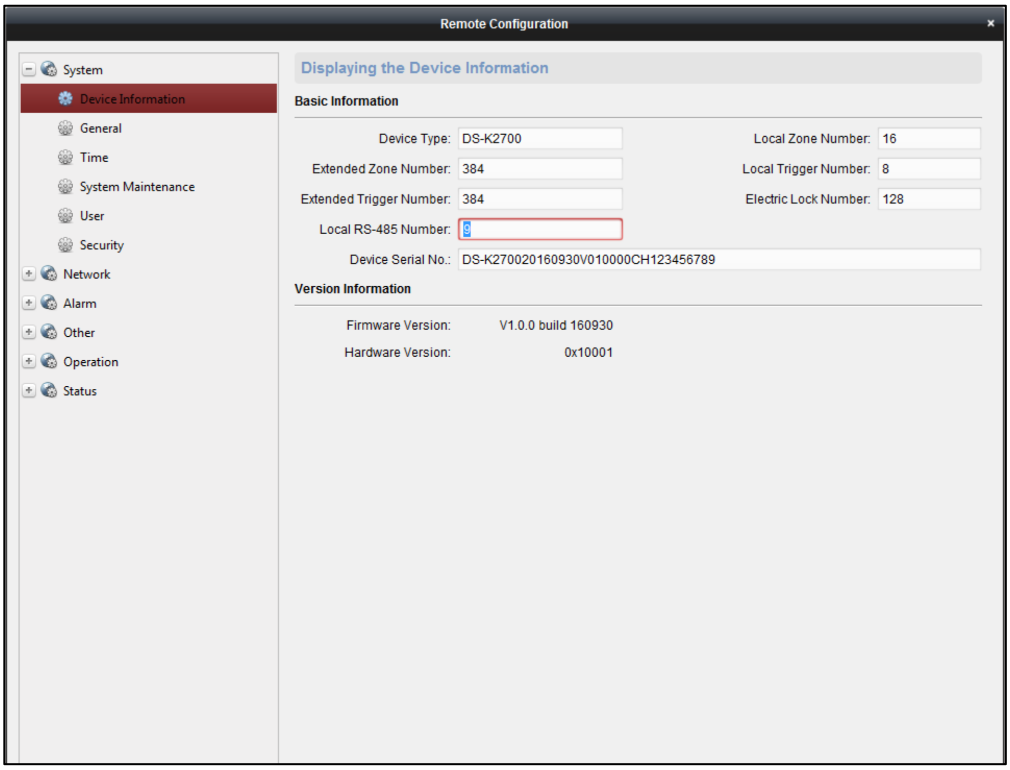
Purpose:

In this this interface, you can set the access control parameters, remotely reboot device, restore the device parameters, remotely update the access controller and the distributed access controller, remotely configure the alarm zone parameters, remotely configure alarm.

➢ **Checking Device Information**

Steps:

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



Displaying the Device Information

Basic Information

Device Type: DS-K2700

Local Zone Number: 16

Extended Zone Number: 384

Local Trigger Number: 8

Extended Trigger Number: 384

Electric Lock Number: 128

Local RS-485 Number: 8

Device Serial No.: DS-K270020160930V010000CH123456789

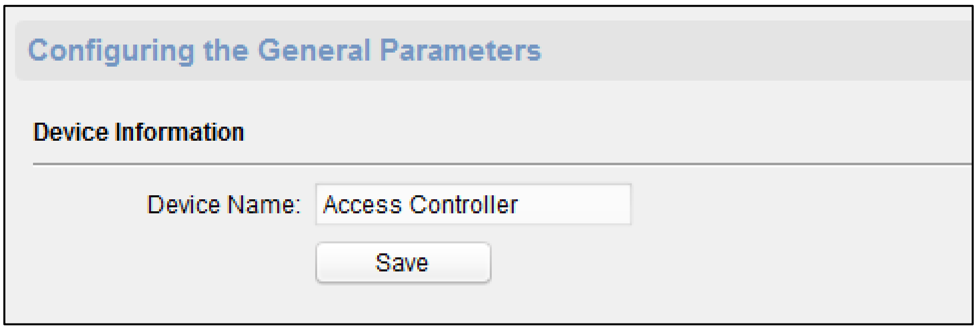
Version Information

Firmware Version: V1.0.0 build 160930

Hardware Version: 0x10001

- **Editing Device Name**

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



Configuring the General Parameters

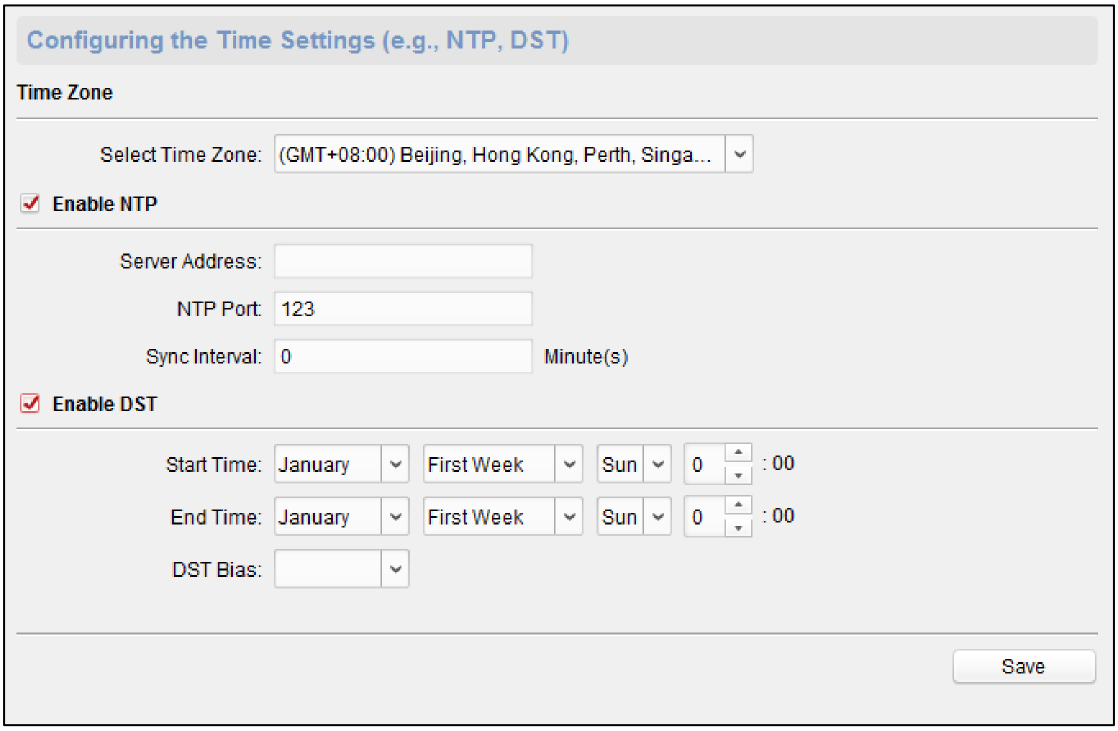
Device Information

Device Name: Access Controller

- **Editing Time**

Steps:

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



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

Time Zone

Select Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singa...

☑ Enable NTP

Server Address:

NTP Port: 123

Sync Interval: 0 Minute(s)

☑ Enable DST

Start Time: January First Week Sun 0 : 00

End Time: January First Week Sun 0 : 00

DST Bias:

➢ **System Maintainance Settings**

Steps:

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

2. Click Reboot to reboot the device.

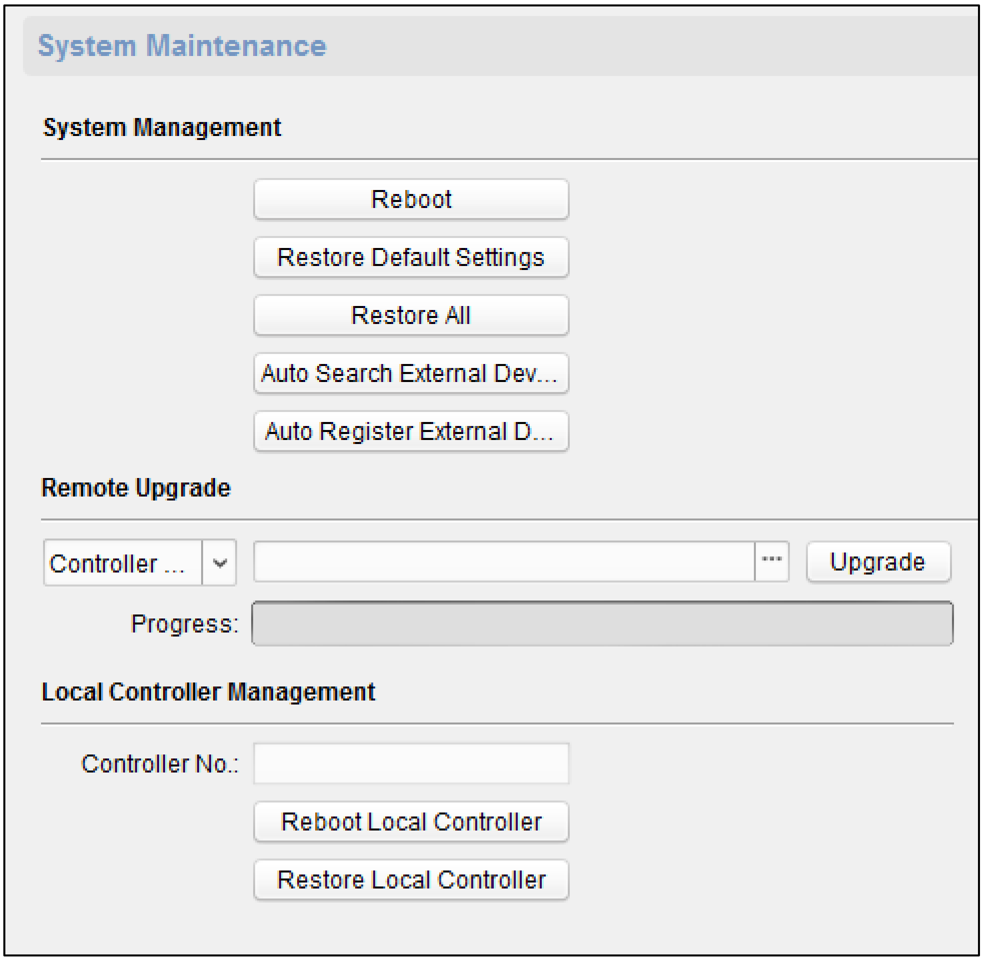
   Or click Restore Default Settings to restore the device settings to the default ones, excluding the IP address.

   Or click Restore All to restore the device parameters to the default ones. The device should be activated after restoring.

   Note: The access controller and the distributed access controller do not support Auto Search External Dev... and Auto Register External D... function.

3. In the Remote Upgrade part, select a upgrade file type in the dropdown list. Click ··· to select the upgrade file. Click Upgrade to start upgrading.

4. You can configure the local controller in the Local Controller Management (Distributed Controller) part. Configure the controller No. Click Reboot Local Controller or Restore Local Controller to reboot the local controller (Distributed Controller) or restore the local controller (Distributed Controller) parameters.



System Maintenance

System Management

Remote Upgrade

Progress:

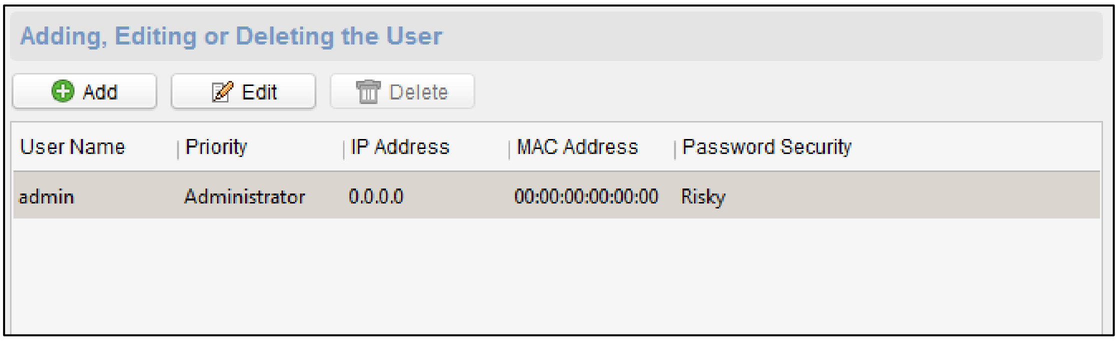
Local Controller Management

Controller No.:

➢ **Managing User**

Steps:

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

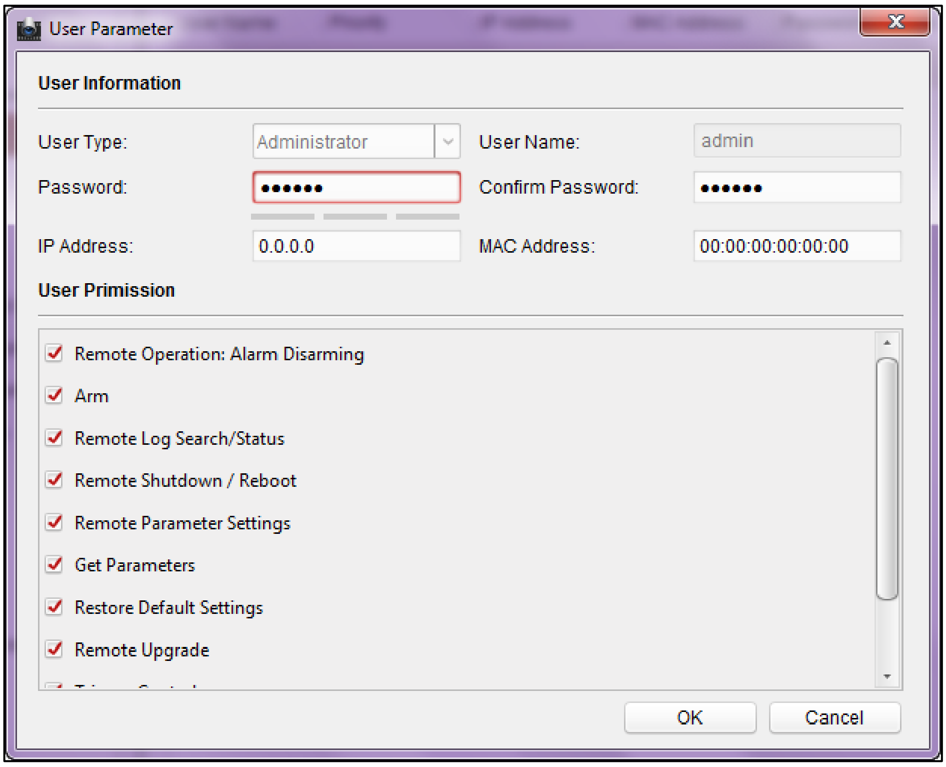


Adding, Editing or Deleting the User

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

2. Click Add to add the user (Do not Support).

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



User Parameter

User Information

User Type: Administrator

User Name: admin

Password: ••••••

Confirm Password: ••••••

IP Address: 0.0.0.0

MAC Address: 00:00:00:00:00:00

User Primission

☑ Remote Operation: Alarm Disarming

☑ Arm

☑ Remote Log Search/Status

☑ Remote Shutdown / Reboot

☑ Remote Parameter Settings

☑ Get Parameters

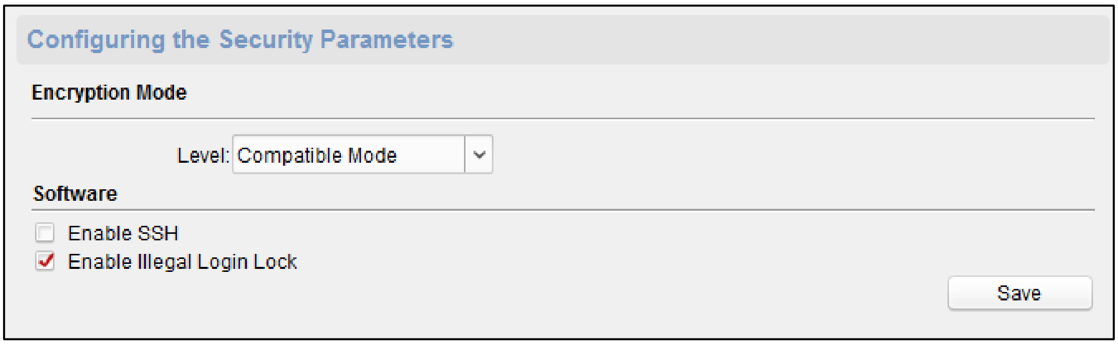
☑ Restore Default Settings

☑ Remote Upgrade

- **Setting Security**

Steps:

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



Configuring the Security Parameters

Encryption Mode

Level: Compatible Mode

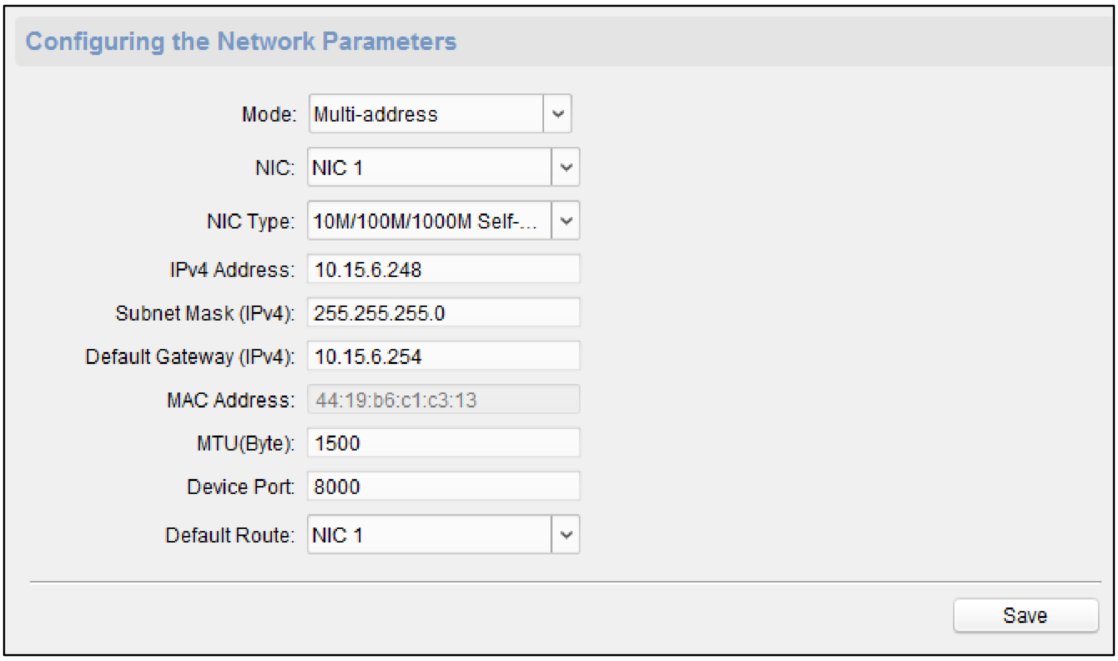
Software

□ Enable SSH

☑ Enable Illegal Login Lock

- **Configuring Network Parameters**

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

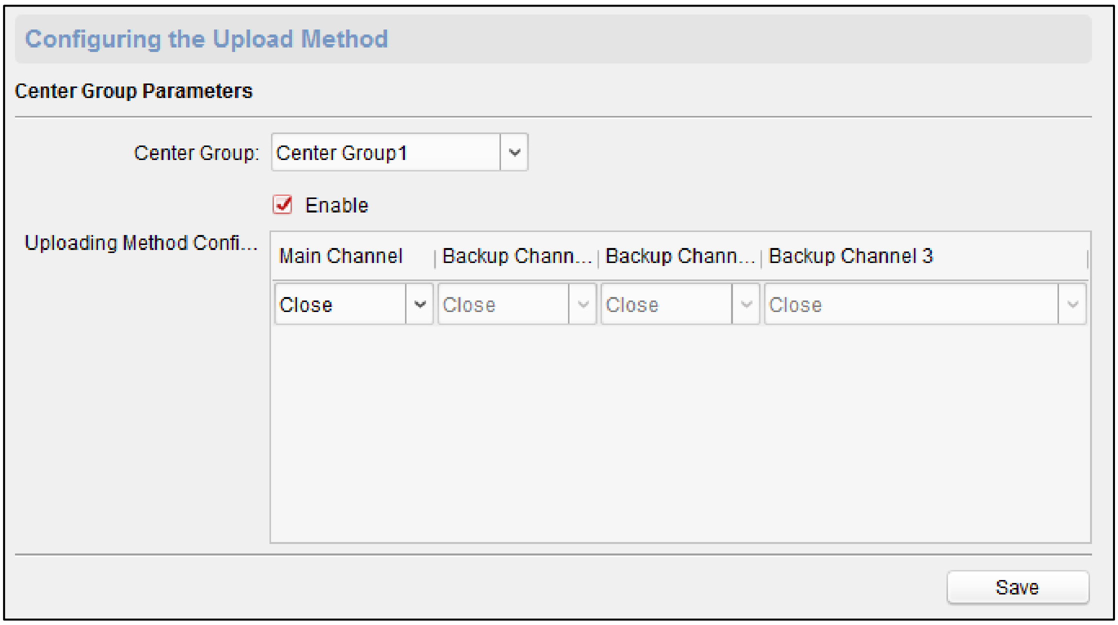


Configuring the Network Parameters

Mode:	Multi-address
NIC:	NIC 1
NIC Type:	10M/100M/1000M Self-...
IPv4 Address:	10.15.6.248
Subnet Mask (IPv4):	255.255.255.0
Default Gateway (IPv4):	10.15.6.254
MAC Address:	44:19:b6:c1:c3:13
MTU(Byte):	1500
Device Port:	8000
Default Route:	NIC 1

➢ **Configuring Upload Method**

Click **Network** -> **Uploading Method Configuration**. You can configure the cener group parameters. Select the center group in the dropdwon list. Check **Enable** and configure the uploading method channel. Click Save to save the settings.



Configuring the Upload Method

Center Group Parameters

Center Group: Center Group1

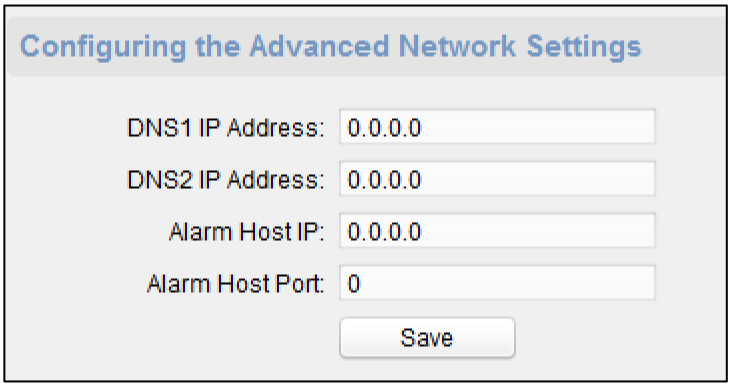
☑ Enable

Uploading Method Confi...

Main Channel	Backup Chann...	Backup Chann...	Backup Channel 3
Close	Close	Close	Close

➢ **Configuring Advanced Network**

Click **Network** -> **Advanced Settings**. You can configure the DNS1 IP address, the DNS2 IP address, the alarm host IP and the alarm host port. Click Save to save the settings.



Configuring the Advanced Network Settings

DNS1 IP Address: 0.0.0.0

DNS2 IP Address: 0.0.0.0

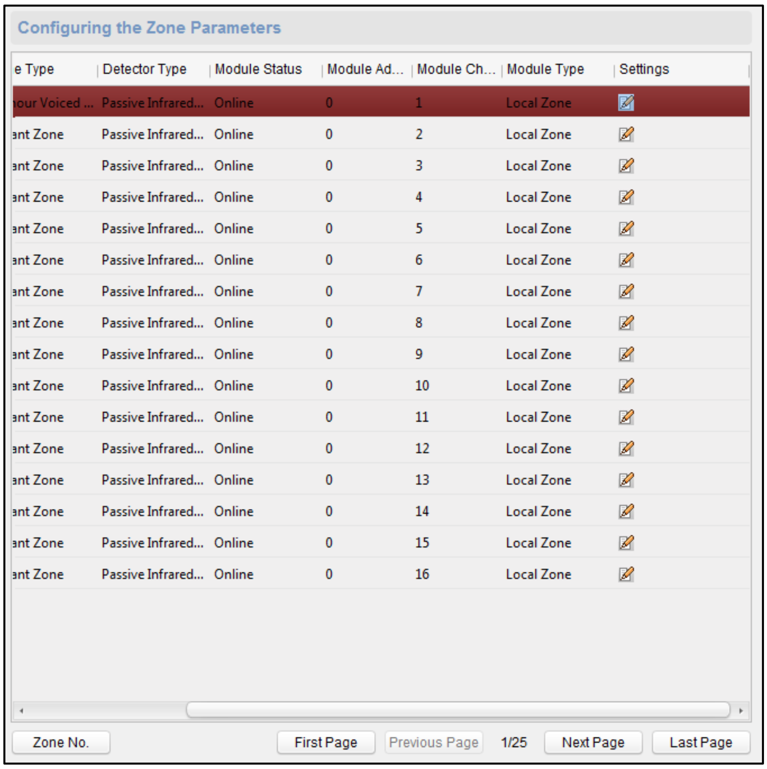
Alarm Host IP: 0.0.0.0

Alarm Host Port: 0

➢ Configuring Alarm Zone Parameters

Steps:

1. In the Remote Configuration interface, click **Alarm** -> **Zone**. You can check the zone parameters.

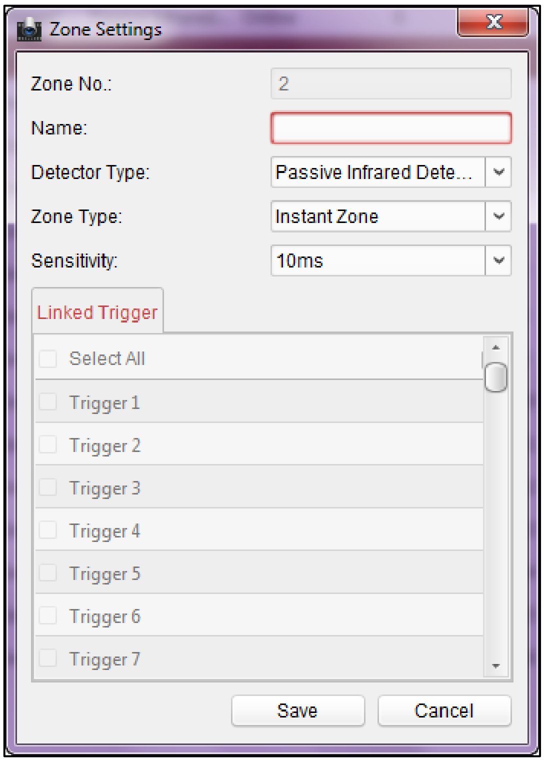


Configuring the Zone Parameters

e Type	Detector Type	Module Status	Module Ad...	Module Ch...	Module Type	Settings
our Voiced ...	Passive Infrared...	Online	0	1	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	2	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	3	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	4	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	5	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	6	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	7	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	8	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	9	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	10	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	11	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	12	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	13	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	14	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	15	Local Zone	✎
ant Zone	Passive Infrared...	Online	0	16	Local Zone	✎

2. Click the icon ✎ to enter the Zone Settings window. You can configure the zone name the detector type, the zone type, and the sensitivity.

3. Click Save to save the settings.



Zone Settings

Zone No.: 2

Name:

Detector Type: Passive Infrared Dete...

Zone Type: Instant Zone

Sensitivity: 10ms

Linked Trigger

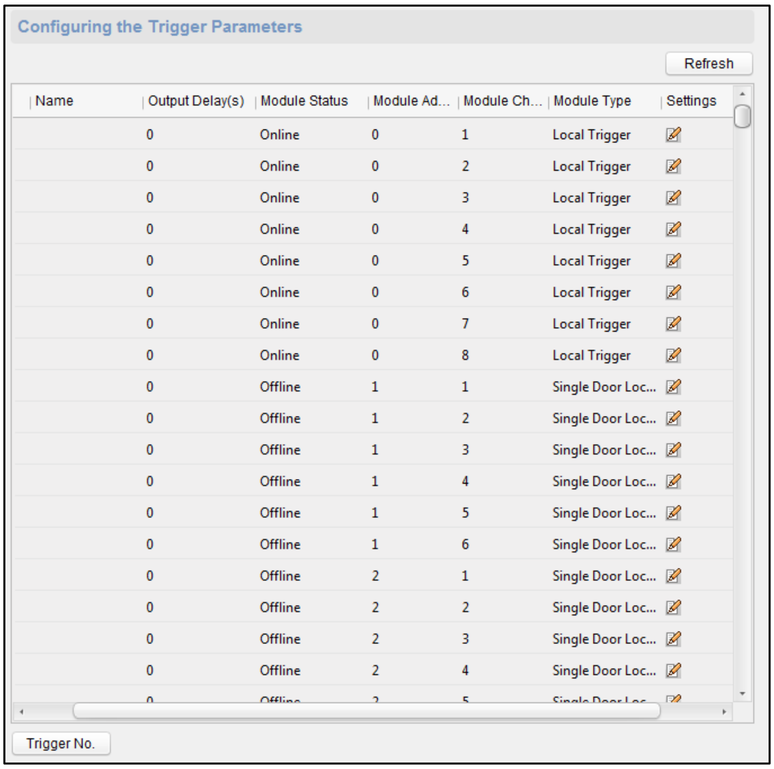
- □ Select All
- □ Trigger 1
- □ Trigger 2
- □ Trigger 3
- □ Trigger 4
- □ Trigger 5
- □ Trigger 6
- □ Trigger 7

Save Cancel

➢ Configuring Trigger Parameters

Steps:

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



Configuring the Trigger Parameters

Refresh

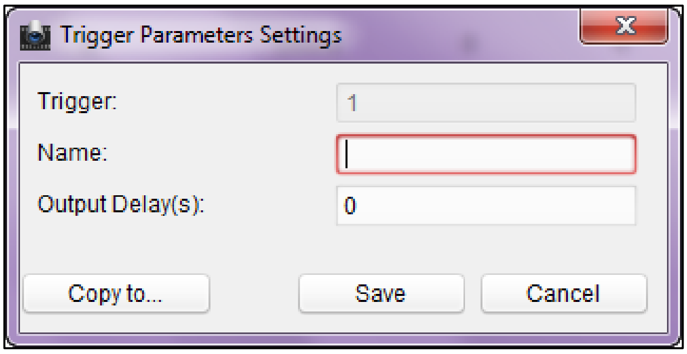
Name	Output Delay(s)	Module Status	Module Ad...	Module Ch...	Module Type	Settings
	0	Online	0	1	Local Trigger	✎
	0	Online	0	2	Local Trigger	✎
	0	Online	0	3	Local Trigger	✎
	0	Online	0	4	Local Trigger	✎
	0	Online	0	5	Local Trigger	✎
	0	Online	0	6	Local Trigger	✎
	0	Online	0	7	Local Trigger	✎
	0	Online	0	8	Local Trigger	✎
	0	Offline	1	1	Single Door Loc...	✎
	0	Offline	1	2	Single Door Loc...	✎
	0	Offline	1	3	Single Door Loc...	✎
	0	Offline	1	4	Single Door Loc...	✎
	0	Offline	1	5	Single Door Loc...	✎
	0	Offline	1	6	Single Door Loc...	✎
	0	Offline	2	1	Single Door Loc...	✎
	0	Offline	2	2	Single Door Loc...	✎
	0	Offline	2	3	Single Door Loc...	✎
	0	Offline	2	4	Single Door Loc...	✎
	0	Offline	2	5	Single Door Loc...	✎

Trigger No.

2. Click the icon ✎ to enter the Trigger Parameters Settings window. You can configure the trigger name.

3. Click Save to save the paramters.

   Or click Copy to... to copy the trigger information to other triggers.



Trigger Parameters Settings

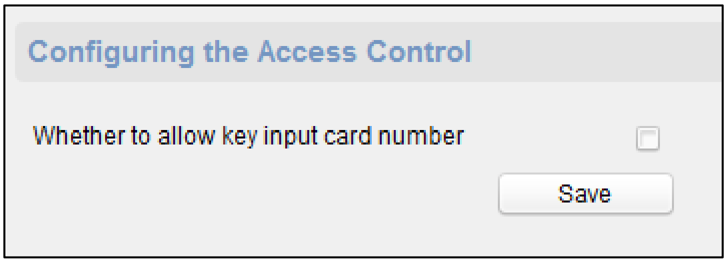
Trigger: 1

Name:

Output Delay(s): 0

- **Configuring Access Control**

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

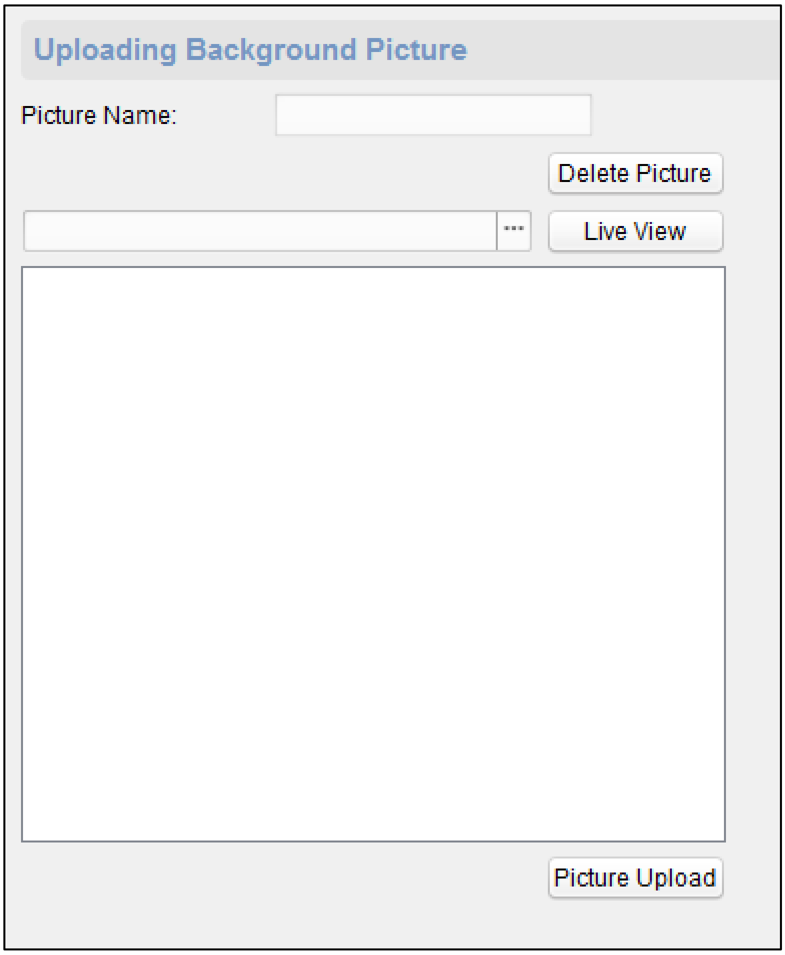


Configuring the Access Control

Whether to allow key input card number □

- **Uploading Background Picture**

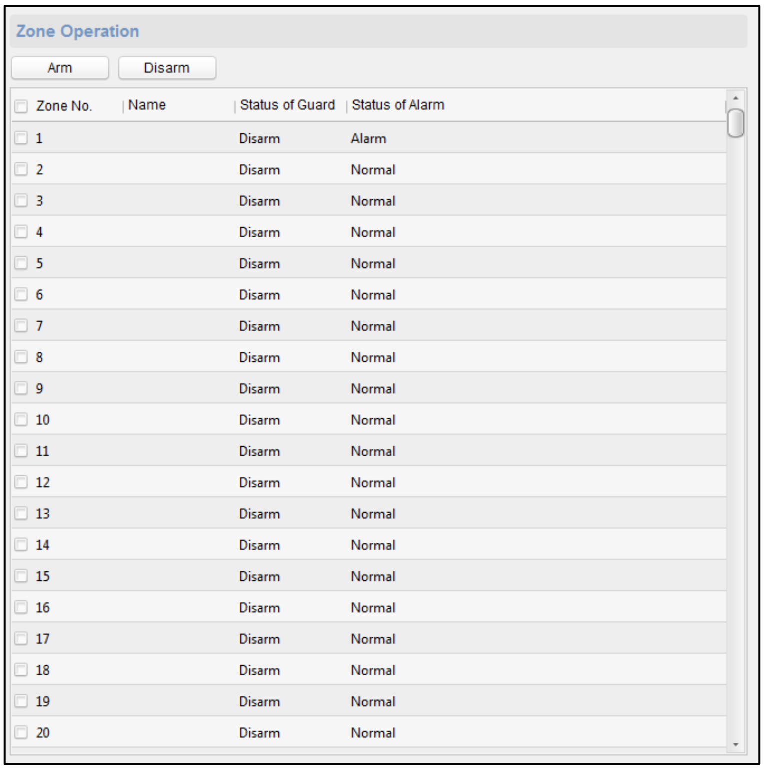
Click **Other** -> **Picture Upload**. Click ... to select the picture from the local. You can click Live View to preview the picture. Click Picture Upload to upload the picture.



➢ **Operating Zone**

Steps:

1. Click **Operation** -> **Zone**. You are able to check the zone status.
2. Check the zone and click Arm or Disarm to arm/disarm the zone.



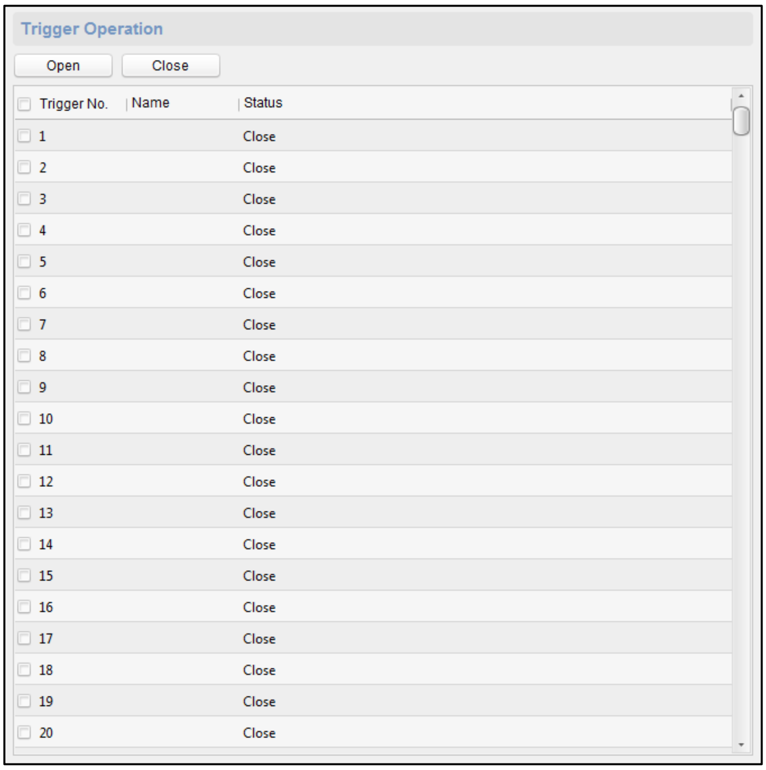
Zone Operation

□ Zone No.	Name	Status of Guard	Status of Alarm
□ 1		Disarm	Alarm
□ 2		Disarm	Normal
□ 3		Disarm	Normal
□ 4		Disarm	Normal
□ 5		Disarm	Normal
□ 6		Disarm	Normal
□ 7		Disarm	Normal
□ 8		Disarm	Normal
□ 9		Disarm	Normal
□ 10		Disarm	Normal
□ 11		Disarm	Normal
□ 12		Disarm	Normal
□ 13		Disarm	Normal
□ 14		Disarm	Normal
□ 15		Disarm	Normal
□ 16		Disarm	Normal
□ 17		Disarm	Normal
□ 18		Disarm	Normal
□ 19		Disarm	Normal
□ 20		Disarm	Normal

- **Operating Trigger**

Steps:

1. Click **Operation** -> **Trigger**. You can check the trigger status.
2. Check the trigger and click Open or Close to open/close the trigger.



Trigger Operation

□ Trigger No.	Name	Status
□ 1		Close
□ 2		Close
□ 3		Close
□ 4		Close
□ 5		Close
□ 6		Close
□ 7		Close
□ 8		Close
□ 9		Close
□ 10		Close
□ 11		Close
□ 12		Close
□ 13		Close
□ 14		Close
□ 15		Close
□ 16		Close
□ 17		Close
□ 18		Close
□ 19		Close
□ 20		Close

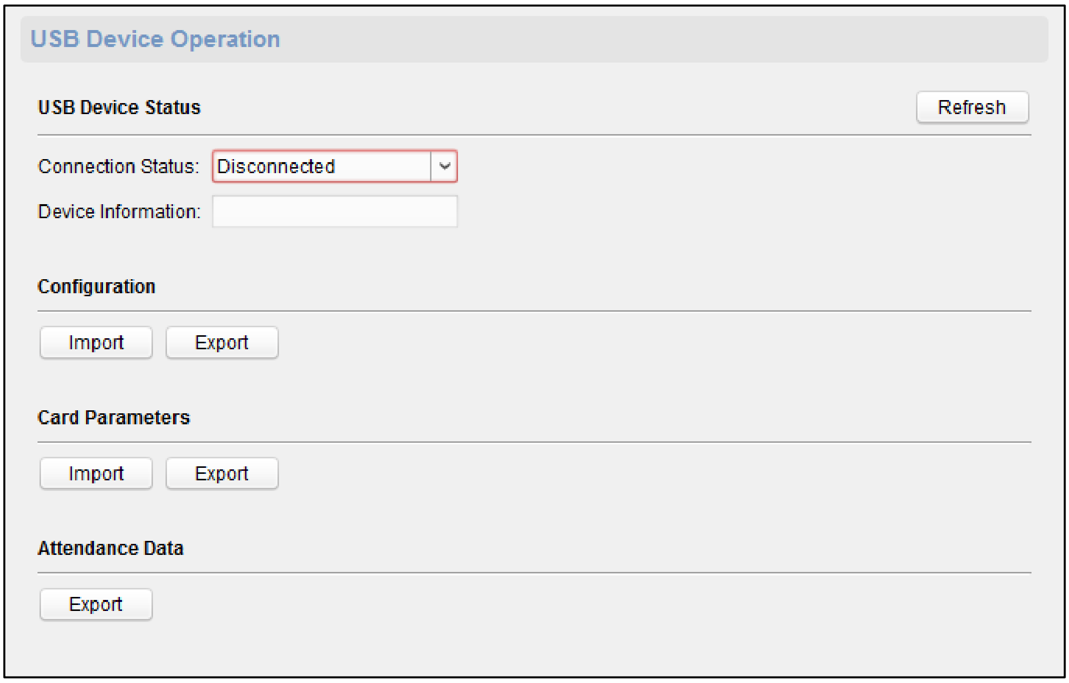
- **Operating USB Device**

Before you start:

Insert a USB device to the device.

Steps:

1. Click **Operation** -> **USB Device**.



USB Device Operation

USB Device Status

Connection Status: Disconnected

Device Information:

Configuration

Card Parameters

Attendance Data

2. You can select the USB connection status in the dropdown list. The USB device information will be displayed in the Device Information box.

3. Click Import or Export to import/export the configuration, the card paramters from/to the USB device.

   Or click Export to export the attendance data.

➢ **Checking Status**

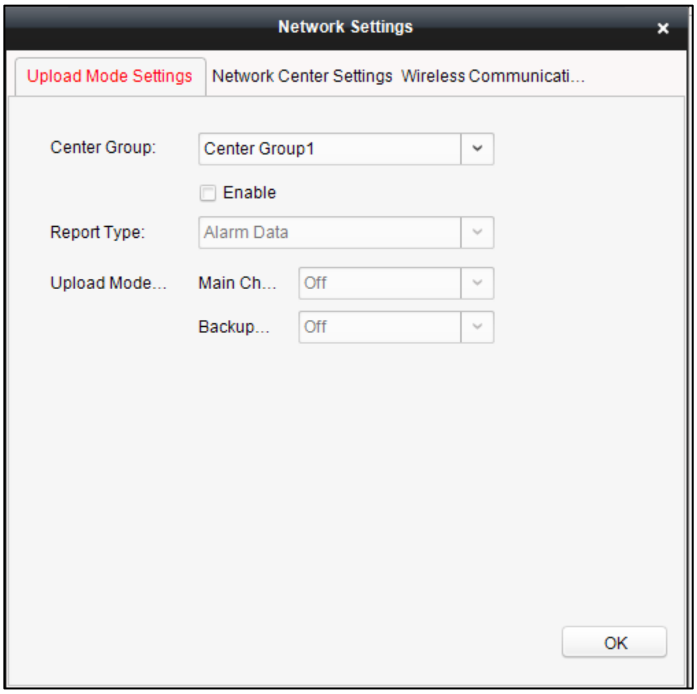
Click **Status** -> **Alarm** or **Status** -> **Trigger** to check the zone status and the trigger status.

19.1.3 Network Settings

Purpose:

In the network settings interface, the network settings of the device can be uploaded and reported.

Uploading Mode Settings



Center Group: Center Group1

□ Enable

Report Type: Alarm Data

Upload Mode... Main Ch... Off

Backup... Off

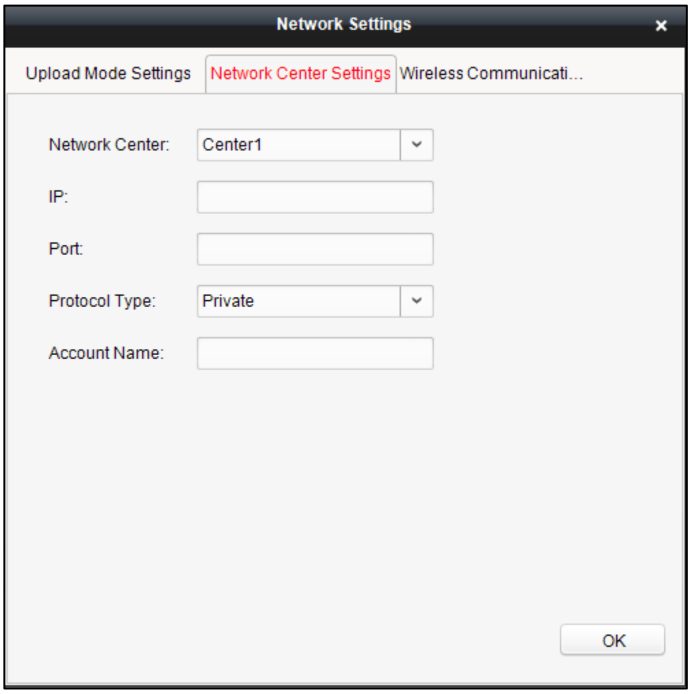
Steps:

1. In the access controller editing interface, click Network Settings button to enter the network settings interface.
2. Click **Uploading Mode Settings**.
3. Select the center group in the dropdown list.
4. Tick the **Enable** to enable the selected center group.
5. Select the report type in the dropdown list.
6. Select the uploading mode in the dropdown list. You can enable N1/G1 for the main channel and the backup channel, or select off to disable the main channel or the backup channel.

Note: The main channel and the backup channel cannot enable N1 or G1 at the same time.

7. Click the **OK** button to save parameters.

Network Center Settings



Network Center: Center1

IP:

Port:

Protocol Type: Private

Account Name:

Steps:

1. In the access controller editing interface, click Network Settings button to enter the network settings interface.
2. Click **Network Center Settings**.
3. Select the network center in the dropdown list.
4. Input IP address.
5. Input port number.
6. Select the protocol type: Private, NAL2300.

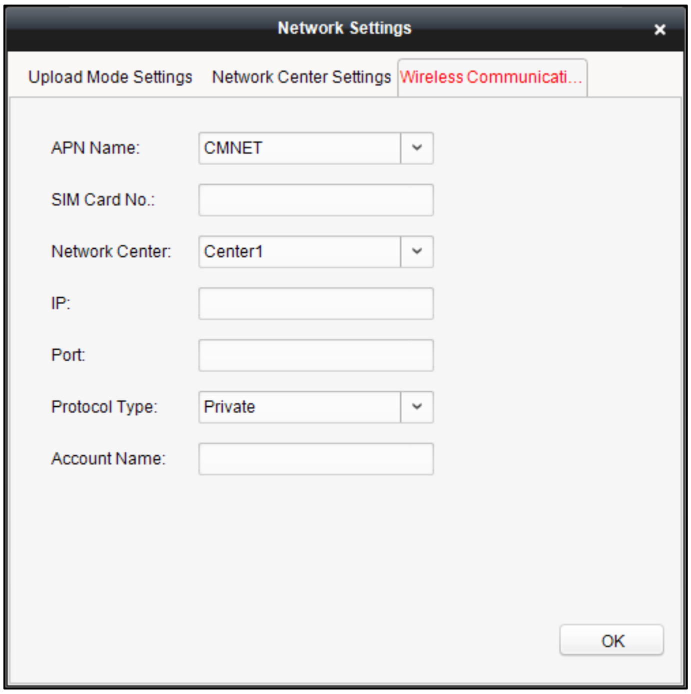
   Note: Ehome is not supported.
7. Set an account name for the network center. A consistent account should be used in one platform.
8. Click the **OK** button to save parameters.

Wireless Communication Center Setting

Steps:

1. In the access controller editing interface, click Network Settings button to enter the network settings interface.
2. Click **Wireless Communication Center Setting** to configure the report uploading type.
3. Configure the APN name, the SIM card center, the IP address, the port, the protocol type and the account name.

   Note: The protocol type of DS-K2700 Access Controller, DS-K27M01, DS-K27M02 or DS-K27M04 Distributed Access Controller does not support ehome.
4. Click the **OK** button to save the parameters.



APN Name: CMNET

SIM Card No.:

Network Center: Center1

IP:

Port:

Protocol Type: Private

Account Name:

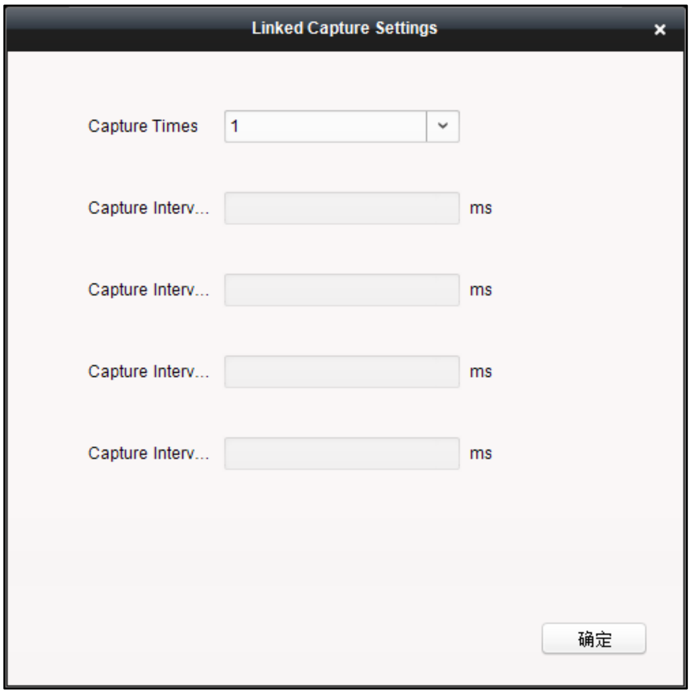
19.1.4 Linked Capture Settings (Do Not Support)

Purpose:

Configure the size and the quality of the linked capture picture, the linked capture times, and the capture interval.

Steps:

1. In the Edit Access Controller interface, click the button Linked Captur... .
2. In the pop-up window, configure the capture times and the interval.
3. Click the **OK** button to save the parameters.



Linked Capture Settings

Capture Times: 1

Capture Interv... ms

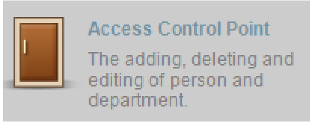
Capture Interv... ms

Capture Interv... ms

Capture Interv... ms

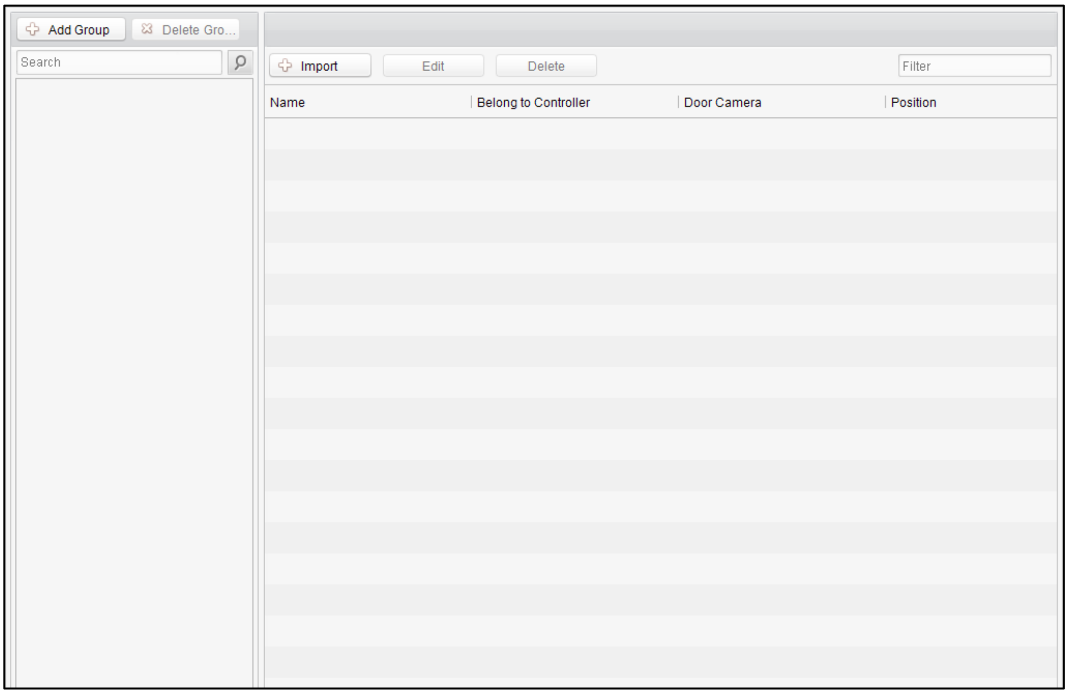
Note: Getting the linked capturing parameters from the device is available.

19.2 Access Control Point Management

Click the  icon on the control panel to enter the door management interface.

Access Control Point

The adding, deleting and editing of person and department.



Name	Belong to Controller	Door Camera	Position

Group Management

The doors can be added to different groups to realize the centralized management.

Door Management

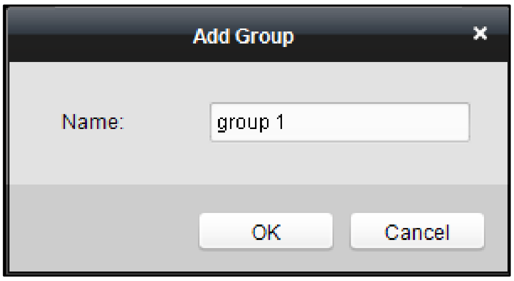
Manage the specific door under the door group, including importing, editing and deleting door.

19.2.1 Group Management

Adding Group

Steps:

1. Click the ✚ Add Group button to pop up the Add Group dialog.



Name: group 1

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

Note: Multi-level groups are not supported yet.

Editing Group

Steps:

Double-click the group or right-click the group and select Edit in the right-click menu.

Deleting Group

To delete a group, three ways are supported.

- Click to select a group and click the ☒ Delete Group button.
- Right-click a group and select Delete in the popup menu.
- Move the mouse onto the group and click ☒ icon of it.

And then click the OK button in the popup window.

19.2.2 Access Control Point Management

Purpose:

Access control points under the group can also be edited, refer to the following instructions.

Importing Access Control Point

Steps:

1. Click the ✚ Import button to pop up the access control point importing interface.
2. Select a access control point to import by clicking it.
3. Click to select a group in the right side bar to import to.
4. Click Import button to import the selected access control points or click Import All to import all the available access control points.

Notes:

- You can click ✚ button on the upper-right corner of the window to create a new group.
- Up to 64 access control points can be added.

Editing Access Control Point

Steps:

1. Click to select a access control point in the list and click the Edit button to edit the access control point.
2. Edit the Door Name and Position.
3. Click OK button to finish editing.

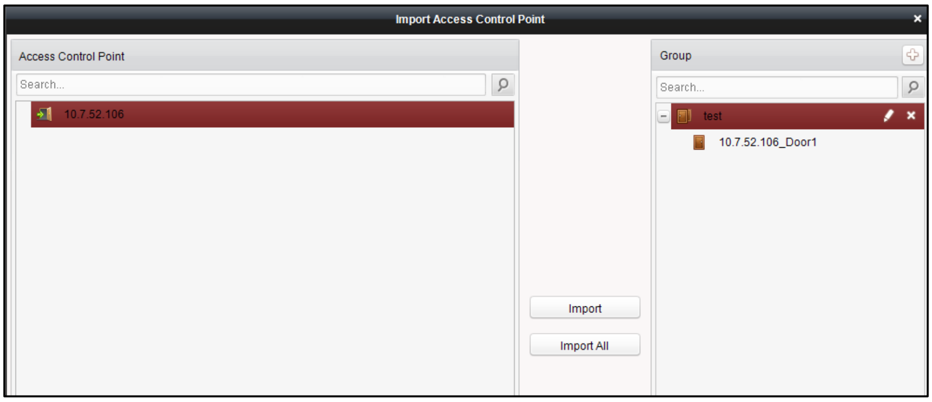
Note: you can also enter the Edit interface by double clicking the door from the list.

Deleting Access Control Point

Several ways are supported to delete the access control point, as shown below.

- Click to select a group in the group list, select door(s) under it, and click Delete button.
- Click to select a group in the group list, and click Delete button to delete all access control points under the group.
- Move the mouse onto a group in the group list, and click ☒ button to delete all access control points under the group.

Note: you can also edit/delete a door on the Import Access Control Point panel.



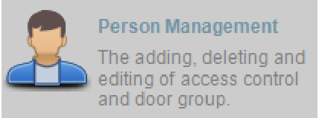
Steps:

1. Select a control point on the **Group** panel.

2. Click the ✎ /✕ icon to enter the **Edit Access Control Point** panel or to delete the control point.

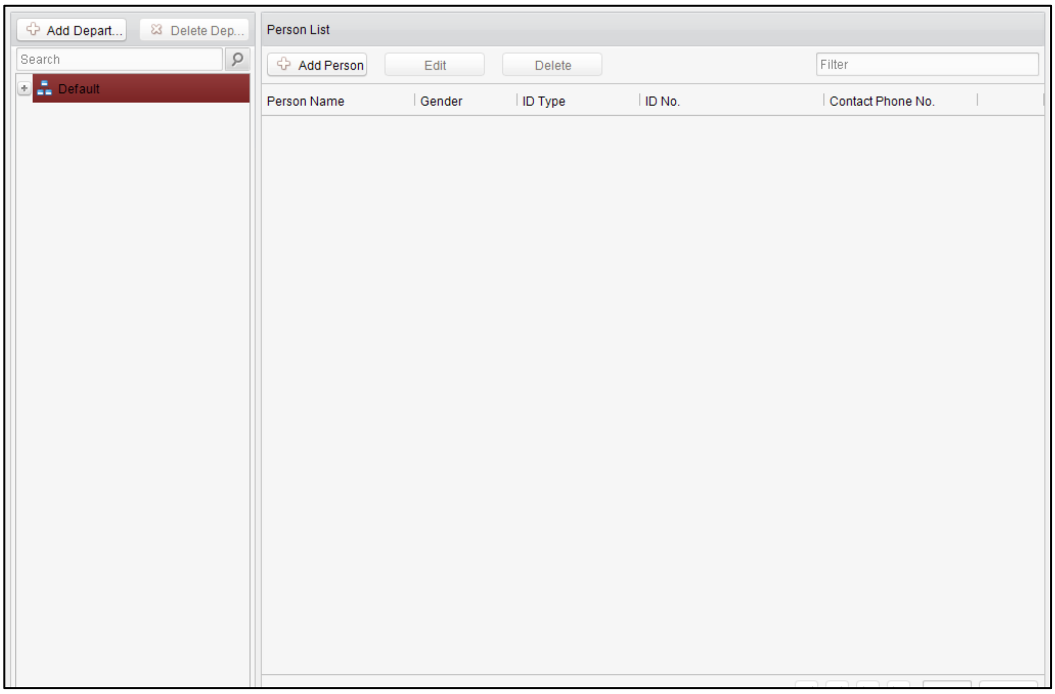
Chapter 20 Permission Management

20.1 Person Management

Click the  icon on the control panel of the software.

Person Management
The adding, deleting and editing of access control and door group.

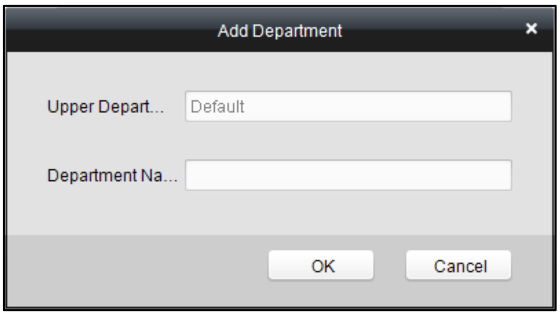
Adding, editing, deleting and filtering of the department and person are supported in this interface.



20.1.1 Department Management

Steps:

1. In the department list, click Add Depart... button to pop up the adding department interface.



Add Department

Upper Depart... Default

Department Na...

Notes:

- Multi-level department system can be created. Click a department as the upper-level deparment and click Add Depart... button, and then the added department will be the sub-department of it.
- Up to 10 levels can be created.

2. You can double-click an added department to edit its name.
3. You can click to select a department, and click the Delete Depa... button to delete it.

Notes:

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

20.1.2 Person Management

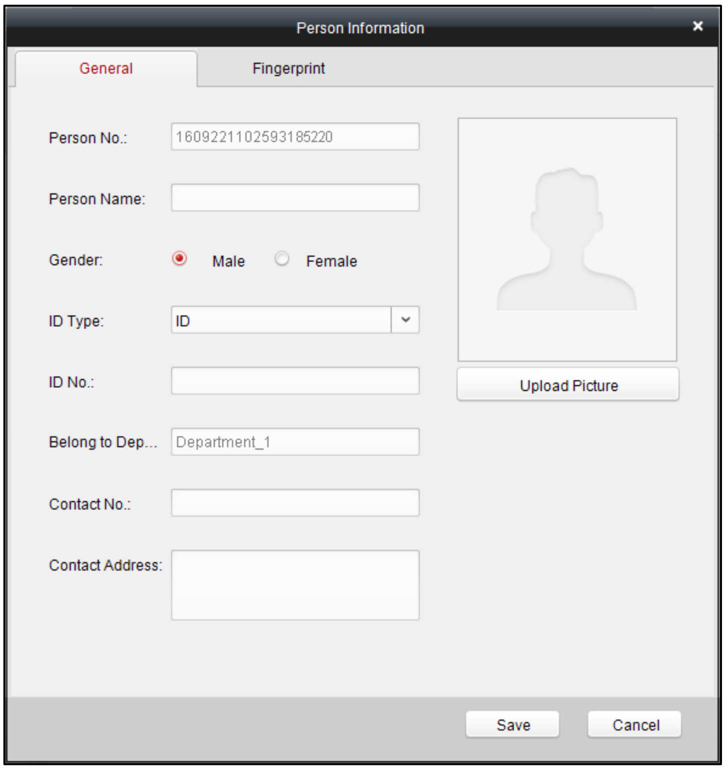
Notes:

- In the person management interface, double-click the person name or click the **Edit** button to edit the person informationt
- In the person management interface, click the **Delete** button to delete the person.
- Up to 2000 persons ban be added.

- **Inputting General Information**

Steps:

1. Select a department in the list and click the Add Person in the person infoarmation list to pop up the adding person interface.



Person No.: 1609221102593185220

Person Name:

Gender: ● Male ○ Female

ID Type: ID

ID No.:

Belong to Dep…: Department_1

Contact No.:

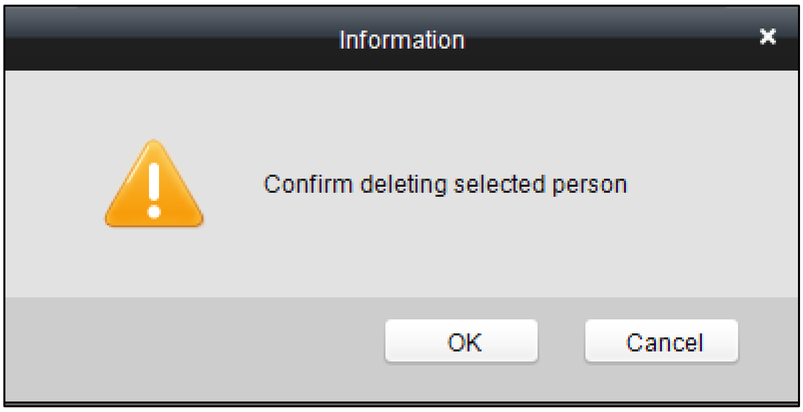
Contact Address:

2. Input the Person Name (required), Gender, ID Card, etc., upload the photo of the person and click the Save icon to finish adding.

   Note: The format of the photo should be .jpg, or .jpeg.

3. You can double-click an added person to edit its information.

4. You can click to select a person, and click the Delete button to delete it.



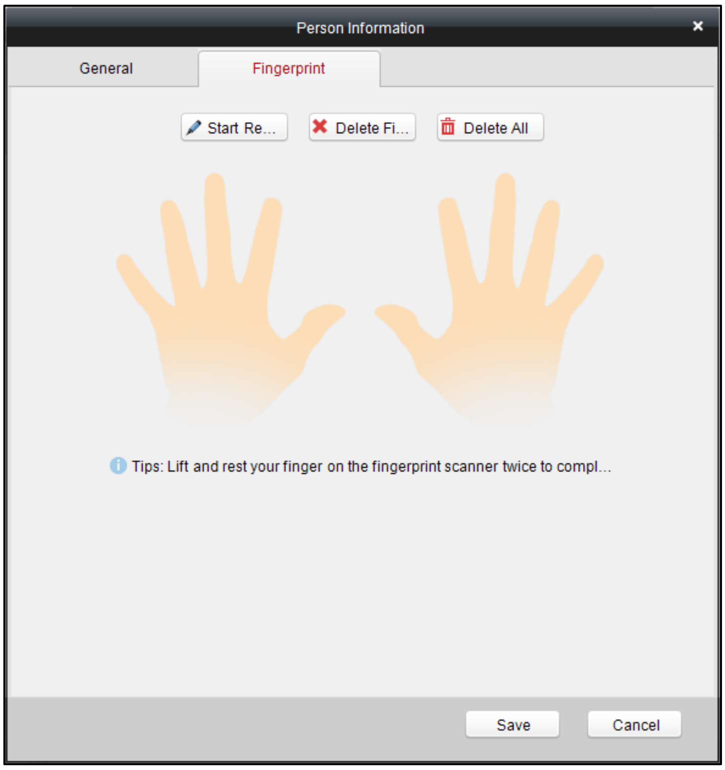
Confirm deleting selected person

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

- **Inputting Fingerprint**

Steps:

1. In the personal information interface, click the **Fingerprint** button.



Tips: Lift and rest your finger on the fingerprint scanner twice to compl...

2. Click the **Start Register** button, and select the fingerprint to be input. For details about inputting fingerprint, see *Chapter 24 Appendix: Tips for Scanning Fingerprint*.
3. Click the **Save** button to save the parameter.

Notes:

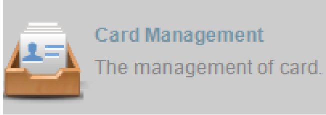
- Click the **Delete Fingerprint** button to delete the fingerprint.
- Click the **Delete All** button to clear all fingerprints input.

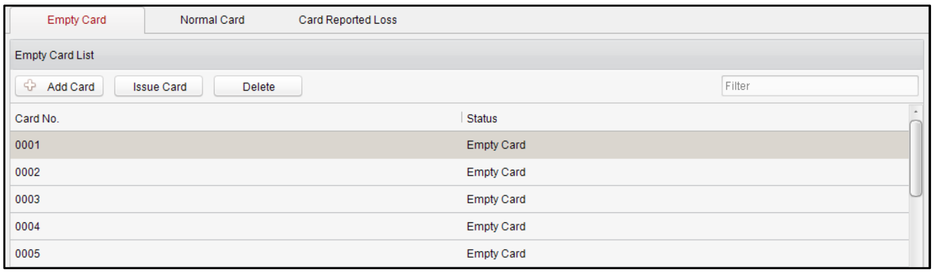
- **Editing Person Information**

Steps:

1. In the Person List in the Person Management interface, select a person.
2. Click Edit to enter the Person Information interface.
3. Edit the parameters.
   If possible, click Fingerprint to enter the fingerprints.
4. Click **Save** to save the parameters.

20.2 Card Management

Click  on the control panel of the software to enter the card management interface.


Empty Card | Normal Card | Card Reported Loss

Empty Card List

Card No.	Status
0001	Empty Card
0002	Empty Card
0003	Empty Card
0004	Empty Card
0005	Empty Card

The cards are divided into 3 types: Empty Card, Normal Card, and Lost Card.

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

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

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

20.2.1 Empty Card

- **Adding Card**

Before you start:

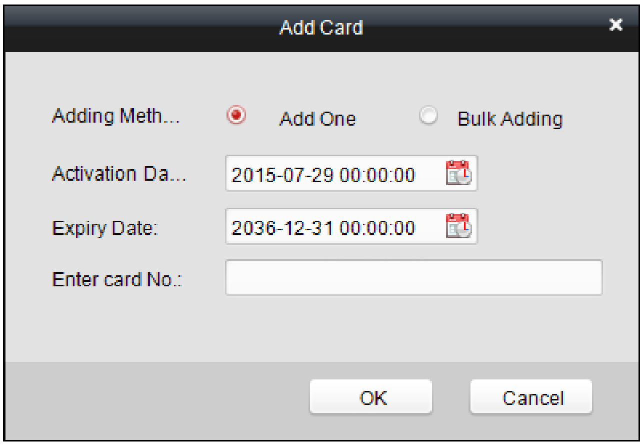
Make sure a card dispenser is connected to the PC and is configured already. Refer to Section *23.2.2 Card Dispenser Configuration* for details.

Steps:

1. Click the Add Card button to add cards.
2. Two modes of adding cards are supported.

   Adding Single Card

   Choose the Single Add as the adding mode by clicking the ○ to ● and input the Start Date, Expiring Date and Card No. in the text field.


Add Card

Adding Meth... ● Add One ○ Bulk Adding

Activation Da... 2015-07-29 00:00:00

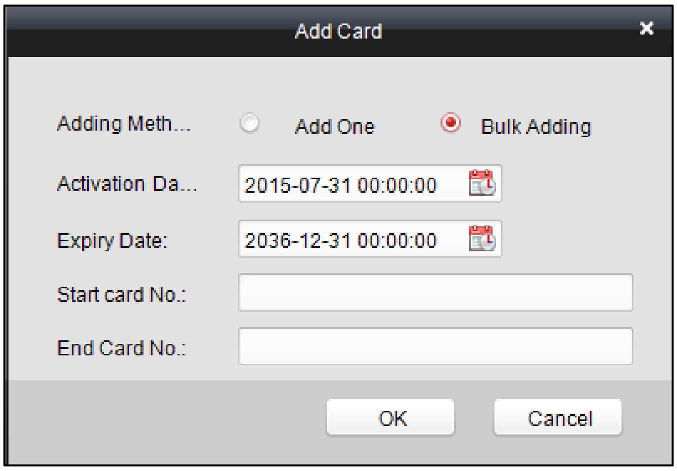
Expiry Date: 2036-12-31 00:00:00

Enter card No.:

Batch Adding Cards

Choose the **Bulking Adding** as the adding mode by clicking the ○ to ● and input the activation date, expiry date, start card No. and last card No. in the corresponding text fields.

Note: The start card No. and the last card No. should be the with same length. E.g., the last card No. is 234, then the start card No. should be like 028



Add Card

Adding Meth... ○ Add One ● Bulk Adding

Activation Da... 2015-07-31 00:00:00

Expiry Date: 2036-12-31 00:00:00

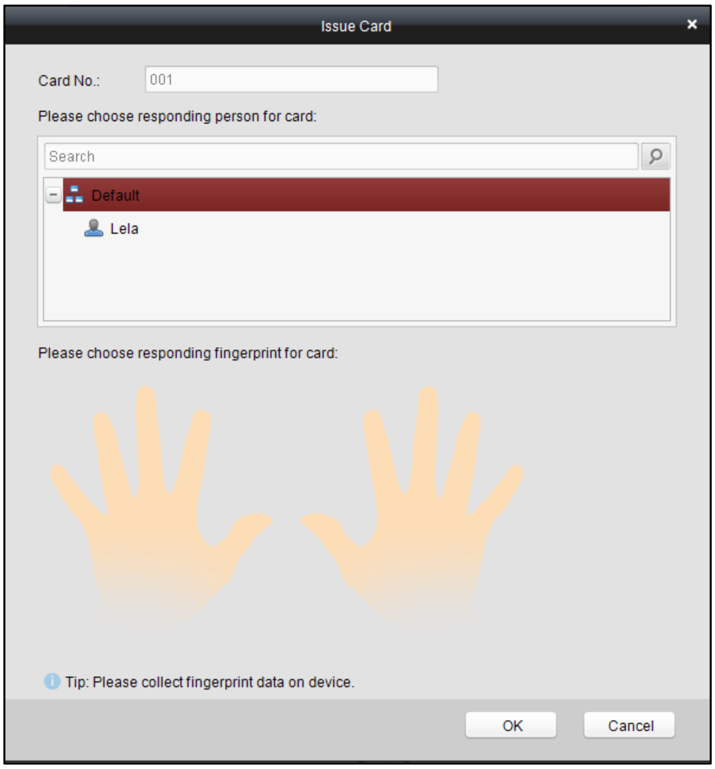
Start card No.:

End Card No.:

3. Click the OK button to finish adding.

4. Click an added empty card in the list and click Issue Card button to issue the card with a person.

Note: you can double click the empty card in the card list to enter the **Issue Card** Page.



Issue Card

Card No.: 001

Please choose responding person for card:

Please choose responding fingerprint for card:

Tip: Please collect fingerprint data on device.

5. Click to choose a person on your demand in the popup dialog box, select a fingerprint, and click OK to finish.

Notes:

- The issued card will disappear from the Empty Card list, you can check the card information in the Normal Card list.
- Up to 2000 cards can be added.

- Each card can link up to 10 fingerprints.

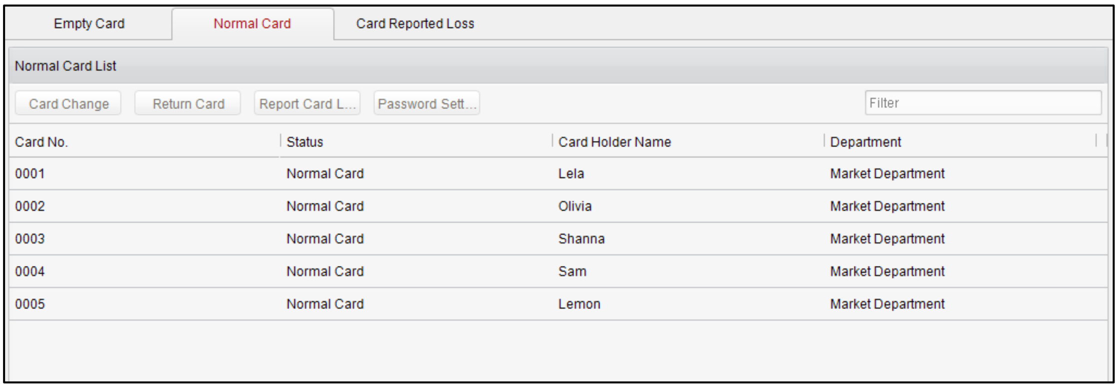
- **Deleting Card**

You can click an added empty card in the list and click Delete button to delete the selected card.

20.2.2 Normal Card

Purpose:

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



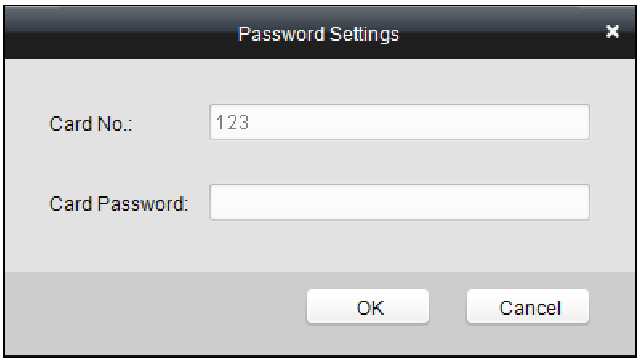
Card No.	Status	Card Holder Name	Department
0001	Normal Card	Lela	Market Department
0002	Normal Card	Olivia	Market Department
0003	Normal Card	Shanna	Market Department
0004	Normal Card	Sam	Market Department
0005	Normal Card	Lemon	Market Department

- ◆ Click to select a card and click Card Change button to change the associated card for card holder. Select another card in the popup window to replace the current card. The old card will turn to the empty card. You should configure the permission to the card again.

- ◆ Click to select an issued card and click Return Card to cancel the assotiation of the card, then the card will disappear from the Normal Card list, which you can find it in the Empty Card list. You should configure the permission to the card again.

- ◆ Click to select an issued card and click Report Card L... (Report Card Loss) to set the card as the Lost Card, that is, an invalid card.

- ◆ Click to select an issued card and click Password Sett... (Password Settings) to set the password for the card, set the password in the text filed and click the **OK** button to finish setting.



Password Settings

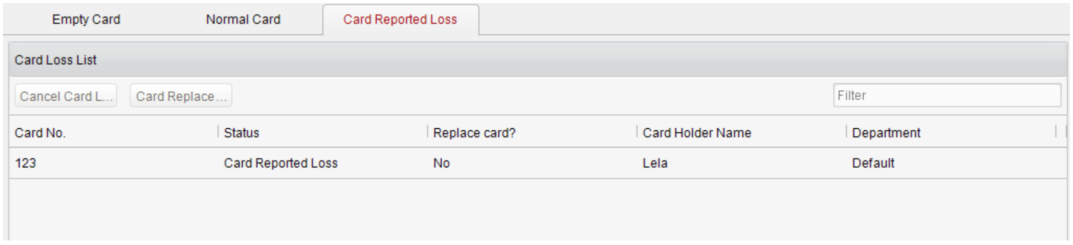
Card No.: 123

Card Password:

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&password authentication on the advanced configuration page.

20.2.3 Lost Card

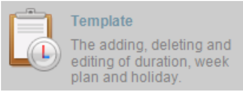
Click the Card Reported Loss tab in the card managemet interface to show the Lost Card list. You can view all the lost card information, including card No., card holder, and the department of the card holder.



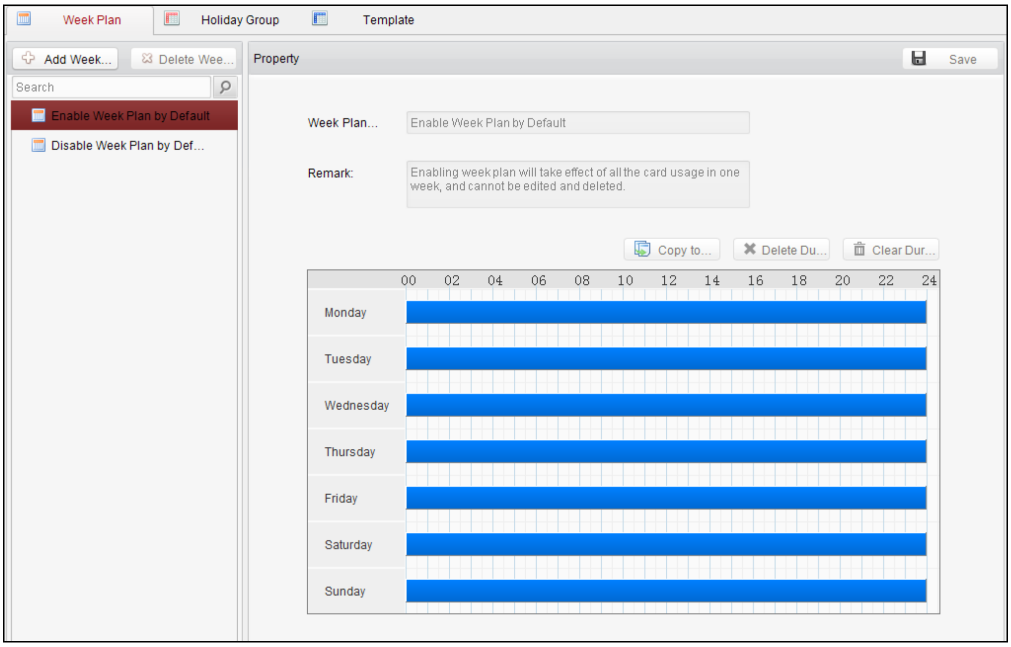
Card No.	Status	Replace card?	Card Holder Name	Department
123	Card Reported Loss	No	Lela	Default

- Click the **Cancel Card Loss** button to resume the card to the normal card. You should configure the permission to the card again.
- Click the **Card Replacement** button to issue a new card to the card holder replacing for the lost card. Select another card in the popup window as the new card and the predefined permissions of the lost card will be copied to the new one automatically.

20.3 Schedule Template

Click  on the control panel of the software to enter the schedule template interface.

Template
The adding, deleting and editing of duration, week plan and holiday.



Week Plan...: Enable Week Plan by Default

Remark: Enabling week plan will take effect of all the card usage in one week, and cannot be edited and deleted.

There are 3 settings in this interface: Week Plan, Holiday Group, and Template.

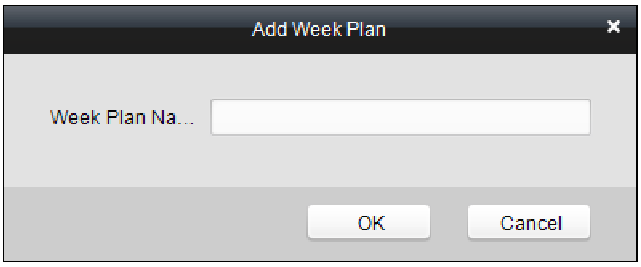
20.3.1 Setting Week Plan

- **Adding Week Plan**

System defines 2 kinds of week plan by default, Enable Week Plan by Default and Disable Week Plan by Default. You can define custom plans on your demand.

Steps:

1. Click the **Add Week Plan** button to pop up the adding plan interface.



2. Input the name of week plan and click the **OK** button to add the week plan.
3. Select a week plan in the plan list on the left-side of the window to edit.
4. Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that period of time, the cofigured permission is activated.
5. Repeat the above step to configure other time periods.

   Or you can select a configured day and click the **Copy to Week** button to copy the same settings to the whole week.

   Note: Up to 8 time periods can be added in one day.

- **Deleting Week Plan**

  - Click to select a configured duration and click the **Delete Duration** button to delete it.
  - Click the **Clear Duration** button to clear all the configured durations, while the week plan

still exists.

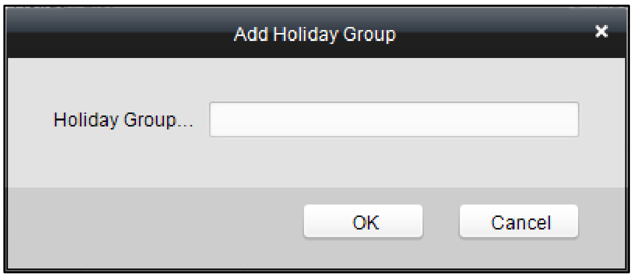
- Click the **Delete Week Plan** button to delete the week plan directly.

20.3.2 Setting Holiday Group

- **Adding Holiday Group**

Steps:

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



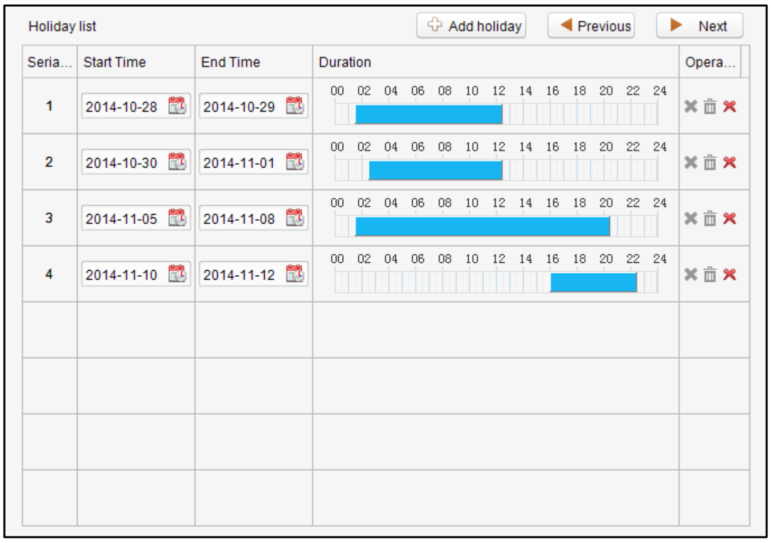
Add Holiday Group ×

Holiday Group...

2. Input the name of holiday group in the text filed and click the OK button to add the holiday group.

3. Click the ✚ Add holiday icon to add a holiday in the holiday list and configure the duration of the holiday.

   Note: At most 16 holiday periods can be added.



Seria...	Start Time	End Time	Duration	Opera...
1	2014-10-28	2014-10-29	00 02 04 06 08 10 12 14 16 18 20 22 24	✖ 🗑 ✖
2	2014-10-30	2014-11-01	00 02 04 06 08 10 12 14 16 18 20 22 24	✖ 🗑 ✖
3	2014-11-05	2014-11-08	00 02 04 06 08 10 12 14 16 18 20 22 24	✖ 🗑 ✖
4	2014-11-10	2014-11-12	00 02 04 06 08 10 12 14 16 18 20 22 24	✖ 🗑 ✖

   1) Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that duration, the cofigured permission is activated.
   2) Click to select a configured duration and click the ✖ to delete it.
   3) Click the 🗑 to clear all the configured durations, while the holiday still exists.
   4) Click the ✖ to delete the holiday directly.

4. Click the 💾 Save button to save the settings.

Note: The holidays cannot be overlapped with each other.

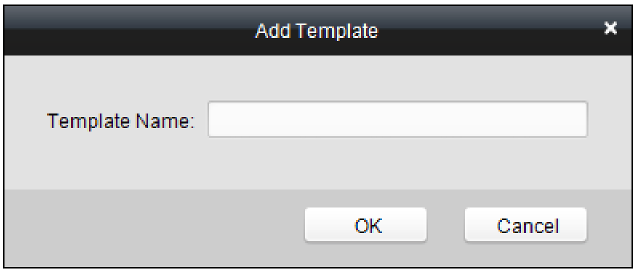
20.3.3 Setting Schedule Template

The schedule consists of week plan and holiday group; you can only choose which plan and group to enable in the schedule template configuration interface. Configure the week plan and holiday group before configuring the schedule template.

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

Steps:

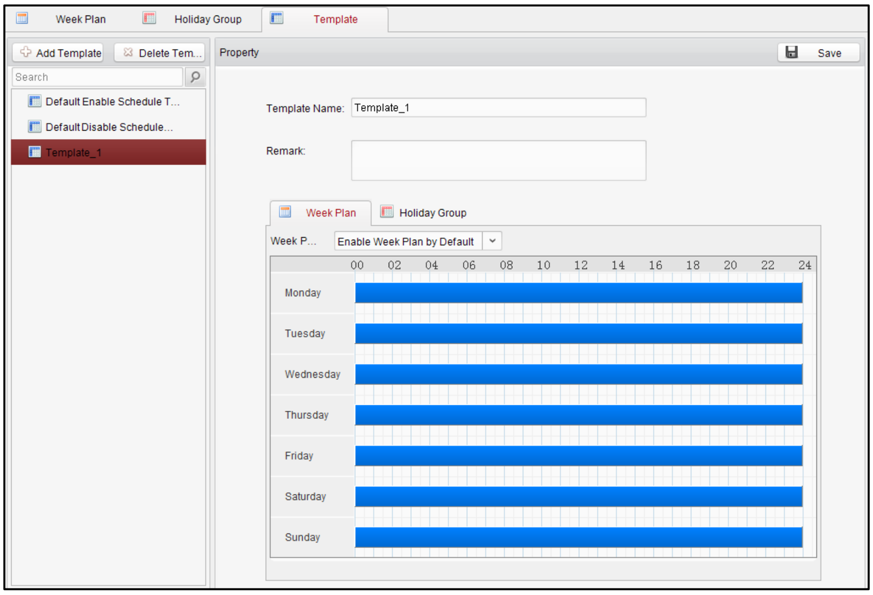
1. Click the Add schedul... to pop up the adding schedule interface.



Add Template

Template Name:

2. Input the name of schedule in the text filed and click the OK button to add the schedule.
3. Select a week plan you want to apply to the schedule.
   Click the Week Plan tab and select a plan in the dropdown list.

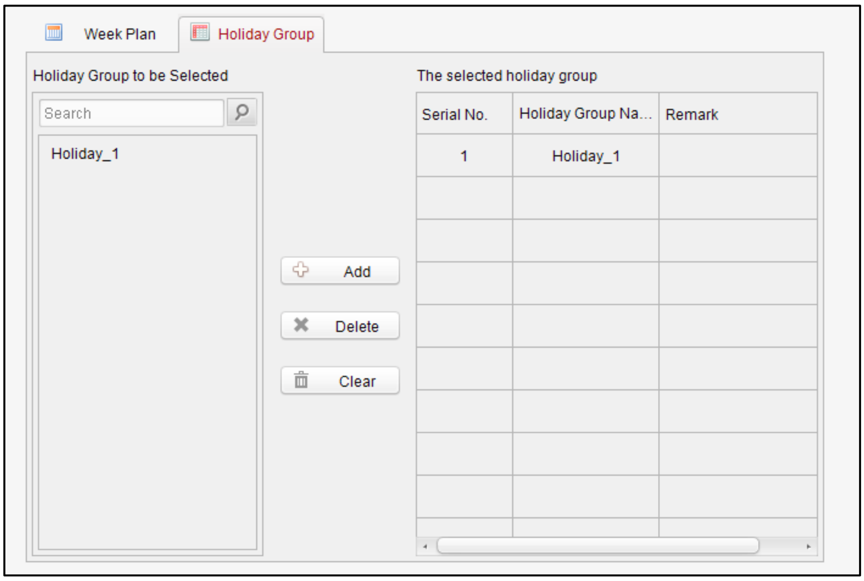


Template Name: Template_1

Remark:

Week P... Enable Week Plan by Default

4. Select holiday groups you want to apply to the schedule.
   Note: At most 4 holiday groups can be added.



Serial No.	Holiday Group Na...	Remark
1	Holiday_1	

- ◆ Click to select a holiday group in the left-side list and click the Add to add it.

- ◆ Click to select an added holiday group in the right-side list and click the Delete to delete the it.

- ◆ Click the Clear to delete all the added holiday groups.

5. Click the Save button to save the settings.

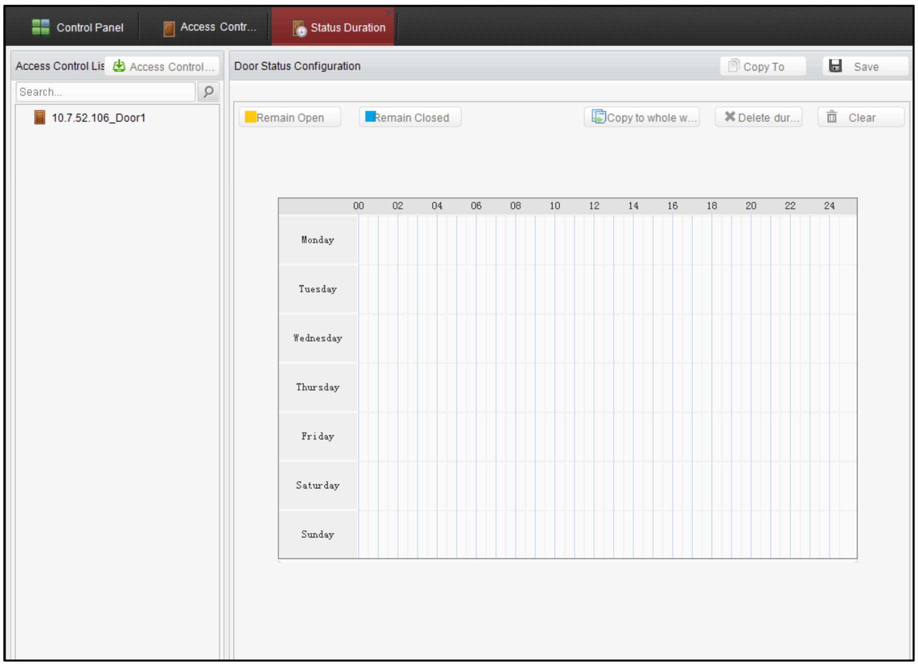
   Note: Up to 4 schedule templates can be added.

20.4 Door Status Management

Purpose:

The function of **Door Status Management** allows you to schedule weekly time periods for a door to remain open or closed.

Click the Status Duration Configure the door state Durations. icon on the control panel to enter the interface.



Steps:

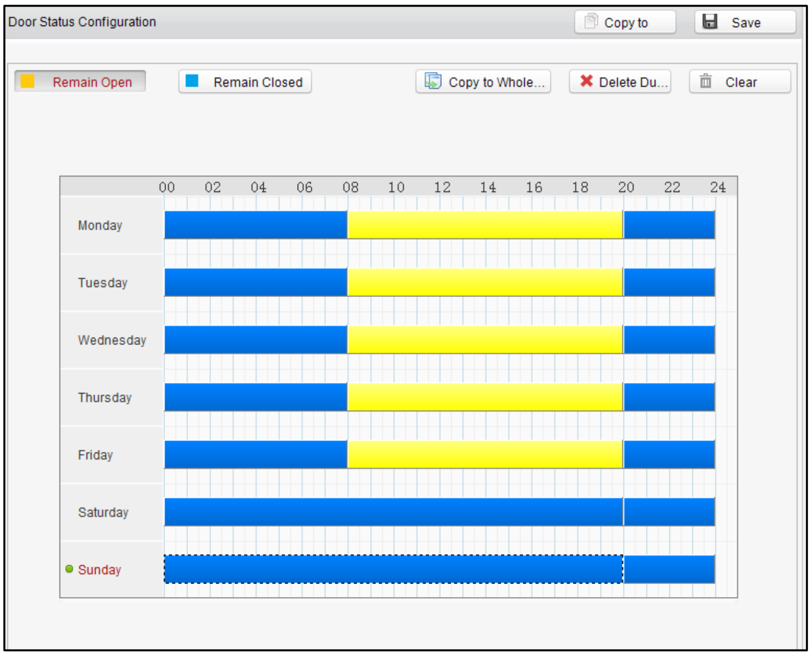
1. Enter the Door Status Management page.
2. Click and select a door from the door list on the left side of the page.
3. Draw a schedule map.

   1) Select a door status brush 🟨Remain Open / 🟦Remain Closed on the upper-left side of the **Door Status Settings** panel.

      Remain open: the door will keep open during the configured time period. The brush is marked as yellow.

      Remain Closed: the door will keep closed during the configured duration. The brush is marked as blue.

   2) Click and drag the mouse to draw a color bar on the schedule map to set the duration.



Notes

- The min. segment of the schedule is 30min.
- You can copy the configured time periods of a day to the whole week.

Steps:

1. Select a day which has already been configured.
2. Click on Copy to whole w... to copy the time periods to the whole week.

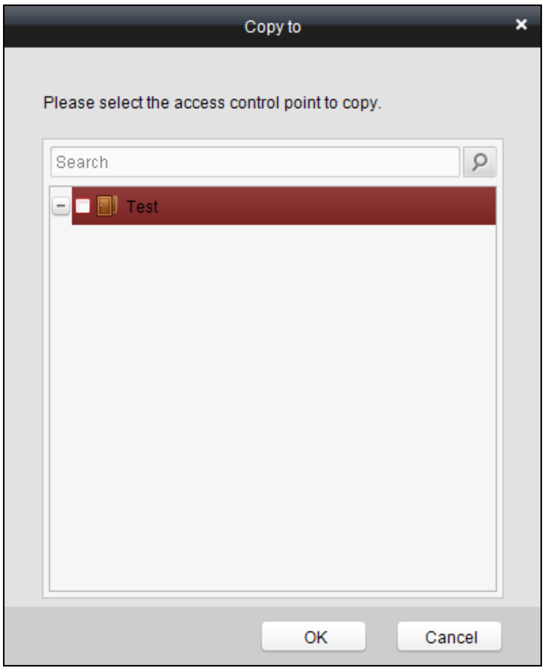
4. Edit the schedule map.
   - **Edit Duration:**

     Click and drag the color bar on the schedule map and you can move the bar on the time track.

     Click and drag the mouse on the ends of the color bar and you can adjust the length of the bar.
   - **Delete a Duration:**

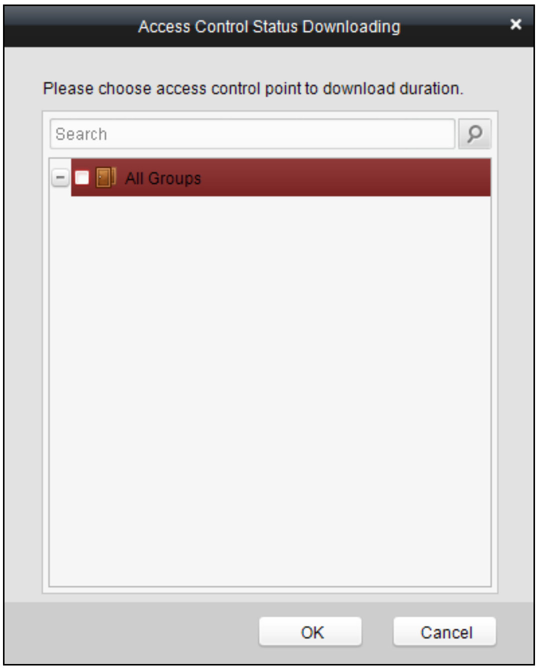
     Click and select a color bar and click ✖ Delete dur... to delete the time period.
   - **Clear All Durations:**

     Click Clear to clear all configured durations on the schedule map.
5. Click on Save to save the settings.
6. You can copy the schedule to other doors by clicking on Copy To and select the required doors.



Please select the access control point to copy.

7. Click on Access Control... to enter the Download Door State page.



Please choose access control point to download duration.

8. Select a control point and click **OK** to download the settings to the system.

20.5 Interact Configuration

Click Interact Configuration Case, event/card interaction configuration. on the control panel of the software to enter the interact configuration interface.

In this interface, you can set alarm linkage modes of the access host, including the event card interact, and the client interact.

20.5.1 Event Card Interact

In the Interact Configuration interface, click the **Event Card Interact** button to enter the settings interface.

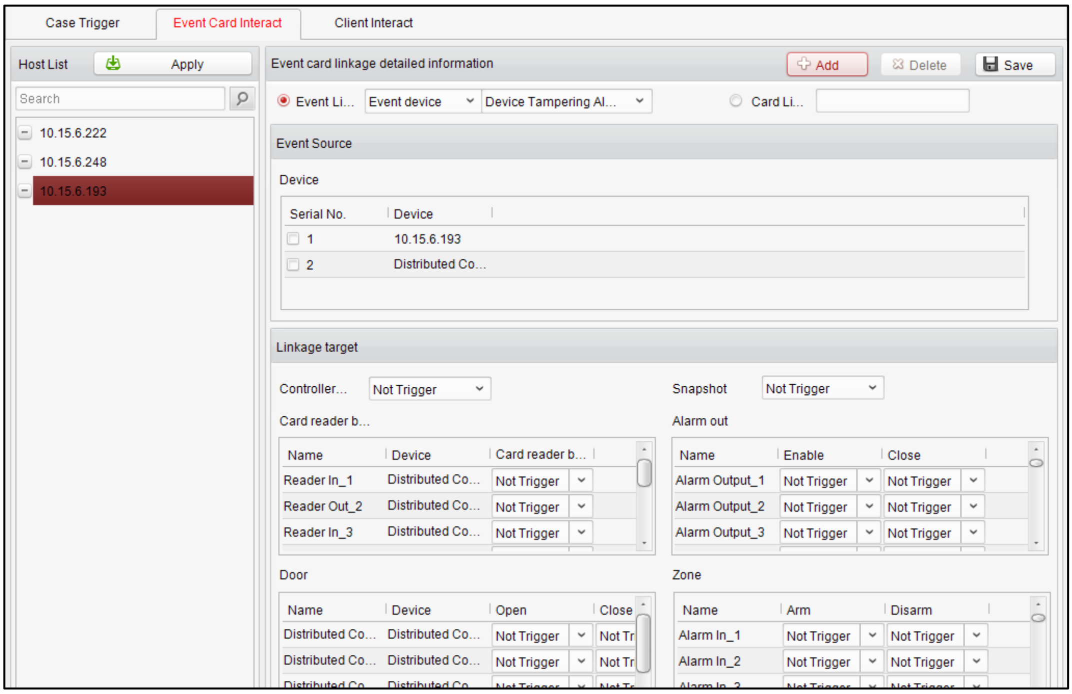
Note: Do not support the Case Trigger function.

- **Event Linkage**

In the Event Interact interface, the linkage alarm action, after triggering alarm event, can be set. The alarm event can be divided into four types: event device, event input alarm, door event, and card reader event.

Steps:

1. Click the Event Card Interact tab to enter the event card interface.
2. Select the host to be set from the host list.
3. Click Add to start setting the event linkage.



● Event Li... Event device Device Tampering Al... ○ Card Li...

Event Source

Device

Serial No.	Device
□ 1	10.15.6.193
□ 2	Distributed Co...

Linkage target

Controller... Not Trigger

Snapshot Not Trigger

Card reader b...

Name	Device	Card reader b...
Reader In_1	Distributed Co...	Not Trigger
Reader Out_2	Distributed Co...	Not Trigger
Reader In_3	Distributed Co...	Not Trigger

Alarm out

Name	Enable	Close
Alarm Output_1	Not Trigger	Not Trigger
Alarm Output_2	Not Trigger	Not Trigger
Alarm Output_3	Not Trigger	Not Trigger

Door

Name	Device	Open	Close
Distributed Co...	Distributed Co...	Not Trigger	Not Tr
Distributed Co...	Distributed Co...	Not Trigger	Not Tr

Zone

Name	Arm	Disarm
Alarm In_1	Not Trigger	Not Trigger
Alarm In_2	Not Trigger	Not Trigger

4. Click the radio button of the event linkage, and select the event type from the dropdown list.
5. Set the linkage target, and set the property as **Trigger** to enable this function.

   Controller Buzzer: The audible warning of controller will be triggered.

   Snapshot: Select Trigger in the dropdown list. The connected device real-time capture will be triggered.

   Card Reader Buzzer: The audible warning of card reader will be triggered.

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

   Door: The door status of open, close, normally open, and normally close will be triggered.

   Zone: The zone status of arm or disarm.
6. Click Save to save parameters.
7. Click Apply to apply the updated parameters to the local memory of the device.

Notes:

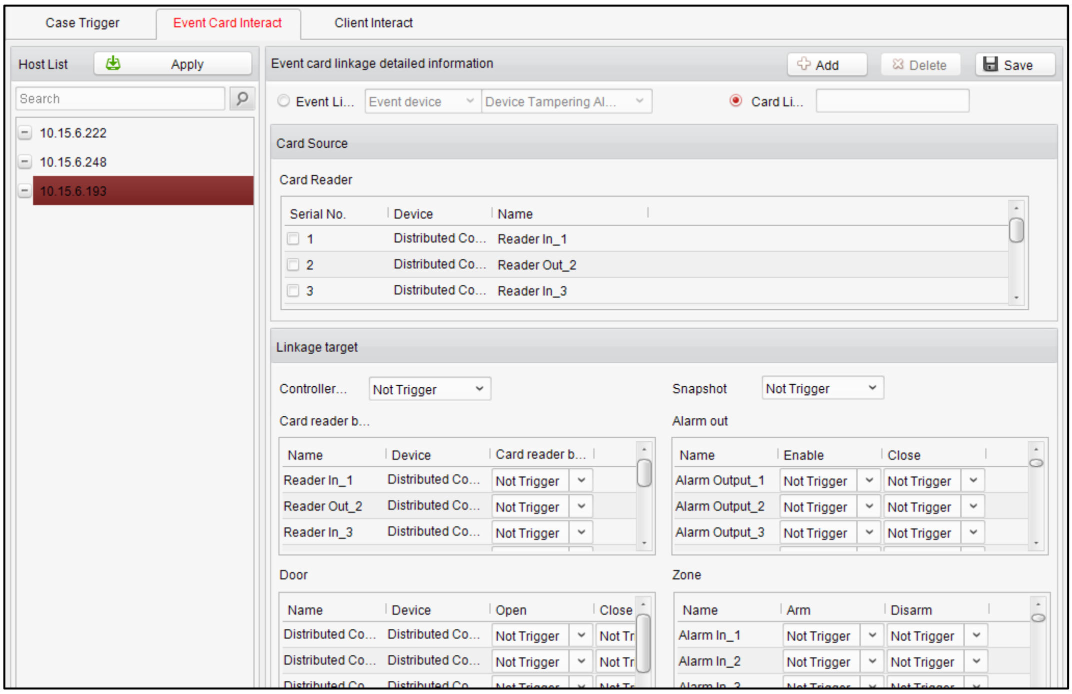
- The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- The normal access controller can configure up to 50 event linkages and card linkages. The device of DS-K2700 can configure up to 500 event linkages and card linkages.

- **Card Linkage**

In the Event Interact interface, the linkage alarm action, after triggering the card number, can be set.

Steps:

1. Click the Event Card Interact tab to enter the event card interact interface.
2. Select the host to be set from the host list.
3. Click Add to start setting the event linkage.



Serial No.	Device	Name
□ 1	Distributed Co...	Reader In_1
□ 2	Distributed Co...	Reader Out_2
□ 3	Distributed Co...	Reader In_3

Name	Device	Card reader b...
Reader In_1	Distributed Co...	Not Trigger
Reader Out_2	Distributed Co...	Not Trigger
Reader In_3	Distributed Co...	Not Trigger

Name	Enable	Close
Alarm Output_1	Not Trigger	Not Trigger
Alarm Output_2	Not Trigger	Not Trigger
Alarm Output_3	Not Trigger	Not Trigger

Name	Device	Open	Close
Distributed Co...	Distributed Co...	Not Trigger	Not Tr
Distributed Co...	Distributed Co...	Not Trigger	Not Tr
Distributed Co...	Distributed Co...	Not Trigger	Not Tr

Name	Arm	Disarm
Alarm In_1	Not Trigger	Not Trigger
Alarm In_2	Not Trigger	Not Trigger
Alarm In_3	Not Trigger	Not Trigger

4. Click the radio button of card linkage, and input the card number.
5. Select the event source, and check the checkbox of the card reader's serial number.
6. Set the linkage target, and set the property as **Trigger** to enable this function.

   Controller Buzzer: The audible warning of controller will be triggered.

   Snapshot: Select Trigger in the dropdown list. The connected device real-time capture will be triggered.

   Card Reader Buzzer: The audible warning of card reader will be triggered.

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

   Door: The door status of open, close, normally open, and normally close will be triggered.

   Zone: The zone status of arm or disarm.

7. Click the Save button to save parameters.

8. Click Apply to apply the updated parameters to the local memory of the device.

Notes:

- The door status of open, close, normally open, and normally close cannot be triggered at the same time.
- The normal access controller can configure up to 50 event linkages and card linkages. The device of DS-K2700 can configure up to 500 event linkages and card linkages.

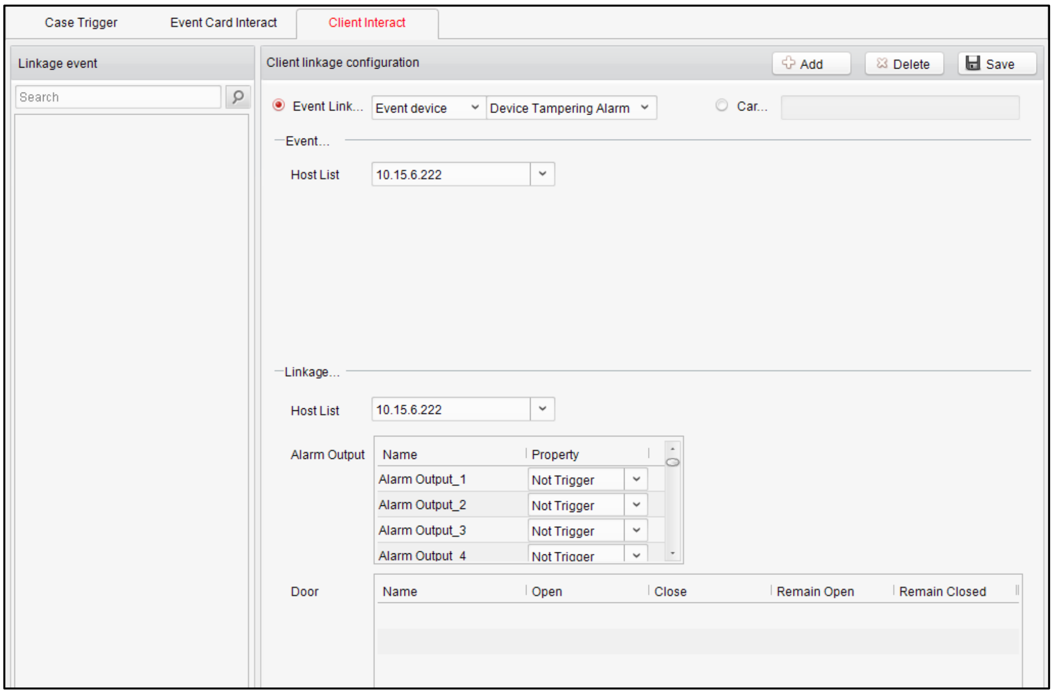
20.5.2 Client Interact

Purpose:

The alarm event will be sent to the client software to trigger other devices operation.

Steps:

1. Click **Client Interact** to enter the Client Interact tab.



Case Trigger | Event Card Interact | Client Interact

Linkage event

Search

Client linkage configuration — Add | Delete | Save

● Event Link... Event device | Device Tampering Alarm ○ Car...

Event...

Host List: 10.15.6.222

Linkage...

Host List: 10.15.6.222

Alarm Output

Name	Property
Alarm Output_1	Not Trigger
Alarm Output_2	Not Trigger
Alarm Output_3	Not Trigger
Alarm Output_4	Not Trigger

Door

Name	Open	Close	Remain Open	Remain Closed

2. Click Add.
3. Select an event linkage main type and the corresponding minor type in the dropdown list.
4. Select a host in the Host List dropdown list.

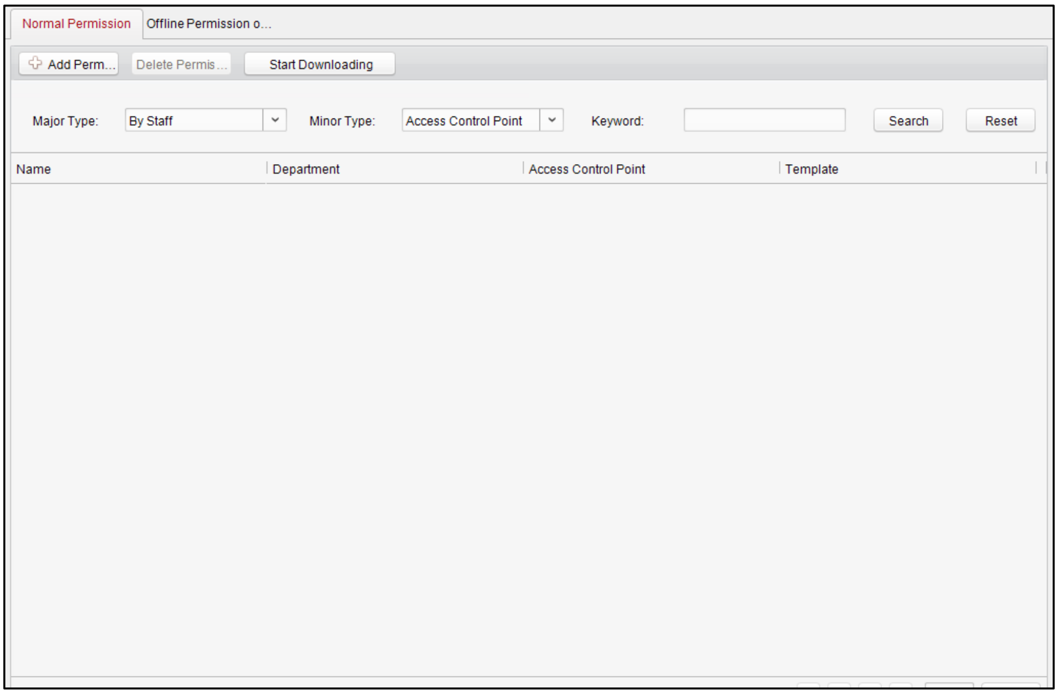
   If you do not select the alarm input event, in the main type dropdown list, you should check an alarm input.
5. Configure the Linkage Target parameters. You are able to link the event to the alarm output and the door status. Select Trigger in the Property dropdown list to link the alarm output to the event.

   Or click Card Linkage, input the card No., check a card reader and the configure the linkage target.
6. Click Save to save the parameters. The saved event will be displayed in the linkage event list.

   Or select an event in the Linkage event list and click Delete to delete the event.

20.6 Access Permission Configuration

Click the Access Control Permis... The adding, deleting and downloading of access control permission. icon on the control panel to enter the interface.



20.6.1 Access Permission Settings

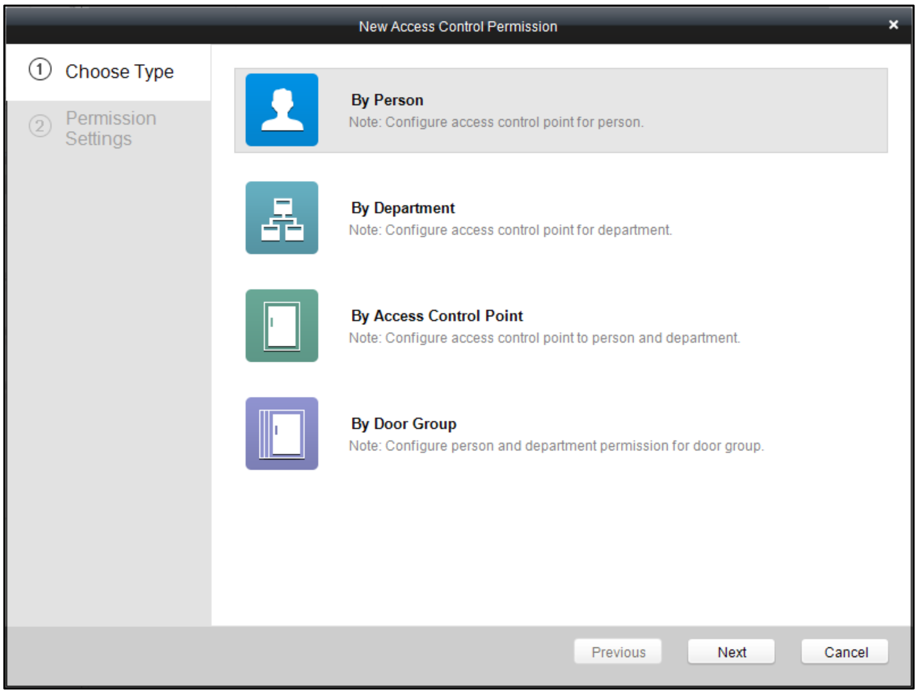
Purpose:

You can allocate permission for people/department to enter/exist the control points (doors) and the offline permission of the distributed access controller in this section.

Normal Permission Settings

Steps:

1. Enter the Access Control Permission page.
2. Click **Normal Permission** to enter the Normal Permission tab.
3. Click Add Permi... (Add Permission) on the upper-left side of the page to enter the Add Permission window.



New Access Control Permission

① Choose Type

② Permission Settings

By Person
Note: Configure access control point for person.

By Department
Note: Configure access control point for department.

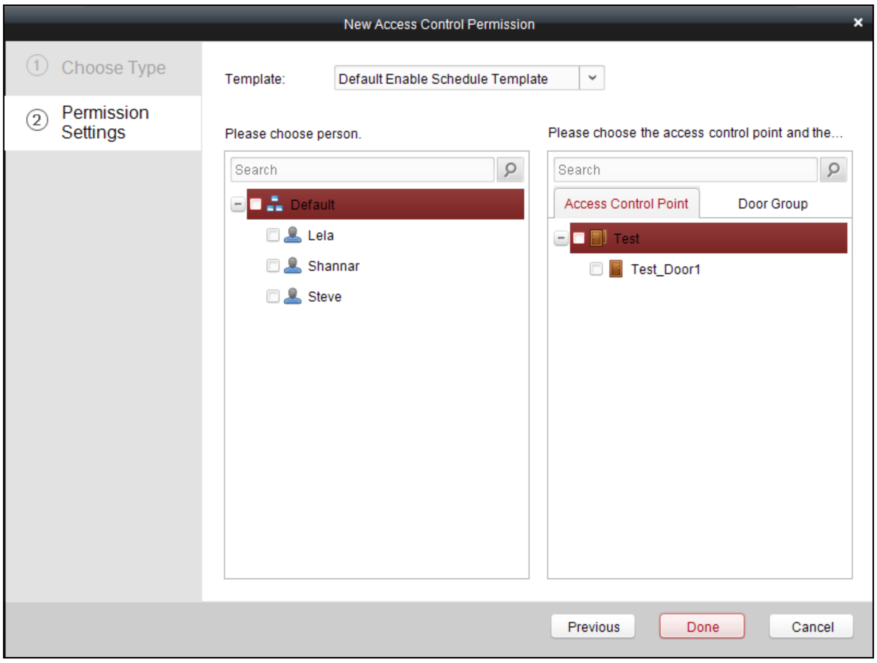
By Access Control Point
Note: Configure access control point to person and department.

By Door Group
Note: Configure person and department permission for door group.

4. Select an adding type in the **Select Type** interface.

   - **By Person:** you can select people from the list to enter/exit the door. The following steps will take By Person as an example.
   - **By Department:** You can select departments from the list to enter/exit the door. Once the permission is allocated, all the people in this department will have the permission to access the door.
   - **By Access Control Point:** You can select doors from the door list for people to enter/exit.
   - **By Door Group:** You can select groups from the door list for people to enter/exit. The permission will take effect on the door in this group.

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



New Access Control Permission

① Choose Type

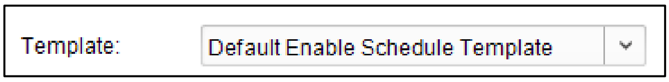
② Permission Settings

Template: Default Enable Schedule Template

Please choose person.

Please choose the access control point and the...

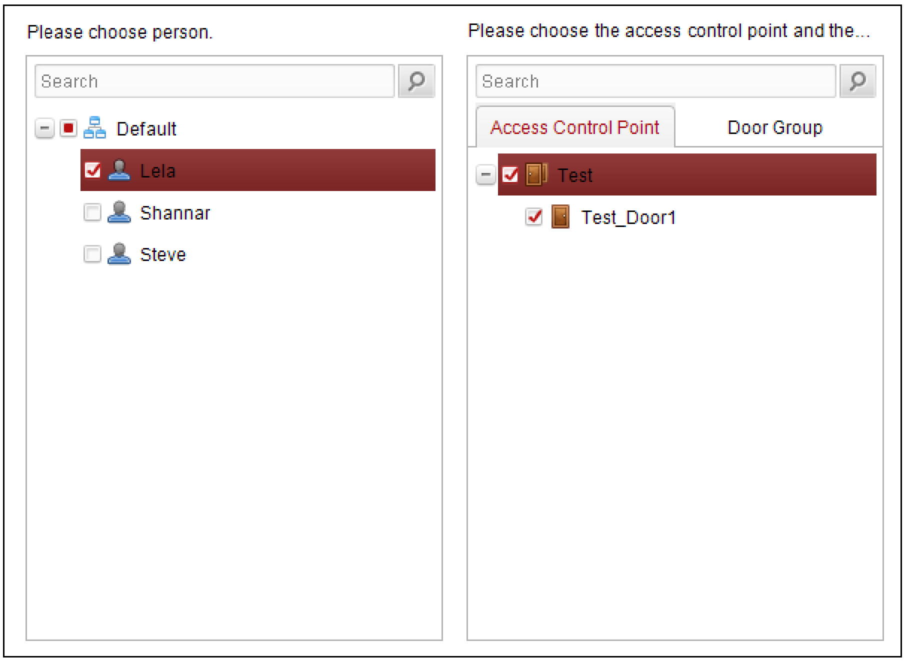
6. Click on the dropdown menu to select a schedule template for the permission.



Template: Default Enable Schedule Template

Note: The schedule template must be configured before any permission settings. Refer to *Section 20.3 Schedule Template* for detailed configuration guide.

7. Select people/ department and corresponding doors/door groups from the appropriate lists.



Please choose person.

Search

- Default
  - ☑ Lela
  - □ Shannar
  - □ Steve

Please choose the access control point and the...

Search

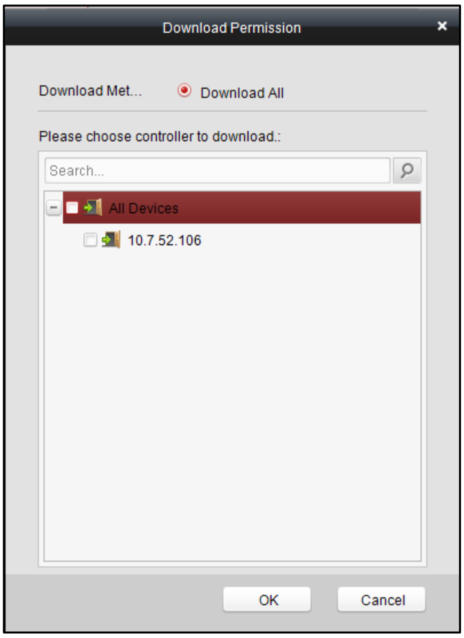
Access Control Point | Door Group

- ☑ Test
  - ☑ Test_Door1

Note: The lower-level of department will also be selected if the highest-level of department is selected.

8. Click the **Done** button to complete the permission adding.

9. Click Start Downloading to enter the **Download Permission** page.



Download Permission

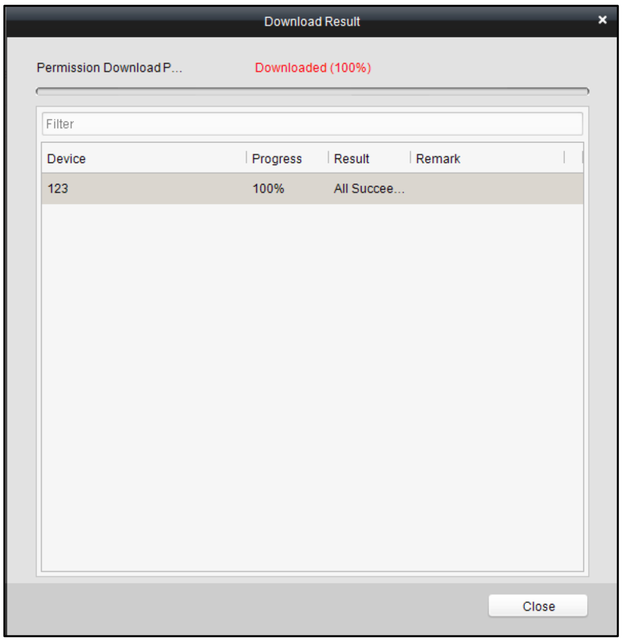
Download Met... ● Download All

Please choose controller to download.:

Search...

- □ All Devices
  - □ 10.7.52.106

10. Select the control point and click the **OK** button, to enter the download result interface, to download the permission to the device.



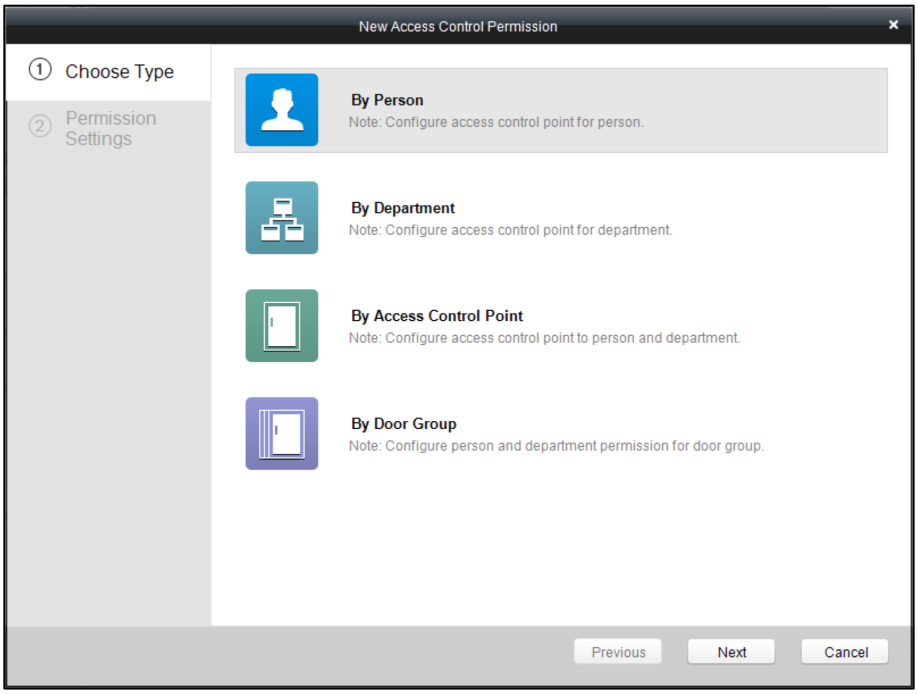
Permission Download P... Downloaded (100%)

Device	Progress	Result	Remark
123	100%	All Succee...	

Offline Permission of Distributed Controller Settings

Steps:

1. Enter the Access Control Permission page.
2. Click Offline Permission of Distributed Controller to enter the Offline Permission of Distributed Controller tab.
3. Click ✚ Add Permi... (Add Permission) on the upper-left side of the page to enter the Add Permission window.



By Person
Note: Configure access control point for person.

By Department
Note: Configure access control point for department.

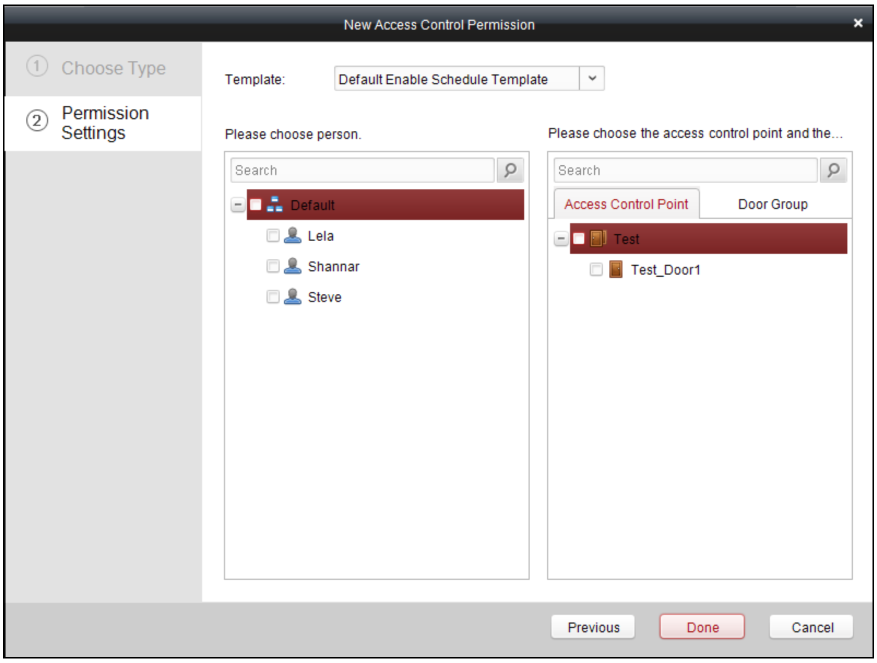
By Access Control Point
Note: Configure access control point to person and department.

By Door Group
Note: Configure person and department permission for door group.

4. Select an adding type in the **Select Type** interface.
   - **By Person:** you can select people from the list to enter/exit the door. The following steps will take By Person as an example.

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

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



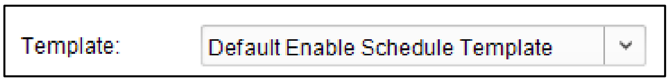
New Access Control Permission

Template: Default Enable Schedule Template

Please choose person.

Please choose the access control point and the...

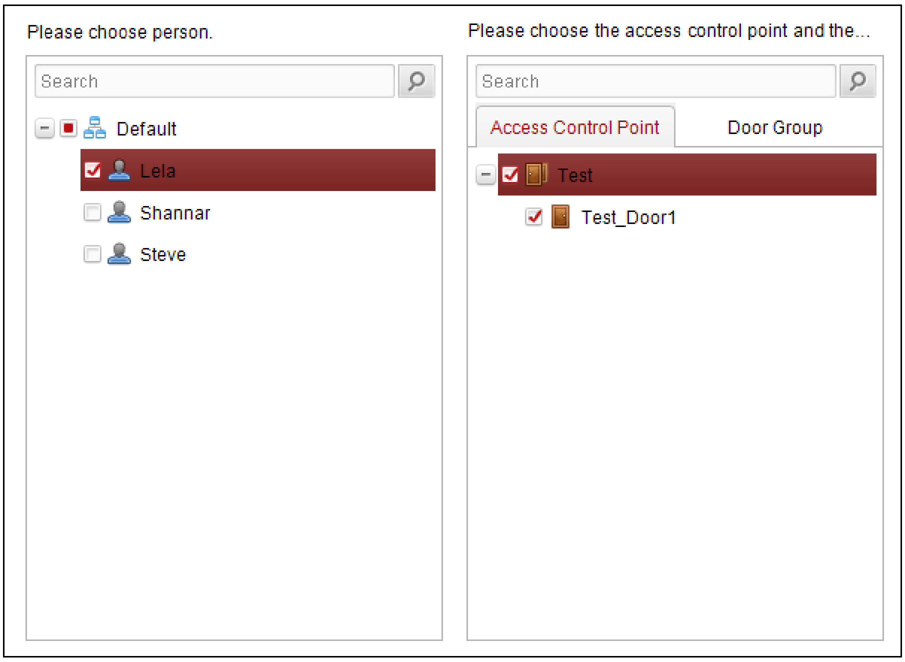
6. Click on the dropdown menu to select a schedule template for the permission.



Template: Default Enable Schedule Template

Note: The schedule template must be configured before any permission settings. Refer to *Section 20.3 Schedule Template* for detailed configuration guide.

7. Select people/ department and corresponding doors/door groups from the appropriate lists.



Please choose person.

Search

- Default
  - ☑ Lela
  - □ Shannar
  - □ Steve

Please choose the access control point and the...

Search

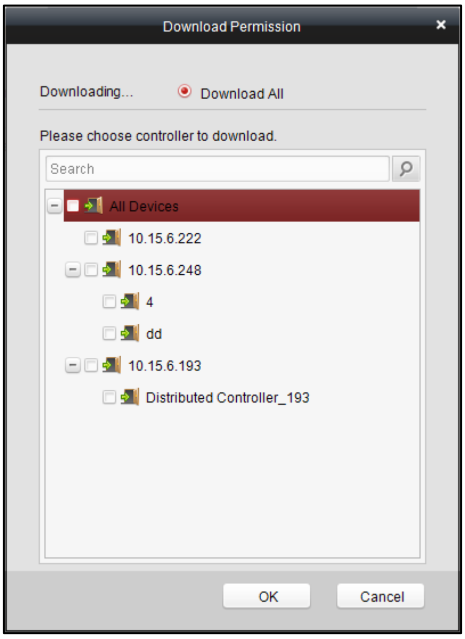
Access Control Point | Door Group

- ☑ Test
  - ☑ Test_Door1

Note: The lower-level of department will also be selected if the highest-level of department is selected.

8. Click the **Done** button to complete the permission adding.

9. Click Start Downloading to enter the **Download Permission** page.



Download Permission

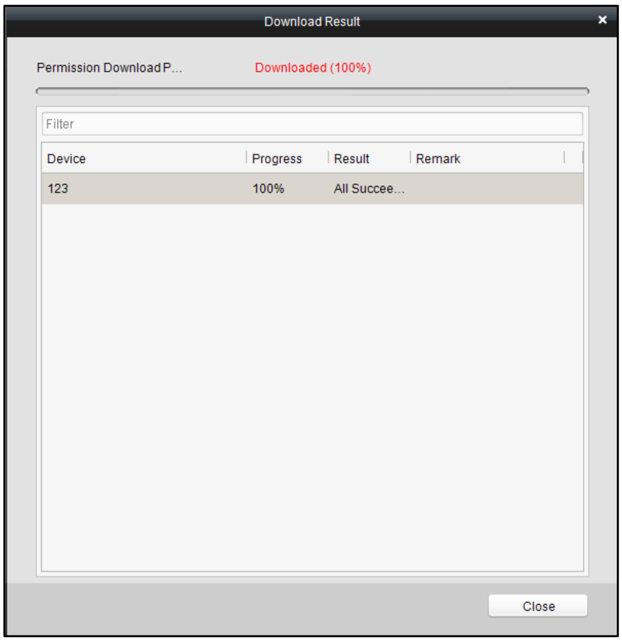
Downloading... ● Download All

Please choose controller to download.

Search

- □ All Devices
  - □ 10.15.6.222
  - □ 10.15.6.248
    - □ 4
    - □ dd
  - □ 10.15.6.193
    - □ Distributed Controller_193

10. Select the distributed controller and click the **OK** button, to enter the download result interface, to download the permission to the device.



Permission Download P... Downloaded (100%)

Filter

Device	Progress	Result	Remark
123	100%	All Succee...	

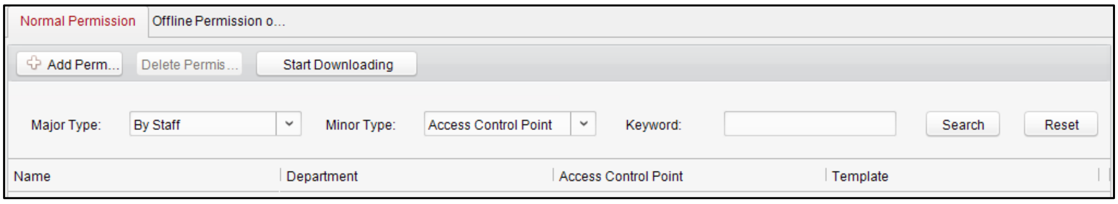
20.6.2 Access Permission Searching

Purpose:

After the permission settings being completed, you can search and view permission assigning condition on the searching interface.

Steps:

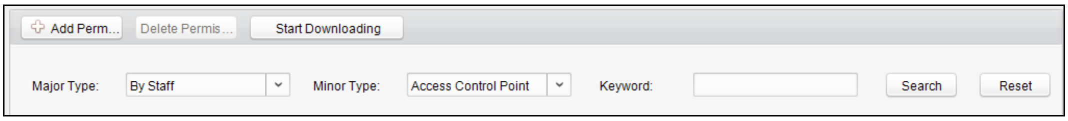
1. In the Access Control Permission page, select the Normal Permission tab or the Offline Permission of Distributed Controller tab.



Major Type: By Staff Minor Type: Access Control Point Keyword:

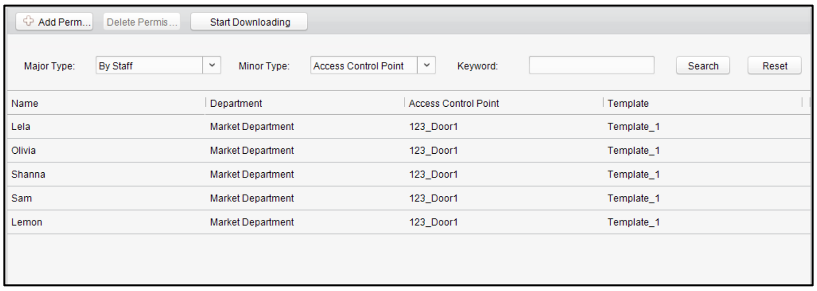
Name	Department	Access Control Point	Template

2. Enter the search criteria (main type/minor type/Keyword).



Major Type: By Staff Minor Type: Access Control Point Keyword:

3. Click **Search** to get the search results.



Major Type: By Staff Minor Type: Access Control Point Keyword:

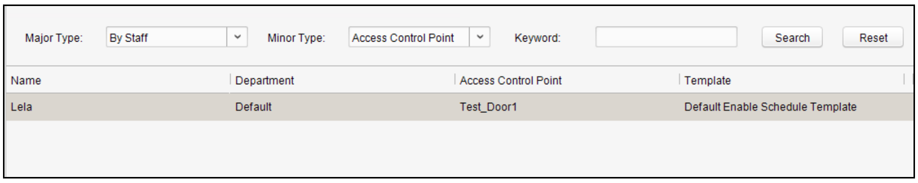
Name	Department	Access Control Point	Template
Lela	Market Department	123_Door1	Template_1
Olivia	Market Department	123_Door1	Template_1
Shanna	Market Department	123_Door1	Template_1
Sam	Market Department	123_Door1	Template_1
Lemon	Market Department	123_Door1	Template_1

Note: You can click **Reset** on the search criteria panel to clear all the displayed search results.

20.6.3 Permission Deleting

Steps:

1. Follow steps 1-3 in the Permission Searching section to search for the permission needs to be deleted.
2. Select the permission from the results list.

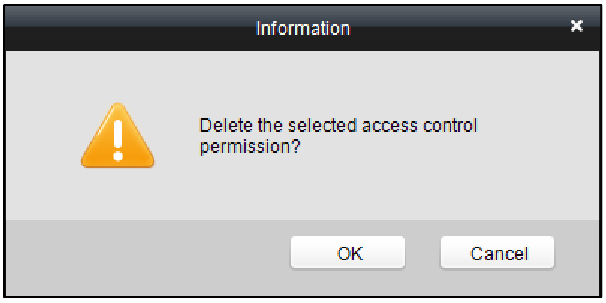


Major Type: By Staff   Minor Type: Access Control Point   Keyword:

Name	Department	Access Control Point	Template
Lela	Default	Test_Door1	Default Enable Schedule Template

Note: you can press the Ctrl or Shift key on the keyboard,

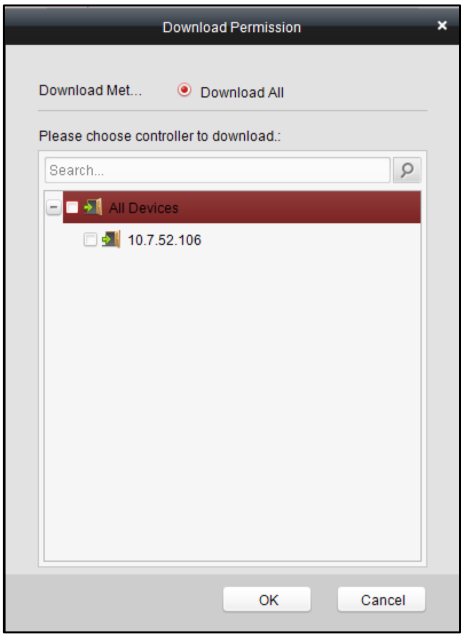
3. Click the **Delete Permission** button to delete the permission.



Information

Delete the selected access control permission?

4. Click Start Downloading to enter the **Download Permission** page.



Download Permission

Download Met... ● Download All

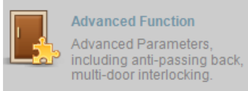
Please choose controller to download.:

5. Select a control point and click the **OK** button to download the deletion operation to the device.

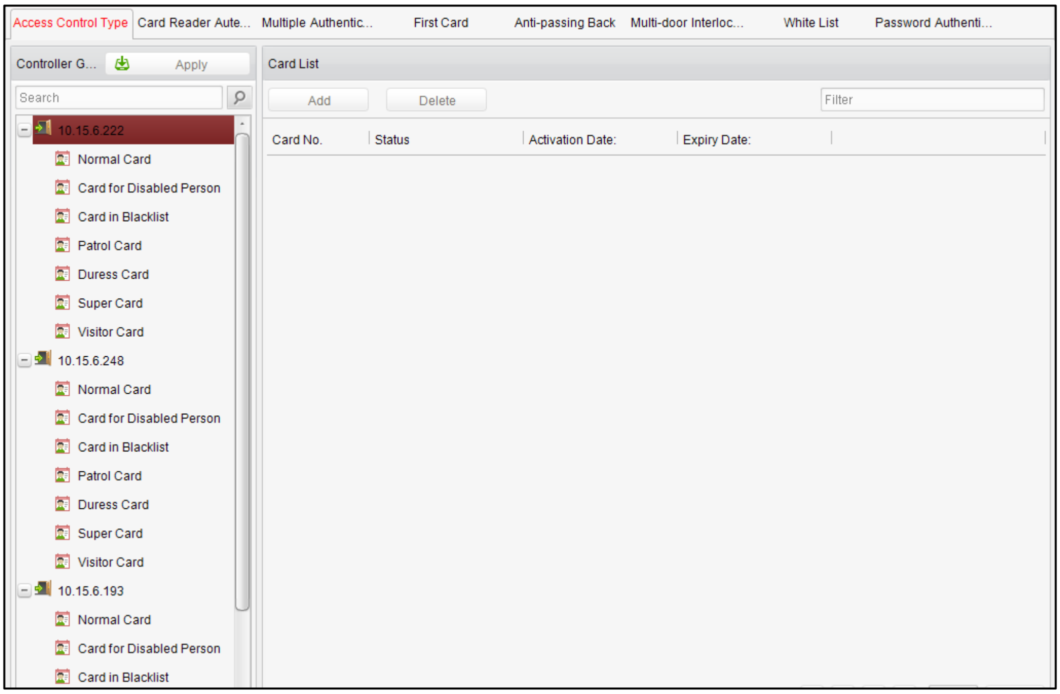
20.7 Advanced Functions

Purpose:

The advanced functions of the access control system can be configured, such as access control type, password authentication and first card.

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

Advanced Function
Advanced Parameters, including anti-passing back, multi-door interlocking.



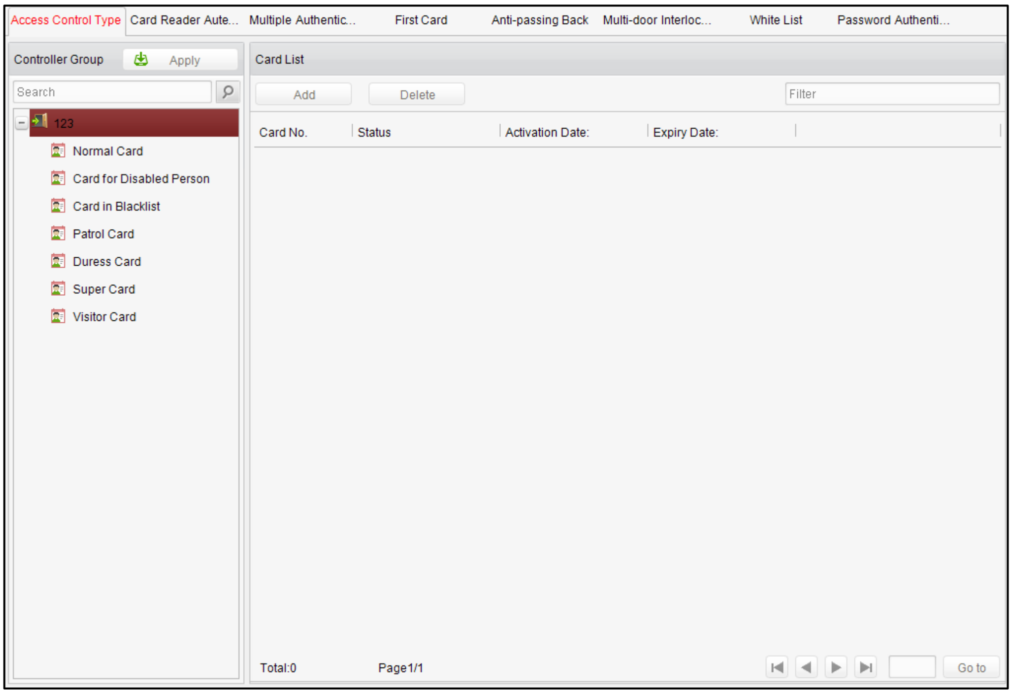
20.7.1 Access Control Type

Purpose:

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

Steps:

1. Click the Access Control Type tab and select a card type.



Normal Card: By default, the card is set as normal card.

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

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

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

Duress Card: The card swiping action will be uploaded.

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. Double click to edit the

2. Click **Add** and select the available card.
3. Click **OK** to confirm assigning the card(s) to the selected card type.
4. Click Apply to take effect of the new settings.

Notes:

- You can click **Delete** to remove the card from the card type and the card can be available for being re-assigned.
- Double click the added card in the card list of Visitor Card to edit the maximum card swipe time.

20.7.2 Card Reader Authentication

Purpose:

You can only open the door by both swiping card and entering the password during the set time periods.

Notes:

- For this authentication mode, the card swiping operation cannot be replaced by entering the card No..

- For password settings, please refer to *Section 21.2.2 Normal Card*.

Steps:

1. Click the Card Reader Authentication tab and select a card reader.
2. Select a card reader authentication type from the dropdown list.

   Fingerprint: The door can open by only inputting the fingerprint.

   Swipe Card: The door can open by only swiping the card.

   Fingerprint/Swipe Card: The door can open by inputting the fingerprint or swiping the card.

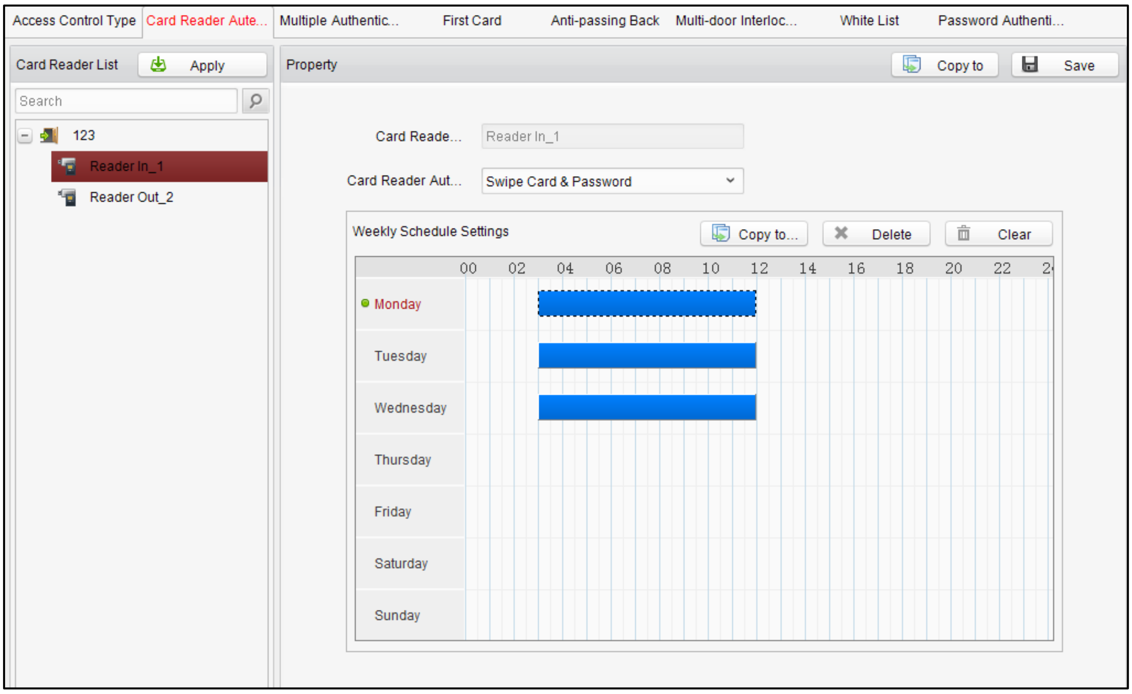
   Swipe Card/Password: The door can open by inputting the password or swiping the card.

   Fingerprint and Password: The door can open by both inputting the password and inputting the fingerprint.

   Swipe Card and Password: The door can open by both inputting the password and swiping the card.

   Fingerprint and Swipe Card: The door can open by both inputting the fingerprint and swiping the card.

   Fingerprint and Swipe Card and Password: The door can open by inputting the fingerprint, inputting the password, and swiping the card.
3. Click and drag your mouse on a day to draw a blue bar on the schedule, which means in that period of time, the password authentication is valid.



Card Reade... Reader In_1

Card Reader Aut... Swipe Card & Password

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

   Or you can select a configured day and click the **Copy to Week** button to copy the same settings to the whole week.

   You can click the **Delete** button to delete the selected time period or click the **Clear** button to delete all the configured time periods.
5. (Optional) Click the **Copy to** button to copy the settings to other card readers.
6. Click the **Save** button to save parameters.
7. Click the Apply button to take effect of the new settings.

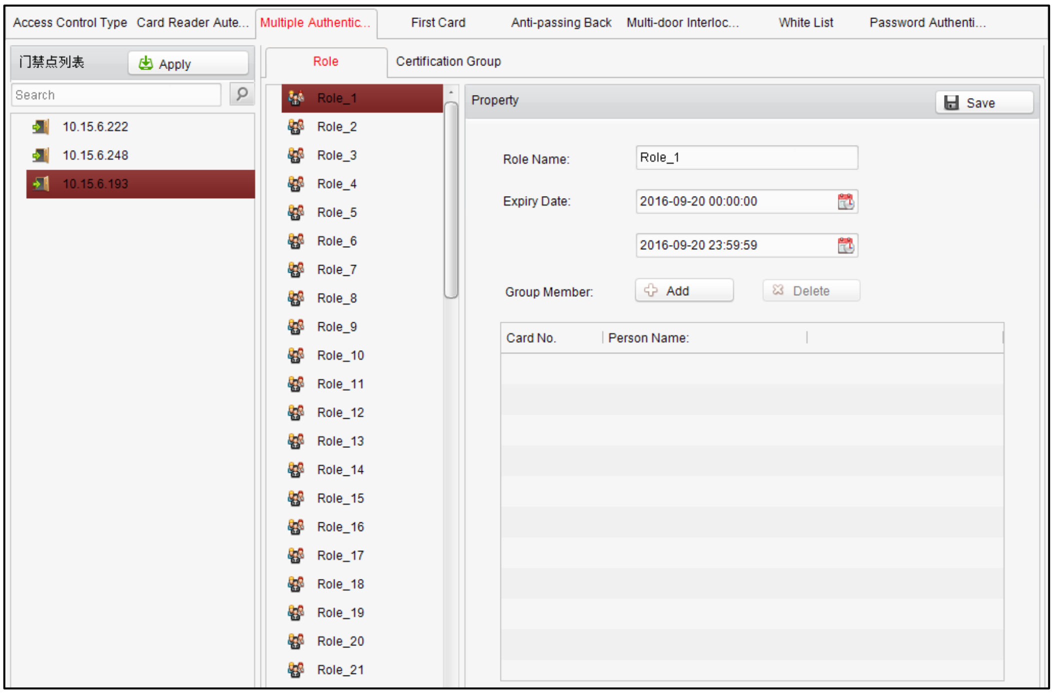
20.7.3 Multiple Authentication

Purpose:

You can manage the cards by group and set the authentication for multiple cards for one access controller.

Steps:

1. Click the Multiple Authentication tab and select a group in the access controller from the list on the left.
2. Click Role to enter the Role tab. Select a role in the role list and edit the role name and the expiry date.
3. Click Add to add the group members.



Access Control Type | Card Reader Aute... | Multiple Authentic... | First Card | Anti-passing Back | Multi-door Interloc... | White List | Password Authenti...

门禁点列表 Apply

Search

10.15.6.222
10.15.6.248
10.15.6.193

Role | Certification Group

Role_1
Role_2
Role_3
Role_4
Role_5
Role_6
Role_7
Role_8
Role_9
Role_10
Role_11
Role_12
Role_13
Role_14
Role_15
Role_16
Role_17
Role_18
Role_19
Role_20
Role_21

Property Save

Role Name: Role_1

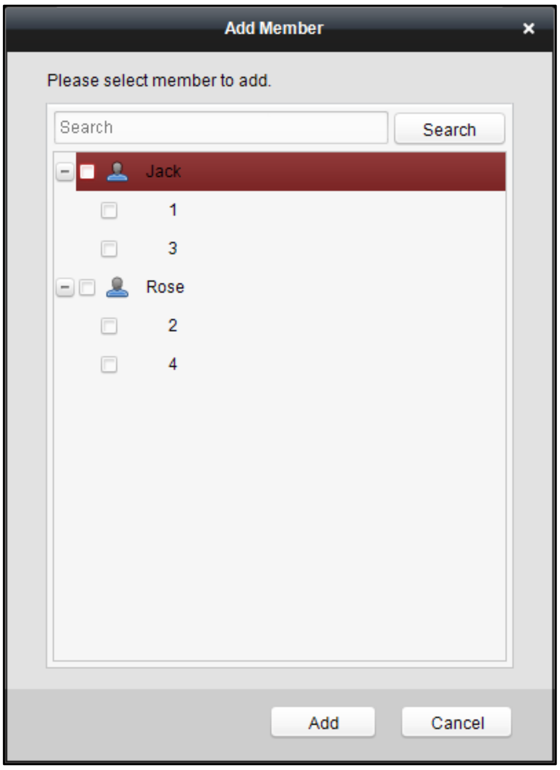
Expiry Date: 2016-09-20 00:00:00

2016-09-20 23:59:59

Group Member: Add Delete

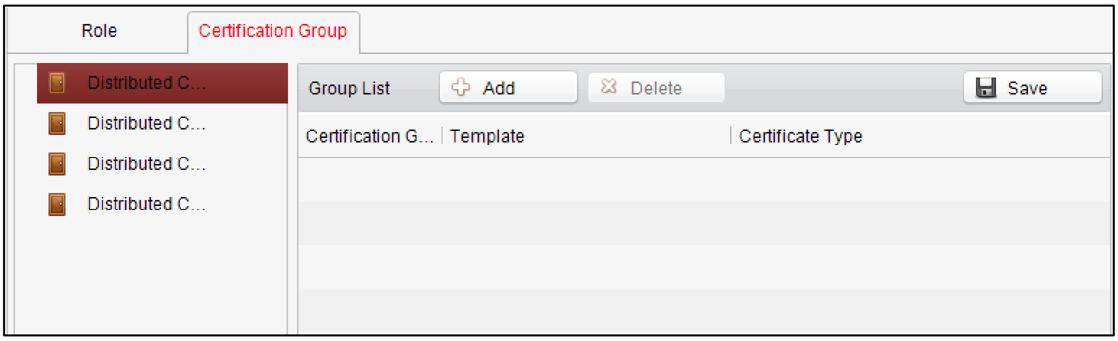
Card No.	Person Name:

4. Check the target card No. and click Add to add the selected member with the corresponding card. The added members will be displayed in the group member list.



Or select the member in the group member list and click Delete to delete the member.

5. Click Save to save the configuration.
6. Click Certification Group to enter the Certification Group tab.
7. Select a distributed access controller and click Add.

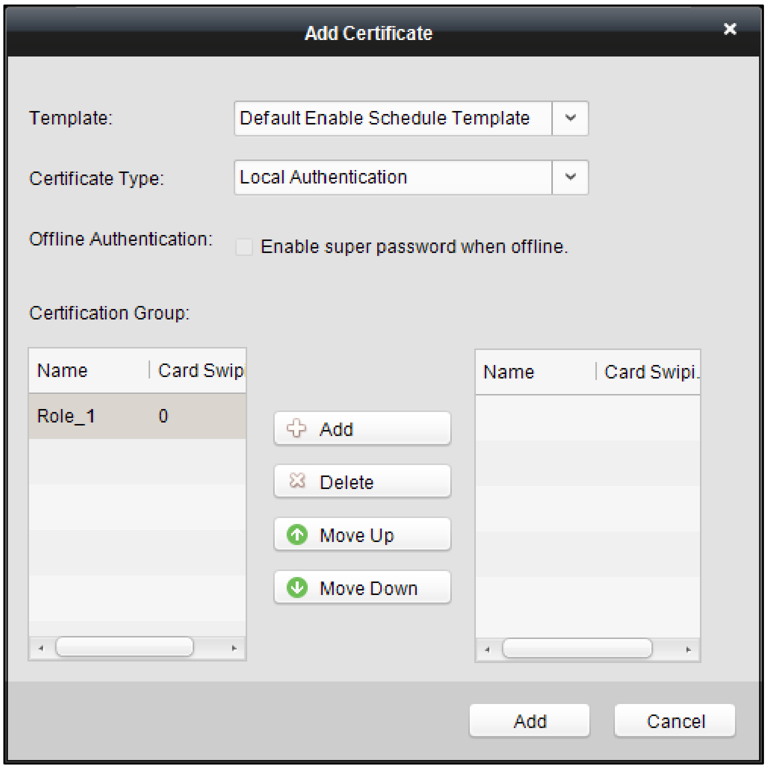


8. Configure the template, the certificate type, the offline authentication and the certification group. And click Add in the middle to add the role from the left list to the right one.

   Note: If the certificate type is Local Authentication, you can add up to 8 certificate groups. If the certificate type is not Local Authentication, you can add up to 7 certificate groups.

   Or select the target role in the right list and click Delete to delete the selected role.

Or select the target role and click Move Up or Move Down to change the role swiping card order.



Add Certificate

Template: Default Enable Schedule Template

Certificate Type: Local Authentication

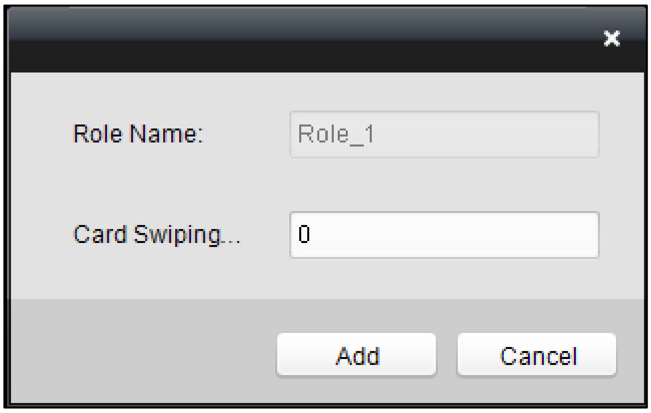
Offline Authentication: □ Enable super password when offline.

Certification Group:

Name	Card Swip
Role_1	0

Name	Card Swipi

9. Double click the Card Swiping Times and edit the card swiping times. Click Add.



Role Name: Role_1

Card Swiping... 0

10. Click Add at the bottom to add the configured the authentication group to the group list. And click Save to save the configuration.

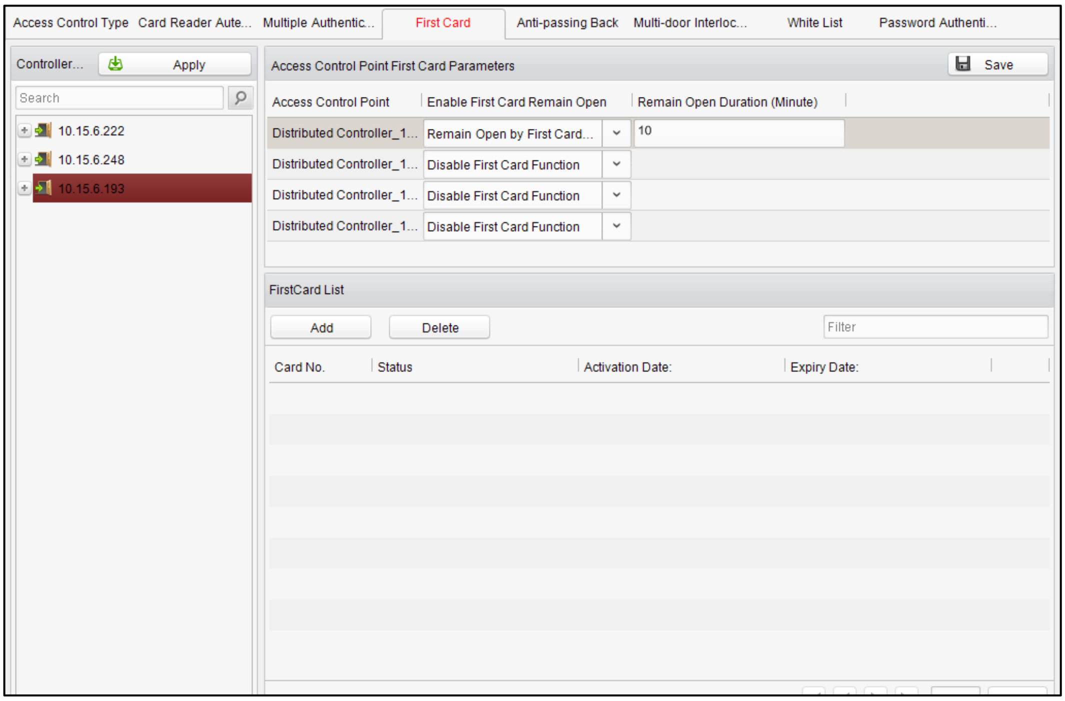
Notes:

- Click Apply on the upper-left to take effect of the new settings.
- The card swiping time should be more then 0.

20.7.4 First Card

Purpose:

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



Access Control Type | Card Reader Aute... | Multiple Authentic... | First Card | Anti-passing Back | Multi-door Interloc... | White List | Password Authenti...

Controller... | Apply

Search

- 10.15.6.222
- 10.15.6.248
- 10.15.6.193

Access Control Point First Card Parameters | Save

Access Control Point	Enable First Card Remain Open	Remain Open Duration (Minute)
Distributed Controller_1...	Remain Open by First Card...	10
Distributed Controller_1...	Disable First Card Function	
Distributed Controller_1...	Disable First Card Function	
Distributed Controller_1...	Disable First Card Function	

FirstCard List

Add | Delete | Filter

Card No.	Status	Activation Date:	Expiry Date:

Steps:

1. Click the First Card tab and select an access control point.
2. Select in **Enable First Card Remain Open**. You are able to select Disable First Card Function, Remain Open by First Card Mode and First Card Authorization Mode.

Remain Open by First Card Mode:	If you select Remain Open by First Card Mode, you should input the time duration for remaining open the door. The door will open for the configured time duration for people accessing the door.
First Card Authorization Mode:	Swipe the authorized first card before other cards swiping. Swipe the first card again to dismiss other cards accessing authorization. After 24:00 every day, you should authorize the first card again.

3. Click Add and select the cards to add as first card for the door and click the **OK** button.
4. Click Save and then click the Apply button to take effect of the new settings.

20.7.5 Anti-Passing Back

Purpose:

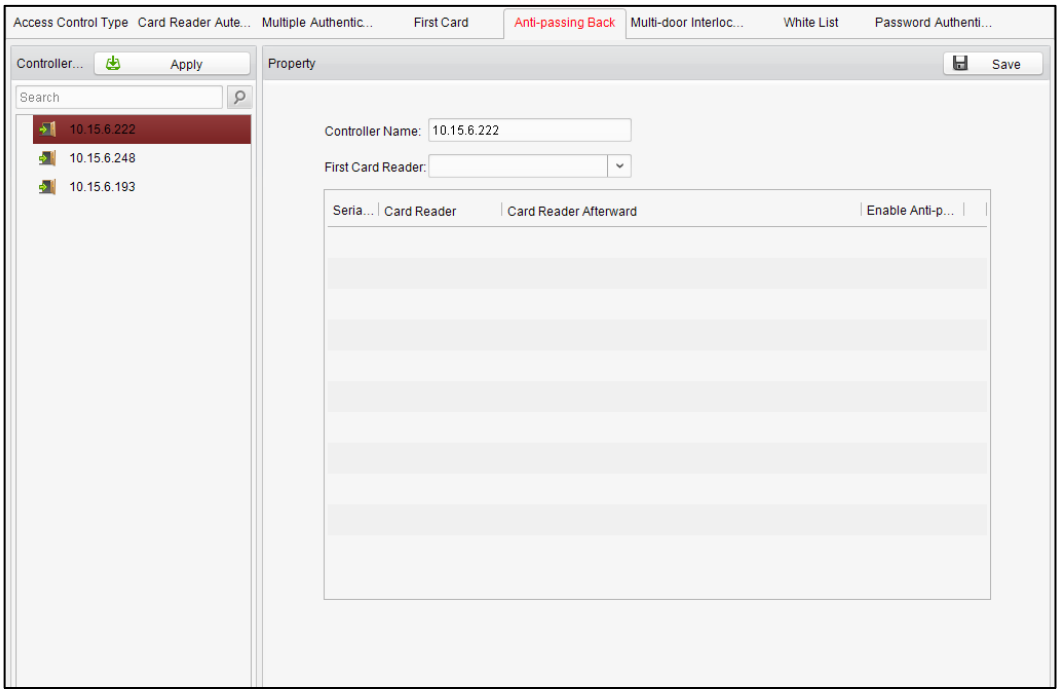
In this mode, you can only pass the access control system according to the specified path.

Note: Either the anti-passing back or multi-door interlocking can be configured for an access controller at the same time.

Setting the Path of Swiping Card (Card Reader Order)

Steps:

1. Click the Anti-passing Back tab and select an access control point.



10.15.6.222
10.15.6.248
10.15.6.193

Controller Name: 10.15.6.222

First Card Reader:

2. You can set the name for the controller and select the card reader as the beginning of the path.
3. 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 system by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.
4. Check the checkbox of **Enable Anti-Passing back**.
5. Click Save and then click the Apply button to take effect of the new settings.

20.7.6 Multi-door Interlocked (Do Not Support)

Purpose:

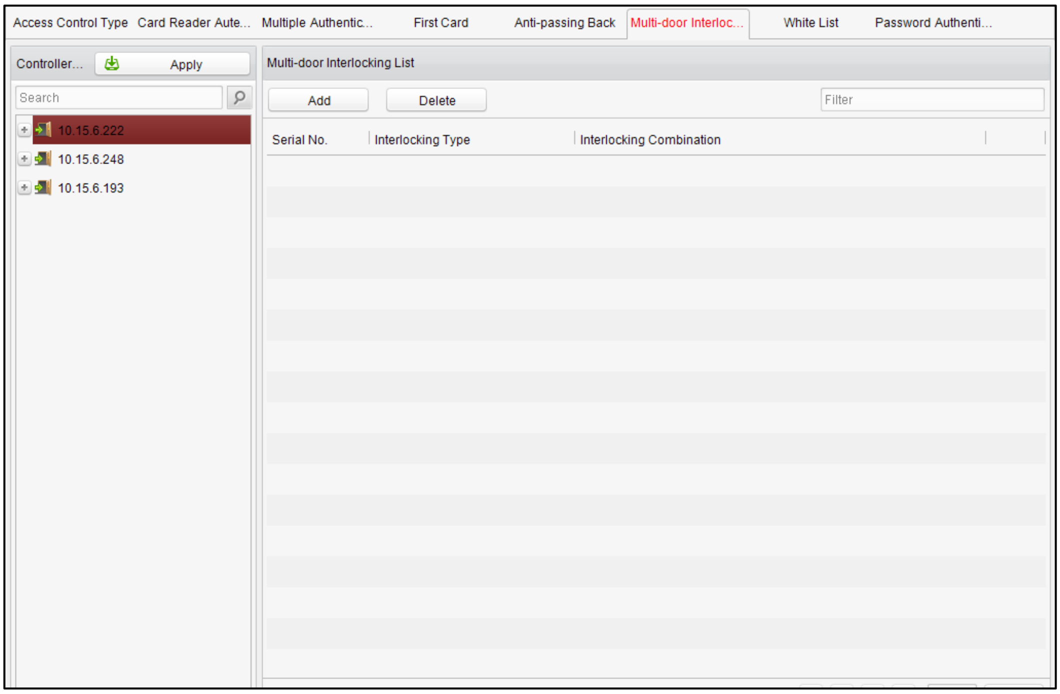
You can set the multi-door interlocking between multiple doors of the same access controller. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Notes:

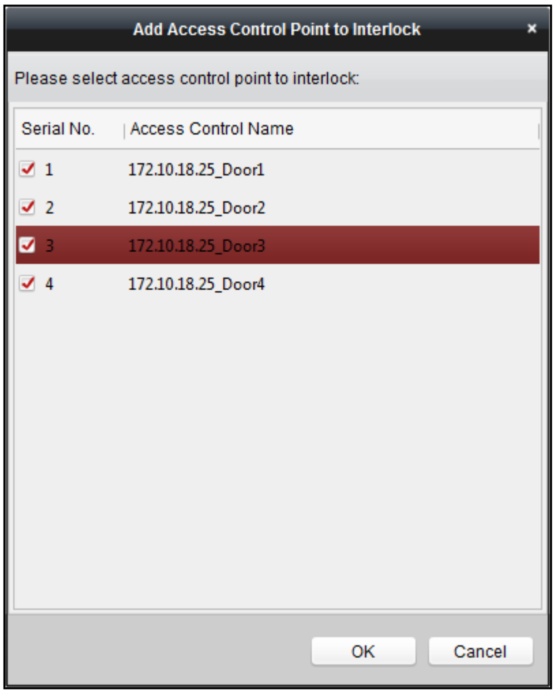
- The Multi-door Interlocking function is only supported by the access controller which has more than one access control points (doors).
- Either the anti-passing back or multi-door interlocking function can be configured for an access controller at the same time.

Steps:

1. Click Multi-door Interlocking tab and select an access controller from the list.



2. Click Add to pop up the Add Access Control Point window.



Please select access control point to interlock:

Serial No.	Access Control Name
☑ 1	172.10.18.25_Door1
☑ 2	172.10.18.25_Door2
☑ 3	172.10.18.25_Door3
☑ 4	172.10.18.25_Door4

3. Select the access control point (door) from the list.

   Note: Up to four doors can be added in one multi-door interlocking combination.

4. Click OK to save the adding.

5. (Optional) After adding the multi-door interlocking combination, you can select it from the list and click Delete to delete the combination.

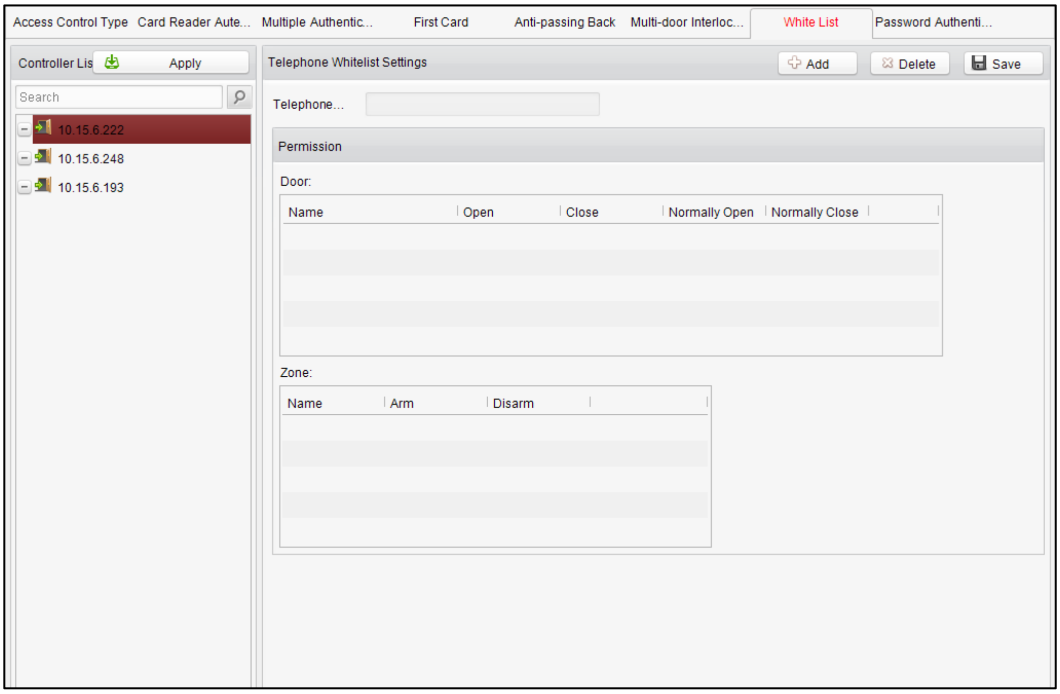
Notes:

- Click Apply button to take effect of the new settings.
- The normal access controller can add up to 4 multi-door interlocks. The device of DS-K2700, DS-K27M01, DS-K27M02 and DS-K27M04 can add up to 8 multi-door interlocks.

20.7.7 White List (Do Not Support)

Steps:

1. Click the White List tab to enter into the white list interface.



2. Select the access control point, and click Add.
3. Input the mobile number.
4. Select the settings of control permission, and set the property as **Allow** to enable this function.
   Door: The mobile can control the door (open, closed, normally open, or normally closed).
   Zone: The mobile can arm and disarm the arming channels.
5. Click Save to save parameters.
6. Click Apply to take effect of the new settings.

Notes:

- The mobile can control the door and the arming region by sending SMS control instructions.
- The SMS control instruction is composed of Command, Operation Range, and Operation Object.
- Each access controller can add up to 8 mobile phone numbers.

Instruction Content	**Digit**	**Description**	**Format**

Command	3	010-Open, 011-Closed, 020-Normally open, 021-Normally Closed, 120-Disarm, 121-Arm	
Operation Range	1	1-all objects with permission, 2-single operation	Command#1#
Operation Object	3	Starts from 1 (corresponding to different doors or arming regions according to commands)	Command#2#Operation Object#

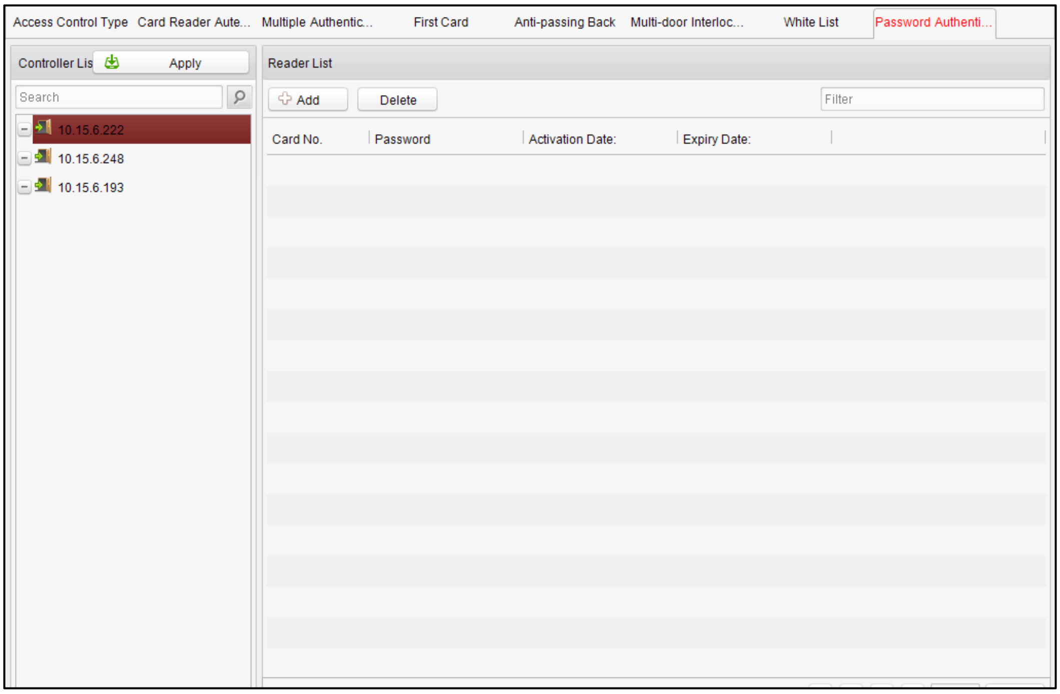
20.7.8 Password Authentication

Purpose:

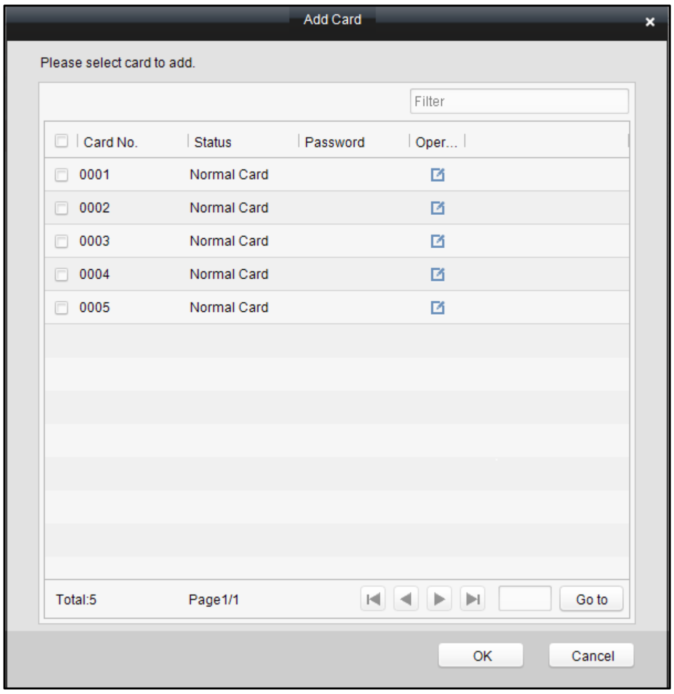
You can open the door by inputting the password only after finishing the operation of password authentication.

Steps:

1. Click **Password Authentication** tab and select a host.



2. Click Add to enter the Add Card window.



Add Card

Please select card to add.

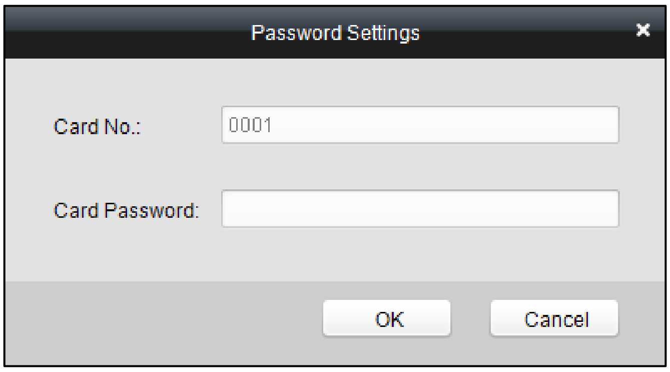
Filter

□ Card No.	Status	Password	Oper...
□ 0001	Normal Card		✎
□ 0002	Normal Card		✎
□ 0003	Normal Card		✎
□ 0004	Normal Card		✎
□ 0005	Normal Card		✎

Total:5 Page1/1 Go to

OK Cancel

3. Check the checkbox of the corresponding card, and click the ✎ button to pop up the password setting dialogue box.



Password Settings

Card No.: 0001

Card Password:

OK Cancel

4. Input the card password.

5. Click OK to finish adding the card.

6. Click Apply to take effect of the new settings.

Notes:

- The card, which has added the password, will be displayed in the card list.
- You can select the card in the card list, and click Delete to delete the password authentication of the selected card.
- The normal access controller supports up to 500 cards to open door via password. The 500 cards' password should not be duplicated.
- The device of DS-K2700 supports up to 1000 card to open door via password.

Chapter 21 Attendance Management (Do Not Support)

Purpose:

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

21.1 Attendance Configuration

Click Attendance Management Configure attendance rule and count attendance analysis result icon on the control panel to enter the Attendance Configuration interface.

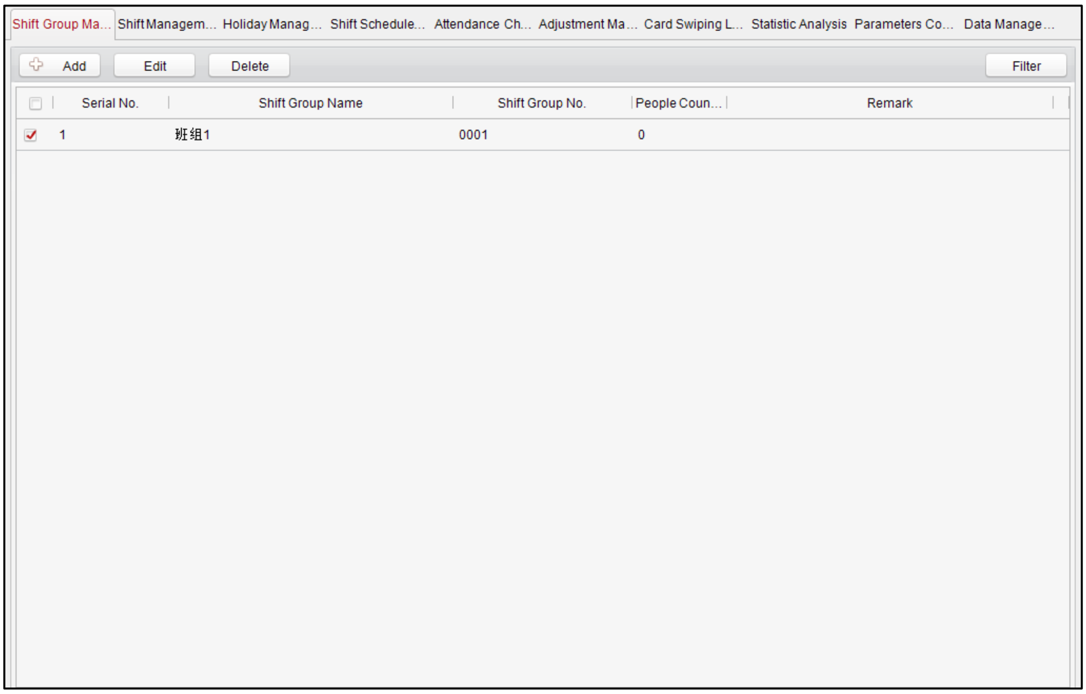
21.1.1 Shift Group Management

Purpose:

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

Steps:

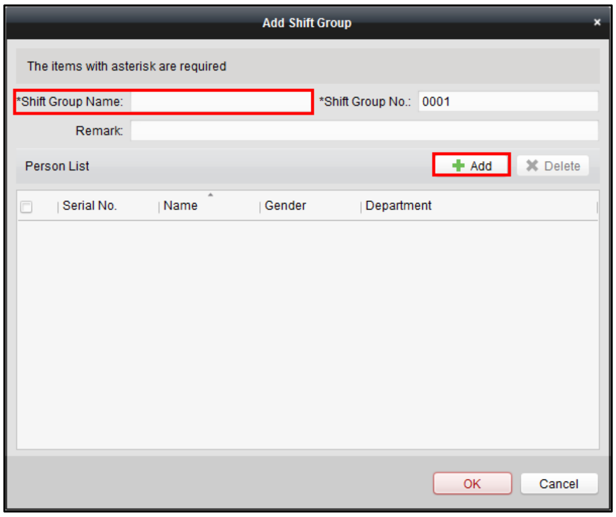
1. Click the Shift Group Management tab to enter the following page.



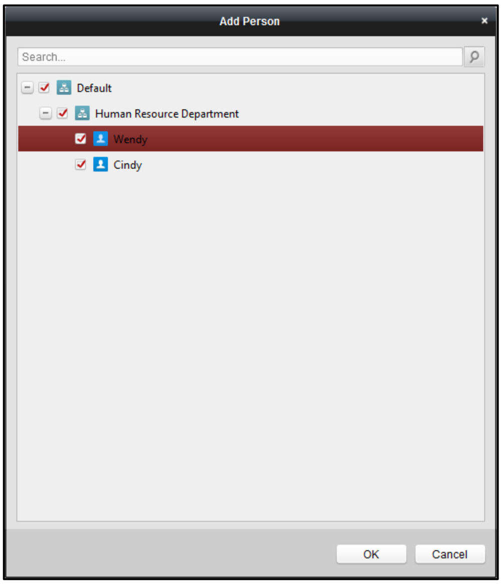
Shift Group Ma... | Shift Managem... | Holiday Manag... | Shift Schedule... | Attendance Ch... | Adjustment Ma... | Card Swiping L... | Statistic Analysis | Parameters Co... | Data Manage...
Add
Edit
Delete
Filter

□	Serial No.	Shift Group Name	Shift Group No.	People Coun...	Remark
☑	1	班组1	0001	0	

2. Click Add to pop up the Shift Group window.



3. Enter the shift group name, and click Add on the person list area to pop up the Add Person window.



4. Check the checkbox to select the person and click **OK** button and return to the shift group settings interface.

   To delete the added person, check the person from the person list, and click Delete.

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

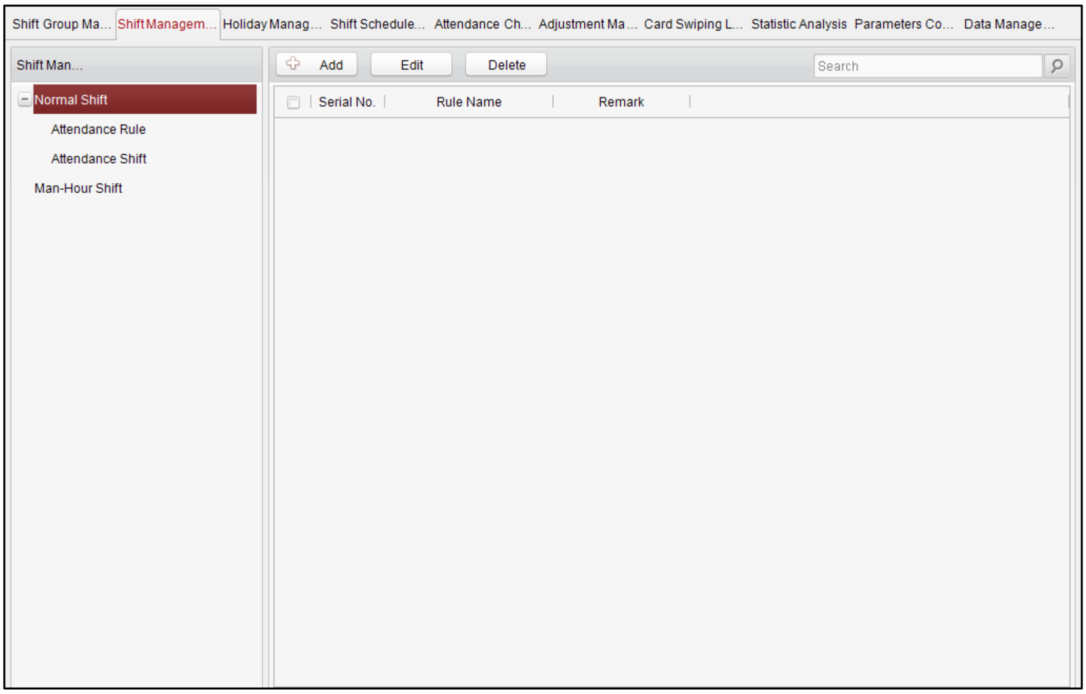
6. You can edit or delete the added shift groups by clicking Edit or Delete.

Notes:

- After deleting the shift group, the shift schedule of the shift group will be deleted as well. For details about shift schedule, refer to *Chapter 22.1.4 Shift Schedule Management.*
- If the person has been added to one shift group, he/she cannot be added to other shift groups.
- No person amount limit when adding the person.

21.1.2 Shift Management

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



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

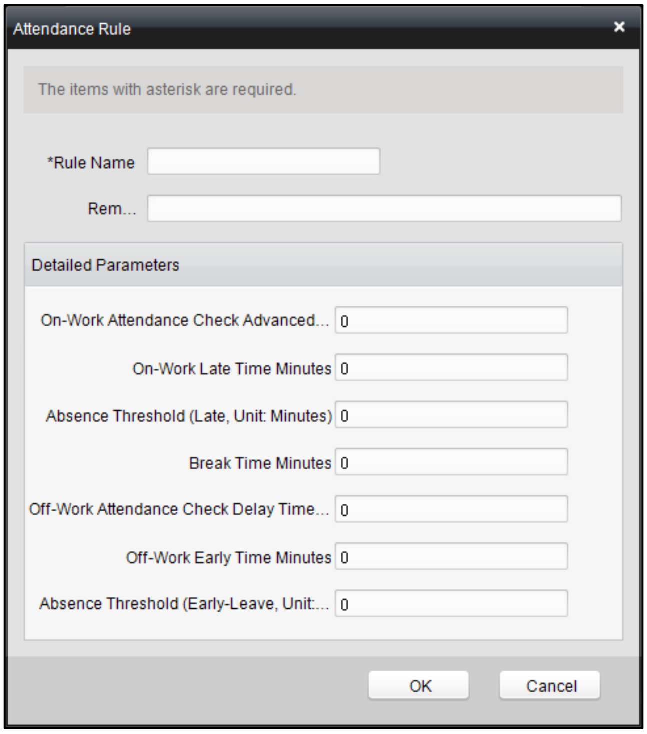
Normal Shift

✧ **Setting Attendance Rule**

Steps:

1. Click **Attendance Rule** to set the rule for the attendance management.

2. Click Add to pop up the Attendance Rule window.



Attendance Rule

The items with asterisk are required.

*Rule Name

Rem...

Detailed Parameters

On-Work Attendance Check Advanced... 0

On-Work Late Time Minutes 0

Absence Threshold (Late, Unit: Minutes) 0

Break Time Minutes 0

Off-Work Attendance Check Delay Time... 0

Off-Work Early Time Minutes 0

Absence Threshold (Early-Leave, Unit:... 0

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

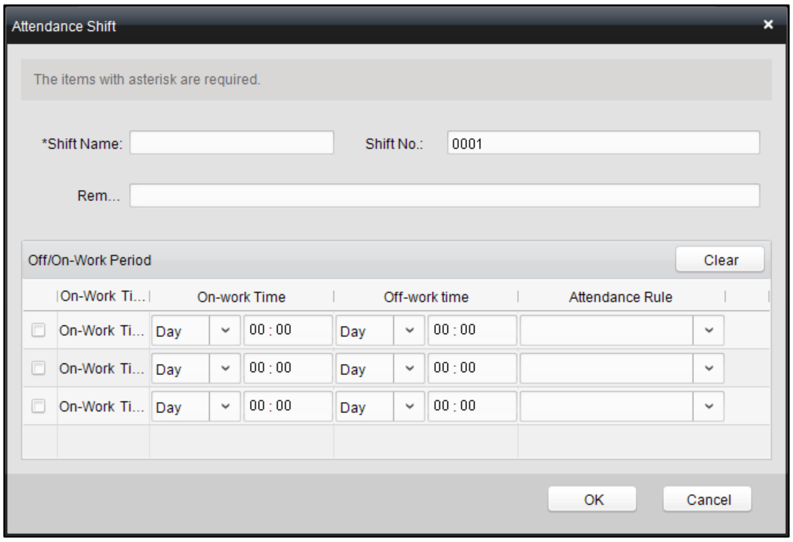
   Notes:

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

✧ **Setting Attendance Shift**

Steps:

1. Click **Attendance Shift** to set the normal attendance shift.
2. Click Add to pop up the attendance shift setting window.



Attendance Shift

The items with asterisk are required.

*Shift Name: Shift No.: 0001

Rem...

Off/On-Work Period | Clear

	On-Work Ti...	On-work Time		Off-work time		Attendance Rule
□	On-Work Ti...	Day	00 : 00	Day	00 : 00	
□	On-Work Ti...	Day	00 : 00	Day	00 : 00	
□	On-Work Ti...	Day	00 : 00	Day	00 : 00	

OK | Cancel

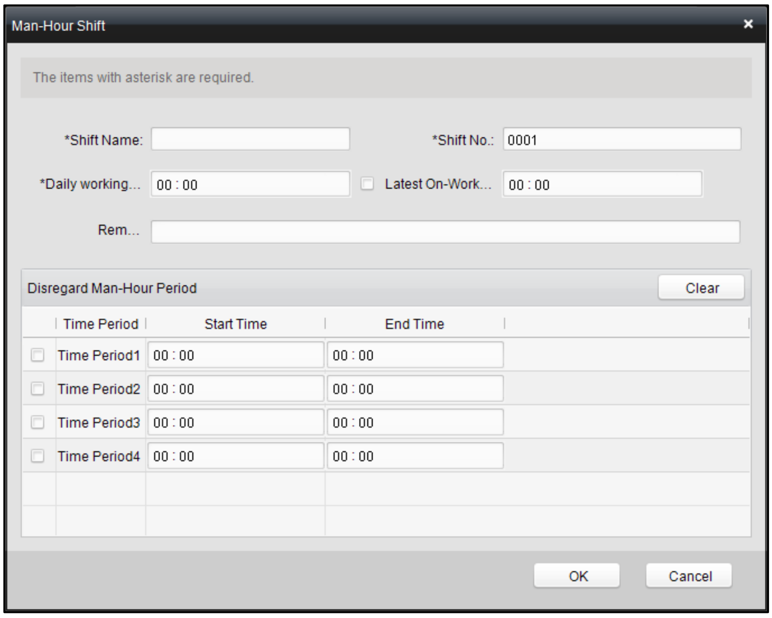
3. Set a shift name.
4. Set on-work duration for the shift, and select the attendance rule from the dropdown list.
5. Click OK to complete the operation.
6. (Optional) You can edit or delete the shift by clicking Edit or Delete.

   Note: After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to *Chapter 22.1.4 Shift Schedule Management.*

Man-Hour Shift

Steps:

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



Man-Hour Shift

The items with asterisk are required.

*Shift Name: *Shift No.: 0001

*Daily working... 00 : 00 □ Latest On-Work... 00 : 00

Rem...

Disregard Man-Hour Period | Clear

	Time Period	Start Time	End Time
□	Time Period1	00 : 00	00 : 00
□	Time Period2	00 : 00	00 : 00
□	Time Period3	00 : 00	00 : 00
□	Time Period4	00 : 00	00 : 00

OK | Cancel

3. Set a shift name, and daily work duration.
4. (Optional) Check the checkbox of latest on-work time, and set the latest on-work time.

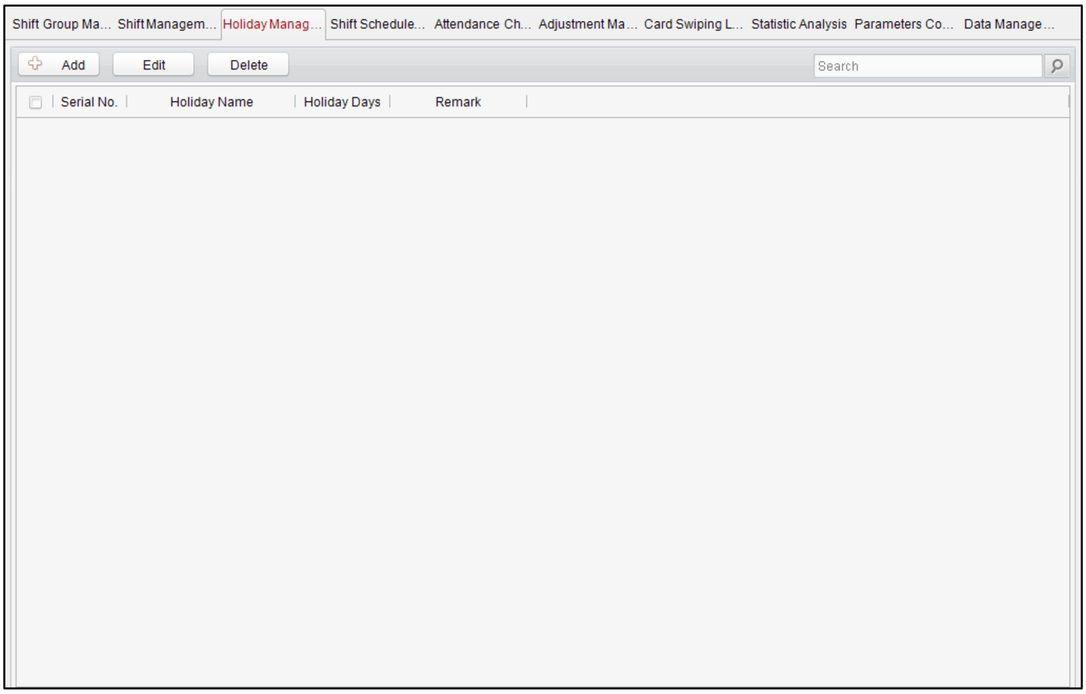
5. (Optional) Set the durations excluded from man-hour duration.
6. Click **OK** button to complete the operation.
7. (Optional) You can edit or delete the shift by clicking Edit or Delete.

   Note: After deleting the shift, its shift schedule will be deleted as well. For details about shift schedule, refer to *Chapter 22.1.4 Shift Schedule Management.*

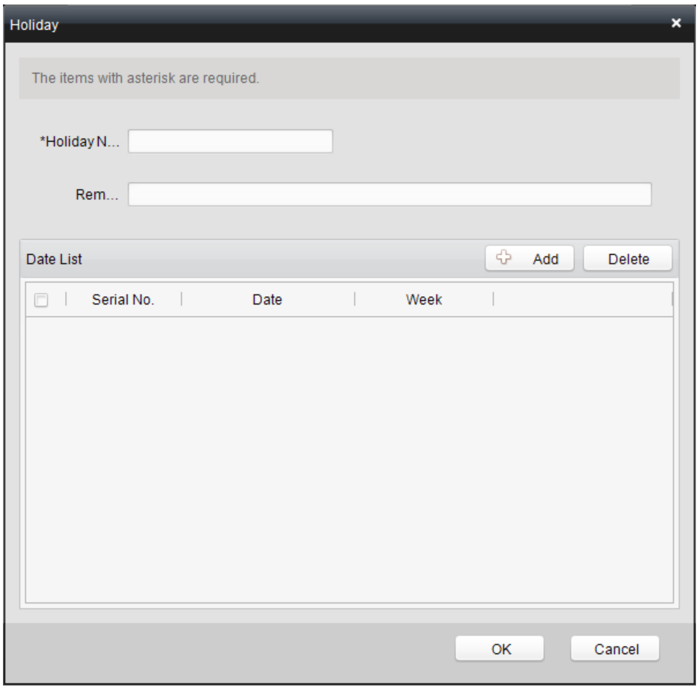
21.1.3 Holiday Management

Steps:

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

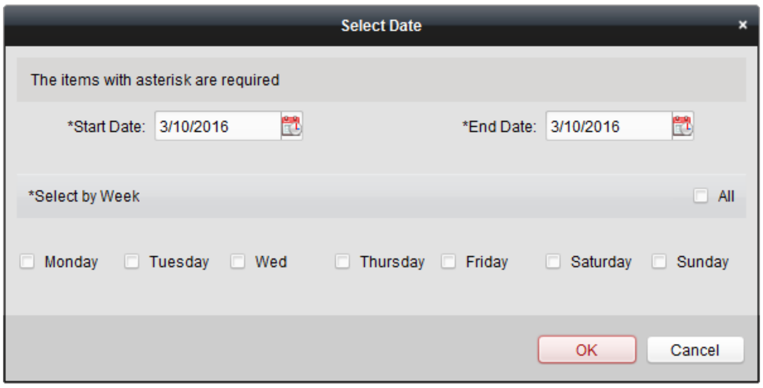


2. Click Add to pop up the Holiday window.



The items with asterisk are required.

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



The items with asterisk are required

*Start Date: 3/10/2016

*End Date: 3/10/2016

□ Monday □ Tuesday □ Wed □ Thursday □ Friday □ Saturday □ Sunday

4. Set the start date and end date, select the date of week, and click OK.

5. Click OK to save the settings.

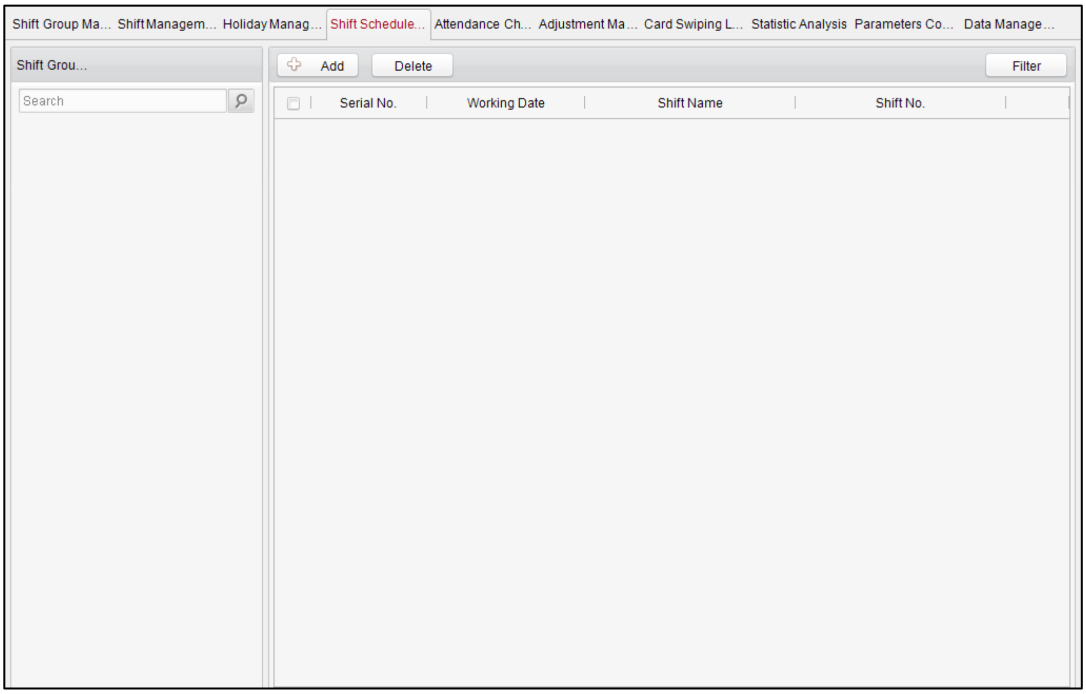
21.1.4 Shift Schedule Management

Purpose:

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

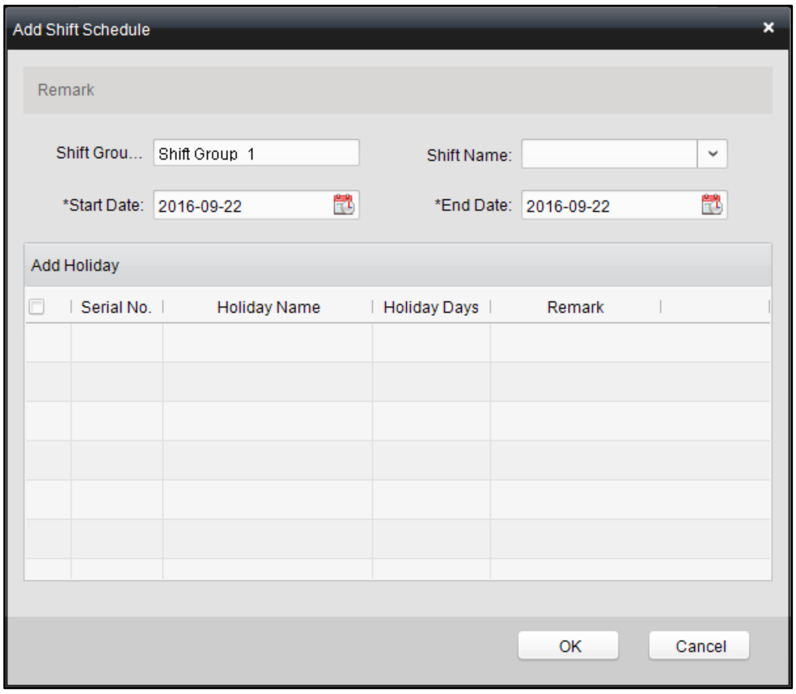
Steps:

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



2. Select the shift group from the list on the left.

3. Click Add to pop up the shift schedule settings window.



Shift Grou...: Shift Group 1

Shift Name:

*Start Date: 2016-09-22

*End Date: 2016-09-22

4. Select the shift name from the drop-down list and set the start data and end data. (Optional) You can check the checkbox of holiday to add the holiday shift.

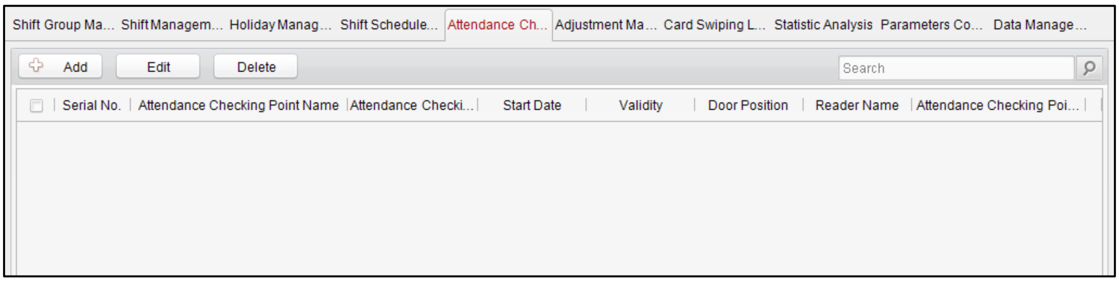
   Click OK to complete the operation.

5. Click OK to save the settings.

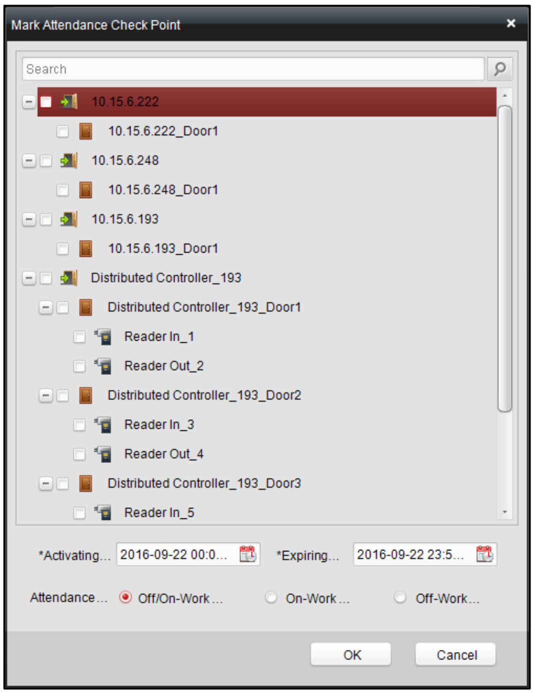
21.1.5 Attendance Check Point Management

Steps:

1. Click the Attendance Check Point Management tab to enter the Attendance Check Point Management interface.



2. Click Add to pop up the Mark Attendance Check Point window.



*Activating... 2016-09-22 00:0... *Expiring... 2016-09-22 23:5...

Attendance... ● Off/On-Work... ○ On-Work... ○ Off-Work...

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

Click OK to save the adding.

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

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

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

Click OK to complete the operation.

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

21.1.6 Adjustment Management

Click the Adjustment Management tab to enter the adjustment management interface.
In this module, **Reason Management** and **List Management** can be realized.

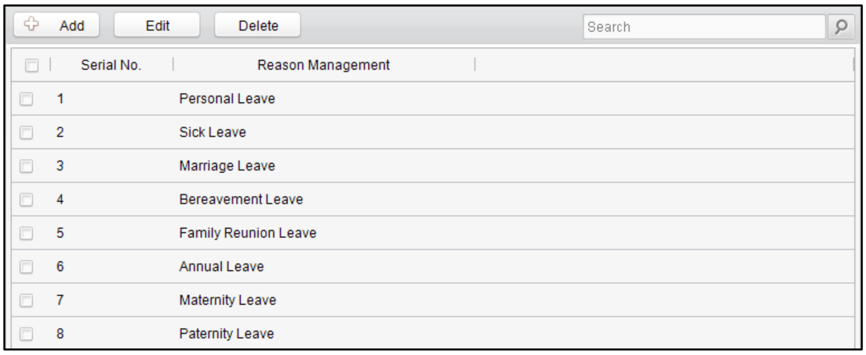
Reason Management

✧ **Leave**

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

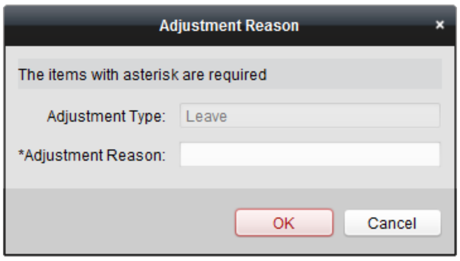
Steps:

1. Click **Leave** to enter the leave interface.



□	Serial No.	Reason Management
□	1	Personal Leave
□	2	Sick Leave
□	3	Marriage Leave
□	4	Bereavement Leave
□	5	Family Reunion Leave
□	6	Annual Leave
□	7	Maternity Leave
□	8	Paternity Leave

2. Click Add to pop up the Adjustment Reason adding dialog box.



The items with asterisk are required

Adjustment Type: Leave

*Adjustment Reason:

3. Enter the adjustment reason, and click OK to save the adding.

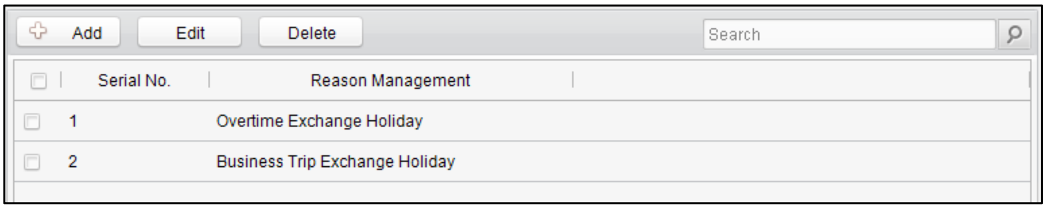
Notes:

- The default adjustment reasons include leave for personal affairs, sick leave, marriage leave, funeral leave, home leave, annual leave, maternity leave, and paternity leave.
- You can check the checkbox of a reason and click Edit to edit the reason, and click Delete to delete the reason.

✧ **Leave in Lieu**

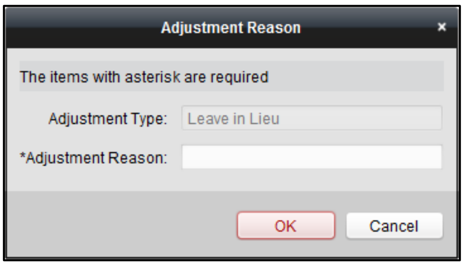
Steps:

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



□	Serial No.	Reason Management
□	1	Overtime Exchange Holiday
□	2	Business Trip Exchange Holiday

2. Click Add to pop up the Adjustment Reason adding dialog box.



The items with asterisk are required

Adjustment Type: Leave in Lieu

*Adjustment Reason:

3. Enter the adjustment reason, and click OK.

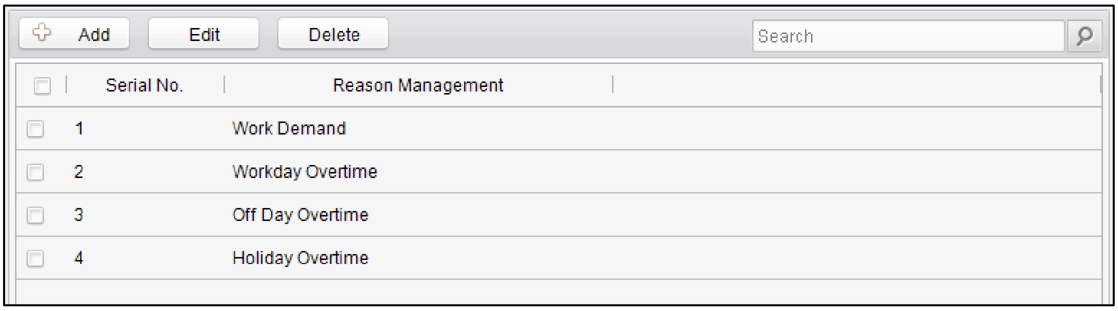
Notes:

- The default adjustment reasons for leave in lieu include overtime, and business trip.
- You can check the checkbox of a reason and click Edit to edit the reason, and click Delete to delete the reason.

✧ **Overtime**

Steps:

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



□	Serial No.	Reason Management
□	1	Work Demand
□	2	Workday Overtime
□	3	Off Day Overtime
□	4	Holiday Overtime

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

3. Enter the adjustment reason, and click OK.

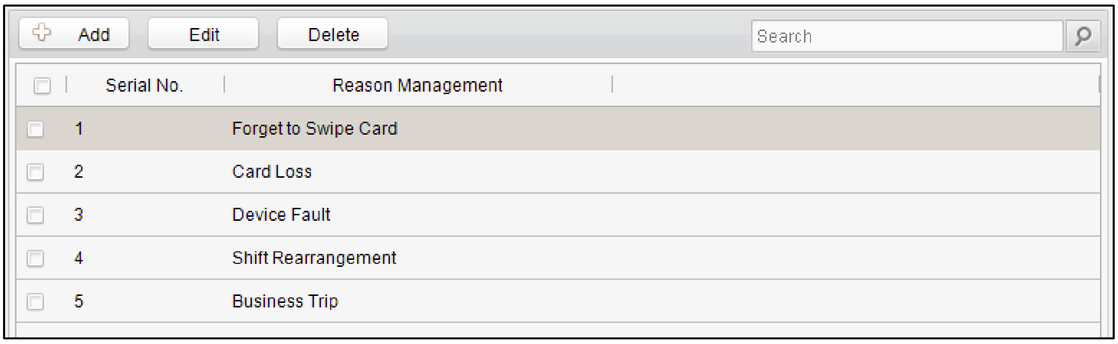
Notes:

- The default adjustment reasons for overtime include work requirement, working day overtime, rest day overtime, and holiday overtime.
- You can check the checkbox of a reason and click Edit to edit the reason, and click Delete to delete the reason.

✧ Replace Card

Steps:

1. Click **Replace Card** to enter the following interface.



□	Serial No.	Reason Management
□	1	Forget to Swipe Card
□	2	Card Loss
□	3	Device Fault
□	4	Shift Rearrangement
□	5	Business Trip

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

3. Enter the adjustment reason, and click OK.

Notes:

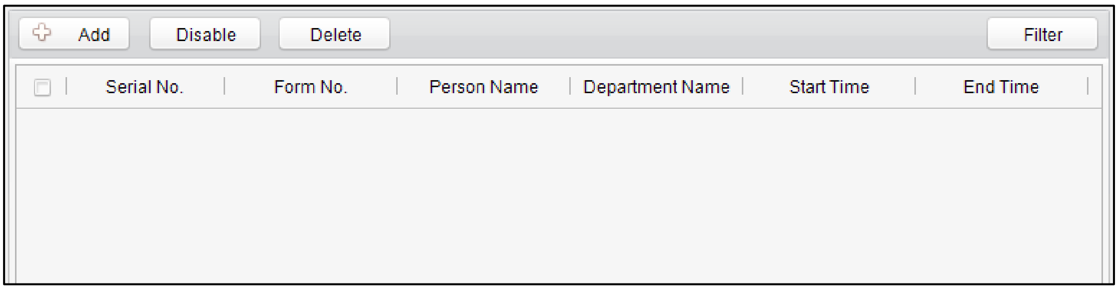
- The default adjustment reasons for card replacing include forget to swipe card, attendance card lost, device fault, shift adjustment, and business trip.
- You can check the checkbox of a reason and click Edit to edit the reason, and click Delete to delete the reason.

List Management

✧ Enabled List

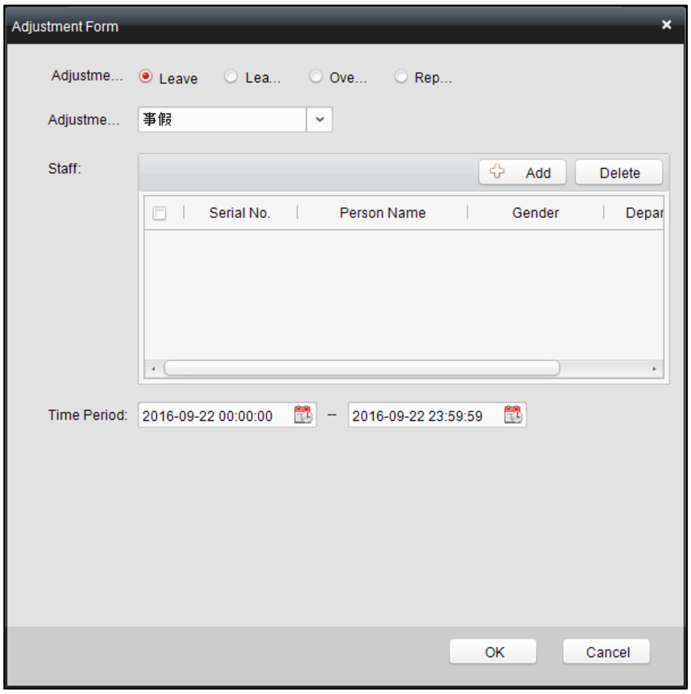
Steps:

1. Click **Enabled** to enter the enabled list interface.



□	Serial No.	Form No.	Person Name	Department Name	Start Time	End Time

2. Click Add to add an attendance management form.



Adjustment Form

Adjustme... ● Leave ○ Lea... ○ Ove... ○ Rep...

Adjustme... 事假

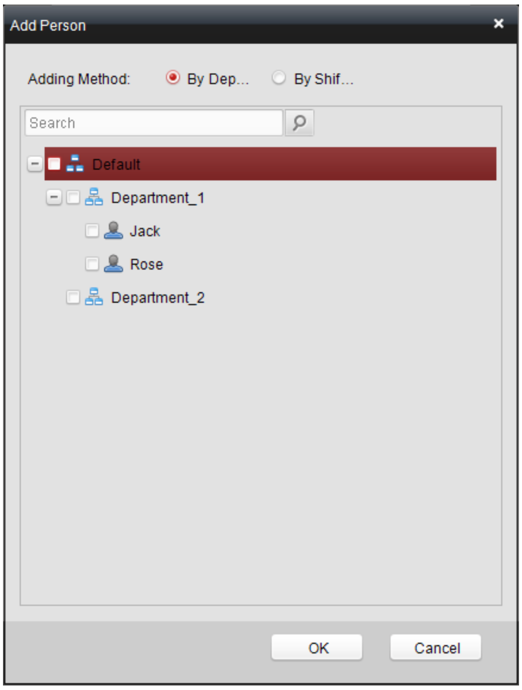
Time Period: 2016-09-22 00:00:00 -- 2016-09-22 23:59:59

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

Leave, Leave in Lieu, and Overtime

1) Select the adjustment reason from the drop-down list.

2) Click Add to pop up the Add Person window.



Add Person

Adding Method: ● By Dep... ○ By Shif...

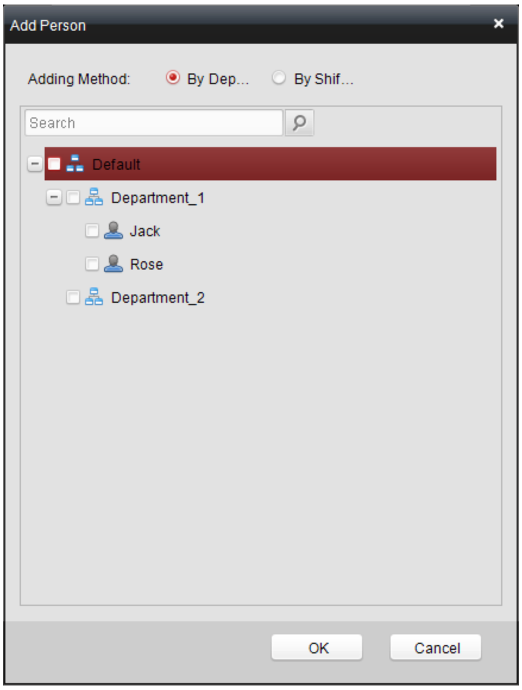
3) Select the adding type as by department or by shift group. Select the person and click OK.

4) Set the time duration.

Replace Card

1) Select the adjustment reason from the drop-down list.

2) Click Add to pop up the Add Person window.



3) Select the adding type as by department or by shift group. Select the person and click OK.

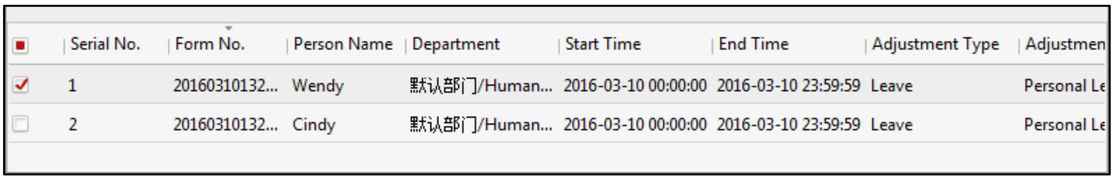
4) Set the date, attendance shift type, and card replacing time.

4. Click OK to complete the operation.

✧ **Disabled List**

Steps:

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

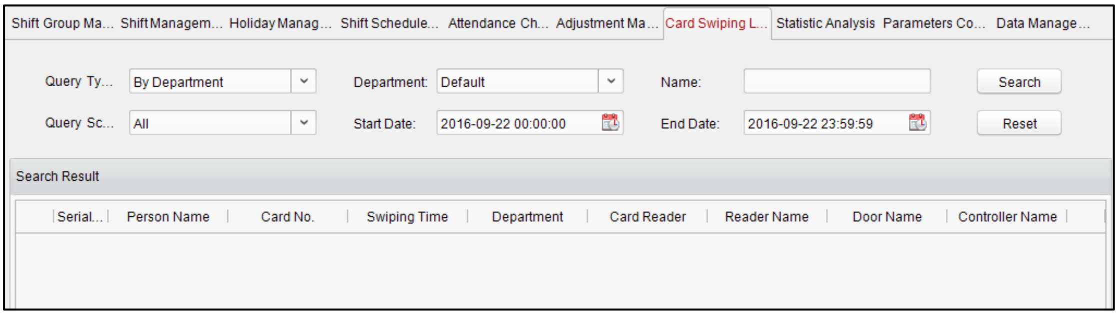


■	Serial No.	Form No.	Person Name	Department	Start Time	End Time	Adjustment Type	Adjustmen
☑	1	20160310132...	Wendy	默认部门/Human...	2016-03-10 00:00:00	2016-03-10 23:59:59	Leave	Personal Le
□	2	20160310132...	Cindy	默认部门/Human...	2016-03-10 00:00:00	2016-03-10 23:59:59	Leave	Personal Le

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

21.1.7 Card Swiping Log Query

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


Shift Group Ma... ShiftManagem... Holiday Manag... Shift Schedule... Attendance Ch... Adjustment Ma... Card Swiping L... Statistic Analysis Parameters Co... Data Manage...
Search
Reset
Search Result

Query Ty...: By Department
Department: Default
Name:
Query Sc...: All
Start Date: 2016-09-22 00:00:00
End Date: 2016-09-22 23:59:59

Serial...	Person Name	Card No.	Swiping Time	Department	Card Reader	Reader Name	Door Name	Controller Name

You can search the card swiping log by two query types: **By Shift Group**, and **By Department**.

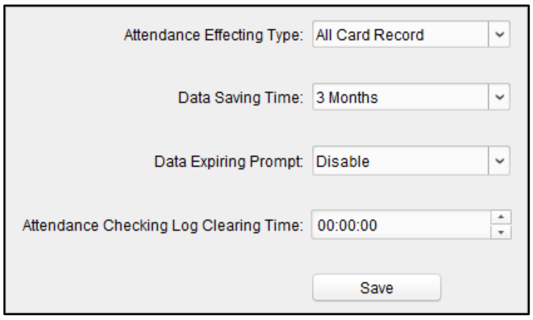
Input other search conditions and click Search to start query the card swiping log.

Or click Reset to reset the search conditions.

21.1.8 Parameters Configuration

Steps:

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



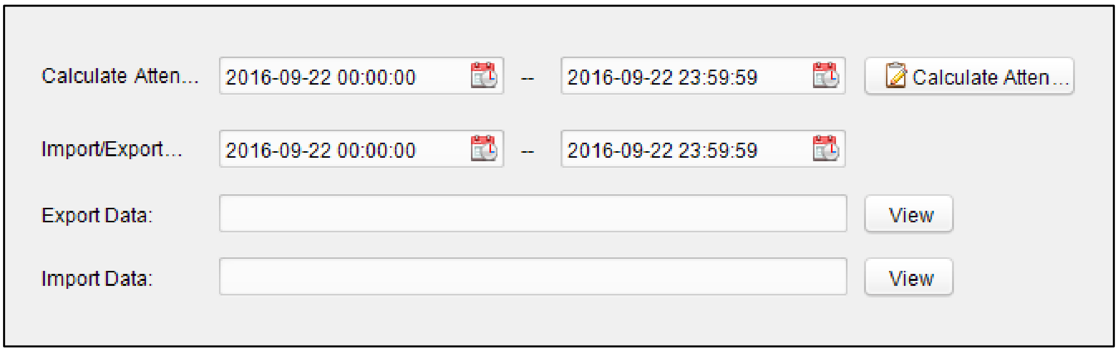
Attendance Effecting Type: All Card Record
Data Saving Time: 3 Months
Data Expiring Prompt: Disable
Attendance Checking Log Clearing Time: 00:00:00

2. Select the attendance effecting type, data saving time, data expiring prompt.
3. Set the attendance checking log clearing time.
4. Click Save to save the parameters.

21.1.9 Data Management

Steps:

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



Calculate Atten... 2016-09-22 00:00:00 -- 2016-09-22 23:59:59 Calculate Atten...

Import/Export... 2016-09-22 00:00:00 -- 2016-09-22 23:59:59

Export Data: View

Import Data: View

2. Select the date and time period for calculation and click Calculate Atten... (Calculate Attendance Data) to start calculating the attendance data.
3. After calculation, you can also export and import the attendance data.

21.2 Attendance Statistic

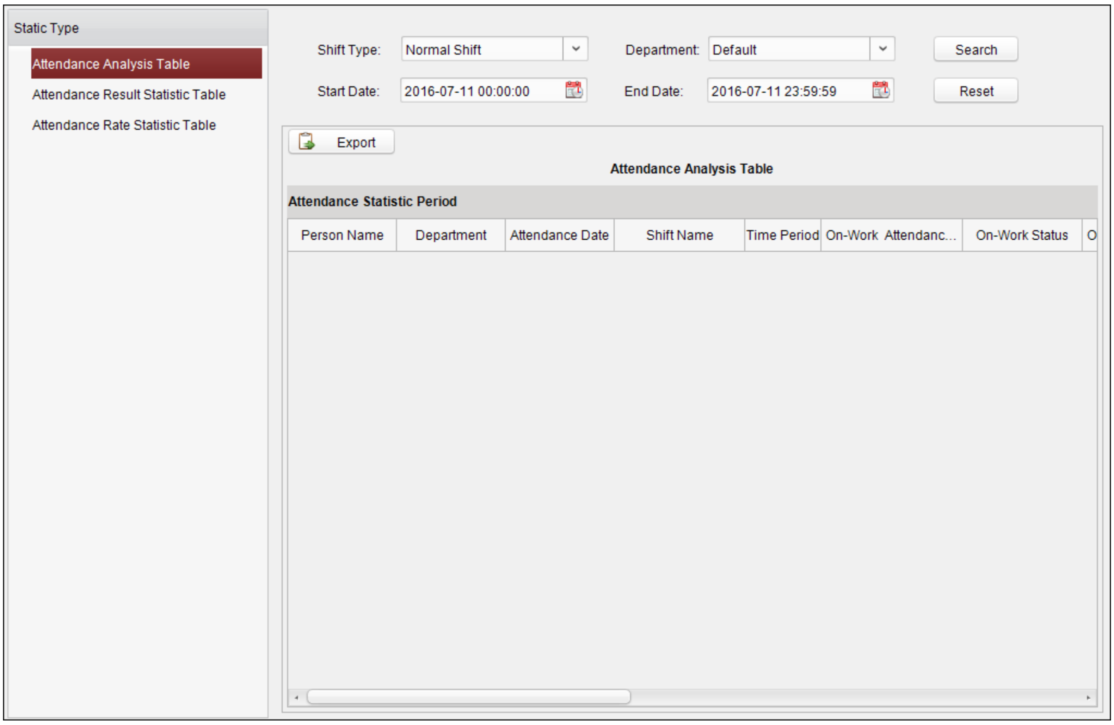
Click the Attendance Statistics tab to enter the Attendance Statistics interface.

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

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

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

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



Static Type
- Attendance Analysis Table
- Attendance Result Statistic Table
- Attendance Rate Statistic Table

Shift Type: Normal Shift

Department: Default

Start Date: 2016-07-11 00:00:00

End Date: 2016-07-11 23:59:59

Attendance Analysis Table

Attendance Statistic Period

Person Name	Department	Attendance Date	Shift Name	Time Period	On-Work Attendanc...	On-Work Status	O

Chapter 22 Checking Status and Event

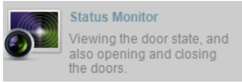
Purpose:

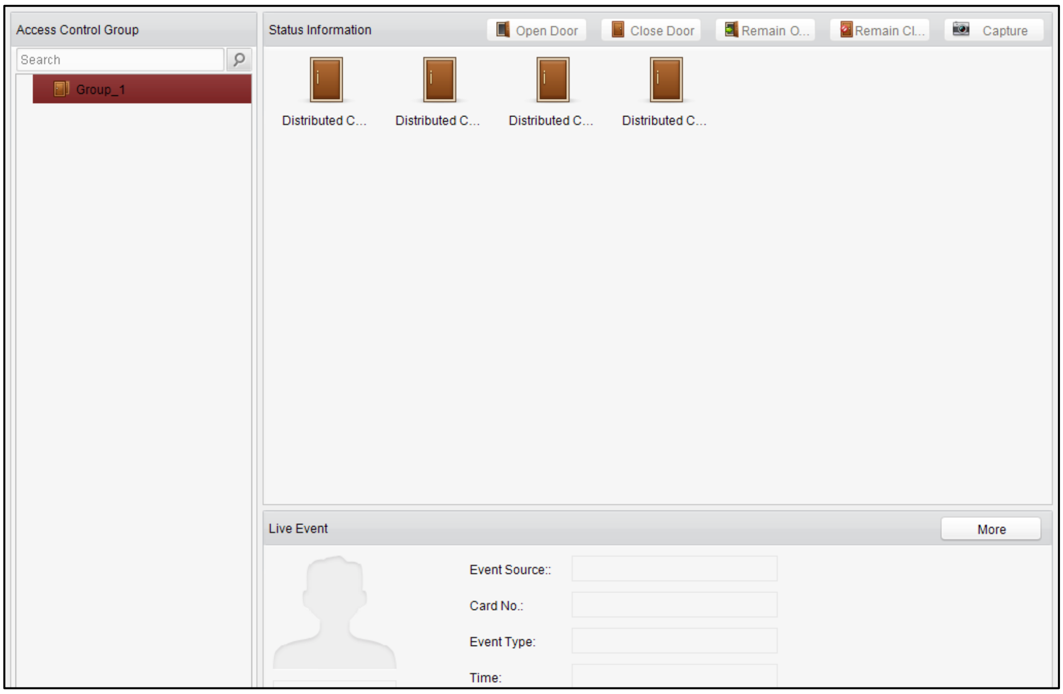
In this section, you are able to anti-control the status of the door and to check the event report of the control point.

22.1 Status Monitor

Purpose:

You can anti-control the door status and check the real-time access event information for the control point.

Click the 
Status Monitor
Viewing the door state, and also opening and closing the doors.
icon on the control panel to enter the interface.



Note: The door status will be displayed according to the door magnetic or the lock.

22.1.1 Access Anti-control

Door Anti-control

Purpose:

You can control the status for a single control point (a door) in this section.

Steps:

1. Enter the status monitor page.

2. Click on the icon on the **Status Information** panel to select a door.
3. Click on the button listed on the upper-left side of the **Status Information** panel to select a door status for the door.

   Open Door : Click the button to open the door once.

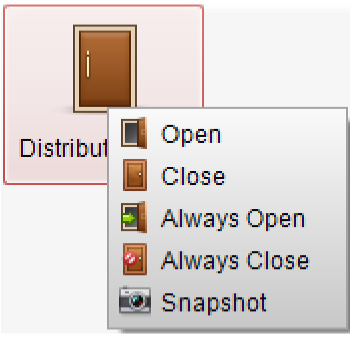
   Close Door : Click the button to close the door once.

   Remain O... : (Remain Open) Click the button to keep the door open.

   Remain Cl... : (Remain Closed) Click the button to keep the door closed.

   Capture **:** Click on the button to capture the picture.

4. You can also right click the icon and to select a status for the door.



Notes:

- If the status is selected as **Remain Open/Remain Closed**, the door will keep open/ closed until a new anti-control command being made.
- The function of picture capturing cannot be realized until the storage server is installed.

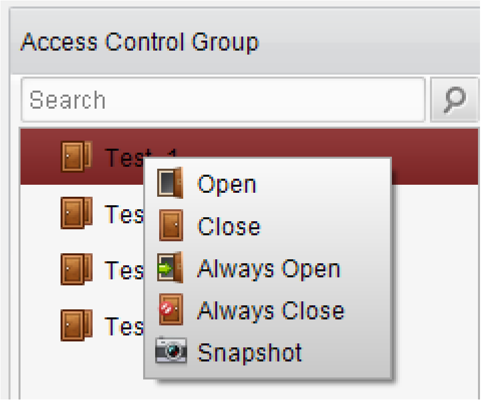
Group Anti-control

Purpose:

You can control the status for a group of control points (doors) in this section.

Steps:

1. Enter the status monitor page.
2. Right click on a group in the **Group** list and to select a door status for the group.

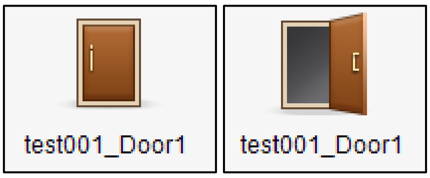


Notes:

- If the status is selected as **Remain Open/Remain Closed**, all the doors in the group will keep open/ closed until a new anti-control command being made.
- The function of picture capturing cannot be realized until the storage server is installed.

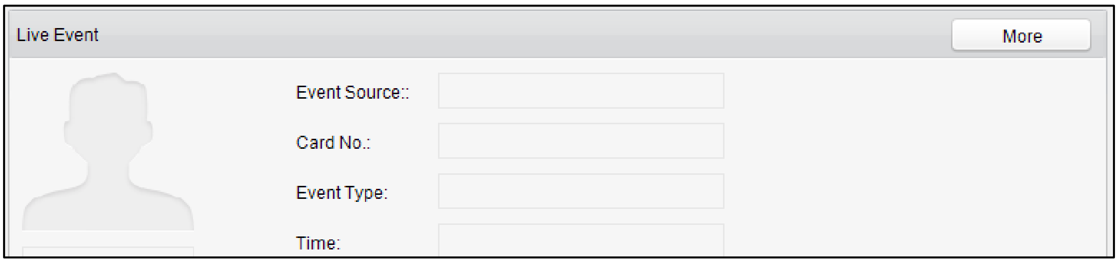
22.1.2 Access Status

The door status will be represented instantly by the change of icon on the **Access Information** panel if the access event is triggered or an anti-control command is made.



22.1.3 Real-Time Event

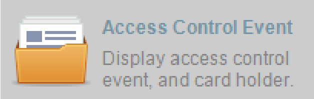
You can check the Real-time information of the access event on this panel. Click **More** to enter the Access Event page to view more event information.

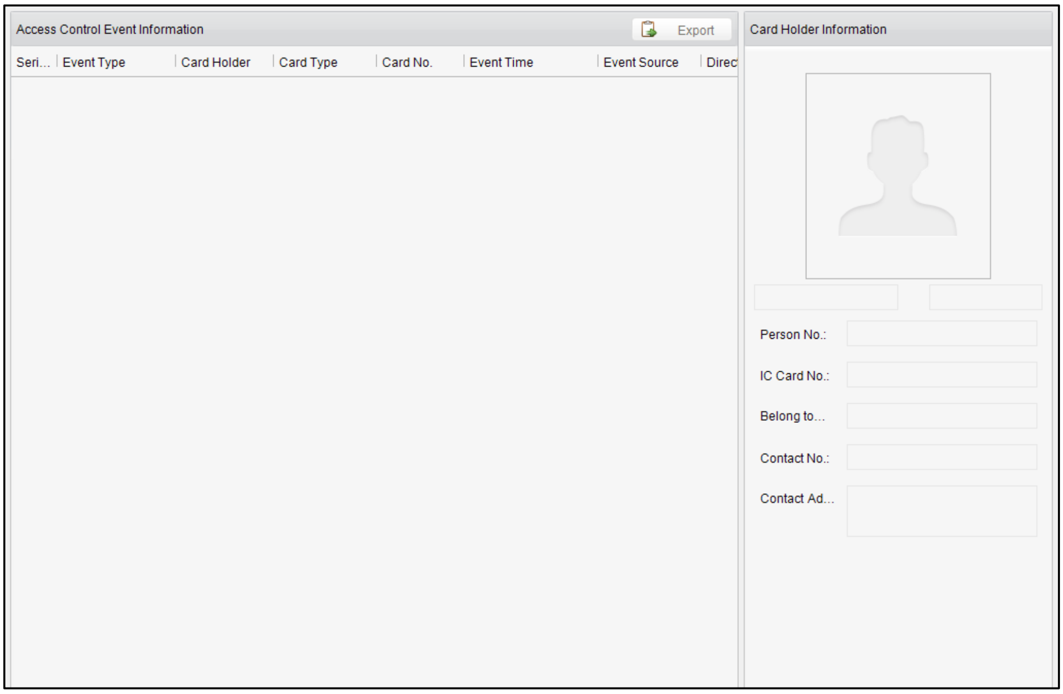


22.2 Access Control Event

Purpose:

You can view real-time access event (such as swiping to open the door, unrecognized card number, duration group error, etc.) information in this section.

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



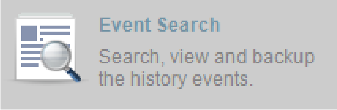
Steps:

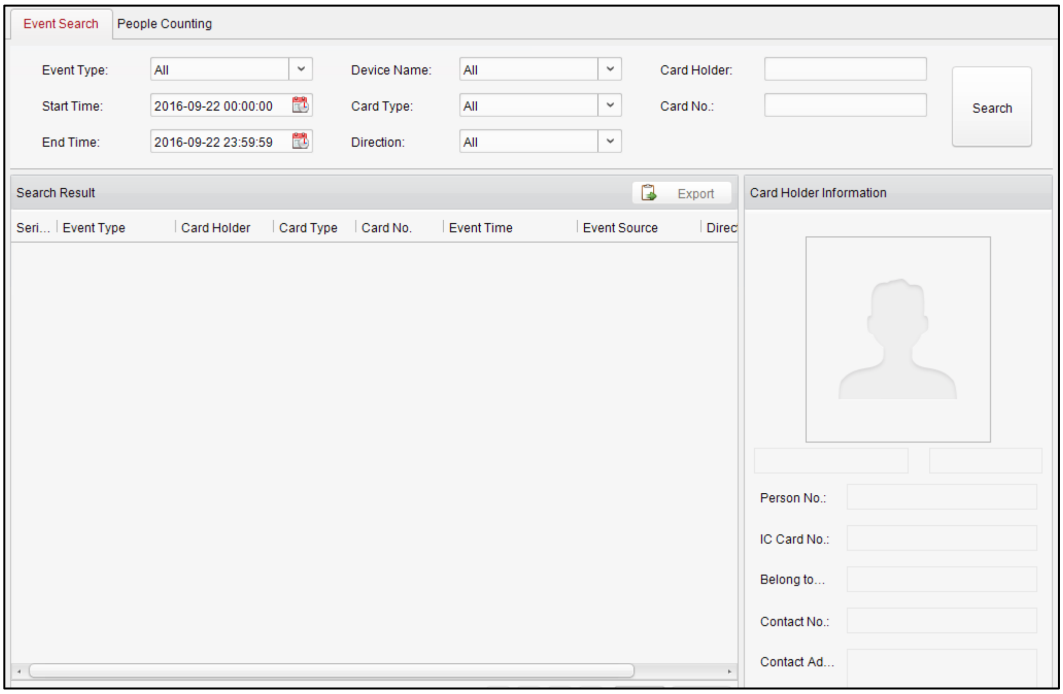
1. Enter the access event page.
2. View the event information in the event list.
3. Click on an event to view the information of the card holder on the **Person Information** panel on the left side of the page.

22.3 Event Search

Purpose:

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

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



Event Type: All

Start Time: 2016-09-22 00:00:00

End Time: 2016-09-22 23:59:59

Device Name: All

Card Type: All

Direction: All

Card Holder:

Card No.:

Person No.:

IC Card No.:

Belong to...

Contact No.:

Contact Ad...

Steps:

1. Enter the event search page.
2. Enter the search criteria (event type/ person name/ card No/ start &end time).
3. Click Search to get the search results.
4. View the event information in the event list.
5. Click an event to view the information of the card holder on the **Person Information** panel on the left side of the page.

   Or click Export to export the result.

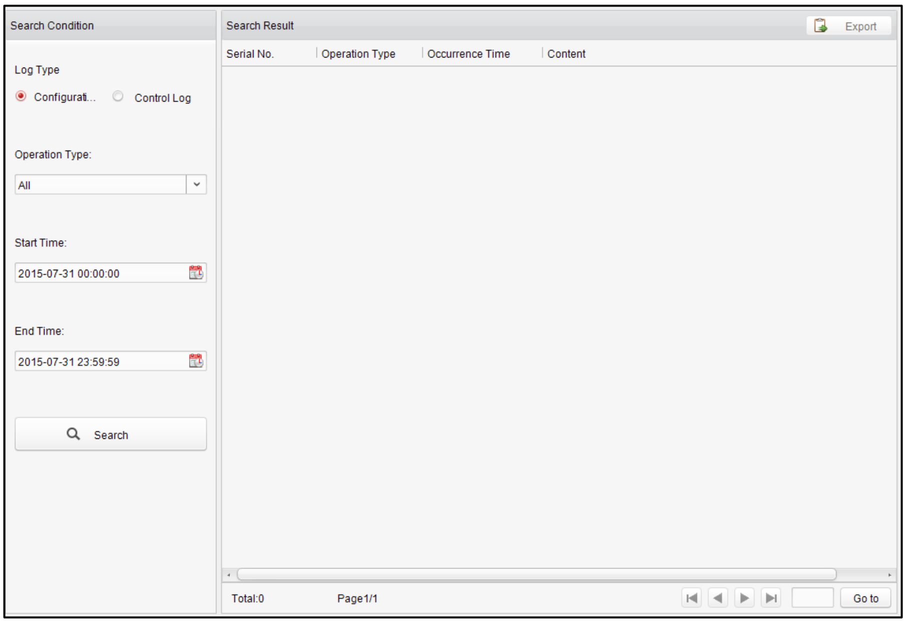
Chapter 23 System Maintenance

23.1 Log Management

Purpose:

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

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



Search Condition

Log Type

● Configurati... ○ Control Log

Operation Type: All

Start Time: 2015-07-31 00:00:00

End Time: 2015-07-31 23:59:59

Search

Search Result

Serial No.	Operation Type	Occurrence Time	Content

Total:0 Page1/1

Configuration Logs Searching

Purpose:

The Configuration Log files of the Access Control System can be searched by time ,including One-card Configuration, Access Control Configuration, Downloading Permission and System Configuration.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the Operation Type of log files.
4. Click the icon 📅 to specify the start time and end time.
5. Click Search. The matched log files will display on the list.

   You can check the operation time, log type and other information of the logs.

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

Control Logs Searching

Purpose:

The Control Log files of the Access Control System can be searched by time ,including Access Control and Log Search.

Steps:

1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the Operation Type of log files.
4. Click the icon 📅 to specify the start time and end time.
5. Click 🔍 Search. The matched log files will display on the list.

   You can check the operation time, log type and other information of the logs.

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

23.1.1 Searching Configuration Log

Searching One-card Configuration Logs

Purpose:

The One-card Configuration Log files include departments, persons and cards log files. One-card Configuration of the Access Control System can be operated as adding ,modifying and deleting logs.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as One-card Configuration.
4. Click the icon 📅 to specify the start time and end time.
5. Click 🔍 Search. The matched log files will display on the list.

   You can check the operation time, log type and other information of the logs.

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

Searching Access Control Configuration Logs

Purpose:

The Access Control Configuration Log files include Access Control devices log files. Access Control Configuration of the Access Control System can be operated as adding, modifying and deleting door groups or doors and access control device permission operations.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as Access Control Configuration.
4. Click the icon 📅 to specify the start time and end time.
5. Click 🔍 Search. The matched log files will display on the list.

   You can check the operation time, log type and other information of the logs.

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

Searching Downloading Permission Logs

Purpose:

The Downloading Permission Log files include downloading permission log files, and no record for downloading permission failure log files.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as Downloading Permission.
4. Click the icon 📅 to specify the start time and end time.
5. Click Search. The matched log files will display on the list.

   You can check the operation time, log type and other information of the logs.

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

Searching System Configuration Logs

Purpose:

The System Configuration Log files of the Access Control System can be searched as system configuration interface log files.

Steps:

1. Open the Log Search page.
2. Select the radio button of Configuration Logs.
3. Select the operation type as System Configuration Logs.
4. Click the icon 📅 to specify the start time and end time.
5. Click Search. The matched log files will display on the list.

   You can check the operation time, log type and other information of the logs.

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

23.1.2 Searching Control Log

Searching Access Control Logs

Purpose:

The Access Control Log files of the Access Control System include door groups and doors access control logs and door on/off control log files.

Steps:

1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the operation type as Access Control Logs.
4. Click the icon 📅 to specify the start time and end time.
5. Click Search. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.

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

Log Search

Purpose:

The Log Search of the Access Control System include informations for configuration log files and control log files.

Steps:

1. Open the Log Search page.
2. Select the radio button of Control Logs.
3. Select the operation type as Log Search.
4. Click the icon to specify the start time and end time.
5. Click Search. The matched log files will display on the list.

You can check the operation time, log type and other information of the logs.

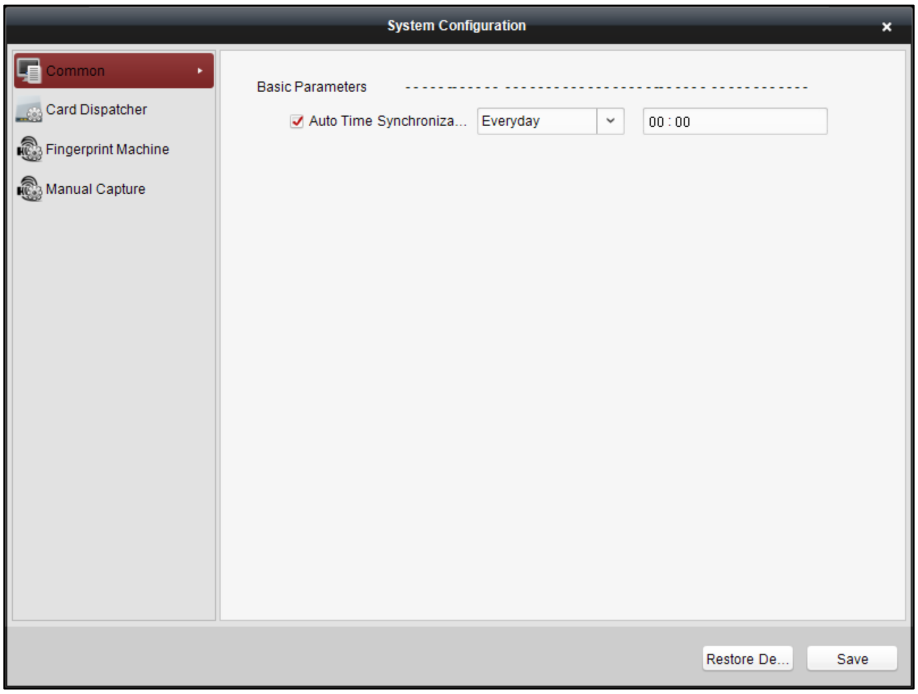
Note: Please narrow the search condition if there are too many log files.

23.2 System Configuration

Purpose:

The general parameters, Auto Time Adjustment and Card Reader of the Access Control System can be configured.

Click the System Configuration (Configure parameters for normal system and card dispatcher.) icon on the control panel to open the System Configuration page.



Basic Parameters

☑ Auto Time Synchroniza... Everyday 00 : 00

Auto Time Synchronization

The Auto Time Synchronization of the Access Control System can operate auto time adjustment to all access control devices of the Access Control System according to specified period and time.

Card Reader Configuration

The Card Reader Configuration is for Access Control System to read the card by setting Card Reader parameters. For now DS-K1F100-D8、DS-K1F100-M、DS-K1F100-D8E card reader types are supported.

Fingerprint Machine

The Fingerprint Machine is for Access Control system to collect fingerprints.

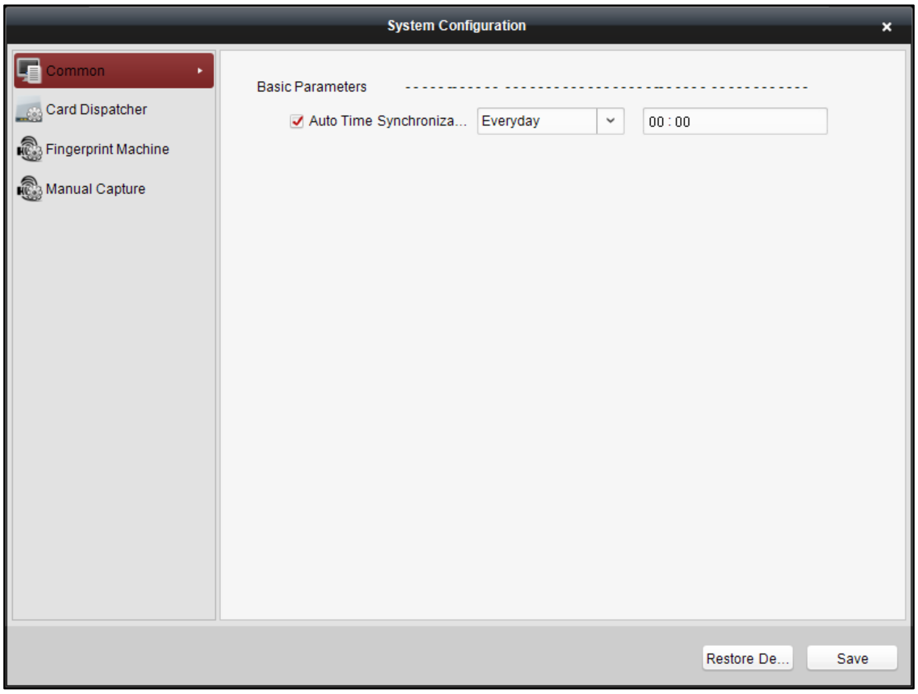
Manual Capture Configuration

The Manual Capture Configuration is for Access Control system to take photos remotely.

23.2.1 Auto Time Synchronization

Steps:

1. Open the System Configuration page.
2. Click the **Common** tab to enter the Common Settings interface.



☑ Auto Time Synchroniza... Everyday 00 : 00

3. Tick the checkbox to enable Auto Time Synchronization.
4. Select the matched day and input the time to operate the time adjustment.
5. Click Save to save the settings.

Note: You can click the Restore De... (Restore Default Value) to restore the defaults of all the local configurations.

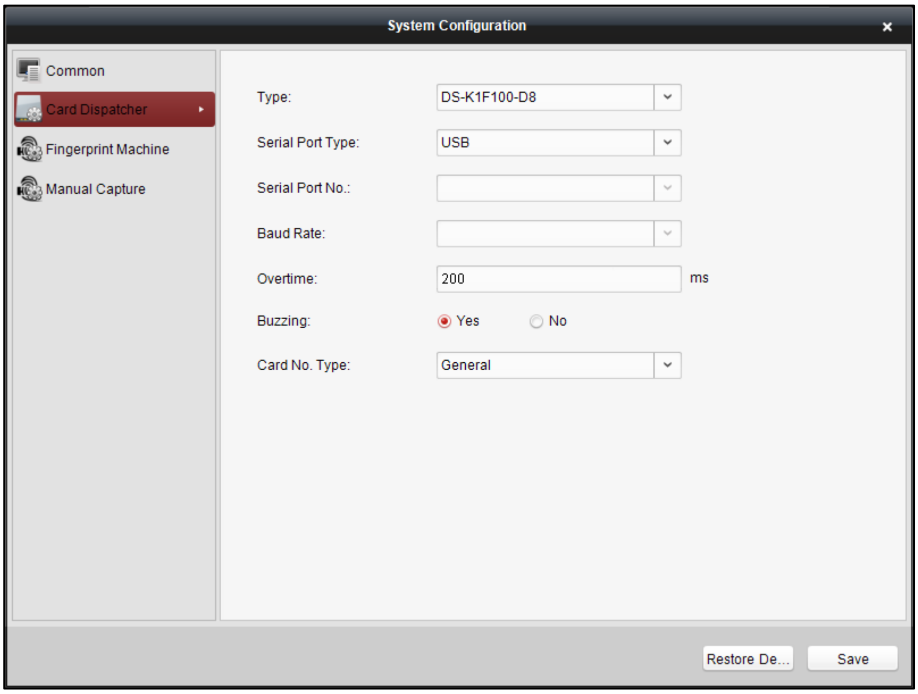
23.2.2 Card Dispenser Configuration

Purpose:

The Card Reader Configuration of the Access Control System can configure device type, connection mode, serial port, baud rate and other parameters of the Card Reader Configuration.

Steps:

1. Click **Card Dispatcher** on the System Configuration interface to open the Card Dispatcher Configuration page.



Type: DS-K1F100-D8

Serial Port Type: USB

Serial Port No.:

Baud Rate:

Overtime: 200 ms

Buzzing: ● Yes ○ No

Card No. Type: General

2. Select the device type, serial port type, serial port, baud rate, and other parameters of the Card Dispatcher.
3. Click the save button to save the settings.

Notes:

- Configuration Instruction

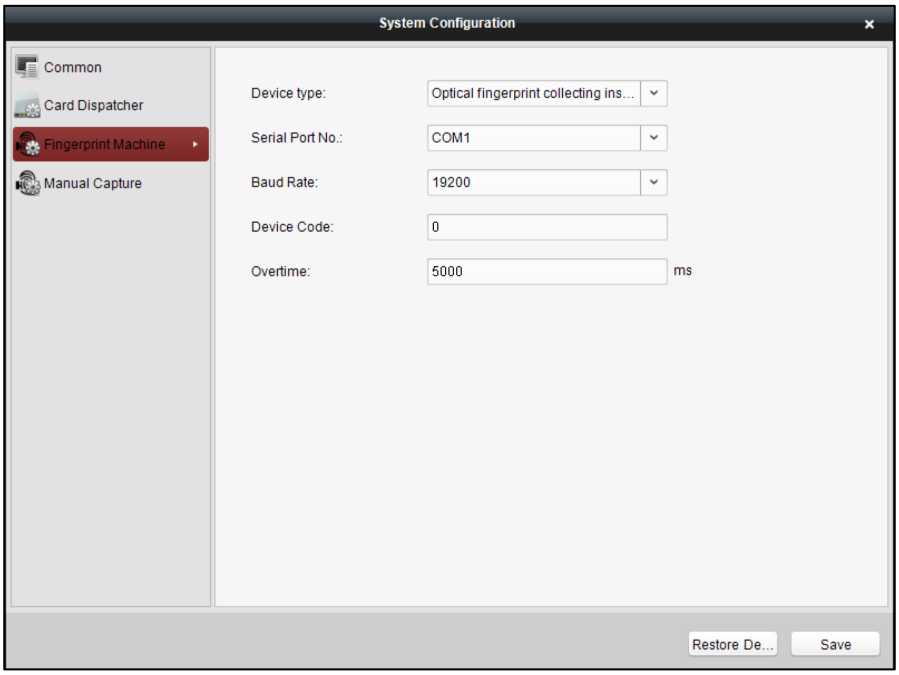
  DS-K1F100-M: select Serial Port Mode as accessing mode (currently only support serial port mode), the serial port No. is the COM port No. of the computer. Set other parameters as default.

  DS-K1F100-D8E and **DS-K1F100-D8E:** select USB Mode as accessing mode (currently only support USB mode). Set other parameters as default.
- It is supported using card type as regular and Wiegand.
- When the Buzzing is selected as "YES", the audio will be off when you click Save. If the Card Reader Configuration is set wrong; the audio will be on when you click Save and when you insert the card reader if the configuration is set correct.
- You can click Restore De... (Restore Default Value) to restore all of the local configuration to the defaults.

23.2.3 Fingerprint Machine Configuration

Steps:

1. Click **Fingerprint Machine** on the System Configuration interface to open the Fingerprint Machine Configuration page.



Device type: Optical fingerprint collecting ins...

Serial Port No.: COM1

Baud Rate: 19200

Device Code: 0

Overtime: 5000 ms

2. Select the device type, serial port number, baud rate, device code, and overtime parameters of the fingerprint machine.

3. Click Save to save the settings.

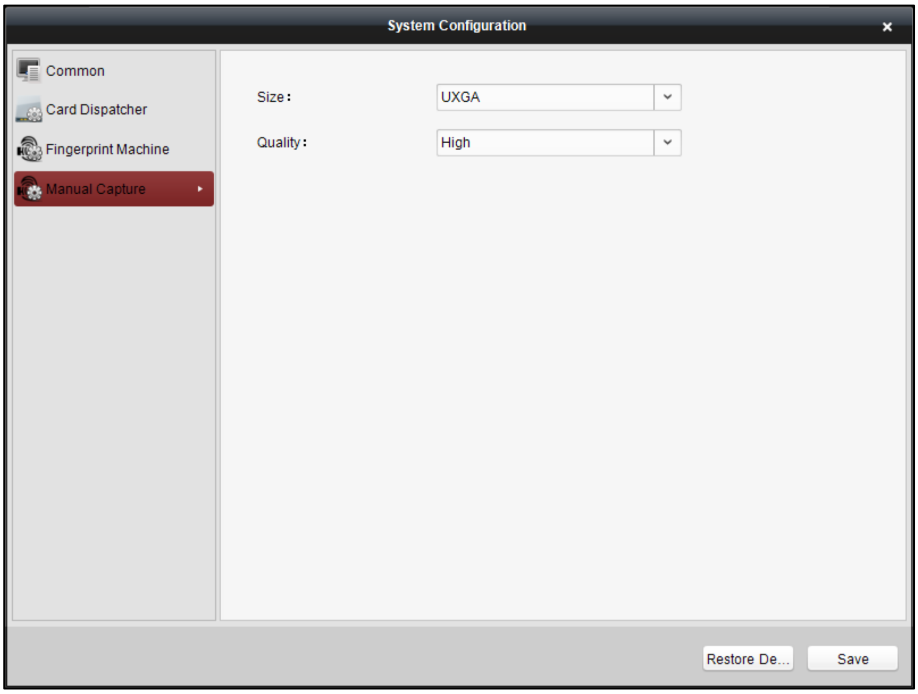
Notes:

- It is supported using device type as Optical Fingerprint Collecting Instrument and Capacitive Fingerprint Collecting Instrument.
- The serial port number should correspond to the serial port number of PC.
- The baud rate should be called according to the external fingerprint card dispatcher. The default value is 19200.
- Overtime refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.
- You can click the Restore De... button to restore the defaults of all local settings.

23.2.4 Manual Capture Configuration

Steps:

1. Click **Manual Capture** on the System Configuration interface to open the Manual Capture Configuration page.



Size: UXGA

Quality: High

2. Select the picture size from the dropdown list
3. Select the picture quality from the dropdown list.

Notes:

- It is supported using the picture size as CIF, QCIF, 4CIF/D1, SVGA, HD720P, VGA, WD1, and AUTO.
- It is supported using the picture quality as High, Medium and Low.

You can click Restore De... (Restore Default Value) to restore all of the local settings the the defaults.

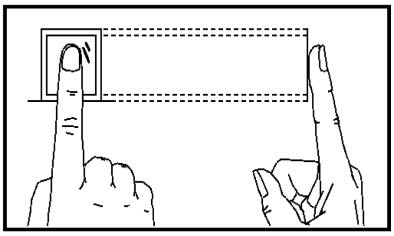
Chapter 24 Appendix: Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

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

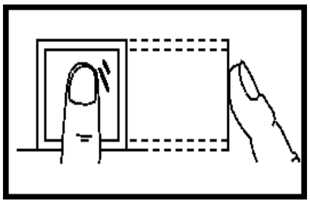


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

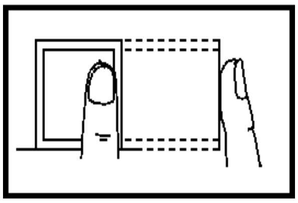
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

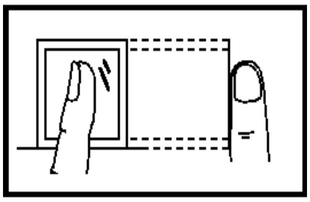
Vertical



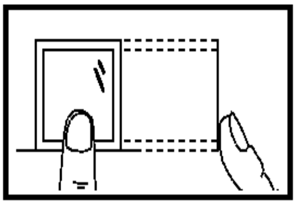
Edge I



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.

Troubleshooting

Live View

Problem:

- Failed to get the live view of a certain device.

Possible Reasons:

- Unstable network or the network performance is not good enough.
- The device is offline.
- Too many accesses to the remote device cause the load of the device too high.
- The current user has no permission for live view.
- The version of the client software is below the needed version.

Solutions:

- Check network status and disable other not in use process on your PC.
- Check the device network status.
- Restart the device or disable other remote access to the device.
- Log in with the admin user and try again.
- Download the client software of the latest version.

Recording

Problem:

- Local recording and remote recording are confused.

Solutions:

- The local recording in this manual refers to the recording which stores the video files on the HDDs, SD/SDHC cards of the local device.
- The remote recording refers to the recording action commanded by the client on the remote device side.

Playback

Problem:

- Failed to download the video files or the downloading speed is too slow.

Possible Reasons:

- Unstable network or the network performance is not good enough.
- The NIC type is not compatible.
- Too many accesses to the remote device
- The current user has no permission for playback.
- The version of the client software is below the needed version.

Solutions:

- Check network status and disable other not in use process on your PC.
- Directly connect the PC running the client to device to check the compatibility of the NIC card.
- Restart the device or disable other remote access to the device.
- Log in with the admin user and try again.
- Download the client software of the latest version.

FAQ

Q: **During live view, an error message prompts and the error code is 91.**

A: For live of multiple window, the channel may not support sub stream. Please disable the function of **Auto-change Stream Type** in **System Configuration -> Image**, and select the appropriate steam type for live view.

Q: **During live view, the image is blurred or influent.**

A: Please check the driver of video card. We highly recommend you update the driver of video card to the latest version.

Q: **Memory leak and the client crashed after running for a while.**

A: In the installation directory of the client software, open the **Setup.xml** file with Notepad and modify the value of **EnableNetandJoystickCheck** to **false**. Restart the client, and if the problem is still not solved, please contact our technique support.

Q: **During live view, when getting stream via the Stream Media Server, an error message prompts and the error code is 17.**

A: Please check the port mapping of Stream Media Server, especially RTSP port.

Error Code

Code	Error Name	Description
317	No videos.	It will be prompted when the user has no permission to play back.
1	Invalid user name or password	
2	No permission.	The user in the device has no enough permission.
4	Invalid channel number.	It will be prompted in the live view of remote screen control.
5	No more devices can be connected.	
7	Failed to connect the device.	
23	Do not support.	
29	Operating failed.	
43	No buffer.	It will be prompted when adding a device and the device port is occupied by a web server.
55	Invalid IP address.	
56	Invalid MAC address.	
91	The channel does not support the operation.	It will be prompted when failed to get the sub stream.
96	The device is not registered on the DDNS.	
153	The user is locked.	
250	The device is not activated.	
404	Channel No. error or the device does not support the sub stream.	It will be prompted when failed to get the sub stream or the sub stream does not exist.
424	Failed to receive the data for RTSP SETUP.	It will be prompted when adding the live view for the software DVS via external network.
800	No more bandwidth can be used.	
2		The stream is not a Video & Audio stream.
6		The playback window turns black when adopting H.265 in the 64bit operating system.
3		The connection problem between the software and the stream media server.
17		The streaming problem between the stream media server and the device.

First Choice for Security Professionals

HIKVISION | www.hikvision.com