iVMS-4200 Client Software

User Manual

User 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 security management software for the DVRs, NVRs, IP cameras, encoders, decoders, security control panel, video intercom device, access control 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.

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, 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

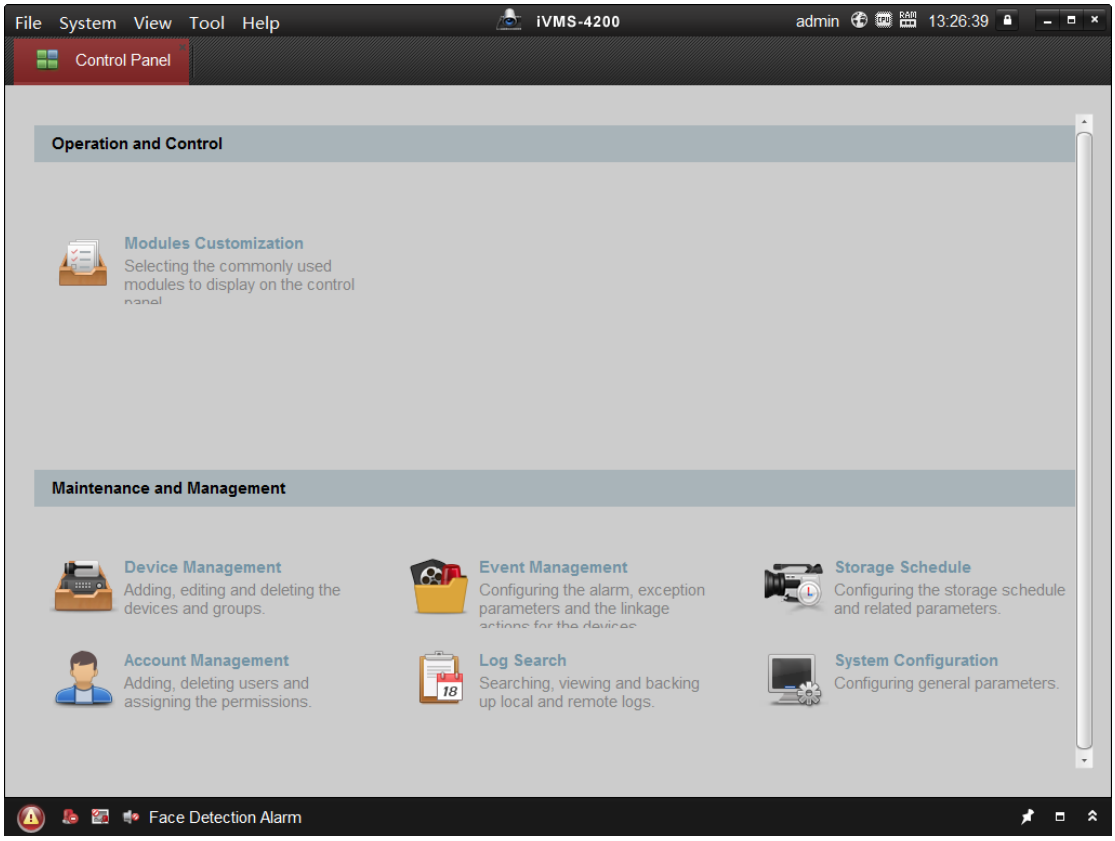
GPU: 256 MB or above

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

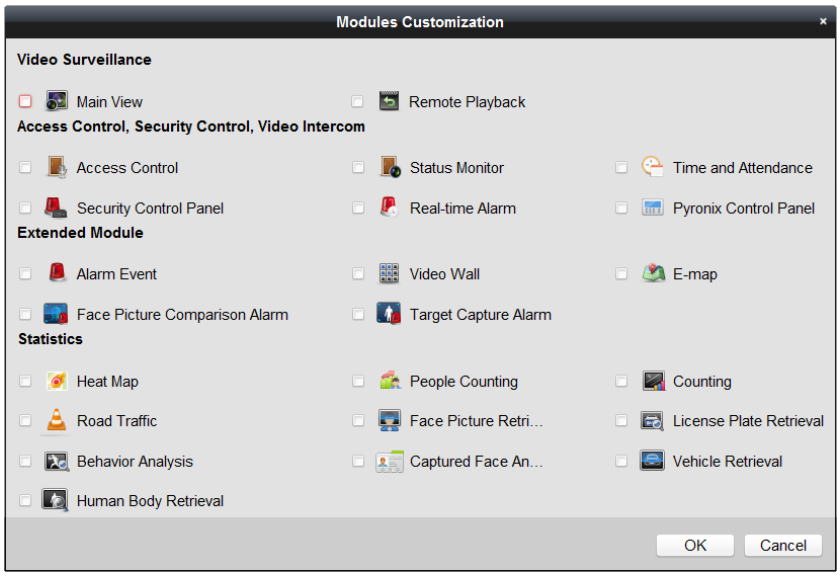
Control Panel of iVMS-4200:



For the first time running the software, you can click **Modules Customization** on the control panel to select the modules to display on the Operation and Control area of the control pane.

Steps:

1. Click  to pop up the following window.



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

Notes:

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

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 Update Instructions

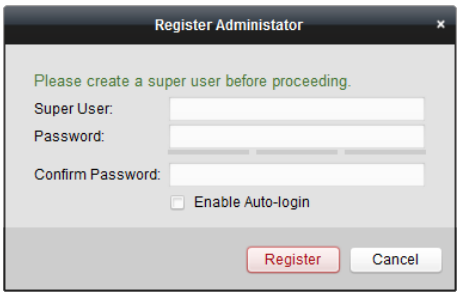
- **Encrypt Database**
  For data security, encrypt the database and encrypt the sensitive information with random secret key.
- **RTSP Streaming Protocol**
  Add RTSP streaming protocol for getting stream when live view when editing channel parameters.
- **Divide Remote Configuration to General and Advanced Configuration**
  Divide remote configuration to general or advanced parameters configuration if the device supports.
- **Resource Overview**
  Add resource overview in Help > Resource Overview.
- **Open Source Software License**
  Provide open source software License in Help > Open Source Software License.
- **Face Picture Comparison Alarm**
  Add Face Picture Comparison module to view the captured face pictures and the matched face picture in face picture library
- **Target Capture Alarm**
  Add Target Capture Alarm module to view the captured target pictures, such as face, human body, vehicle, etc.
- **Face Retrieval, Human Body Retrieval, Vehicle Retrieval**
  Add statistics modules: Face Retrieval, Human Body Retrieval, Vehicle Retrieval to analyze and search the face information, human body information, and vehicles information.
- **Manual Temperature Measurement and Fire Source Detection Alarm Acknowledgement**
  For thermal cameras, add manually measuring temperature function and fire source detection alarm acknowledgement function.
- **New UI Design for Security Control Panel and Pyronix Control Panel Module**
- **Smart Card for Person**
  Add smart card to person and store fingerprints and ID card infomration in the smart card.
- **Person in Blacklist Management**
  Configure the person information in the blacklist and apply to the device.

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.

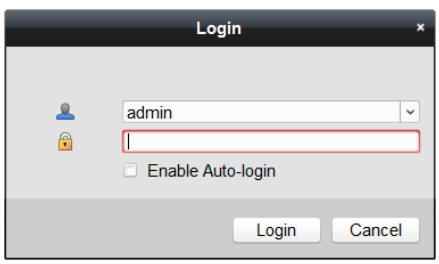


- *A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.*
- *For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case 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.
2. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
3. Click **Login**.



After running the client software, you can open the wizards (including video wizard, video wall wizard, security control panel wizard, access control and video intercom wizard, and attendance wizard), to guide you to add the device and do other settings and operations.

Chapter 3 Device Management

3.1 Adding Device

Purpose:

After running the iVMS-4200, devices including network cameras, video encoders, DVRs, NVRs, decoders, security control panels, video intercom devices, access control devices, 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  on the control panel to open the Device Management page.
2. Click **Device** tab to enter the device management page.
3. On the Device Type panel on the right, select **Hikvision Device** to add the Hikvision devices, including network cameras, video encoders, DVRs, NVRs, decoders, security control panels, video intercom devices, access control devices, etc.
4. (Optional) Click **Add New Device Type** to add other types of devices, including stream media server, Hik-Connect device (device which supports Hik-Connect service), Pyronix control panel, and third-party encoding device.

   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.
5. (Optional) Select a device and click **Remote Configuration** to configure further parameters of the selected device if needed.

   Notes:

   - For some models of devices, you can open its general or advanced parameters configuration window. To open the original remote configuration window, press *CTRL* and click **Remote Configuration**.
   - For detailed settings about the settings, refer to the *User Manual* of the devices.
6. (Optional) Select access control device and CVR from the list and click **Device Status** to view the device status including recording status, signal status, hardware status, etc.

   Note: For CVR, You can click **Device Status** to view the recording status and ANR (Automatic Network Replenishment) recording status.

3.1.1 Activating Device

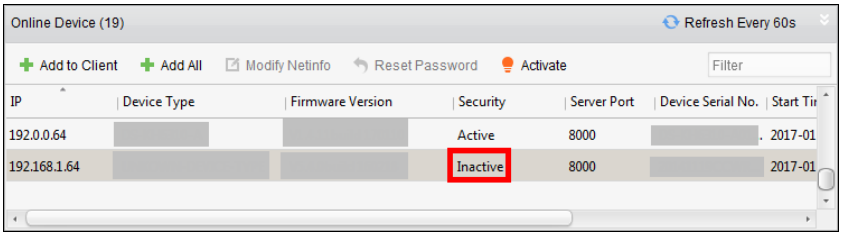
Purpose:

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

Note: This function should be supported by the device.

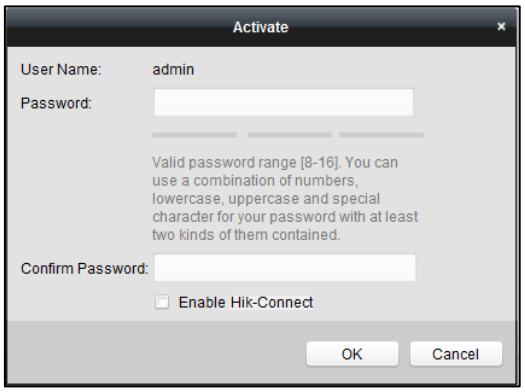
Steps:

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

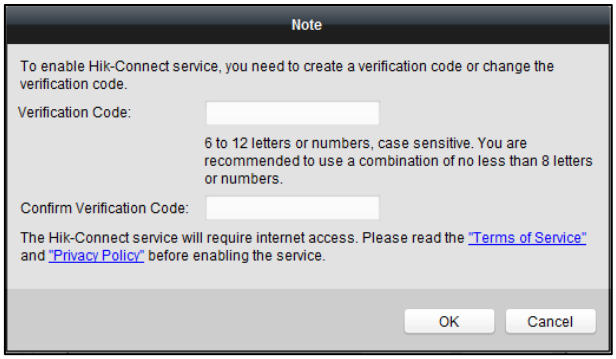


3. Click **Activate** to pop up the Activation interface.
4. Create a password in the password field, and confirm the password.

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



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



   2) Create a verification code.
   3) Confirm the verification code.
   4) Click **Terms of Service** and **Privacy Policy** to read the requirements.

5) Click **OK** to enable the Hik-Connect service.

6. Click **OK** to activate the device.

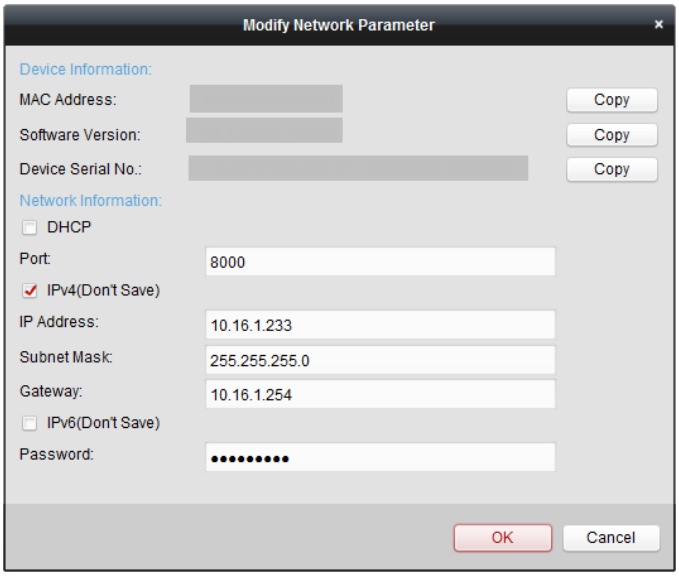
   A "The device is activated." window pops up when the password is set successfully.

7. Click **Modify Netinfo** to pop up the Modify Network Parameter interface.

   Note: This function is only available on the **Online Device** area. You can change the device IP address to the same subnet with your computer if you need to add the device to the software.

8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of DHCP.

9. Input the password set in step 4 and click **OK** to complete the network settings.

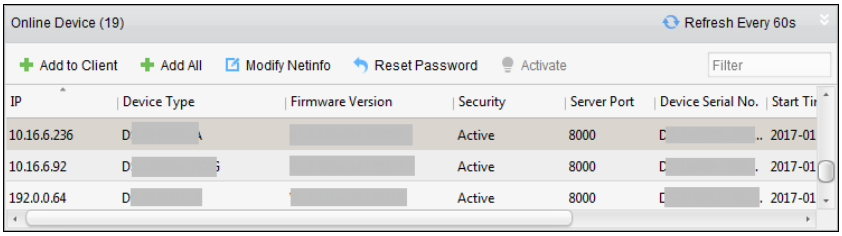


3.1.2 Adding Online Devices

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.



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, refer to *Chapter 3.1.1 Activating Device.*

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

3. Input the required information.

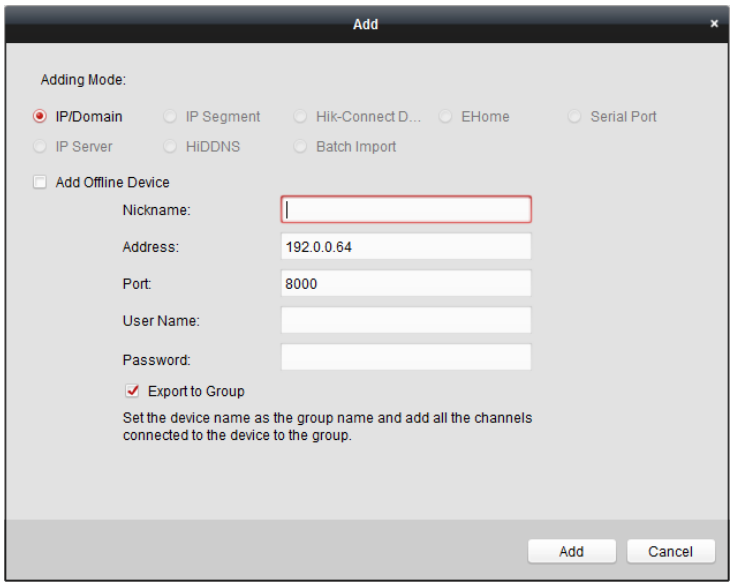
   - **Address:** Input the device's IP address. The IP address of the device is obtained

automatically in this adding mode.

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



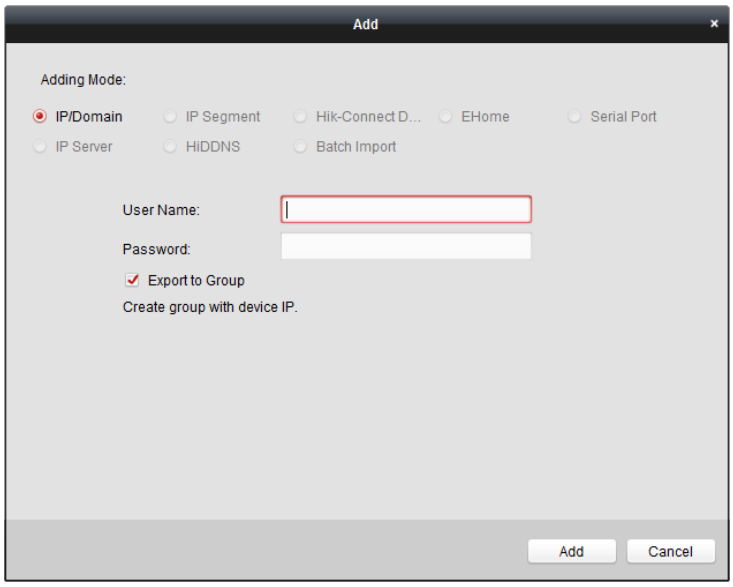
Add Multiple Online Devices

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 window box. In the pop-up message box, enter the user name and password for the devices to be added.

Add All Online Devices

If you want to add all the online devices to the client software, click **Add All** and click **OK** in the

pop-up message box. Then enter the user name and password for the devices to be added.



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.

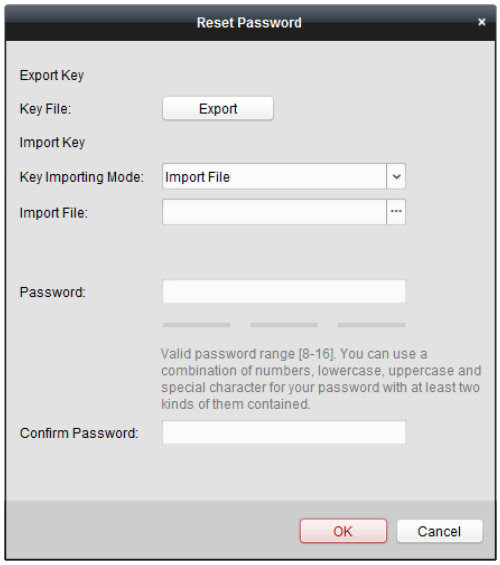
Reset Password

According to the different devices, the software provides five 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 Export button, password and confirm password field pops up, follow the steps below to reset the password:



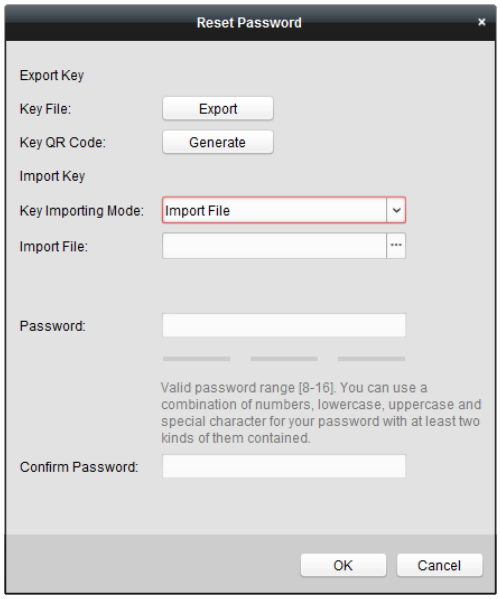
Steps:

1. Click **Export** to save the device file on your PC.
2. Send the file to our technical support.
   For the following operations for resetting the password, contact our technical support.

- *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.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Option 2:

If the window with Export and Generate buttons, password and confirm password field pops up as follows, follow the steps below to reset the password:



Steps:

1. Click **Generate** to pop up the QR Code window.
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 support.
   For the following operations for resetting the password, contact our technical support.

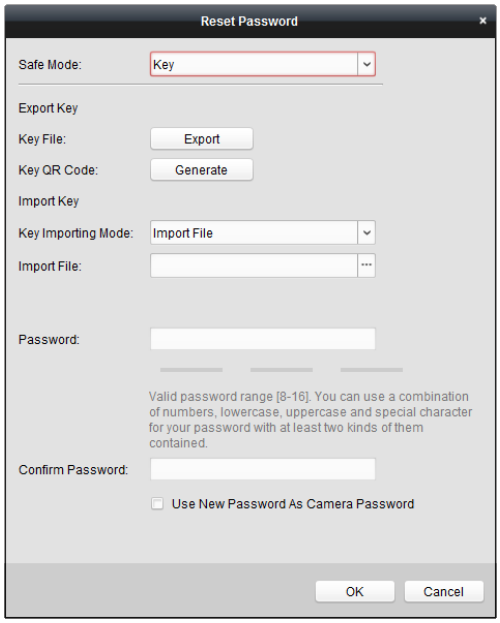
- *The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a*

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.

- *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 safe mode selectable pops up as follows, you can perform the following steps to reset the device password.



Steps:

1. Select the Safe Mode for resetting the device password.
   If you select **Key** as the safe mode, refer to *Option 2* above for detailed operations.
   If you select **Security Question** as the safe mode, go to *step 2*.
   If you select **GUID File** as the safe mode, go to *step 3*.
2. (Optional) If you select **Security Question** as the safe mode, input the answers of the three security questions.
   Note: You can set the security question when activating the device or in the remote configuration. For details, refer to the User Manual of the device.
3. (Optional) If you select **GUID File** as the safe mode, in the Import File field, click ... to import the GUID file.
   Note: You can save the GUID file when activating the device. For details, refer to the User Manual of the device.
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.

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Option 4:

For some old version device, 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: For getting the security code, contact our technical support.

- *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. 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.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Option 5:

For some old version device, if the window with Import and Export 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 support.
3. For the following operations for resetting the password, contact our technical support.

- *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. 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.

- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Synchronizing 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 by IP or Domain Name

Steps:

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

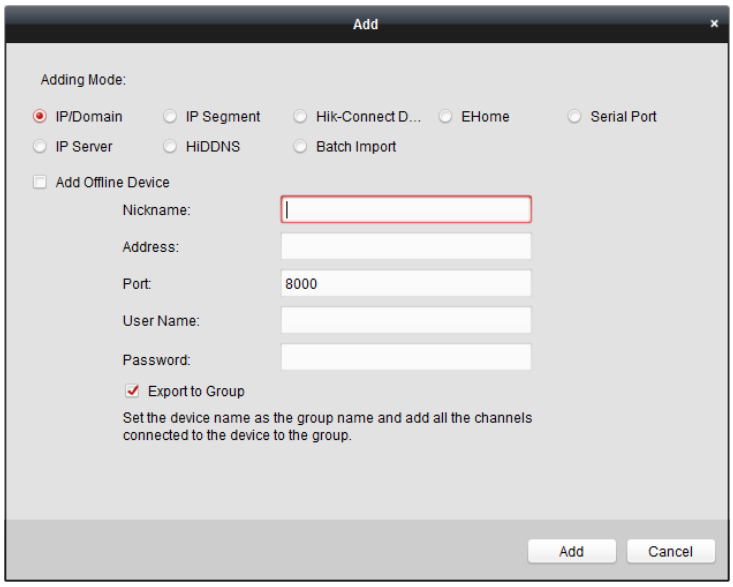
   The password strength of the device can be checked by the software. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase 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, check the **Export to Group** checkbox to create a group by the device name.

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

   Note: iVMS-4200 also provides a method to add the offline devices.

   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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



3.1.4 Adding Devices by IP Segment

Steps:

1. Click **Add** to open the device adding window 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, check the **Export to Group** checkbox to create a group by the device name.

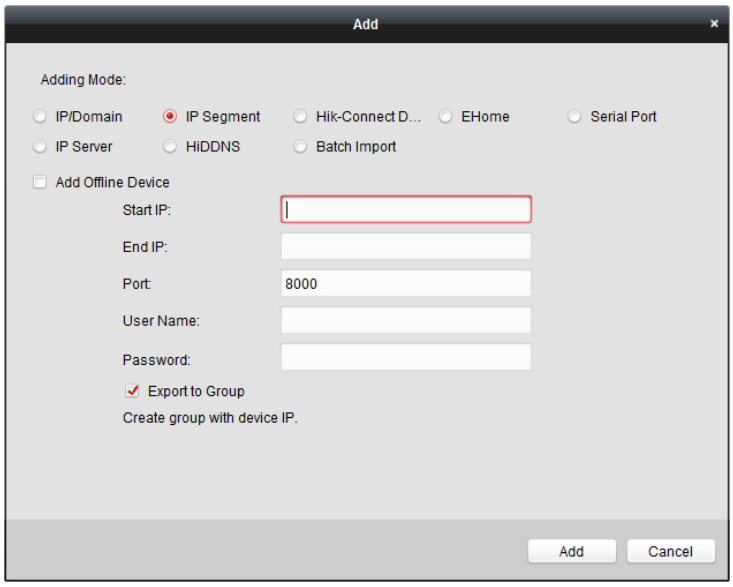
   You can import all the channels of the device to the corresponding group by default.

   Note: iVMS-4200 also provides a method to add the offline devices.

   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

You can add the device which the IP address is between the start IP and end IP to the device list.



3.1.5 Adding Devices by Hik-Connect Domain

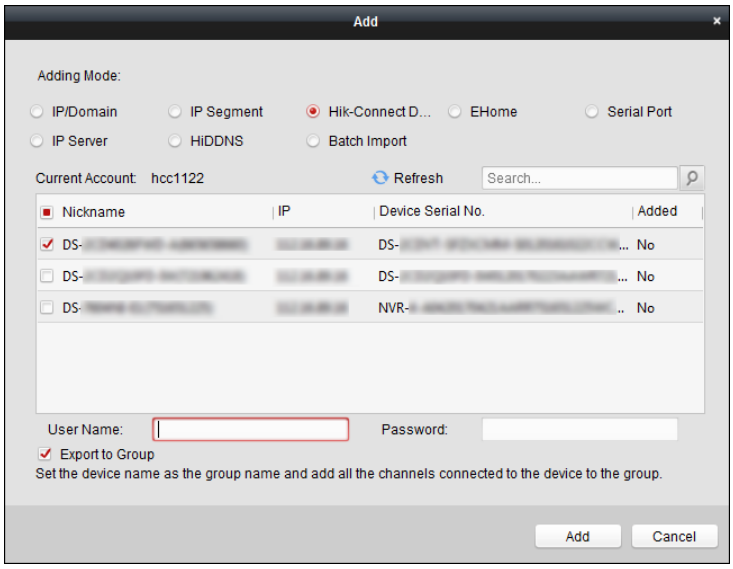
Purpose:

You can add the devices to the client via Hik-Connect by inputting the device username and device password.

Before you start: Add the devices to Hik-Connect account via iVMS-4200, iVMS-4500 Mobile Client, or Hik-Connect first. For details about adding the devices to Hik-Connect account via iVMS-4200, refer to *Chapter 9.3 Device Management*.

Steps:

1. Log into the Hik-Connect account. For details, refer to *Chapter 9.2 Logging into Hik-Connect Account.*
2. Click **Hikvision Device -> Add** to open the device adding window.
3. Select **Hik-Connect Domain** as the adding mode.
   The device(s) under the Hik-Connect account will display.
4. (Optional) Click **Refresh** to refresh the device list.
5. (Optional) Input keyword of the device name in the **Search** field to search the device(s).
6. Check the checkbox(es) to select the device(s).
7. Input the device user name and the device password in the **User Name** field and **Password** field respectively.



Notes:

- The device user name is *admin* by default.
- The device password is created when you activate the device. For details, refer to *Chapter 3.1.1* Activating Device.

8. (Optional) Check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
9. Click **Add** to add the device to the local client.

3.1.6 Adding Devices by EHome Account

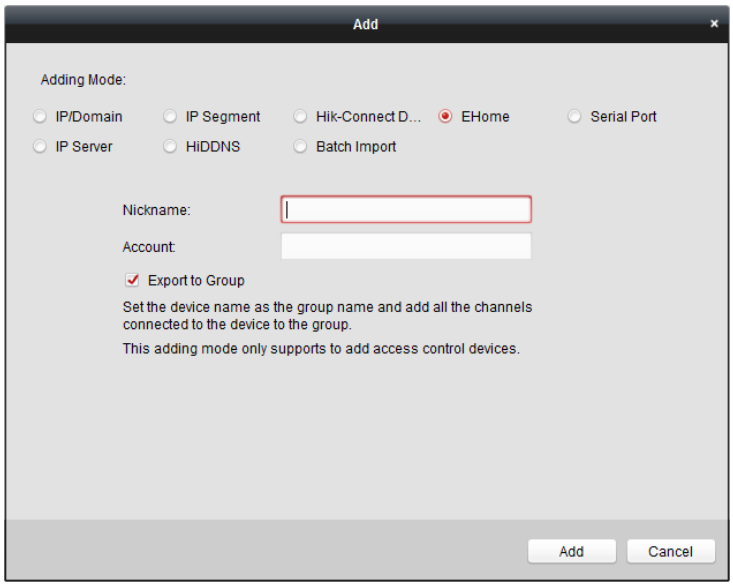
Purpose:

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

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

Steps:

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



3. Input the required information.

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

   Account: Input the account name registered on EHome protocol.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name.

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

   Note: iVMS-4200 also provides a method to add the offline devices.

   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

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

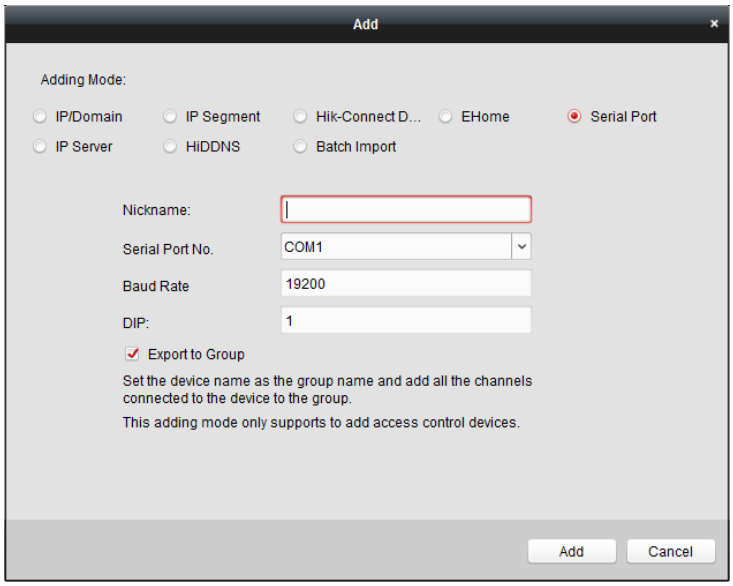
3.1.7 Adding Devices by Serial Port

Purpose:

You can add access control device connected via serial port.

Steps:

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



3. Input the required information.

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

   Serial Port No.: Select the device's connected serial port No.

   Baud Rate: Input the baud rate of the access control device.

   DIP: Input the DIP address of the device.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.

   Note: iVMS-4200 also provides a method to add the offline devices.

   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

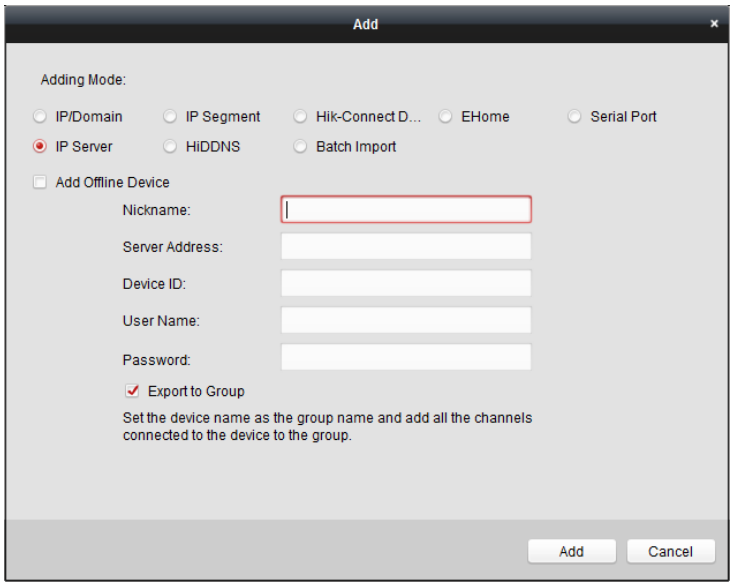
   When the offline device comes online, the software will connect it automatically.

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

3.1.8 Adding Devices by IP Server

Steps:

1. Click **Add** to open the device adding window 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, check the **Export to Group** checkbox to create a group by the device name.

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

   Note: iVMS-4200 also provides a method to add the offline devices.

   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

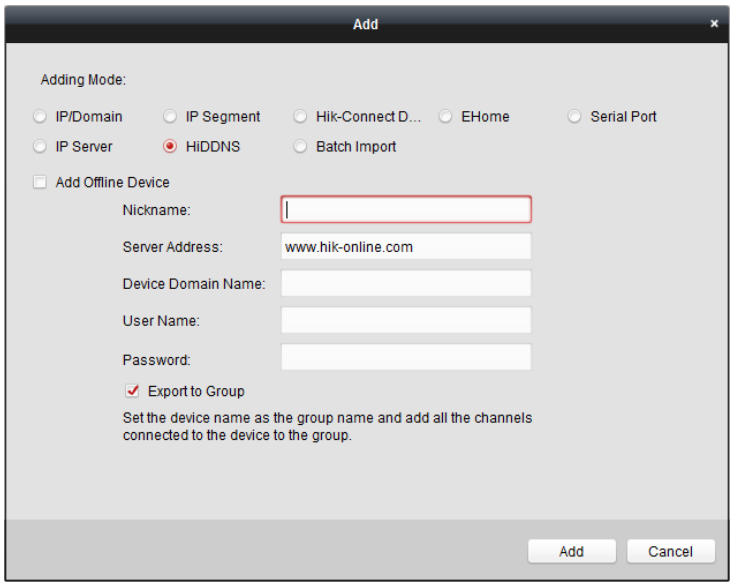
   When the offline device comes online, the software will connect it automatically.

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

3.1.9 Adding Devices by HiDDNS

Steps:

1. Click **Add** to open the device adding window 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, check the **Export to Group** checkbox to create a group by the device name.

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

   Note: iVMS-4200 also provides a method to add the offline devices.

   1) Check the **Add Offline Device** checkbox.
   2) **I**nput the required information, including the device channel number and alarm input number.
   3) Click **Add**.

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

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

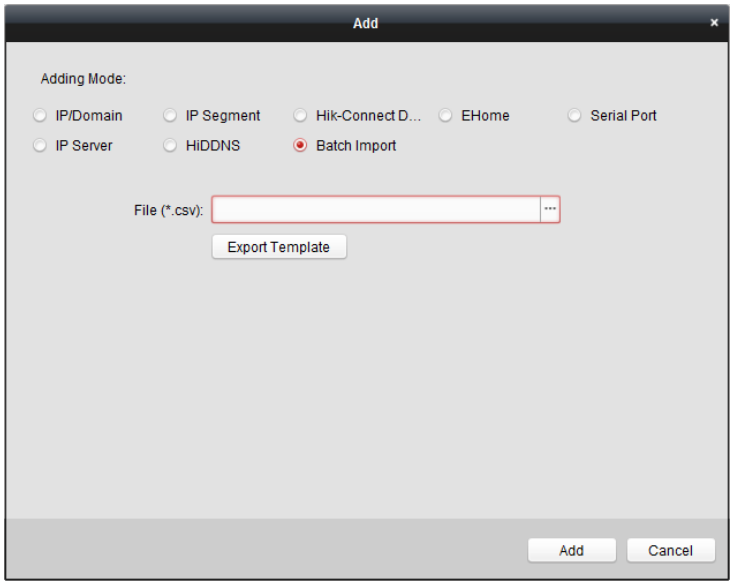
3.1.10 Importing Devices in Batch

Purpose:

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

Steps:

1. Click **Add** to open the device adding window 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.
   - **Adding Mode**: You can input 0, 2, 3, 4, 5, or 6 which indicated different adding modes. 0 indicates that the device is added by IP address or domain name; 2 indicates that the device is added via IP server; 3 indicates that the device is added via HiDDNS; 4 indicates that the device is added via EHome protocol; 5 indicates that the device is added by serial port; 6 indicates that the device is added via Hik-Connect Domain.
   - **Address**: Edit the address of the device. If you set 0 as the adding mode, you should input the IP address or domain name of the device; if you set 2 as the adding mode, you should input the IP address of the PC that installs the IP Server; if you set 3 as the adding mode, you should input *www.hik-online.com*.
   - **Port**: Input the device port No.. The default value is *8000*.
   - **Device Information**: If you set 0 as the adding mode, this field is not required; if you set 2 as the adding mode, input the device ID registered on the IP Server; if you set 3 as the adding mode, input the device domain name registered on HiDDNS server; if you set 4 as the adding mode, input the EHome account; if you set 6 as the adding mode, input the device serial No.
   - **User Name**: Input the device user name. By default, the user name is *admin*.
   - **Password**: Input the device password.

     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.
- **Serial Port No.:** If you set 5 as the adding mode, input the serial port No. for the access control device.
- **Baud Rate:** If you set 5 as the adding mode, input the baud rate of the access control device.
- **DIP:** If you set 5 as the adding mode, input the DIP address of the access control device.
- **Hik-Connect Account:** If you set 6 as the adding mode, input the Hik-Connect account.
- **Hik-Connect Password:** If you set 6 as the adding mode, input the Hik-Connect password.

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

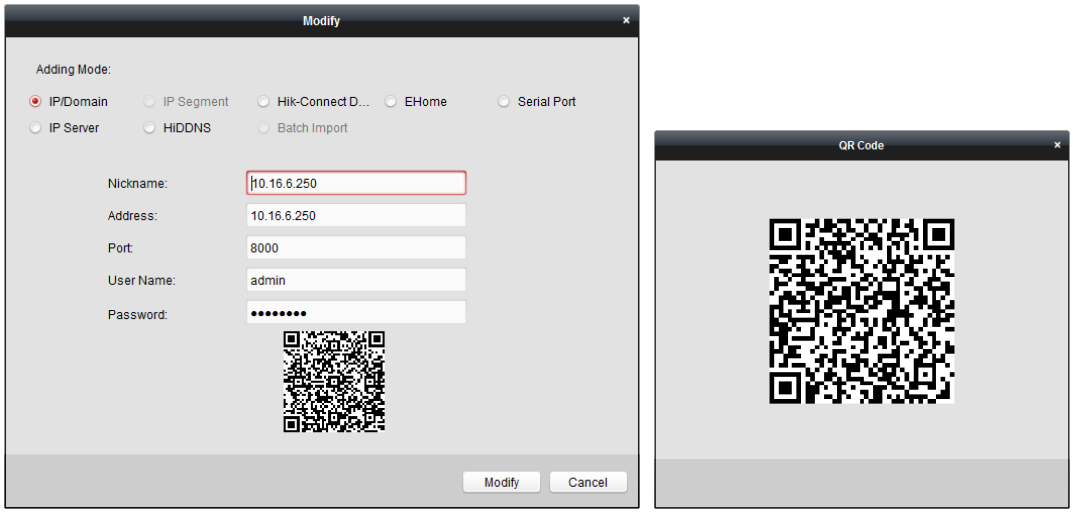
3.1.11 QR Code of Encoding Devices

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, refer to the *User Manual* of the mobile client software.

Check 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.



3.1.12 Checking Device's Online Users

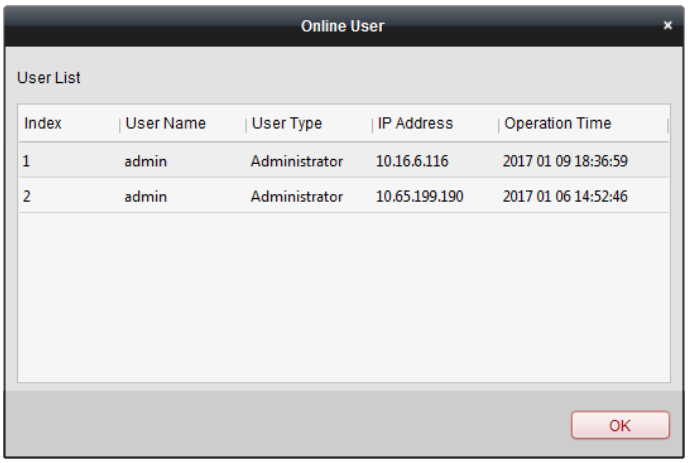
Purpose:

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 User window.



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

3.2 Managing Group

Purpose:

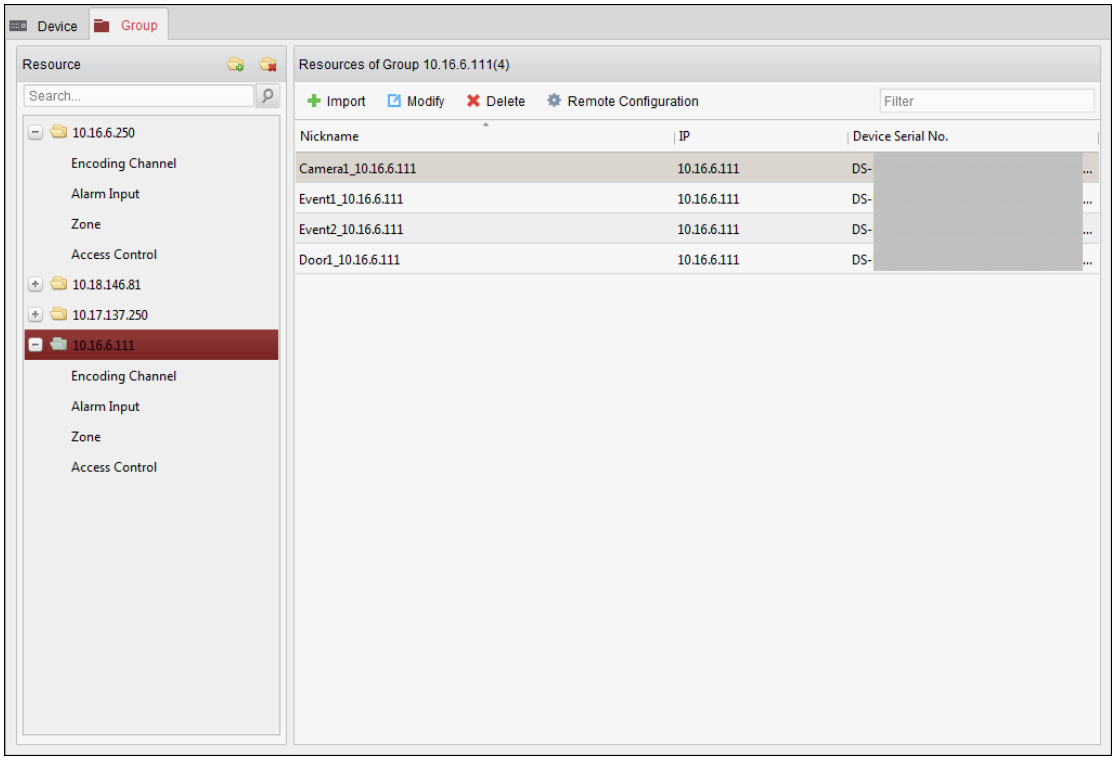
The devices added should be organized into groups for a convenient management. You can get the live view, play back the video files, and do some other operations of the device through the group.

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.



3.2.1 Adding Group

Steps:

1. Click  to open the Add Group window 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.

3.2.2 Importing Channels to Group

Steps:

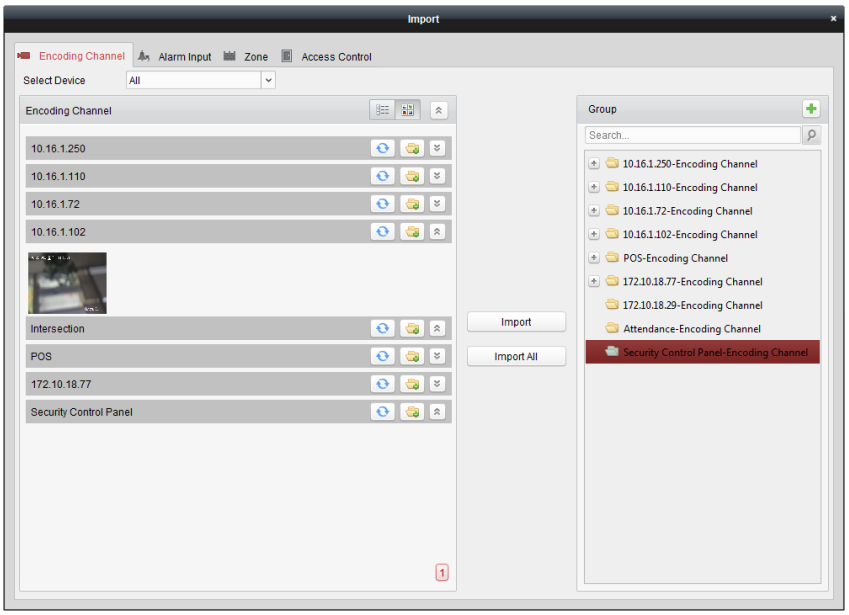
1. Click **Import** on Group Management interface, and then click the **Encoding Channel** tab to open the Import Encoding Channel page.

   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.



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.

3.2.3 Modifying Channel Parameters

Purpose:

After importing the channels to the group, you can edit the channel's parameters. For encoding channel, you can edit the channel name, stream type, protocol type, etc. For alarm input, zone, and other types of channels, you can edit the channel name.

Here we take modifying the encoding channel's parameters as an example.

Note: For modifying the camera(s) of Hik-Connect device, refer to *Chapter 9.3.2 Modifying Camera.*

Steps:

1. Enter **Device Management > Group**.
2. Select the group/camera from the group list on the Resource panel.
3. Click **Modify** or double click the channel to open the modifying channel information window.

4. Edit the camera information, including camera name, stream type, etc.
   - **Video Stream**: Select the stream for the live view of the camera as desired.
   - **Playback Stream Type**: Select the stream for the playback of the camera as desired.
     Note: The Playback Stream Type field will display if the device supports dual-stream.
   - **Rotation 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.
   - **Streaming Protocol:** Select the protocol as RTSP or private for getting stream when live view.
     Note: You should get stream again to take effect.
   - **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.
5. 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 window box.

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.

3.2.4 Removing Channel from 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.

3.2.5 Deleting 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.

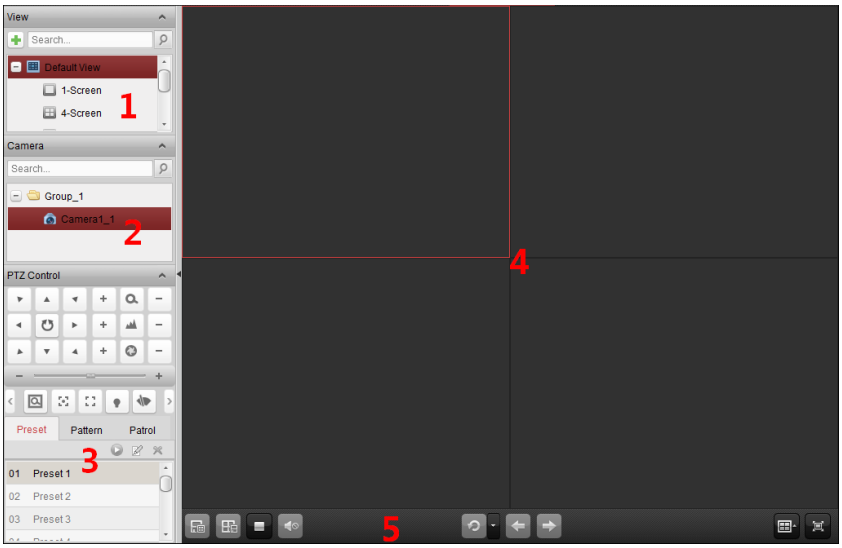
Before you start:

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 *Chapter 3.2.3 Modifying* .

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  .

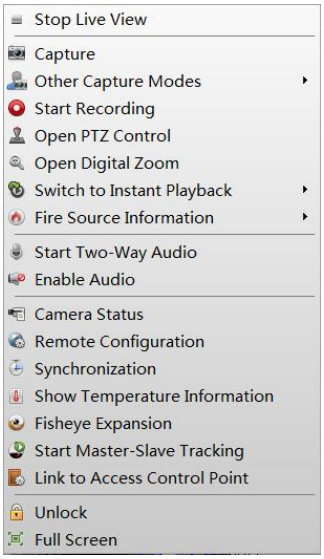
- If the camera is offline, the client can still get the live video via the stream media server if the stream media server is configured. The camera icon will display as . For configuring the stream media server of the camera, refer to *Chapter 10 Forwarding Video Stream through Stream Media Server.*

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, display the fire source region, locate the maximum temperature region, or display the fire source target.
	Start/Stop Two-way Audio	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. You can select to open the general or advanced parameters configuration window if the device supports.
	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.
	Show/Hide Temperature Information	For thermal camera, click to show or hide the temperature on the live view image.
	Fisheye Expansion	Enter the fisheye expansion mode. Only available when the device is fisheye camera. For details, refer to *Chapter 4.7 Live View in Fisheye Mode.*
	Start/Stop Master-Slave Tracking	Click to start/stop locating or tracking the target according to your demand. Only available when the device is box or bullet

		camera. For details, refer to *Chapter 4.8 Starting Master-Slave Tracking.*
	**Link to Access Control Point**	Set the camera's linked access control point (door) and you can control the door status during live view. For details, refer to *Chapter 14.10 Controlling Door during Live View.*
	**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 Live View

Note: For Hik-Connect device, if the live view or video file(s) of its camera(s) is encrypted, you should input the verification code. For details, refer to *Chapter 9.3.2 Modifying Camera.*

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.

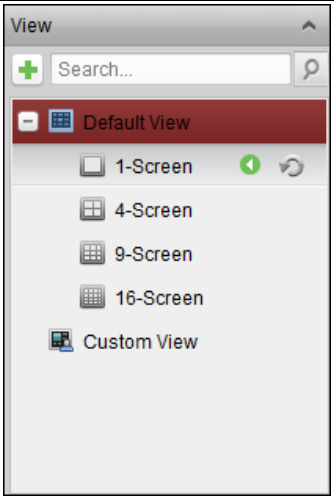
Steps:

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



Starting Live View in Custom View Mode

Purpose:

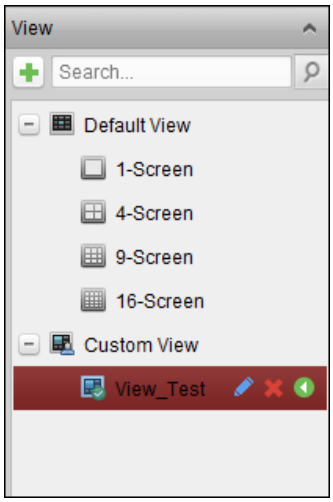
The view mode can also be customized for the video live view.

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.

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, 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, 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, refer to the *User Manual* of the speed dome.
- Hik-Connect device only supports the PTZ movement to the direction of upside, downside, left, and right.

4.3.1 Configuring 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 window 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 .

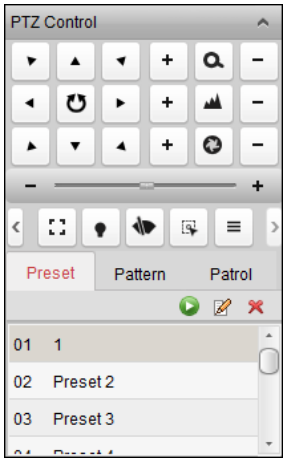
You also perform the following steps to call the preset.

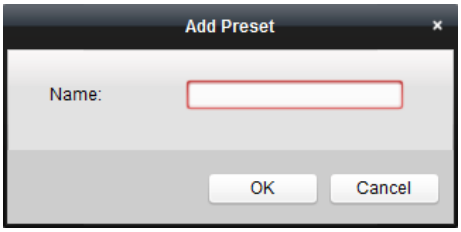
Steps:

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 .





4.3.2 Configuring 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.

4.3.3 Configuring 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:

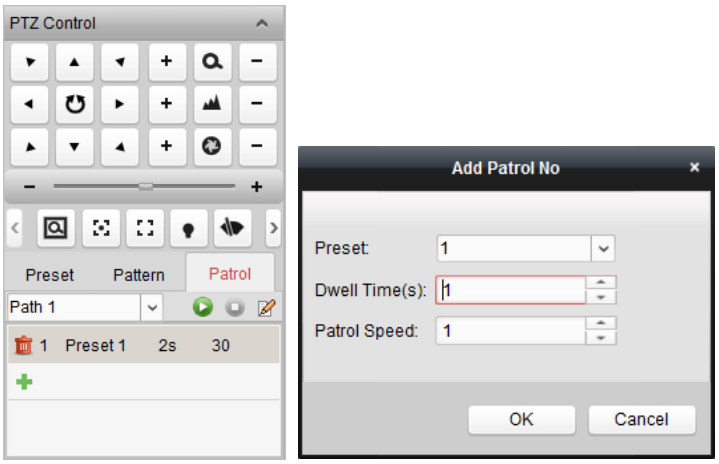
Two or more presets for one PTZ camera need to be added.

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.



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.
	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 22.5 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  .
3. Click the icon  to stop the manual recording.
   A prompt box with the saving path of the video files you just recorded will pop up if all the operations succeed.

Notes:

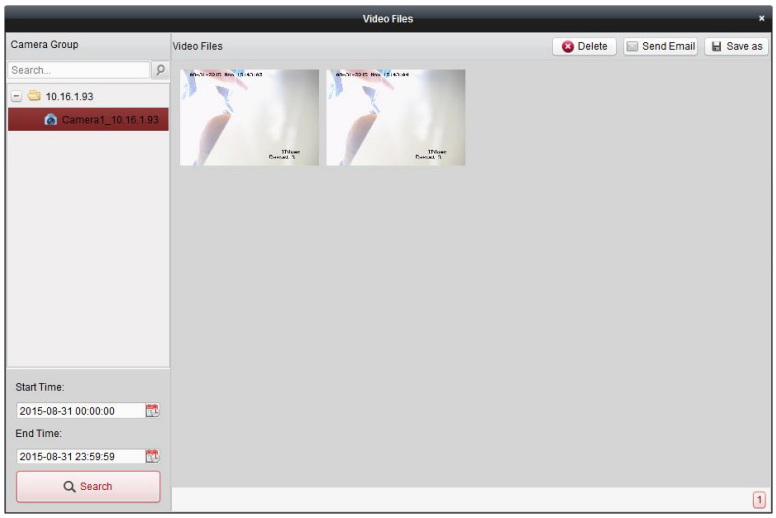
- During the manual recording, an indicator  appears in the upper-right corner of the display window.
- The saving path of video files can be set on the System Configuration interface. For details, refer to *Chapter 22.4 File Saving Path Settings.*
- For Hik-Connect device, the manual recording is not 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, refer to *Chapter 22.8 Email Settings*.



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, refer to *Chapter 22.4 File Saving Path Settings.*

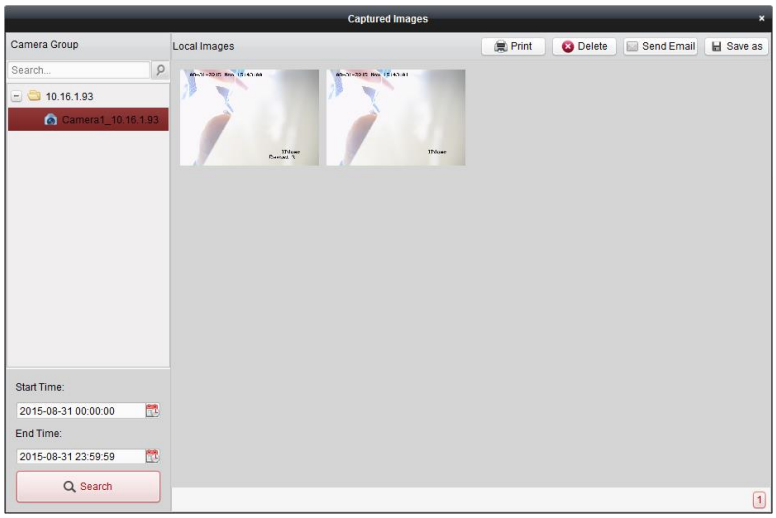
Viewing Captured Pictures

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.



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.

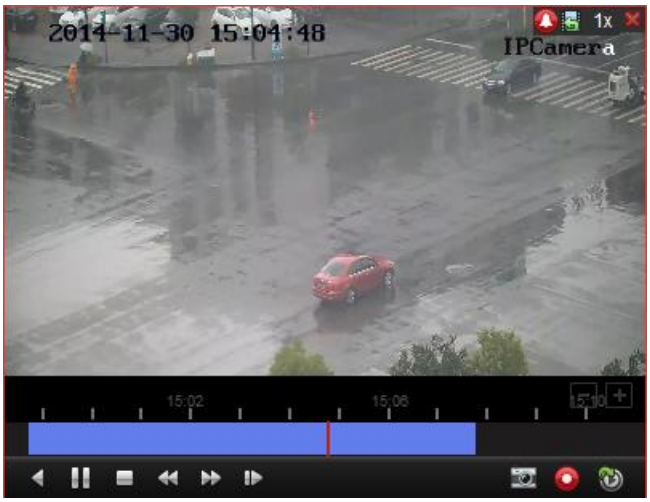
Before you start:

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.

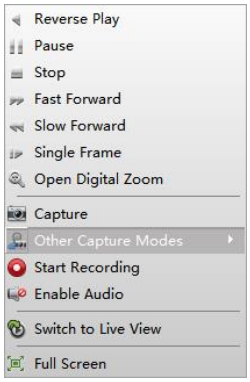
Note: During the instant playback, an indicator appears in the upper-right corner of the display window.



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.

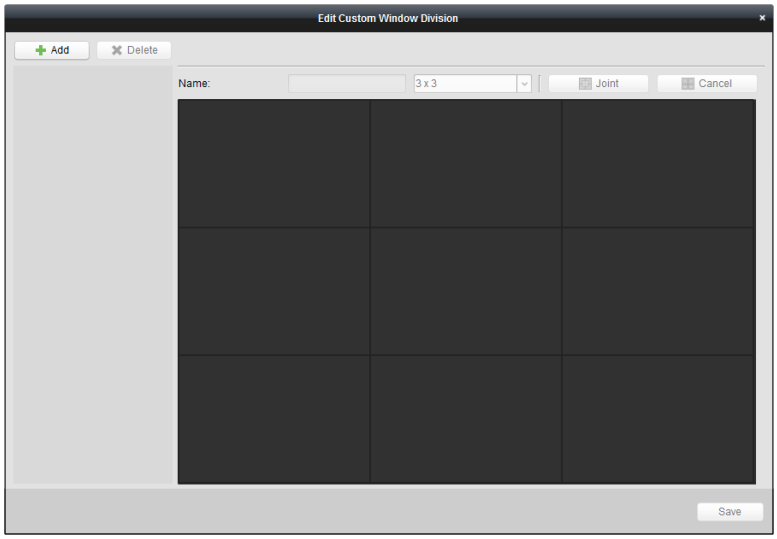
4.6 Custom Window Division

Purpose:

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

Steps:

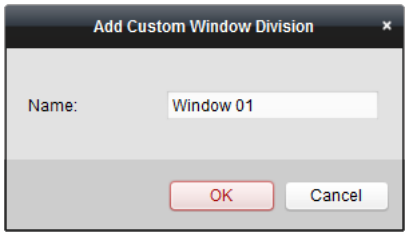
1. Click on the live view toolbar and select Edit to pop up the custom window division window box.



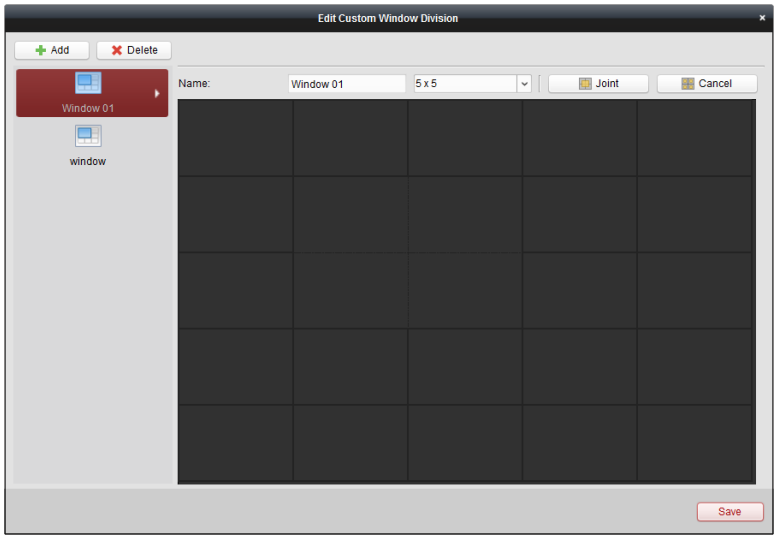
2. Click **Add** to open the custom window division adding window box.

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

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



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



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

   Notes:

   - You can also enter the Remote Playback page and perform the steps above to configure the custom window division.
   - For remote playback, up to 16 windows can be played back at the same time. The custom window division with more than 16 windows is invalid for playback.

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 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 expanding mode for live view as desired.

   Note: For some devices, you can select the mounting type of the device and the related expanding 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

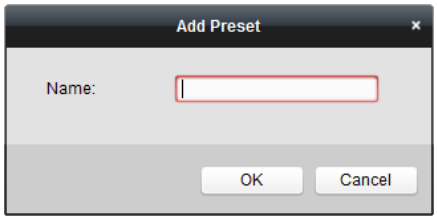
Note: The preset is only supported by specific fisheye camera.

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.



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.

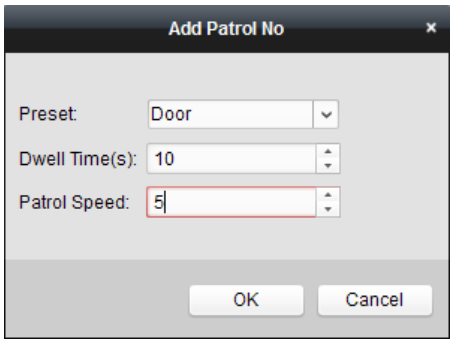
A patrol is a scanning track specified by a group of user-defined presets, with the scanning speed between two presets and the dwell time at the preset separately programmable. Please follow the steps below to configure the patrol.

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.



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 Tracking

Purpose:

The box or bullet camera which supports master-slave tracking function can locate or track the target according to your demand.

Notes:

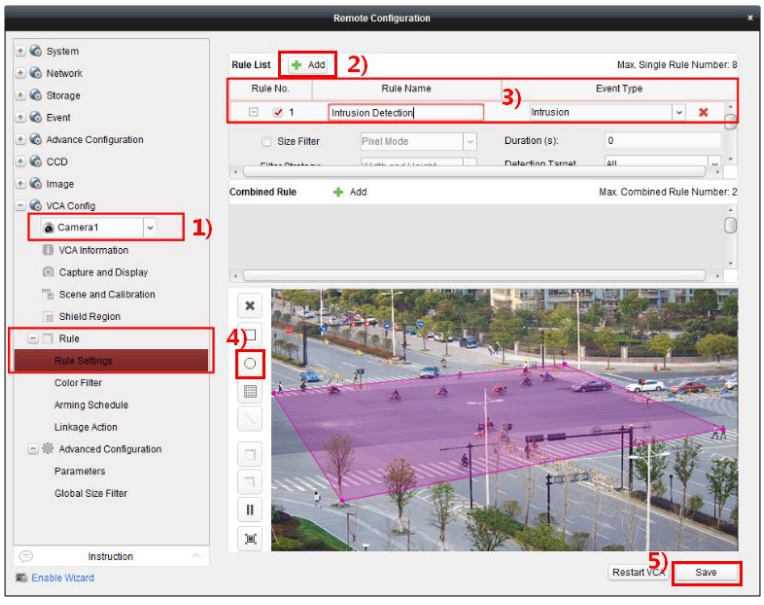
- This function in only supported by the specific box or bullet camera.
- A speed dome with the auto-tracking function is required to be installed near the camera.

4.8.1 Configure Master-Slave Tracking Rule

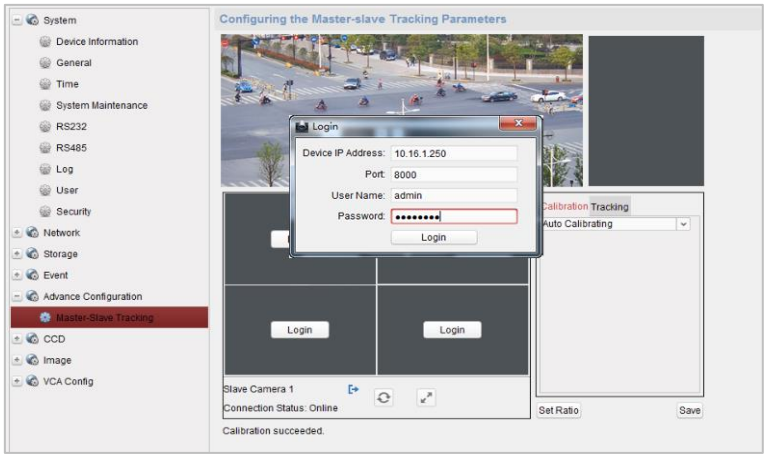
Before performing master-slave tracking during live view, you should configure the master-slave tracking rules for the box or bullet camera.

Steps:

1. In the device management interface, select the box or bullet camera and click **Remote Configuration** and enter **VCA Config** -> **Rule** -> **Rule Settings**.
2. Configure the intrusion rule.
   1) Select the camera in the channel list
   2) Click **Add** in Rule List panel to add a rule.
   3) Select **Intrusion** as Event Type.
   4) Click to draw the zone of intrusion rule.
   5) Click **Save** to save the settings.

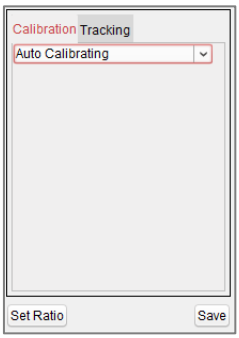


3. Login the speed dome.
   1) In the Remote Configuration interface, select **Advanced Configuration**->**Master-Slave Tracking** to show the login interface.



2) Click **Login** button to pop up the speed dome login window box.
3) Input the required information.
4) Click Login to login the speed dome.

4. Click **PTZ**, and use the direction arrows to adjust the speed dome to a horizontal position.
5. Set the camera calibration mode.

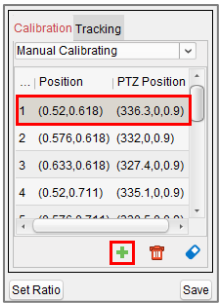


For Auto Calibrating:

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.



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.

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

4.8.2 Perform Master-Slave Tracking in Live View

Steps:

1. Start live view for box or bullet camera.
2. Right-click on the live view window and click **Enable Master-slave Tracking.**
3. 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 Thermal Camera Live View

Purpose:

For thermal camera, during live view, you can view the fire source information and temperature. You can measure the temperature manually to get temperature information in the live view image.

4.9.1 Viewing Fire Source Information During Live View

Purpose:

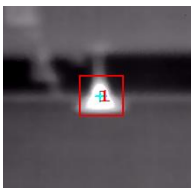
During live view, you can view the fire source information detected.

Before you start:

You need to configure the alarm rules on the thermal device. For details, refer to the *User Manual* of the device.

Steps:

1. Enter Main View module.
2. Start live view for the thermal camera. For details, refer to *Chapter 4.1 Starting and Stopping Live View.*
3. Right click on the live view image and select **Fire Source Information** in the right-click menu. You can select to display the fire source region, locate the maximum temperature region, or display the fire source target.
   - **Fire Source Region:** The region in which the temperature is higher than the configured alarm threshold.
   - **Maximum Temperature Region:** Mark the region in which the temperature is highest in the fire source region. It is marked in green.
   - **Fire Source Target:** Display the target location information.



4.9.2 Showing Temperature Information on Live View Image

Purpose:

You can show or hide the real-time temperature information of the monitoring scene when viewing the live video.

Before you start:

- Switch the device VCA source type as Temperature Measurement + Behavior Analysis.
- Enable the device temperature measurement function and set the temperature measurement rules. For details, refer to the *User Manual* of the device.

Steps:

1. Enter Main View module.
2. Start live view for the thermal camera.
   For details, refer to *Chapter 4.1 Starting and Stopping Live View.*
3. Adjust the scene to the area which has configured with temperature measurement rule.
4. Right click on the live view image and select **Show Temperature Information** in the right-click menu to show the temperature on the live view image.
5. Click on the image to view the temperature information

6. To hide the temperature on the live view image, right click on the live view image and select **Hide Temperature Information**.

4.9.3 Measuring Temperature Manually

Purpose:

You can get the temperature of point or region on the live view image of thermal camera by drawing points or frames on the live view image.

Notes:

- Up to 10 measurement rules (points and frames) can be drawn for one camera.
- When multiple clients are viewing the live video of one camera, if one client add or delete the measurement rules (points and frames), other clients' live view will be affected as well. The measurement rules will be cleared after all the users stopping live view of the camera.

Measuring Temperature on Points Manually

Purpose:

You can measure the temperature on different points in the live view image by drawing points.

Steps:

1. Enter Main View module.
2. Start live view for the thermal camera.
   For details, refer to *Chapter 4.1 Starting and Stopping Live View.*
3. Right click on the live view image and select **Manual Temperature Measurement > By Point.**
   Or click  on the live view toolbar and select **By Point**.
4. Click on the live view image to set the points to get the temperature.
   The temperature of the point will show as follows:

5. (Optional) To delete the drawn point, click **Cancel** and click the drawn cross on the live view image.
6. (Optional) To hide the measured temperature, right click the live view window and select **Disable Manual Temperature Display**.

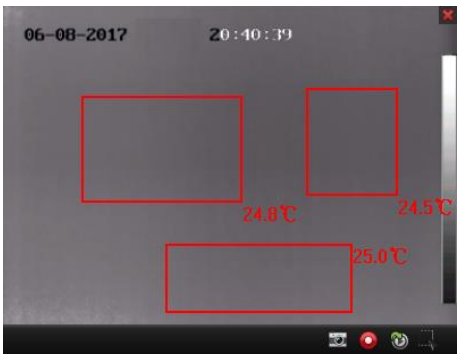
Measuring Temperature in Area Manually

Purpose:

You can measure the temperature in different area in the live view image by drawing frames.

Steps:

1. Enter Main View module.
2. Start live view for the thermal camera.
   For details, refer to *Chapter 4.1 Starting and Stopping Live View.*
3. Right click on the live view image and select **Manual Temperature Measurement > By Frame.**
   Or click  on the live view toolbar and select **By Frame**.
4. Drag on the live view image to draw the frames to get the temperature.
   The average temperature in the frame will show as follows:



5. (Optional) To delete the drawn frame, click **Cancel** and click the drawn frame on the live view image.
6. (Optional) To hide the measured temperature, right click the live view window and select **Disable Manual Temperature Display**.

4.9.4 Acknowledge Fire Source Detection Alarm

Purpose:

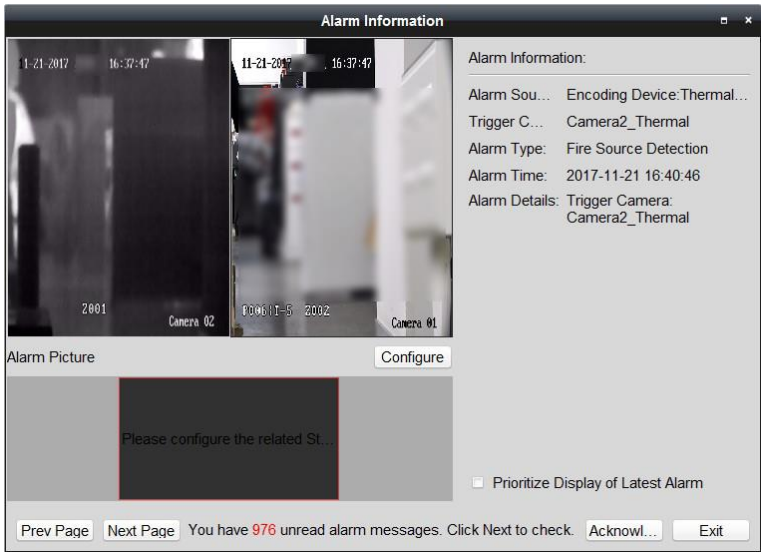
During scanning, when the thermal device detects fire source, the fire source detection alarm will be triggered and the device will stop moving. You can view the alarm details including alarm video and alarm picture. When the alarm is handled, you can acknowledge the alarm and the device will continue moving according to the configured path.

Before you start:

You should configure the fire source acknowledgement mode on the device. For details, refer to the *User Manual* of the device.

Steps:

1. Trigger a fire source detection alarm.
2. In Alarm Event module, open the fire source detection alarm details window.
   Or the window will pop up when the alarm is triggered if you configured alarm pop-up image.
   For setting the alarm pop-up image linkage, refer to *Chapter 6 Alarm Management*.



3. Click **Acknowledge** to acknowledge the alarm.

Notes:

- If you set the fire source acknowledgement mode as *Manual*, after you click **Acknowledge**, the device will continue scanning according to the configured path.
- If you set the fire source acknowledgement mode as *Auto*, when it exceeds the configured acknowledgment duration, the device will continue scanning automatically.
- For setting the acknowledgment duration, refer to the *User Manual* of the device.

4.10 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.

Note: Hik-Connect device doesn’t support selecting channel during two-way audio.

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.

5.1.1 Storing on 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.

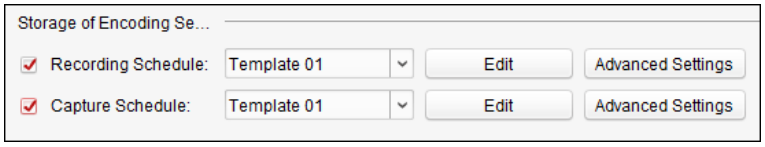
Note: The pictures captured through the capture schedule are stored on the local device and can be searched on the remote configuration page of the device.

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.



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, refer to *Configuring Recording Schedule Template*.

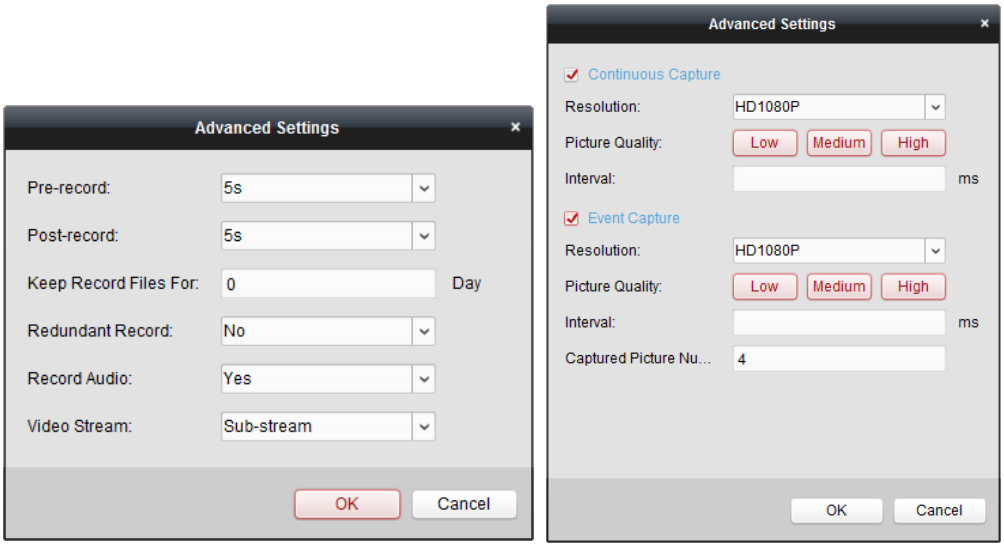
5. Click **Advanced Settings** to set the recording parameters.

   Note: The displayed items vary with the devices.

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.

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.

6. Optionally, click **Copy to…** to copy the recording schedule settings to other channels.
7. Click **Save** to save the settings.



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.

   Continuous refers to normal recording. The schedule time bar is marked with .

   Event Recording refers to the recording for the event. The schedule time bar is marked with .

   Command refers to the recording 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,

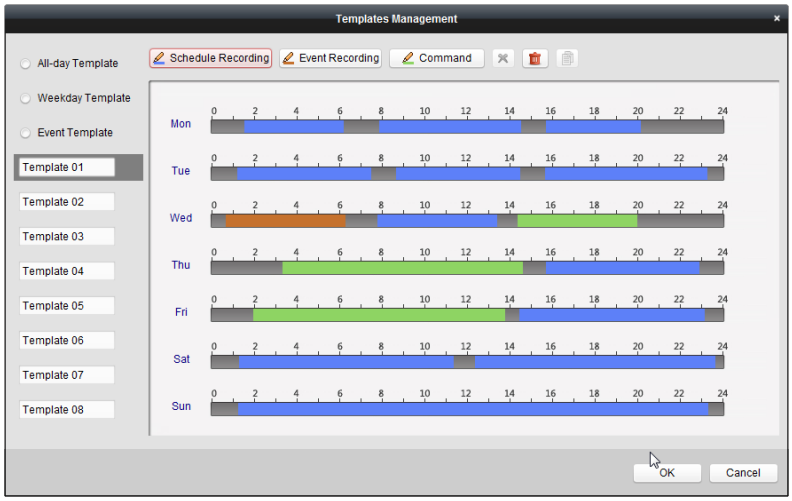
   and then click the icon to delete the selected time bar,

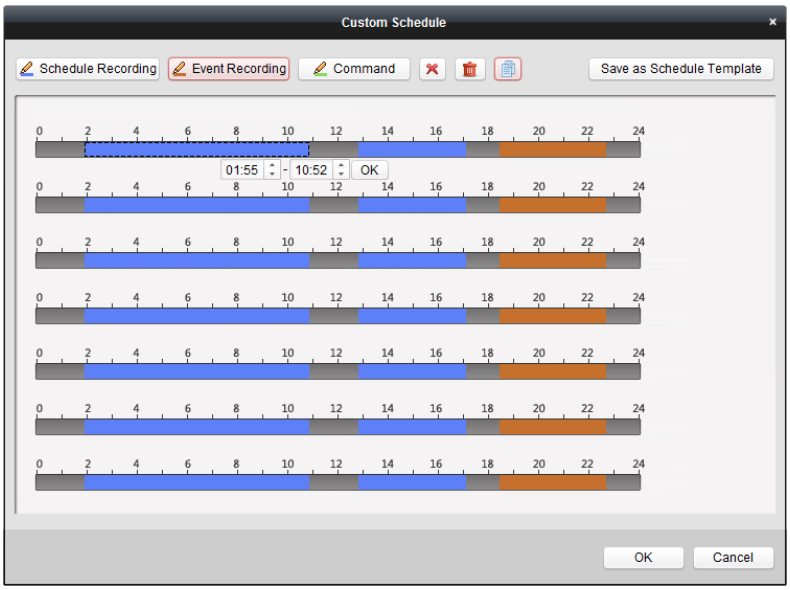
   or click the icon to delete all the time bars,

   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.





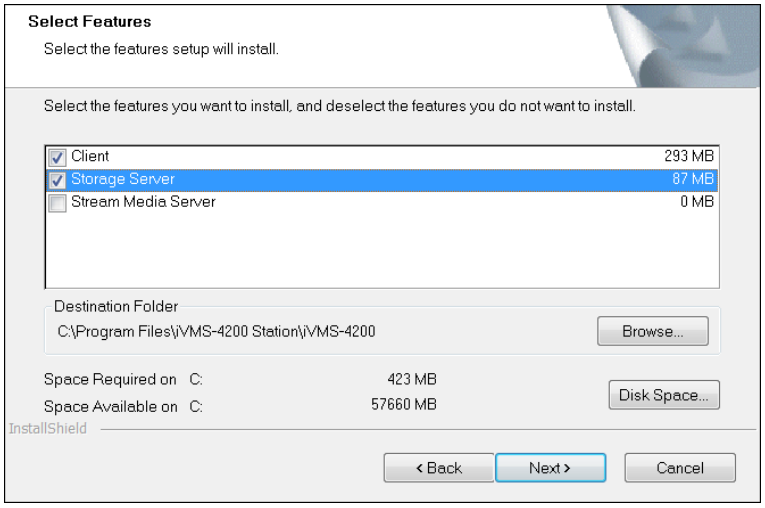
5.1.2 Storing on Storage Device

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. After running the installation package, check **Storage Server** to enable the installation of Storage Server.



Resetting Password for Storage Server

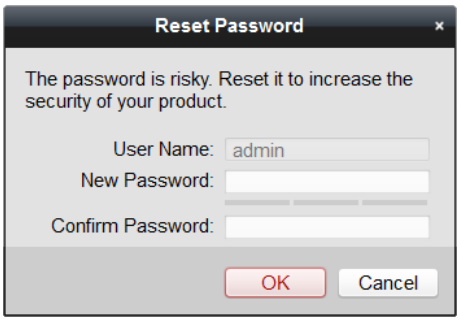
If it is the first running the iVMS-4200 Storage Server, you are required to set a password for the Storage Server.

Steps:

1. Click the shortcut icon  on the desktop of the PC installed with Storage Server to run it.

   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 window box will pop up. You should change the port No. to other value to ensure the proper running of the Storage Server.
2. The following window pops up.



3. Input the new password and confirm password.

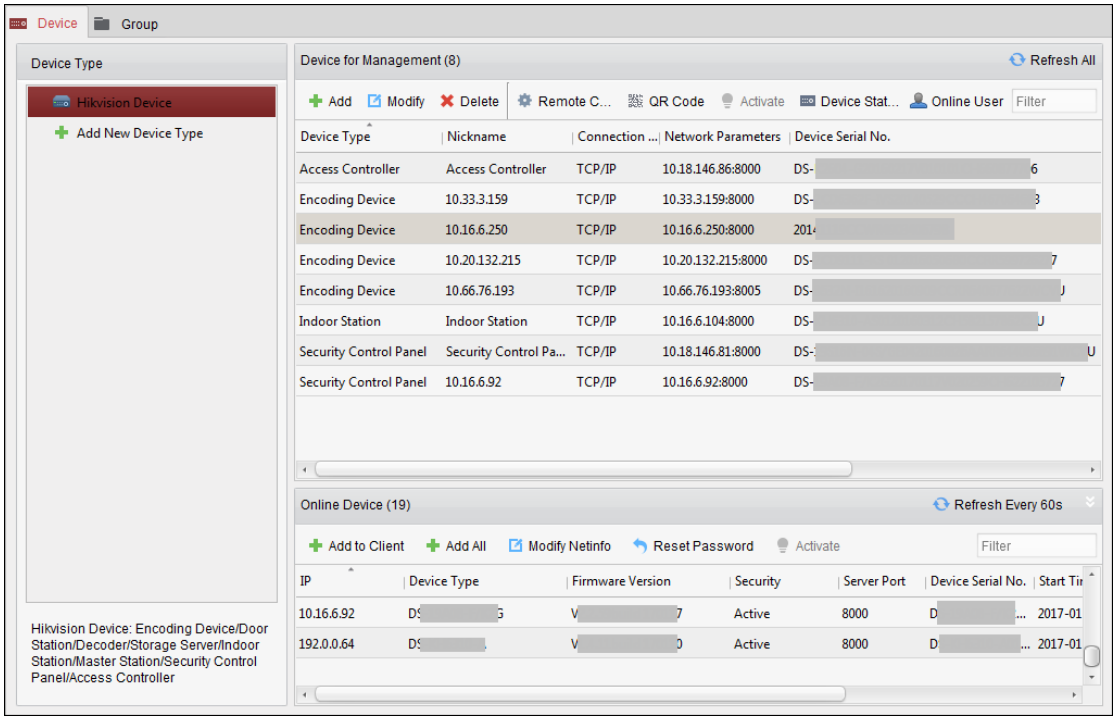
   - *A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.*
   - *For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case 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.*
4. Click **OK** to change the password.

   After changing the password, the Storage Server will run automatically.

Adding Storage Server

Steps:

1. Open the Device Management page of iVMS-4200 Client and click **Device** tab.



2. Click **Hikvision Device** to display the Hikvision Device list.
   For adding Storage Server, refer to *Chapter 3.1 Adding Device.*

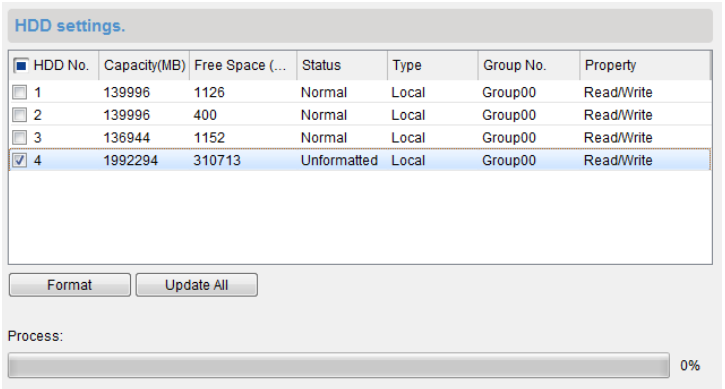
Formatting HDDs

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.



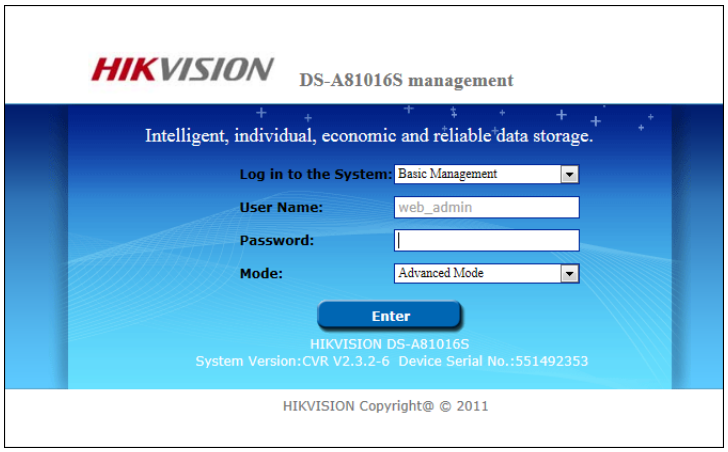
Configuring CVR on Web Client

Purpose:

Client provides entry to the CVR configuration web client for convenient usage. You can configure the CVR parameters on the web client.

Note: This function should be supported by the device.

Select the added CVR from the list and click **Configuration on Device** to go to the CVR configuration web client.



Note: For details about configuring CVR parameters on the web client, refer to the User Manual of the device.

Configuring Storage Schedule

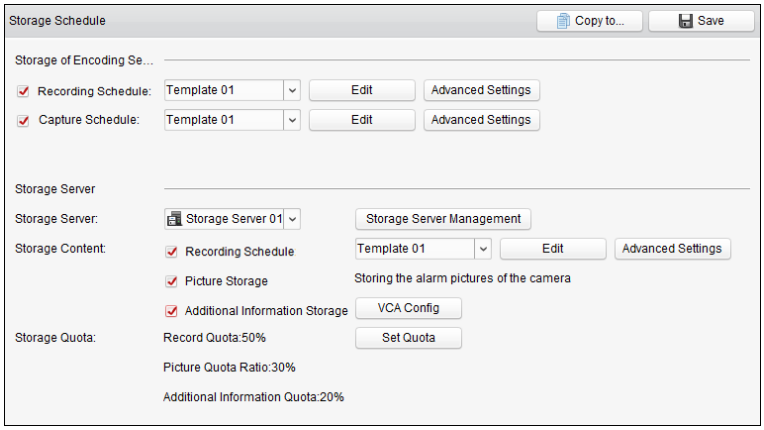
Before you start:

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 21.1 Heat Map, Chapter 21.2 People Counting* and *Chapter 21.4 Road Traffic* for checking the data.
   Note: For detailed configuration about setting the VCA rule, 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, refer to *Configuring Recording Schedule Template.*
6. Click **Advanced Settings** to set the pre-record time, post-record time, video stream, and other parameters for recording.
   Note: The iVMS-4200 Storage Server only supports main-stream.
7. Click **Set Quota** to enter the HDD management interface of the Storage Server. You can set the corresponding quota ratio for record, picture and additional information.
   Example: If you set the record quota as 60%, then the 60% of the storage space can be used for storing the video files.
8. Click **Save** to save the settings.



Note: The Storage Server supports storage of line crossing detection alarm, intrusion detection alarm, region entrance detection alarm, region exiting detection alarm, fast moving detection alarm, people gathering detection alarm, loitering detection alarm, parking detection alarm, object removal detection alarm, and unattended baggage detection alarm recording. For details, refer to *Chapter 6 Alarm 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.

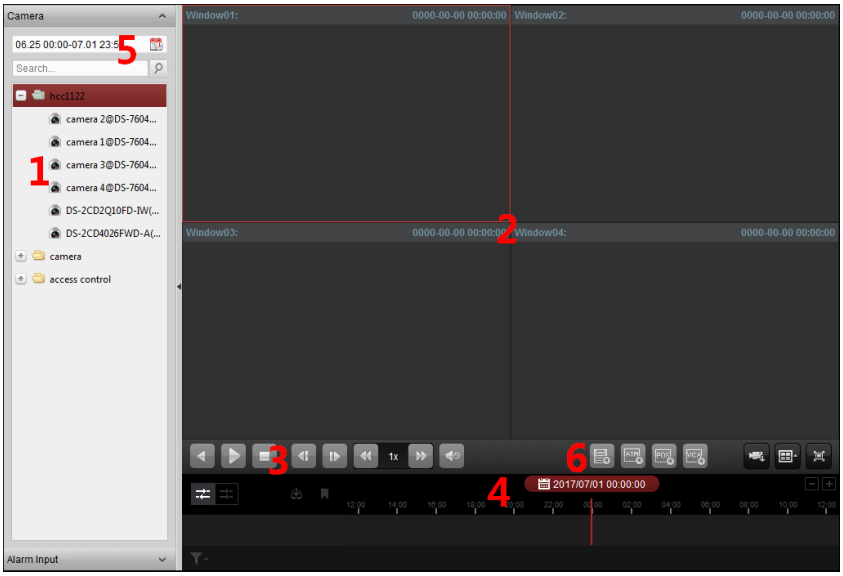
Before you start:

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 *Chapter 22.2 Live View and Playback Settings*.

Optionally, you can set the cameras rotate direction for playback in Group Management. Refer to *Chapter 3.2.3 Modifying .*

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.

Note: For Hik-Connect device, it only supports 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 DVR, NVR, or Network Camera* for details.

Note: This function should be support by the device.

Steps:

1. Enter Group Management interface and open the Modify Camera window (refer to *Chapter 3.2.3 Modifying)*.
2. Set the video stream of the camera to main stream or sub-stream.

Searching Video Files for Normal Playback

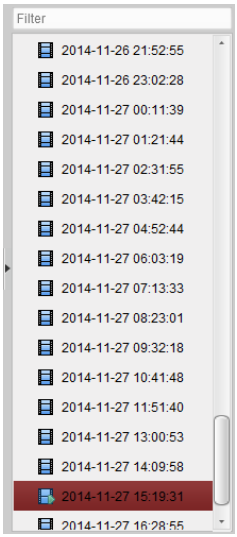
Steps:

1. Open the Remote Playback page.
2. Click the calendars icon to activate the calendars window.

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

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

3. Click-and-drag the camera or group to the display window,
   or double-click the camera or group to start the playback.
4. The found video files of the selected group or camera will be displayed on the right of the interface in chronological order. You can filter the results through the **Filter** text field.
   The first video file will be played back automatically by default.



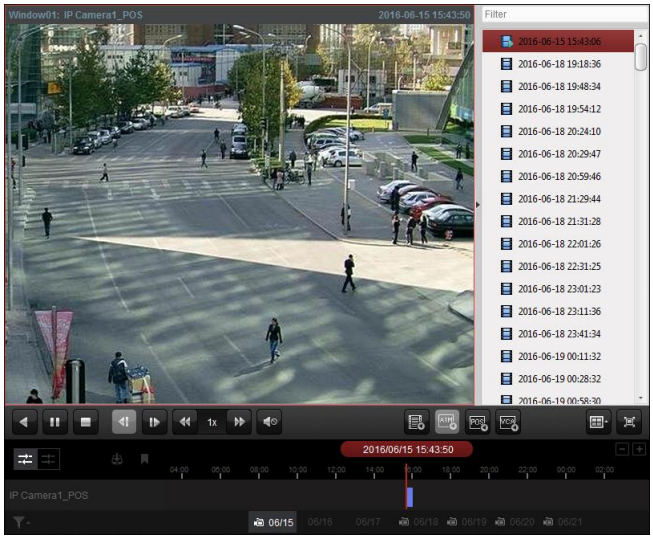
Notes:

- Up to 16 cameras can be searched simultaneously.
- In the calendar, the date which has scheduled records will be marked with and the date with event records will be marked with .

Playing Back Video Files

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

- **Playback by File List**
  Select the video file from the search result list, and then click the icon on the video file, or double-click the video file to play the video on the display window of playback.
- **Playback by Timeline**
  The timeline indicates the time duration for the video file, and the video files of different types are color coded. Click on the timeline to play back the video of the specific time.
  You can click or to scale up or scale down the timeline bar.
  You can drag the timeline bar to go to the previous or the next time period.
  You can use the mouse wheel to zoom in or zoom out on the timeline.



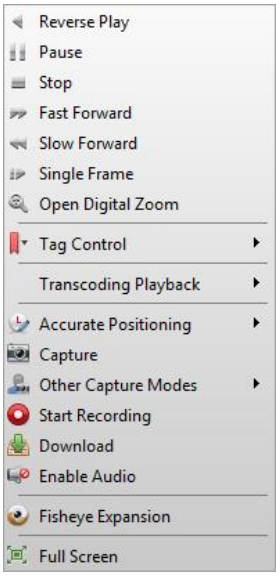
Normal Playback Toolbar:

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

	Reverse Playback	Play back the video file reversely. ***Note:*** The Hik-Connect device doesn't support this function.
	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. ***Note:*** The Hik-Connect device doesn't support this function.
	Volume	Click to turn on/off the audio and adjust the audio volume.
	Event Playback	Search the recordings triggered by event, such as motion detection, video loss or video tampering.
	ATM Playback	Search the recordings of ATM devices.
	POS Playback	Search the recordings which contain POS information.
	VCA Playback	Set the VCA rule to the searched video files that VCA event occurs, including motion detection, Intrusion and Line Crossing.
	Download for Multiple Cameras	Download video files of multiple cameras at the same time.
	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. ***Note:*** The Hik-Connect device doesn't support this function.
	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.
	Show/Hide Temperature Information	For thermal camera, click to show or hide the temperature on the live view image.
	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, 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.

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 window.
   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.

- **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, behavior analysis, or access control event (for video access control terminal), can be searched for Event Playback and this function requires the support of the connected device.

Searching Video Files for Event Playback

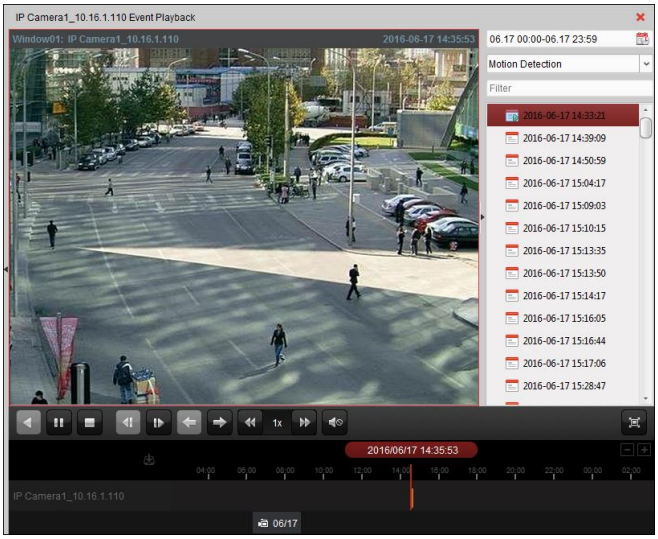
Steps:

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 window box.

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

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

   Note: In the calendar, the date which has scheduled records will be marked with  and the date with event records will be marked with  .
5. Select the event type from the drop-down list and the found video files will be displayed. You can filter the results by inputting the keyword in the **Filter** text field. Or you can click  to go back to the normal playback.
6. Select the video file from the search result list, and then click the icon  on the video file, or double-click the video file to play the video on the corresponding display window of playback.



Playing Back Video Files

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

- **Playback by File List**

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

- **Playback by Timeline**

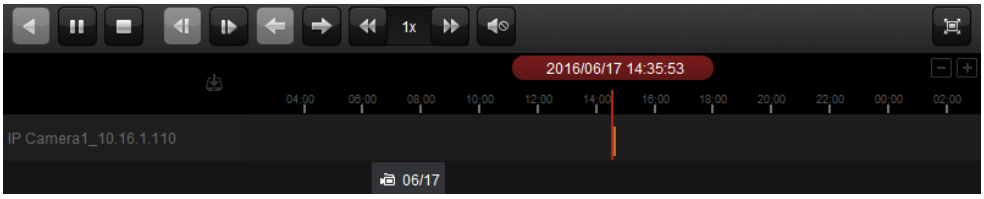
  The timeline indicates the time duration for the video file. Click on the timeline to play back the video of the specific time.

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

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

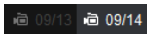
  You can use the mouse wheel to zoom in or zoom out on the timeline.

Event Playback Toolbar:



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

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

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

Please refer to *Chapter 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 *Chapter 22.2 Live View and Playback Settings*.

5.2.4 ATM Playback

Purpose:

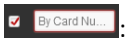
Search the video files for ATM DVR.

Note: This function should be supported by the device and the device should be configured with transaction rules. For details, 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  to enter the ATM playback interface.
4. Enter the search conditions.

    : Input the card number that is contained in the ATM information.

    : 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 window.

   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, 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  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 window 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

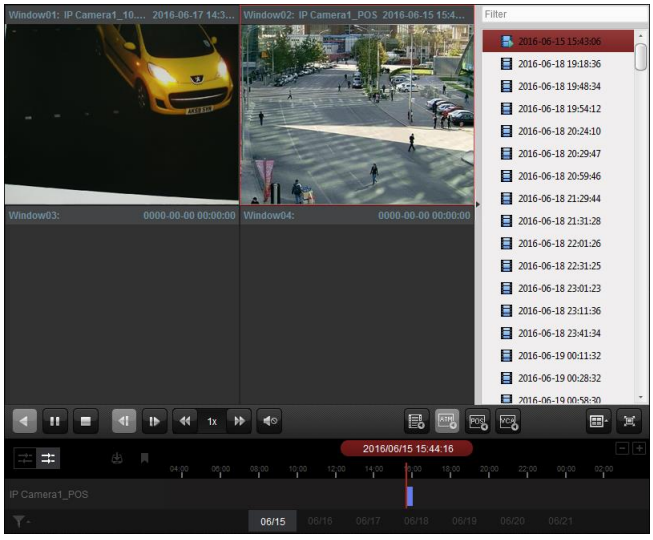
Purpose:

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 (*Chapter 5.2.1 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.



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 Motion, Intrusion and Line Crossing. This function helps to search out the video that you may be more concerned and mark it with red color.

- **Motion Detection**: 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:

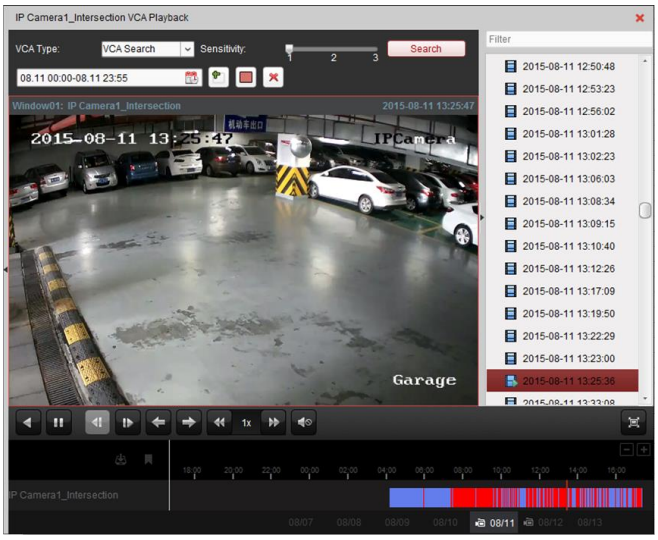
   - For Motion, click  , and then click and move on the playback window to set the grid rectangle as the detection region. Or you can click  to set all the area shot by the camera as the detection region.
   - For Intrusion, click  and then click on the playback window to set the vertex for the detection 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 window 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 *Chapter 22.2 Live View and Playback Settings.*



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:

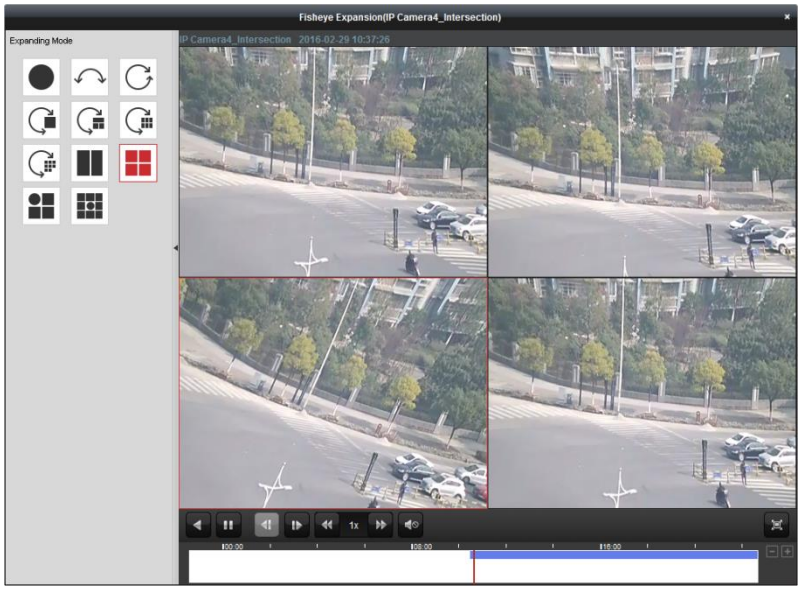
The video files can be played back in fisheye expansion mode.

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, refer to *Chapter 4.7 Live View in Fisheye Mode*.
4. You can select the expanding 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.



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.

5.2.9 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.

You can also download the video files of multiple cameras at the same time.

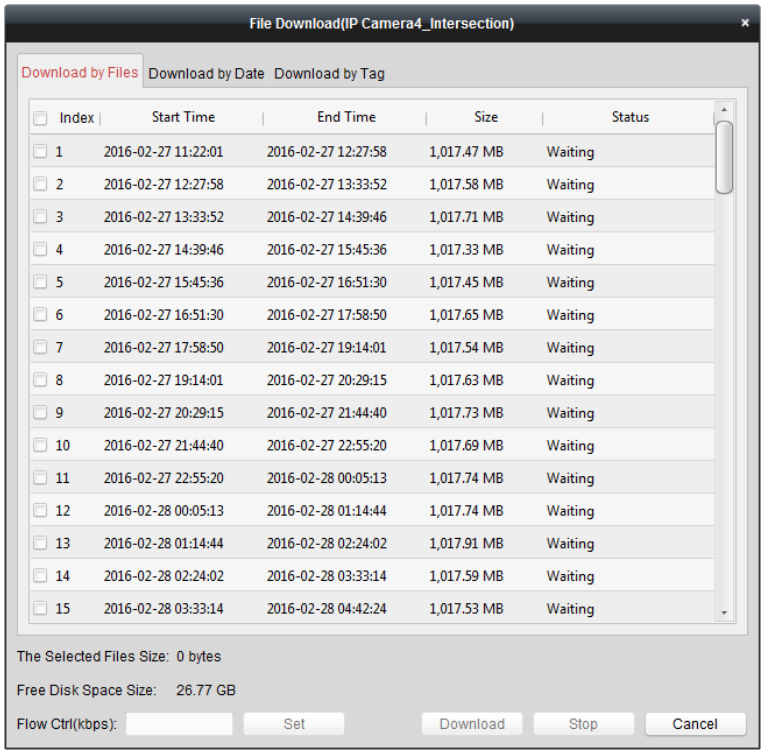
Note: You cannot download the video files of Hik-Connect device.

Download by Files

Steps:

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

4. Optionally, you can click **Stop** to stop downloading manually.

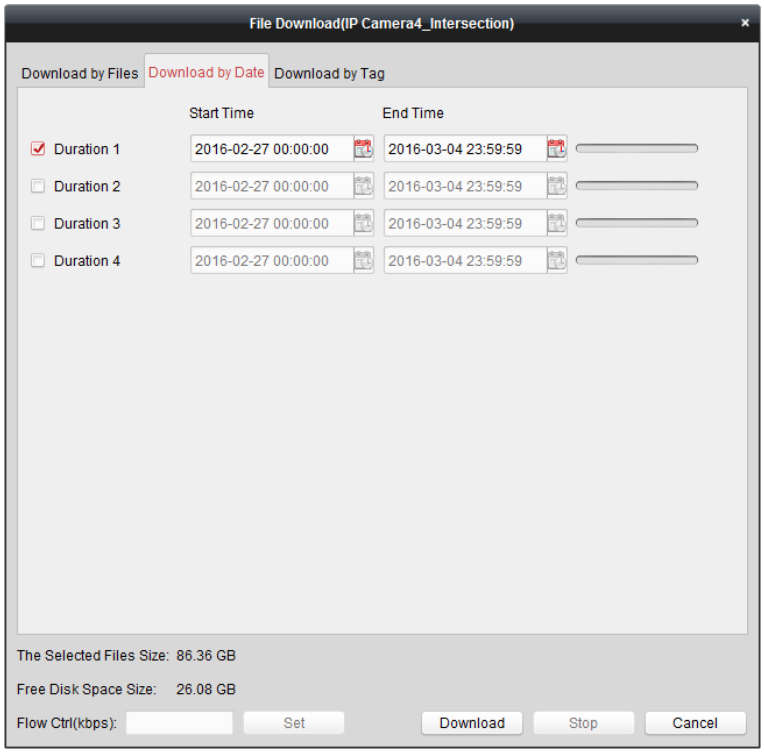


Download by Date

Steps:

1. Click **Download by Date** tab in the File Download interface.
2. Check the checkbox of the time duration to enable it, and click to set the start and end time.
3. Click **Download** to start downloading the file to the local PC. The progress bar shows the downloading process.

   You can input the flow (0 to 32768 kbps) and click **Set** to control the downloading speed.
4. Optionally, you can click **Stop** to stop downloading manually.

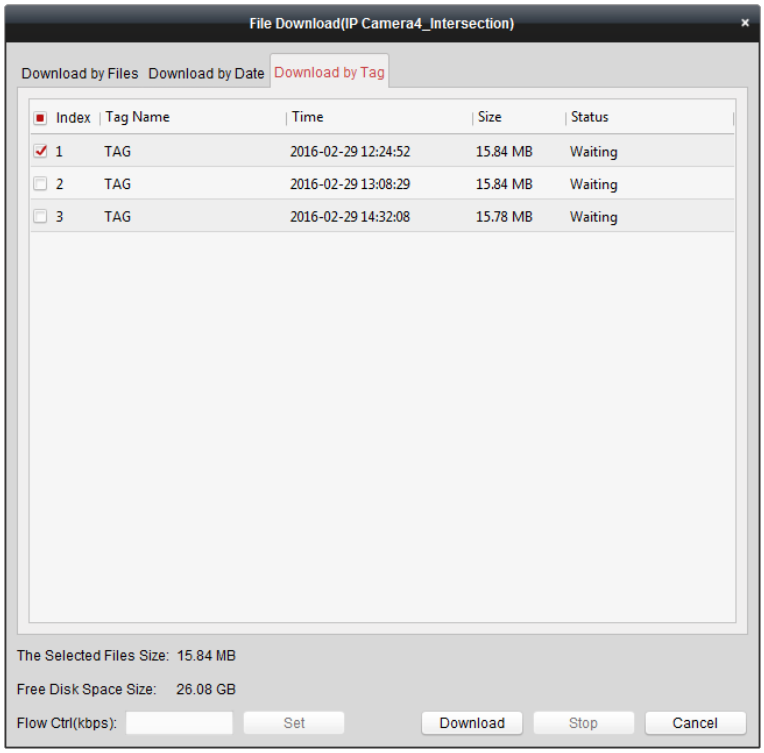


Note: When downloading video file of one time duration, you can set to merge the video files. The video files in the set time duration can be merged for downloading. For configuring merging downloaded video files, refer to *Chapter 22.2 Live View and Playback Settings*.

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.



Download for Multiple Cameras

Purpose:

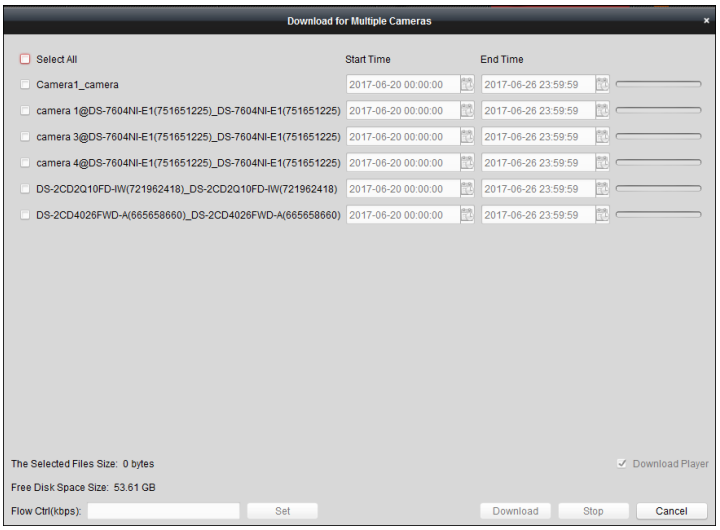
You can download the video files of the multiple cameras simultaneously.

Before You Start:

Play the video files of multiple cameras.

Steps:

1. Start playback for multiple cameras.
2. Click  to open the Download for Multiple Cameras window.



3. Check the checkbox(es) to select cameras.
4. Set the start time and end time.
5. (Optional) Check the **Download Player** checkbox to download the player.

6. 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.

7. Optionally, you can click **Stop** to stop downloading manually.

Note: The client support downloading video files of up to 16 cameras.

Chapter 6 Alarm 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.

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, refer to *Chapter 12.1 Configuring Zone Event.*)
- Access Control Event (For details, refer to *Chapter 14.7.1 Configuring Client Linkage for Access Control Alarm.*)
- Access Control Alarm Input (For details, refer to *Chapter 14.7.2 Configure Device Linkage for Access Control Alarm Input.*)
- Event Card Linkage (For details, refer to *Chapter 14.7.3 Event or Card* Linkage.)
- Cross-Device Linkage (For details, refer to *Chapter 14.7.4 Cross-Device Linkage.*)
- Pyronix Control Panel Event (For details, refer to Chapter *13.2 Configuring Event.*

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, 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, refer to the *User Manual* of the devices.

Steps:

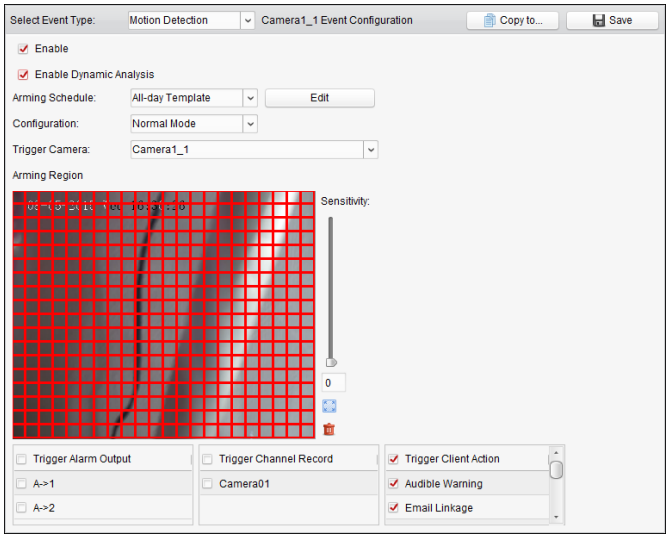
1. Open the Event Management page and click **Camera Event** tab.
2. Select the camera to be configured and select **Motion Detection** as the event type.
3. Check the checkbox **Enable** to enable the function of motion detection. Check the checkbox **Enable Dynamic Analysis** to mark the detected objects 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, refer to *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, 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.

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, refer to *Chapter 22.7 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. ***Note:*** You should set the triggered camera first.
Alarm Triggered Video Wall Display	Display the video of the trigged camera on the Video Wall when alarm is triggered. ***Note:*** You should set the triggered camera first.

10. Optionally, click **Copy to…** to copy the event parameters to other channels.
11. Click **Save** to save the settings.



Configuring Arming Schedule Template

Perform the following steps to configure the arming schedule template:

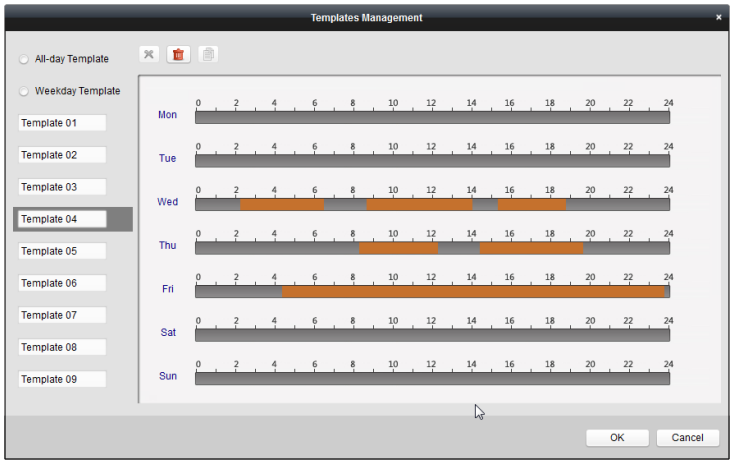
If **Template 01 to 09** is selected in the drop-down list, start from step 1;

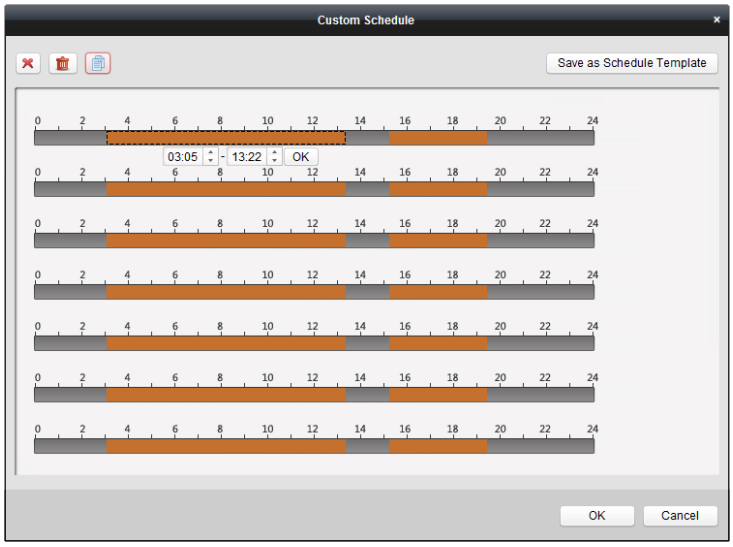
If **Custom** is selected in the drop-down list, start from step 2.

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.

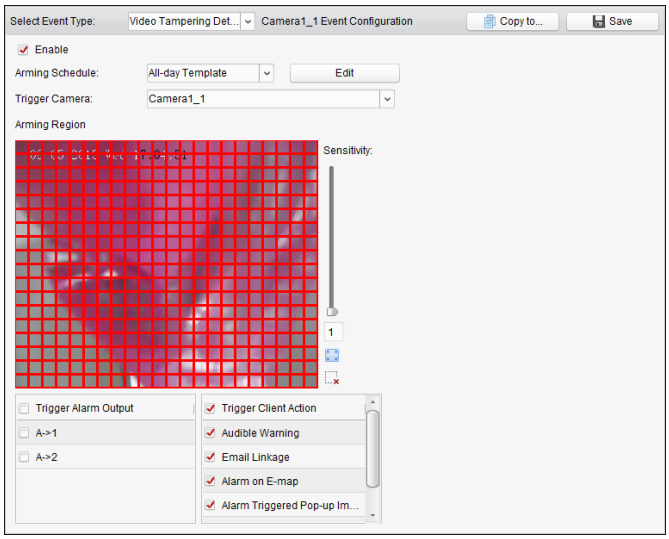
Steps:

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, refer to *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.

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, refer to *Chapter 22.7 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. ***Note:*** You should set the triggered camera first.
Alarm Triggered Video Wall Display	Display the video of the trigged camera on the Video Wall when alarm is triggered. ***Note:*** You should set the triggered camera first.

9. Optionally, click **Copy to…** to copy the event parameters to other cameras.
10. Click **Save** to save the settings.



6.3 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.

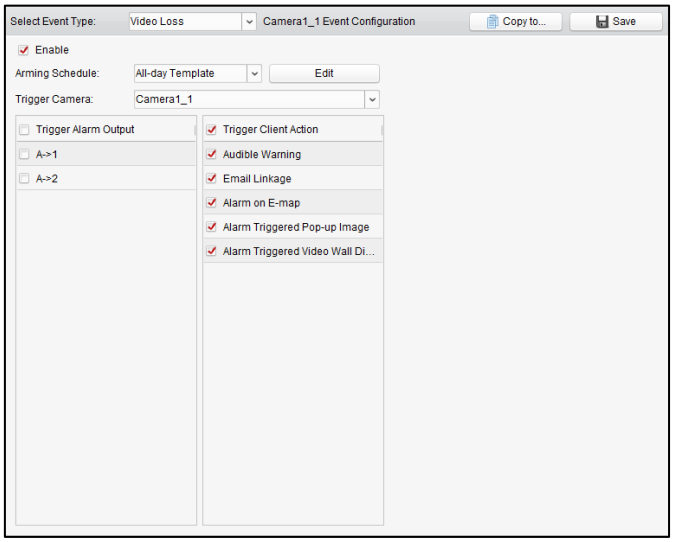
Steps:

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, refer to *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.

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, refer

	to *Chapter 22.7 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. ***Note:*** You should set the triggered camera first.
Alarm Triggered Video Wall Display	Display the video of the trigged camera on the Video Wall when alarm is triggered. ***Note:*** You should set the triggered camera first.

7. Optionally, click **Copy to…** to copy the event parameters to other cameras.
8. Click **Save** to save the new settings.



6.4 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.

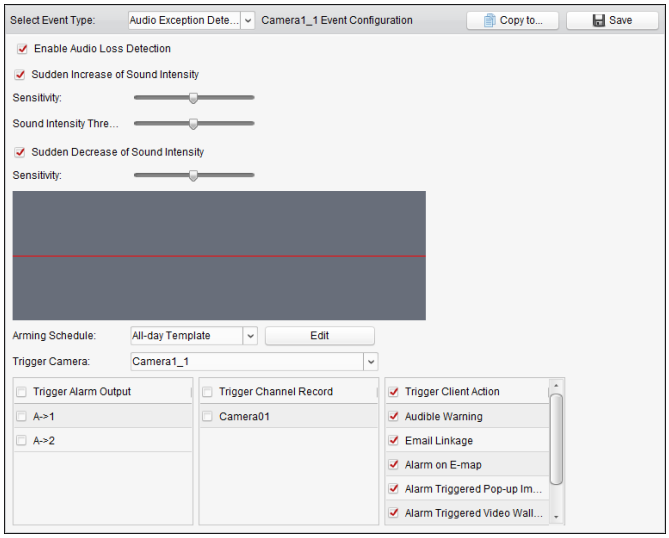
Note: The Audio Exception function requires the support of connected device.

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, refer to *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.

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, refer to *Chapter 22.7 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. ***Note:*** You should set the triggered camera first.
Alarm Triggered Video Wall Display	Display the video of the trigged camera on the Video Wall when alarm is triggered. ***Note:*** You should set the triggered camera first.

8. Optionally, click **Copy to…** to copy the event parameters to other cameras.
9. Click **Save** to save the new settings.



6.5 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, refer to *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.

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, refer to *Chapter 22.7 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. ***Note:*** You should set the triggered camera first.
Alarm Triggered Video Wall Display	Display the video of the trigged camera on the Video Wall when alarm is triggered. ***Note:*** You should set the triggered camera first.

9. Optionally, click **Copy to…** to copy the event parameters to other cameras.
10. Click **Save** to save the new settings.

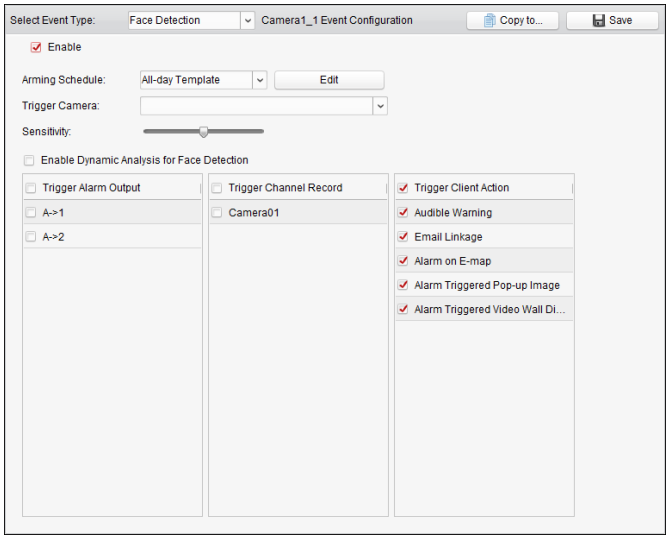


Table 6. 1 Linkage Actions for Face Detection Alarm

6.6 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, refer to *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.

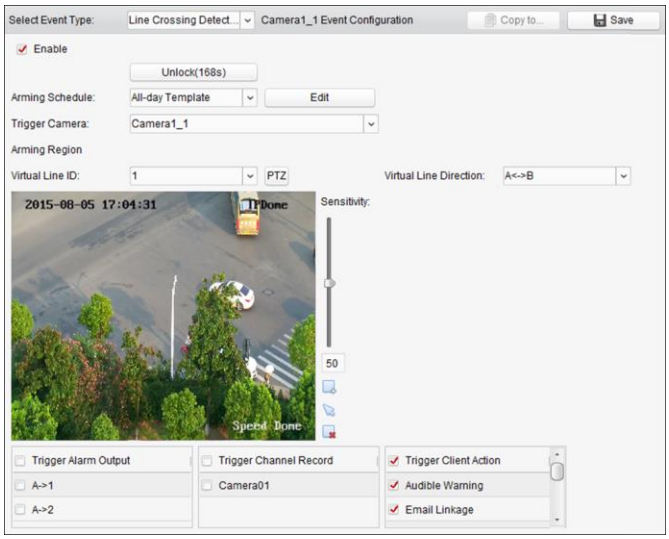
   Virtual Line Direction: You can select the directions as A<->B, A ->B, and B->A.

- **A<->B**: When an object going across the line with both directions, it 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.

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, refer to *Chapter 22.7 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. ***Note:*** You should set the triggered camera first.
Alarm Triggered Video Wall Display	Display the video of the trigged camera on the Video Wall when alarm is triggered. ***Note:*** You should set the triggered camera first.

10. Optionally, click **Copy to…** to copy the event parameters to other cameras.
11. Click **Save** to save the settings.



6.7 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:

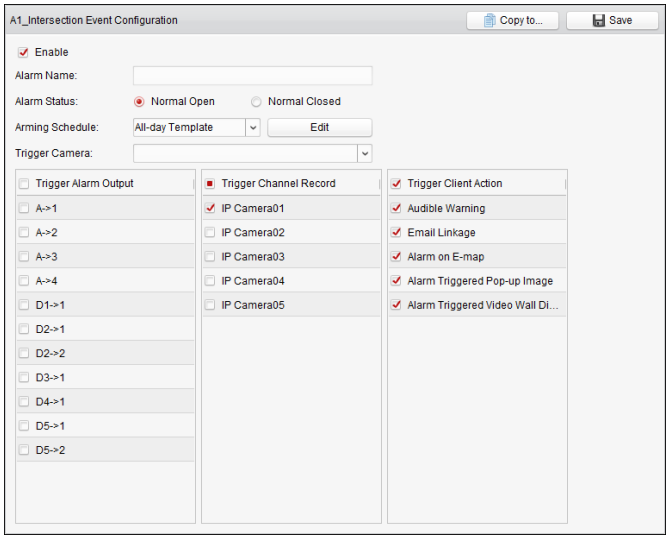
Add the alarm inputs to the client, click **Import** on the Group Management interface, click the **Alarm Input** tab and import alarm inputs into groups for management.

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, refer to *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.

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, refer to *Chapter 22.7 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. ***Note:*** You should set the triggered camera first.
Alarm Triggered Video Wall Display	Display the video of the trigged camera on the Video Wall when alarm is triggered. ***Note:*** You should set the triggered camera first.

9. Optionally, click **Copy to…** to copy the event parameters to other alarm inputs.
10. Click **Save** to save the settings.



6.8 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.

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, refer to *Chapter 22.7 Alarm Sound Settings.*
Email Linkage	Send an email notification of the alarm information to one or more receivers.

6. Optionally, click **Copy to…** to copy the event parameters to other devices.
7. Click **Save** to save the settings.

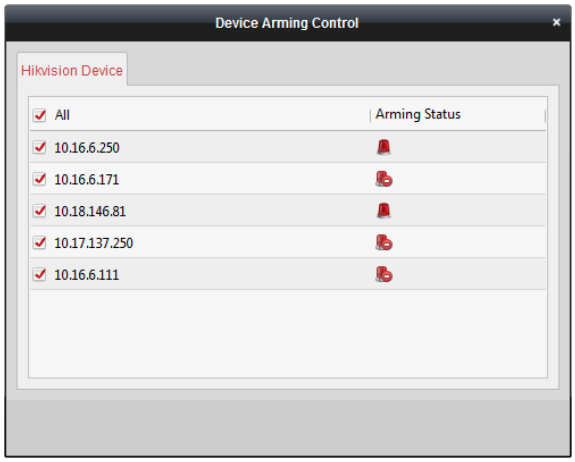
Chapter 7 Alarm and Event Center

Purpose:

The received recent alarms and events of all added devices can be displayed.

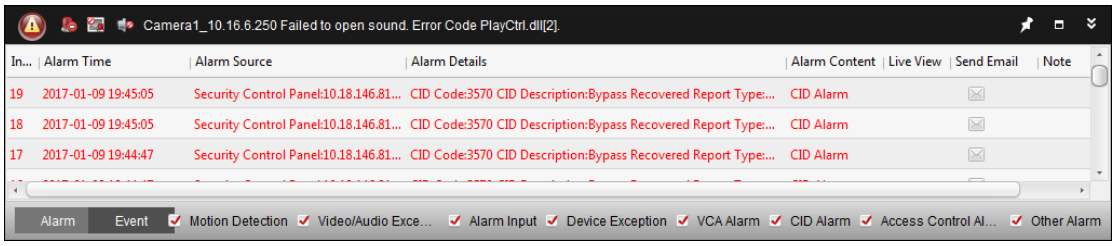
Before you start:

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. Then the alarm information will be auto uploaded to the client software when alarm occurs.



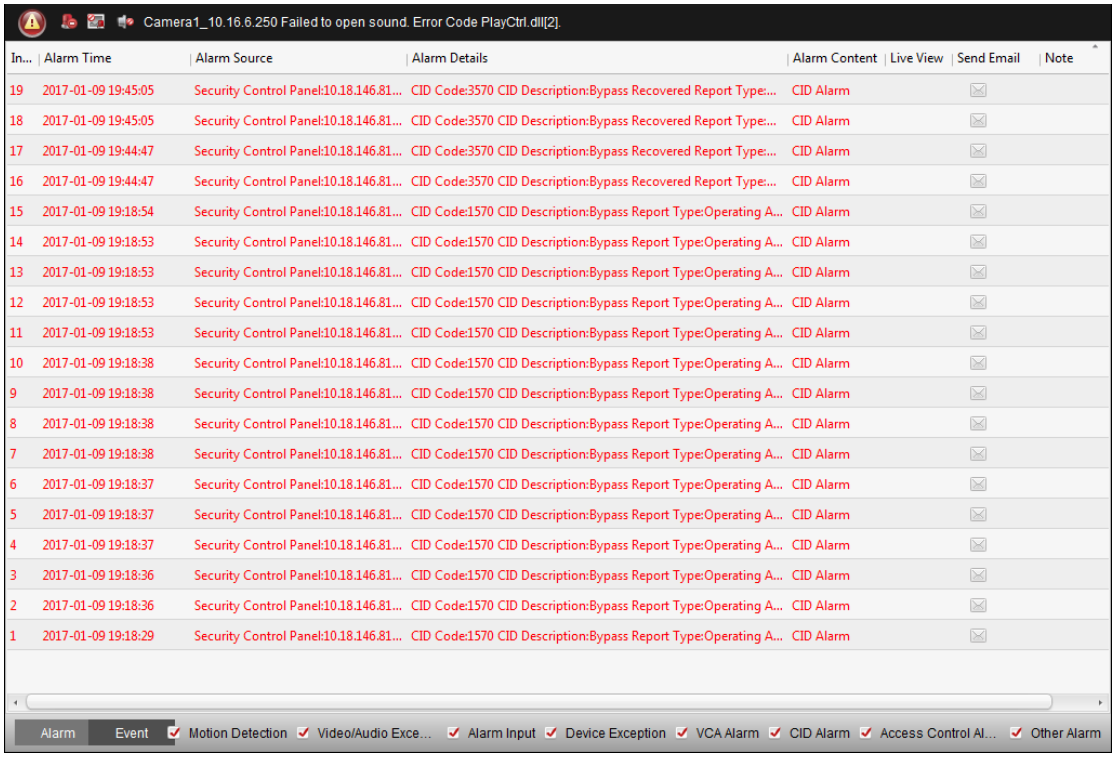
Steps:

1. Click the icon in Alarms and Events Toolbar to show the Alarms and Events panel.



2. You can click to display the Alarm Event interface.

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



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.

7.1 Viewing Alarms Information

Purpose:

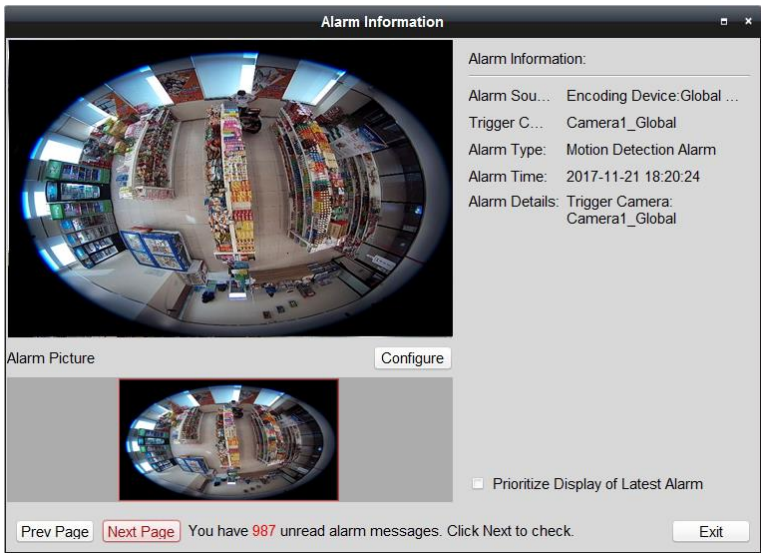
Different alarm types can be displayed on the panel: Motion Detection, Video/Audio Exception, Alarm Input, Device Exception, VCA Alarm, CID Alarm, Access Control Alarm, and Other Alarm. You can check the checkbox to enable the displaying of that type alarm.

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 or double click the alarm to get a live view of the alarm triggered camera.



Note: 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. In the alarm picture panel, view the alarm pictures captured when alarm is triggered.

   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, refer to *Chapter 5.1.2 Storing on Storage Device*.
   - For thermal camera and target capture camera, the live view of the two channels will display at the same time.

6. Click to send an email notification of the alarm to one or more receivers if the email settings are properly configured (*Chapter 22.8 Email Settings*).
7. 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, refer to *Chapter 11 Decoding and Displaying Video on Video Wall*.

   Click under the **Note** column to input the description for the alarm.
8. To clear the alarm information, click the icon , or right-click on an alarm log and then click **Clear**.

7.2 Viewing Events Information

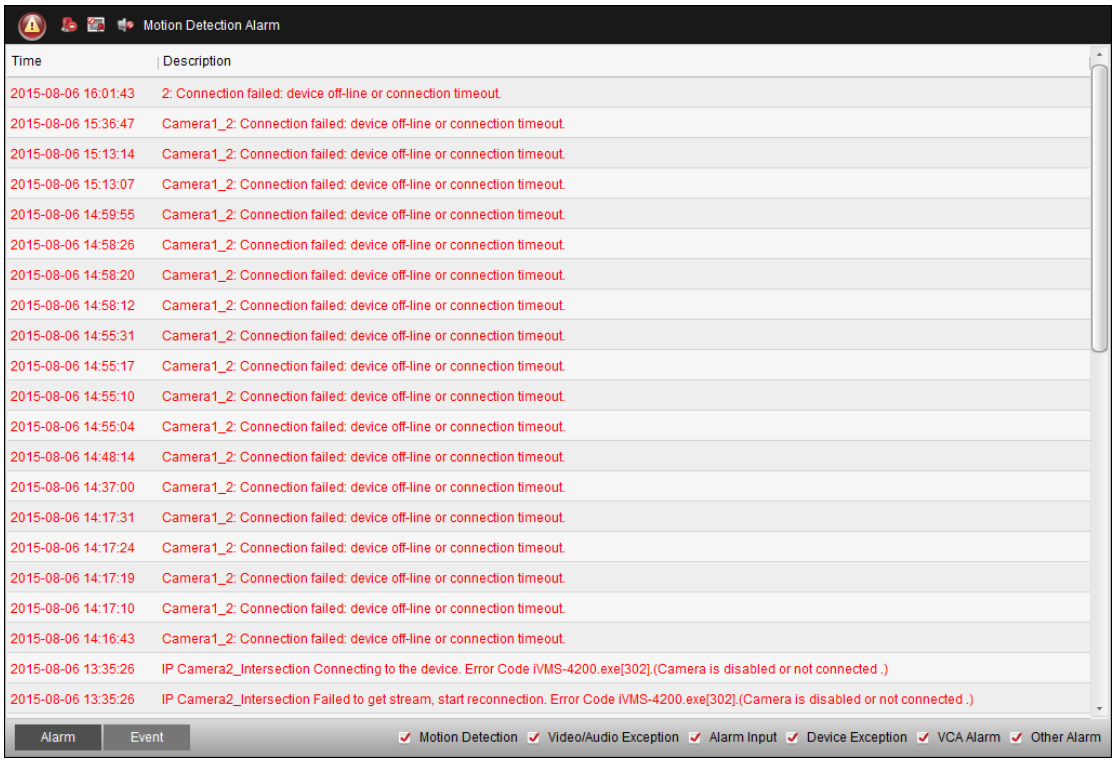
Purpose:

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

Steps:

1. Click the **Event** tab.

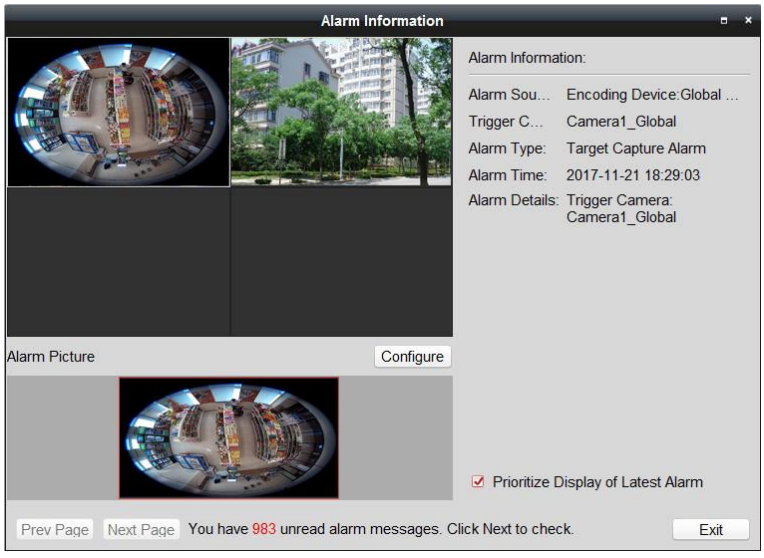
   The event information, including the time and detailed description will be displayed.
2. To clear the event information, click the icon , or right-click on the event log and then click **Clear**.



7.3 Viewing Pop-up Alarm Information

Purpose:

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.



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 previous or next alarm information.

You can view the live video of the triggered camera.

Note: For thermal camera and target capture camera, the live view of the two channels will display at the same time.

You can also view the alarm picture capture when the alarm is triggered.

Note: 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, refer to *Chapter 5.1.2 Storing on Storage Device*.

Chapter 8 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.

8.1 Adding an E-map

Purpose:

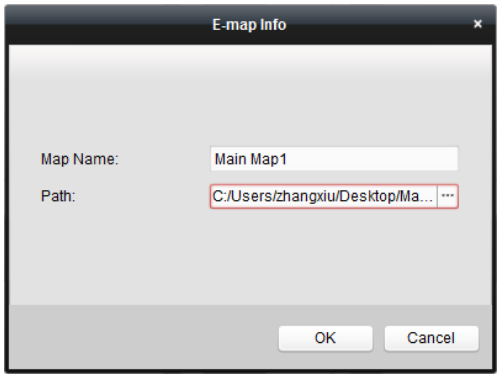
An E-map needs to be added as the parent map for the hot spots and hot regions.

Steps:

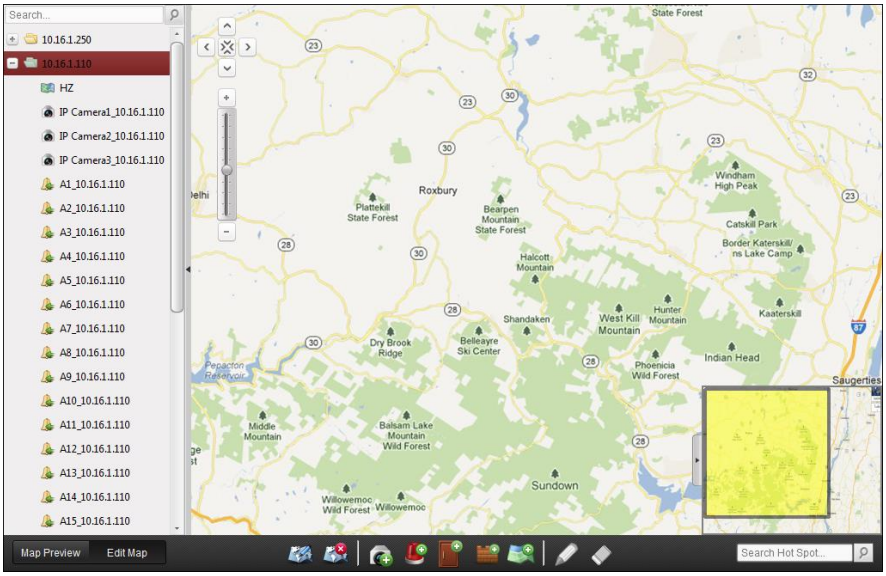
1. Open the E-map page.
2. Select a group for which you want to add a map.
3. Click the icon  in the Map Display Area to open the map adding window box.
4. Input a descriptive name of the added map as desired.
5. Click the icon  and select a map file from the local path.
6. Click **OK** to save the settings.

Notes:

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

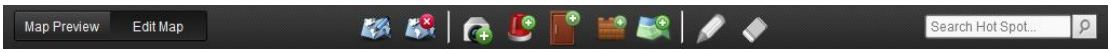


The map added is displayed in the Map Display Area. Use the mouse wheel or click  or  , to zoom in or zoom out on the map. You can click-and-drag the yellow window in the lower-right corner or use the direction buttons and zoom bar to adjust the map area for view.



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.

8.2 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 zone hot spot, refer to *Chapter 12.3 Displaying Zone on E-map.*
- For managing and previewing the access control point hot spot, refer to *Chapter 14.11* Displaying Access Control Point on E-map.

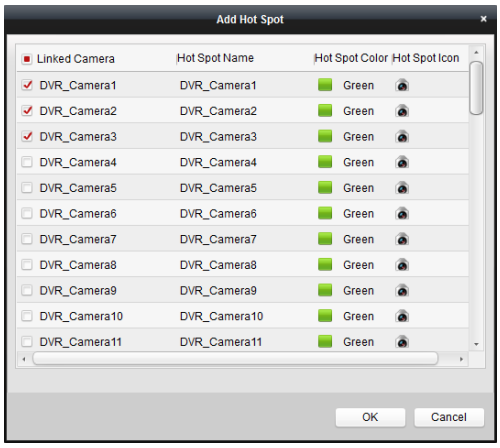
8.2.1 Adding Hot Spots

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 window 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.



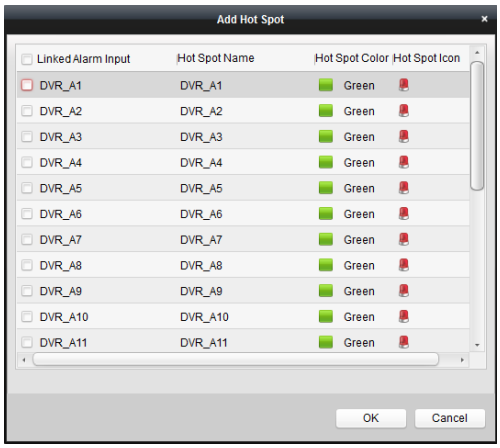
Adding Alarm Inputs as Hot Spots

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 window 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.



8.2.2 Modifying Hot Spots

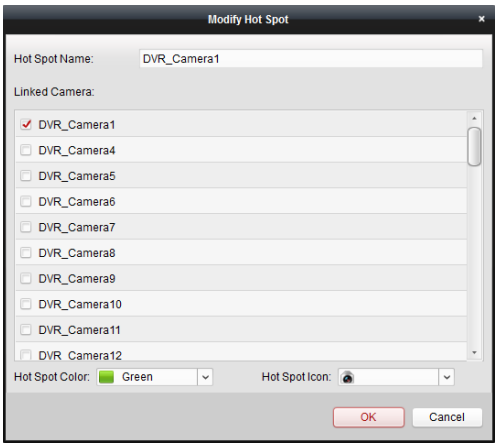
Purpose:

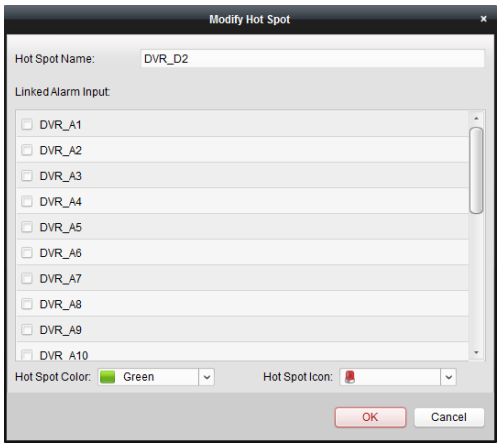
You can modify the information of the added hot spots on the map, including the name, the color, the icon, etc.

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 window 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**.



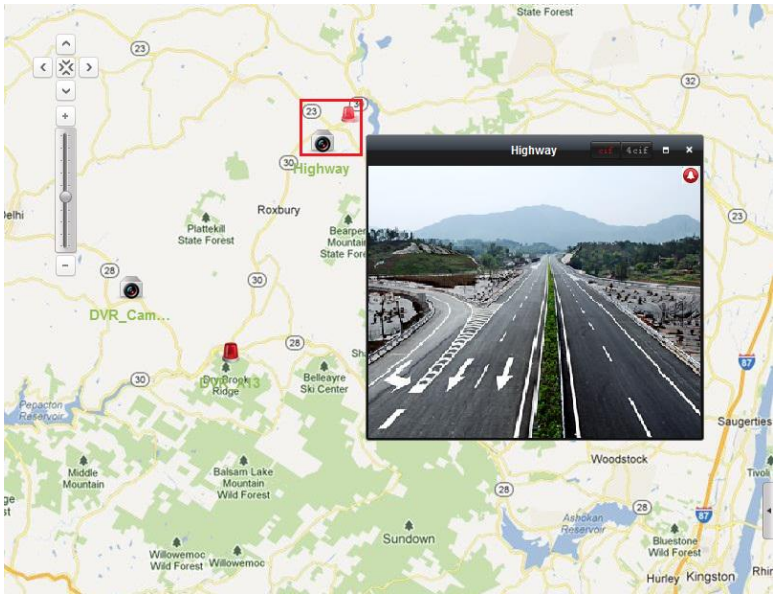


8.2.3 Previewing Hot Spots

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 (it will twinkle for 10s). 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 Alarm Management.*



8.3 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.

8.3.1 Adding Hot Regions

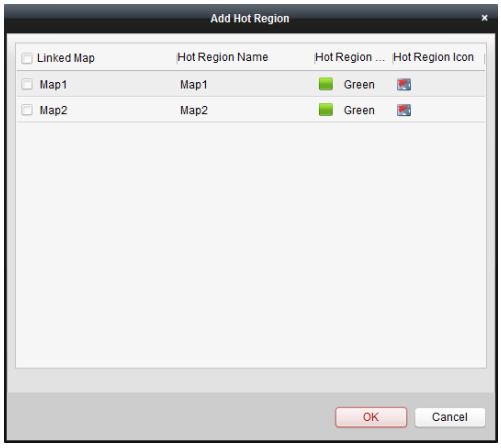
Before you start:

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 window 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.



8.3.2 Modifying Hot Regions

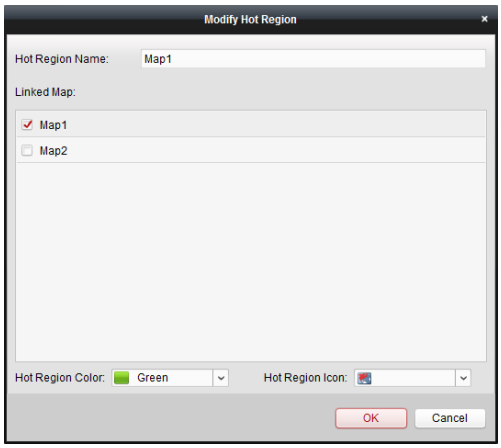
Purpose:

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 window 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.

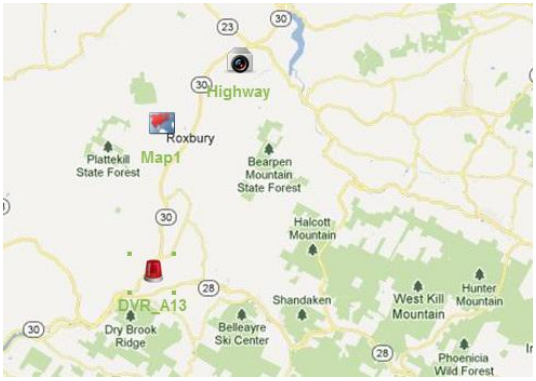
   To delete the hot region, select the hot region icon and click  in the toolbar, or right-click the hot spot icon and select **Delete**.

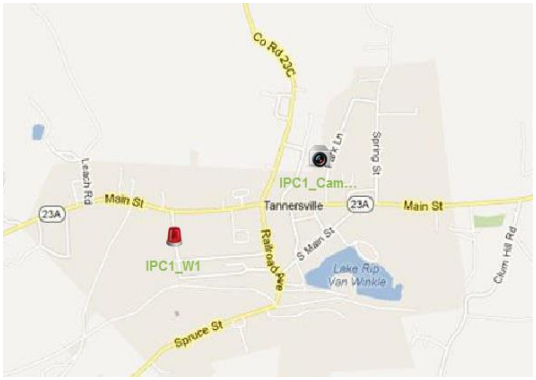


8.3.3 Previewing Hot Regions

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 9 Hik-Connect

Purpose:

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

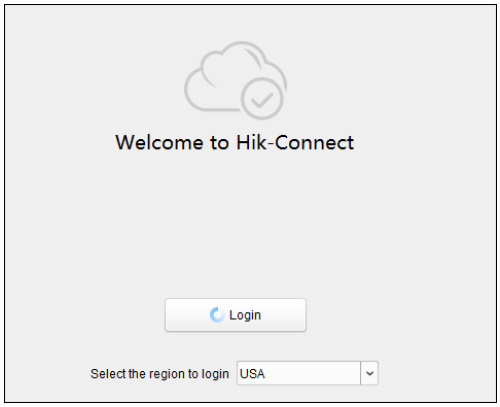
9.1 Registering a Hik-Connect Account

Purpose:

If you do not have a Hik-Connect account, you can register one.

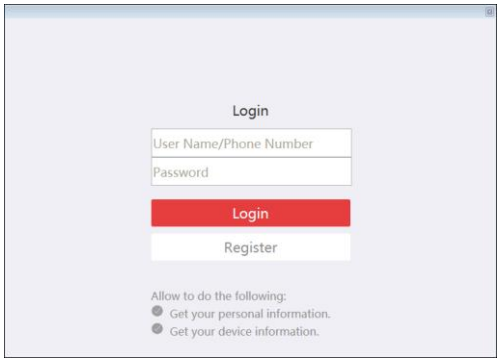
Steps:

1. Open the Device Management page and click the **Device** tab.
2. Click **Add New Device Type**, select **Hik-Connect Device** and click **OK**.
3. Click **Hik-Connect Device** on the list to enter the following page.

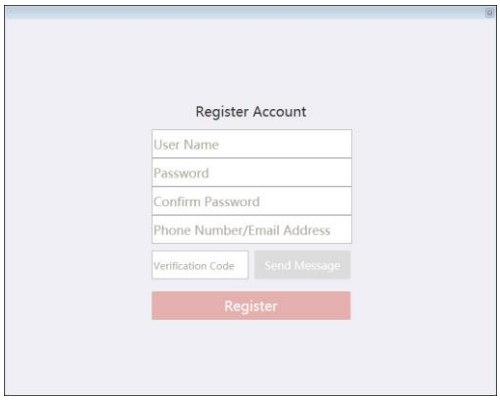


4. Select the region of your Hik-Connect account.
5. Click **Login** to pop up the following window.

   Note: The web browser should be Internet Explorer version 9 and later.



6. Click **Register** to pop up the Register Account window.



7. Enter the required information to register an account.
   User Name: Edit a user name for your account as desired.
   Password and **Confirm Password**: Enter the password for your account and confirm it.
   Phone Number/Email Address: Enter your phone number or email account to register the account.
   Verification Code: Click **Send Message** and system will send verification code to your phone or email. Input the received verification code in the **Verification Code** field.

   - *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.*
8. Click **Register** to finish registeration.

9.2 Logging into Hik-Connect Account

Note: The login will expire in 7 days. You should login the account again when expired.

Steps:

1. Click **Login**.
   Note: The web browser should be Internet Explorer version 9 and later.
2. Enter the user name/phone number and password.
3. Click **Login** to log into your account.
4. (Optional) Click **Logout** to log out of your Hik-Connect account.
   Note: You cannot receive alarm information of the devices of the account if you log out.

9.3 Device Management

Purpose:

You can add the Hik-Connect device to the Hik-Connect account, and delete the added device(s) from the account. You can also do remote configuration and group management to the devices of

the Hik-Connect account.

9.3.1 Adding Device to Hik-Connect Account

Purpose:

You can add the Hik-Connect device to the Hik-Connect Account via two ways on the client, i.e., adding manually or adding via Online Device.

Note: You can add 256 devices (1024 cameras) to one Hik-Connect account at most.

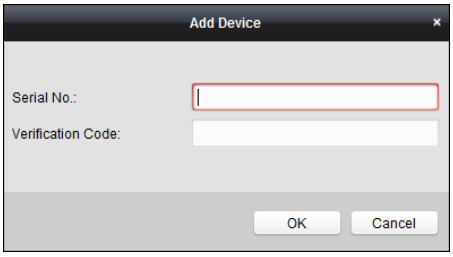
Adding Device Manually

Purpose:

You can add Hik-Connect device to the Hik-Connect account manually.

Steps:

1. Click **Add Device** to pop up the Add device window.



2. Input the serial No. and verification code of the device.

   Notes:

   - Only the device that supports the Hik-Connect service can be added.
   - The serial No. is marked on the label of you device.
   - The verification code is created when you enabling the Hik-Connect service. For details, refer to *Chapter 3.1.1 Activating Device.*
   - The device can only be added to one Hik-Connect account.

3. Click **OK** to add the device.

   The successfully added device will list on the device management interface.

   Note: After adding the device to the Hik-Connect account, you should add the device by Hik-Connect domain if you want to add the device to the local client. For details, refer to *Chapter 3.1.5 Adding Devices by Hik-Connect Domain.*

Adding Device via Online Device

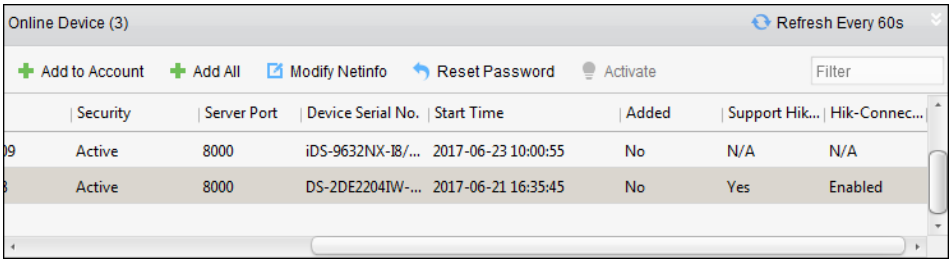
Purpose:

You can add Hik-Connect device via the online device list.

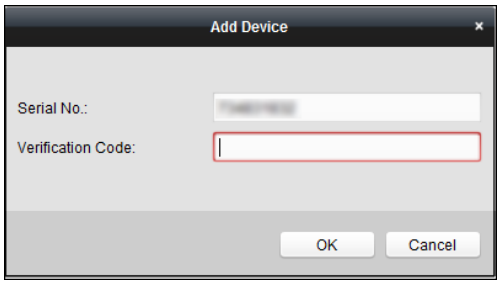
Steps:

1. Select the device(s) which support Hik-Connect service on the online device list.

   You can also input the keyword in the **Filter** field to filter the required device.



2. (Optional) Activate the device if it is inactivated. For details, refer to *Chapter 3.1.1 Activating Device*.
3. (Optional) Enable the Hik-Connect service. For details, refer to *Chapter 3.1.1 Activating Device*.
4. Click **Add to Account** to pop up the Add Device window.



5. Input the verification code.
   Note: The verification code is created when you enabling the Hik-Connect service. For details, refer to *Chapter 3.1.1 Activating Device.*
6. Click **OK** to add the device.
   Note: After adding the device to the Hik-Connect account, you should add the device by Hik-Connect domain if you want to add the device to the local client. For details, refer to *Chapter 3.1.5 Adding Devices by Hik-Connect Domain.*
7. (Optional) You can select device from the device management interface and click **Delete** to remove the device from the Hik-Connect account.

9.3.2 Modifying Camera

Purpose:

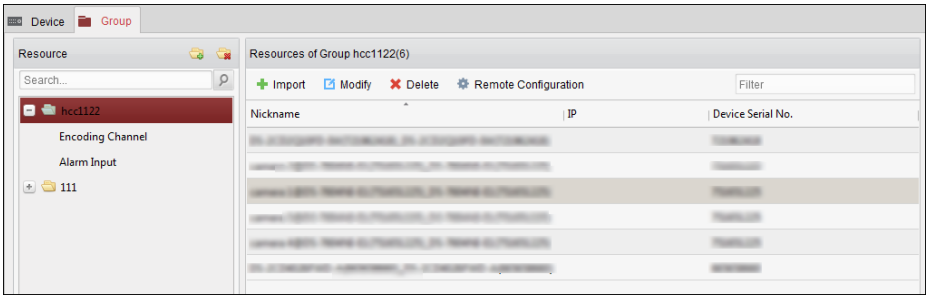
After adding the Hik-Connect device to the client, you can edit the camera parameters and set stream key.

Before you start:

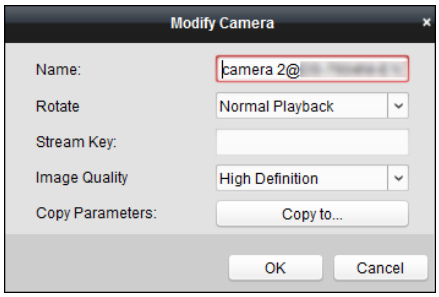
You should import the cameras of the added devices to groups. For details, refer to *Chapter 3.2 Managing Group.*

Steps:

1. Click **Group** tab to enter the group management page.
2. Select camera from the resource list.



3. Click **Modify** to pop up the Modify Camera window.



4. Edit the camera information, including name, rotate, protocol type, etc.

   Stream Key: For Hik-Connect device, the stream key is the same with the verification code, which is created when you enable the Hik-Connect service. For details, refer to *Chapter 3.1.1 Activating Device.*

   Notes:

   - If the live view or video file(s) of the Hik-Connect device is encrypted, you should input the stream key on the Modify Camera window before you can view the live view or video file(s) of the device.
   - You can set whether to encrypt the live view or video file(s) of the Hik-Connect device on the Hik-Connect mobile client software. For details, refer to the *User Manual of the Hik-Connect Mobile Client Software.*

9.4 Live View and Playback

Purpose:

You can view the live view of the device, and play the video files stored on the local device or the Storage Server. For details, refer to *Chapter 4 Live View and Chapter 5 Remote Storage Schedule Settings and Playback*.

Before you start:

Input the stream key on the Modify Camera window if the live view of the Hik-Connect device is encrypted. For details, refer to *9.3.2 Modifying Camera*.

Notes:

- You can perform two-way audio for Hik-Connect device during live view.
- The Hik-Connect device only supports normal playback.
- The Hik-Connect device doesn't support reverse playback, adding tags, fast forward, and slow forward during playback.
- You cannot download the video files for Hik-Connect device.
- For PTZ control during live view, the Hik-Connect device only supports the PTZ movements to the upside, downside, left, and right.

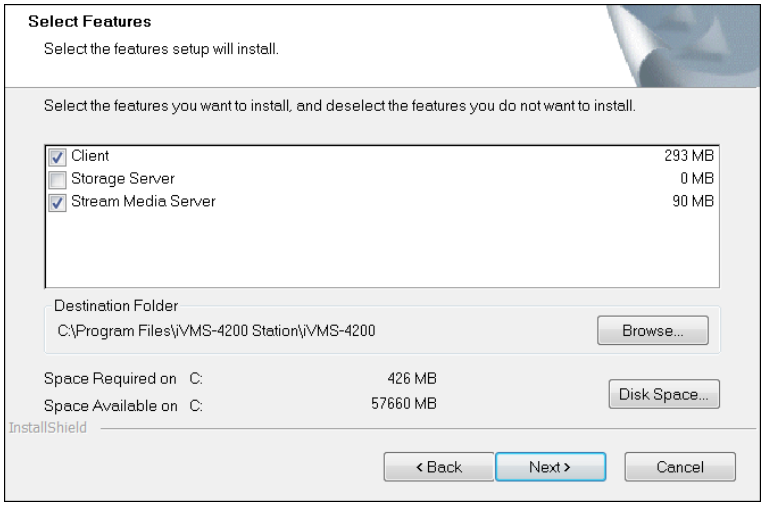
Chapter 10 Forwarding Video Stream through Stream Media Server

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.

Before you start:

The stream media server application software needs to be installed and it is packed in the iVMS-4200 software package. After running the installation package, check **Stream Media Server** to enable the installation of stream media server.



10.1 Importing Certificate to Stream Media Server

Purpose:

Before adding the stream media server to the client, you should import the client's security certificate to the stream media server first to perform security authentication and ensure data security.

Note: If the client's security certificate is updated, you should export the new certificate from the client and import it to the stream media server again to update.

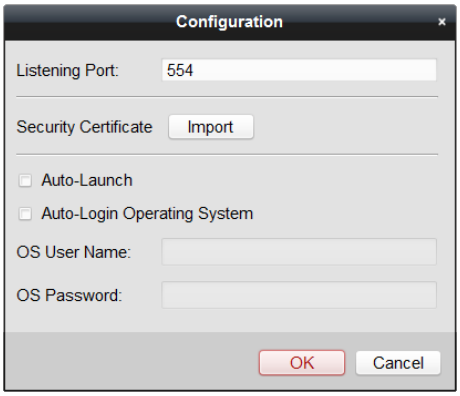
Perform the following steps to import the security certificate to the stream media server.

Steps:

1. Export the certificate from the client.
   1) Enter **System Configuration** -> **Service Certificate.**
   2) Click **Export** to export the certificate.
2. Copy the certificate to the PC which has installed with stream media server.
3. Click the shortcut icon  on the desktop of the PC installed with stream media server to

run it.

4. Import the certificate to the stream media server.
   1) Right click on the task bar and click **Display**.
   2) Click **Configuration** to enter the following interface.



   3) In the security certificate field, click **Import** and select the certificate file you export from client in Step 1.
   4) Click **OK** to save the settings.
   5) Restart the stream media server to take effect.

10.2 Adding Stream Media Server

10.2.1 Adding One Stream Media Server to Client

Purpose:

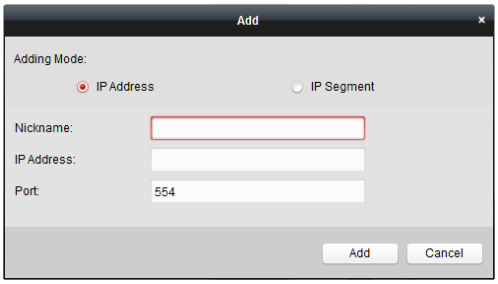
You can add stream media server to the client one by one for further operations.

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

Steps:

1. Click the shortcut icon on the desktop of PC that installed with stream media server to run it.

   Note: If the stream media server port (value: 554) is occupied by other service, you should change the port number to other value to ensure the proper running of the stream media server.
2. Run iVMS-4200 and click Device Management > **Device** to enter the device management page.
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**.



5. Select **IP Address** as the adding mode.
6. Input the nickname and IP address of the stream media server.
   The default port value is *554*.
7. Click **Add** to add the stream media server to the client software.
   The added server will display in the server list, showing the server details and status.
   Note: If the added Stream Media Server's security certificate doesn't match with the client's, it will prompt you with  after the server nickname. Move to the  icon to view exception message and follow the provided steps to keep certificates consistent.

10.2.2 Batch Adding Stream Media Servers to Client

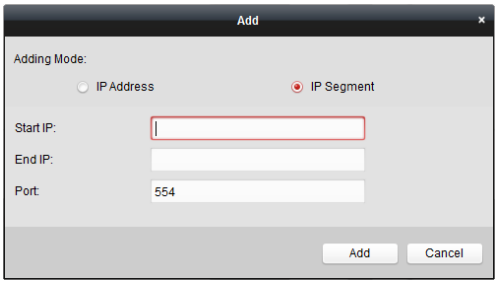
Purpose:

You can add stream media servers to the client in a batch for further operations.

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

Steps:

1. Click the shortcut icon  on the desktop of PC that installed with stream media server to run it.
   Note: If the stream media server port (value: 554) is occupied by other service, a window box will pop up. You should change the port No. to other value to ensure the proper running of the stream media server.
2. Run iVMS-4200 and click **Device Management > Device** to enter the device management page.
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**.
5. Select **IP Segment** as the adding mode.



6. Input the start IP and end IP. The default port value is *554*.
7. 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, showing the servers' details and status.
   Note: If the added Stream Media Server's security certificate doesn't match with the client's, it will prompt you with  after the server nickname. Move to the  icon to view exception message and follow the provided steps to keep certificates consistent.

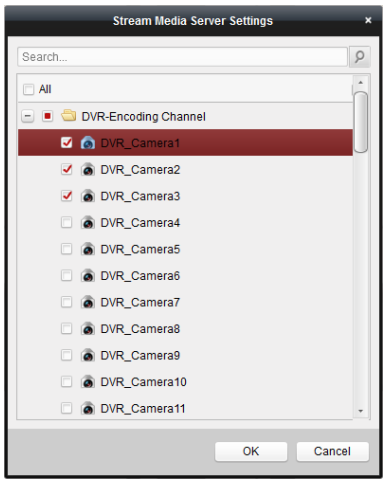
10.3 Adding Cameras to Stream Media Server to Forward Video Stream

Purpose:

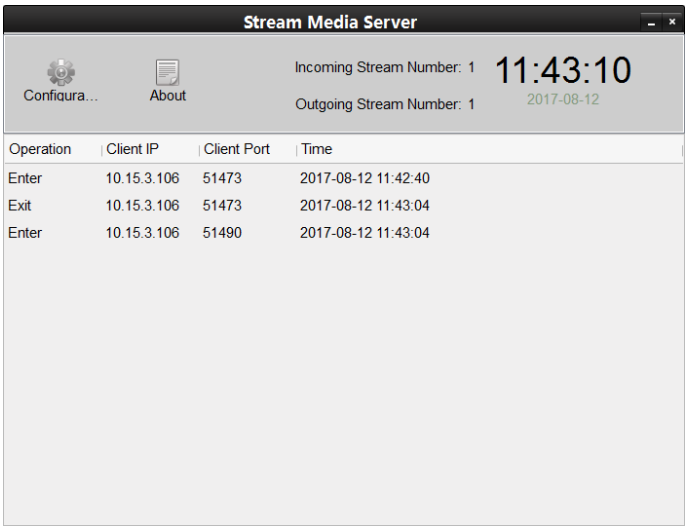
To get the video stream of a camera via stream media server, you need to connect the camera to the stream media server.

Steps:

1. Enter the Device Management interface and click **Device** tab.
2. Select **Stream Media Server** on the Device Type panel.
3. Select the stream media server from the Device for Management list.
4. Click **Configure** to enter the Stream Media Server Settings interface.



5. Select the cameras of which the video stream is to be forwarded via the stream media server.
6. Click **OK** to save the new settings.
7. 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.

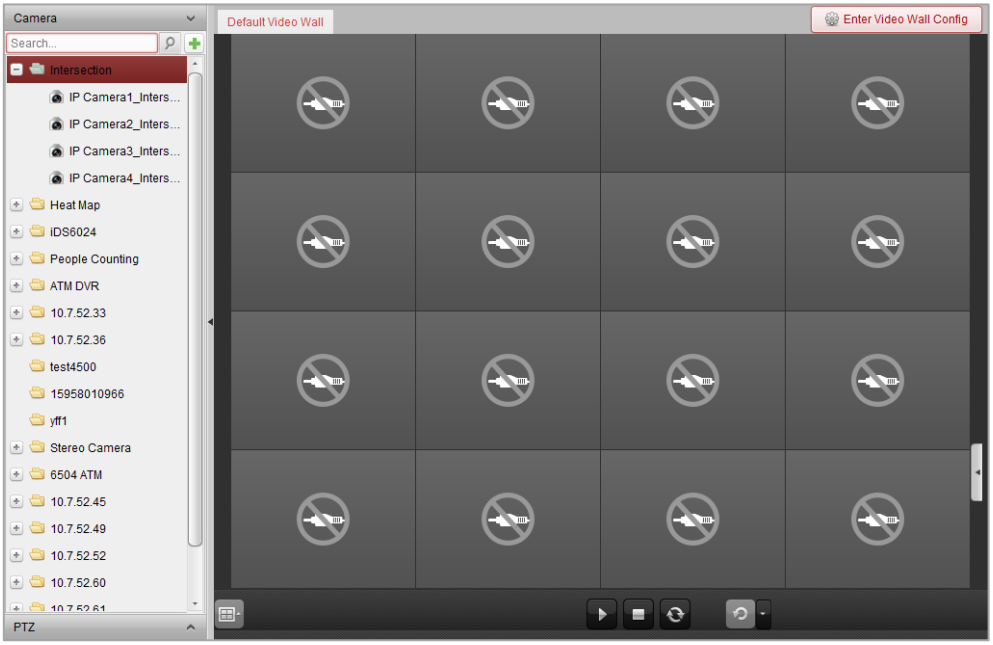
- If the camera is offline, the client can still get the live video via the stream media server.

Chapter 11 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.



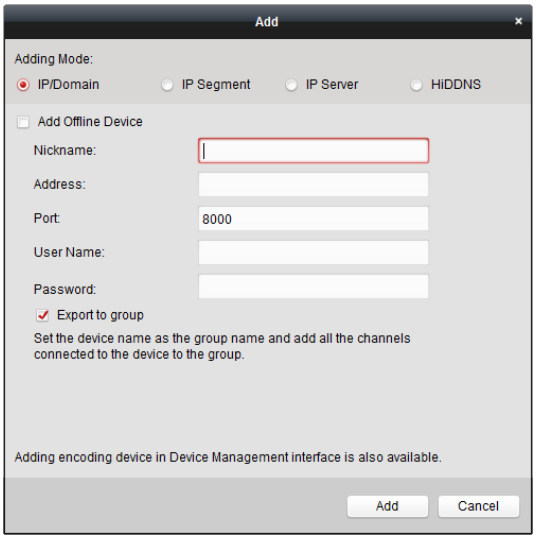
11.1 Adding Encoding Device

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.

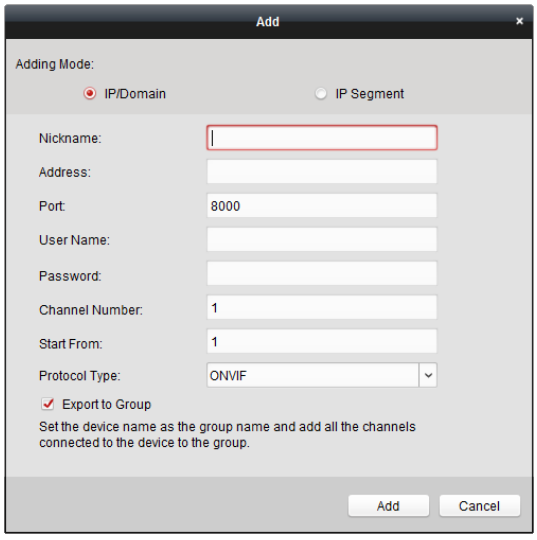


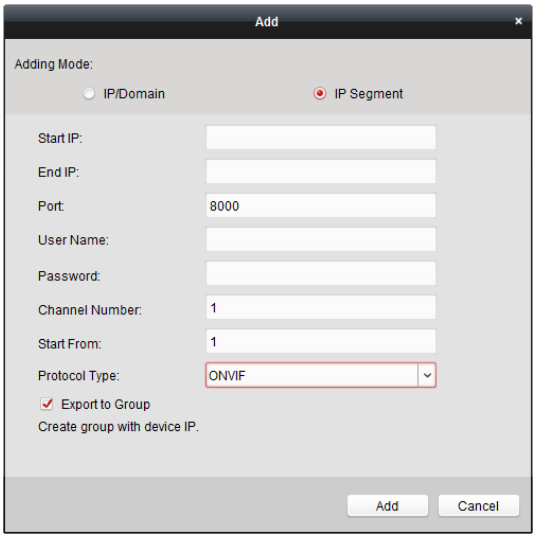
2. Select the adding mode and configure the corresponding settings for the device.
   For the detailed configuration about the 4 adding modes, refer to the following chapters:
   - By specifying the device IP address, refer to *Chapter 3.1.3 Adding Devices by IP or Domain Name.*
   - By specifying an IP segment, refer to *Chapter 3.1.4 Adding Devices by IP Segment.*
   - By IP Server, refer to *Chapter 3.1.8 Adding Devices by IP Server.*
   - By HiDDNS, refer to *Chapter 3.1.9 Adding Devices by HiDDNS.*

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

Steps:

1. Go to the Device Management page and click the **Device** tab.
2. Click **Add New Device Type**, select **Third-party Encoding Device** and click **OK**.
3. Select Third-party Encoding Device in the device type panel and click **Add** 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.
     Example: If you input 4 in **Start From** field, it means that the starting channel No. is 4.





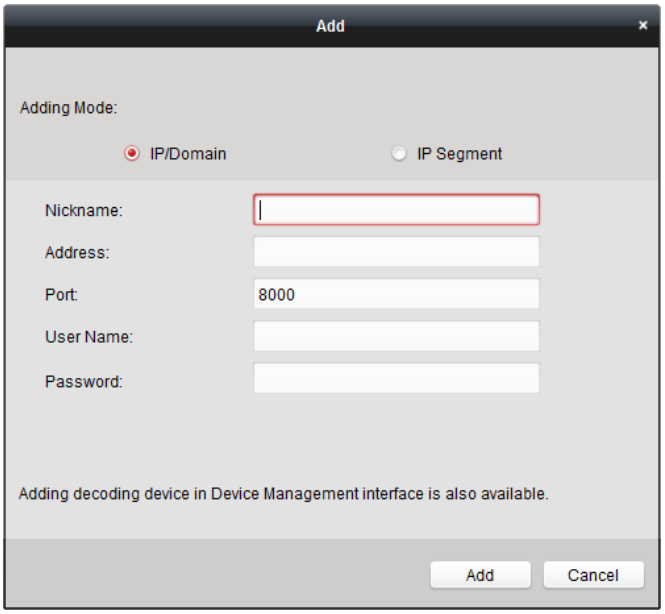
11.2 Adding Decoding Device

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.



3. 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, refer to the following chapters:

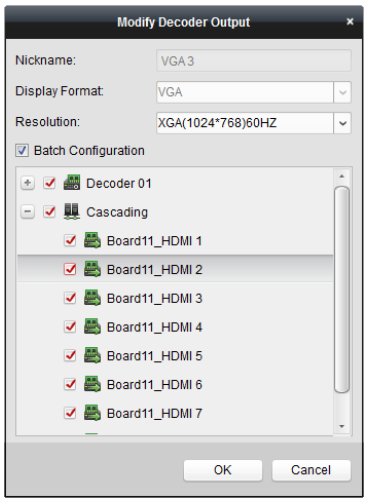
   - By specifying the device IP address or domain, refer to *Chapter 3.1.3 Adding Devices by IP or Domain Name.*
   - By specifying an IP segment, refer to *Chapter 3.1.4 Adding Devices by IP Segment*.

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.



Notes:

- 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, refer to the *User Manual* of the NVR.

11.3 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.

11.3.1 Linking Decoding Output with Video Wall

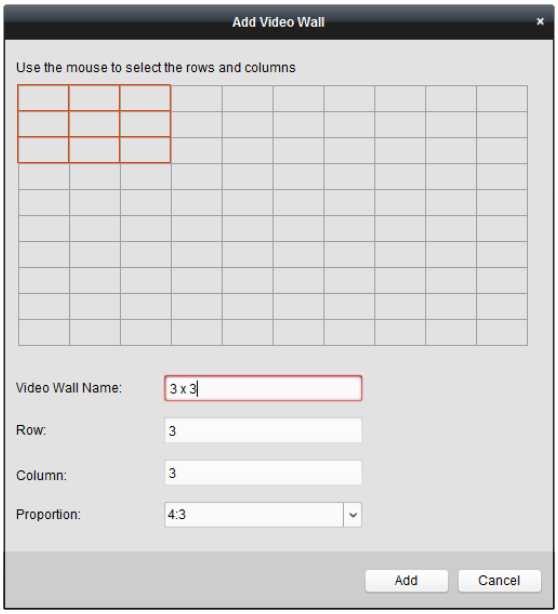
Steps:

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.



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.

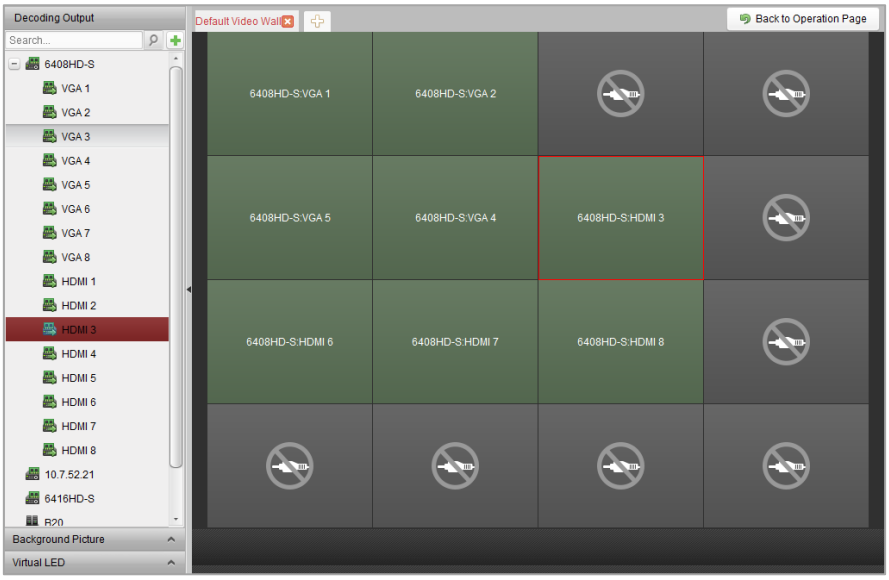
Task 3: Delete a Video Wall

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.



11.3.2 Multi-Screen Display

Purpose:

For DS-6400HDI-T series and DS-6900UDI series decoder, you can span multiple screens as a whole window. In this way, the decoded video of one camera can be shown on the spanned window.

Before you start:

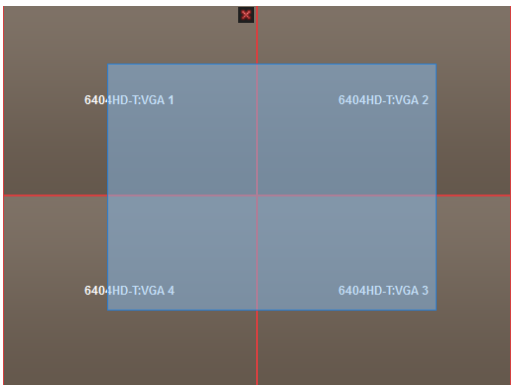
You should add DS-6400HDI-T series and DS-6900UDI series decoding device to the client. Refer to *Chapter 11.2 Adding Decoding Device* for detailed configuration about adding decoding device.

Steps:

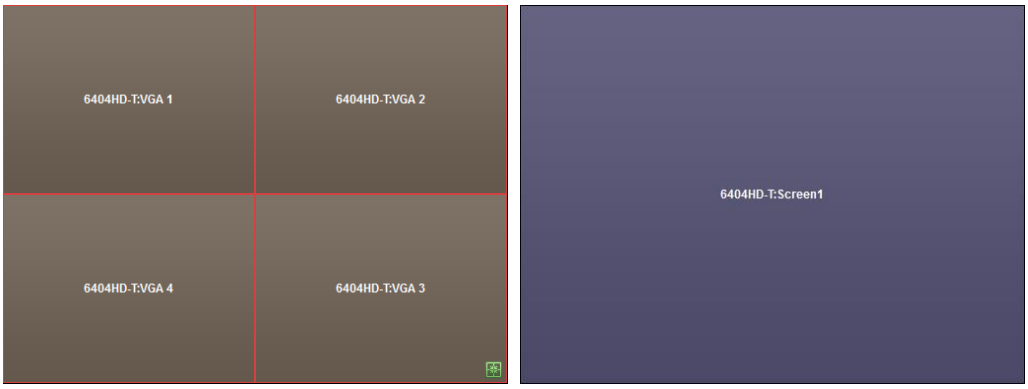
1. Perform the step 3 of *Chapter 11.3.1 Linking Decoding Output with Video Wall* to configure the linkage between the decoder and video wall.
2. Click-and-drag you mouse to select the adjacent display windows for jointing.

   Notes:

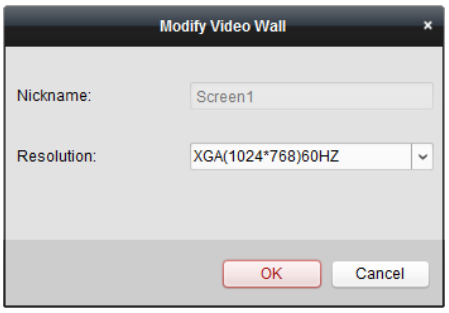
   - You can only joint the same output interfaces as a whole window. E.g., you can only joint 4 VGA interfaces or HDMI interfaces.
   - BNC interface does not support jointing.



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.



11.3.3 Configuring Background

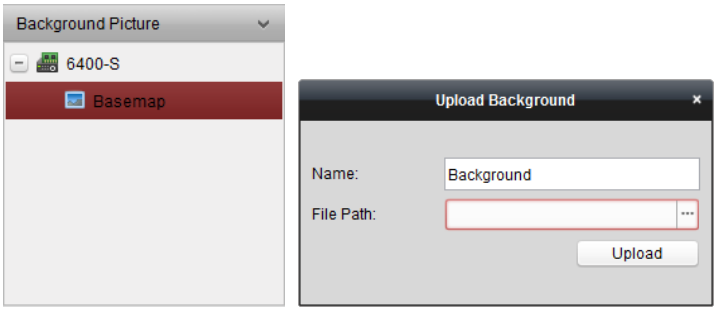
Purpose:

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

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

Steps:

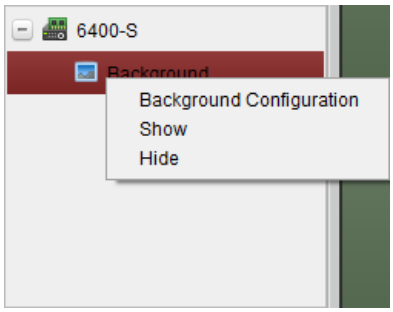
1. Click to expand the Background Picture panel.
2. Select a background picture and double-click (or right-click and select **Background Configuration**) it to activate the background uploading window.



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.



11.3.4 Configuring Virtual LED

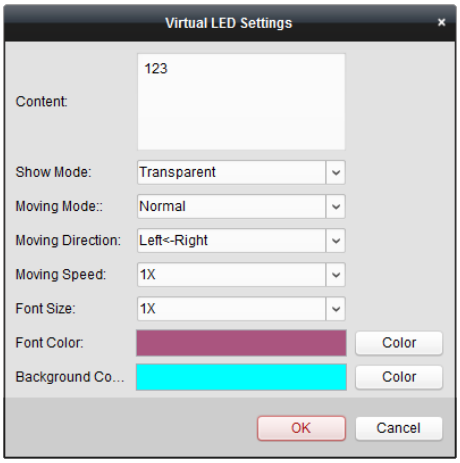
Purpose:

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 decoding device.
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



11.4 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, refer to the *User Manual* of the device.

11.4.1 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.

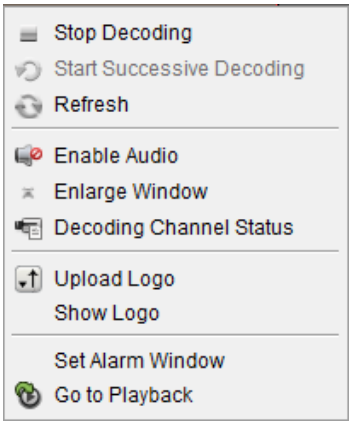
   Notes:

   - 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 and DS-6900UDI 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, 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.

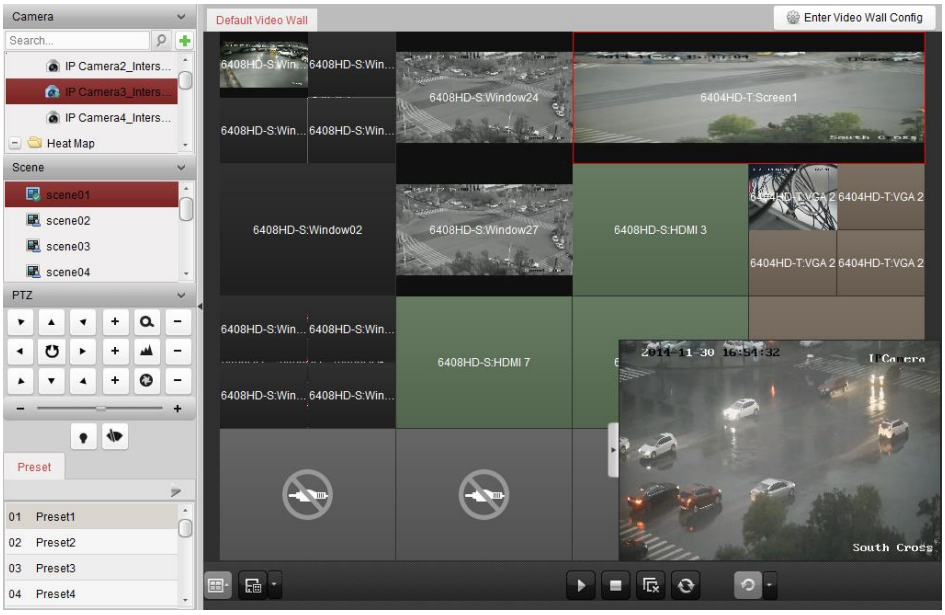
Stick at Bottom: Always stick the window at the bottom layer.

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.

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

11.4.2 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.

11.4.3 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 22.4 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.

11.4.4 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 and DS-6900UDI.
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.

Chapter 12 Security Control Panel

Purpose:

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

Note: For the users with security control panel permissions, they can enter the Security Control Panel module to manage the security control panel and real-time alarm. For setting the user permission of Security Control Panel module, refer to *Chapter 20 Account Management*.

Before you start:

Before you can remotely configure and control the security control panel, you should add device to the software. For details about adding security control panel, refer to *Chapter 3.1 Adding Device.*

12.1 Configuring Zone Event

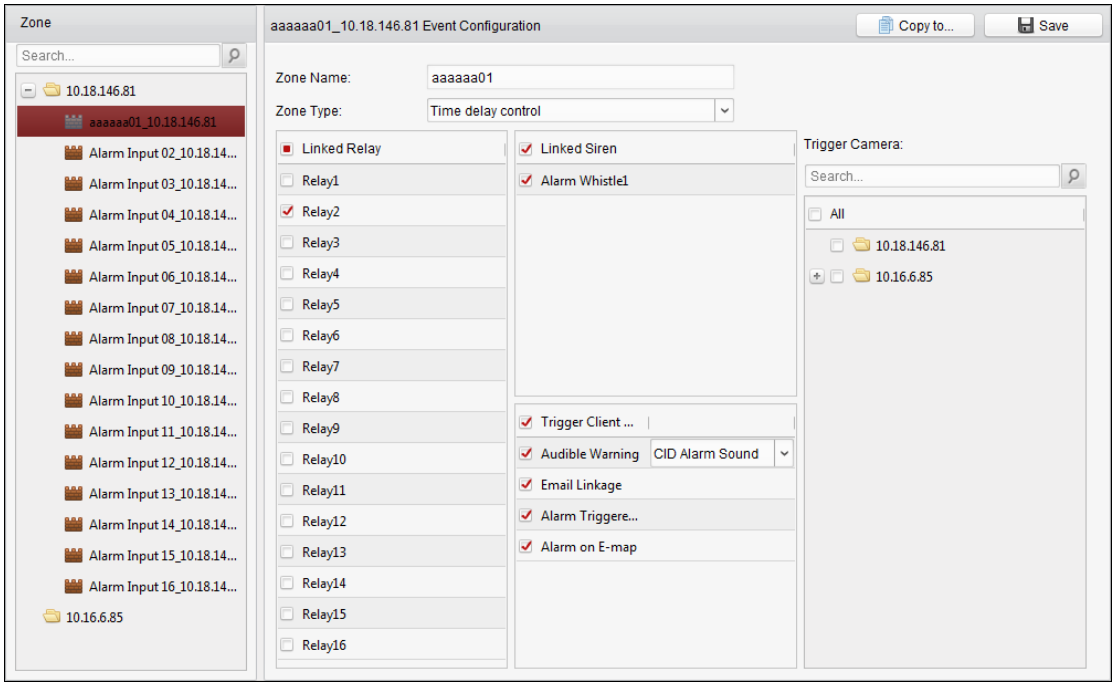
Purpose:

You can configure the event linkages, including siren, relay, client linkage and triggered cameras, for the zones of the security control panel.

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

Steps:

1. Click  on the Control Panel, or click **Tool** -> **Event Management** to open the Event Management page.
2. Click **Zone Event** tab.
3. Click the icon  to unfold the zone list of a security control panel on the left panel.
4. Click a zone name on the list to activate the configuration of the zone event.



5. Configure the name, type and event linkages for the zone.

1) Edit the zone name in the Zone Name field.
2) Unfold the drop-down list of the Zone Type field and select a type.
3) Check the checkbox(es) to select the linked relay(s) on the Linked Relay panel.
4) Check the checkbox(es) to select the linked siren(s) on the Linked Siren panel.
5) Check the checkbox(es) to activate the linkage action(s) on the Trigger Client Action panel. See the detailed actions below:

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, refer to *Chapter 22.7 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. ***Note:*** You should set the triggered camera first.
Alarm Triggered Video Wall Display	Display the video on the Video Wall when alarm is triggered. ***Note:*** You should set the triggered camera first.

6) Select the camera(s) on the Trigger Camera panel to be triggered 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 should set the capture schedule and the storage in Storage Schedule. For details, refer to *Chapter 5.1 Remote Storage.*
   Note: Up to 4 cameras can be set as the triggered cameras.

6. Optionally, click **Copy to…** to copy the event settings to other zones.
7. Click **Save** to save the settings.

12.2 Remote Control

Purpose:

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

Click  on the Control Panel to open the Security Control Panel page.

All the added security control panels will display.

You can click the dropdown list on the upper-left corner to filter the security control panel by device types.

Click the icon  or  at the upper right corner of the page to switch the display mode between the tile or list mode.

12.2.1 Partition Remote Control

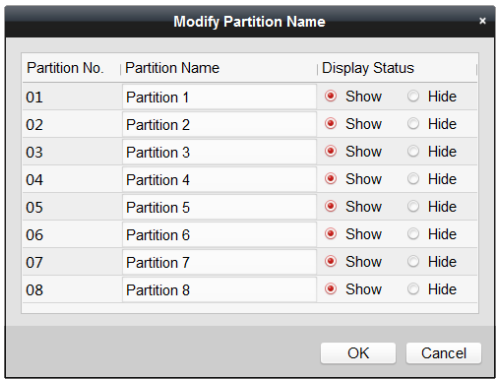
Purpose:

You can remotely perform operations of away arming, stay arming, instant arming, disarming,

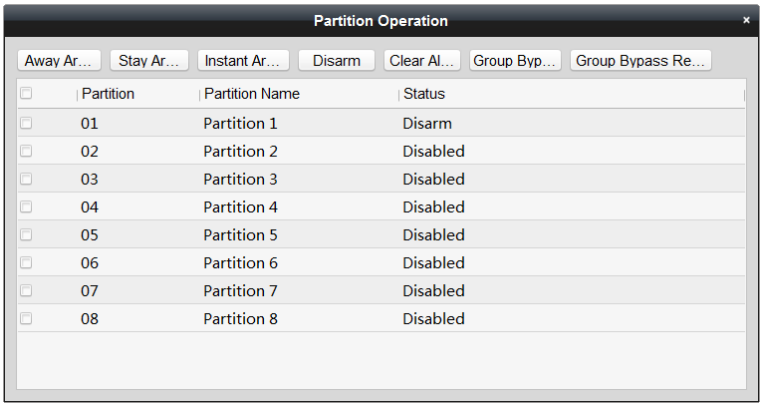
clearing alarm, group bypass, and recovering group bypass for the configured partitions.

Steps:

1. (Optional) Click **Modify** to edit the partition name as you want and change the partition display status as show or hide.



2. (Optional) In tile mode, click **Operation** to open the Partition Operation window.
   You can control the partitions in batch.



3. Select the partition(s) to operate.
4. Click the operation button (e.g., Away Arming, Stay Arming, Instant Arming, Disarm, Clear Alarm, Group Bypass or Group Bypass Recovery) to control the selected partition(s).
5. If the partition is in alarm status:
   - **Tile mode:** A  icon will display and twinkle near the partition name. You can hover over the mouse to the icon to device the partition's zones status. For the details about the triggered zone alarm, refer to *Chapter 12.4 Handling Alarms.*
   - **List mode:** The partition name will turn red and a  icon will display near the partition name. You can hover over the mouse to the icon to device the partition's zones status. For the details about the triggered zone alarm, refer to *Chapter 12.4 Handling Alarms.*

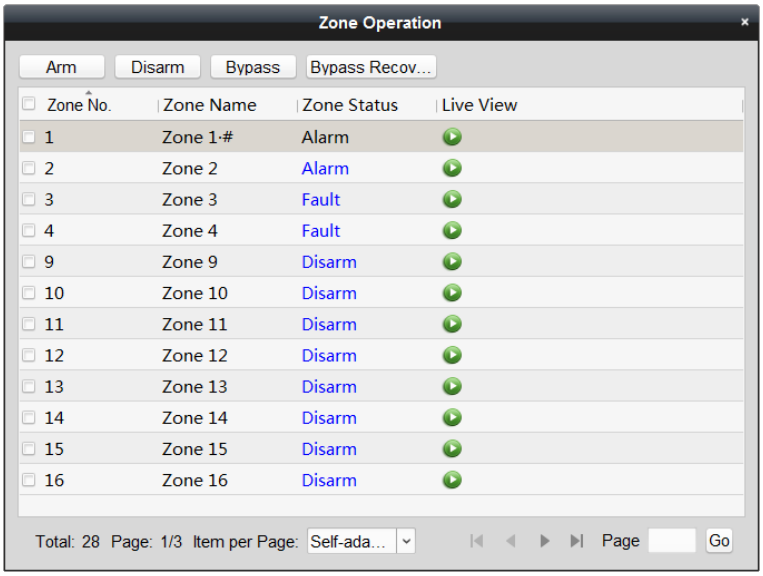
12.2.2 Zone Remote Control

Purpose:

You can remotely perform bypass, or recover bypass for the zones.

Steps:

1. Click  to open Zone Operation window.
   You can view the all linked zones of the partition in this window and check the zone status.



2. Select the zone(s) for operation.
3. Click **Arm, Disarm, Bypass** or **Bypass Recovery** to control the selected zones.
4. Click in the Live View column to view the live view of the triggered camera in the zone.
   Note: You can set the triggered camera of the zone in the Event Management module. For details, refer to *Chapter 12.1 Configuring Zone Event*.

12.3 Displaying Zone on E-map

Purpose:

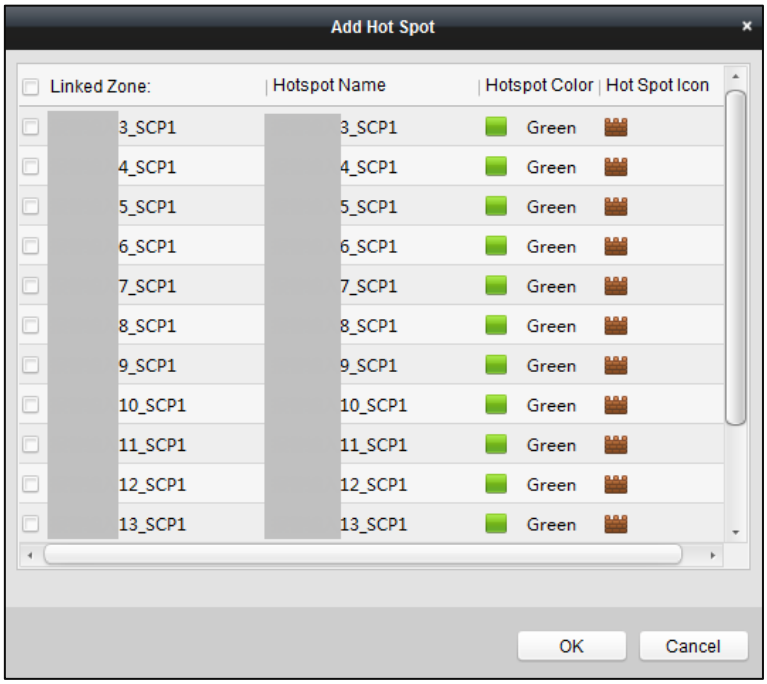
You can add the zones on the E-map, and when the alarm in the zone is triggered, you can view the alarm notification on the E-map and check the alarm details.

Note: For detailed operations of E-map, refer to *Chapter 8 E-map Management.*

12.3.1 Adding Zones as Hot Spots

Steps:

1. In the E-map module, click **Edit Map** tab at the lower left corner to enter the map editing mode.
2. Click the icon on the E-map Toolbar to open the Add Hot Spot window.
   Or you can directly drag the zone icons from the group list on the left panel of E-map page to the map to add the hot spots.



3. Check the checkbox(es) to select the zone(s) to be added.
4. Click **OK** to save the settings.

The zone icon(s) will be added to the map as hot spot(s) and the icon(s) of added zone(s) in the group list of the left panel will change from to .

You can drag the zone icon to move the hot spot to the desired location.

12.3.2 Modifying Hot Spots

Purpose:

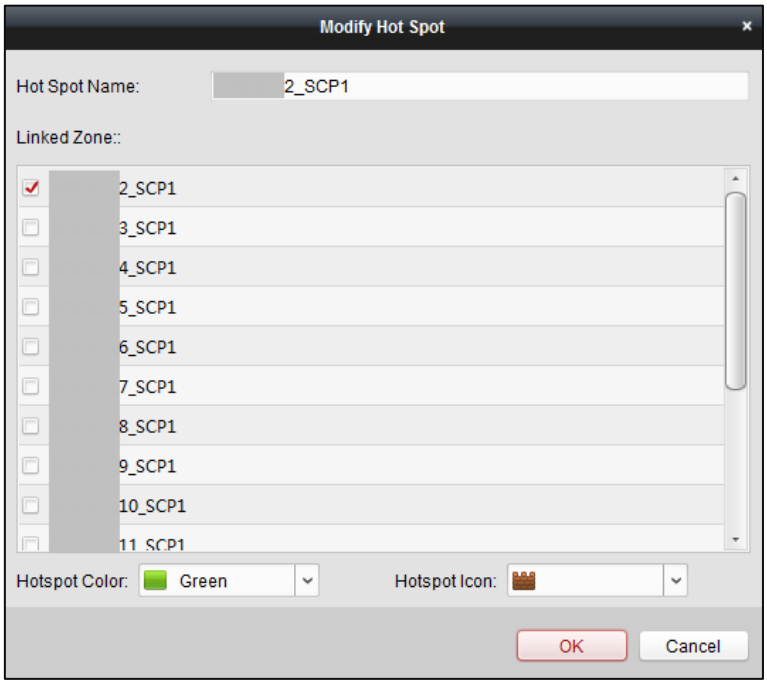
You can modify the information of the added hot spots on the map, including the name, the color, the icon, etc.

Steps:

1. In the E-map module, click the **Edit Map** tab at the lower left corner to enter the map editing mode.
2. Select the hot spot icon on the map and then click in the E-map Toolbar to open the Modify Hot Spot window.

   Or right-click the hot spot icon on the map and select **Modify** in the right-click menu to open the Modify Hot Spot window.

   Or double-click the hot spot icon on the map to pop up the Modify Hot Spot window.



You can edit the hot spot name in the text field and select the color, the icon and the linked zone.

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

12.3.3 Previewing Hot Spots

In the E-map module, click the **Map Preview** tab at the lower left corner to enter the map preview mode.

If there is any alarm triggered in the zone, an icon will appear and twinkle near the hot spot (it will twinkle for 10s). Click the alarm icon, or right-click the hot spot icon and select **Display Alarm Information,** to check the alarm information, including alarm type and triggered time.

Notes:

- 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 12.1 Configuring Zone Event.*
- You can also check the zone alarm information in the Real-time Alarm module. For details, refer to *Chapter 12.4 Handling Alarms*.

To clear the alarm information displayed on the map, you can click on the toolbar, or right-click the zone icon and select **Clear Alarm Information** to clear the alarms of the selected zone.

12.4 Handling Alarms

Purpose:

In this section, you can view the real-time triggered CID alarm information of the security control panel and handle alarms. And you can also search the history alarms by time or by alarm type.

12.4.1 Real-time Alarm

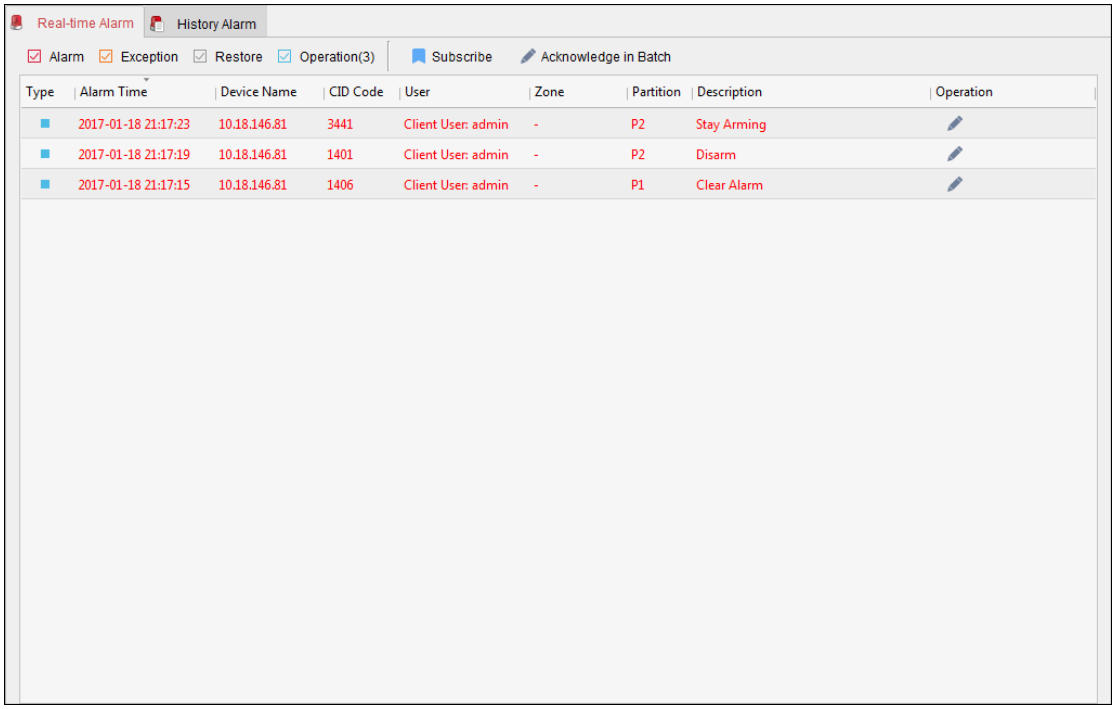
Purpose:

You can check the real-time triggered alarm information, including alarm type, alarm time, device name, CID code, zone, partition, alarm description, etc. You can also subscribe and acknowledge the alarms, or check the triggered cameras' live view and view the linked hot spots on the E-map.

Steps:

1. Click  on the Control Panel, or click **View->Real-time Alarm** to open the Real-time Alarm page.

   All the real-time triggered alarms will display on this page and you can check the alarm type, alarm time, device name, user, CID code, zone, partition, alarm description and so on.



   You can check the **Alarm**, **Exception**, **Restore**, or **Operation** checkbox(es) to show the alarms in corresponding type(s).

   Notes:

   - The Alarm type is marked with ; the Exception type is marked with ; the Restore type is marked with ; and the Operation type is marked with .
   - The number after the alarm type indicates the alarm quantity of this type.

2. Click the icon in the Operation column to acknowledge the selected alarm.

   Or you can click the **Acknowledge in Batch** button to acknowledge all the real-time triggered alarms.

   The acknowledged alarm will disappear from the list.

3. (Optional) Click the icon in the Operation column to view the live view of the triggered cameras.

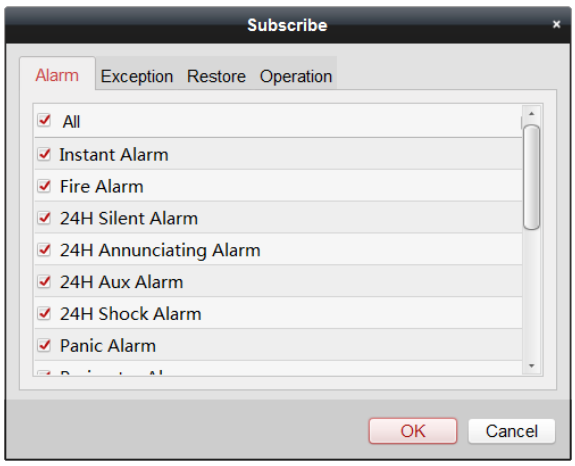
   Note: Before you can get the linked live view, you should configure triggered cameras for the zone. For details about setting triggered cameras, refer to *Chapter 12.1 Configuring Zone Event*.

4. (Optional) Click the icon in the Operation column to check the zone as hot spot on the map.

   Note: Before you can check the zone on the map, you should add the zone as hot spot to the map. For details about adding zone as hot spot, refer to *Chapter 12.3 Displaying Zone on E-map*.

5. (Optional) You can also subscribe the alarm types to receive desired alarms.

   1) Click the **Subscribe** button to pop up the Subscribe window.



   2) Click **Alarm**, **Exception**, **Restore** or **Operation** tab to select the major alarm type(s).
   3) Check the checkbox(es) under the tab to select the minor alarm type(s).
   4) Click **OK** to save the selections.

12.4.2 Searching History Alarms

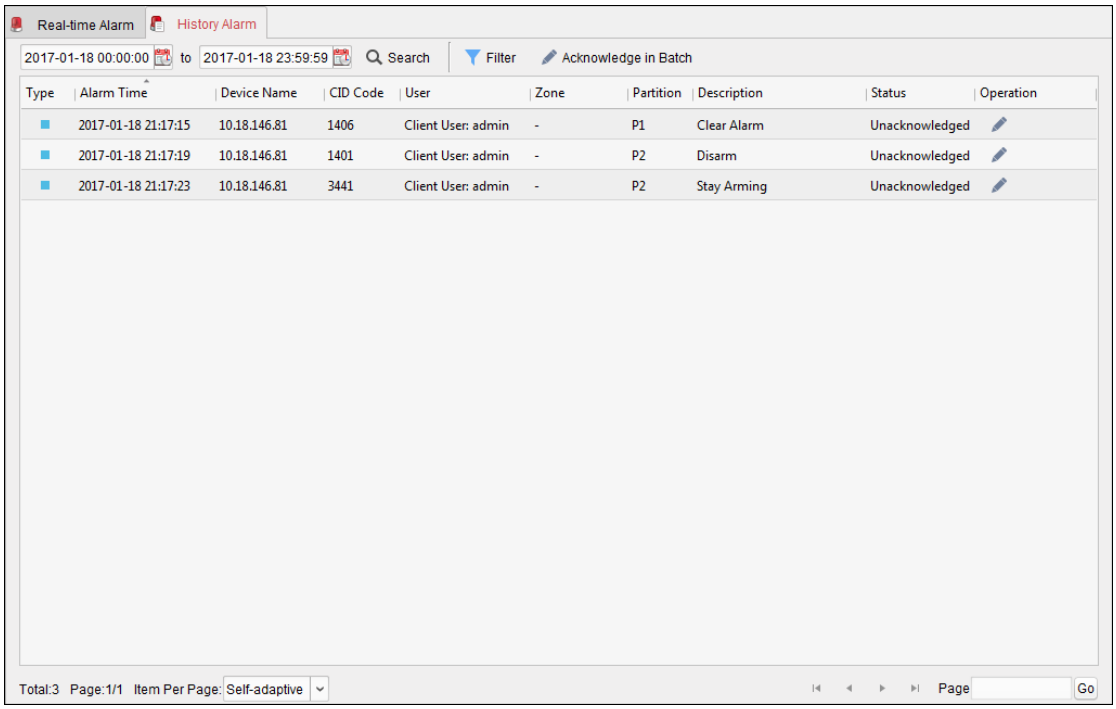
Purpose:

In this section, you can search the history alarms by time and filter the searching results by alarm type. You can also handle the matched alarms.

In the Real-time Alarm module, click **History Alarm** tab to enter the History Alarm page.

Steps:

1. In the Real-time Alarm module, click **History Alarm** tab to enter the History Alarm page.



2. Click to set the start time and end time of a time period.
3. Click **Search** button and the matched alarms will display on this page.
4. (Optional) Filter the searching results by alarm type.
   1) Click **Filter** button to pop up the Filter window.
   2) Click **Alarm**, **Exception**, **Restore,** or **Operation** tab to select the major alarm type(s).
      Note: The Alarm type is marked with ; the Exception type is marked with ; the Restore type is marked with ; and the Operation type is marked with .
   3) Check the checkbox(es) under the tab to select the minor alarm type(s).
   4) Click **OK** to start filtering history alarms by alarm types
5. (Optional) For the searched alarms, click or click **Acknowledge in Batch** button to acknowledge the unacknowledged alarms, and the acknowledged alarm items will turn to gray.
   You can also click and to check the linked live view of the alarms and view the linked hot spots on the e-map.
   For details about operating the alarms, refer to *Chapter 12.4.1 Real-time Alarm*.

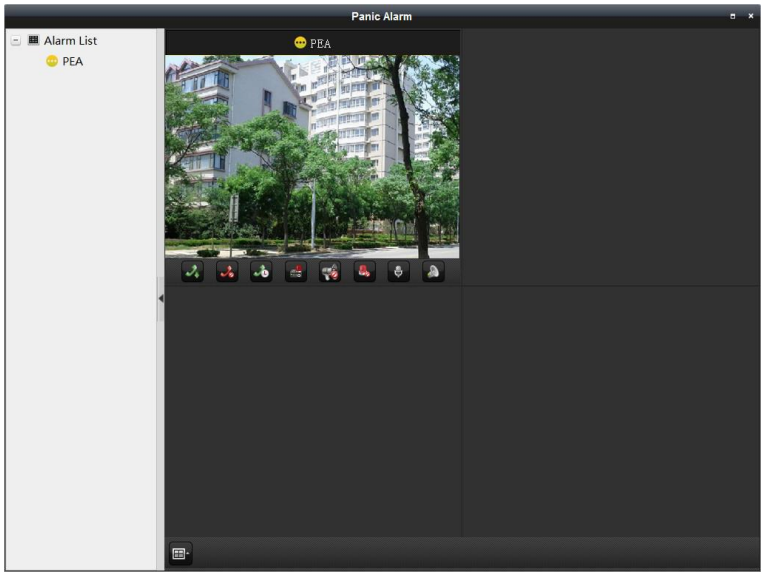
12.4.3 Handling Panic Alarm

Purpose:

For the pole panic alarm station, when the panic alarm is triggered, you can handle the alarm via the client.

Steps:

1. When the user calls the center via panic alarm station, the panic alarm is triggered. The following window will pop up.



You can view the live video.

The following icons are available on the toolbar.

Icon	Name
	Answer
	Refuse
	Waiting
	Unlock
	Turn On Alarm Lamp
	Turn On Alarm Lamp (Remote)
	Volume In
	Volume Out

2. You can click  to answer the call.
3. Right-click on the live view window to open the right-click menu.

The following buttons are available

Icon	Name	
	Capture	Capture the picture in the live view process.
	Start/Stop Recording	Start/Stop the manual recording. The video file is stored in the PC.
	Open PTZ Control	If the zone is linked to the speed dome, you can enable PTZ control function on the display window. Click again to disable the function. ***Note:*** For setting the triggered camera, refer to *Chapter 12.1 Configuring Zone Event.*

Chapter 13 Pyronix Control Panel

Purpose:

Pyronix cntrol panel can be added to the client for management and control. You can control the partitions, zones, and alarm outputs of the added Pyronix control panel. After setting the zone event for the Pyronix control panel, the client can receive the alarms triggered by Pyronix control panel when the device is in alarm mode.

You can also add the zone of Pyronix control panel to 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. For detailed operations for adding zone to E-map, refer to *Chapter 12.3 Displaying Zone on E-map*.

You can also search the operation logs stored in Pyronix control panel. For details, refer to *Chapter 19 Log Management*.

Note: For the users with Pyronix control panel permissions, they can enter the Pyronix Control Panel module to manage the Pyronix control panel and real-time alarm. For setting the user permission of Pyronix Control Panel module, refer to *Chapter 20 Account Management*.

13.1 Device Management

Purpose:

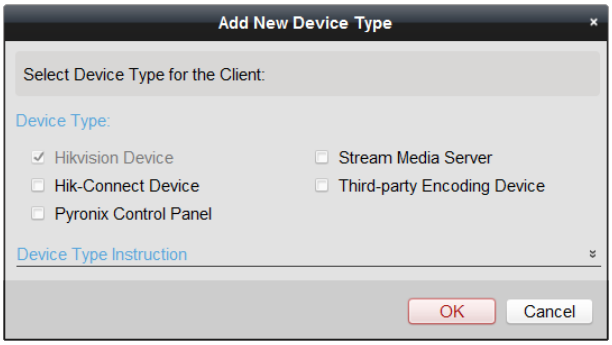
You can add the Pyronix control panel to the client in Device Management module. The device can be managed and controlled via the client once it is authorized by the device administrator on the PyronixCloud service.

13.1.1 Adding Pyronix Control Panel

Perform the following steps to add the Pyronix control panel.

Steps:

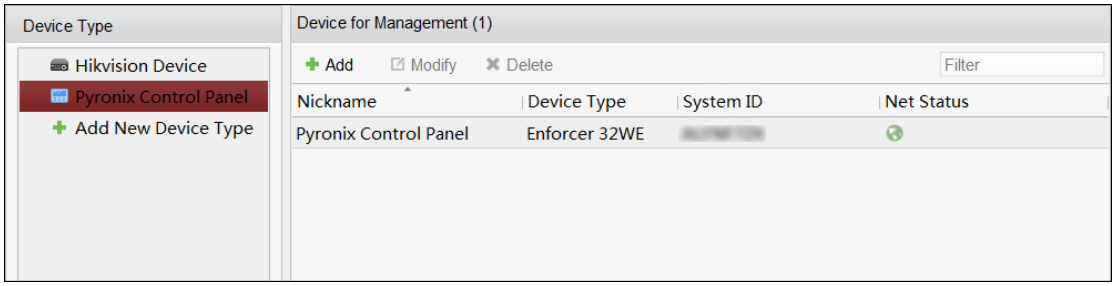
1. Click  icon on the control panel,
   or click **Tools**->**Device Management** to open the Device Management page.
2. Click **Device** tab.
3. Click **Add New Device Type** to pop up the following window box.



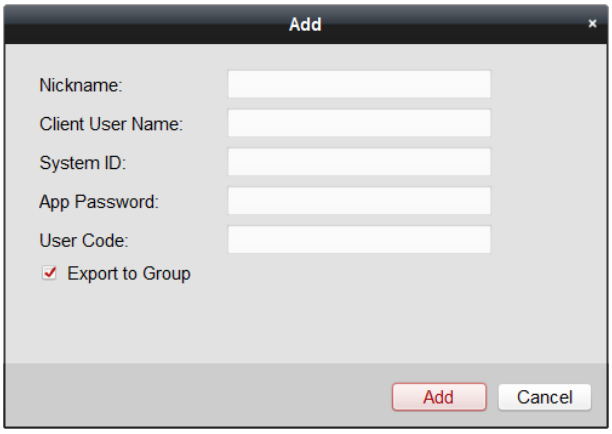
4. Check **Pyronix Control Panel** checkbox and click **OK**.

The Pyronix control panel will display in the device type panel.

5. Click **Pyronix Control Panel** to enter the Pyronix control panel management interface.



6. Click **Add**.
7. In the pop up window box, input the required information for adding a Pyronix control panel.



- **Nickname:** Set a nickname for the device as you want.
- **Client User Name:** Set the user name which is used for applying the permission from PyronixCloud.

  Note: See *Chapter 13.1.2 Authorizing iVMS-4200 via PyronixCloud* for details.
- **System ID:** The system ID of the Pyronix control panel. It is a unique serial number for each control panel.

  Note: You can get the control panel ID via the device. For details, refer to the specified device user manual.
- **App Password:** The password used to identify the control panel together with the ID on the user cloud account.

  Note: The App password should be set via the device. For details, refer to the specified device user manual.
- **User Code:** The code for every user with different priorities to arm/disarm the control panel and perform allowed operations.

  Note: You should set the user code via the device. For details about setting the user code, refer to the specified device user manual.

8. Optionally, check the **Export to Group** checkbox to create a group by the device name.
   You can import all the zones of the Pynonix control panel to the corresponding group by default.
9. Click **Add** to add the Pyronix control panel.
10. (Optional) To edit the device parameters, you can select the device and click **Modify**.
11. (Optional) To delete the added device, select the device and click **Delete**.

If it is the first time you add the Pyronix control panel to your client, after adding the Pyronix control panel, its network status is offline. You cannot manage and operate it via the control client until the administrator authorizes the client via the PyronixCloud.

What to do next: You should contact the administrator to authorize the client via the PyronixCloud. For details, refer to *Chapter 13.1.2 Authorizing iVMS-4200 via PyronixCloud.*

13.1.2 Authorizing iVMS-4200 via PyronixCloud

Purpose:

For the administrator, you need to login the PyronixCloud website to authorize the client so that the user can operate and control the Pyronix control panel via iVMS-4200.

Note: For one computer, you should ask for authorization if it is the same time adding the Pyronix control panel.

Creating PyronixCloud Account

Purpose:

Before you can authorize the phone, you need to register a PyronixCloud account and connect the Pyronix control panel to PyronixCloud.

Steps:

1. Go to www.pyronixcloud.com via PC to register an account.

2. Click **Create an account** and complete the form.

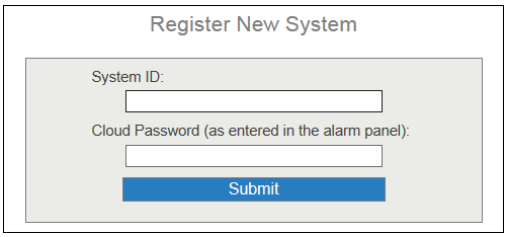
   Note: Once the form is completed, you will receive an email from admin@pyronixcloud.com with a confirmation link. Click this link and you can continue on to PyronixCloud and connect your device.

3. Return to PyronixClound home page and login.

Connecting Device to PyronixCloud

Steps:

1. Input the Pyronix control panel's system ID in the System ID field.



2. Input the cloud password that you entered in the Pyronix device.
3. Click **Submit**.
4. Input a system reference to set a different name for the device.
5. Click **Submit** to compete the operation.

Notes:

- The system ID is the device unique ID. You can get the system ID via the device. For details, refer to the specified device user manual.
- The cloud password should be set via the device. For details, refer to the specified device user manual.
- After clicking the Submit button, you will receive an email. Click the confirmation link in the email to continue.
- The control panel will be appeared on View Systems interface. You can click the tick at the upper-right corner of the interface to make sure the device is connected successfully.

Authorizing iVMS-4200

Steps:

1. In the View Systems interface, click a user in the User column and make sure the user is from the client that you want to authorize.

   Note: The user name in the User column is the client user name you input when adding the Pyronix control panel. See *Chapter 13.1.1 Adding Pyronix Control Panel for details*.
2. Click the permission icon  next to the selected user
3. Click **Save Now** to save the settings.

   The icon will turn to  .

   Then you can access the device via the client successfully.

13.2 Configuring Event

Purpose:

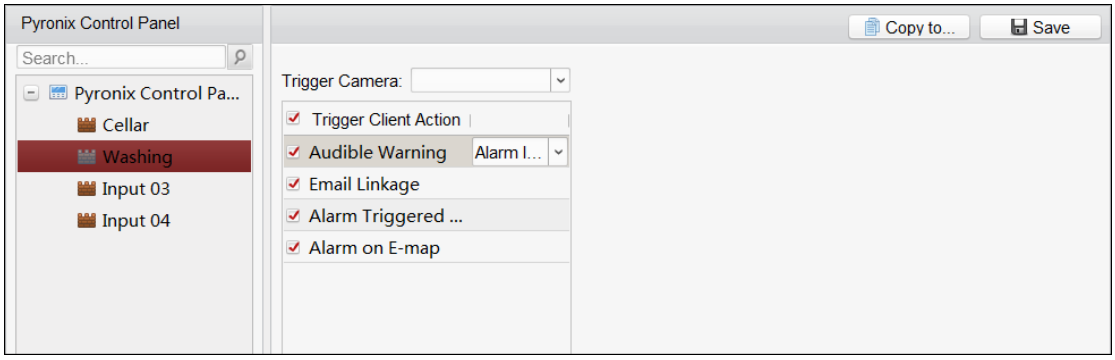
You can configure the client linkage and triggered cameras for the triggered events of Pyronix control panel's zones, or for the device event of Pyronix control panel.

Steps:

1. Click  on the Control Panel, or click **Tool** -> **Event Management** to open the Event

Management page.

2. Click **Pyronix Control Panel Event** tab.
   The added Pyronix control panel is displayed in the list on the left.
3. Click to unfold the zone list and select the zone icon to configure its zone event linkage. You can also click the Pyronix Control Panel's icon to configure its device event linkage.



4. In the Trigger Camera field, select the camera to be triggered for popping up image when the alarm is triggered.
   To capture the picture of the triggered camera when the selected event occurs, you should set the capture schedule and the storage in Storage Schedule. For details, refer to *Chapter 5.1 Remote Storage.*
   Note: Up to one camera can be set as the triggered camera.
5. Check **Trigger Client Action** checkbox to activate the client linkage actions.
   You can check the detailed actions as the client linkage. See the detailed actions below for details:

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, refer to *Chapter 22.7 Alarm Sound Settings.*
Email Linkage	Send an email notification of the alarm information to one or more receivers.
Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered. ***Note:*** You should set the triggered camera first.
Alarm on E-map	Display the zone's alarm information on the E-map. ***Note:*** This linkage is only available for device event.

6. Optionally, click **Copy to…** to copy the event settings to other zones.
7. Click **Save** to save the settings.

13.3 Remote Control

Purpose:

In this section, you can control the Pyronix control panel remotely to perform operations such as arming, disarming, bypass, bypass recovery, and so on for partitions and zones. You can also control the alarm output connected to the Pyronix control panel.

Note: You can control the Pyronix control panel remotely after you switch the device to operation

mode.

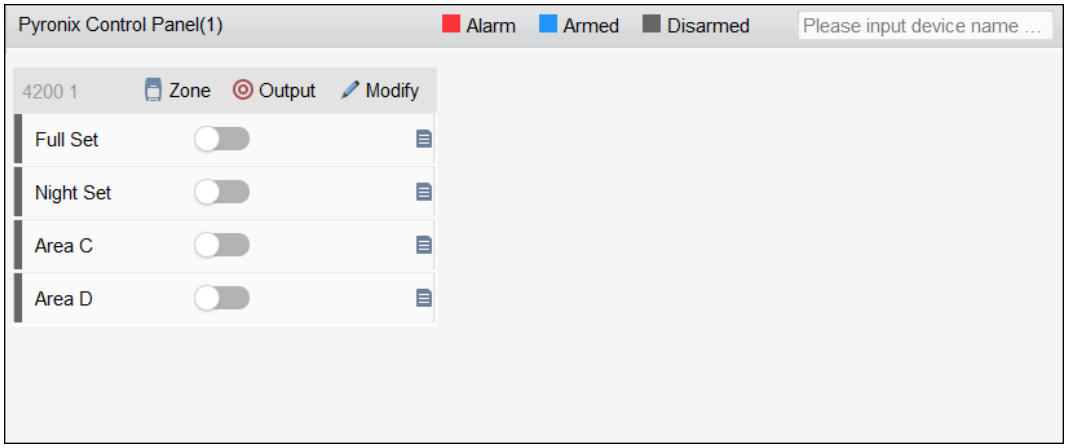
13.3.1 Partition Remote Control

Purpose:

You can arm and disarm the partition of the added Pyronix control panel. The status of the partitions will be displayed in real-time.

Steps:

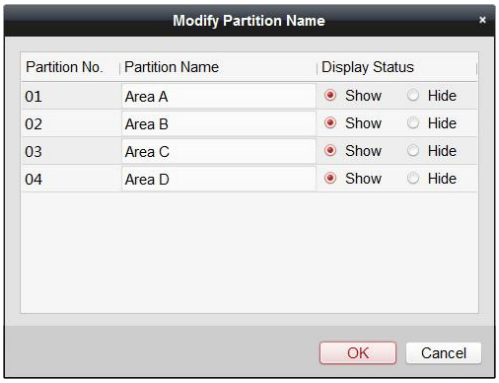
1. Click  on the Control Panel, or click **View->Pyronix Control Panel** to open the Pyronix Control Panel page as follows.



All the added Pyronix control panels and partitions will be displayed.

Note: The device name will turn grey if it is offline.

2. (Optional) If the partition is in fault status, an  icon will display near the partition name. You can hover the  icon to view the fault details.
3. (Optional) Click **Modify** to edit the partition name as you want and change the partition display status as show or hide.



4. Click on the switch of each partition to arm or disarm the partition.
5. (Optional) Hover over the  to view the last operation.

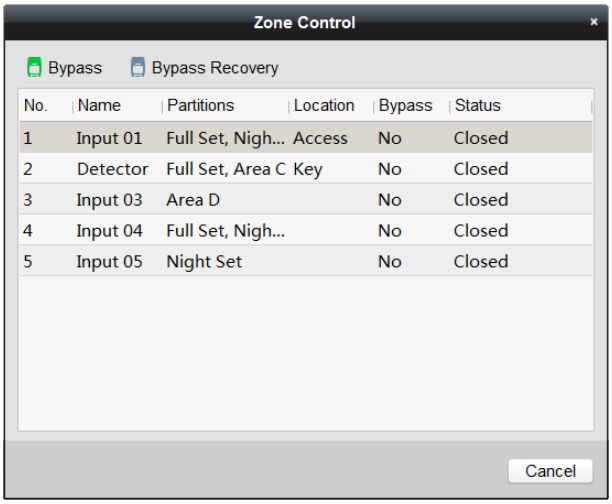
13.3.2 Control Zone Remotely

Purpose:

You can view the zone real-time status of the added Pyronix control panel and perform bypass and bypass recovery operations to control the zone.

Steps:

1. Click **Zone** to enter the zone control interface as follows.



   The zones will be displayed.

   You can view the zone details including name, linked partitions, and its location.

   The zone's bypass status and running status are displayed in real-time.

2. To bypass the zone, select the zone and click **Bypass**.

   To recover the bypass, select the zone and click **Bypass Recovery**.

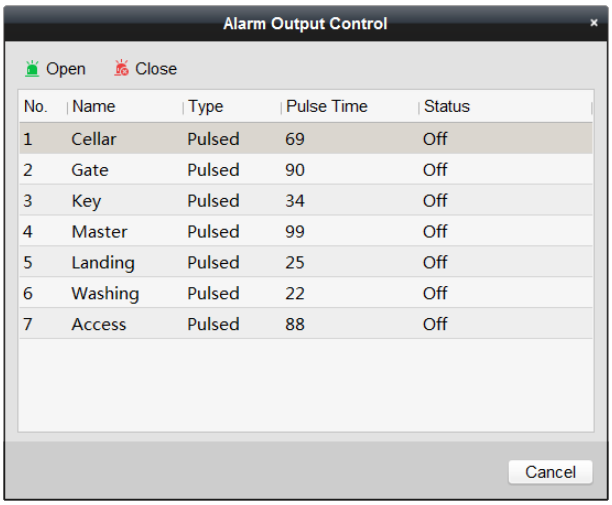
13.3.3 Control Alarm Output Remotely

Purpose:

When the Pyronix control panel is connected with alarm outputs, such as siren, alarm lamp, etc., you can also control the alarm output status.

Steps:

1. Click **Output** to enter the alarm output control interface as follows.



   Its connected alarm outputs will be displayed.

   You can view the alarm output details including No., name, type, and pulse duration.

   The alarm output's running status is displayed in real-time.

2. To turn on the alarm output, select the alarm output and click **Open**.
   The countdown will start in pulse time. When the countdown finishes, the output status will turn to **Off** automatically.
3. To turn off the alarm output, select the alarm output and click **Close**.

Chapter 14 Access Control

Purpose:

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

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

Note: For the user with access control module permissions, the user can enter the Access Control module and configure the access control settings. For setting the user permission of Access Control module, refer to *Chapter 20 Account Management*.

Click  to enter the Access Control Module.

Before you start:

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

You can select the scene as **Non-residence** and **Residence**.

Notes:

- Once the scene is configured, you cannot change it later.
- When you select **Non-Residence** mode, you cannot configure the Attendance Rule when adding person.

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

	**Person and Card**	Managing the organizations, persons, and assigning cards to persons.
	**Schedule and Template**	Configuring the week schedule, holiday group, and setting the template.
	**Permission**	Assigning access control permissions to persons and applying to the devices.
	**Advanced Function**	Providing advanced functions including access control parameters settings, card reader authentication, opening door with first card, anti-passing back, multi-door interlocking, and authentication password.

	Video Intercom	Video intercom between client and resident, searching the dial log, and releasing notice.
	Search	Searching history events of access control; Searching call logs, unlocking logs, and released notices.
	Device Management	Managing the access control devices and video intercom devices.

Note: In this chapter, we only introduce the operations about access control. For detailed operations about video intercom, refer to *Chapter 16 Video Intercom.*

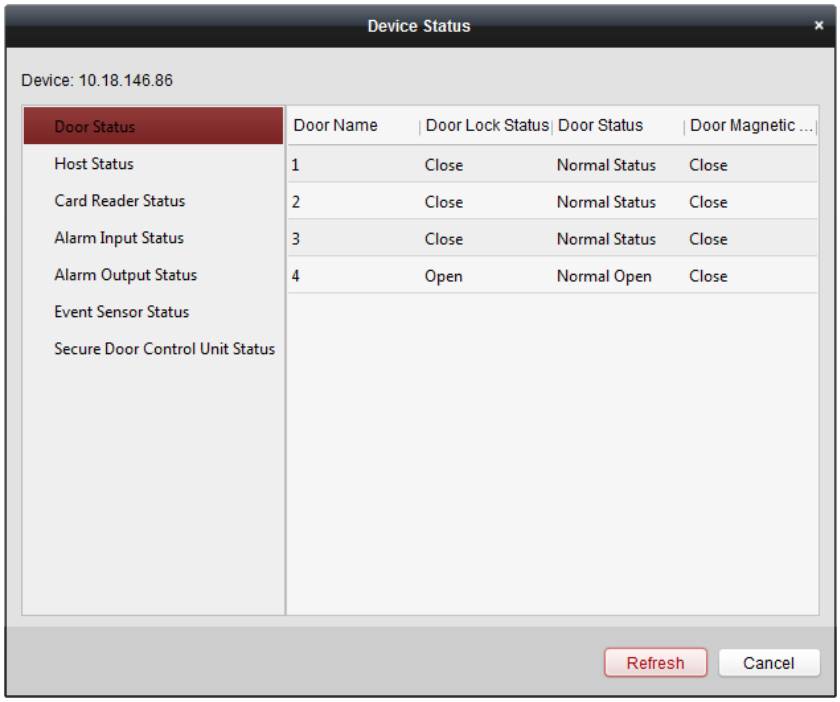
14.1 Access Control Device Management

Before you start:

You can add and manage the access control devices in **Device Management**, or in **Access Control -> Device Management** module. For details about adding device, refer to *Chapter 3.1 Adding Device*.

14.1.1 Viewing Device Status

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



- **Door (Floor) Status**: The status of the connected door (floor).
- **Distributed Elevator Controller Status:** The distributed elevator controller status and its tamper-proof status.
- **Host Status**: The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, and Host Anti-Tamper Status.
- **Card Reader Status**: The status of card reader.
- **Alarm Input Status**: The alarm input status of each port.

- **Alarm Output Status**: The alarm output status of each port.
- **Event Sensor Status**: The event sensor status of each port.
- **Secure Door Control Unit Status:** The online status and tamper status of the Secure Door Control Unit.
- **Arming Status:** The arming status of the device.

You can click **Refresh** to get the latest device status.

14.1.2 Network Settings

Purpose:

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

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

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

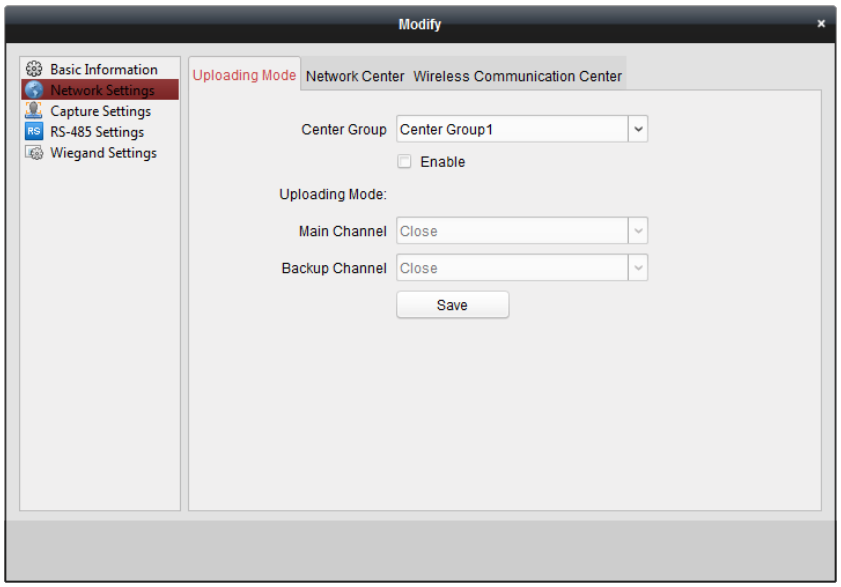
Log Uploading Mode Settings

Purpose:

You can set the mode for uploading logs via EHome protocol.

Steps:

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



2. Select the center group in the dropdown list.
3. Check the **Enable** checkbox to enable the selected center group.
4. Select the uploading mode in the dropdown list. You can enable **N1/G1** for the main channel and the backup channel, or select **Close** to disable the main channel or the backup channel.

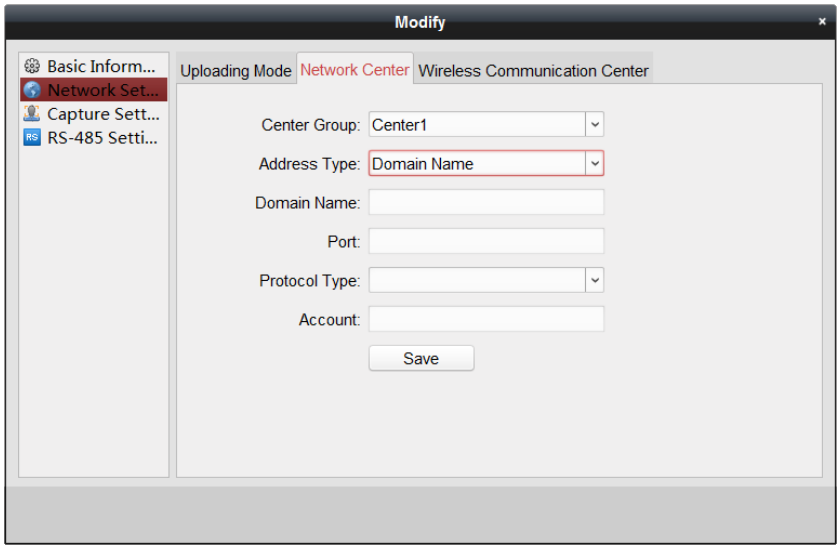
   Note: The main channel and the backup channel cannot enable N1 or G1 at the same time.
5. Click **Save** button to save parameters.

Network Center Settings

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

Steps:

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



2. Select the center group in the dropdown list.
3. Select the Address Type as **IP Address** or **Domain Name.**
4. Input IP address or domain name according to the address type.
5. Input the port No. for the protocol.
6. Select the protocol type as EHome.
7. Set an account name for the network center.

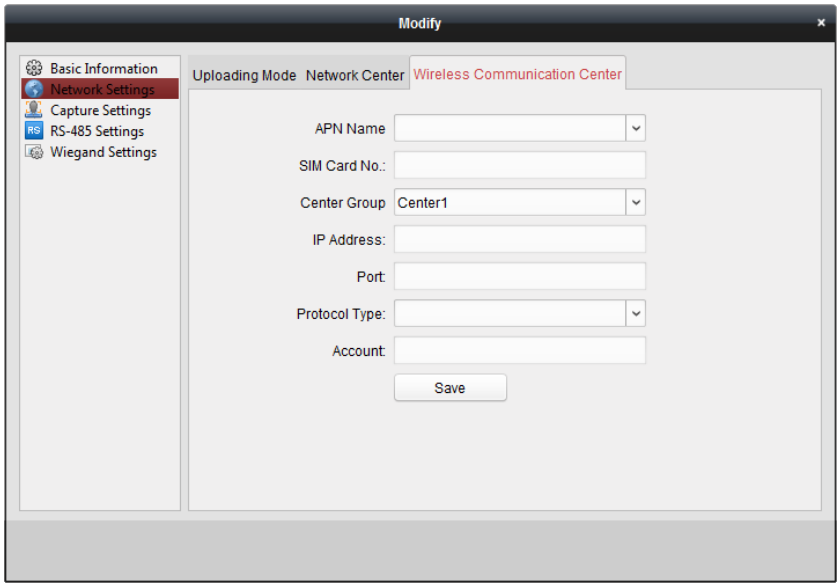
   Note: The account should contain 1 to 32 characters and only letters and numbers are allowed.
8. Click **Save** button to save parameters.

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

Wireless Communication Center Settings

Steps:

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



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

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

14.1.3 Capture Settings

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

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

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

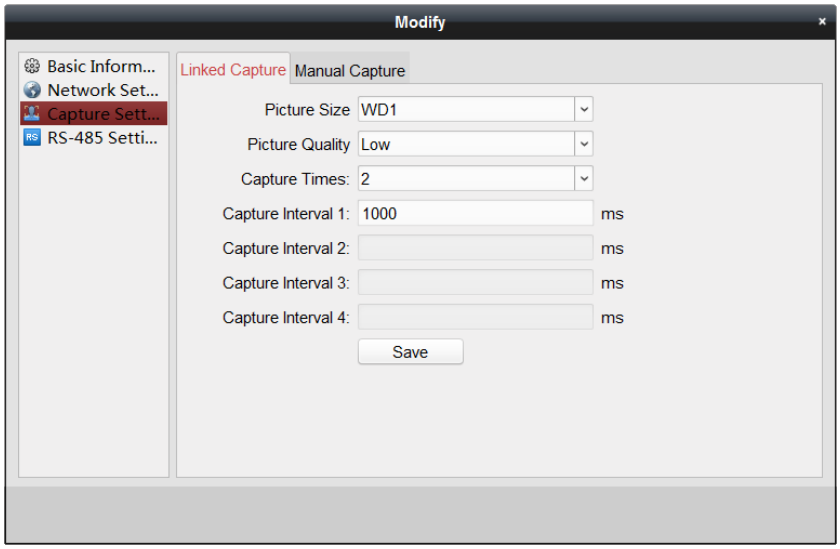
Notes:

- The **Capture Settings** should be supported by the device.
- Before setting the capture setting, you should configure the Storage Server for picture storage. For details, refer to *Chapter 5.1 Remote Storage.*

Linked Capture

Steps:

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

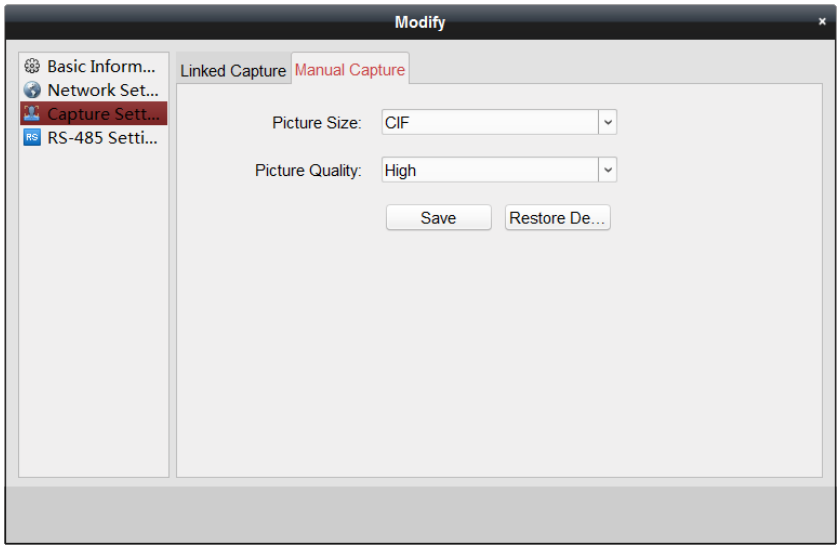


2. Set the picture size and quality.
3. Set the linked capture times once triggered.
4. Set the capture interval according to the capture times.
5. Click **Save** to save the settings.

Manual Capture

Steps:

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



2. Select the resolution of the captured pictures from the dropdown list.

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

14.1.4 RS-485 Settings

Purpose:

You can set the RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

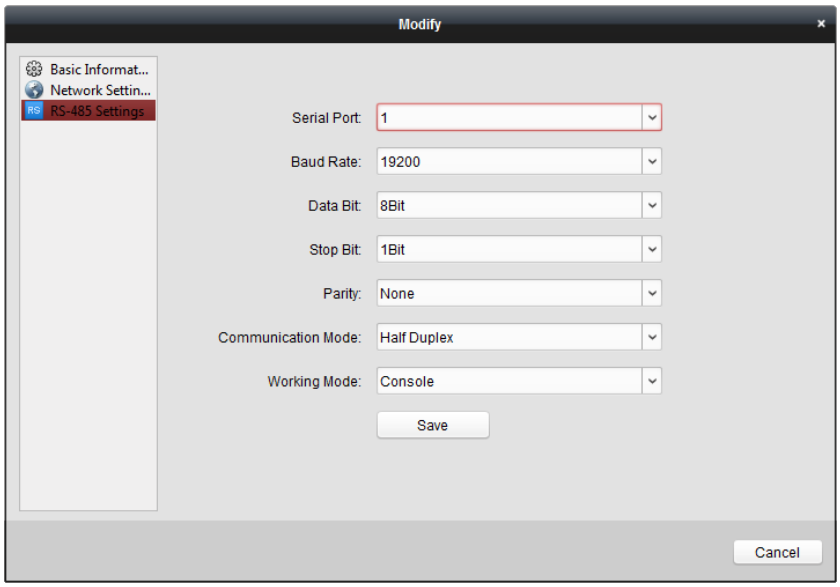
Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **RS-485 Settings** tab to enter the RS-485 settings interface.

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

Steps:

1. Click **RS-485 Settings** tab to enter the RS-485 settings interface.



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

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

14.1.5 Wiegand Settings

Purpose:

You can set the Wiegand channel and the communication mode.

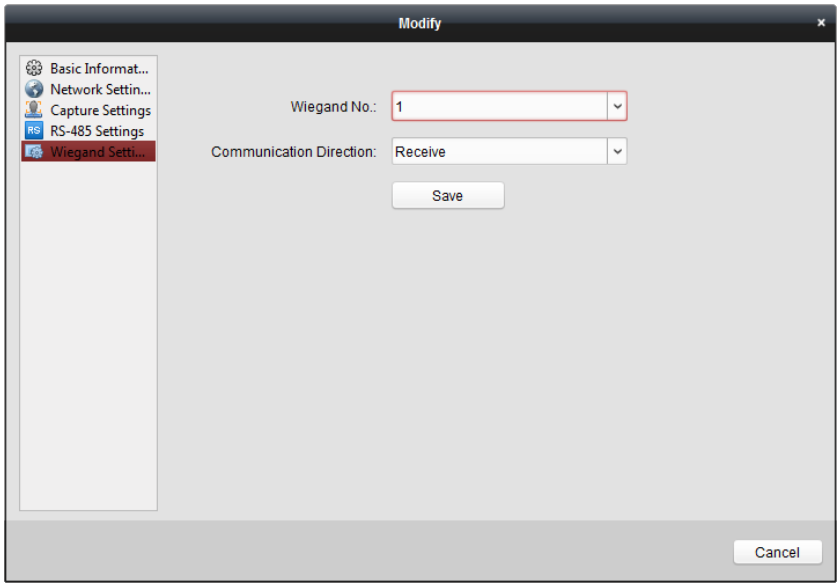
Select the device in the device list, and click **Modify** to pop up the modifying device information window.

Click **Wiegand-485 Settings** tab to enter the Wiegand settings interface.

Note: The Wiegand Settings should be supported by the device.

Steps:

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



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

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

14.1.6 Authenticating M1 Card Encryption

Before you start:

You should use the specified Hikvision card enrollment station to issue card. For details, refer to *Adding Person (General* Card).

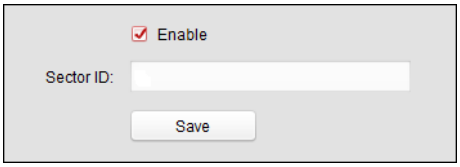
Purpose:

M1 card encryption can improve the authentication security level. After issuing the card, you can enable the M1 card encryption function in the client software.

Note: The function should be supported by the access control device and the card reader.

Steps:

1. Select the device in the device list, and click **Modify** to pop up the modifying device information window.
2. Click **M1 Card Encryption** tab to enter the M1 Card Encryption interface.
3. In the M1 Card Encryption interface, check **Enable** checkbox to enable the M1 card encryption function.



4. Set the sector ID.
5. Click **Save** to save the settings.
   Note: The Sector ID ranges from 1 to 100.

14.2 Organization Management

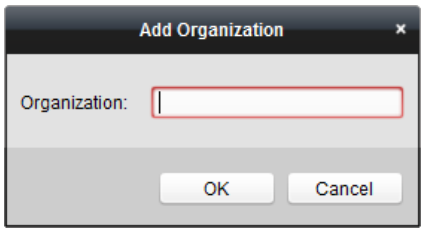
Purpose:

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

14.2.1 Adding Organization

Steps:

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



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

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

14.2.2 Modifying and Deleting Organization

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

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

Notes:

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

14.3 Person Management

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

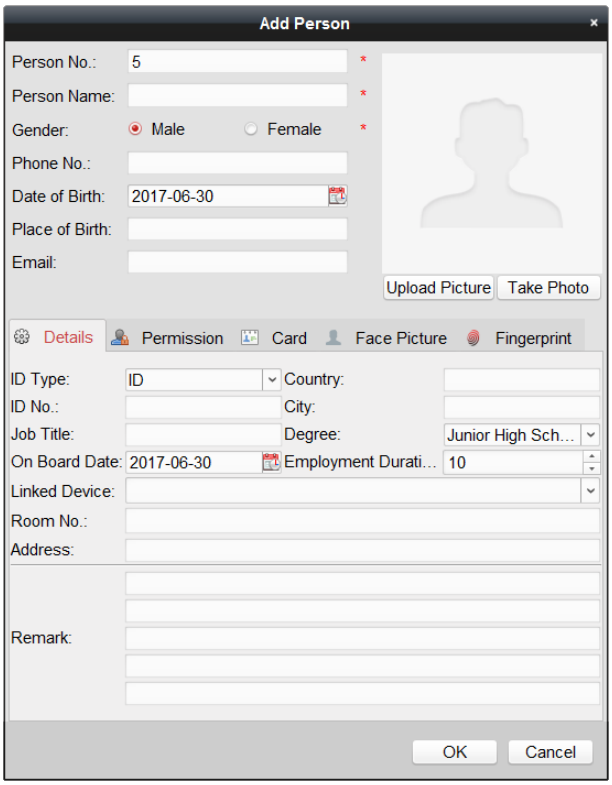
Note: Up to 10,000 persons or cards can be added.

14.3.1 Adding Person

Adding Person (Basic Information)

Steps:

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

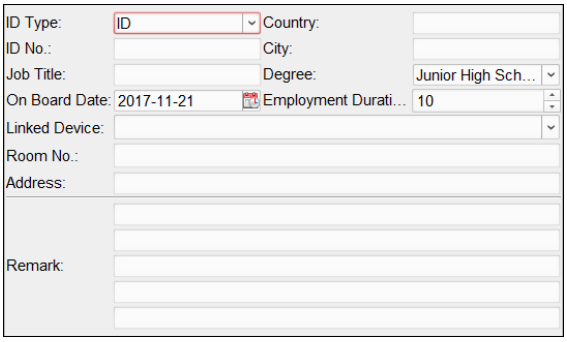


2. The Person No. will be generated automatically and is not editable.
3. Input the basic information including person name, gender, phone No., birthday details, and email address.
4. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
   Note: The picture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

Adding Person (Detailed Information)

Steps:

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



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

     Note: If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.
   - **Room No.:** You can input the room No. of the person.
3. Click **OK** to save the settings.

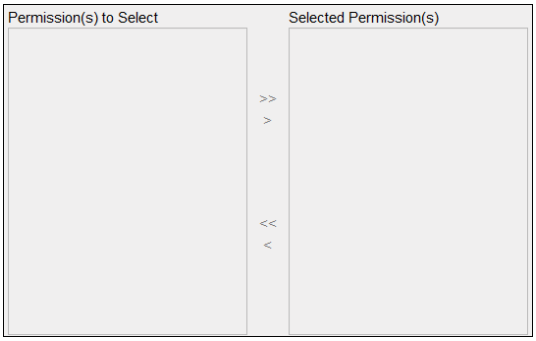
Adding Person (Permission)

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

Note: For setting the access control permission, refer to *Chapter 14.5 Permission Configuration.*

Steps:

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



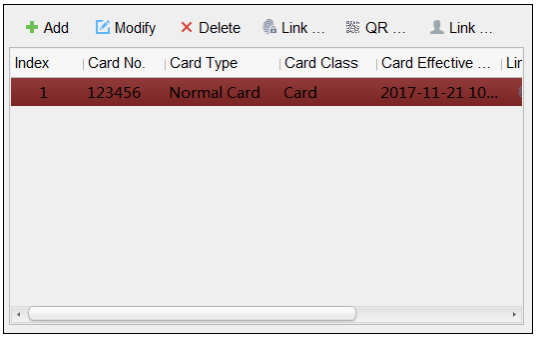
   In the Permission(s) to Select list, all the configured permissions display.
2. Check the permission(s) checkbox(es) and click **>** to add to the Selected Permission(s) list.
3. Click **OK** to save the settings.

Adding Person (General Card)

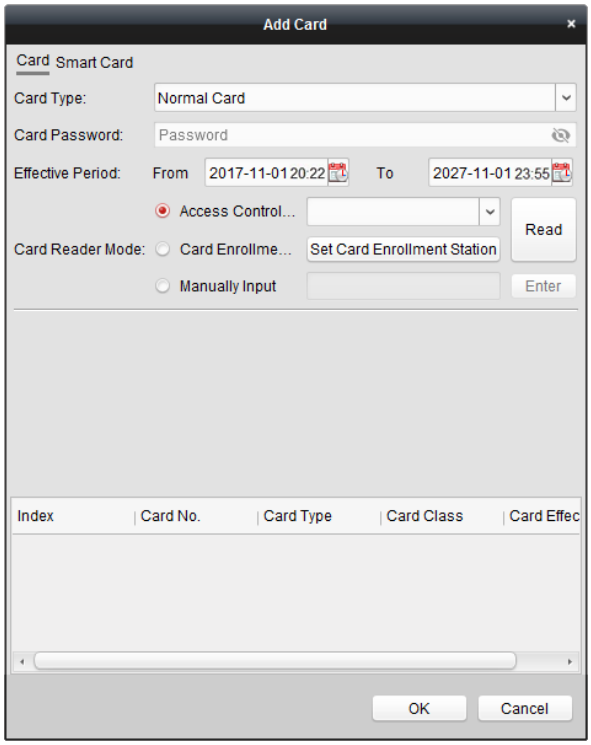
You can add card and issue the card to the person.

Steps:

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



2. Click **Add** to pop up the Add Card window.
3. Click **Card** to enter the Card tab.



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

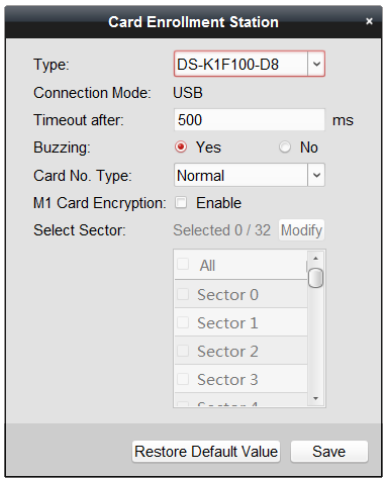
     Note: The Max. Swipe Times should be between 0 and 255. When setting as 0, it means the card swiping is unlimited.
   - **Dismiss Card:** The card can stop the buzzer of the card reader.
5. Input the password of the card itself in the Card Password field. The card password should

contain 4 to 8 digits.

Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, *Chapter 14.6.2 Card Reader Authentication.*

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

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



     1) Select the Card Enrollment Station type.

        Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

     2) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.

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

        Note: The M1 Card Encryption function is supported by DS-K1F100-D8, DS-K1F100-D8E, and DS-K1F180-D8E.

     4) Click **Save** button to save the settings.
   - **Manually Input:** Input the card No. and click **Enter** to input the card No.
8. Click **OK** and the card(s) will be issued to the person.
9. (Optional) You can generate and save the card QR code for QR code authentication.

   1) Select an added card and click **QR Code** to generate the card QR code.

   2) In the QR code pop-up window, click **Download** to save the QR code to the local PC.

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

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

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

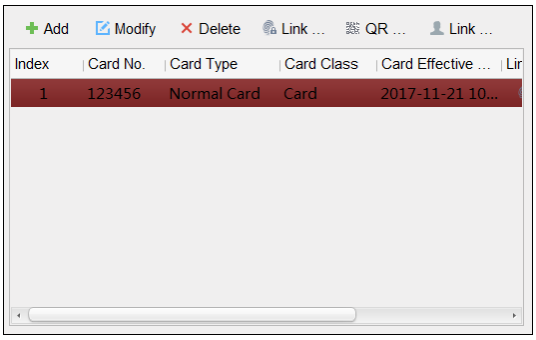
Adding Person (Smart Card)

Purpose:

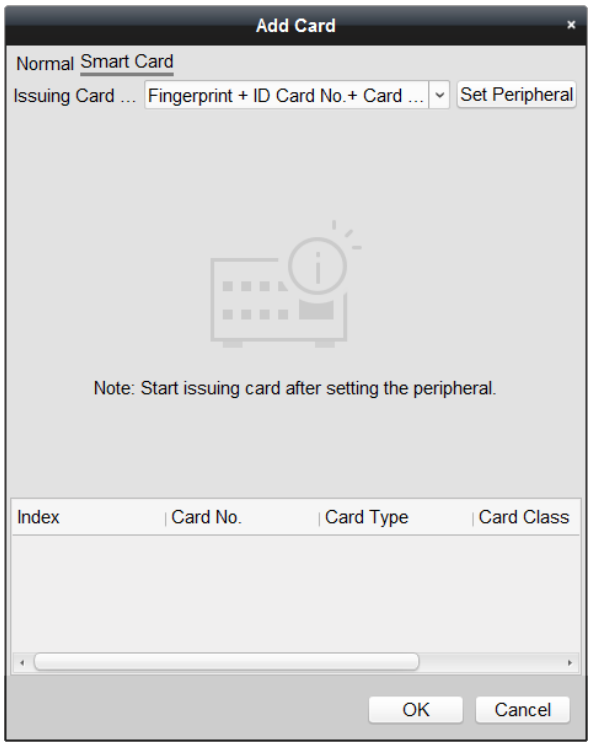
You can store fingerprints and ID card infomration in the smart card. When authenticating, after swiping the smart card on the device, you can scan your fingerprint or swipe your ID card on the device. The device will compare the fingerperint or ID card information in the smart card with the ones collected. If you use the smart card for authentication, there is no need to store the fingerprints or ID card information in the device in advance.

Steps:

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



2. Click **Add** to pop up the Add Card window.
3. Click **Smart Card** to enter the Smart Card tab.



4. Select an issuing card mode from the dropdown list.
5. Set the external device.
   1) Click **Set Peripheral** to enter the Set Peripheral page.
   2) (Optional) Select the issuing card mode again.
   3) Set a card enrollment station.
   4) If you select "Fingerprint + Card No." as the issuing mode, set the fingerprint recorder model.
      If you select "ID Card No. + Card No." as the issuing mode, set the ID card reader model.
      If you select "Fingerprint + ID Card No. + Card No." as the issuing mode, set the fingerprint recorder model and the ID card reader model.
   5) Click **OK** save the settings.
6. Select a card type for the smart card.
   - **Card for Disabled Person**: The door will remain open for the configured time period for the card holder.
   - **Card in Blacklist:** The card swiping action will be uploaded and the door cannot be opened.
   - **Patrol Card:** The card swiping action can used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
   - **Duress Card:** The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.
   - **Super Card:** The card is valid for all the doors of the controller during the configured schedule.
   - **Visitor Card:** The card is assigned for visitors. For the Visitor Card, you can set the Max. Swipe Times.
     Note: The Max. Swipe Times should be between 0 and 255. When setting as 0, it means the card swiping is unlimited.
   - **Dismiss Card:** The card can stop the buzzer of the card reader.
7. Set other parameters of the card.
   1) Set the card password.
   2) Set the card effective date.
   3) Scan your fingerprint and swipe your ID card according to the promt.
   4) Swipe the smart card.
      The added card information will display in the list below.
8. Click **OK** and the card(s) will be issued to the person.
9. (Optional) Generate and save the card QR code for QR code authentication.
   1) Select an added card and click **QR Code** to generate the card QR code.
   2) In the QR code pop-up window, click **Download** to save the QR code to the local PC.
      You can print the QR code for authentication on the specified device.
      Note: The device should support the QR code authentication function. For details about setting the QR code authentication function, see the specified device user manual.
10. (Optional) Click **Link Fingerprint** to link the card with the person's fingerprint, so that the person can place the finger on the scanner instead of swiping card when passing the door.
11. (Optional) Click **Link Face Picture** to link the card with the face picture, so that the person can pass the door by scanning the face via the device instead of swiping card when passing the door.

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

Adding Person (Face Picture)

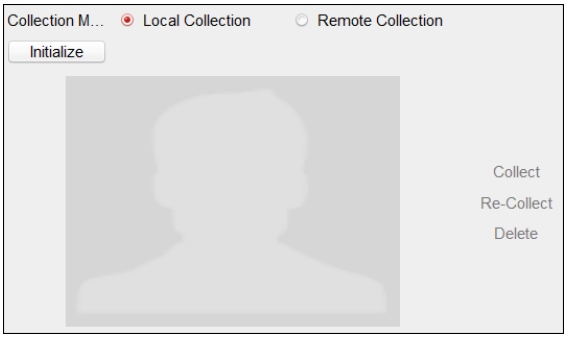
You can collect the face picture in two ways: Local Collection and Remote Collection.

- **Local Collection:** Collect the face picture via face picture scanner.
- **Remote Collection:** Collect the face picture via the access control terminal.

  Note: The access control terminal should support face recognition function.

Steps:

1. In the Add Person interface, click **Face Picture** tab



2. To get the face picture via face picture scanner:
   1) Select **Local Collection**.
   2) Connect the face picture scanner to the PC running the client.
   3) (Optional) You can click **Initialize** to initialize the face picture scanner.
3. To get the face picture via access control terminal:
   1) Select **Remote Collection**.
   2) Click **Select Device** to select the access control terminal which supports face recognition function.
4. Click **Collect** to capture the face picture.

   You can click **Re-Collect** the captured picture again.

   You can click **Delete** to delete the captured picture.
5. Click **OK** to save the settings.

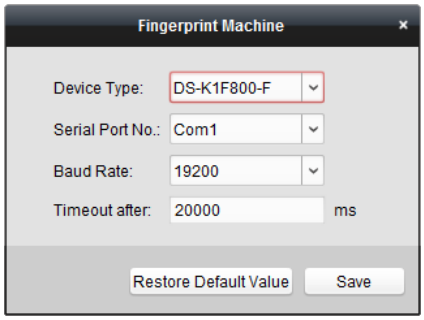
Adding Person (Fingerprint)

Steps:

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

2. Select **Local Collection** as desired.
3. Before inputting the fingerprint, you should connect the fingerprint machine to the PC and set its parameters first.

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



   1) Select the device type.

      Currently, the supported fingerprint machine types include DS-K1F800-F, DS-K1F300-F, DS-K1F810-F, and DS-K1F820-F.

   2) For fingerprint machine type DS-K1F800-F, you can set the serial port number, baud rate, and overtime parameters of the fingerprint machine.

      Notes:

      - The serial port number should correspond to the serial port number of PC.
      - The baud rate should be set according to the external fingerprint card reader. The default value is 19200.
      - **Timeout after** field refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that the fingerprint collecting is over.

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

   Note: The function should be supported by the device.
7. Click **OK** to save the fingerprints.

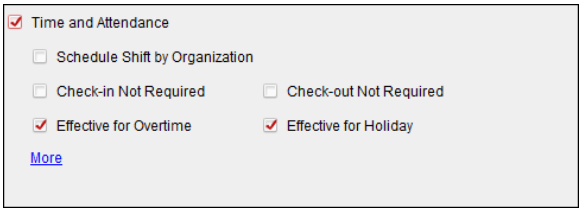
Adding Person (Attendance Rule)

You can set the attendance rule for the person.

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

Steps:

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



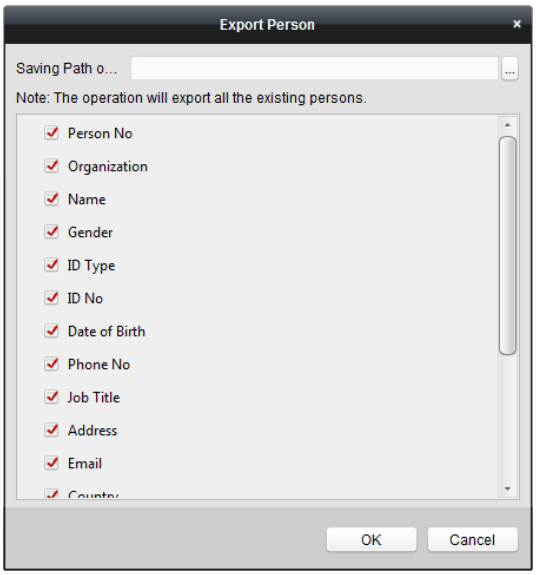
2. If the person joins in the time and attendance, check the **Time and Attendance** checkbox to enable this function for the person. Then the person's card swiping records will be recorded and analyzed for time and attendance.
   For details about Time and Attendance, click **More** to go to the Time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

Importing and Exporting Person Information

The person information can be imported and exported in batch.

Steps:

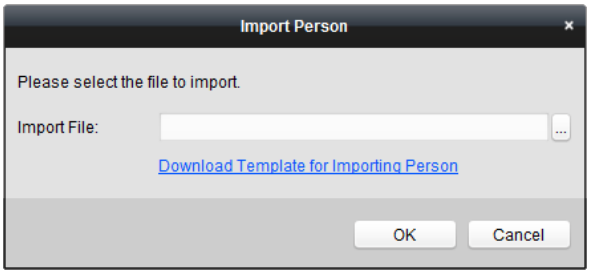
1. **Exporting Person:** You can export the added persons' information in Excel format to the local PC.
   1) After adding the person, you can click **Export Person** button to pop up the following window.
   2) Click ... to select the path of saving the exported Excel file.
   3) Check the checkboxes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



   4) Click **OK** to start exporting.
2. **Importing Person:** You can import the Excel file with persons information in batch from the local

PC.

1) click **Import Person** button.



2) You can click **Download Template for Importing Person** to download the template first.
3) Input the person information in the downloaded template.
   Note: If the person has multiple cards, separate the card No. with semicolon.
4) Click ... to select the Excel file with person information.
5) Click **OK** to start importing.

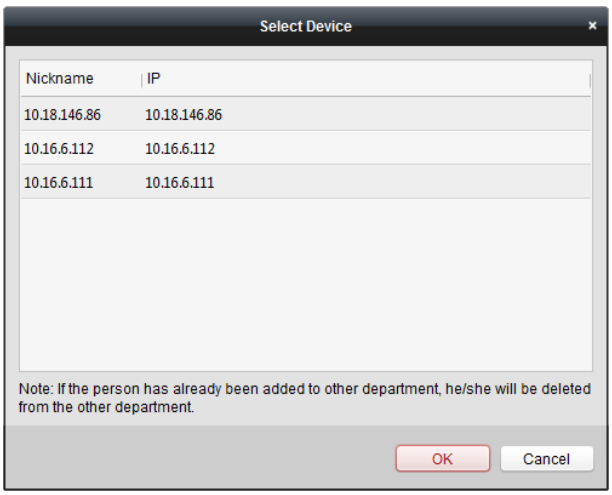
Getting Person Information from Access Control Device

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

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

Steps:

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



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

Notes:

- The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
- If the person name stored in the device is empty, the person name will be filled with the issued

card No. after importing to the client.

- The gender of the persons will be **Male** by default.

14.3.2 Managing Person

Modifying and Deleting Person

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

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

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

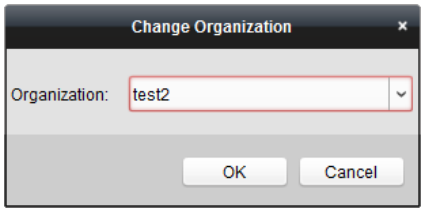
Note: If a card is issued to the current person, the linkage will be invalid after the person is deleted.

Changing Person to Other Organization

You can move the person to another organization if needed.

Steps:

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



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

Searching Person

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

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

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

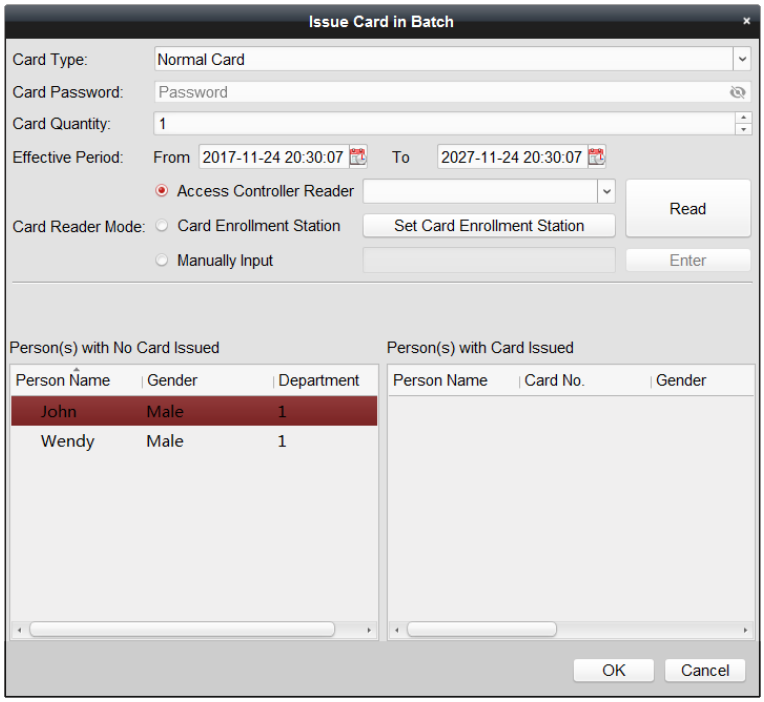
14.3.3 Issuing Cards in Batch

You can issue multiple cards to one person in batch.

Steps:

1. Click **Issue Card in Batch** button to enter the following window.

   All the added person with no card issued will display in the Person(s) with No Card Issued list.



2. Select the card type according to actual needs.

   Note: For details about the card type, refer to *Adding Person (General* Card).

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

   Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, refer to *Chapter 14.6.2 Card Reader Authentication.*

4. Input the card quantity issued for each person.

   For example, if the card quantity is 3, you can read or enter three card numbers for each person.

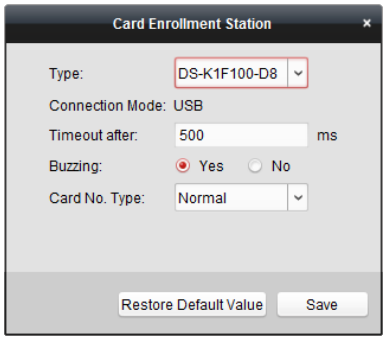
5. Click to set the effective time and expiry time of the card.

6. In the Person(s) with No Card Issued list on the left, select the person to issue card.

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

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

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



1) Select the Card Enrollment Station type.

   Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

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

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

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

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

14.4 Schedule and Template

Purpose:

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

Click  to enter the schedule and template interface.

You can manage the schedule of access control permission including Week Schedule, Holiday Schedule, and Template. For permission settings, refer to *Chapter 14.5 Permission Configuration.*

14.4.1 Week Schedule

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

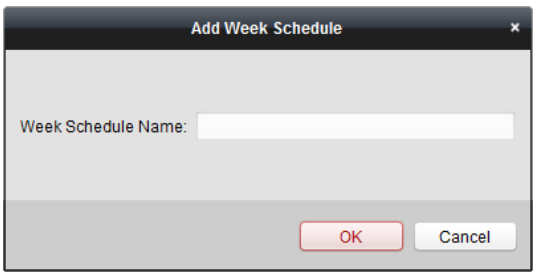
The client defines two kinds of week plan by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

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

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

Steps:

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



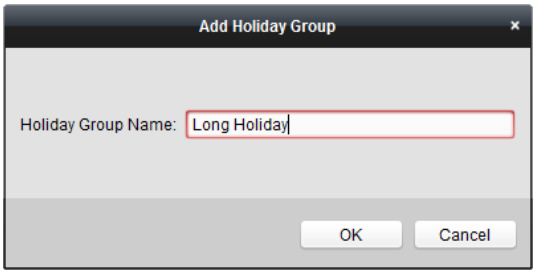
2. Input the name of week schedule and click **OK** button to add the week schedule.
3. Select the added week schedule in the schedule list and you can view its property on the right. You can edit the week schedule name and input the remark information.
4. On the week schedule, click and drag on a day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

14.4.2 Holiday Group

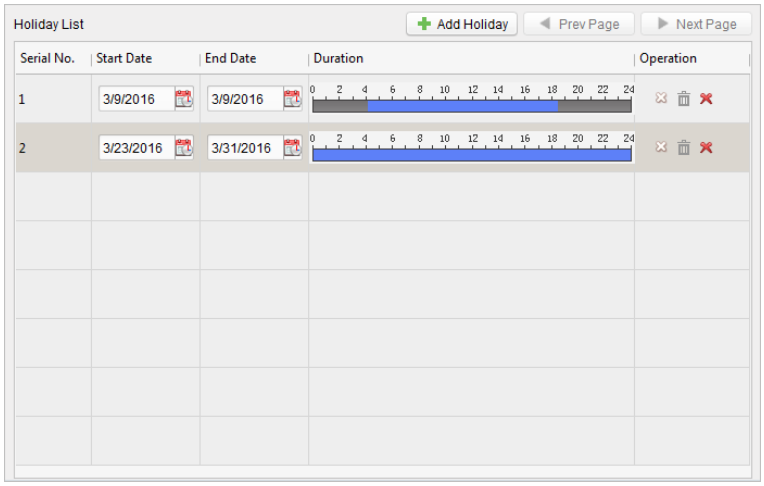
Click **Holiday Group** tab to enter the Holiday Group Management interface.

Steps:

1. Click **Add Holiday Group** button on the left to open the adding holiday group window.



2. Input the name of holiday group in the text filed and click **OK** button to add the holiday group.
3. Click **Add Holiday** icon on the right to add a holiday period to the holiday group and configure the duration of the holiday.
   Note: Up to 16 holiday periods can be added to one holiday group.



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

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

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

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

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

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

Note: The holidays cannot be overlapped with each other.

14.4.3 Template

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

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

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

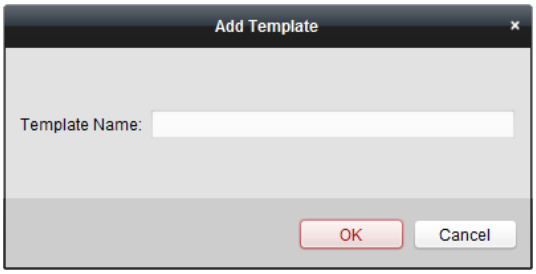
There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

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

You can define custom templates on your demand.

Steps:

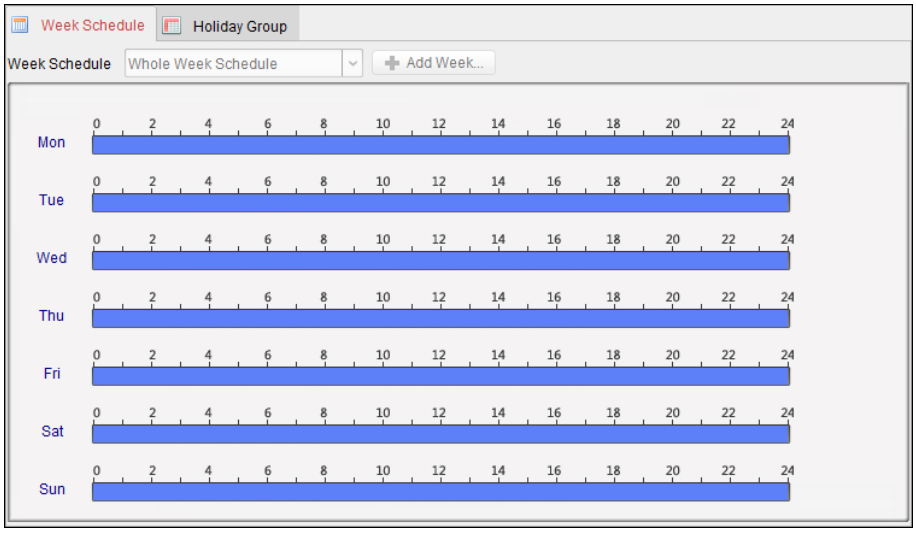
1. Click **Add Template** to pop up the adding template interface.



2. Input the template name in the text filed and click **OK** button to add the template.
3. Select the added template and you can edit its property on the right. You can edit the template name and input the remark information.
4. Select a week schedule to apply to the schedule.

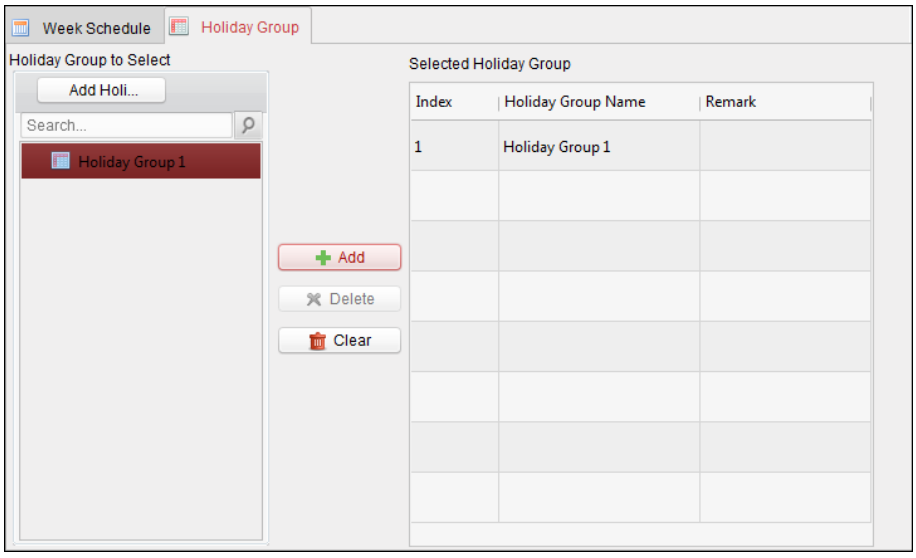
   Click **Week Schedule** tab and select a schedule in the dropdown list.

   You can also click **Add Week Schedule** to add a new week schedule. For details, refer to *Chapter 14.4.1 Week Schedule.*



5. Select holiday groups to apply to the schedule.

   Note: Up to 4 holiday groups can be added.



Click to select a holiday group in the list and click **Add** to add it to the template. You can also

click **Add Holiday Group** to add a new one. For details, refer to *Chapter 14.4.2 Holiday Group.*

You can click to select an added holiday group in the right-side list and click **Delete** to delete it.

You can click **Clear** to delete all the added holiday groups.

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

14.5 Permission Configuration

Purpose:

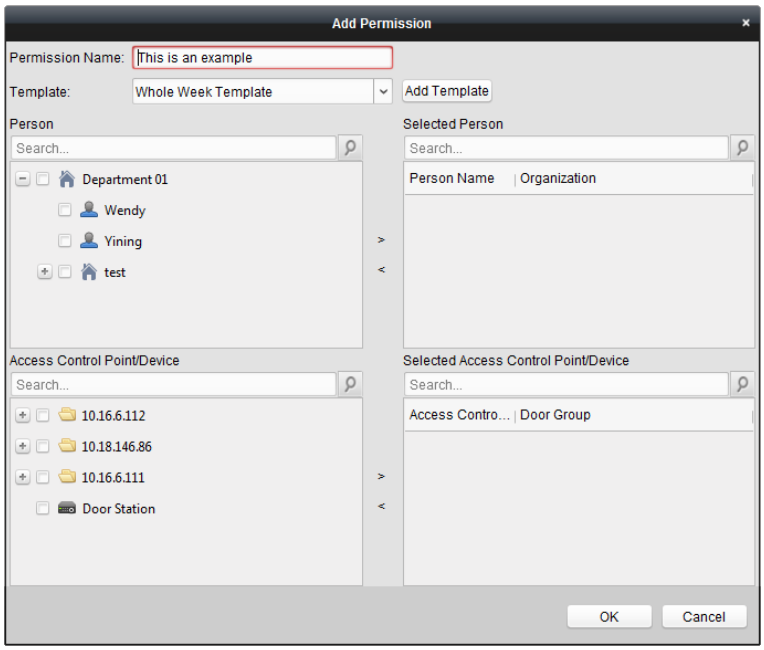
You can assign permission for persons to enter/exist the access control points (doors) in this section.

Notes:

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

Steps:

1. Click  icon to enter the Access Control Permission interface.
2. Click **Add** icon to enter following interface.



3. In the Permission Name field, create a name for the permission as you want.
4. Click on the dropdown menu to select a template for the permission.

   Note: You should configure the template before permission settings. You can click **Add Template** button to add the template. Refer to *Chapter 14.4 Schedule and Template* for details.
5. Select person(s) in the Person list and click **>** to add to the Selected Person list.
6. Select door(s) or door station(s) in the Access Control Point/Device list and click **>** to add to the selected list.
7. Click **OK**.

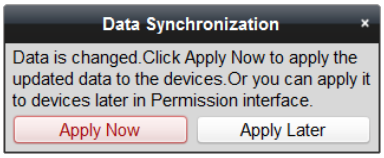
   The selected person will have the permission to enter/exit the selected door/door station with their linked card(s) or fingerprints.
8. (Optional) after adding the permission, you can click **Details** to modify it. Or you can select the permission and click **Modify** to modify.

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

9. After configuring the permissions, you should apply the added permission parameters (including relevant person details, related access control points, etc.) to the access control device to take effect.
   1) Select the permission(s) to apply to the access control device.
      To select multiple permissions, you can hold the *Ctrl* or *Shift* key and select permissions.
   2) Click **Apply All** to start applying all the selected permission(s) to the access control device or door station.
      You can also click **Apply Changes** to apply the changed part of the selected permission(s) to the device(s).

Notes:

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



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

14.6 Advanced Functions

Purpose:

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

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

Click  icon.

14.6.1 Access Control Parameters

Purpose:

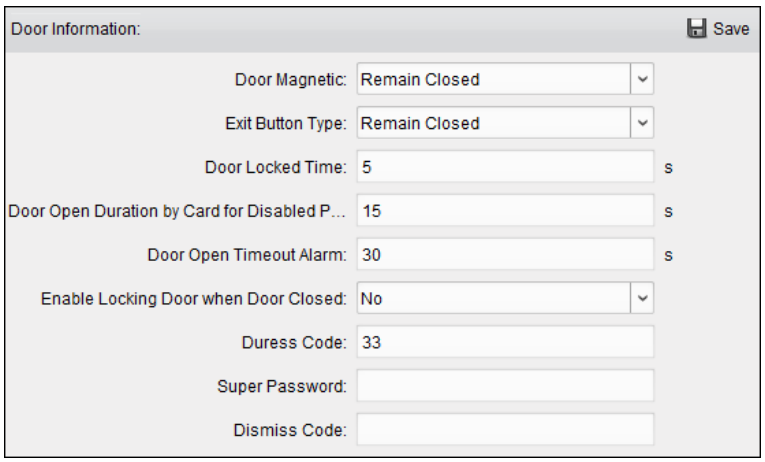
After adding the access control device, you can configure its access control point (door or floor)'s parameters, and its card readers' parameters.

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

Configuring Door (Floor) Parameters

Steps:

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



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

     Notes:

     ✧ The duress code, Super password, and dismiss code should be different.

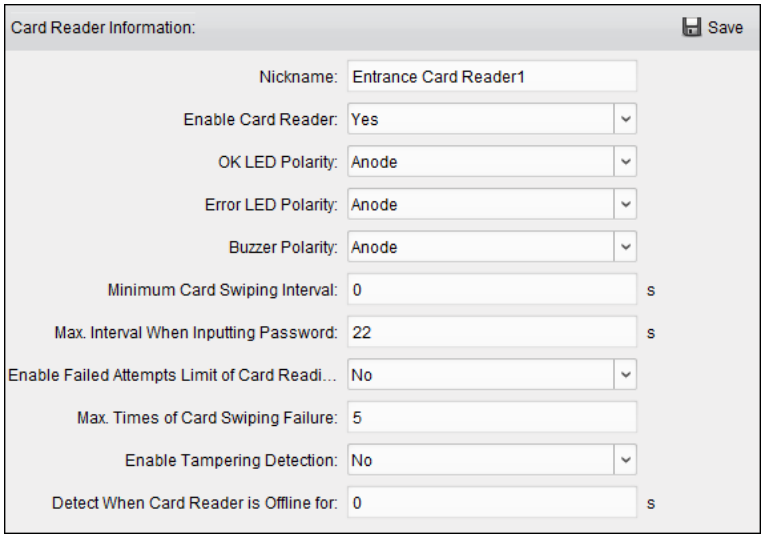
     ✧ The duress code, super password, and the dismiss code should be different from the authentication password.

     ✧ The duress code, super password, and the dismiss code should contain 4 to 8 numerics.**Elevator Control Delay Time** (available for elevator controller)**:** The time duration of the visitor using the elevator.
3. Click **Save** button to save parameters.

Configuring Card Reader Parameters

Steps:

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



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

when authenticating. By default, it is 2s.

- **Live Face Detection:** Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.
- **1:1 Security Level:** Set the matching security level when authenticating via 1:1 matching mode.
- **1:N Security Level:** Set the matching security level when authenticating via 1:N matching mode.

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

14.6.2 Card Reader Authentication

Purpose:

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

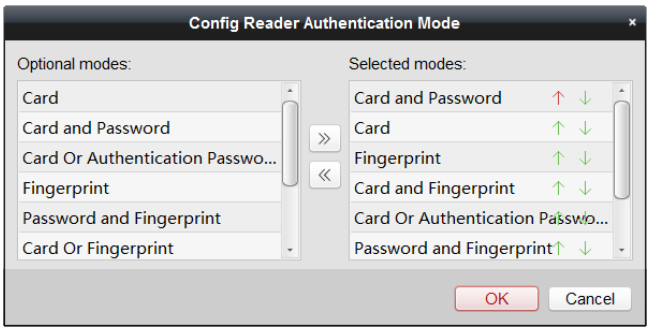
Steps:

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

   Notes:

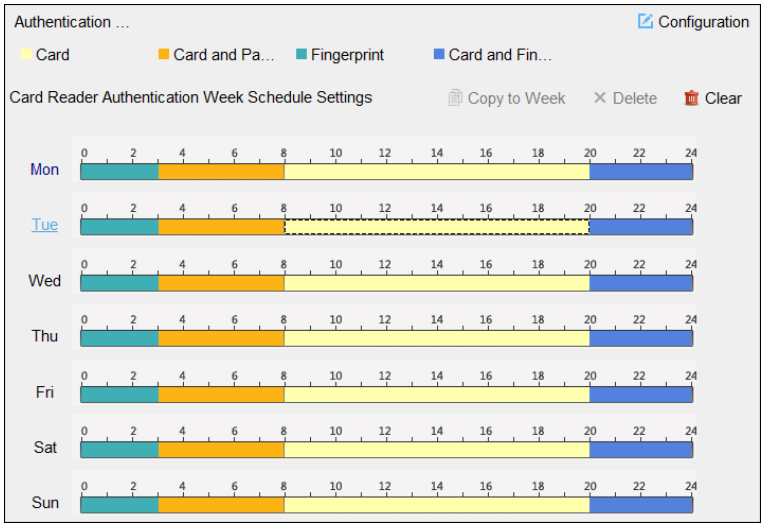
   - The available authentication modes depend on the device type.
   - Password refers to the card password set when issuing the card to the person. *Chapter 14.3 Person Management*.
   - Authentication password refers to the password set to open the door. Refer to *Chapter 14.6.8 Authentication Password*

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

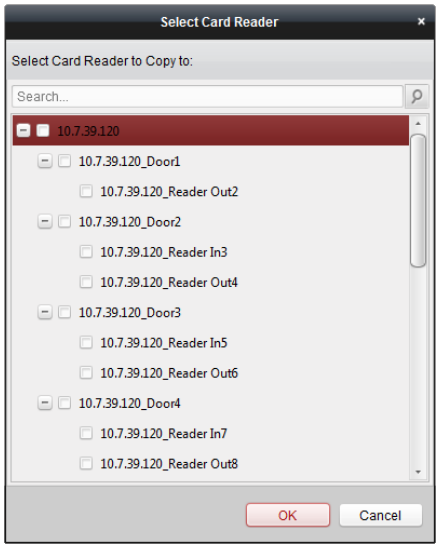


   2) Click **OK** to confirm the selection.

3. After selecting the modes, the selected modes will display as icons.
   Click the icon to select a card reader authentication mode.
4. Drag on a day to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.



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



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

14.6.3 Multiple Authentication

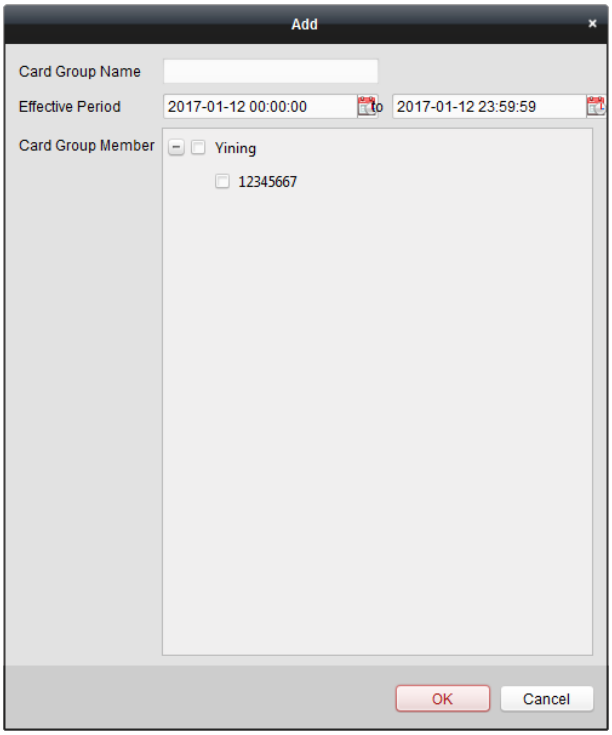
Purpose:

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

Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 14.5 Permission Configuration.*

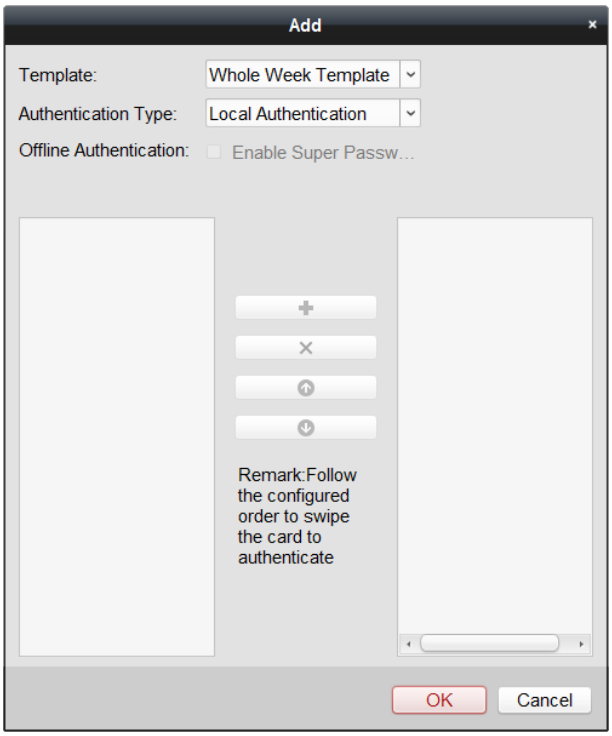
Steps:

1. Click **Access Control > Advanced Function > Multiple Authentication** tab.
2. Select access control device from the list on the left.
3. Add a card group for multiple authentication.
   1) In the Set Card Group panel, click **Add** button to pop up the following window:



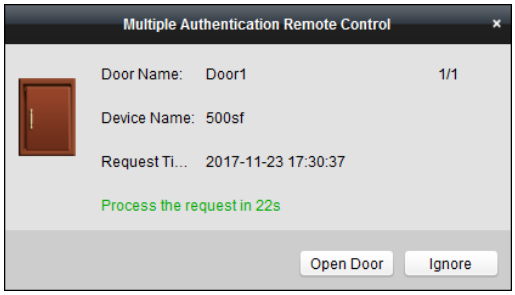
2) Create a name for the group as desired.
3) Click to set the effective time and expiry time of the card group.
4) Check the checkbox(es) to select the card(s) to add the card group.
5) Click **OK** to save the card group.

4. In the Set Authentication Group panel, select the access control point (door) of the device for multiple authentication.
5. Input the time interval for card swiping.
6. Add an authentication group.
   1) In the Set Authentication Group panel, click **Add** to pop up the following window.



2) Select the template of the authentication group from the dropdown list. For details about setting the template, refer to *Chapter 14.4 Schedule and Template*.
3) Select the authentication type of the authentication group from the dropdown list.
   - **Local Authentication:** Authentication by the access control device.
   - **Local Authentication and Remotely Open Door:** Authentication by the access control device and by the client. You can enable the super password authentication when the access control device is disconnected with the client.

     Note: If you set the authentication type as Local Authentication and Remotely Open Door, when the person swipes the card on the device, a window will pop up. You can unlock the door via the client.



   - **Local Authentication and Super Password:** Authentication by the access control device and by the super password.
4) In the list on the left, the added card group will display. You can click the card group and click to add the group to the authentication group.

   You can click the added card group and click to remove it from the authentication group.

   You can also click or to set the card swiping order.
5) Input the **Card Swiping Times** for the selected card group.

   Notes:
   - The Card Swiping Times should be larger than 0 and smaller than the added card quantity in the card group.
   - The upper limit of Card Swiping Times is 16.
6) Click **OK** to save the settings.

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

Notes:

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

14.6.4 Open Door with First Card

Purpose:

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

- **Remain Open with First Card:** The door remains open for the configured time duration after the first card swiping until the remain open duration ends.
- **Disable Remaining Open with First Card:** Disable the function.
- **First Card Authorization:** All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first card authorization.

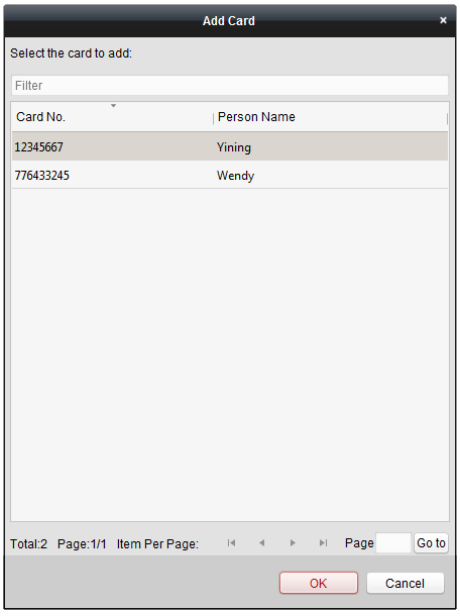
  Notes:

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

Steps:

1. Click **Access Control > Advanced Function > Open Door with First Card** tab.
2. Select an access control device from the list on the left.
3. Select the first card mode in the drop-down list for the access control point.
4. (Optional) If you select Remain Open with First Card, you should set remaining open duration.

   Note: The Remaining Open Duration should be between 0 and 1440 minutes. By default, it is 10 minutes.
5. In the First Card list, Click **Add** button to pop up the following window box.



   1) Select the cards to add as first card for the door

      Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 14.5 Permission Configuration.*
   2) Click **OK** button to save adding the card.
6. You can click **Delete** button to remove the card from the first card list.
7. Click **Save** to save and take effect of the new settings.

14.6.5 Anti-Passing Back

Purpose:

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

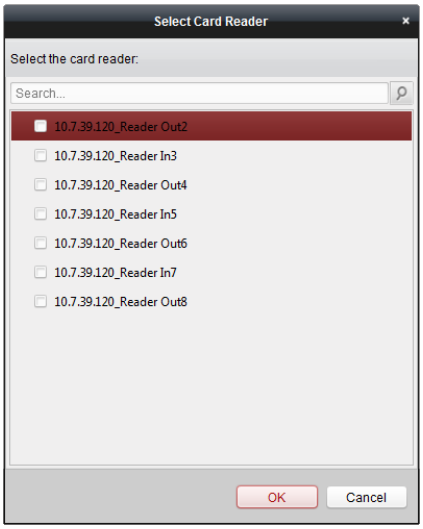
Notes:

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

Steps:

1. Click **Access Control > Advanced Function > Anti-passing Back** tab.
2. Select an access control device from the device list on the left.
3. In the First Card Reader field, select the card reader as the beginning of the path.
4. In the list, click the text filed of **Card Reader Afterward** and select the linked card readers.

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



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

14.6.6 Cross-Controller Anti-passing Back

Purpose:

You can set anti-passing back for card readers in multiple access control devices. You should swipe the card according to the configured swiping card route. And only one person could pass the access control point after swiping the card.

Setting Route Anti-passing Back

Purpose:

The route anti-passing back depends on the card swiping route. You should set the first card reader and the card readers afterwards.

Steps:

1. Click **Access Control > Advanced Function > Cross-Controller Anti-passing Back** to enter the Cross-Controller Anti-passing Back tab.
2. Check the **Enable Cross-Controller Anti-passing Back** checkbox to enable the function.
3. Set the anti-passing back parameters.
   - **Based on Card**

     Note: The system will judge the anti-passing back according to the entrance and exit records on the card.

     1) Select **Based on Card** as the anti-passing back mode in the drop-down list.
     2) Select **Route Anti-passing Back** as the rule.
     3) Set the sector ID.
     4) Click **Select Access Controller** to select a device in the pop-up window.
     5) In the **Card Reader** area, click the icon on the left of the card reader column to select the first card reader. The icon will turn to  .
     6) Click the card reader afterward input field to select the card readers afterward in the pop-up window.
     7) Check the checkbox in the Enable Anti-passing Back column to enable the anti-passing back function.

        Notes:

        - The displayed card readers in the card reader afterward input field should be in authentication order.
        - Up to 64 devices with anti-passing back function can be added.
        - Up to 16 card readers afterward can be added for each card reader.
        - It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to *14.1.6 Authenticating M1 Card* Encryption.

   - **Based on Network**

     Note: Authenticate the anti-passing back according to the entrance and exit information on the card reader.

     1) Select **Based on Network** as the anti-passing back mode in the drop-down list.
     2) Select **Route Anti-passing Back** as the rule.
     3) Select a server in the drop-down list for judging the anti-passing back.
     4) (Optional) You can click **Delete Record** and select the card in the pop-up window to delete the card swiping information in all devices.

        The user should be start swiping card again from the first card reader.
     5) Click **Select Access Controller** to select a device in the pop-up window.
     6) In the Card Reader area, click the icon on the left of the card reader column to select the first card reader. The icon will turn to  .
     7) Click the card reader afterward input field to select the card readers afterward in the

pop-up window.

8) Check the checkbox in the Enable Anti-passing Back column to enable the anti-passing back function.

Notes:

- The displayed card readers in the card reader afterward input field should be in authentication order.
- Up to 64 devices with anti-passing back function can be added.
- Up to 16 card readers afterward can be added for each card reader.
- Up to 5000 cards' swiping records can be stored in the selected server.

Setting Entrance/Exit Anti-passing Back

Purpose:

You can set the entrance card reader and the exit card reader only for entering and exiting, without setting the first card reader and the card readers afterwards.

Steps:

1. Click **Access Control > Advanced Function > Cross-Controller Anti-passing Back** to enter the Cross-Controller Anti-passing Back tab.
2. Check the **Enable Cross-Controller Anti-passing Back** checkbox to enable the function.
3. Set the anti-passing back parameters.

➢ **Based on Card**

Note: The system will judge the anti-passing back according to the entrance and exit records on the card.

1) Select **Based on Card** as the anti-passing back mode in the drop-down list.
2) Select **Entrance/Exit Anti-passing Back** as the rule.
3) Set the sector ID.
4) Click **Select Access Controller** to select a device in the pop-up window.
5) In the Card Reader area, check the checkboxes in the Enable Anti-passing Back column to select the entrance card reader and the exit card reader.
6) Click **Save** to save the settings.

Notes:

- Up to one entrance carder and one exit card reader should be checked.
- Up to 64 devices with anti-passing back function can be added.
- It supports M1 card at present and the sector cannot be encrypted. For details about sector encryption, refers to *14.1.6 Authenticating M1 Card* Encryption.

➢ **Based on Network**

Note: Authenticate the anti-passing back according to the entrance and exit information on the card reader.

1) Select **Based on Network** as the anti-passing back mode in the drop-down list.
2) Select **Entrance/Exit Anti-passing Back** as the rule.
3) Select the server in the dropdown list for judging the anti-passing back.
4) (Optional) You can click **Delete Record** and select the card in the pop-up window to delete the card swiping information in all devices.
5) Click **Select Access Controller** to select a device in the pop-up window.

6) In the Card Reader area, check the checkboxes in the Enable Anti-passing Back column to select the entrance card reader and the exit card reader.

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

Notes:

- Up to one entrance carder and one exit card reader should be checked.
- Up to 64 devices with anti-passing back function can be added.
- Up to 5000 cards' swiping records can be stored in the selected server.

14.6.7 Multi-door Interlocking

Purpose:

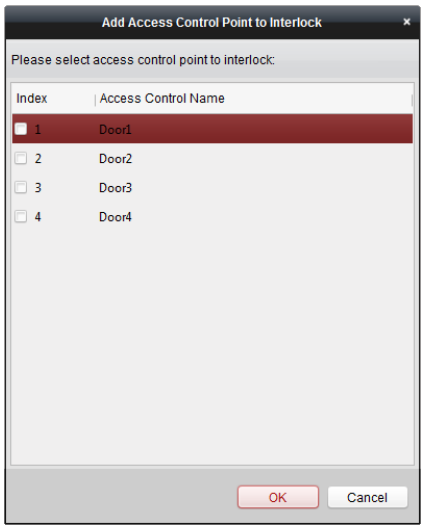
You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Notes:

- The Multi-door Interlocking function is only supported by the access control device 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 control device at the same time.

Steps:

1. Click **Access Control > Advanced Function > Multi-door Interlocking** tab to enter the multi-door interlock settings page.
2. Select an access controller from the Controller List.
3. Click **Add** to pop up the Add Access Control Point to Interlock interface.



4. Select the access control point (door) from the list.
   Note: Up to four doors can be added in one multi-door interlocking combination.
5. Click **OK** to save the adding.
6. (Optional) After adding the multi-door interlocking combination, you can select it from the list and click **Delete** to delete the combination.
7. Click **Save** button to save and take effect.

14.6.8 Authentication Password

Purpose:

You can open the door by inputting the authentication password on the card reader keypad after finishing the operation of setting authentication password.

Notes:

- This authentication password function is only valid during the schedules when the card reader authentication mode for the access control device is set as **Card or Authentication Password**. For details, refer to *Chapter 14.6.2 Card Reader Authentication.*
- This function should be supported by the access control device.

Steps:

1. Click **Access Control > Advanced Function > Authentication Password** tab and select an access control device from the list.
   All the cards and persons which have been applied to the device will be displayed.
   Note: For setting and applying the permissions to the device, refer to *Chapter 14.5 Permission Configuration.*
2. Click the **Password** field of the card and input the authentication password for the card.
   Note: The authentication password should contain 4 to 8 digits.
3. After setting the authentication password, the authentication password function of the card will be enabled by default.
4. (Optional) You can input the keywords of card No., person name, or authentication password to search.

Note: Up to 500 cards with authentication password can be added to one access control device. The password should be unique and cannot be same with each other.

14.6.9 Relay Settings

Purpose:

For elevator controller, you can manage the relationship between the floor and the relay in this chapter.

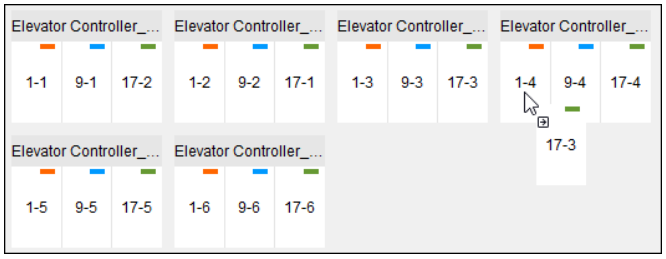
Configuring Relay and Floor

Steps:

1. Click **Access Control > Advanced Function > Relay Settings** tab to enter the Relay Settings interface.
2. Select an elevator controller in the Controller List on the left of the interface.
3. Select an unconfigured relay in the Unconfigured Relay panel on the right of the interface.
   There are three types of unconfigured relays: Button Relay, Call Elevator Relay and Auto Button Relay.
   - **Button Relay:** Control the validity for buttons of each floor.
   - **Call Elevator Relay:** Control to call the elevator to go to the specified floor.

- **Auto Button Relay:** Control to press the button when the user swipes card inside the elevator. The button of the floor will be pressed automatically according to the user's permission.

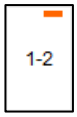
4. Click and drag the unconfigured relay from the Unconfigured Relay panel to the coressponding floor in the Floor List panel.
   Or click and drag the relay from the Floor List panel to the Unconfigured Relay panel.
   Or click and drag the relay from one floor to another floor in the Floor List panel.
   When clicking and dragging, if two relays are of the same relay type in the two different floors, the relays will change the place.



5. Click **Save** to apply the settings to the selected device.

Notes:

- An elevator controller can link to up to 24 distributed elevator controllers. A distributed elevator controller can link up to 16 relays.
- Three types of relay are available: Button Relay, Call Elevator Relay and Auto Button Relay. ▬ represents the button relay, ▬ represents the call elevator relay, and ▬ represents the auto button relay.

  Take the fiugre 

as an example. In the number 1-2, 1 represents the distributed elevator controller number, 2 represents the ralay, and the icon ▬ represents the relay type. You can click **Relay Type** to configure the relay type. For details about configuring the relay type, see *Configuring Relay Type*.
- By default, the relay total amount is the added floor number *3 (three types of relay).
- Each floor contains up to 3 types of relay. You can click and drag one relay once.

- If you change the floor number in the door group management, all relays in the Relay Settings interface will restore to the default settings.

Configuring Relay Type

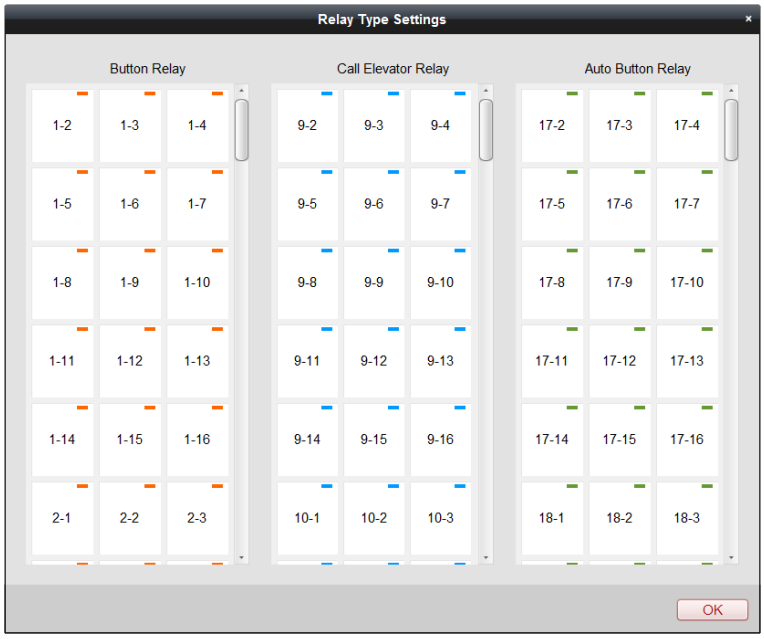
Purpose:

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

Steps:

1. Click **Access Control > Advanced Function > Relay Settings** tab to enter the Relay Settings interface.
2. In the Relay Settings interface, click **Relay Type** to pop up the Relay Type Settings window.

   Note: All relays in the Relay Type Settings window are unconfigured relays.



3. Click and drag the relay from one relay type panel to the other one.
4. Click **OK** to save the settings.

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

14.6.10 Custom Wiegand

Purpose:

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand protocols to communicate between the device and the third party card readers.

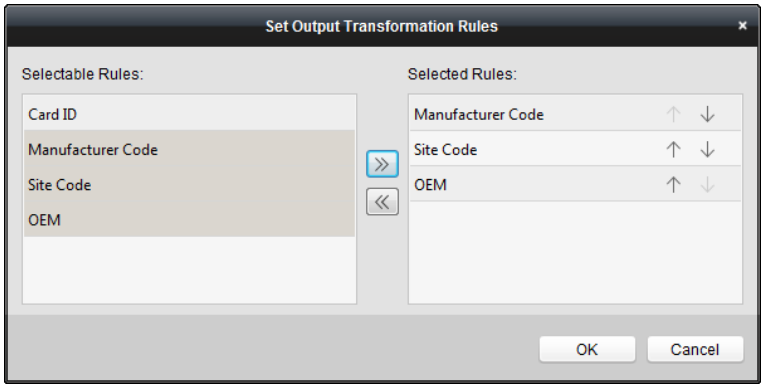
Before you start:

Wire the third party card readers to the device.

Steps:

1. Click **Access Control > Advanced Function > Custom Wiegand** to enter the Custom Wiegand tab.

2. Select a custom wiegand on the left.
3. Check **Enable** checkbox to enable the custom wiegand.
4. Set the wiegand name.
5. Select device.
   1) Click **Select Device**.
   2) Select the device to use custom wiegand.
   3) Click **OK** to save the settings.
6. Input the total length and select the parity mode in the drop-down list.
   If you select **Odd-Even Parity**, you should set the odd parity start bit, the odd parity length, the even parity start bit and the even parity length.
   If you select **XOR Parity**, you should set the XOR parity start bit, length per group and total length.
   If you select **None**, you are no need to set the parity mode.
7. Set output transformation rule.
   1) Click **Set Rule** to pop up the Set Output Transformation Rules window**.**



   2) Select rules on the left list.
      Note: Press the *Shift* key to select multiple rules.
   3) Click  to move the selected rules to the right list.
   4) (Optional) Click  or  to change the rule order.
   5) (Optional) Select the rules in the Selected Rule list and click  to remove the rule from the list on the right.
   6) Click **OK** to save the settings.
   7) In the Custom Wiegand tab, set the rule start bit, length, and the decimal digit.
8. Click **Save** at the upper right corner of the interface to save the settings.

Notes:

- By default, the device disables the custom wiegand function.
- If the device enables the custom wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom wiegands can be set.
- Up to 32 characters are allowed in the custom wiegand name.
- Up to 80 bits are available in the total length.
- The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.

- The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.

14.6.11 Person in Blacklist

Purpose:

You can configure the person information in the blacklist and apply to the device.

Adding Person to Blacklist

Purpose:

You can add persons to the blacklist, and configure the person's face pictures, gender, and ID number.

Steps:

1. Click **Access Control > Advanced Function > Blacklist** to enter the person in blacklist management page.
2. Click **Person** to enter the person management page.
3. Click **Add**.
4. Click **Select Picture** to select a face picture for the person from local PC.
   Note: The picture should be in JPG format and it should be smaller than 1 MB.
5. Set the person details including name, gender, and ID number.
6. Click **Save** to add the device to the blacklist.
7. (Optional) Select the added person and click Delete to remove it from the blacklist.
8. Apply the person in blacklist to the device to take effect.
   1) Select the person(s) to apply to the device.
   2) Click **Apply**.
   3) Click **Apply All** to start applying all the selected permission(s) to the access control device or door station.
      You can also click **Apply Changes** to apply the changed part of the selected permission(s) to the device(s).
   4) Click **OK** to start applying.

Managing Blacklist Application Result

Purpose:

After applying the configured person information in blacklist, you can view the application results and manage the applied person.

Steps:

1. Click **Access Control > Advanced Function > Blacklist** to enter the person in blacklist management page.
2. Click **Application Result** to enter the application result management page.
   You can check the person in blacklist applying record and view the application results.

3. (Optional) Remove the applied person in blacklist from device.
   1) Click **Delete Person**.
      All the devices which support person in blacklist will display.
   2) Select the device that you want to remove person(s) from.
   3) Click **Next**.
      All the persons in blacklist applied to the device will display.
   4) Select the person(s) you want to remove from the device.
   5) Click **OK** to remove the selected person from the blacklist of the device.
4. (Optional) Click **Clear Persons** and select the device to clear all the persons in the blacklist of the device.

14.7 Configure Access Control Event Linkage

Purpose:

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

Click the  icon on the control panel,

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

14.7.1 Configuring Client Linkage for Access Control Alarm

Purpose:

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

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

Steps:

1. Click **Access Control Event** tab.
2. The added access control devices will display in the Access Control Device panel on the left. Select the access control device, or alarm input, or access control point (door), or card reader to configure the event linkage.
3. Select the event type to set the linkage.
4. Select the triggered camera. The image or video from the triggered camera will pop up when the selected event occurs.
   To capture the picture of the triggered camera when the selected event occurs, you can also set the capture schedule and the storage in Storage Schedule. For details, refer to *Chapter 5.1 Remote Storage.*
5. Check the checkboxes to activate the linkage actions.

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, refer

	to *Chapter 22.7 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. ***Note:*** This linkage is only available to access control point and alarm input.
Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered. ***Note:*** You should set the triggered camera first.

6. Click **Save** to save the settings.
7. You can click **Copy** to button to copy the access control event to other access control device, alarm input, access control point, or card reader.
   Select the parameters for copy, select the target to copy to, and click **OK** to confirm.

14.7.2 Configure Device Linkage for Access Control Alarm Input

Purpose:

The access control alarm inputs can be linked to some actions (e.g., alarm output, host buzzer) when it is triggered.

Steps:

1. Click **Access Control Alarm Input** tab.
2. In the alarm input list on the left, select an alarm input.
3. Switch the property from to  to enable this action.
   Host Buzzer: The audible warning of controller 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.
   Access Control Point (Open/Close): The door will be open or closed when the case is triggered.
   Note: The door cannot be configured as open or closed at the same time.
4. Click **Save** button to save the settings.

14.7.3 Event or Card Linkage

Click **Event Card Linkage** tab.

Note: The Event Card Linkage should be supported by the device.

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

Click **Add** button to add a new linkage.

Configuring Device Linked Actions for Access Control Event

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

Steps:

1. Select the linkage type as **Event Linkage**, and select the event type from the dropdown list.

- For Device Event, select the detailed event type from the dropdown list.
- For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.
- For Door Event, select the detailed event type and select the source door from the table.
- For Card Reader Event, select the detailed event type and select the card reader from the table.

2. Set the linkage target, and switch the property from to  to enable this function.
   - **Host Buzzer**: The audible warning of controller will be triggered.
   - **Capture**: The real-time capture will be triggered.
   - **Recording**: The recording will be triggered.
     Note: The device should support recording.
   - **Card Reader Buzzing**: The audible warning of card reader will be triggered.
   - **Alarm Output**: The alarm output will be triggered for notification.
   - **Zone:** Arm or disarm the zone.
     Note: The device should support zone function.
   - **Access Control Point**: The door status of open, close, remain open, and remain close will be triggered.
     Notes:
     - The door status of open, close, remain open, and remain close cannot be triggered at the same time.
     - The target door and the source door cannot be the same one.
3. Click **Save**.
   The configured device linkage will display in the device list on the left.
   You can click its name to edit its detailed settings or delete it.

Configuring Device Linked Actions for Card Swiping

Steps:

1. Select the linkage type as **Card Linkage**.
2. Input the card No. or select the card from the dropdown list.
3. Select the card reader from the table for triggering.
4. Set the linkage target, and switch the property from to  to enable this function.
   - **Host Buzzer**: The audible warning of controller will be triggered.
   - **Capture**: The real-time capture will be triggered.
   - **Recording**: The recording will be triggered.
     Note: The device should support recording.
   - **Card Reader Buzzing**: The audible warning of card reader will be triggered.
   - **Alarm Output**: The alarm output will be triggered for notification.
   - **Zone:** Arm or disarm the zone.
     Note: The device should support zone function.
   - **Access Control Point**: The door status of open, close, remain open, and remain closed will be enabled.
5. Click **Save**.
   The configured device linkage will display in the device list on the left.

You can click its name to edit its detailed settings or delete it.

Configuring Device Linkage for Mobile Terminal's MAC Address

Steps:

1. Select the linkage type as **MAC Linkage**.
2. Input the MAC address of the event source.
   MAC Address Format: AA:BB:CC:DD:EE:FF.
3. Set the linkage target, and switch the property from to  to enable this function.
   - **Host Buzzer**: The audible warning of controller will be triggered.
   - **Capture**: The real-time capture will be triggered.
   - **Recording**: The recording will be triggered.
     Note: The device should support recording.
   - **Card Reader Buzzing**: The audible warning of card reader will be triggered.
   - **Alarm Output**: The alarm output will be triggered for notification.
   - **Zone:** Arm or disarm the zone.
     Note: The device should support zone function.
   - **Access Control Point**: The door status of open, close, remain open, and remain closed will be enabled.
4. Click **Save**.
   The configured device linkage will display in the device list on the left.
   You can click its name to edit its detailed settings or delete it.

14.7.4 Cross-Device Linkage

Purpose:

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

Click **Cross-Device Linkage** tab.

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

Configuring Cross-Device Linkage for Event

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

Steps:

1. Click to select the linkage type as **Event Linkage**, select the access control device as event source, and select the event type from the dropdown list.
   - For Device Event, select the detailed event type from the dropdown list.
   - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the table.

- For Door Event, select the detailed event type and select the door from the table.
- For Card Reader Event, select the detailed event type and select the card reader from the table.

2. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from to  to enable this function.
   - **Alarm Output**: The alarm output will be triggered for notification.
   - **Access Control Point**: The door status of open, close, remain open, and remain close will be triggered. ***Note:*** The door status of open, close, remain open, and remain close cannot be triggered at the same time.
3. Click **Save** button to save parameters.

Configuring Cross-Device Linkage for Card Swiping

Steps:

1. Select the linkage type as **Card Linkage**.
2. Select the card from the dropdown list and select the access control device as event source.
3. Select the card reader from the table for triggering.
4. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from to  to enable this function.
   Alarm Output: The alarm output will be triggered for notification.
5. Click **Save** button to save parameters.

14.8 Searching Access Control Event

Purpose:

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

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

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

Click  icon and click **Access Control Event** tab.

14.8.1 Searching Local Access Control Event

Steps:

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

6. (Optional) If the event contains linked video, you can click in the **Playback** column to view the recorded video file of the triggered camera when the alarm is trigged.
   Note: For setting the triggered camera, refer to *Chapter 14.7.1 Configuring Client Linkage for Access Control Alarm.*
7. You can click **Export** to export the search result to the local PC in *.csv file.

14.8.2 Searching Remote Access Control Event

Steps:

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

14.9 Door Status Management

Purpose:

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

14.9.1 Access Control Group Management

Purpose:

Before controlling the door status and setting the status duration, you are required to organize it into group for convenient management.

Perform the following steps to create the group for the access control device:

Steps:

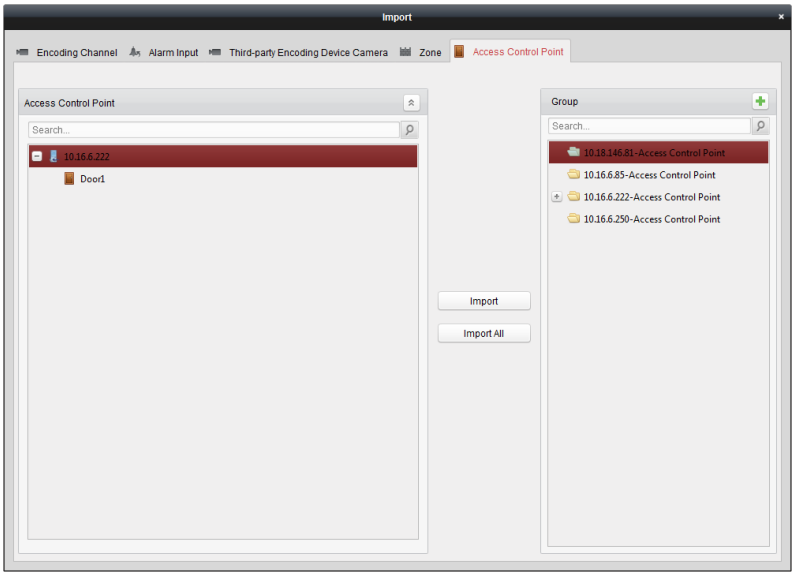
1. Click  on the control panel to open the Device Management page.
2. Click **Group** tab to enter the Group Management interface.
3. Perform the following steps to add a group.
   1) Click  to open the Add Group window box.
   2) Input a group name as you want.
   3) Click **OK** to add the new group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

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

      Notes:

      - You can also select **Alarm Input** tab and import the alarm inputs to group.
      - For the Video Access Control Terminal, you can add the cameras as encoding channel to the group.

   2) Select the names of the access control points in the list.
   3) Select a group from the group list.
   4) Click **Import** to import the selected access control points to the group.



5. After importing the access control points to the group, you can click , or double-click the group/access control point name to modify it.
   For other detailed operations, refer to *Chapter 3.2 Managing Group.*

14.9.2 Controlling Door Status

Purpose:

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

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

Steps:

1. Select an access control group on the left. For managing the access control group, refer to

Chapter 14.9.1 Access Control Group Management.

2. The access control points of the selected access control group will be displayed on the right.

   Click icon  on the Status Information panel to select a door.

3. Click the following button listed on the **Status Information** panel to control the door.
   - **Open Door**: Click to open the door once.
   - **Close Door**: Click to close the door once.
   - **Remain Open**: Click to keep the door open.
   - **Remain Closed**: Click to keep the door closed.
   - **Capture**: Click to capture the picture manually.

     Note: The **Capture** button is available when the device supports capture function. And it cannot be realized until the Storage Server is configured. Refer to *Chapter 5.1 Remote Storage.*

14.9.3 Controlling Elevator Status

Purpose:

You can control the elevator status for elevator controller, including opening elevator's door, controlled, free, calling elevator, etc.

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

1. Select an access control group on the left. For managing the access control group, refer to *Chapter 14.9.1 Access Control Group Management.*

   The floors of the selected access control group will be displayed on the right of the interface.

2. Click  on the Status Information panel to select a floor.
3. Click the following button listed on the **Status Information** panel to control the elevator.
   - **Open Door**: The floor's button in the elevator will be valid for a period of time and the elevator's door is open.
   - **Controlled**: You should swipe the card to press the selected floor button. And the elevator can go to the selected floor.
   - **Free**: The selected floor's button in the elevator will be valid all the time.
   - **Disable**: The selected floor's button in the elevator will be invalid and you cannot go to the selected floor.
   - **Call Elevator (Visitor)**: The elevator will go down to the first floor. The visitor can only press the selected floor button.
   - **Call Elevator (Resident)**: Call the elevator to the selected floor.
4. You can view the anti-control operation result in the Operation Record panel.

Notes:

- You can control the elevator via the current client if it is not armed by other client. The elevator cannot be controlled by other client software if the elevator status changes.
- Only one client software can control the elevator at one time.
- The client which has controlled the elevator can receive the alarm information and view the

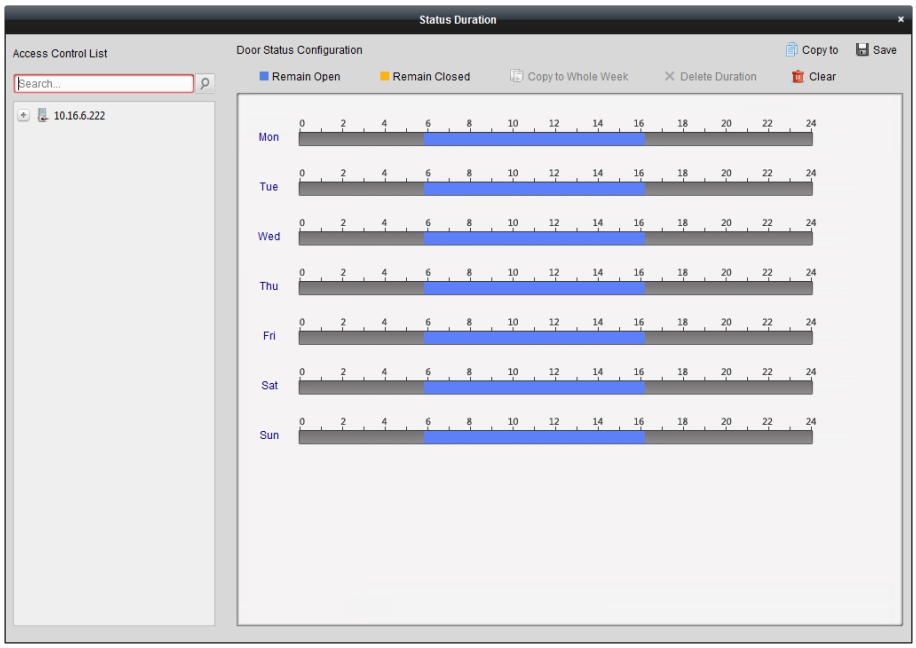
elevator real-time status.

14.9.4 Configuring Status Duration for Door

Purpose:

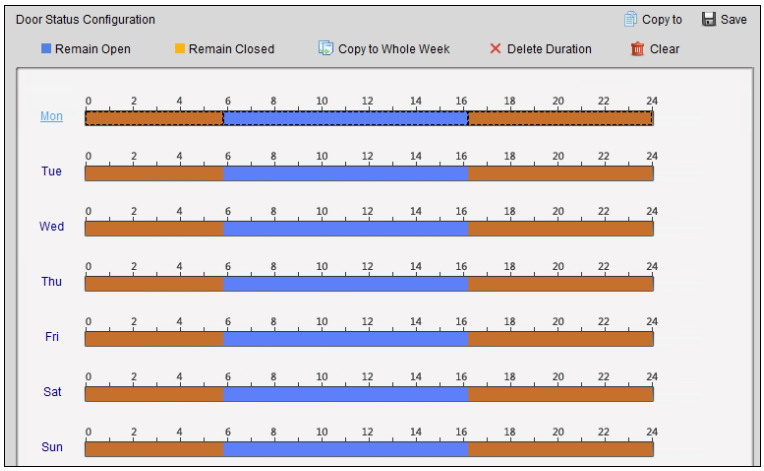
You can schedule weekly time periods for an access control point (door) to remain open or remain closed.

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



Steps:

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



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

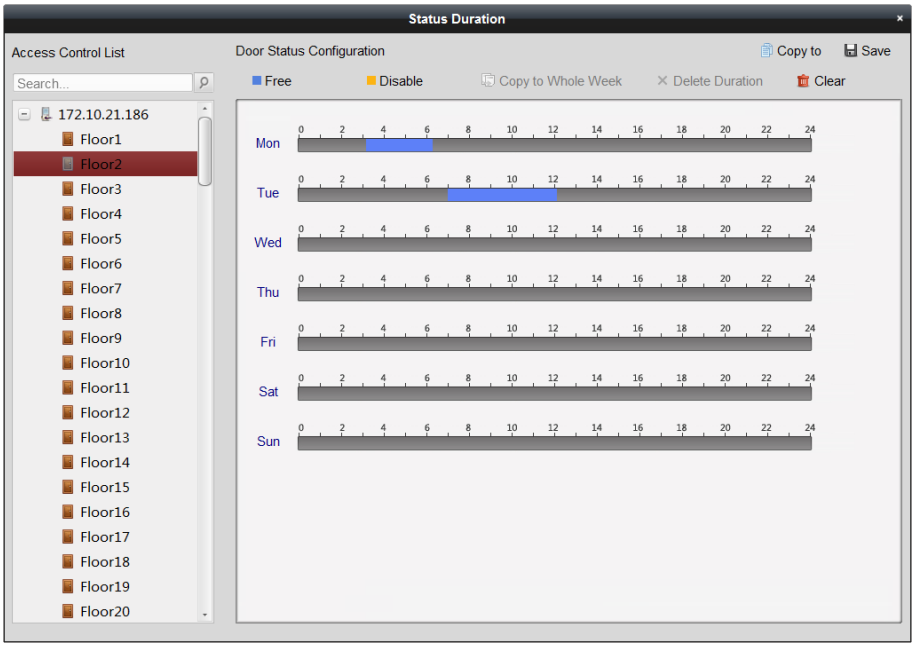
3. Optionally, you can select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
4. You can select the time bar and click **Delete Duration** to delete the time period.
Or you can click **Clear** to clear all configured durations on the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

14.9.5 Configuring Status Duration for Floor

Purpose:

You can schedule weekly time periods for an access control point (floor) to be free or disabled.

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



Steps:

1. Click to select a floor from the elevator controller list on the left.
2. On the Door Status Configuration panel on the right, draw a schedule for the selected floor.
   1) Select a status brush as **Free** or **Disabled**.
      - **Free**: The floor button will be free during the configured time period. The brush is marked as .
      - **Disabled:** You cannot press the floor button during the configured duration. The brush is marked as .
   2) Drag on the timeline to draw a color bar on the schedule to set the duration.

   3) When the cursor turns to , you can move the selected time bar you just edited. You can also edit the displayed time point to set the accurate time period.
      When the cursor turns to , you can lengthen or shorten the selected time bar.
3. Optionally, you can select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.
4. You can select the time bar and click **Delete Duration** to delete the time period.
   Or you can click **Clear** to clear all configured durations on the schedule.
5. Click **Save** to save the settings.
6. You can click **Copy to** button to copy the schedule to other floors.

14.9.6 Real-time Card Swiping Record

Click **Card Swiping Record** tab.

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

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

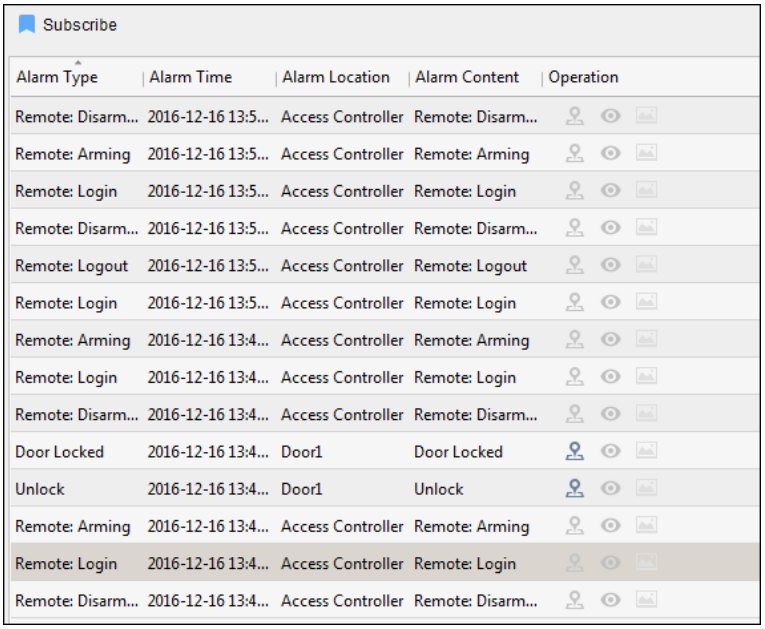
Note: Authentication result refers to the card swiping result, such as card No. not registered, succeeded, etc.

14.9.7 Real-time Access Control Alarm

Purpose:

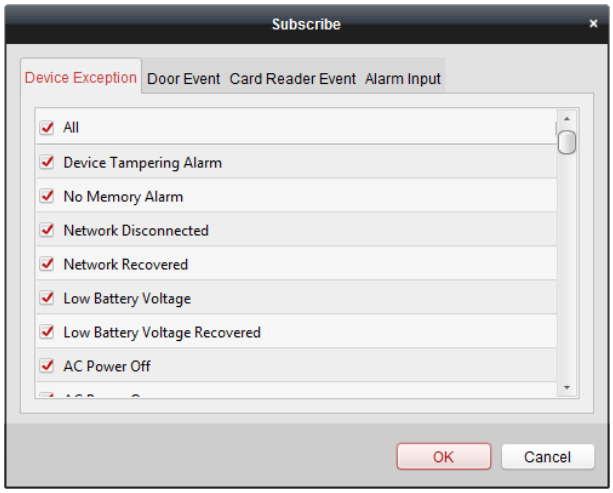
The logs of access control events will be displayed in real time, including device exception, door event, card reader event, and alarm input.

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



Steps:

1. All access control alarms will display in the list in real time.
   You can view the alarm type, alarm time, location, etc.
2. Click to view the alarm on E-map. For configuring the access control point on E-map, refer to *Chapter 14.11 Displaying Access Control Point on E-map.*
3. You can click or to view the live view or the captured picture of the triggered camera when the alarm is trigged.
   Note: For setting the triggered camera, refer to *Chapter 14.7.1 Configuring Client Linkage for Access Control Alarm.*
4. Click **Subscribe** to select the alarm that the client can receive when the alarm is triggered.



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

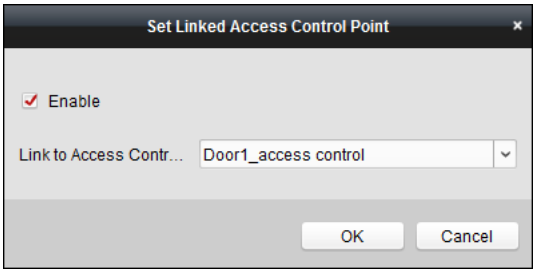
14.10 Controlling Door during Live View

Purpose:

You can control the door during live view.

Steps:

1. Right click on the live view window to pop up the right-click menu.
2. Click **Link to Access Control Point** to pop up the Set Linked Access Control Point window.
3. Check the **Enable** checkbox to enable the linkage function.
4. Select access control point from the dropdown list.



5. Click **OK** to save the settings.
6. Get the stream again (double-click the camera) to make the settings effective.

   Four door control buttons will appear on the toolbar during live view.

   The following table shows the descriptions of the four buttons.

Button	Description
	Open the door.
	Close the door.
	Remain open.
	Remain closed.

7. Click  to open or close the door.

   Or click  to set the door status as remain open or remain closed.

Note: One camera can be linked to only one access control point; Different cameras can be linked to the same access control point.

14.11 Displaying Access Control Point on E-map

Purpose:

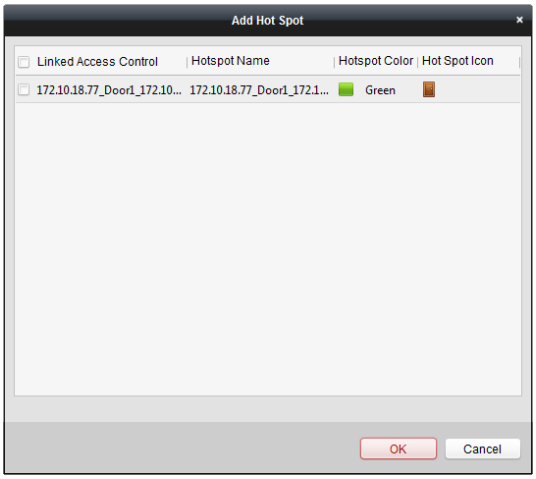
You can add the access control point on the E-map, and when the alarm of the access control point is triggered, you can view the alarm notification on the E-map, check the alarm details, and control the door.

Note: For detailed operations of E-map, refer to *Chapter 8 E-map Management*.

14.11.1 Adding Access Control Point 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 window box.
3. Check the checkboxes to select the access control point 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 door icons are added on the map as hot spots and the icons of added access control points change from to in the group list. You can click-and-drag the access control point icons to move the hot spots to the desired locations.
   You can also click-and-drag the access control point icons from the group list to the map directly to add the hot spots.



Note: For Video Access Control Terminal, you can also add its camera to the E-map to view the live view of the camera.

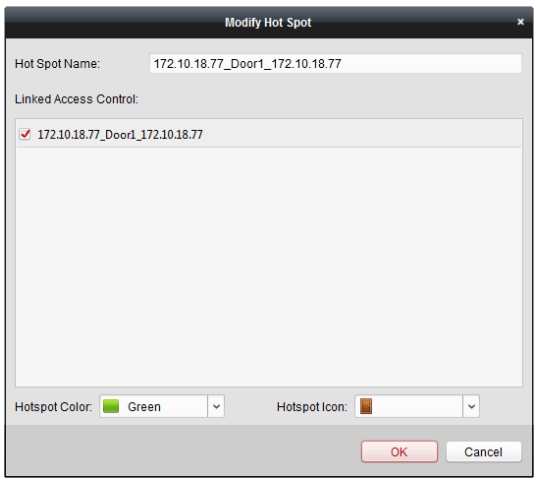
14.11.2 Modifying Hot Spots

Purpose:

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

Steps:

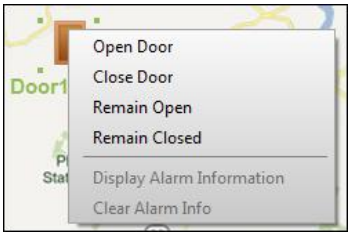
1. Click the **Edit Map** button in the E-map toolbar to enter the map editing mode.
2. Select the hot spot icon on the map and then click in the toolbar, right-click the hot spot icon and select **Modify**, or double-click the hot spot icon on the map to open the Modify Hot Spot window box.
3. You can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



14.11.3 Previewing Hot Spots

Steps:

1. Click the **Map Preview** button in the E-map toolbar to enter the map preview mode.
2. To control the access control point, you can right click the access control point icon on the map, and click **Open Door**, **Close Door**, **Remain Open**, and **Remain Closed** to control the door.



3. If there is any alarm triggered, an icon will appear and twinkle near the hot spot (it will twinkle for 10s). Click the alarm icon, or you can right click the door 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 14.7 Configure Access Control Event* .
4. To clear the alarm information displayed on the map, click on the toobar, or right click the access control point icnon and select **Clear Alarm Information** to clear the alarms of the selected zone.

Chapter 15 Time and Attendance

Purpose:

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.

Before you start:

You should add organization and person in Access Control module. For details, refer to *Chapter 14.2 Organization Management* and *Chapter 14.3 Person Management.*

Click  to enter the Time and Attendance module.

15.1 Shift Schedule Management

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

15.1.1 Shift Settings

Purpose:

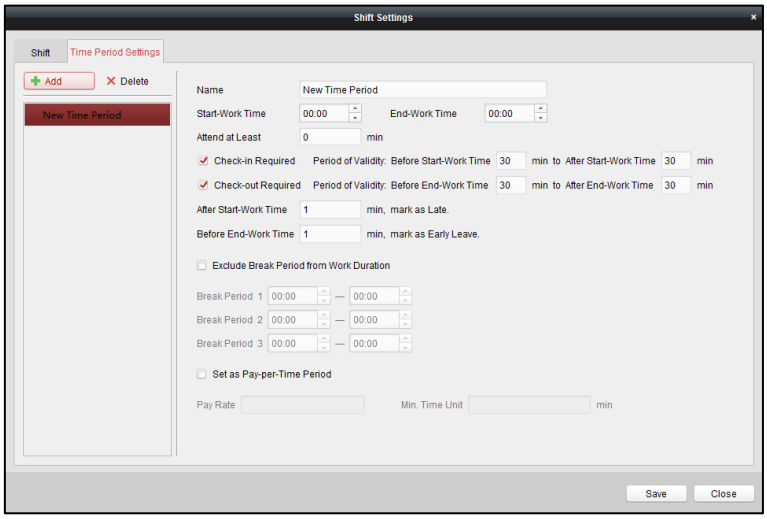
You can add time period and shift for the shift schedule.

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

Adding Time Period

Steps:

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



3. Set the related parameters.

   Name: Set the name for time period.

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

   Attend at Least: Set the minimum attendance time.

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

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

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

   Note: Up to 3 break periods can be set.

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

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

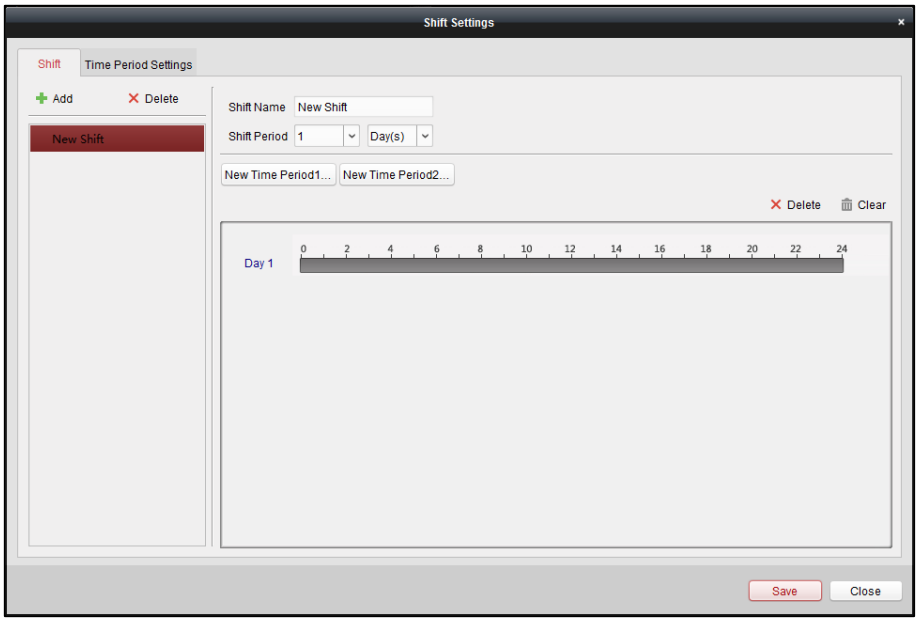
   The added time period will display on the left panel of the window.

   You can also click **Delete** to delete the time period.

Adding Shift

Steps:

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



3. Set the name for shift.
4. Select the shift period from the drop-down list.
5. Configure the shift period with the added time period.
   1) Select the time period.
   2) Click the time bar to apply the time period for the select day.

   You can click the time period on the bar and click or **Delete** to delete the period.

   You can also click **Clear** to delete all days' time period.
6. Click **Save** to save the settings.

   The added shift will display on the left panel of the window.

You can also click **Delete** on the left panel to delete the shift.

15.1.2 Shift Schedule Settings

Purpose:

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

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

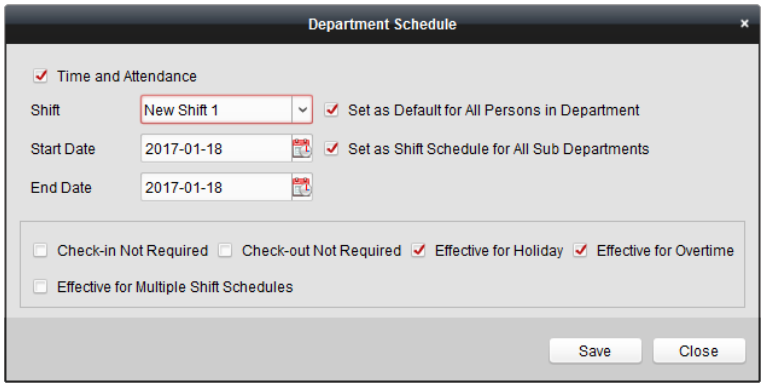
Department Schedule

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

Note: In Time and Attendance module, the department list is the same with the **organization** in Access Control. For setting the organization in Access Control, refer to *Chapter 14.2 Organization Management*.

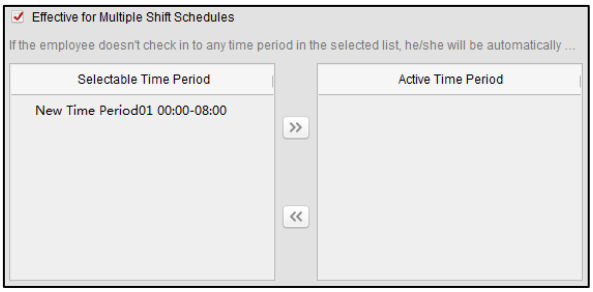
Steps:

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



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

- After checking the **Effective for Multiple Shift Schedules** checkbox, you can select the effective time period(s) from the added time periods for the persons in the department.



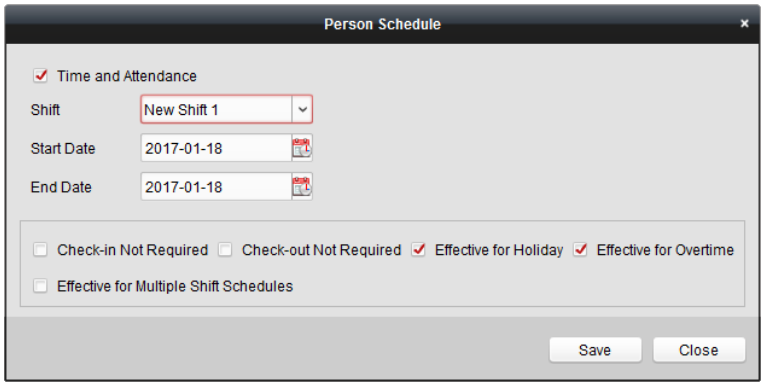
1) In the Selectable Time Period list on the left, click the added time period and click » to add it to the right.
2) (Optional) To remove the selected time period, select it and click «.

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

Person Schedule

Steps:

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

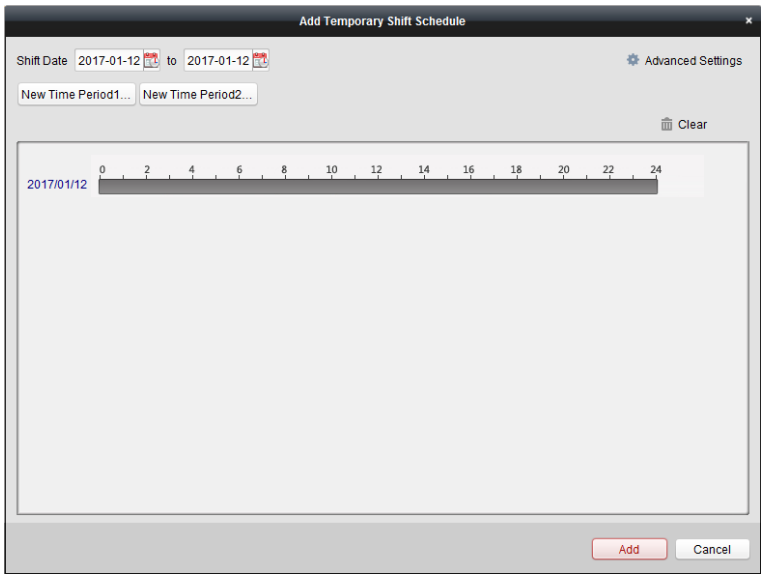


4. Check **Time and Attendance** checkbox.
   The configured person will apply the attendance schedule.
5. Select the shift from the drop-down list.
6. Set the start date and end date.
7. (Optional) Set other parameters for the schedule.
   You can select Check-in Not Required, Check-out Not Required,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

Temporary Schedule

Steps:

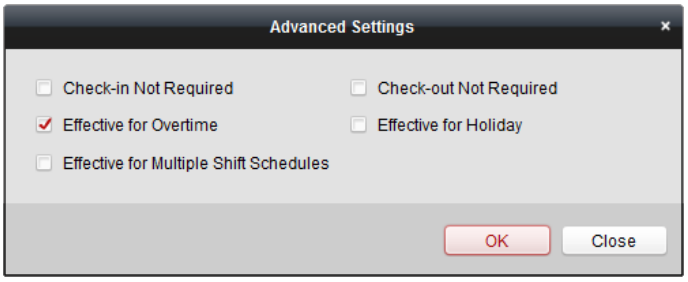
1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **Temporary Schedule** to pop up Temporary Schedule window.



4. Click  to set the shift date.
5. Configure the shift date with the added time period.
   1) Select the time period.
   2) Click the time bar to apply the time period for the select date.

   You can click the time period on the bar and click  to delete the period.

   You can also click **Clear** to delete all days' time period.
6. You can click **Advanced Settings** to advanced attendance rules for the temporary schedule.



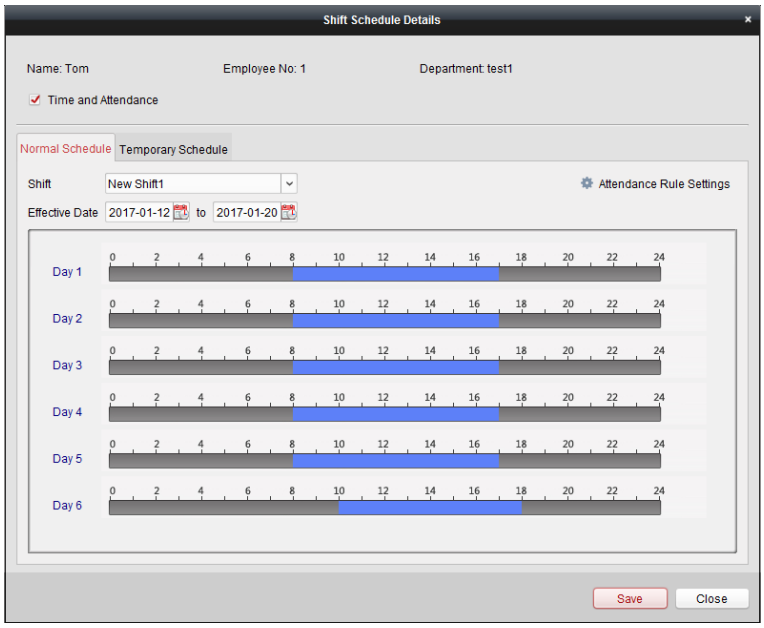
7. Click **Add** to save the settings.

Checking Shift Schedule Details

Steps:

1. On the Shift Schedule Management interface, select the department on the left panel.
2. Select the person(s) on the right panel.
3. Click **View** to pop up Shift Schedule Details window.

   You can check the shift schedule details.

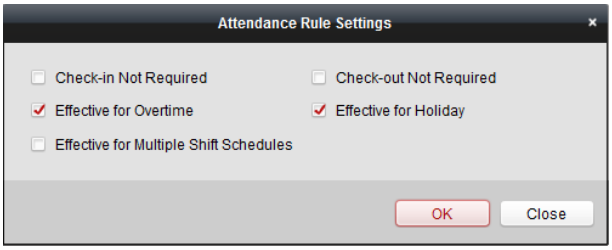


4. Click **Normal Schedule** tab.

   You can check and edit the normal schedule details.

   1) Select the shift from the drop-down list.

   2) Click **Attendance Rule Settings** to pop up Attendance Rule Settings window.

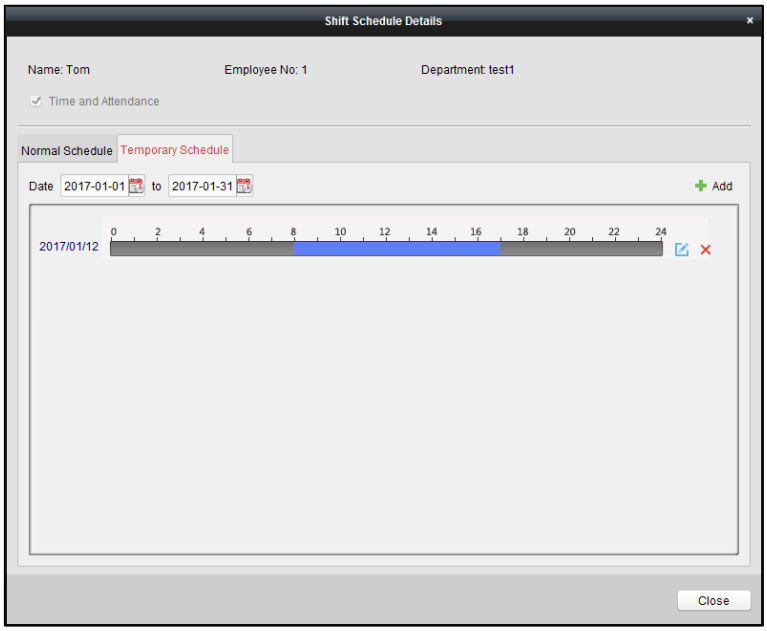


   You can check the attendance rules as desired and click **OK** to save the settings.

   3) Click  to set the effective date.

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

5. (Optional) Click **Temporary Schedule** tab.



You can check and edit the temporary schedule details.

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

(Optional) Click to edit the time period.

(Optional) Click to delete the temporary schedule.

Exporting Shift Schedule Details

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

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

15.2 Attendance Handling

Purpose:

You can handle the attendance, including check-in correction, check-out correction, leave and business trip, and calculating attendance data manually.

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

15.2.1 Check-in/out Correction

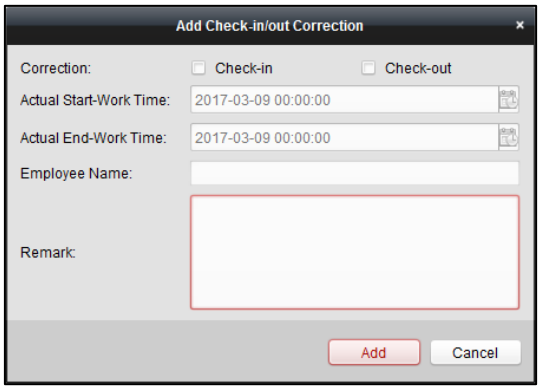
Purpose:

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

Add Check-in/out Correction

Steps:

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



3. Set the check-in/out correction parameters.

   For Check-in Correction: Check **Check-in** checkbox and set the actual start-work time.

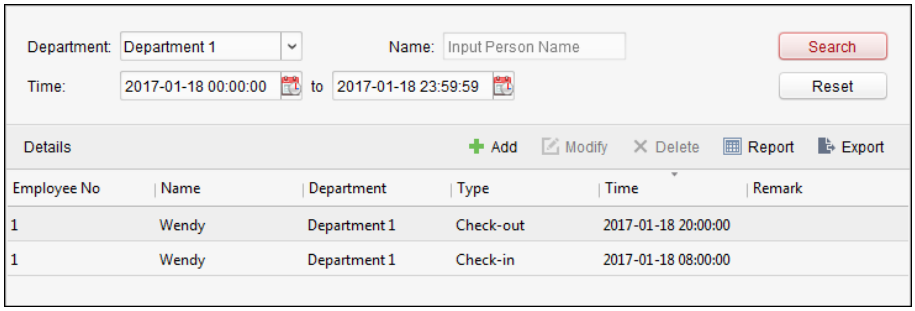
   For Check-out Correction: Check **Check-out** checkbox and set the actual end-work time.

4. Click **Employee Name** field and select the person.
   You can also input the keyword and click to search the person you want.
5. (Optional) Input the remark information as desired.
6. Click **Add** to add the check-in/out correction.
   The added check-in/out correction will display on the Attendance Handling interface.
   (Optional) Select the check-in/out correction and click **Modify** to edit the correction.
   (Optional) Select the check-in/out correction and click **Delete** to delete the correction.
   (Optional) Click **Report** to generate the check-in/out correction report.
   (Optional) Click **Export** to export the check-in/out correction details to local PC.
   Note: The exported details are saved in *.csv format.

Search Check-in/out Correction

Steps:

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



15.2.2 Leave and Business Trip

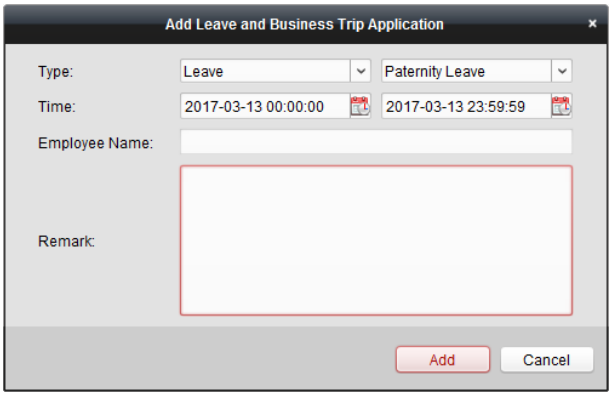
Purpose:

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

Add Leave and Business Trip

Steps:

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

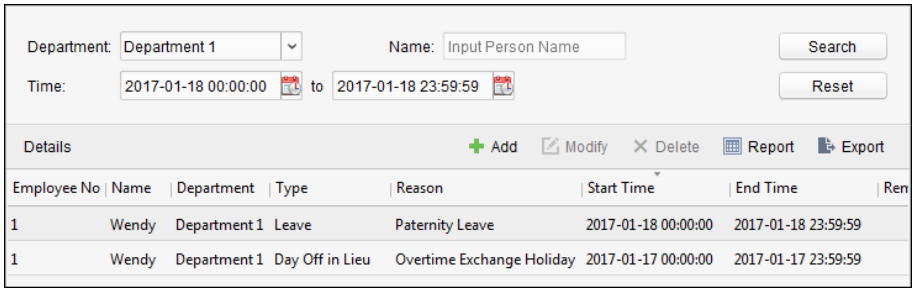


3. Select the leave and business trip type from the Type drop-down list.
   You can configure the leave type in Advanced Settings. For details, refer to *Chapter 15.3.5 Leave Type Settings*.
4. Click to set the specified time as time range.
5. Click **Employee Name** field and select the person for this application.
   You can also input the keyword and click to search the person you want.
6. (Optional) Input the remark information as desired.
7. Click **Add** to add the leave and business trip.
   The added leave and business trip will display on the Attendance Handling interface.
   (Optional) Select the leave and business trip and click **Modify** to edit the leave or business trip.
   (Optional) Select the leave and business trip and click **Delete** to delete the leave or business trip.
   (Optional) Click **Report** to generate the leave or business trip report.
   (Optional) Click **Export** to export the leave or business trip details to local PC.
   Note: The exported details are saved in *.csv format.

Search Leave and Business Trip

Steps:

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



15.2.3 Manual Calculation of Attendance

Purpose:

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

Steps:

5. Click **Manual Calculation of Attendance** tab.
6. Set the start time and end time for calculation.
7. Click **Calculate** to start.

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

15.3 Advanced Settings

Purpose:

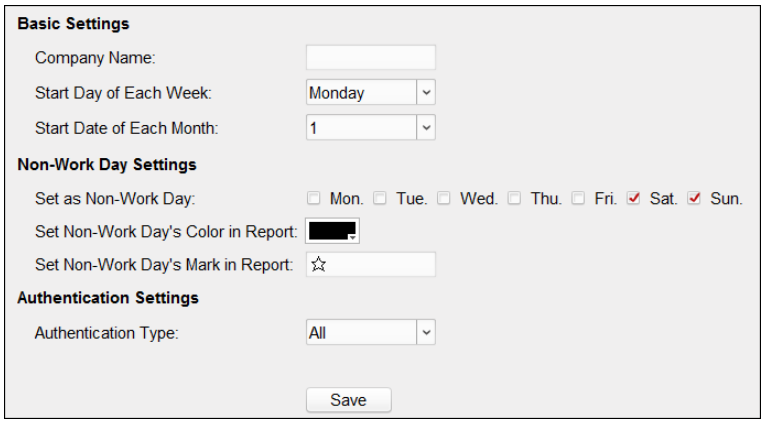
You can configure the basic settings, attendance rule, attendance check point, holiday settings and leave type for attendance.

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

15.3.1 Basic Settings

Steps:

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



2. Set the basic settings.

   Start Day of Each Week: You can select one day as the start day of each week.

   Start Date of Each Month: You can select one day as the start date of each month.

3. Set the non-work day settings.

   Set as Non-Work Day: Check the checkbox(es) to set the selected day(s) as non-work day.

   Set Non-Work Day's Color in Report: Click the color filed and select the color to mark the non-work day in report.

   Set Non-Work Day's Mark in Report: Input the mark as non-work day in report.

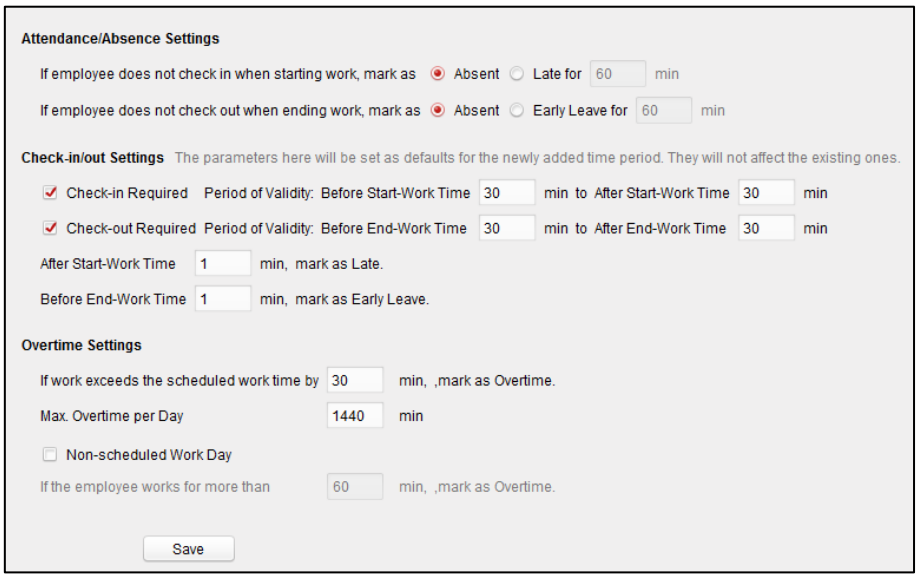
4. Set the authentication type, which means the client will calculate the attendance data recorded based on the selected authentication type.

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

15.3.2 Attendance Rule Settings

Steps:

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



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

15.3.3 Attendance Check Point Settings

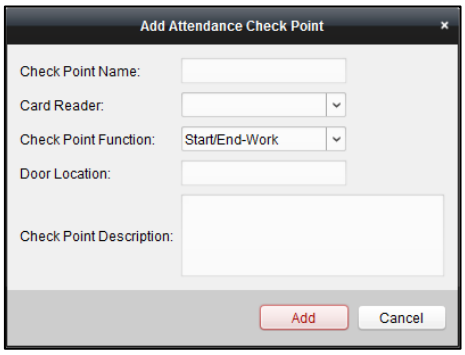
You can set the card reader(s) of the access control point as the attendance check point, so that the card swiping on the card reader(s) will be valid for attendance.

Steps:

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

interface.

2. Click to pop up Add Attendance Check Point window.



3. Set the related information.

   Check Point Name: Input a name for check point.

   Card Reader: Select the card reader from the drop-down list.

   Check Point Function: Select the function for check point.

   Door Location: Input the door location.

   Check Point Description: Set the description information for check point.

4. Click **Add** to add the attendance check point.

   The added attendance check point will display on the list.

5. (Optional) Check **Set All Card Readers as Check Points** checkbox.

   You can use all the card readers as check points.

   Note: If this checkbox is unchecked, only the card readers in the list will be added as attendance check points.

You can also edit or delete the card readers.

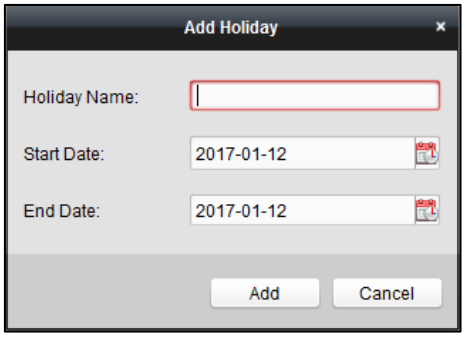
Click to edit the card reader.

Click to delete the card reader.

15.3.4 Holiday Settings

Steps:

1. Click **Holiday Settings** tab to enter the Holiday Settings interface.
2. Click to pop up Add Holiday window.



3. Set the related parameters.

   Holiday Name: Input the name for the holiday.

   Start Date / End Date: Click to specify the holiday date.

4. Click **Add** to add the holiday.

The added holiday will display on the list.

You can also edit or delete the holiday.

Click to edit the holiday.

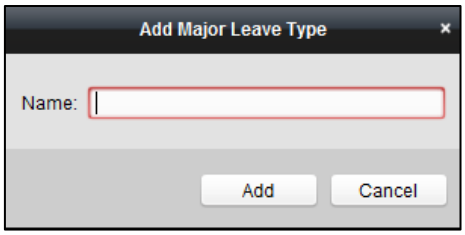
Click to delete the holiday.

15.3.5 Leave Type Settings

Purpose

Steps:

1. Click **Leave Type Settings** tab to enter the Leave Type Settings interface.
2. Add the major leave type.
   1) Click on the left panel to pop up the Add Major Leave Type window.



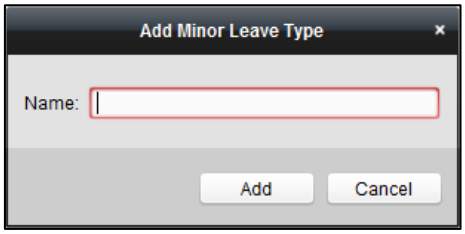
   2) Input the name for major leave type.
   3) Click **Add** to add the major leave type.

   You can also edit or delete the major leave type.

   Click to edit the major leave type.

   Click to delete the major leave type.
3. Add the minor leave type.
   1) Select the major leave type.

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



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

   You can also edit or delete the major leave type.

   Click to edit the minor leave type.

   Click to delete the minor leave type.

15.4 Attendance Statistics

Purpose:

After calculating attendance data, you can check the attendance summary, attendance details,

abnormal attendance, overtime, card swiping logs and reports based on the calculated attendance data.

Notes:

- The client automatically calculates the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to *Chapter 15.2.3 Manual Calculation of Attendance.*

15.4.1 Attendance Summary

Purpose:

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

Steps:

1. In the Time and Attendance module, click **Attendance Statistics** tab to enter the Attendance Statistics page.
2. Click **Attendance Summary** item on the left panel to enter the Attendance Summary interface.
3. Set the search conditions, including department, employee name and attendance date.
   (Optional) You can click **Reset** to reset all the configured search conditions.
4. Click **Search** to start searching and the matched results will list on this page.
   (Optional) Click **Report** to generate the attendance report.
   (Optional) Click **Export** to export the results to the local PC.

15.4.2 Attendance Details

Steps:

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

15.4.3 Abnormal Attendance

You can search and get the statistics of the abnormal attendance data, including No., name and department of the employees, abnormal type, start/end time and date of attendance. For detailed operations, refer to *Chapter 15.4.1 Attendance Summary*.

15.4.4 Overtime Search

You can search and get the overtime status statistics of the selected employee in the specified time period. And you can check the detailed overtime information, including No., name and department of the employees, attendance date, overtime duration and overtime type. For detailed operations, refer to *Chapter 15.4.1 Attendance Summary*.

15.4.5 Card Swiping Log

You can search the card swiping logs used for the attendance statistics. After searching the logs, you can check the card swiping details, including name and department of the employees, card swiping time, card reader authentication mode and card No.. For detailed operations, refer to *Chapter 15.4.1 Attendance Summary*.

15.4.6 Report

In the Attendance Statistics page, click **Report** item on the left panel to enter the Report interface. It supports to generate 12 kinds of attendance report: Total Overtime Monthly Report, Overtime Details Monthly Report, Attendance Monthly Report, Start/End-Work Time Report, Department Attendance Report, Valid Card Swiping Record Report, Attendance Daily Report, First Check-in and Last Check-out Report, Continuous Absence Report, Continuous Early Leave Report, and Continuous Early late Report.

Chapter 16 Video Intercom

Purpose:

The Video Intercom Management module provides the function of video intercom, checking call logs and managing notice via the iVMS-4200 client software.

Note: For the user with access control module permissions, the user can enter the Access Control module and manage video intercom and search information. For setting the user permission of Access Control module, refer to *Chapter 20 Account Management.*

Before you start:

Before you can remote control the video intercom, you should add the device to the software and configure the person to link the device in the Access Control module.

Notes:

- Up to 16 door stations can be added, and up to 512 indoor stations or master stations can be added. For details about adding the video intercom, refer to *Chapter 3.1 Adding Device*.
- For details about configuring person in the Access Control module, refer to *Chapter 14.3 Person Management*.

Click  on the Control Panel, or click **View-> Access Control** to open the Access Control page.

Click  tab on the left icon bar to enter the Video Intercom interface.

16.1 Video Intercom

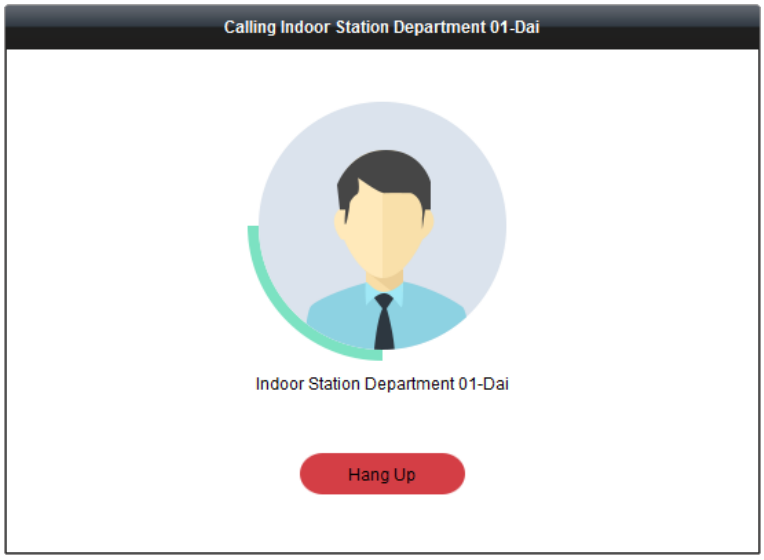
Purpose:

In this section, you can call the residents via the iVMS-4200 client software and the residents can also call the client software via the indoor station. In addition, calling the client software via door station is also available.

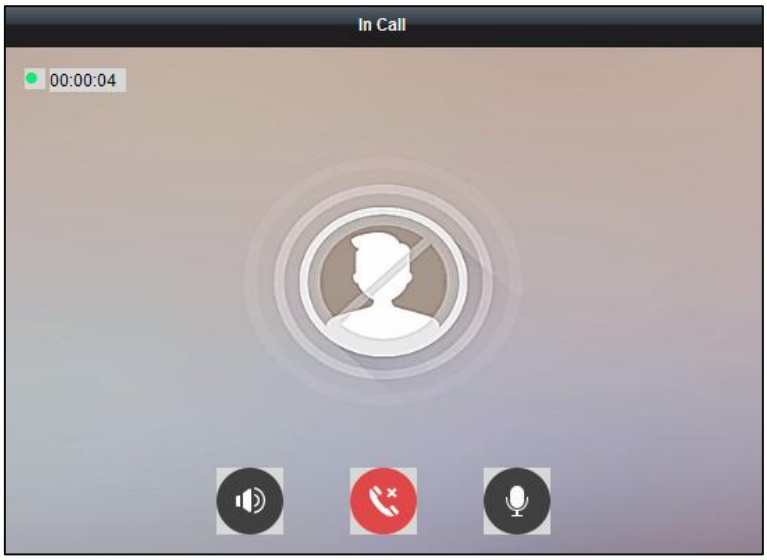
16.1.1 Calling Indoor Station via iVMS-4200

Steps:

1. Click  tab on the left icon bar to enter the Video Intercom interface.
2. Unfold the organization list on the left panel and click to select a resident group.
   The information, including resident name, linked device name and device IP address, of all the residents in the selected group will display on the right panel.
3. Select a resident, or input the keyword in the Filter field to find the desired resident.
4. Click the icon  in the Call Household column to start calling the selected resident.



After answered, you will enter the In Call window.



Click to adjust the volume of the loudspeaker.

Click to hang up.

Click to adjust the volume of the microphone.

Notes:

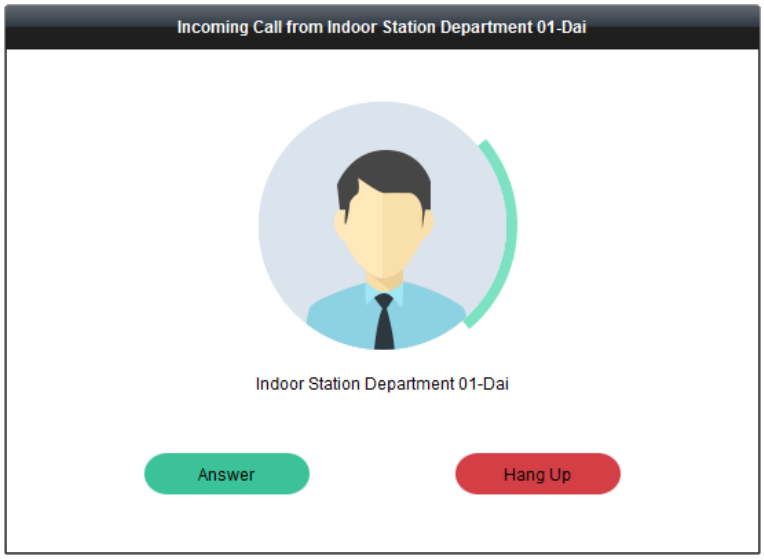
- One indoor station can only connect with one client software.
- You can set the maximum ring duration ranging from 15s to 60s, and the maximum speaking duration ranging from 120s to 600s via the Remote Configuration of indoor station.

16.1.2 Calling iVMS-4200 via Indoor Station/Door Station

Steps:

1. Select the client software in the indoor station or door station interface to start calling the iVMS-4200 and an incoming call window will pop up in the client software.

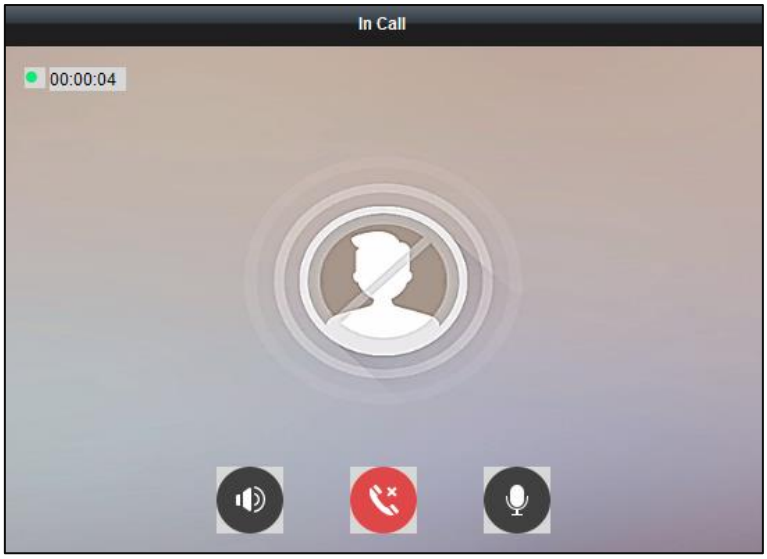
Here we take the **indoor station** as an example.



2. Click **Answer** to answer the call.

   Or click **Hang Up** to decline the call.

3. After you answer the call, you will enter the In Call window.



Click  to adjust the volume of the loudspeaker.

Click  to hang up.

Click  to adjust the volume of the microphone.

For door station, you can click  to open the door remotely.

Notes:

- One video intercom device can only connect with one client software.
- The maximum ring duration can be set from 15s to 60s via the Remote Configuration of the video intercom device.
- The maximum speaking duration between indoor station and iVMS-4200 can be set from 120s to 600s via the Remote Configuration of indoor station.

- The maximum speaking duration between door station and iVMS-4200 can be set from 90s to 120s via the Remote Configuration of door station.

16.1.3 Viewing Live Video of Door Station and Outer Door Station

Purpose:

You can get the live view of the door station and outer door station in the Main View module and control the door station and outer door station remotely.

In the Main View module, double-click a door station or outer door station device or drag the device to a display window to start the live view.

Note: For detailed operations of live view, refer to *Chapter 4* Live View.

Right-click the live view window to open the right-click menu.

You can click **Unlock** on the menu to open the door remotely.

16.2 Real-Time Call Logs

Purpose:

You can view all the real-time call logs, including dialed call logs, received call logs and missed call logs. You can also directly dial via the log list and clear the logs.

Steps:

1. In the Video Intercom page, click **Call Log** tab to enter the Call Log page.
   All the call logs will display on this page and you can check the log information, e.g., call status, start time, resident's organization and name, device name and ring or speaking duration.
2. (Optional) Click in the Operation column to re-dial the resident.
3. (Optional) Click in the Operation column to delete the call log.

Or you can click **Clear** button at the upper right corner to clear all the logs.

Note: If you delete or clear the call log in real-time call log interface, you can still find the deleted logs in Search – Call Log interface. For details, refer to *Chapter 16.4.1 Searching Call Logs.*

16.3 Releasing Notice

Purpose:

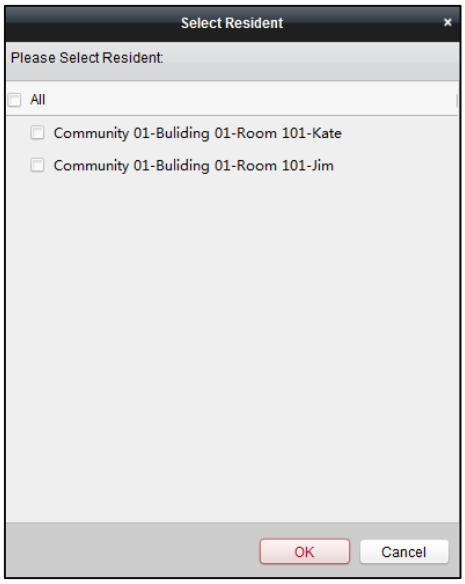
You can create different types of notices and send them to the residents. Four notice types are available, including Advertising, Property, Alarm and Notice Information.

Steps:

1. In the Video Intercom page, click **Release Notice** tab to enter the Release Notice page.
2. Click **New Notice** button on the left panel to create a new notice.
3. Edit the notice on the right panel.

   Steps:

   1) Click icon on the Send To field to pop up the Select Resident window.



   2) Check the checkbox(es) to select the resident(s).
   3) Click **OK**.
   4) Input the subject on the Subject field.

      Note: Up to 63 characters are allowed in the Subject field.
   5) Click in the Type field to unfold the drop-down list and select the notice type.
   6) (Optional) Click **Add Picture** to add a local picture to the notice.

      Note: Up to 6 pictures in the JPGE format can be added to one notice. And the maximum size of one picture is 512KB.
   7) Input the notice content in the Content field.

      Note: Up to 1023 characters are allowed in the Content field.
4. Click **Send** to send the edited notice to the selected resident(s).

The sent notice information will display on the left panel. You can click a notice to view the details on

the right panel.

16.4 Searching Video Intercom Information

Purpose:

You can search the call logs between the iVMS-4200 client software and video intercom devices, device unlocking logs, and the sent notice information.

In the Access Control module, click icon  tab to open the Search page.

16.4.1 Searching Call Logs

Purpose:

You can search the call logs of the video intercom devices in the specified time period.

Steps:

1. In the Search page, click **Call Log** tab to enter the searching call log interface.
2. Set the search conditions, including call status, device type, start time and end time.
3. Click **Search** and all the matched call logs will display.
4. (Optional) Click **Export** to export the call logs to your PC.

16.4.2 Searching Unlocking Logs

Purpose:

You can search the unlocking logs of the video intercom devices (Door Station or Door Station (V Series)) in the specified time period.

Steps:

1. In the Search page, click **Unlocking Log** tab to enter the searching unlocking log interface.
2. Set the search conditions, including unlocking type, device type, start time and end time.
   - **Unlocking Type:** Select who or how to unlock the door.
3. Click **Search** and all the matched unlocking logs will display.
4. (Optional) Click  in the Capture column to view the captured pictures.

   Note: It should be supported by device.
5. (Optional) Click **Export** to export the unlocking logs to your PC.

16.4.3 Searching Notice

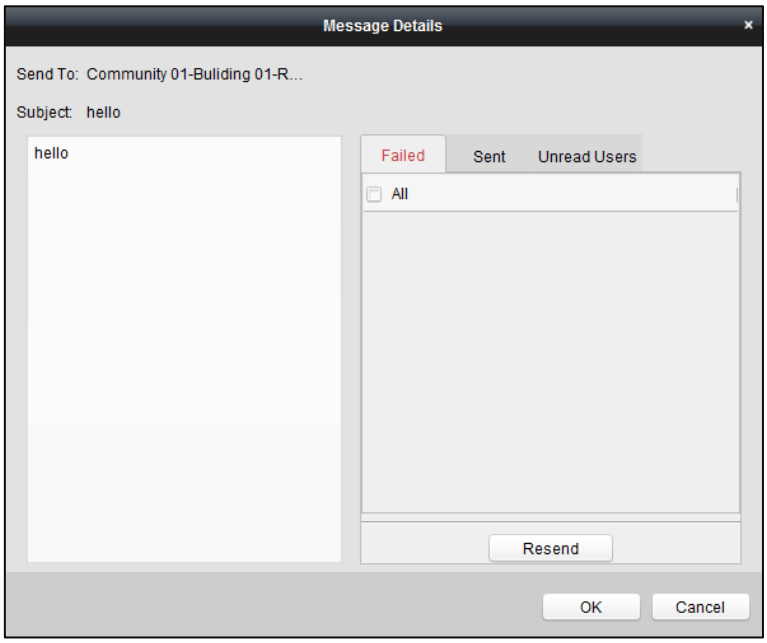
Purpose:

You can search the notice sent to the residents in the specified time period.

Steps:

1. In the Search page, click **Notice** tab to enter the searching notice interface.

2. Set the search conditions, including notice type, subject, recipient, start time and end time.
   - **Notice Type:** Select the notice type as **Advertising Information**, **Property Information**, **Alarm Information** or **Notice Information**.
3. Click **Search** and all the matched notices will display.
4. You can click  in the Operation column to view the notice details.



You can view and edit the notice details, check the sending failed/sent succeeded/unread users, and resend the notice to sending failed/unread users.

5. (Optional) Click **Export** to export the notices to your PC.

Chapter 17 Face Picture Comparison Alarm

Purpose:

For the device which supports face picture comparison, you can view the captured face pictures and the matched face picture in face picture library. You can also view the face capture alarm logs and face picture comparison alarm logs.

17.1 Viewing Captured Face Picture

Purpose:

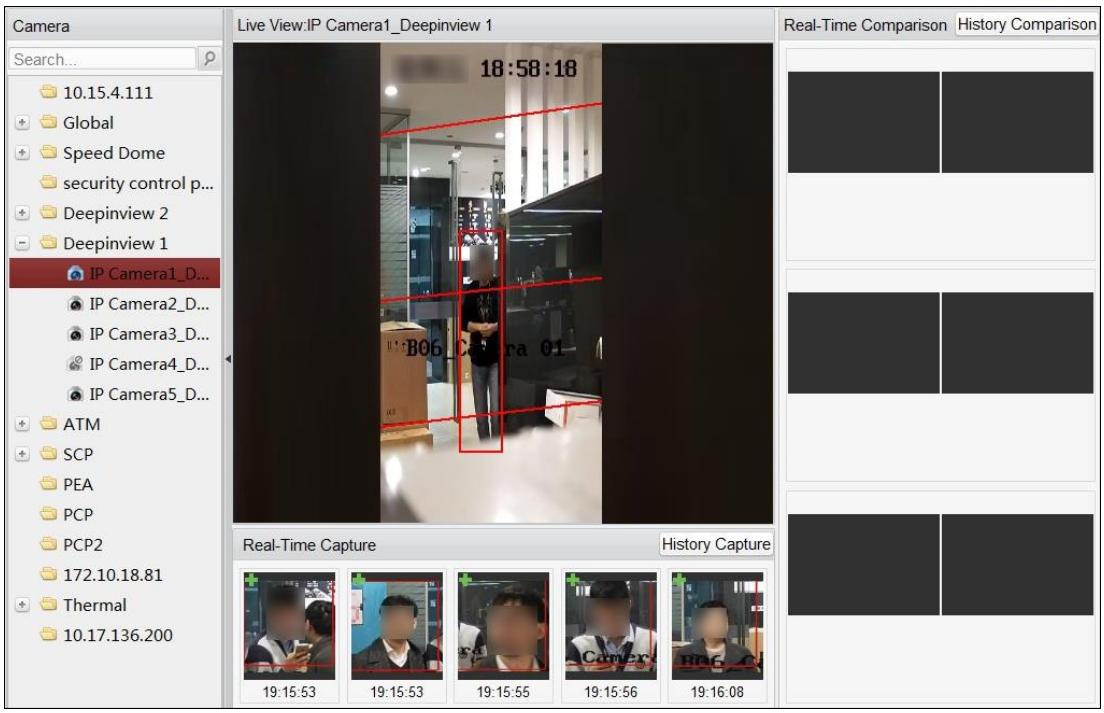
You can view the real-time or historical captured face pictures. You can add the face picture to the face picture library if no result matched in the library when necessary.

Before you start:

You should configure the capture rule first for the device. For details, refer to the *User Manual* of the device.

Steps:

1. Click **Face Picture Comparison Alarm** on the control panel to enter this module.
2. Double click a camera in the camera list to start live view.
   The captured face pictures and capture time will display in the Real-Time Capture list in real time.



3. (Optional) Click **History Capture** to view the historical captured face pictures.

   Notes:

   - Up to five pictures will be displayed in the real-time captured face pictures list.
   - Up to 100 pictures will be displayed in the historical captured face pictures list.

4. (Optional) Add the captured face picture to the face picture library.
   1) Click on the upper-left corner of the captured face picture to open the following window.

   2) Select a face picture library from the drop-down list.
   3) Input the person details.
   4) Click **OK**.
5. If the captured face picture is matched with the face picture in the library, the captured picture and picture in library will display in the Real-Time Comparison list on the right.
   You can view the matched person details, such as similarity, name, gender, age, etc.
6. (Optional) Click **History Comparison** to view the historical matched face pictures.
   Notes:
   - Up to three real-time matched records (captured face and face in library) will be displayed in the linked face/human body pictures list.
   - Up to 100 historical matched records (captured face and face in library) will be displayed in the history list.

17.2 Viewing Matched Face Pictures

Purpose:

If the captured face picture matches with the face picture in the face picture library, you can view the matched person details. You can view the real-time or historical face picture comparison records.

Before you start:

You should configure the face picture library first for the device. For details, refer to the *User Manual* of the device.

Steps:

1. Click **Face Picture Comparison Alarm** on the control panel to enter this module.
2. Double click a camera in the camera list to start live view.
   If the captured face picture is matched with the face picture in the library, the captured picture and picture in library will display in the Real-Time Comparison list on the right.
3. View the matched person details, such as similarity, name, gender, age, etc.
4. (Optional) Click **History Comparison** to view the historical matched face pictures.
   Notes:
   - Up to three real-time matched records (captured face and face in library) will be displayed in the linked face/human body pictures list.

- Up to 100 historical matched records (captured face and face in library) will be displayed in the history list.

17.3 Viewing Alarm Logs

Purpose:

You can view the face capture alarm logs and face picture comparison alarm logs and export them to the local PC.

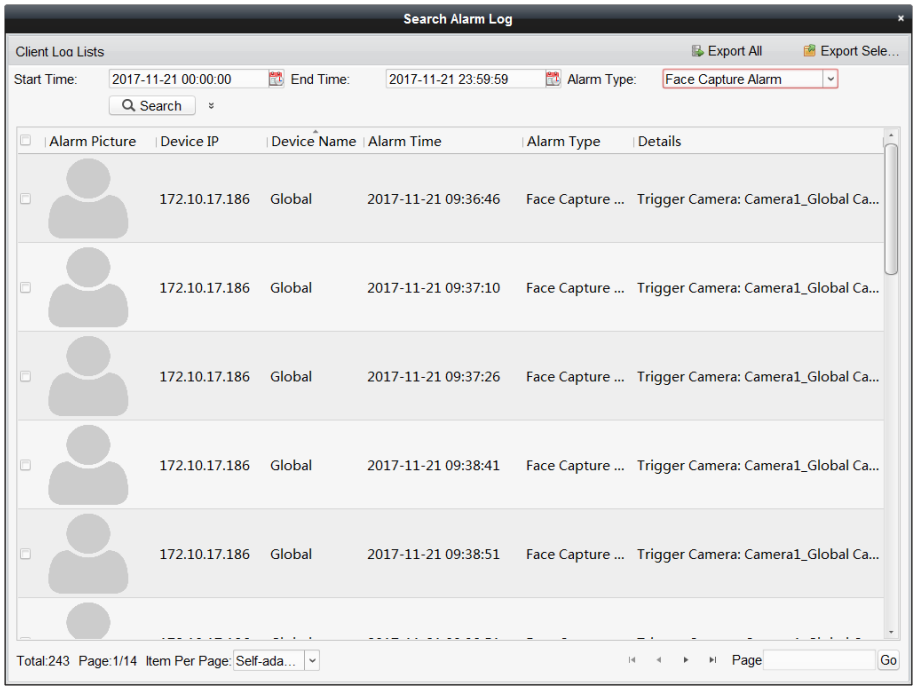
17.3.1 Searching Alarm Logs

Purpose:

You can search the client logs including face capture alarm or face picture comparison alarm on the current client. You can also export the logs to the local PC.

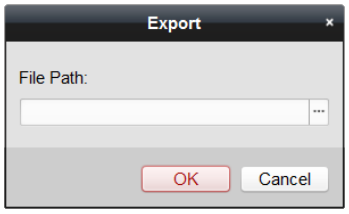
Steps:

1. On the client menu bar, click **Tool > Search Alarm Log**.
2. Click to display other search conditions.
3. Set the search condition, such as time period for search, alarm type, device IP address, device name, etc.
4. Click **Search** to start searching the alarm logs.
   The matched alarm logs will display.
   Note: You can view the alarm logs if the camera has been configured with Storage Server to save the alarm pictures. For setting the picture storage on Storage Server, refer to *Chapter 5.1.2 Storing on Storage Device.*



5. (Optional) Export the all the searched alarm logs, including alarm picture, device IP address, device name, alarm time, alarm details, etc.

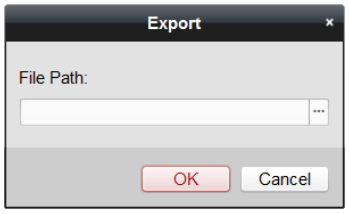
1) Click **Export All.**



2) Click ... to select a saving path on local PC and create a name for the exported file.
3) Click **OK** to start exporting the alarm logs.

Note: The file exported is in XML file.

6. (Optional) Export the selected alarm logs, including alarm picture, device IP address, device name, alarm time, alarm details, etc.
   1) Click **Export Selected.**



   2) Click ... to select a saving path on local PC and create a name for the exported file.
   3) Click **OK** to start exporting the alarm logs.

      Note: The file exported is in XML file.

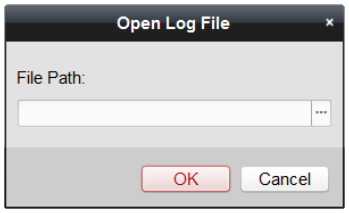
17.3.2 Open Alarm Logs

Purpose:

You can open the alarm log files exported from other client and search the alarm logs by setting search conditions to view the alarm details.

Steps:

1. On the client menu bar, click **Tool > Open Alarm Log**.
2. Open the exported alarm log file.
   1) Click **Open**.



   2) Click ... to select an exported log file.

      Note: The log file is in XML format.

   3) Click **OK** to import the logs.

      The alarm logs in the log file will display.
3. Click ⌄⌄ to display other search conditions.
4. Set the search condition, such as time period for search, alarm type, device IP address, device name, etc.
5. Click **Search** to start searching the alarm logs.

   The matched alarm logs will display.

Chapter 18 Target Capture Alarm

Purpose:

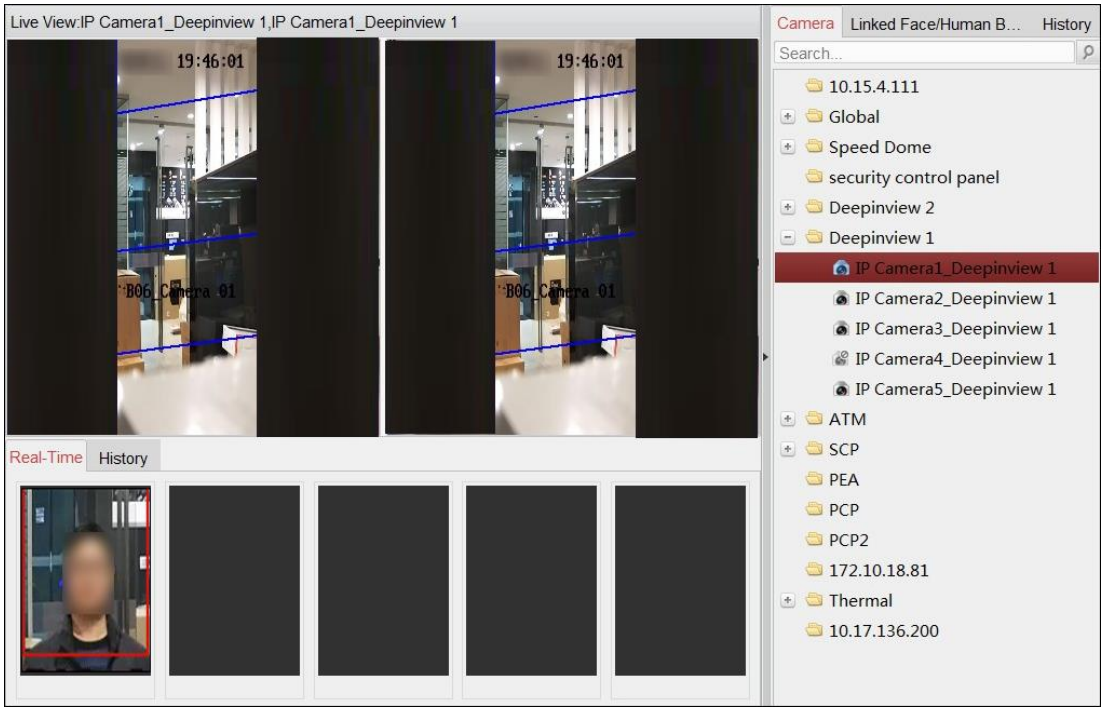
For the target capture camera which supports target capture alarm, you can view the captured target pictures, such as face, human body, vehicle, etc.

Before you start:

You should configure the target capture alarm rule of the device first. For details, refer to the *User Manual* of the device.

Steps:

1. Enter the Target Capture Alarm module.
2. Start live view for the cameras.
   1) Select a window for live view.
   2) In the Camera tab, double-click the camera to start live view in the selected window.
      The captured target pictures will be displayed below.



   3) (Optional) Move to the live view window and click on the toolbar to capture a picture.
   4) (Optional) Move to the live view window and click on the toolbar to start recording.
3. Click **Real-Time** or **History** tab below to view the real-time captured or historical pictures.

   Notes:

   - Up to five pictures will be displayed in the real-time captured target pictures list.
   - Up to 100 pictures will be displayed in the historical captured target pictures list.
4. (Optional) If the captured target is human body or face, you can click **Linked Face/Human Body** or **History** tab on the right to view the target's captured face and human body pictures.

   Notes:

   - Up to three real-time records (human body and face) will be displayed in the linked face/human body pictures list.
   - Up to 100 historical records (human body and face) will be displayed in the history list.

Chapter 19 Log Management

Purpose:

The log files of the client software are stored on the local PC and can be searched for checking. Two types of log files are provided: client logs and remote logs. The client logs refer to the log files of the client and are stored on the local PC; the remote logs refer to the log files of the connected devices and are stored on the local device.

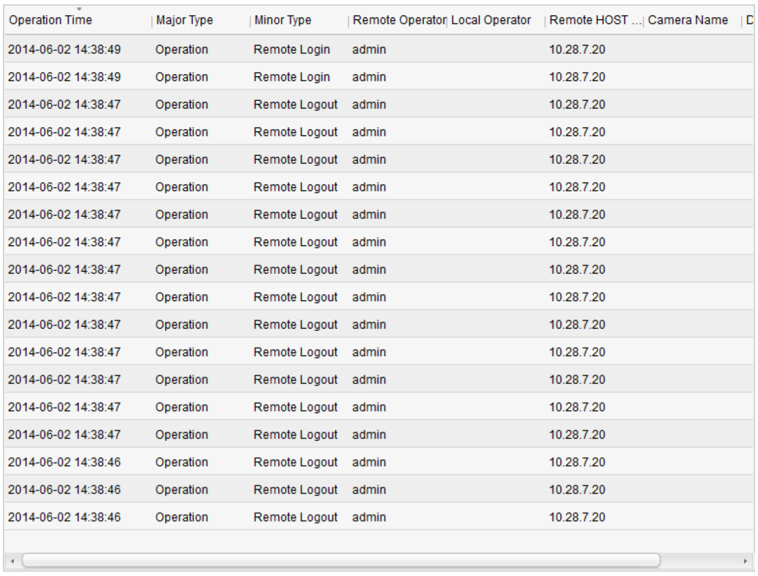
Click icon on the control panel to open the Log Search page.

19.1 Searching Log Files

Steps:

1. Open the Log Search page.
2. Select the log type. If **Remote Logs** is selected, then click to specify the device for search.
3. Click the icon to specify the start time and end time.
   Note: You can search the logs within one month.
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		

19.2 Filtering Log Files

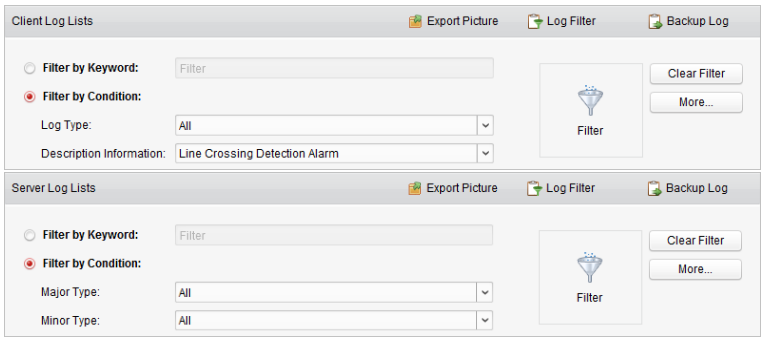
Purpose:

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.



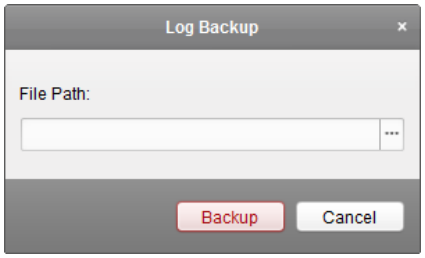
19.3 Backing Up Log Files

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 window 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.



19.4 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 window 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 20 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.

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

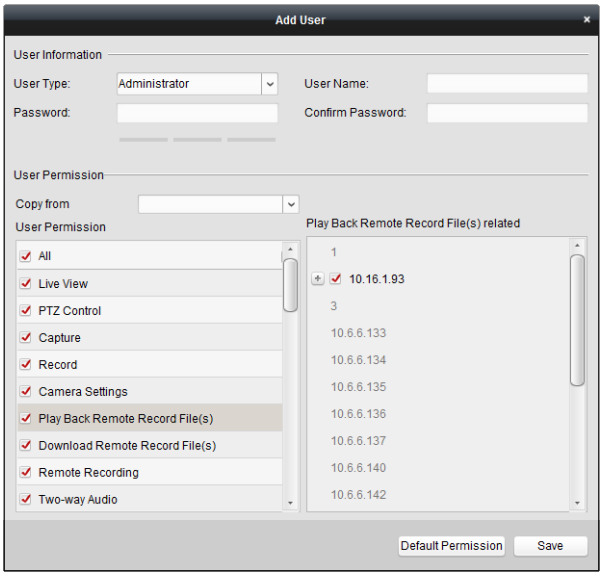
20.1 Adding User

Steps:

1. Open the Account Management page.
2. Click **Add User** to open the Add User window box.
3. Select the user type from the drop-down list. Two 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.
6. Optionally, you can select a user in the **Copy from** drop-down list, to copy the permissions of the selected user.
7. Optionally, you can click **Default Permission** to restore the default permissions of this user.
8. 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.



20.2 Managing 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.

Chapter 21 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.

21.1 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:

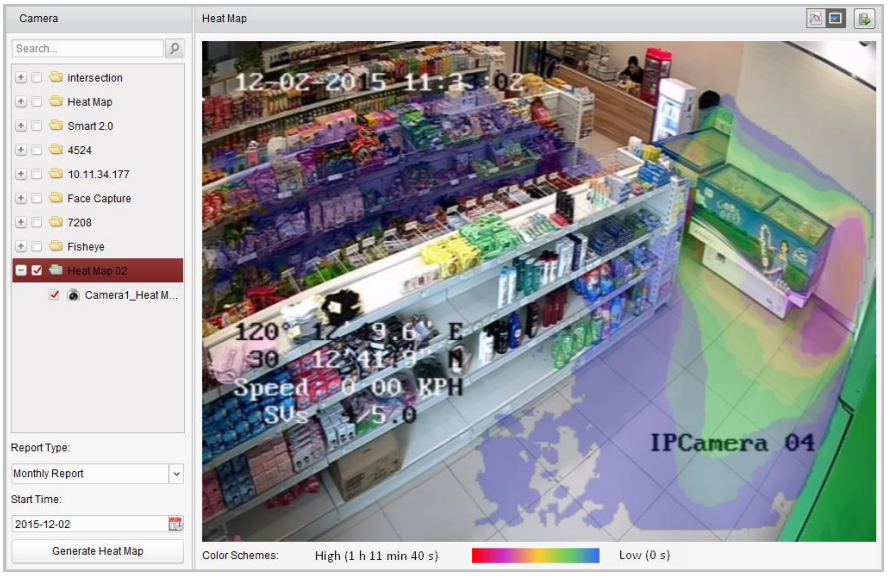
Please add a heat map network camera to the software and properly configure the corresponding area. The added camera should have been configured with heat map rule.

Note: The heat map network camera should be added to the software as Encoding Device, refer to *Chapter 3.1 Adding Device* for detailed configuration. For configuring heat map rule, refer to the *User Manual* of the heat map network camera.

Steps:

1. Open the Heat Map page.
2. 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.



21.2 People Counting

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.

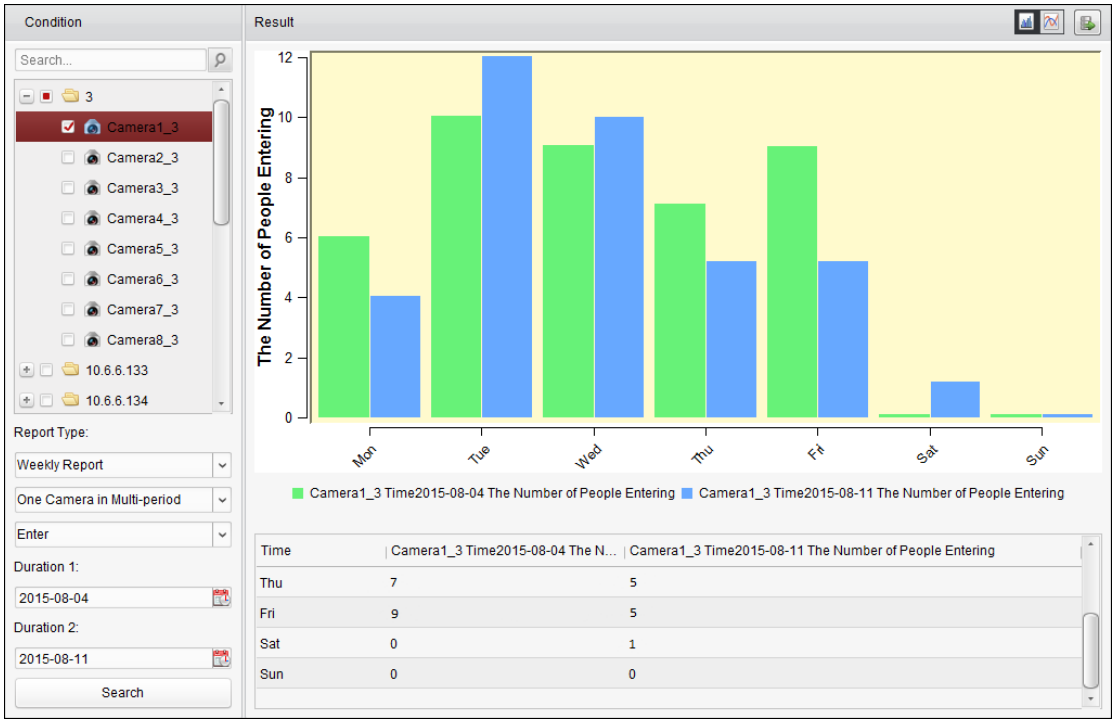
Before you start:

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, refer to *Chapter 3.1 Adding Device* for detailed configuration. For configuring people counting rule, refer to the *User Manual* of the people counting device.

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.



21.3 Counting

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, refer to *Chapter 3.1 Adding Device* for detailed configuration. For configuring counting settings, refer to the *User Manual* of the counting device.

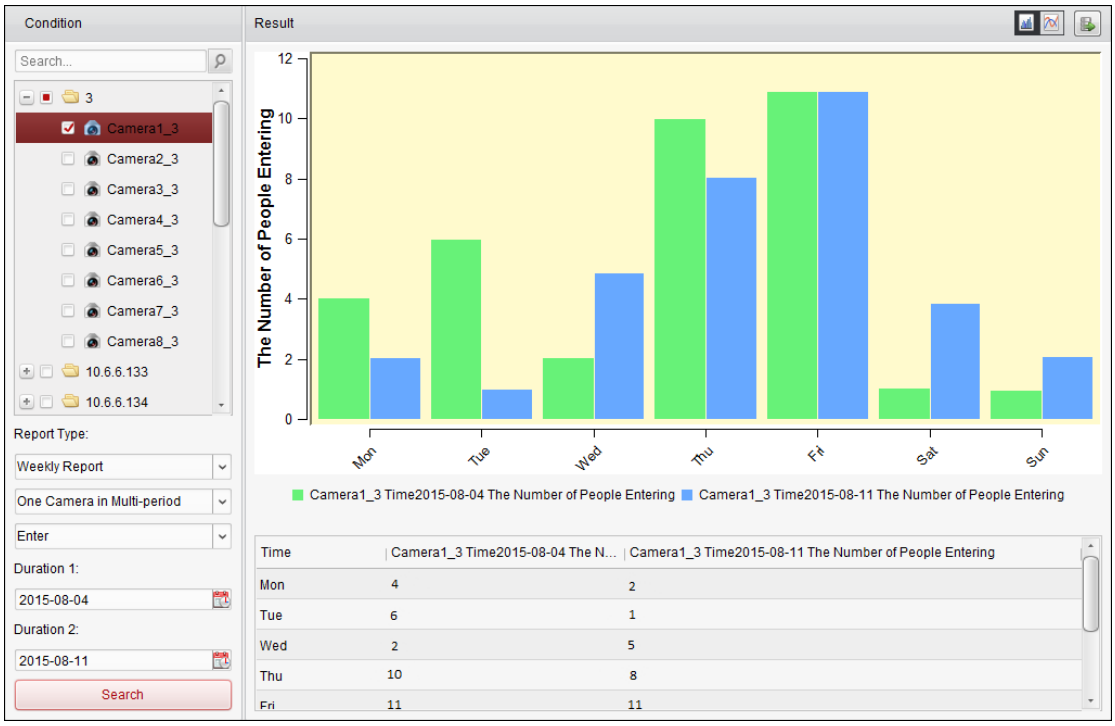
Steps:

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.



21.4 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, 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, refer to *Chapter 3.1 Adding Device* for detailed configuration. For configuring capture settings, refer to the *User Manual* of the device.

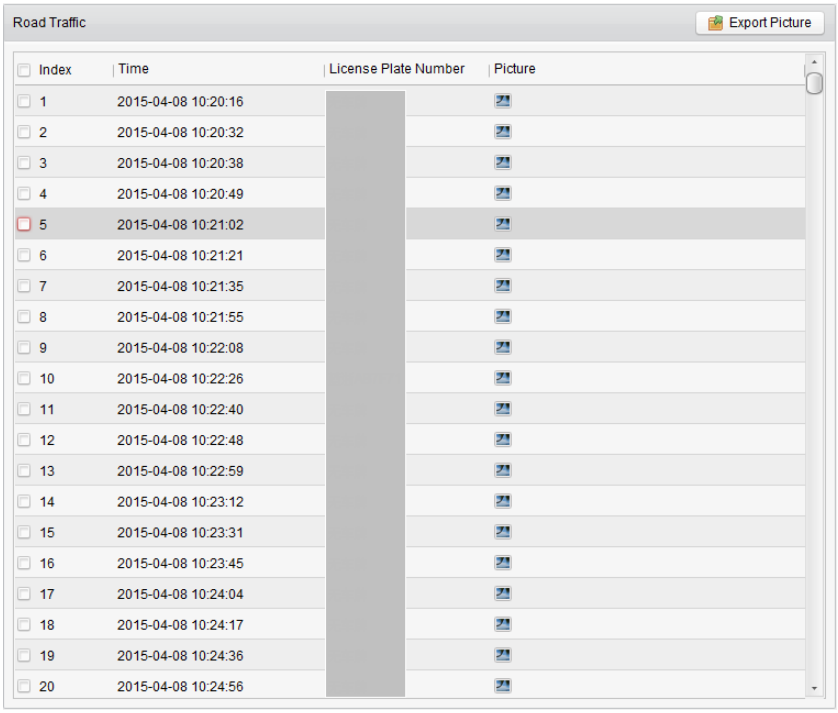
Steps:

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.

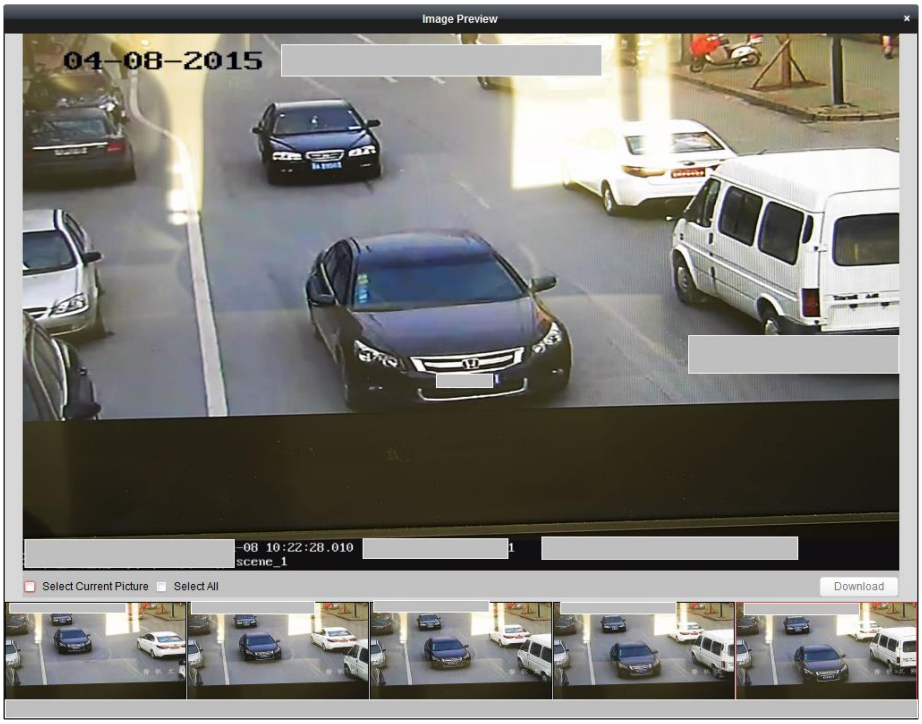
   Type: Select the query type and the pictures triggered by the event type can be found.

   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.



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.

21.5 Face Picture Retrieval

Purpose:

When the connected device (NVR, HDVR, or DeepinMind device) supports face search, you can search the related picture and play the picture related video file.

21.5.1 Searching Face Picture by Uploaded Picture

Purpose:

You can upload a face picture from local PC and compare the uploaded picture with the device's captured face pictures.

Before you start:

Add the device to the software and properly configure the corresponding settings. For detailed settings, refer to the *User Manual* of the device.

Steps:

1. Open the Face Picture Retrieval page.
2. Select a device in the camera panel.

   Note: This function should be supported by the connected device.
3. Check **By Picture** and click **Select Picture** to select a picture for comparison from local PC.

   Notes:

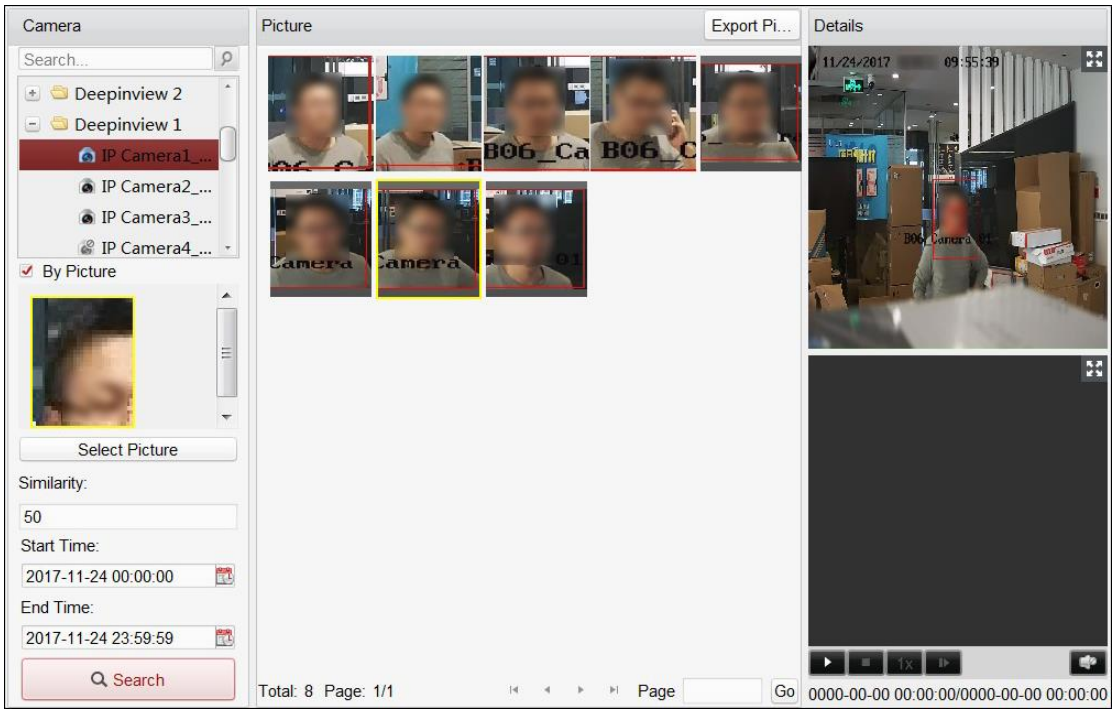
   - The picture should be smaller than 4 MB.
   - The resolution of the picture should be smaller than 4096*4080.

- Only JPG and JPEG formats are supported.

4. Select a face you want to search by.
5. 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.
6. Click to set the start time and end time for searching the captured face pictures or video files.
7. Click **Search** to start searching.

   The search results of the pictures are displayed in list by similarity.



8. (Optional) Perform secondary search based on the search result.
   1) Move to the searched picture and click .

      All the faces in this picture will be analyzed and displayed.
   2) Select a face you want to do secondary search.
   3) Set the similarity and time period.
   4) Click **Search**.

      The client will search and compare the faces in the captured pictures based on the face picture you selected.
9. 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.
10. 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.
11. 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 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.

21.5.2 Searching Face Picture by Event Type

Purpose:

You can search the device's captured face pictures by filtering different event types.

Before you start:

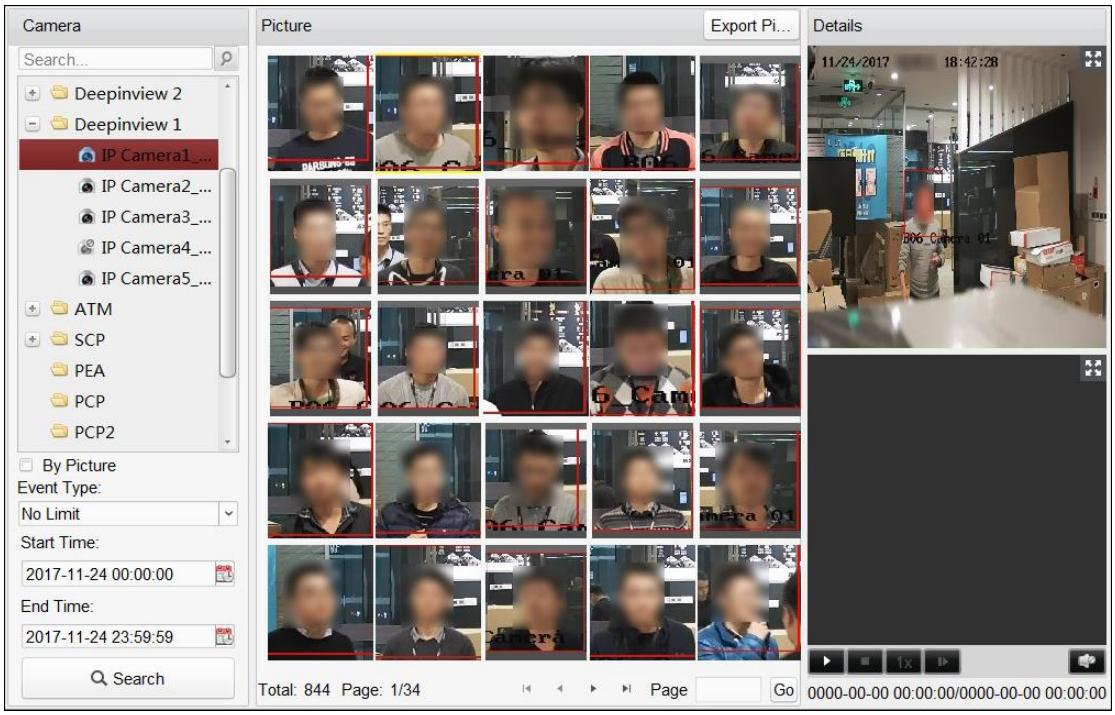
Add the device to the software and properly configure the corresponding settings. For detailed settings, refer to the *User Manual* of the device.

Steps:

1. Open the Face Retrieval page.
2. Select a device in the camera panel.

   Note: This function should be supported by the connected device.
3. Select the event type of the face pictures you want to search.
4. Click to set the start time and end time for searching the captured face pictures or video files.
5. Click **Search** to start searching.

   The search results of the pictures are displayed in list.



6. (Optional) Perform secondary search based on the search result.
   1) Move to the searched picture and click .

      All the faces in this picture will be analyzed and displayed.
   2) Select a face you want to do secondary search.
   3) Set the similarity and time period.
   4) Click **Search**.

      The client will search and compare the faces in the captured pictures based on the face picture you selected.

7. Click on a picture from the list to check the detailed information.
   You can click to show the large picture, and click to restore.
8. 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.
9. 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 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.

21.6 License Plate Retrieval

Purpose:

When the connected device 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, refer to the *User Manual* of the device.

Note: The device should be added to the software as Encoding Device, refer to *Chapter 3.1 Adding Device* for detailed configuration.

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 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.

21.7 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:

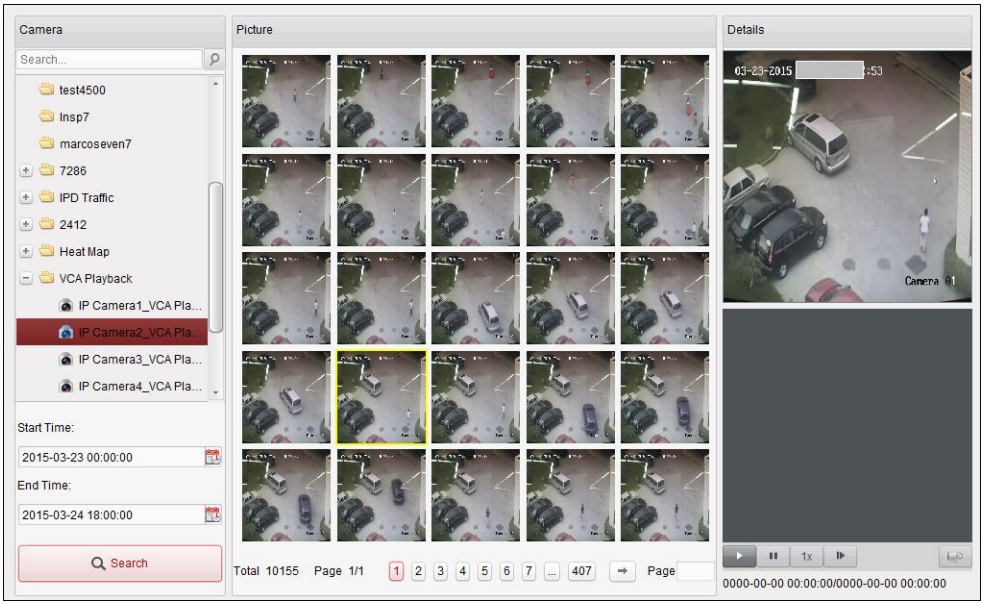
Please add the device to the software and properly configure the corresponding settings. For detailed settings, refer to the *User Manual* of the device.

Note: The device should be added to the software as Encoding Device, refer to *Chapter 3.1 Adding Device* for detailed configuration.

Steps:

1. Open the Behavior Analysis page.
2. 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.



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  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.

21.8 Captured Face Analysis

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, refer to the *User Manual* of the device.

Note: The face capture device should be added to the software as Encoding Device, refer to *Chapter 3.1 Adding Device* for detailed configuration.

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.

21.9 Human Body Retrieval

Purpose:

For the DeepinMind device, you can search the captured human body pictures by setting search conditions including uploading a picture from local PC and setting personnel features.

21.9.1 Searching Human Body Picture by Uploaded Picture

Purpose:

You can upload a human body picture from local PC and compare the uploaded picture with the device's captured human body pictures.

Before you start:

Add the device to the software and properly configure the corresponding settings. For detailed

settings, refer to the *User Manual* of the device.

Steps:

1. Open the Human Body Retrieval page.
2. Select a device in the camera panel.

   Note: This function should be supported by the connected device.
3. Check **By Picture** and click **Select Picture** to select a picture for comparison from local PC.

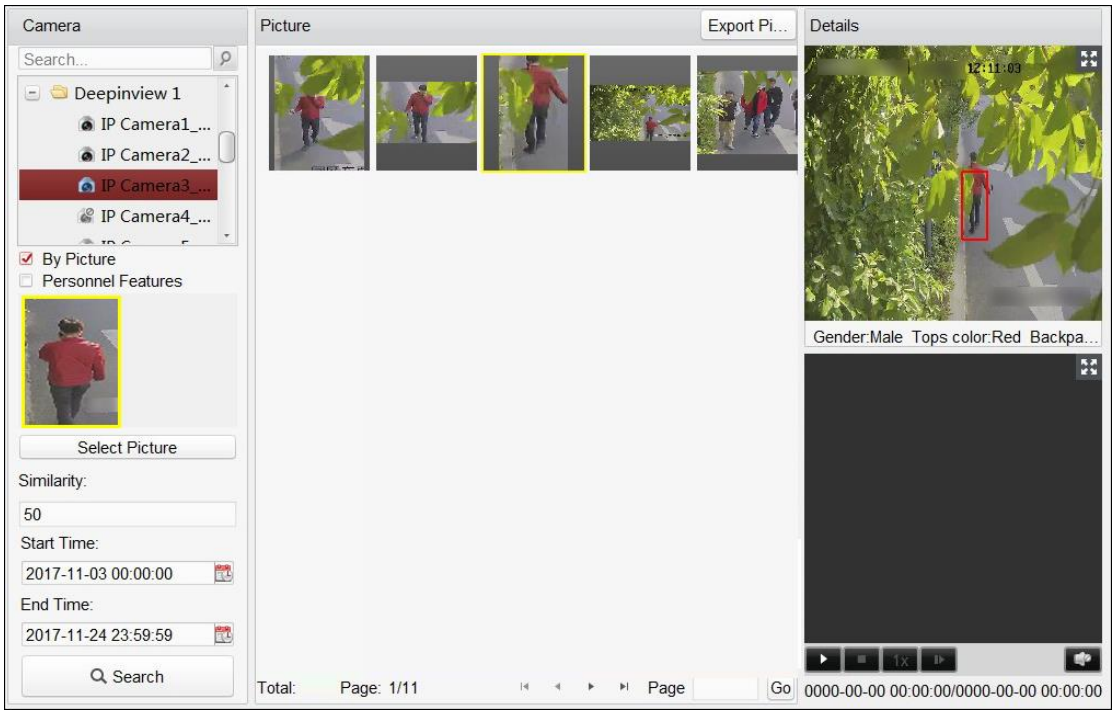
   All the human bodies in this picture will be analyzed and displayed.

   Notes:

   - The picture should be smaller than 4 MB.
   - The resolution of the picture should be smaller than 4096*4080.
   - Only JPG and JPEG formats are supported.
4. Select a human body you want to search for.
5. 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.
6. Click  to set the start time and end time for searching the captured human body pictures or video files.
7. Click **Search** to start searching.

   The search results are displayed in list.



8. (Optional) Perform secondary search based on the search result.

   1) Move to the searched picture and click  .

      All the human bodies in this picture will be analyzed and displayed.
   2) Select a human body you want to do secondary search.
   3) Set the similarity and time period.
   4) Click **Search**.

      The client will search and compare the human bodies in the captured pictures based on the human body picture you selected.

9. 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.
10. 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.
11. 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  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.

21.9.2 Searching Human Body Picture by Personnel Features

Purpose:

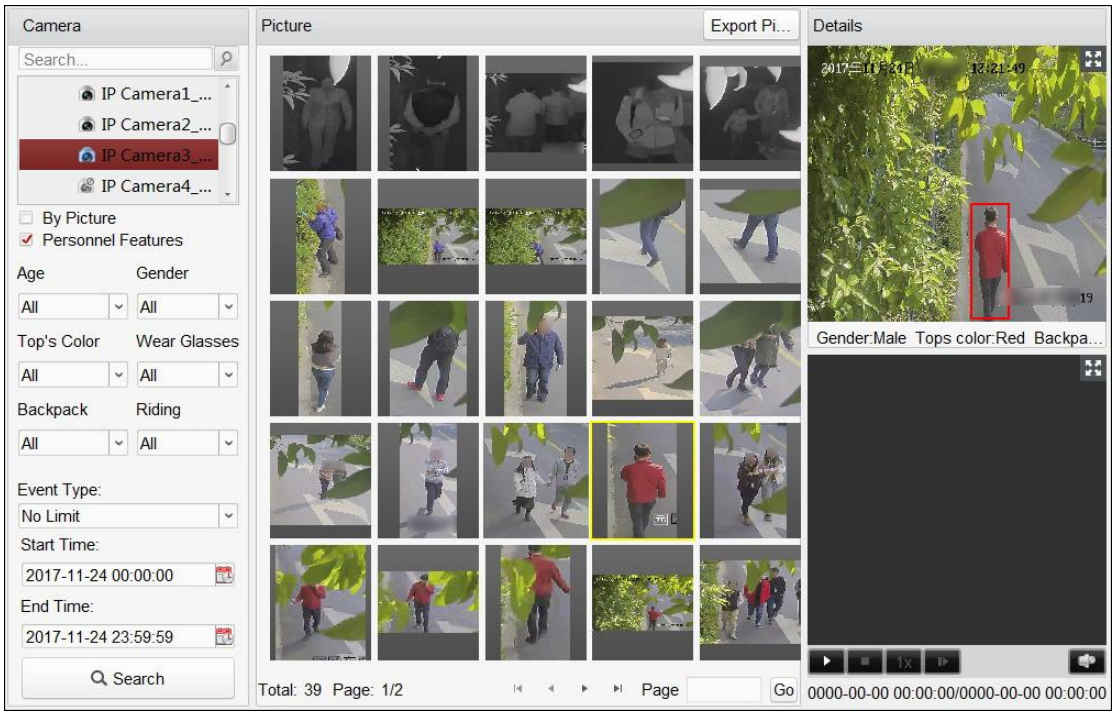
You can search the device's captured human body pictures by setting the personnel features as the search conditions, such as age group, gender, clothes, etc.

Before you start:

Add the device to the software and properly configure the corresponding settings. For detailed settings, refer to the *User Manual* of the device.

Steps:

1. Open the Human Body Retrieval page.
2. Select a device in the camera panel.
   Note: This function should be supported by the connected device.
3. Check **Personnel Features**.
4. Set the personnel features such as age group, gender, top's color, wearing glasses or not, etc.
5. Select the event type of the human body pictures you want to search.
6. Click  to set the start time and end time for searching the captured human body pictures or video files.
7. Click **Search** to start searching.
   The search results are displayed in list.



8. (Optional) Perform secondary search based on the search result.
   1) Move to the searched picture and click .
      All the human bodies in this picture will be analyzed and displayed.
   2) Select a human body you want to do secondary search.
   3) Set the similarity and time period.
   4) Click **Search**.
      The client will search and compare the human bodies in the captured pictures based on the human body picture you selected.
9. Click on a picture from the list to check the detailed information.
   You can click to show the large picture, and click to restore.
10. 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.
11. 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 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.

21.10 Vehicle Retrieval

Purpose:

You can search the device's captured vehicle pictures by setting the vehicle features as the search conditions, such as vehicle brand, color, type, plate number, etc.

Before you start:

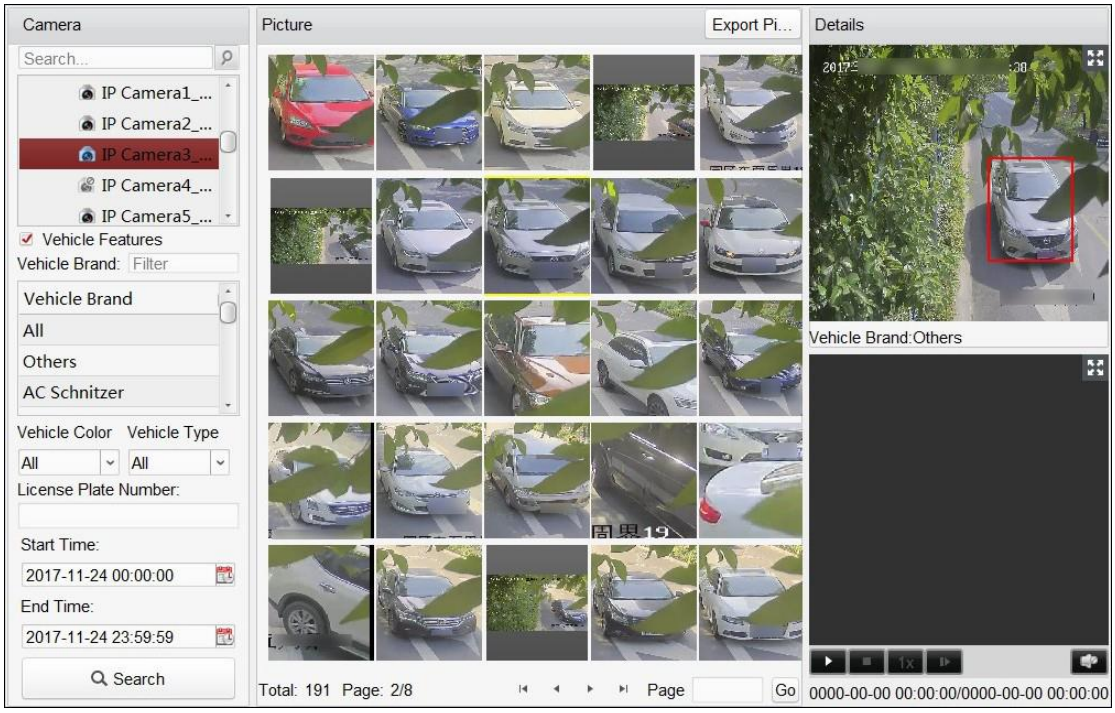
Add the device to the software and properly configure the corresponding settings. For detailed settings, refer to the *User Manual* of the device.

Steps:

1. Open the Vehicle Retrieval page.
2. Select a device in the camera panel.

   Note: This function should be supported by the connected device.
3. Check **Vehicle Features**.
4. Set the vehicle features such as vehicle brand, color, type, and plate number.
5. Click to set the start time and end time for searching the captured vehicle pictures or video files.
6. Click **Search** to start searching.

   The search results are displayed in list.



7. 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.
8. Click on a picture from the list to check the detailed information.

   You can click to show the large picture, and click to restore.
9. 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 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.

Chapter 22 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.

Note: You can click **Default Value** to restore the defaults of all the system configurations.

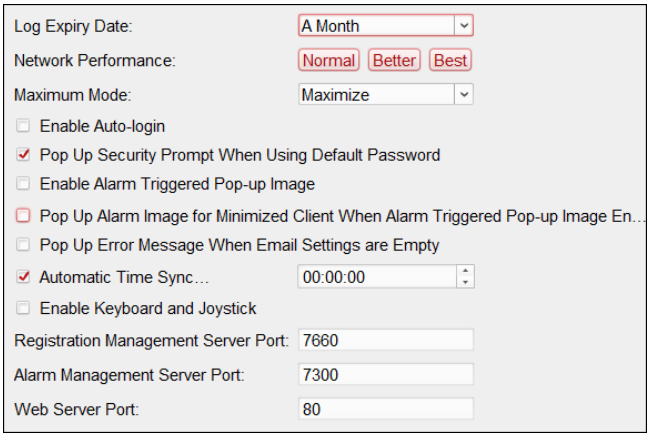
22.1 General Settings

Purpose:

The frequently-used parameters, including the log expired time, network performance, etc., can be set.

Steps:

1. Open the System Configuration page and click **General** tab to enter the General Settings interface.



2. Configure the 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	Enable the image pop-up when alarms occur. You can also click  or 

Pop-up Image	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 Alarm 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 22.8 Email Settings*.
Automatic Time Synchronization	Automatically synchronize the time of the added devices with the time of the PC running the client at a specified time point.
Enable Keyboard and Joystick	Set to enable the keyboard or joystick. After enabled, you can set the shortcuts for the keyboard and joystick. For details, refer to *Chapter 22.6 Keyboard and Joystick Shortcuts Settings.*
Registration Management Server Port	EHome port for registration management server. The port No. should be between 2000 to 65535. The default port No. is 7660. ***Note:*** Please restart the client to take effect.
Alarm Management Server Port	EHome port for alarm management server. The port number should be between 2000 to 65535. The default port number is 7300. ***Note:*** Restart the client to take effect.
Web Server Port	The port for device remote configuration via web server. The port number should be between 1 to 65535. The default port number is 80. ***Note:*** Restart the client to take effect.

3. Click **Save**.

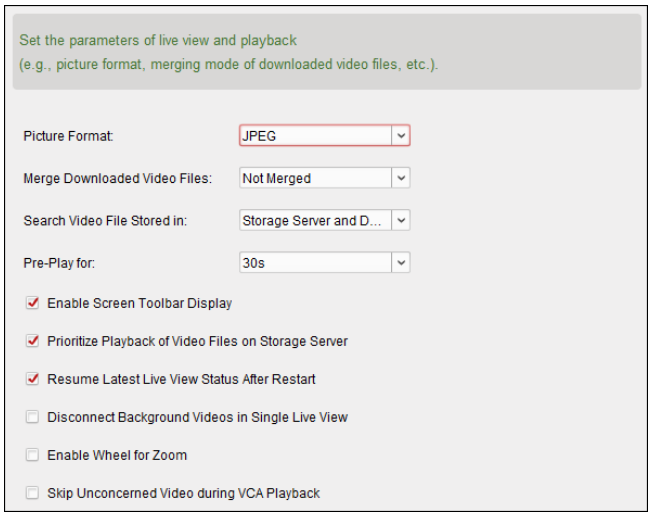
22.2 Live View and Playback Settings

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 and click **Live View and Playback** tab to enter the Live View and Playback Parameter Settings interface.



2. Configure the 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.

3. Click **Save**.

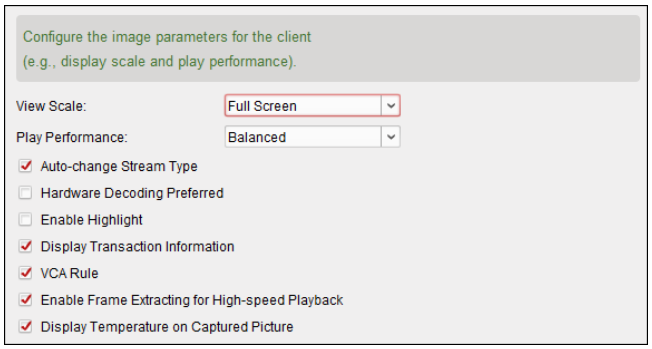
22.3 Image Settings

Purpose:

The image parameters of the software can be configured, such as view scale, play performance, etc.

Steps:

1. Open the System Configuration page and click **Image** tab to enter the Image Settings interface.



2. Configure the 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, Balanced, or Fluency.
Auto-change Stream Type	Change the video stream (main stream or sub-stream) automatically in live view according to the window division. When the window division is larger than 9, it will switch to sub-stream automatically. Or it remains main stream.
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.
Display Temperature on Captured Picture	For the thermal device, set to display the temperature information on the captured pictures.

3. Click **Save**.

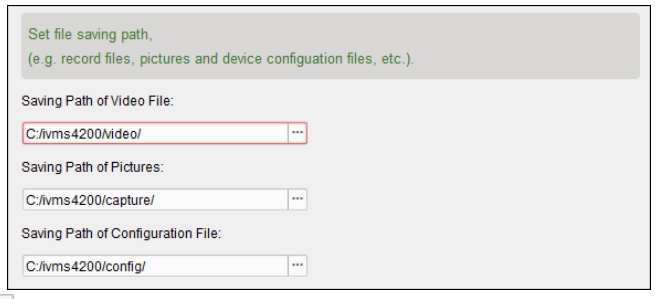
22.4 File Saving Path Settings

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 and click **File** tab to enter the File Saving Path Settings interface.



2. Click the icon and select a local path for the files.
3. Click **Save**.

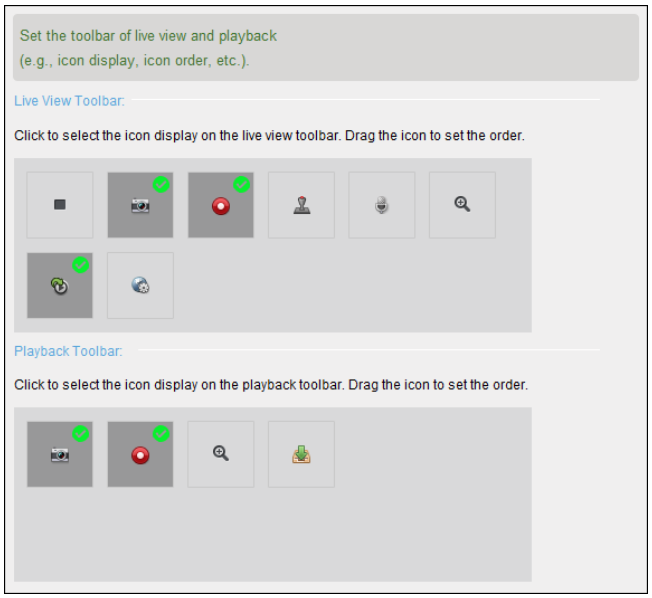
22.5 Toolbar Settings

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 and click **Toolbar** tab to enter the Toolbar Settings interface.



2. 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.

3. Click **Save**.

22.6 Keyboard and Joystick Shortcuts Settings

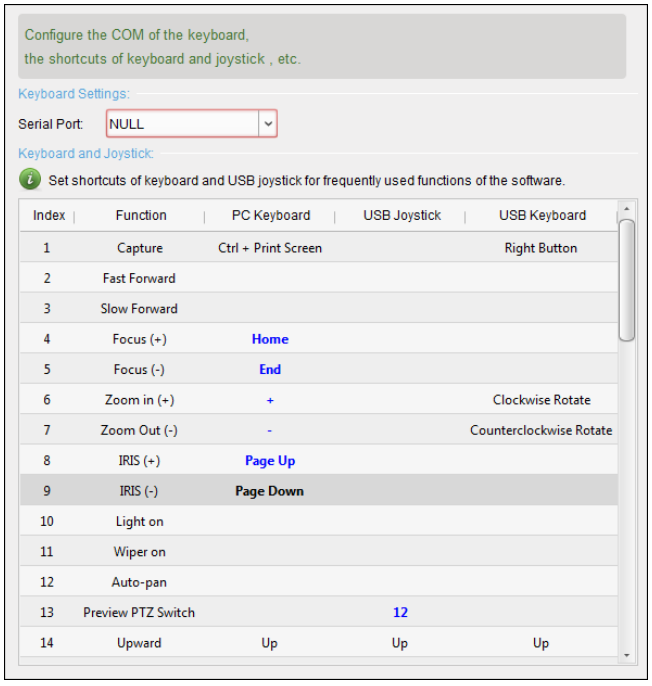
Purpose:

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.

Note: This configuration page will display after enabling keyboard and joystick in General Settings. For details, refer to *Chapter 22.1 General Settings.*

Steps:

1. Open the System Configuration page and click **Keyboard and Joystick** tab to enter the Keyboard and Joystick Shortcut Settings interface.



2. For keyboard: Select the COM port from the drop-down list if the keyboard is connected to the

PC installed with the client.

3. 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.
4. Click **Save**.

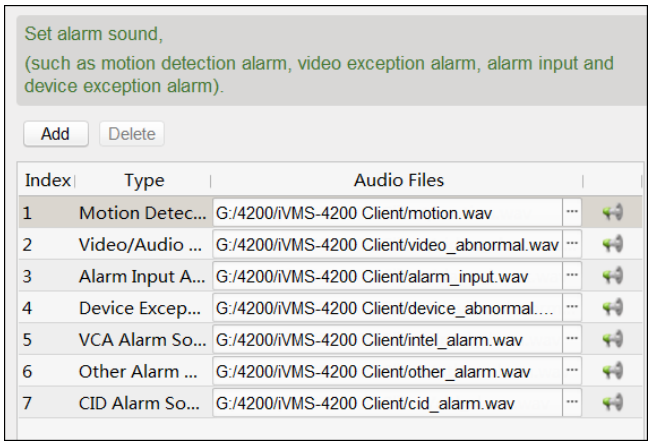
22.7 Alarm Sound Settings

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 and click **Alarm Sound** tab to enter the Alarm Sound Settings interface.



2. 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.
3. 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.
   

4. Optionally, you can click the icon  for a testing of the audio file.
5. You can select the added custom alarm sound and click **Delete** to delete it.
6. Click **Save**.

Note: The format of the audio file can only be *wav.

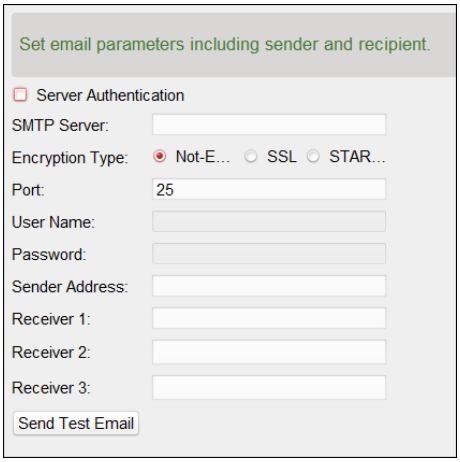
22.8 Email Settings

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 and click **Email** tab to enter the Email Settings interface.



2. 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.
   - **Encryption Type:** You can check the radio to select **Non-Encrypted**, **SSL**, or **STARTTLS.**
   - **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.
3. Optionally, you can check the checkbox **Enable SSL** to increase the security of email sending.
4. Optionally, you can click **Send Test Email** to send an email to the receiver for test.
5. Click **Save**.

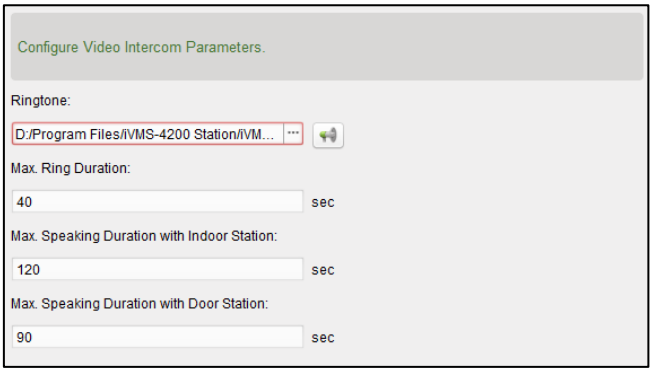
22.9 Video Intercom Settings

Purpose:

You can configure the video intercom parameters accordingly.

Steps:

1. Open the System Configuration page and click the **Video Intercom** tab to enter the Video Intercom Settings interface.



2. 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.

3. Click **Save**.

22.10 Access Control Settings

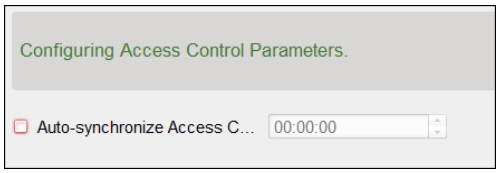
Purpose:

You can set the time so that the system will get the access control events which are not uploaded to the client from the access control device and save them to the client's database.

For Example: If the device is armed by another client B, the triggered events cannot be uploaded to the current client A during the arming period. When the client A arms the device again, you can synchronize these events from device to client A via this function.

Steps:

1. Open the System Configuration page and click **Access Control** tab to enter the Access Control Settings interface.



2. Check the **Auto-synchronize Access Control Event** checkbox to enable this function and set the time for synchronization.
3. Click **Save**.

22.11 Security Certificate

Purpose:

For the data security purpose, the security certificate of clients and added servers (stream media server) should be same.

As a result, before adding the stream media server to the client, you should export the service certificate stored in the client, and import it to the stream media server. If multiple clients use the same server, you should make the security certificates of the clients and the server same with each other.

22.11.1 Exporting Certificate from Client

Purpose:

You can export the security certificate from the current client and import the exported certificate file to the server or other clients.

Steps:

1. Open the System Configuration page and click **Security Certificate** tab to enter the security certificate interface.
2. Click **Export**.
3. Save the certificate file in the local PC.

   Note: The certificate file is in XML format.
4. Click **Save**.

After exporting the certificate, you can copy the certificate to the PC installed with the service and import it to the stream media server, or to other clients. For importing to the stream media server *Chapter 10.1 Importing Certificate to Stream Media Server.*

22.11.2 Import Certificate to Client

Purpose:

If there are multiple clients accessing the same server, you are required to import the same certificate to the clients and server.

Before you start:

You should export the security certificate from one of the client. For details, refer to *Chapter 22.11.1 Exporting Certificate from Client.*

Steps:

1. Copy the certificate file exported from other client to the local PC.
2. Open the System Configuration page and click **Security Certificate** tab to enter the security certificate interface.
3. Click **Import**.
4. Select the certificate file from your local PC.
5. Click **Save**.

   Note: You should restart the system to take effect.

Appendix: Custom Wiegand Rule Descriptions

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

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

Wiegand Data = Valid Data + Parity Data

Total Length: Wiegand data length.

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

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

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

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

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

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

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

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

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

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.**

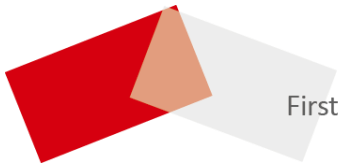
A: In the installation directory of the client software, open the **Setup.xml** file with Notepad and modify the value of **EnableNetandJoystickCheck** to **false**. Restart the client, and if the problem is still not solved, contact our technique support.

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
iVMS-4200		
317	No videos.	It will be prompted when the user has no permission to play back.
HCNetSDK.dll		
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.	
Playctrl.dll		
2		The stream is not a Video & Audio stream.
6		The playback window turns black when adopting H.265 in the 64-bit operating system.
SMS		
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

UD08250B